



UI PORTAL USER GUIDE

UltraDNS Managed Services Portal User Guide

This guide provides comprehensive step-by-step instructions on how to manage your DNS Records and Domains on the Neustar UltraDNS Portal.

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.

© 2019 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 requirement.

Table of Contents

Welcome!	1
Logging In	2
Logging in with Symantec Two Factor Authentication	2
Two Factor Mobile Authentication	3
SAML	8
Moving Around the UI	11
Navigation Pane	11
Domain Search Bar	11
Activity Report	12
Support and Account Details	12
Tasks	12
Domains	14
Managing Your Domains	14
Additional Domain Functions	20
Domain Filtering and Sorting	23
Permissions and Exceptions	25
Viewing your Domain	28
Records and Pools	41
Records	42
Pools	48
Available Records and Pool Types	53
A Records	55
AAAA Records	56
Resource Distribution Pool	57
SiteBacker Pool	60
Traffic Controller Pool	69
Simple Load Balancing Pool	73
Simple Monitor / Failover Pool	79
Directional Pool	85
CNAME Records	94
NS Records	95
PTR Records	96
HINFO Records	97
MX Records	98
TXT Records	99
RP Records	100
SRV Records	101
NAPTR Records	103
SPF Records	106
CAA Records	107
TLSA Records	109

Apex Alias Records	111
SSH Fingerprint	112
Delegation Signer	114
Web Forwarding	116
Reports	118
Usage Summary Report	118
Domain Alerts Report	119
Probe Statistics	120
Projected Query Volumes Report	125
Accounts	127
Users and Groups	128
SAML	137
Account Info	144
Exceptions	148
Notification Settings	151
TTL Settings	154
Directional Groups	156
Zone Transfer Settings	161
Audit	166
Service Status	167
My Profile	169
Contact Information	169
Security Preferences	170
News	173
Support	174
Support Center	174
Contact Neustar	174

Table of Figures

Figure 1 How to Log In	2
Figure 2 Two Factor Mobile Auth – Enable Step 1	4
Figure 3 Two Factor Mobile Auth – Enable Step 2	5
Figure 4 Two Factor Mobile Auth – Enable Step 3	5
Figure 5 Two Factor Mobile Auth - Log In.....	6
Figure 6 Two Factor Mobile Auth - Disable.....	6
Figure 7 SAML - Initial Setup Details	8
Figure 8 SAML - Map Users for SSO.....	9
Figure 9 SAML - Edit User Details	10
Figure 10 SAML - Confirm Mapping of Users	10
Figure 11 Dashboard Home Screen	11
Figure 12 Activity Report.....	12
Figure 13 Pending Task List	13
Figure 14 Domains - How to Create a Domain - Step 1	15
Figure 15 Domains - How to Create a Domain - Step 2	15
Figure 16 Domains - Creating a Primary Domain	16
Figure 17 Domains - Creating a Secondary Domain	17
Figure 18 Domains - Creating an Alias Domain.....	18
Figure 19 Domains - Delete a Domain.....	18
Figure 20 Domains - Export a Domain.....	19
Figure 21 Domains - Export a Domain Confirmation	19
Figure 22 Domains - Exporting a Domain Task and Download.....	20
Figure 23 Domain Features - Zone Transfer	21
Figure 24 Domain Features - Copy Domain	22
Figure 25 Domain Features - Load a Domain File.....	23
Figure 26 Domain Filtering and Sorting	24
Figure 27 Domains – Permissions and Exceptions - Setting Exceptions	26
Figure 28 Domains – Permissions and Exceptions - Exceptions Enabled	27
Figure 29 Domains - Permissions and Exceptions - Reset Permissions.....	28
Figure 30 Domains - Properties	29
Figure 31 Domains SOA Record - Edit Details.....	30
Figure 32 Domains DNSSEC - Sign a Zone	32
Figure 33 DNSSEC - Unsign a Zone	33
Figure 34 Domains - Zone Transfer Overview.....	33
Figure 35 Domains - Zone Transfer - Restrict IPs	34
Figure 36 Domains - Restrict IPs - Inherit Account Settings.....	35
Figure 37 Domains - Zone Transfer - Notify Addresses	36
Figure 38 Domains - Zone Transfer - TSIG Key	37
Figure 39 Domains - Create Snapshot	39
Figure 40 Domains - Restore a Snapshot.....	39
Figure 41 Domains - Delete a Snapshot.....	40
Figure 42 Records – Add a Record Step 1	42
Figure 43 Records – Add a Record Step 2	43
Figure 44 Records – Adding a Record Step 3	43
Figure 45 Records - Edit a Record	44

Figure 46 Records - Edit a Record Step 2	45
Figure 47 Records – How to Delete a Record	45
Figure 48 Records – How to Delete a Record Confirmation.....	46
Figure 49 Records - Sorting and Viewing options.....	46
Figure 50 Pools - How to Create a Pool	49
Figure 51 Pools - Pool Labels in the Record Section	49
Figure 52 Pools - Edit a Pool	50
Figure 53 Pools - Edit a Pool - Add a Record	51
Figure 54 Pools - Delete a Pool	52
Figure 55 Pools - Delete a Pool's Record(s).....	52
Figure 56 "A" Record Fields	55
Figure 57 "AAAA" Record Fields.....	56
Figure 58 Records - Create an RD Pool	57
Figure 59 Records - Editing a Resource Distribution Pool	58
Figure 60 Editing a Resource Distribution Pool Step 2.....	59
Figure 61 Sitebacker Pool - Create a Pool	60
Figure 62 Sitebacker Pool - Pool Information	61
Figure 63 Sitebacker Pool - Add New Record	62
Figure 64 Sitebacker Pool - Records List	63
Figure 65 Sitebacker Pool - Probe Definitions	64
Figure 66 Sitebacker Pool - Scheduled Events	67
Figure 67 Sitebacker Pool - Notifications.....	68
Figure 68 Sitebacker Pool – Alerts	68
Figure 69 Traffic Controller Pool - Create a Pool.....	69
Figure 70 Traffic Controller Pool - Pool Information	70
Figure 71 Traffic Controller Pool - Add TC Record.....	71
Figure 72 Traffic Controller Pool - Records List.....	72
Figure 73 Simple Load Balancing Pool - Create SLB Pool.....	74
Figure 74 Simple Load Balancing Pool - Records	75
Figure 75 Simple Load Balancing Pool - Information Details	77
Figure 76 Simple Load Balancing Pool - Probe Definition.....	78
Figure 77 Simple Failover Pool - Create a Pool.....	80
Figure 78 Simple Monitor / Failover Pool - Edit Pool Details	81
Figure 79 Simple Monitor / Failover Pool - Probe Definitions	82
Figure 80 Simple Monitor / Failover Pool - Manual Failover	83
Figure 81 Simple Monitor / Failover Pool - Undo Manual Failover	84
Figure 82 Directional Pool - Conflict Resolves To	86
Figure 83 Directional Pool - Create a Pool	87
Figure 84 Directional Pool - Pool Records.....	88
Figure 85 Directional Pool - Add Geolocation Record - Regions.....	89
Figure 86 Directional Pool - Add Geolocation Record - Countries	90
Figure 87 Directional Pool - Add Geolocation Record - Save.....	91
Figure 88 Directional Pool - Add SourceIP Record - Source Type.....	92
Figure 89 Directional Pool - Convert to Global Group	93
Figure 90 "CNAME" Record Fields	94
Figure 91 "NS" Record Fields	95
Figure 92 "PTR" Record Fields	96
Figure 93 "HINFO" Record Fields.....	97

Figure 94 "MX" Record Fields	98
Figure 95 "TXT" Record Fields	99
Figure 96 "RP" Record Fields	100
Figure 97 "SRV" Record Fields	102
Figure 98 "NAPTR" Record Fields	105
Figure 99 "SPF" Record Fields	106
Figure 100 "CAA" Record Fields	108
Figure 101 "TLSA" Record Fields	110
Figure 102 "Apex Alias" Record Fields	111
Figure 103 Create an SSH Fingerprint Record	113
Figure 104 Create a Delegation Signer Record	115
Figure 105 Create a Web Forwarding Record	117
Figure 106 Reports - Usage Summary Report	119
Figure 107 Reports - Domain Alerts	120
Figure 108 Probe Statistics Report - Simple Load Balancing or Simple Monitor / Failover	121
Figure 109 Probe Statistics Report - SLB and SM/SF - Probe Summary Results	121
Figure 110 Probe Statistics - Probe Details Report SLB and SM/SF	122
Figure 111 Probe Statistics Report - SiteBacker or Traffic Controller	124
Figure 112 Probe Statistics Report - SB or TC - Probe Summary Results	124
Figure 113 Probe Statistics - Probe Details Report SB or TC	125
Figure 114 Reports - Projected Query Volumes	126
Figure 115 Reports - PQV Report - Data Point Capture	126
Figure 116 Accounts Landing Page	127
Figure 122 Accounts – Users and Groups	128
Figure 123 Accounts – Users and Groups - Add Group	129
Figure 124 Accounts – Users and Groups - Invite User(s)	130
Figure 125 Accounts – Users and Groups - Moving a User	131
Figure 126 Accounts – User Groups - Moving a User cont.	131
Figure 127 Accounts – User Groups - Remove Access	132
Figure 128 Accounts – Users and Groups - Delete Group	133
Figure 129 Users and Groups - View Permissions	134
Figure 130 Users and Groups - Apply Permissions	135
Figure 131 Accounts - Users and Groups - Standalone User Permissions	136
Figure 132 Accounts - SAML Setup and Submit	138
Figure 133 Accounts - SAML - UltraDNS Users Details – NameID is Email	139
Figure 134 Accounts - SAML - UltraDNS Users Details - NameID is Username	140
Figure 135 SAML - Edit User Details - NameID is Email	141
Figure 136 SAML - Edit User Details - NameID is Username	141
Figure 137 SAML - Confirm Map Users	142
Figure 117 Accounts - Account Info	144
Figure 118 Accounts - Edit Primary User Address	145
Figure 119 Accounts - Change Primary User	146
Figure 120 Default SOA Contact Info	146
Figure 121 Accounts - Account Level Allowed IP Range	147
Figure 138 Accounts – Exceptions	149
Figure 139 Accounts - Edit an Exception	149
Figure 140 Accounts - Delete an Exception	150
Figure 141 Accounts - Notification Settings	151

Figure 142 Accounts - Notification Settings - Enabling DDOS Notifications	152
Figure 143 Accounts - Notification Settings - Enabling Zone Transfer Notifications	153
Figure 144 Accounts - TTL Settings	154
Figure 145 Accounts - Edit TTL Settings	155
Figure 146 Accounts - Directional Groups	156
Figure 147 Accounts - Add SourceIP Directional Group	157
Figure 148 Accounts - Add SourceIP Directional Group cont.....	158
Figure 149 Accounts - Add Geolocation Directional Group	159
Figure 150 Accounts - Zone Transfer Settings	161
Figure 151 Account - Zone Transfer Settings - IP Address Start/End	162
Figure 152 Accounts - Zone Transfer Settings - CIDR Notation.....	162
Figure 153 Accounts - Zone Transfer Settings - Single IP Address	163
Figure 154 Accounts - Zone Transfer Settings – Delete.....	163
Figure 155 Accounts - Add Notify Address	164
Figure 156 Accounts - TSIG Key	165
Figure 157 Service Status Dashboard - Current Status	167
Figure 158 Service Status Dashboard - Event History	168
Figure 159 My Profile	169
Figure 160 My Profile - Contact Information	170
Figure 161 My Profile - Security Preferences	171
Figure 162 My Profile - Security Preferences cont.	172
Figure 163 News - Landing Page	173
Figure 164 Support - Support Center.....	174
Figure 165 Support - Contact Neustar	175

Welcome!

Welcome to the UltraDNS Managed Services Portal (UI Portal), which you will use for managing your DNS Records and Domains information.

This guide is designed to be a “cookbook” type of User Guide, with the intent to make it easier for you to find and accomplish the tasks you are wanting to complete, without having to dig through pages of examples and reference material to do so. Each section starts with a “How To” to give you the basic understanding of what the action or section does on the UI, and why it might be important to you. Once you understand the basics, you can delve deeper into this guide for more case-by-case scenarios that may fit your needs.

As always, your feedback is immensely helpful in allowing us to better meet your needs, so please reach out to our Customer Support team with feedback at www.support.neustar, or 1.844.NSR.CUST (677.2878).

Logging In

Before you can begin to manage your domains and records, you need to log into the UltraDNS Management Portal (UI Portal).

For now, we are only providing one base URL to log into as we continue to finalize our portal and create a Customer Test Environment (where you can experiment without worrying about breaking anything).

The UI Portal can be reached at: <https://portal.ultradns.neustar>

Enter your **Username** and **Password**, and then click the **Login** button.

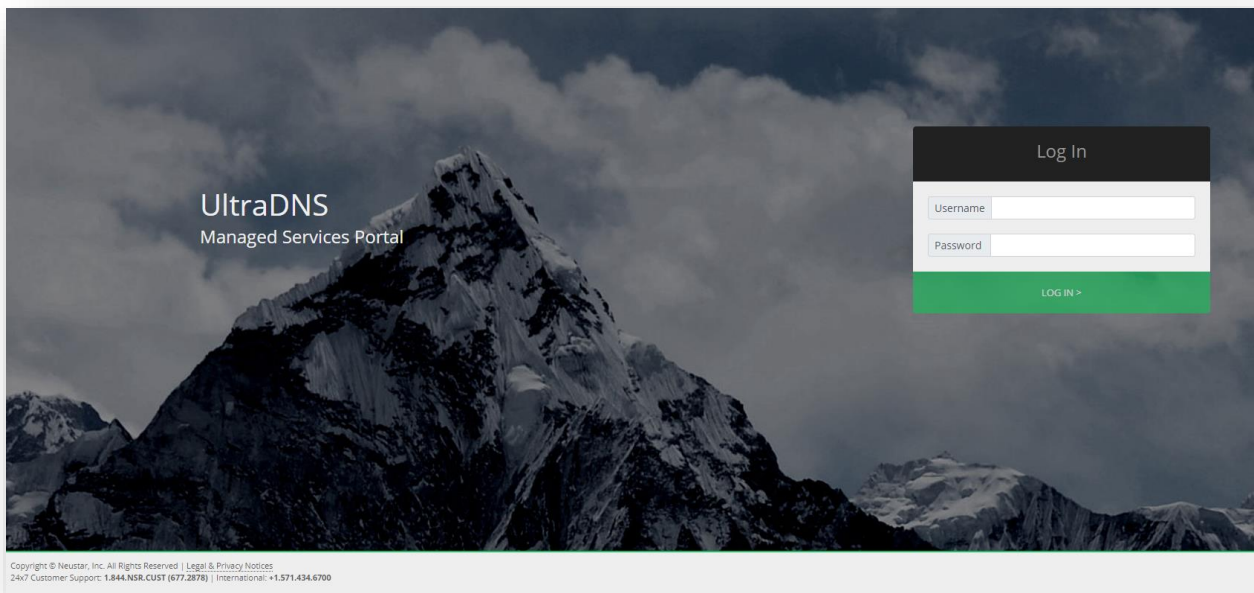


Figure 1 How to Log In

Logging in with Symantec Two Factor Authentication

For users that wish to log in using a **Symantec Two Factor Authentication** (2FA) device or tool, please follow the below steps:

1. Go to <https://idprotect.vip.symantec.com/mainmenu.v> and download/install for either Mobile or Desktop depending on your login method.
2. Once installed, contact UltraDNS Support at [1.844.NSR.CUST \(677.2878\)](tel:1844NSRCUST). You will need to provide your UserID for the UI Portal, along with your Credential ID.
3. UltraDNS Support will update your account, and send an email with a temporary password to log into the UI Portal.
4. Using the temporary password to log in, add your security code from your 2FA device to the end of your password to log in.

- a. Your password with security code will look as follows – {password}{security code}
5. Once you have logged in, you can navigate to the [My Profile](#) section of your account, and click on **Security Preferences**.
6. On the Security Preferences tab, create a new password of your choosing.
 - a. Password must be 6-32 characters long and include at least 3 of the following: an uppercase letter, a lowercase letter, a numeral, or a non-alphabetic character (such as !, \$, #, %). Spaces are not allowed.

Two Factor Mobile Authentication

For users that do not use the Symantec Two Factor Authentication for their account, we offer **Two Factor Mobile Authentication** as an alternative. When enabled, you will receive a six-digit verification code sent to your registered mobile device each time you attempt to log into your account. Once the code has been verified, you will be logged in and have full access to the UltraDNS Portal.



The Two Factor Mobile Authentication feature needs to be enabled at the account level first before it can be enabled per user / at the user level.

Enabling Two Factor Mobile Authentication

1. Once you are logged into the UltraDNS Portal, click the **My Profile** link in the upper right hand corner of the screen.
2. Verify that there is an accurate and up-to-date Mobile Number provided, as this will be the mobile number to which the verification code is sent to.
3. Click **Save**.



Make sure the Mobile Number field adheres to the required [E.164](#) (International Public Telecommunication Numbering plan) format. Do not include spaces or dashes in your mobile number.

The screenshot shows the 'My Profile' tab selected in a dark-themed interface. The 'Contact Information' section is active, displaying various input fields. The 'Mobile Number' field, containing '5512270854', is highlighted with a red border. Other fields include First Name (RajTEST), Last Name (Lastname), Primary Email, Secondary Email, Phone Number (5512270854), Fax Number (5712203241), Company Name (fsd), Address 1 (asis), Address 2 (ad444482), Country (United Kingdom), City (Weehawken), State/Province (MADHYA PRADESH PROVINCE), and ZIP Code (20147). 'Reset' and 'Save' buttons are located in the top right corner of the form area.

First Name:	RajTEST
Last Name:	Lastname
Primary Email:	@team.neustar
Secondary Email:	@team.neustar
Phone Number:	5512270854
Fax Number:	5712203241
Mobile Number:	5512270854
Company Name:	fsd
Address 1:	asis
Address 2:	ad444482
Country:	United Kingdom
City:	Weehawken
State/Province:	MADHYA PRADESH PROVINCE
ZIP Code:	20147

Figure 2 Two Factor Mobile Auth – Enable Step 1

4. Next, click the **Security Preferences** tab. In the Two Factor Authentication section, click on the drop-down menu and select **Enabled**.
 - a. An error message will appear if any of the following issues arise:
 - i. User has not provided the mobile number in the My Profile section.
 - ii. The Two Factor Mobile Authentication service is currently down.
 - iii. The Mobile Number provided is not in the correct format.

The screenshot shows a settings interface with three main sections: 'Inactivity Timeout' with a dropdown set to '5 minutes'; 'Password Expiration' with a dropdown set to '30'; and 'Two Factor Authentication' with a 'Mobile Authentication' dropdown set to 'Disabled'. A green bar highlights the 'Disabled' option. Below this, 'Account Level A' is set to 'Enabled'. 'Reset' and 'Save' buttons are present for each section. A 'No records found' message is at the bottom.

Figure 3 Two Factor Mobile Auth – Enable Step 2

5. Check your mobile device for a six-digit verification code, and then enter the number into the “Enter Verification Code” section.
6. Click the **Submit** button.

The screenshot shows the 'Two Factor Authentication' screen. A light blue notification banner at the top states: 'A new Verification Code has been sent to xxx-xxx-3667 per your request. If you do not receive the new code in 60 seconds, verify your mobile number and try again.' Below this, the 'Mobile Authentication' dropdown is now set to 'Enabled'. The 'Enter Verification Code:' field is empty and highlighted with a red border. 'Resend Verification Code (57)' and 'Submit' buttons are at the top right.

Figure 4 Two Factor Mobile Auth – Enable Step 3

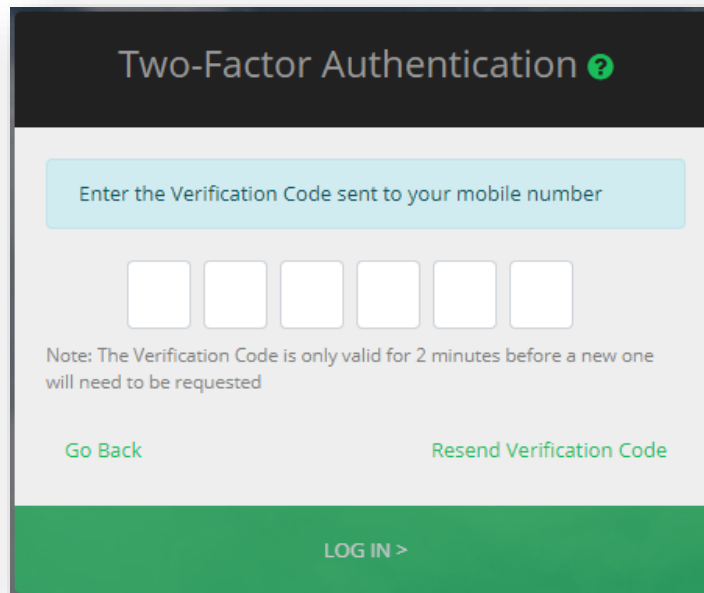
The Two Factor Mobile Authentication feature is now enabled! Any future login attempt will trigger a Verification Code to be sent to the mobile number, and the code will need to be provided.



The *Resend Verification Code* button is disabled until the 60 second counter has elapsed to prevent additional verification codes from being sent. If you receive multiple verification codes, use the most recent code received.

By default, the verification code is only valid for two minutes after being sent to a mobile device. If you do

not receive the initial verification code, or it has been accidentally deleted, click the **Resend Verification Code** button.

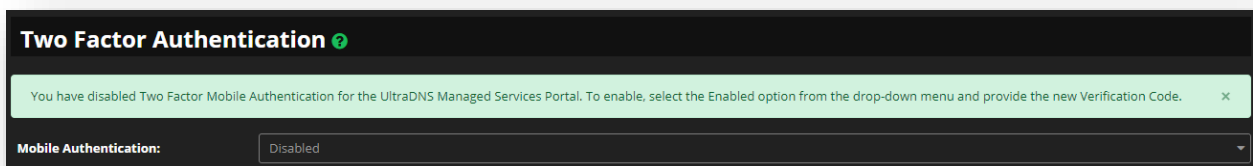


The image shows a mobile application screen titled "Two-Factor Authentication" with a green question mark icon. Below the title is a light blue instruction box: "Enter the Verification Code sent to your mobile number". Underneath are six white square input fields for the code. A note states: "Note: The Verification Code is only valid for 2 minutes before a new one will need to be requested". At the bottom of the form area are two green links: "Go Back" and "Resend Verification Code". A large green button at the very bottom says "LOG IN >".

Figure 5 Two Factor Mobile Auth - Log In

Disabling Two Factor Mobile Authentication

1. To disable Two Factor Mobile Authentication, click on the **My Profile** link in the upper right-hand corner of the screen.
2. Click on the **Security Preferences** tab.
3. In the Two Factor Authentication section, select the **Disabled** option from the drop-down menu.
 - a. You will receive a confirmation message that you have successfully disabled the Two Factor Mobile Authentication feature.



The image shows a settings screen titled "Two Factor Authentication" with a green question mark icon. A green confirmation message at the top reads: "You have disabled Two Factor Mobile Authentication for the UltraDNS Managed Services Portal. To enable, select the Enabled option from the drop-down menu and provide the new Verification Code." Below this is a section labeled "Mobile Authentication:" with a drop-down menu currently set to "Disabled".

Figure 6 Two Factor Mobile Auth - Disable

Customer Support

Customer Support can be reached at either 1-844-677-2878 or www.support.neustar.com.

Contact Customer Support for further assistance with any of the following issues:

- Invalid mobile phone number on the account.
- If you no longer have access to the mobile phone number provided in the My Profile section.
- If the mobile phone number provided is valid, but the verification code was never received.

SAML

Security Assertion Markup Language (SAML) provides the solution for providing both Authentication and Authorization services for Neustar customers. By sharing security credentials between customers and our Security Services team(s) at Neustar, we are able to transition your users' internal login credentials to a Neustar UltraDNS Managed Services Portal (UI Portal) username. Once successfully completed, we are able to create a Single Sign On (SSO) relationship between our services and systems.

We highly recommend you review the **SAML Quick Start Guide** to avoid any confusion or errors in your SAML request, as you will need to reach out to Customer Support for further assistance as your SAML details cannot be updated once they have been submitted.

Initiating SAML Setup

To submit a request to setup SAML from the UI Portal:

1. Click on **Accounts** from the left-hand navigation pane.
2. Click on your **Account Name**.
3. Click on **SAML** from the header options.

Accounts / Accounts / teamtest

Account Info Users and Groups **SAML** Notification Settings TTL Settings Zone Transfer Settings

Customer Contact Information ⓘ

Security Technical POC:

Security Technical POC Email:

Security Technical POC Phone:

Federation Related Information ⓘ

Neustar will be acting as the SP and will normally initiate the SAML authentication request to your IDP.

If your IDP supports IDP initiated SAML, provide the IDP initiated URL:

NameID Field:

Upload your SAML IDP XML Metadata: No file chosen

Neustar SAML Metadata URL:

DNS Related Information ⓘ

DNS URL for end-user access to Neustar when using single SAML login: .sso.security.neustar

Allow the owner of the account dual access (via SAML & via direct, non-SAML login): ☐

Figure 7 SAML - Initial Setup Details

4. Complete the required contact information and then click the **Submit** button.
 - a. The **NameID Field** allows you to determine if your users will be using their email address, or a designated UserID value to login.

5. Once submitted, verify your users' contact and login information by clicking on the **pencil icon** and updating their email address and/or their SSO login details.
 - a. For users that should no longer be on the UI portal, please use the **Delete Selected Users** button to remove them.

Accounts / Accounts / vcurz

Account Info Users and Groups **SAML** Notification Settings TTL Settings Zone Transfer Settings

SAML Information

Security Technical POC:	Admin Samluser	Security Technical POC Email:	ben.ackerman@team.neustar
Security Technical POC Phone:	1234567890	If your IDP supports IDP initiated SAML, provide the IDP initiated URL:	
NameID Field:	EMAIL	DNS URL for end-user access to Neustar when using single SAML login:	https://vcurz.sso.security.neustar

UltraDNS Users Details

— Delete Selected Users — Map Users for SSO

SAML mapping implementation is a two-step process. The first step requires you to *map your users*, and the second requires your users to log in via SSO for their new UDNS Usernames to take effect. Your current UltraDNS users' logins are listed below. Please complete the following actions before proceeding with the mapping of your users.

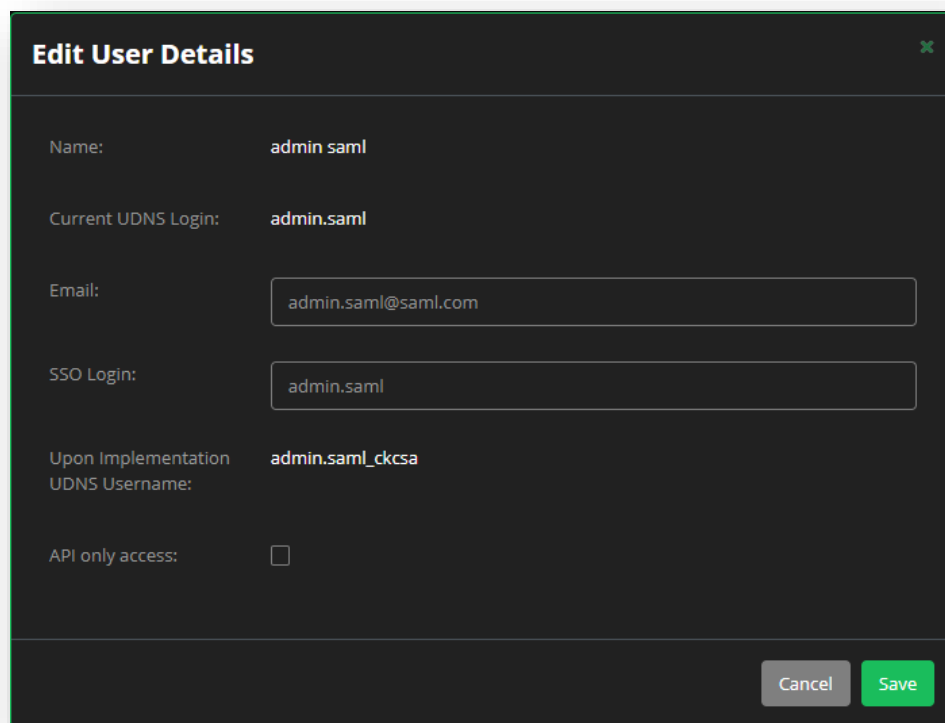
- **Delete Users** - Delete any users from the list that should no longer have access to the UI Portal or API.
 - *Warning - This process is irreversible, and the successful deletion of a user will remove them from the UI Portal completely.*
- **Edit Users** - Click the pencil icon next to each of your users to update their information if it is no longer accurate.

Once you have verified your users' details are correct, click the **Map Users for SSO** button to proceed.

<input type="checkbox"/>	Name	Current UDNS Login	Email	Upon Implementation UDNS Username	API Access Only
<input checked="" type="checkbox"/>	owner samluser	samluser.owner	samluser.owner@saml.com	samluser.owner@saml.com	<input type="checkbox"/>
<input checked="" type="checkbox"/>	delete samluser	samluser.delete	samluser.delete@saml.com	samluser.delete@saml.com	<input type="checkbox"/>
<input checked="" type="checkbox"/>	admin samluser	samluser.admin	samluser.admin@saml.com	samluser.admin@saml.com	<input type="checkbox"/>
<input checked="" type="checkbox"/>	tech samluser	samluser.tech	samluser.tech@saml.com	samluser.tech@saml.com	<input type="checkbox"/>
<input checked="" type="checkbox"/>	api samluser	samluser.api	samluser.api@saml.com	samluser.api@saml.com	<input type="checkbox"/>

Figure 8 SAML - Map Users for SSO

6. Once updated, click the **Map Users for SSO** button.



Edit User Details

Name: admin saml

Current UDNS Login: admin.saml

Email: admin.saml@saml.com

SSO Login: admin.saml

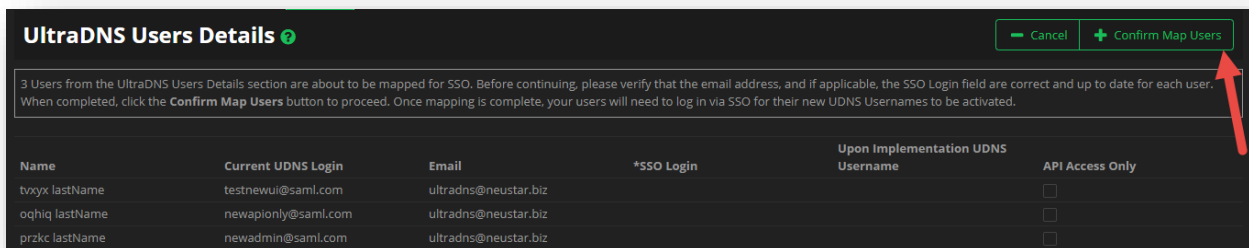
Upon Implementation UDNS Username: admin.saml_cksa

API only access: ☐

Cancel Save

Figure 9 SAML - Edit User Details

7. Confirm you have setup all of the required users for SAML, and then click the **Confirm Map Users** button.



UltraDNS Users Details

3 Users from the UltraDNS Users Details section are about to be mapped for SSO. Before continuing, please verify that the email address, and if applicable, the SSO Login field are correct and up to date for each user. When completed, click the **Confirm Map Users** button to proceed. Once mapping is complete, your users will need to log in via SSO for their new UDNS Usernames to be activated.

Name	Current UDNS Login	Email	*SSO Login	Upon Implementation UDNS Username	API Access Only
tvxyx lastName	testnewui@saml.com	ultradns@neustar.biz			<input type="checkbox"/>
oqhiq lastName	newapionly@saml.com	ultradns@neustar.biz			<input type="checkbox"/>
przkc lastName	newadmin@saml.com	ultradns@neustar.biz			<input type="checkbox"/>

Cancel Confirm Map Users

Figure 10 SAML - Confirm Mapping of Users

8. Once your users log in with their SSO login credentials, the SAML process will be complete.

Moving Around the UI

The UltraDNS Managed Services (UI) Portal has been designed for quick and easy navigation, so that you don't waste time navigating through needless trickle down screens to get the section(s) that you need to. The following image shows the breakdown of the basic navigation principles, as well as the key sections of your account once you are logged in.

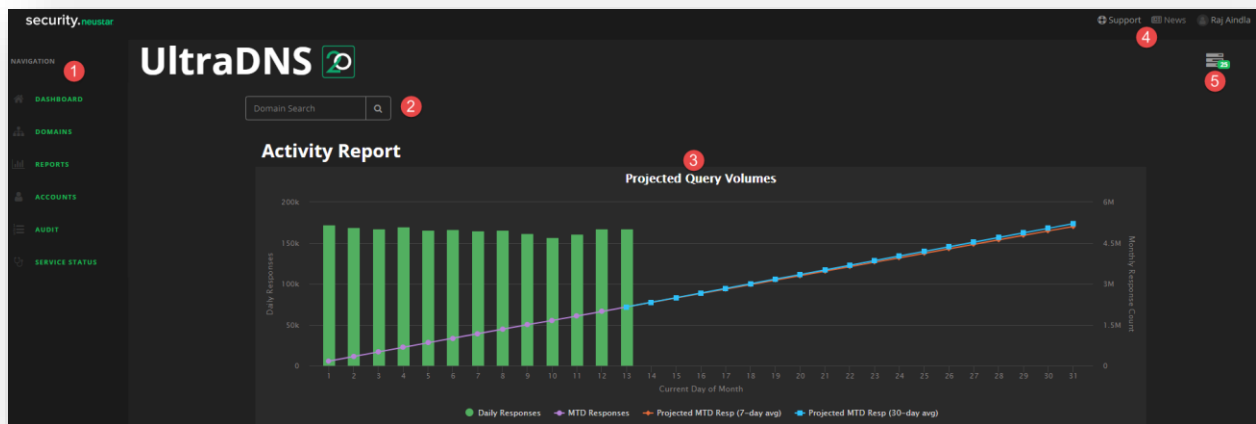


Figure 11 Dashboard Home Screen

1. *Navigation Pane*
2. *Domain Search Bar*
3. *Activity Report*
4. *Support and Account Details*
5. *Tasks*

Navigation Pane

Whether you just logged into the UI or have been navigating through different sections, the left-hand navigation panel is your guide through the UI. Click on each section to begin exploring all the features and management that the UI Portal allows you.

Domain Search Bar

The Domain Search Bar allows you to search for a specific domain name without having to search through a slew of Domains on the **Domains** page. When you type in the domain name, a wildcard search automatically returns the possible matches for your search criteria. Click on the desired domain name, and then click the **magnifying glass** to navigate to the domain's page.

Activity Report

The Activity Report displays the Projected Query Volumes report for the month, for your account. The graph displays the average Time to Live (TTL) values along with the Daily Query Response time on the UI. You can hover over a point on the chart to get additional details.

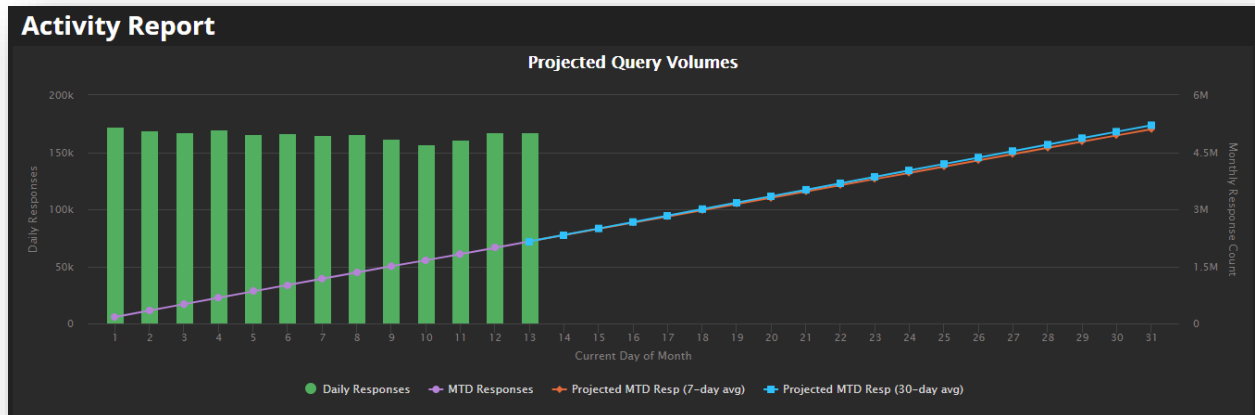


Figure 12 Activity Report

Support and Account Details

Clicking the **Support** link gives you the option of navigating to either the [Support Center](#), or directly to Neustar's Contact Us home page at <https://www.home.neustar/contact-us>.

Click the **My Profile** link to open your account's profile details, as well as display the Security Preferences tab.

Tasks

The Pending Tasks icon displays the list of items that are generated by actions that occur when you are logged into your account.

Some examples of actions that will create a task are:

- Deleting a record or a zone
- Creating a Primary Zone via Zone Transfer
- Creating a Secondary Zone
- Exporting a zone's details

When you click on the Tasks icon, a list showing the description of each item that triggered a task will appear. You can delete individual tasks by clicking the X icon next to the task description, or you can click the **Clear All** link to delete all the current tasks.

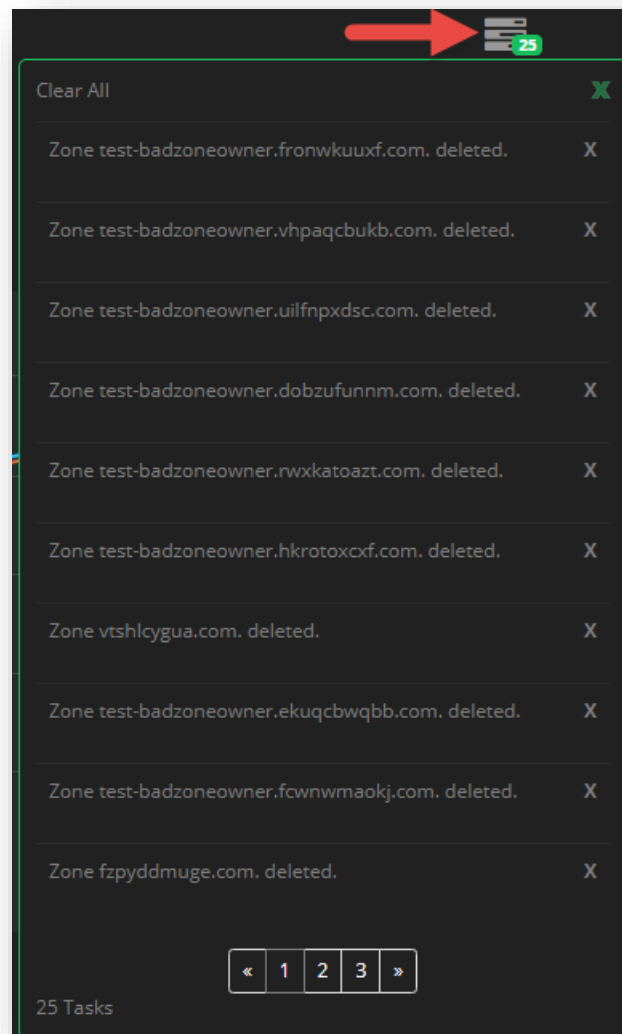


Figure 13 Pending Task List

Domains

The Domains section of the UI Portal displays all of the domains that you have created or transferred to Neustar's UltraDNS Managed Services. These domains can be any of the following types:

- **Primary** - A domain that is managed by Neustar UltraDNS.
- **Secondary** - A domain that is managed by Neustar, but obtains its data from a primary name server that is managed by another entity.
- **Alias** - A domain that points to (is an alias for) a parent domain. The parent domain must be an existing primary domain.

For our Secondary Users, you will only be able to create Secondary Domains on the UI Portal, and will have limited access to various aspects of the Portal.



If your Domain displays Suspended as the Type, please contact Support for additional assistance.

Managing Your Domains

Creating a Domain

If you want to create a new domain on the UI Portal:

1. Click on the **Domains** section from the navigation pane.
2. Click the **Add Domain** button.

UltraDNS

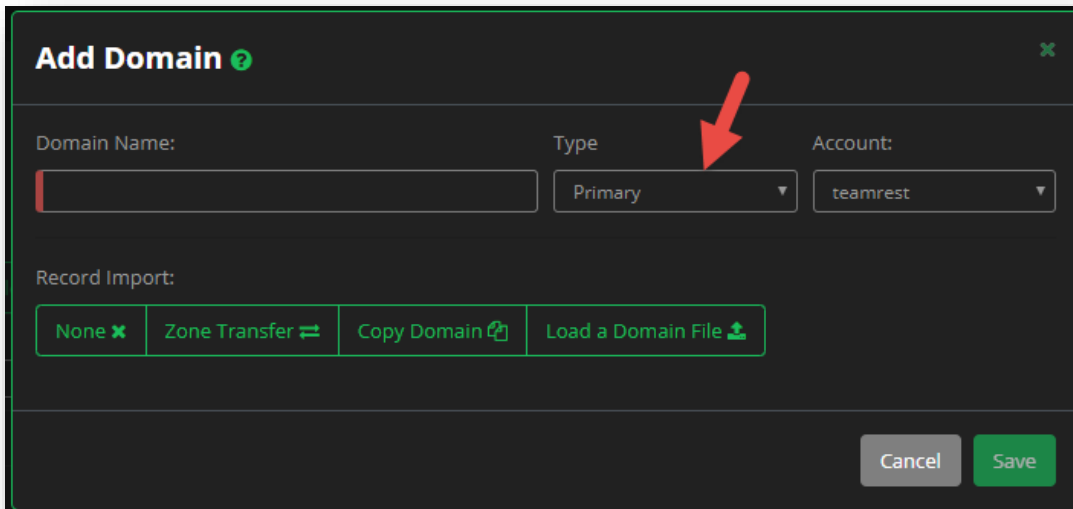
Domains ? / Domains

+ Add Domain Delete Selected Export

Domain	Type	# Recs	Account	DNSSEC Status	Perms
0-1acopy.com	PRIMARY	99	teamrest	🔒	🔑
0-1simple.com	PRIMARY	1064	teamrest	🔒	🔑
0-a-rectypes.com	PRIMARY	135	teamrest	🔒	🔑
0-a-rectypes2.com	PRIMARY	23	teamrest	🔒	🔑
0-a-rectypescopy.com	PRIMARY	31	teamrest	🔒	🔑
0-a-signme.com	PRIMARY	16	teamrest	🔒	🔑
0-a1.com	PRIMARY	10045	teamrest	🔒	🔑
0-ankit-dir-test.com	PRIMARY	10	teamrest	🔒	🔑
0-ankit-test-sign.com	PRIMARY	12	teamrest	🔒	🔑
0-ankit1.com	PRIMARY	166	teamrest	🔒	🔑
0-ankit222.com	PRIMARY	39	teamrest	🔒	🔑
0-copy001.com	PRIMARY	10009	teamrest	🔒	🔑
0-copy.com	PRIMARY	139	teamrest	🔒	🔑
0-copydomain.com	PRIMARY	10009	teamrest	🔒	🔑
00-1-rr-list.com	PRIMARY	14	teamrest	🔒	🔑

Figure 14 Domains - How to Create a Domain - Step 1

3. Enter the Domain Name. The format must match either of the following:
 - a. *Example.com*
 - b. *Example.com.* (with a trailing dot)
4. Select the **Type** from the drop-down menu.
 - a. **Primary** - A domain that is managed by Neustar UltraDNS.
 - b. **Secondary** - A domain that is managed by Neustar, but obtains its data from a primary name server that is managed by another entity.
 - c. **Alias** - A domain that points to (is an alias for) a parent domain. The parent domain must be an existing primary domain.

**Figure 15 Domains - How to Create a Domain - Step 2**

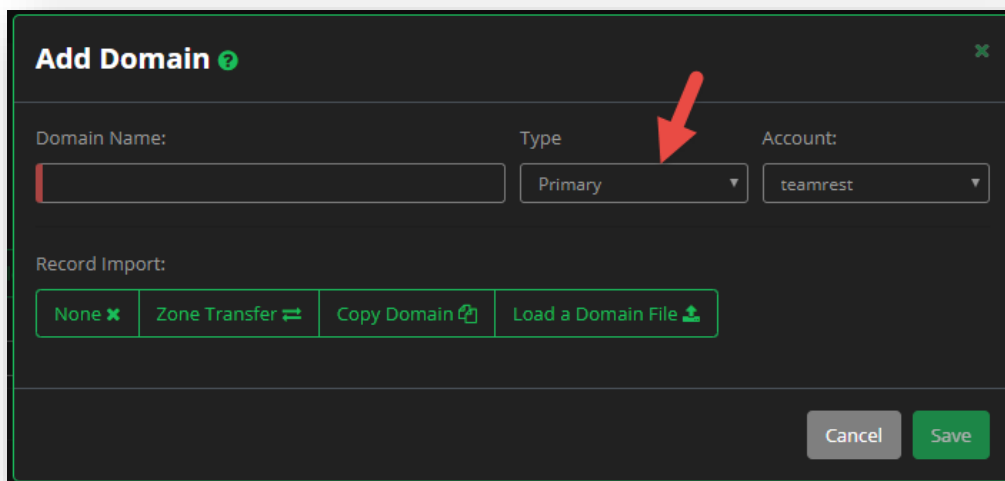
5. If you have multiple accounts, select the **Account** from the drop-down menu that the domain should be associated with.
6. If you want to perform one the **Record Import** functions, click on the feature below.
 - a. *Zone Transfer*
 - b. *Copy Domain*
 - c. *Load a Domain File*
7. Once you have provided all the required details, click **Save Changes**.

For additional details about various types of Domains you can create, or different ways you can provide records, go to the [How to Export a Domain](#) section of this guide.

Creating a Primary Domain

A Primary domain is managed by Neustar UltraDNS. If you want to create a Primary Domain:

1. Click the **Add Domain** button.
2. Ensure that **Primary** is selected in the **Type** drop-down menu. (*Primary* is selected by default.)
3. Select an option for **Record Import** (*Additional Domain Functions*) if you have existing Domains or Records you wish to add to this Domain.
4. Click **Save** when finished.



The screenshot shows a dark-themed 'Add Domain' dialog box. At the top, it says 'Add Domain' with a green question mark icon. Below this are three fields: 'Domain Name:' with an empty text input, 'Type' with a dropdown menu showing 'Primary' (highlighted by a red arrow), and 'Account:' with a dropdown menu showing 'teamrest'. Below these is a 'Record Import:' section with four buttons: 'None' (with a close icon), 'Zone Transfer' (with a double-headed arrow icon), 'Copy Domain' (with a document icon), and 'Load a Domain File' (with a download icon). At the bottom right are 'Cancel' and 'Save' buttons, with 'Save' being green.

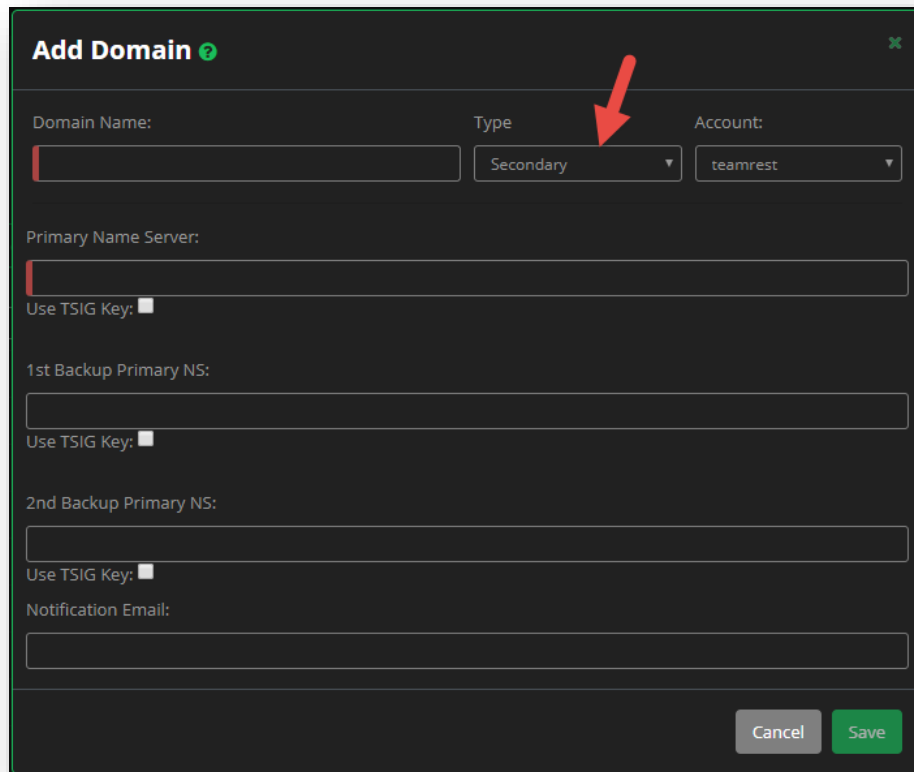
Figure 16 Domains - Creating a Primary Domain

Creating a Secondary Domain

A secondary domain contains data managed on a name server outside of the Neustar UltraDNS network. The secondary domain is transferred and updated via zone transfers into the UltraDNS system. You must modify your primary nameserver allow-transfer ACLs and firewall security policies for DNS to include the ten (10) IP addresses listed below. This is the set of IP addresses that will request zone transfers from your primary nameserver(s) for the Neustar secondary domains.

If you want to create a Secondary Domain instead of the default Primary Domain, change the **Type** from the drop-down menu.

As you can see, Secondary Domains provide the capability to use TSIG keys as an additional layer of security for your Name Server, as well as the Backup Name Server(s) if you choose to add them.



Add Domain ⓘ

Domain Name: Type: **Secondary** Account: **teamrest**

Primary Name Server:

Use TSIG Key: ☐

1st Backup Primary NS:

Use TSIG Key: ☐

2nd Backup Primary NS:

Use TSIG Key: ☐

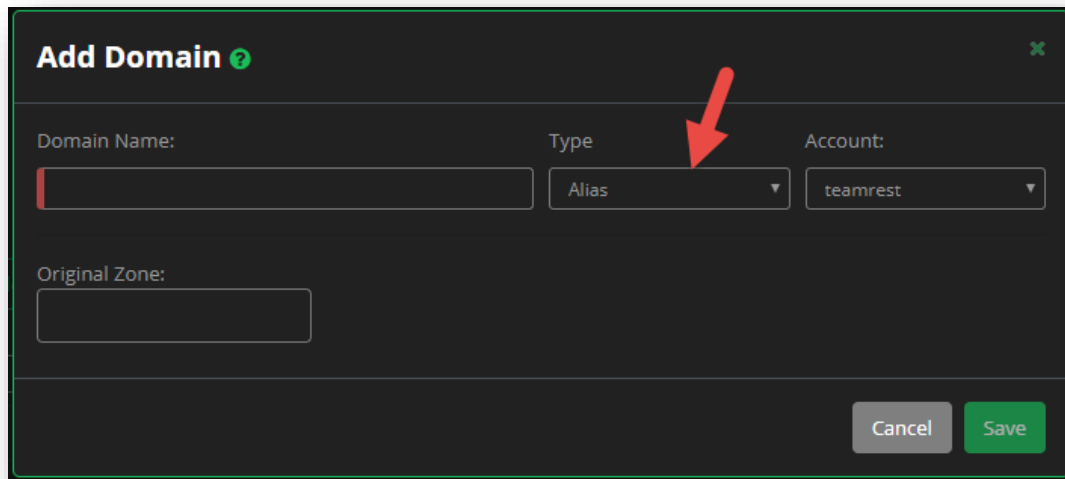
Notification Email:

Figure 17 Domains - Creating a Secondary Domain

Creating an Alias Domain

An Alias domain is one that points to (is an alias for) a parent domain. The parent domain must be an existing primary domain on the UltraDNS UI Portal.

If you need to create an Alias domain, change the **Type** drop-down menu to **Alias**. Then provide the Original Zone name and click the **Save** button.

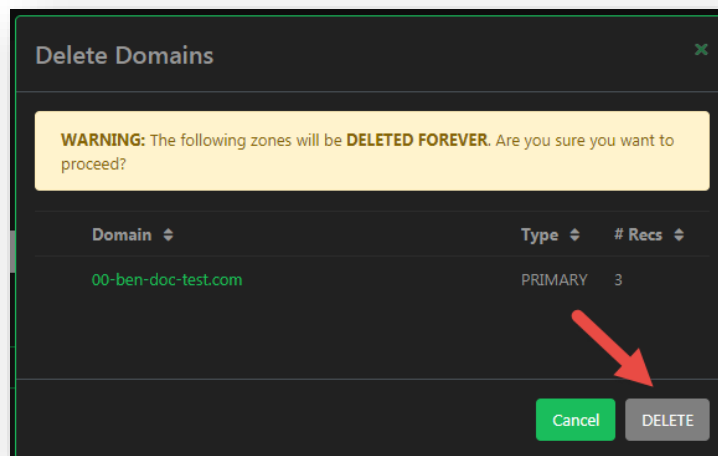


The 'Add Domain' dialog box features a title bar with a question mark icon. It contains three input fields: 'Domain Name:' with a red vertical bar on the left, 'Type' with a dropdown menu showing 'Alias', and 'Account:' with a dropdown menu showing 'teamrest'. Below these is an 'Original Zone:' input field. At the bottom right are 'Cancel' and 'Save' buttons. A red arrow points to the 'Type' dropdown menu.

Figure 18 Domains - Creating an Alias Domain

How to Delete a Domain

Click in the checkbox next to your domain, and then click **Delete Selected**. You'll see from the message, that clicking the **DELETE** button will permanently delete your domain from our system. Please ensure that deleting the domain is the necessary course of action before continuing.



The 'Delete Domains' dialog box has a title bar with a close icon. A yellow warning box at the top states: 'WARNING: The following zones will be DELETED FOREVER. Are you sure you want to proceed?'. Below is a table with columns 'Domain', 'Type', and '# Recs'. The table contains one row: '00-ben-doc-test.com', 'PRIMARY', and '3'. At the bottom right are 'Cancel' and 'DELETE' buttons. A red arrow points to the 'DELETE' button.

Domain	Type	# Recs
00-ben-doc-test.com	PRIMARY	3

Figure 19 Domains - Delete a Domain

How to Export a Domain

To export the details of a domain to plain a text file:

1. Click **Domains** from the navigation pane.
2. Click in the **check box** for the desired Domain.
3. Click the **Export** button.

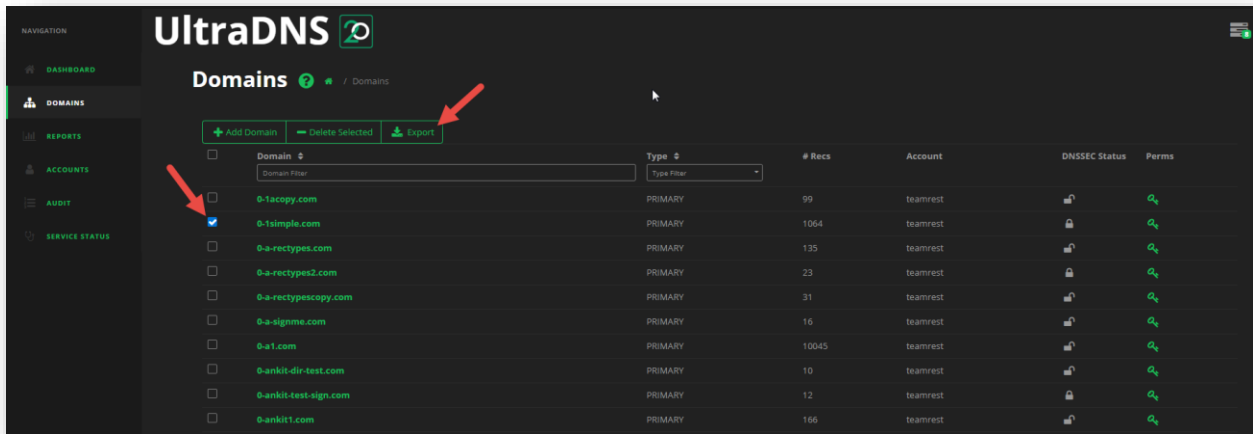


Figure 20 Domains - Export a Domain

4. The confirmation window will open, displaying the Domain Name, the Type of domain, and the number of Records in the domain.

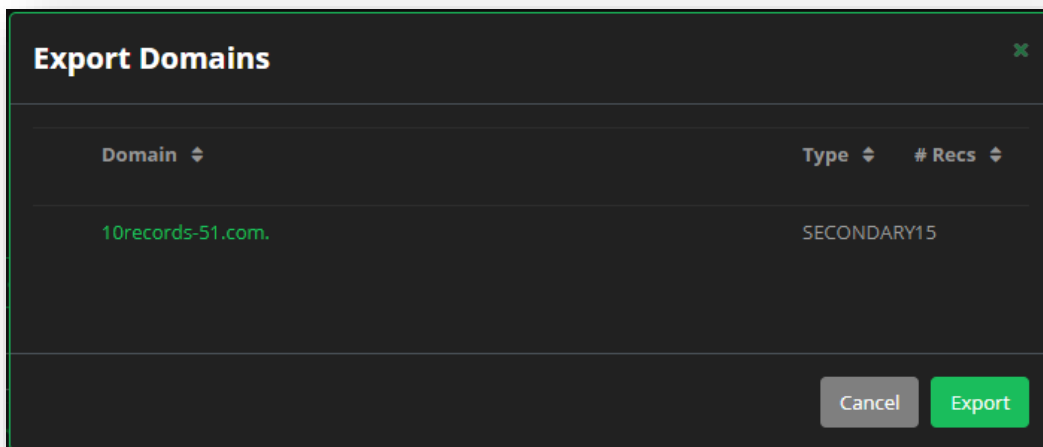


Figure 21 Domains - Export a Domain Confirmation

5. Click the **Export** again to begin the export of the domain.
6. You can check the progress of the export by clicking on the **Tasks** icon.

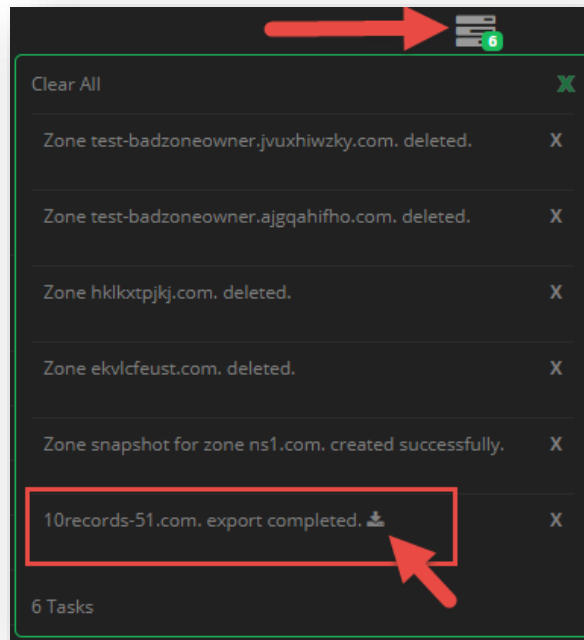


Figure 22 Domains - Exporting a Domain Task and Download

Additional Domain Functions

This section provides alternative methods to creating Domains beyond manually creating them. Additionally, this section also addresses different filtering and sorting features that are helpful to narrowing down your Domain search results.

The following features are only available for Primary Domains.

Zone Transfer

The Zone Transfer function initiates a zone transfer from a name server that contains your domain's data. The current name server must allow zone transfers to the Neustar servers at the following IP addresses. *(Also send DNS NOTIFY and allow TSIG zone transfers to the same IP addresses.)*

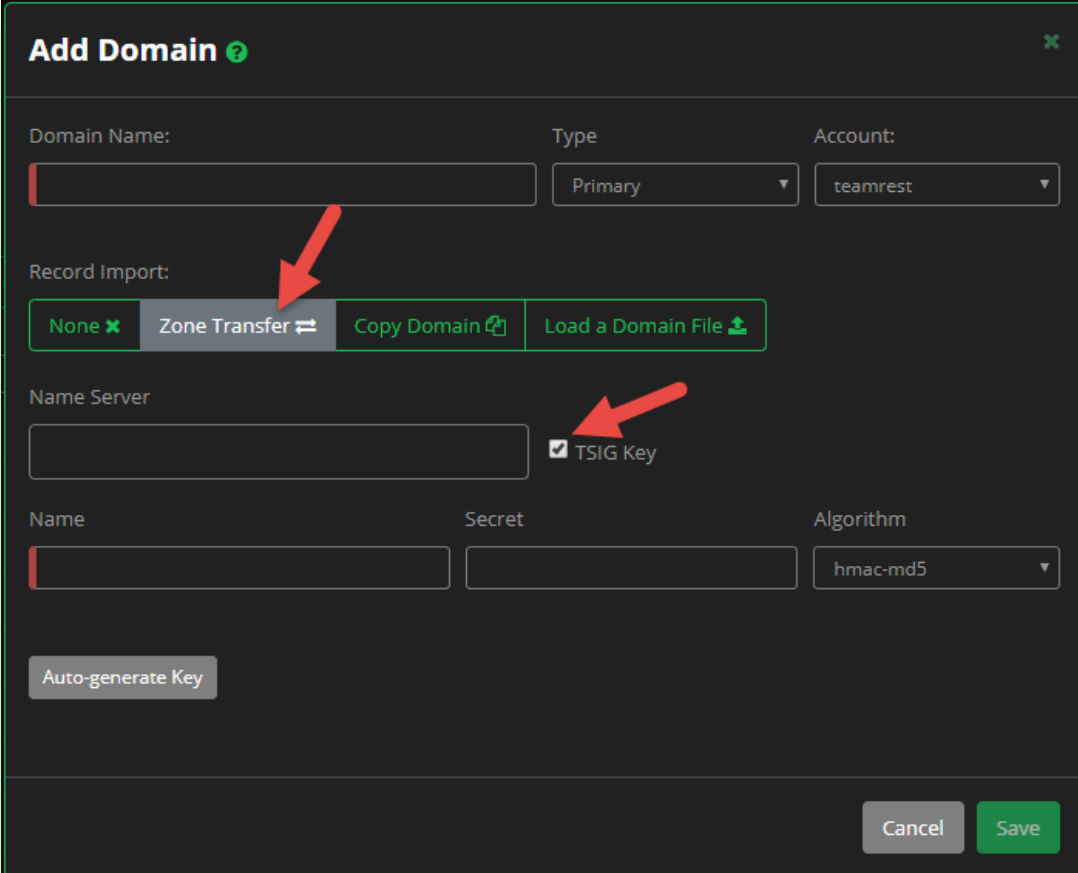
Allow Transfer

- 23.21.200.163
- 23.21.206.251
- 50.112.240.144
- 50.112.240.145
- 54.75.253.83
- 176.34.183.208

Also Notify

- 54.217.202.161
- 107.21.214.87
- 54.245.253.13

After clicking the **Add Domain** button from the Domains home screen, select **Zone Transfer**. You can provide your TSIG Key information, check the box, and your zone information will transfer automatically into the new domain you are creating.



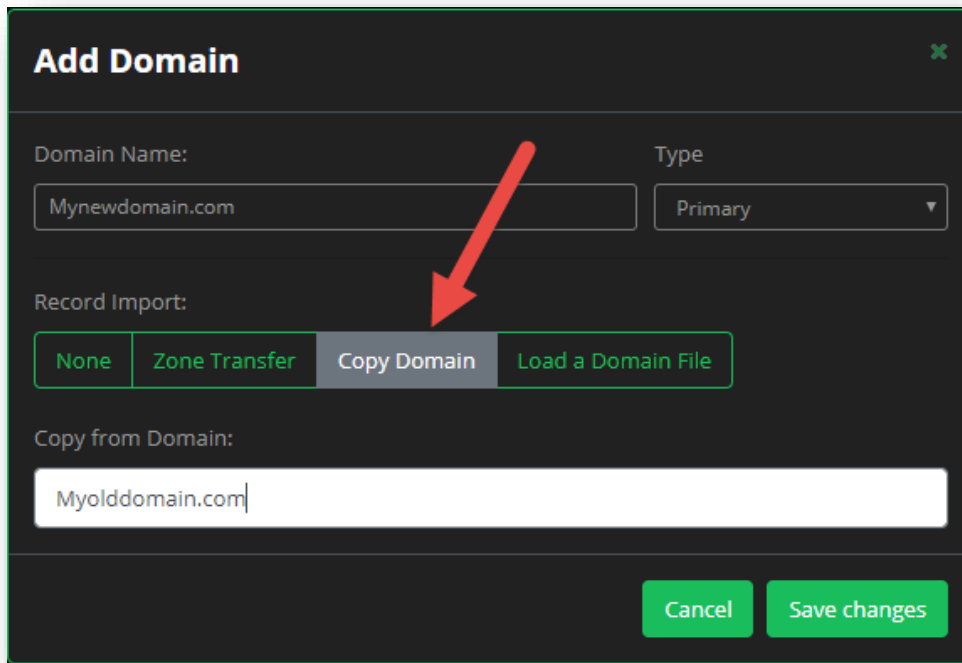
The screenshot shows the 'Add Domain' dialog box with the following fields and options:

- Domain Name:** A text input field.
- Type:** A dropdown menu with 'Primary' selected.
- Account:** A dropdown menu with 'teamrest' selected.
- Record Import:** A row of buttons: 'None' (with a close icon), 'Zone Transfer' (highlighted with a red arrow), 'Copy Domain' (with a copy icon), and 'Load a Domain File' (with a download icon).
- Name Server:** A text input field.
- TSIG Key:** A checkbox that is checked, with a red arrow pointing to it.
- Name:** A text input field.
- Secret:** A text input field.
- Algorithm:** A dropdown menu with 'hmac-md5' selected.
- Auto-generate Key:** A button.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

Figure 23 Domain Features - Zone Transfer

Copy Domain

Another option is to create a new domain by copying the records in an existing domain currently on the UI Portal. When creating a domain, click the **Copy Domain** button, and then provide the name of the domain to copy, and then click the **Save Changes** button.



The screenshot shows the 'Add Domain' dialog box. It has a title bar with 'Add Domain' and a close button. The form contains the following fields and controls:

- Domain Name:** A text input field containing 'Mynewdomain.com'.
- Type:** A dropdown menu showing 'Primary'.
- Record Import:** A row of four buttons: 'None', 'Zone Transfer', 'Copy Domain' (highlighted with a red arrow), and 'Load a Domain File'.
- Copy from Domain:** A text input field containing 'Myolddomain.com'.
- Buttons:** 'Cancel' and 'Save changes' at the bottom right.

Figure 24 Domain Features - Copy Domain

Load a Domain File

The **Load a Domain** option allows you two different ways to use an existing domain to create your new domain. You can either:

1. Upload a standard BIND formatted file by clicking the **Choose File** button.

OR

2. Copy and paste your BIND text into the empty text box.

The following is an example of a BIND file:

```
$TTL 86400

$ORIGIN example.com.
@ 1D IN SOA ns1.example-zone.com. hostmaster.example-zone.com.

(
  2002022401 ; serial
  3H ; refresh
  15 ; retry
  1w ; expire
  3h ; minimum
)
```

```
IN NS ns1.example.com. ; in the domain
IN NS ns2.anotherexample.com. ; external to domain
IN MX 10 mail.another.com. ; external mail provider
ns1 IN A 192.168.0.1 ; name server definition
www IN A 192.168.0.2 ; web server definition
ftp IN CNAME www.example.com. ; ftp server definition
host1 IN A 192.168.0.3
host2 IN A 192.168.0.4

srvce.prot.name ttl class rr pri weight port target
_http._tcp.example.com. IN SRV 0 5 80 www.example.com.
```

Add Domain

Domain Name: Type: Primary Account: teamrest

Record Import:

None Zone Transfer Copy Domain Load a Domain File

Choose File No file chosen

1

OR

Enter BIND Text into text field

2

Notice: System will not process following resource records types: DLV, DNSKEY, DS, NSEC, NSEC3, NSEC3PARAM, RRSIG

Cancel Save

Figure 25 Domain Features - Load a Domain File

Domain Filtering and Sorting

Each domain entry on the Domains home page will display the following details:

- **Domain Name**
- **Type** - The type of Domain.

- **# Recs** - The number of records in the Domain.
- **Account** - The account name that the Domain is assigned to.
- **DNSSEC Status** - Either Signed (locked) or Un-signed (unlocked).

You can sort the list of domains in either ascending or descending order by clicking on the up or down arrow in the domain name search bar.

You can also filter domains by using the **Type Filter** drop-down menu, and select a domain type to organize the list of displayed domains.

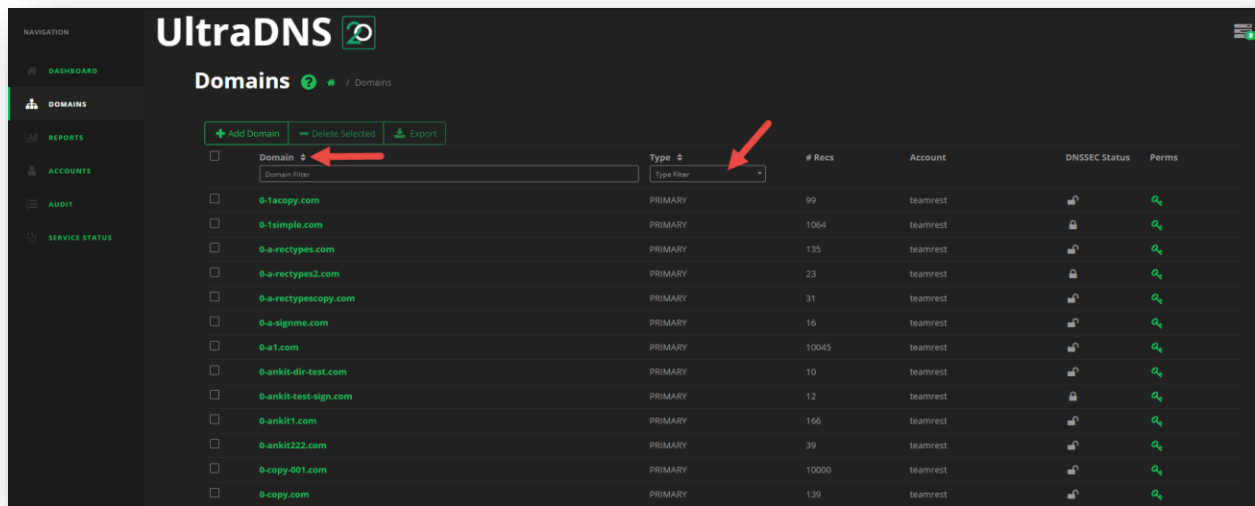


Figure 26 Domain Filtering and Sorting

Permissions and Exceptions

You can view the Permissions that all of the configured *Users and Groups* have for your domain by clicking the green Key icon underneath the **Perms** column header.

Exceptions provide a customized permission for a specific **Object** (i.e. domain, record) on the UI Portal. Normally, permissions apply to all **Object Types** (i.e. Zone, Account, Report) once they are set, but the exception allows you to set a specific permission level for an object.

For example, if you created **Group A** in the Users and Groups section, and gave all the users in Group the permission level of READ WRITE for all Domains, but there is a specific domain name that you want them to only have READ access for, you would create an exception for that domain name.

Creating an Exception

To create an exception for a Domain:

1. Find your desired Domain name from the Domains list, and then click the green **Key** icon under the **Perms** heading.
2. The Permissions window displays all of the currently configured groups and standalone users, along with the permission level that each has for the specified domain.
3. Use the slider bar to set the desired permission level for each group or user for the current domain.
 - a. Standalone users (users not assigned to a group) will appear on the very last page of the Groups list.

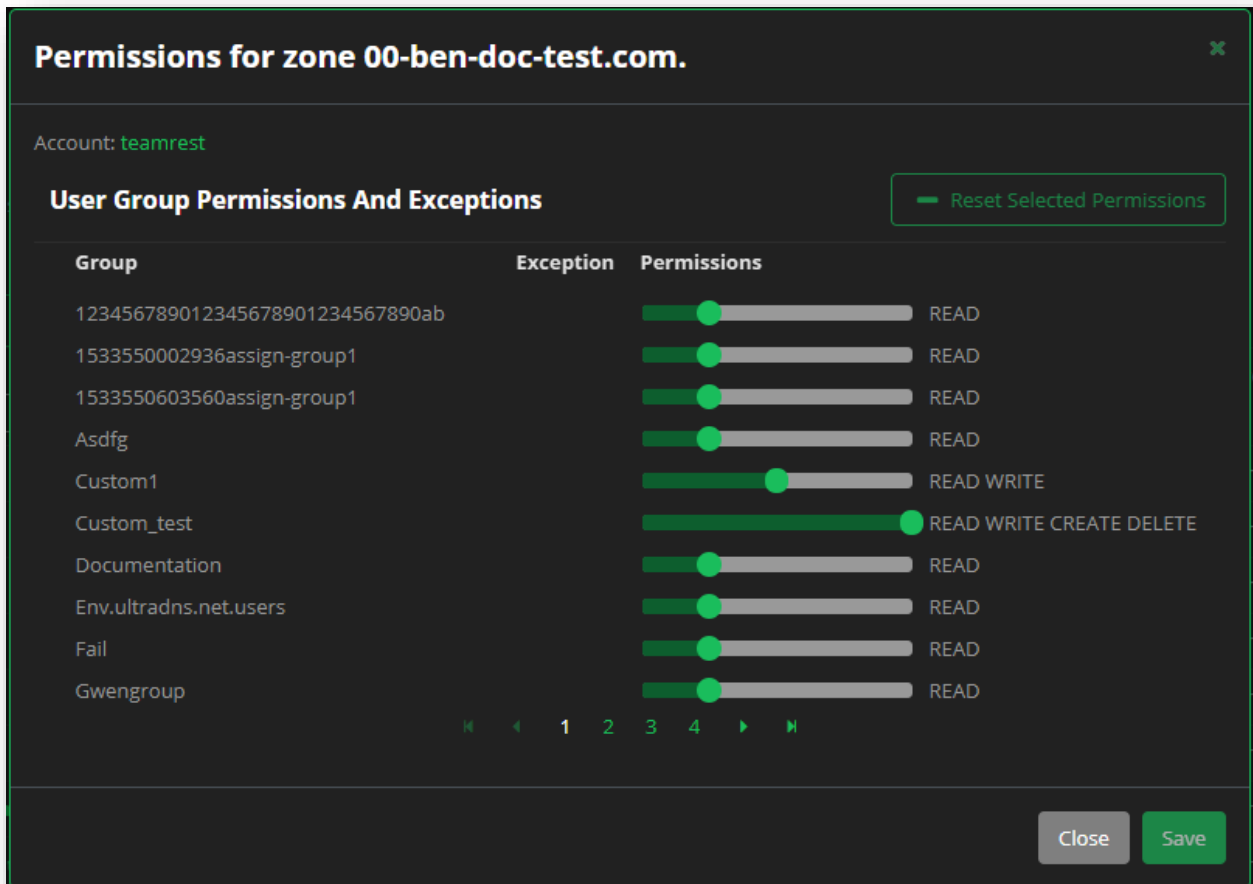


Figure 27 Domains – Permissions and Exceptions - Setting Exceptions

- Once you have set all of the new permissions for the desired groups / users, click the **Save** button.
- Each group or user that had their permission changed will have a checkbox next to their name, as well as a green arrow under the Exceptions header, indicating that an exception is currently in place for the specified domain (object).

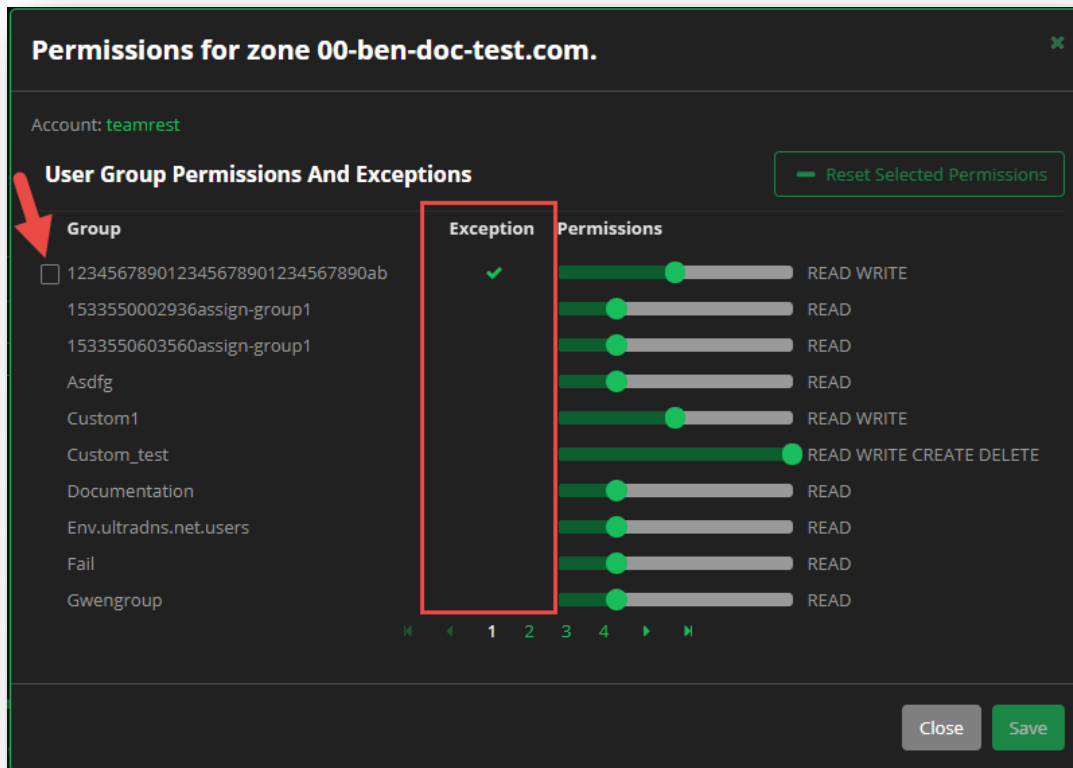


Figure 28 Domains – Permissions and Exceptions - Exceptions Enabled

Resetting Permissions and Exceptions

Once an exception has been created for a group, you can either reset the permission from the specific domain, or delete it from the **Accounts** section.

To reset an exception to a Domain:

1. Click the green **Key** icon next to the domain that has the exceptions set.
2. Click into the checkbox for each Group or User you want to reset the permissions for.
3. Click the **Reset Selected Permissions** button.

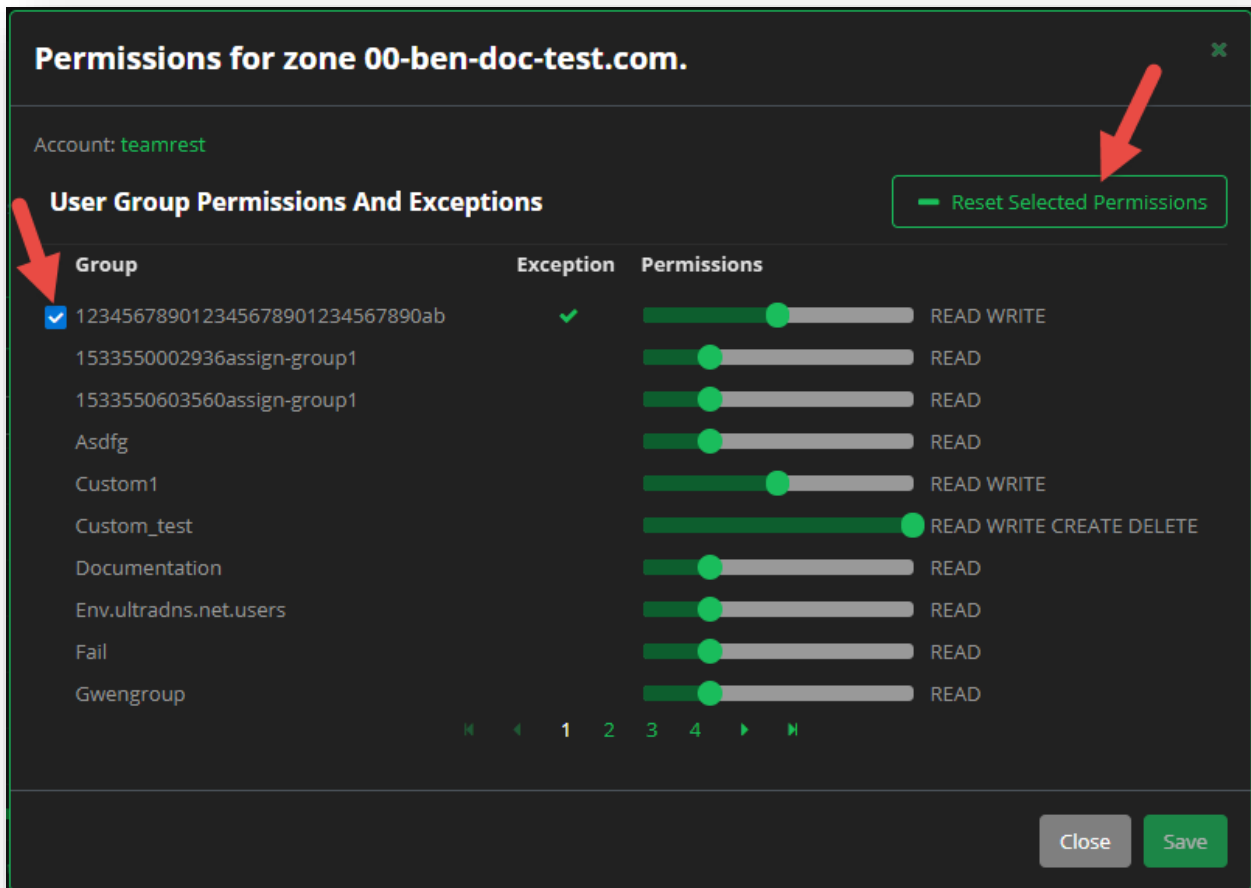


Figure 29 Domains - Permissions and Exceptions - Reset Permissions

- The permissions will automatically revert back to the default permissions (or the last updated permissions from the **Users and Groups** section of the **Accounts** tab.

Viewing your Domain

Clicking on a Domain name will open the Domain Details. From here, you can manage your Records and Pools, Properties, DNSSEC details, Zone Transfer settings, or review the Snapshot details for the specified domain.

Properties

The Properties section displays the following details for your domain:

- **General Properties** – Displays the basic details for the current domain.
- **SOA Record** – A Start of Authority (SOA) Record specifies the authoritative name server for the domain, the email of the domain administrator, the domain serial number, and the timers.
- **Name Server** – Displays the current Name Servers for the account, along with any possible alerts

for the name servers.

- **Aliased Domains** – Displays any alias domains associated to the current domain.

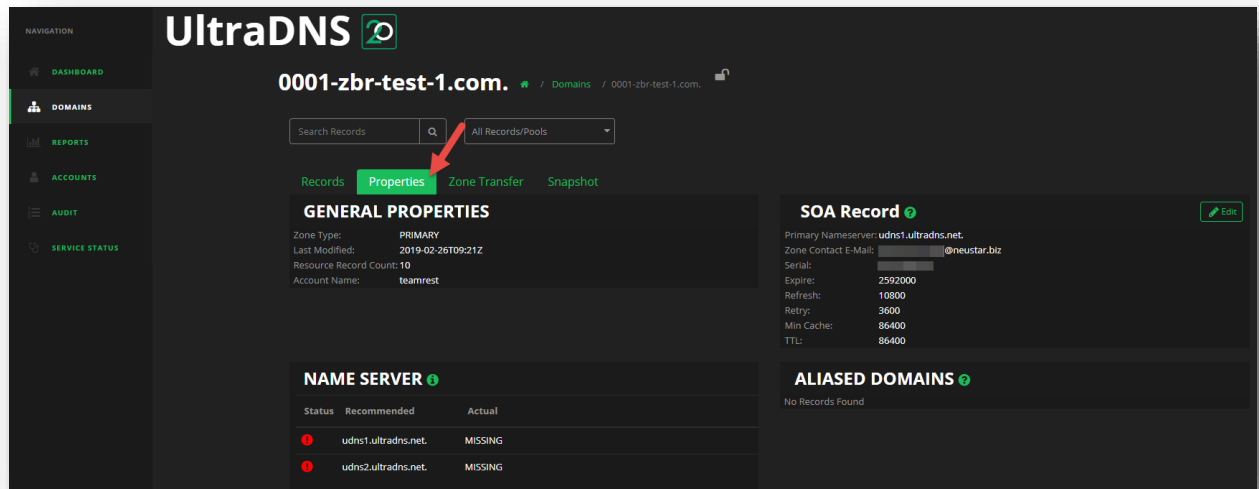


Figure 30 Domains - Properties

An additional feature available is the **Force Zone Transfer** function. Clicking this button will automatically start a transfer of the zone / domain details from your configured Primary Name Server. If the transfer fails, the Backup Primary NameServer will be initiated.

General Properties

The General Properties section displays the activity for your account.

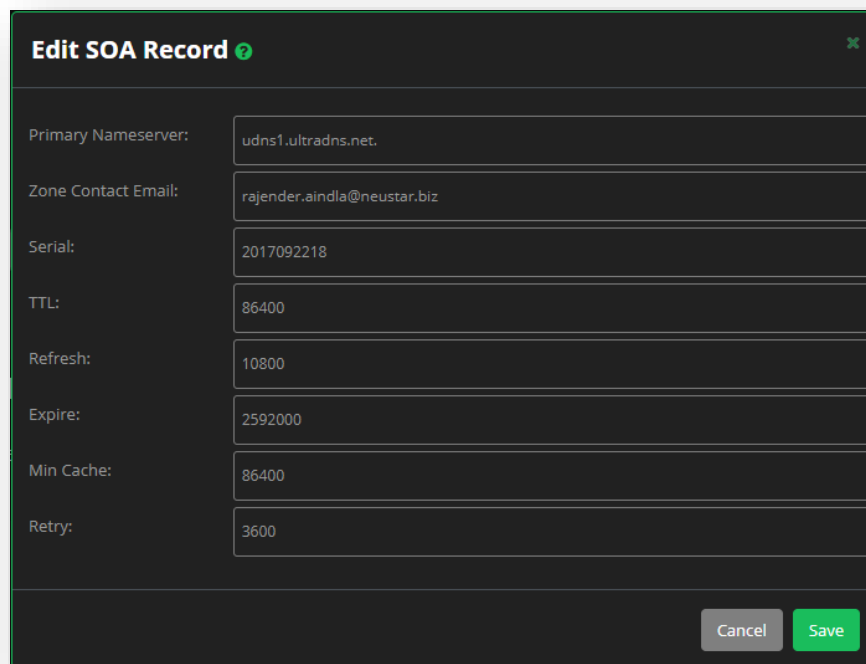
- **Zone Type** – The type of zone is associated to your account.
- **Last Modified** – The date and time your account was last modified on.
- **Resource Record Count** – The total count of Resource Records on your account.
- **Account Name** – The account name you are currently logged in with.

SOA Record

Click the **Edit** button to update your SOA Record details for your domain.

- **Primary Nameserver** - The nameserver that has the domain's authoritative data.
- **Zone contact E-mail** - The domain administrator's e-mail address
- **Serial** - By default, yyyyymmddx, where yyyyymmdd is the date of the domain creation and x is the version number of the data, which is automatically incremented whenever the domain data changes.
- **TTL** - Defines amount of time, in seconds, that any nameserver or resolver may cache the record.

- **Refresh** - The amount of time, in seconds, that secondary nameservers should check for updated domain data. Pertains only to secondary nameservers that obtain data from the primary nameserver.
- **Expire** - The amount of time, in seconds, a secondary nameserver attempts to obtain data from the primary nameserver. After this time passes, the secondary nameserver expires its data and no longer hands out answers for the domain. Pertains only to secondary nameservers that obtain data from the primary nameserver. Note: The Expire value should be much greater than the Refresh and Retry values. Otherwise, your secondary servers may expire the data before they can upload new data.
- **Min Cache** - Defines the amount of time, in seconds, that any nameserver or resolver should cache a negative response.
- **Retry** - The amount of time, in seconds, that secondary nameservers should attempt to contact the primary nameserver if the Refresh time has passed. Pertains only to secondary nameservers that obtain data from the primary nameserver.



Primary Nameserver:	udns1.ultradns.net.
Zone Contact Email:	rajender.ainda@neustar.biz
Serial:	2017092218
TTL:	86400
Refresh:	10800
Expire:	2592000
Min Cache:	86400
Retry:	3600

Cancel Save

Figure 31 Domains SOA Record - Edit Details

Name Server

The Name Server information is updated every seven calendar days for your account, and displays the two default Name Server records that are created along with any additional Name Server records you have created. The “Actual” status of the records is displayed as well.

Aliased Domains

The Aliased Domains section will display any aliased domains that you may have on the UI.

DNSSEC (DNS Security Extensions)

DNSSEC authenticates the response origin and denial of existence of a zone. UltraDNS makes it easy to sign and maintain the necessary keys and resource records, including the following:

- RRSIG: crypto signature of RR data
- DNSKEY (public keys)
 - ZSK (signs zone data)
 - KSK (signs the zone)
- DS (Digital Signer) verifies trust; secure pointer to checksum of KSK. Similar to an NS record, but instead of delegating authority, the DS record delegates trust.
- NSEC3 authenticates denial of existence (NXDOMAIN)

DNSSEC Restrictions and Recommendations

UltraDNS has the following limitations and recommendations to zone signing:

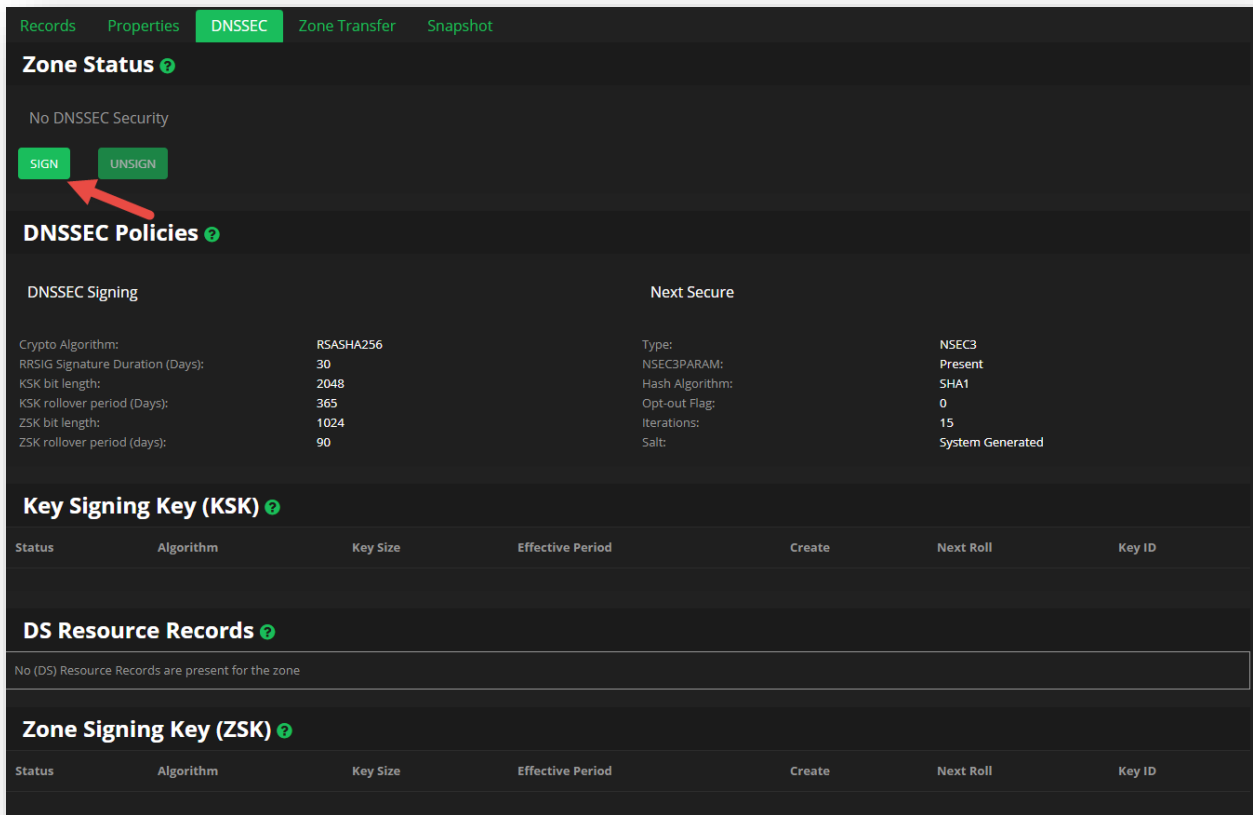
- **DNSSEC does not support Apex Alias Zones.**
- **DNSSEC does not support zones with SiteBacker/Traffic Controller or Directional DNS pools.**
- Every record in a DNSSEC-enabled zone is signed, so responses to a query for a record include the record *and* an RRSIG record; this increases the record query count.
- UltraDNS does not recommend setting TTLs for DNSSEC enabled zones to less than 5 minutes. (Go to **Accounts**, and then click **TTL Settings**.)
- UltraDNS queues changes to the zone; you must re-sign the zone to complete the changes (open the **DNSSEC** tab and click **Re-sign**).

If you are interested in using DNSSEC and do not see the **DNSSEC** tab when you open a domain, contact UltraDNS Support.

Signing a Zone

To sign a zone:

1. Click the **Domain Services** tab and select the domain you want to sign.
2. Click the **DNSSEC** tab.
3. Under the Zone Status section, click the **Sign** button.
 - a. UltraDNS queues the request and creates the RRSIG, DS, and DNSKEY records.
4. Once the signing process is complete, you will see details in the **Key Signing Key (KSK)**, **DS Resource Records**, and the **Zone Signing Key (ZSK)** sections.



The screenshot shows the 'DNSSEC' tab in the Neustar interface. At the top, there are tabs for 'Records', 'Properties', 'DNSSEC', 'Zone Transfer', and 'Snapshot'. Below these, the 'Zone Status' section indicates 'No DNSSEC Security' and features 'SIGN' and 'UNSIGN' buttons. A red arrow points to the 'SIGN' button. The 'DNSSEC Policies' section is divided into 'DNSSEC Signing' and 'Next Secure'. The 'DNSSEC Signing' section lists parameters: Crypto Algorithm (RSASHA256), RRSIG Signature Duration (Days) (30), KSK bit length (2048), KSK rollover period (Days) (365), ZSK bit length (1024), and ZSK rollover period (days) (90). The 'Next Secure' section lists: Type (NSEC3PARAM), Hash Algorithm (SHA1), Opt-out Flag (0), Iterations (15), and Salt (System Generated). Below this is the 'Key Signing Key (KSK)' section with a table showing columns for Status, Algorithm, Key Size, Effective Period, Create, Next Roll, and Key ID. The 'DS Resource Records' section shows a message: 'No (DS) Resource Records are present for the zone'. Finally, the 'Zone Signing Key (ZSK)' section has a similar table with columns for Status, Algorithm, Key Size, Effective Period, Create, Next Roll, and Key ID.

Zone Status ⓘ

No DNSSEC Security

SIGN **UNSIGN**

DNSSEC Policies ⓘ

DNSSEC Signing

Crypto Algorithm: RSASHA256
RRSIG Signature Duration (Days): 30
KSK bit length: 2048
KSK rollover period (Days): 365
ZSK bit length: 1024
ZSK rollover period (days): 90

Next Secure

Type: NSEC3PARAM
Hash Algorithm: SHA1
Opt-out Flag: 0
Iterations: 15
Salt: System Generated

Key Signing Key (KSK) ⓘ

Status	Algorithm	Key Size	Effective Period	Create	Next Roll	Key ID
--------	-----------	----------	------------------	--------	-----------	--------

DS Resource Records ⓘ

No (DS) Resource Records are present for the zone

Zone Signing Key (ZSK) ⓘ

Status	Algorithm	Key Size	Effective Period	Create	Next Roll	Key ID
--------	-----------	----------	------------------	--------	-----------	--------

Figure 32 Domains DNSSEC - Sign a Zone

Re-Sign a Zone

Once a zone has been signed, any additional changes to the domain (new records being added, etc.) will require the zone to be re-signed. Click the **RE-SIGN** button to update your zone information.

Unsign a Zone

If you no longer want to have your zone signed, you can click the **UNSIGN** button. A confirmation screen will appear with additional details reminding you to verify your Delegation Signer (DS) records before confirming the process.

Click the **Confirm** button to complete the Unsign action for your zone. As a reminder, this process is irreversible. You will have to re-sign a zone in the future which will require new Key Signing Keys and Zone Signing Keys.

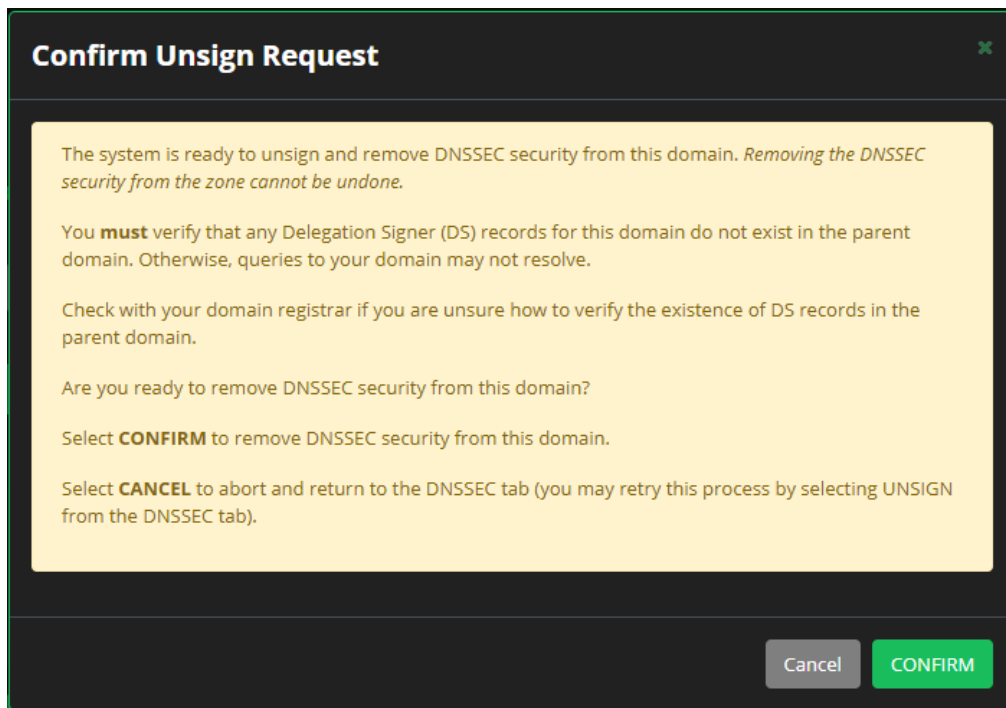


Figure 33 DNSSEC - Unsign a Zone

Zone Transfer

The Zone Transfer section displays the Restrict IPs, Name Server Notify Addresses, as well as the TSIG Key (if used) for your domain.

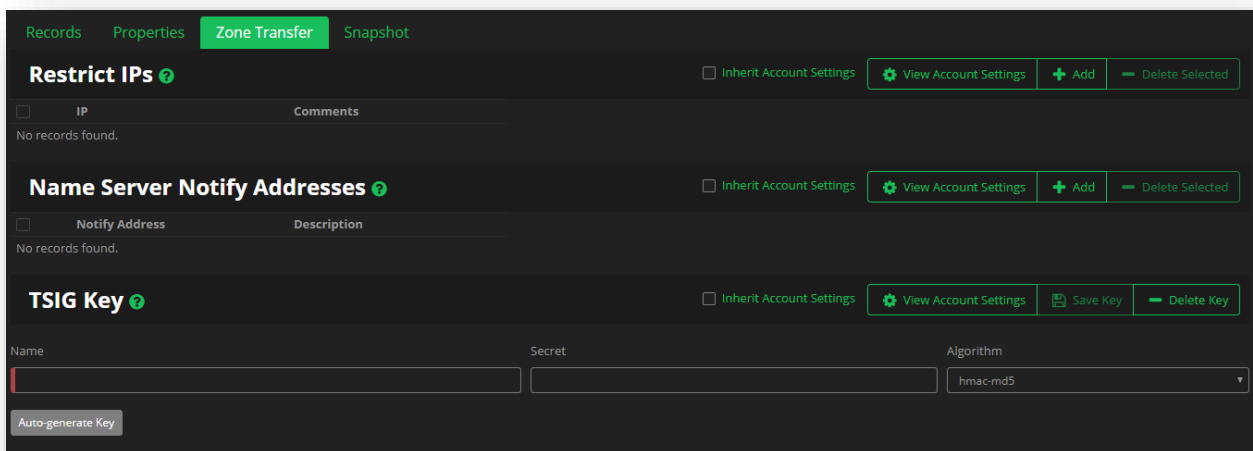


Figure 34 Domains - Zone Transfer Overview

Restrict IPs

The Restrict IPs list identifies the IP addresses that are allowed to request a zone transfer from this Neustar managed domain. Unless specified, Neustar restricts all zone transfers.

- Only IPv4 format is accepted.
- You can manually configure Restrict IPs for each zone, or, use the Inherit Account Settings to have the zone automatically use the account-level settings.
 - The Inherit Account Settings list of Restrict IPs can be found under the [Accounts](#) section.

To manually populate the Restrict IP list:

1. In the Restrict IP panel, click **Add**.
2. Select an IP Range Type from the drop-down list. Your choices include:
 - a. **IP Address Start/End** - Enter a range of IP addresses using the Start and End IP addresses of the range.
 - b. **CIDR Notation** - Allows you to enter IP addresses in the Classless Inter-Domain Routing (CIDR) format.
 - c. **Single IP Address** - For a single IP address entry.
3. You can add Comments if necessary. For example, you can specify the domain name or other common text identifiers for the IP number or range.
4. Click **Save**.

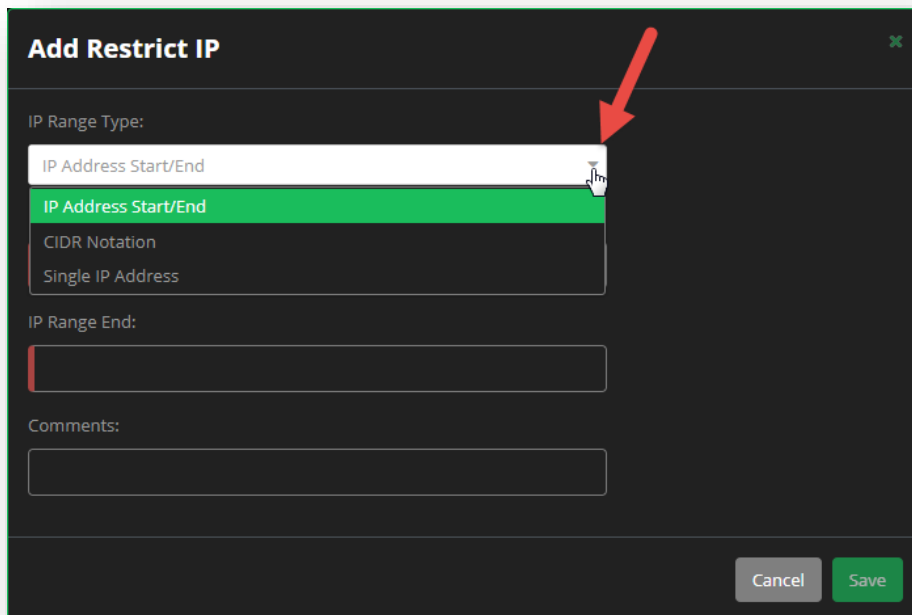


Figure 35 Domains - Zone Transfer - Restrict IPs

Using the Inherit Account Settings to populate the Restrict IPs:

You can view the current account level Restrict IPs by either clicking the **View Account Settings** button, or navigating to the [Accounts](#) section of your account, and clicking **Zone Transfer**.

1. Click the checkbox next to **Inherit Account Settings**.
 - a. A warning message appears stating that the account level Restrict IPs will override your current domain settings.
2. Click **OK**.
3. The account level list of Restrict IPs will appear under the Restrict IPs section.

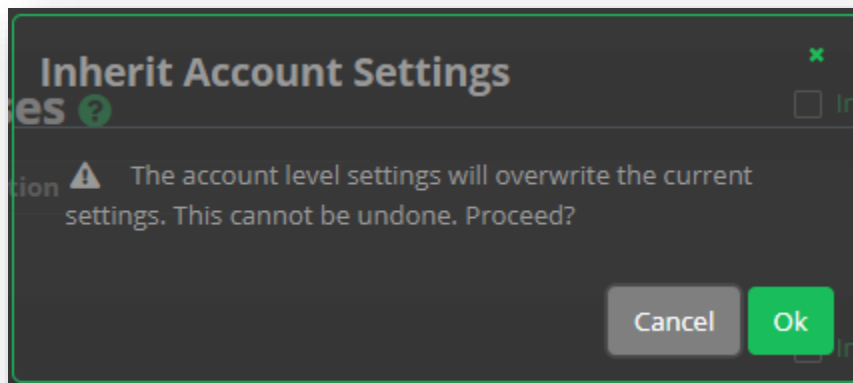


Figure 36 Domains - Restrict IPs - Inherit Account Settings

To delete one or more Restrict IPs from the list:

1. Click on the checkbox to the left of each Restrict IP that you want to delete.
2. Click **Delete Selected**.
3. Click **Delete** to confirm the deletion.

Name Server Notify Addresses

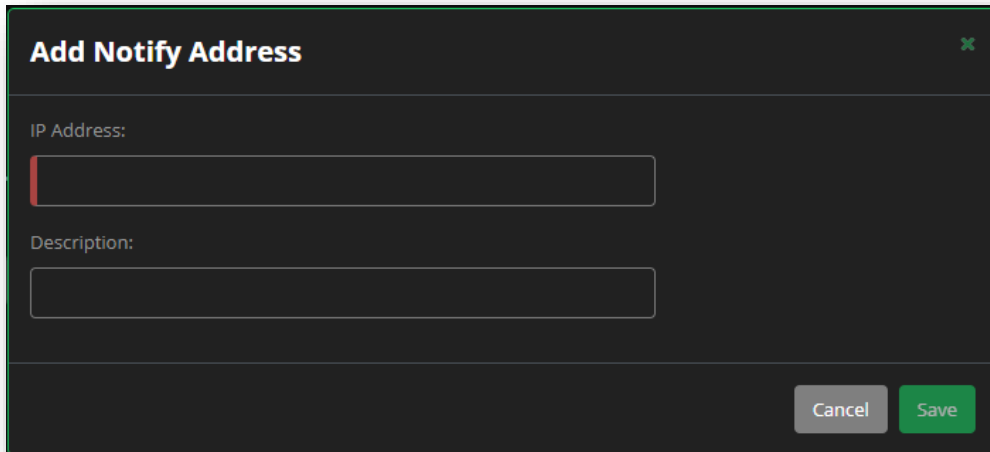
The Name Server Notify Addresses section provides a way to identify the IP address(es) that need to be notified when there are changes to the Primary zone that initiate a zone transfer.

- Only IPv4 format is accepted.
- You can manually configure the Notify Addresses for each zone, or, use the **Inherit Account Settings** to have the zone automatically use the account-level settings.

To manually populate the Notify Address list:

1. In the Notify Addresses panel, click **Add**.
2. Enter an IP address to receive notification of changes to this zone.

3. You can add Comments if necessary. For example, you can specify recipient domain names or other common text identifiers for the IP address(es) entered.
4. Click **Save**.
 - a. Repeat the above steps for all addresses to be added to the list.



Add Notify Address

IP Address:

Description:

Cancel Save

Figure 37 Domains - Zone Transfer - Notify Addresses

Using the Inherit Account Settings to populate the Notify Addresses

You can view the current account level Name Server Notify Addresses by either clicking the **View Account Settings** button, or navigating to the [Accounts](#) section of your account, and clicking **Zone Transfer**.

1. Click the checkbox next to **Inherit Account Settings**.
 - a. A warning message appears stating that the account level Restrict IPs will override your current domain settings.
2. Click **OK**.
3. The account level list of name server notify addresses will appear under the Name Server Notify Addresses.

To delete one or more Notify Addresses from the list:

1. Click on the checkbox to the left of each address that you want to delete.
2. Click **Delete Selected**.
3. Click **Delete** to confirm the deletion.

TSIG Key

The Transaction Signature (TSIG) Key section provides a way to enter and maintain the TSIG key for the domain. TSIG security requires that both sides of a transfer pass the same TSIG key value.

You can copy a key value from the corresponding server into the TSIG configuration, or Auto-generate the key in UltraDNS.

NOTE: If you elect to Autogenerate a TSIG Key, be sure to copy and paste the generated value to the corresponding zone server.

- Only one TSIG Key can be applied to a zone at a time.

To manually add a TSIG Key:

1. Enter a Name for the key.
2. Select the proper Algorithm for the key using the drop-down list. This is either the algorithm used to generate the key you are copying in, or the algorithm you want to use to generate a new key.
3. Paste (we highly recommend copy and pasting in your TSIG key) or Enter the key value into the Secret field, or, click **Autogenerate Key** to have the system provide a key for you.
4. Click **Save Key** when done.

The screenshot shows a 'TSIG Key' configuration form. At the top, there's a title 'TSIG Key' with a green info icon. To the right of the title is a checkbox labeled 'Inherit Account Settings' with a red arrow pointing to it. Further right are three buttons: 'View Account Settings' (with a gear icon), 'Save Key' (with a floppy disk icon), and 'Delete Key' (with a minus icon). Below the title, there are three input fields: 'Name', 'Secret', and 'Algorithm'. The 'Algorithm' field is a dropdown menu currently showing 'hmac-md5'. Below the 'Name' field is a button labeled 'Auto-generate Key' with a red arrow pointing to it.

Figure 38 Domains - Zone Transfer - TSIG Key

Using the Inherit Account Settings to populate the Notify Addresses:

You can view the current account level TSIG Key by either clicking the **View Account Settings** button, or navigating to the [Accounts](#) section of your account, and clicking **Zone Transfer**.

1. Click the checkbox next to **Inherit Account Settings**.
 - a. A warning message appears stating that the account level TSIG Key will override your current domain settings.
2. Click **OK**.

The account level TSIG Key details will appear in the associated fields. You do NOT need to click **Save Key**.

To delete the TSIG Key:

1. Click the **Delete Key** button. The TSIG Key will be instantly removed from the domain.

Snapshot

In UltraDNS, a backup is also known as a Snapshot. A zone snapshot represents the state of a zone (i.e. primarily its RRSet configuration) at the time the Snapshot is created.

Performing a zone Restore uses the most recent zone snapshot, and overwrites the zone's current configuration with that of the one stored in the Snapshot. The zone snapshot can be restored at any point in time, as long as the zone meets the required criteria.

Snapshot or Restore are background activities, and as such, it is highly recommended that you refrain from performing any activity that could change the zone configuration while a Snapshot or Restore is in-progress. Doing so might lead to data inconsistency or other unexpected results.

Snapshot Restrictions

- A zone can have a maximum of *one* Snapshot at a time. In other words, a zone snapshot request will either create a Snapshot (if it does not already exist), or will overwrite the existing Snapshot (if it already exists).
- Snapshot and Restore only supports primary zones
- The zone should not have more than 50,000 records, including the allowed pool's resource records.
- The zone should not have or include the following:
 - Mail Forwarding records.
 - Signed zones
 - Secondary zones
 - Alias zones
 - Suspended zones

To Create a Snapshot:

1. Create a Backup Name for the record backup you are about to create.
2. The Description is an optional field.
3. Click the **Create Backup** button.
4. Once the backup completes, you will see an entry with the Name you provided, the description (if any), and the date and time the backup was created.

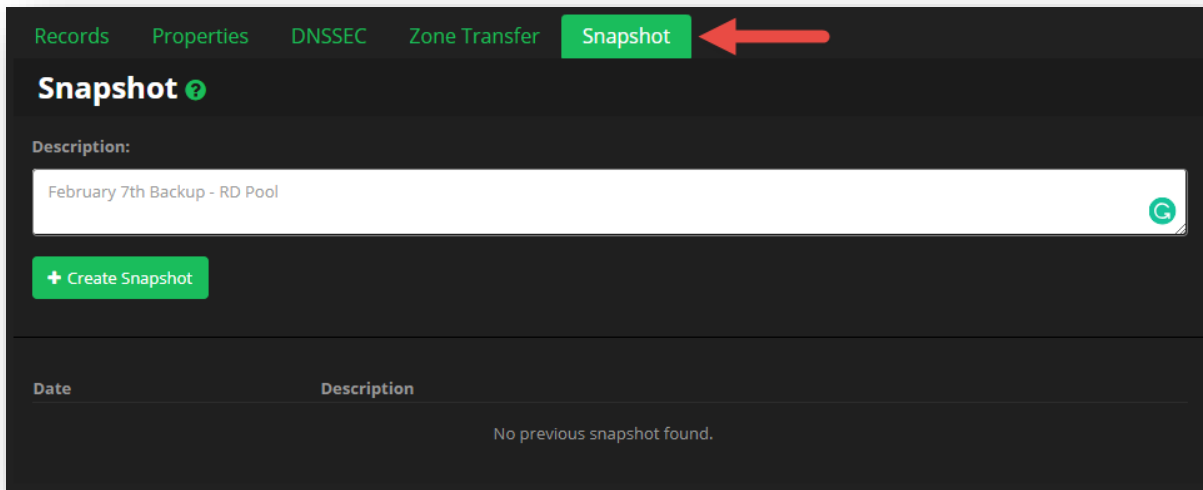


Figure 39 Domains - Create Snapshot

To Restore a Backup:

1. Click the **Restore** button on an existing backup record.
2. Click the **Restore** button on the Warning message that states that performing the backup action will overwrite your existing zone state upon completion.
3. Once the Restore completes, your new/old zone details will appear in your account.

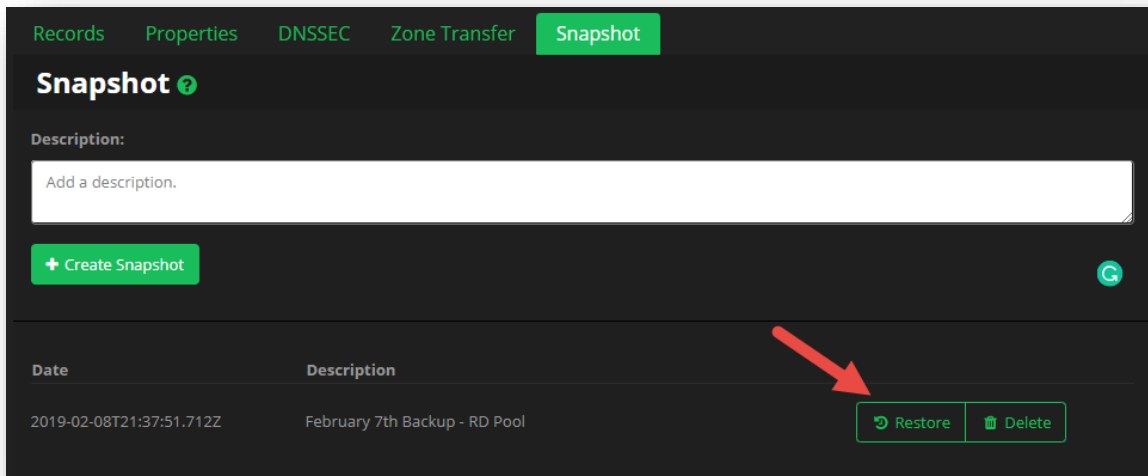


Figure 40 Domains - Restore a Snapshot

To Delete a Snapshot:

It is recommended that you delete any backups that you no longer need.

1. Click the **Delete** button next to the backup that you want to delete.
2. Click the **Delete** button again to confirm the deletion of the backup.

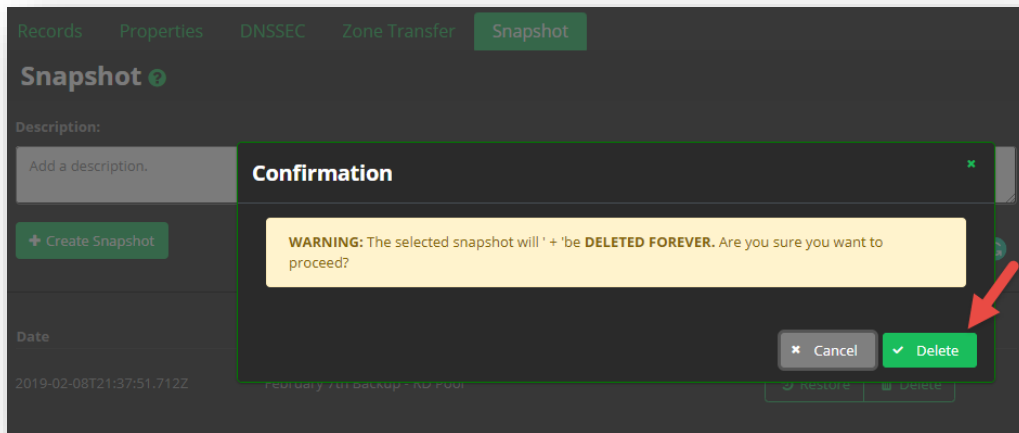


Figure 41 Domains - Delete a Snapshot

Records and Pools

Now that you have created your domain, you can begin to add your records (in addition to those that were created by default by the UI, or that you may have imported or copied over).

The UI Portal creates two default Name Server (NS) records, which in turn, determine which name servers are authoritative for the zone. A Start of Authority (SOA) record is also created, and can be found under the [Properties](#) tab.

Important Concepts and Definitions

Before you begin creating records, here are some common occurring field names and their descriptions that we recommend you familiarize yourself with.

Table 1 Record Fields and Descriptions

Field Type / Name	Description
Host	The hostname for the record, entered as either a simple, one-part name, or as a Fully Qualified Domain Name (FQDN) with or without a trailing dot. Examples: <ul style="list-style-type: none">▪ hostname▪ hostname.example.biz▪ hostname.example.biz.▪ example.biz▪ example.biz.
FQDN	“Fully Qualified Domain Name.” When a field states it requires a FQDN, you must provide the domain name with dot separators. For example: <ul style="list-style-type: none">▪ hostname – This is not a FQDN.▪ hostname.example.com – This constitutes a FQDN.
TTL	The Time to Live for a record. Provided as an integer value. This field is not required, and if left empty, will be set to the default value (which can be specified from the Properties tab of your account) of the record type.

Records

What is a DNS Record?

DNS records are resource records that tell a DNS server which IP address each domain is associated with, as well as how to handle requests sent to the domain. When someone visits a website, a request is sent to the DNS server and then forwarded to the web server provided by a web hosting company, which provides the data contained on the website.

A short string, such as “A,” “CNAME,” or “TXT,” denotes the type of commands that dictate the actions of the DNS server, and these strings of commands are called DNS syntax. You can find the various record types that we support available on the [Available Records and Pool Types](#) portion of this guide.

<http://www.pcnames.com/articles/what-are-dns-records> provides additional details about DNS records.

Adding a Record

1. Click **Domains** from the Navigation panel, and then click on your domain name from the list.
 - a. Now that you're looking at your detailed domain information, you will by default, be under the **Records** tab.
2. Scroll through the list of record types, and then click the **Add Record** button next to the record type you want to add to your domain.

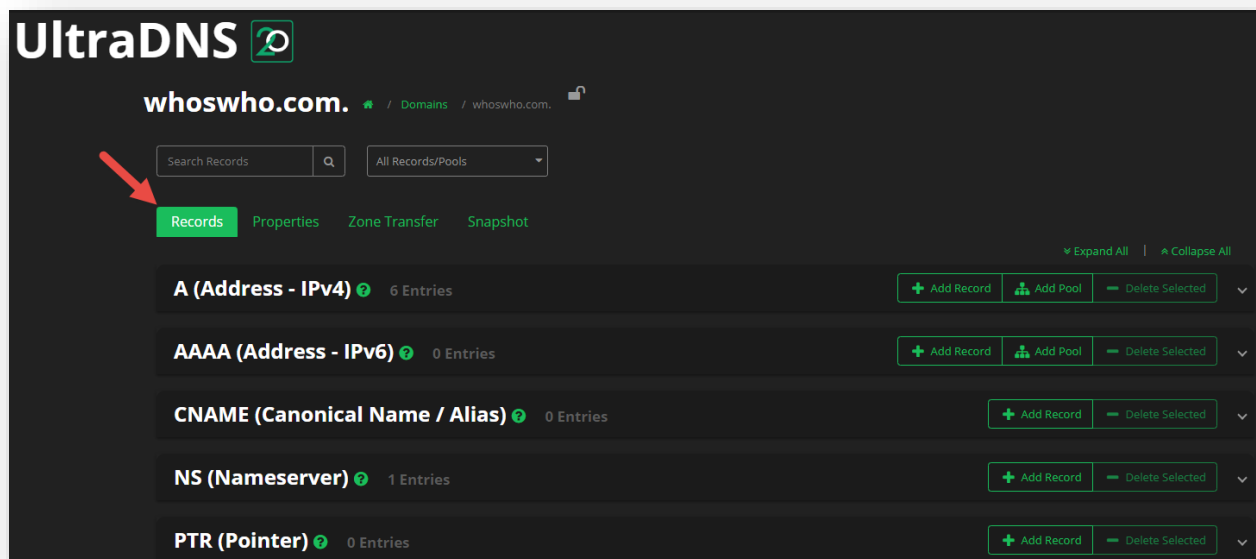


Figure 42 Records – Add a Record Step 1

3. We will use the A Record as an example.

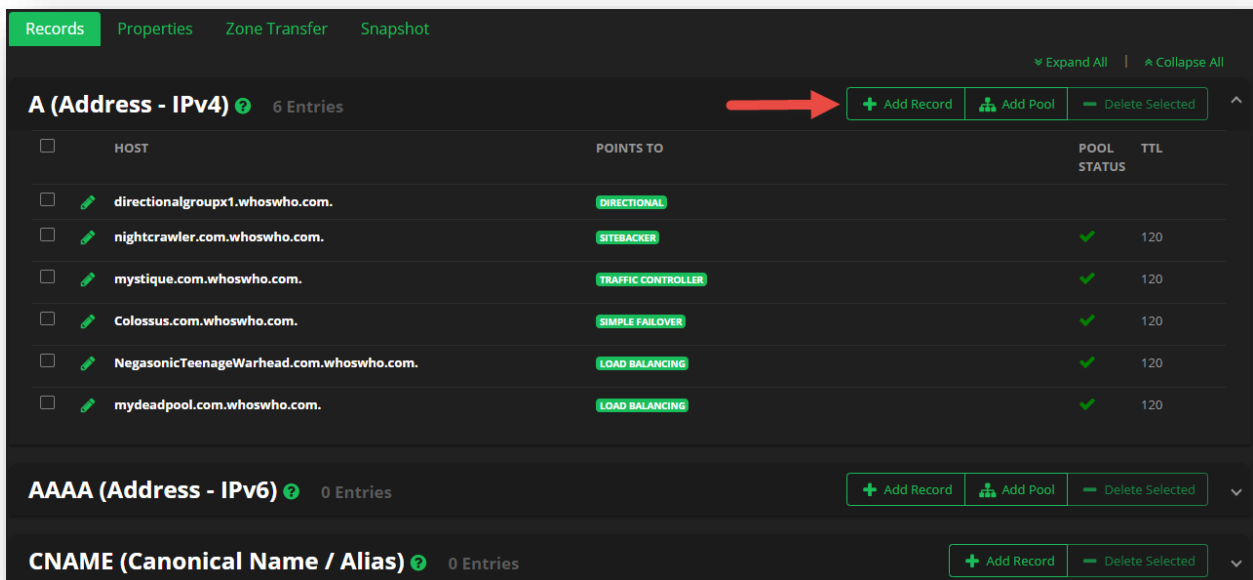


Figure 43 Records – Add a Record Step 2

- Each record type can require different details as they pertain to that record type. Once you have finished providing the details requested in the Add Record screen, click the **Save** button to finish the creation of your record.

The screenshot shows the 'Add Record: A (Address - IPv4)' dialog box. The 'Host' field contains 'www.HowToCreateAnARecord.com'. The 'Points To' field contains '1.2.3.4'. The 'TTL' field contains '90'. The 'Save' button is highlighted.

Host:

A valid hostname


Points To: TTL:

A valid IPv4 address Time to live, in seconds

Figure 44 Records – Adding a Record Step 3

- Once you save your record, it will appear immediately under the record type on your screen.

How to Edit a Record

Once you've created a record, you can easily go back and change the information you've provided in the various fields. Next to each record type there is a green pencil icon . Clicking this icon will open the edit record screen.

We will once again use an A record type for this example.

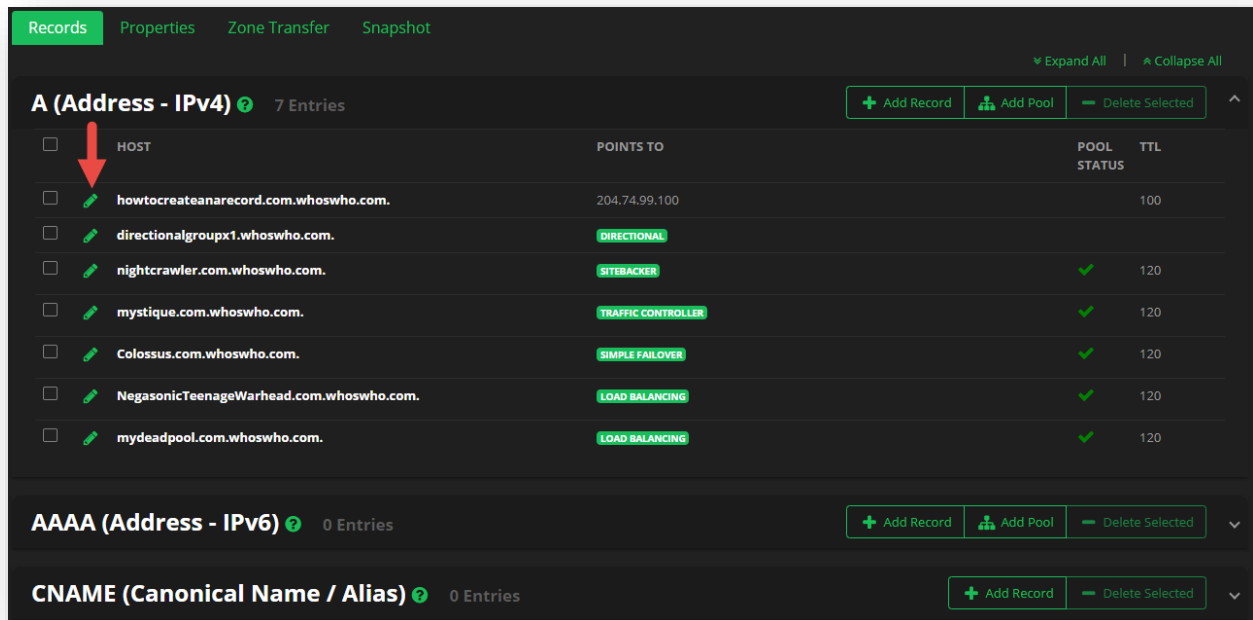


Figure 45 Records - Edit a Record

You will see the top of the dialogue box display "Edit Record," and your previously submitted data will be present. Make any changes you need to, and then click the **Save Changes** button when you are done.

It is important to note that not every field can be edited in this way. For example, the **Host** section cannot be changed once the record is created. For fields that cannot be changed, you will not see a dialogue box item.

Edit Record: A (Address - IPv4)

apexaliastestarecord.bentest.com.

Points To: 1.1.1.1
A valid IPv4 address

TTL: 90
Time to live, in seconds

Cancel Save

Figure 46 Records - Edit a Record Step 2

How to Delete a Record

If you have records that you no longer need, you can easily delete them using the UI. However, once you delete a record, there is no way to retrieve it so you will have to create new records again. If you do delete a record by mistake, and confirm the deletion, then you will have to recreate that record.

To delete a record, click in the checkbox next to the record name, and then click the **Delete Record** button.

Records Properties Zone Transfer Snapshot

Expand All Collapse All

A (Address - IPv4) 7 Entries

+ Add Record + Add Pool - Delete Selected

	HOST	POINTS TO	POOL STATUS	TTL
<input checked="" type="checkbox"/>	howtocreteanarecord.com.whoswho.com.	204.74.99.100		100
<input type="checkbox"/>	directionalgroupx1.whoswho.com.	DIRECTIONAL		
<input type="checkbox"/>	nightcrawler.com.whoswho.com.	SITEBACKER	✓	120
<input type="checkbox"/>	mystique.com.whoswho.com.	TRAFFIC CONTROLLER	✓	120
<input type="checkbox"/>	Colossus.com.whoswho.com.	SIMPLE FAILOVER	✓	120
<input type="checkbox"/>	NegasonicTeenageWarhead.com.whoswho.com.	LOAD BALANCING	✓	120
<input type="checkbox"/>	mydeadpool.com.whoswho.com.	LOAD BALANCING	✓	120

Figure 47 Records – How to Delete a Record

You'll be able to verify the records that you have marked for completion, and then verify by clicking the **Delete** button.

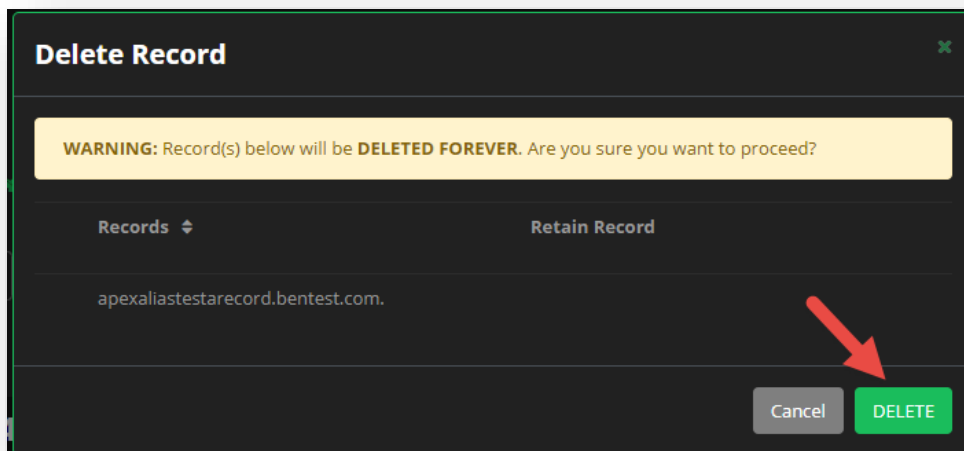


Figure 48 Records – How to Delete a Record Confirmation

Sorting and Viewing

There are several features on the UI Portal to assist you in viewing and filtering specific records or pools.

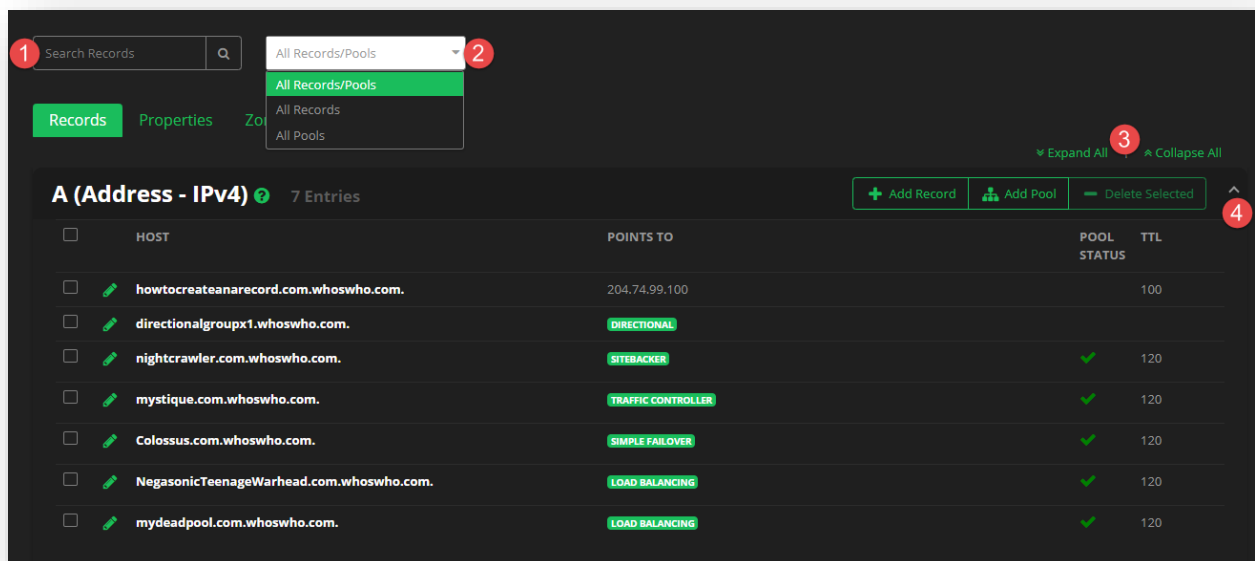


Figure 49 Records - Sorting and Viewing options

1. **Search Records** – Using the search bar, you can search for a specific record name from your list of created records. The returned results will be wildcard, meaning any record matching a portion of your search will be displayed.
2. **Records and Pools filtering** – Using the filter box, you can narrow down the results you see on your

screen.

- a. **All Records/Pools** – Every record and/or pool will be displayed when viewing a specific record type.
 - b. **All Records** - Only records not in a pool will be displayed when viewing a specific record type.
 - c. **All Pools** – Only pools will be displayed when viewing a specific record type.
3. **Expand All / Collapse All** – Instead of manually expanding and collapsing each record type, you can click **Expand All** to open every record type on the screen, or **Collapse All** to close them all.
4. **Expand / Collapse Record** – By default, when viewing the records page, every record will be collapsed. Clicking the **down arrow** will open or expand the record details, while clicking the **up arrow** will collapse or close the record details.

Pools

What is a Pool?

A Pool is a collection of records that can be grouped together by record type (A, or AAAA, or TXT) that allow you to randomly distribute requests to different hosts (CNAMEs).

The following list displays the available pool types:

- **Resource Distribution (RD)**
- **Sitebacker (SB)**
- **Traffic Controller (TC)**
- **Simple Load Balancing (SLB)**
- **Simple Monitor/Failover (SF)**
- **Directional (DIR)**

How to Create a Pool

To create a Pool:

1. Click **Domains** from the Navigation panel, and then click on your domain name from the list.
2. Find the desired Record Type that will make up your pool from the record list, and then click the **+Add Pool** button.
 - a. *Note: Not all records can be grouped into pools. For those records that are not compatible, you will not see the **+Add Pool** button.*
3. Based upon the Record Type you selected, provide the required record/pool details, and then select the **Pool Type** from the drop down menu.
 - a. In the following example, we are creating a Directional pool using an A record.

Add Pool Record: A (Address - IPv4)

Host:

A valid hostname

Points To:

A valid IPv4 address

TTL:

Time to live, in seconds

Select Pool Type

- Directional (DIR)
- Resource Distribution (RD)
- Sitebacker (SB)
- Traffic Controller (TC)
- Simple Load Balancing (SLB)
- Simple Monitor/Failover (SF)
- Directional (DIR)

Cancel Save

Figure 50 Pools - How to Create a Pool

- Click **Save** when you are finished.
- Your pool will now be displayed in the matching record section, with a green pool label under the **Points To** column.

Records Properties Zone Transfer Snapshot

Expand All Collapse All

A (Address - IPv4) 5 Entries

+ Add Record + Add Pool - Delete Selected

	HOST	POINTS TO	POOL STATUS	TTL
<input type="checkbox"/>	www.mywebpage.com.00-ben-doc-test.com.	204.74.99.100		300
<input type="checkbox"/>	ben_rd_test.00-ben-doc-test.com.	RD POOL		90
<input type="checkbox"/>	dirpool1.primary-example.com.00-ben-doc-test.com.	DIRECTIONAL		
<input type="checkbox"/>	SBrecord.00-ben-test.com.00-ben-doc-test.com.	SITEBACKER	✓	300
<input type="checkbox"/>	arecord.00-ben-test.com.00-ben-doc-test.com.	SITEBACKER	✓	500

Figure 51 Pools - Pool Labels in the Record Section

How to Edit a Pool

A Pool is a collection of records, so when you edit a Pool, you are either able to edit the individual records that make up the pool, or you can edit the details specific to the pool itself.

For this example, we will edit an A record, that is part of a *Resource Distribution Pool*.

1. Click the pencil icon next to the record that is a part of the pool you want to edit.

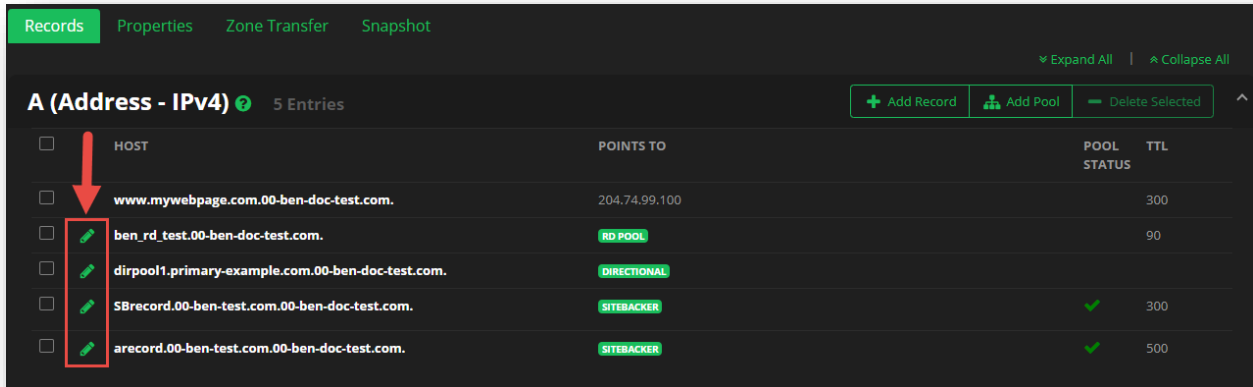
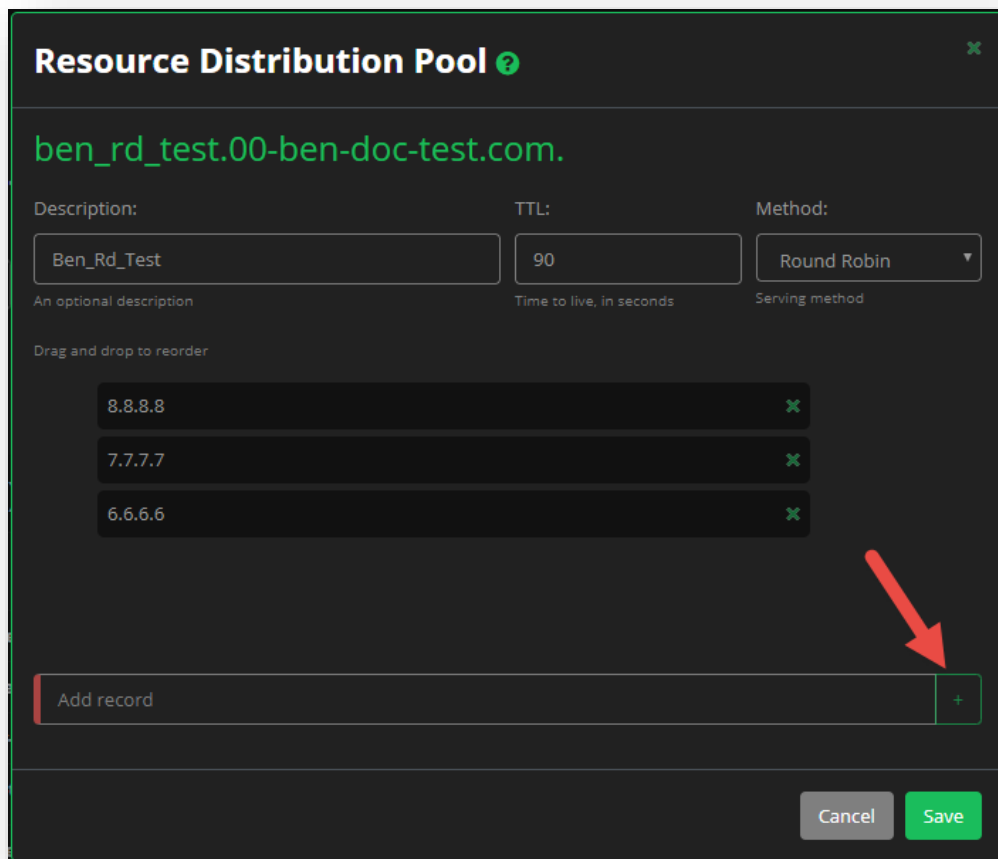


Figure 52 Pools - Edit a Pool

2. You can click into the **Description** and/or **TTL** fields to change the details currently listed. You can also change the **Method** type by selecting a new option from the drop-down menu.
3. To add a new record to the pool, type in the new IP address in the **Add Record** field, and then click the green plus icon.



Resource Distribution Pool ?

ben_rd_test.00-ben-doc-test.com.

Description: TTL: Method:

An optional description Time to live, in seconds Serving method

Drag and drop to reorder

- 8.8.8.8
- 7.7.7.7
- 6.6.6.6

Add record +

Cancel Save

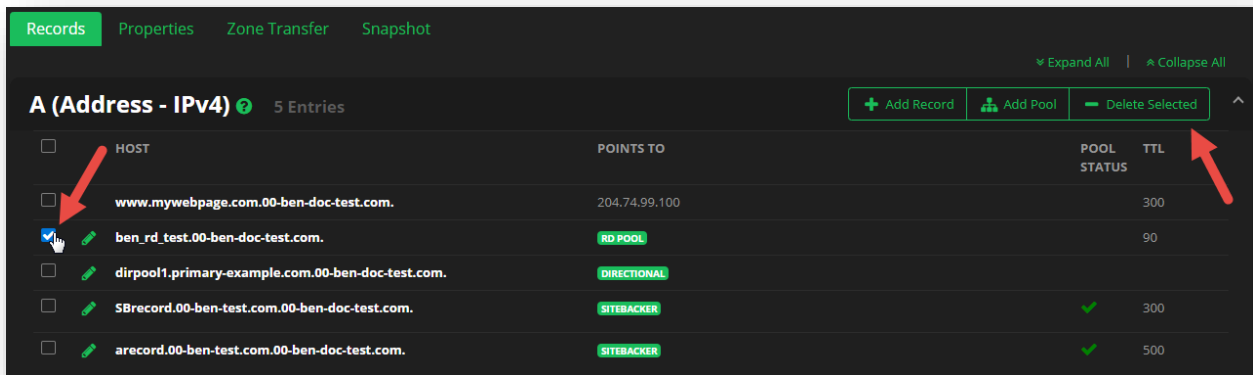
Figure 53 Pools - Edit a Pool - Add a Record

4. To remove a record from the pool, click the green **X** to the right of the record.
5. Once you have made your changes, click the **Save Changes** button.
 - a. Clicking **Close** will ignore all of the changes you made to the pool and records.

How to Delete a Pool

To delete a pool:

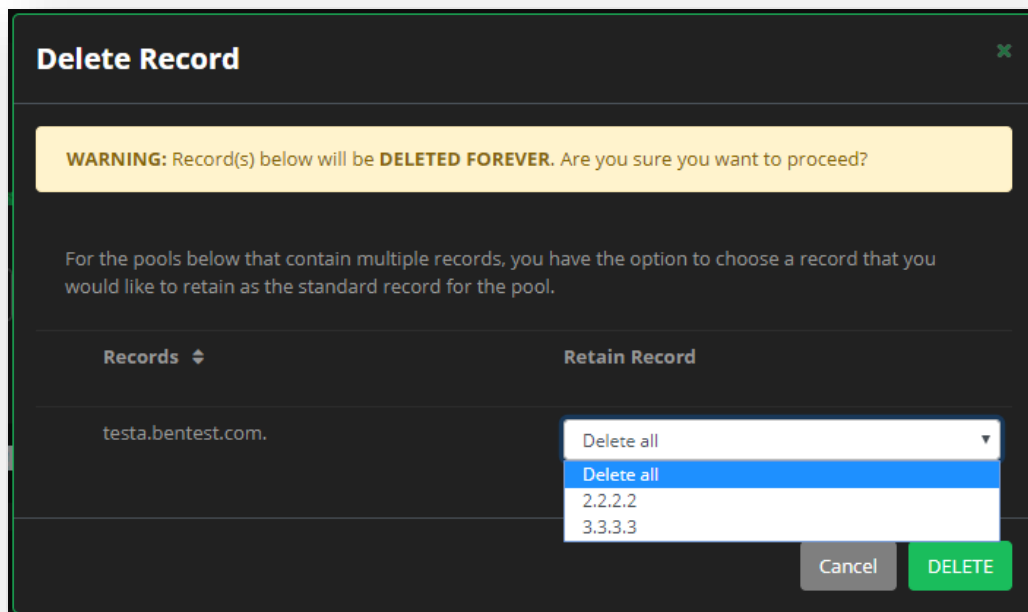
1. Click in the checkbox next to the record / pool, and then click the **Delete Record** button.
2. A confirmation message will appear to confirm that you want to delete the Pool, but will give you the option to retain any of the records that make up the Pool, or you can delete all of the associated records.
3. Click the **Delete** button to confirm the deletion.



The screenshot shows the 'Records' tab for a specific pool. The table lists records with columns for selection, host, points to, pool status, and TTL. The 'ben_rd_test.00-ben-doc-test.com.' record is selected. A red arrow points to the 'Delete Selected' button in the top right corner.

	HOST	POINTS TO	POOL STATUS	TTL
<input type="checkbox"/>	HOST			
<input type="checkbox"/>	www.mywebpage.com.00-ben-doc-test.com.	204.74.99.100		300
<input checked="" type="checkbox"/>	ben_rd_test.00-ben-doc-test.com.	RD POOL		90
<input type="checkbox"/>	dirpool1.primary-example.com.00-ben-doc-test.com.	DIRECTIONAL		
<input type="checkbox"/>	5Brecord.00-ben-test.com.00-ben-doc-test.com.	SITEBACKER	✓	300
<input type="checkbox"/>	arecord.00-ben-test.com.00-ben-doc-test.com.	SITEBACKER	✓	500

Figure 54 Pools - Delete a Pool



Delete Record

WARNING: Record(s) below will be **DELETED FOREVER**. Are you sure you want to proceed?

For the pools below that contain multiple records, you have the option to choose a record that you would like to retain as the standard record for the pool.

Records	Retain Record
testa.bentest.com.	<div>Delete all Delete all 2.2.2.2 3.3.3.3</div>

Cancel DELETE

Figure 55 Pools - Delete a Pool's Record(s)

Available Records and Pool Types

You can find a list of the record types with brief descriptions, as along with the details for each field that is required to create a given record. For additional field details, please refer back to [Record Fields and Descriptions](#).

Table 2 Available DNS Record Types

Record Type	Description
A (Address – Ipv4)	An “A” record, which stands for “address” is the most basic type of syntax used in DNS records, indicating the actual IP address of the domain. Regular DNS addresses are mapped for 32-bit IPv4 addresses.
AAAA (Address – Ipv6)	A “AAAA” (“quad A”) record is also an “address” record that indicates the actual IP address of the domain. It allows for mapping 128-bit IPv6 addresses.
CNAME	“CNAME” stands for “canonical name” and serves to make one domain an alias of another domain. The CNAME record is often used to associate new subdomains with the DNS records of an existing domain.
HINFO (Host Info)	“HINFO” stands for “Host Information Record,” and identifies the hardware and operating system of a host.
MX (Mail Exchange)	“MX” stands for “Mail Exchange” and contains a list of mail exchange servers that are to be used for the domain.
TXT (Text)	A “TXT” record lets an administrator insert any text they would like into the DNS record, and it is often used for denoting facts about the domain.
RP (Responsible Person)	“RP” stands for “Responsible Person,” and the RP record identifies the contact information of the person (or group) responsible for a host or zone.
SRV (Service Locator)	“SRV” stands for “Service” and the SRV record is used to define a TCP (TCP description) service on which the domain operates.
NAPTR (Naming Authority Pointer)	“NAPTR” stands for “Naming Authority Pointer.” The NAPTR record is most commonly used for applications in Internet telephony, for example, in the mapping of servers and user addresses in the Session Initiation Protocol (SIP). The combination of NAPTR records with Service Records (SRV) allows the chaining of multiple records to form complex rewrite rules which produce new domain labels or uniform resource identifiers (URIs).
SPF (Sender Policy Framework)	“SPF” stands for “Sender Policy Framework” and the SPR record is a type of TXT record that identifies which mail servers are permitted to send email on behalf of your domain. The purpose of an SPF record is to detect and prevent spammers from sending messages with forged From addresses on your domain.
CAA (Certification Authority Authorization)	“CAA” stands for “Certification Authority Authorization” and its purpose is to allow domain owners to declare which certificate authorities are allowed to issue a certificate for a domain. This record also provides a means for indicating notification rules in case someone requests a certificate from certificate authority that is not authorized.

Record Type	Description
TLSA (TLS Association)	Transport Layer Security Authentication (TLSA) provides communication security across the internet, by using channel encryption. The TLSA record is used to associate a TLS server certificate or public key with the domain name where the record is found, thereby forming a “TLSA certificate association.”
Apex Alias	An “Apex Alias” record basically prevents your users from having to enter the “www” at the beginning of a URL. Apex Alias allows you to replace an A record with a CNAME record that resolves to another host name. The Apex Alias functionality supports both IPv4 and IPv6 resolution, returning A and AAAA records as appropriate.
SSH Fingerprint	The DNS Secure Shell Fingerprint (SSHFP) record provides a way to verify Secure Shell (SSH) host keys using Domain Name System Security (DNSSEC). The SSHFP record is used to provide out-of-band verification, which looks up the SSHFP fingerprint of the server public key in DNS, and then uses DNSSEC to verify the lookup.
Delegation Signer	The DNS Delegation Signer (DS) record indicates that the delegated zone is digitally signed and contains the hash of the DNSSEC Key Signing Key (KSK).
Web Forwarding	A Web Forwarding record is used to redirect queries from a domain to another site. With web forwarding, you can register misspellings, alternate extensions (e.g., .biz, .net, etc.) and / or abbreviations, and then forward them to your primary website.

Table 3 Available DNS Pool Types

Record Type	Description
Resource Distribution Pool	An RD Pool is simply a grouping of type A (IPv4 address) or type AAAA (IPv6 address) records, in which you can specify how the records answer a query.
Sitebacker (SB) Pool	An SB pool is a grouping of A or CNAME records that monitors your servers and redirects traffic to a “hot” standby in case of server failure.
Traffic Controller (TC) Pool	A TC pool grouping of A or CNAME records that extends SiteBacker as a Global Server Load Balancing solution.
Simple Load Balancing (SLB) Pool	Simple Load Balancing (SLB) Pools are used to define a pool of up to five A records (the live / primary pool), an HTTP / HTTPS / No monitor, and a backup address. One resource record will be served based upon the response method configured.
Simple Monitor / Failover (SF) Pool	A Simple Monitoring pool is designed to provide single resource record sites with a very basic website availability monitor. This monitor tracks if a website is available or unreachable, and alerts the customer to unavailability via email notification. A Simple Failover Pool is used to define a single address (the live record), a simple HTTP monitor, and a backup address. If the monitor detects that the live record is unreachable from too many global regions, the backup (Failover) record is displayed.
Directional (DIR) Pool	A Directional DNS Pool represents a Directional Load Balancing Pool, which is a collection of records configured to use your geographic location or source IP address to determine a response.

A Records

An “A” record consists of the following three fields:

- **Host** – The hostname for the record, entered as either a simple, one-part name, or as a Fully Qualified Domain Name (FQDN) with or without a trailing dot. Examples:
 - hostname
 - hostname.example.biz
 - hostname.example.biz.
 - example.biz
 - example.biz.
- **Points To** – The IPv4 address for the domain.
- **TTL** – The Time to Live (TTL) for the record. Provide as either an integer or an annotated value. *This field is not required, and will be set to the default value if left empty.*

Add Record: A (Address - IPv4) ✕

Host:

www.ARecordType.com

A valid hostname

Points To:

1.2.3.4

A valid IPv4 address

TTL:

100

Time to live, in seconds

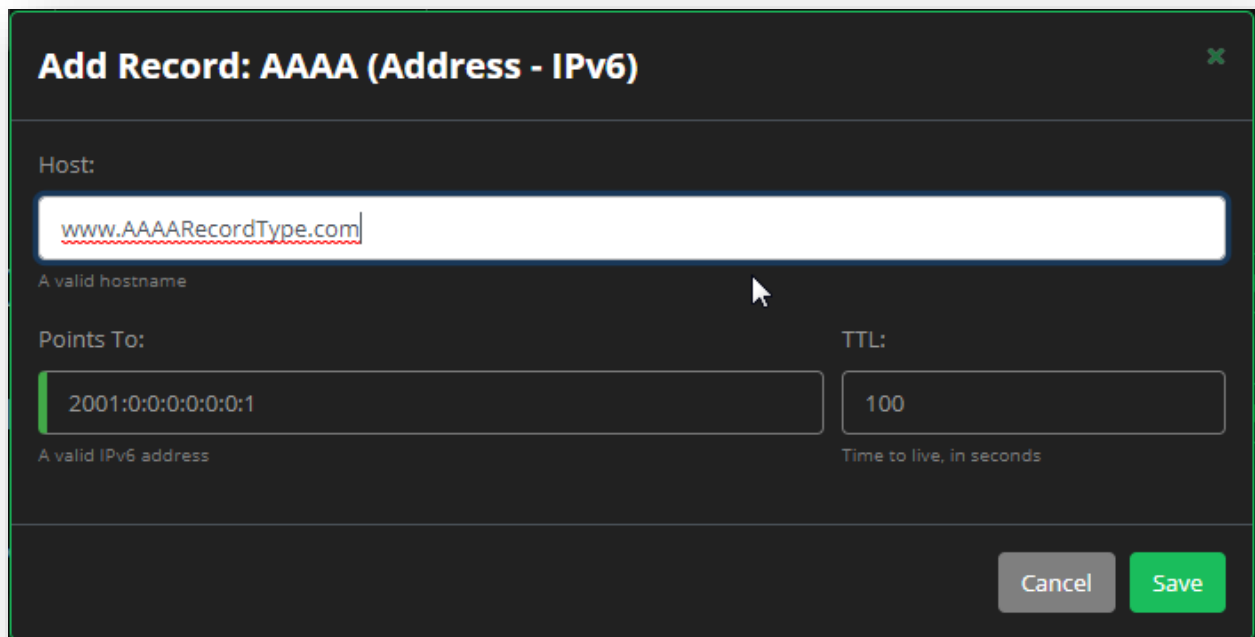
Cancel Save

Figure 56 “A” Record Fields

AAAA Records

An “AAAA” record consists of the following three fields:

- **Host**
- **Points To** – The IPv6 address for the domain.
- **TTL**



The screenshot shows a modal window titled "Add Record: AAAA (Address - IPv6)" with a close button (X) in the top right corner. The form contains three main input fields:

- Host:** A text input field containing "www.AAAARecordType.com". Below the field is the label "A valid hostname".
- Points To:** A text input field containing "2001:0:0:0:0:0:1". Below the field is the label "A valid IPv6 address".
- TTL:** A text input field containing "100". Below the field is the label "Time to live, in seconds".

At the bottom right of the form are two buttons: "Cancel" (grey) and "Save" (green).

Figure 57 “AAAA” Record Fields

Resource Distribution Pool

A Resource Distribution Pool is simply a grouping of type A (IPv4 address) or type AAAA (IPv6 address) records, in which you can specify how the records answer a query.

Creating an RD Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **Resource Distribution (RD)** from the **Select Pool Type** drop-down menu.
3. Provide the **Host**, the **Points To**, and the **TTL** (optional).
4. Click **Save** when finished.

Add Pool Record: A (Address - IPv4)

Host:
www.AddaRDPool.com
A valid hostname

Points To: 1.3.5.7
A valid IPv4 address

TTL: 100
Time to live, in seconds

Select Pool Type

- Resource Distribution (RD)
- Resource Distribution (RD)
- Sitebacker (SB)
- Traffic Controller (TC)
- Simple Load Balancing (SLB)
- Simple Monitor/Failover (SF)
- Directional (DIR)

Cancel Save

Figure 58 Records - Create an RD Pool

Once an RD pool is created, you can edit the pool record to add additional records (IP addresses) under the pool. You can also edit the Serving Method as well as the TTL value for pool.

The Serving Methods act as follows:

- **Round Robin** (default) – The records will rotate in priority.
- **Fixed** – The records will appear in a set order.
- **Random** – The records will appear in a random order.

Editing an RD Pool

1. Click the **Pencil** icon next to the RD Pool record.

Records

Properties

Zone Transfer

Snapshot

Expand All

Collapse All

A (Address - IPv4)

5 Entries

+ Add Record

+ Add Pool

- Delete Selected

<input type="checkbox"/>	HOST	POINTS TO	POOL	TTL
<input type="checkbox"/>	www.mywebpage.com.00-ben-doc-test.com.	204.74.99.100		300
<input checked="" type="checkbox"/>	ben_rd_test.00-ben-doc-test.com.		RD POOL	90
<input checked="" type="checkbox"/>	dirpool1.primary-example.com.00-ben-doc-test.com.		DIRECTIONAL	
<input checked="" type="checkbox"/>	5Brecord.00-ben-test.com.00-ben-doc-test.com.		SITEBACKER	300
<input checked="" type="checkbox"/>	arecord.00-ben-test.com.00-ben-doc-test.com.		SITEBACKER	500

Figure 59 Records - Editing a Resource Distribution Pool

2. Change the Description, TTL, and/or Method values as needed.
3. Click into the **Add Record** field, and provide a new record.
4. Click the **Plus Icon** to add the new record to the pool.

Resource Distribution Pool ?

ben_rd_test.00-ben-doc-test.com.

Description: An optional description

TTL: Time to live, in seconds

Method: Serving method

Drag and drop to reorder

- 8.8.8.8
- 7.7.7.7
- 6.6.6.6

Figure 60 Editing a Resource Distribution Pool Step 2

5. Click **Save** to update the pool.

You can use a “drag and drop” function to re-order your records. Click on a record, and then move it to a new location in the list of existing records.

- The order / rank determines the priority and sorting of the records and how they will be queried. No two records can have the same priority.

The green X will delete the record from the pool. Whenever you make changes, click the **Save Changes** button.

SiteBacker Pool

A SiteBacker pool is a grouping of A or CNAME records that monitors your servers and redirects traffic to a host standby in case of server failure.

Creating an SB Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **Sitebacker (SB)** from the **Select Pool Type** drop-down menu.
3. Provide the **Host** and the **Points To** fields.
4. Click **Save** when finished.

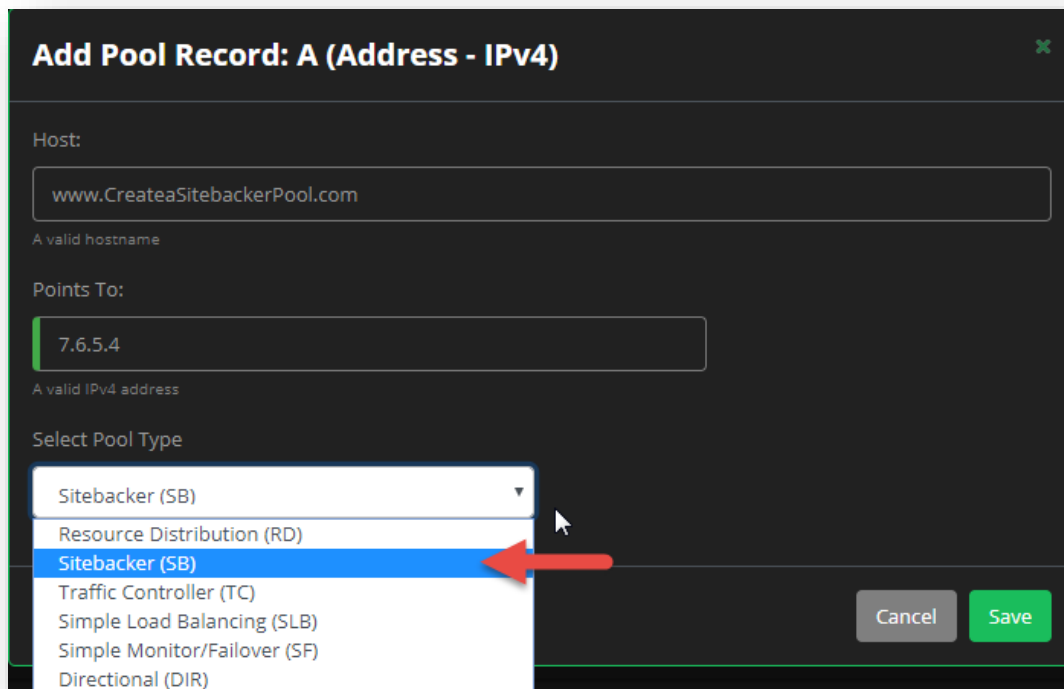


Figure 61 Sitebacker Pool - Create a Pool

Editing an SB Pool

Sitebacker pools consists of various tabs of available functions and details that beyond just displaying associated records. So when editing a Sitebacker pool, there are multiple sections that you can edit.

Pool Information

1. Once the pool is created, you will be taken to the Sitebacker Pool display.
 - a. You can also click the pencil icon next to the Sitebacker pool from your records section to navigate to this section.

2. From the Pool Information tab, you will see the following details you can edit:
 - a. **Description** – Defaults to the pool name. The description can be a maximum of 255 characters.
 - b. **Pool Type** – Displays if the pool is a Sitebacker pool, or a Traffic Controller pool. This field cannot be edited.
 - c. **Failover** – Select **Enabled** if you want to enable a failover record, or **Disabled** if you wish to only serve the primary record.
 - d. **Probing** – When probing is **Enabled**, a probe can be sent to verify that a URL can be reached, and that the record can be served.
 - i. *Note* – Probing cannot be set to **Disabled** unless Failover is set to **Disabled**.
 - e. **Response Method** – Determines in what type of order that records will be returned.
 - i. **Round Robin** – The records will rotate (in a round robin fashion).
 - ii. **Fixed** – The records will appear in the order in which they are set.
 - iii. **Random** – The records appear in a completely random order.
 - f. **Max Active Records** - Specifies the maximum number of active servers in the pool, and determines when SiteBacker takes backup servers offline. For example, consider a pool with six servers. Setting **Max Active** to 4 means SiteBacker takes two servers offline and sends the four active records in the answer.
 - g. **Max Served Records** - Specifies whether all records will be served, or only a specified number will be.
 - h. **Configured** - Displays the current number of records (including sub-pools) in the pool.
3. Click **Save** once you make any of your changes.

The screenshot shows the 'Pool Information' tab for a Sitebacker pool. The form includes the following fields:

- Description:** www.CreateASitebackerPool.com.00
- Pool Type:** SITEBACKER
- Failover:** Disabled
- Probing:** Disabled
- Response Method:** Round Robin
- Max Active Record:** All
- Max Served Record:** All Active
- TTL:** 120
- Configured:** 1
- Save** button

Below the form is the 'Records List' table:

Points To	Record Type	Record State	Probing	Priority	Serving
7.6.5.4	A	Force Active	Enabled	1	✓

Figure 62 Sitebacker Pool - Pool Information

Records List

The Records List displays all of the currently associated records to the Sitebacker pool. From this section, you can Add, Edit, or Delete records from the pool list as needed.

Add a Record

To add a new record to your pool:

1. Click the **+Add Record** button.
2. Provide the IP address or hostname for the record in the **Points To** field.
3. Select the **Failover Delay** value from the drop-down menu, which is measured in minutes.
4. Check the box to designate if this record will be a part of the All Fail record(s) or not.
5. Select the **Probe Threshold** value from the drop-down menu.
6. Select the **Record State** value from the drop-down menu.
7. Choose whether to **Enable** or **Disable** Probes for the record.
8. Provide an integer value for the **Priority** of the record.
9. Click **Save** when you are finished.

Add New Record

Points To:

Failover Delay: Value in Minutes

All Fail: ☐

Probe Threshold:

Record State:

Probes:

Priority:

Figure 63 Sitebacker Pool - Add New Record

Records List

The Records list displays your current Sitebacker pool records as follows:

- **Points To** - Displays the IPv4 address or hostname for the record.
- **Record Type** - The available record types can include A, SB (SiteBacker) / TC (Traffic Controller), or CNAME.
- **Record State** - Lists how the record should behave.
 - The default value, Normal, indicates that a pool record succeeds and fails with normal behavior (that is, SiteBacker serves records with the highest priority first).
 - Force Fail - Forces a record into a not-served state.

- Force Active - Forces a record into a served state.
- **Probing** - Signifies if Probing is enabled for the record or not.
- **Priority** - Displays the priority value for the records, which is used to determine the order in which records are returned via the Response Method.
- **Serving** - Signifies if the record is Available to Serve or not (meaning if a probe was successful or not). A green check mark indicates that serving is available, while a red X indicates it is not.




Records List 							+ Add Record	- Delete Records
<input type="checkbox"/>	Points To	Record Type	Record State	Probing	Priority	Serving		
<input type="checkbox"/>	 7.6.5.4	A	Force Active	Enabled	1			

Figure 64 Sitebacker Pool - Records List

Probes

The Probes list includes Enabled (the default) or Disabled.

Tip: Combinations of the Record State and Probes states produce the following results:

- Record State Force Active + Probes Enabled = forces a record into a served state and probes the record, but does not act on the results
- Record State Force Active + Probes Disabled = forces a record into a served state and does not probe the record
- Record State Force Fail + Probes Enabled = forces a record into a not-served state and probes the record, but does not act on the results
- Record State Force Fail + Probes Disabled = forces a record into a not-served state and does not probe the record

Probe Definitions

There are types of probes:

- **Pool probes** - These probe types probe all records in a pool.
- **Record probes** - These probe types probe only a specific record.

Within these two types of probes, are seven probe classes: DNS, FTP, HTTP, Ping, Proxy, SMTP, and TCP.

Add New Probe

Select Probe Type: HTTP | Select Host: Pool Level | Select Regions: Select SB Agents | Region Threshold: | Probe Interval: 15 Minutes

HTTP Probe Transactions

URL	Method	Transmitted Data	Follow Redirect
-----	--------	------------------	-----------------

+ Add - Delete

Cancel Save Probe

Figure 65 Sitebacker Pool - Probe Definitions

To Create a Probe

1. Click the **+Add Probe** button.
2. Select the **Probe Type** (class) from the drop-down menu.
3. Select the **Host** type, which can either be Pool, or a specific record within your pool.
4. Click in the **Select Regions** box to select a maximum of four regions to possibly probe from.
5. Select the **Region Threshold** value from the drop-down menu. This will determine how many probe failures are required before a failover occurs.
6. Select the **Probe Interval** value from the drop-down menu. This will determine how often a probe runs.
7. Based upon the Probe Type selected, the **Probe Transactions** section will request specific probe details.
8. Click the **Save Probe** button when you are finished.

Probe Types and Definitions

All probes require a Probe Interval (30 seconds or 1-15 minutes) and an Agent Threshold. The Agent Threshold is the number of agents running the probe that must fail for SiteBacker/Traffic Controller to consider the probe failed. Records also have thresholds to determine the number of probes that must fail for SiteBacker/Traffic Controller to fail the record and possibly take further action.

DNS probe

- A DNS probe verifies a DNS service. This probe requires two fields: Port (defaults to 53) and TCP only (defaults to No, which means that the probe uses UDP first, and then TCP if the UDP fails; Yes skips UDP and just uses TCP). If you set the Resource Record type to NULL and leave the Name to query blank, the application sends a bogus A record query and expects a name error in response, thus verifying the DNS service. You can complete these fields with valid data for your site.
- If you select a record in the Resource Record type list and leave Name to query blank, the DNS probe ensures the query returns a properly formatted response.
- If you select a record in the Resource Record type list and complete the Name to query, the DNS probe ensures the appropriate record responds to the query. The Resource Record Type AXFR tests if an AXFR (complete zone transfer) completed successfully. AXFR ignores the Response field.

FTP probe

- The FTP probe verifies an FTP service. This probe requires Port (typically 21), Passive Mode (if Yes, initiates both connections to the FTP server), and Path to file (for example, /pub/testfile).
- You can also specify a username and password, if required by your FTP service.

HTTP/HTTPS probe

- The HTTP probe verifies an HTTP service by making a request to a web server and testing the response. Any status code in a response other than a number in the 200's (including 301 - Moved Permanently) will fail a probe, regardless of a specified search string.
- The HTTP probe requires Port (typically 80 for HTTP and 443 for HTTPS), Host name, Web page, Protocol (HTTP or HTTPS), and Method (GET or POST). The Transmitted Data field applies to the POST method only.
- If Follow Redirects is set to Yes (default is No), and you have configured Web Forwarding redirection, then SiteBacker will follow the redirection with these restrictions:
- For DNS-level and web server-level redirects, SiteBacker will follow 300, 301, 302, and 307 redirect codes.
- For DNS-level and web server-level redirects, SiteBacker will not follow HTTP 303, 304, 305, and 306 redirect codes.
- If IP addresses are pool records in a Load Balancing pool, and the domain name is the hostname for the Load Balancing pool, SiteBacker will not recognize the DNS-level redirect; however, if the domain name is a CNAME pool record, SiteBacker will recognize the DNS-level redirect.
- If the domain name (example.com) is a CNAME pool record in a Load Balancing pool, redirects from example.com/pageA.html to example.com/pageB.html will not work, and the HTTP probe will fail.

- If a non-apex level host name (hostname.example.com) is configured as a CNAME pool record in a Load Balancing pool, then a redirect to another host name will not work and the HTTP probe will fail.

Ping probe

- The ping probe determines if a host is reachable across the network via the ICMP echo request/reply protocol (also known as ping).
- The ping probe requires Number of packets (defaults to 3) and Size of packets (does not include the IP and ICMP headers and defaults to 56 bytes).

Proxy probe

- The proxy probe connects to a proxy server and has it request the specified URL.
- The proxy probe requires the URL and Port.

SMTP Availability and SMTP Send Mail probes

- The SMTP probes test a mail server.
- SMTP Availability requires the Port (default 25), Connect time and Run time.
- SMTP Send Mail requires the Port (default 25), Mail From Address, Mail To Address, Connect time and Run time.

TCP probe

- The TCP probe attempts connection to a specified port (Port is the only required field). If you specify a Control IP Address, you can provide a control mechanism that allows the web administrators to stop the TCP port on the control system and thus cause a failover of resources to backup resources.

Scheduled Events

The Scheduled Events tab lists any upcoming events for your pool records. For example, you can schedule an event to test the failover functionality of your pool.

Schedule an Event

1. Click the **+Add Event** button.
2. From the **Select Host** drop-down menu, select a record.
3. Select an **Event Type** from the drop-down menu:
 - a. The default value, **Normal**, indicates that a pool record succeeds and fails with normal behavior (that is, SiteBacker serves records with the highest priority first).
 - b. **Force Active - Test** forces a record into a served state and probes the record, but does not act on the results.
 - c. **Force Active - No Test** forces a record into a served state and does not probe the record.
 - d. **Force Fail - Test** forces a record into a not-served state and probes the record, but does not act on the results.
 - e. **Force Fail - No Test** forces a record into a not-served state and does not probe the record.

4. Select how the **Notify On** configuration should be set.
 - a. **Never Notify** - You won't receive notifications related to the scheduled events.
 - b. **Notify only on error** - You will only receive an email notification if there is an error or failure.
 - c. **Notify on error and success** - You will receive an email notification for both failures and successes.
5. Select the check box for **Recurring Event** if you wish to schedule this event more than once.
6. Select the **Event Start** by either typing in a date by following the designated format, or by using the calendar icon. Additionally, you can set the specific hour and minute you want the event to begin.
7. Click **Save** when you are finished.

Schedule an Event

Select Host: 7.6.5.4

Select Event Type: Normal

Notify On: Never notify

Recurring Event: ☐

Event Start: yyyy-mm-dd [Calendar Icon] HH : MM AM

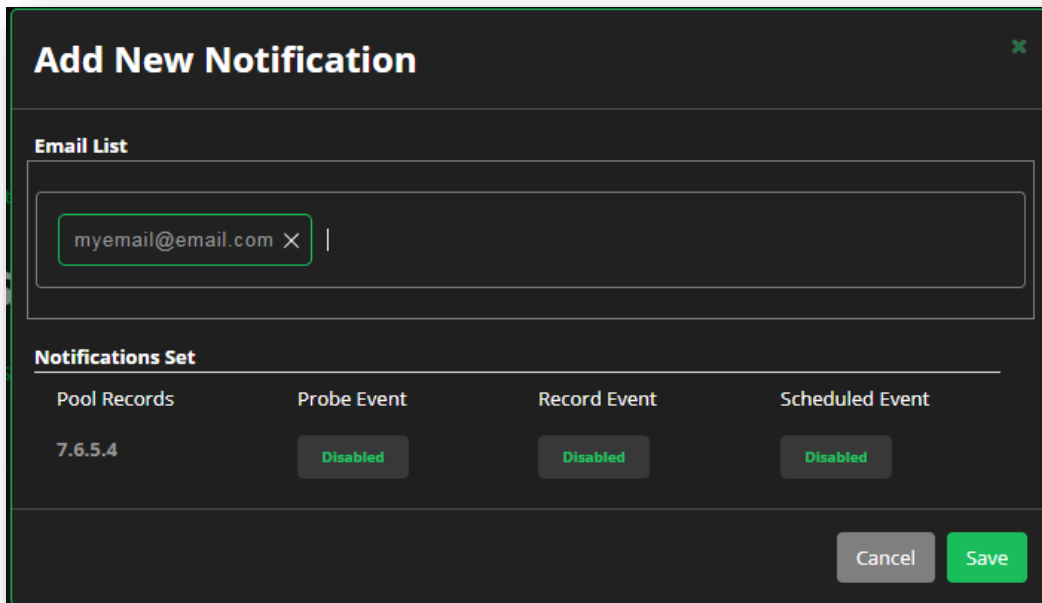
Cancel Save

Figure 66 Sitebacker Pool - Scheduled Events

Notifications

The Notifications tab allows you to add email addresses that you can then associate different notification types to.

1. In the Email List section, provide a valid email address in the addr-spec format. Multiple email addresses can be separated with a space or comma.
2. Once an email address is provided, select the different **event types** for each record that you want to receive notifications for.
 - a. **Probe Event**
 - b. **Record Event**
 - c. **Scheduled Event**
3. Click **Save** once you've added the necessary email addresses, and selected the notification types per record that you want to receive.



The 'Add New Notification' dialog box features a dark theme. At the top, the title 'Add New Notification' is displayed in white. Below the title is a section labeled 'Email List' containing a text input field with the email 'myemail@email.com' and a close icon. Underneath is a section titled 'Notifications Set' which contains four columns: 'Pool Records' (with the value '7.6.5.4'), 'Probe Event', 'Record Event', and 'Scheduled Event'. Each of these columns has a 'Disabled' button. At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

Figure 67 Sitebacker Pool - Notifications

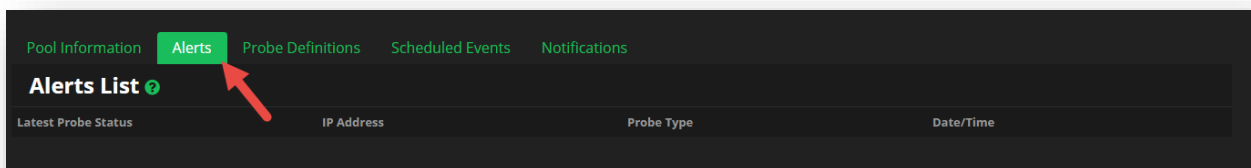
Alerts

The Alerts section displays all of the alerts for the pool's probes. The alerts page is laid out as follows:

- **Latest Probe Status** - Displays the most recent returned probe status result.
- **IP Address** - Displays the IP Address that was probed / associated to the probe.
- **Probe Type** - Displays whether the Probe was a POST (send a request) or a GET (receive a response).
- **Date/Time** - The Date and Time in which the alert occurred.

Click on the link for the probe alert to obtain additional alert details.

Tip: Add an email addresses to the Notifications section for automatic event notifications.



The 'Alerts List' interface shows a navigation bar with tabs: 'Pool Information', 'Alerts' (highlighted with a red arrow), 'Probe Definitions', 'Scheduled Events', and 'Notifications'. Below the tabs, the title 'Alerts List' is followed by a help icon. A table with the following headers is visible: 'Latest Probe Status', 'IP Address', 'Probe Type', and 'Date/Time'.

Figure 68 Sitebacker Pool – Alerts

Traffic Controller Pool

A Traffic Controller (TC) pool is a grouping of A or CNAME records that extends SiteBacker as a Global Server Load Balancing solution. Traffic Controller and SiteBacker pools are very similar in their makeup, therefore in this guide, certain tabs may be referred back to the SiteBacker section that has already explained their usage.

Creating an TC Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **Traffic Controller (TC)** from the **Select Pool Type** drop-down menu.
3. Provide the **Host** and the **Points To** fields.
4. Click **Save** when finished.

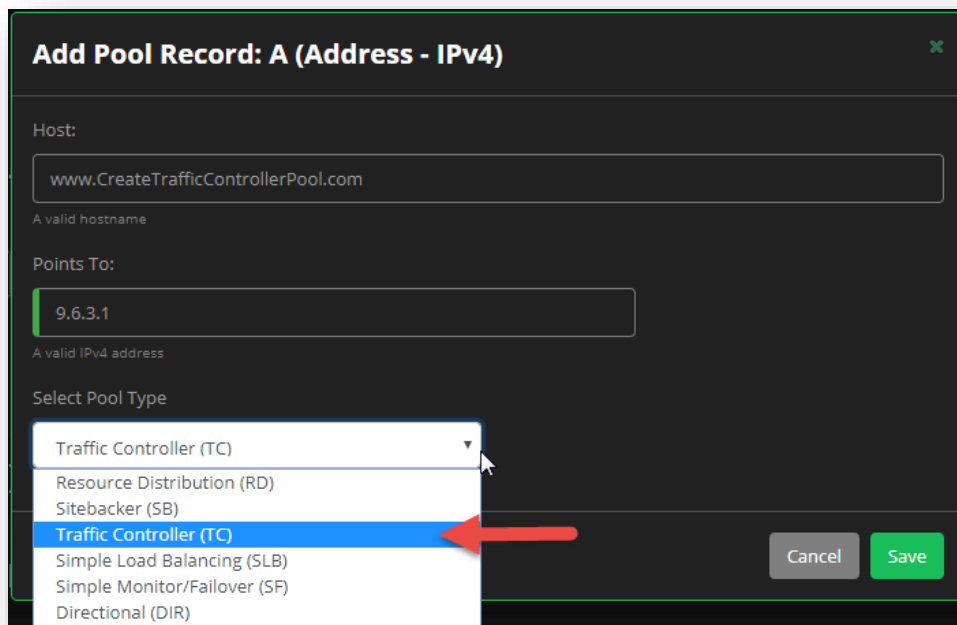


Figure 69 Traffic Controller Pool - Create a Pool

Editing a TC Pool

Traffic Controller pools consists of various tabs of available functions and details that beyond just displaying associated records. So when editing a Traffic Controller pool, there are multiple sections that you can edit.

Pool Information

- Once the pool is created, you will be taken to the Traffic Controller Pool display.
 - You can also click the pencil icon next to the Traffic Controller pool from your records section to navigate to this section.
- From the Pool Information tab, you will see the following details you can edit:
 - Description** – Defaults to the pool name. The description can be a maximum of 255 characters.
 - Pool Type** – Displays if the pool is a Sitebacker pool, or a Traffic Controller pool. This field cannot be edited.
 - Failover** – Select **Enabled** if you want to enable a failover record, or **Disabled** if you wish to only serve the primary record.
 - Probing** – When probing is **Enabled**, a probe can be sent to verify that a URL can be reached, and that the record can be served.
 - Note* – Probing cannot be set to **Disabled** unless Failover is set to **Disabled**.
 - Max Active to LB** - Specifies the maximum number of active servers in the pool, and determines when Traffic Controller takes backup servers offline. For example, consider a pool with six servers. Setting **Max Active** to 4 means Traffic Controller takes two servers offline and sends the four active records in the answer.
 - TTL** - Specifies the Time to Live value for the pool.
 - Configured** - Displays the current number of records (including sub-pools) in the pool.
- Click **Save** once you make any of your changes.

The screenshot shows the 'Pool Information' tab selected. The form contains the following fields:

- Description:** www.CreateTrafficControllerPool.co
- Pool Type:** TRAFFIC CONTROLLER
- Failover:** Enabled
- Probing:** Enabled
- Max Active To LB:** All
- TTL:** 120
- Configured:** 1
- Save** button

Below the form is the 'Records List' table:

Points To	Record Type	Record State	Probing	Weight	Priority	Serving
9.6.3.1	A	Normal	Enabled	2	1	✓

Figure 70 Traffic Controller Pool - Pool Information

Records List

The Records List displays all of the currently associated records to the Traffic Controller pool. From this section, you can Add, Edit, or Delete records from the pool list as needed.

Add a Record

To add a new record to your pool:

1. Click the **+Add Record** button.
2. Provide the IP address or hostname for the record in the **Points To** field.
3. Select the **Failover Delay** value from the drop-down menu, which is measured in minutes.
4. Provide an even integer value for the **Weight** for the record.
 - a. The Weight value determines the traffic load to send to each server in the pool.
5. Check the box to designate if this record will be a part of the All Fail record(s) or not.
6. Select the **Probe Threshold** value from the drop-down menu.
7. Select the **Record State** value from the drop-down menu.
8. Choose whether to **Enable** or **Disable** Probes for the record.
9. Provide an integer value for the **Priority** of the record.
10. Click **Save** when you are finished.

Figure 71 Traffic Controller Pool - Add TC Record

Records List

The Records list displays your current Traffic Controller pool records as follows:

- **Points To** - Displays the IPv4 address or hostname for the record.
- **Record Type** - The available record types can include A, SB (SiteBacker) / TC (Traffic Controller), or CNAME.
- **Record State** - Lists how the record should behave.

- The default value, Normal, indicates that a pool record succeeds and fails with normal behavior (that is, SiteBacker serves records with the highest priority first).
- Force Fail - Forces a record into a not-served state.
- Force Active - Forces a record into a served state.
- **Probing** - Signifies if Probing is enabled for the record or not.
- **Weight** – The integer value that helps determine the traffic load that is sent to each server in the pool.
- **Priority** - Displays the priority value for the records, which is used to determine the order in which records are returned via the Response Method.
- **Serving** - Signifies if the record is Available to Serve or not (meaning if a probe was successful or not). A green check mark indicates that serving is available, while a red X indicates it is not.

Records List ?							+ Add Record	- Delete Records
<input type="checkbox"/>	Points To	Record Type	Record State	Probing	Weight	Priority	Serving	
<input type="checkbox"/>	9.6.3.1	A	Normal	Enabled	2	1		

Figure 72 Traffic Controller Pool - Records List

Probe Definitions

For the Probe Definition details, please refer to the Sitebacker section [Probe Definitions](#).

Scheduled Events

For the Scheduled Events details, please refer to the Sitebacker section [Scheduled Events](#).

Notifications

For the Notification details, please refer to the Sitebacker section [Notifications](#).

Alerts

For the Alerts details, please refer to the Sitebacker section [Alerts](#).

Simple Load Balancing Pool

Simple Load Balancing (SLB) Pools are used to define a pool of up to five IPv4 A records (Primary Records) or IPv6 AAAA records, an HTTP(S) monitor, and a backup (All Fail) IPv4 / IPv6 address. One resource record will be served based upon the Response Method that is configured.

When using Simple Load Balancing, the defined monitor (probe) sends HTTP(S) GET or POST requests from four locations pointed at the target addresses once every five minutes. Optionally, the request to the target system can include HTTP(S) request data, and/or the HTTP response data can be searched for specific content. If no search string is specified, the probe of the target is considered Successful if any non-error HTTP response from the target is received. The availability of the target system is evaluated upon receipt of each successful or unsuccessful probe result from each location.

Creating an SLB Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **Simple Load Balancing (SLB)** from the **Select Pool Type** drop-down menu.
3. Provide the **Host** and the **Points To** fields.
4. Provide the **All Fail Record** (the backup record).
5. Include the **HTTP Test URL** that will be used to verify the service is available.
6. Click **Save** when finished.

Add Pool Record: A (Address - IPv4)

Host:
www.CreateASimpleLoadBalancingPool.com
A valid hostname

Points To:
8.2.6.5
A valid IPv4 address

All Fail Record:
54.58.56.52
IPv4 address of a backup record

HTTP Test URL:
https://www.neustar.biz

Select Pool Type

- Simple Load Balancing (SLB)
- Resource Distribution (RD)
- Sitebacker (SB)
- Traffic Controller (TC)
- Simple Load Balancing (SLB)**
- Simple Monitor/Failover (SF)
- Directional (DIR)

Cancel Save

SITEBACKER

Figure 73 Simple Load Balancing Pool - Create SLB Pool

Editing an SLB Pool

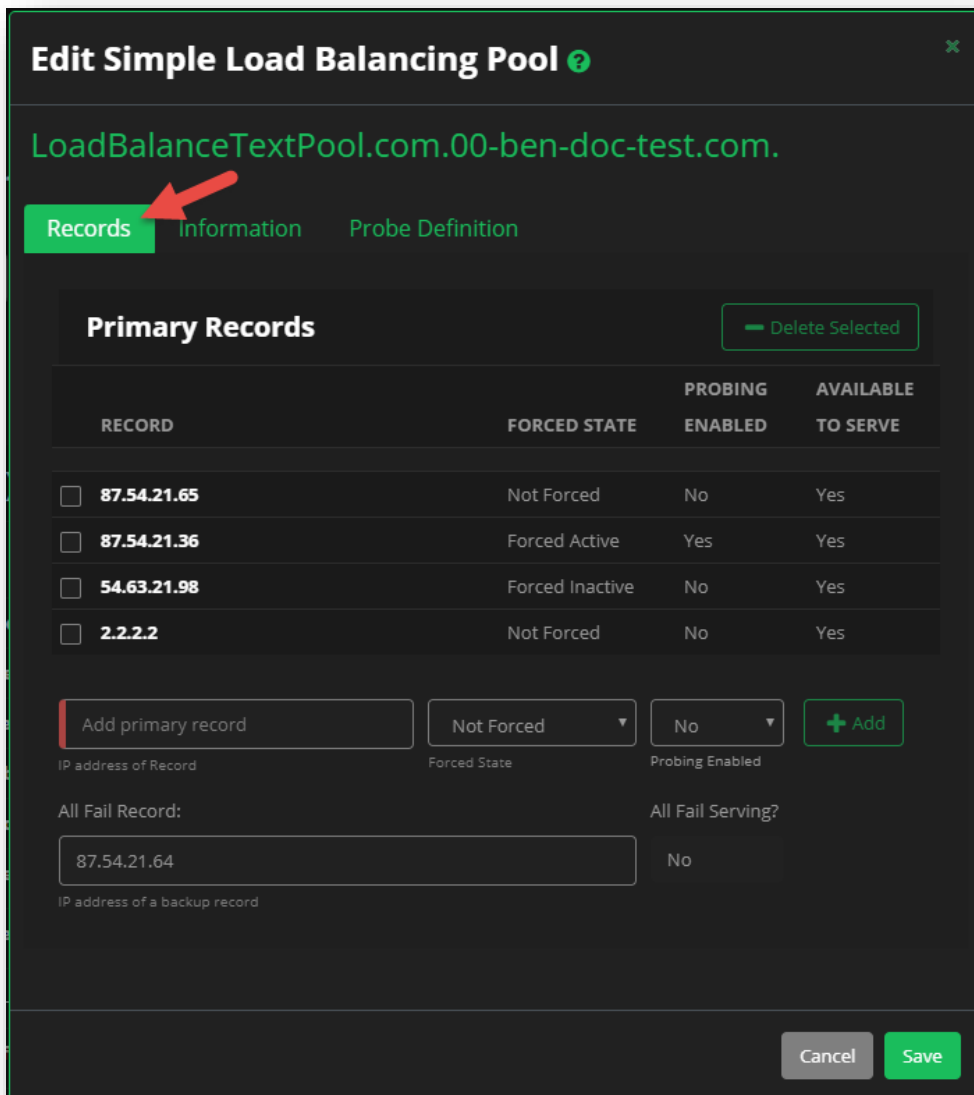
Records

Once your Simple Load Balancing pool is created, you will see three tabs that comprise the pool. The first tab is the **Records** tab, that displays the primary records for the pool, and allows you to set the Forced State, as well as enabling Probes or not.

Add Primary Record

1. Click in the **Add Primary Record** field, and provide an IP address for the new record.
2. Select the **Forced State** from the drop-down menu.
 - a. **Not Forced** - Indicates the record could be served if the probe succeeds, or will not be served if the probe fails.
 - b. **Forced Active** - Indicates the record should be served even if the probe fails and determines that the record cannot be served.

- c. **Forced Inactive** - Indicates the record should NOT be served even if the probe succeeds and indicates that the record can be served.
3. Select whether **Probing** should be enabled or not. If Probing is NOT enabled, the primary record cannot be served unless the forced state is set to Forced Active.
 4. Click the **+Add** button to add the new record to the list of Primary Records.
 5. Always remember to keep your **All Fail Record** up to date, as this will be the backup record served if the primary records all fail.
 6. Click **Save** when you are finished adding records to save this list and your settings.



Edit Simple Load Balancing Pool ?

LoadBalanceTextPool.com.00-ben-doc-test.com.

Records Information Probe Definition

Primary Records [Delete Selected](#)

RECORD	FORCED STATE	PROBING ENABLED	AVAILABLE TO SERVE
<input type="checkbox"/> 87.54.21.65	Not Forced	No	Yes
<input type="checkbox"/> 87.54.21.36	Forced Active	Yes	Yes
<input type="checkbox"/> 54.63.21.98	Forced Inactive	No	Yes
<input type="checkbox"/> 2.2.2.2	Not Forced	No	Yes

[+ Add](#)

IP address of Record Forced State Probing Enabled

All Fail Record: All Fail Serving?

IP address of a backup record

[Cancel](#) [Save](#)

Figure 74 Simple Load Balancing Pool - Records

Information

The information tab provides details about how the records will be served and returned. If you make any changes to this section, make sure to click the **Save** button afterwards.

- **Description** – You can provide a description for the SLB pool if you wish, but by default, it will display the pool name.
- **TTL** – The Time to Live in seconds for the pool.
- **Response Method** – Select a method which is responsible for selecting records to be served in the return response.
 - **Round Robin** - The order of the records being returned is determined in a "Round Robin" fashion, based upon the priority of the active records.
 - **Random** - The order of the records being returned is random, and ignores the priority of the active records.
 - **Priority Hunt** - The order of the records being returned is fixed, and is based on the priority value of the active records (High to Low). The highest priority record is always returned.
- **Serving Preference** – Determines if records will be selected from the Primary Records or the All Fail Records.
 - **Auto Select** - The default serving method, which will serve either the Primary Records or the All Fail Record depending on the probe results (and the forced state) of the primary records.
 - **Serve Primary** - Indicates that only the Primary Records are served based upon the probe results (and the forced state) of the primary records.
 - **Serve All Fail** - Indicates that only the All Fail Record will be served, thereby ignoring the probe results (and the forced state) of the primary records.

Edit Simple Load Balancing Pool

LoadBalanceTextPool.com.00-ben-doc-test.com.

Records **Information** Probe Definition

Description: TTL:
An optional description Time to live, in seconds

Response Method: Serving Preference:

Figure 75 Simple Load Balancing Pool - Information Details

Probe Definition

When using Simple Load Balancing, an HTTP(S) probe is automatically configured for the pool. The All Fail Record's IP address is not probed. This probe can be configured for either GET or POST. The Probe monitors the Target System (each record in the Primary Records pool once every 300 seconds from each of four geographic regions).

Response data can optionally be validated for the presence of specific content from the Search String field on a successful response. If no Search String is specified, the probe is considered as successful if any non-error response (not HTTP 2xx response) from the target is received. The probe will follow an HTTP 3xx Redirect received from the target system. Availability of the target system is evaluated upon receipt of each successful or unsuccessful probe result from each location.

From the **Probe Definition** tab, you can do the following:

- **HTTP Test URL** – Provide an http(s) URL to run a test probe against to verify it can be queried.
- **HTTP Method** – You can select either **GET** in an attempt to retrieve data from the test probe, or **POST** to send data to the URL with the test probe.
 - If you select **POST**, the **Transmitted Data** field will appear, allowing you to specify the data you wish to send.
- **Search String** – You can provide a specific search string that should be present in a test probe response for the probe to be considered successful.

- **Region Failure Sensitivity** – Allows you to specify the conditions under which UltraDNS will serve the **All Fail Record** instead of one of the **Primary Records**.
 - **High** - Probes in two or more regions are reporting failure of the probe target
 - **Low** - Probes in ALL (four) regions are reporting failure of the probe target.

Once you have provided all of the Probe details, click the Test Probe button to test your newly configured probe information to verify the functionality of the probe. UltraDNS will attempt to execute the configured probe towards the probe target system. When the test probe completes, the results will be displayed below the pool name of your Simple Load Balancing pool.

Edit Simple Load Balancing Pool ?

LoadBalanceTextPool.com.00-ben-doc-test.com.

Records Information **Probe Definition**

HTTP Test URL:

HTTP Method:

Search String: Region Failure Sensitivity:

Search for string in HTTP response

Figure 76 Simple Load Balancing Pool - Probe Definition

Simple Monitor / Failover Pool

Simple Monitor / Failover (SF) provides probing, notification and failover of a web site's IPv4 address record to one other IPv4 address.

When using Simple Monitor / Failover, the defined probe sends HTTP(S) GET or POST requests from four locations towards the target system once every five minutes. The target system may be any host. Optionally, the request to the target system can include HTTP(S) Request data and/or the HTTP response data can be searched for specific content. If no search string is specified, the probe of the target is considered as successful if any non-error HTTP response from the target is received. The availability of the target system is evaluated upon receipt of each successful or unsuccessful probe result from each location.

Simple Monitoring is a subset of Simple Failover and Simple Load Balancing (SLB). You can run all the Simple Failover calls as a Simple Monitor call instead by ensuring that the Failover record information is removed from the body of the call. Examples will be provided for each call.

Simple Monitoring (SM) is designed to provide single resource record sites with a very basic website availability monitor. This monitor tracks if a website is available or unreachable, and alerts the customer to unavailability via email notification. This feature does not provide fail over assistance to an alternative record (i.e. All fail), nor does it provide any measurement statistics on the health of the website (beyond whether the site is available or down).

Creating a SF Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **Simple Monitor / Failover (SF)** from the **Select Pool Type** drop-down menu.
3. Provide the **Host** and the **Points To** fields.
4. Optionally you can provide the **TTL** value.
5. Provide the **All Fail Record** (the backup record).
6. Include the **HTTP Test URL** that will be used to verify the service is available.
7. Click **Save** when finished.

Add Pool Record: A (Address - IPv4)

Host:

A valid hostname

Points To: TTL:
A valid IPv4 address Time to live, in seconds

All Fail Record:

IPv4 address of a backup record

HTTP Test URL:

Select Pool Type

- Simple Monitor/Failover (SF)
- Resource Distribution (RD)
- Sitebacker (SB)
- Traffic Controller (TC)
- Simple Load Balancing (SLB)
- Simple Monitor/Failover (SF)**
- Directional (DIR)

SITEBACKER

Figure 77 Simple Failover Pool - Create a Pool

Editing an SF Pool

When editing a Simple Monitor / Failover Pool, the following options are available:

- **Description** – You can provide a description for the SF pool if you wish, but by default, it will display the pool name.
- **TTL** – You can set the Time to Live value for the pool (optional).
- **Primary** – The Primary Record for the pool. This can be changed at any point, and as long as you are serving the primary record, the **Primary Serving** section will display “Yes.”
- **Add Backup (Failover)** – In the event that you have a backup record that you want to failover (fall back to) should your primary record fail, click in the checkbox. This will display the **Failover** field.
 - **Failover** – Provide the IP Address for the backup record that you want to failover to in the event your primary record fails.
 - If you are not currently in a failover situation, the **Failover Serving** will display “No.”

Edit Simple Failover Pool ?

MySimpleFailoverPool.com.00-ben-doc-test.com.

Manual Failover

Description: MySimpleFailoverPool.com
An optional description

TTL: 120
Time to live, in seconds

Primary: 98.54.69.37

Primary Serving?: Yes

Add Backup (Failover)? ☒

Failover: 5.5.5.5

Failover Serving?: No

Probe Definition

HTTP Test URL: https://www.neustar.biz/

HTTP Method: GET

Search String: status: ok

Region Failure Sensitivity: High

Test Probe

Cancel Save

Figure 78 Simple Monitor / Failover Pool - Edit Pool Details

Probe Definition

When using Simple Monitor / Failover, an HTTP(S) probe is automatically configured for the Primary IP address. The Failover IP address is not probed.

This probe can be configured for GET or POST. It monitors the target system once every 300 seconds from each of four geographic regions. If POST is selected, the Transmitted Data section must be completed. Target system is the configured Primary IPv4 address.

- **HTTP Test URL** – Provide the URL that you wish to run the probe against.
- **HTTP Method** – You can select either **GET** in an attempt to retrieve data from the test probe, or

POST to send data to the URL with the test probe.

- If you select **POST**, the **Transmitted Data** field will appear, allowing you to specify the data you wish to send.
- **Search String** – You can provide a specific search string that should be present in a test probe response for the probe to be considered successful.
- **Region Failure Sensitivity** – Allows you to specify the conditions under which UltraDNS will serve the **All Fail Record** instead of one of the **Primary Records**.
 - **High** - Probes in two or more regions are reporting failure of the probe target
 - **Low** - Probes in ALL (four) regions are reporting failure of the probe target.
- Click the **Test Probe** button once you have configured your probe details. The Probe result will display at the top of the screen once completed.
- Click **Save** if you made any alterations to the screen.

Probe Definition

HTTP Test URL:

HTTP Method:

Search String:

Region Failure Sensitivity:

Test Probe

Cancel **Save**

Figure 79 Simple Monitor / Failover Pool - Probe Definitions

Manual Failover

In the event that you need to failover to your backup record, as long as you have specified the **Failover** record, you can click the **Manual Failover** button to begin the failover process.

1. Click the **Manual Failover** button.
2. Verify that the backup record you will be pointing to is correct.
3. Click the **Yes** button.
 - a. As per the disclaimer, please allow at least 15 seconds to see the updated **Primary Serving** and **Failover Serving** status changes before proceeding.

4. Click **Save** when you are finished.

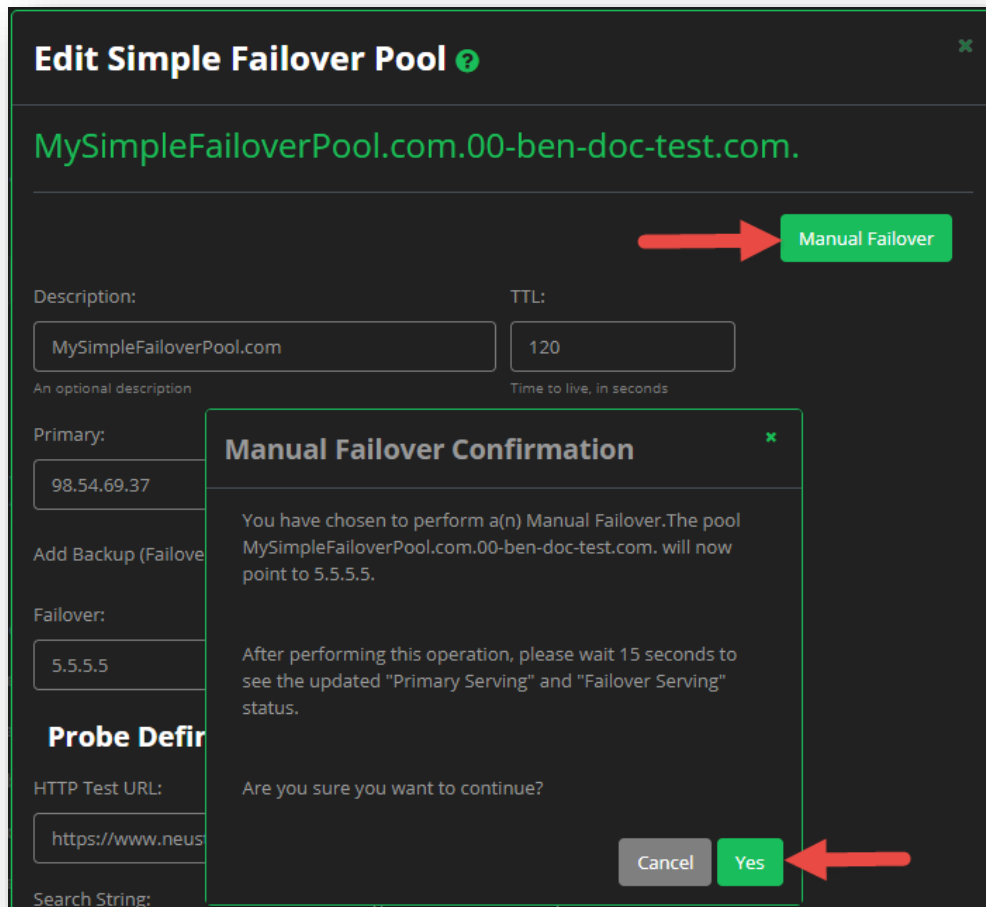


Figure 80 Simple Monitor / Failover Pool - Manual Failover

Undo Manual Failover

1. To “failback” to your Primary Record, first ensure that the **Failover Serving** status says “Yes.”
2. Next, make sure the **Primary** displays the correct IP Address.
3. Click the **Undo Manual Failover** button.
4. Ensure the details are correct, and then click the **Yes** button.
 - a. As per the disclaimer, please allow at least 15 seconds to see the updated **Primary Serving** and **Failover Serving** status changes before proceeding.
5. Click **Save** when you are finished.

The screenshot shows the 'Edit Simple Failover Pool' interface. At the top, the title is 'Edit Simple Failover Pool' with a help icon. Below the title, the pool name 'MySimpleFailoverPool.com.00-ben-doc-test.com.' is displayed. A red arrow points to a green button labeled 'Undo Manual Failover'. The form contains several fields: 'Description:' with the value 'MySimpleFailoverPool.com', 'TTL:' with the value '120', 'Primary:' with the value '98.54.69.37', 'Add Backup (Failover):', 'Failover:' with the value '5.5.5.5', 'Probe Definition', 'HTTP Test URL:' with the value 'https://www.neustar.com', and 'Search String:'. A modal dialog box titled 'Manual Failover Confirmation' is open in the center. It contains the text: 'You have chosen to perform a(n) Undo Manual Failover. The pool MySimpleFailoverPool.com.00-ben-doc-test.com. will now point to 98.54.69.37.' followed by 'After performing this operation, please wait 15 seconds to see the updated "Primary Serving" and "Failover Serving" status.' and 'Are you sure you want to continue?'. At the bottom of the dialog are 'Cancel' and 'Yes' buttons. A red arrow points to the 'Yes' button.

Edit Simple Failover Pool ?

MySimpleFailoverPool.com.00-ben-doc-test.com.

Undo Manual Failover

Description: MySimpleFailoverPool.com
TTL: 120

An optional description Time to live, in seconds

Primary: 98.54.69.37

Add Backup (Failover):

Failover: 5.5.5.5

Probe Definition

HTTP Test URL: https://www.neustar.com

Search String:

Manual Failover Confirmation

You have chosen to perform a(n) Undo Manual Failover. The pool MySimpleFailoverPool.com.00-ben-doc-test.com. will now point to 98.54.69.37.

After performing this operation, please wait 15 seconds to see the updated "Primary Serving" and "Failover Serving" status.

Are you sure you want to continue?

Cancel Yes

Figure 81 Simple Monitor / Failover Pool - Undo Manual Failover

Directional Pool

A Directional DNS Record represents a Directional Load Balancing (DIR) Pool, which is a collection of records configured to use your geographic location or Source IP address to determine a response.

Configuration Rules

- Create any Resource Distribution/SiteBacker/Traffic Controller pools first if you plan to route traffic for a region or group of regions to the RD/SB/TC pools.
- RD/SB/TC pools cannot point to a Directional pool.
- Directional pools on the zone apex (for example, the example.com zone) cannot contain CNAME records.
- Combinations of A and CNAME records or AAAA and CNAME records are allowed in the same pool.
- The record type No Response is available for all pools, but other record types may only exist in their own pool. The No Response record blocks traffic from specified regions by returning No Error, No Response.

There are three types of possible Directional pools:

- **Geolocation & Source IP** – Responses are based upon a user's geographic location and IP address.
- **Geolocation** – Responses are based upon a user's geographic location.
- **Source IP** – Responses are based upon a user's IP address.

Conflict Resolves To

If your Directional Pool contains both Geolocation and SourceIP records, then an additional drop-down menu will appear when you view/edit your pool. When there is a conflict between a matching Geolocation group and a matching Source IP group, the selected type takes precedence.

Select a record type from the drop-down list, and then click the **Save Changes** button. Your selection can be changed at any time, and as often as you need.

A/CNAME Directional Pool

Description:

Conflict Resolves To: **Geolocation** (dropdown menu open showing: Geolocation, Source IP)

Ignore ECS: ☐

Save changes

Pool Records

Groups	Record Type	Points To	TTL
<input type="checkbox"/> IP Primary	A	1.1.1.1	86400
<input type="checkbox"/> NA - East Coast	A	1.2.3.4	86400
<input type="checkbox"/> + IP All Non-Configured	A	54.56.12.21	300

+ Add **Delete Selected**

Figure 82 Directional Pool - Conflict Resolves To

Ignore ECS

Enabling the Ignore ECS option determines whether or not to ignore the EDNSO (which is an extended label type allowing for greater DNS message size) Client Subnet data when available in the DNS request. We recommend that if you are not familiar with this concept, do not check the box to enable this feature.

Create a DIR Pool

1. Select either an A or AAAA record type, and then click the **+Add Pool** button.
2. Select **Directional (DIR)** from the **Select Pool Type** drop-down menu.
3. Provide the **Host** and the **Points To** fields.
4. Optionally you can provide the **TTL** value.
5. Click **Save** when finished.

Add Pool Record: A (Address - IPv4)

Host:
www.CreateADirectionalPool.com
A valid hostname

Points To: 54.56.12.21
A valid IPv4 address

TTL: 300
Time to live, in seconds

Select Pool Type

- Directional (DIR)
- Resource Distribution (RD)
- Sitebacker (SB)
- Traffic Controller (TC)
- Simple Load Balancing (SLB)
- Simple Monitor/Failover (SF)

Cancel Save

Figure 83 Directional Pool - Create a Pool

Edit a DIR Pool

After you have created a Directional Pool, you will see the **Pool Records** screen. From here, you can add additional records and customize whether you want them to contain Geolocation data, SourceIP details, or a combination of both.

From the Pool Records screen, you can see the currently associated records, along with the **Groups** assigned to them. You can click on

- The “globe” or “earth” icon denotes that the record contains Geolocation data.
- The “IP” icon denotes that SourceIP details are associated to the record.
 - To edit either of these fields, click on the **icon** itself to open the details.
- “All Non-Configured” implies that every geographic region is associated to the record, as well as any preconfigured SourceIP details.

A/CNAME Directional Pool ⓘ

Description: Conflict Resolves To: Ignore ECS: ☐

Pool Records

<input type="checkbox"/> Groups	Record Type	Points To	TTL
<input type="checkbox"/> IP Primary	A	12.23.34.45	86400
<input type="checkbox"/> + IP All Non-Configured	A	54.56.12.21	300
<input type="checkbox"/> + North America	A	98.87.76.65	86400

Figure 84 Directional Pool - Pool Records

Add a Record - Geolocation

Adding Geolocation details to your record works in a "drill-down" manner, meaning that you can select specific states and provinces from within a selected territory, or select an entire overarching region (continent) instead. There is no limit to the number of regions / territories / states that can be associated to your record.

To add a new record that contains Geolocation data:

1. Click the **+Add** button.
2. Select a **Record Type** from the drop-down menu.
 - a. **A** record
 - b. **CNAME** record
 - c. **No Response**
3. Provide the IPv4 address for the record in the **Points To** field.
 - a. Optionally, you can add the **TTL** value.
4. Click **Add a Group** when finished.
5. Select the **Geolocation** from the **Add Directional Group** drop-down menu.
6. Select **Create New Group** to associate new Geolocation details to the record, or, select **Assign Global Group** to associate a pre-configured *Directional Groups* to your record.
 - a. If you opt to use an existing Global Directional Group, select the **Group Name** from the drop-down list of Global Groups you have access to.
7. Provide a **Group Name** for your record.
8. Click in the **Select Regions** field to select any applicable regions for your record.
 - a. In the following example, we selected North America.

The screenshot shows a dark-themed form titled "Add Directional Pool Record". At the top, there are two dropdown menus: "Add Directional Group" (set to "Geolocation") and "Type" (set to "Create New Group"). Below these is a "Group Name:" field containing "NA - East Coast". The form is divided into two main sections: "Available Regions" and "Selected Regions". The "Available Regions" section has a dropdown menu that is open, showing a list of regions: "Anonymous Proxy", "Satellite Provider", "South America", "Australia / Oceania", "Antarctica", "Unknown / Uncategorized IPs", and "North America". A red arrow points to "North America". The "Selected Regions" section has a "Filter" input field and the text "No items found". At the bottom right, there are four buttons: "Cancel", "Back", "Add Another Group", and "Save".

Figure 85 Directional Pool - Add Geolocation Record - Regions

9. Once you've selected your region(s), click outside of the **Available Regions** field.
 - a. If you click on the **green arrow** at this point, you will select the region and by default, every country and state / province as well.

The screenshot shows the 'Add Directional Pool Record' form. At the top, there are two dropdown menus: 'Add Directional Group' (set to 'Geolocation') and 'Type' (set to 'Create New Group'). Below these is a 'Group Name' field containing 'NA - East Coast'. The main section is divided into two columns: 'Available Regions' and 'Selected Regions'. In the 'Available Regions' column, there is a dropdown menu labeled 'x North America' which is open, showing a list of countries: Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, and Bermuda. A red arrow points to the 'Select Countries' field. Another red arrow points to a green arrow button located between the two columns. The 'Selected Regions' column has a 'Filter' input field and the text 'No items found'. At the bottom of the form are four buttons: 'Cancel', 'Back', 'Add Another Group', and 'Save'.

Figure 86 Directional Pool - Add Geolocation Record - Countries

10. Click in the **Select Countries** field, and select any applicable territories for your record.
 - a. If you click on the **green arrow** at this point, you will select the country / countries and by default, every associated state / province
11. Click in the **Select States/Provinces** field, and select any applicable states or provinces for your record. Once you have made your selections, click the **green arrow** to move your selections to the **Selected Regions** column.
 - a. To remove a selected location, click the green **X** next to the location name.

Figure 87 Directional Pool - Add Geolocation Record - Save

12. Once you have made all of your selections, click **Save** to complete the record, or click **Add Another Group** to associate SourceIP data to the record as well.

Add a Record – SourceIP

A Source IP Directional Pool tailors a response based on your IP address (either IPv4 or IPv6). The UI portal supports standard IPv6 address notation: eight groups of four hexadecimal digits, separated by a colon (:). You can simplify the notation by omitting leading zeros in a group, or by replacing one or any number of consecutive groups of 0 with two colons (::). For example, these IPv6 addresses are equivalent:

```
3FFE:0B80:0447:0001:0000:0000:0000:0001
3FFE:0B80:0447:1:0:0:0:1
3FFE:0B80:0447:1::1
```

To add a new record that contains SourceIP data:

1. Click the **+Add** button.
2. Select a **Record Type** from the drop-down menu.
 - a. **A** record
 - b. **CNAME** record

c. **No Response**

3. Provide the IPv4 address for the record in the **Points To** field.
 - a. Optionally, you can add the **TTL** value.
4. Click **Add a Group** when finished.
5. Select the **SourceIP** from the **Add Directional Group** drop-down menu.
6. Select **Create New Group** to associate new SourceIP details to the record, or, select **Assign Global Group** to associate a pre-configured *Directional Groups* to your record.
 - a. If you opt to use an existing Global Directional Group, select the **Group Name** from the drop-down list of Global Groups you have access to.
7. Provide a **Group Name** for your record.
8. Select the **SourceIP Type** in which you will provide your IP address details.
 - a. **IP Range** – Provide a beginning and ending IP address to create a range.
 - b. **Single IP** – Provide a single IP address for the record.
 - c. **CIDR** – Specify the network and routing prefix. For example, 192.168.0.0/16 or 2001::/64.
 - i. Note: The UI Portal automatically converts the CIDR notation to an IP range.

Figure 88 Directional Pool - Add SourceIP Record - Source Type

9. Once you have selected your input type, provide your Source IP details, and then click the **Add** button.
10. You can add as many IP address as you wish. Click **Save** when you are done, or, click **Add Another Group** if you want to associate Geolocation data to the record.

Overlaps

You **CANNOT** overlap regions or Source IP ranges at the record pool level. However, Global Directional Groups (both Geolocation and Source IP) may overlap. For example, you could have a North America group consisting of Canada, the United States, and Mexico, and three groups consisting of Canada, the United States, and Mexico separately; or you may have overlapping networks.

Converting a Mixed Pool to a Geolocation or Source IP Pool

Carefully consider before converting a Mixed Pool (a pool that contains BOTH Geolocation and Source IP Groups and records) to a Geolocation or Source IP Pool (pools that contain ONLY Geolocation or Source IP Groups and records). Once you click **Convert**, the Groups and Records that do not match the pool type will be removed.

Convert to Global Group

Once you have successfully created a record containing either SourceIP data or Geolocation details, you can convert your saved settings to a Global Directional Group.

1. Click on the **Globe** or **IP** icon to edit the record.
2. Click the **Convert to Global Group** link.
3. Provide a new **Global Group Name**, and then click the green **Checkmark** icon.

The screenshot shows a dark-themed dialog box titled "Edit Directional Group" with a close button (X) in the top right corner. Inside the dialog, there is a "Group Name:" label above a text input field containing the word "Primary". To the right of this input field is a green link labeled "Convert to Global Group", which is highlighted by a red arrow. Below the "Group Name" section, there is a "Source IP" section. It contains two checkboxes: "IP" (unchecked) and "1.1.1.1" (checked with a green checkmark icon). To the right of these checkboxes is a "Delete Selected" button. Below the checkboxes, there is an "IP Range" dropdown menu, followed by two empty input fields separated by a hyphen, and an "Add" button. At the bottom right of the dialog are "Close" and "Save" buttons.

Figure 89 Directional Pool - Convert to Global Group

CNAME Records

A “CNAME” record consists of the following three fields:

- **Host**
- **Points To** – The canonical name, entered as an FQDN with or without a trailing dot.
 - For example: targetname.example.com
- **TTL**

Add Record: CNAME (Canonical Name / Alias)

Host:

www.AddaCNAMERecord.com

A valid hostname

Points To:

somewebsite.com

The canonical name, entered as an FQDN

TTL:

100

Time to live, in seconds

Cancel Save

Figure 90 “CNAME” Record Fields

NS Records



Note: When you create or transfer a domain to UltraDNS, you will see two NS records created automatically: udns1.ultradns.net and udns2.ultradns.net. You cannot edit or delete these records.

An “NS” or Name Server record consists of the following three fields:

- **Zone Delegation** – The simple name of the subdomain for which the NS record is authoritative.
- **Name Server** – The FQDN of the Name Server (with or without the trailing dot).
- **TTL**

Add Record: NS (Nameserver)

Zone Delegation:

Simple name of the subdomain for which the NS record is authoritative

Name Server:

FQDN of the nameserver

TTL:

Time to live, in seconds

Cancel Save

Figure 91 "NS" Record Fields

PTR Records

A "PTR" or Pointer record consists of the following three fields:

- **In-Addr** - The fourth octet of the IP address or the entire reverse address appended with in-addr.arpa. For example, for a host with the IP address 172.16.2.42 in the 2.16.172.in-addr.arpa domain, you could enter any of the following:
 - 42
 - 42.2.16.172.in-addr.arpa
 - 42.2.16.172.in-addr.arpa.
- **Points To** - The FQDN of the hostname.
- **TTL**

Add Record: PTR (Pointer)

In-Addr:
42.2.16.172.in-addr.arpa.AddaPTRRecord.com.
The fourth octet of the IP address or the entire reverse address appended with in-addr.arpa.

Points To:
https://www.neustar.ultradns.com
The FQDN of the hostname

TTL:
100
Time to live, in seconds

Cancel Save

Figure 92 "PTR" Record Fields

HINFO Records

The "HINFO" or "Host Info" record consists of the following four fields:

- **Host**
- **Machine Type** - The host's hardware type, entered as free text (maximum of 255 alphanumeric characters).
- **OS** - The host's operating system, entered as free text (maximum of 255 alphanumeric characters).
- **TTL**

Add Record: HINFO (Host Info) ✕

Host:

A valid hostname

Machine Type:

The host's hardware type (maximum of 255 alphanumeric characters)

OS:

The host's operating system (maximum of 255 alphanumeric characters)

TTL:

Time to live, in seconds

Cancel Save

Figure 93 "HINFO" Record Fields

MX Records

An “MX” or “Mail Exchange” record consists of the following four fields:

- **Host** - The domain name of your mail recipient's email addresses (that is, the portion after the @ symbol in the email address).
- **Goes To** - The FQDN of the mail host. The host must have a valid IP address and cannot point to a CNAME (alias).
- **Pref** - A preference integer value between 0–999 that indicates which mailer to use. The preference value is only relevant in comparison to other MX records' values. Lower values have higher priority.
- **TTL**

Add Record: MX (Mail Exchange)

Host:

A valid hostname

Goes To:

FQDN of the mail host

Pref:

A number indicating record preference.
Lowest takes precedence.

TTL:

Time to live, in seconds

Cancel Save

Figure 94 "MX" Record Fields

TXT Records

A “TXT” or “Text” record consists of the following three fields:

- **Host**
- **Comments** - Provide comments as free text.
- **TTL**

Add Record: TXT (Text) ✕

Host:

A valid hostname

Comments:

Freeform ASCII text.

TTL:

Time to live, in seconds

Cancel Save

Figure 95 "TXT" Record Fields

RP Records

An “RP” or “Responsible Person” record consists of the following four fields:

- **Host**
- **RP Email** - The email address of the responsible person or group, entered as either:
 - local-part@domain
 - local-part.domain
- **TXT Records** - The domain that includes a TXT record providing further contact information.
- **TTL**

Add Record: RP (Responsible Person) ✕

Host:

A valid hostname

RP Email:

A valid email address

TXT Records:

Domain that includes a TXT record providing further contact information.

TTL:

Time to live, in seconds

Cancel Save

Figure 96 "RP" Record Fields

SRV Records

An “SRV” or Service Locator record consists of the following fields:

- **Service Name** - The name of the service, which is entered as a combination of the following three fields:
 - Service - the symbolic name of the desired service (with an underscore)
 - Protocol - the transport protocol (usually TCP or UDP) of the desired service (with an underscore)
 - Name - the domain name for the record (with or without the trailing dot)
 - For example: `_sip._tls.example.biz`
- **Target** - The canonical host name of the machine providing the service, entered as an FQDN with or without a trailing dot. Examples include:
 - `targetname.example.biz`
 - `targetname.example.biz.`
- **Priority** - The priority of the target host, entered as an integer. A lower value identifies a higher priority.
- **Weight** - A relative weight for records with the same priority, entered as an integer. A larger value increases the weight.
- **Port** - The Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port on which to find the service.
- **TTL**

Add Record: SRV (Service Locator) ✕

Service Name:

The name of the service

Target:

The canonical host name of the machine providing the service, entered as an FQDN with or without a trailing dot.

Priority:	Weight:	Port:
<input type="text" value="10"/>	<input type="text" value="15"/>	<input type="text" value="443"/>
The priority of the target host, entered as an integer (a lower value will identify a higher priority).	A relative weight for records with the same priority, entered as an integer (a larger value will increase the weight).	The TCP or UDP port on which to find the service.

TTL:

Time to live, in seconds

CancelSave

Figure 97 "SRV" Record Fields

NAPTR Records

An “NAPTR” or Naming Authority Pointer record consists of the following fields:

- **Host** -
- **Service Name** - Specifies the service(s) available down the rewrite path or a protocol. This field must contain a protocol if the Flags field contains P. This field is not case-sensitive.
- **Pref** - Provide an integer value between 0 – 65535 that specifies the processing preference (order) of the NAPTR records (if multiple NAPTR records have equal **Order** values. *Low numbers are processed before higher numbers.*
- **Order** - Provide an integer value to determine the order in which the NAPTR records are supposed to be processed in. *Low numbers are processed before higher numbers.*
- **Flags**: A character string consisting of a single character (from the set [A–Z0–9], that is case insensitive, and that controls aspects of rewriting and interpreting fields in the NAPTR record. Currently, the NAPTR record supports the following four flags:
 - **S** indicates the output of the rewrite will be an SRV record.
 - **A** indicates the output of the rewrite will be an A or AAAA record.
 - **U** indicates the output of the Regexp field is a Uniform Resource Identifier (URI) (which is used in ENUM).
 - **P** indicates the next step is to look for protocol-specific rules in the Services field.
- **Regexp** - (“Regular Expression”) A character string containing a substitution expression applied to a client's original string, in order to construct the next domain name to lookup.
- **Replacement** - An FQDN of the next domain-name to query, depending on the values in the Flags field. Use the Replacement field when the Regexp is a simple replacement operation.
- **TTL**

Additional Examples:

This following NAPTR record set provides three ways to contact example.biz.

Host	Service	Order	Pref	Flags	regexp	Replacement
example.biz	sip+d2u	10	101	S		_sip._udp.example.biz.
example.biz	sip+d2t10	10	102	S		_sip._tcp.example.biz.
example.biz	e2u+email	10	103	S		!^.*\$!mailto:info@example.biz!

This example is the NAPTR set for the phone number 1+202-555-1212, with a preference for SIP, then H323, and finally email.

Host	Service	Order	Pref	Flags	regexp	Replacement
2.1.2.1.5.5.5.2. 0.2.1.itrs.us.	e2u+sip	10	101	U	!^.*\$!sip:info@itrs.us!	
2.1.2.1.5.5.5.2. 0.2.1.itrs.us.	E2U+h323	10	102	U	!^.*\$!h323:info@itrs.us!	
2.1.2.1.5.5.5.2. 0.2.1.itrs.us.	E2U+msg	10	103	U	!^.*\$!mailto:info@itrs.us!	

Add Record: NAPTR (Naming Authority Pointer) ✕

Host:

Service Name:

Specifies the service(s) available down the rewrite path or a protocol.

Order: ? Pref: ? Flag: ?

Regexp:

A regex applied to a client's original string in order to construct the next domain name to lookup.

Replacement:

An FQDN of the next domain-name to query, depending on the values the Flags field.
One of Regexp or Replacement must be defined, but not both.

TTL:

Time to live, in seconds

CancelSave

Figure 98 "NAPTR" Record Fields

SPF Records



Note: Note If you have already implemented SPF using TXT records, the SPF and TXT records must match.

Copy and paste the TXT record's Comments field to the SPF record.

An “SPF” or “Sender Policy Framework” record consists of the following three fields:

- **Host**
- **Comments** - Provide any additional comments as free text.
- **TTL**

Add Record: SPF (Sender Policy Framework)

Host:

www.AddaSPFRecord.com

A valid host name

Comments:

SPF Record 1

Freeform ASCII text.

TTL:

100

Time to live, in seconds

Cancel Save

Figure 99 "SPF" Record Fields

CAA Records

A “CAA” or “Certification Authority Authorization” record consists of the following fields:

- **Host**
- **Flags** - Entered as an integer value between 0 - 255.
- **Property Tag** - Select one of the following options from the dropdown menu.
 - **Issue** - Authorizes the domain name owner to issue certificates for the domain in which the property is published.
 - **Issuewild** - Authorizes the domain name owner to issue wildcard certificates for the domain in which the property is published. Issuewild properties are ignored during processing if the domain is not a wildcard domain. If the domain has a wildcard rrset specified, all other properties will be ignored during processing.
 - **Iodef** - Specifies a URL to which an issuer may report certificate issue requests that are inconsistent with the issuer's Certification Practices or Certificate Policy, or that a Certificate Evaluator may use to report possible policy violations. Accepted schema types are mailto and http/https.
- **Property Value** - Entered as free text.
- **TTL**

Add Record: CAA (Certification Authority Authorization) ✕

Host:

A valid hostname

Flags: Property Tag: ?

An integer value between 0-255

Property Value:

 G

Entered as free text, in a format that will vary according to the value of Property Tag

TTL:

Time to live, in seconds

Cancel Save

Figure 100 "CAA" Record Fields

TLSA Records

A “TLSA” or Transport Layer Security Protocol record consists of the following fields:

- **Host**
- **Port** - Enter an integer value between 0 - 65535.
- **Service** - Select one of the following options from the dropdown menu:
 - **tcp** – Transmission Control Protocol
 - **udp** – User Datagram Protocol
 - **sctp** – Stream Control Transmission Protocol
- **Selector** - The Selector Field specifies which part of the TLS certificate presented by the server will be matched against the association data. Select one of the options from the dropdown menu:
 - Full Certificate - The certificate binary structure.
 - SubjectPublicKeyInfo – Distinguished Encoding Rules (DER) encoded binary structure.
- **Matching** - The Matching Type specifies how the certificate association is presented. Select one of the following options from the dropdown menu:
 - **0** - An exact match of the selected content.
 - **1** - SHA-256 hash match of the selected content.
 - **2** - SHA-512 hash match of the selected content.
- If the TLSA record's matching type is a hash, having the record use the same hash algorithm that was used in the signature in the certificate (if possible) will assist clients that support a small number of hash algorithms.
- **Usage** - Select one of the following options from the dropdown menu:
 - **0 (CA Constraint)** - The certificate or public key MUST be found in any of the Public Key Infrastructure (PKIX) certification paths for the end entity certificate given by the server in Transport Layer Security (TLS). This certification limits which CAs can be used to issue certificates for a given service.
 - **1 (Service Certificate Constraint)** - Used to specify an end entity certificate (or the public key) that MUST be matched with the end entity certificate given by the server in TLS. This certification limits which end entity certificate can be used by a given service on a host.
 - **2 (Trust Anchor Assertion)** - Used to specify a certificate (or the public key) that MUST be used as the “trust anchor” when validating the end entity certificate given by the server in TLS. This certification allows a domain administrator to specify a trust anchor. For example, if the domain issues its own certificates under its own CA that is not expected to be in the end user's collection of trust anchors.
 - **3 (Domain-Issued Certification)** - Used to specify a certificate (or the public key) that MUST match the end entity certificate given by the server in TLS. This certification allows for a domain named administrator to issue certificates for a domain without involving a third-party CA. This certificate does NOT need to pass PKIX validation.
- **Data** - Enter the hexadecimal string value for the certificate.
- **TTL**

Add Record: TLSA (TLS Association) ✕

Host:

Port:

Service:

www.AddaTLSARecord.com

444

tcp

The actual hostname will be generated from a combination of Host, Port and Service:

Selector: ?

Matching: ?

Usage: ?

FullCertificate

Exact match

1

Data:

4e6575737461722

A hexadecimal string

TTL:

100

Time to live, in seconds

Cancel

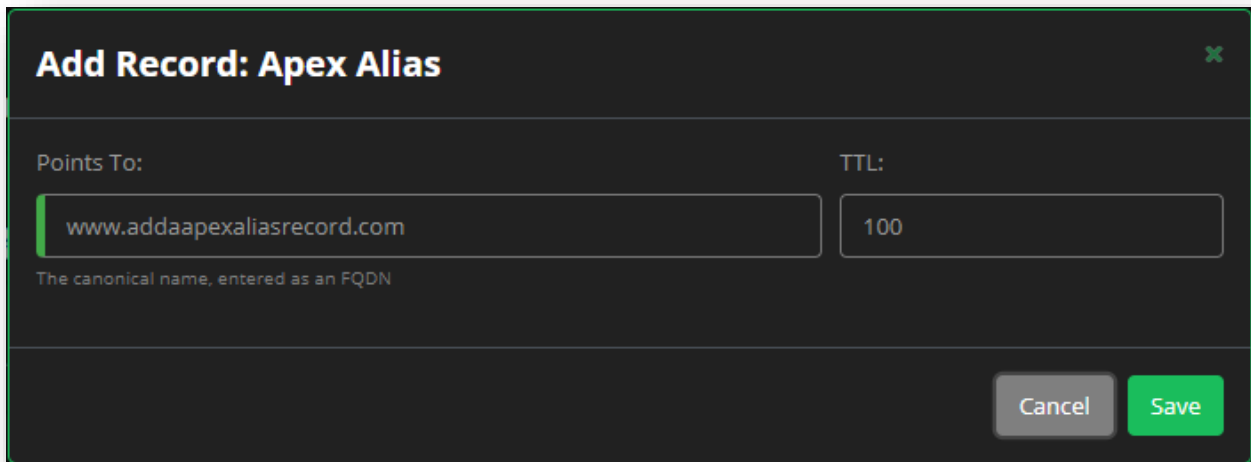
Save

Figure 101 "TLSA" Record Fields

Apex Alias Records

An “Apex Alias” record consists of the following two fields:

- **Points To:** Provide the hostname the Apex Alias is pointing to.
- **TTL**



Add Record: Apex Alias ✕

Points To: TTL:

The canonical name, entered as an FQDN

Cancel Save

Figure 102 "Apex Alias" Record Fields

SSH Fingerprint

The DNS Secure Shell Fingerprint (SSHFP) record provides a way to verify Secure Shell (SSH) host keys using Domain Name System Security (DNSSEC). The SSHFP record is used to provide out-of-band verification, which looks up the SSHFP fingerprint of the server public key in DNS, and then uses DNSSEC to verify the lookup.

An SSH client connecting to an SSH server can look up the SSHFP resource records for the host it is connecting to. The algorithm and fingerprint of the key from the SSH server are matched against the algorithm and fingerprint combinations in the SSHFP resource records (RR). The SSHFP RR includes the owner name, algorithm, type, fingerprint, and time to live (ttl) associated with it.

The SSHFP record consists of the following validation fields:

- **Host** - Entered as a standard host name validation.
- **Algorithm** - Select one of the following options from the dropdown menu.
 - RSA
 - DSS
 - ECDSA
 - A
 - Ed25519
- **Hash Type** - The Algorithm used to hash the public key. Select one of the following options from the dropdown menu.
 - SHA-1
 - SHA-256
- **Fingerprint** - Provide the hexadecimal value of the key.
- **TTL**

Add Record: SSH Fingerprint ✕

Host:

Algorithm: Hash Type:

RSA ▾

SHA-256 ▾

Fingerprint:

A hexadecimal string

TTL:

Time to live, in seconds

CancelSave

Figure 103 Create an SSH Fingerprint Record

Delegation Signer

The DNS Delegation Signer (DS) record indicates that the delegated zone is digitally signed and contains the hash of the DNSSEC Key Signing Key (KSK).

The DS record contains the following fields:

- **Host** - Entered as a standard host name validation.
- **Key Tag** - A number between 0 and 65535 used to match the key to the signature that generated it.
- **Algorithm** - The algorithm in the referenced DNSKEY record. Select one of the following options from the dropdown menu.
 - RSA/MD5 (1)
 - Diffie-Hellman (2)
 - DSA/SHA-1 (3)
 - Elliptic Curve (4)
 - RSA/SHA-1 (5)
 - Indirect (252)
- **Hash Type** - The algorithm used to hash the public key. Select one of the following options from the dropdown menu.
 - SHA-1 (1)
 - SHA-256 (2)
- **Digest** - Provide the hexadecimal value of the key. For SHA-1 the length of the digest key will be 40. For SHA-2 the length of the digest key will be 64.
- **TTL**

In the following example DS record:

- DS 12345 3 1 123456789abcdef67890123456789abcdef67890
 - 12345 is the key tag
 - 3 is the algorithm (DSA/SHA-1 in this case)
 - 1 is the hash type (SHA-1 in this case)
 - 123456789abcdef67890123456789abcdef67890 is the forty-character digest key.

Add Record: DS (Delegation Signer) ✕

Host:

Key Tag:

A value between 0 and 65535

Algorithm: Digest Type:

Digest:

A hexadecimal string

TTL:

Time to live, in seconds

Figure 104 Create a Delegation Signer Record

Web Forwarding

A Web Forwarding record redirects queries to another site. Utilizing this feature, you can denote a domain, site, directory, or page that you want to redirect.

UltraDNS supports HTTP to HTTP or HTTP to HTTPS forwarding. UltraDNS does not support HTTPS to HTTP or HTTPS to HTTPS forwarding.

The Web Forwarding record is comprised of the following fields:

- **Requests To** – The domain, site, directory or page that you want to redirect. This field can be left blank, and will by default, use your zone/domain name.
 - You can use the wildcard character (*) in the string. Using a wildcard on a redirection record tells the server to match the most specific string, and then append any unmatched portion of the source URL to the target URL.
- **Redirects To** – The location that you want to redirect to. This can be a domain, site, directory or a page.
 - You can use the wildcard character (*) in this field as well.
- **Type** – Select a redirect type from the drop-down menu.
 - **301 Redirect** - Permanent Redirect
 - **302 Redirect** - Found (unspecified reason redirect)
 - **303 Redirect** - See Other
 - **307 Redirect** - Temporary Redirect
 - **Framed** - Creates an invisible frame set and loads the destination URL in the frame, thus making it more difficult to determine that a redirection has occurred. The disadvantage to this approach is that any bookmarks created by the user while navigating the site will point to the home page of the original URL.
- **Relative Forward** – When enabled, appends a portion of the incoming URL to the Redirects To URL provided by using one of the following options:
 - **Path** – The incoming Parameter will be discarded.
 - **Parameter** – The incoming Path will be discarded.
 - **Parameter & Bath (Both)** - Both the Path and Parameter are both appended appropriately.

The following example demonstrates how each Relative Forwarding Type works. If your **Requests To** field is `www.Neustar.biz/documents?a=userguide#supp`, and your **Redirects To** field is `www.Neustar.biz/support?c=sales#home`, then:

- **Path** will append the response to - `www.Neustar.biz/documents/support?a=userguide#supp`. The Path `/Support` is appended to the Requests To `/documents`. The incoming parameter is removed.
- **Parameter** will append the response to - `www.Neustar.biz/documents?a=userguide&c=Sales#supp`. The incoming path is removed.
- **Parameter and Path** will append the response to - `www.neustar.biz/documents/support?a=userguide&c=sales#supp`. The incoming parameter AND path are both appended.

Add Record: Web Forwarding ✕

Requests To:

www.neustar.biz/documents?a=userguide#supp

The domain, site, directory, or page that you want to redirect

Redirects To:

www.neustar.biz/support?c=sales#home

Type: HTTP 301 REDIRECT ▼

The domain, site, directory, or page to redirect to

Relative Forward:

No ☒ Yes

Type:

☒ Parameter

☐ Path

☐ Parameter & Path

Cancel Save

Figure 105 Create a Web Forwarding Record

Reports

The UltraDNS Portal Reports section provides various report types that display your account details and record query results.

To access the Reports section, use the left-hand navigation pane and click on the **Reports** link. A list of available reports will appear, along with an **Account** drop-down menu that will allow you to change the account you are viewing the report for (if you have access to multiple accounts).

At the top of the screen you will see a button for **LAUNCH ULTRADNS REPORT CENTER**. Clicking on this button will take you to our Reporting website where you can access additional reports and details for your account. For more details, please refer to the [Report Center User Guide](#).

Usage Summary Report

The Usage Summary Report displays peak data statistics for an account for the last thirty-six months. Each month that is returned consists of domains counts, record type counts, and query statistics for the given account.

The following content for the report is displayed:

- **Domains** - The peak (highest) number of domains that existed for your account during the month.
- **Records** - The peak number of records that existed for your account.
- **Query Responses** - The total number of DNS Query Responses that were served by your account.
- **URL Forward** - The peak number of URL or Web Forwarding requests that existed for your account.
- **Email Forward** - The peak number of Email Forwarding requests that existed for your account.
- **SB Records** - The peak number of SiteBacker records that existed for your account.
- **TC Records** - The peak number of Traffic Controller records that existed for your account.
- **Directional Records** - The peak number of Directional Records/Pools that existed for your account.

When viewing the Usage Summary Report, you may see various colors displayed with your data. The following table provides an explanation of the different colors you may see, and any action (if any) required.

Table 4 Usage Summary Report - Color Designations

Color	Description / Action
Red	100% usage. Contract Threshold Exceeded. Contact Neustar immediately to increase the threshold.
Orange	90-99.9% usage. Contact Neustar to increase the threshold before usage is exceeded.

Color	Description / Action
Yellow	80-89% usage. Usage near threshold. Monitor usage closely to avoid exceeding threshold.
White	<80% usage. No action needed at this time

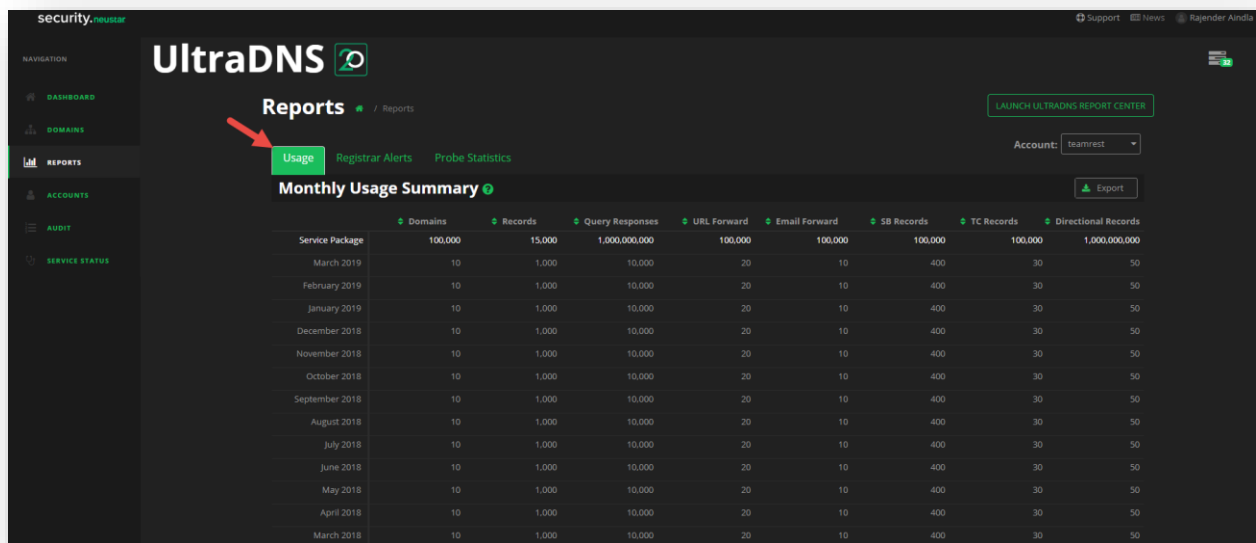


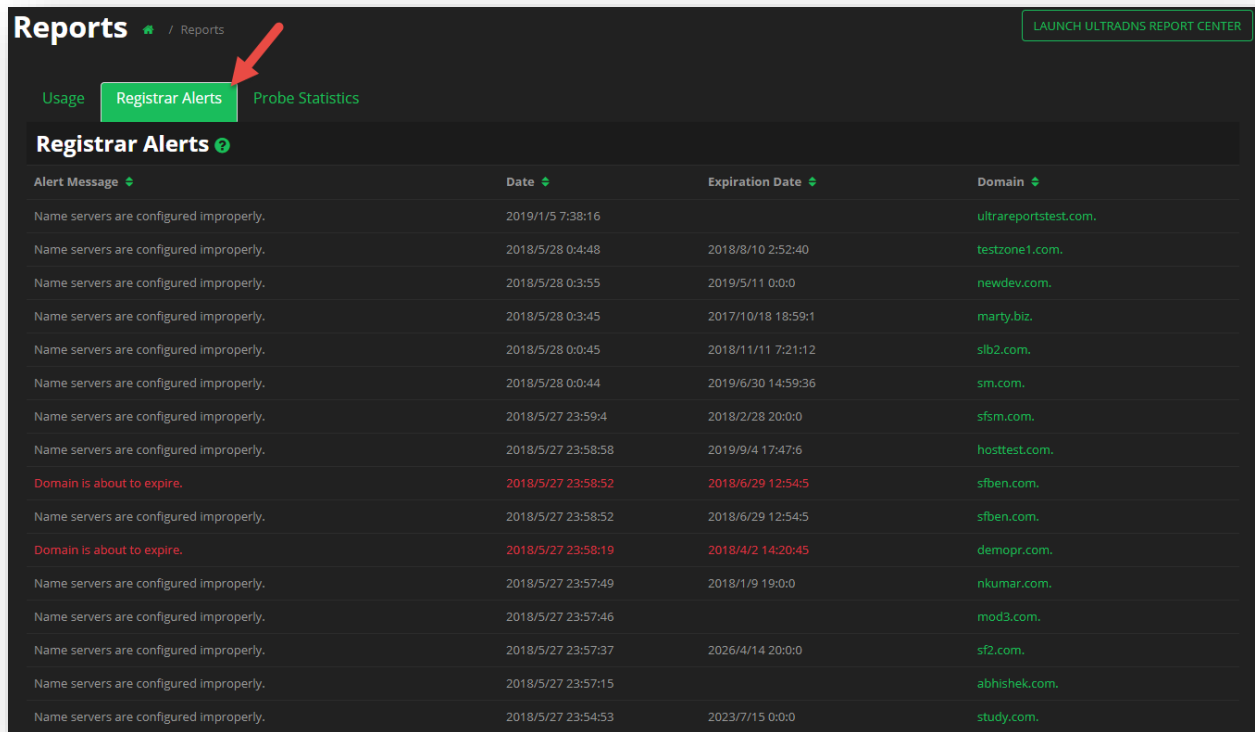
Figure 106 Reports - Usage Summary Report

Domain Alerts Report

The Domain Alerts report displays alerts that include invalid registration for domains, as well as domain expirations.

Each alert contains the following:

- **Alert Message** – Displays a basic message explaining why the alert was triggered.
- **Date** – The date in which the alert was triggered.
- **Expiration Date** – For
- **Domain** – Lists the domain for which the alert was triggered. You can click on the domain to navigate directly to that domain and its details.



Reports / Reports LAUNCH ULTRADNS REPORT CENTER

Usage **Registrar Alerts** Probe Statistics

Registrar Alerts

Alert Message	Date	Expiration Date	Domain
Name servers are configured improperly.	2019/1/5 7:38:16		ultrareporttest.com.
Name servers are configured improperly.	2018/5/28 0:4:48	2018/8/10 2:52:40	testzone1.com.
Name servers are configured improperly.	2018/5/28 0:3:55	2019/5/11 0:0:0	newdev.com.
Name servers are configured improperly.	2018/5/28 0:3:45	2017/10/18 18:59:1	marty.biz.
Name servers are configured improperly.	2018/5/28 0:0:45	2018/11/11 7:21:12	sib2.com.
Name servers are configured improperly.	2018/5/28 0:0:44	2019/6/30 14:59:36	sm.com.
Name servers are configured improperly.	2018/5/27 23:59:4	2018/2/28 20:0:0	sfsn.com.
Name servers are configured improperly.	2018/5/27 23:58:58	2019/9/4 17:47:6	hosttest.com.
Domain is about to expire.	2018/5/27 23:58:52	2018/6/29 12:54:5	sfben.com.
Name servers are configured improperly.	2018/5/27 23:58:52	2018/6/29 12:54:5	sfben.com.
Domain is about to expire.	2018/5/27 23:58:19	2018/4/2 14:20:45	demopr.com.
Name servers are configured improperly.	2018/5/27 23:57:49	2018/1/9 19:0:0	nkumar.com.
Name servers are configured improperly.	2018/5/27 23:57:46		mod3.com.
Name servers are configured improperly.	2018/5/27 23:57:37	2026/4/14 20:0:0	sf2.com.
Name servers are configured improperly.	2018/5/27 23:57:15		abhishek.com.
Name servers are configured improperly.	2018/5/27 23:54:53	2023/7/15 0:0:0	study.com.

Figure 107 Reports - Domain Alerts

Probe Statistics

The Probe Statistics report allows you search by Zone Name, as well as by a specific pool type to return probe results within a time period for the designated zone and pool combination.

The Probe Statistics Report is broken down into two reports: **Probe Summary** which is a basic overview of data, and **Probe Details** which provides a more detailed account of the results returned.

Additionally, each report provides different results based upon the Pool Type you select. Once results are returned, you can click on a returned value to

Simple Load Balancing or Simple Failover / Monitor

1. Provide a **Zone Name** (the report will search by Wildcard).
2. Select a **Pool Type** from the drop-down menu.
3. Click into the **From** field to select a beginning date from the calendar that appears.
 - a. The start date cannot be more than 6 months older than the current date.
4. Click into the **To** field to select an ending date from the calendar that appears.
 - a. The end date cannot be more than seven (7) calendar days from the start date.

5. Optionally, you can provide a **Pool Name** to narrow the search.
6. Click the **Apply Filter** button when you are done.

Reports / Reports LAUNCH ULTRADNS REPORT CENTER

Usage Registrar Alerts **Probe Statistics**

Filters

Zone Name: PoolType:

From: To:

The period between 'From Date' and 'To Date' cannot be more than 7 days.

Pool Name:

Figure 108 Probe Statistics Report - Simple Load Balancing or Simple Monitor / Failover

Reports / Reports LAUNCH ULTRADNS REPORT CENTER

Usage Registrar Alerts **Probe Statistics**

Filters

Zone Name: PoolType:

From: To:

The period between 'From Date' and 'To Date' cannot be more than 7 days.

Pool Name:

Probe Summary

Zone Name	Zone	Pool Type	From	To	Successes	Failures	Total
Z		SIMPLE FAILOVER	2019-03-26 10:25:58 GMT	2019-04-02 10:25:57 GMT			
Account Name	Zone	Pool	Successes	Failures	Total		
teamrest	dGlmCA5FNj4CNORazCVVboejxyl8T3t-sanityzone.com.	testchroniclerSF	4	4	4		
teamrest	KCVpY3zkLSpT3v8UIPpuyUPtDoUbleTe-sanityzone.com.	testchroniclerSF	4	4	4		

Figure 109 Probe Statistics Report - SLB and SM/SF - Probe Summary Results

The Probe Summary Report for Simple Load Balancing and/or Simple Monitor / Failover pools returns the following data:

- **Account Name** – The account name associated to the logged in user, and that the zone belongs to.
- **Zone** – The full zone name that was queried.
- **Pool** - The specific Simple Load Balancing or Simple Monitor / Failover Pool name that is under the Zone being queried.
- **Successes** - The count and percentage of Probes that were successful for the Pool / Zone account combination.
- **Failures** - The count and percentage of Probes that failed for the Pool / Zone account combination.
- **Total** - The total number of Probes that were returned for the Account / Zone / Pool combination.

If any matching results are found, the **Probe Summary** report results will be displayed. For any integer values in green, you can click on the value to view the specific **Probe Result Details** report, which will provide additional details for the specific Zone / Pool type you selected.

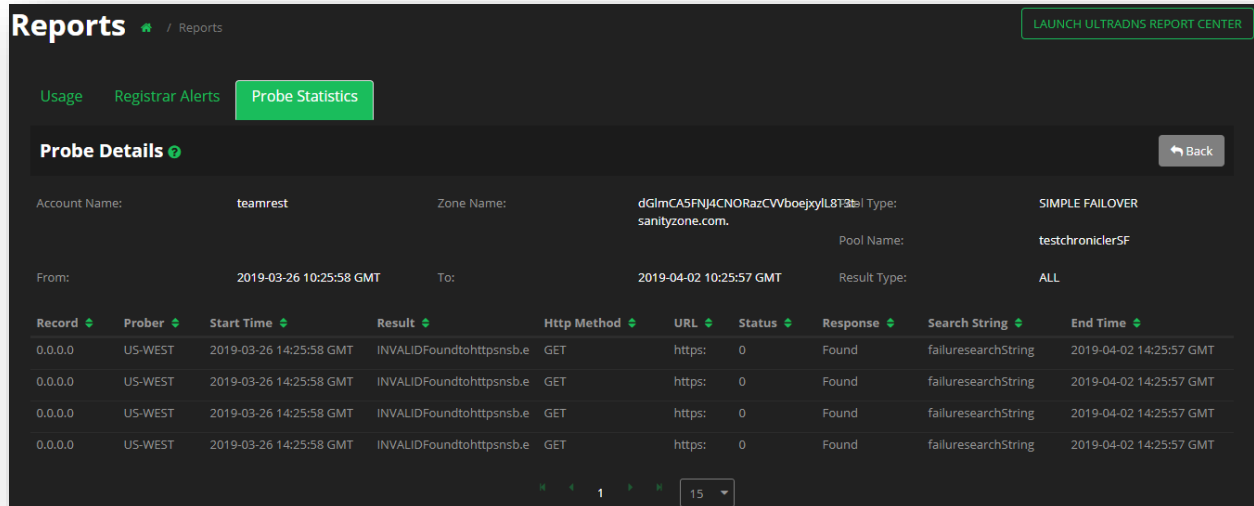


Figure 110 Probe Statistics - Probe Details Report SLB and SM/SF

The Probe Details Report for Simple Load Balancing and/or Simple Monitor / Failover returns the following data:

- **Record** - The IP address within the pool that was being probed.
- **Prober** - The region from which the record was being probed.
- **Start Time** - The start time and date in which the probing began.
- **Result** - Whether the probe was Successful, or why it Failed.
- **Http Method** - The type of method that was used during the probing.
- **URL** - The URL that was used for the Probing.
- **Status** - The response (code) that was returned as part of the Probe response.

- **Response** - The response message that was returned by the probe.
- **Search String** - The string that was searched within the Probe response, and used in order to determine the Probe Result.
- **End Time** - The time and date that the probing finished.

SiteBacker or Traffic Controller

1. Provide a **Zone Name** (the report will search by Wildcard).
2. Select a **Pool Type** from the drop-down menu.
3. Click into the **From** field to select a beginning date from the calendar that appears.
 - a. The start date cannot be more than 6 months older than the current date.
4. Click into the **To** field to select an ending date from the calendar that appears.
 - a. The end date cannot be more than seven (7) calendar days from the start date.
5. You can provide a **Pool Name** to narrow the search.
6. You can provide a **Pool Record Type** to further narrow down the search results.
7. Using the **Account Name** drop-down menu, select an account you want to return the report results for.
8. You can provide a **Pool Record** to further narrow down the search results.
9. Using the **Pool Probe Region** drop-down menu, you select a specific region you wish to return results for.
10. Click the **Apply Filter** button when you are done.

The screenshot displays the 'Reports' section of the Neustar interface, specifically the 'Probe Statistics' filter panel. The panel is titled 'Filters' and contains several input fields and dropdown menus. A red arrow points to the 'PoolType' dropdown menu, which is currently set to 'Site Backer'. Below the 'From' and 'To' date fields, a note states: 'The period between 'From Date' and 'To Date' cannot be more than 7 days.' At the bottom right of the filter panel, there are two buttons: 'Reset' and 'Apply Filter'.

Field	Value
Zone Name	z
PoolType	Site Backer
From	03/26/2019 10:25:58
To	04/02/2019 10:25:57
Pool Name	
Account Name	teamrest
Pool Record Type	
Pool Record	
Pool Probe Region	None

Figure 111 Probe Statistics Report - SiteBacker or Traffic Controller

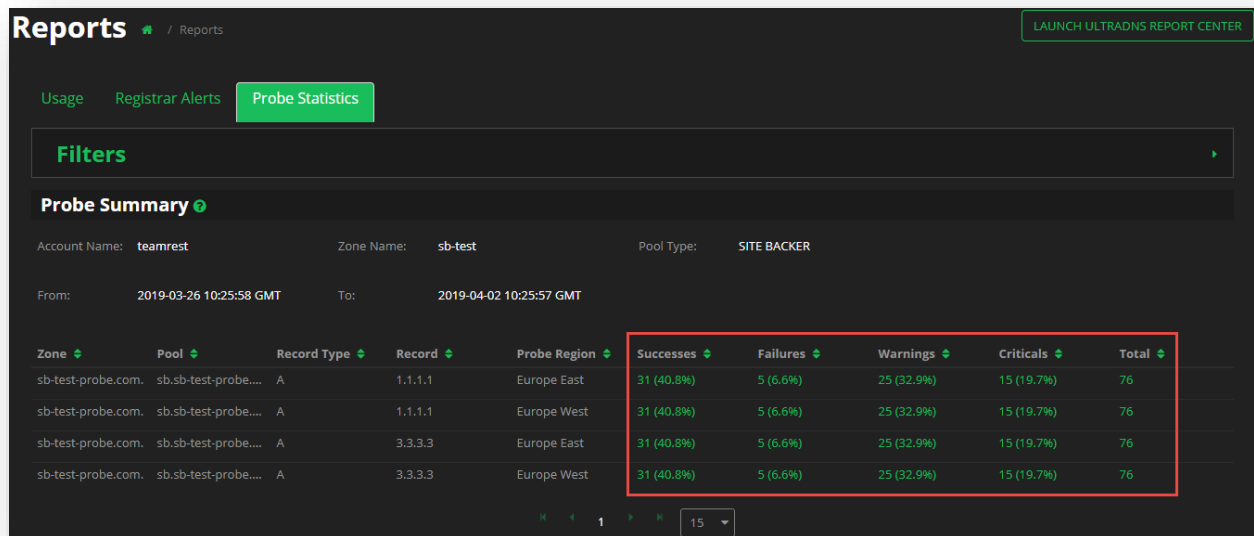
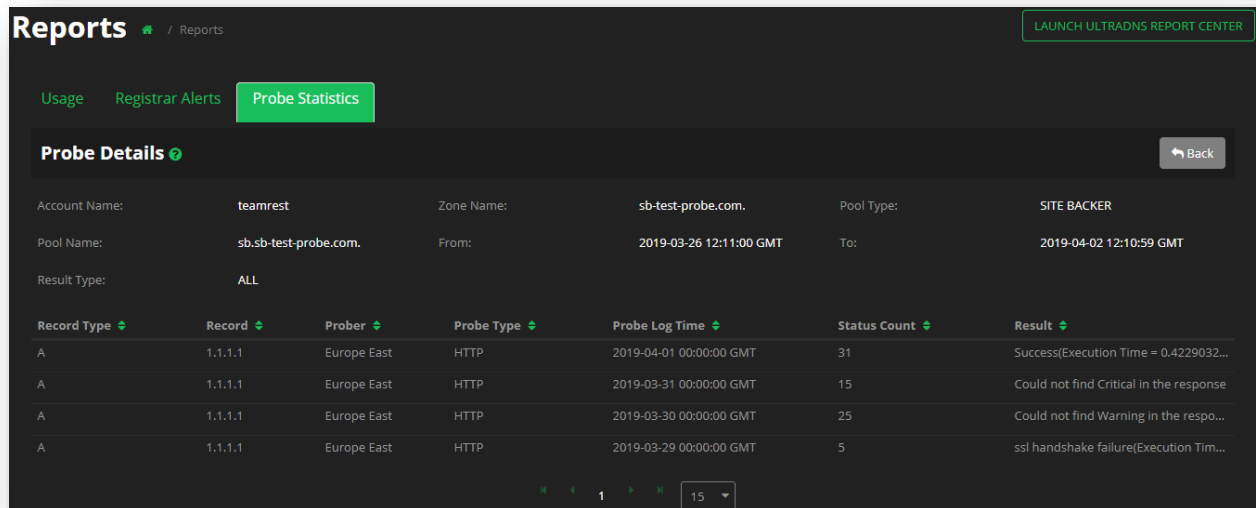


Figure 112 Probe Statistics Report - SB or TC - Probe Summary Results

The Probe Summary Report for SiteBacker and/or Traffic Controller pools returns the following data:

- **Zone** - The full Zone Name that was being queried.
- **Pool** - The specific SiteBacker or Traffic Controller Pool name that is under the Zone being queried.
- **Record Type** - The type of record within the pool that was queried.
- **Record** - The IP address for the record that was queried.
- **Probe Region** - The Region that performed the query.
- **Successes** - The count and percentage of Probes that were successful for the Pool / Zone account combination.
- **Failures** - The count and percentage of Probes that failed for the Pool / Zone account combination.
- **Warnings** - The count and percentage of Probes that indicated a warning for the Pool / Zone account combination.
- **Criticals** - The count and percentage of Probes that indicated a critical issue for the Pool / Zone account combination.
- **Total** - The total number of Probes that were returned for the Account / Zone / Pool combination.

If any matching results are found, the **Probe Summary** report results will be displayed. For any integer values in green, you can click on the value to view the specific **Probe Result Details** report, which will provide additional details for the specific Zone / Pool type you selected.



Reports / Reports LAUNCH ULTRADNS REPORT CENTER

Usage Registrar Alerts **Probe Statistics**

Probe Details Back

Account Name: teamrest Zone Name: sb-test-probe.com. Pool Type: SITE BACKER

Pool Name: sb.sb-test-probe.com. From: 2019-03-26 12:11:00 GMT To: 2019-04-02 12:10:59 GMT

Result Type: ALL

Record Type	Record	Prober	Probe Type	Probe Log Time	Status Count	Result
A	1.1.1.1	Europe East	HTTP	2019-04-01 00:00:00 GMT	31	Success[Execution Time = 0.4229032...
A	1.1.1.1	Europe East	HTTP	2019-03-31 00:00:00 GMT	15	Could not find Critical in the response
A	1.1.1.1	Europe East	HTTP	2019-03-30 00:00:00 GMT	25	Could not find Warning in the respo...
A	1.1.1.1	Europe East	HTTP	2019-03-29 00:00:00 GMT	5	ssl handshake failure[Execution Tim...

1 15

Figure 113 Probe Statistics - Probe Details Report SB or TC

The Probe Details Report for SiteBacker and/or Traffic Controller returns the following data:

- **Record Type** - The type of record that was queried within the pool.
- **Record** - The IP address within the pool that was being probed.
- **Prober** - The region from which the record was being probed.
- **Probe Type** - The type of method that was used during the probing.
- **Probe Log Time** - The time at which the probe was received, and the results were logged.
- **Status Count** - The Number of times this result was received for this probe request.
- **Result** - The explanation as to why the probe returned with the corresponding **Result Type**.

Projected Query Volumes Report

The Projected Query Volumes (PQV) report provides a snapshot of projected monthly volumes based on seven and thirty day average query amounts. The **Projected Query Volumes Report** can be found on the **Dashboard** of the UI Portal.

The details returned by the Projected Query Volume Report for a user that has access to multiple accounts will be consolidated across all of these accounts.

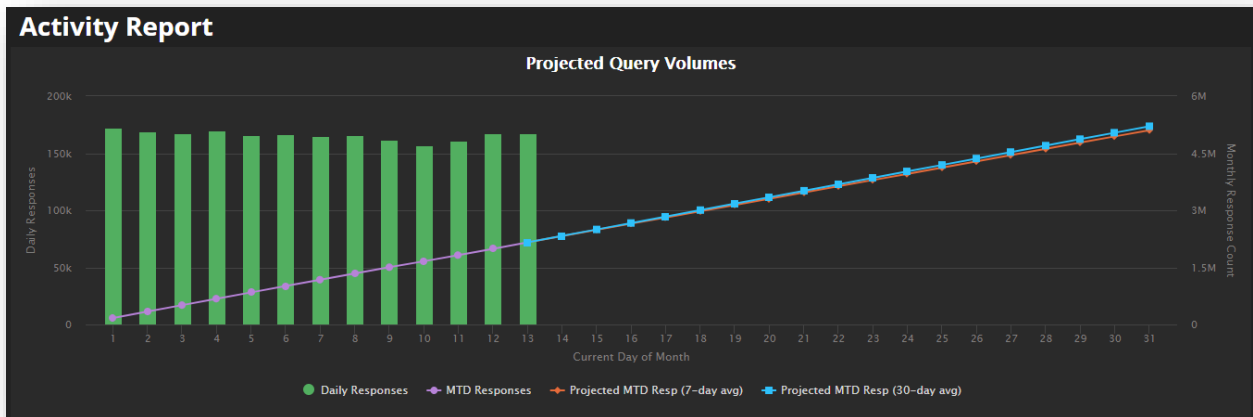


Figure 114 Reports - Projected Query Volumes

The PQV report is displayed using the following parameters: **Daily Responses** and the **Current Day of Month**. You can hover over each data point in the chart to view the specific daily response value for the given date. The data is broken down into the following categories:

- Daily Responses – The captured responses for the day.
- MTD Responses – The month to day responses.
- Projected MTD Resp – Based upon the previous day's averages, projects what the next seven days response count will be.
- Projected MTD Resp – Based upon previous day's averages, projects what the next 30 day average will be. This number will change as additional data for the month is captured.

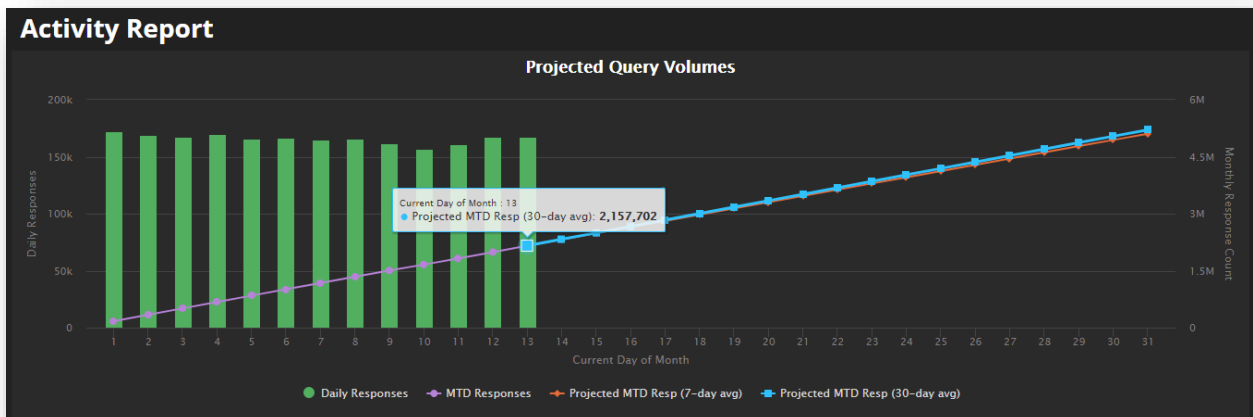


Figure 115 Reports - PQV Report - Data Point Capture

Accounts

The Accounts feature displays the current accounts that are associated to the username and password that you logged in with.

The Accounts page displays the following information:

- **Account** – The name of the account.
- **Account Holder** – The username associated to the account.
- **Primary User** – The name of the individual associated to the account holder name.
- **Users** – The total number of users that belong to the account.
- **User Groups** – The number of user groups associated to the account.

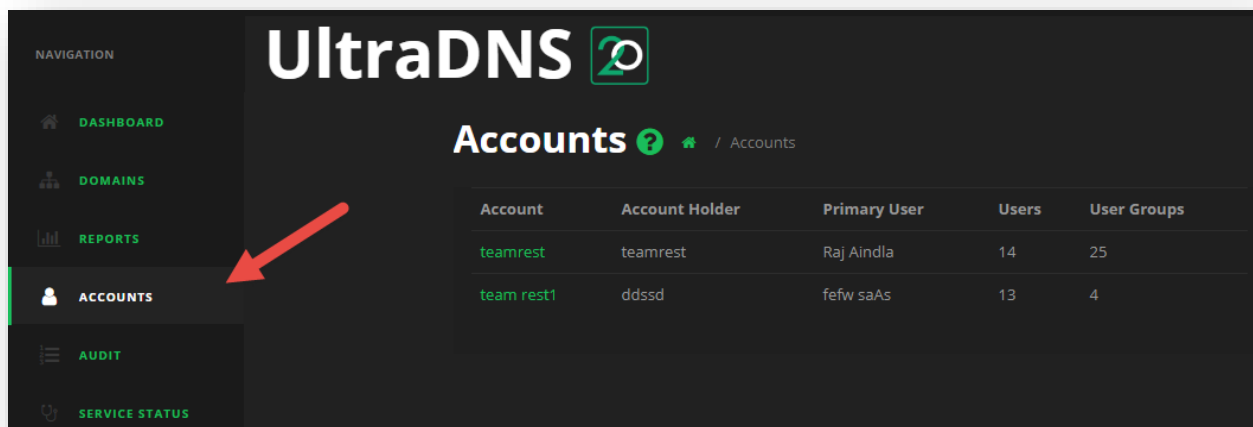


Figure 116 Accounts Landing Page

Once you select an Account, you will be taken to the *Account Details* page.

Users and Groups

The Users and Groups section displays the organizational groups you have created for your account, the system generated groups, as well as any users that have been created or invited to join the UI Portal in association to your account.

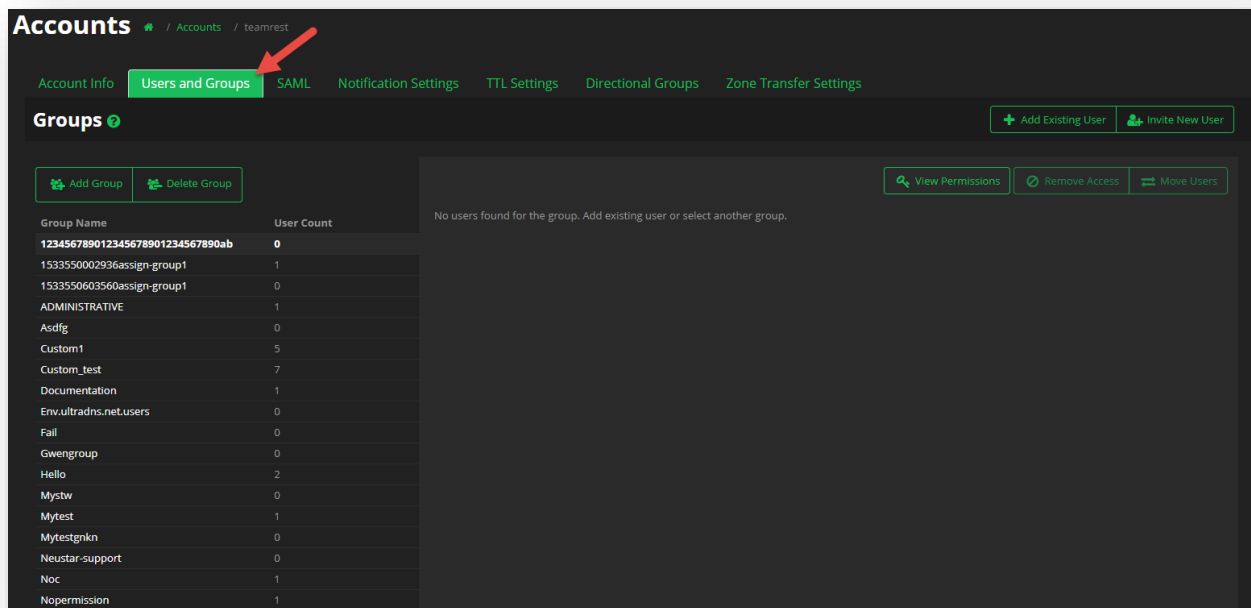
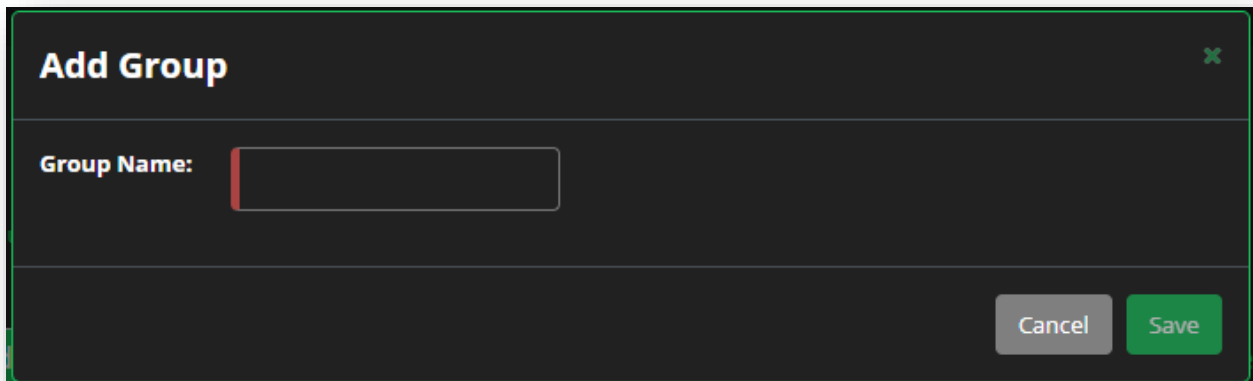


Figure 117 Accounts – Users and Groups

Add Group

To add a new group to your account:

1. Click the **Add Group** button.
2. Provide a Group Name.
3. Click **Save**.



Add Group

Group Name:

Cancel Save

Figure 118 Accounts – Users and Groups - Add Group

Your new group will be listed in the Group Name list on the left-hand side of the screen.

Invite Users (to a Group)

To invite users (to a group) on the UI Portal:

1. Click on the group name from the list on the left-hand side of the screen.
 - a. The group name you select will remain highlighted.
 - b. Any existing users will be listed in the middle of the screen.
2. Click the **Invite User** button in the upper right-hand section of the screen.
3. Select the appropriate Account name from the **Invite to Account** drop-down menu.
4. Select the group you want to assign the user to from the **Assign to Group** drop-down menu.
 - a. If the new user should only have access to the API, click in the check box for API only access.
5. Provide the email address(es) for the user(s) you wish to add to the group.
 - a. Multiple email addresses should be comma separated.
6. Click the **Invite** button when you are finished.

Invite Users

Invite to Account:

teamrest

A valid account name

Assign to Group:

Not in a Group

A valid group name

☐ API only access:

Email addresses (comma separated):

A valid email

Close Invite

Figure 119 Accounts – Users and Groups - Invite User(s)

Moving Users to Groups

To move an existing user to a new group:

1. Select the group from the list of available group names that the user is currently assigned to.
2. Click the check box next to the user's name.
3. Click the **Move Users** button.
4. Select the **Destination** using the drop-down menu to select the new group to move the user to.
5. Click the **Move** button to move the user to the new group.

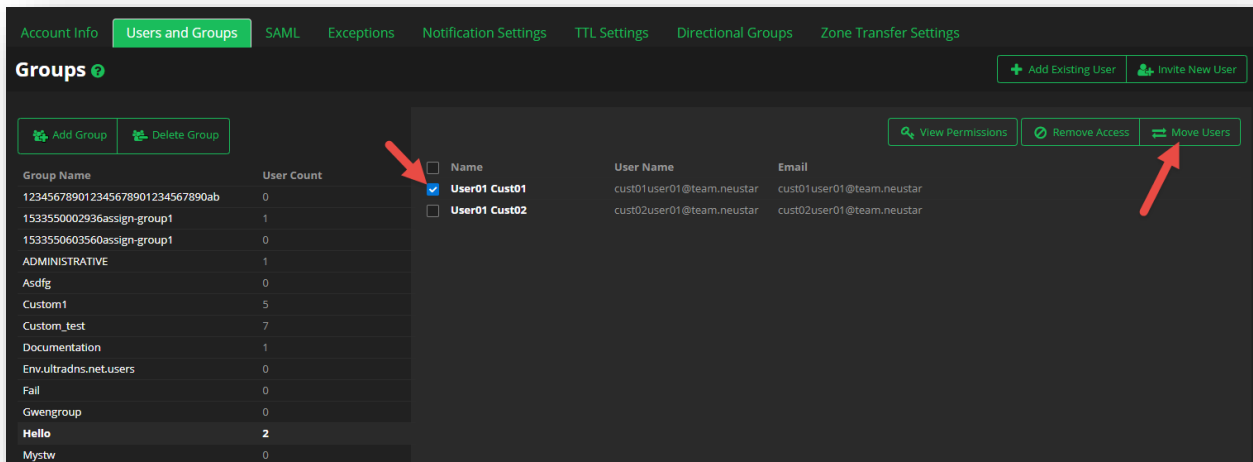


Figure 120 Accounts – Users and Groups - Moving a User

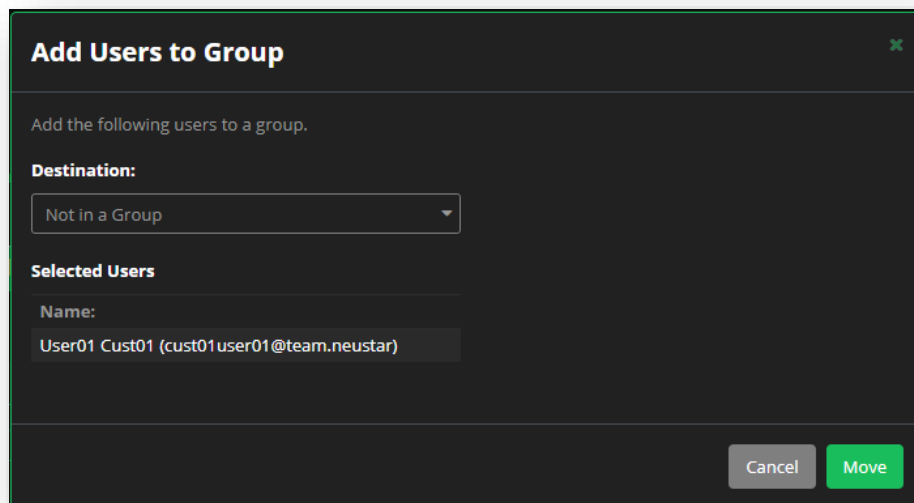


Figure 121 Accounts – User Groups - Moving a User cont.

Removing Access to a Group

To remove a user's access to a group:

1. Select the group that the user currently belongs to.
2. Click the check box next to the user's name.
3. Click the **Remove Access** button.
4. Confirm you want to remove the user from the group by clicking the **Remove** button.

IMPORTANT: Once removed, the designated user will no longer have access to the group.

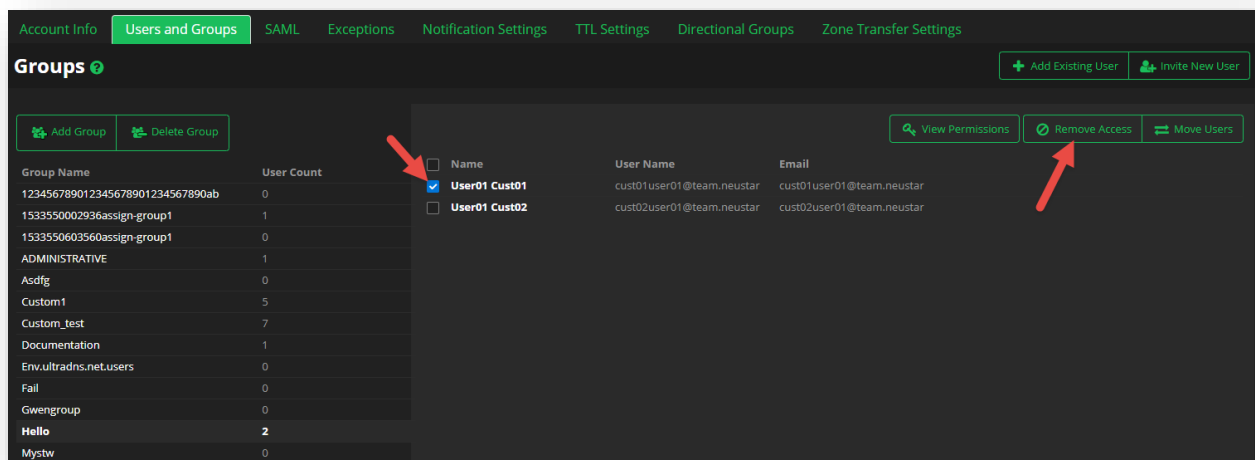


Figure 122 Accounts – User Groups - Remove Access

Deleting a Group

To delete a group from the UI portal:

1. Click the **Delete Group** button.
2. Select the group name from the drop-down menu (if there are any that are able to be deleted).
3. Confirm the deletion of the group by clicking the **Delete** button.
 - a. Any users associated with the group will automatically lose their access to the group.

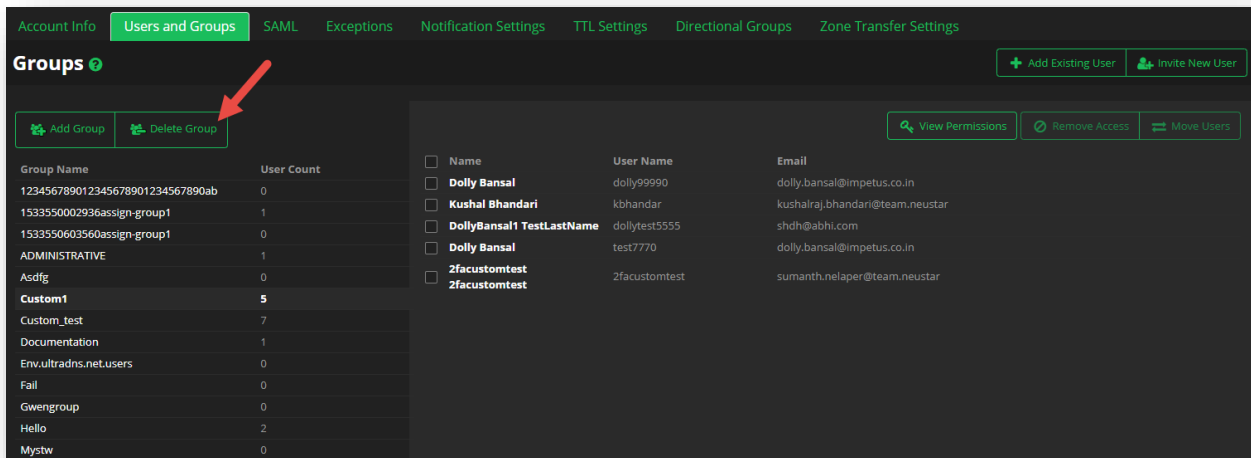


Figure 123 Accounts – Users and Groups - Delete Group

Permissions

The Permission section of the UI Portal allows you to customize by group, the permissions that users within that group will have throughout the UI Portal. As users can be a part of multiple groups, their permissions will be based upon the highest allowable permission granted to them.

For instance, if a user is in Group A with Read, Write and Create, and also in Group B with only Read, that user will maintain Read, Write, and Create permissions across the UI Portal even though their Group B permissions are only for Read access.

To access the Permissions for Groups:

1. Click on **User Groups** from the Accounts page.
2. Click on a **Group Name** from the list of available groups.
3. Click the **View Permissions** button.

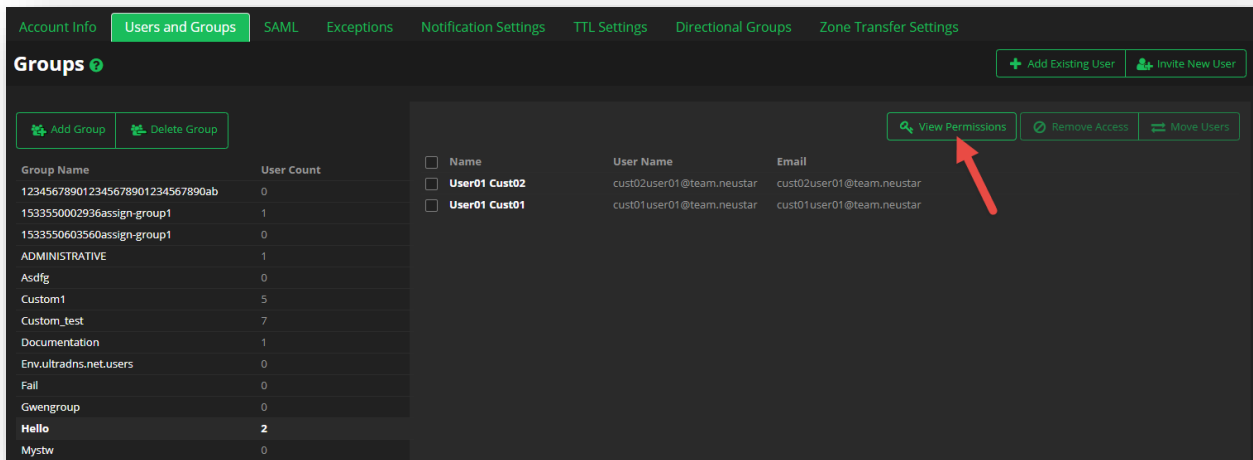


Figure 124 Users and Groups - View Permissions

4. Use the slider bar to increase or decrease the permissions for a specific **Type**, and then click **Save** when you are done setting the permission level.
 - a. The following are the different permission levels you can apply (permission types cannot be customized):
 - i. None
 - ii. Read
 - iii. Read Write
 - iv. Read Write Create
 - v. Read Write Create Delete
 - vi. Read Write Create Grant
 1. Reports can have either None or Read.

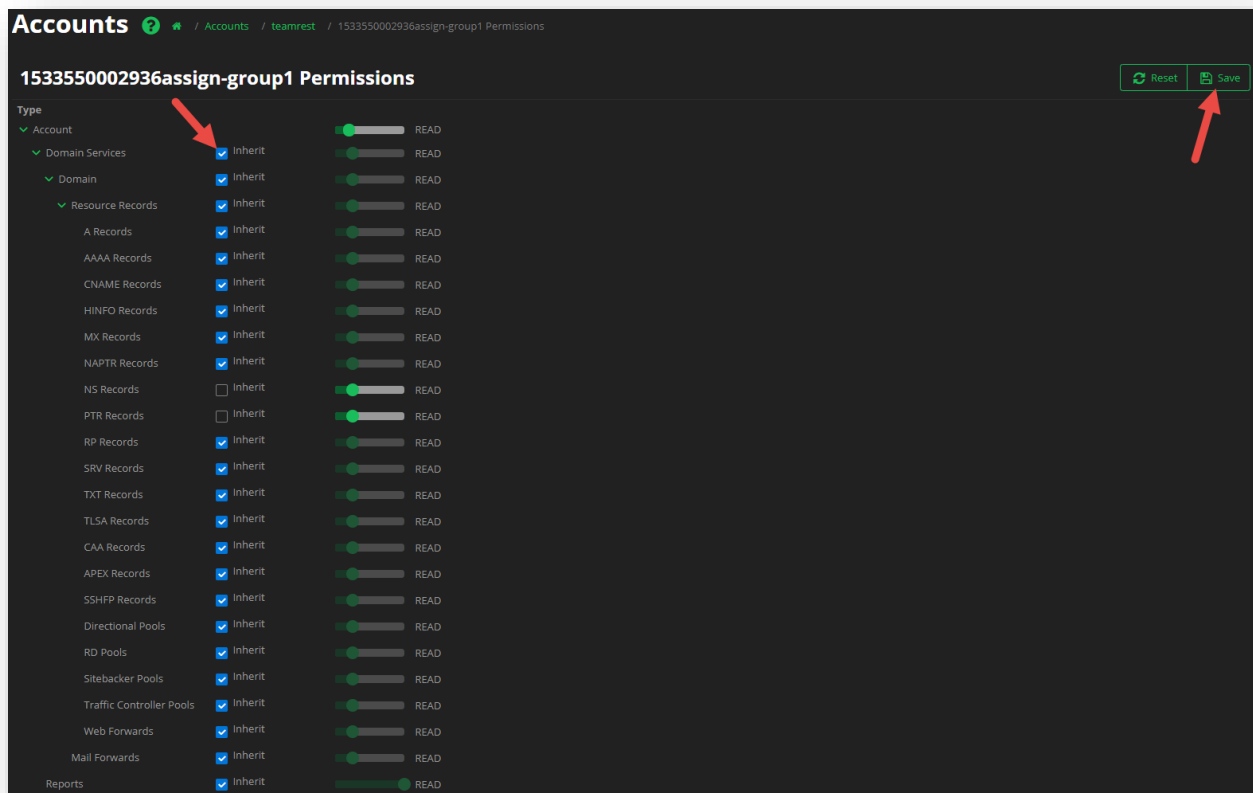


Figure 125 Users and Groups - Apply Permissions

5. You can also use the **Inherit** checkbox option to apply the settings from a higher tier to a lower tier from the Type column.
 - a. For example, apply Read Write Create to the **Domain** type (click **Save**), and then click **Inherit** next to Resource Records. The permissions from the Domains will apply to the Resource Records, and then trickle down to each subsequent type that is also set to Inherit.
6. Click **Save** when you are done applying permissions.

As a note, the following default (created by the UI) Groups cannot have their permissions changed:

- **Administrative** - Users will have access to all account functions including being able to change the Primary user for the account. The Primary user and Administrative users are the only users that can invite new users to the account.
- **Reporting** - Users will have Read-only access for the entire account, meaning they cannot edit any account level or domain level details.
- **Technical** - Users will have access to all account functions except for changing the primary user, and editing the Account Info (username and password).

To access Permissions for Users not in a Group (standalone):

1. Click on **User Groups** from the Accounts page.

2. Click on the **Not in a Group** group name.
3. Click the **Permissions** button next to the desired user.
4. Select the desired permission level per **Type**, and then click **Save**.

The screenshot displays the 'Users and Groups' management interface. On the left, a list of groups is shown with their respective user counts. The 'Not in a Group' group is highlighted with a red arrow. On the right, a list of users is shown with their names, user names, and email addresses. The 'Permissions' button for the user 'Sandeep Jain' is highlighted with a red arrow.

Group Name	User Count
123456789012345678901234567890ab	0
1533550002936assign-group1	1
1533550603560assign-group1	0
ADMINISTRATIVE	1
Asdfg	0
Custom1	5
Custom_test	7
Documentation	1
Env.ultradns.net.users	0
Fail	0
Gwengroup	0
Hello	2
Mystw	0
Mytest	1
Mytestgnkn	0
Neustar-support	0
Noc	1
Nopermission	1
REPORTING	3
TECHNICAL	2
Test#	0
Test#23	0
Testgroup	0
Testgrp1forzbr	0
Testsecgroup	0
Ton	0
Ultradns.net	3
Von3	0
Zan	0
Zbr	0
Pending Invitations	4
Not in a Group	4

Name	User Name	Email
<input type="checkbox"/> Sandeep Jain	sandeepjain	sandeep.s.jain@impetus.com
<input type="checkbox"/> Jayesh Neema	jayeshjain	jayeshneema@impetus.co.in
<input type="checkbox"/> testui console	reportteam	ketki.singh@team.neustar
<input type="checkbox"/> Sandeep Jain	sjain001	sandeep.s.jain@impetus.co.in

Figure 126 Accounts - Users and Groups - Standalone User Permissions

SAML

Security Assertion Markup Language (SAML) provides the solution for providing both authentication and authorization services for Neustar customers. By sharing security credentials between customers and our Security Services teams, we are able to transition your user's internal login credentials to a Neustar UltraDNS Managed Services Portal (UI Portal) username, thereby creating a Single Sign On (SSO) relationship between our services and systems.

Submit SAML Request

To create a request to get SAML initiated for your account:

1. Click on **Accounts** from the left-hand navigation menu.
2. Select the Account Name that you want to enable SAML for.
3. Click the **SAML** tab.
4. Complete each of the required fields for all three sections:
 - a. **Customer Contact Information** – Neustar support will reach out to the person listed if any assistance or issues arise during the SAML submission and provisioning process.
 - b. **Federation Related Information** - Download the sample XML metadata file so that you can copy the format exactly before uploading your data.
 - i. Please use the corresponding **NameID Format** option that matches how your internal login IDs are currently formatted. *This option will determine how your new SAML logins are generated.*
 - c. **DNS Related Information** – Please provide your unique company name (or a unique version of your company name) to complete the URL that will be issued to allow your users to log in.
 - i. **Allow the owner of the account dual access** – If you (as the Admin) need to retain access to the UI Portal, as well as getting access via SAML (SSO), check the box for dual access.
 1. If you opt not to check the box, you will no longer be able to log in directly to the UltraDNS Managed Services Portal.
5. Click **Submit SAML Setup Request** when finished.



Please note that submitting inaccurate or invalid data during the SAML Setup process will delay and cause further complications for our Support team to provision the SAML process. Please ensure that all of the information you are providing is accurate, and matches the required format being requested.

Accounts / Accounts / teamrest

Account Info Users and Groups **SAML** Exceptions Notification Settings TTL Settings Directional Groups Zone Transfer Settings

Customer Contact Information ? [Reset](#) [Submit SAML Setup Request](#)

Security Technical POC:

Security Technical POC Email:

Security Technical POC Phone:

Federation Related Information ?

Neustar will be acting as the SP and will normally initiate the SAML authentication request to your IDP.

If your IDP supports IDP initiated SAML, provide the IDP initiated URL:

NameID Format:

Upload your SAML IDP XML Metadata: [Choose File](#) No file chosen

Neustar SAML Metadata URL: [Download](#)

DNS Related Information ?

DNS URL for end-user access to Neustar when using single SAML login:
.sso.security.neustar

Allow the owner of the account dual access (via SAML & via direct, non-SAML login): ☐

Figure 127 Accounts - SAML Setup and Submit

Once your SAML request has been submitted, and email will be sent to the Primary Point of Contact's email address you provided. Please verify the information in the email is correct, and retain the vanity URL provided, as this will be the URL that you and your users will use to access the UI Portal moving forward. For further assistance, please refer to the [SAML Quick Start Guide](#) found on the **Support** page of the UI Portal.

Please wait a few minutes before trying to log in using the vanity URL that has been emailed to you. While you wait for the email confirmation, please continue through this guide for the final steps of setup.

After your submission has been processed, the **UltraDNS Users Details** section will appear with the list of your users currently found on the UltraDNS UI Portal. Your users' details will be displayed in one of two different formats, which is determined by the **NameID Format** type that you selected.

UltraDNS Users Details

The UltraDNS Users Details section displays the SAML features for your users based upon existing UI Portal details, and the NameID Format field type that you selected during the initial SAML setup request.

■ UltraDNS Current User Details

- **Name** – The user's name on the UI Portal.
- **UDNS Username** – The current username for the UI Portal.
- **Email** – The current email address for the UI Portal.

■ SSO

- **New UDNS Username** – Displays what the user's new UI Portal login will be.
- **API Access Only** – Displays if the designated user will ONLY have access to the API. Otherwise, the user will ONLY have access to the UI portal.

UltraDNS Users Details

SAML mapping implementation is a two-step process. The first step requires you to *map your users*, and the second requires your users to log in via SSO for their new UDNS Usernames to take effect.

Your current UltraDNS users' logins are listed below. Please complete the following actions before proceeding with the mapping of your users.

- **Delete Users** - Delete any users from the list that should no longer have access to the UI Portal or API.
 - *Warning - This process is irreversible, and the successful deletion of a user will remove them from the UI Portal completely.*
- **Edit Users** - Click the pencil icon next to each of your users to update their information if it is no longer accurate.

Once you have verified your users' details are correct, click the **Map Users for SSO** button to proceed.

	UltraDNS Current User Details			SSO	
	Name	UDNS Username	Email	New UDNS Username	API Access Only
<input type="checkbox"/>	owner samluser	samluser.owner	samluser.owner@saml.com	samluser.owner@saml.com	<input type="checkbox"/>
<input type="checkbox"/>	admin samluser	samluser.admin	samluser.admin@saml.com	samluser.admin@saml.com	<input type="checkbox"/>
<input type="checkbox"/>	api samluser	samluser.api	samluser.api@saml.com	samluser.api@saml.com	<input type="checkbox"/>
<input type="checkbox"/>	hekli lastName	samluser.reporting1	ultradns@neustar.biz	ultradns@neustar.biz	<input type="checkbox"/>

Figure 128 Accounts - SAML - UltraDNS Users Details – NameID is Email

If you selected **Username** from the **NameID Format** drop-down menu, an additional field will appear in the **SSO** section.

■ SSO

- **SSO Login** – Displays what the user's SSO login will be after the mapping process is complete.

UltraDNS Users Details ⓘ

SAML mapping implementation is a two-step process. The first step requires you to *map your users*, and the second requires your users to log in via SSO for their new UDNS Usernames to take effect.

Your current UltraDNS users' logins are listed below. Please complete the following actions before proceeding with the mapping of your users.

- **Delete Users** - Delete any users from the list that should no longer have access to the UI Portal or API.
 - *Warning* - This process is irreversible, and the successful deletion of a user will remove them from the UI Portal completely.
- **Edit Users** - Click the pencil icon next to each of your users to update their information if it is no longer accurate.

Once you have verified your users' details are correct, click the **Map Users for SSO** button to proceed.

	UltraDNS Current User Details			SSO		
<input type="checkbox"/>	Name	UDNS Username	Email	SSO Login	New UDNS Username	API Access Only
<input checked="" type="checkbox"/>	owner.saml	owner.saml	owner.saml@saml.com	owner.saml	owner.saml_ckcsa	<input type="checkbox"/>
<input checked="" type="checkbox"/>	admin.saml	admin.saml	admin.saml@saml.com	admin.saml	admin.saml_ckcsa	<input type="checkbox"/>
<input checked="" type="checkbox"/>	api.saml	api.saml	api.saml@saml.com	api.saml	api.saml_ckcsa	<input type="checkbox"/>

Figure 129 Accounts - SAML - UltraDNS Users Details - NameID is Username

Edit Users Details

If any of the user details are incorrect, click the green **pencil icon** next to the user to update their details accordingly. This is also how you will designate if the user should **ONLY** have access to the API, or if they will **ONLY** have access to the UI Portal.

- Only unique email addresses are allowed. If duplicate email addresses are detected, an error will occur and the SAML Mapping process will be cancelled.
- The email address will directly update the *Upon Implementation UDNS Username* (the future SSO login credential) field for the user.

The 'Edit User Details' dialog box is shown with a dark background. It contains the following fields and values:

- Name: owner samluser
- Current UDNS Login: samluser.owner
- Email: samluser.owner@saml.com (text inside a text box)
- Upon Implementation UDNS Username: samluser.owner@saml.com
- API only access: ☐

At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 130 SAML - Edit User Details - NameID is Email

The 'Edit User Details' dialog box is shown with a dark background. It contains the following fields and values:

- Name: owner saml
- Current UDNS Login: owner.saml
- Email: owner.saml@saml.com (text inside a text box)
- SSO Login: owner.saml (text inside a text box)
- Upon Implementation UDNS Username: owner.saml_ckcsa
- API only access: ☐

At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 131 SAML - Edit User Details - NameID is Username

Map Users for SSO

Once you have verified that all of your users' information is accurate, click the **Map Users for SSO** button. **Every user from the list will be selected automatically**, which is why it is important for the account owner to review the initial list of users and use the **Delete Selected Users** option to remove any obsolete users.

A confirmation screen will appear listing the total number of users that are being mapped for SAML, along with the details their details and login credentials. Click the **Confirm Map Users** button to complete the SAML setup process.

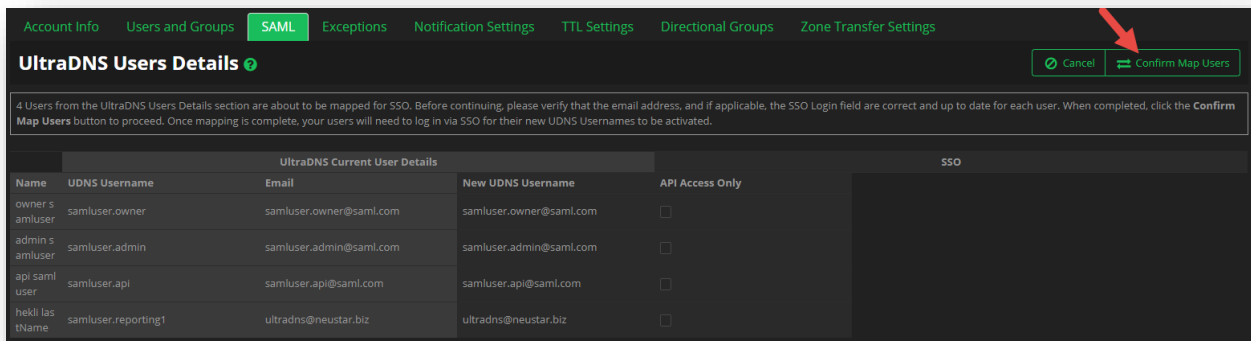


Figure 132 SAML - Confirm Map Users

Please only click the **Confirm Map Users** button once, as doing so multiple times could cause issues with your submission.

Once the confirmation of the SAML submission appears, your request will be processed. At this point, you can log in using the SAML credentials and vanity URL that have been emailed to you.

The SAML process will work around a trial time period. Once you have become familiar and comfortable using SAML login to access the UI Portal and manage your users, Neustar will remove all of your user's direct access to the UDNS Portal. Our Customer Support team will reach out to you directly to confirm your readiness to begin using SAML, and have your access to the Portal removed.

User Access and Permissions

For existing users on the UltraDNS Portal, your permissions will remain once your Account Administrator completes the Setup Users for SSO step (before you attempt to log in using the vanity URL).

If the **Setup Users for SSO** step has not been completed, and you log in using the vanity URL, your account will inherit the Reporter Role permissions upon logging in. The Reporter Role provides only Read Access. Your Account Administrator will need to log in and change your permissions from the UltraDNS Portal.

Creating New Users

Once you have completed the SAML setup, new users are dynamically provisioned from your end. Once you have established a new user's credentials, they will automatically be enabled for SAML and have the *Reporter Role* access, which gives them Read Only access. You can change their access if necessary through the UI.

Account Info

The first tab on the Accounts page is **Account Info**. This tab displays the basic overview details of your account.

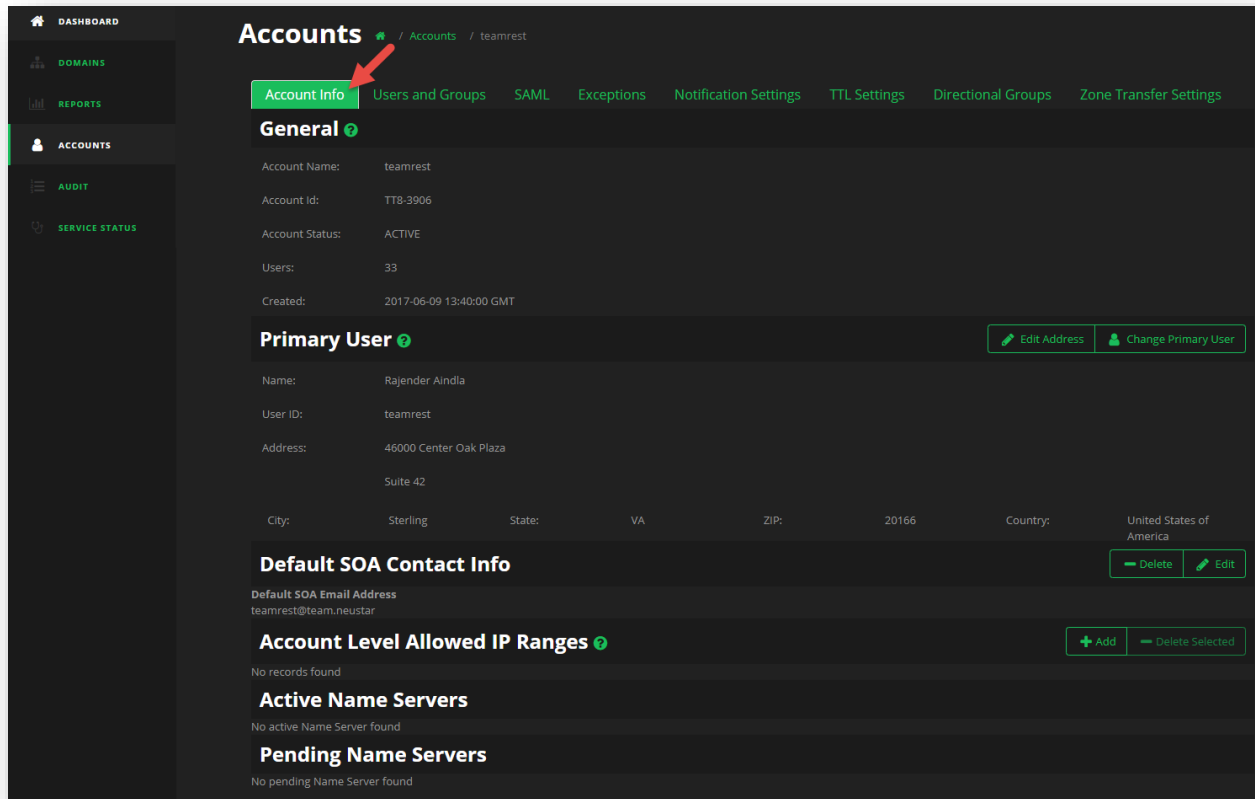


Figure 133 Accounts - Account Info

General

The **General** section displays the Account Name, Account ID, Account Status, Users, and the Account Creation date. Clicking the **Edit** button allows you to change the Account Name only.

Primary User

The **Primary User** section displays the Name and the User ID for the Primary User, along with the Address and Address2 details.

You can think of the Primary User as the Account Administrator or “Super-User” for the account. The Primary User has unrestricted access to every part of the account on the UI Portal, and is not listed under the Users and Groups tab because their permissions cannot be altered or restricted.

Additionally, the Primary User is ideally the Primary Point of Contact for Neustar Support if there are ever any issues with your Account, or if additional information is every required.

You can click the **Edit Address** button to change either the primary or the secondary address details.

Edit Primary User Address

Address:
address101_address101_address101_address101_address101_address101_address101
A valid address1

Address2:
A valid address2

City: Noida A valid city name

State: NJ A valid state name

Zip: 20147 A valid zip code

Country: United States of America A valid country name

Close Save

Figure 134 Accounts - Edit Primary User Address

Clicking the **Change Primary User** button allows you to change the primary user for the account from the drop-down list of available users.

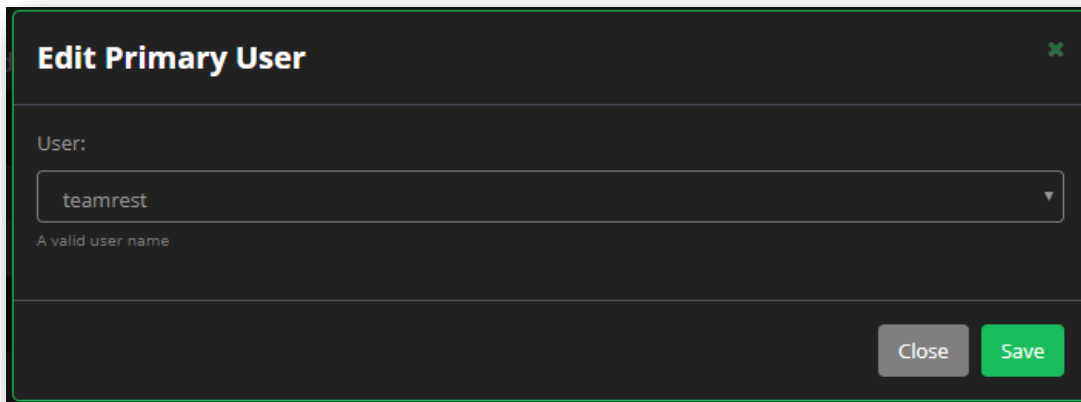


Figure 135 Accounts - Change Primary User

Default SOA Contact Info

The Default SOA Contact Info section displays the default SOA email address for the account. You can click the **Edit** button to change the email address, or click the **Delete** button to remove the email address entirely.

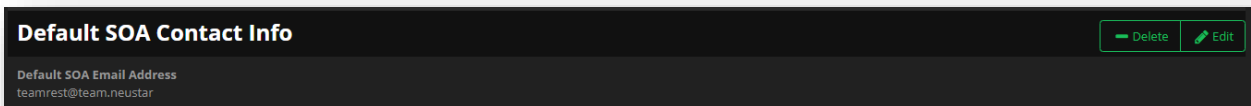


Figure 136 Default SOA Contact Info

Account Level Allowed IP Ranges

The Account Level Allowed IP Ranges provides enhanced security, allowing you to specify one or more IP addresses from which you can access your account. By default, you can access your account from any IP address using the correct username and password.

To add an IP Range:

1. Click the **Add** button.
2. Provide the **Starting IP** address (this can be in either IPv4 or IPv6 format).
3. Provide the **Ending IP** address (the format must match the format you provided in the *Starting IP* section).
4. Check the box the type of account access you want to allow from the IP Range, either **UI** (UltraDNS Portal) or **API** (the REST API).
5. Add additional **Comments** if necessary.

6. Click **Save** when finished.

Add Allowed IP Range

Starting IP:

A valid IP

Ending IP:

A valid IP

UI: ☐ API: ☐

Comments:

A valid comments

Close Save

Figure 137 Accounts - Account Level Allowed IP Range

Exceptions

The Exceptions tab displays all of the current permission exceptions that have been created for Users and Groups under the specified account.

When the permission level is set for an **Object Type** (i.e. Account, Domain, Resource Record etc), every sub-Object adheres to that permission level; unless you create an exception. Let's say for instance, you create Group A, and you set the permission level for **Domain** to READ WRITE, thereby allowing every user in Group A to View and Edit all domains. However, there is one specific zone that you don't want the users in Group A to be able to edit, so you create an exception for that one zone, to set the permission level to READ only.

To set exceptions for a domain, refer to *Permissions and Exceptions* in the Domains section.

Viewing Exceptions

To see a list of the current exceptions for an account:

1. Click on **Accounts** from the left-hand navigation menu.
2. Select the desired **Account Name**.
3. Click on the **Exceptions** tab. The Permission Exceptions menu will appear.
4. Each exception provides the following details:
 - a. **User/Group** – The current User or Group that has the exception.
 - b. **Object** – The specific object name being impacted. (i.e. a zone name)
 - c. **Object Type** – The category to which the Object belongs.
 - i. For example, if a specific zone has been given the exception, the Object Type will be Zone.
 - d. **Permission** – The current permission level (with the exception included) that is impacting the object.

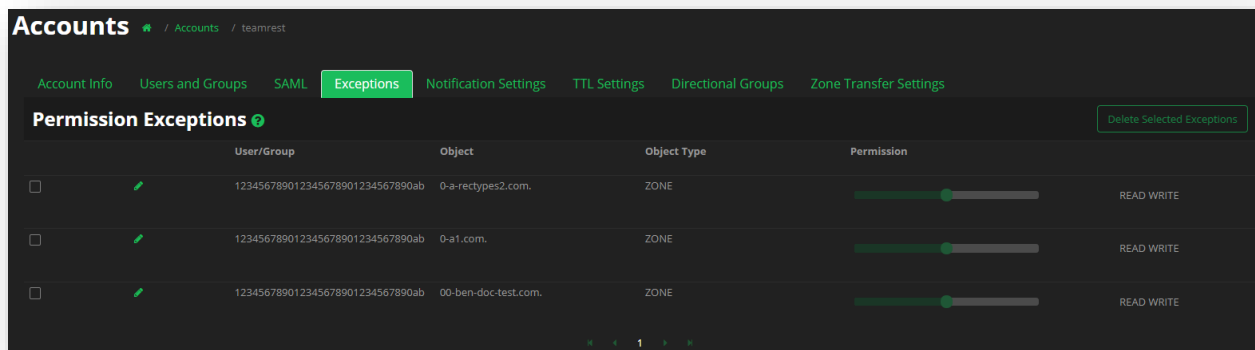


Figure 138 Accounts – Exceptions

Edit an Exception

To edit an exception from the **Permission Exceptions** menu:

1. Click the **pencil icon** next to the exception that you want to edit.
2. Use the **slider bar** to change the permission level for the object.
3. Once done, click the **green checkmark icon**.
 - a. Clicking the **green X icon** will cancel the change you've made.

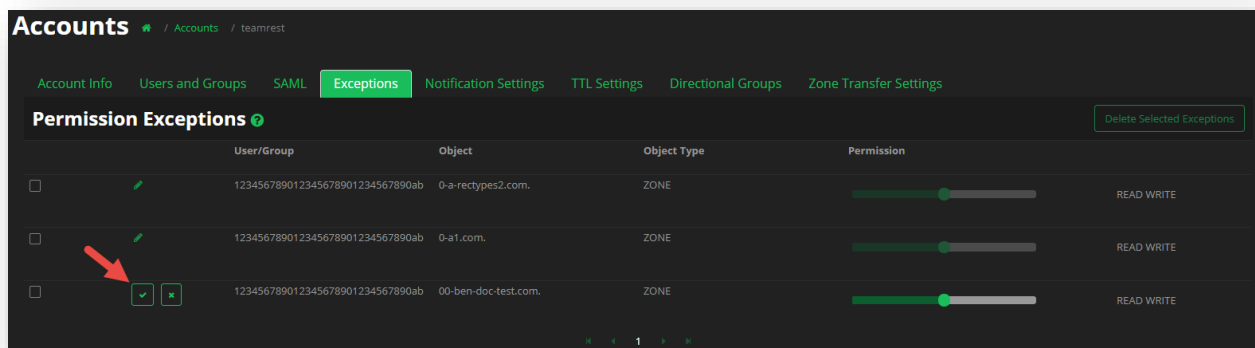


Figure 139 Accounts - Edit an Exception

Delete an Exception

To delete an exception that has been created for the account:

1. Click the **checkbox** next to the exception that you want to delete.
2. Click the **Delete Selected Exceptions** button.

3. Click the **Delete** button to confirm the deletion of the exception.
 - a. Deleting an exception will not change the base permission for the User or Group, it will only remove the exception that was placed on the specific Object.

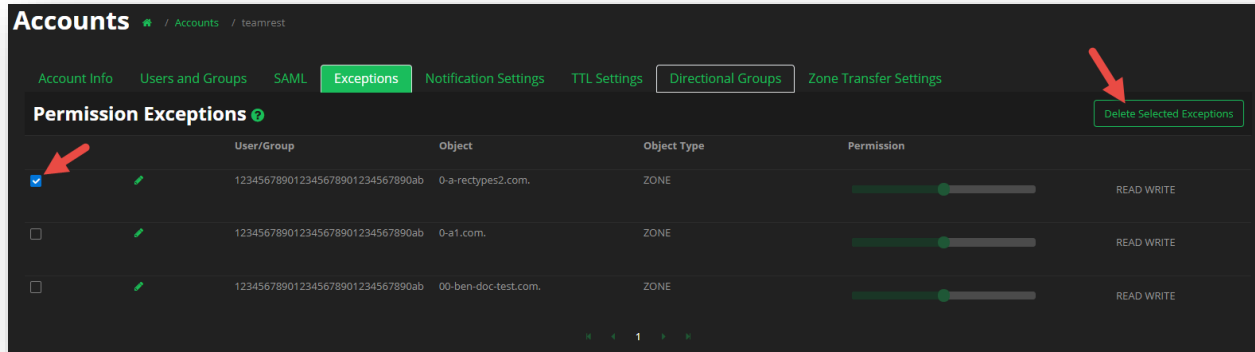


Figure 140 Accounts - Delete an Exception

Notification Settings

The Notification Settings section allows you to customize how you wish to receive notification alerts, as well as customizing who the alerts should be sent to.

Accounts / Accounts / teamrest

Account Info Users and Groups SAML Exceptions **Notification Settings** TTL Settings Directional Groups Zone Transfer Settings

DDOS Notification

Email Notification: Enabled

Email Address(s): raviraj.katwate@team.neustar x rohan.pandhare@parkar.consulting x

Comma or Tab can be used to separate multiple email addresses.

Save

Zone Transfer Notification

Threshold: 100

Email Notification: Enabled

Email Address(s): sanity@test.com x

Comma or Tab can be used to separate multiple email addresses.

Save

Figure 141 Accounts - Notification Settings

DDOS Notification

The DDOS Notification section allows you to customize the recipient(s) that should be notified, and how they should be notified when there is a DDOS (type) event.

To enable DDOS Notifications:

1. Select **Enabled** from the drop-down menu for Email Notification.
2. In the Email Addresses field, enter the email address in the addr-spec format for the recipients that should be notified.
 - a. Email addresses can be comma separated, or by using the Tab or Enter key on your keyboard.
3. Click **Save**.

The screenshot shows the 'DDOS Notification' settings panel. It has a dark background with white text. At the top, the title 'DDOS Notification' is followed by a help icon. Below this, there are two main sections. The first section is 'Email Notification', which has a dropdown menu currently set to 'Enabled'. The second section is 'Email Address(s)', which contains a text input field with two email addresses: 'rkatwate@parkar.consulting' and 'rohan.pandhare@team.neustar'. Below the input field, there is a small note: 'Comma or Tab can be used to separate multiple email addresses.' In the bottom right corner, there is a green 'Save' button.

Figure 142 Accounts - Notification Settings - Enabling DDOS Notifications

Zone Transfer Notification

When there are Zone Transfer updates or failures, this section allows you to customize the recipient(s) that should be notified, how they should be notified, and the threshold limit at which the notifications should be sent.

To enable Zone Transfer Notifications:

1. In the **Threshold** field, provide an integer value that will determine at what threshold value a Zone Transfer Notification will be sent.
 - a. The threshold value is equivalent to the number of zone transfer failures that will occur before notifications are sent. The threshold value can be between 0 and 100,000.
2. Select **Enabled** from the drop-down menu for Email Notification.
3. In the Email Addresses field, enter the email address in the addr-spec format for the recipients that should be notified.
 - a. Email addresses can be comma separated, or by using the Tab or Enter key on your keyboard.
4. Click **Save**.

The screenshot shows the 'Zone Transfer Notification' settings panel. It has a dark background with white text. At the top, the title 'Zone Transfer Notification' is followed by a help icon. Below this, there are three main sections. The first section is 'Threshold', which has a text input field containing the value '100'. The second section is 'Email Notification', which has a dropdown menu currently set to 'Enabled'. The third section is 'Email Address(s)', which contains a text input field with the email address 'sanity@test.com'. Below the input field, there is a small note: 'Comma or Tab can be used to separate multiple email addresses.' In the bottom right corner, there is a green 'Save' button.

Figure 143 Accounts - Notification Settings - Enabling Zone Transfer Notifications

To disable your current Notification Settings, simply change the **Email Notification** drop-down option to **Disabled**.

TTL Settings

The TTL (Time To Live) Settings displays the configured TTL settings for records in the account by displaying the **Default**, **Min** (minimum), and **Max** (maximum) values. If you have the necessary privileges, you can configure individual record settings.

Enter the TTL value as an integer number of seconds (maximum of 2147483647) by clicking the **pencil** icon next to the record type / SOA value. Change the necessary value(s), and then click the **Save** button.

The screenshot shows the 'Accounts' page with the 'TTL Settings' tab selected. The page displays a list of DNS record types and their associated TTL settings. A red arrow points to the 'TTL Settings' tab in the navigation menu.

	Default	Min	Max
Global (All Records) TTL			
A (IPv4 Host) TTL			
AAAA (IPv6 Host) TTL			
CNAME (Alias) TTL			
MX (Mail Exchange) TTL			
TXT (Text) TTL			
SRV (Service Locator) TTL			
NS (Nameserver) TTL			
PTR (Pointer) TTL			
RP (Responsible Person) TTL			
HINFO (Host Info) TTL			
NAPTR (Naming Authority Pointer) TTL			
SOA (Start of Authority) Refresh			
SOA (Start of Authority) Retry			
SOA (Start of Authority) Expire			
SOA (Start of Authority) Min Cache			
SOA (Start of Authority) TTL			

Figure 144 Accounts - TTL Settings

Edit TTL Setting ✕

Global (All Records) TTL

Default

121

Min

Max

Cancel Save

Figure 145 Accounts - Edit TTL Settings

Directional Groups

The Directional Global Groups section displays the directional group templates (at the account level) that you can use to create Directional Record pools in your domains. These configured groups can either contain SourceIP addresses, GeoLocation regions, or a combination of the two.

Using these (Account Level) Directional Groups can help simplify the creation process of your Directional Pools, by removing the need to assign multiple regions or IP ranges per pool (or record type) that you need to create. Once you've created and configured a Directional Group, you can add that group name directly to a record that is being created under your Directional Pool.

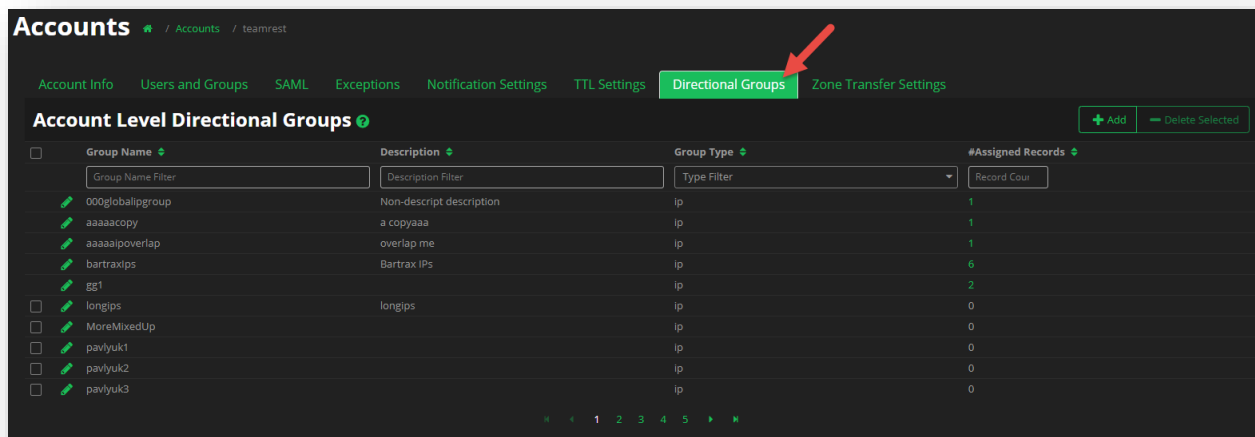


Figure 146 Accounts - Directional Groups

The Directional Groups landing page provides various sorting and filtering options while viewing your existing configured groups. You can click the green up or down arrows to sort the list alphabetically, or use the filter option to perform a search for a matching filter type. All searches are performed as a wildcard, meaning any record matching a portion of your search will be displayed.

- **Group Name** – Displays the Group name for the configured Directional groups.
- **Description** – Displays the description (if any) provided for the directional group.
- **Group Type** – Displays if the current Directional Group is configured for SourceIP (IP) addresses or GeoLocation (Geo) data.
- **#Assigned Records** – Displays the current number of pools / records that are currently using the configured Directional Group. You can click on the green number to retrieve a list of the associated pools.

Add Directional Group - SourceIP

To create a new Directional Group that contains SourceIP details:

1. Click the **+Add** button.

Add Account Level Directional Group

Group Name:

Group Type: Source IP Geolocation Source IP

Copy Global Group: None

Description:

Source IP Delete Selected

☐ IP

IP Range - Add

Cancel Save

Figure 147 Accounts - Add SourceIP Directional Group

2. Provide the **Group Name**.
3. Select **SourceIP** from the **Group Type** drop-down menu.
4. If you have an existing SourceIP Global Group you can want to copy from, select it from the **Copy Global Group** drop-down menu.
5. (Optional) Provide a description for the Directional Group.
6. Select the **IP Type** from the drop-down menu.
 - a. **IP Range** – Provide the beginning and end IP addresses to create the range.
 - b. **Single IP** – Provide a single IP address.
 - c. **CIDR** – Provide the network and routing prefix values.

Add Account Level Directional Group ?

Group Name:

Group Type:

Copy Global Group:

Description:

Source IP

☐ IP

-

Figure 148 Accounts - Add SourceIP Directional Group cont.

7. Click **Add** when you are finished to add the SourceIP details to the Group. You can add as many SourceIP records as needed.
8. Click **Save** when finished adding SourceIP records.

Add Directional Group – Geolocation

1. Click the **+Add** button.

Add Account Level Directional Group

Group Name:

Group Type: **Geolocat** ▼

Copy Global Group: **None** ▼

Description:

Available Regions

Select Regions ▼

Selected Regions

Filter

No items found

Cancel Save

Figure 149 Accounts - Add Geolocation Directional Group

2. Provide the **Group Name**.
3. Select **Geolocation** from the **Group Type** drop-down menu.
4. If you have an existing Geolocation Global Group you can want to copy from, select it from the **Copy Global Group** drop-down menu.
5. (Optional) Provide a description for the Directional Group.
6. Select the **Region(s)** for the directional group from the **Available Regions** drop-down menu. Click outside of the selection box when finished making your selections.
 - a. To select an entire region, click the **green arrow** to move the region and all of the associated countries and states/provinces to the **Selected Regions** section.
7. Select the associated **Countries** for the directional group (you can select as many as necessary). Click outside of the selection box when finished making your selections.
 - a. To select the entire country, click the **green arrow** to move the country and all of the associated states/provinces to the **Selected Regions** section.
8. Select the available **States/Provinces** for the directional group (you can select as many as necessary). Click outside of the selection box when finished making your selections.

9. Once you are done, click the **green arrow** to move the selected locations to the **Selected Regions** column. Once done, you will see a hierarchal breakdown of your selections.
 - a. To clarify, if you select specific states/provinces, only those selections will move to the Selected Regions column, not the previous countries or region selections.

Zone Transfer Settings

The Zone Transfer Settings section consists of the following three sections:

- *Restrict IPs*
- *Notify Addresses*
- *TSIG Key*

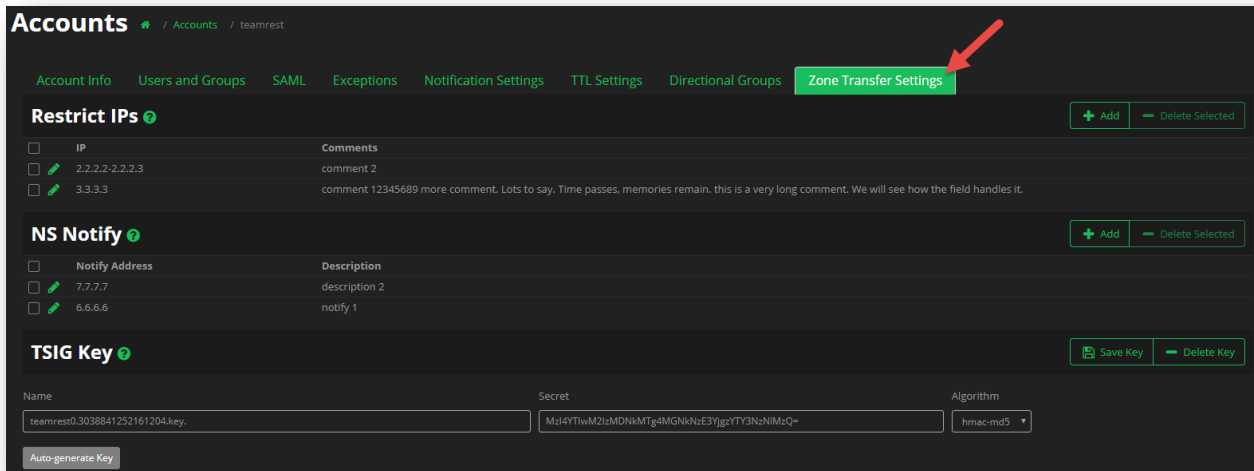


Figure 150 Accounts - Zone Transfer Settings

Restrict IPs

The Restrict IPs list identifies the IP addresses that are allowed to request a zone transfer from this Neustar managed domain/account. Unless otherwise specified, Neustar, by default, restricts all zone transfers.

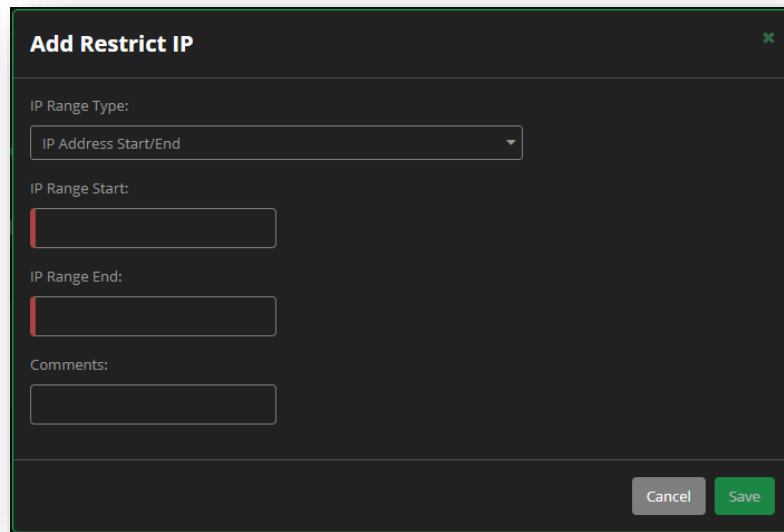
You can manually configure Restrict IPs for each zone or use the Inherit Account Settings checkbox to have the zone automatically use the account-level settings.



Only the IPv4 Address format is accepted.

To specify an allowable IP address:

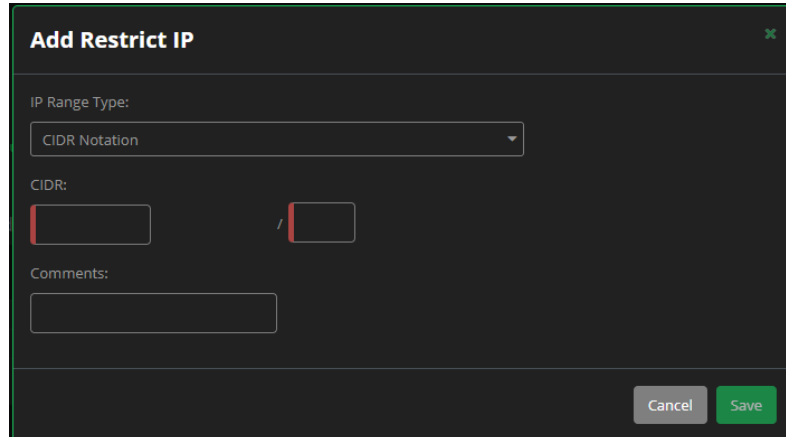
1. Click the **Add** button.
2. Select an IP Range Type from the drop-down list. Your choices include:
 - a. **IP Address Start/End** - Enter a range of IP addresses using the Start and End IP addresses of the range.



The 'Add Restrict IP' dialog box is shown with a dark background. It features a title bar with a close button (X). Below the title bar, there is a section for 'IP Range Type:' with a dropdown menu currently set to 'IP Address Start/End'. Underneath, there are two input fields: 'IP Range Start:' and 'IP Range End:', each with a red vertical bar on its left side. Below these is a 'Comments:' section with a text input field. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Figure 151 Account - Zone Transfer Settings - IP Address Start/End

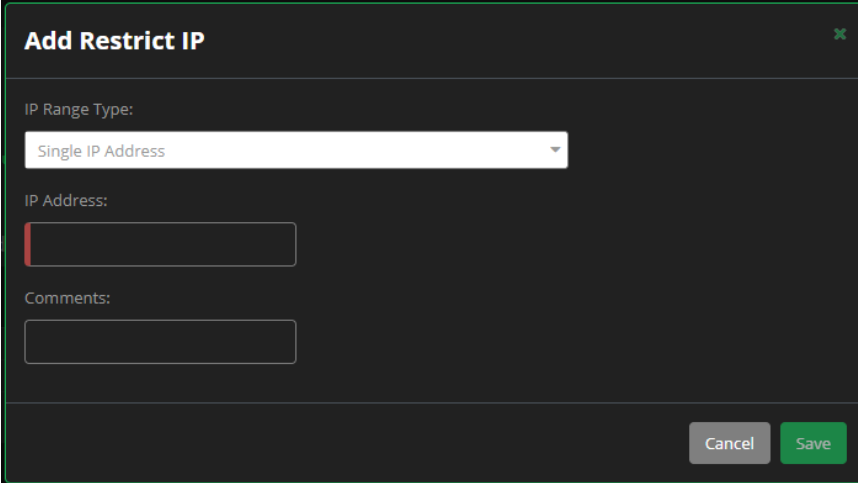
- b. **CIDR Notation** - Allows you to enter IP addresses in the Classless Inter-Domain Routing (CIDR) format.



The 'Add Restrict IP' dialog box is shown with a dark background. It features a title bar with a close button (X). Below the title bar, there is a section for 'IP Range Type:' with a dropdown menu currently set to 'CIDR Notation'. Underneath, there is a 'CIDR:' section with two input fields separated by a slash (/), each with a red vertical bar on its left side. Below this is a 'Comments:' section with a text input field. At the bottom right, there are two buttons: 'Cancel' and 'Save'.

Figure 152 Accounts - Zone Transfer Settings - CIDR Notation

- c. **Single IP Address** - For a single IP address entry.

A dark-themed dialog box titled "Add Restrict IP" with a close button (X) in the top right corner. It contains three input fields: "IP Range Type:" with a dropdown menu showing "Single IP Address", "IP Address:" with a text input field, and "Comments:" with a text input field. At the bottom right, there are "Cancel" and "Save" buttons.

Add Restrict IP

IP Range Type:
Single IP Address

IP Address:

Comments:

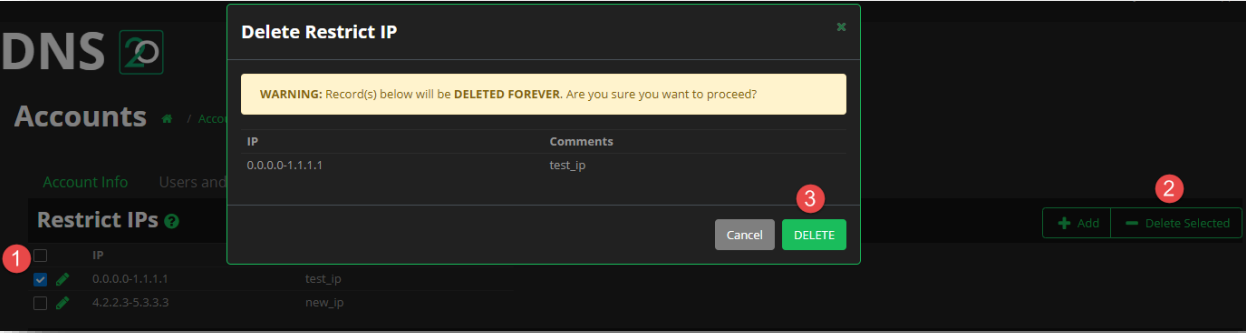
Cancel Save

Figure 153 Accounts - Zone Transfer Settings - Single IP Address

3. You can add Comments if necessary. For example, you can specify the domain name or other common text identifiers for the IP number or range.
4. Click **Save**.

To Delete one or more Restrict IPs from the list:

1. Click on the checkbox to the left of each Restrict IP that you want to delete.
2. Click **Delete Selected**.
3. Click **Delete** to confirm the deletion.

A screenshot of the "Accounts" page showing a table of "Restrict IPs". The table has columns for "IP" and "Comments". The first row is selected, and a "Delete Restrict IP" dialog box is open. The dialog box contains a warning message: "WARNING: Record(s) below will be DELETED FOREVER. Are you sure you want to proceed?". Below the warning is a table with the same columns as the main table, showing the selected record. At the bottom of the dialog are "Cancel" and "DELETE" buttons. In the background, the "Restrict IPs" table has a checkbox (1) next to the first row, and "Delete Selected" (2) and "DELETE" (3) buttons are visible.

DNS

Accounts

Account Info Users and

Restrict IPs

1 ☐ IP

☒ 0.0.0.0-1.1.1.1 test_ip

☐ 4.2.2.3-5.3.3.3 new_ip

Delete Restrict IP

WARNING: Record(s) below will be **DELETED FOREVER**. Are you sure you want to proceed?

IP Comments

0.0.0.0-1.1.1.1 test_ip

3 Cancel DELETE

2 + Add - Delete Selected

Figure 154 Accounts - Zone Transfer Settings – Delete

Notify Addresses

This section provides a way to identify the IP address(es) that should be notified when there are changes to the Primary zone that initiate a zone transfer.

You can manually configure the Notify Addresses for each zone, or click the **Inherit Account Settings** checkbox to have the zone automatically use the Account-level settings.



Only the IPv4 Address format is accepted.

To populate the Notify Address list:

1. In the Notify Addresses panel, click **Add**.
2. Enter an IP address to receive notification of changes to this zone.
3. You can add Comments if necessary. For example, you can specify recipient domain names or other common text identifiers for the IP address(es) entered.
4. Click **Save**.

Add Notify Address

IP Address:

Description:

Cancel Save

Figure 155 Accounts - Add Notify Address

Repeat the above steps for adding additional addresses to the list.

To delete one or more Notify Addresses from the list:

1. Click on the checkbox to the left of each address that you want to delete.
2. Click **Delete Selected**.
3. Click **Delete** to confirm the deletion.

TSIG Key

This section provides a way to enter and maintain the TSIG (Transaction Signature) key for the account. TSIG security requires that both sides of a transfer pass the same TSIG key value.

You can copy a key value from the corresponding server into the TSIG configuration, or Auto-generate the key in UltraDNS.

NOTE: If you elect to Autogenerate a TSIG Key, be sure to copy and paste the generated value to the

corresponding zone server.

Only one TSIG Key can be applied to a zone at a time.

You can manually configure TSIGs for each zone or click the Inherit Account Settings checkbox to have the zone automatically use the account-level TSIG value.

To enter a TSIG Key:

1. Enter a Name for the key.
2. Select the proper Algorithm for the key using the drop-down list. This is either the algorithm used to generate the key you are copying in, or the algorithm you want to use to generate a new key.
3. Paste/Enter the key value into the Secret field or click **Autogenerate Key** button to have the system provide a key for you.

TSIG Key ⓘ

Name	Secret	Algorithm
teamrest0.5474000958755469.key	YzdiODA3MjU0MTFhMmJkYzAwNTc3YTZGM0ZDk3Y2U0ZDc3Mzk3ZDdmLw	hmac-sha384

Auto-generate Key

Figure 156 Accounts - TSIG Key

To delete the TSIG Key:

1. If there is an active TSIG Key, click **Delete Key**.
2. Click **Delete** to confirm the deletion.

Audit

The Audit page lists changes made to your domains, various records and pools, as well as user functions and activities in your account.

The Audit page includes the following columns:

- **Change Time** - The date and time the change occurred.
 - Click on the green arrow to expand the event and see additional details.
- **Changed Object** - Lists either the Domain or the Record being impacted.
- **Parent Object** – Lists the hierarchical object impacted by the change.
 - If an A record that is part of a Pool is altered, the Pool would be the Parent Object.
 - If a zone transfer fails, the domain would be the Parent Object.
- **Object Type** - Lists the specific object that was impacted (zone, pool, record type, or user).
- **Change Type** - Displays the action that was taken on the object (Add, Modify, Login etc.).
- **User** - Lists the username responsible for the change.

You can narrow your search results by using the **Audit Filters** menu. Use the various categories' drop-down menus to customize your search parameters and then click the **Apply Filters** button. To remove all of your filter criteria, click the **Clear Filter** button.

Service Status

The Service Status Dashboard is comprised of two tabs. The first, **Current Status**, displays the current service availability (status) for the various Neustar service offerings. Each service is broken down by region, which can be expanded by clicking the green + (plus) icon next to each region to see the sub-locations status. Alternatively, to expand every region, you can click the **All** link next to Expand Regions just below the status legend.

UltraDNS Service Status / Service Status

Current Status Event History

Current Status is continuously updated with the most current information on service availability across our various offerings. Please check any time to get current status information on each individual service.

Current status as of Fri, 08 Feb 2019 21:09:40 GMT

☒ All Clear
 ☐ Performance Issues
 ☐ Service Unavailable

Expand Regions: **All** | None

REGION/NODE	ENTERPRISE	FORWARDING	RECURSIVE	SMALL & MEDIUM BUSINESS
Asia	✓	—	✓	✓
Europe	✓	✓	✓	✓
NA Central	✓	✓	✓	✓
NA East	✓	✓	✓	✓
NA West	✓	✓	✓	✓
ROW	✓	—	✓	✓

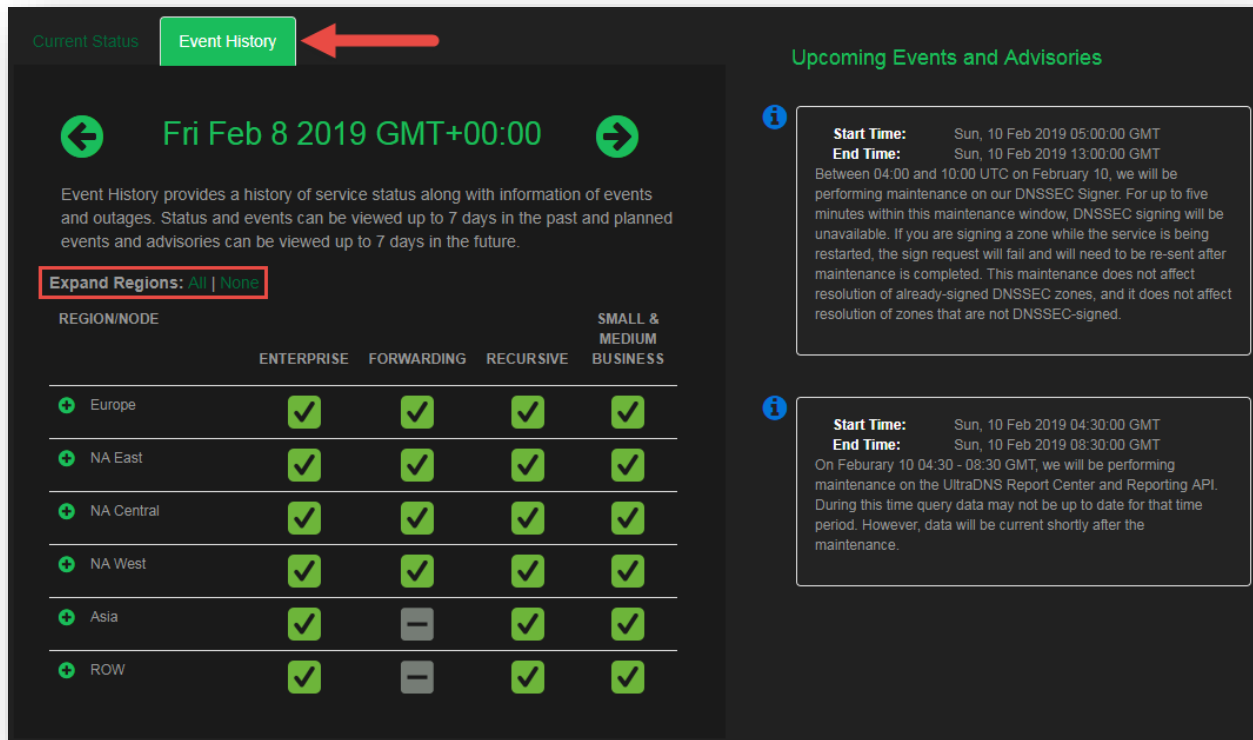
Upcoming Events and Advisories

Start Time: Sun, 10 Feb 2019 05:00:00 GMT
End Time: Sun, 10 Feb 2019 15:00:00 GMT
 Between 04:00 and 10:00 UTC on February 10, we will be performing maintenance on our DNSSEC Signer. For up to five minutes within this maintenance window, DNSSEC signing will be unavailable. If you are signing a zone while the service is being restarted, the sign request will fail and will need to be re-sent after maintenance is completed. This maintenance does not affect resolution of already-signed DNSSEC zones, and it does not affect resolution of zones that are not DNSSEC-signed.

Start Time: Sun, 10 Feb 2019 04:30:00 GMT
End Time: Sun, 10 Feb 2019 08:30:00 GMT
 On February 10 04:30 - 08:30 GMT, we will be performing maintenance on the UltraDNS Report Center and Reporting API. During this time query data may not be up to date for that time period. However, data will be current shortly after the maintenance.

Figure 157 Service Status Dashboard - Current Status

The second tab, **Event History**, provides a history of service statuses along with detailed information of planned events and outages. The service status data can be viewed up to seven days in the past from the current date, along with future planned events and advisories being viewable up to seven days in the future (from the current date). Use the **green arrows** to navigate to previous or future dates.



Current Status **Event History**

← **Fri Feb 8 2019 GMT+00:00** →

Event History provides a history of service status along with information of events and outages. Status and events can be viewed up to 7 days in the past and planned events and advisories can be viewed up to 7 days in the future.

Expand Regions: All | None

REGION/NODE	ENTERPRISE	FORWARDING	RECURSIVE	SMALL & MEDIUM BUSINESS
Europe	✓	✓	✓	✓
NA East	✓	✓	✓	✓
NA Central	✓	✓	✓	✓
NA West	✓	✓	✓	✓
Asia	✓	—	✓	✓
ROW	✓	—	✓	✓

Upcoming Events and Advisories

Start Time: Sun, 10 Feb 2019 05:00:00 GMT
End Time: Sun, 10 Feb 2019 13:00:00 GMT
Between 04:00 and 10:00 UTC on February 10, we will be performing maintenance on our DNSSEC Signer. For up to five minutes within this maintenance window, DNSSEC signing will be unavailable. If you are signing a zone while the service is being restarted, the sign request will fail and will need to be re-sent after maintenance is completed. This maintenance does not affect resolution of already-signed DNSSEC zones, and it does not affect resolution of zones that are not DNSSEC-signed.

Start Time: Sun, 10 Feb 2019 04:30:00 GMT
End Time: Sun, 10 Feb 2019 08:30:00 GMT
On February 10 04:30 - 08:30 GMT, we will be performing maintenance on the UltraDNS Report Center and Reporting API. During this time query data may not be up to date for that time period. However, data will be current shortly after the maintenance.

Figure 158 Service Status Dashboard - Event History

My Profile

The **My Profile** section of your account displays two sections of information allowing you to provide contact information, and additional security measures for your account.

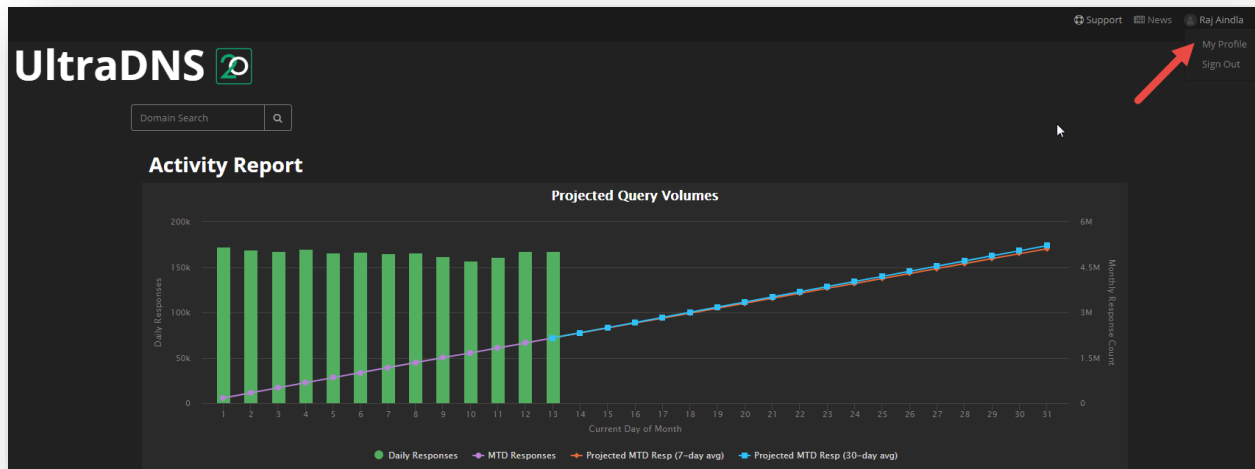


Figure 159 My Profile

Contact Information

Clicking on the **My Profile** link in the upper right-hand side of your screen will open the Contact Information section of your account.

This section provides Neustar with your immediate contact information should we need to reach out to you directly, or if you opt into additional services and features (Two Factor Mobile Authentication, Notifications etc.).

Each field that contains red line on the left-hand side is a required field that we ask you to provide as basic contact information and profile details. Once you've provided all the required information, click the **Save** button. Clicking the **Reset** button will replace every field with the previously submitted data.

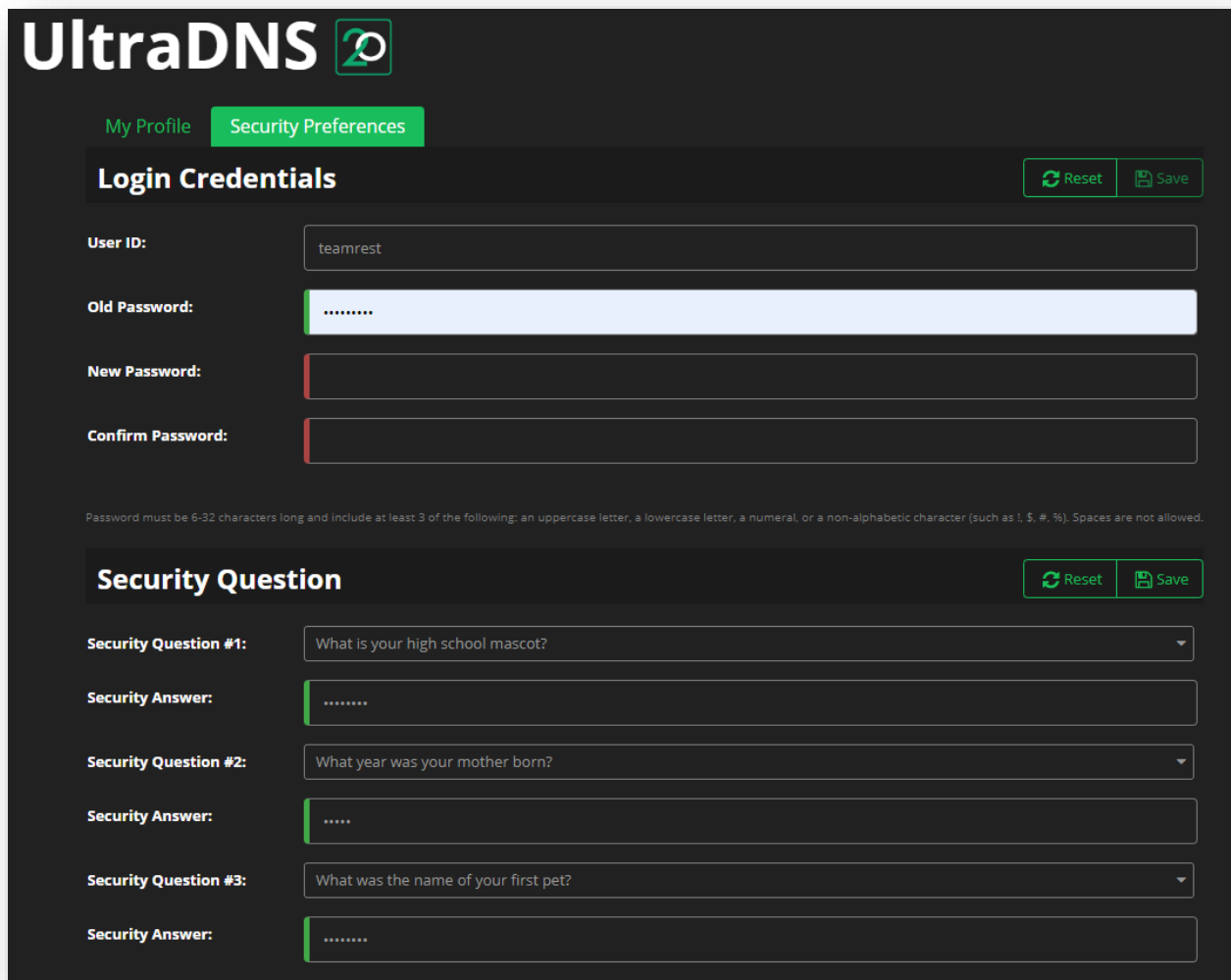
The screenshot shows the 'UltraDNS' logo at the top left. Below it are two tabs: 'My Profile' (active) and 'Security Preferences'. The 'Contact Information' section is highlighted. It contains a 'Reset' button and a 'Save' button. The form fields are as follows:

Field Label	Field Type
First Name:	Text Input
Last Name:	Text Input
Primary Email:	Text Input
Secondary Email:	Text Input
Phone Number:	Text Input
Fax Number:	Text Input
Mobile Number:	Text Input
Company Name:	Text Input
Address 1:	Text Input
Address 2:	Text Input
Country:	Dropdown Menu (United States of America)
City:	Text Input
State/Province:	Text Input
ZIP Code:	Text Input

Figure 160 My Profile - Contact Information

Security Preferences

The second configurable tab is **Security Preferences**. This section contains your login credentials, security questions and answers if you forget your password, along with customizable account management content.



UltraDNS 2.0

My Profile **Security Preferences**

Login Credentials [Reset](#) [Save](#)

User ID: teamrest

Old Password:

New Password:

Confirm Password:

Password must be 6-32 characters long and include at least 3 of the following: an uppercase letter, a lowercase letter, a numeral, or a non-alphabetic character (such as !, \$, #, %). Spaces are not allowed.

Security Question [Reset](#) [Save](#)

Security Question #1: What is your high school mascot?

Security Answer:

Security Question #2: What year was your mother born?

Security Answer:

Security Question #3: What was the name of your first pet?

Security Answer:

Figure 161 My Profile - Security Preferences

Login Credentials

The Login Credentials allows you to reset the password for your account, rather than using the “Forgot Password” option on the login screen, and using a temporary password to log in.

Once you’ve provided a new password, click the **Save** button.

Security Question

In order to use the *Forgot Password* function, you’ll need to provide three different security questions, with corresponding answers. A random security question will be selected when you attempt to reset your password for your account.

Click **Save** once you’ve provided all three security questions and answers, or click the **Reset** button to

restore your previous security questions and answers.

Inactivity Timeout Reset Save

Inactivity Timeout: 30 minutes

Password Expiration Reset Save

Password Expiration: Never

Account Level Allowed IP Ranges + Add - Delete Selected

No records found

Figure 162 My Profile - Security Preferences cont.

Inactivity Timeout

The Inactivity Timeout section gives you control of when the UI Portal will automatically sign you out of your account for inactivity. Select a time limit from the drop-down menu, and then click the **Save** button.

Password Expiration

The Password Expiration section allows you to determine how often your password needs to be reset. Select an option from the drop-down menu, and then click the **Save** button.

Account Level Allowed IP Ranges

The Account Level Allowed IP Ranges allows you to specify the IP addresses that your individual account can access the UI Portal from, unlike the [Accounts](#) section – Account Level Allowed IP Ranges which restricts which IPs that the overall Account name can access the UI Portal from.

News

The News section of the UI Portal displays important updates and features being made to the UI Portal and across Neustar, as well as providing direct links to other departments and resources within Neustar that you may find valuable and useful.

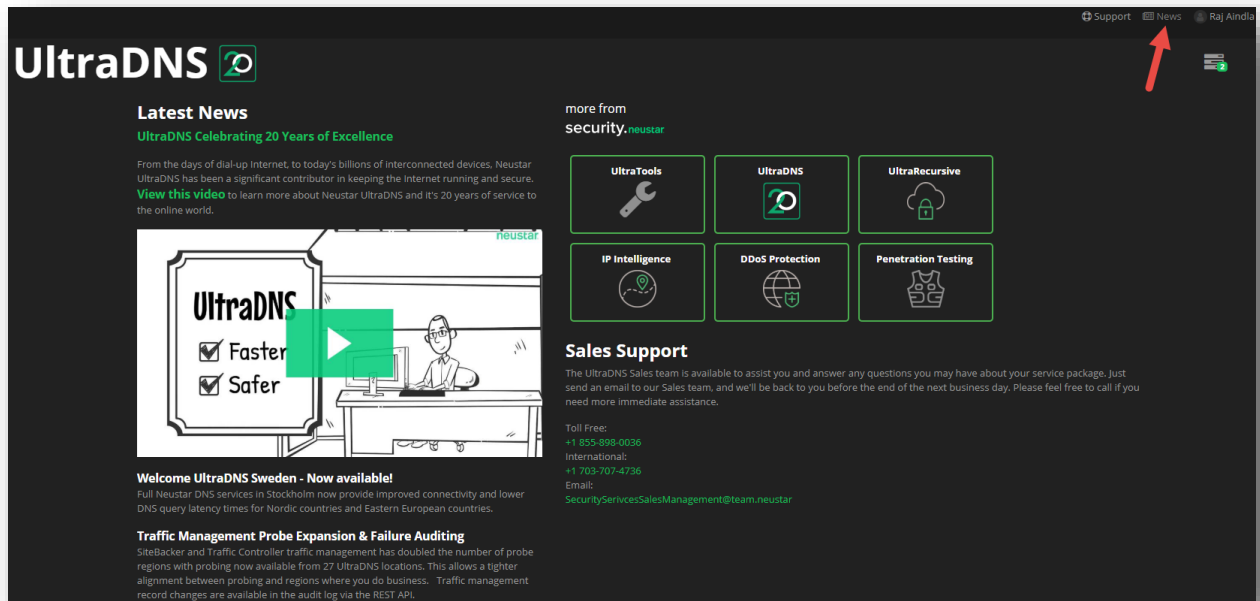


Figure 163 News - Landing Page

Support

The Support section of the UI Portal can either direct to the Neustar Support Website, or to the UI Support center that contains our User Guides, Tech Notes, and additional support documentation.

Support Center

The Support Center provides the Neustar Support contact information which is available 24/7 to our customers, along with a link to our Support portal.

Additionally, you will find User Guides, Quick Start Guides, and Tech Notes to assist you in your day-to-day operations on the UI Portal. The bottom of the Support Center displays our Release Notes, which provide short descriptions of new features and updates that we make to the Portal as well as our API.

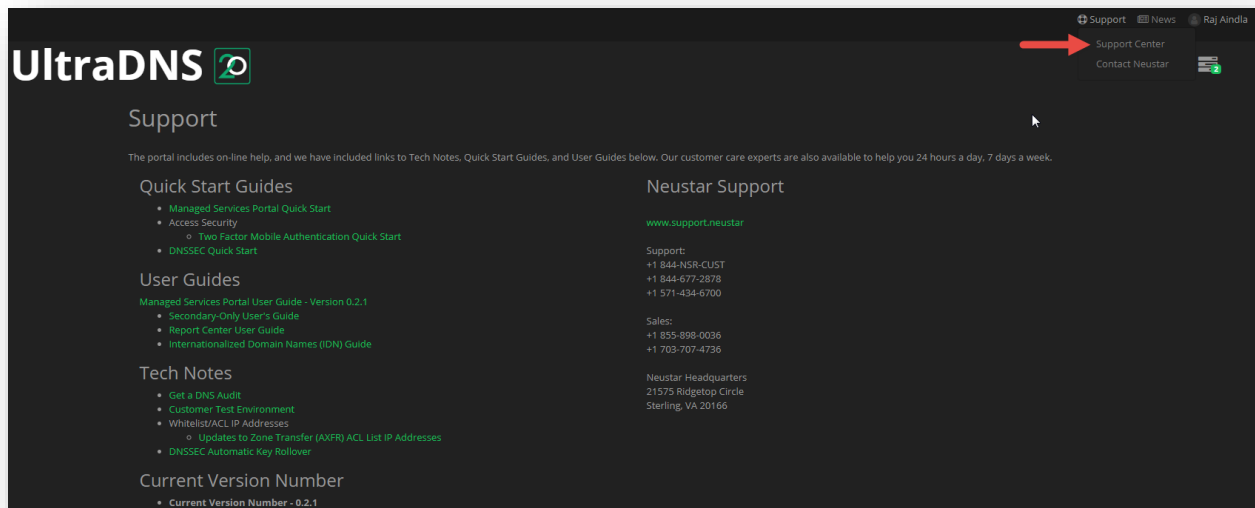


Figure 164 Support - Support Center

Contact Neustar

Clicking on the **Contact Neustar** link will direct you to the Neustar home webpage that provides a list of our office locations, sales and marketing information, along with contact information for specialized inquiries.

The screenshot displays the Neustar website's contact page. At the top, the Neustar logo is on the left, and navigation links for Identity, Solutions, Clients, Partners, Industries, About, and Blog are on the right. A hero section features a cityscape background with the text: "With offices all over the globe, we want to make it easy for you to reach us. Whether it's for a billing question, a sales inquiry, product support, or even if you're under a DDoS attack and need immediate assistance, we're here to help." A green "Let's Connect" button is on the right, with the phone number "+1-855-898-0036" below it.

U.S. Locations

Neustar Headquarters 21575 Ridgetop Circle Sterling, VA 20166 +1 571-434-5400	Chicago 311 S Wacker Suite 1060 Chicago, IL 60606 +1 571-434-5400	Los Angeles 11150 Santa Monica Blvd 5th Floor Los Angeles, CA 90025 +1 310-914-5677
Louisville 1650 Lyndon Farm Court Suite 300 Louisville, Kentucky 40223 +1 (502) 653-3800	New York 100 Park Avenue New York, NY 10017 +1 571-434-5400	San Diego 4655 Executive Drive 4th Floor San Diego, CA 92121 +1 858-461-2400
San Francisco 505 Howard Street San Francisco, CA 94105 +1 415-659-1500		

Global Locations

Bangalore 57/A 1st Main Road Sarakki Industrial Estate JP Nagar 3rd Phase Bangalore, Karnataka 560078 India	Costa Rica Metro Free Zone, Lot 5, Block C, Building, 5C Heredia, Costa Rica, 40104 +1 506-2298-3700	Hamburg WeWork Europa Passage Neustar (7th floor) Hermannstrasse 13 20095 Hamburg Germany +49.40.226 115 68
Hyderabad 4-51/SLNT/L05-03-01, SLN Terminus, Gachibowli, Hyderabad - 500032 Telangana, India +91 40 45210003	London 21 Palmer Street London, SW1H 0AD United Kingdom +44 (0) 1784 448 444	Melbourne Level 8, 10 Queens Road Melbourne 3004 Australia +61 3 9866 3710

Specialized Inquiries

Product Support Get answers to service questions. Sign in to our easy-to-use portal. Submit support requests. Product Support	Billing Call toll free (US/Canada): +1 877-245-5277 Billing questions?	Under DDoS Attack? Call now and we'll help you mitigate the attack and restore service to your site. 1-855-727-1209	Media and Press Relations Email: PR@team.neustar Have a Privacy question? Read our Privacy Policy .
---	--	--	---

Figure 165 Support - Contact Neustar