

Transition to Secure Admiral SmarterMail

Email is essentially a plaintext communication sent from mail clients to a receiving server. Its limitations leave message content exposed to interception while in transit. Email is often susceptible to such when connected to public hotspots or even with your IP. Spyware is an additional threat to your emails.

Email certificates help solve this issue by encrypting your transmitting message from one certified email server to another. This result is a secure email that protects your data. You may also have heard this as SSL/TLS encrypted email transfer.

Admiral IT has provided this security option for all our users and will fully enforce secured email by 31st October 2022. We urge all our users to update your computers and mobile devices to utilise secure email as soon as possible for your protection.

TARGET FULL TRANSITION: 31ST OCTOBER 2022

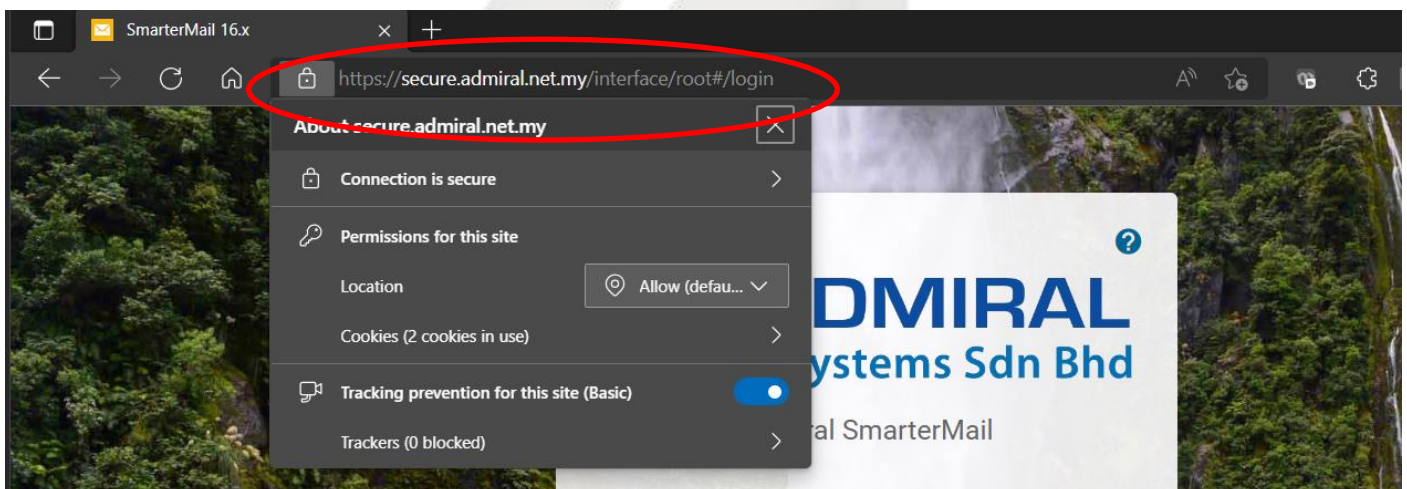
Technical support is available by submitting a ticket via our ticketing system via <https://www.admiralit.com.my>

Current unsecured POP3, SMTP and IMAP will be disabled by 31st October 2022

Secured Admiral SmarterMail – Immediate Effect

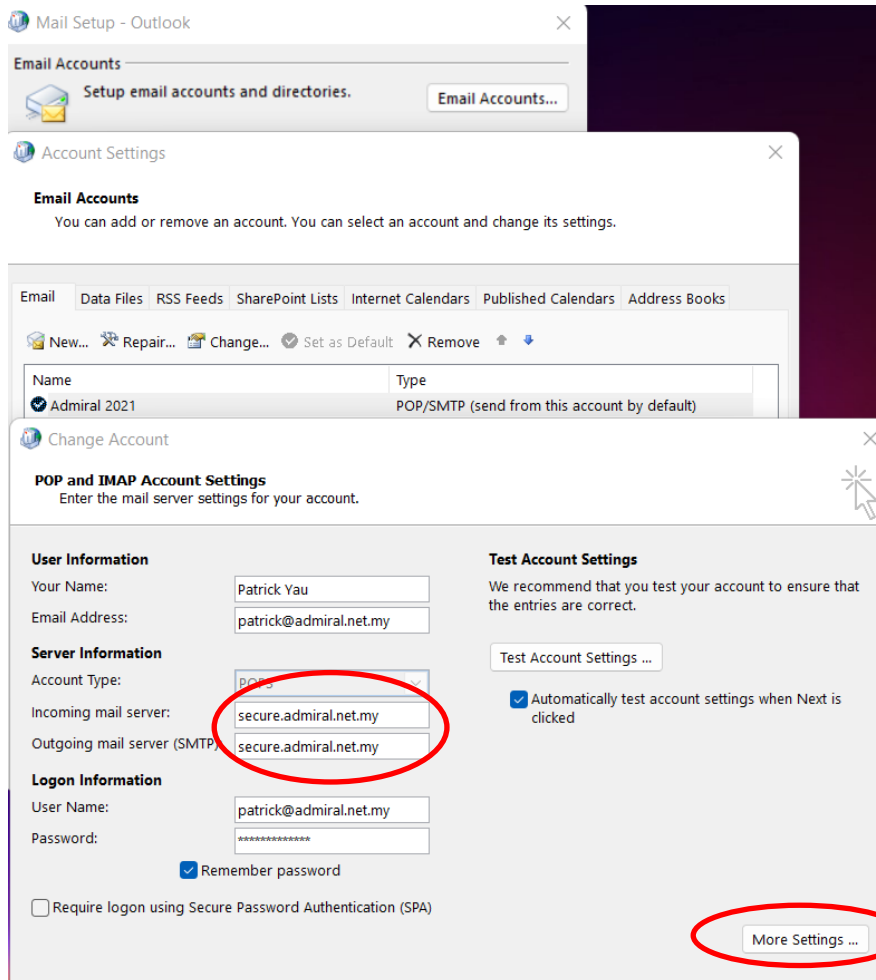
Your current <http://mail.companyname.com> URL will automatically be redirected to <https://secure.admiral.net.my> from now on. Please ensure that you are logging in to ONLY <https://secure.admiral.net.my> to prevent phishing attempts to steal your email password. DO NOT LOGIN to your email other than the domain above.

Note the “Padlock” icon is locked and it shows “Connection is secure” when clicked on it.



Note: This has been enforced with immediate effect. You will notice the change the next time you login to Admiral SmarterMail.

Microsoft Outlook or Similar Email Client (POP3)



- In Windows 10 or Windows 11, go to **Control Panel > Mail (Microsoft Outlook) > Email Accounts > Double Click on the email account hosted with Admiral.**

- Change the following Settings

Incoming mail server:

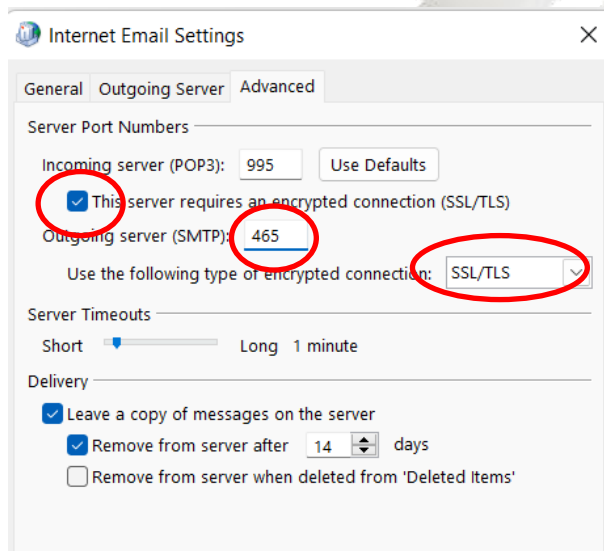
[Secure.admiral.net.my](https://secure.admiral.net.my)

Outgoing mail server (SMTP):

[Secure.admiral.net.my](https://secure.admiral.net.my)

No changes required on User Information and Logon Information

- Click on **More Settings**



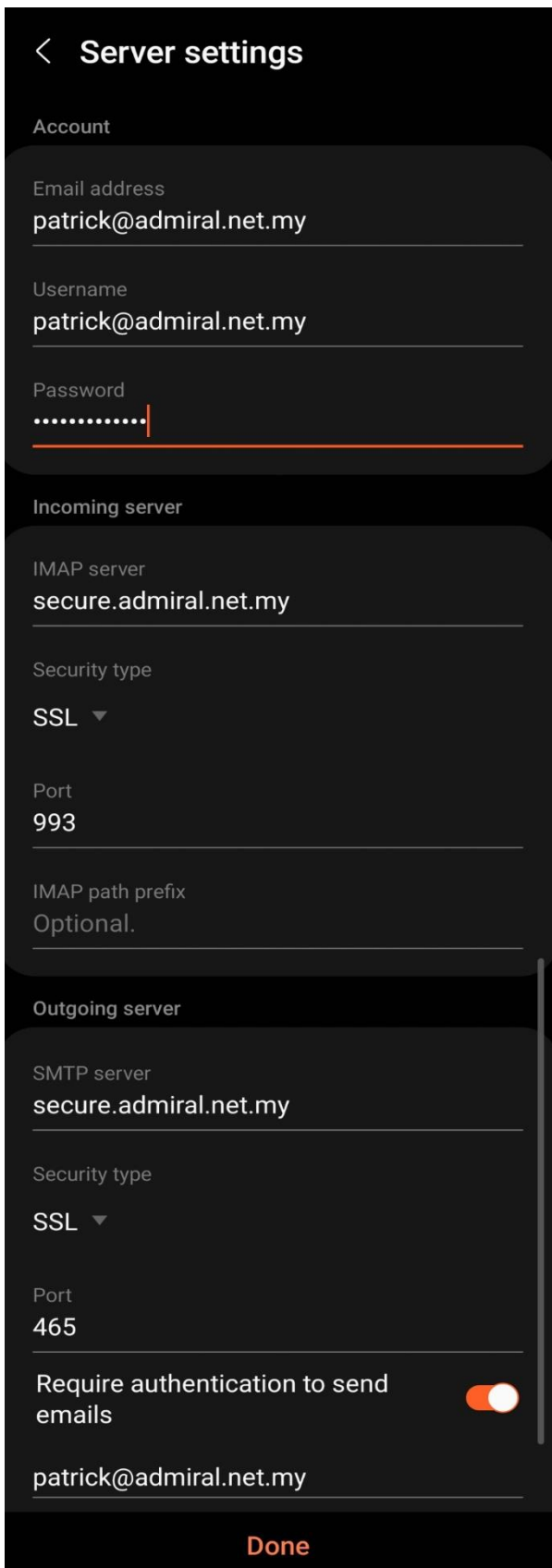
- Check "This server requires an encrypted connection (SSL/TLS) and you will notice Incoming server (POP3) port number changes from 110 to 995 automatically

- Manually change Outgoing server (SMTP) port to 465

- Manually change "use the following type of encrypted connection to "SSL/TLS"

- Click **OK** to exit the window, then **Next** to test receiving and sending then **Finish** to exit.

*It is advisable to check on Leave a copy of message on server and remove from server after 14 days, but this does not affect email security.



Devices using IMAP

Due to various mobile devices operating system variation and versions, we will provide the general settings required to connect to our server securely.

Below settings apply to all Android and iOS devices as well as Windows devices that wishes to use IMAP.

- Username requires your full email address
- IMAP server MUST be changed to secure.admiral.net.my
- Security Type: [SSL](#)
- Port: [993](#)
- SMTP server MUST be changed to secure.admiral.net.my
- Security Type: [SSL](#)
- Port: [465](#)
- Require authentication to send emails must be [enabled](#)

TARGET FULL TRANSITION: 31ST OCTOBER 2022

Current unsecured POP3, SMTP and IMAP will be disabled