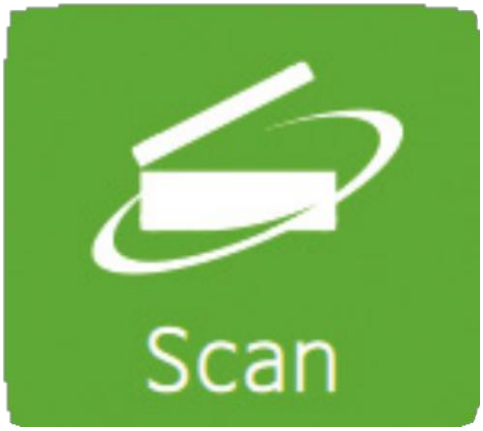
RISO FW/FT/GD/GL

Scan to Email

Setup Guide



RISO UK Ltd

Contents

Scan to Email Initial Setup

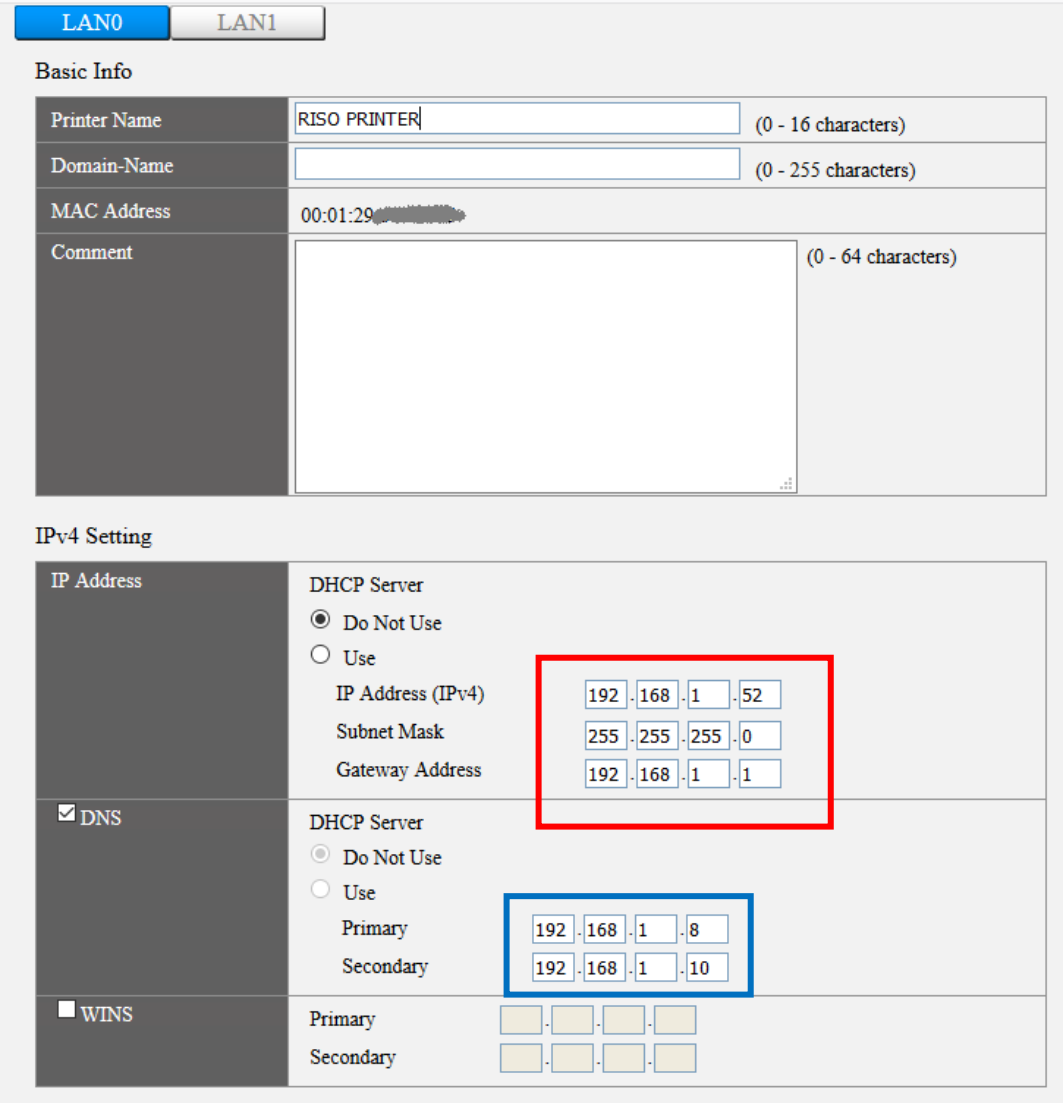
RISO ComColor devices support scan to email through a compatible SMTP server.

Requirements for Scan to email are:

- The RISO device configured with appropriate TCP/IP details such as:
  a. IP Address & Subnet Mask
  b. Gateway
  c. DNS Server(s)

- The RISO device should have network access to an appropriate SMTP Server.

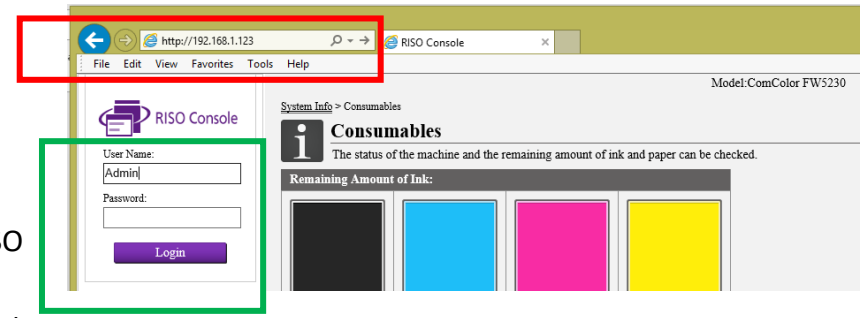
- Where necessary, an email address/account with authenticate credentials capable of sending emails through the SMTP server.



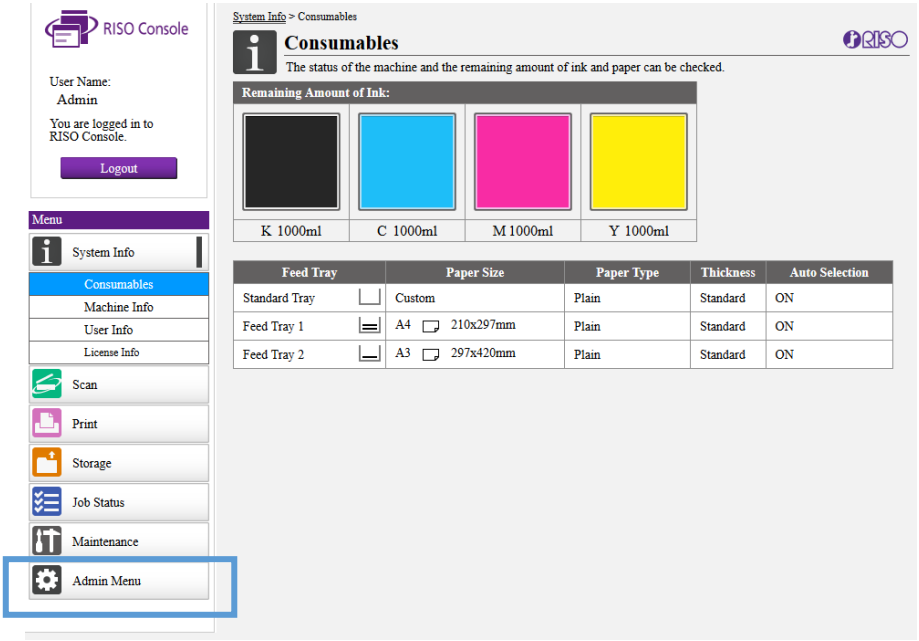
1. Using a web browser, connect to the RISO ComColor web console interface.

a) Open your chosen web browser (Firefox, Chrome, IE etc.) and enter **http://** followed by the **IP Address** of the RISO device in the address bar.

Example:

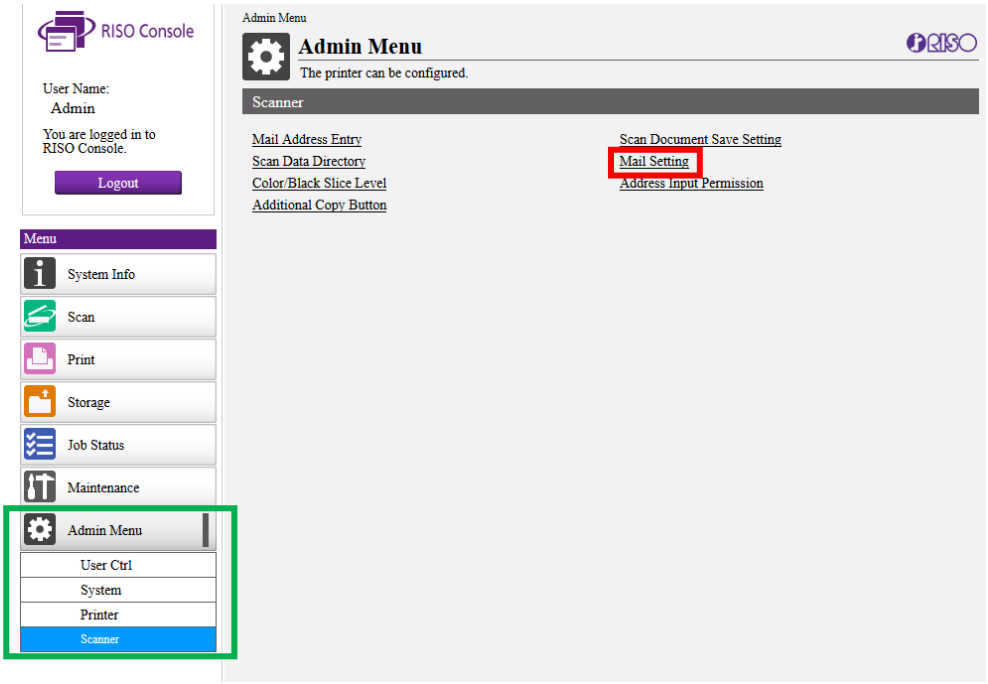


b) Login into the RISO device as **Admin** using an Admin account & password.



c) Select: **Admin Menu**

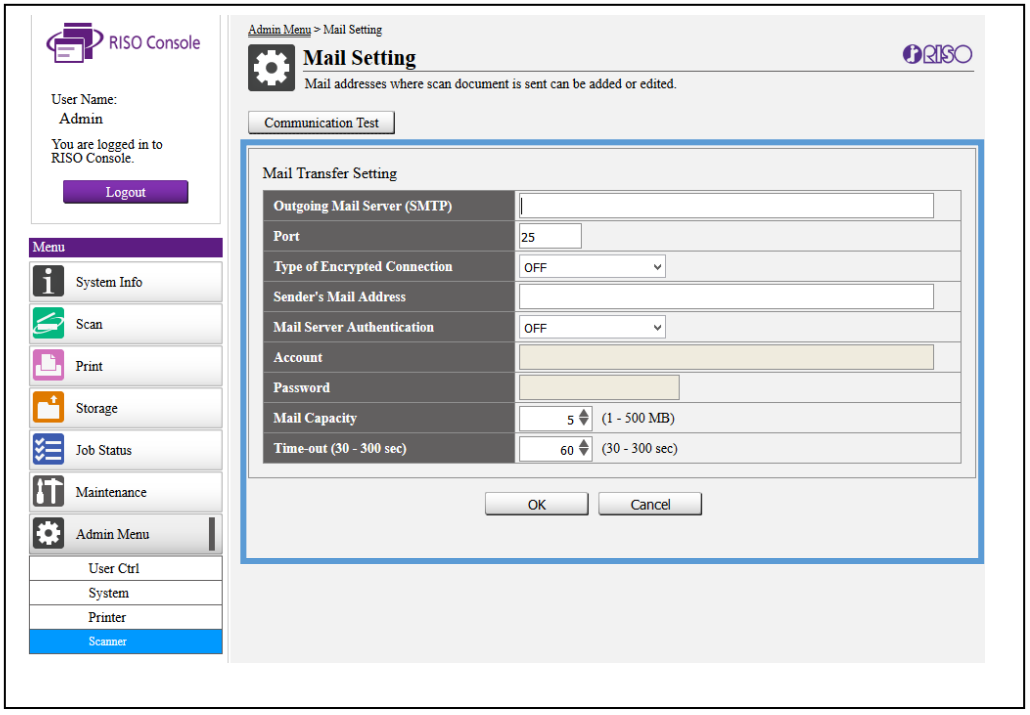
d) From the Admin Menu select: **Scanner**



e) From the list of menu items on the right, select: **Mail Setting**

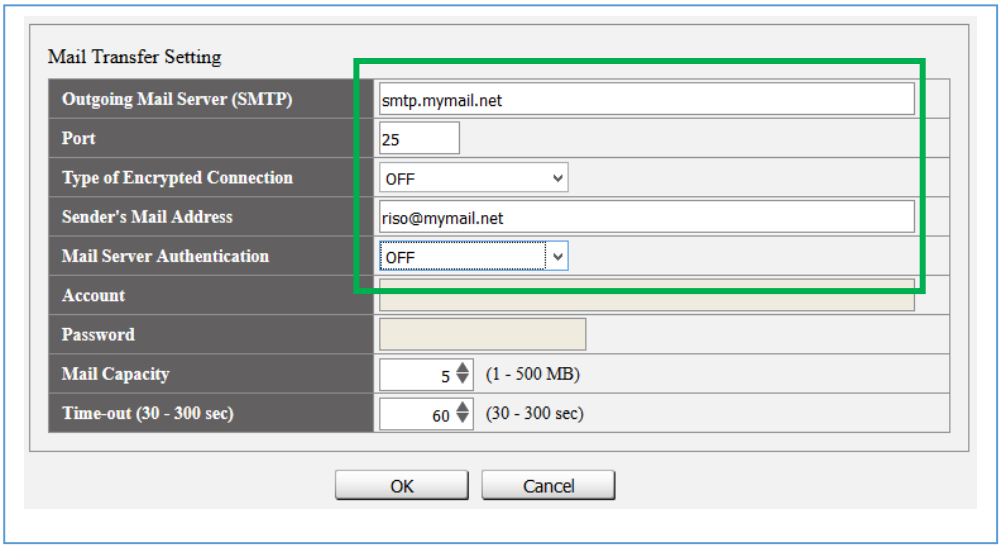
f) Enter the settings according to email server requirements.

The IT Administrator for your network should be able to advise what settings are required for your type of email server.



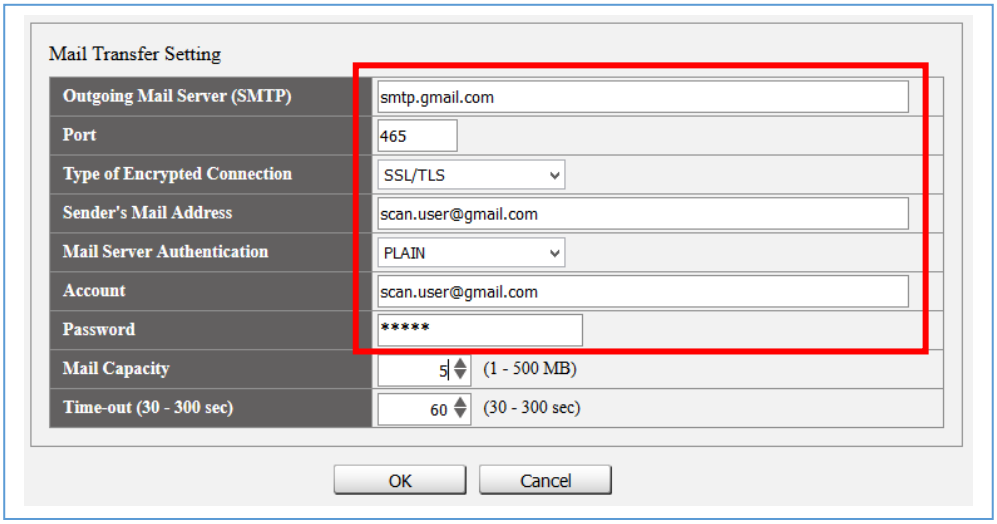
For example:

g) A server that uses PORT **25** & doesn't require any form of authentication.



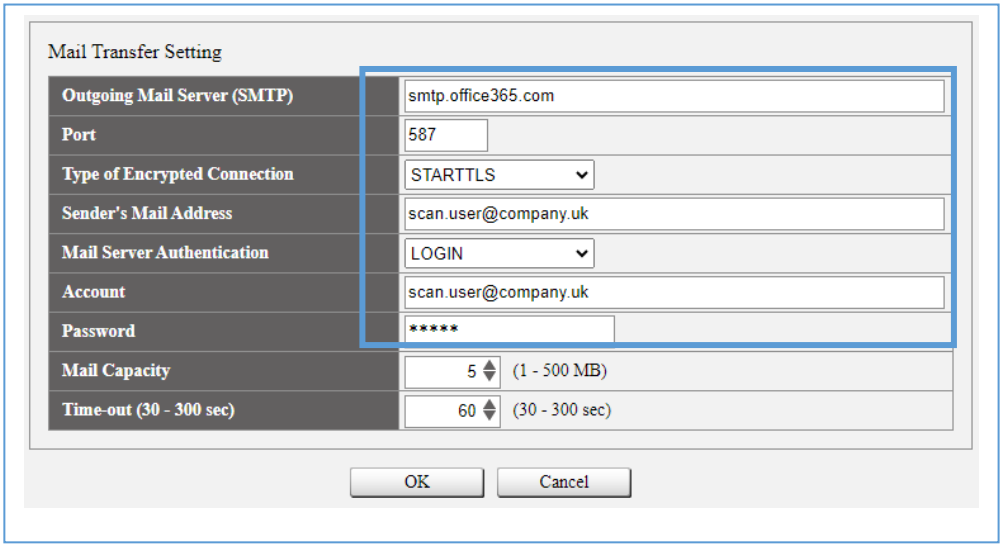
h) A Server that uses PORT 465 and requires SSL/TLS authentication such as Google GMAIL service.

NB: When using GMAIL refer to the notes on page 19 & 23



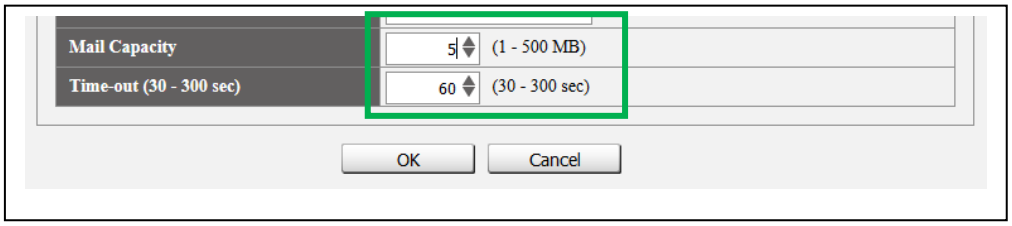
i) A Server that uses PORT **587** and **STARTTLS** authentication such as **Microsoft Office 365** or **Google GMAIL service**.

NB: When using GMAIL refer to the notes on page 19 & 23



IMPORTANT: When using an email service that requires authentication (such as Office 365 or Gmail), please create a user account in your email system beforehand. This user account will be used to access the email server and transmit emails to recipients, so must have necessary privileges/access to the email system in order to do so.
This email address will also be used for the Senders Mail Address. Recipients' inbox will show this email address as the sender when receiving emails from the RISO device.

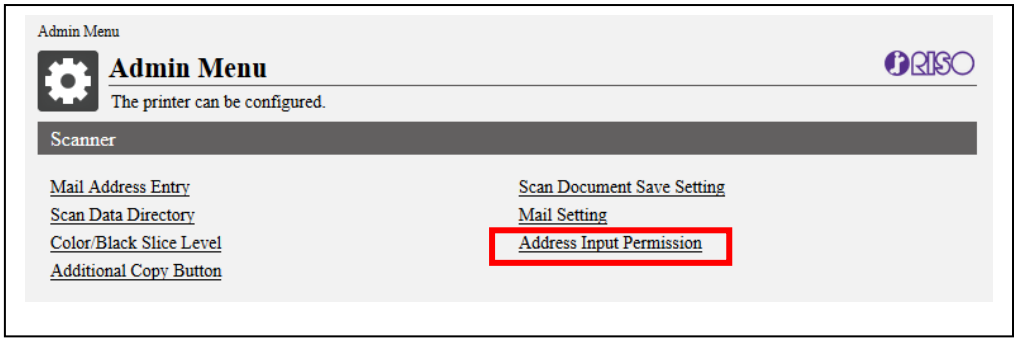
j) Set appropriate values for Mail Capacity & Time-out and Press **OK** to save the settings.



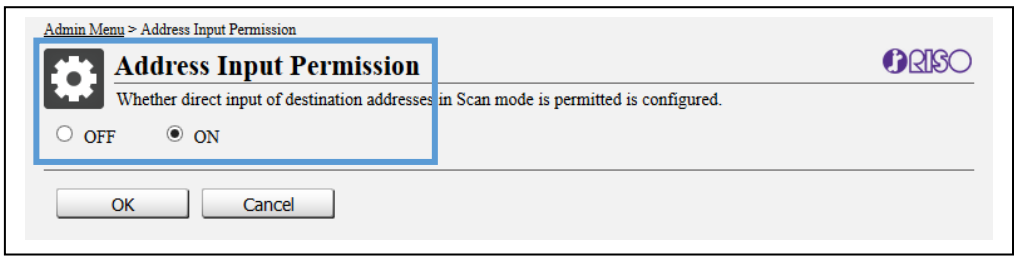
A confirmation box will appear if successful.

The next step is to send an email to a user to test the configuration.

Select **Address Input Permission**.



k) Select ON to allow direct input of email addresses when scanning.



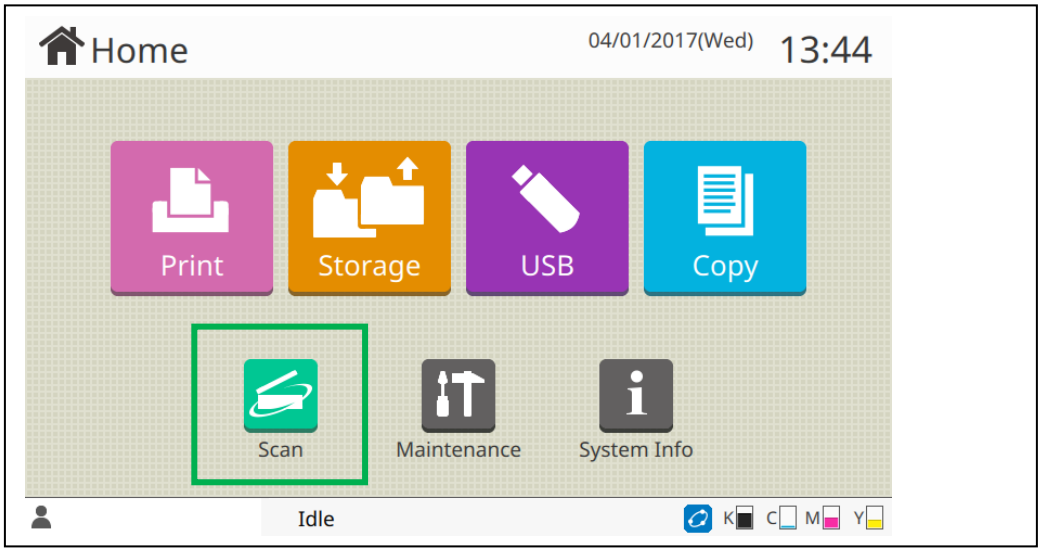
IMPORTANT: The communication test button on the RISO Console, can be unpredictable.

To test the settings, please perform a scan to email directly at the RISO device, if the scan fails, an error code will display. Please refer to pages 24-30 for information regarding the error code

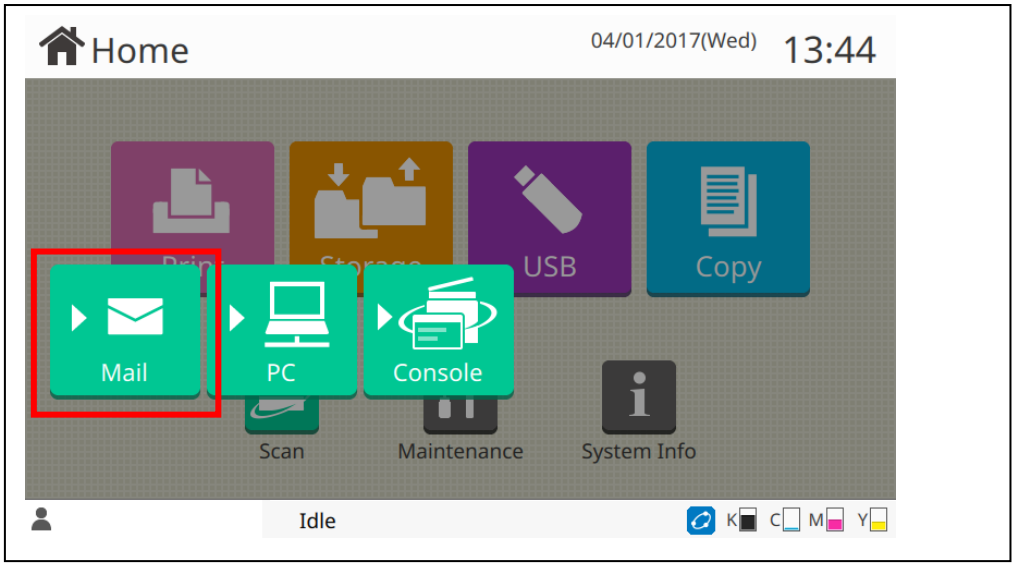
Go to the RISO device, place an A4 original in the ADF scanner and then access the LCD panel

l) Select **Scan** from the LCD Panel.

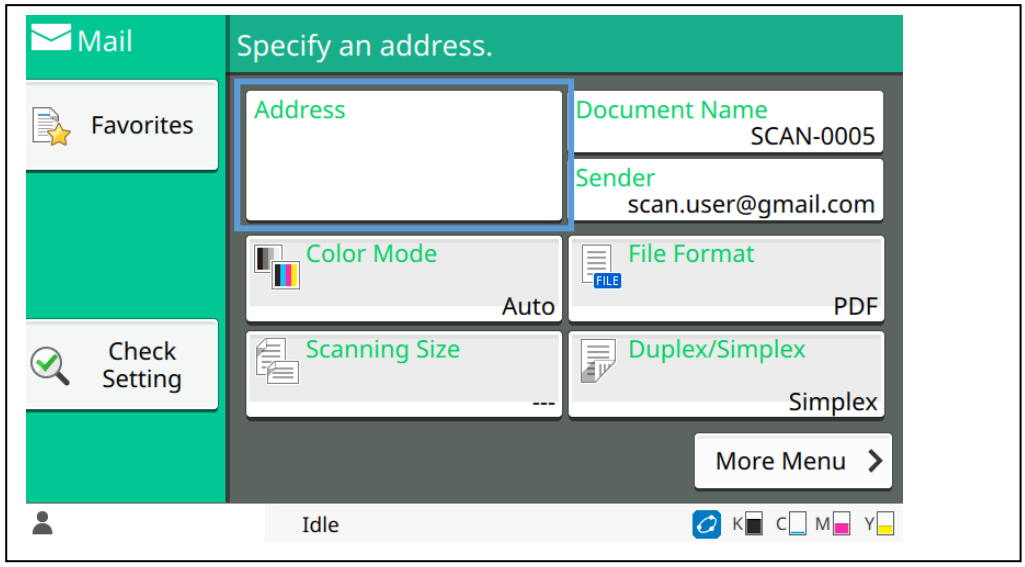
NB: Scan button may appear in a different location as the panel layout & buttons can be customised by the Admin User.



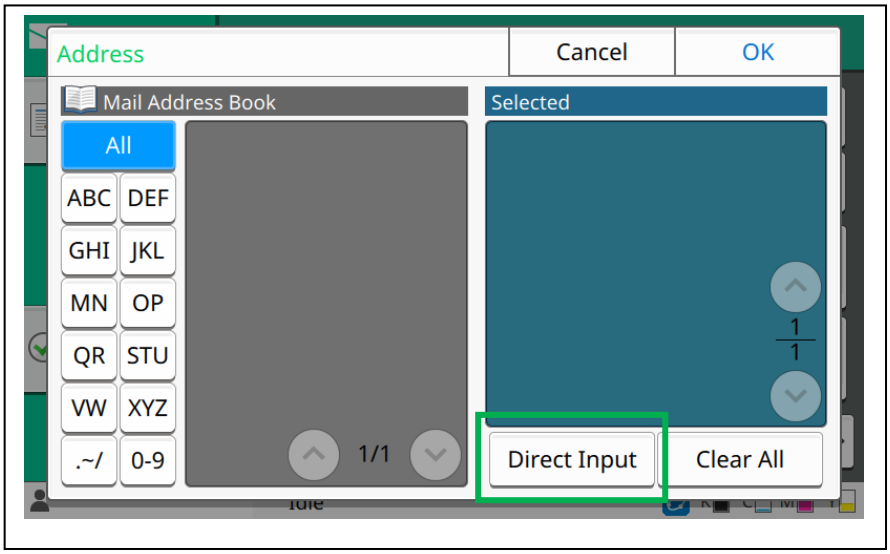
m) Select **Mail** as the scan method.



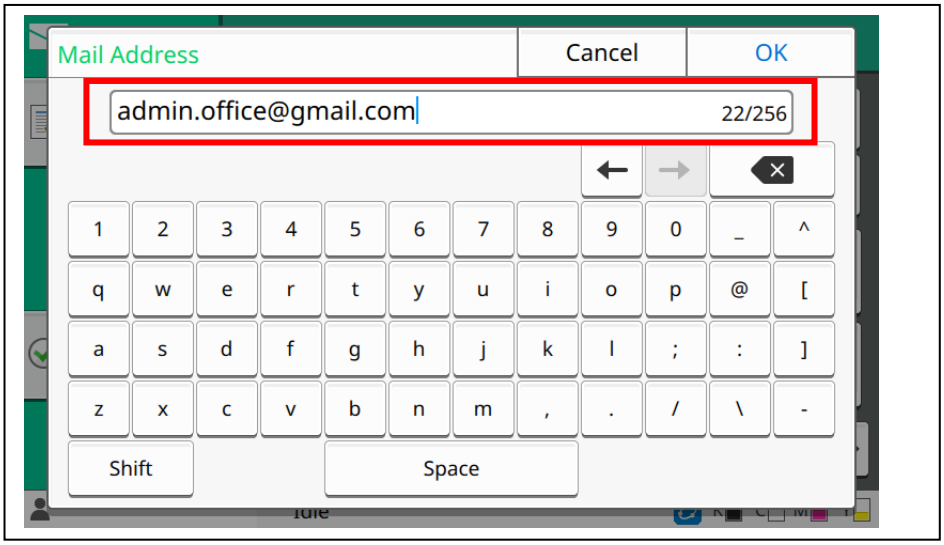
n) Press the **Address** button to enter an email address.



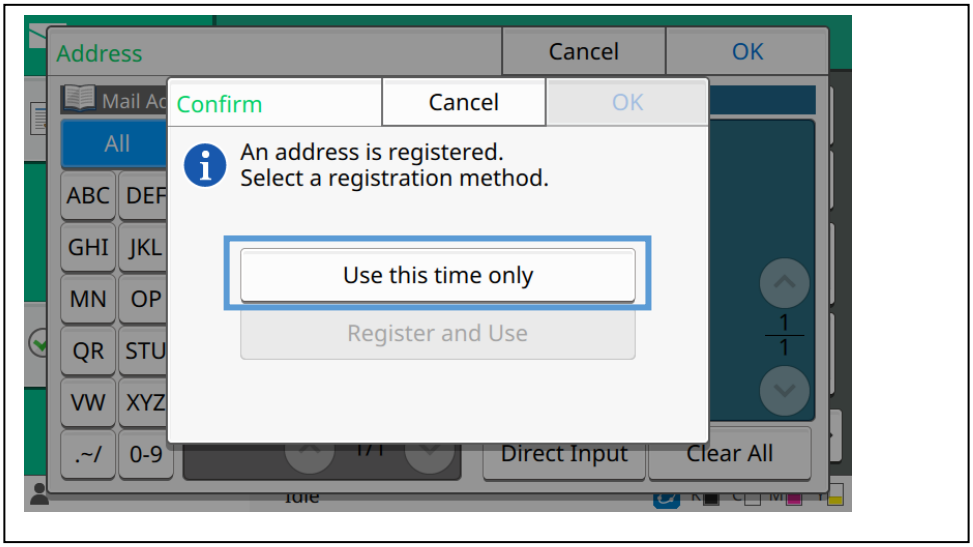
o) Select **Direct Input**



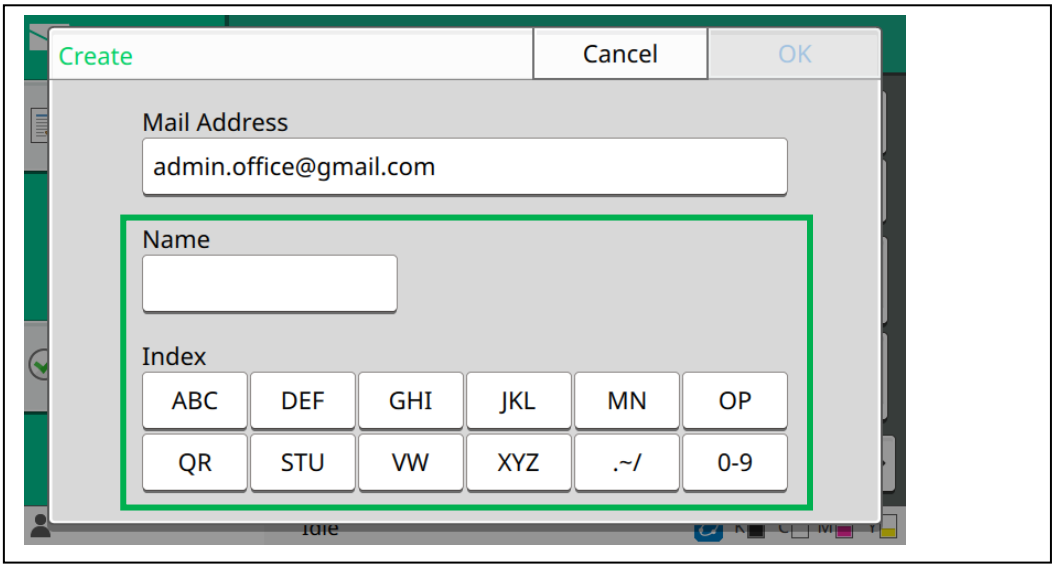
p) Enter the email address of the recipient you wish to scan to.



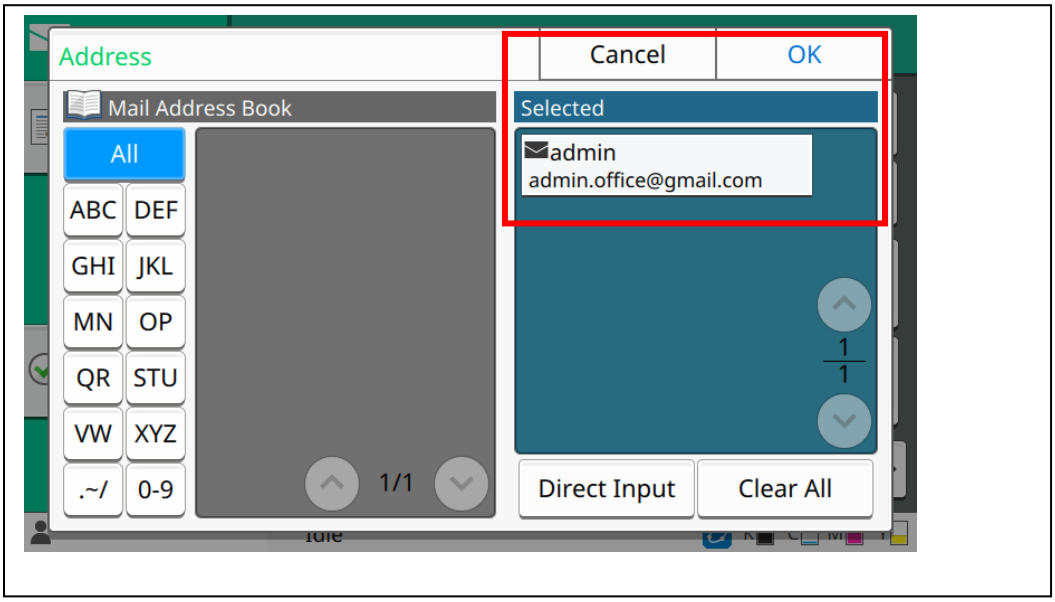
q) Select **Use this time only** and press OK.



r) Enter a **Name** and **Index location** and press OK to continue.

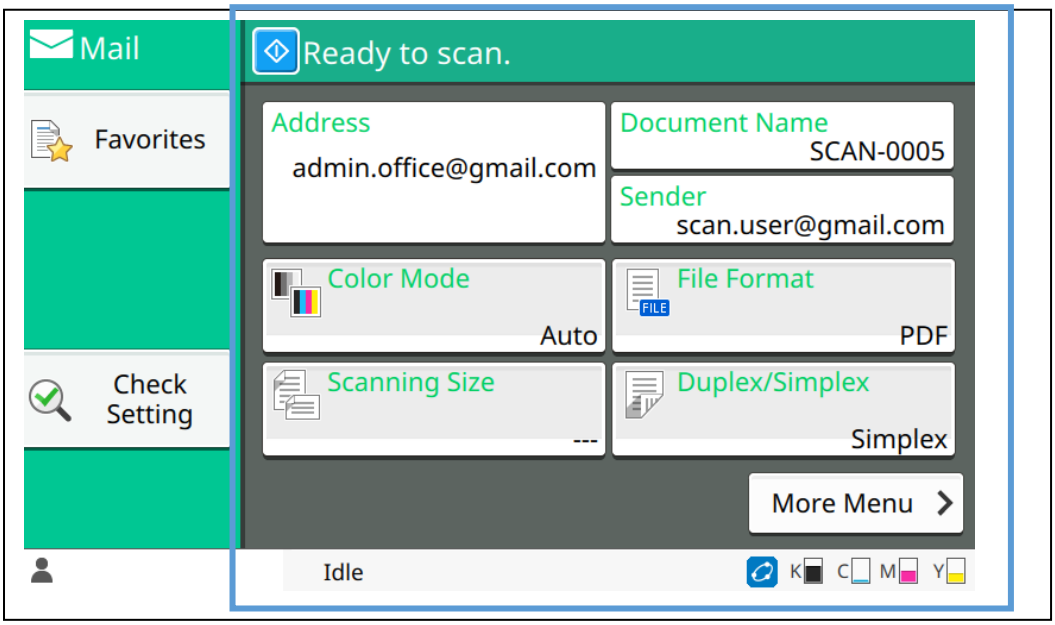


s) The recipients email address will appear in the selected windows on the left.
Press **OK** to continue.



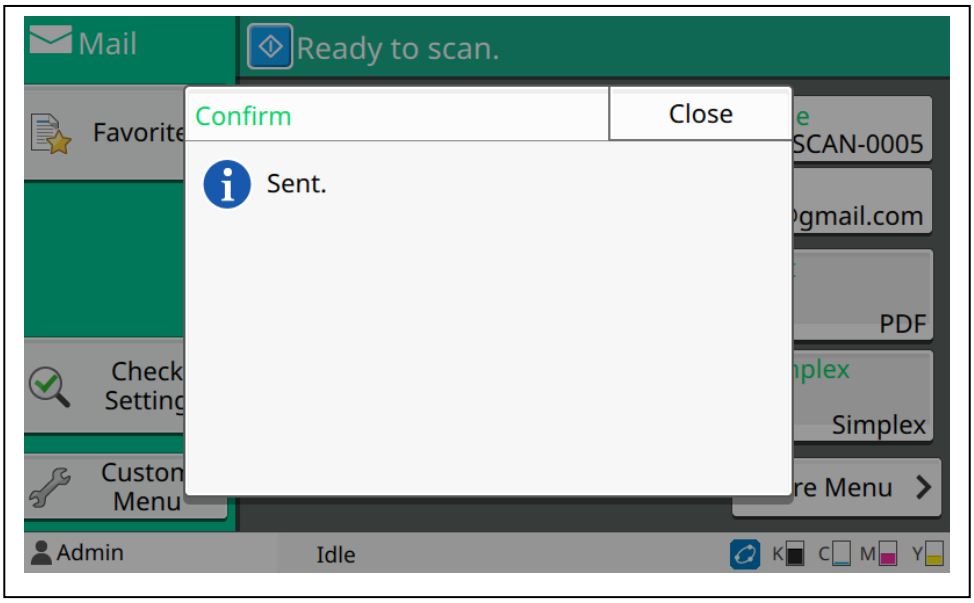
t) The document is now ready to scan.

Change the scanner settings as required then press the **START** button on the control panel to initiate the scan.



u) After a few seconds you should receive a message confirming the email was successfully sent.

If you receive an error, please check all the email settings are correct and try again.



Registering individual email addresses in the RISO Device

Frequently used individual email addresses can be registered in the RISO device either from the LCD panel itself or via the web console interface.

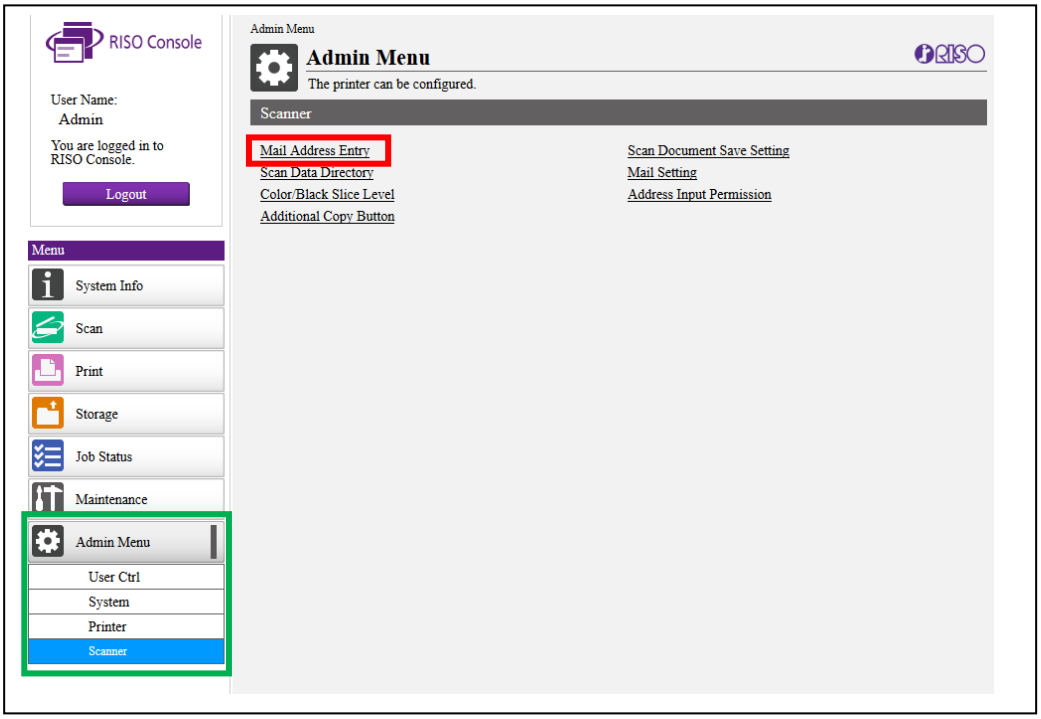
Multiple email addresses can be registered from the web console interface by means of a CSV file containing a list of the usernames and email addresses.

Register individual email addresses

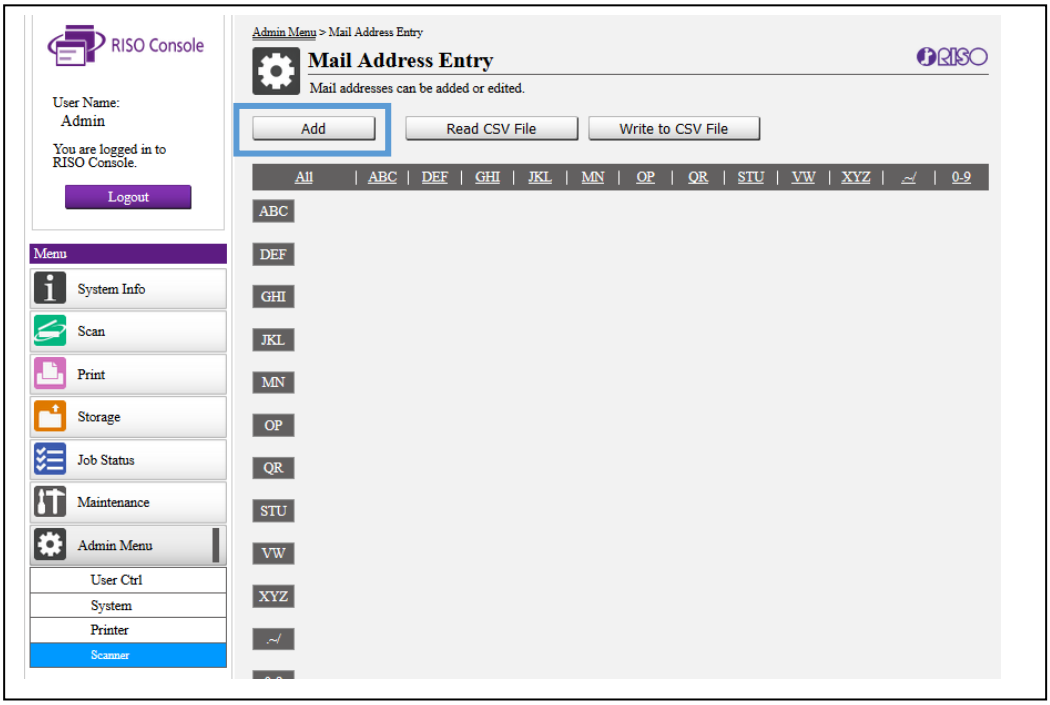
a) Using a web browser log into the RISO device as **Admin** and enter **Admin Mode** (refer to page 2 of this guide for instructions on how to do this).

b) Once in **Admin Mode**, navigate to the **scanner** section

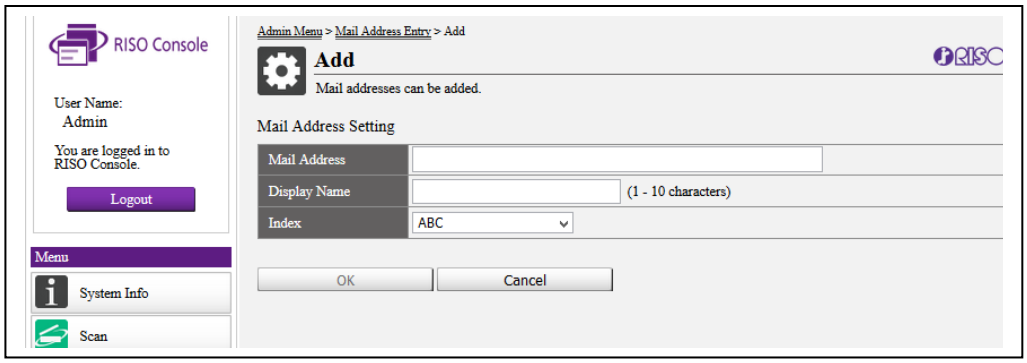
c) Select **Mail Address Entry** from the list of options.



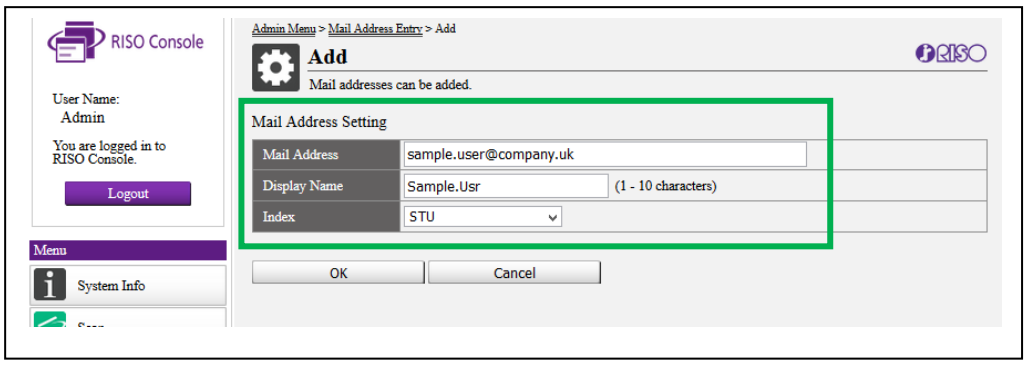
d) To add individual email addresses select **Add**



e) Once opened, you will find entry fields such as Email Address, Display name and Index.

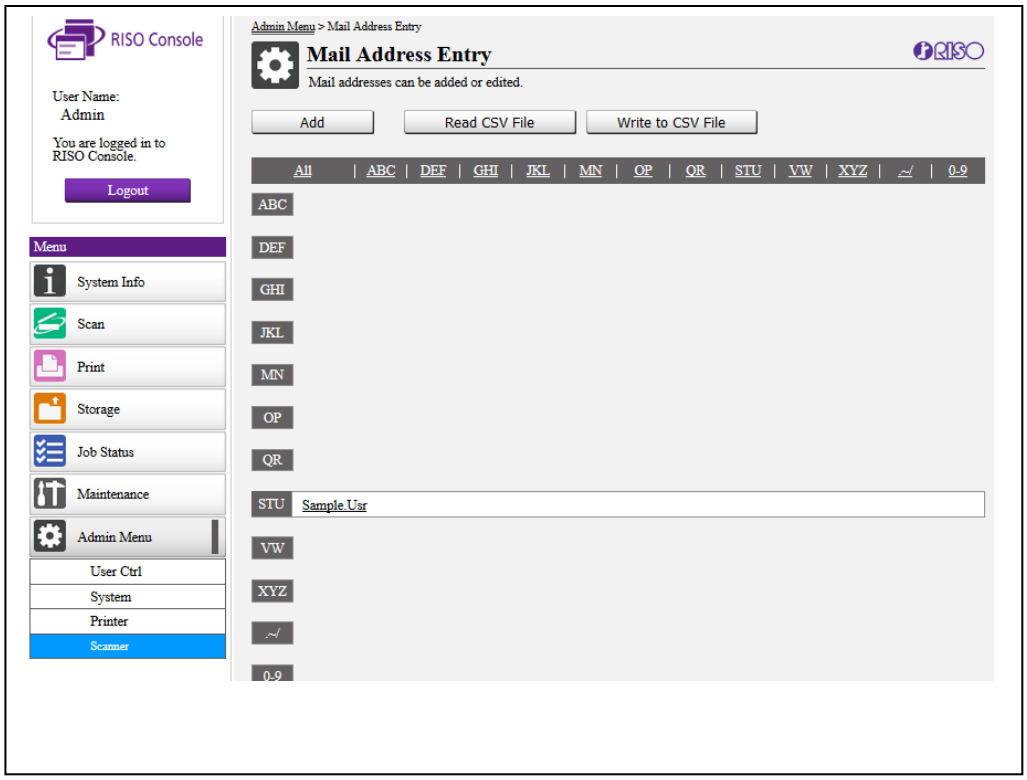


f) **Example:** Complete the entry fields as necessary and press **OK**.



g) The entry is now registered in the RISO device and will be listed on the Mail Address Entry window

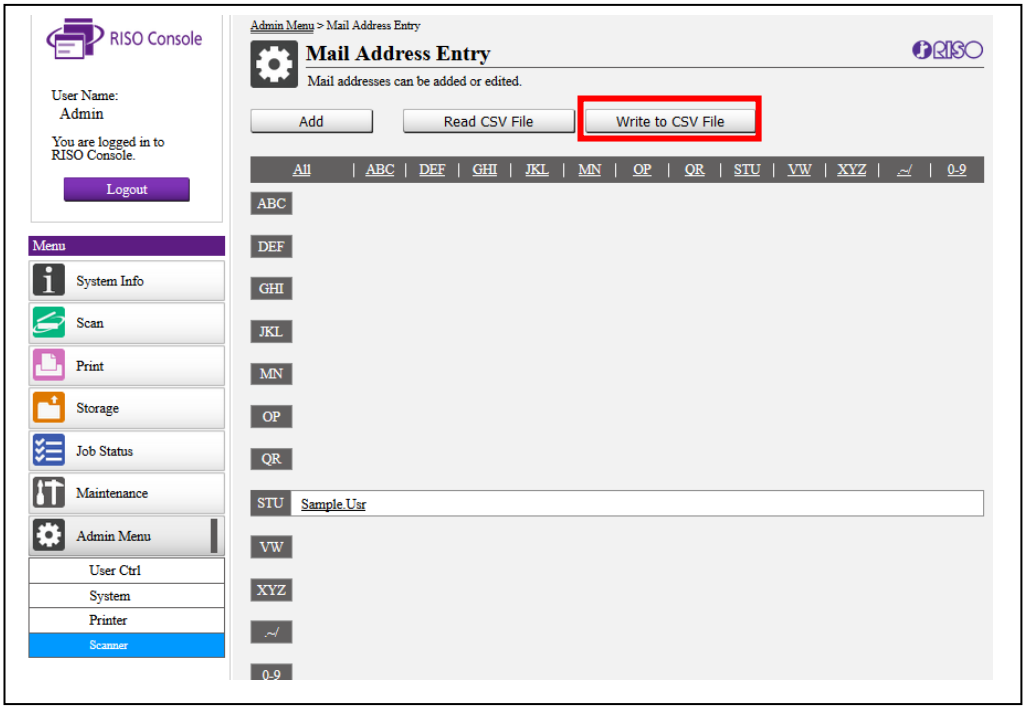
Continue to input additional email addresses as required.



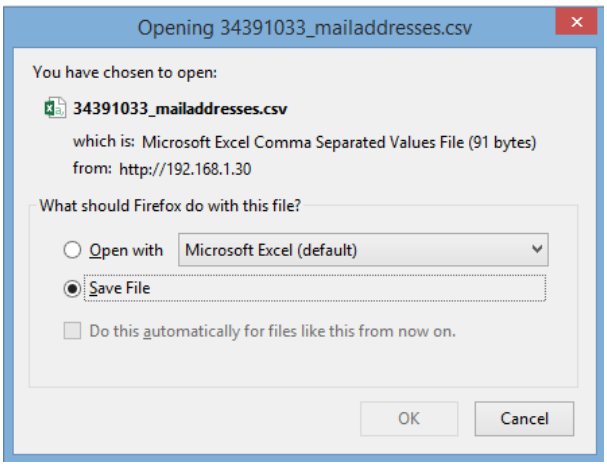
Registering multiple email addresses via CSV

Multiple email addresses can be registered on the RISO device by uploading a CSV file containing the relevant fields. A CSV file from can be downloaded from the RISO device and used as a template.

h) While in the Mail Address Entry Window, **Select Write to CSV File**



i) Save the CSV to your computer. Open the file with Microsoft Excel or notepad if you prefer a simple text document.



Add new email address to the CSV file according to the following format.

j) In this example we have used Excel to open the file.

	A	B	C	D	E
1	Ver.03.02.01				
2	Display name	Index	Mail address		
3	Sample.Usr	8	sample.user@company.uk		
4					

Column A contains the display name/ username that will appear on the RISO device address list.
Note: This field is restricted to a maximum of 10 characters.

Column B represents the index field where the address is to be registered.
Note: The Index fields are entered as numerical values correlating to index groups.
i.e. ABC = **1**, DEF = **2**, GHI = **3**, JKL = **4**, MN = **5**, OP = **6**, QR = **7**, STU = **8**, VW = **9**, XYZ = **10**, .~/ = **11**, 0-9 = **12**

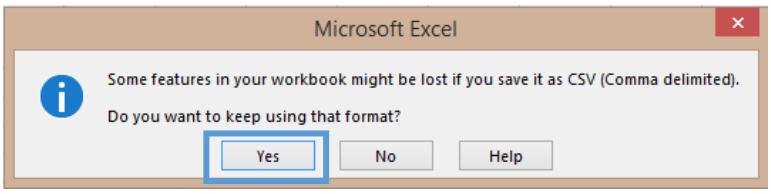
Column C contains the user's email address.

k) Example: Two new addresses are added to the CSV file.

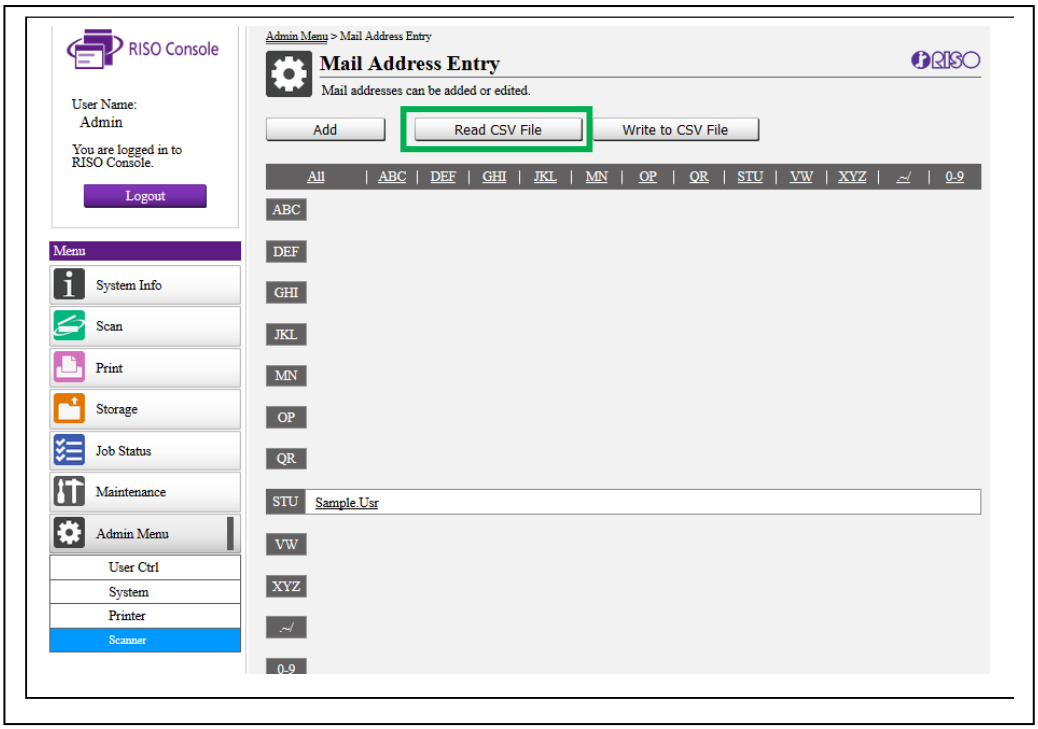
Once all the required fields have been completed, save the file to your computer or a location you can easily access.

	A	B	C
1	Ver.03.02.01		
2	Display name	Index	Mail address
3	Sample.Usr	8	sample.user@company.uk
4	Ann.Usr	1	ann.user@company.uk
5	01test.usr	12	01test.user@company.uk
6			

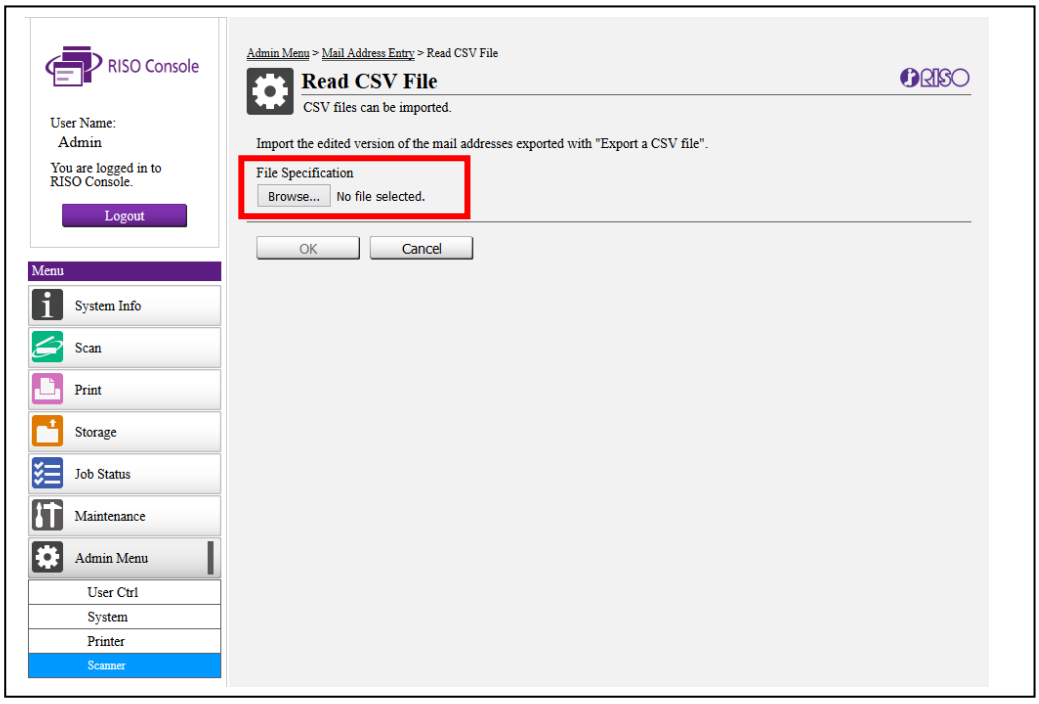
l) **Important:** You will be prompted to keep using the CSV format. Ensure you select YES.



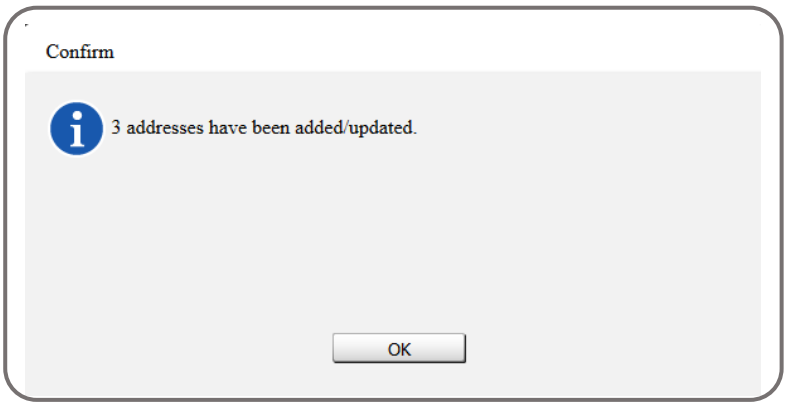
m) Navigate back to the Mail Address Entry Window and select **Read CSV File**



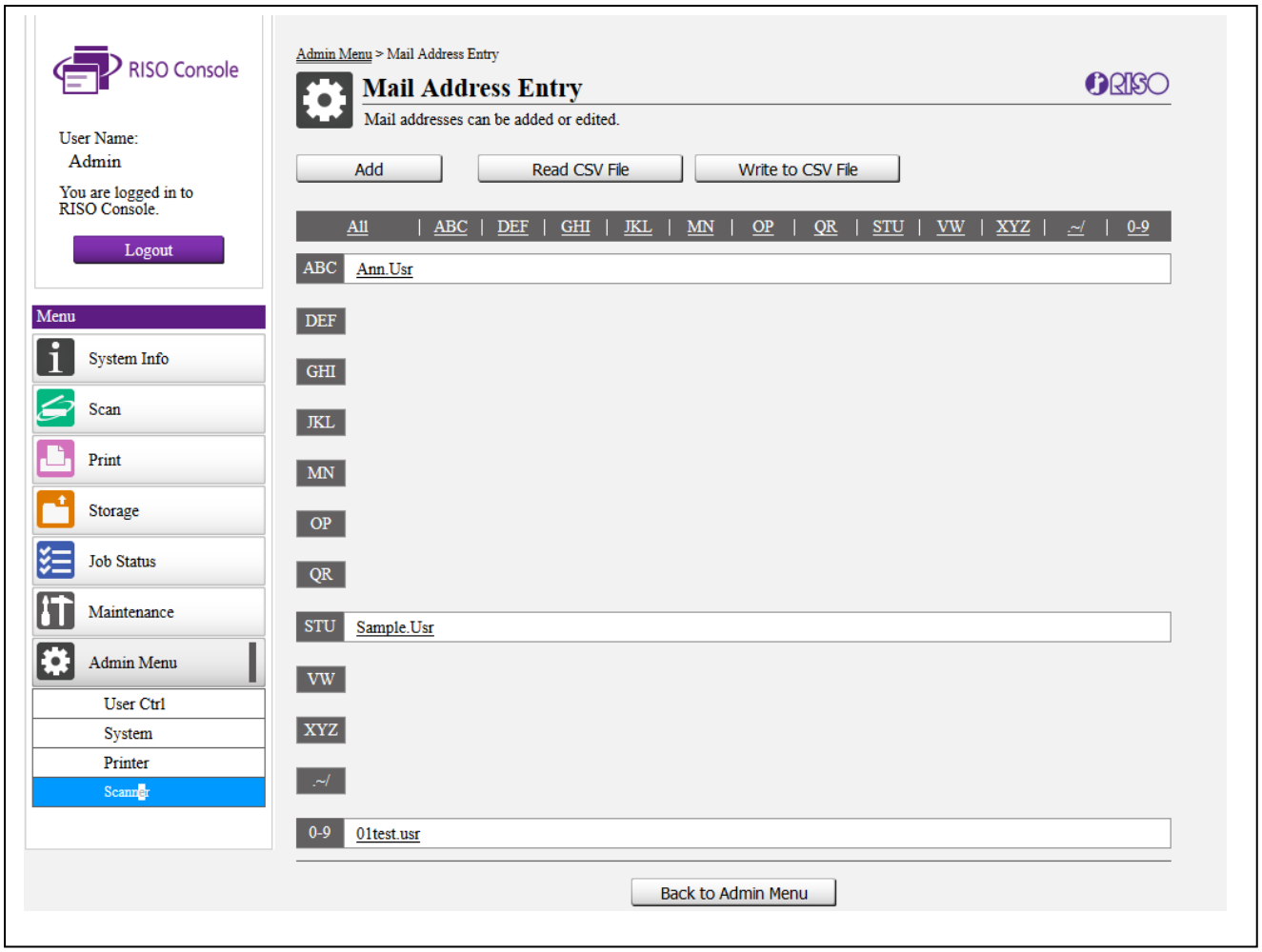
n) Select **BROWSE** and navigate to the location where the file was saved.



o) Click **OK** to import the addresses.
If successful a confirmation message will appear.



p) The address are now imported into the RISO and will appear in the address list



q) **Logout of the Admin Menu, the device is now ready to scan to email.**

GMAIL - SMTP settings to send mail from a printer, scanner, or app

You can set up your on-premises multifunction printer, scanner, fax, or application to send email through G Suite. The three available options are: SMTP relay service, Gmail SMTP server and Restricted Gmail SMTP server.

For details about configuring your device or application to send SMTP messages, refer to its documentation. Google Support cannot assist with the configuration settings.

SMTP relay service - used to send mail from your organization by authenticating with the IP address(s). You can send messages to anyone inside or outside of your domain

Gmail SMTP server - requires authentication with your Gmail/G Suite account and password. Messages can be sent to anyone inside or outside of your domain.

Restricted Gmail SMTP server - does not require authentication, and you will be restricted to send messages to Gmail or G Suite users only.

The table below will help you decide which one of these options will best meet your needs:**Option**	**G Suite SMTP relay (recommended)**	**Gmail SMTP server**	**Restricted Gmail SMTP server**
FQDN of SMTP Service	smtp-relay.gmail.com	smtp.gmail.com	aspmx.l.google.com
Configuration requirements	Port 25, 465, or 587 SSL/TLS optional. One or more static IP addresses are required.	Port 465 (SSL required) Port 587 (TLS required) Dynamic IPs allowed	Port 25 TLS not required Dynamic IPs allowed Mail can only be sent to Gmail or G Suite users
Requires authentication	IP address provides authentication.	Your full Gmail or G Suite email address required for authentication	No.
Bypasses anti-spam	No. Suspicious emails may be filtered.	No. Suspicious emails may be filtered.	No. Suspicious emails may be filtered.
Sending Limits	**Limits for registered G Suite users.** A registered user cannot relay messages to more than 10,000 recipients per day. For full SMTP relay limits please see Sending limits for the SMTP relay service.	2000 Messages per day. See Sending limits for more detailed information.	Per user receiving limits will apply.

You can use the SMTP relay service in the Google Admin console to relay mail from your device or application. This is possible once you add your network IP range to the SMTP relay service. You will need to configure your device to connect to smtp-relay.gmail.com on ports 25 or 465, 587. For more details about using this setting, see SMTP relay service setting.

Gmail SMTP Server could also be used to relay messages from your device or application. You can connect to Gmail mail servers using SMTP, SSL/TLS. If you connect using SMTP, you can only send mail to Gmail or G Suite users; if you connect using SSL/TLS, you can send mail to anyone.

If your device or application supports SSL - connect to smtp.gmail.com on port 465.To connect with SSL, you need to provide a Google username and password for authentication. Ensure that the username you use has cleared the CAPTCHA word verification test that appears when the user first logs in. We also recommend ensuring that the account has a secure password.

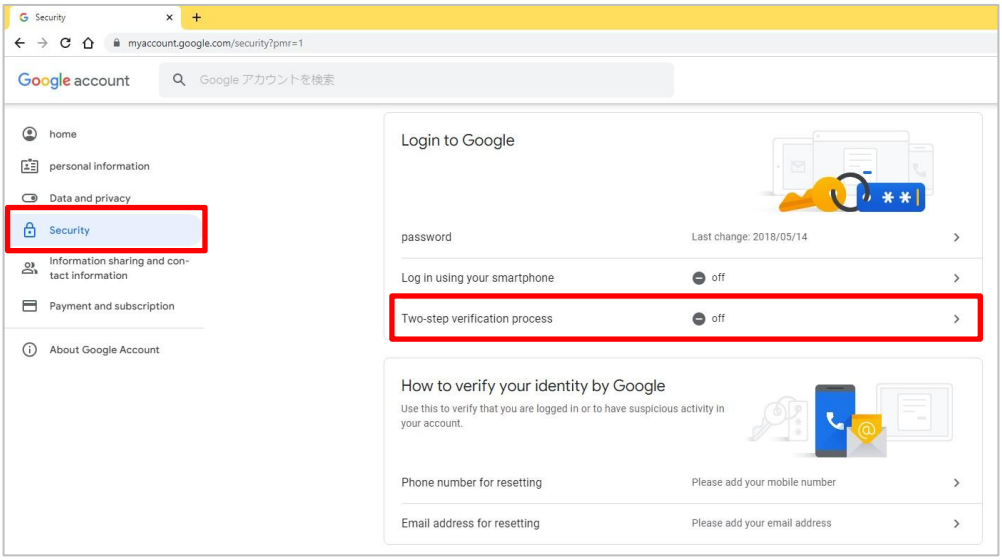
If your device or application does not support SSL – connect to aspmx.l.google.com on port 25.You must configure an SPF record for your domain with the IP address of the device or application to ensure that recipients do not reject mail sent from it. You must also add this IP address to the Email Whitelist box in your Google Admin console. For example, if your sending device sends from 123.45.67.89, add that address to your SPF record without removing the G Suite mail servers from the record: v=spf1 ip4:123.45.67.89 include:_spf.google.com ~all

Enabling non-Google Apps/devices to use GMAIL SMTP server

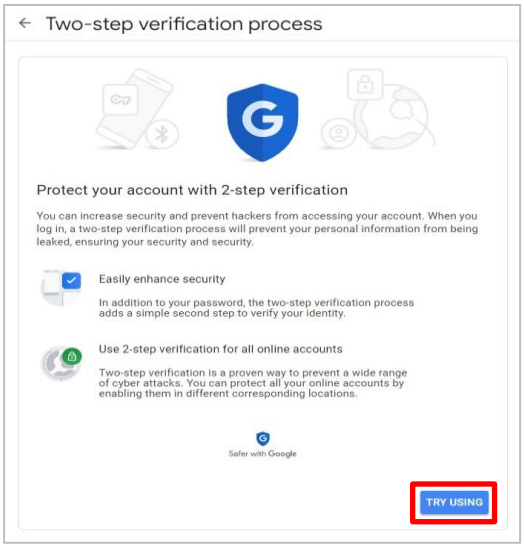
If you are using a google account for scan to mail on ComColor, two-step verification setting and creating App password are needed on google account. By setting created App password on ComColor

1. Two-step verification setting of google account

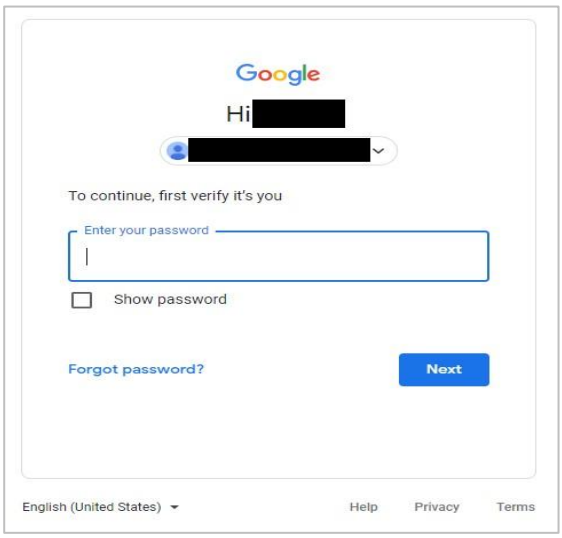
1. Access to google account security setting page. https://myaccount.google.com/security
2. Select “Security” > “Two-step verification process.”



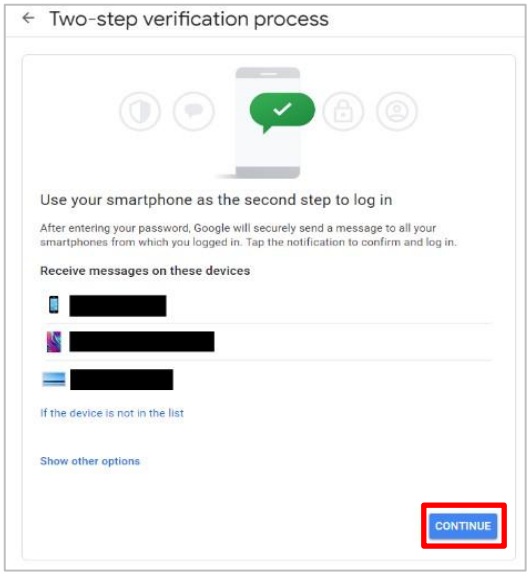
3. Click” TRY USING”



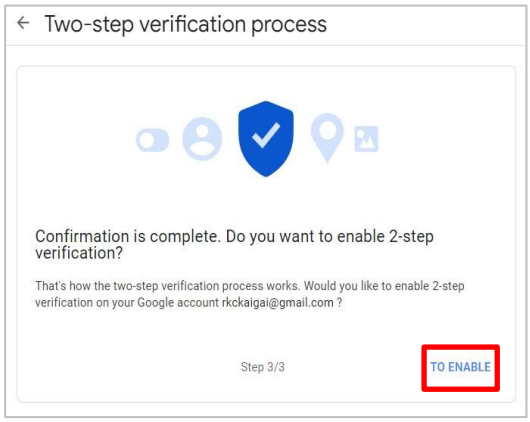
4. Login with your google account.



5. Select verification method and click continue.

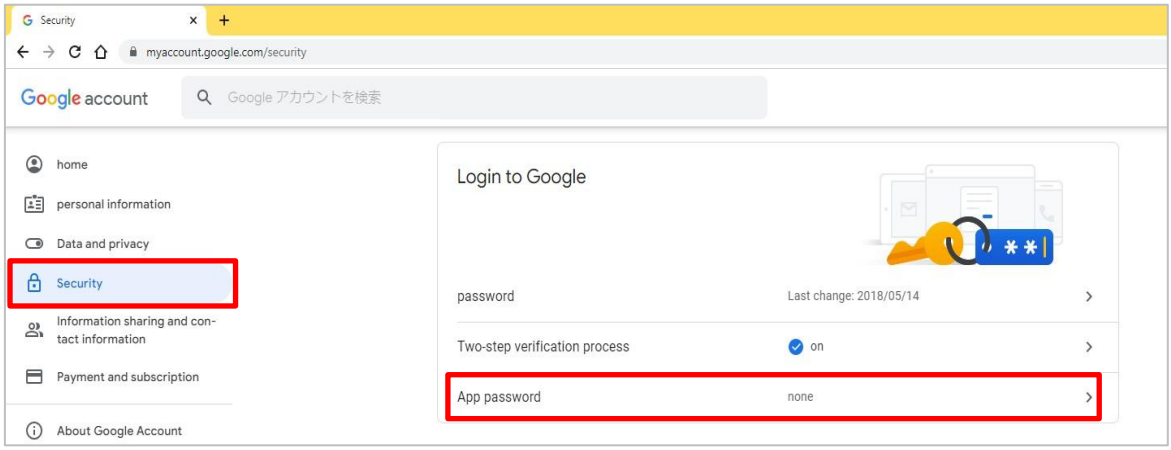


6. Enable Two-step

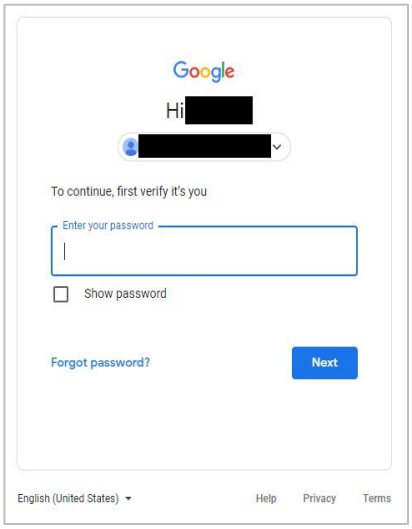


2. Create App password

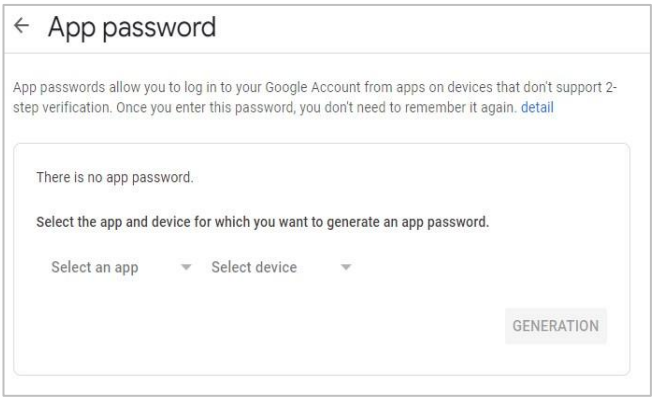
1. Access to google account security setting page. https://myaccount.google.com/security
2. Select “Security” > “App password.”



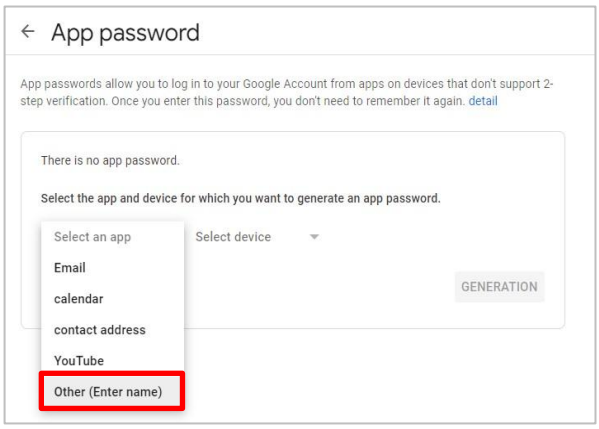
3. Sign in using your Google account.

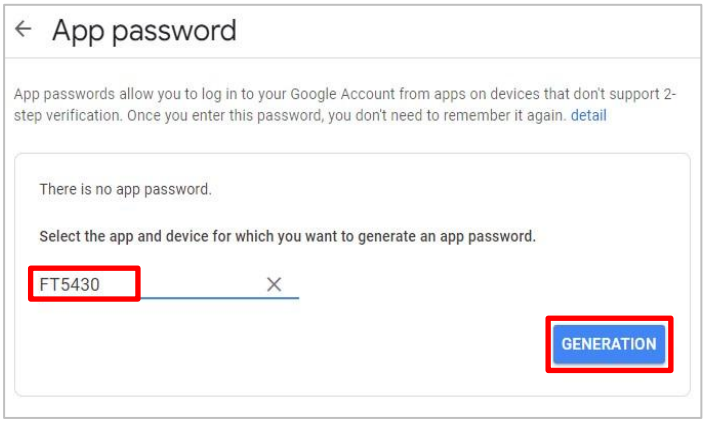


4. App password settings will display.

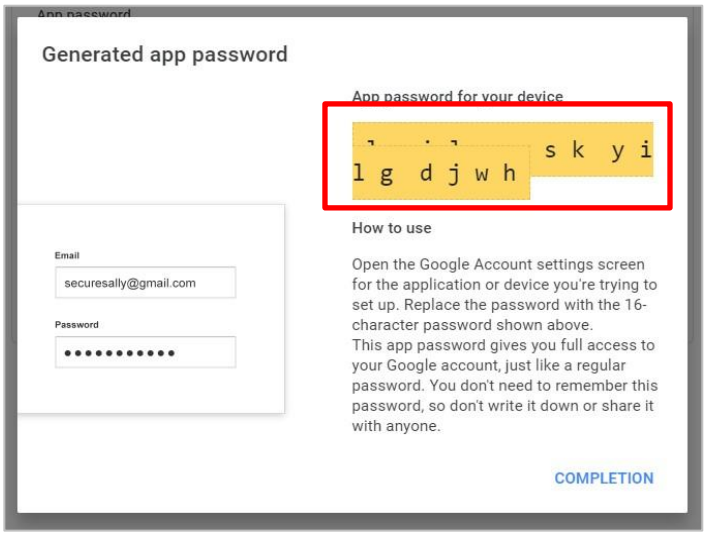


5. Select "Other (Enter name)," enter the machine name, and then click “GENERATION.”

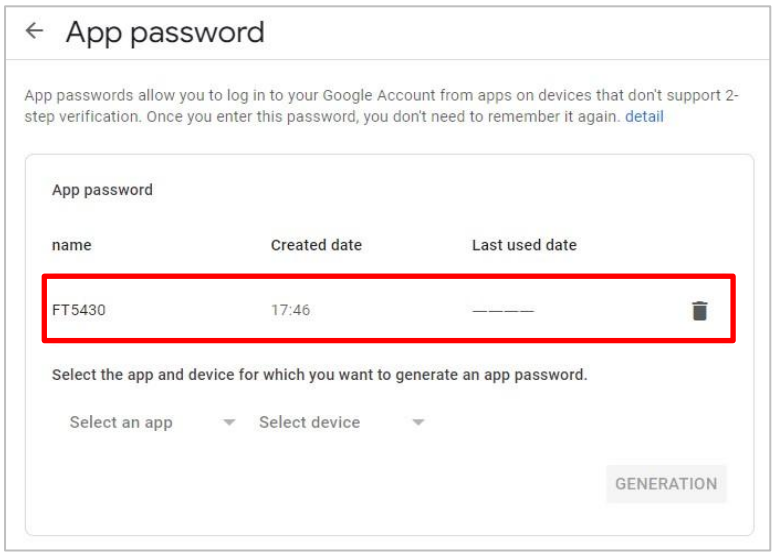




5. Confirm 16 digits of App password

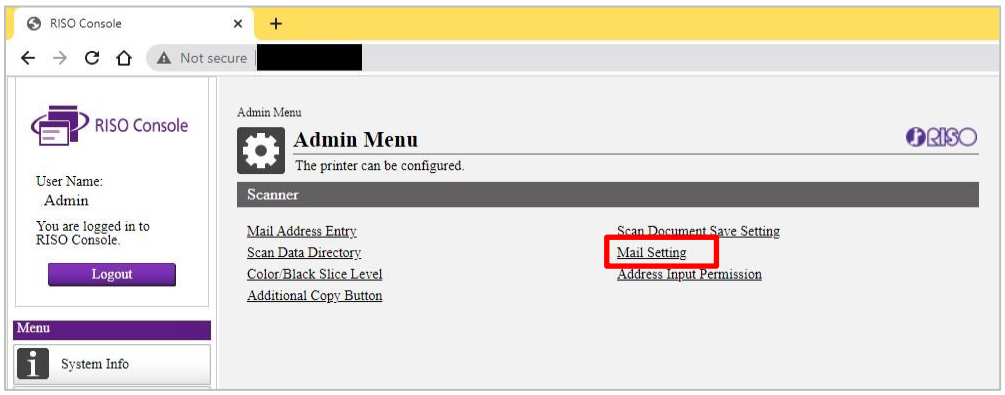


6. Confirm that the app password has been created correctly



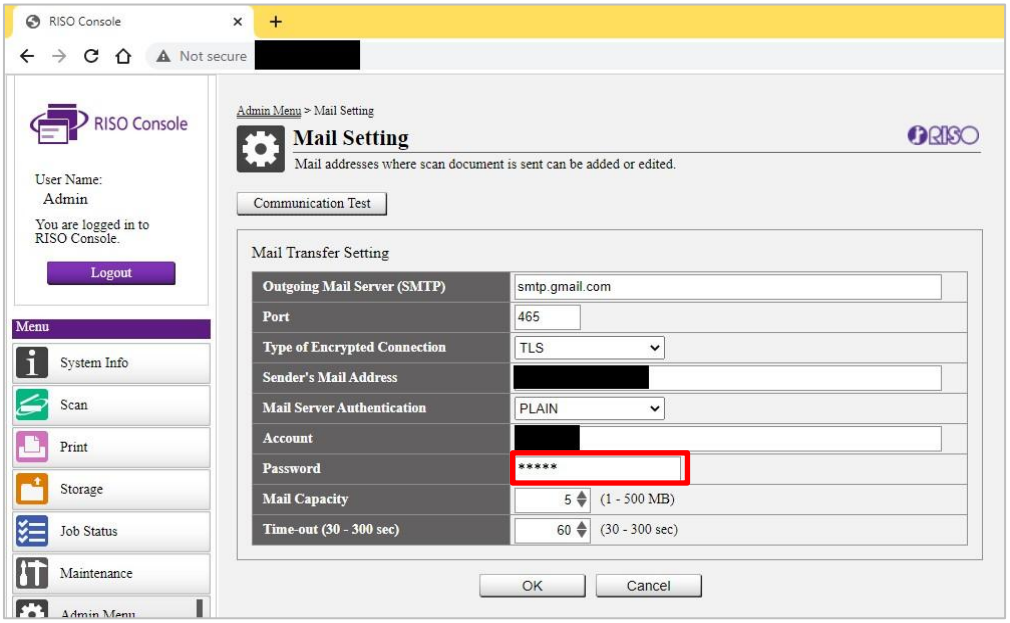
3. ComColor setting

1. Access the console and navigate to Admin Menu > Scanner > Mail Settings.



2. Enter the 16-digit app password in the password field instead of using your Google account password.

Note: When entering or pasting the app password into the RISO Console 'Password' field, please ensure it contains no spaces. Click Here for additional information.



3. Perform a scan-to-email and confirm that the scanned document is received in your email inbox.

If the scan fails and an error code appears, please refer to pages 24-30 in the documentation for error code details or page 31 for troubleshooting steps.

Error Codes

RISO Error Code	SMTP Error Code	What's Causing This Error	Solution
W093-230-1	550	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. Email error "550 Authentication is required for relay" indicates that the client requires authentication. Server error "550 this domain is not hosted here" indicates that the recipient address is not found or is inaccessible. Server error 550 or 550 Blocked Error indicates that the recipient is blocking your email on the recipient's email server.	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. Email error "550 Authentication is required for relay" - The user must check the configuration for proper authentication on the email client. Server error "550 this domain is not hosted here" - The user must ensure that all the recipient email addresses are valid. 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.
W093-230-2	551	SMTP error 551 occurs when an email bounces during the delivery process. Two types of bounces may take place: **Soft Bounce** - Soft bounce takes place when the recipient's mailbox is full or if their email server is temporarily unavailable. **Hard Bounce** - 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.	To resolve this error, ensure no underlying issues affect the email server or the connectivity. The following common troubleshooting steps can help narrow down and resolve the issue at hand. • Ensure that all recipient's email addresses are valid. • Ensure that the recipient has enough space in their mailbox to receive the email. • Ensure that the recipient's email server is available and is accepting email

W093-230-3	553	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. Some of the most common reasons for rejection are: The recipients spam filter detects the email as malicious or spam. Blocklisted email address Blocklisted IP Address	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.

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: • Invalid credentials • Disabled account • Invalid or incompatible connection encryption settings • Invalid or incompatible Authentication Methods	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	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. The most common causes for this error are: • Too many connections from your host • The server is busy and cannot accept the connection. • Service is temporarily unavailable	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. 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
W096—233-2	450	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: • The recipient server cannot find the email address on its server. • The recipient mail server rejected your request as your email content did not pass through its filter. • Your mail server's IP address gets denylisted	Here are some actions that you can take to solve the problem. 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. 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) Use MXToolBox to ensure that your mail server's IP address is not denylisted
W096—233-3	451	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	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
W096—233-4	452	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.	To resolve the error, you can do either of the following. • Increase email limit. • Use third-party email providers. • Split recipients

W096—233-5	454	This error occurs when emailing via the SMTP server without authenticating with it or when the authentication credentials are invalid	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. If nothing works, disable your firewall or anti-virus guard, and try sending the email
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	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. 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
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	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. 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)
W096—233-8	554	SMTP error 554 indicates that the mail server did not accept the email. Several reasons typically cause this error: • Invalid Recipient • Blocklisted IP • Bad DNS • SPF Record • DKIM Record • DMARC Record • Sender Flagged As Spam • Email Violation Policy	**Invalid Recipient Address** - Check if the email address(es) you are attempting to send the emails to is valid and if there are no spelling mistakes. **Blocklisted IP Address** - The user must remove their IP Address or domain from public blocklists. **Bad DNS Records** - Make sure that the "DMARC," "SPF," and "DKIM" records configurations are valid. **SPF Record** - 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. **DKIM Record** - Check if the sender's DKIM record is valid. **DMARC Record** - Check if the sender's DMARC record is valid. **Sender Flagged As Spam** - Check if the sender's domains are marked as spam by the recipient or the recipient's email provider/server. **Email Violation Policy** - Check with the recipient's email violation policy and adhere to the policy to resolve this issue.

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.	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. Secondly, ensure that the receiving SMTP server supports the command you are trying to execute. Lastly, disabling the anti-virus guard may help solve an SMTP 500 Error
W097-234-2	501	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). Furthermore, specific SMTP servers throw the 501 error when the email address does not comply with the RFC 2821 Specifications.	**For command-line users** If you're sending the email using an SMTP command exceeding 512 characters, you can use the SMTP extensions to increase this limit **For non-command-line users** 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. 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: 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 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.
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	It is essential to ensure that the SMTP client's authentication settings do not have errors and validate the user credentials. 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.

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 Agent) configuration, you may run into this error	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
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.