

Enabling outgoing zone transfers

Zone transfer is a mechanism to send zone data from one DNS server to another. Typically, this occurs after a change to data in a zone. A secondary server discovers it no longer possesses the current version of the zone via one of the following:

- The primary server informs the secondary of any changes in the zone using a [DNS NOTIFY](#) message.
- The secondary identifies changes after checking the primary based on SOA timers.

In terms of **outgoing zone transfers**, the NS1 Connect platform supports taking the role of the primary name server with one or multiple external secondary name servers receiving zone transfers from NS1.

This article describes the configuration of outgoing zone transfers within NS1 Connect, which allows zone transfers via [AXFR](#) and supports the following:

- NOTIFYs sent from primary servers to inform secondary servers of changes to a zone's data
- NOTIFYs signed with [TSIG](#) to ensure the authenticity of the sender

NOTE

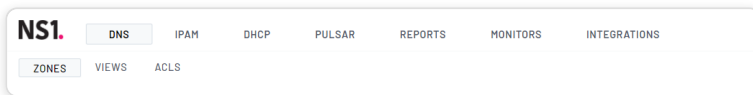
Transaction signature (TSIG) is a mechanism for authenticating DNS messages by signing them with a shared secret. Presently, NS1 Connect supports the TSIG-signing of NOTIFY messages. At this time, zone transfers where NS1 Connect is primary will not be TSIG-signed for Managed DNS customers; however, Cloud-managed DDI customers will be able to sign zone transfers with TSIG.

Enable outgoing zone transfers

After configuring NS1 as a [primary](#) or [secondary](#) DNS provider, visit the **Zone Transfers** page which contains the *Allow Outgoing Transfers* mechanism. This lets you define a secondary server for a zone being served on NS1 Connect.

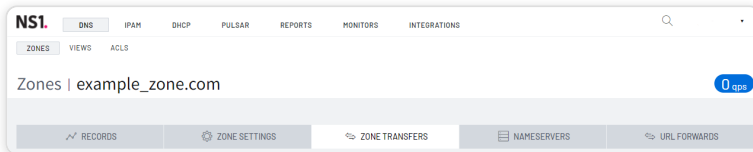
Follow the steps below to configure outgoing zone transfers in the NS1 Connect platform.

1. Navigate to **DNS > Zones**.

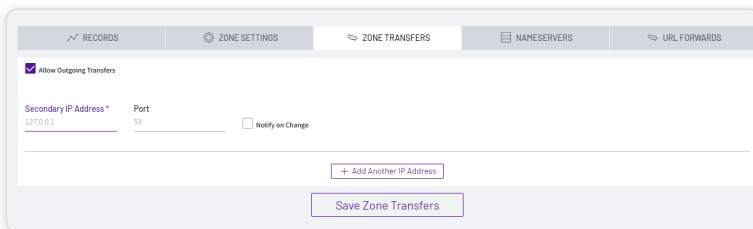


2. From your list of zones, click the zone on which you want to configure an outgoing zone transfer.

3. Click **Zone Transfers**.



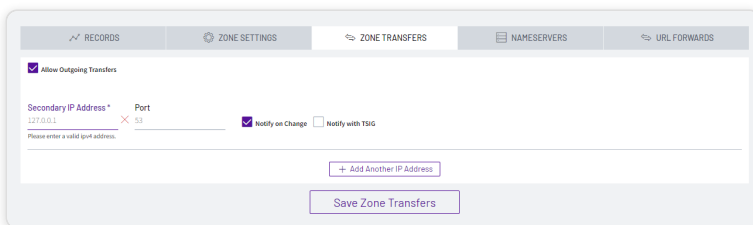
4. Enable the *Allow Outgoing Transfers* checkbox. Additional parameters will appear.



5. Add a *secondary IP address* (a valid IPv4 address) and *port* number. This is the server to which you will allow outgoing zone transfers.

6. Optionally, click **Add Another IP Address** if you want to add more servers as a list of those allowed.

7. Optionally, enable the *Notify on Change* checkbox for each server added.



NOTE

If you enable *Notify on Change*, a primary DNS server sends a NOTIFY to secondary servers informing them of the zone data change. After a secondary receives a NOTIFY, it sends a zone transfer request to the primary to get in sync with it.

8. Optionally, enable the *Notify with TSIG* checkbox to send a **TSIG-signed NOTIFY**. Fill out the fields that appear—select a *TSIG hash* from the drop-down and input a *TSIG key name* and *TSIG key value*.

These are required fields if you want to send a TSIG-signed NOTIFY.

Notify on Change Notify with TSIG TSIG hash TSIG Key name * TSIG Key Value *

WARNING

This is a TSIG-signed NOTIFY, **not** TSIG authentication on the actual zone transfer. For TSIG authentication on the zone transfer itself, you need to create a [DNS view](#), add a TSIG Access Control List (ACL), and attach it to the zone.

NOTE

Currently, the NS1 DNS views functionality required to allow TSIG authentication is only available for zones in [Cloud-Managed DDI](#) networks. Managed DNS networks do not yet support DNS views; however, this is a future feature.

9. Click **Save Zone Transfers** when finished. Your specified server(s) will now receive outgoing zone transfers.