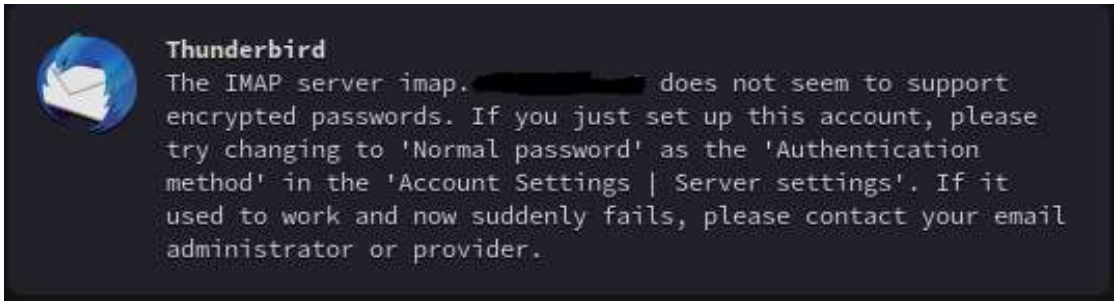
Email Authentication Update

DIGEST-MD5 and CRAM-MD5

You may have heard these terms in the past regarding mail. It is known as “Encrypted Password” in Thunderbird and other clients when setting up accounts. We will be deprecating this authentication mechanism in the not so distant future, and clients will need to be updated with the correct mechanism. If clients are not updated, They will see an error message similar to this. Mail will not continue to work until action is taken.

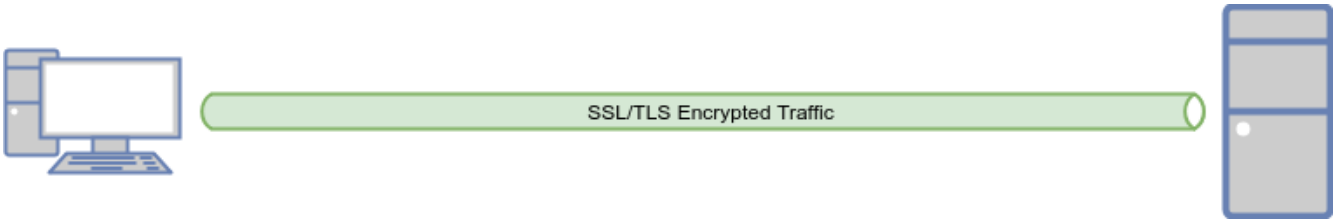



Why is this change necessary ?

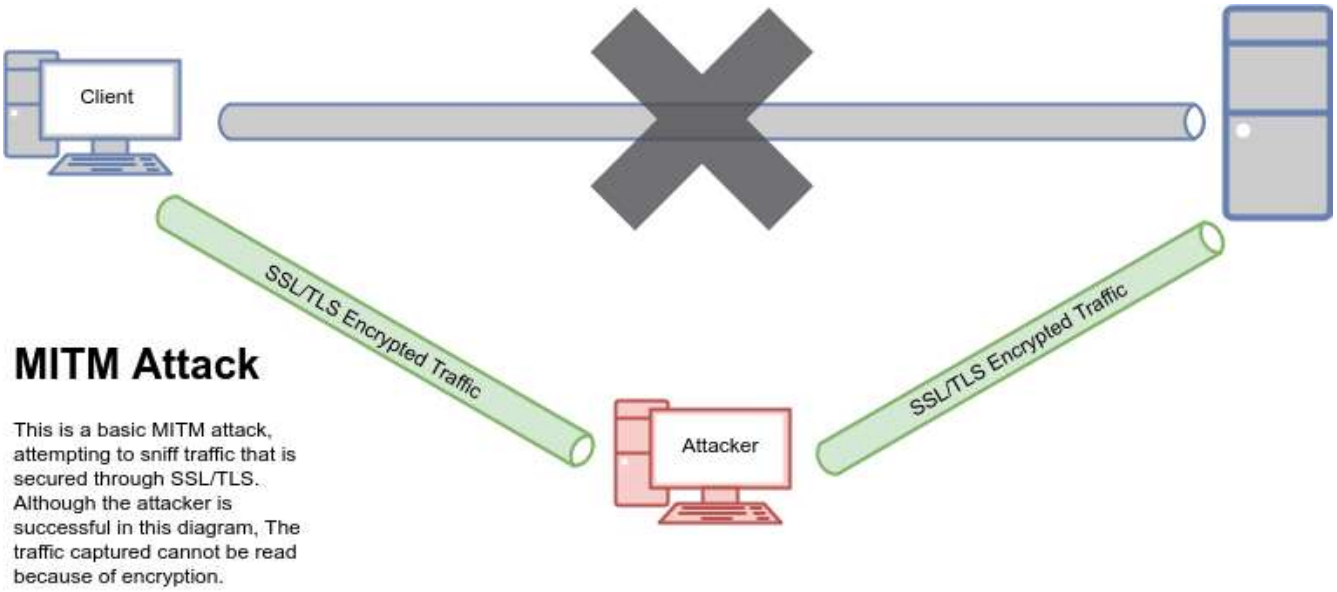
A Brief History

Before SSL/TLS was viewed as a standard for secure transportation of sensitive information, A more secure way to transfer usernames/passwords over the internet was needed. Around this time, the MD5 hashing scheme was considered secure. The amount of technology that was available was not sufficient enough to correctly ‘guess’ what this hash might be, but things have changed throughout the years. Currently, by the time you finish reading this sentence, a standard computer could have guessed millions of different combinations. In short, MD5 is deprecated. It is not a secure hashing algorithm. PLAIN or LOGIN over TLS is the preferred method.

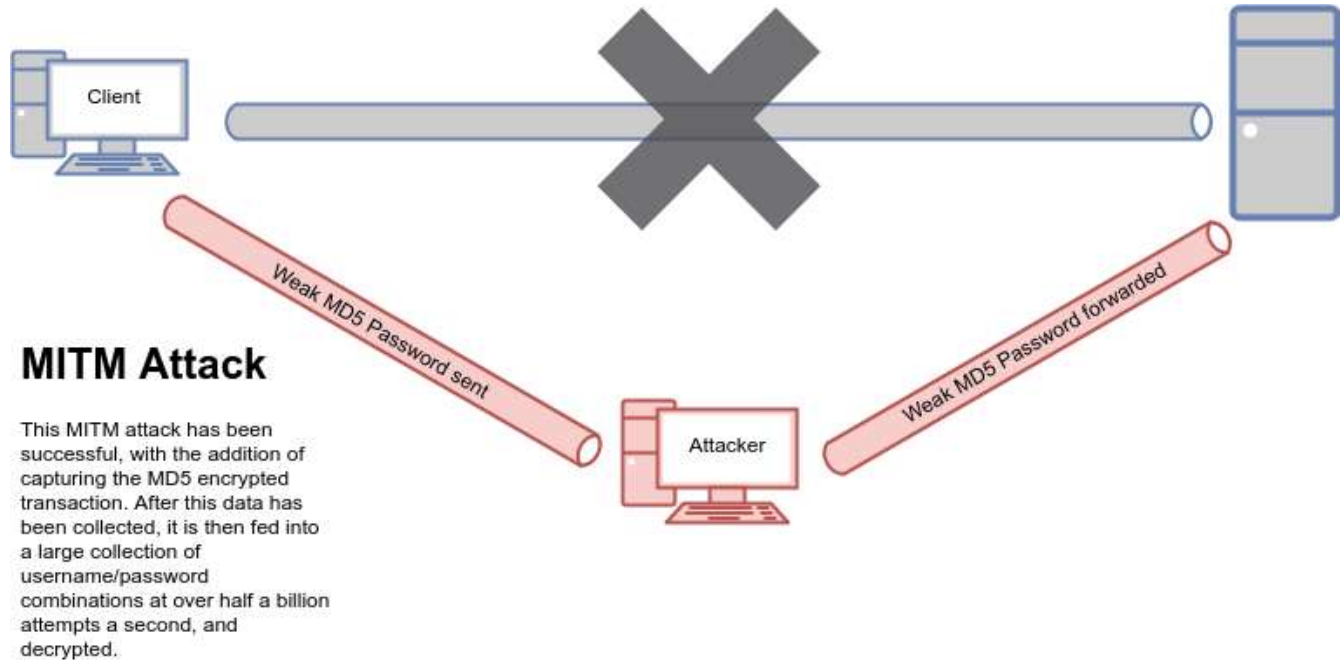
Hackers can preform what is known as a “MITM Attack”, (Man in the middle attack). This is done by placing a new connection between you and the remote server, where your machine will send data to the attackers machine rather than the correct location, to which then the attacker will forward that data to the correct location. The reason for this is to analyze the traffic which is coming from your device. Below is a normal connection. Your client connects to the remote server, and it is not altered in any way.



When an attack is in place, This connection is broke, and data is now sent to the attacker, which is then forwarded to the remote server. Refer to the image below:




As noted in the above image, This attack was successful, however, the data collected from the hacker is useless, as it is protected with SSL/TLS encryption.




This attack, however, has DIGEST-MD5 in place, with no SSL. The data is not encrypted, however the password sent is. But remember, MD5 is extremely deprecated.

As noted in the above image, The MD5 hash of the password is extracted, and decrypted within seconds.

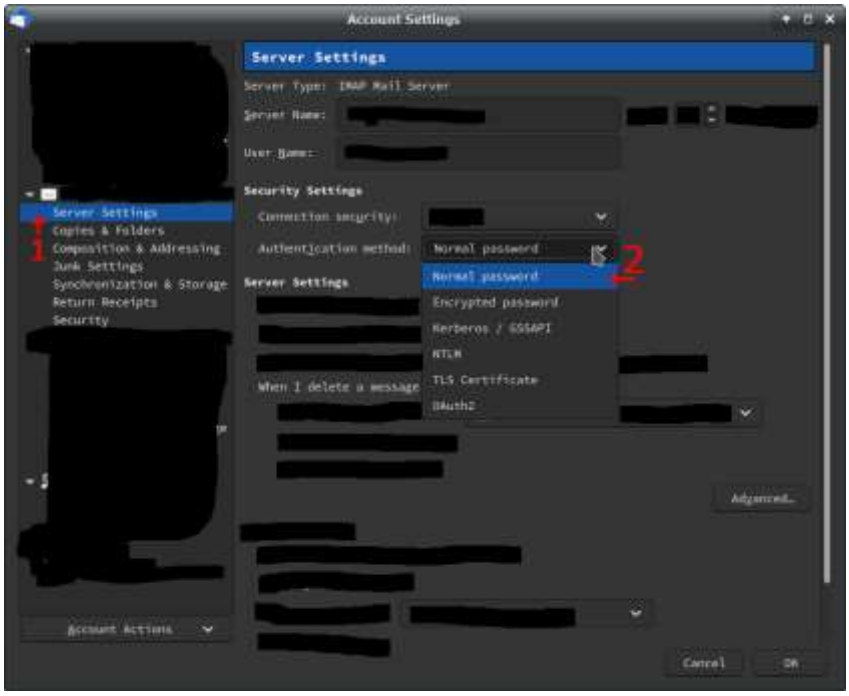
To further the cause of deprecating and disabling the use of MD5, a quick quote from Wikipedia states:

- "Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities."

Kleppmann, Martin (April 2, 2017). *Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems* (1 ed.). O'Reilly Media. p. 203.

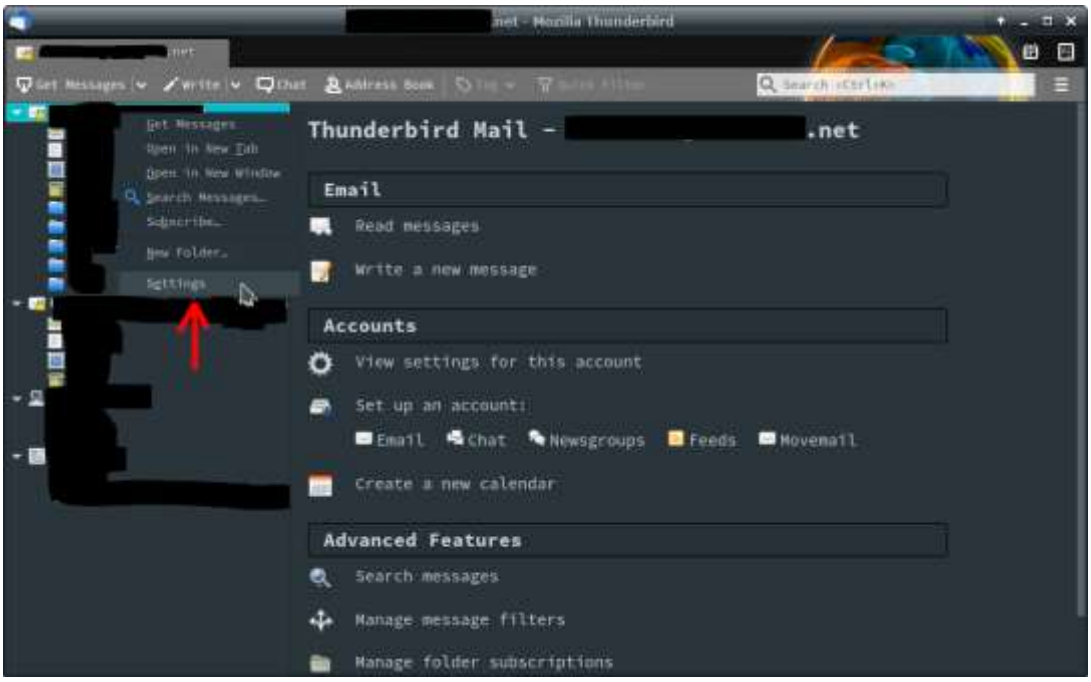
How to reconfigure clients to use PLAIN is shown below.

Thunderbird:
These steps assume the account is setup to use "Encrypted Password" (See attached image, Step 2)
Begin by right clicking on your email address in the left pane and select 'Settings'.
This will open up the 'Account Settings' Pane.
Click on Server Settings (1)
Choose 'Normal Password' under 'Authentication method' (2)
Click 'OK'.

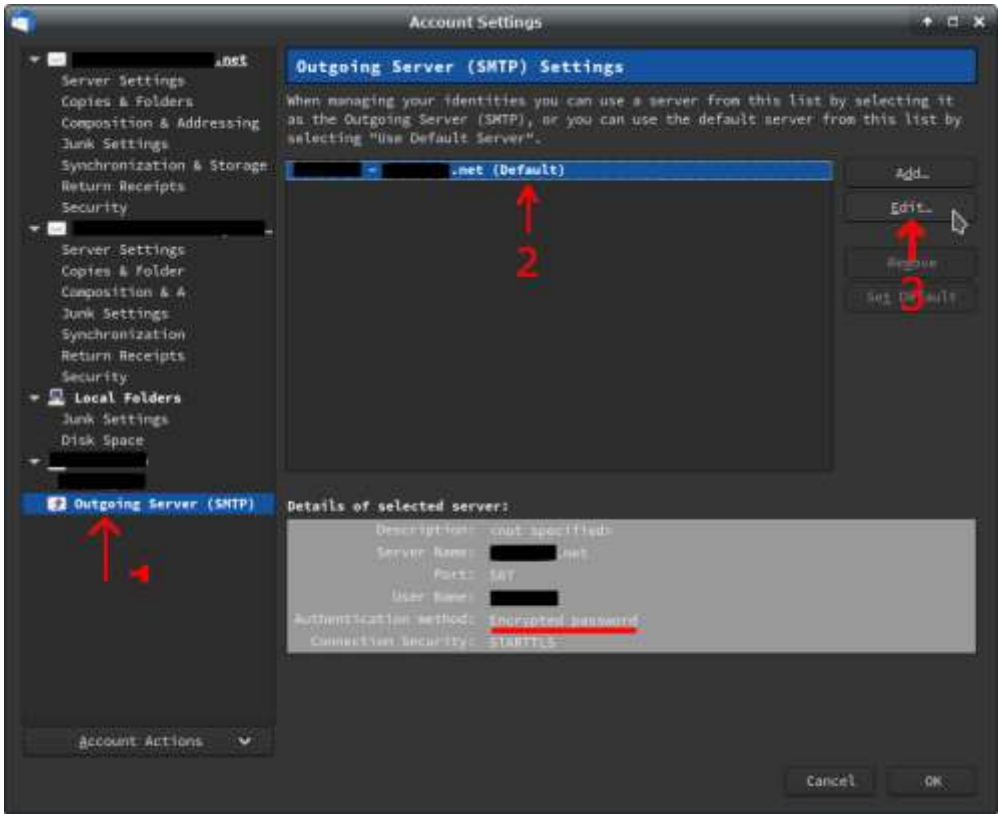



You should not lose any mail in this process.

Outgoing settings maybe configured to use MD5 as well. To check and disable this, Right click on the account and choose “Settings”




Once the account settings are open,
Click “Outgoing Server (SMTP)” (1), click your configured outgoing server from the list (2), and and click “Edit” (3).

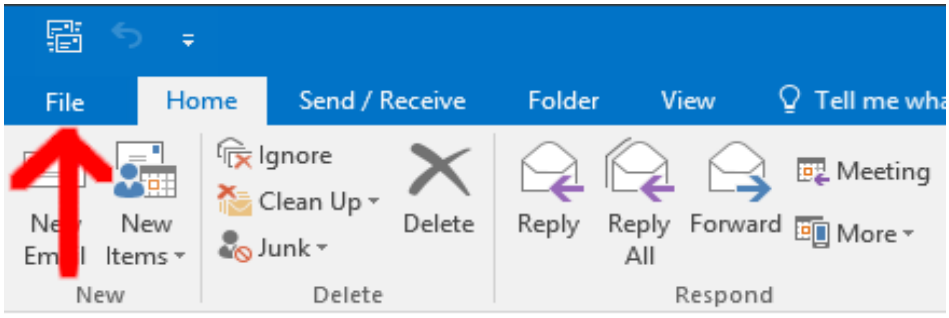


This will open up the SMTP server settings. Under "Authentication method", Choose "Normal Password". Click "OK", and the account will be configured correctly.

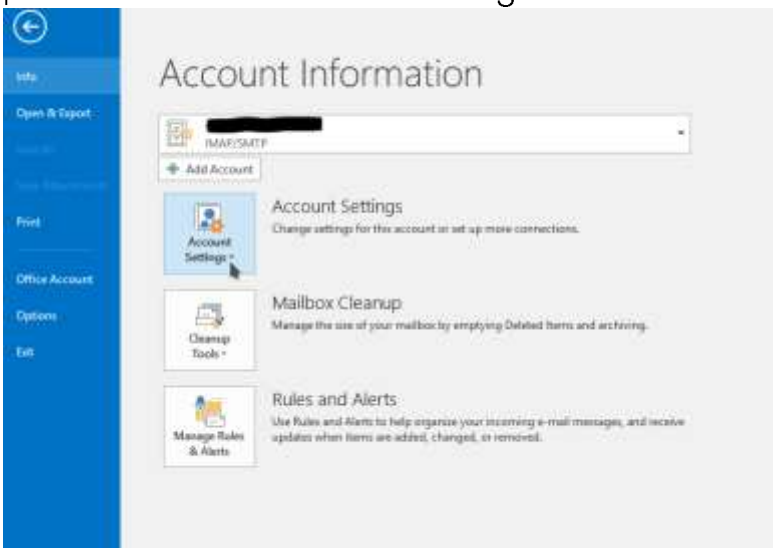

## Outlook:

With Outlook, If the email server is advertising the use of CRAM-MD5 or DIGEST-MD5, it will always favor this choice, no matter if you choose to not force "SPA" (Secure Password Authentication). These steps should be taken *after* the mail server has been reconfigured to not advertise CRAM or DIGEST-MD5. These steps are also assuming the checkbox labeled "Require Secure Password Authentication" has been checked when the account is set up. If this checkbox has not been checked, Outlook should fall back to PLAIN.

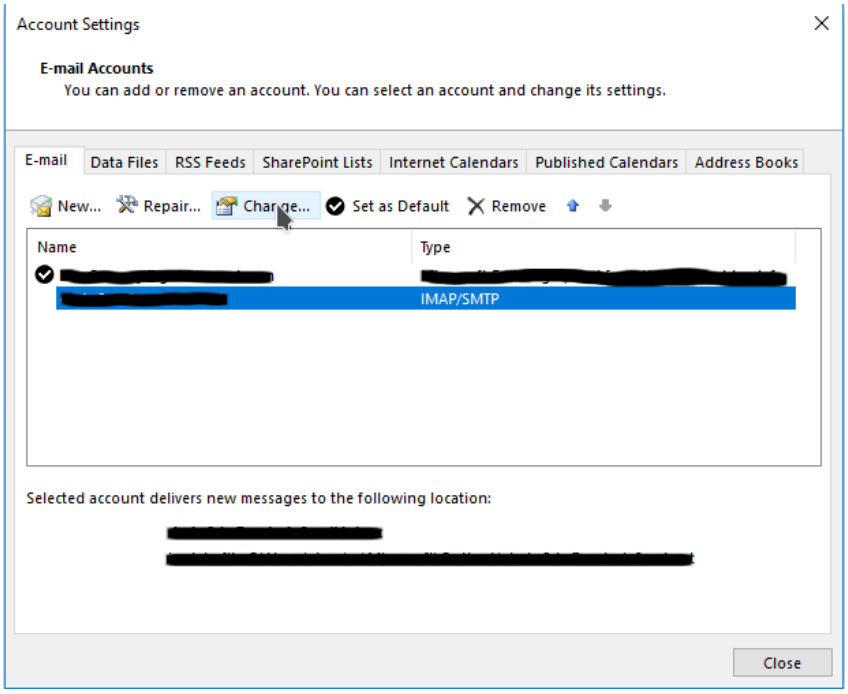
Begin by modifying the settings of your account by clicking File in the top left corner:



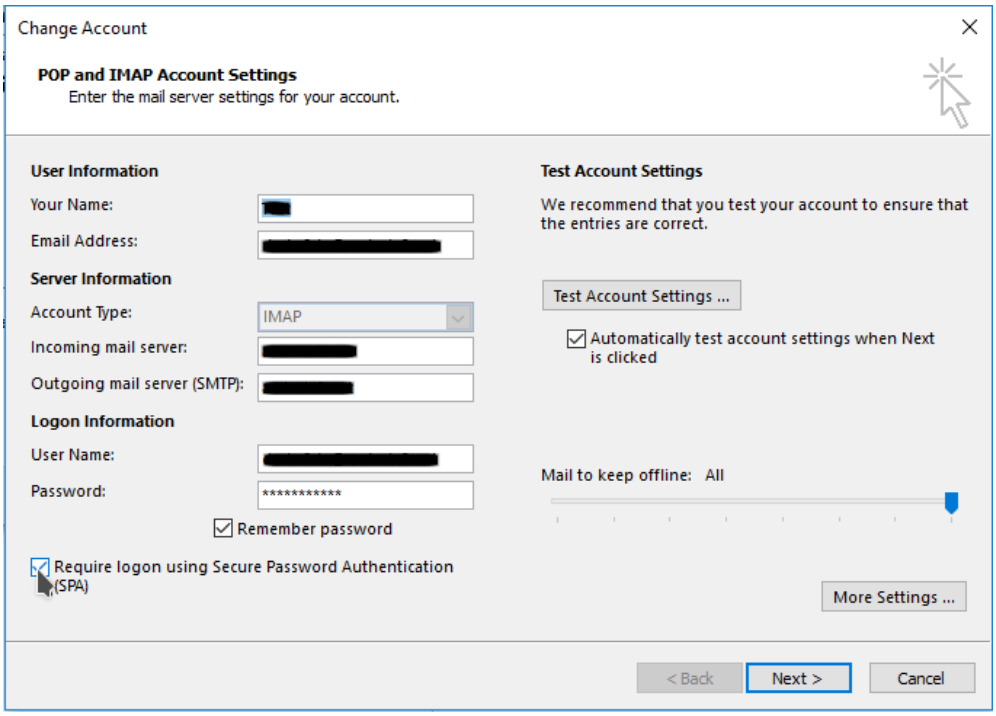

Click on the drop down menu of "Account Settings":



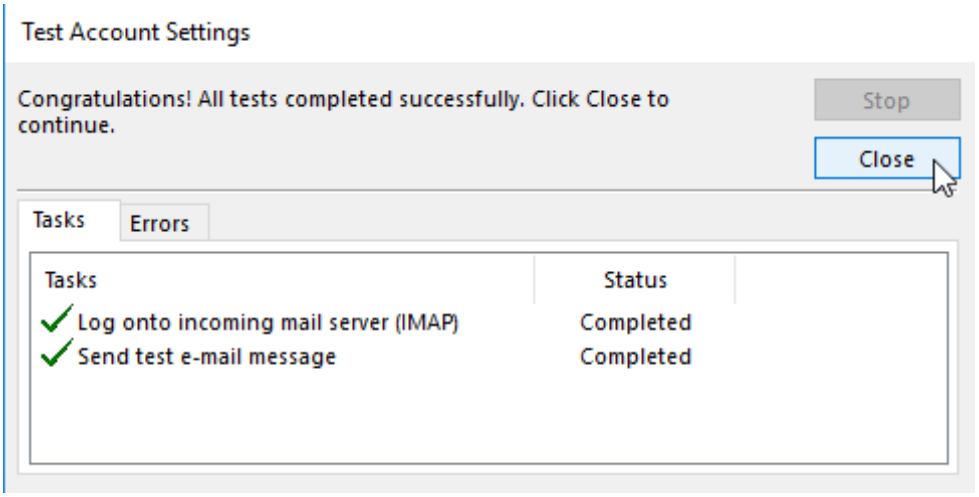
This will reveal the “Account Settings” pane. Click on “Change”




This will open up the “Change Account pane. Uncheck the “Require logon using Secure Password Authentication” checkbox.



After clicking next, Outlook will retest the account, without the use of CRAM or DIGEST.
If the update was successful, You will see green checkmarks next to the following tests:




## Windows Mail:

This client should not have any issues with the transition, As it appears to reconfigure itself based on what the mail server is advertising.

## Incredimail:

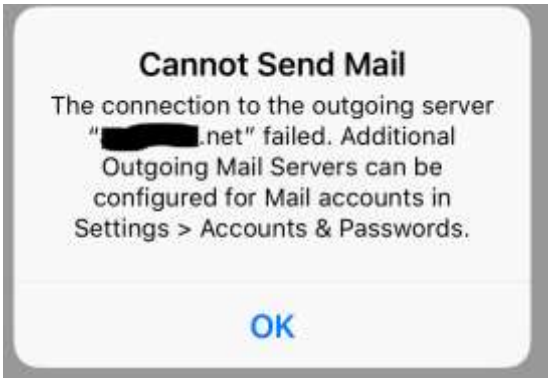
This client should also have no issues with the transition, As it appears to fall back to using PLAIN when MD5 of any type is advertised.

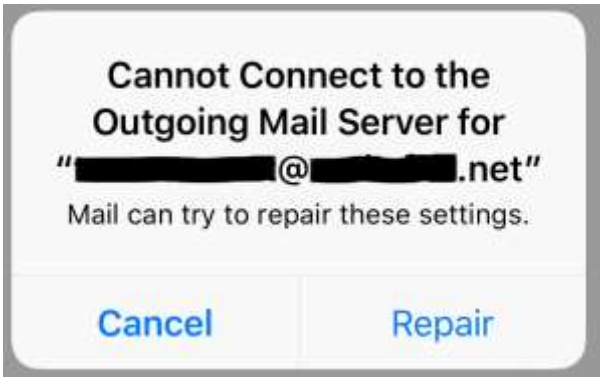
## IOS Mail:

iOS Mail should have no issues with this transition, As it takes an explicit step to enable MD5.
If MD5 was enabled for any reason, Some symptoms could include the following:

If messages such as this appear, Ensure that MD5 is not being used.

After the “Repair” button is clicked, Nothing appears to happen. Until the “Cannot Send Mail” prompt appears.




To ensure MD5 is not being used for *outgoing* settings, Begin by opening the account in iOS by tapping "Passwords & Accounts" under "Settings".


Tap the account that is having trouble connecting:

Tap “SMTP” under “Outgoing Mail Server”:


Tap the primary server under the “Primary Server” Header

This will pull up the primary settings for the outgoing mail server. Tap “Authentication”.


Select “Password” from this list. The account is now configured to not use MD5 for authentication.