

Agency SMTP Relay Readiness Guidance

Introduction and Purpose

The purpose of the *Agency SMTP Relay Readiness Guidance* document is to provide general steps that agencies and CTS will perform at the time agencies wish to prepare to enter the Shared Services Email Centralized Gateway SMTP Relay (CGSR) offering. It is anticipated that agency technical staff will work closely with CTS, and that the tasks identified in this *Guidance* document may be replaced or supplemented based on the individual characteristics of each agency's environment.

General Prerequisites

Agencies wishing to use the CTS SMTP Relay service will need to:

1. Complete an inventory of all applications/devices which require SMTP Relay Service using a CTS-provided template. Agencies will need to identify all SMTP relay activity and the volume of activity generated by the application or device.
2. Identify individual IP addresses. CTS will permit on individual IP addresses only; CTS will not permit to a range, or to a subnet.
3. CTS will only permit to production and hot standby IP's. Customer test scenarios will be permitted separately and only with coordination and authorization with CTS.
4. Undertake mailing list maintenance to provide reasonable certainty that mailing lists do not contain invalid addresses.
5. Submit a ticket requesting SMTP Relay service to the CTS Service Desk. Upon receipt of the Inventory, CTS technicians will evaluate the request and notify the agency of any additional work needed.
6. Once CTS has permitted the IP addresses of your application servers, you will need to point the SMTP traffic from those servers to a DNS provided address.

Customer Responsibilities

To protect the service, the sending agency, and all other state agencies using the relay service, there are certain responsibilities that lie with the customer:

1. Provide CTS with early notification of unusual (e.g. Annual bulk mailing; unusually large bulk mailing).
2. Reasonable certainty that mailing lists are "clean" (do not contain invalid addresses).
3. Mailing lists are managed and maintained regularly.
4. Customer must be proactive in designing their bulk distributions to avoid overloading the system and/or causing our gateway to be block listed on the internet.
5. Customer will create a SPF record that will include SMTP relay addresses.

EXAMPLE: Bulk mail job sending to 15,000 internet recipients

- Split the mailing into 15 separate jobs, each with 1000 recipients.
- Wait 10 minutes between each job.

- Each job should consist of multiple connections

Keep in mind that the success of your bulk mailing is mostly dependent on how you are impacting the recipient internet mail hosts. CTS does not and cannot control the policies of those hosts. If an internet mail provider, such as Yahoo.com is receiving mail from a single sending address (our internet mail gateway) that exceeds any of **their** acceptable thresholds, they will take action to block further mailing from our server. Your job will be, at a minimum, delayed. Depending on the severity of the incident, it may be as much as a “permanent” block which may take days or weeks to be released. Remember, this not only affects your job, but other customers as well.

The threshold concerns for any one provider that can adversely affect your mailing are:

- Too many invalid addresses
- Too many messages per connection
- Too many recipients per message
- Connection time exceeded

The thresholds mentioned are purposely and necessarily vague because no internet mail service provider will publish those thresholds. Why? Well, if you were actually attempting to spam an organization, wouldn't you like to know exactly what those limits were?

Therefore, familiarity with your recipient list is important. If, in this example 15,000 recipient list, there are 800 recipients at hotmail.com, take care to divide those 800 Hotmail recipients across multiple messages, across multiple connections, across all of the 15 jobs. This will result in a time-spaced distribution to the Hotmail organization that will more likely be “palatable” to their thresholds.

Service Provider Termination of Service

In order for the service provider to maintain the most reliable service for all customer agencies the service provider may need to take the following actions which may include;

1. Temporarily “block listing” of customer servers and/or application from connection.
2. Permanently “block listing” customer server and/or application from connection.
3. Provide Agencies with notification of substantial delays in the relay system due to activities such as “block listing” or application bulk mailing.