Responsys

Domain Branding

What is Domain Branding?

By default, our clients are assigned a Responsys-hosted sub-domain, e.g., brandx.rsys1.com. This sub-domain is used for the From Address, Responsys-hosted Reply-To Address, and the Response Handler (Click-Through URLs). However, some of our clients do not like the "rsys1.com" and would like to have a domain/sub-domain more akin to their own brand; this is Domain Branding.

For domain branding, a customer's IT department will have to create a new sub-domain and delegate it over to Responsys. Delegating means you are assigning responsibility for assigning responsibility for the given sub-domain to another organization.

Behind the scenes, your zone's data, instead of containing information in the sub-domain you have delegated, includes pointers to the sub-domain's authoritative nameservers. When the delegation is in place and one of your nameservers is queried for data in the sub-domain, your nameserver should reply with a list of Responsys nameservers with whom to talk.

Why should Domain Branding be used?

- **Responsys runs a multi-tenant environment.**
Our environment services hundreds of medium to large business clients. These clients demand that we ensure protection of their brand. They also demand that we ensure that we will have the necessary infrastructure capacity when they need it and that we can react in minutes, not hours, to incidents that impact that need.
- **Responsys manages the zone records.**
Responsys' experience in setting up and tuning DNS entries like SPF (Sender Policy Framework) records, Domain Keys, and other records will have a tremendous effect on deliverability. In addition, when Responsys controls the domain, the client does not need to worry about any further configuration settings.
- **Authority.**
Many third party anti-spam technologies (especially Bayesian classifiers such as SpamAssassin) use NS records to determine whether a From Address is from an authorized sender. Not having delegation via NS records can trip one of these filters and impact deliverability.
- **Flexibility.**
Because of the dynamics of the Internet, technologies change frequently. These new technologies may require additional records to be created, or other periodic changes (SPF records, 'A' records, etc.). Failure to make these changes immediately may seriously impact deliverability. Having Responsys control the zone allows for these changes to be made in a timely manner.
- **The client leverages the Responsys infrastructure.**
Responsys clients often experience extremely high open and response rates. This

corresponds linearly with the number of DNS queries. Responsys' DNS servers are geared to handle peak load.

- **Responsys provides monitoring and availability.**

Responsys monitors what is in our zones by dynamically calculating everything in the zone files themselves. Further, we often make changes to a Response Handler IP address as availability issues come up.

- **Ability to respond to problems.**

There have been occasions where a client's domain had been used for illicit activities (phishing, spamming, etc.). When these types of activities are discovered, Responsys needs to be able to act quickly. Having the domain delegated allows us to make any needed updates immediately.

- **Ease of Administration.**

Whenever Responsys make changes to our network we may need to update SPF records, 'A' records and possibly MX records. If we have to coordinate these activities with our client's IT department, then these changes would not be made as timely as needed.

Domain Branding Requirements

Delegation may be performed in multiple ways:

- Delegation using NS records in the client's DNS zone is used when the client will use a sub-domain of their primary domain. For example, if the company BrandX with the domain www.brandx.com wants to use domain branding, they would use something like email.brandx.com and delegate the sub-domain to Responsys via NS records.

- Delegation using a new domain is used when the client wants to use a completely separate domain for their branding. For example BrandX might purchase brandxmail.com and when they purchase it, specify Responsys' nameservers during the initial configuration.

- Delegation using CNAME records is used when the client **only** wishes to use domain branding for the Response Handler (click-through URLs). For example, using the BrandX domain, the client might make email a CNAME to a Responsys name (provided by Responsys). This will not be sufficient for From and Responsys-hosted Reply-To addresses, nor with SSL support for the Response Handler.

The Responsys name servers are:

ns1.responsys.net
ns2.responsys.net

Disclaimer - This document is provided as is without any express or implied warranties. While some effort has been taken to ensure the accuracy of the information contained in this article, the maintainer assumes no responsibility for errors or omissions, or for damages resulting from use of the information contained herein.

Frequently Asked Questions (FAQ)

Q: Why can't I use CNAME style branding with my from address?

A: The Internet Engineering Task Force (IETF) does not define a standard for what happens when a CNAME is used in lieu of an MX record. Some widely used MTAs (mail servers) do not respect these records, and so mail would be lost.

Q: Can't I just use a CNAME and add my own MX record?

A: This is not possible. The standards for DNS specifically disallows using a CNAME and other DNS entry, thus you can't have a zone with both a CNAME and an MX entry for the same record.

Q: My company does not delegate subdomains by policy, what can I do?

A: Responsys would be happy to discuss the implications of this with your IT staff as we have done this before and are generally able to convince organizations of the value.

Q: Okay, but that won't help, what else can I do?

A: You can use CNAME style branding for the Response Handler (click-through URLs) and not use branded From and Reply-To Addresses. Or, you can purchase a new domain and have Responsys responsible for managing it.

Definitions

Domain Keys

An e-mail authentication system (developed at Yahoo!) designed to verify the DNS domain of an E-mail sender and the message integrity. The DomainKeys specification has adopted aspects of **Identified Internet Mail** to create an enhanced protocol called DomainKeys Identified Mail **(DKIM).** This merged specification is the basis for an IETF Working Group which plans to guide the specification toward becoming an IETF standard.

Disclaimer - This document is provided as is without any express or implied warranties. While some effort has been taken to ensure the accuracy of the information contained in this article, the maintainer assumes no responsibility for errors or omissions, or for damages resulting from use of the information contained herein.

NS Record

An **NS record** or **name server record** maps a domain name to a list of DNS servers authoritative for that domain. Delegations depend on NS records.

SPF

The Sender Policy Framework (SPF) is an open standard specifying a technical method to prevent sender address forgery. More precisely, the current version of SPF — called *SPFv1 or SPF Classic* — protects the *envelope sender address*, which is used for the delivery of messages. See the box on the right for a quick explanation of the different types of sender addresses in e-mails.

CNAME

Short for *canonical name*, also referred to as a *CNAME record*, a record in a DNS database that indicates the true, or canonical, host name of a computer that its aliases are associated with. A computer hosting a Web site must have an IP address in order to be connected to the World Wide Web. The DNS resolves the computer's domain name to its IP address, but sometimes more than one domain name resolves to the same IP address, and this is where the CNAME is useful. A machine can have an unlimited number of CNAME aliases, but a separate CNAME record must be in the database for each alias.

DNS

*Short for **D**omain **N**ame **S**ystem (or **S**ervice or **S**erver)*, an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name w*ww.example.com* might translate to *198.105.232.4*.

Disclaimer - This document is provided as is without any express or implied warranties. While some effort has been taken to ensure the accuracy of the information contained in this article, the maintainer assumes no responsibility for errors or omissions, or for damages resulting from use of the information contained herein.