GNet Solutions - Support #721

SMTP Error Codes

01/11/2016 07:08 PM - Daniel Curtis

Status:	Closed	**Start date:**	01/11/2016
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Mail Server	**Estimated time:**	1.00 hour
Target version:	*nix	**Spent time:**	1.00 hour

Description

The values of interest for this article are:

1. **4xx**: The server has encountered a temporary failure. If the command is repeated without any change, it may be successful, depending on the reason for the initial failure. Mail servers can use such temporary failures to hold connections from untrusted sources, while additional security checks are performed
2. **5xx**: The server has encountered a permanent error and the email delivery has failed. The remaining two numbers in the code provide more information regarding the reason for the temporary or permanent failure.

400 Error Codes

Error 400 codes are typically temporary failures, so a correctly configured mail server should retry the connection based on their Delivery.

Temporary Email Connection Failures Failures (ordered by most common to least common):

Code	Reason Given to Sending MTA	Description	Recommended Resolution
421	Sender address blocked	The sender's IP address has been blocked by a Block Policy	The entry will need to be removed from the Block Senders Policy
421	Unable to process connection at this time	The Mail Server is currently under maximum load. The sending mail server should retry the connection	The email will be processed on retry, when the mail service has processed some of the current load
451	Internal resource temporarily unavailable	The sending mail server has been subjected to Greylisting . Greylisting requires that the server retries the connection, between 1 minute and 12 hours. OR The senders IP address has a poor reputation. The connection is temporarily failed while updated reputation information is obtained.	These reputation checks can be bypassed with an Auto Allow entry, a Permitted Senders Policy ; or if it is legitimate traffic being blocked by greylisting, by creating a Greylisting bypass policy.
451	Message ended early	The message was incorrectly terminated. This can be caused by files that have previously been infected with a virus, and have not been cleaned correctly by an anti-virus product, which has then left traces in the email. This can also be caused by Firewall issues on the sender's side, or incorrectly configured content rules on a security device.	The Administrator should investigate their Intrusion Detection software or other SMTP protocol analyzers. If running a Cisco Firewall, ensure that the Mailguard or SMTP Fixup module is disabled.
451	Open relay not allowed	This error indicates that both	mail server customers should

		the sender AND the recipient email domains specified in the transmission are external to the mail service and therefore are not allowed to relay through the mail service and / or the connecting IP address was not recognized as authorized.	contact network administrator for the Authorized Outbound address to be added or to take other remedial action as appropriate.
451	Account outbounds disabled	The customer account outbound emails have been disabled in the Mail Server Administration Console.	Contact the network administrator if the account outbound traffic should be allowed.
451	Account inbounds disabled	The customer account inbound emails have been disabled in the Mail Server Administration Console.	Contact the network administrator if the account outbound traffic should be allowed.
451	Account service temporarily unavailable	There are too many concurrent inbound connections for this account (the default is 20).	The IP address will automatically be removed from the mail server temporary block list after 5 minutes. Continued invalid connections will result in the IP getting added to the mail server temporary block list again. Please ensure that you do not try to route outbound or journal messages to the mail server from an IP address that has not been authorized to do so.
451	Recipient Temporarily Unavailable	The Sender's IP address has been placed on the mail server temporary block list due to too many invalid connections.	The senders mail server will need to retry the connection. The mail server performing is the recipient address validation is not responding.
451	Unable to process email at this time	Temporary mail server internal error: an AV scanner or store server is temporarily unavailable due to updates being deployed to it.	The email will be processed on retry once the updates have been deployed.
451	Unable to process email at this time	Catch all error if reason is unknown	Please contact the network administrator to investigate.
452	Too many recipients	By default, the mail server only accepts 100 RCPT TO entries per message body (DATA). If the sending server issues more RCPT TO entries, then the mail server platform will respond with "452 Too many recipients". This transient error code should trigger the sending mail server to provide the DATA for the first 100 recipients before it provides the next batch of RCPT TO entries.	None. Most mail servers correctly respect the transient error and will treat it as a "truncation request". If your mail server, firewall or on-site solution does not respect the transient error, you may need to ensure that no more than 100 recipients are submitted. Note: Solutions like SMTP Fix Up / MailGuard and ESMTP inspection on Cisco Pix and ASA Firewalls are known not to respect the transient error.

500 Error Codes

Error 500 codes are typically permanent failures. These connections are rejected in protocol, and the connection is logged in the Rejection Viewer. As the email is rejected in protocol, it is not retrievable from the Mail Server Administration Console, and will need to be resent once the issue has been addressed.

Permanent Email Connection Failures (ordered by most common to least common):

Code	Reason Given to Sending MTA	Description	Recommended Resolution
501	Invalid address	The email address is not a valid SMTP address.	The sender should resend the email to a valid internal email address.
535	Incorrect authentication data	Messages submitted to SMTP port 587 require authentication. This error indicates that the authentication details provided were incorrect.	Ensure your authentication details match an internal email address on the mail server platform with a corresponding mail account password. Alternatively consider sending the message on SMTP port 25 instead.
550	Administrative prohibition - envelope blocked	The sender's email address or domain matches an entry in a Block Sender Policy	The Administrator set Block Sender Policy must be removed or modified to exclude the sender address.
550	Administrative Lockout - Inbound not allowed	This is a spoofed email and has been flagged by the Inbound Lockout Policy	The Inbound Lockout Policy must be removed or modified to exclude (creating a bypass policy) the sender address or IP address.
550	Envelope blocked - User Entry	A personal block policy is in place for this email address.	Remove the entry from the Managed Sender list.
550	Envelope blocked - User Domain Entry	A personal block policy is in place for this domain.	Remove the entry from the Managed Sender list.
550	Rejected by header based Blocked Senders – Block policy for Header From	A Block Sender Policy has been applied to reject emails based on the Header From address	Remove or adjust the Block Sender Policy
550	Envelope Rejected – Block policy for Envelope from address	A Block Sender Policy has been applied to reject emails based on the Envelope From address	Remove or adjust the Block Sender Policy.
550	Rejected by header based manually Blocked Senders – block for manual block	A personal block policy is in place for this email address.	Remove the entry from the Managed Sender list.
550	<details of RBL>	The sender's IP address is listed in an RBL. The text displayed is specific to the RBL which lists the senders IP address.	The RBL can be bypassed with an Auto Allow entry or Permitted Senders Policy. It is also recommended that the sender requests removal of the associated IP address from the RBL.
550	Local CT IP Reputation - (reject)	This error is based on ongoing reputation checks, which have resulted in the email being rejected due to poor IP reputation (this could be subsequent to temporary failures).	This rejection can be bypassed with an Auto Allow entry, or by creating a Permitted Senders Policy.
550	Invalid Recipient	Known recipient, LDAP or SMTP call forwarding recipient validation checks have not returned a valid internal user.	The sender must resend the email to a valid internal recipient address.
550	Exceeding outbound thread limit	There are too many concurrent outbound connections for the	Send the outbound emails in smaller chunks of recipients.

		account.	
550	Submitter failed to authenticate	Messages submitted to SMTP port 587 require authentication. This error indicates that no authentication details were provided.	Configure your authentication details. These should match an internal email address on the mail server platform with a corresponding mail acount password. Alternatively consider sending the message on SMTP port 25 instead.
550	Message bounced due to Content Examination Policy	A Content Examination Definitions and associated Policy are being used to reject emails based on the specified text matches within the email.	Create a Content Examination Bypass Policy or adjust the existing Content Examination Definition/Policy as needed.
553	This route requires encryption (TLS)	This email has been sent using SMTP, however TLS is required by policy.	Review or disable the Secure Receipt/Delivery Policy which is enforcing TLS. Alternatively ensure that the certificates on the mail server have not expired. If using a proxy server, ensure that it is not intercepting the traffic and modifying encryption parameters.
554	Email rejected due to security policies (E.g. MCSpamSignature.x	A signature was detected, which could either be a virus signature, or a spam score over the maximum threshold. The spam score is not available in the Administration Console. Please contact the network administrator for further assistance.	Anti-virus checks cannot be bypassed, and the sender should be notified. Anti-spam checks can be bypassed using a Permitted Senders Policies or an Auto Allow entry.
554	Mail loop detected	There are too many "received headers" in this email, as it has been forwarded across multiple hops. Once 25 hops has been reached, the email is rejected.	Investigate the email addresses involved in the communication pairs to see what forwarders have been configured on the involved mail servers. Maximum email size exceeded The email size either exceeds an Email Size Limits Policy, or is larger than mail service limit: * Default 100 MB for "the Legacy MTA" * Default 200 MB for "the Latest MTA" Resend the email ensuring that it is smaller than the limitation set. The transmission and content encoding can add significantly to the total size of the email. This means that an email with a 70 MB attachment, can have an overall size larger than 100 MB.

Resources

- https://community.mimecast.com/docs/DOC-1369

History

#1 - 01/11/2016 07:14 PM - Daniel Curtis

- Description updated

#2 - 01/11/2016 07:26 PM - Daniel Curtis

- Description updated

- Status changed from New to In Progress

- % Done changed from 0 to 50

#3 - 01/11/2016 07:31 PM - Daniel Curtis

- Description updated

#4 - 01/11/2016 07:32 PM - Daniel Curtis

- Description updated

#5 - 01/11/2016 07:37 PM - Daniel Curtis

- Description updated

#6 - 01/11/2016 07:39 PM - Daniel Curtis

- % Done changed from 50 to 100

- Status changed from In Progress to Resolved

#7 - 02/20/2016 07:18 PM - Daniel Curtis

- Status changed from Resolved to Closed