Legacy CIM Email Instructions

CIM has it's own email server. Your email address at CIM is username@cim.mcgill.ca, the username being the name you use to log in to CIM computers. There are multiple ways to access your CIM email, the quickest and likely easiest for some users is webmail. The address of the webmail server is http://webmail.cim.mcgill.ca, this is available from anywhere in the world and is a quick and easy way to access your CIM email. There is more information on using the webmail interface available in the section on webmail.

The CIM mail server has some advanced spam filtering mechanisms, you can modify how these affect your personal email using the “Spam Filters” configuration page in the webmail, there is more information available on this in the Spam Filtering portion of the webmail section. You are also free to use any built-in spam filtering that your email client contains, though many users find it unnecessary since the server's filters block a large majority of incoming spam emails.

You can also set up server side filtering of incoming messages through the webmail configuration page, there is more information on this in the Message Filtering portion of the section on the webmail. You can also use built in filter mechanisms of your preferred mail client.

It is also possible to forward your CIM email to another account, either keeping a copy at CIM or not saving it locally at all. There is more information on this in the mail forwarding portion of the webmail section.

Server Addresses

If you prefer to use a client, there is some information on configuring clients lower down on this page, but in case you simply need the basic server addresses, they are listed here. If you do not know what to do with this information, please ignore it and look at one of the client sections below.

- **SMTP**: '''`smtp.cim.mcgill.ca`'''
- **IMAPv4**: '''`imap.cim.mcgill.ca`'''
- **POP3**: '''`pop.cim.mcgill.ca`'''

'`IMAP and POP3 will not accept logins over any connection that is not using` TLS' (Transport Layer Security), please make sure that your client supports TLS. If your client does not support TLS, you can alternatively use IMAPS (IMAP over SSL) on port 993. If your client does not support either TLS or SSL, you will have to use a different client to connect to the CIM IMAP server. You may also use the CIM webmail.

Outside of CIM, POP3 is not available. Only POP3S is available on port 995. For SMTP, remote authenticated access is available so you can use the CIM email server to send email from anywhere in the world. To use authenticated SMTP, you '`must`' enable encryption, SMTPS (SMTP over SSL) is available at port 465 and TLS is available on port 25. There is also mail submission protocol available on port 587 which can be used for TLS connections if you are somewhere that does not allow outgoing port 25 connections (just about everywhere these days).

Clients

It is possible to use just about any mail client that supports POP or IMAP with the CIM mail system. We recommend that you use an IMAP client, since that will keep your mail on the server where it is regularly backed up, and will be available from the webmail interface.

We request that you do not use a mail-fetching program to download your email to another account, as this creates extra load on our server. It is preferable that you use the interface in webmail to set up mail forwarding to the other account. This forwarding is “bounce” style forwarding, meaning all headers are preserved, so you can still use filters on the external account you are forwarding to.

Webmail

There are two webmail systems currently available at CIM. Roundcube and SquirrelMail. The default is currently SquirrelMail, but there is a plan to switch to Roundcube in early 2011. Roundcube offers a superior interface, wider browser compatibility and is currently under active development.

Roundcube

The CIM Roundcube interface should be easy to use, as it attempts to work in a similar way to a local mail client. There is a list of your folders on the left, and the message list is on the right, with a “preview” area below. The top has a toolbar and holding the mouse cursor over a button will display a short description. The “Check for new messages” button refreshes the message list, adding any new messages. By default, the message list is automatically refreshed every 1 minute. For more information on normal usage of Roundcube, please see the official Roundcube user guide.

To access the Roundcube configuration, use the Settings button at the top right of the main window. This contains the configuration settings for the webmail interface, as well as the configuration page for Filters, Vacation/Forwarding and a utility to change your CIM password. Although the SpamAssassin Configuration interface is currently available only under SquirrelMail, any changes made to the SpamAssassin under SquirrelMail will also apply to Roundcube.

Filters

Mail filters allow you to configure the mail server to perform certain actions based on the contents of incoming messages. These actions can be move/copy the message to a certain folder, send an automatic reply or simply delete the message. You can also redirect messages to another email address. This is essentially the same as forwarding, with and without keeping a local copy.

Since 2011, the CIM mail server is using the Sieve filtering language. This is a standardized filtering language for mail servers. The preferred way to setup the filters is with the easy-to-use webmail GUI as described here. It is also possible to directly edit the text of the filter scripts by connecting to '''imap.cim.mcgill.ca''' on port '''4190''' with a Client.

To set up mail filters, you can use the Filters tab at the top of the Roundcube settings screen.

This interface allows you to add, delete and rearrange filters and filter sets. A filter set is a group of filters, You can have any number of filter sets defined, but it is only possible to have one set active at any given time. Each time a message is delivered, the filters from the currently active filter set are executed in order starting with the top of the list, when a match is found, the server will do the action specified in the filter, and continue executing filters unless the '`Stop evaluating rules`' action is contained in the filter. This rule is automatically added to new filters by the Roundcube interface.

To add a filter, click the '`Add Filter`' button at the top left of the Filter settings screen. Enter a filter name, this can be anything you like. Under '`For incoming mail`' section, you can add multiple rules to filter based on the message headers. It is possible to specify your own headers by selecting '`[…]`' as the header and entering the name of the header in the text box that appears. Once you have selected the rules, then under '**…**`execute the following actions`' section, you can add any number of actions to perform. On new rules, the '`Stop evaluating rules`' action will be automatically added at the end. Once you have finished setting up your rule, you can click '`Save`' to save your new rule, and the '`Add Filter`' button again to add another filter.

Once you have finished adding the filters to your filters set, click the '`Activate current filters set`' so that the filters set will be activated. *'**`Make sure that the filters set says '(active)'" beside the name in the 'Filters set:' list box.`**'"* Otherwise the '`filters will NOT work`'. You can only have one active filter set at a time. You can use the '`Add filters set`' button to add more filter sets. Most people will only use a single filter set.

Putting SPAM in the "Junk" Folder

If you want to create a filter to move all messages marked as SPAM to a folder called Junk, create a filter that matches the following description:

'`[…]`' '`X-Spam-Flag`' '`Contains`' '`YES`'

'`Move message to`' '`Junk`'

'`Stop evaluating rules`'

If you would like to move messages marked as SPAM by the central McGill anti-spam system, create a filter rule that matches the following description:

'`[…]`' '`X-McGill-Spam`' '`Contains`' '`#####`'

'`Move message to`' '`Junk`'

'`Stop evaluating rules`'

Vacation/Forwarding

The '`Vacation`' link under the Roundcube '`Settings`' is where you can configure mail forwarding and/or vacation messages. A vacation message is an automatic reply to any message sent to your CIM email address. This can be a notice about being out of the office until a certain date, or a notification of some other kind. Forwarding allows you to send all mail sent to your CIM address to

another email address. If you are going to use another account for reading email forwarded from CIM, please do not keep a local copy of your CIM email if you are not going to actively manage your CIM mailboxes (mail deleted on other servers will remain on CIM's servers, using our very limited resources).

To set up email forwarding, enter a comma-separated list of email addresses in the '`Forward mail mail to`' at the bottom of the screen, and click '`Save`'. If you would like the messages to skip your CIM account completely (so there are no copies of the message kept at CIM), check '`Keep a copy of the mail`'. To disable forwarding, remove all text in the '`Forward mail mail to`' field.

To set up vacation, enter a subject for the automated response in the '`Autoreply Subject`' box, and a message in the '`Autoreply message`' box. Finally, check '`Send a notification`' at the top, and click '`Save`' at the bottom of the screen. To disable vacation, simply uncheck '`Send a notification`', this will preserve your message in case you would like to use it in the future, but disable the vacation program.

SquirrelMail

SquirrelMail has been the webmail client used at CIM for many years. There is not currently any active development happening by the SquirrelMail team, and the current version has trouble with some browsers. There is currently a plan in place to replace SquirrelMail with Roundcube at CIM. SquirrelMail will continue to be available for some time after the change.

The CIM SquirrelMail interface should be fairly straightforward and easy to use. There is a list of your folders on the left, and the message list is on the right. The check mail link in the message list will refresh any new mail counts, and highlight folders with new messages. To create/delete folders, use the Folders link at the top of the left frame.

To access the webmail configuration, use the Options link at the top of the left frame. This contains the configuration settings for the webmail interface, as well as the configuration page for server side filters, spam filters, forwarding and vacation.

For more detailed information on any portion of the webmail, context-sensitive help is available by clicking the “Help” link at the top of the left frame of the webmail interface.

Filtering

'`PLEASE NOTE: The SqurrelMail (maildrop) filters are currently disabled on the server, please use Roundcube (sieve) Filters`'

Forwarding/Vacation

The Autoresponder / Mail Forwarding link under the webmail Options is where you can configure mail forwarding and/or vacation messages. A vacation message is an automatic reply to any message sent to your CIM email address. This can be a notice about being out of the office until a certain date, or a notification of some other kind. Forwarding allows you to send all mail sent to your CIM address to another email address. You can keep a copy at your CIM address if you like, or you can simply forward

it to another address without keeping a copy at CIM.

To set up email forwarding, enter a list of email addresses in the Forwarding email addresses at the bottom of the screen, and check “Forward incoming messages to addresses listed below”. If you would like to disable local delivery (so there are no copies of the message kept at CIM), uncheck “Keep copies of incoming messages in this account”. To disable forwarding, uncheck Forward incoming messages to addresses listed below.

To set up vacation, enter a subject for the automated response in the Subject box, and a message in the Message box. Finally, check “Enable auto-reply to sender” at the top, and click Submit. To disable vacation, simply uncheck “Enable auto-reply to sender”, this will preserve your message in case you would like to use it in the future, but disable the vacation program.

SpamAssassin Configuration

Here at CIM, we have an advanced SPAM filtering system which is capable of “learning” the difference between spam and non-spam messages. This filter is individual to each person, and it can be trained using the Spam and Not Spam links under “Options” on the message reading screen.

The spam filter is somewhat configurable. The configuration page is located under the Spam Filters link the Options screen in webmail. Here you can add email addresses to your white or black lists, and configure your scoring policy. The configuration page itself has more information on white/black lists and scoring policy.

The anti-spam system works by assigning a score to a message according to how much it looks like SPAM. The higher the score, the more likely the message is SPAM. Currently if a message has a score of 4.5 or higher, then it is marked as SPAM by adding a “*__SPAM__*” tag to the subject and adding “X-Spam-Flag: YES” to the message headers. If the message scores a 13 or higher, it is dropped and not delivered. Both these actions are logged to the mail server logs. If you would like to change these values from the defaults, you can use the Spam Filters configuration screen to change the policy.

If you would like to have the mail server automatically move suspected SPAM to an alternative folder, please see the section on message filtering or for sieve filters.

McGill Central Filter

The CIM email server does not filter any email coming from within the McGill network, this is to prevent any false positives on internal McGill mail. Recently, spammers have been using the central McGill list server to pass spam to users at the McGill campus. These messages are marked as spam by the central system, but they are not filtered, simply marked. If you would like to use a filter to move these messages to a “Junk” folder, please see the section on Moving SPAM to "Junk" Folder or for sieve Putting SPAM in the "Junk" Folder.

Message Filtering

'PLEASE NOTE: The SqurrelMail (maildrop) filters are currently disabled on the server, please use Roundcube (sieve) Filters'

Thunderbird

Mozilla Thunderbird is a robust, easy to use, open source email client. It is the recommended graphical email client for using with CIM email due to it's standards compatibility and robustness. You can download it from http://www.mozilla.com/en-US/thunderbird/

To set up your CIM account in Thunderbird, the first time you run Thunderbird an add-account wizard will start up. On the “New Account Setup” screen, select that you want to add an email account.

On the “Identity” screen, enter your name and CIM email address.

On the “Server Information” screen, select “IMAP” for the server type, and enter “imap.cim.mcgill.ca” for the Incoming Server, and “smtp.cim.mcgill.ca” for the Outgoing Server.

Enter your CIM username for both the “Incoming User Name” and “Outgoing User Name”.

Enter an account name, this can be anything you like, generally it is a good idea to keep it short so it will fit on the folder list pane.

Once you have select an account name click Next and Finish. At this point, if you get an error about not being able to connect to the server, simply click Ok and ignore it.

Next, if you are using Windows click Tools→Preferences, on any other operating system click Edit→Preferences. In the dialog that comes up, under the CIM account you just added, select Server Settings. Under the Security Settings section, under Use secure connection select TLS. Make sure that Use secure authentication is 'not' selected, this is not necessary if you are using a secure connection, and it will not work. Make sure that “Clean up (Expunge) Inbox on Exit” and “Empty Trash on Exit” are also selected.

Click the Advanced... button, make sure that IMAP server directory is blank. Also ensure that “Use IDLE command if the server supports it” is selected.

Finally, click Ok until you are back at the main Thunderbird screen, and click “Get new messages”, it should be a button at the top left of the Thunderbird window.

The “Website Certified by an Unknown Authority” dialog will pop up, select “Accept this certificate permanently” and click Ok. If you want to verify the authenticity of the certificate, the CIM IMAP certificate's SHA1 Fingerprint is CF:32:00:B0:39:62:F6:E9:F8:CB:89:C4:48:AD:FE:55:0C:10:25:3B and the MD5 Fingerprint is 02:CA:A9:39:25:94:A5:EC:34:9F:80:60:41:0F:C5:79

From:
http://wiki.cim.mcgill.ca/ - **Centre for Intelligent Machines**

Permanent link:
http://wiki.cim.mcgill.ca/doku.php?id=email-legacy

Last update: **2024/10/03 16:36**