

---

# IT Knowledgebase

SoM E-Mail Category

---

# Contents

<b>SoM E-Mail</b>	<b>1</b>
<i>How to view/share a SoM e-mail calendar</i>	1
<i>I am unable to receive email from a sender</i>	1
<i>Tumbleweed Secure Messaging Service</i>	2
<i>What do I do if I receive an email asking me for my user ID and password?</i>	2
<i>What happens when a mailbox exceeds the mailbox quota limit?</i>	3
<i>What is Outlook Web Access (OWA)?</i>	4
<i>What is the email quota limit on the SoM mail servers?</i>	4
<i>Whitelisting emails or domain names</i>	4
<i>WSUSOM MailScanner Quarantine</i>	5
<i>Android Mail (Basic) Setup for SoM Exchange</i>	7
<i>How to setup secure POP Email?</i>	18
<i>How to AutoArchive email with Microsoft Outlook</i>	19
<i>Mac Mail for OS 10.5.x (Leopard) - POP Account Type</i>	20
<i>Modify Junk Mail Settings in Microsoft Outlook 2003</i>	22
<i>Remove Previously Used Names/Addresses from Microsoft Outlook</i>	23
<i>SoM E-Mail setup on iPhone &amp; iPad</i>	23
<i>Blocked Email Attachment Types at the SoM</i>	25
<i>I received an email to my @med.wayne.edu account saying I sent a virus to someone.</i>	27
<i>How to forward WSU email to SoM Email</i>	27
<i>Microsoft Windows Outlook 2007/2010 - External E-Mail Setup for SoM</i>	28

# SoM E-Mail

## How to view/share a SoM e-mail calendar

If you have an Exchange Mailbox, you can allow other users to access your entire calendar or selected calendar items. To share your calendar and its items, you must set permission levels for various users. In most cases, permissions are set by using built-in roles, but you can also set custom permissions for the rare cases when the built-in role does not fit the situation. Some permissions allow users to view your calendar; others allow users to add or even edit

items.

Permission	Description	Owner
The Owner	role gives full control of the folder. An Owner can create, modify, delete, and read folder items; create subfolders; and change permissions on the folder.	Publishing Editor
The Publishing Editor	role has all rights granted to an Owner, except the right to change permissions. A Publishing Editor can create, modify, delete, and read folder items and create subfolders.	Editor
The Editor	role has all rights granted to a Publishing Editor, except the right to create subfolders. An Editor can create, modify, delete, and read folder items.	Publishing Author
A Publishing Author	can create and read folder items and create subfolders but can modify and delete only folder items that he or she creates, not items created by other users.	Author
An Author	has all rights granted to a Publishing Author but cannot create subfolders. An Author can create and read folder items and modify and delete items that he or she creates.	Nonediting Author
A Nonediting Author	can create and read folder items but cannot modify or delete any items, including those that he or she creates.	Reviewer
A Reviewer	can read folder items but nothing else.	Contributor
A Contributor	can create only folder items and cannot read items.	None
The None	role has no access to the folder.	

If you would like to give a person permission to access a folder in Outlook, you need to give the person permission to access each Folder/Subfolder you want to share. The process for sharing your Calendar, Mailbox and your Individual folders is the same. To set Share Permissions on your calendar, Open the Calendar Properties - Permissions window by doing one of the following: In the Folder List Navigation Pane, Right-click the Calendar folder and select Sharing from the pop-up menu. In the Calendar Navigation Pane, under My Calendars, Right-click your Calendar folder and select Sharing from the pop-up menu. Select the Permissions tab. Select the Add button. Select the person you wish to give permission to from the address list and press the Add button. Press the OK button. Click on the person's name and select the appropriate permissions from 'Permission Level:' drop down list. (e.g., Owner, Editor, Author...) Click the OK button. To share additional folders/subfolders, right-click on the folder or subfolder and follow steps 1-7 above.

Once the permissions are set, you will also want to make sure the mailbox is visible. In the folder list, right click on Mailbox - Last Name, First Name. Select Properties. Select the Permissions tab, and click Add. Add the user you wish to grant access, and click OK to continue. In the Permissions section, make sure that Folder Visible is checked.

Note: This will not grant the user access to your email, this just makes sure that the outlook folder is visible so they are able to see the Outlook Calendar.

How to View a shared calendar/folder:

Before you are able to access another user's folder (calendar, Inbox...) they must give you access to them. (See how to set Permissions above.) Select Tools | Email Accounts and then select View or change existing e-mail accounts. Click on the Microsoft Exchange Server and then select Change. Click the option for More Settings. A window will now appear that contains Microsoft Exchange Server settings. Click on the Advanced tab. Click the Add button to Open these additional mailboxes. Type the name or the SoM ID of the mailbox you have permission to access. Click OK to continue. The mailbox will now show up in the list. Click Apply and OK to close the window. Click Next to continue. Click Finish to close the email accounts wizard.

Note: the mailbox will now show up in your folder list.

## I am unable to receive email from a sender

Question: I am unable to receive email from a sender to my @med.wayne.edu address.

Answer: In order to troubleshoot email delivery issues, MSIS needs detailed information.

One of the more frequently asked questions received by the MSIS Helpdesk is mail did not arrive from a sender. In order to troubleshoot email delivery issues, MSIS needs the following information: Email address of the sender Date and approx. time the message was sent

---

The email server logs only go back 14 days. If the message was sent longer than 14 days ago, the sender should attempt to resend the message.

Please note: If a sender received a bounced message when trying to send email to an @med.wayne.edu address, they should be reporting the problem to their email administrator or postmaster to initiate investigation with the SoM postmaster. Based on past investigations, the stats still remain that nearly 98% of every issue reported to the MSIS Helpdesk is due to a problem with the sender's email system - many times of which is due to misconfigurations or non-compliance to the SMTP protocol RFCs.

## **Tumbleweed Secure Messaging Service**

What is it? Tumbleweed Secure Messenger is an e-mail delivery solution that gives you the reliability, security and privacy not possible in most email clients. Tumbleweed allows School of Medicine email users to send secured e-mail messages to external addresses and allows you to track the status of the message delivery. This tool works in coordination with your Outlook email client and Exchange email system to provide a simple way to send secured messages to addresses outside the School of Medicine email environment. Internal email communications do not use this tool as all internal email is encrypted and protected by default.

Why use it? If you need to ensure a message sent to an external address is secured throughout the e-mail delivery process, this tool provides that ability. Anytime protected health information (PHI) as defined by HIPAA is sent via e-mail to an external address, you MUST use this tool to ensure that information is encrypted as it's sent.

How do I use it? To send an e-mail or file attachment securely to an external e-mail address, using your standard Outlook e-mail client, you will need to add {secure} (including the brackets) to the subject of the e-mail message (e.g. {Secure} Top Secret Email). When you click the send button, the Exchange e-mail server will transfer the message automatically to the Tumbleweed service which will then send out the message securely to the external addresses. After the message is sent from Tumbleweed, you will receive a delivery status notification to your @med.wayne.edu account. All messages stored on Tumbleweed will expire in 30 days of the message being sent. When the recipient replies to your message, you will receive that reply in your Outlook Inbox as you would any other standard message. The process is relatively transparent to an internal School of Medicine user. Only the external recipients will see a difference in how they are communicating with you using this tool.

If you have a personal e-mail account outside the School of Medicine system you can test this process by sending your personal account a secure message using the above instructions.

Please note: Only e-mail sent from the School of Medicine Exchange system (example: Outlook XP/2003; Entourage for Macintosh), or using smtp.med.wayne.edu as the SMTP server when connected to the School of Medicine Network is routed through Tumbleweed.

When the message is received by an external e-mail account, the user will see a message similar to the one below:

When the "View Message" button is pressed, the user will automatically be taken to a secure web site to retrieve the message as shown in the below screenshot. A login ID and password is not required because the link is unique for each message sent using the Tumbleweed Secure Messenger service.

Please Note: At this time Internet Explorer 6.0 and above for PC and Safari 2.0 for Macintosh are the only supported Internet browsers.

## **What do I do if I receive an email asking me for my user ID and password?**

---

The MSIS helpdesk has recently seen an increase in phishing attempts. "Phishing" is an attempt to criminally and fraudulently acquire sensitive information, such as usernames and passwords, by masquerading as a trustworthy entity via an email message. The most recent attempts to steal login information are messages that appear as if they are being sent from computer support teams &ndash; below is an example:  
----- Original Message -----

From: XXXX  
Sent: Tuesday, March 18, 2008 7:41 PM  
To: undisclosed-recipients  
Subject: Update YOUR WAYNE EMAIL NOW .

Dear wayne.edu Email Owner,  
This message is from wayne messaging center to all wayne email  
Email owners. We are currently upgrading our data base and  
e-mail center. We are deleting all unused wayne email  
to create more space for new one.

To prevent your account from closing you will have to update it  
below so that we will know that it's a present used account.

CONFIRM YOUR EMAIL BELOW  
Email Username : .....  
EMAIL Password : .....  
Date of Birth : .....  
Country or Territory : .....

Warning!!! Email owner that refuses to update his or her  
Email, within Seven days of receiving this warning will lose his or her  
Email permanently.

Thanks,  
wayne Team  
WAYNE.EDu BETA

-----  
Please note: Support personnel from the School of Medicine or Wayne State C&IT helpdesk will never  
ask for your password. If you receive an email asking to provide your user ID and password,  
immediately delete the message - DO NOT REPLY with your login information.  
If you have replied to a phishing attempt and feel your @med.wayne.edu account has been  
compromised, please follow these steps:  
\*\* IMPORTANT INFORMATION\*\*Reset your SoM password at once! Do NOT use the same password  
as before.  
Contact the MSIS Helpdesk at 313-577-1527 to have your password reset if needed. If you feel your  
@wayne.edu account has been compromised, contact the C&IT helpdesk at 313-577-4778 to have  
your password reset.  
The MSIS Helpdesk will most like monitor these activities over the network. If you account was  
comprised, your SoM Account will be disabled to protect our servers and your information.  
There could be a chance we need to run a Virus scan on your work machine if needed.  
If you need more help, please call us at 577-1527.

## What happens when a mailbox exceeds the mailbox quota limit?

Once the quota on the post office server has exceeded the size limit, mail must be deleted from the  
School of Medicine exchange server - the user will not be able to send any email, and new arriving  
mail will not be delivered.

If a person tries to send a message to a recipient with an @med.wayne.edu address that is over the  
size limit, the sender will receive a bounced message that states:Your message did not reach some  
or all of the intended recipients.Subject:  
Sent: The following recipient(s) could not be reached:Last Name , First Name on The message could  
not be delivered because the recipient's mailbox is full.

The sender may also receive a less detailed bounced message if sending an email from an external

---

mail system:This is an automatically generated Delivery Status Notification.Delivery to the following recipients failed.user@med.wayne.edu

## **What is Outlook Web Access (OWA)?**

Outlook Web Access (OWA) is a service that allows Exchange users at the School of Medicine to access their Exchange mailbox over the Internet from from a PC, Macintosh or Mobile Device. OWA provides basic email functionality through a web interface to a secure site, allowing you to read your email from anywhere in the world without having to reconfigure a browser or email client software.

You can access the OWA website:

<https://owa.med.wayne.edu/> (PC/Macintosh)

<https://owa.med.wayne.edu/oma/> (Mobile Devices)

Please Note: Some features of the Outlook Client are not available in OWA, such as the ability to use the Auto Archive feature.

## **What is the email quota limit on the SoM mail servers?**

Email Quotas exist on the servers to guarantee mail storage for the 5,000+ users of the School of Medicine post office mail system.

The School of Medicine Exchange environment consists of several central shared servers. With the number of mailboxes that exist, which also increase in number everyday, there is not enough disk space for everyone to keep an unlimited number of messages on the server. The current approved limit is 1 Gigabyte for faculty, staff and students - SoM Alumni have a 50 MB size limit.Can I get more than 1 Gigabyte of space?

At this time we do not offer to purchase additional mailbox space at MSIS. When such process is in place, we will duly inform our customers on this matter.

## **Whitelisting emails or domain names**

What is Whitelisting?

Whitelisting refers to a list of e-mail addresses or domain names from which an e-mail blocking program will allow messages to be received.

To whitelist e-mail addresses or domain names, follow the directions below:

- 1) Go to: <http://directory.med.wayne.edu/>
- 2) Search for your SOM user ID or last name.
- 3) Click on your name and you will be taken to your Directory User information page.
- 4) Click on the View or edit Entire Entry (login) button, then log in with your SOM user ID and Password.

5) Find the AntiSpam Options section:

6) To add or delete items click on the icon to the left of the "Edit your white/Black&hellip;"

7) The next screen will take you to your option for whitelist or black list. Type in the email address or domain name.

- a. For email addresses type the full address, for example johnsmith@company.com
- b. For domain addresses type either company.com or @company.com

- 
- 8) If you want to allow email to arrive from that sender or domain, click the Add to whitelist button. If you do not want to get email from that sender or domain, select add to blacklist.
  - 9) When you are done adding senders or domains, select submit change. If you do not want to keep the changes you made, select cancel change.
  - 10) If you want to remove a selection from either list, select the entry you want to remove, then select the arrow that points to the middle column.

11) Select submit change.

If you need Additional help with any of these steps, please contact the MSIS Helpdesk at 577-1527

## **WSUSOM MailScanner Quarantine**

Medical School Information Systems has implemented a MailScanner Quarantine system that allows you to view the messages that are being detected as SPAM by the WSUSOM mail scanners. This system will provide you individual control of what senders and messages will pass through our Spam filters.

By default the WSUSOM MailScanner Quarantine is enabled on your WSUSOM email account. To review the reports directly you can login into <https://mx.med.wayne.edu/mailscanner> . Directions on how to manage this page can be found below. With this capability you have the option to enable a Dailey Spam Quarantine report which is sent to you via email . To enable this you will first log into the SoM Online Directory by going to <https://directory.med.wayne.edu/you/login.cfm?user> and you will see this page.

Once you have entered your SoM username and password, you will now be viewing your directory information.

Note: Click on the

icon next to any of these fields to edit/update your information.

Under your AntiSpam Options, you have three options. You can Enable/Disable the Daily Spam Quarantine Report from being sent to your email. This option will send you an email when the SpamChecking system blocks or quarantines email that is potential spam. This email is sent around 5:30am only if an email has been quarantined for the previous 24 hour period. Click on the "Check quarantine" link to take you directly to the MailWatch site. (which will be covered later) Click on the

icon to edit your whitelist or blacklist settings. For directions on how to edit your whitelist or blacklist settings go to the following article: [Whitelisting emails or domain names.](#)

How to Enable the Daily SPAM Quarantine email report

To activate the Dailey SPAM quarantine email, check the box, "Enable Daily Spam Quarantine report to your address or Check quarantine directly". You will be taken to the following screen which will give you a brief description about how it works. When you are at this screen, click,

---

&ldquo;Submit Change&rdquo; and it will take you back to the directory page.

Once you have done this, click on &ldquo;Review/Change your entry again&rdquo; and you will be returned back to your directory entry edit page.

At this point, you have activated the report function and will be notified IF a spam or potentially harmful email is blocked by the system.

How to Manage the Daily Quarantine Report Email

In the event that mail is blocked, you will receive an email very similar to the following screen shot. This will give you a brief overview as to the sender, time sent, subject, and the reason it was blocked. You will ONLY receive this email in the event that one or more emails were blocked or quarantined from the system. If you do not receive a quarantine report email, no messages were blocked.

If you click on &ldquo;View&rdquo; to the right of the subject line, you will be taken to the MailWatch system and prompted for your School of Medicine credentials. Once logged in the following detailed information page will be displayed.

Here, you will be able to either: Add to whitelist (which will allow this sender&rsquo;s email through these filters in the future). Add to blacklist (which will block messages from this sender in the future). Release the message (which will pass it on to your inbox, delete the message which will delete it from this system). View more message details which will take you to the full detailed view of the message which was outlined earlier in this article.

Using The MailWatch Page by going to <https://mx.med.wayne.edu/mailscanner>

MailWatch &ldquo;Recent Message&rdquo; tab

Once logged into the MailWatch page the default page is &ldquo;Recent Message&rdquo;. The recent Message page displays a color coded view of the last 200 messages and their score. Just as explained earlier in this article, you can click in the middle of the &ldquo;[ ]&rdquo; for a more detailed view of that message.

You will notice there is a key at the top defining the color codes related to the various types of messages based on their score. This window will show you both messages that have been passed to your inbox (marked

in color if they were clean), as well as messages that have been blocked for various reasons as described and color coded based on the color codes key.

MailWatch &ldquo;List&rdquo; tab

If you click on the &ldquo;Lists&rdquo;, it will display a similar window to this one below that displays your whitelist and your blacklist. You can add or remove addresses or domains to either list in this window.

MailWatch &ldquo;Quarantine&rdquo; tab The &ldquo;quarantine&rdquo; page displays the messages that were either blocked or quarantined. You will be looking now at a screen that is very similar to this one.

---

Once you click on the folder it will display the items that were blocked for that given date. These items are color coded (refer to the key at the top of the screen) for why the message was blocked. Each line will have the details about the message and why it was blocked or quarantined.

In the left most column, if you click in the middle of the " " , it will take you to a detailed view of the message that you selected. In this area, you will see the detailed mail view which will look similar to this. Just below the "Logout" button, you can add the sender of this specific email to the whitelist or blacklist. If you whitelist the sender, that address will bypass the mail filters in the future. If you blacklist the sender, it will block all emails from this sender in the future.

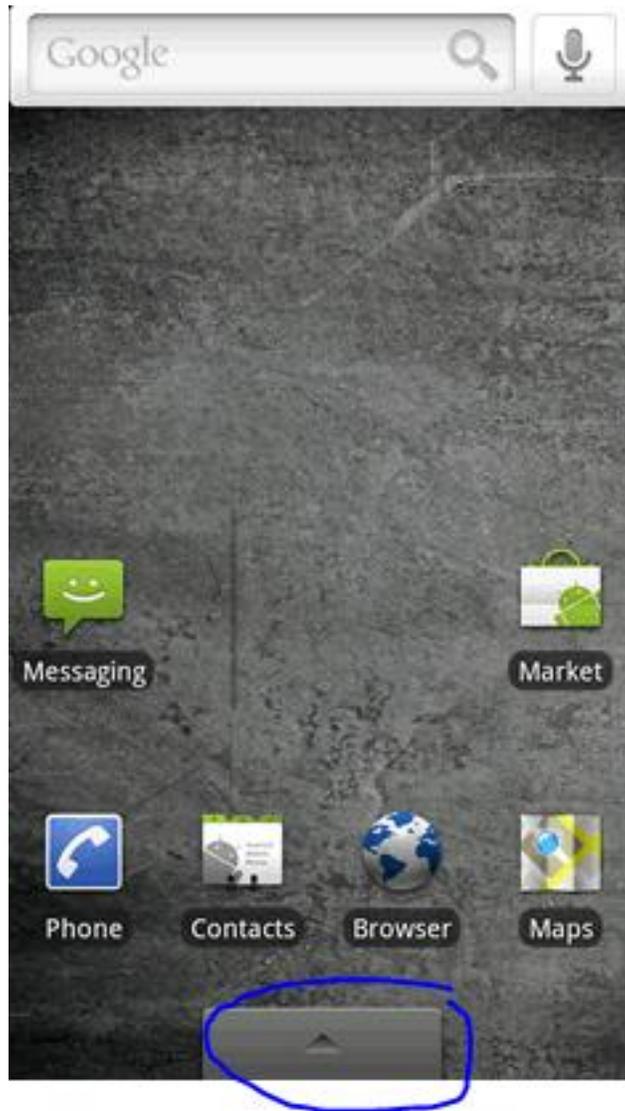
MailWatch "Tools/Links" tabOnce you click on the "Tools/Links" tab, it will display window which will allow you to click on User Management or various informational links regarding the mail system and other email information sites.

Under User Management, you will be looking at a similar screen to this one. You can enable or disable email notification from this system of blocked or quarantined emails as well as being able to change the Quarantine Report Recipient. This will allow you to change the address in which this report is sent to if you desire to do so.

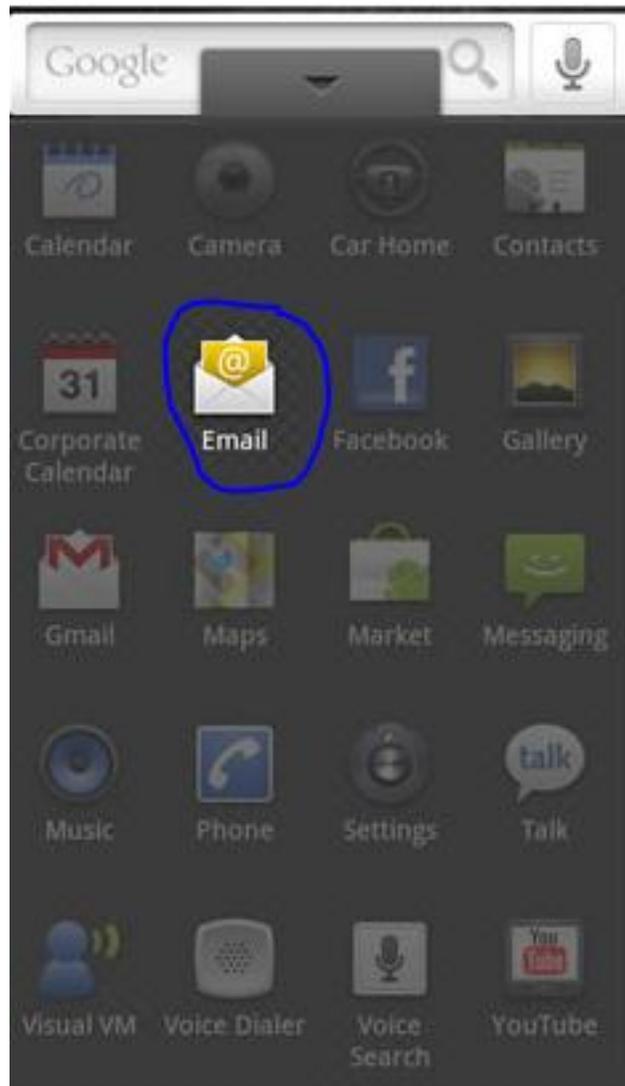
## **Android Mail (Basic) Setup for SoM Exchange**

All Droid devices will have this client and it's the default one. These instructions were designed for the Motorola (MOTO) model. They all have the same appearance so these steps should work for most Droid devices. This is a very slim version for Exchange and it's quite limited and what it can do. For SoM and especially for heavy email users, we will not recommend this setup. For heavy email users, we would instead recommend installing Touchdown from the Android Market.

Setup From the home screen, touch the applications tab (located on the bottom of the screen).



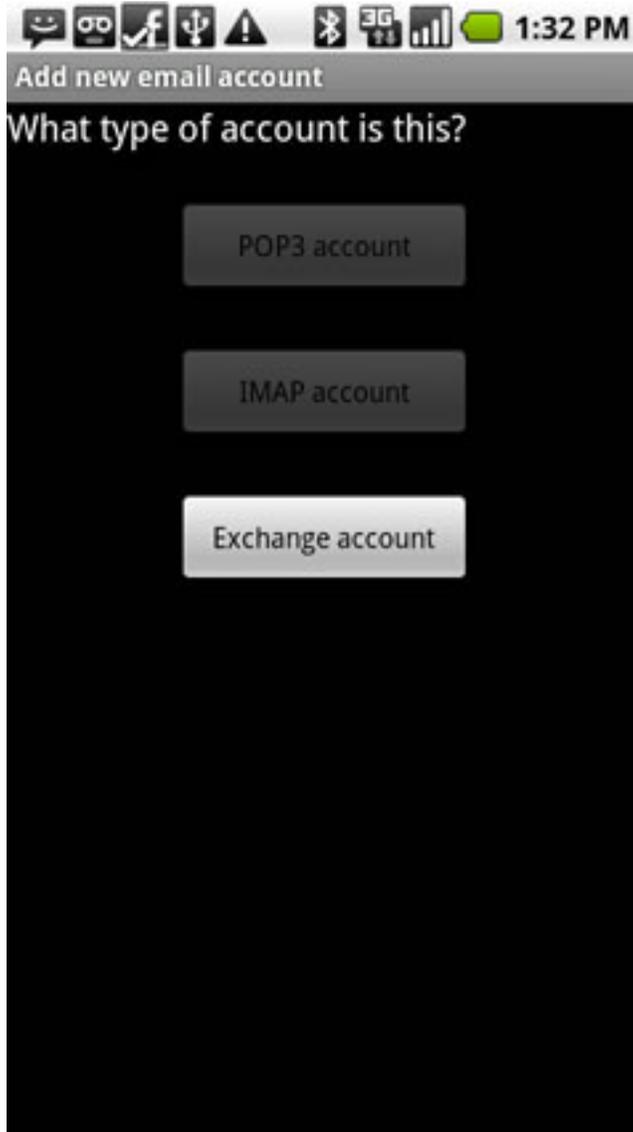
Touch Email.



Enter the exchange email address and password then touch Next.

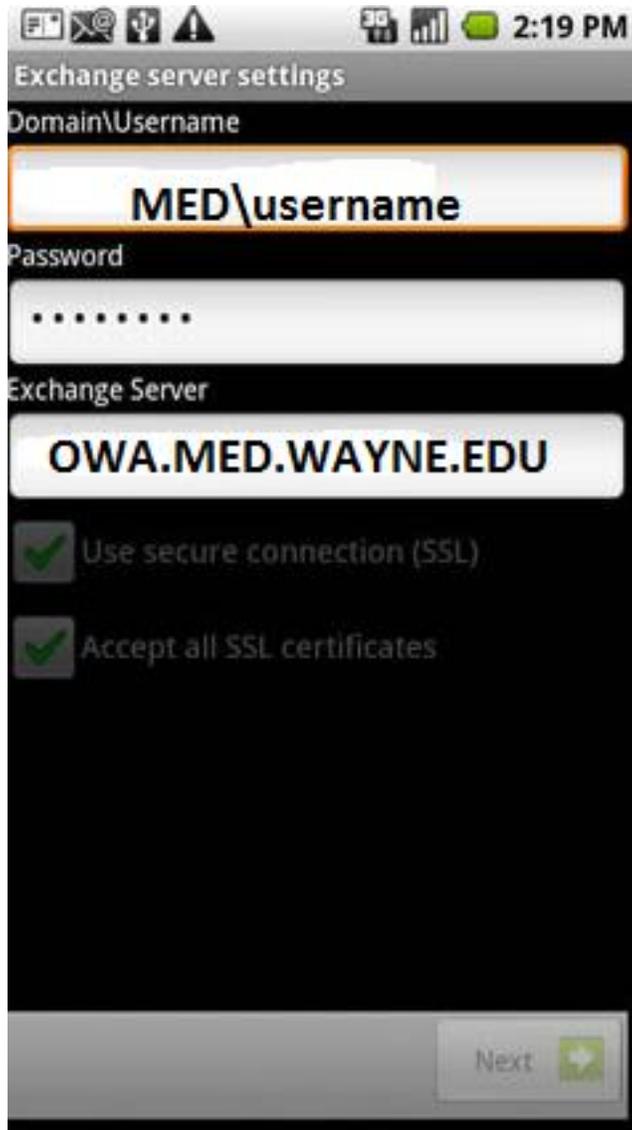


Touch Exchange account.

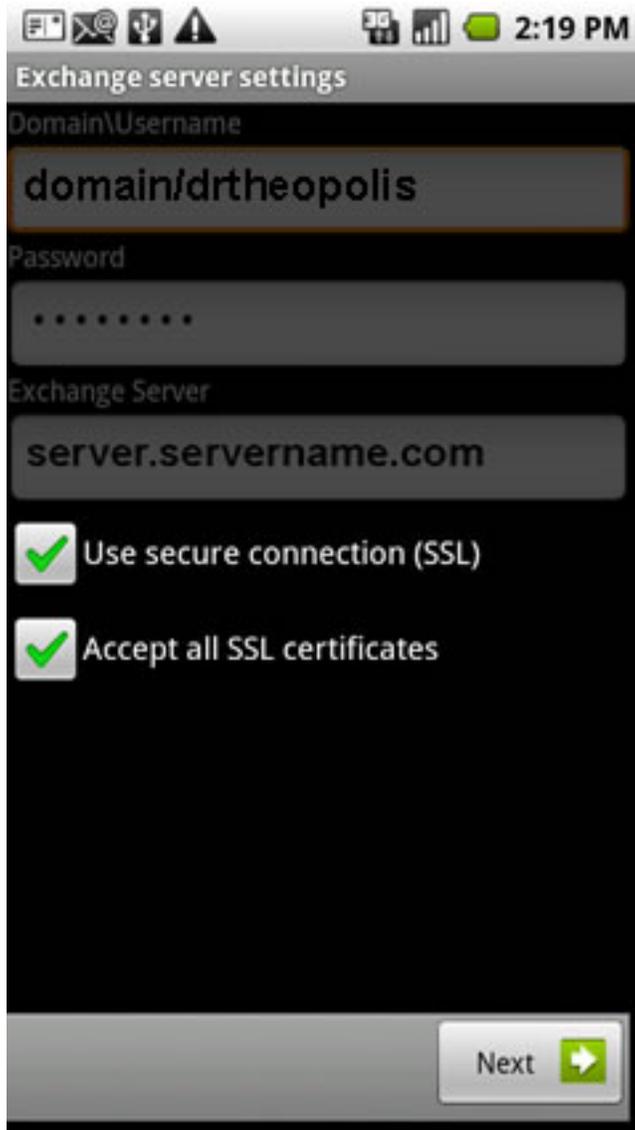


Enter the exchange server settings in the appropriate fields:

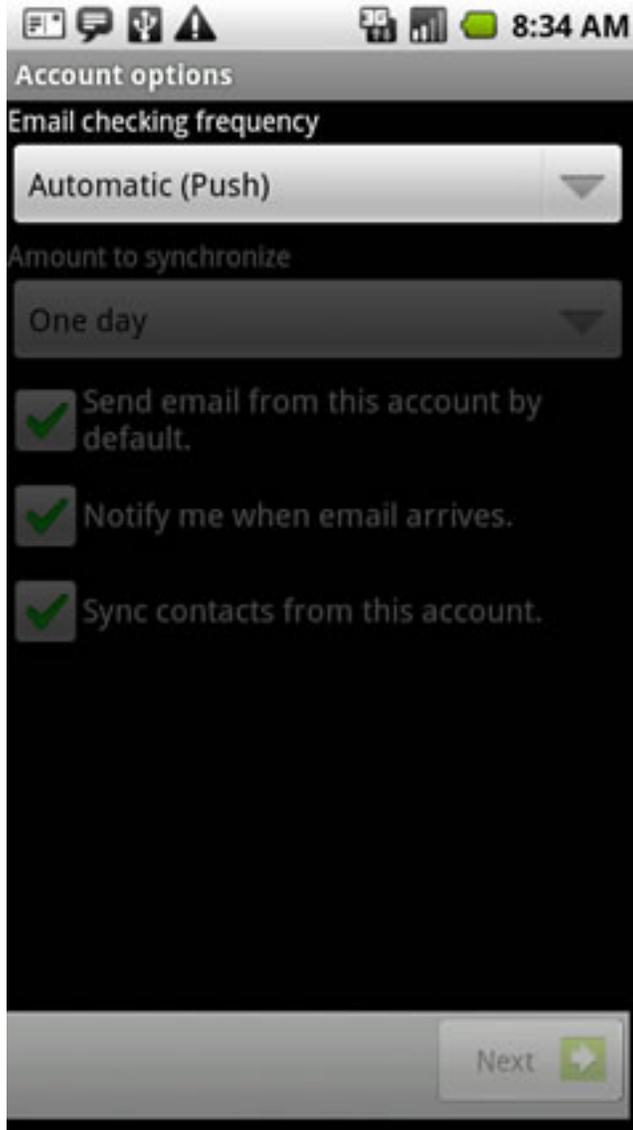
Domain\username  
Password  
Exchange Server



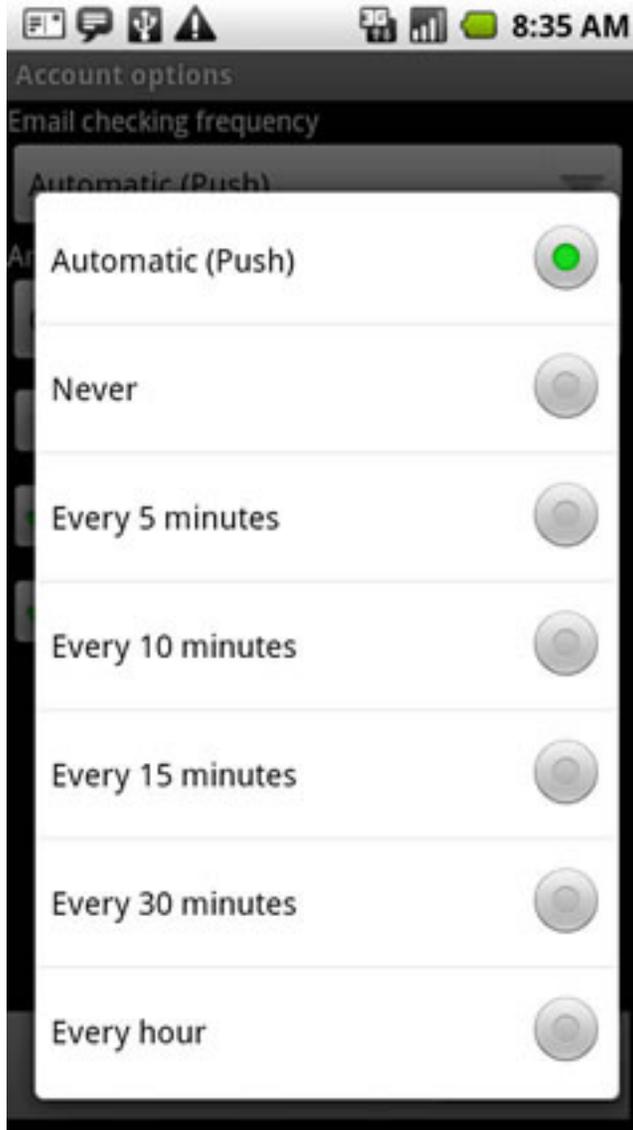
Use secure connection (SSL) and Accept all SSL certificates are checked then click Next.



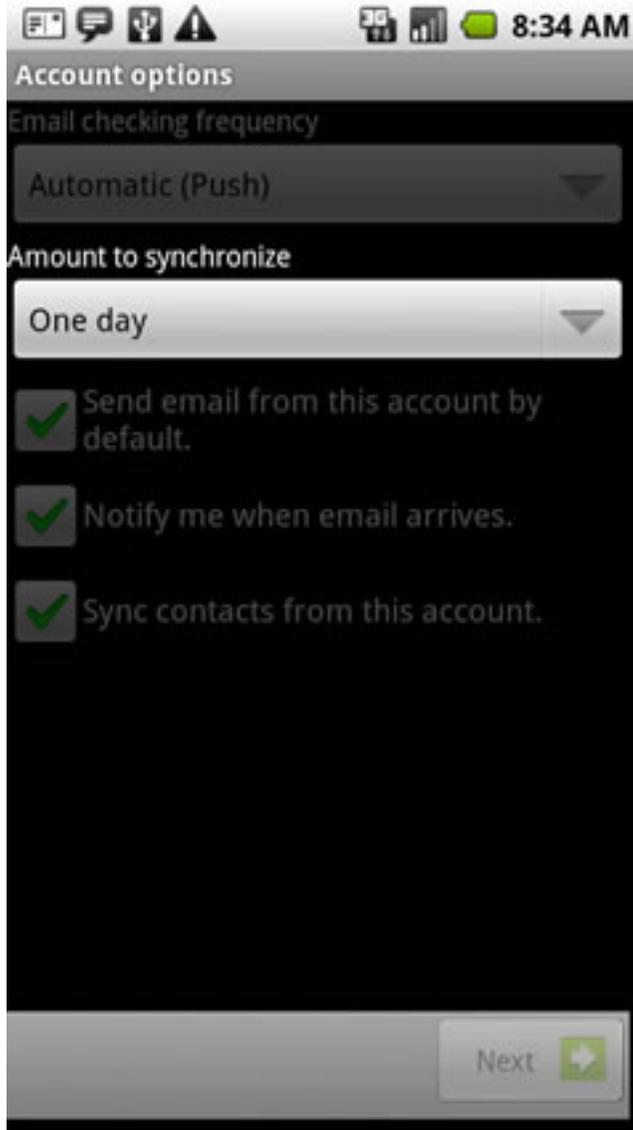
Touch the Email Checking Frequency dropdown (if available).



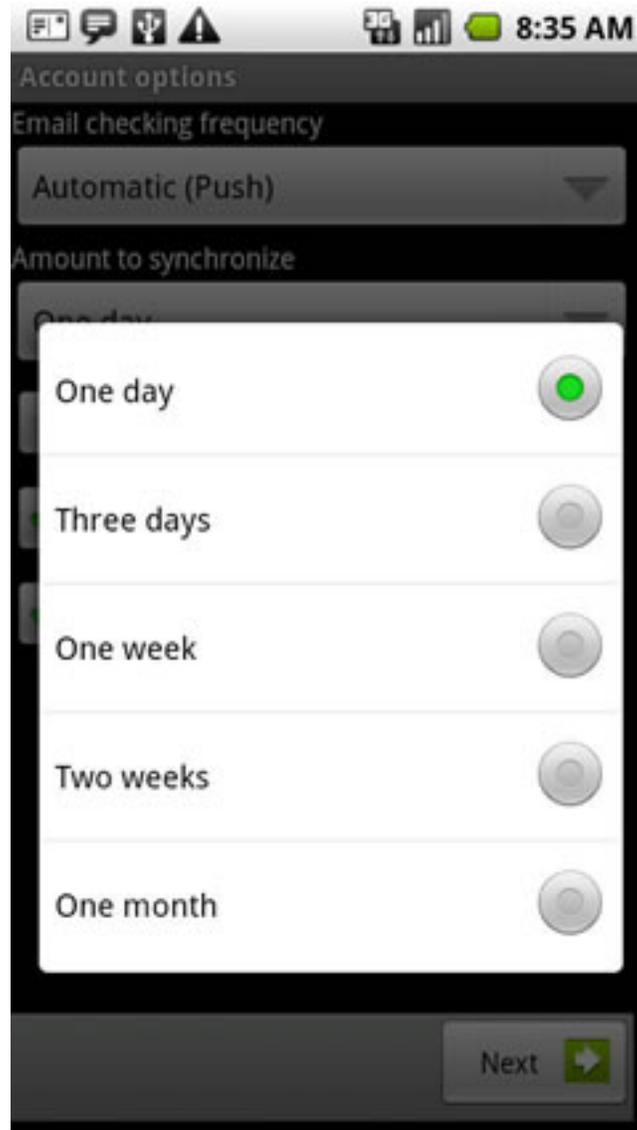
Touch the desired frequency. Select Automatic PUSH.



Touch the Amount to synchronize dropdown.

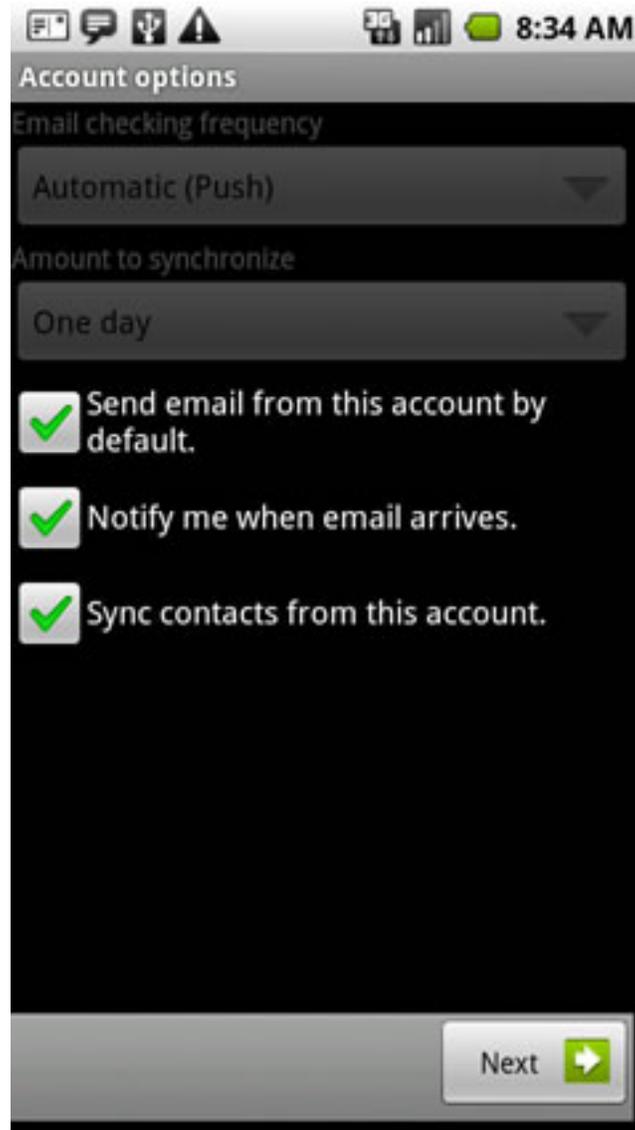


Touch the desired amount. We would recommend ALL available (at least 1 month).



Touch the desired account options then touch Next.

- \*The account option is enabled if a green check mark is present.
- \*Send email from this account by default.
- \*Notify me when email arrives.
- \*Sync contacts from this account



Enter an account name and outgoing message name then touch Done.

## How to setup secure POP Email?

### Configuring Your POP Client

POP, or Post Office Protocol, is a widely used standard for connecting an e-mail program on your desktop (the client) to a mail server which handles your incoming messages. Requirements  
This is mainly for all Windows email clients. If for MAC systems, it will be noted here with an \* sign.

### POP Server

This is the name of the server which provides your incoming mail. For SoM accounts, the incoming name for the SoM POP server is owa.med.wayne.edu  
Use SSL for Inbound Mail Server

---

You must use SSL, with POP-SSL port#: 995

You will need to install the WSUSoM Certificate Authority certificate. If you have not installed this already, then you can download it by going to <http://owa.med.wayne.edu> and retrieving from the left-hand menu. All Med domain machines automatically have this installed so you don't have to do this. If you use Eudora or Mozilla or another operating system, then you'll need to download and import the certificate based on the specific email apps instructions.

\* For MAC systems, the WSUSoM certificate from <http://owa.med.wayne.edu> homepage needs to be downloaded and added to SYSTEM under keychain access on Apple computers.

#### Username

Your SoM username. This is normally your 1st initial and last name (i.e. bsmith)

#### SMTP Server

This is the computer that handles your outgoing mail. Enter [smtp.med.wayne.edu](mailto:smtp.med.wayne.edu). The SoM mail gateway will only accept mail to be delivered if the computer that you are using is on the WSU Campus or using the WSU/SoM VPN service. If you are using a broadband connection or another Internet Service Provider at home, then you will need to use their SMTP server to send email. Unless you use authentication, as described below.

Use SSL for Outbound Mail Server

#### On Campus Mode

This means this mode (or setting) is used on machines within the School of Medicine Campus.

You must use SSL: On the SOM campus USE SMTP-SSL port: 25. This is commonly used on Windows machines with a Med domain access.

#### Off Campus Mode

You can now use the SMTP(outbound Mail Server) on other networks using authentication.

#### Authentication Settings

Use SMTP-SSL port: 587

Requires TLS: YES

Requires login: YES Specify your MED login ID and Password

It's recommended to just use port 587 on traveling laptop (notebooks)

\*This is recommended for all MAC clients.

#### Return Address

This is the e-mail address that will appear in the From: field of mail that you send out. Here you should enter the simplified form of your e-mail address, [username@med.wayne.edu](mailto:username@med.wayne.edu).

#### LDAP Server

Some mail clients include support for the LDAP directory access protocol. The School of Medicine's LDAP server can be found at [ldap.med.wayne.edu](http://ldap.med.wayne.edu), and if you add this server to your client's list of LDAP directories, you should be able to use it to find the e-mail address of anyone at the School of Medicine that has an entry in our directory. Information about the SoM LDAP Server can be found at <http://www.med.wayne.edu/msis/email/ldap.asp>.

## How to AutoArchive email with Microsoft Outlook

Your Exchange mailbox grows as items are created in the same way that paper piles up on your desk. In the paper-based world, you can occasionally shuffle through your documents and store those that are important but not frequently used. Documents that are less important, such as newspapers and magazines, you can discard based on their age. You can quickly complete the same process in Outlook.

The current approved limit is 1 gigabyte for faculty, staff and students (SoM Alumni accounts have a 50 MB limit) - Auto-archiving helps to keep your mailbox size under the 1 gigabyte limit at the School of Medicine without discarding mail you may need. When you archive, your existing folder structure is maintained in your new archive file. In this way, an identical folder structure exists between the archive file and your mailbox. Folders are left in place after being archived, even if they are empty.

#### Turning on Auto-Archive

First, turn on Auto-Archive. On the Tools menu, click Options.

---

Click the Other tab, and then click Auto-Archive.

Specify how often you want Auto-Archive to check your folders and where the default Auto-Archive location should be &ndash; example: C:\archive.pst. Click Ok and apply your changes and close out of the Outlook options.

Once you configure your computer with an archive location, you can run the Auto-Archive by clicking Archive on the File menu.

Select the option to archive your inbox and all the sub folders, and type your Archive File location that you configured in the Outlook Options.

You are now done activating the Auto-Archive tool. If you checked &lsquo;Prompt before Auto-archive&rsquo;, you will be prompted when it is time to auto-archive. If you want to run the auto archive manually, from the Microsoft Outlook click on File, and select Archive. Customize the archive selection for your needs. Once the archive process runs, you can click and drag any items from your mail box into the archive folder to remove the messages from the server.

Opening up Auto-Archive Items

You can retrieve items from an archive file by opening the archive file. When you open the archive folder, it is added to your folder list, and you can access all of your archived mail from this folder. You can also manually copy items into appropriate folders in your mailbox if you need them back on the mail server. \* Note &ndash; Items that are Auto-Archived will not appear in your inbox if you access your mail via <http://owa.med.wayne.edu> &ndash; this is why you would want to manually copy messages back to your inbox if needed.

To open your archived mail, click File, Open, Outlook Data File, and browse to the location where you set Auto-Archive to save the \*.pst file. (e.g. &ndash; C:\archive.pst).

Additional information for how to manage email is available from the Microsoft Website: <http://office.microsoft.com/training/training.aspx?AssetID=RC010970841033>

## **Mac Mail for OS 10.5.x (Leopard) - POP Account Type**

### Overview

This document will help you to configure your Mac Mail (built-in MacOS X software) e-mail client to work with the med.wayne.edu e-mail system.

Compatible MacOS Version: OS 10.5.x (Leopard)

Note: These instructions do not apply to Mac Mail for OS 10.2 Jaguar, 10.3 Panther, or OS 10.4 Tiger

### Step 1: Create Your Email Account

1. Start Mail.
2. If it is the first time you are setting up your account, a wizard will walk you through the steps. If the wizard does not appear you can open up the wizard by going to the File menu, then Add Account to launch the wizard.
3. Fill out the requested information.
4. Click Continue.

---

## Step 2: Incoming Mail Server

### 1. Enter the following information:

- o Select the Account Type from the menu: POP or Imap
- o Imap is the preferred mail protocol to use.
- o Description: [Optional, may be left blank]
- o Incoming Mail Server for POP: pop.med.wayne.edu
- o Incoming Mail Server for Imap: imap.med.wayne.edu
- o User Name: [SOM ID]
- o Password: [Your password]

### 2. Click Continue.

## Step 3: Incoming Mail Security

1. The Incoming Mail Security window will only show up if the attempt to detect the settings fails. If you do see it, enter the following information.

- o Check the box for Use Secure Sockets Layer (SSL).
- o Select Passwords for Authentication.

### 2. Click Continue.

## Step 4: Outgoing Mail Server

1. To configure the Outgoing Mail Server, enter the following information.

- o Description: [Optional, may be left blank]
- o Outgoing Mail Server: smtp.med.wayne.edu
- o Check the "Use only this server" box.
- o Check the "Use Authentication" box.

- o User Name: [Your SOM id]
- o Password: [Your Password]

### 2. Click Continue.

## Step 5: Outgoing Mail Security

1. The Outgoing Mail Security window will only show up if the attempt to detect the settings fails. If you do see it, enter the following information.

- o Check the box for Use Secure Sockets Layer (SSL).
- o Select Passwords for Authentication.

### 2. Click Continue.

3. Select connect if a Verify Certificate window appears.

---

## Step 6: Account Summary

1. This section summarizes the settings that you have made. It should look like the graphic below.
2. Check the "Take account online" box.
3. Click Create.

## Required Additional Incoming Settings

For additional incoming server settings

1. Click on the Mail menu
2. Click on Preferences
3. Click on Accounts and select the appropriate account
4. In the right-hand section, click on Advanced
5. Make sure the settings are the same as in the picture below
6. Port 995 is for POP and Port 993 is for Imap

Required Additional Outgoing Settings For additional outgoing server settings

1. Click on the Mail menu
2. Click on Preferences
3. Click on Accounts and select the appropriate account
4. In the right-hand section, look for the Outgoing Mail Server (SMTP) dropdown.
5. In the dropdown, select Edit Server List...
6. Click on Advanced
7. Make sure the settings are the same as the picture below
8. Select OK, close Mail and relaunch.

## Modify Junk Mail Settings in Microsoft Outlook 2003

The Microsoft Outlook application has the ability to filter potential junk e-mail, and by default the Junk E-mail Filter is set to Low. This level is designed to catch only the most obvious junk e-mail messages. Any message that is caught by the Junk E-mail Filter is moved to a special Junk E-mail folder. You should review messages in the Junk Email folder from time to time to make sure no legitimate messages that you want to receive have been moved - example: an email sent from the WSU ListServe is tagged as being potential junk mail by Microsoft Outlook and moved to the Junk Email folder.

To quickly add a sender, domain name, or mailing list name to the Safe Senders or Safe Recipients Lists, within the Junk Email folder right-click the message you consider safe, and then point to Junk Email, and then you can select either Add Sender to Safe Senders List, Add Sender's Domain (@example.com) to Safe Senders List, or Add Recipient to Safe Recipients List as shown in the below screenshot:

---

At the SoM we recommend that users add @dmc.org, @karmanos.org, @kresgeeye.org, @med.wayne.edu and @wayne.edu to the safe senders list.

Additional information about the Junk EMail Filter is available from the following web site:

<http://office.microsoft.com/en-us/outlook/HP052429671033.aspx>

## **Remove Previously Used Names/Addresses from Microsoft Outlook**

When addressing e-mail, Outlook has a feature that allows it to remember previously used names that were entered in any of the address fields (To, Cc, or Bcc). At some point it may become necessary to remove all or some of these cached names and addresses or to turn off this feature entirely.

To turn off this feature: Go to the Tools menu and select Option... From the Preferences tab click the E-mail Options... button From the E-mail Options window click the Advanced E-mail Options... button Under the "When sending a message" section uncheck the box next to "Suggest names while completing To, Cc, and Bcc fields" Click OK to close out any open windows to return to Microsoft Outlook

By un-checking this box, the "suggest" feature is off. Rechecking the box turns it back on, and returns it to the state it was in before it was turned off.

Removing specific entries from the auto suggest list:

You may want to keep the auto suggest feature on, but remove only those outdated or incorrect entries on the list. To do this you will delete the names when they appear as the message is being addressed (To, Cc, or Bcc). Begin typing the name on the To, Cc, or Bcc line When the list pops-up under your cursor, use the Down Arrow to highlight the name you want to remove Press the Delete key Repeat for each name you wish to delete

This method permanently removes the name from the list. Any deleted name will not show up again unless you enter and use that same name/E-Mail address again on one of the address lines.

However, if the auto suggest list gets corrupted, this will not work. In such cases, the entire list must be erased and rebuilt.

To delete the auto suggest list: Close any running copies of Microsoft Outlook. Open up My Computer. Make sure hidden files and folders are visible by navigating to Tools -> Folder Options -> Advanced Settings, and select "Show hidden files and folders." From your C: drive, browse to the folder Documents and Settings\Application Data\Microsoft Outlook Look for any files with the .NK2 extension - these are the nickname caches. (If they're not visible there, you may need to search the system for any files that match that extension.) Rename the file to something else. For example, if the file name is Outlook.NK2, you could rename it to Outlook.NK2.bak. Restart Microsoft Outlook - a new Microsoft Outlook nickname cache should now be rebuilt.

## **SoM E-Mail setup on iPhone & iPad**

iPhone and iPad Email Setup for School of Medicine

Please follow these simple steps to configure your device for School of Medicine Exchange Email.

1) Click "Settings" on your iPhone and you will be taken to this screen:

2) Click on "Mail, Contacts, Calendars" and you will be taken to this screen:

---

3) Click on "Add Account" and you will be taken to this screen:

4) Click on "Microsoft Exchange" and you will be taken to this screen:

5) In this window, fill in all of the fields with your information. ALL information is necessary; nothing is optional as it says. An example is below:

6) Once you have filled in ALL of the information (I named the Description: SoM E-Mail), click "Next" at the top right and you will be taken to the following screen:

7) If you are presented with the following prompt, click "Continue";

8) You will now be taken to the following screen once it has verified the account and automatically fill in the Server field and you will be looking at the following screen:

9) Click "Next", and you will be at the following screen that asks you what you would like to turn on from this account. Note: Contacts will OVERWRITE your phone's address book / contacts / phone numbers with the exchange servers contact list. Also, with older iPhone OS versions (older than iOS4) Calendar will do the same thing, it will overwrite whatever you have saved on your phone's calendar with your exchange server. Newer and updated iPhones will allow you to "combine" the two calendars and it will tell you just this if you try to enable this.

10) Click "Save" and you will start receiving email on your iPhone from your Wayne State University School of Medicine email account. If you go back into the Settings and select, "Mail, Contacts, Calendars" again, you will see the following screen where you can change the settings and behavior of your phone in regards to the SoM E-Mail system.

---

If you click on your SoM E-Mail account, you can see these settings related to the options that you initially set up.

If you have any questions, please contact the MSIS Helpdesk at (313)577-1527 or helpdesk@med.wayne.edu.

## Blocked Email Attachment Types at the SoM

### Email Attachment Blocking

Certain windows attachment types are blocked from entry into the SoM email environment. These attachment types are all known to be capable of executing/running programs on systems. The primary purpose of such blocks is to prevent virus outbreaks in the SoM email system that can occur if there is a new email based virus on the internet that the Antivirus software writers having provided detection for at the early outset of the virus discovery.

These are all the attachment types recommended that mail administrators block:

- \*.reg Windows registry entries are very dangerous in email
- \*.chm Compiled help files are very dangerous in email
- \*.cnf SpeedDials are very dangerous in email
- \*.hta HTML archives are very dangerous in email
- \*.ins Windows Internet Settings are dangerous in email
- \*.jse\* JScript Scripts are dangerous in email
- \*.job Task Scheduler requests are dangerous in email
- \*.lnk Eudora \*.lnk security hole attack
- \*.mad Microsoft Access Shortcuts are dangerous in email
- \*.maf Microsoft Access Shortcuts are dangerous in email
- \*.mag Microsoft Access Shortcuts are dangerous in email
- \*.mam Microsoft Access Shortcuts are dangerous in email
- \*.maq Microsoft Access Shortcuts are dangerous in email
- \*.mar Microsoft Access Shortcuts are dangerous in email
- \*.mas Microsoft Access Shortcuts are dangerous in email
- \*.mat Microsoft Access Shortcuts are dangerous in email
- \*.mav Microsoft Access Shortcuts are dangerous in email
- \*.maw Microsoft Access Shortcuts are dangerous in email
- \*.pif Shortcuts to MS-Dos programs are very dangerous in email
- \*.scf Windows Explorer Commands are dangerous in email
- \*.sct Windows Script Components are dangerous in email
- \*.shb Shortcuts Into Documents are very dangerous in email
- \*.shs Shell Scrap Objects are very dangerous in email
- \*.vbe Visual Basic Scripts are dangerous in email
- \*.vbs Visual Basic Scripts are dangerous in email
- \*.wsc Windows Script Host files are dangerous in email
- \*.wsf Windows Script Host files are dangerous in email
- \*.wsh Windows Script Host files are dangerous in email
- \*.xnk Microsoft Exchange Shortcuts are dangerous in email
- \*.com Executable DOS/Windows programs are dangerous in email
- \*.exe Executable DOS/Windows programs are dangerous in email
- \*.scr Windows Screensavers are often used to hide viruses
- \*.bat Batch files are often malicious
- \*.cmd Batch files are often malicious
- \*.cpl Control panel items are often used to hide viruses
- \*.mhtml MHTML files can be used in an attack against Eudora
- \*.wmf Windows Metafile security vulnerability
- \*.bmp Windows bitmap file security vulnerability. Possible buffer overflow in Windows
- \*.ico Windows icon file security vulnerability. Possible buffer overflow in Windows
- \*.ani Windows animated cursor file security vulnerability. Possible buffer overflow in Windows
- \*.cur Windows cursor file security vulnerability. Possible buffer overflow in Windows
- \*.hlp Windows help file security vulnerability. Possible buffer overflow in Windows

\*.cab Possible malicious Microsoft cabinet file  
\*.cer Dangerous Security Certificate (according to Microsoft Q883260)  
\*.its Dangerous Internet Document Set (according to Microsoft Q883260)  
\*.mau Dangerous attachment type (according to Microsoft Q883260)  
\*.mda Dangerous attachment type (according to Microsoft Q883260)  
\*.mdz Dangerous attachment type (according to Microsoft Q883260)  
\*.prf Dangerous Outlook Profile Settings (according to Microsoft Q883260)  
\*.pst Dangerous Office Data File (according to Microsoft Q883260)  
\*.tmp Dangerous Temporary File (according to Microsoft Q883260)  
\*.vsmacros Dangerous Visual Studio Macros (according to Microsoft Q883260)  
\*.vss Dangerous attachment type (according to Microsoft Q883260)  
\*.vst Dangerous attachment type (according to Microsoft Q883260)  
\*.vsw Dangerous attachment type (according to Microsoft Q883260)  
\*.ws Dangerous Windows Script (according to Microsoft Q883260)

Filetype restrictions (renaming file will NOT bypass filename restriction):

No self-extracting archives allowed

ELF programs are not allowed

executable programs are not allowed

No MPEG movies allowed

No AVI movies allowed

No MNG movies allowed

No QuickTime movies allowed

ASF Windows media files are not allowed

No Windows Registry files allowed

No Windows Metafont (WMF) drawings allowed

File attachments that try to disguise themselves using double extensions or CLSIDs will be rejected:

CLSID example:

"document.{00152EF2-ED80-4406-8F0A-A2E1AAA8DB1D}"Lots of contiguous white space example:

"document .doc"Double filename extension examples:

"document.pdf.doc"

"readme.doc.exe"

Also due to security implications, messages that are HTML formatted are checked for 3 known security problems:

Object Codebase Tags:

This will allow various Microsoft security vulnerabilities to go unprotected. Codebase tags are used to instruct HTML-based clients such as web browsers and email clients to install ActiveX components. Preventing HTML based messages with codebase tags prevents malicious programs from being installed on your computer just by opening the such an email message. There shouldn't be any logical reason to send people such messages.

IFrame Tags:

Allowing IFRAME tags is not a good idea as it allows various Microsoft Outlook security vulnerabilities to go unprotected. Iframe tags are similar to codebase tags, but instead of directly installing programs on a computer, the Iframe tag is used to automatically spawn an instance of Internet Explorer internally and access a web page, which in real life situations could be infectious.

Form Tags:

Everyone is familiar with filling out forms on web pages. What they may not be aware of is that web pages with forms can be emailed to people as well and have been used to trick people into providing personal information such as login ids, passwords, social security numbers, credit card numbers, etc. This tactic has been widely publicized as being used to hijack eBay and aol accounts. Due to the nature of this organization as a medical institution, there is the potential that this tactic may be used to obtain patient or other private information without the recipient being truly aware of who is collecting the information or where it's being submitted.

Password protected Zip Files

As of late February 2004, password protected zip files are now blocked due to the outbreak of the Beagle/Bagle viruses which hide inside password protected zip files to prevent being detected by virus scanners which rely on people to open using the password supplied in the email message. Also because of this outbreak, the blocked attachment rules now end up applying to the attachments hidden into zip files. We apologize for the inconvenience this may cause since the recommendations have always been to send executable code in a Zip file, but due to the virus software changes we can't prevent it from applying the block attachment rules to the contents of zip files.

Outlook attachment blocking:

Besides the attachment blocking that the SoM email router does, the Outlook and Outlook Express clients as well as Outlook Web Access may also restrict certain file attachment types. To see the list that they may restrict, visit Microsoft Office Online from the following URL:  
<http://office.microsoft.com/en-us/assistance/HP030850041033.aspx>

---

## **I received an email to my @med.wayne.edu account saying I sent a virus to someone.**

Unless you are contacted by the School of Medicine Helpdesk, your computer should be free of viruses.

If you did not send the message then it most likely is an email virus that sent the message using your return address - your email address is probably listed in the address book of the infected computer. There isn't anything we can do about email address forging since that is the nature of email, just as it's the nature of U.S. Postal mail where you can put anything for a return address and drop it in a mailbox.

If your computer is setup to log into the MED domain and your virus definition files are up to date, your computer should be free of viruses. Email that goes thru the SoM email servers is scanned for viruses - if your computer is infected and sending out viruses you will be notified by the helpdesk.

## **How to forward WSU email to SoM Email**

If you are a Wayne State student or employee, you have or will be assigned a WSU AccessID. With your WSU AccessID, you can access a free e-mail account and many other Main Campus Web resources.

However, if you also work for or attend the School of Medicine, you have another e-mail account also (e.g., yourmail@med.wayne.edu). Here's why you'll want to set mail forwarding from your WSU Access e-mail to your School of Medicine email address.

Consider the following types of potentially important e-mail that would normally go to your WSU AccessID e-mail account: A student or instructor may send e-mail to your WSU AccessID. The Public Safety Department sends e-mail to WSU AccessIDs. WSU Library systems may send you email about overdue books to your WSU AccessID. WSU's president sends e-mail to WSU AccessIDs. When people search for your name in the WSU People Directory, they will find your WSU AccessID e-mail address and send e-mail there.

Unless you have e-mail forwarding setup you won't receive those emails in your School of Medicine mailbox. Here's how to set mail forwarding on your WSU AccessID e-mail account to your School of Medicine e-mail account

Setting mail forwarding is a one-time process. Follow the steps given below: Log in to WSU Pipeline and click Account.

OR

Log in to WSU WebMail

Once logged in, please click Zimlets on the left pane on your window and expand Account Management.

Once you click on Account Management you will see the next window

Now click on Forwarding (highlighted in above image). In the Mail Forwarding Address box type your preferred e-mail address (e.g., yourmail@med.wayne.edu). In Mail Forwarding Settings, you will have to make a choice to have keep all your mail at WAYNE.EDU or not. If your mail is not kept at WAYNE.EDU it will be deleted once it is forwarded to MED.WAYNE.EDU. On the other hand, if you decide to keep your mail at WAYNE.EDU, your messages will still be forwarded to MED.WAYNE.EDU. Click the OK button. That's it. Your WSU AccessID e-mail will be forwarded to your School of Medicine e-mail account.

Note: if you don't know your AccessID password, call the C&IT Help Desk, 313-577-4778.

---

Note: if you don't know your School of Medicine password, call the SoM Help Desk, 313-577-1527.

## Microsoft Windows Outlook 2007/2010 - External E-Mail Setup for SoM

### Description

This setup is mainly intended for machines outside School of Medicine Campus. This can be applied for Home or other external places (Karmanos, DMC, etc). If you require a SoM PC setup, please call us directly for this setup.

Requirements Microsoft Office 2007/2010. Office 2003 will have connectivity issues at this point. Windows XP, Vista, 7 Administrator Rights to make changes to PC. SoM ID and Password.

### Setup

These steps are mainly for Windows XP yet Vista and Windows 7 will have the identical configuration settings. Click on your Start button and then select Control Panel.

In Control Panel, do one of the following tasks: If you are using Category View, in the left pane, under See Also, click Other Control Panel Options, and then click Mail. If you are using Classic View, double-click Mail.

In Mail Setup, under Profiles, click Show Profiles.

In Mail, click Add.

In New Profile, in the Profile Name box, type a name for this profile, and then click OK.

In the E-mail Accounts wizard, click Add a new e-mail account, and then click Next. For Outlook 2010, choose manually configure server setting or additional server types.

On the Server Type page, click Microsoft Exchange Server, and then click Next. For Outlook 2010 choose Microsoft Exchange or compatible service.

On the Exchange Server Settings page, do the following steps: In the Microsoft Exchange Server box, type the name of the back-end Exchange server - outlookcas.med.wayne.edu. Select the check box next to Use Cached Exchange Mode. In the User Name box, type the user name. Click More Settings. In the Connection tab, in the Exchange over the Internet pane, select the Connect to my Exchange mailbox using HTTP check box. For Outlook 2010, in the Connection tab, in the Outlook Anywhere Pane, select the Connect to my Exchange mailbox using HTTP check box. Click Exchange Proxy Settings.

Please note: When prompted to login, you must login using MED\login name. The initial connection can be a little slow and doesn't reflect the operational speed. So if Outlook states that it cannot find the Exchange server, just click Retry.

For increased security, you will need to specify Connect with SSL only and Mutually authenticate the session when connecting with SSL. On the Exchange Proxy Settings page, under Connections Settings, do the following steps:

Enter the fully qualified domain name (FQDN) of the RPC proxy server in the section that states Use this URL to connect to my proxy server for Exchange: owa.med.wayne.edu. Select the option for Connect using SSL only. Next, select the Mutually authenticate the session when connecting with SSL check box. Enter the FQDN of the RPC proxy server in the Principle name for proxy server box. Use the format: msstd:\*med.wayne.edu

Under Proxy Authentication Settings, please use the below settings

On a fast network, connect using HTTP first, then connect using TCP/IP

To change the default behavior for fast networks (example: High Speed Internet Connection), clear this check box. On a slow network, connect using HTTP first, then connect using TCP/IP

To change the default behavior for slow networks (example: Dialup Internet Access), clear this check box.

On the Exchange Proxy Settings page, in the Proxy authentication settings window, in the Use this authentication when connecting to my proxy server for Exchange list, select NTLM Authentication. Click OK.

Now we are back to Microsoft Exchange Server window.

In the Security tab, please make sure Always Prompt for User Name and Password is checked under User Identification.

Click OK

If by chance at any point you get a Login Window Outlook or Exchange, please make sure your use

---

the below format to enter your credentials:

med\username

This should work! If you have any other issues, please call us back at 313-577-1527 and will be happy to help! Make sure you are by the PC in question to better assist you.