GRENOX SOFTWARE, INC.

MessagePal Instant Office Messaging System

# Administrative Features

MESSAGEPAL INSTANT OFFICE MESSAGING SYSTEM

# MessagePal Administrative Features

February 2006

Download the latest version of MessagePal at
www.messagepal.com
to ensure you have the latest features described in this manual.

***The features described in this whitepaper are provided on an 'As Is' basis. Grenox Software, Inc., its resellers, agents, affiliates, distributors, publishers, owners and employees (collectively, the "Vendor") make no warranty that the features described will work in every situation. In all cases, the Vendor's liability is limited to the original purchase price of the software. MessagePal should never be relied upon to transmit or store mission-critical, life-threatening or healthcare-related information, instructions or communication, and such use is a violation of the MessagePal License Agreement.***

http://www.messagepal.com • support@messagepal.com

# MessagePal Administrative Features

*MessagePal allows systems administrators to selectively restrict certain program functions.*

MessagePal has been designed to be a very flexible, inexpensive and easy-to-maintain system – perfect for businesses and workgroups who don't want the hassle, expense or exposure of more expensive instant messaging solutions while still taking advantage of MessagePal's unique features. Now, we've added certain capabilities that allow systems administrators to restrict certain features that they may not want certain users to have access to. This paper describes those restrictions and gives specific instructions for installing those restrictions. **It is recommended that this paper *not* be distributed to your users. With access to this paper, many of the desired restrictions could be modified or removed.**

MessagePal's administrative tools allow network administrators to enable/disable the following MessagePal features on a user-by-user basis:

- Allow/Disallow Broadcast Messages (Page 6)
- Password-Protect Setup Screens (Page 6)
- Allow/Disallow Outbound Messages (Page 7)
- Allow Sending To All or Only Certain Users[1] (Page 9)
- Force UserName to be the same as Network Logon ID (Page 9)
- Allow/Disallow Replies (Page 9)
- Allow/Disallow Exiting MessagePal (Page 10)
- Allow/Disallow Clearing the Message Log[2] (Page 10)
- Allow/Disallow Message Logging [3] (Page 11)
- Log All Messages to a Server File[2] (Page 11)
- Use a Common Set of Groups Across Selected Workstations[2] (Page 12)

[1] Available in versions 1.6.2 and later

[2] Available in versions 1.4.5 and later

[3] Available in versions 1.6.0 and later

- Use a Common Set of Buttons Across Selected Workstations[2] (Page 13)
- Allow/Disallow Access to the Group Administration Screens[1] (Page 13)
- Disable Splash Screen Popup[1] (Page 14)
- Customize the Printed Message Header (Page 14)
- Customizing the Logo (Page 15)

Detailed descriptions and instructions for implementing each of these features is available on the page number indicated.

Because it is expected that additional administrative features will continue to be added in future versions of MessagePal, you can check to be sure you have the latest version of this document by downloading the document from the MessagePal website:

`http://www.messagepal.com/admin/adminfea.pdf`

If you have any suggestions for additional administrative features, or want custom features developed for you, contact us at ideas@messagepal.com.

# The MPPRIV.CFG File

Administrative restrictions are imposed through the creation, copying or installation of a file called MPPRIV.CFG on each MessagePal user's machine where restrictions are desired. The file contains a list of keywords along with a value indicating whether the keyword's restriction should be turned on or not. In the absence of this file, MessagePal will run without any restrictions. You may operate a MessagePal network in which some users have the file and its associated restrictions and others do not.

Note that only those users who have the file on their machine will have the restrictions imposed. In addition, different users on the same LAN can have different restrictions if their MPPRIV.CFG files are different.

Another thing to keep in mind is that the MPPRIV.CFG file is read by MessagePal only when MessagePal is started. So, if you make changes to the file that you want to take effect, be sure to exit and restart MessagePal.

### MPPRIV.CFG Installation Directory

The MPPRIV.CFG file needs to be placed in the MessagePal program directory. On most installations, this directory will be:

```
C:\Program Files\MessagePal
```

It is possible that MessagePal was installed in a different directory if that was specified during original installation. In all cases, MPPRIV.CFG should be installed in the same directory as the MessagePal executable, MessagePal.EXE. MPPRIV.CFG is not installed by the MessagePal installer and the file needs to be installed separately if administrative features are desired on a particular machine. Deployment scenarios of the MPPRIV.CFG file will depend on your preferences.

### MPPRIV.CFG File Format

The MPPRIV.CFG file contains optional keywords that are examined by MessagePal upon startup, and depending on those keywords, the desired restrictions are imposed on that session of MessagePal. After the file is installed, the restrictions will continue to be imposed for subsequent sessions of MessagePal and will be preserved if the MessagePal software is subsequently updated to a newer version.

A template MPPRIV.CFG file (which you can edit to your own preferences) can be downloaded from:

`http://www.messagepal.com/admin/MPPRIV.CFG`

An example of the `MPPRIV.CFG` file is also shown here:

**MPPRIV.CFG Example**

```
[COMMENTS--]MPPRIV.CFG: MessagePal Privileges Configuration
[COMMENTS--]Version 1.0 – For XYZ Corp.
[COMMENTS--]
[NOBROADCST]1
[SETUPPASWD]SUMMERTIME
[RECEIVONLY]0
[USENETIDEN]0
[NOEXITALWD]1
[NOREPLIES-]0
```

You can create your own `MPPRIV.CFG` file by downloading and editing the example file, or using Windows' NotePad application to create one.

The construction of the `MPPRIV.CFG` file is fairly straightforward. Each line of the file represents a particular privilege available to be customized by the administrator. The file can contain any or all of the available privilege keywords. If any of the available keywords are not present in the file, then MessagePal will assume that the feature is not restricted and the default MessagePal behavior will be implemented. If any of the keywords are listed more than once, the last one will be the value that will be used.

### Privilege Keywords and Values

Each line of the `MPPRIV.CFG` file should be begin with a 12-character keyword (includes brackets) followed by an appropriate value. For keywords that represent restrictions that can be either on or off, valid values are `0` for 'off' and 1 for 'on'. For example, the following line indicates to MessagePal that the user should not be allowed to send broadcast messages:

```
[NOBROADCST]1
```

The following line indicates that the user should not be allowed to exit MessagePal:

```
[NOEXITALWD]1
```

When adding or editing keywords, make sure to use the exact spelling of the keyword. Unrecognized keywords or values are ignored. To add comments to the file, use the `[COMMENTS--]` keyword followed by any text. For example,

```
[COMMENTS--]This text is ignored by MessagePal
```

The following sections describe the various administrative privileges, their associated keywords, and appropriate values.

# Available Privilege Restrictions

## Restricting Broadcast Messages

**Overview**

Your enterprise may want to restrict which MessagePal users have the ability to send broadcast messages. Broadcast messages are those that are sent by one user to all other online MessagePal users using the 'Broadcast' tab in the MessagePal interface. You may have certain users who shouldn't have the authority to interrupt or bother all others with broadcast messages.

**Note**

Those users who are restricted from sending broadcast messages can still send messages to any individual user(s) or any user group they have defined. In fact, that user can still send a message to all online users by selecting all of their usernames manually from the 'User' list in the MessagePal interface. Disabling Broadcast messages reduces the likelihood that the user will send a message to all users, but does not guarantee it.

**Keywords**

To disable sending broadcast messages, use keyword `[NOBROADCST]`

**Examples**

| | |
|---|---|
| `[NOBROADCST]1` | *Sending broadcast messages is not allowed* |
| `[NOBROADCST]0` | *Sending broadcast messages is allowed* |

## Password-Protecting Setup Screens

**Overview**

MessagePal's 'Setup' screens provide many settings that give individual users the flexibility to customize each installation to the enterprise and users' preferences. Those customizations are made in the MessagePal Setup window. Each tab of the Setup screen allows you to change various aspects of MessagePal's operation and user interface.

In certain enterprises and for certain users, you may not want to allow users to modify these settings. Allowing users to change settings can create support or security issues that particular enterprises may want to avoid.

MessagePal now provides the ability to password-restrict access to the setup screens. Only those who have the password are permitted to access the setup screens to make changes. Without the password, users can use MessagePal to send and receive messages but won't be able to make setup changes. The password is specified individually for each workstation, and can be made consistent across an organization or specific to each workstation.

**Keyword**

To restrict access to setup screens, use keyword `[SETUPPASWD].` To eliminate password protection and give all users setup access, remove this keyword from the file.

**Example**

| | |
|---|---|
| `[SETUPPASWD]HAWAII45` | *Access to setup available only when password 'HAWAII45' is entered.* |

## Preventing New Outbound Messages / Creating a Receive-Only MessagePal

**Overview**

MessagePal can be used as a one-way broadcast infrastructure, as well as a mixed one-way and two-way solution. This may be desirable in environments where only certain users are permitted to send messages, but other users should only be able to receive. For example, a network administrator may want to notify users of important networking announcements, without giving users the ability to send messages for other purposes on their own.

The receive-only restriction is implemented on a workstation-by-workstation basis. Once imposed, the receive-only restriction will prohibit that workstation from sending new messages or forwarding messages. It does <u>not</u> prevent a user from replying to messages received. If you want to restrict those messages as well, see the `[NOREPLIES-]`keyword.

**Keywords**

To prevent new messages from being sent or forwarded, use keyword `[RECEIVONLY]`

**Examples**

| | |
|---|---|
| `[RECEIVONLY]1` | *No new messages can be sent or forwarded* |
| `[RECEIVONLY]0` | *Messages can be sent or forwarded* |

# Allow Sending To All or Only Certain Users

#### Overview

MessagePal can be configured to allow a user to send messages to any other MessagePal user[4] (the default setting), or can be configured so that each individual workstation can be restricted such that it can send messages to only certain users. The following notes apply to situations where workstations are restricted to be able to send messages to only certain users:

- When a workstation is set so that it can send to only certain users, the 'Broadcast' function on that workstation is automatically disabled and the user will receive an error message if they attempt to so send a broadcast message to all users and the broadcast will not be sent.

- If a user has Groups that contain users to whom they are not authorized to send messages, those user names will be ignored when messages are sent to those Groups and the messages will be sent only to the authorized destinations.

- Restricting workstation A from sending messages to workstation B (by not including Workstation A's username in the allowed user list) does not automatically exclude Workstation B from sending messages to Workstation A. Workstation A will not be able to reply back to messages sent from Workstation B. If it is desired that neither Workstation should be able to send messages to each other, then the configuration file on each workstation should <u>not</u> include the other Workstation's username on the allowed list.

The sender restrictions are implemented on a workstation-by-workstation basis.

#### Keywords

To allow messages to be sent to only certain users, specify those usernames using the keyword `[ONLYSENDTO]`

#### Examples

```
[ONLYSENDTO]JACK
[ONLYSENDTO]ANNIE
```

*Messages can be sent only to users named 'Jack' and/or 'Annie'*

*Note: Omit the* `[ONLYSENDTO]` *keyword from the configuration file completely if you want that workstation to be able to send messages to <u>any</u> user.*

*For more information on this keyword, send your questions to <u>support@messagepal.com</u>*

[4] If 'Team Messaging' functionality is implemented on that workstation (see MessagePal's Advanced Setup tab), then this include only those users belonging to the same team.

# Forcing MessagePal UserName to be User's Network ID

**Overview**

In certain circumstances, many different users may use a particular workstation, depending on time of day, shift, etc. If you want MessagePal usernames to reflect people instead of fixed workstation locations, then it might be desirable to have MessagePal automatically use the network login ID rather than some constant username specified in the setup screen. Otherwise, a user at an often-shared workstation would have to go into the MessagePal setup screen every time to change the user name to their own name, which would be extremely inconvenient.

Note that MessagePal only checks the Network User ID when MessagePal is started. If the workstation is logged out and then logs in under a different name while MessagePal is still running, it will not be detected.

**Keywords**

To force MessagePal to use the current network login ID as the MessagePal username, use the keyword `[USENETIDEN]`

**Examples**

| | |
|---|---|
| `[USENETIDEN]1` | *The MessagePal username will be set to the network user ID* |
| `[USENETIDEN]0` | *The MessagePal username will be set to the name specified in 'Setup' screen* |

# Preventing Replies

**Overview**

If you want to use MessagePal as a 1-way communication system to certain workstation, without the option for users to reply to the received message, then this administrative feature will be of interest. When this option is enabled, received message windows will not have the capabilities to reply to the message. The only option available for a user will be to close the window.

If you also want to prevent users from creating their own new messages, see keyword `[RECEIVONLY].`

**Keywords**

To disable the ability to reply to received messages, use keyword `[NOREPLIES-]`

**Examples**

| | |
|---|---|
| `[NOREPLIES-]1` | *No broadcast messages allowed* |
| `[NOREPLIES-]0` | B*roadcast messages allowed* |

# Preventing User Exiting MessagePal

#### Overview

Users can exit MessagePal by choosing the Exit option from the File menu, or by pressing the ‘X’ in the upper right corner of the main MessagePal window. The ‘X’ can be disabled in the setup screens so that the program won’t exit but instead will be minimized. However, some administrators might want to make sure that MessagePal is always running and ready to receive messages, rather than giving the user an option to exit. Thus, the [NOEXITALWD] keyword.

Note that determined users can force MessagePal to shutdown if they terminate the MessagePal process using the Task Manager screen that pops up under most versions of Windows when the user presses ‘Ctrl-Alt-Delete’.

#### Keywords

To prevent users from exiting MessagePal, use keyword [NOEXITALWD]

#### Examples

| | |
|---|---|
| [NOEXITALWD]1 | *User cannot exit MessagePal* |
| [NOEXITALWD]0 | *User can exit MessagePal if desired* |

# Allow/Disallow Clearing the Message Log

#### Overview

Users can clear the message log by pressing the ‘Clear Log’ option on the main MessagePal screen or highlighting a log entry and pressing the ‘Delete’ key. In some circumstances, an administrator or supervisor may want the message log preserved as a record of all transmissions.

> Note: If users have access to the setup screens, they could choose to elect *not* to have the message log saved between MessagePal sessions. In this case, the message log would be deleted if the user exits MessagePal. See the [SETUPPASWD] keyword elsewhere in this document to prevent access to the setup screens.
>
> In addition, the MessagePal log is saved only when the computer and MessagePal are shut down normally. If either the program or the computer running MessagePal is terminated abnormally, the message log may not be complete. Note that determined users can force MessagePal to shutdown if they terminate the MessagePal process using the Task Manager screen that pops up under most versions of Windows when the user presses ‘Ctrl-Alt-Delete’.
>
> The message log is stored in a file called MPHIST.BIN. If a user were to find that file and has the rights to delete it, deleting it would erase the message log.

### Keywords

The `[NOCLEARLOG]` keyword provides the mechanism for restricting the user's ability to delete the log or log entries.

### Examples

| | |
|---|---|
| `[NOCLEARLOG]1` | *User cannot delete entries in the message log* |
| `[NOCLEARLOG]0` | *User can delete message log entries if desired* |

## Allow/Disallow Message Logging

### Overview

Message logging on the main MessagePal screen is a key feature of the software. However, some administrators may prefer that no message logging takes place for privacy or other reasons.

### Keywords

The `[DONOTLOG--]` keyword provides the mechanism for restricting the user's ability to keep a message log of all messages sent or received.

### Examples

| | |
|---|---|
| `[DONOTLOG--]1` | *No new entries will be added to the Message Log* |
| `[DONOTLOG--]0` | *The end-user can configure which messages are logged using user setup screen.* |

## Log All Messages to a Server File

### Overview

In addition to the message log on the main MessagePal user screen, some administrators may want to have all messages also logged to a central log file maintained on another PC or network file server. This may be useful for monitoring employee communications, reviewing issues, and monitoring system performance or errors.

You can establish a single file on a common file server that selected (or all) users can be configured to log to. Then, you'll have a single, time-sequenced log available of all messages sent/received by those users. Note that the log will include all sent/received messages (so you'll see a log entry from the sender and then separate log entries for each recipient) as well as all error and information messages that normally appear in the log. If messages are deleted by the user from their local message log, the will <u>not</u> be deleted from the central log.

When server message logging is enabled for any particular workstation, the workstation user will *not* be aware that central logging is taking place, unless they are informed by the administrator. MessagePal's user features will continue to work as normal, including local logging. Therefore, confidential employee monitoring can be accomplished, if desired.

When central logging is established, the log file is automatically built by MessagePal in HTML format. Therefore, when establishing a new filename for the central log file, use `.htm` or `.html` as the file extension. You should use a web browser to view the file.

Note that you should NOT create an empty file with the file name when first starting to log. You should just specify the filename in the configuration file. If the file does not exist, MessagePal will automatically create it and insert the appropriate, required HTML header information.

**Note**

Each workstation you want to enable for central logging must have appropriate file access rights to the central log file in order to ensure logging can occur. Make sure that the user has write/append rights to the file. If the file is not accessible to MessagePal because of network or security issues, it will not notify the user because that would divulge that central logging is enabled, which may not be desirable. The best way to see if central logging is working is to test it.

**Keywords**

The `[CENTRALLOG]` keyword provides the mechanism for instructing MessagePal to log the user's messages to a server-based file.

**Examples**

| | |
|---|---|
| `[CENTRALLOG]F:\LOGS\MPLOG.HTM` | *New messages will be appended to the file.* |
| `[CENTRALLOG]\\Server1\MPLOG.HTM` | *New messages will be appended to the file.* |
| `[CENTRALLOG]` | *No central log will be kept.* |

# Use A Common Set of Groups Across Selected Workstations

**Overview**

In some circumstances, an administrator or supervisor may want to administer the list of Groups and the Group members on a central basis, rather than letting each user configure their own. This avoids the problem of visiting each workstation when you need to add/change/delete groups or their members. MessagePal includes the capability to have the group file stored at a central location on the LAN (usually a commonly-accessible file server) rather than on each user's local harddrive.

When the central group file function is enabled, individual users will not be able to modify the groups. Administrators should decide what file server location they want to use for the common groups file, then copy a GROUPS.CFG file from their workstation to that server location.

In order for changes to me made to the GROUPS.CFG, either the administrator can modify the file with a text editor, or they can press 'CTRL' with 'ALT' while clicking on the 'edit groups' icon. That will override the edit restrictions and they'll be able to make any necessary changes to the group file.

#### Keywords

The `[GROUPSFILE]` keyword provides the mechanism for enabling a central groups file.

#### Examples

```
[GROUPSFILE]F:\SPEC\GROUPS.CFG
```

*Use the specified group file*

## Use A Common Set of Buttons Across Selected Workstations

#### Overview

In some circumstances, an administrator may want to have a common set of button definitions across a set of users. This can be accomplished with the BUTTONFILE keyword and a location to store a common button file.

#### Keywords

When the central button file function is enabled, individual users will not be able to modify the button definitions, although they may review them in settup. Administrators should decide what file server location they want to use for the common groups file, then copy a MSGPAL.BTN file from their workstation to that server location.

In order for changes to me made to the MSGPAL.BTN, either the administrator can modify the file with a text editor, or they can press 'CTRL' with 'ALT' while clicking on the 'setup' icon. That will override the edit restrictions and they'll be able to make any necessary changes to the common button file.

#### Examples

```
[BUTTONFILE]F:\CheckIn\MSGPAL.BTN
```

*Designate a central button file*

## Allow/Disallow Access to the Group Administration Screens

#### Overview

In some circumstances, an administrator or supervisor may want to prevent users from changing the defined groups and their members.

#### Keywords

The `[NOGROUPCHG]` keyword provides the mechanism for restricting the user's ability to modify MessagePal groups.

#### Examples

```
[NOGROUPCHG]1
```

*User cannot access the group administration screens*

```
[NOGROUPCHG]0
```

*User can make any changes to groups*

# Disable Splash Screen Popup

**Overview**

In some circumstances, an administrator may want to eliminate the MessagePal splash screen that appears when clicking on the MessagePal logo on the main MessagePal screen. This may be useful when MessagePal is used in a touch-screen environment. The splash screen will still be accessible through the 'Help', 'About MessagePal…' menu selection.

**Keywords**

The `[NOABOUTBOX]` keyword provides the mechanism for restricting the splash screen popup.

**Examples**

| | |
|---|---|
| `[NOABOUTBOX]1` | *Splash screen will not appear when user clicks on MessagePal icon.* |
| `[NOABOUTBOX]0` | *Splash screen has normal popup behavior* |

# Customize the Printed Message Header

**Overview**

In default mode, MessagePal will print the words "Message Detail" at the top of each page when a user prints a message. You may wish to customize this message for your company. For example, "Customer Request", "Phone Message", or "ABC, Inc. Message". Also see instructions on using a custom logo on your printed reports, later in this document.

**Keywords**

The `[PRINTHEADR]` keyword provides the mechanism for customizing the printed messagae header.

**Examples**

| | |
|---|---|
| `[PRINTHEADR]Customer Request` | *Changes print report header to "Customer Request"* |
| `[PRINTHEADR]Phone Message` | *Changes print report header to "Phone Message"* |

# Customizing The Logo

### Overview

You can change the MessagePal logo on the main MessagePal screen and on messages you print to your printer.  This feature will give the software a custom look.

### Customization Instructions

First, you need to create a .jpg file with your logo.  We recommend dimensions 169 w x 81 h. There is a sample logo available for download from our website at…

`http://www.messagepal.com/admin/mplogo.jpg`

Next, name the logo file `MPLOGO.JPG` and save it in the MessagePal directory (usually C:\Program Files\MessagePal).

Finally, restart MessagePal and the logo will appear on the main MessagePal screen.   Also, when you print individual messages to your printer, MessagePal will use this same logo at the top of the printed page in place of the MessagePal logo.

The logo file needs to be installed in the MessagePal directory on each computer you want to have the custom logo.  You can experiment with our sample logo file, then try it with a logo you customize.

## New Feature Requests

Requests for other administrative or software features are welcome. In some cases, there may be a small fee for customization. Please submit your suggestions or requests to: ideas@messagepal.com.

**Grenox Software, Inc.**

**http://www.messagepal.com**
**support@messagepal.com**