Zone Management Portal Manual

21 August 2015

This document is provided pursuant to the disclaimer provided on the last page.

**Revisions**

| **Version** | **Date** | **Author(s)** | **Changes** |
| --- | --- | --- | --- |
| 0.1 | 15/10/2013 | Chris Wright; Peter Maurer | Initial draft |
| 0.2 | 16/10/2013 | Raymond Zylstra | Initial review |
| 0.3 | 17/10/2013 | Chris Wright; Peter Maurer | Additional sections incorporated |
| 0.4 | 29/10/2013 | Chris Wright; Peter Maurer | Final additional section incorporated |
| 0.5 | 18/07/2014 | Peter Maurer | Review and formatting |
| 0.6 | 21/07/2014 | Raymond Zylstra | Review |
| 0.9 | 22/07/2014 | Chris Wright | Review |
| 1.0 | 23/07/2014 | Raymond Zylstra | Finalise for release |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| **File Path** | \\Ausregistrygroup.Local\Shares\Company\Proposal Services\Projects\Central Projects File\DDNS - Managed DNS Manual\DDNS - Managed DNS Manual - 1.0.Docx |
| --- | --- |
| **Last Save Date** | 2015/08/10 - 11:36:00 |

Contact

|  |  |
| --- | --- |
| Name | Chris Wright |
| Title | Chief Technology Officer |
| Address | L8, 10 Queens Rd, Melbourne, Vic 3004, Australia |
| Number | +61 3 9866 3710 |
| Email | chris.wright@ariservices.com |

Classification

Public

About DiscoveryDNS

Based on client demand and leveraging over 11 years of experience ARI Registry Services launched DiscoveryDNS. DiscoveryDNS provides a global DNS service to ARI Registry Services’ clients around the world.

About ARI Registry Services

ARI Registry Services, part of the Bombora Technologies group of companies, is driving innovation and the expansion of the Internet through the delivery of world-class domain name Registry Services. With over 11 years of experience, ARI Registry Services is a leading provider of Domain Name Infrastructure Services and DNS Services for generic Top-Level Domain applicants and country code Registry Operators.

We help governments, major brands and entrepreneurs across the globe realise the full potential of the Internet by providing expertise, security and reliability in operating a core Internet infrastructure.

Contents

[1 Zone Management Portal 1](#_Toc426969499)

[2 On-boarding 2](#_Toc426969500)

[2.1 Link generation 2](#_Toc426969501)

[3 Process 3](#_Toc426969502)

[3.1 Resource records edition 3](#_Toc426969503)

# Zone Management Portal

The Zone Management Portal is an embeddable web interface to edit the DNS records of the zones hosted on the DiscoveryDNS Reseller system. This interface is designed to be integrated into a Registrar’s Portal, and made available to the Registrar’s customers, in these possible forms:

* An *<iframe>* nested browsing context, embedded in the original Registrar Portal’s page,
* A pop-up window,
* A clickable navigation link.

This interface supposes that the Zone to edit has already been created by the Registrar in the Reseller system, through the REST API interface or Web interface, in the desired plan and group, and with the desired features activated (DNSSEC, branded Name Servers, etc.).

This interface is only a way to add, edit and remove the Zone’s user resources records, similarly to what could be done by the Registrar on the Reseller Web interface.

The Zone Management Portal does not include the management of end-users authentication and authorisation. It supposes that the Registrar makes this interface available only to the users that have the authority to edit the Zone’s records.

The security is based on the validation of the link that will open the interface, based on the validation of the hash generated from a secret key, shared between the Registrar’s Portal and the Reseller system.

# On-boarding

Prior to being able to use the interface, several on-boarding steps are necessary:

* The Registrar Account has to be enabled for Zone Management Portal access, by the Reseller’s Support team.
* The Support team will then generate the shared secret key.
* A specific User will also be created under the Registrar Account, with the permission to access only the Zone Management Portal interface.
* The Support team will provide the Registrar with the shared secret key, the ID of the User created above and the base URL to generate the link, by an offline process.
* The Registrar will import these pieces of information into his Portal configuration, to be able to generate the link.

## Link generation

The link generation is a simple server-side operation, based on the generation of an HMAC-256 hash from the shared secret key.

The link should include:

* The base URL of the Zone Management Portal,
* The User ID that was provided by the Reseller Support,
* The ID or the name of the Zone to edit,
* The current timestamp,
* An HMAC-256 hash of these pieces of information, generated from the shared secret key provided by the Reseller Support.

More information and code examples can be made available upon request.

N.B.: An “ID” is a unique identifier of the resource in the DiscoveryDNS Reseller system. It is a unique reference to the resource that is necessary for some operations (e.g. for the REST API), and is displayed in the resource’s View web page.

# Process

The Zone Management Portal enables an end-user to edit the Zone user-provided DNS resource records. The process is as follows:

* The Registrar creates the Zone in the Reseller system, through the REST API interface or Web interface, in the desired plan and group, and with the desired features activated (DNSSEC, branded Name Servers, etc.).
* The end-user logs in the Registrar’s Portal and navigates to the Zone edition page.
* The Registrar’s Portal generates the link on the server-side. This link has to be used in a short period of time, or it will become invalid.
* The Registrar’s Portal displays the link on the page, in the desired form (iframe, pop-up window, or clickable link).
* The end-user clicks on the link.
* The Zone Management Portal receives the request and validates all the pieces of information included in the link:
  + If the link is valid, it creates a short-lived session for the end-user.
  + If the link is invalid, it returns an “Authentication Failed” error message. The Registrar’s Portal receives a notification of this.
* The end-user adds and removes the Zone’s resource records, and submits his changes.
* Once he’s done, he closes the Zone Management Portal interface.
* The Registrar’s Portal receives a notification of this. It can then decide to either refresh the page or redirect the end-user to a different page.
* This link can then never be used anymore. If the end-user requires editing the Zone’s records once again, the Registrar’s Portal has to generate and display a new link for him to do so.

## Resource records edition

The interface to edit the Zone’s resource records is similar to the Reseller Web interface’s one.

The user can add or remove resource records of all the different types that are supported by the system (see below) and are enabled in the Plan the Zone is in. The system-generated records (SOA, NS at the zone origin) will be displayed, but the user won’t be able to edit them.

All the different validation rules (records validity, zone state, etc.) apply.

Once the update is submitted, the Zone will be re-published to DNS in the matter of seconds.

Any subsequent updates can also be submitted, as long as the Zone’s state permits.

Note that only managed zones can be edited in such a way, as AXFR zones are handled through zone transfer only.

Supported Resource Records

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Definition | Value | Function |
| **A**  Address record | [RFC 1035](http://tools.ietf.org/html/rfc1035) | 1 | Returns a 128-bit IPv6 address, commonly used to map hostnames to an IP address of the host. |
| **AAAA**  IPv6 address record | [RFC 3596](http://tools.ietf.org/html/rfc3596) | 28 | Returns a 32-bit IPv4 address, commonly used to map hostnames to an IP address of the host, but also used for DNSBLs, storing subnet masks in RFC 1101. |
| **NS\*\***  Name server record | [RFC 1035](http://tools.ietf.org/html/rfc1035) | 2 | Delegates a DNS zone to use the given authoritative name servers. |
| **MX**  Mail exchange record | [RFC 1035](http://tools.ietf.org/html/rfc1035) | 15 | Maps a domain name to a list of message transfer agents for that domain. |
| **SOA\***  Start of authority record | [RFC 1035](http://tools.ietf.org/html/rfc1035)  [RFC 2308](http://tools.ietf.org/html/rfc2308) | 6 | Specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone. |
| **CNAME**  Canonical name record | [RFC 1035](http://tools.ietf.org/html/rfc1035) | 5 | Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name. |
| **SRV**  Service locator | [RFC 2782](http://tools.ietf.org/html/rfc2782) | 33 | Generalised service location record, used for newer protocols instead of creating protocol-specific records such as MX. |
| **TXT**  Text record | [RFC 1035](http://tools.ietf.org/html/rfc1035) | 16 | Carries machine-readable data, such as specified by RFC 1464, opportunistic encryption, Sender Policy Framework, DKIM, DMARC, DNS-SD, etc. |
| **NAPTR**  Naming authority pointer | [RFC 3403](http://tools.ietf.org/html/rfc3403) | 35 | Allows regular expression based rewriting of domain names which can then be used as URIs, further domain names to lookups, etc. |
| **SPF**  Sender policy framework | [RFC 4408](http://tools.ietf.org/html/rfc4408) | 99 | Specified as part of the SPF protocol as an alternative to storing SPF data in TXT records, using the same format – considered for obsolescence as of August 2013. |
| **DS**  Delegation signer | [RFC 4034](http://tools.ietf.org/html/rfc4034) | 43 | The record used to identify the DNSSEC signing key of a delegated zone. |
| **CERT**  Certificate record | [RFC 4398](http://tools.ietf.org/html/rfc4398) | 37 | Stores PKIX, SPKI, PGP, etc. |
| **PTR**  Pointer record | [RFC 1035](http://tools.ietf.org/html/rfc1035) | 12 | Pointer to a canonical name. Unlike a CNAME, DNS processing does not proceed, just the name is returned. The most common use is for implementing reverse DNS lookups, but other uses include such things as DNS-SD. |
| **SSHFP**  SSH Public key fingerprint | [RFC 4255](http://tools.ietf.org/html/rfc4255) | 52 | Resource record for publishing SSH public host key fingerprints in the DNS System, in order to aid in verifying the authenticity of the host. RFC 6594 defines ECC SSH keys and SHA-256 hashes. |
| **TLSA**  TLSA certificate association | [RFC 6698](http://tools.ietf.org/html/rfc6698) | 37 | A record for DNS-based Authentication of Named Entities (DANE). RFC 6698 defines "The TLSA DNS resource record is used to associate a TLS server certificate or public key with the domain name where the record is found, thus forming a 'TLSA certificate association'". |
| **LOC**  Location record | [RFC 1876](http://tools.ietf.org/html/rfc1876) | 29 | Specifies a geographical location associated with a domain name. |
| **DNSKEY\***  DNS Key Record | [RFC 4034](http://tools.ietf.org/html/rfc4034) |  | Holds the public key used to sign records in the zone. |
| **RRSIG\***  Resource Record Signature | [RFC 4034](http://tools.ietf.org/html/rfc4034) |  | Holds the generated cryptographic signature which can be used in conjunction with the corresponding public key DNSKEY record to verify that the response received from the DNS by a client is as intended by the zone administrator. |
| **NSEC\***  Next Secure | [RFC 4034](http://tools.ietf.org/html/rfc4034) |  | Points to the next secured entry in a signed zone file, used for authenticated denial of existence in DNSSEC queries for domain names that are not present. |

\* These records cannot be provided by the client, they will be generated by the server as required and will be returned in responses only.

\*\* These records at a zones APEX will be managed by the server as above, but can be used at other levels in the zone for the purpose of delegation.

**Definitions**

We, us and our means any or all of the Bombora Technologies Pty Ltd group of companies, their related entities and their respective officers, employees, contractors or sub-contractors.

**Disclaimer**

This document has been produced by us and is only for the information of the particular person to whom it is provided (the Recipient). This document is subject to copyright and may contain privileged and/or confidential information. As such, this document (or any part of it) may not be reproduced, distributed or published without our prior written consent.

This document has been prepared and presented in good faith based on our own information and sources which are believed to be reliable. We assume no responsibility for the accuracy, reliability or completeness of the information contained in this document (except to the extent that liability under statute cannot be excluded).

To the extent that we may be liable, liability is limited at our option to replacing, repairing or supplying equivalent goods or paying the cost of replacing, repairing or acquiring equivalent, or, in the case of services, re-supplying or paying the cost of having such re-supplied.

**Confidentiality Notice**

This document contains commercially sensitive information and information that is confidential to us. This document is intended solely for the named recipient, and its authorised employees, and legal, financial and accounting representatives (collectively, Authorised Recipients).

The recipients of this document must keep confidential all of the information disclosed in this document, and may only use the information for the purpose specified by us for its use. Under no circumstance may this document (or any part of this document) be disclosed, copied or reproduced to any person, other than the Authorised Recipients, without our prior written consent.

**Trademarks Notice**

Any of our names, trademarks, service marks, logos, and icons appearing in this document may not be used in any manner by recipients of this document without our prior written consent. All rights conferred under law are reserved.

All other trademarks contained within this document remain the property of their respective owners, and are used only to directly describe the products being provided by them or on their behalf. Their use in no way indicates any relationship between us and the owners of those other trademarks.