Conexim DNS Administrator's Guide

Last Updated February 2016

Contents

Conexim DNS Quick Reference

If you are familiar with Conexim DNS and DNS in general, the details below will get you up and running in no time at all.

DNS Delegation Information

Delegate your domain names to the Conexim DNS AnyCast network using the below name servers:

Name Server	IPv4 Address	IPv6 Address
ns.cdns1.net	203.124.190.53	2401:400:e001::53
ns.cdns2.io	203.124.191.53	2401:400:e002::53

Control Panel Access

Access to the Control Panel for managing Conexim DNS can be accessed from https://my.conexim.com.au

Supported Record Types

Conexim DNS supports any current or emerging DNS RR (Resource Record) type as per RFC 3597, but includes full validation support for the following types.

Resource Record Type	Entry	RFC
A	IPv4 Address	RFC 1035
AAAA	IPv6 Address	RFC 3596
CNAME	Alias to another hostname	RFC 1035
MX	Mail Exchanger Host	RFC 1035
NS	Name Server	RFC 1035
TXT	Text	RFC 1035
SRV	Service Locator	RFC 2782
SPF	Sender Policy Framework	RFC 4408
PTR	Pointer (Reverse DNS)	RFC 1035
ANAME	CNAME-Like on Zone Apex	Conexim Proprietary
All Others	-	RFC 3597

Getting Support

Speak to someone with a deep understanding of DNS whenever you contact Conexim Support:

Phone: 1300 133 900 (+61 2 8214 5800)
Email: support@conexim.com.au or via the DNS Control Panel.

Introduction

DNS is at the foundation of your web sites, email, applications and cloud services, so it's important that it's secure, always available and delivers high performance. Conexim is trusted by thousands of companies to deliver professional, managed DNS services that meet the strictest requirements for performance, reliability and security.

Conexim's Managed DNS platform has been engineered from the ground up with years of Internet engineering experience in delivering always available DNS services.

The DNS platform is managed through Conexim's management portal which provides a familiar interface for managing all Conexim managed services. It provides powerful DNS functionality beyond basic DNS zone management in a way that is both accessible and helps avoid common mistakes that may compromise availability or performance of DNS.

Feedback

Conexim encourages and welcomes feedback to ensure we're delivering the best services possible. If you have ideas for a new feature, or if there's an aspect of Conexim DNS you feel we could improve, please let us know – we'd love to hear from you.

Please send feedback to feedback@conexim.com.au.

1. Logging in to DNS Management

When you subscribe to a Conexim Managed DNS Service, you will be provided with an email detailing the username and password to login to My Conexim.

To access DNS Management, simply visit https://my.conexim.com.au and enter your email address and assigned password. Once logged in, there are two ways you can access DNS Management – either from the home page, or the icon on the front dashboard.
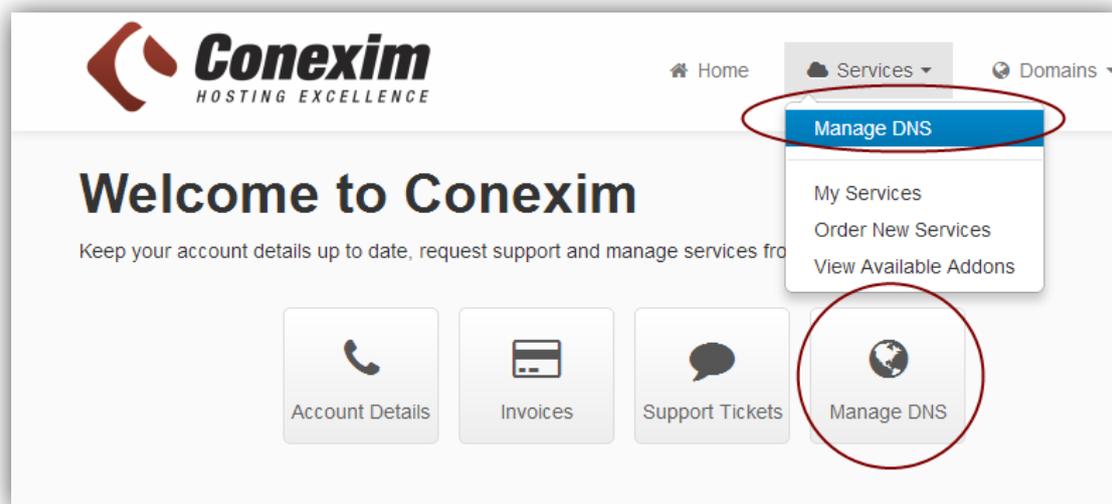
2. Basic Zone Management

The screen below displays a typical display of current DNS Zones that are configured for the service.

2.1 Creating a New Zone

Conexim DNS allows you to create three types of zones:

- **Standard Zone (Default):** There are no primary or secondary DNS servers other than those run as part of Conexim's platform.
- **Master Zone with Slaves:** Select this option if you wish to use Conexim's DNS platform to act as a DNS Master server, with your own server(s) operating as slaves.
- **Slave Zone:** If you already operate a DNS server operating as a Master and wish to use Conexim's DNS platform as a Slave, select this option.

With the exception of very specific use cases, **Standard Zone** suits most situations. See the sections on **Managing Master and Slave Zones** for details on additional configuration required for each of these options.

6

When creating a new DNS Zone, you are provided with several options for creating the zone:
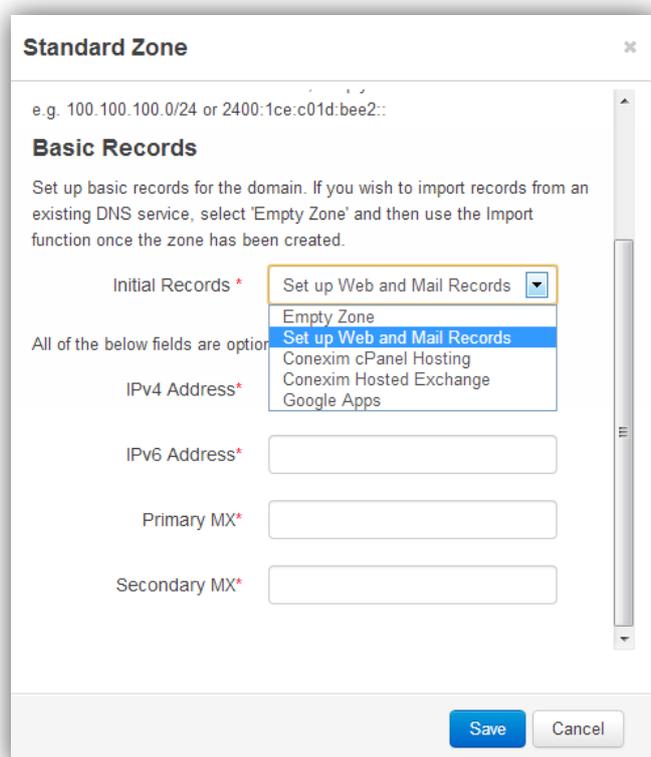
Once you've entered the name for the new zone to be created, there are several options for populating the zone with an initial set of records. These are:

Empty Zone: Creates only the NS records and sets up the SOA.

Web and Mail Records: If you know the IP address (IPv4 and/or IPv6) of the web server and also the MX (mail exchanger) server details, select this option.

Conexim cPanel Hosting: Sets up hosting for Conexim cPanel Shared Hosting Services.

Conexim Hosted Exchange: Sets up the appropriate DNS records for Hosted Microsoft Exchange.

Conexim DNS also contains a template for **Google Apps**, allowing you to set up a zone for running Google Apps in a single operation. This configures the appropriate MX records, CNAME and also prompts you to enter the Google Apps Domain Verification TXT Record if you have one.

2.2 Resource Records

Each DNS zone contains a collection of Resource Records (RRs). In their simplest form, Resource Records define mappings between names and IP addresses (A and AAAA Records), define aliases between names (CNAMEs) or provide Email Server (Mail Exchanger / MX) information.
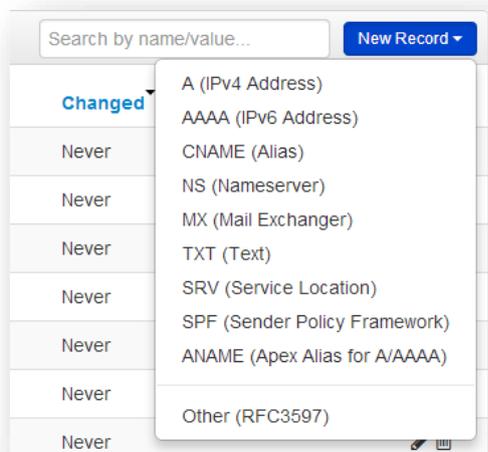
Conexim DNS supports a standard set of RR types as described below, but in addition, supports virtually any RR type that may be defined in the future by supporting RFC 3597.

For each type of Resource Record that Conexim DNS directly supports, thorough validation of entries (where possible) is performed to ensure that common mistakes are avoided.

**A:** IPv4 address - maps a name to an IPv4 address.

AAAA: Equivalent of an A Record, but for an IPv6 address. If the server supports both IPv4 and IPv6 (Dual-Stack), you must crease both an A and an AAAA record.

CNAME: Aliases one record to another. For example, www.yourdomain.tld may be aliased to server cpanel1.conexim.com.au. If you need to apply an alias to the apex (or root) of a DNS zone, please refer to the **ANAME** record type.

NS: Name Server records define the servers that respond to DNS queries for the zone.

MX: Mail Exchanger records define hosts that will accept email on behalf of the domain.

TXT: Text Records serve multiple purposes, but at their lowest level contain text. They are commonly used for DKIM (DomainKeys) Email Signing and SPF (Sender Policy Framework).
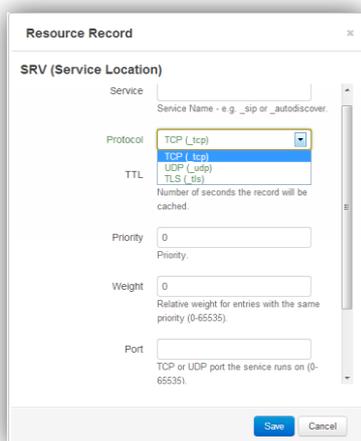
SRV: Service Records define the location (specifically, the hostname and port number) of servers for specified services. Common uses for SRV records are SIP (IP telephony), Microsoft Exchange, Lync and Active Directory. Conexim DNS provides a single form to assist in correctly setting up each of the attributes of an SRV record.

SPF: Sender Policy Framework records define a list of servers or networks that are allowed to send emails on your domain's behalf. Conexim DNS includes a single form for managing SPF records.
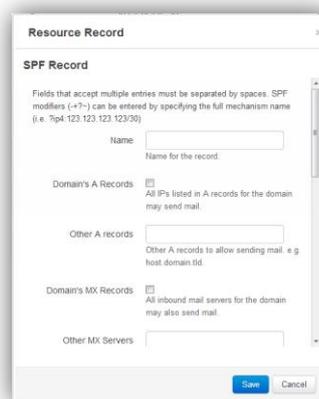
ANAME: RFC 1033 does not allow CNAMEs (aliases) to be applied to the apex (root) of a zone. This means that while it's valid to have:

   www.conexim.net CNAME server.conexim.net

It is not possible to have:

   conexim.net CNAME server.conexim.net

There are a number of use cases that legitimately require pointing the zone apex to another record and Conexim supports this through a proprietary **ANAME** record type.

The ANAME type can only be applied to the apex of a zone. When used, upon receiving a request from a DNS client or resolver to return records for the root of the zone, it internalises a lookup of all A and AAAA records on the target's fully qualified domain name and returns them as part of the result set.

Any existing A or AAAA records on the zone containing the ANAME record are not included in the result set.

TTLs on the returned records are assigned the value of the TTL defined as part of the ANAME record and in general, are recommended to be set to 60 seconds. TTLs on the destination record apply during the lookup of the zone.

In establishing a TTL for the A/AAAA records the DNS client ultimately receives, it's important to consider that the TTL can be up to the sum of the TTL defined for the ANAME record and the TTL for the destination record.

Other Records: If there is a Resource Record type that does not exist in the list above, it can be created by selecting **Other (RFC 3597).** From here, you can enter any type desired. This can be used for creating new types of resource record or specifying rarely used RR types such as **HINFO**, **SSHFP, LOC, AFSDB** and **NAPTR**.

<u>Naming Resource Records</u>

If you are familiar with other types of DNS server such as BIND, you will note that zone files typically allow you to specify the complete fully qualified domain name (www.testzone2.net) or just the name of the record itself (www). Conexim DNS requires that you enter the name of the record itself or leave the name field blank if you wish to create the record on the base (apex) of the domain.

The Time to Live (TTL) Attribute

In addition to the record-specific attributes that RRs contain, there is also a TTL (Time to Live). The TTL defines for how long a caching nameserver should keep the current version of the record before a new request is made to the authoritative nameserver.

It's important to set the TTLs for records appropriately to ensure you can take advantage of a caching nameserver's ability to quickly respond to DNS requests and at the same time, ensure that the setting is such that records that are likely to need to be changed quickly are not inhibited by delays in caching nameservers serving the updated record.

While the settings will depend on your exact implementation, Conexim offers the following guidance in setting DNS records:

Record Type	TTL	Comment
NS	86400 (24h)	Name Servers are unlikely to change often and can usually be planned with some notice.
MX	86400 (24h)	The nature of email being able to store and forward allows for longer TTLs.
A and AAAA	300-3600 (5m-1h)	Depending on the purpose of the record, A/AAAA records are more likely to require a change. If the record may need to be changed as part of Disaster Recovery, these must be set lower.
SPF	86400 (24h)	SPF records are unlikely to experience frequent change.
ANAME	60 (1m)	Setting the TTL to the lowest possible ensures that reliance is on the TTLs of the target of the CNAME record.

Priority Attribute

Both MX and SRV records contain a priority attribute. Where there are multiple servers serving mail or providing a specific service, configure multiple records with the same name (usually blank for MX), the record with the lowest priority number is the more preferred.

2.3 SOA (Start of Authority)

The Start of Authority (SOA) specifies authoritative records for the DNS Zone. In the vast majority of cases, these values do not need to be changed, however each of these are configurable if needed.

Nameserver: Primary/master name server that can respond authoritatively for the domain.

Hostmaster Email: Email contact for the domain. Note that this is not entered in the standard way of entering an email address – it must be entered as **user.domain.tld** (replacing the "@" with a ".").

Refresh Interval: Only applicable when operating a zone with slaves, indicate how frequently slaves should refresh from the master.

Update Retry: Interval between retries when a slave server fails to contact the master.

Expiry: When slaves should stop responding to requests for a given zone if they have not been able to successfully contact the master.

Minimum: The minimum amount of time resource records should remain in another nameserver's cache.

Serial Number: The serial number is system managed and is updated each time a change is made either to the SOA or one of the Resource Records. The format of the serial number indicates the date on which the record was last changed as YYYYMMDDXX with the last two characters incremented from 01.

2.4 Internationalised Domain Names (IDN)

An internationalised domain name (IDN) is an Internet domain name that contains at least one name that is displayed in software applications, in whole or in part, in a language-specific script or alphabet, such as Arabic, Chinese, Russian, Tamil or the Latin alphabet-based characters with diacritics, such as French.

Conexim DNS fully supports IDN either by first converting names (or domain names when creating zones) to the ASCII equivalent format, or by simply entering the original language-specific script. Conversion takes place on-the-fly.

Where IDNs are used, ConeximDNS displays both the original Unicode character as well as the ASCII equivalent.
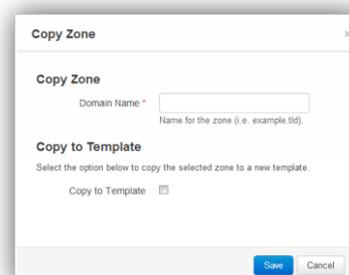
3. Templates

When operating a large number of zones, it's often inevitable that zones share similar configuration. Changing individual records on each zone can be a time consuming, tedious and error prone task.

Conexim DNS supports Zone Templates which address this problem by allowing you to build a template containing all of your desired records and then creating new zones based on the template. Changes made to the template apply to all dependent zones.

3.1 Creating a Template

There are two ways in which you can create a template:

1. Create a template from scratch from the **Templates** section. You can either configure RRs manually or use the import function to import records from another DNS server (see ***Importing Records)***.

2. Copy an existing zone to a template. This is done by selecting the **copy** icon next to the DNS zone and selecting the **Copy to Template** option. The domain name entry represents the name you wish to apply to the template.

3.2 Creating Zones from a Template

To create zones that are based on the template, simply select the template and select the **Templated Zones** tab. From here, you can add, delete or detach zones from the template.

Detaching zones from a template allows the zone to be modified independently as a regular zone.
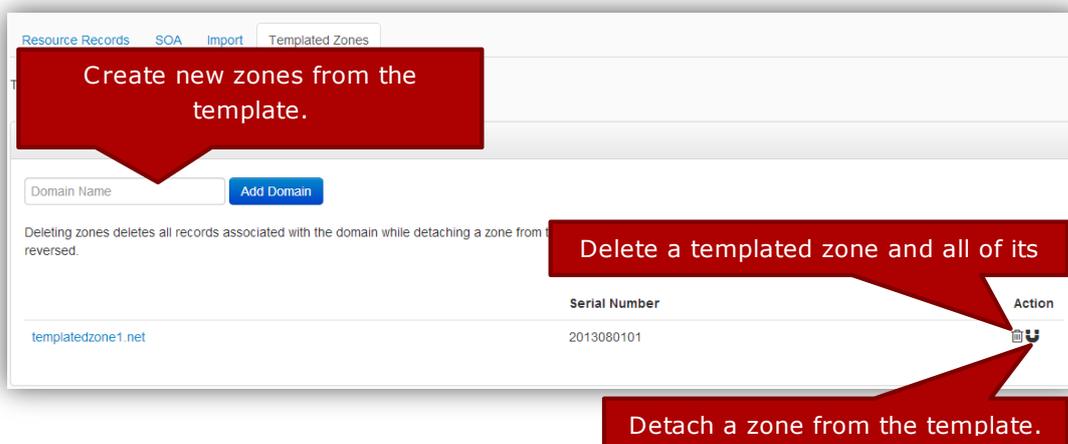

3.3 Deleting Templates

Deleting a template deletes the template, but none of the zones that are created from the template. Zones continue to work as regular independent zones, but cannot be re-attached to a template.

4. Importing Records

Conexim DNS supports importing records from another DNS server. Records can be imported into existing or newly created DNS zones or templates from the following sources. Each source may have specific requirements to enable you to import records from – these are detailed as follows:

Import Type	Requirements
AXFR Zone Transfer	Import DNS records from a BIND or compatible server using an AXFR request. The source DNS Server must support AXFR zone transfers – you may need to configure an Access Control List (ACL) on the source server to allow AXFR requests from **my.conexim.com.au.**
AXFR Zone Transfer with TSIG Auth.	Similar to a regular AXFR request, this method offers improved authentication using TSIG (Transaction Signature) keys. The TSIG keys must be preconfigured on your source DNS Server. As with a regular AXFR zone transfer, you may be required
Record Discovery	This method attempts to guess common DNS records, including MX, SPF/TXT and common A/AAAA records such as 'www'. This method is ineffective if you use a wildcard name (*.yourdomain.tld) as all requests will return a response.
Import BIND Zone File	If the source DNS server runs BIND or can produce BIND-compatible Zone Files, these can be copy/pasted. This is also effective if you have output from a utility such as **dig** (Linux/FreeBSD/Mac OS X) that produces output compatible with BIND zone files.

To import records, simply create the zone (in the case of creating a new zone) and selecting the **Import** tab.
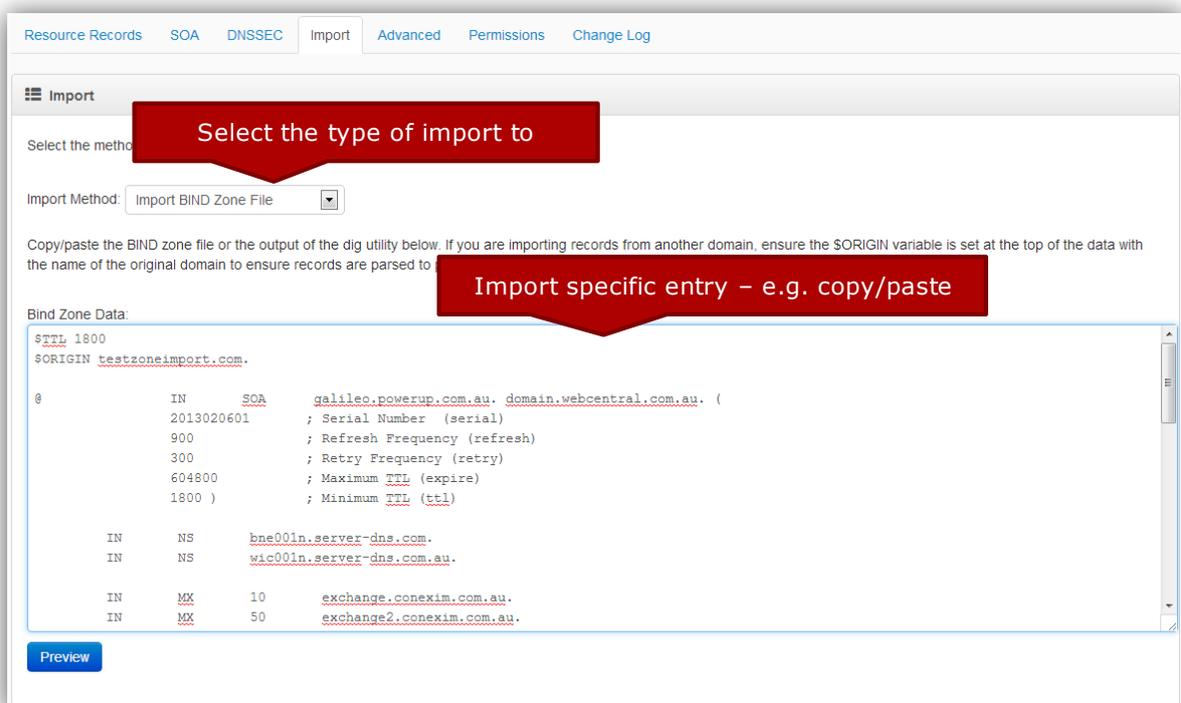
Once you click on the **Preview** button, records are validated and you can select which ones are to be imported. By default **NS** records are deselected from the list as they are generally modified to match that of the destination DNS servers.

5. DNSSEC

Recently discovered vulnerabilities in the original DNS specifications from the early 1980s have significantly reduced the time it takes an attacker to hijack the DNS lookup process and thereby take over control of a session to, for example, direct users to their own deceptive Web sites for account and password collection. The only long-term solution to this vulnerability is the end-to-end-deployment of a security protocol called DNS Security Extensions – or DNSSEC.

Conexim DNS fully supports DNSSEC for providing origin authentication of DNS data. The purpose of DNSSEC is to provide certainty that DNS responses are from the intended source.

In order to use DNSSEC, it's imperative that the following are in place:

1. The registry operating the TLD (Top Level Domain) is DNSSEC signed and supports DS (Delegation Signer) records. An up to date list is available from http://stats.research.icann.org/dns/tld_report/. The Australian .au namespace currently DOES NOT support DNSSEC, however a large number including .net, .com, .net and .nz do.
2. The registry supports configuring of DS (Delegation Signer) records. In some cases, it's necessary to submit requests to your registrar manually to apply DS records.
3. The DNS Zone has DNSSEC enabled and the generated DS records match those configured at the registry.

While DNSSEC offers a multitude of options for DNSSEC key management, Conexim DNS makes DNSSEC straightforward to enable and maintain while still allowing advanced users to manage keys to their preferences.

Enabling DNSSEC for a DNS Zone

After confirming that the domain name can be DNSSEC enabled, simply enable DNSSEC for the zone within Conexim DNS. Two modes of operation are available:

- **NSEC3: Recommended**. Avoids zone enumeration by returning next valid NS records on an unsuccessful DNS query.
- **NSEC**: Offered for backward compatibility only. This method is part of the original DNSSEC specification and while useful for authenticating originating DNS data; it is vulnerable to exposing more information than is necessary about a zone.
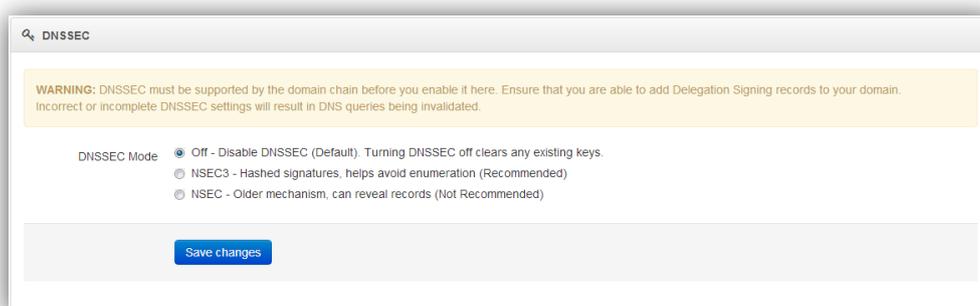
DNSSEC KSK and ZSK Keys

Once DNSSEC has been enabled, two types of keys are generated:

KSK (Key Signing Key): Used longer term, these keys are used for signing ZSKs. Current best practice is that these keys are rotated yearly.

ZSK (Zone Signing Key): Used shorter term, these keys are used for signing DNS zone data and should be rolled over much more frequently.

For both DNSSEC KSK and ZSK, Conexim DNS supports the following algorithms at 1024 or 2048 bit.

- RSA/SHA1
- RSA/SHA256 (default)
- RSA/SHA512
- ECC-GHOST

DS (Delegation Signer) Records

Delegation signer records are records signed by the KSK and are stored with the parent zone (e.g. .com) by the registry. If you wish to use a new ZSK, it's important that you generate new DS records and assign these to the zone with the registrar.


Verifying DNSSEC Records

In order to ensure your DNSSEC records have been configured correctly, it's recommended that you use a tool to validate the correct set up of the zones. Two such tools include:

Verisign Labs DNSSEC Debugger: http://dnssec-debugger.verisignlabs.com/
DNSViz: http://dnsviz.net

6. Reverse DNS Records

Conexim DNS fully supports reverse DNS entries and provides several facilities to simplify management of both IPv4 and IPv6 reverse DNS.

In order to use Reverse DNS, you must ensure that the owner of the address space is able to delegate the subnet to Conexim's DNS servers.
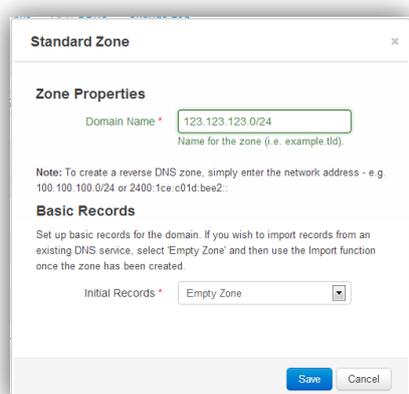
While it is possible to manually create .in-addr.arpa (IPv4) and ip6.arpa (IPv6) reverse DNS zones, Conexim DNS will create the appropriate zones simply by entering an IPv4 or IPv6 CIDR.

IPv4 Reverse DNS Schemas

For IPv4, reverse DNS delegations are typically performed on a /24 block, however smaller allocations can also be handled by Conexim DNS – either automatically, or manually.

If you enter an IPv4 subnet with a subnet size smaller than a /24, Conexim DNS will generate the DNS zone based on RFC 4183 notation.

RFC 2137 and DeGroot notation are fully supported if are manually entered.

IPv6 Reverse DNS

IPv6 Reverse DNS is fully supported with zones automatically created when you enter an IPv6 subnet in CIDR notation or create the .ip6.arpa zone manually.

Creating and Updating PTR Records
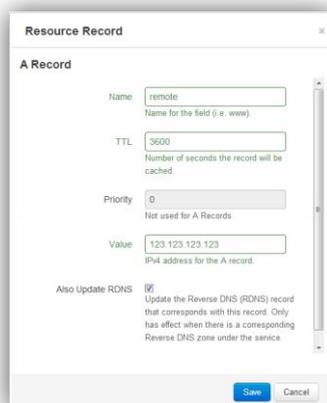
PTR records can be created manually within the reverse DNS zone, however they can also be created/updated when managing an A or AAAA record for a regular DNS zone.

# 7. Managing Permissions and Auditing Changes

7.1 Managing Sub-Accounts

Conexim DNS provides full access control capabilities, allowing you to create user accounts for each person responsible for managing DNS zones. Furthermore, user accounts can be restricted by the level of access that they have on either a global basis, or per DNS zone.

Before permissions can be granted to a user, they must first have a sub-account configured within the Conexim Portal. To manage sub-accounts, login to the Conexim Portal with your login and locate your name at the top-right hand corner and select **Contacts/Sub-Accounts** from the drop-down menu.
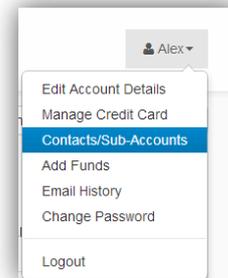
7.2 Assigning Permissions

Once the sub-contacts have been created, you can assign permissions either on a global level (enabling the permissions to all zones) or on a per-zone basis by clicking on the **Permissions** link within a zone or at the top of the DNS management page.
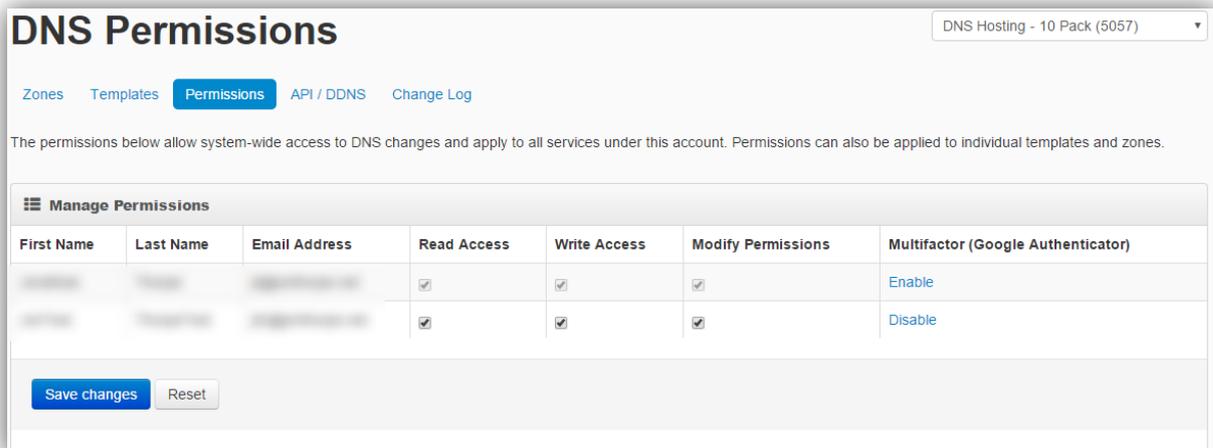
Permissions are assigned as follows:

> **Read Access:** The specified user can read all properties and records, but not modify.
> **Write Access:** Make changes to all aspects of a zone with the exception of permissions. If assigned on a global level, modify all zones.
> **Modify Permissions:** Allows the user to change permissions or assign permissions to another user.
> **Multifactor (Google Authenticator):** Enable or disable multi-factor authentication with Google Authenticator.

It is also possible to enable **Read** access on all zones at a global level and then enable **Write** or **Modify Permissions** on a per-domain level to enable more granular control.

7.3 Multifactor Authentication

For plans that support it, Conexim offers multi-factor authentication to ensure multiple levels of authentication are verified before a user can make changes. Multifactor authentication requires that the user has a mobile device (e.g. iPhone or Android) running Google Authenticator that is paired with their account.

To enable multi-factor authentication, perform the following steps:

1. Navigate to the **Permissions** tab.
2. Click on **Enable** for the user under which you would like to enable the multi-factor authentication.
3. Scan the QR code or take note of the Secret Key for manual entry into the Google Authenticator app.
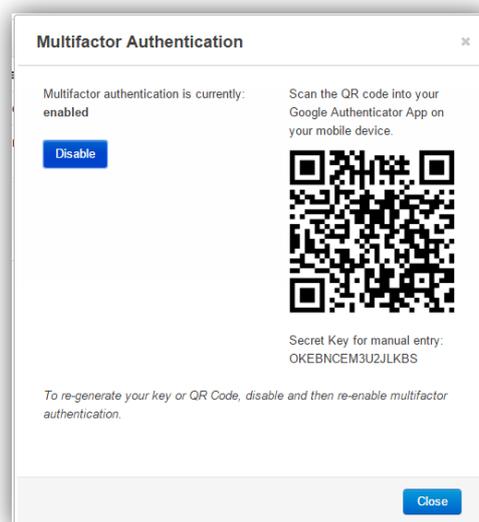
7.4 Auditing Changes

All actions relating to zones (create, update or delete) are logged. The level of logging varies depending on what has been changed, however, the following details are logged:

Timestamp: Time and Date of the change. Times are stored in Sydney Time.
Login IP Address: Either the IPv4 or IPv6 address from which the request came.
Modified By: Keeps track of the user who made the change. If the change was made by means of DDNS Update or through an API call, the API key identifier is logged.

Timestamp	Modified By	IP Address	Item	Operation	Message
2013-08-01 13:37:13	Conexim Support ID 3		RR	create	Create NS with name testzone.net to value ns.cdns2.io for testzone.net
2013-08-01 13:37:13	Conexim Support ID 3		RR	create	Create CNAME with name autodiscover.testzone.net to value exchange-autodiscover.conexim.com.au for testzone.net
2013-08-01 13:37:13	Conexim Support ID 3		RR	create	Create SRV with name _autodiscover._tcp.testzone.net to value 1 443 exchange.conexim.com.au for testzone.net
2013-08-01 13:37:13	Conexim Support ID 3		RR	create	Create CNAME with name webmail.testzone.net to value exchange.conexim.com.au for testzone.net
2013-08-01 13:37:13	Conexim Support ID 3		RR	create	Create MX with name testzone.net to value exchange.conexim.com.au for testzone.net
2013-08-01 13:37:13	Conexim Support ID 3		RR	create	Create MX with name testzone.net to value exchange2.conexim.com.au for testzone.net
2013-08-01 13:37:12	Conexim Support ID 3		Domain	create	Create domain testzone.net type: Standard master IP:
2013-08-01 13:37:12	Conexim Support ID 3		RR	create	Create SOA with name testzone.net to value ns.cdns1.net hostmaster.conexim.com.au 2013080101 86400 7200 1209600 3600 for testzone.net
2013-08-01 13:37:12	Conexim Support ID 3		RR	create	Create NS with name testzone.net to value ns.cdns1.net for testzone.net

Changes may be viewed on either a per-domain basis, or globally.

8. External Zone Transfers (AXFR Access)

Conexim DNS includes the ability to set up external AXFR (DNS Zone Transfer) access to support access from third party software, or to run a slave server external to Conexim DNS infrastructure.

Conexim DNS provides two modes of authentication for AXFR requests:

IPv4 / IPv6 Access Control Lists

Nominated IPv4 and IPv6 addresses are allowed to perform full zone transfer requests (AXFR) on a given zone.

TSIG (Transfer Signature) Shared Secrets

TSIG Shared Secrets can be used on their own, or in addition to IPv4/IPv6 Access Control Lists for a given zone to enhance the level of authentication required to provide access to zone information.

AXFR access is configured within the **Advanced** tab of a given zone.

In addition to supporting TSIG keys for incoming AXFR requests, TSIG keys can also be configured for outgoing AXFR requests when Conexim DNS is configured as a slave for another master DNS server.

26

9. API and Dynamic DNS (DDNS)

Conexim DNS provides external access by means of RESTful API and Dynamic DNS (DDNS) updates.

9.1 Managing Authentication

Conexim DNS manages authentication for DDNS and API access as follows:

1. An API key is created that can be used for DDNS and/or API access.
2. Dynamic DNS is authenticated using the API Key ID (12 digit unique ID) and a user-specified password.
3. API Access is authenticated by hashing the request against a secret, pre-shared key. The key itself is never sent from the client to the server to ensure the request is secure.

A number of permissions are available for authenticating API and DDNS requests:

Read (GET): Allows properties of a DNS record/zone to be read.

Update (PUT): Enable updating of DNS records/zone, but cannot create new records.

Create (POST): Create a new DNS record/zone, but not update any existing ones.

Delete (DELETE): Allows deletion of a DNS record/zone.

Dynamic DNS: Enables DDNS access. Enabling DDNS access enforces that you enter a password to enable Dynamic DNS authentication. If you wish to enable DDNS, but not API access, **only** enable Dynamic DNS and disable the API-specific permissions (GET/PUT/POST/DELETE).

In addition to key/password authentication, access to the API or Dynamic DNS can be restricted by IP address or subnet. This is useful in the following situations:

1. You use Dynamic DNS and cannot restrict DDNS by IP address, but know what subnet the request is coming from. This can be configured in CIDR (Classless Inter-domain Routing) format.
2. You wish to limit API access from specific IP addresses.

9.2 Conexim DNS API

Please refer to the Conexim DNS API Guide for details on how to make use of the API.

9.3 Dynamic DDNS

Conexim supports Dynamic DNS (DDNS) using an open protocol widely adopted by most Dynamic DNS providers to facilitate the widest possible adoption by equipment vendors. Conexim enforces that Dynamic DNS updates are performed over a secure SSL connection to avoid eavesdropping of DDNS authentication information.
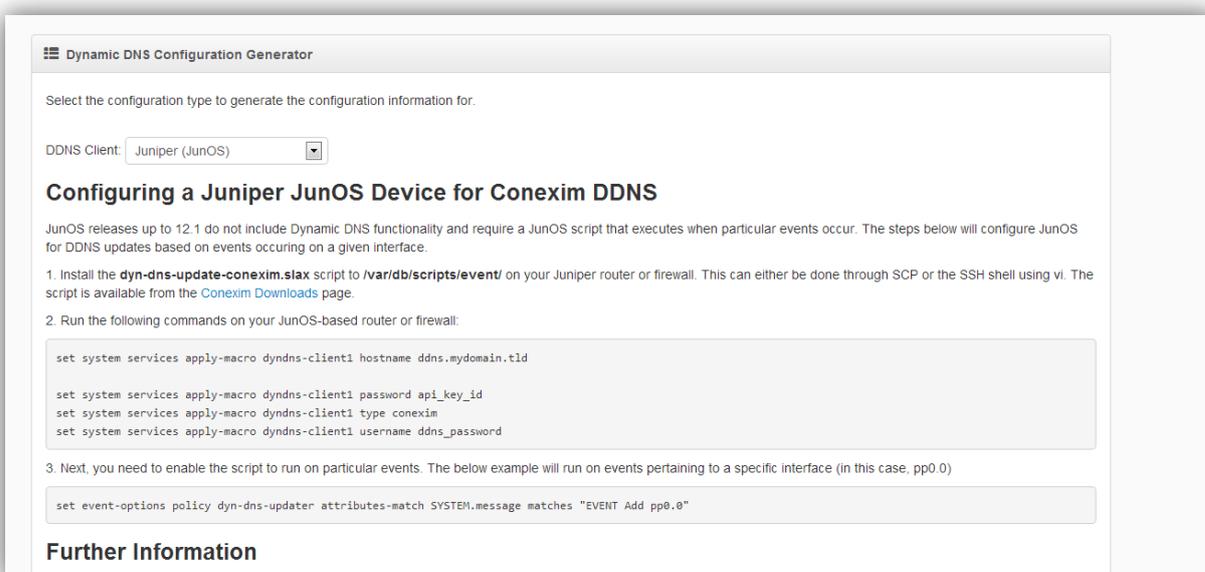
Old DDNS clients that cannot connect over HTTPS may not work with Conexim DDNS. Please contact Conexim Support to discuss your requirements if your device manufacturer cannot support SSL.

9.3.1 Dynamic DNS Configuration Generators

Conexim DNS can generate DDNS configuration information for the following platforms/software:

- Cisco IOS® based routers.
- Juniper JunOS® based routers.
- ddclient for Linux, FreeBSD and other Unix-compatible operating systems.
- A modified version of InaDyn that supports SSL (download from the download page of the Conexim Portal).

To use the configuration generation utility, simply select the type of client you wish to use from the dropdown in the DDNS section of Conexim DNS. This will include instructions and any additional information you may need to successfully configure DDNS.

9.3.2 DDNS Update Protocol

Some devices provide configurable Dynamic DNS support based on the provider's protocol. The Conexim Dynamic DNS Update Protocol is as follows:

> https://**api_key_id**:**password**@**ddns.conexim.com.au**/nic/update?hostname=**ddnshostname.mydomain.tld**&myip=**123.123.123.123**

Conexim DNS also supports an alternative format:

> https://**api_key_id:ddns_password@ ddns.conexim.com.au**/nic/update/**ddnshostname.mydomain.tld**/**123 .123.123.123**

In the above examples, the following items need to be set:

> **api_key_id:** The API Key ID (DDNS Username). Not to be confused with the API Key itself.

> **ddnshostname.mydomain.tld:** The fully qualified domain name of the record you wish to update. This record must exist as an "A" and/or "AAAA" record. If you wish to update multiple records at the same time, specify multiple fully qualified domain names separated by commas.

> **myip:** The IP address to update the record with. If 0.0.0.0 is specified, the incoming IP address is automatically detected and used as the update IP.

Important Note: Conexim DNS requires that requests specify a **User-Agent** header in all requests. This is used to help security mechanisms detect suspicious behaviour and is usually sent by default.

Unsupported Parameters

Similar Dynamic DNS protocols may support the following additional parameters. Conexim does not support the following. Passing these parameters will be silently ignored.

- system
- mx
- wildcard
- backupmx

Server Responses

The Conexim DDNS Update protocol will return one of the following

Status	Description
good <IP>	Successful Dynamic DNS Update
nochg <IP>	Record not changed as the existing record is the same.
nohost	Unable to find the record to update. Please ensure you have the A or AAAA (if performing an update over IPv6) already configured.
badauth	Bad Authentication – verify the authentication settings.
abuse	Most likely, the quota has been exceeded for the DNS Service. Please contact Conexim Support for further information.
badagent	The request is malformed or not understood by the server.