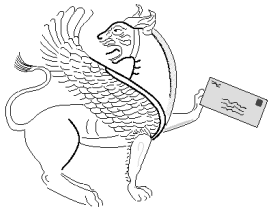
Administrator's Guide

Mulberry Internet Mail Client
(Version 3.0.2)

Cyrusoft International, Inc.
Suite 780
The Design Center
5001 Baum Blvd.
Pittsburgh PA 15213
USA.



Tel: +1 412 605 0499
Fax: +1 412 605 0705

mailto:mulberry@cyrusoft.com
http://www.cyrusoft.com

Document Revision 302.000

Cyrusoft International, Inc.
Suite 780, The Design Center,
5001 Baum Blvd.,
Pittsburgh PA15213
USA.

Contents

v3.0.2

OVERVIEW

This document provides a description of features in Mulberry that can be configured by system administrators. All of the features described are available in both the Mac OS, Win32 and Unix versions of Mulberry. The administrative options available in Mulberry include 'locking-down' certain preference values, setting up Mulberry for 'multi-user' use, and activating certain 'spoof-proof' features to prevent users from sending messages with inaccurate header information.

This document assumes that you are familiar with the operation of Mulberry and its preferences. For a detailed look at each preference value and how it affects the operation of Mulberry, please see the Mulberry Reference Guide, which comes with the main Mulberry distribution.

MULBERRY AND EMAIL SYSTEM ADMINISTRATION

Mulberry is a single component in an Internet communications system. The system at any particular site or domain encompasses not simply software components and computer networks and hardware, but also a set of policies, procedures, and user behaviors that are important determining factors in the ultimate success of an email service. Collectively, one might call the development, fine-tuning, and debugging of this broader system "administration".

The goal of this guide is to provide an overview of Mulberry's role in administering this overall Internet communications system, and assistance to the human being in charge of setting up Mulberry for a site in matching Mulberry's configuration to the needs of the site and the end users of the program. Most of this guide is a descriptive manual to the functions built into the Mulberry Administration Tool application, a software component used to pre-configure Mulberry for use in a variety of scenarios. However, this application is only a tool to enabling (or disabling) certain behaviors by users, the Mulberry application itself, and to a limited degree the interactions with various server components.

The most important part of making the best use of the Mulberry Administration Tool is to think of it as a way of enforcing policies, creating procedures, or encouraging (or discouraging) user behaviors.

Here's one small example: Mulberry allows one to limit the size of outgoing messages. Some mail (SMTP) servers can also do this. Whether Mulberry is used to limit the size of the messages being sent, or the server does it, or if this isn't done at all, is a policy question -- related to your site's security, performance, and appropriate-use goals and requirements. The Administrator's Toolkit simply provides a capability in this area for prescribing or proscribing Mulberry's capabilities, that you may or may not choose to use.

The Mulberry Administration concept is really a penumbra of facilities surrounding the Internet mail architecture and Mulberry itself. Mulberry provides close support for the Internet Messaging Support Protocol, IMSP (and its successor, the Application Configuration Access Protocol, ACAP), which provides capabilities to users and administrators to retrieve both personal and site-wide Mulberry program preferences and associated data (such as personal or shared address books). Mulberry also works with the capabilities built-in to the native operating systems on which it is designed to run. For example, standard MIME to file type and application launching defaults to that provided by the Windows Registry for Windows machines, or the Mac's Internet Preferences. And for messages and mailboxes, Mulberry works with the permissions and control systems provided by some IMAP servers. Mulberry itself is yet another part that can be administered in conjunction with these other facilities to match the bottom-line administrative goals of a particular site or set of users. Obviously, the focus of this guide is Mulberry itself and the Administrator's Toolkit application, but it should be remembered that there may be other components or layers at which it may be better or more appropriate to set administrative policy.

Similarly, there are many different "administrative scenarios" in which Mulberry is used, and for which it can be configured and tuned. The simplest is a single user using Mulberry on a single computer with a single mail account, where that user has complete control over Mulberry. Others might include serial use in public laboratories; a public access "kiosk"; shared use of a single computer by several people over a dial-up line or in a shared office; a single person using Mulberry on multiple machines for multiple email accounts; and virtually every other combination of relationships between numbers of users, machines, mail accounts, and locations.

Another way of looking at this might be as different types of end users. Some users will have little experience or sophistication with electronic mail, and pre-configuration and simplicity are probably a premium in setting up an environment for them. Others are 'power' users who want to be able to tinker with minutiae (and perhaps sometimes should be prevented from doing so!)

For each of these scenarios, a different set of pre-configurations or lockdowns might be appropriate, and the role of Mulberry in establishing and maintaining the configuration varies. There is no right or wrong approach, other than the one that works best for your users.

It may be desirable for you to configure more than one distribution copy of Mulberry based on the appropriate scenario at hand. The most common examples are where Mulberry is used in lab settings and in offices or at home by single users. A single configuration probably won't be appropriate for both sets of users.

Mulberry preferences and key data values can be locked and read in several ways. Certain preferences come 'out of the box' as defaults. These can be modified and locked into the Mulberry binary itself; saved and launched from external preferences files; saved and launched using local system defaults (such as Windows registry or Mac OS System folder

preferences); saved and launched from remote preferences services (IMSP / ACAP); or defaulted to a combination of paths. There are certain preference items that can also be changed dynamically. Mulberry can also be set into a special 'kiosk' mode, which provides a different login screen and set of behaviors. All of these values can be set and controlled to a certain degree using the Administrator's Toolkit application.

We also offer some general suggestions about expanding your set of tools above and beyond Mulberry and the Administrator's Toolkit program.

If your site isn't using IMSP or ACAP, we strongly encourage you to take look at it. We provide a separate 'Cyrusoft Guide to IMSP' as an overview of the subject and a guide to running the freeware IMSP server from Carnegie Mellon University. IMSP / ACAP provides an additional layer of capabilities, one that goes a long way towards providing a true 'kiosk' option. The Administrator's Toolkit application also has the ability to generate some defaults for these servers, described later in this document.

We also encourage the use of IMAP servers that support certain IMAP extensions which are also useful in administering a site. IMAP extensions are optional bits of functionality provided via the server, but which the client (Mulberry) must also support to make best use of them. The Access Control List (ACL) extension provides users and administrators with the ability to fine-tune, and set via Mulberry, specific access rights to specific IMAP folders. The QUOTA extension provides, through Mulberry, the ability to examine the amount of mailbox space allocated to a user and the amount remaining. The NAMESPACE extension is a way of having a server administrator provide a default list of interesting or important mailboxes or folders to users, one that's particularly useful for shared mailbox environments.

Note that some authentication and authorization policies may be better set through the server, particularly SMTP and IMAP authentication. Mulberry can be forced to use only an acceptable authentication method, or optionally configured to use multiple authentication methods. Check with your server vendor for details, and the current version of Mulberry to find out what methods are available.

This Mulberry Administrator's Toolkit is designed to make it easier in the long run to use Mulberry. To do so requires some investment in time by the Administrator in both setting up Mulberry configurations and articulating the policies and procedures instantiated by the Administrator's Toolkit program (or other servers and tools aside from Mulberry). If some of these options seem a little complex, it's to 'factor up' the complexity to the Administrator, so the end user of Mulberry and the front-line support staff answering questions on Mulberry have it much simpler.

As ever, questions, suggestions for improvements, or feature requests are warmly welcomed at the Mulberry support address <support@cyrusoft.com>.

INTRODUCTION TO THE MULBERRY ADMINISTRATION TOOL

Mulberry includes special features that allow system administrators to 'lock-down' various preference values (for example, to prevent users from using incorrect email return addresses). The application can also be configured for 'multi-user' use, a mode that makes it easy for novice users to start using Mulberry without having to set up preferences for themselves. If your site has licensed Mulberry for several users, you can also configure Mulberry with the registration details for your site, eliminating the need to give out the registration information to end-users. These special features and modes are activated through a process called preconfiguration.

There are two ways to carry out the preconfiguration process. The first allows you to modify the Mulberry application file by writing into it the required resource information for configuration. The second allows the base Mulberry installer to preconfigure Mulberry immediately after installation. The latter option is useful because it enables you to distribute a modified Mulberry installer to end users, instead of having to 'unpack' the installer, run the configuration tool on the application, and then repackage it for distribution to end users.

This document will first describe the basic concept behind the multi-user mode and then go on to describe how to use the configuration toolkit. It describes in detail each of the panels used in the 'wizard' style graphical user interface configuration application, indicating what each option in the panel controls.

New in Version 1.4

The administration tool has been completely rewritten and now features a graphical user interface. The new tool uses a 'wizard' style interface to perform the configuration and set the various configuration options. It can also be used to automatically generate the most commonly used default preferences, without having to do so in Mulberry by saving a preference file. Default IMSP options files can also be generated for use on an IMSP server in conjunction with Mulberry's remote kiosk mode.

The new administration tool also provides the ability to save standard configuration options to a user-specified file for later use, and always saves its current state to disk, for reuse the next time it is launched. This removes the previous constraint of having to re-enter all the configuration parameters each time a configuration is run.

This version of the administration tool is designed for use with Mulberry v1.4 and higher. It cannot be used with earlier versions of Mulberry, which must continue to be configured with the v1.3.x version of the Administration Tool.

In addition, Mulberry v1.4.4 and higher now supports a new type of plugin: a 'Configuration' plugin that allows full customization of the configuration process, and can be tailored to each individual site's needs.

New in Version 2.0

The administration tool has been updated to allow control over the new options provided in Mulberry v2.0 and higher. This includes adding options to lock out the use of local mailboxes for local mail storage, disconnected mail storage, POP3 mail storage and SMTP queues for outgoing messages. There is also a new option to limit the preferences and

IMSP options file output to only those preferences which are different from the built-in Mulberry defaults.

> **Important** The 2.0 version of the administration tool must only be used with Mulberry v2.0 and higher. The earlier version of the administration tool will not generate the correct set of preferences from Mulberry v2.0. Similarly, this version of the administration tool cannot generate preferences for Mulberry v1.4.x, so the earlier administration tool must still be used if configuring Mulberry v1.4.x.

New in Version 2.1

The administration tool has been updated to allow control over some new options. This includes adding options to prevent local file attachments in drafts, and prevent the use of rules and filtering. There are also new options to control the use of SSL in each account's options dialog.

New in Version 3.0

The administration tool has been updated to allow control over the new options provided in Mulberry v3.0 and higher. This includes adding options to lock the 3-pane/1-pane window state, and force the use of automatic MDN read-receipt responses. A new option to allow SMTP server addresses to be edited even when server addresses are locked has also been added to allow users at sites that need to use their local (ISP) SMTP server to still be able to change that, even when the mail servers (IMPA, POP3) are locked.

> **Important** The 3.0 version of the administration tool must only be used with Mulberry v3.0 and higher.

New in Version 3.0.2

The administration tool has been updated to be 'virtual domain' aware. Its now possible to use '*' characters in server addresses and the email domain and have a user supplied domain (as part of their user id) substituted in. This allows for a single configured version of Mulberry to work in a multiple domain/sub-domain environment, rather than requiring separate configurations for each domain/sub-domain.

Multi-User Mode

Mulberry has a ‘multi-user’ feature that allows System Administrators to configure it for use in an environment where many users use Mulberry on shared computers. It can also be used to provide a default configuration for use by individuals at a site, so that they are not required to enter configuration information into the preferences when first using the program. In all cases, users can create their own specialized preference files which can be used with Mulberry, but certain settings in the multi-user configuration can always override these.

When multi-user mode is active, a simple login dialog is presented to the user (see Figure 1) if they do not launch Mulberry with their own personalized preferences or a default set of preferences is not present.

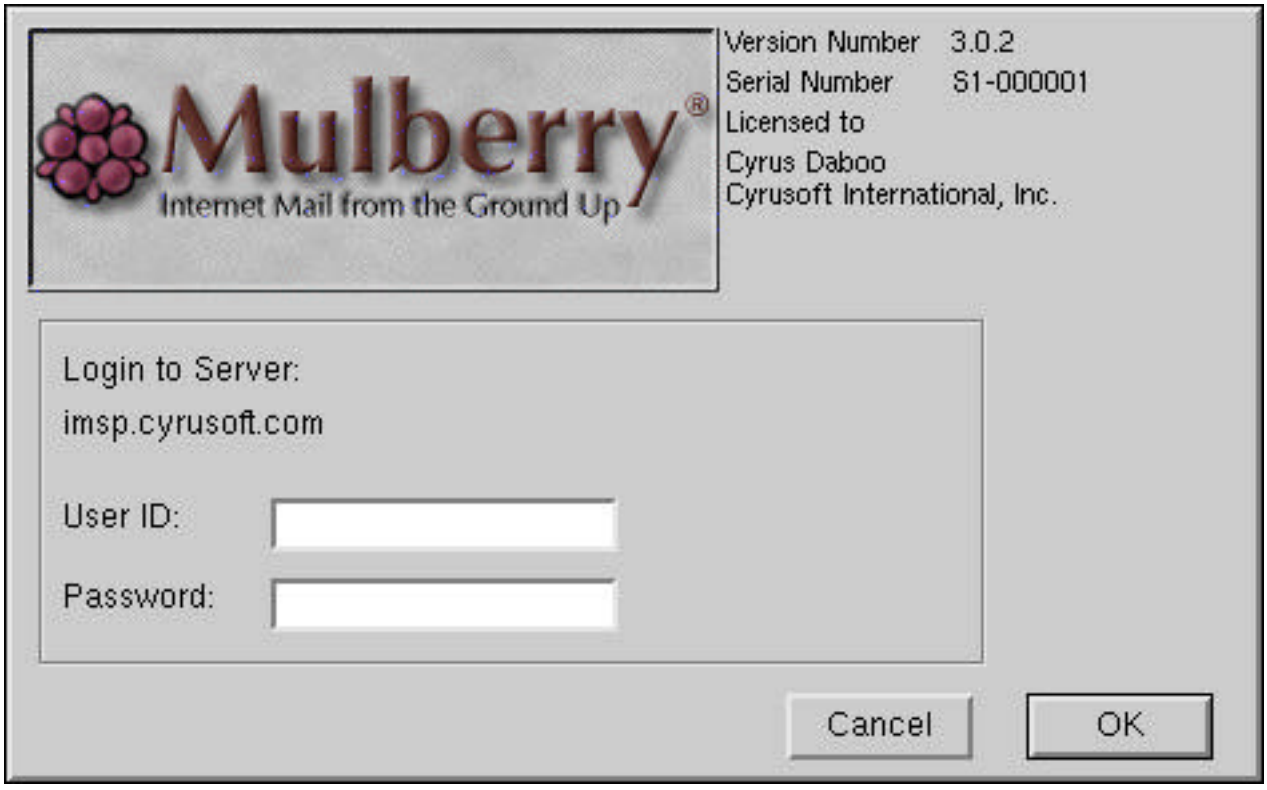


Figure 1 The multi-user start-up dialog

Note: The password field may or may not be present depending on the value of the 'Login at Startup' entry in the multi-user preferences. Also, both the User ID and Password boxes will not be present if Kerberos V4 or GSSAPI (Kerberos V5) authentication is selected. In addition, a 'Real Name' field may be present. Also, the server name can be configured to be a popup list from which the user can choose the one suitable for them.

There are a number of ways in which Mulberry can be started, and how it behaves in each case depends on whether the multi-user configuration is present and how it is configured:

- Double-clicking the application
  - No multi-user configuration:

    If a set of default preferences exist (in the Preferences folder inside the System Folder on Mac OS, or in the Windows Registry on Win32, or in the ~/.mulberry directory on Unix) Mulberry will use those as its preferences. If no default preferences exist, then Mulberry starts by displaying the Preferences dialog (see the 'Mulberry Reference Guide' for more details) and will force the user to enter the minimum required set of preference values before it will continue.
  - Multi-user configuration present:

    The System Administrator has the option of setting the multi-user configuration to allow any default preferences (in the System Folder on Mac OS, or in the Windows Registry on Win32, or in ~/.mulberry on Unix) to be used. If this option is disabled, then Mulberry will always use all the settings in the multi-user configuration, regardless of whether a default set of preferences is available or not, and it will present the user with the simple login dialog (Figure 1) on start-up. If this option is enabled, then Mulberry will use the default preferences, if they are present, ahead of the multi-user configuration, and the simple login dialog is not displayed. However, certain settings in the multi-user configuration may still be used (as described below).
- Double-clicking one of its preferences files
  - No multi-user configuration:

    Mulberry uses the information in the preference file to configure itself for use.
  - Multi-user configuration present:

    Mulberry uses the information in the preference file to configure itself for use, but certain settings in the multi-user configuration may still override the user's settings (as described below). The simple login dialog is not displayed.
- Double-clicking another type of Mulberry document (either an address book or a draft message)

  This is equivalent to double-clicking the application, except that the documents double-clicked will be opened after the application has started up.

MULBERRY PRE-CONFIGURATION

Changing the Configuration

You should always keep an unmodified copy of Mulberry or its base installer in a safe place just in case you need to revert to the original settings.

The configuration program gives you the option of configuring the application or the installer, simply by choosing the appropriate file to configure. It then presents a series of 'wizard' style panels that allow you to setup the parameters for the pre-configuration and internal registration. Internal registration will only succeed if valid registration details are entered. For security purposes, the configuration program will never save the registration code, and thus requires this to be entered each time a configuration is done. This ensures that end users (who should not have access to the registration details for the site) are unable to modify the configuration information without destroying the registration details.

You can choose to remove configuration or registration information from an application or installer by turning off all the relevant options.

Configuring the installer allows you to distribute the base Mulberry installer without having to unpack it, configure Mulberry, and then repackage it for distribution at your site. When the pre-configured installer runs, it will pre-configure and pre-register Mulberry immediately after installation. The administration tool directly modifies the Mac OS installer. For the Win32 installer, it produces a 'Mulberry.key' file that should be distributed with the base installer. The Win32 installer will look for this file after installing Mulberry and use it to do the pre-configuration and pre-registration. The file itself is encrypted and thus tamper-proof. On Unix the administration tool can only modify the application file itself.

Special Note About Using an IMSP Server

It is possible to configure Mulberry to always retrieve a user's personal preferences from an IMSP remote preference server. When this mode is selected, it is necessary to add a set of default preferences to the IMSP server itself, so that brand new users, who have not previously used Mulberry and IMSP, will 'inherit' the correct settings for things like their email address and IMAP server. The new administration tool includes an option to automatically generate the default IMSP options file for the chosen configuration which can then be merged with the actual default options file on the IMSP server. More information on this process can be found in the 'Cyrusoft Guide to IMSP', available at ftp://ftp.cyrusoft.com/pub/Mulberry/docs/imsp_guide.pdf.

Running the Administration Tool

General

To run the administration tool, double-click its icon in the Finder (Mac OS), or the Explorer (Win32), or launch it via the command line on Unix. This will launch the application, which will display a series of 'wizard' style panels that allow all configuration options to be set. The main application window is shown in Figure 2.

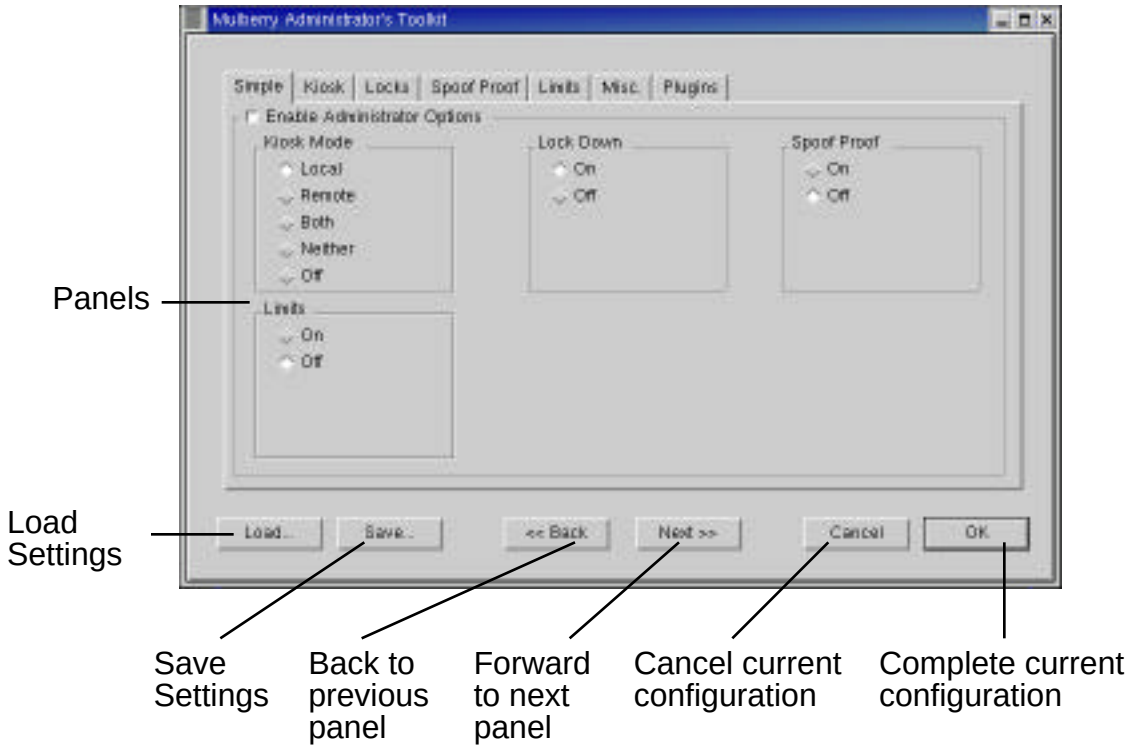


Figure 2 The main administration tool window

Items	*Description*
Panels	This area displays the set of 'wizard' panels used to set and apply the configuration options. Use the **Back** and **Next** buttons to move between the panels.
Load...	Click to load a different set of options that was previously saved to a file on disk. This will result in a standard open file dialog, allowing the relevant file to be chosen.
Save...	Click to save the current set of options to a file, which can subsequently be loaded to restore the options. Use this in conjunction with the **Load...** button to save and restore frequently used configuration options.

<<Back	Click to display the previous panel in the panel area. This button will be disabled when the first panel is shown.
Next>>	Click to display the next panel in the panel area. This button will be disabled when the last panel is shown.
Cancel	Click to cancel the current configuration process. This will exit the application without saving the current settings.
OK	Click to initiate the configuration process. You can click this button at any time, irrespective of which panel is currently visible. If there are errors in the configuration, you will be automatically taken to the last panel in the set, which will show the errors.

Application/Installer Choice Panel

The first panel in the administration tool is shown in Figure 3. This panel is used to select which file, either an application file or an installer file, is to be operated on by the administration tool.

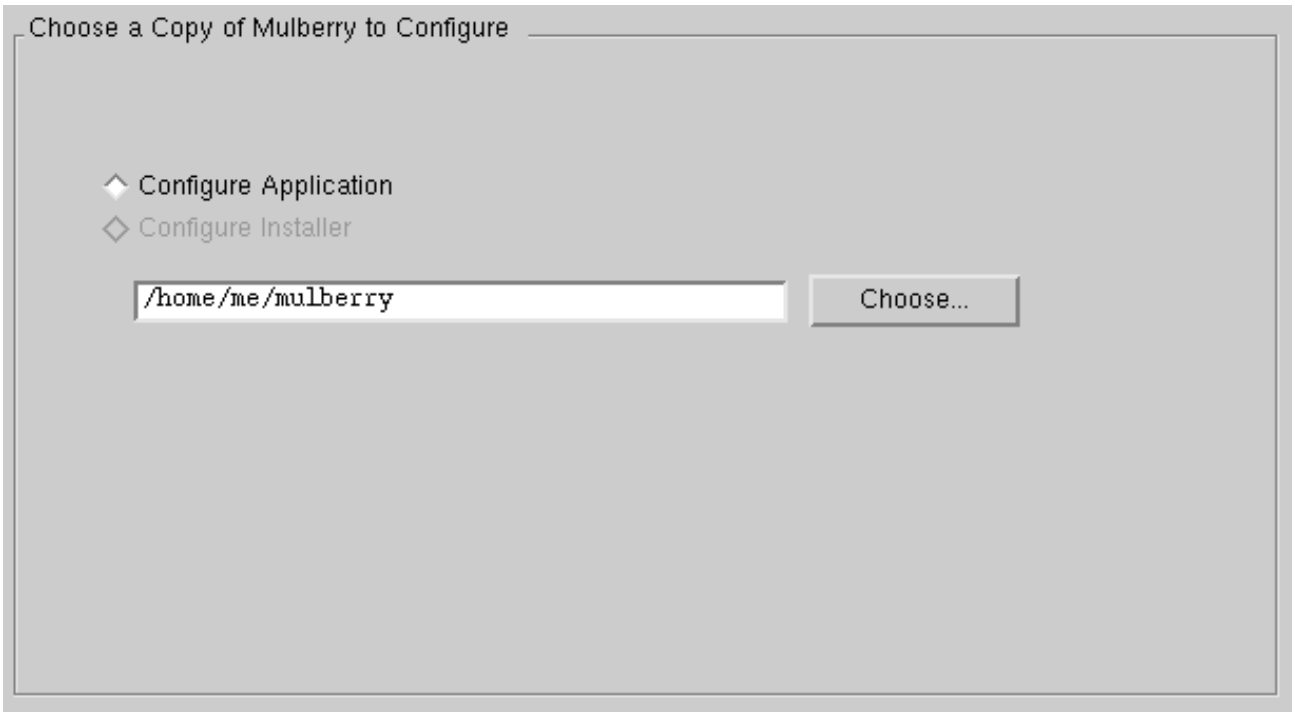


Figure 3 The Application / Installer choice panel

Items	*Description*
Configure Application	Select this option if you wish to configure and register a copy of the Mulberry application.

Configure Installer	Select this option if you wish to generate configuration and registration information for the Mulberry installer. **Note:** The option to configure an installer is not available on Unix as Mulberry is only distributed as a tar file.
File Name	This shows the full path name of the file that will be configured. This will either be a Mulberry application file or an installer file. On Mac OS this field cannot be edited. Use the **Choose** button to change it.
Choose...	Click to browse for the file to configure. You should choose a Mulberry application file or an installer file.

Registration Panel

The second panel in the administration tool is used to set the registration details that will be used to internally register the copy of Mulberry being configured, or the copy of Mulberry being installed by the installer being configured. If you choose to internally register the application, you must provide valid registration details in this panel. The administration tool will never save the registration code value to disk. Instead you will need to re-enter it each time you run the administration tool.

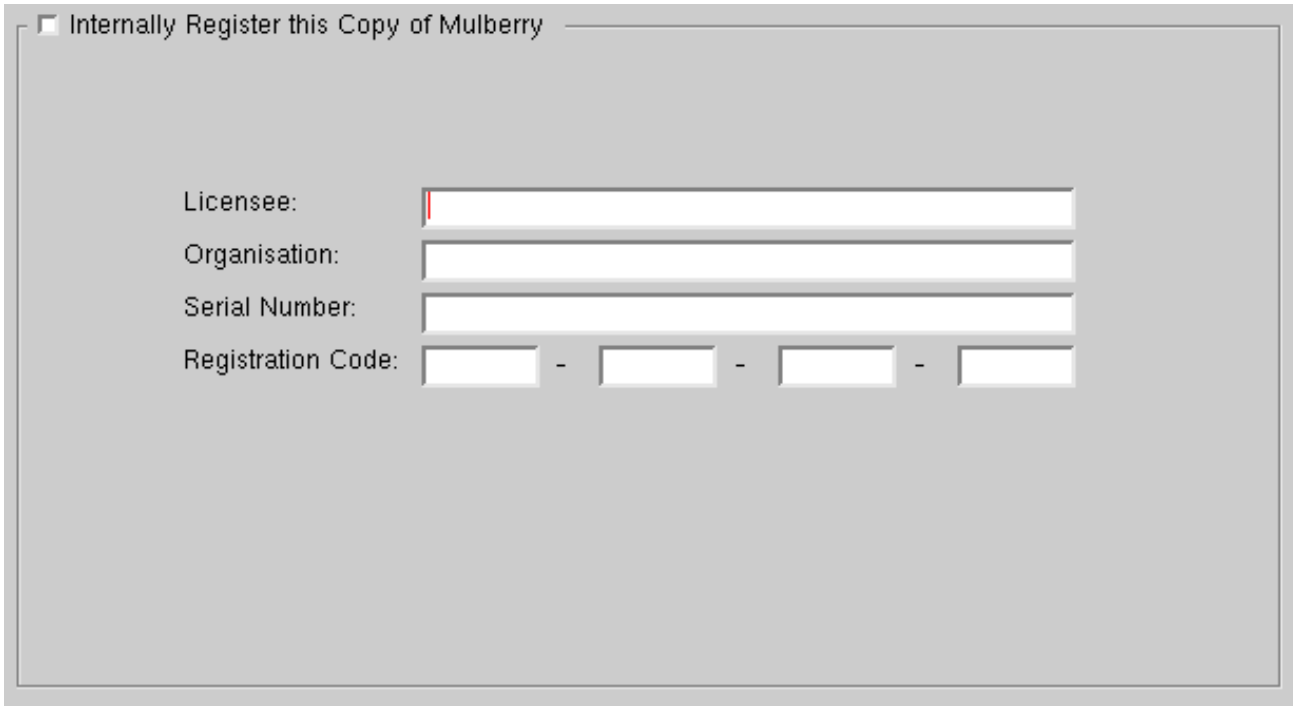


Figure 4 The Registration panel

Items	*Description*
Internally Register this Copy of Mulberry	Turn this on to pre-register the copy of Mulberry being configured. When applied to the Mulberry application file, this will insert the registration details into the application file. When applied to an installer, the installer will add the registration details after installing a copy of Mulberry. Leave this option off if you are not pre-registering Mulberry. If off, the remaining fields in the panel will be disabled. **Advice:** Turn this option on and use the registration details provided for your site so that end-users do not need to register the application themselves.
Licensee Name	Enter the *Licensee* details for this registration. This value is optional and can be whatever you like. **Advice:** Enter some text describing the name of your institution, or a department within the institution.
Organization	Enter the *Organization* details for the registration. This value is optional and can be whatever you like. **Advice:** Leave this empty, or enter some text describing your institution if you entered a department name in the **Licensee Name** field.
Serial Number	Enter the *Serial Number* value provided in your Mulberry registration exactly as it appears in the registration document. This value is required if pre-registration is turned on.
Registration Code	Enter the 16 character *Registration Code* value provided in your Mulberry registration exactly as it appears in the registration document. This value is required if pre-registration is turned on.

Configuration Panels

The third panel contains a set of seven tabs, each of which is used to set the administrative options for the configuration being applied. The administrator controls are grouped into six sets:

- **Kiosk** – options that enable kiosk mode operations, to enable multiple users to use the same copy of Mulberry on one machine.
- **Locks** – options that lock down various preference values in Mulberry to prevent users from accidentally or deliberately changing crucial preference values.
- **Spoof Proof** – options that lock down various preference values relating to the identity of the person who is using Mulberry. This is used to help prevent users from faking email from other people, and to confirm the identity of the actual sender.
- **Limits** – options that limit the use of Mulberry to prevent users from overstepping bounds when using email.

- **Miscellaneous** – other options that do not fit into any of the categories listed above.
- **Plugins** – options that define the behavior of the various plugins included with the Mulberry distribution.

The first tab presents a simple set of 'on / off' options for the first four categories listed above. Turning on a category will result in the administration tool setting the options in that category to default values used in a standard configuration. Setting the options in the other tabs allows a finer control of the configuration in more advanced situations. In most cases you should be able to just set the options in the **Simple** tab.

Simple Tab

The first tab in the administration tool is shown in Figure 5. This panel presents a simple interface to Mulberry's administrative options, allowing an administrator to turn on or off different general categories of options.

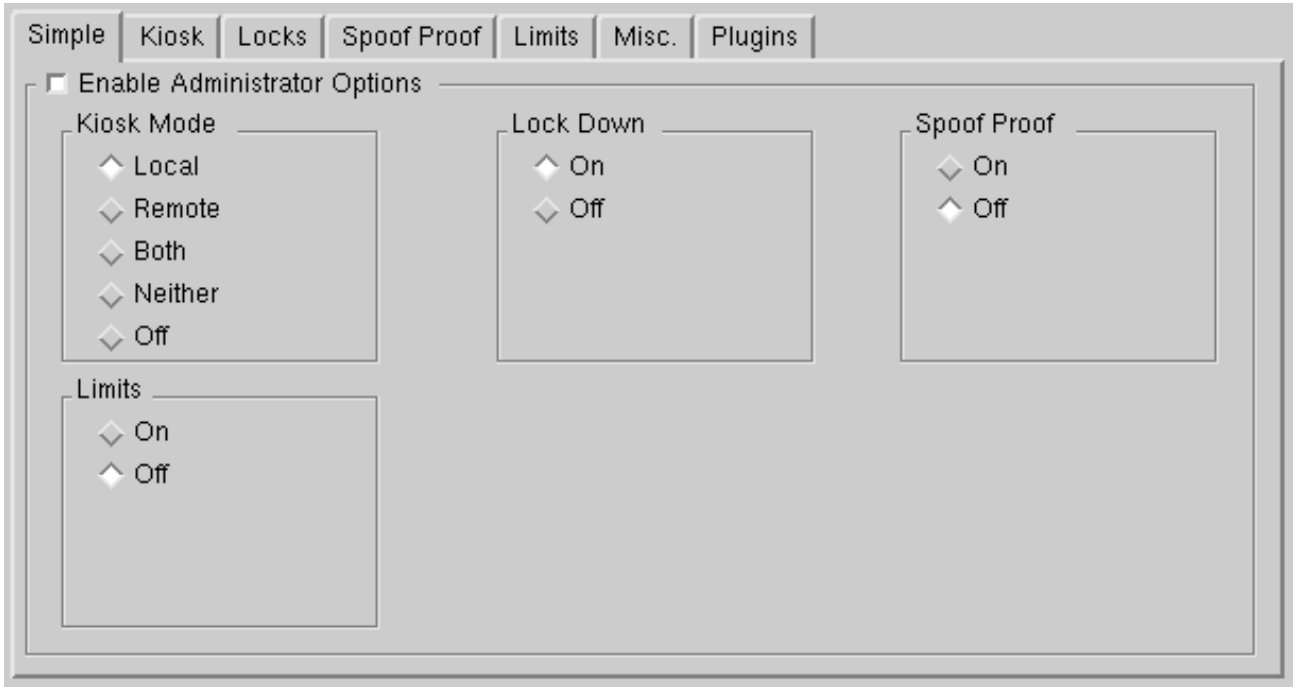


Figure 5 The Simple tab

Items	*Description*
Enable Administrator's Options	Turn this on to enable the administrator options. When this is on, the administration tool will add the administrative options to the Mulberry application or installer being configured. Turn this off to remove any existing configuration in the chosen Mulberry application or installer. If you do this, the other tab panels will be disabled.

Kiosk Mode	· **Local** – enables the kiosk options and sets them to default values used with local preferences. Use this option when you do not have a remote preference server. · **Remote** – enables the kiosk options and sets them to default values used with remote preferences. Use this option when you have an IMSP or ACAP server for storage of remote preferences. This ensures that only remote preferences can be used to startup, and that if the remote preference server is not available, Mulberry will not startup. · **Both** – enables the kiosk options and sets them to default values used with both local and remote preferences. Use this option when you have an IMSP or ACAP server for storage of remote preferences. This ensures that if the remote preference server is not available, then a default set of local preferences will be used instead. · **Neither** – enables the kiosk options and prevents the user from saving or using any preferences, either local or remote. Only the built-in administrative preferences, as specified later in the administration tool, will be used. · **Off** – disables the kiosk options.
Lock Down	· **On** – enables the lock down options and sets them to default values. · **Off** – disables the lock down options.
Spoof Proof	· **On** – enables the spoof proof options and sets them to default values. · **Off** – disables the spoof proof options.
Limits	· **On** – enables the limit options and sets them to default values. · **Off** – disables the limit options.

Kiosk Tab

The second tab, shown in Figure 6, allows administrative options relevant to Mulberry's kiosk mode to be set.

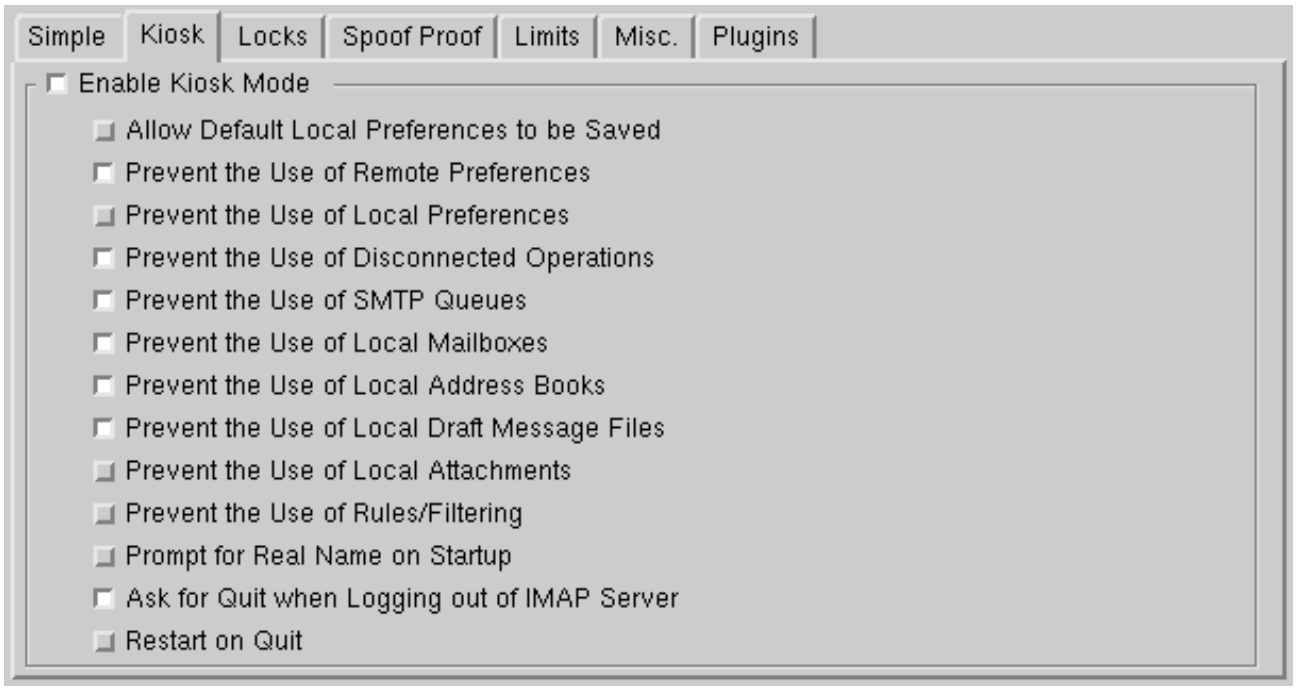


Figure 6 The Kiosk tab

Items	*Description*
Enable Kiosk Mode	Turn this on to enable the kiosk mode options. When this is on the administration tool will add the kiosk mode options to the copy of Mulberry being configured. Turn this off to prevent the kiosk mode options from being used to configure Mulberry.

Allow Default Local Preferences to be Saved	Turn this on to allow users to save their default preferences on the local machine. Default preferences are stored in the 'System Folder:Preferences' directory on Mac OS, in the Windows registry on Win32, and in the ~/.mulberry directory on Unix. Turn this off to prevent users from saving their default preferences on the local machine. When this option is off, the 'Save Default' button will be unavailable when Local preferences are being used. **Advice:** Turn this option off for copies of Mulberry used on shared machines. This will prevent one user 'leaving behind' their preferences for the next user to pick-up. Turn this option on for copies of Mulberry used by individuals on their own machine, so that they can have their default set of preferences automatically saved and reused each time Mulberry is launched.
Prevent the Use of Remote Preferences	Turn this on to prevent the use of remote preference servers. The remote preference controls will be disabled in the preferences dialog, and Mulberry will not make a connection to a remote preference server even if launched with a preference file that requests such a connection. **Advice:** Turn this option on if you do not have a remote preference server (and are not likely to add one in the near future).
Prevent the Use of Local Preferences	Turn this on to prevent the use of local preference files. The local preference controls are disabled in the preferences dialog, and Mulberry will not run unless a remote connection can be made to the server specified in the multi-user configuration.
Prevent use of Disconnected Operations	Turn this on to prevent the use of disconnected operations with IMAP accounts. Mulberry will prevent connect/disconnect commands, and disable synchronization for IMAP mailboxes in any accounts marked for disconnected operations. **Advice:** Turn this option on if you do not want users to have cached disconnected messages stored on local disk.
Prevent use of SMTP Queues	Turn this on to prevent the use of SMTP queues to store outgoing messages and send them in the background. **Advice:** Turn this option on if you do not want users to accidentally leave outgoing messages stored on local disk.
Prevent the use of Local Mailboxes	Turn this on to prevent the use of Local and POP3 mailbox accounts. **Advice:** Turn this option on if you do not want users to leave messages stored on local disk.

Prevent the Use of Local Address Books	Turn this on to prevent the use of local address books. The 'Local' folder in the Address Book Manager will be disabled. **Advice:** Turn this option on if you do not want users to leave address books stored on local disk.
Prevent the Use of Local Draft Message Files	Turn this on to prevent users from saving draft messages on the local computer. The 'Save' and 'Save As…' menu options will be disabled when a draft window is active. **Advice:** Turn this option on if you do not want users to leave outgoing messages stored on local disk.
Prevent the Use of Local Attachments	Turn this option on to prevent users from adding local files as attachments to drafts. **Advice:** Turn this on for versions of Mulberry being configured for use on shared / public access work stations, where local files will not be accessible to users.
Prevent the Use of Rules/Filtering	Turn this option on to prevent users from creating and using rules for filtering messages.
Prompt for Real Name on Startup	Turn this on to have Mulberry prompt the user for their real name on startup. If a user launches Mulberry using a preference file that has the 'Name' field on the 'From' tab of the default identity undefined, a box will appear asking the user to enter their real name.
Ask for Quit when Logging out of IMAP Server	Turn this on to have Mulberry prompt the user when they click the 'Logout' button. The user will be presented with a choice of just logging out of the IMAP server, or completely quitting the Mulberry application.
Restart on Quit	Turn this on to have Mulberry automatically restart itself and display the multi-user login dialog after a user selects the Quit (Mac OS or Unix) or Exit (Win32) command from the File menu. **Advice:** Use this to implement a 'true kiosk' in which a copy of Mulberry is always running waiting for the next user to arrive.

Locks Tab

The third tab, shown in Figure 7, allows certain Mulberry features to be locked down when the multi-user settings are active.

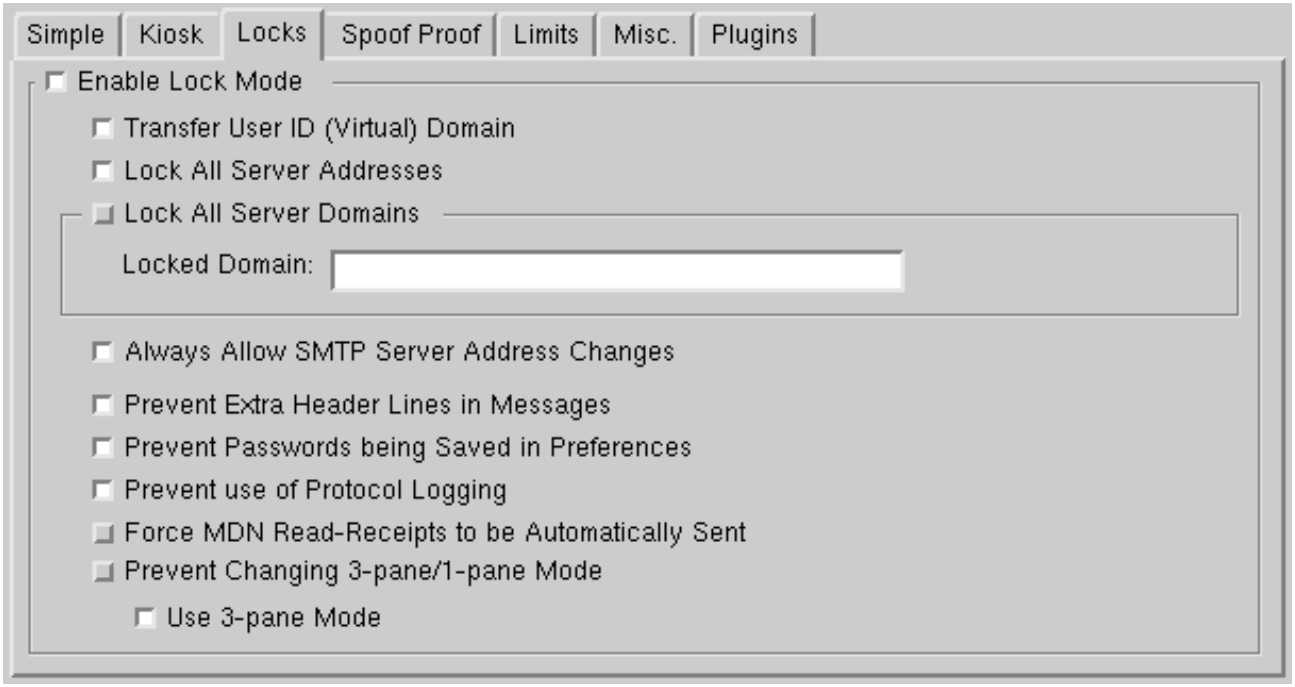


Figure 7 The Locks tab

Items	*Description*
Enable Lock Mode	Turn this on to enable the lock-down mode options. When this is on, the administration tool will add the lock-down mode options to the copy of Mulberry being configured. Turn this off to prevent the lock-down mode options being used to configure Mulberry.
Transfer User ID (Virtual) Domain	Turn this on to have a domain supplied by the user in their user id substituted for '*' characters wherever they appear in server addresses or the email domain.
Lock All Server Addresses	Turn this on to prevent users from changing any server IP addresses for any type of account, including IMAP, SMTP, IMSP preference or address accounts, ACAP, and LDAP accounts.

Lock All Server Domains	Turn this on to limit all server IP addresses to a particular domain (which you must enter in the 'Locked Domain' box if you select this option). **Advice:** Turn this on to prevent users from using servers outside of your domain. This option is useful if you want to ensure that only end users at your site can use the copy of Mulberry registered to you, since only those with accounts on your servers will be able to use it. (e.g. for domain 'cyrusoft.com', 'imap.cyrusoft.com' and 'smtp.cyrusoft.com' would be valid, but 'imap.cmu.edu' or 'smtp.cam.ac.uk' would not.)
Locked Domain	If you have selected the 'Lock All Server Domains' option, enter the domain to which you wish to limit server IP addresses in this box.
Always Allow SMTP Server Address Change	If you have selected either 'Local All Server Addresses' or 'Local All Server Domains' above, turning on this option will unlock the SMTP server address entry only. **Advice:** This allows users to change their SMTP server address to a local SMTP server (e.g. an ISP's) even when the other server addresses are locked down. This may be required in order to work around anti-relaying policies of your site or the ISP.
Prevent Extra Header Lines in Messages	Turn this on to prevent users from entering their own email header lines for inclusion in messages they send. This applies to the main identity, and any user defined identities.
Prevent Passwords being Saved in Preferences	Turn this on to prevent the saving of passwords to local or remote preference sets. **Advice:** This is useful if it is likely that users' preference files can be accessed by someone other than themselves. The passwords are encrypted when saved in a preference set, but another user can gain access to the email account of the person to whom the preferences belong if passwords have been saved and they gain access to the preference file.
Prevent use of Protocol Logging	Turn this on to prevent users from turning on protocol logging in Mulberry to record data sent to and from a server.
Prevent use of Personal Internet Config settings **(Mac OS only)**	Turn this on to prevent the use of personal Internet Config settings.

Force MDN Read-Receipts to be Automatically Sent	Turn this on to force automatic sending of MDN read-receipts when a read-receipt is requested by the sender of the message. **Advice:** This is useful if you need to enforce a policy of requiring read-receipts as acknowledgements of successful message delivery and read.
Prevent Changing 3-pane/1-pane Mode	Turn this on to prevent users from changing the 3-pane or separate windows mode of the Mulberry user-interface. **Advice:** Use this in conjunction with the next option to force users to use a particular windowing mode.
Use 3-pane Mode	When the previous option is on, turn this on to Mulberry to use 3-pane mode, or turn this off to Mulberry to use separate window mode. When the previous option is off, this option controls the initial setting for the window mode in Mulberry. By default 3-pane mode is used for all new users. If you wish to default to separate window mode, turn this option off.

Spoof Proof Tab

The fourth tab, shown in Figure 8, enables certain options to prevent users from 'spoofing' messages, or making it appear that a message originated from a different user or site.

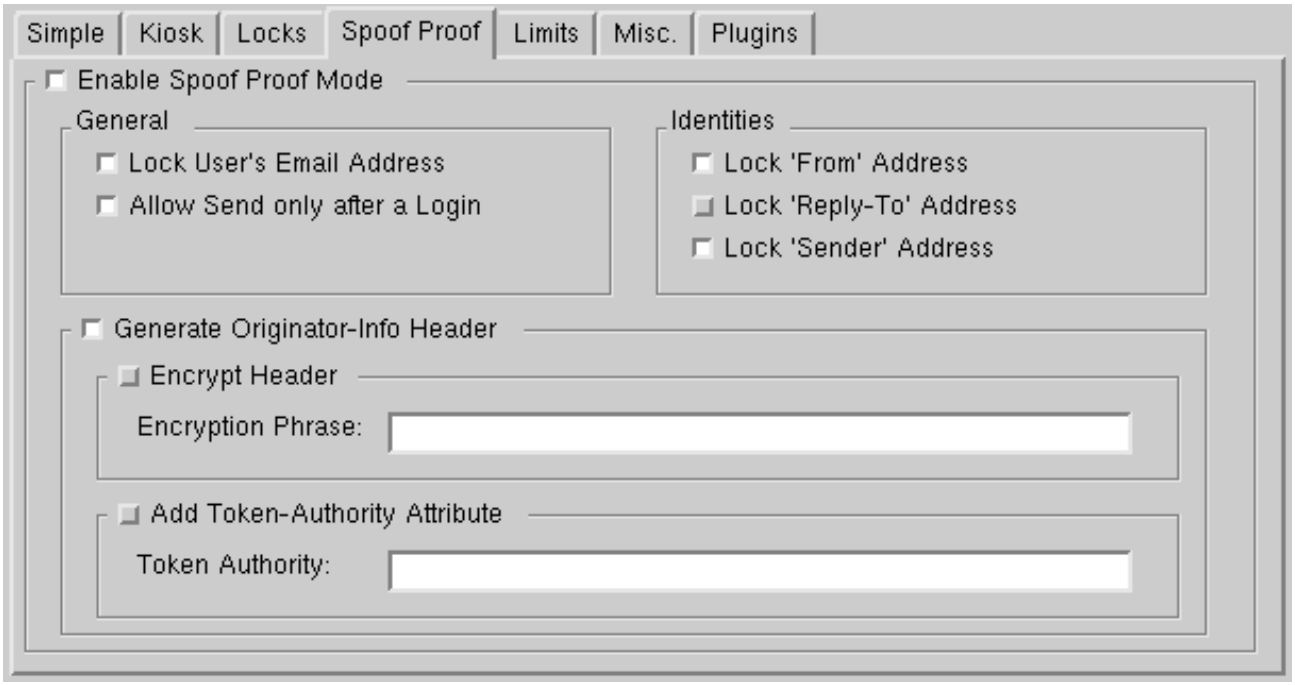


Figure 8 The Spoof Proof tab

Items	*Description*
Enable Spoof Proof Mode	Turn this on to enable the spoof-proof mode options. When this is on, the administrator's tool will add the spoof-proof mode options to the copy of Mulberry being configured. Turn this off to prevent the spoof-proof mode options from being used to configure Mulberry.
Lock User's Email Address	Turn this on to ensure that the 'From' address for email sent with Mulberry always has the correct value for the user running Mulberry. When this option is on, Mulberry will form the 'From' address by concatenating the IMAP user ID and the 'Return Address' value in the multi-user preferences, and inserting an '@' between them (if required). This occurs after at least one successful login to the IMAP server with one particular IMAP user ID. Mulberry will not send mail unless at least one successful IMAP login with the current user ID has been completed. Also, if the user changes the user ID or server address in the preferences, the 'From' address will be invalidated, forcing another successful IMAP login before mail can be sent.
Allow Send only after a Login	Turn this option on to prevent users from sending messages without first making a successful login to an IMAP server.
Lock 'From' Addresses	Turn this on to prevent users from using a different 'From' address than their default when setting up user-defined identities.
Lock 'Reply-To' Addresses	Turn this on to prevent users from using a different 'Reply-To' address than their default when setting up user-defined identities. **Advice:** In general you should turn this off to allow reasonable use of identities. However, in situations where identities may be misused, turn this option on.
Lock 'Sender' Addresses	Turn this on to prevent users from using a different 'Sender' address than their default when setting up user defined identities.
Generate 'Originator-Info' Header	Turn this on to generate the 'Originator Info' header in an outgoing message. See the later descriptive section on the Originator-Info header for more details. For more information see 'Originator-Info Header' on page 38.
Encrypt Header	Turn this on to encrypt the information in the 'Originator-Info' header. If you select this option, you must enter an encryption phrase in the next field. This option is only available if you turn on the 'Generate Originator-Info Header' option above. For more information see 'Originator-Info Header' on page 38.

Encryption Phrase	Enter the encryption phrase for the Originator-Info header in this box. You will need to remember this phrase to decrypt the Originator-Info header. For more information see ‘Originator-Info Header’ on page 38.
Add Token-Authority Attribute	Turn this on to have a token-authority value appear in the Originator-Info header. For more information see ‘Originator-Info Header’ on page 38.
Token Authority	Enter the token–authority value here when the above option is on. For more information see ‘Originator-Info Header’ on page 38.

Limits Tab

The fifth tab, shown in Figure 9, allows you to set limits on particular attributes of outgoing mail messages as well as generate warnings when a message exceeds a set of limits.

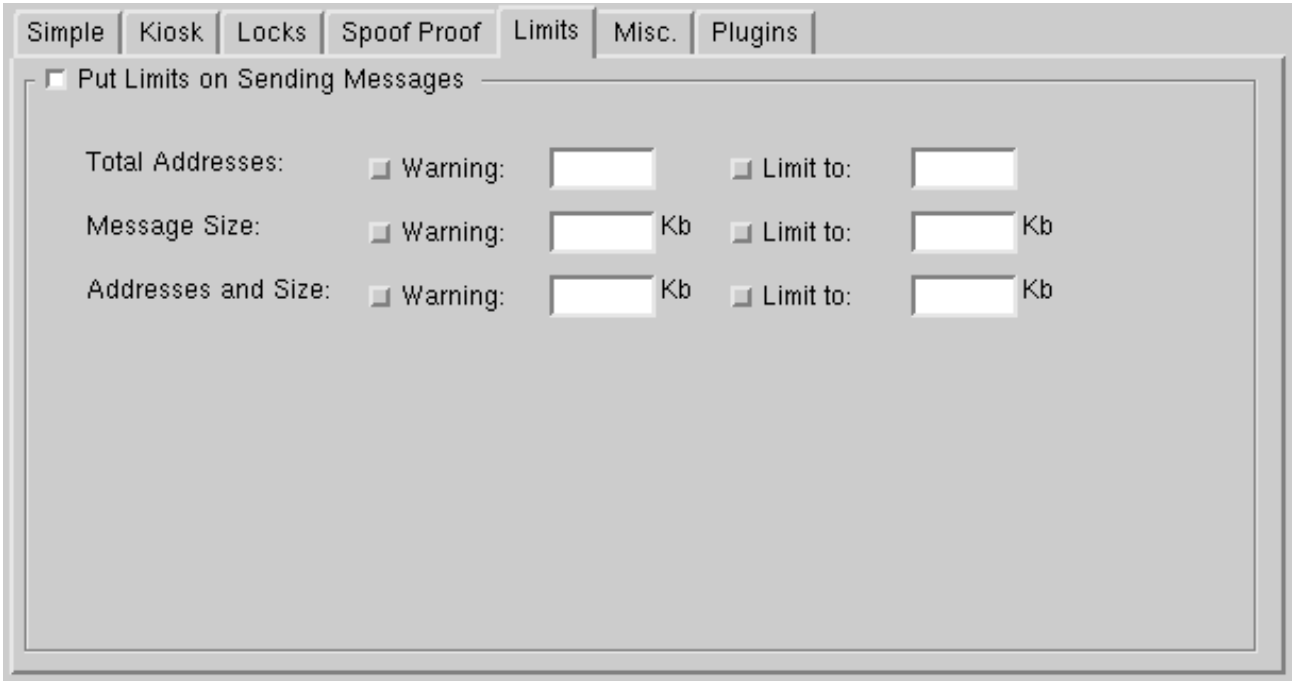


Figure 9 The Limits tab

Items	*Description*
Put Limits on Sending Messages	Turn this on to enable the outgoing message limits options. When this is on, the administration tool will add the outgoing message limits options to the copy of Mulberry being configured. Turn this off to prevent the outgoing message limits options from being used to configure Mulberry. Note: For each of the options below, selecting the 'Warning' checkbox and entering a value in the box to the right will cause the user to be warned before sending an outgoing message that exceeds the chosen value. Selecting the 'Limit to' checkbox and entering a value in the box to the right will prevent messages that exceed the chosen value from being sent. The 'Warning' and 'Limit to' options can both be active at the same time, and different values can be used for each.
Total Addresses	Turn this on to warn the user and/or prevent a message from being sent when the total number of recipients in the To:, CC:, and BCC: lines exceeds a certain number.
Message Size	Turn this on to warn the user and/or prevent a message from being sent when the total size of the message body, in kilobytes, exceeds a certain size.
Addresses and Size	Turn this on to warn the user and/or prevent a message from being sent when the size of the message body multiplied by the total number of recipients, in kilobytes, exceeds a certain size.

Miscellaneous Tab

The Miscellaneous tab, shown in Figure 10, allows various other administrative options to be set.

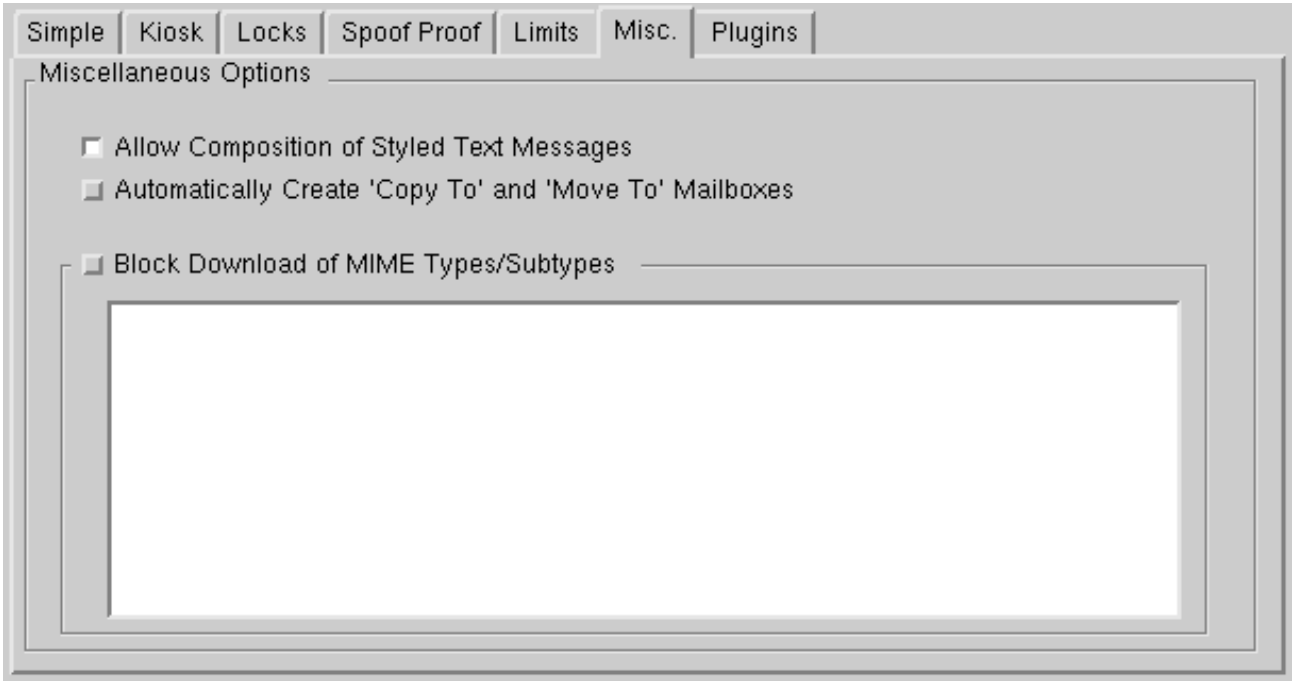


Figure 10 The Miscellaneous tab

Items	*Description*
Allow Composition of Styled Text Messages	Turn this off to prevent users from directly composing text/enriched and text/html messages in Mulberry (they can still attach files and change the MIME type/subtype accordingly). **Advice:** This is useful to prevent the use of styled text if it is found objectionable, or is likely to cause interoperability problems with users using other clients.
Automatically Create 'Copy To' and 'Move To' Mailboxes	Turn this on to have the default 'Copy To' and 'Move To' mailboxes (if specified in the preferences) automatically created when a user logs in. This is useful for users with new accounts who do not yet have these mailboxes set up. It also alleviates the need for the site administrator to pre-create these mailboxes for new user accounts.

Block Download of MIME Types and Subtypes	Turn this on to prevent users from downloading certain MIME type/subtype pairs. Enter each type/subtype that you wish to block in the text box below, one on each line. You can use the '*' character as a 'wildcard' to match a pattern (e.g. 'image/*' will block all image types with any subtype.

Plugins Tab

The Plugins tab, shown in Figure 11, allows you to enable and disable various plugins that are included with the Mulberry distribution as well as define their behavior.

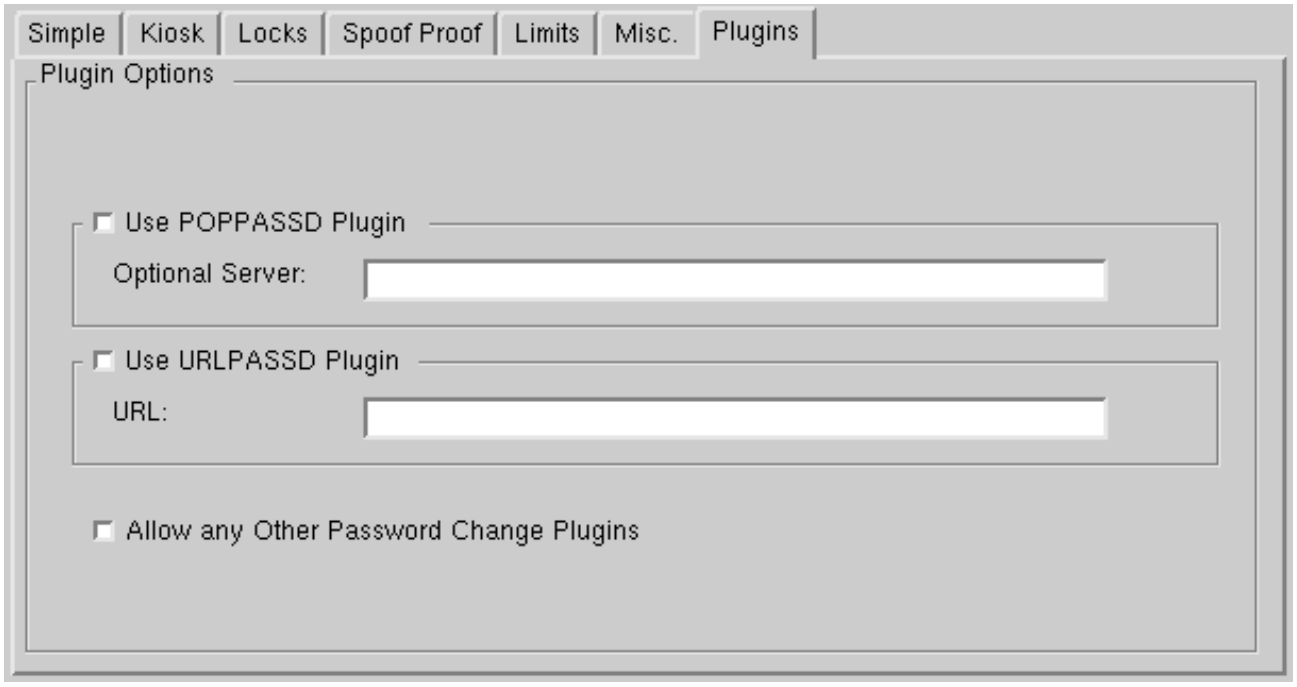


Figure 11 The Plugins tab

Items *Description*

Upgrade 1.3 Plain Text Authentication To	Turn this on to change the authentication method when a preference file is converted from v1.3 to v1.4 and higher format. When a v1.3 preference file is used to launch Mulberry v1.4 or higher, the authentication method for all IMAP Mailbox, IMSP Options, and IMSP Address Book accounts will be set to the option you choose in the popup to the right, either CRAM-MD5, DIGEST-MD5 or Kerberos V4. **Advice:** You only need to use this when converting users of Mulberry v1.3 to later versions and switching their authentication method to something other than Plain Text.
Use POPPASSD Plugin	Turn this on to allow users to use the POPPASSD password-changing plugin. When users select the "Change Password" option from the Edit menu, Mulberry will connect to a poppassd server and attempt a password change. If you have a poppassd server running on a different host than the one for which the password is being changed, you can enter the hostname in the next field. Turn this off to disable the use of the POPPASSD plugin.
Optional Server	Enter the name of the server running poppassd. If you do not enter a value in this field, Mulberry will assume poppassd is running on the same server that the account whose password is being changed is set to.
Use URLPASSD Plugin	Turn this on to allow users to use the URLPASSD password-changing plugin. When users select the "Change Password" option from the Edit menu, Mulberry will launch the URL specified in the next field, which can be any URL type (e.g. web – http / https, email – mailto, etc).
URL	Enter the URL that Mulberry launches when the URLPASSD plugin is used.
Allow Any Other Password Change Plugins	Turn this on to allow the use of future password-changing plugins that may be included with the default Mulberry distribution. Turn this off to disable the use of future password-changing plugins that may be included with the Mulberry distribution.

Default Preferences Override Panel

The next panel in the administration tool allows you to specify a Mulberry preferences file to override any preferences specified in the configuration panels (which follow), as well as add other pre-configuration information (e.g. window positions, server names, etc.) to the application or installer that you are configuring. In most cases, you will only need to set the options that are available to you in the subsequent configuration panels and hence should not enable this panel. For experienced system administrators, this panel gives maximum control over the configuration of all available Mulberry preferences.

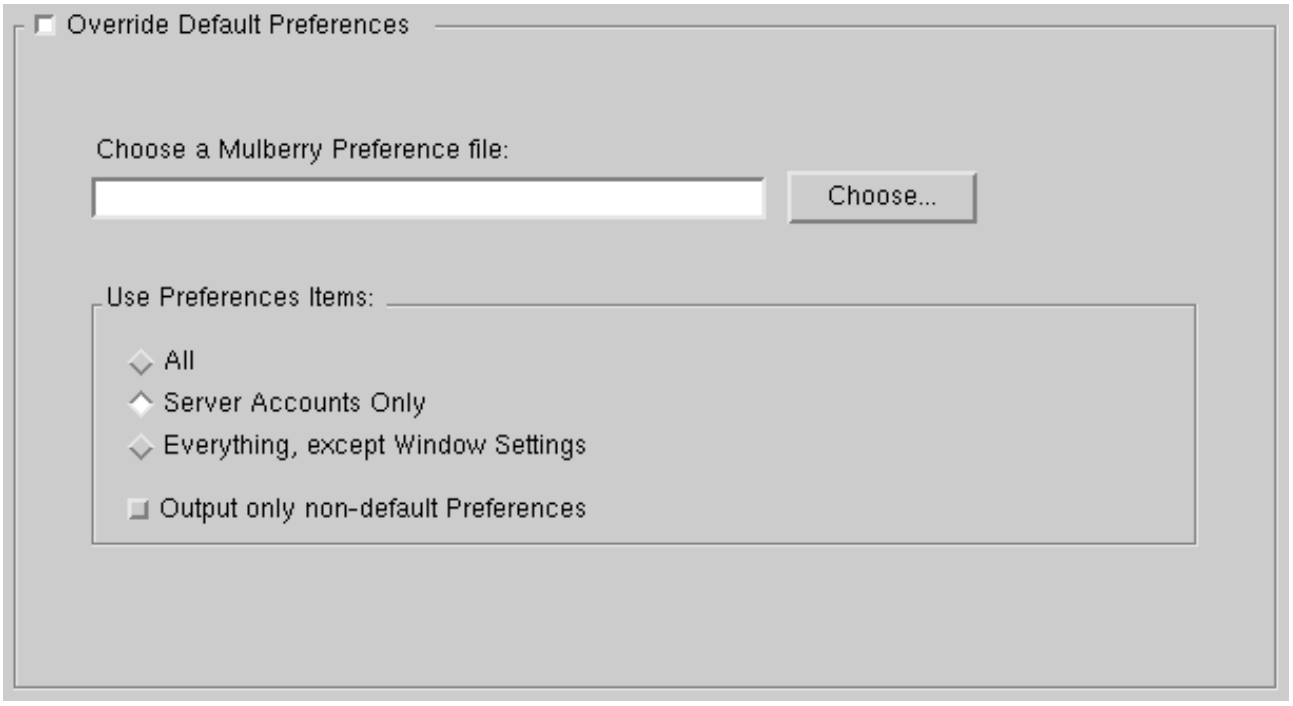


Figure 12 The Override Default Preferences panel

Items	*Description*
Override Default Preferences	Select this option if you wish to specify an external preference file to use in configuring the Mulberry application or installer that you've selected. Any items previously set in the subsequent configuration panels will be ignored.
Choose a Mulberry Preference File	This shows the full path name of the preference file that will be used. On Mac OS this field cannot be edited. Use the **Choose** button to change it.
Choose…	Click to browse for the preference file to use. You can only choose a Mulberry preference file.

All	Select this option to use all preferences in the selected file to configure the Mulberry application or installer.
Server Accounts Only	Select this option to use only the 'Accounts' preferences in the selected file to configure the Mulberry application or installer.
Everything, except window settings	Select this option to use all preferences in the selected file, except those that specify window positions, to configure the Mulberry application or installer.
Output only non-default Preferences	Turn this on to reduce the preferences output to only those that are different from the built-in Mulberry defaults. **Advice:** This is useful to reduce the size of the preferences and IMSP options output by the administration tool.

Multi-User Local Preferences Panel

If you chose not to override the default preferences in the Default Preferences Override panel, and you have set administrative options in previous panels that require Mulberry to have built-in local preferences, the next panel displayed will be the Multi-User Local Preferences panel. This panel allows you to specify a minimal set of local preferences that will allow Mulberry to successfully operate in multi-user mode. To the far-right of each field in this panel, Mulberry distinguishes between preferences that are required and those that are optional.

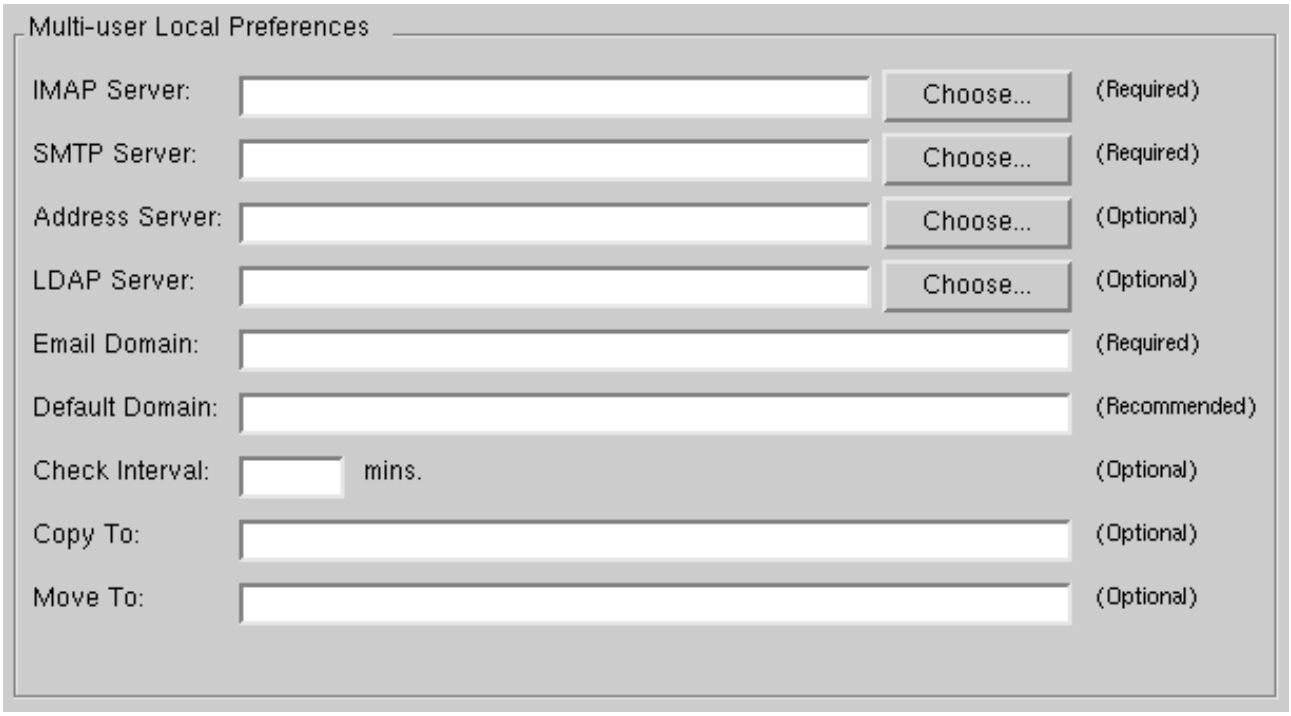


Figure 13 Multi-user Local Preferences Panel

Items	*Description*
IMAP Server	Enter the hostname of your IMAP server. This field is required. The **Options** button allows you to configure the authentication method, security (SSL) settings, directory separator, use of the automatic hierarchy list, and individual search hierarchies for the IMAP server.
SMTP Server	Enter the hostname of your SMTP server. This field is required. The **Options** button allows you to configure the authentication method and security (SSL) settings used when connecting to the SMTP server.
Address Server	Enter the hostname of your remote address book server. This field is optional. The **Options** button allows you to specify the protocol used by the server (either IMSP or ACAP) as well as the authentication method and security (SSL) settings used when connecting to the server.
LDAP Server	Enter the hostname of your LDAP server. This field is optional. The **Options** button allows you to specify the authentication method used when connecting to the server as well as the various LDAP attributes.

Email Domain	Enter the domain name used in email addresses at your site. This field is required. Mulberry concatenates the user ID that was used to login to the IMAP server with '@' and the value in this field to form the user's 'From' address in the default identity. This is required when the 'From' address has been locked-down.
Default Domain	Enter the default domain name that Mulberry will add to unqualified email addresses typed in any of the address fields in a Draft window. This field is optional, but highly recommended.
Check Interval	Enter the time interval (in minutes) Mulberry should wait between attempts to check for new mail. This field is optional.
Copy-To	Enter the name of the 'Copy-To' folder used by default. If the option to create this is on, it will be created for new users. This field is optional.
Move-To	Enter the name of the 'Move-To' folder used by default. If the option to create this is on, it will be created for new users. This field is optional.

Multi-user Remote Preferences Panel

If you chose not to override the default preferences in the Default Preferences Override panel, and you have set administrative options in previous panels that require Mulberry to access preferences from a remote preferences server, the next panel displayed will be the Multi-User Remote Preferences panel. This panel allows you to specify the name and type of the remote preference server where it should look for preferences by default. To the far-right of each field in this panel, Mulberry distinguishes between preferences that are required and those that are optional.

Figure 14 Multi-user Remote Preferences Panel

Items	*Description*
Server	Enter the hostname of your remote preferences server. This field is required. The **Options** button allows you to specify the authentication method and security (SSL) settings used when connecting to the server, as well as, in a situation where both local and remote preferences are allowed, whether Mulberry should use remote preferences by default on startup.
Type	Choose the server type of the host specified in the previous field. Available options are IMSP and ACAP. This field is required.

Generate Remote Options File Panel

If you have set administrative options in previous panels that indicate the use of a remote preferences server, the next panel displayed in the Administrator's Toolkit is the Generate Remote Options File panel. The panel will differ depending on whether you chose to override Mulberry's default preferences in the Default Preferences Override panel. If you did not choose to override the default preferences, the panel will appear as in Figure 15. This panel is very similar to the Multi-User Local Preferences panel (see page 30), allowing you to specify default server names and other options.

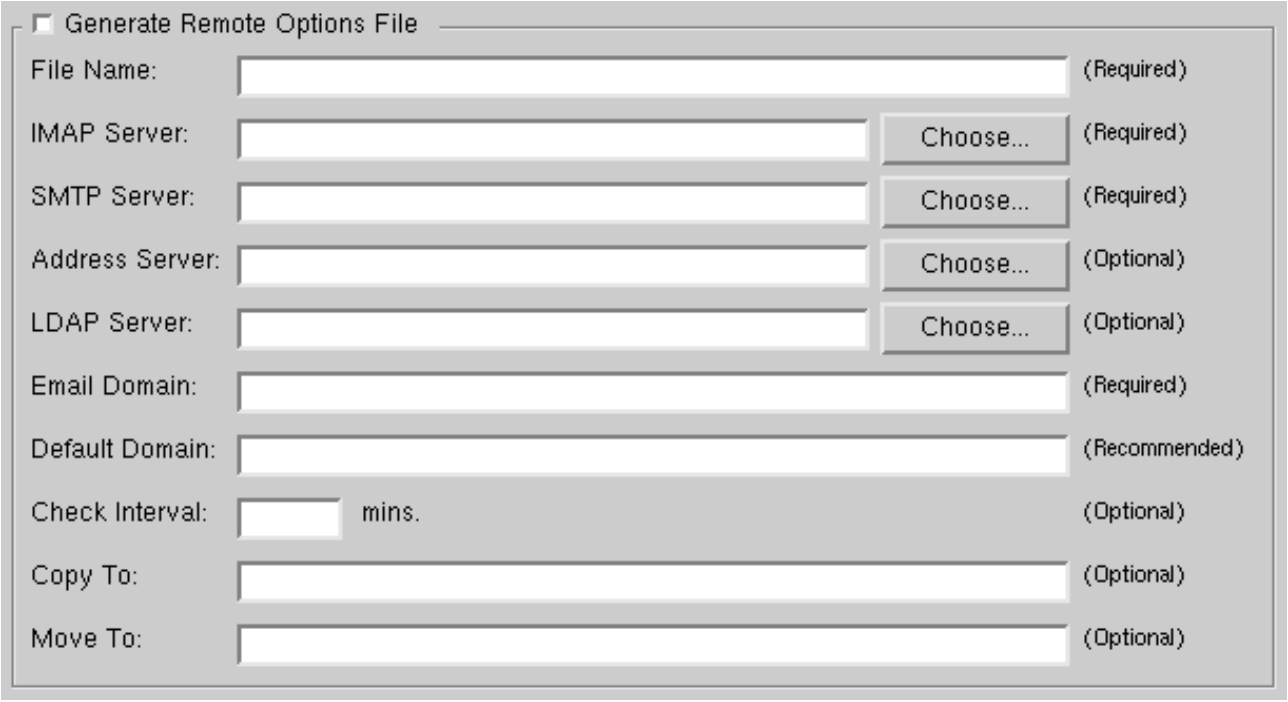


Figure 15 Generate Remote Options File Panel

If you did choose to override Mulberry's default preferences, the Administrator's toolkit will generate a remote options file based on the values in the override preferences file you used. In this case, the panel will appear as in Figure 16.

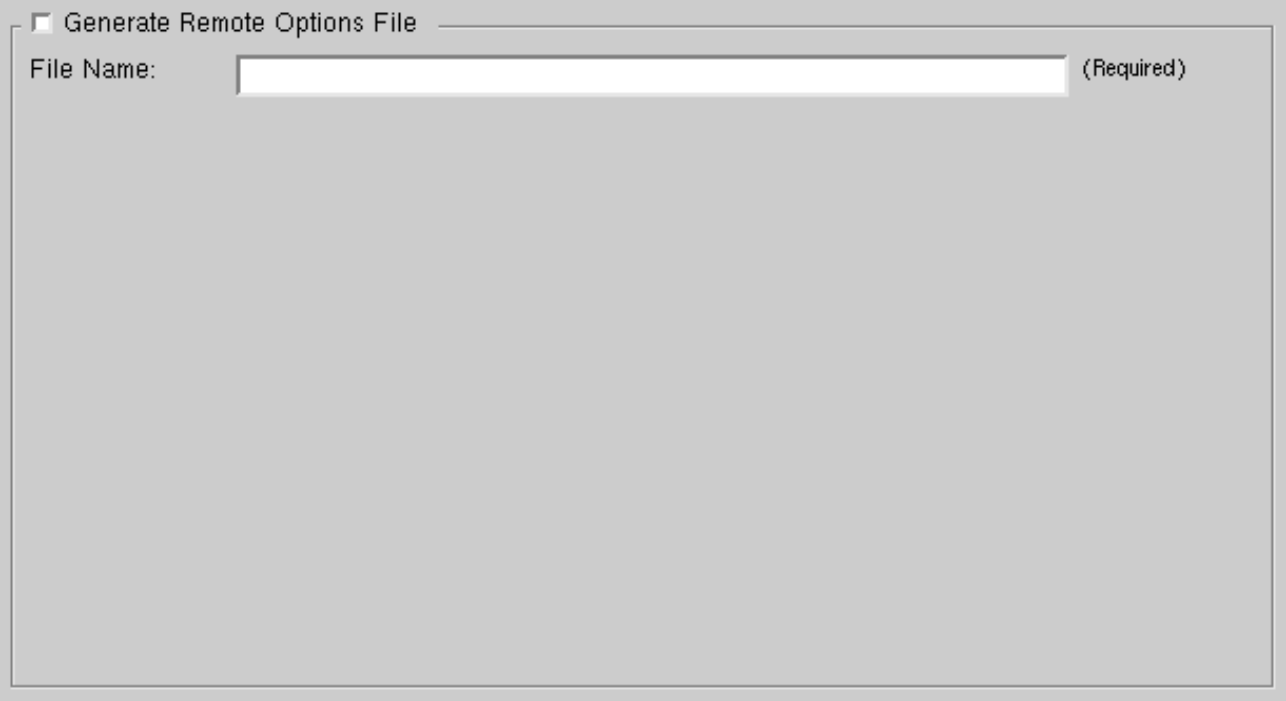


Figure 16 Generate Remote Options File Panel (Default Prefs Override)

In either case, you will need to specify the name of the remote options file that you want to generate.

Items	*Description*
File Name	Enter the name of the remote options file that the Administrator's Toolkit will generate. This field is required.

Errors Panel

The final step in the configuration process is the Errors panel, shown in Figure 17. This panel displays messages indicating any problems with the configuration values set in all of the previous configuration panels. Mulberry examines all of the administrative options set in the configuration panels and verifies that it has sufficient information to configure the application or installer in the manner specified.

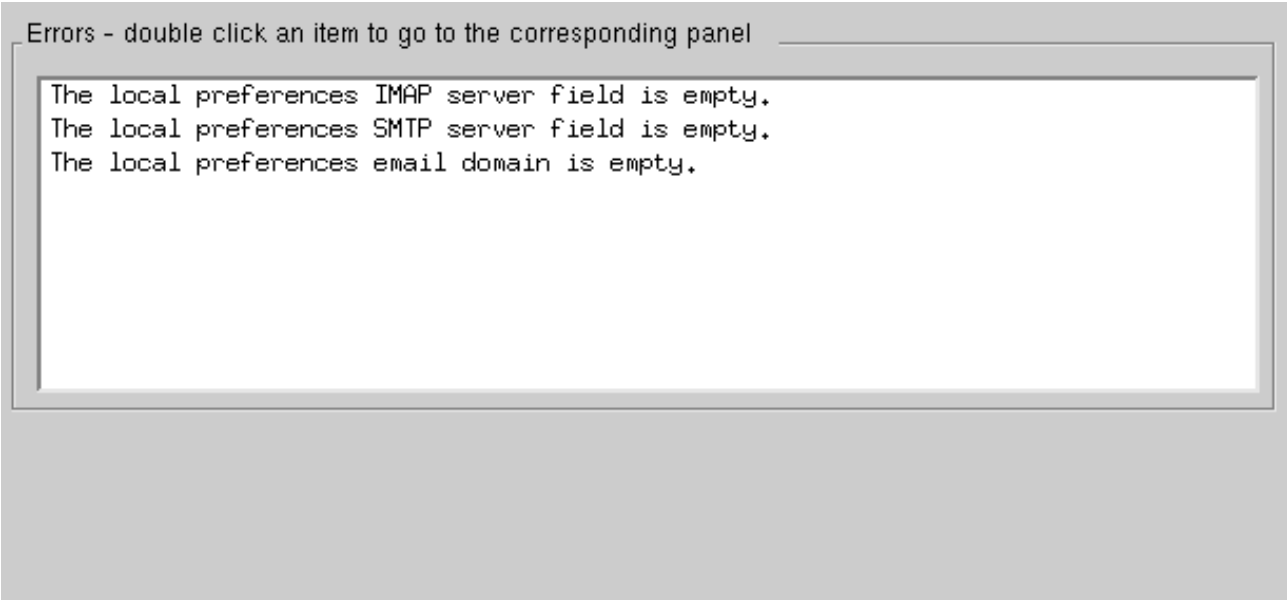


Figure 17 Errors Panel

If there are error messages listed in this panel, you can double-click on the error text to go directly to the problem field, or use the **<<Back** button to return to previous configuration panels and correct the errors.

If no error messages are displayed in this panel, all configuration values have been properly specified. Click the **OK** button to complete the configuration of the Mulberry application or installer specified earlier, and to generate the remote options file if necessary. You can also click the **Cancel** button to exit the Administrator's Toolkit without completing the configuration process, though any changes to settings will not be saved.

SPECIAL CONCERNS

Configuring Installers (Mac OS and Win32 only)

Choosing an Installer

Cyrusoft provides three different version of the Mulberry installer. The first version, usually just called 'Mulberry', is the default commercial distribution of Mulberry. Two additional installers, with 'Site' and 'Site2' suffixes, are also provided, primarily for use by sites. These additional installers have different 'Easy' or 'Typical' installations and include a special 'Site License' licensing document:

Installer	*What gets installed*
'Mulberry' (default installer)	Mulberry application Plugins Release Notes Full documentation Ancillary files (address book etc)
'Site'	Mulberry application Plugins Latest Release Note
'Site2'	Mulberry application Plugins Latest Release Note Full documentation

Configuring the Installer

On Mac OS, the Administrator's Toolkit can write the configuration information directly into the installer's resource fork. This allows a single installer file to be distributed to end users.

On Win32, the installer file cannot be written to once its been created. Thus the Administrator's Toolkit writes the configuration information to an auxiliary 'Mulberry.key' file which needs to be distributed with the original installer. This file must be present in the same directory as the installer when it is run to ensure that pre-configuration and pre-registration occur. Thus the Win32 distribution is two files. For distribution purposes it is sometimes more convenient to wrap these two files inside a self-extracting zip archive.

Multiple choice of Servers

Mulberry v1.4.3 and above includes a new option to allow users to pick a server out of a popup menu list in the multi-user login dialog. When this feature is used, the server name in the multi-user dialog (see Figure 1) is replaced by a popup listing all the servers available to the user. The user can then choose which server to login to.

To setup multiple server choice, simply enter a comma delimited list of server addresses in the corresponding server address field in the Administrator's Toolkit preferences. E.g. to have a list of two servers, enter 'imap1.cyrusoft.com, imap2.cyrusoft.com' in the IMAP server address field.

If the server address field ends with a comma, then Mulberry will additionally add a 'Other…' item to the bottom of the popup menu. When chosen, this displays a dialog allowing the user to manually enter a server address for subsequent use.

This approach can be applied to both IMAP and SMTP servers simultaneously by provided equivalent lists of servers in each field. However, only the IMAP server list is shown in the popup, and selecting a server from this list will select the corresponding SMTP server as well.

The multiple server choice can also be applied to remote preferences servers the in case where Mulberry is set to login to a remote preference server on startup. Simply put the server list in the remote preference server address field.

Virtual Domain Support

Mulberry v3.0.2 and above includes new support for 'virtual domains'. In a 'virtual' or multiple domain/sub-domain environment users will typically be associated with a specific set of servers for the domain/sub-domain they are assigned to. Typically their user id will include the domain/sub-domain, e.g. 'uid123@localdomain'. With previous versions of Mulberry, sites would have to create and maintain multiple configurations of Mulberry for each domain/sub-domain they control. The new virtual domain feature eliminates the need for multiple configurations as a single configuration can now be used for all domains/sub-domains.

If the virtual domain option is turned on in the Administrator's Toolkit, when Mulberry is run and a user enters their user id, Mulberry will extract the domain component from the user id (its assumed to follow any '@' character in the user id). It will then substitute the extracted domain component into any server address or the email domain preference values wherever an '*' character appears in that preferences. E.g. if an IMAP server address is specified as 'imap.*', and the user id is entered as 'uid123@local.domain.com', the resulting IMAP server address will be 'imap.local.domain.com'. Or, if an IMAP server address is specified as 'imap.*.domain.com', and the user id is entered as 'uid123@local', the resulting IMAP server address will be 'imap.local.domain.com'.

Originator-Info Header

Description

The Originator-Info header is a new standard header that is designed to replace the non-standard use of such headers as X-Sender and X-X-Sender as a means of identifying the author of a message. The format of this header is a series of 'attribute-value' pairs separated by commas. The defined keys are:

- login-token – a unique identifier that can be used to identify the sender of the message
- login-id – the user id used by the user to authenticate to a server
- server – identifies the server for which the login-token is valid
- token-authority – a description of the entity that can interpret the login-token value.

Note that this header does not provide a truly reliable way to identify the sender of a message (its quite possible for someone to masquerade as another person by copying this header from the other person's correspondence and inserting it in their own message when not using Mulberry). This header merely provides a standard replacement for the non-standard existing practices.

Mulberry's use of Originator-Info

By default Mulberry generates an Originator-info header with login-id and server attributes based on the user id and server address of the first logged into IMAP server. The Administrator's Toolkit allows this header to be customized under the Spoof Proof tab (see page 22). This includes being able to turn the header of entirely, as well as switching it to use the login-token attribute.

When the login-token is used, Mulberry can be set to encrypt the login-token value using a secret passphrase provided in the panel. This prevents potentially sensitive information from being visible in this header.

The Administrator's Toolkit also allows a token-authority attribute to be added. This allows recipients of messages to know whom to contact in the event of some problem with the message where the login-token needs to be resolved. This can usually be set to a mailto URL for the postmaster at your site (e.g. 'mailto:postmaster@cyrusoft.com').

Encrypted Originator-info login-token values can be decrypted by using the 'Originator-Info Decode' utility provided with the Administrator's Toolkit installation. Simply run this tool, enter your secret passphrase at the first prompt, then enter the login-token value from any message sent with the appropriately configured copy of Mulberry. The decrypted login-id and server values will then be displayed, allowing the message to be traced.

Configuration Plugin

Mulberry v1.4.4 and above has support for a 'Configuration' plugin that individual sites can create for themselves and include with their Mulberry distribution. This plugin, if present, is called by Mulberry during the multi-user startup phase, and can be used to dynamically change the preferences which Mulberry ultimately uses after the initial startup

Situations where its useful

Some sites have elaborate schemes to distribute mail server load by having multiple mail servers and mapping individual users to specific servers. In some cases the number of servers is fixed, in which case the server-popup choice scheme described on page 37 may be more appropriate. In other cases, this mapping may to too complex to express with the Administrator's Toolkit. Examples include:

- mapping some characters of the user's login id to a server address, which in turn, when resolved by DNS, points to the relevant server
- using a directory service to map the user id to a server address (e.g. an LDAP server)
- using the local OS authentication to determine the user id and server address (e.g. Windows login, or Kerberos authentication)

Similar situations, where the user's preferences need to be dynamically configured based on the user, the current environment etc, also require more flexibility than that provided by the 'static' mechanism of the Administrator's Toolkit.

How it works

When a configuration plugin is present in the Mulberry Plug-ins directory, and when multi-user login has been configured via the Administrator's Toolkit, Mulberry will use the plugin to determine the actual preferences used.

First off, the plugin can control which parts of the multi-user dialog are displayed to the user, as well as being able to turn off the dialog altogether.

If the multi-user dialog is presented to the user, after they enter their user id, or other required information, Mulberry will call the configuration plugin with this information. The plugin can then process this in whatever way it likes, and returns to Mulberry a set of Mulberry preference items. These preference items are then used to override the set that Mulberry generated as a result of the normal Administrator's Toolkit startup.

How to use it

Sites that need to use the configuration plugin need to write one of their own tailored to their particular needs. An example plugin project and source files are provided on our website to facilitate this (see <http://www.cyrusoft.com/mulberry/plugins/develop.html> for more information).

Once the plugin has been created, it needs to be added to the default Mulberry distribution, so that it gets installed into the Mulberry Plug-ins directory when the end-user installs Mulberry. In addition, the Administrator's Toolkit needs to be used to set Mulberry into the appropriate multi-user mode to trigger the use of the plugin.