

# RISO FW/FT/GD/GL

## Scan to Email

### Error Codes & Troubleshooting



## Error Codes

RISO Error Code	SMTP Error Code	What's Causing This Error	Solution
W093-230-1	550	<p>SMTP error 550 usually appears when there is an issue with the authentication of the SMTP client and the SMTP server; in most instances, it means that the authentication is missing. However, there are many other reasons to cause this error; these reasons come with the error code for additional information on the exact cause.</p> <p>Email error "550 Authentication is required for relay" indicates that the client requires authentication.</p> <p>Server error "550 this domain is not hosted here" indicates that the recipient address is not found or is inaccessible.</p> <p>Server error 550 or 550 Blocked Error indicates that the recipient is blocking your email on the recipient's email server.</p>	<p>To fix these common issues, the user must pay attention to the description that follows the error code. However, the following common causes would require different resolutions.</p> <p>Email error "550 Authentication is required for relay" - The user must check the configuration for proper authentication on the email client.</p> <p>Server error "550 this domain is not hosted here" - The user must ensure that all the recipient email addresses are valid.</p> <p>Server error 550 or 550 Blocked Error - The user may need to check with the recipient to ensure that the sender's email domain or email address is not within a blocklist.</p>
W093-230-2	551	<p>SMTP error 551 occurs when an email bounces during the delivery process. Two types of bounces may take place:</p> <p><b>Soft Bounce</b> - Soft bounce takes place when the recipient's mailbox is full or if their email server is temporarily unavailable.</p> <p><b>Hard Bounce</b> - Hard bounce occurs when the email address is invalid or if the mail server attempts to deliver the email to another server that does not handle the recipient's email address.</p>	<p>To resolve this error, ensure no underlying issues affect the email server or the connectivity.</p> <p>The following common troubleshooting steps can help narrow down and resolve the issue at hand.</p> <ul style="list-style-type: none"> <li>• Ensure that all recipient's email addresses are valid.</li> <li>• Ensure that the recipient has enough space in their mailbox to receive the email.</li> <li>• Ensure that the recipient's email server is available and is accepting email</li> </ul>

W093-230-3	553	<p>SMTP error code 553 typically occurs when the recipient's mail server rejects the email message. However, the specific reason for rejection may vary depending on the environment.</p> <p>Some of the most common reasons for rejection are:</p> <p>The recipients spam filter detects the email as malicious or spam. Blocklisted email address Blocklisted IP Address</p>	<p>To resolve this issue, ensure that the IP address and domains are within a blocklist. Additionally, ensure that the email does not have signs associated with spam or malware that may cause a false-positive trigger from the security controls, such as a spam filter.</p>
------------	-----	--	---

W094-0231-1	432	This is a Microsoft Exchange Server-specific SMTP status response that occurs when the recipient's Exchange Server mail queue has been stopped. The mail queue can often be stopped due to too many open connections to the server or while the network administrator is troubleshooting an issue	Fixing this issue might be difficult from your end since it is hard to determine the exact reason. For that, you need to contact the network administrator. Meanwhile, you can check your computer's local internet connection, evaluate any probable server network difficulties, or check for any local network issues
W094-0231-2	534	SMTP error 534 occurs when the client authentication is weak, and the server requires stronger authentication to accept the connection. It occurs in cases where email providers such as Google disables weak authentication to ensure secure connectivity	The resolution may depend on the authentication requirements set by the email server. Therefore, it is vital to understand the authentication requirements and configure the client with the necessary controls and settings to facilitate the expected client authentication
W094-0231-3	535	SMTP error 535 indicates an issue with the client's authentication with the email server. It may be the result of many issues, some of the most common causes being: <ul style="list-style-type: none"> <li>• Invalid credentials</li> <li>• Disabled account</li> <li>• Invalid or incompatible connection encryption settings</li> <li>• Invalid or incompatible Authentication Methods</li> </ul>	Depending on the cause of this error, the user may need to take different approaches when attempting to fix this error.  The user must validate the credentials used to login into the email server. Check if the account is in working order and is not disabled. Validate the SMTP configuration to check if the connection encryption and authentication settings are compatible with the email server.
W095-0232		Mail server over limit	Failed to send mail due to over-allocation of storage area in the mail server An SMTP response code indicating a transmission error, 552 (Over-allocation of client storage area), was received after mail transmission.  *Mainly caused by oversized mail data

W096—233-1	421	<p>The SMTP server may display the SMTP error 421 in many instances since this error can have numerous variations. However, it is most likely a temporary issue within the mail server or the recipient's email account.</p> <p>The most common causes for this error are:</p> <ul style="list-style-type: none"> <li>• Too many connections from your host</li> <li>• The server is busy and cannot accept the connection.</li> <li>• Service is temporarily unavailable</li> </ul>	<p>Since these errors are mostly temporary, the user should wait for a considerable amount of time before attempting to send an email to the same server or connect to the same server.</p> <p>However, in instances when the error states that there are multiple connections from or to the host, it is advisable to adhere to any limits within the email server</p>
W096—233-2	450	<p>The SMTP 450 error occurs whenever there is an issue with the DNS routing on the recipient's SMTP server. For example, you may run into this error if:</p> <ul style="list-style-type: none"> <li>• The recipient server cannot find the email address on its server.</li> <li>• The recipient mail server rejected your request as your email content did not pass through its filter.</li> <li>• Your mail server's IP address gets denylisted</li> </ul>	<p>Here are some actions that you can take to solve the problem.</p> <p>Ensure that the email address you are trying to send an email to exists. Make sure that your email content does not simulate a spam email. For example, ensure that your email content does not try to sell a product or advertise about winning a prize. Many spam filters will reject emails with content on this spectrum.</p> <p>If your email contains attachments, make sure that they do not exceed the maximum size accepted by the recipient SMTP server. (Some recipients specify a maximum attachment size of around 5MB)</p> <p>Use MXToolBox to ensure that your mail server's IP address is not denylisted</p>
W096—233-3	451	<p>SMTP error 451 indicates when the user exceeds the limits set on the email server for sending emails. The email server will not allow the user to send more emails than the limits set on the email server; these limits are set as daily or hourly limits to restrict abusive behaviour</p>	<p>There is no immediate resolution for this error but wait until the restriction expires. Then, the user may contact the email server administrators to obtain more information regarding the limits. However, it is essential to stay within limits to avoid running into the same issue in the future</p>
W096—233-4	452	<p>You may run into this error when you try to send many emails at once or if you include too many recipients in a single email. It can cause the SMTP server to overload and run out of storage memory which, in return, throws this error.</p>	<p>To resolve the error, you can do either of the following.</p> <ul style="list-style-type: none"> <li>• Increase email limit.</li> <li>• Use third-party email providers.</li> <li>• Split recipients</li> </ul>

W096—233-5	454	This error occurs when emailing via the SMTP server without authenticating with it or when the authentication credentials are invalid	<p>To resolve the error, ensure to configure SMTP authentication. Verify that you have provided the correct username and password provided by the SMTP server. Furthermore, ensure you connect to the correct port using the proper authentication type. For example, if the SMTP requires port 465, use SSL authentication and if the server requires port 587, use TLS authentication.</p> <p>If nothing works, disable your firewall or anti-virus guard, and try sending the email</p>
W096—233-6	521	SMTP error 521 usually occurs within mail relays, meaning that these mail servers do not accept and deliver the emails themselves but only relay them to a remote mail server. It is essential to remember that from this point onward, the emails may fail, or the email server may relay the email to another	<p>Before fixing this error code, it is important to check the delivery of the emails sent, as the delivery may be successful via the email relay.</p> <p>Suppose the recipients confirm that the emails are not reaching them. In that case, the users need to determine why the recipient's mail server is not accepting emails by contacting the mail server administrators</p>
W096—233-7	530	SMTP error 530 typically occurs when there is an issue with the client's authentication with the sender's email server or in exceptional cases where the sender's IP address is within a public or private blocklist	<p>Resolving this issue involves ensuring that the user credentials used to authenticate with the email server are valid and that there are no syntax errors within the username and password fields.</p> <p>If the user credentials are valid, the next step is to verify if the client's IP address is within a blocklist. If the IP address is within a blocklist, users may follow the appeal process to exclude the specific IP address from the blocklist(s)</p>
W096—233-8	554	<p>SMTP error 554 indicates that the mail server did not accept the email. Several reasons typically cause this error:</p> <ul style="list-style-type: none"> <li>• Invalid Recipient</li> <li>• Blocklisted IP</li> <li>• Bad DNS</li> <li>• SPF Record</li> <li>• DKIM Record</li> <li>• DMARC Record</li> <li>• Sender Flagged As Spam</li> <li>• Email Violation Policy</li> </ul>	<p><b>Invalid Recipient Address</b> - Check if the email address(es) you are attempting to send the emails to is valid and if there are no spelling mistakes.</p> <p><b>Blocklisted IP Address</b> - The user must remove their IP Address or domain from public blocklists.</p> <p><b>Bad DNS Records</b> - Make sure that the "DMARC," "SPF," and "DKIM" records configurations are valid.</p> <p><b>SPF Record</b> - Check with the recipient to verify if the email server or domain contains an SPF record and if so, check if this configuration blocks your domain.</p> <p><b>DKIM Record</b> - Check if the sender's DKIM record is valid.</p> <p><b>DMARC Record</b> - Check if the sender's DMARC record is valid.</p> <p><b>Sender Flagged As Spam</b> - Check if the sender's domains are marked as spam by the recipient or the recipient's email provider/server.</p> <p><b>Email Violation Policy</b> - Check with the recipient's email violation policy and adhere to the policy to resolve this issue.</p>

W097-234-1	500	The SMTP 500 error can occur if the SMTP command used is not recognized or supported by the receiving SMTP server or if the SMTP command is too long.	<p>Firstly, check the length of the SMTP command string. Ensure that the command length does not exceed the maximum length supported by the SMTP implementation.</p> <p>Secondly, ensure that the receiving SMTP server supports the command you are trying to execute.</p> <p>Lastly, disabling the anti-virus guard may help solve an SMTP 500 Error</p>
W097-234-2	501	<p>The SMTP 501 error occurs when you try to send an email to an invalid email address or invalid domain name. Additionally, you may run into this error from time to time due to anti-virus guards dropping your SMTP connection or if the SMTP command exceeds 512 characters (when sending the email from the command line).</p> <p>Furthermore, specific SMTP servers throw the 501 error when the email address does not comply with the RFC 2821 Specifications.</p>	<p><b>For command-line users</b> If you're sending the email using an SMTP command exceeding 512 characters, you can use the SMTP extensions to increase this limit</p> <p><b>For non-command-line users</b> First, verify the validity of the sender's email address and the sender's domain. If the email is invalid, use the valid email address when you send the email to resolve the error.</p> <p>However, if the email you are trying to send is valid, check if your SMTP Server complies with the RFC 2821 specifications. If so, make sure the sender's email is in the following format:</p> <p>The local part (content before the "@" sign) is greater than 0 and less than 64 characters. The domain (content after the "@" sign) does not exceed 255 characters</p> <p>If your email address complies with these standards and the error persists, a quick fix would be to disable your firewall or anti-virus guard.</p>
W097-234-3	502	This error occurs when the SMTP command/function issued by the sending mail server is valid but not yet activated.	To resolve the error, trace back to the failed email and identify the email commands and functions used by the server. Afterward, review the settings currently enabled on your agent and allow the configurations required to send the email
W097-234-5	503	The SMTP "Error 503 Valid RCPT command must precede DATA" can occur when sending an email if the email client did not authenticate with the email server. Therefore, could be due to issues with the SMTP authentication settings on the SMTP client	<p>It is essential to ensure that the SMTP client's authentication settings do not have errors and validate the user credentials.</p> <p>Setting up SMTP authentication on the email client differs with each client; you may refer to the configuration guide for your preferred email client for a detailed step-by-step guide.</p>
W097-234-5	504	This error is similar to a 502 error. If an SMTP command parameter is not implemented in the MTA (Message Transfer	Review the failed request and analyse the SMTP command parameters to resolve the error. Afterward, open the SMTP MTA configuration and configure the MTA to accept the parameter, or try to send the email without using the command causing the error

		Agent) configuration, you may run into this error	
W097-234-6	538	SMTP error 538 occurs when the authentication mechanism requires encryption to complete a client's authentication process, and without the encryption, the authentication process fails. It is primarily due to the mail server or email providers requiring encryption to add a layer of security to the authentication process	To resolve this error, the client must contain the required encryption to authenticate with the email server successfully. These settings may include TLS versions and encryption algorithms.  The user must obtain these encryption requirements from the email server administrator/email service provider.

# Troubleshooting

## Testing Settings

RISO UK advises against relying on the RISO Console's communication test button due to its inconsistent results. To verify settings, perform a direct scan-to-email test from the RISO device. If the scan fails, an error code will appear—refer to pages 24-30 in the documentation for specific troubleshooting steps related to the error.

## Check Network setting on RISO Device

Each RISO device will need to have the correct [DNS, Gateway, Proxy Setting](#) etc. to gain access through to the internet. If the network details have changed recently, please amend these on the RISO device in Admin Menu.

## Firewall settings

Some local authorities require the IP Address of the RISO Device to be registered on the Firewall/Filter.

## Account Password

The account password may not have saved correctly on when using the RISO Console, please enter the account password directly on the RISO touchscreen.

## Confirm Account details are correct.

To verify that the email address and password are correct, please log in to the email account using a web browser.

## Password information

Up to 16 alphanumeric characters

Unavailable characters: " / [ ] : + | < > = ; , \* ? \ ' `

## Google Workspace App Password

When entering the app password via the RISO Console, please ensure that all spaces are removed. To do this, we recommend the following steps:

1. Copy the app password into a Notepad.
2. Remove any spaces from the password.
3. Copy the corrected password from the document and paste it into the RISO Console.

If you need any further information or assistance, please contact us at [softwaresupport@riso.co.uk](mailto:softwaresupport@riso.co.uk)