UbiQ® IDmail

For Total Email Security

UbiQ® IDmail Enrollment Server User Manual

Disclaimer of Warranty

UbiQ Incorporated makes no representation warranties, either expressed or implied by, or with respect to anything in this guide, and shall not be liable for any implied warranties of merchantability and fitness for particular purpose or for any indirect, special, or consequential damages, hence this exclusion may not apply to you.

Copyright Notice

This product and its related software are protected by copyright and are distributed under licenses restricting their use, copying, distribution, and de-compilation.

Paid Version License

(C) UbiQ Incorporated (UBIQ) 2000

THIS SOFTWARE IS NOT IN THE PUBLIC DOMAIN.

UbiQ*IDmail* Enrollment Server Single-User License Statement and Disclaimer

YOUR USE OF THE SOFTWARE DISTRIBUTED WITH THIS LICENSE IS SUBJECT TO ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE STATEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS STATEMENT, DO NOT USE THE SOFTWARE.

1. This Software is protected by copyright law and international copyright treaty. You are NOT granted any rights to use this software with any other software product or application, or with any of the supported electronic mail clients, to provide these functions in any automated or semi-automated way. Additional licenses are available for use with other software or as a part of other applications. Except as provided in this statement, you may not transfer, rent, lease, lend, copy, modify, translate, sublicense, share or electronically transmit the software or any of its documentation. You may not remove the proprietary notices on the Software or any of its documentation. You are hereby granted a non-exclusive license to copy the software onto one computer to be used, and to make archive copies for the sole purpose of backing up the software to protect against loss. You must ensure that there is no possibility that the software can be used by two or more persons simultaneously. This license will terminate automatically if you fail to comply with the terms stated herein. On termination, you must destroy all copies of the Software and documentation. You may transfer all of your rights in the software to another person provided that you transfer all copies of the software and documentation, including this statement, to that person. After such a transfer you may no longer use the software and the person to whom it is transferred may use it only in accordance with this statement and with all applicable domestic and international copyright laws and treaties.

2. THIS SOFTWARE IS PROVIDED “AS IS” AND USE OF THIS SOFTWARE IS ENTIRELY AT THE USER’S RISK. THIS SOFTWARE SHOULD NOT BE UTILIZED IN APPLICATIONS IN WHICH DANGER TO PROPERTY, THE ENVIRONMENT OR HUMAN HEALTH OR LIFE MAY BE PRESENT. NEITHER THE INVENTOR, THE DEVELOPER, THE DISTRIBUTOR NOR LICENSOR MAKE ANY WARRANTY WHATSOEVER, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, PERFORMANCE, AND NON-INFRINGEMENT, WITH RESPECT TO THE SOFTWARE AND THE DOCUMENTATION. IN NO EVENT WILL THE INVENTOR, DEVELOPER, LICENSOR OR DISTRIBUTOR BE LIABLE FOR DAMAGES OF ANY KIND, INCLUDING ANY LOSS OF PROFITS, LOST SAVINGS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE, MISUSE OR INABILITY TO USE THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, NOR ARE ANY OF THEM UNDER ANY OBLIGATION TO ISSUE UPDATES TO THIS SOFTWARE OR TO CORRECT DEFECTS THEREIN.

3. The developer reserves the sole right at any time to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, general availability or other characteristics of current or future versions of this software.

4. Title, ownership rights, and intellectual property rights in and to the Software shall remain in UbiQ Incorporated. You agree to abide by the copyright law and all other applicable laws of the country in which you are located, including, but not limited to, export control laws. You acknowledge that the Software in source code form remains a confidential trade secret of the developer and therefore you agree not to modify the Software or attempt to decipher, decompile, disassemble or reverse engineer the Software, except to the extent applicable laws specifically prohibit such restriction.

5. This statement shall be governed by and construed in accordance with the laws of the State of Minnesota, USA. This statement sets forth the entire agreement between you and UbiQ Incorporated.

Trademarks

All company and product names are trademarks or registered trademarks of their respective owners. This product and related documentation are protected by copyright and are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form by any means without prior written authorization of UbiQ Inc.

Microsoft, Windows, and Internet Explorer are registered trademarks of Microsoft Corporation. Netscape is a registered trademark of Netscape Communications Corporation.

Limitation of Liability

UbiQ Inc. is not responsible for any lost, corrupted or misdirected data through the use of this product. No warranties, whether expressed or implied, are given. The only remedy available to a buyer or anyone claiming through the buyer is the exchange of the defective product, or payment of amount of money equal to the purchase price, at the discretion of UbiQ Inc., within the designated warranty period. UbiQ Inc. reserves the right to change the specifications of this product at any time without notice.

FCC Warning Statement

The card reader has been tested and found to comply with the limits for Class B digital devices, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that utilized by the receiver.

Consult the dealer or an experienced radio/TV Technician for help.

Note: Shielded interface cables must be used in order to comply with emission limits.

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Table of Contents

UbiQ®*IDmail* 1

Introduction

One purpose of this Administrative Manager User Guide is to provide guidance to the enterprise Audit Manager and other enterprise security administrators in the use of the Administrative Manager utility for the central setup and implementation of enterprise e-mail security policy.

The Administrative Manager will also be used in the day-to-day operation of the UbiQ*IDmail* system.

Other UbiQ*IDmail* system documentation includes the following guides:

- Introduction to Information Security

  This describes the architecture and security features of the UbiQ*IDmail* System, and basic cryptographic technology used. It also includes several subjects pertinent to the establishment of an effective enterprise security policy, as well as a definition of typical enterprise security administration roles.

  It also provides suggestions for selecting a pass phrase.

- UbiQ*IDmail* Enrollment Server User Guide.
- UbiQ*IDmail* Client User Guide.
- UbiQ*IDmail* Client Trial Kit User Guide.

  The above three guides cover both installation and operations.

- UbiQ*IDmail* Diagnostic Manager User Guide

  This guide provides guidance in the diagnosis of the UbiQ*IDmail* Client.

UbiQ®IDmail

Individual Users

2

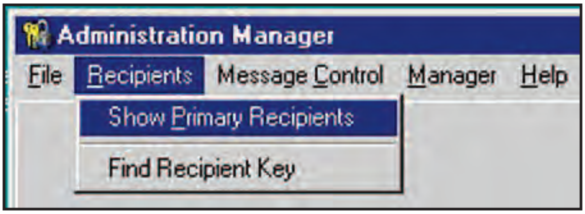
This chapter covers accessing information and modifying system settings for individual Users

In this chapter

- Displaying User’s Information
- Searching for a User by E-mail address
- Deleting a User from the Data Base

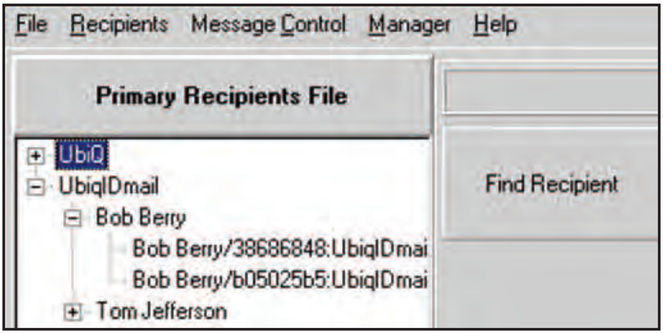
Displaying User Information

1. Select Show Personal Recipients from the Recipients menu.



2. A split window will appear. The left window shows the users enrolled in the system.

- Clicking on the + icon will show all the users under a particular heading.
- Clicking on the + icon next to a user will show the public keys for the user.

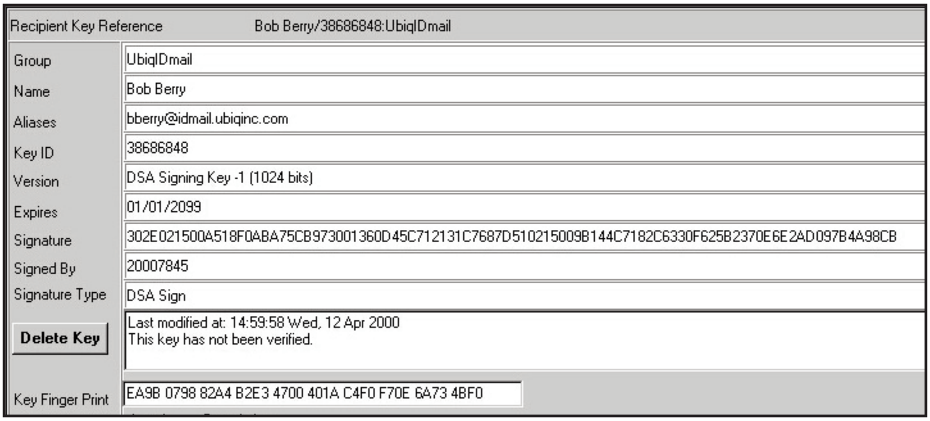


Public Keys

For each user there are two public keys, a RPK key and a DSA key.

For more information about public keys refer to the Public Key Cryptography section of the Introduction chapter.

3. Clicking on one of the user keys will bring up information on the user's key in the right window.



Recipient Key Reference	Bob Berry/38686848:UbiqIDmail
Group	UbiqIDmail
Name	Bob Berry
Aliases	bberry@idmail.ubiqinc.com
Key ID	38686848
Version	DSA Signing Key -1 (1024 bits)
Expires	01/01/2099
Signature	302E021500A518F0ABA75CB973001360D45C712131C7687D510215009B144C7182C6330F625B2370E6E2AD097B4A98CB
Signed By	20007845
Signature Type	DSA Sign
	Last modified at: 14:59:58 Wed, 12 Apr 2000 This key has not been verified.
Key Finger Print	EA9B 0798 82A4 B2E3 4700 401A C4F0 F70E 6A73 4BF0

4. This screen provides the audit manager the following information.

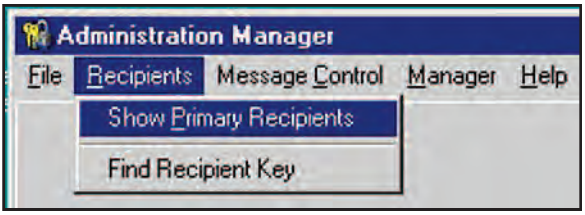
- Group (If applicable)
- The user's name.
- Aliases (The user's e-mail address)
- Key ID (An eight character identifier for the user's public key.)
- Version (The type and strength of the user's public key.)
- Expires (The key expiration date.)
- Signature (A hexadecimal representation of the user's public key certificate.)
- Signed By (A serial number assigned to the security officer who enrolled the user.) This identifies the security officer who enrolled the user.
- Signature Type (The public key algorithm used by the security officer to sign the certificate.)
- Key Finger Print (A hash of the user's key information.)

> **Important**
>
> Compliance, Trust Level and Message Control Options are not currently active. These features may be activated in later versions of the software.

Searching for a User by E-mail Address

This is a useful option if your enterprise has a large number of users in the primary recipient file.

1. Select Show Primary Recipients from the Recipients menu.

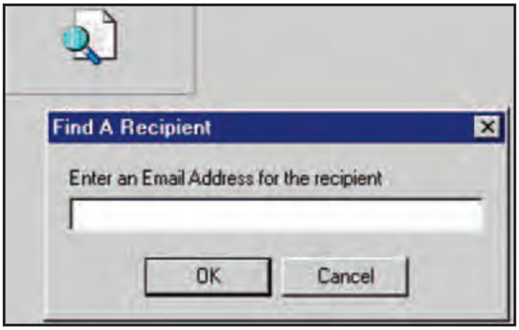


2. A split window will appear. The left window shows the users enrolled in the system.

3. Click on the Find Recipient icon.

   - You can also select Find Recipient Key from the Recipient menu.

4. A window will pop up asking for the user's e-mail address.

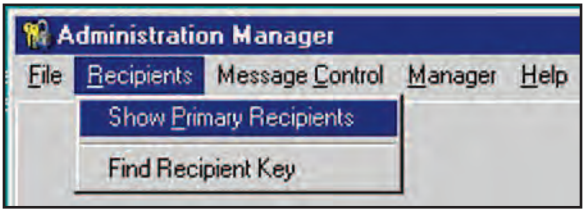


5. Enter the e-mail address and click on the OK button.

6. If a match is found the user will be displayed in the Primary Recipients window.

Deleting a User’s Key from the Database

1. Select Show Primary Recipients from the Recipients menu.



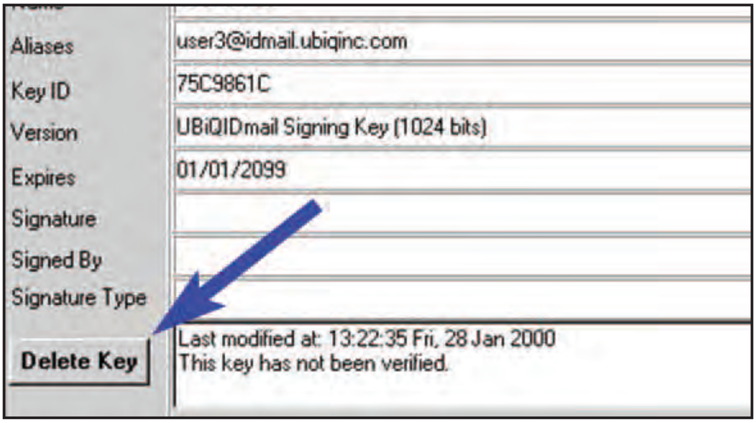
2. A split window will appear. The left window shows the users enrolled in the system.

3. Click on one of the user’s keys in the left window.

4. Information about the key should appear in the right window.

5. Verify the name and e-mail address of the user you wish to delete from the system

6. Click on the Delete Key button.



Aliases user3@idmail.ubiqinc.com
Key ID 75C9861C
Version UBiQIDmail Signing Key (1024 bits)
Expires 01/01/2099
Signature
Signed By
Signature Type

Last modified at: 13:22:35 Fri, 28 Jan 2000
This key has not been verified.

7. A warning window will appear to confirm that you wish to delete this user.

Warning

Once a user is deleted the data cannot be recovered. Once a user has been deleted, the user must be issued a new card before he / she can use the system.

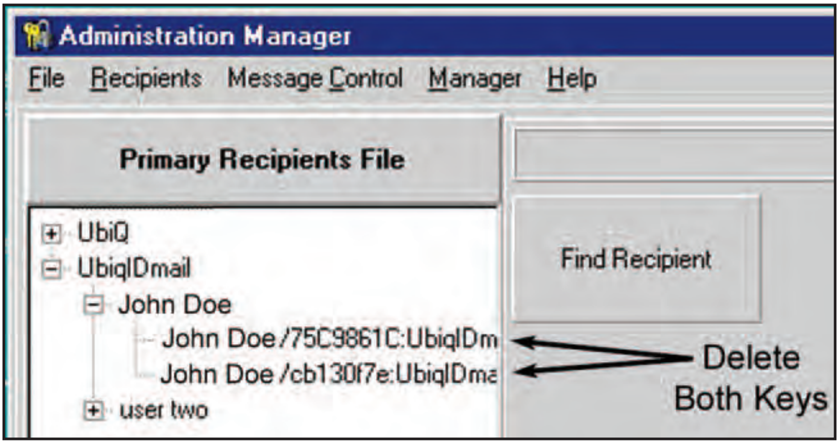
8. Click on the Yes button if you wish to delete the user's key.

9. Click on the remaining user key and delete this key.

Recommendation

When a user's key is deleted from the system it is recommended that the enterprise also recover the user's badge.

When deleting a user key from the system you should delete both the RPK and DSA keys.



UbiQ®IDmail

Message Control Policy

3

This chapter covers reviewing, modifying and creating message control policies.

A single message control policy, often referred to as the default policy, may apply uniformly to everyone in the enterprise.

It is also possible to have more than one policy in the enterprise, each with a separate name, unique action options and list of users it applies to.

For each of the seven part of a message control policy, there exists a number of action options. A policy comprises a combination of action options for the seven parts.

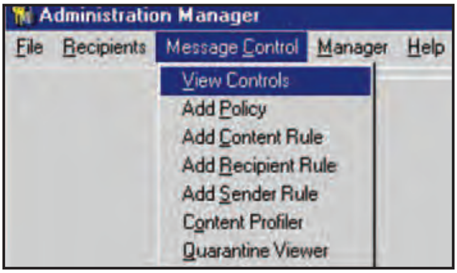
One action option within each part is the default option. If no change is made relative to these message control policy action options, the enterprise would have an active message control policy (default) consisting of the seven action options.

In this chapter

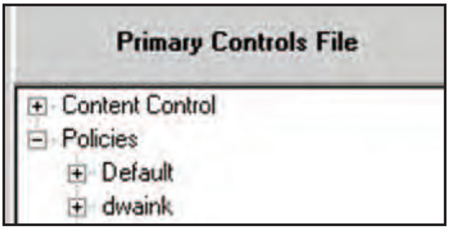
- Viewing Current Controls
- Creating a New Message Control Policy
    - New Recipients
    - Incoming
    - Outgoing
    - Handling
    - Receipts
    - Warning Text
    - Connection

Viewing Current Controls

1. Select View Controls from the Message Control menu.



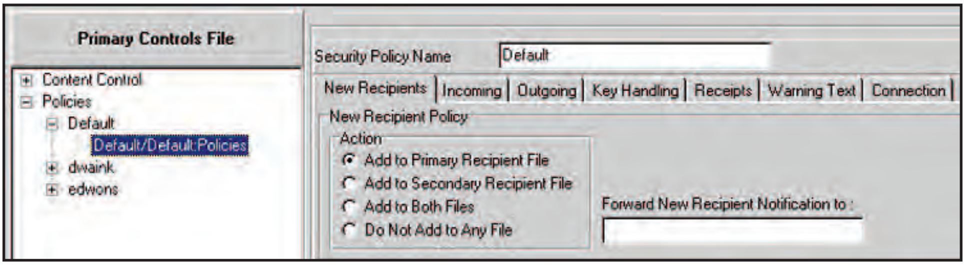
2. Click on the + sign next to the policies folder.



3. Click on the + sign next to the folder containing the policy you wish to view.

4. Click on the policy name.

5. A tabbed window will give you access to the content control settings. By clicking on the seven tabs you are able to review the action settings, as well as the forwarding notification addresses, for the selected policy.


Security Policy Name: Default

New Recipient Policy

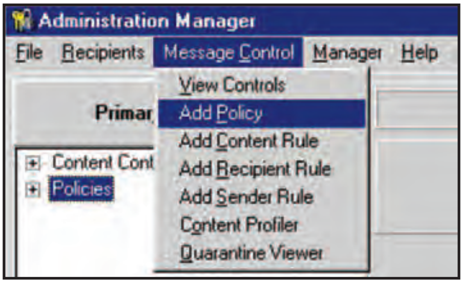
Action

● Add to Primary Recipient File
○ Add to Secondary Recipient File
○ Add to Both Files
○ Do Not Add to Any File

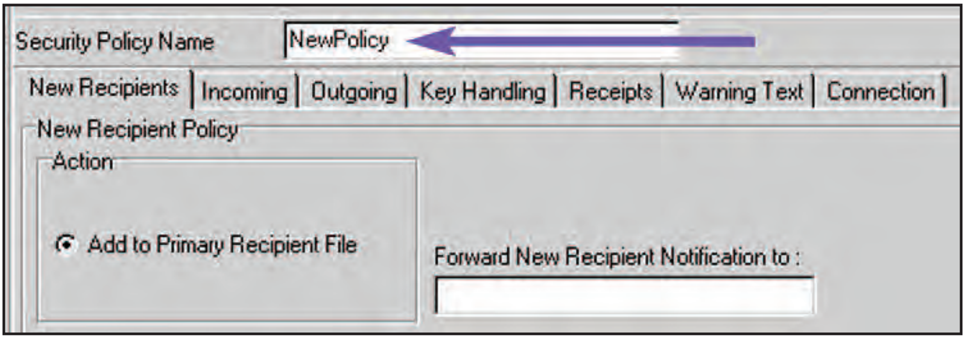
Forward New Recipient Notification to :

Creating a New Message Control Policy

1. Select Add Policy from the Message Control menu.



2. Enter a Name for the new Policy.



Security Policy Name: NewPolicy

● Add to Primary Recipient File

Forward New Recipient Notification to :

3. The following seven sections of this chapter describes the tabbed components of a security policy. Review each of the components and determine how the action options for the new policy will vary from the default actions..

Default Settings

When a new policy is created, default action settings appear, but these can be changed by clicking on the appropriate radio buttons. The default settings are noted for each parameter in the following sections of this chapter.

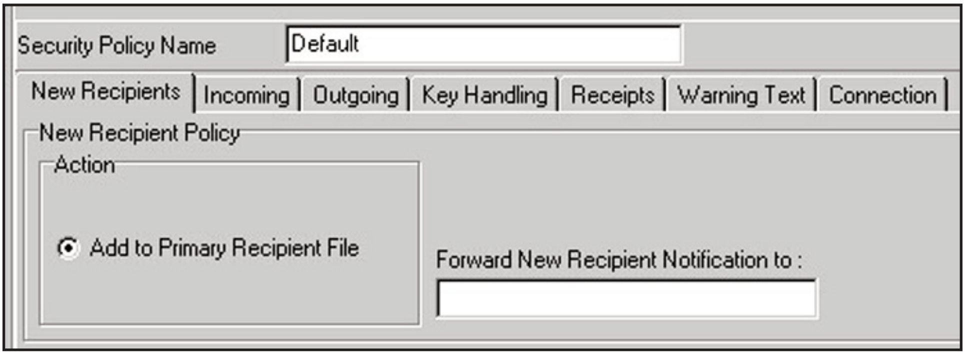
Message Control Policy - New Recipients

Each time a message is received the sender's public keys are embedded in the message header. If the sender's public keys are not in the primary database, the sender is flagged as new recipient.

This policy controls what happens when a new recipient is detected by the UbiQ*IDmail* system.

1. Select Add Policy from the Message Control menu.

2. Click on the New Recipients tab.



Security Policy Name: Default

● Add to Primary Recipient File

Forward New Recipient Notification to :

3. The program automatically sets the action to "Add to Primary Recipient File".

Default Setting - Automatically Add New Recipients

Automatically adds the new recipient to the primary recipients data file.

4. If the notification option is selected, enter the e-mail address of the person to be notified.

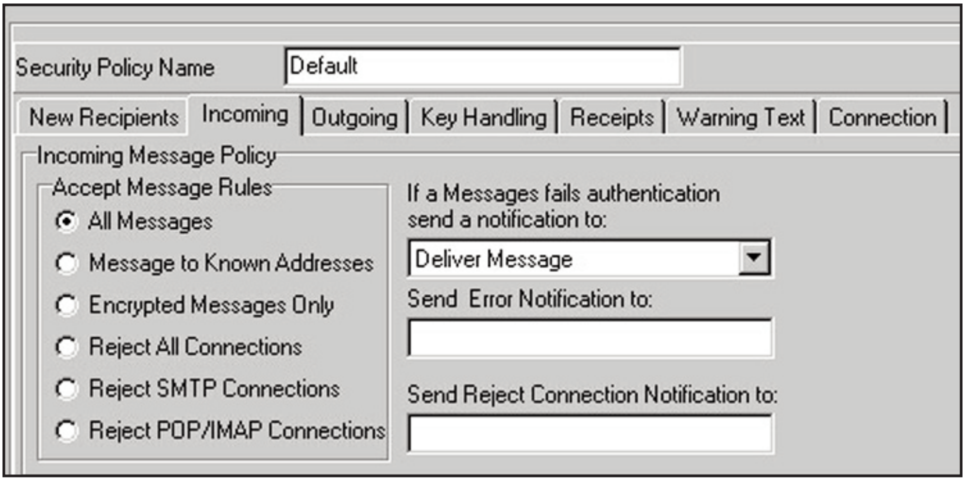
5. Click on the Save button to save any changes.

Message Control Policy - Incoming

This policy determines who can connect to the system, if unencrypted messages are accepted and what action to take if there is an authentication failure.

1. Select Add Policy from the Message Control menu.

2. Click on the Incoming tab.



Security Policy Name: Default

Incoming Message Policy

Accept Message Rules

● All Messages
○ Message to Known Addresses
○ Encrypted Messages Only
○ Reject All Connections
○ Reject SMTP Connections
○ Reject POP/IMAP Connections

If a Messages fails authentication send a notification to: Deliver Message

Send Error Notification to:

Send Reject Connection Notification to:

3. The program allows several options for Accept Message Rules.

Default Setting - Accept All Messages

The UbiQ*IDmail* system will accept all encrypted and clear text e-mail messages.

Messages to Known Address

This option accepts only messages addressed to users in the user database.

Encrypted Messages Only

This option accepts only encrypted messages.

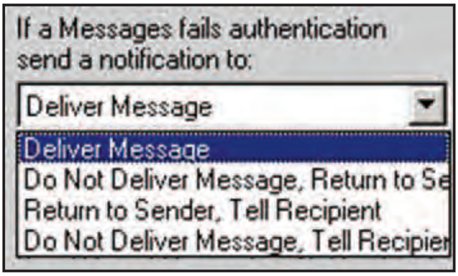
Connections

One of three options can be selected to reject certain types of connections to the system. Normally none of these options are selected. They are provided to control access to the UbiQ*IDmail* system. If you wish to close off the system, consult with the facilities network administrator to determine which option is appropriate to your need and situation.

- If one of these three options are selected, you can choose to enter the e-mail address of the person to be notified of each rejected connection.

4. Select the desired option(s). (The default option is recommended.)

5. The program also allows the system administrator to specify the response if a message fails authentication.



If a Messages fails authentication send a notification to:

Deliver Message

Deliver Message
Do Not Deliver Message, Return to Se
Return to Sender, Tell Recipient
Do Not Deliver Message, Tell Recipie

Default Setting - Deliver Message

Delivers the message regardless of the authentication failure.

Do Not Deliver Message - Return to Sender

Blocks the message but notifies the sender of the authentication failure.

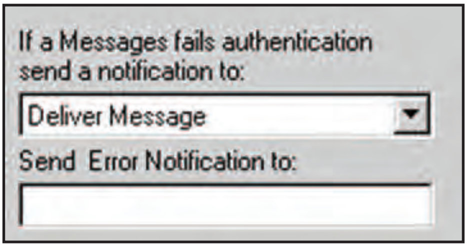
Return to Sender - Tell Recipient

Returns the message to the sender indicating there was an authentication failure. A message is generated to the recipient that the message was returned to the sender.

Do Not Deliver Message - Tell Recipient

Blocks the message but notifies the recipient of the authentication failure.

- The system administrator can choose to enter the e-mail address of the person to be notified of each authentication failure.



If a Messages fails authentication send a notification to: Deliver Message

Send Error Notification to:

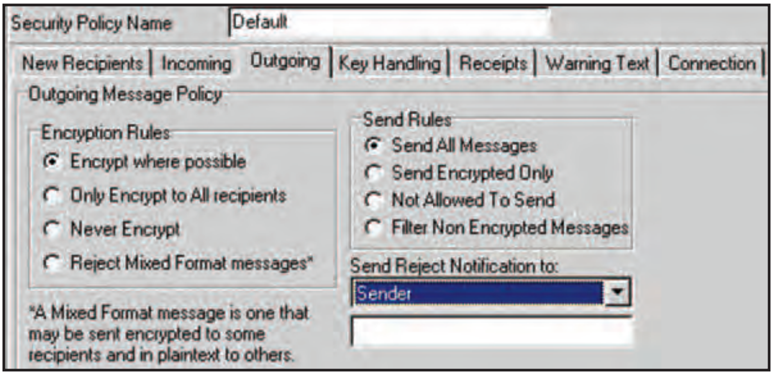
6. Click on the Save button to save any changes.

Message Control Policy - Outgoing

This policy establishes rules for encryption and sending messages.

1. Select Add Policy from the Message Control menu.

2. Click on the Outgoing tab.



Security Policy Name: Default

Outgoing Message Policy

Encryption Rules

● Encrypt where possible

○ Only Encrypt to All recipients

○ Never Encrypt

○ Reject Mixed Format messages*

*A Mixed Format message is one that may be sent encrypted to some recipients and in plaintext to others.

Send Rules

● Send All Messages

○ Send Encrypted Only

○ Not Allowed To Send

○ Filter Non Encrypted Messages

Send Reject Notification to: Sender

3. The program allows several options for Encryption rules.

Default Setting - Encrypt - Where Possible

This setting will encrypt messages to all recipients with public keys accessible to the sender. The same message to recipients not in the primary database will not be encrypted.

Only Encrypt to All Recipients

This option requires all messages to be encrypted.

Never Encrypt

This option disables the encryption function.

Reject Mixed Format Messages

This option rejects messages that specify some recipients that are in the primary database and others that are not.

4. The program allows several options for Send rules.

Default Setting - Send All Messages

Will send all messages.

Send Encrypted Only

This option only allows encrypted messages to be sent.

Not Allowed to Send

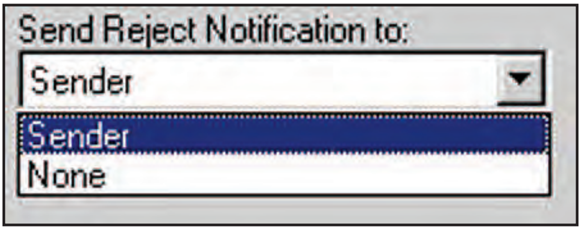
This option disables the user’s ability to send messages.

Filter Non-Encrypted Messages

This option applies to messages sent to multiple recipients. Unencrypted messages are rejected but the encrypted messages are allowed.

5. Select the desired options.

6. The program also allows the system administrator to specify the response if an encryption or send rule has been violated.



Send Reject Notification to:

Sender

Default Setting - Send Rejection Notification to Sender

Notifies the sender of the rule violation.

None

The sender is not notified of the rule violation.

- The system administrator can choose to enter the e-mail address of the person to be notified of each rule violation.

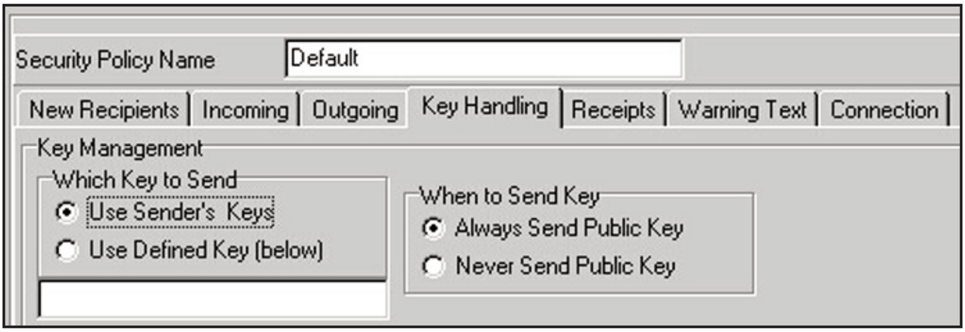
7. Click on the Save button to save any changes.

Message Control Policy - Key Handling

The key management policy provides control over which key to send with an e-mail and when to send it.

1. Select Add Policy from the Message Control menu.

2. Click on the Key Handling tab.



Security Policy Name: Default

Key Management

Which Key to Send

● Use Sender's Keys

○ Use Defined Key (below)

When to Send Key

● Always Send Public Key

○ Never Send Public Key

Which Key to Send

The UbiQ*IDmail* system utilizes a user's card and pass phrase to send and receive secure files. This means Sender's keys is the only option with respect to the type of key that can be sent.

3. The program allows two options specifying if the sender's public key should be sent.

Default Setting - Always Send Public Key

This option should be normally selected. If the public key is not sent with a message, the recipient may not be able to encrypt a response. By always including the sender's public key with the message, the recipient will always have the ability to send an encrypted response.

Never Send Public Key

This option is not recommended.

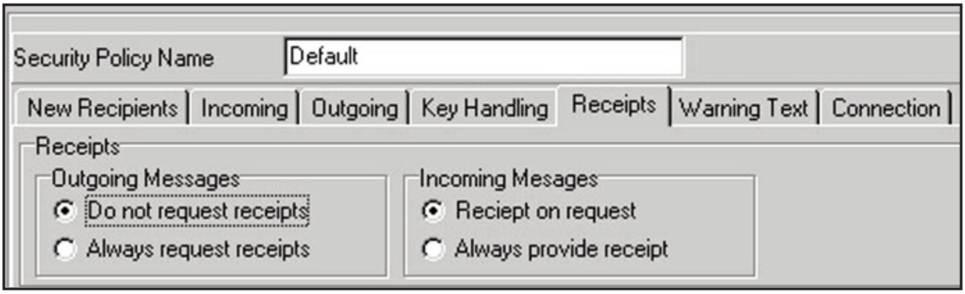
4. Click on the Save button to save any changes.

Message Control Policy - Receipts

The Receipts Policy provides the message sender the option to request receipts from the recipient or not. The recipient has the option to provide receipts only on request or to always provide them.

1. Select Add Policy from the Message Control menu.

2. Click on the Receipts tab.



Security Policy Name: Default

Receipts

Outgoing Messages
● Do not request receipts
○ Always request receipts

Incoming Mesages
● Reciept on request
○ Always provide receipt

3. The program allows two options for outgoing messages.

Default Setting - Do not Request Receipts

The sender will not request the recipient to acknowledge the message.

Always Request Receipts

The sender will always request the recipient to acknowledge the message.

4. The program allows two options for incoming messages.

Default Setting - Receipt on Request

The recipient will acknowledge with a message receipt if requested by the sender.

Always Provide Receipt

The recipient will always acknowledge with a message receipt.

5. Select the desired options.

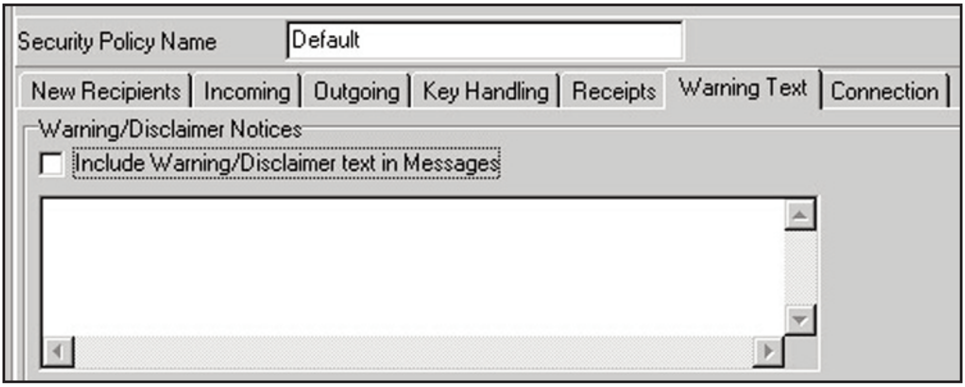
6. Click on the Save button to save any changes.

Message Control Policy - Warning Text

Allows the sender to include a warning disclaimer statement in all messages.

1. Select Add Policy from the Message Control menu.

2. Click on the Warning Text tab.



Security Policy Name: Default

Warning/Disclaimer Notices

□ Include Warning/Disclaimer text in Messages

Default Setting - Option is Off

No message is sent with all messages.

3. To activate the option click on the Include Disclaimer Text in the Message Box.

4. Enter the message you want to include in each message.

Important

The text will appear as a header in every message.

5. Click on the Save button to save any changes.

Message Control Policy - Connection

SMTP

This option controls e-mails send via the Internet. E-mail messages are sent via the Internet using Simple Mail Transfer Protocol (SMTP). As part of setting up Internet e-mail an Internet Provider (IP) number is assigned to each SMTP.

Post Office Protocol (POP)

Messages are received using Post Office Protocol 3 (POP3) or IMAP. The IP number for receiving messages may be the same as the IP for the SMTP or it may be a different number.

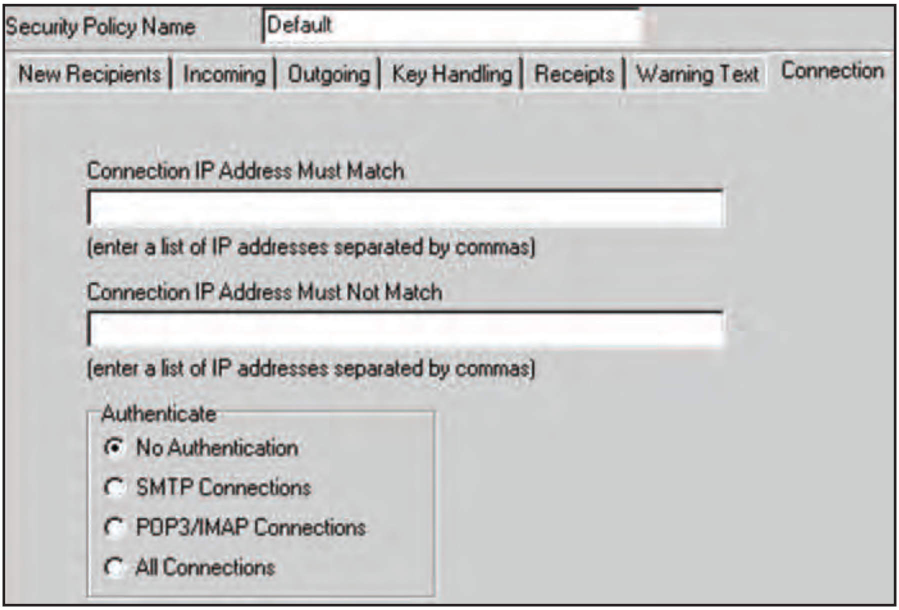
IP Number

The IP numbers allow the system administrator to exclude messages from specific IP addresses. This is useful if the facility wishes to block messages from a specific source.

The system can also be configured so it will allow messages only from certain addresses.

1. Select Add Policy from the Message Control menu.

2. Click on the Connection tab.



Security Policy Name: Default

Connection IP Address Must Match

(enter a list of IP addresses separated by commas)

Connection IP Address Must Not Match

(enter a list of IP addresses separated by commas)

Authenticate

● No Authentication
○ SMTP Connections
○ POP3/IMAP Connections
○ All Connections

3. To block access to specific IP addresses, enter the IP number(s) in the Connection IP Address Must Not Match box.

4. To allow access to only specific IP addresses, enter the IP number(s) in the Connection IP Address Must Match box.

Warning

Entering an IP address may block desired connections. An IP address may cover a very large number of Internet users. This option should be used with extreme caution.

5. The program allows three options for Connection Authentication.

Default Setting - No Authentication

The system will allow users to send and receive messages from any IP address.

SMTP Connections

The system will allow users to send messages only to specified IP addresses.

POP3/IMAP Connections

The system will allow users to receive messages only to specified IP addresses.

All Connections

The system will allow users to send and receive messages only to specified IP addresses.

6. Click on the Save button to save any changes.

4

Message Blocking

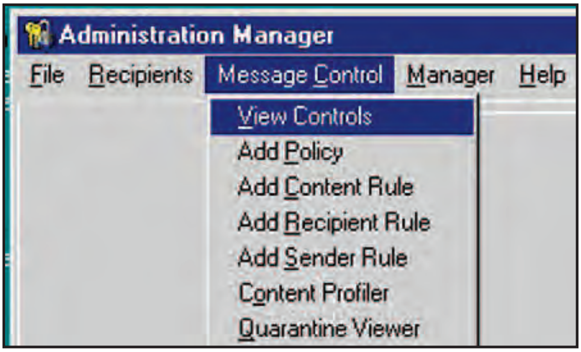
This chapter covers how to establish message blocking for both inbound and outbound messages.

As with Message Control Policy, defined in the Introduction to Chapter 3, there may also exist mor that one Message Blocking rule for the enterprise.

In this chapter

Viewing the Current Message Blocking Rule

1. Select View Controls from the Message Control menu.

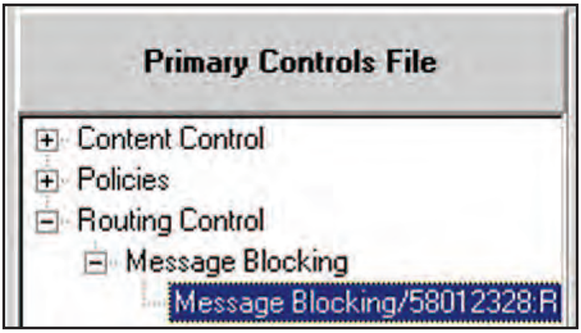


2. Click on the + sign next to the Routing Control folder.

Note - If a Routing Control Folder Does not Exist

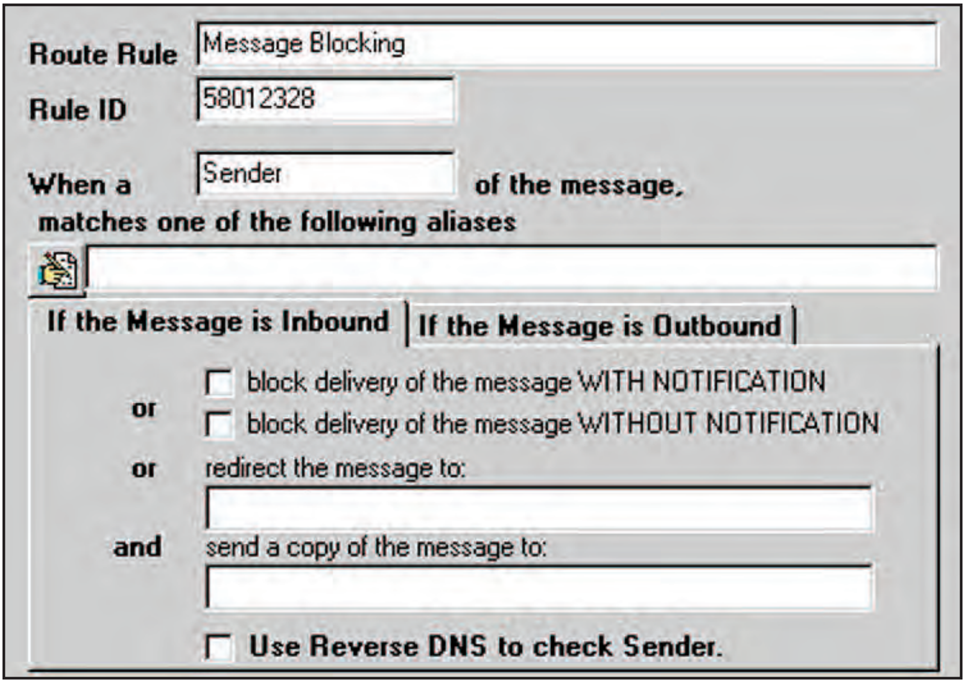
When the system is first installed, the default settings do not contain a Routing Control (Message Blocking) rule. If the folder does not exist you may wish to create a Routing Rule. Refer to the Creating a New Routing Rule section of this chapter.

3. Click on the + sign next to the folder containing the policy you wish to view.



4. Click on the policy name.

5. A Route Rule window will appear allowing you to establish or modify message blocking.



Route Rule: Message Blocking

Rule ID: 58012328

When a Sender of the message, matches one of the following aliases

If the Message is Inbound | If the Message is Outbound

□ block delivery of the message WITH NOTIFICATION

or □ block delivery of the message WITHOUT NOTIFICATION

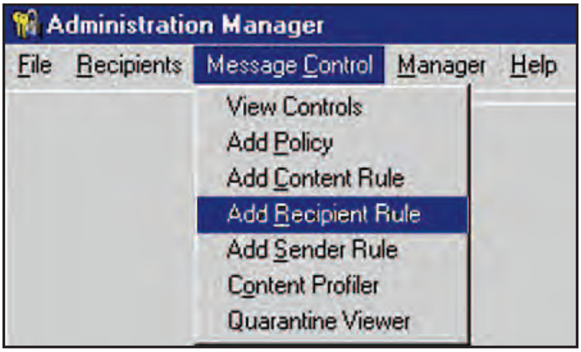
or redirect the message to:

and send a copy of the message to:

□ Use Reverse DNS to check Sender.

Creating a New Routing Rule

1. Select Add Recipient Rule or Add Sender Rule from the Message Control menu.



Recipient Rule and Sender Rule

The program allows the system administrator to create separate rules for the sender of a message and the recipient of a message.

Continue now with the remaining sections of this chapter by:

- Selecting Add Recipient Rule to set up Inbound Message Blocking
- Selecting Add Sender Rule to set up Outbound Message Blocking.

Inbound Message Blocking

Message Blocking by IP Address

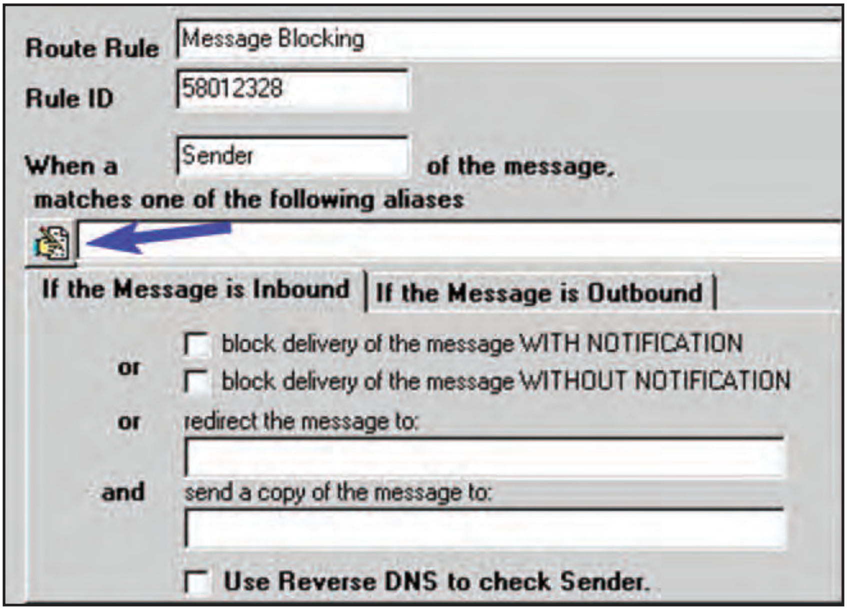
This feature is used to block messages from specific e-mail addresses. If you wish to block messages from a specific network (IP address) use the use the Connections option of the Message Control Policy. (Refer to the Message Control Policy - Connection section of the Message Control chapter of this manual.)

1. Select Add Recipient Rule or Add Sender Rule from the Message Control menu.

2. Enter a name for the Rout Rule.

3. Click on the If the Message is Inbound tab.

4. Click on the Write icon.



Route Rule: Message Blocking

Rule ID: 58012328

When a Sender of the message. matches one of the following aliases

If the Message is Inbound | If the Message is Outbound

□ block delivery of the message WITH NOTIFICATION

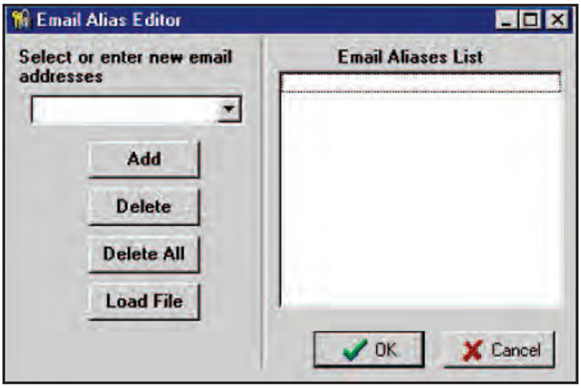
or □ block delivery of the message WITHOUT NOTIFICATION

or redirect the message to:

and send a copy of the message to:

□ Use Reverse DNS to check Sender.

5. An E-mail Alias Editor window will appear.

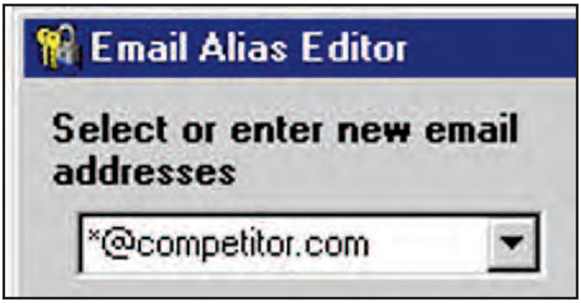


6. Build / modify the list to include all the e-mail aliases you wish to block. Refer to the E-mail Alias Editor section of this chapter.

Blocking All E-mail from a Domain

A domain is the part of the e-mail address after the @ symbol. The domain for the e-mail address “user@company.com” is “company.com”.

You can use the wild card symbol “*” to block all e-mail to a designated domain by entering the following. “*@domain”. Example: *@competitor.com



*@competitor.com

7. Specify what should happen if the system detects a blocked alias. There are three options:

   - Block delivery with notification.

   - Block delivery without notification.

   - Redirect the message to a designated e-mail address and send a copy of the message to a designated e-mail address. Select this option if you wish to designate someone to screen e-mail from specified sources.

     This option allows the message to be copied to a second e-mail address.

> **Important**
>
> If an inbound encrypted message is blocked, and the rule specifies the message to be redirected to a third person, that third person will not be able to decrypt the message.

> **Reverse DNS**
>
> In the United Kingdom and some other countries, the fields in domain names are in reverse order. (Example: “user@uk.ac.smithco” instead of “user@smithco.ac.uk”) If you wish to block these addresses, check the Use Reverse DNS to Check Sender option.

8. Click on the Save button to save any changes.

Outbound Message Blocking

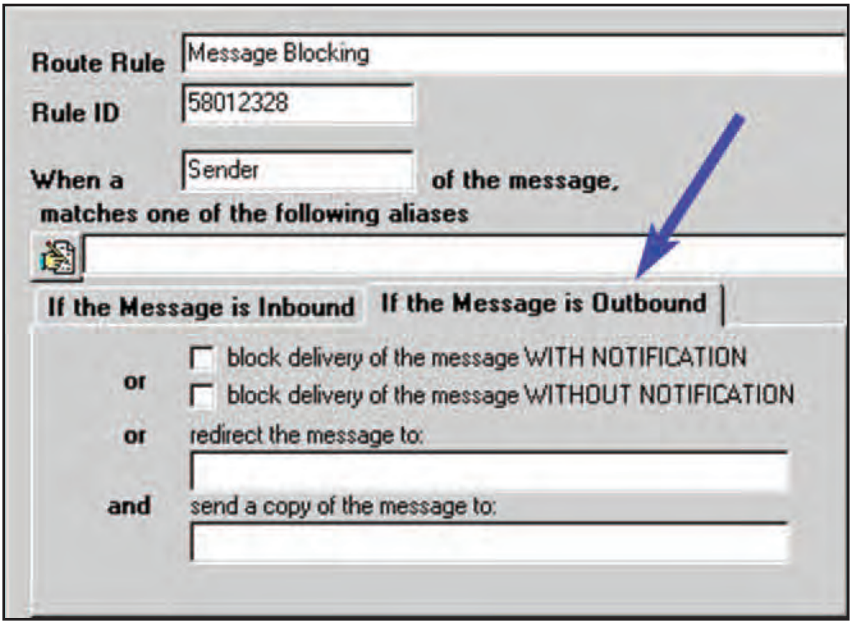
Message Blocking by IP Address

This feature is used to block messages from specific e-mail addresses. If you wish to block messages from a specific network (IP address) use the use the Connections option of the Message Control Policy. (Refer to the Message Control Policy - Connection section of the Message Control chapter of this manual.)

1. Select Add Recipient Rule or Add Sender Rule from the Message Control menu.

2. Enter a name for the Rout Rule.

3. Click on the If the Message is Outbound tab.



Route Rule: Message Blocking

Rule ID: 58012328

When a Sender of the message, matches one of the following aliases

or □ block delivery of the message WITH NOTIFICATION

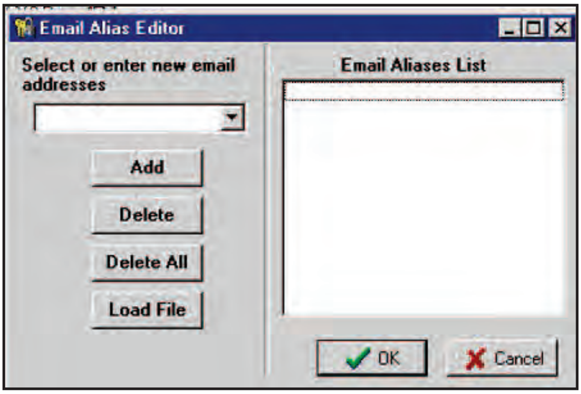
□ block delivery of the message WITHOUT NOTIFICATION

or redirect the message to:

and send a copy of the message to:

4. Click on the Write icon.

5. An E-mail Alias Editor window will appear.

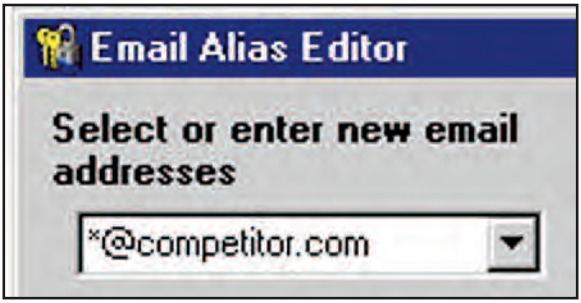


6. Build / modify the list to include all the e-mail aliases you wish to block. Refer to the E-mail Alias Editor section of this chapter.

Blocking All E-mail to a Domain

A domain is the part of the e-mail address after the @ symbol. The domain for the e-mail address "user@company.com" is "company.com".

You can use the wild card symbol "*" to block all e-mail to a designated domain by entering the following. "*@domain". Example: *@competitor.com



*@competitor.com

7. Specify what should happen if the system detects a blocked alias. There are three options.

   - Block delivery with notification.

   - Block delivery without notification.

   - Redirect the message to a designated e-mail address and send a copy of the message to a designated e-mail address. Select this option if you wish to designate someone to screen e-mail from specified sources.

     This option allows the message to be copied to a second e-mail address.

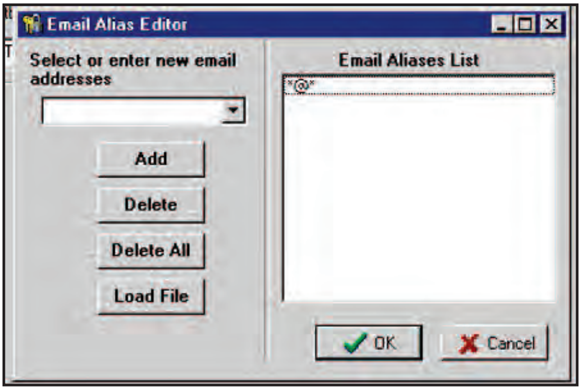
> **Important**
>
> If an inbound encrypted message is blocked, and the rule specifies the message to be redirected to a third person, that third person will not be able to decrypt the message.

> **Reverse DNS**
>
> In the United Kingdom and some other countries, the fields in domain names are in reverse order. (Example: “user@uk.ac.smithco” instead of “user@smithco.ac.uk”) If you wish to block these addresses, check the Use Reverse DNS to Check Sender option.

8. Click on the Save button to save any changes.

E-mail Alias Editor

The e-mail addresses to be blocked are displayed in the E-mail Aliases List window.



Entering a New E-mail Address

1. Enter the address in the Select or Enter New E-mail address window.

2. Click on the Add button.

3. Clicking on the OK button closes the Editor window and saves the changes.

Deleting an E-mail Address from the List

1. Highlight the address to be deleted in the Select or Enter New E-mail address window.

2. Click on the Delete button.

3. Clicking on the OK button closes the Editor window and saves the changes.

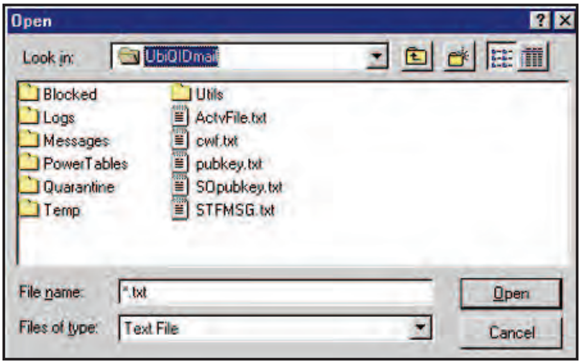
To delete all addresses from the list click on the Delete All button.

Load Addresses from a File

The program allows the user to import a list of address from a file. The file must be a text (.txt) format.

1. Click on the Load File button.

2. Locate the file containing the addresses you wish to import.



Look in: UbiQIDmail

File name: *.txt

Files of type: Text File

3. Click on the Open button.

4. The addresses in the text file will added to the list and should appear in the list window.

5. Clicking on the OK button closes the Editor window and saves the changes.

UbiQIDmail®

5

Content Scanning

Content scanning is active only for users with the Fortress software.

This chapter covers how to set content scanning parameters and what happens if a message violates the defined parameters.

Content Scanning Rules are made up of scanning profiles (which define the content to be scanned) and action options (which define the action to be taken when there is a “hot” against the profile).

The profiles and action options amy vary well be different for inbound and outbound e-mail traffic. There fore, it is important to consider both.

More that one Content Scanning Rule may exist in the enterprise, each with its own profiles, action options and list of users it applies to.

Though the Content Scanning Rules have default action options and some ready-made profiles, it is recommended that these be reviewed by the enterprise, particularly the profiles for Filter Attachments and Banned Attachments.

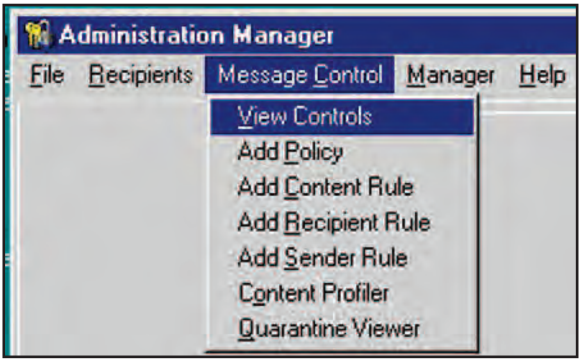
In this chapter

Important

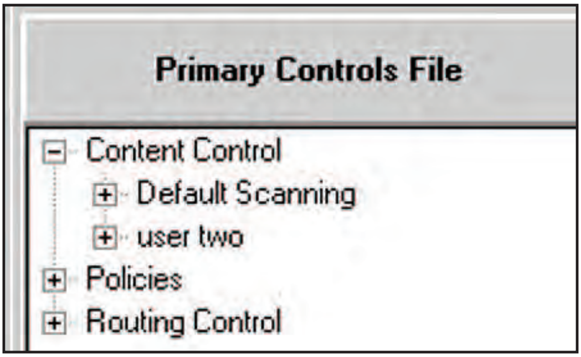
Content scanning is active only with the UbiQ Fortress user software.

Viewing the Current Content Control Rules

1. Select View Controls from the Message Control menu.



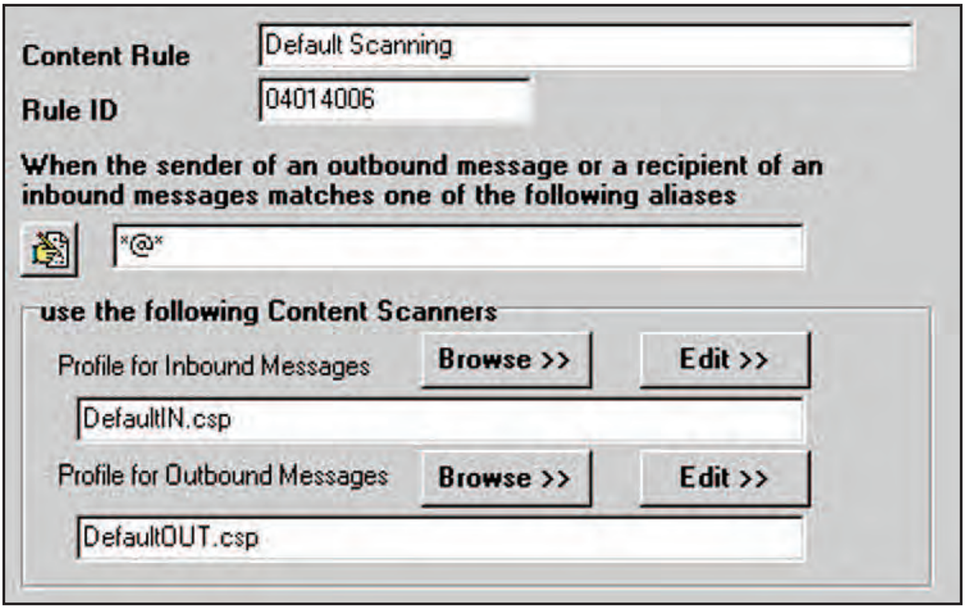
2. Click on the + sign next to the Content Control folder.



3. Click on the + sign next to the folder containing the rule you wish to view.

4. Click on the rule name.

5. The client users affected by this rule are listed in the sender or recipient box.



Content Rule: Default Scanning

Rule ID: 04014006

When the sender of an outbound message or a recipient of an inbound messages matches one of the following aliases: *@*

use the following Content Scanners

Profile for Inbound Messages: DefaultIN.csp

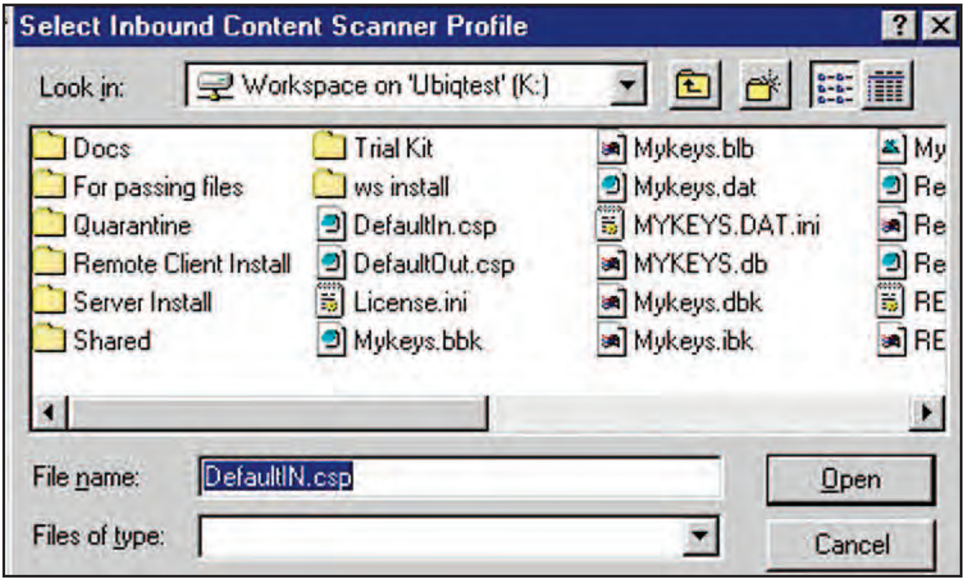
Profile for Outbound Messages: DefaultOUT.csp

- The default setting is "*@*"; this would include all e-mail addresses.

- If you wish to create multiple rules or security policies, refer to the chapter Establishing Multiple Security Policies.

6. Profiles can be specified for both inbound and outbound messages.

   6.1 Click on the Browse button to select a profile.



Select Inbound Content Scanner Profile

Look in: Workspace on 'Ubiqtest' (K:)

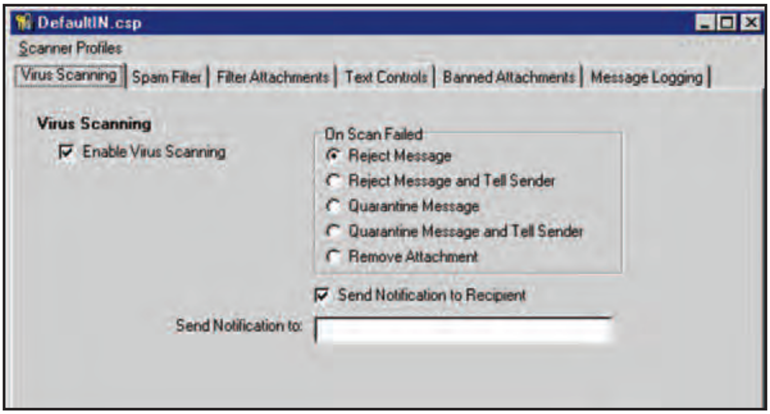
Docs
For passing files
Quarantine
Remote Client Install
Server Install
Shared
Trial Kit
ws install
DefaultIn.csp
DefaultOut.csp
License.ini
Mykeys.bbk
Mykeys.blb
Mykeys.dat
MYKEYS.DAT.ini
MYKEYS.db
Mykeys.dbk
Mykeys.ibk
My
Re
Re
Re
RE
RE

File name: DefaultIN.csp

Files of type:

7. To gain access to the action options click on the Edit button.

8. A tabbed window will appear giving you access to the action options for the various Content Control categories.



DefaultIN.csp

Virus Scanning

☑ Enable Virus Scanning

On Scan Failed

● Reject Message
○ Reject Message and Tell Sender
○ Quarantine Message
○ Quarantine Message and Tell Sender
○ Remove Attachment

☑ Send Notification to Recipient

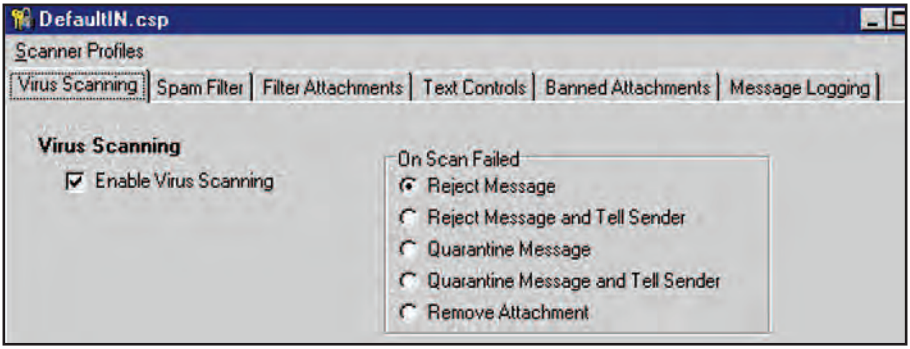
Send Notification to:

Content Control - Virus Scanning

1. Select Add Content Rule from the Message Control menu.

2. Enter a name for the Content Rule.

3. Click on the Virus Scanning tab.



Virus Scanning

☑ Enable Virus Scanning

On Scan Failed

● Reject Message
○ Reject Message and Tell Sender
○ Quarantine Message
○ Quarantine Message and Tell Sender
○ Remove Attachment

4. Virus scanning is turned on and off by clicking on the Enable Virus Scanning Box.

5. The program allows five action options if a virus is detected.

Default Setting - Reject Message

The message is rejected and is not delivered. No notification is given to the sender.

Reject Message and Tell Sender

The message is rejected and is not delivered. A message is generated informing the sender the message was rejected because a virus was detected.

Quarantine Message

The message is routed to a quarantine file. No notification is given to the sender. (To view quarantined messages refer to the Viewing Quarantined Files section of this chapter.)

Quarantine Message and Tell Sender

The message is routed to a quarantine file. A message is generated informing the sender the message was rejected because a virus was detected. (To view quarantined messages refer to the Viewing Quarantined Files section of this chapter.)

Remove Attachment

The message is delivered but the attachment containing the virus is removed. No notification is given to the sender.

6. Notification to the recipient is turned on and off by clicking on the Send Notification to Recipient Box.

7. A third party can be notified by entering an e-mail address in the Send Notification to: text box.

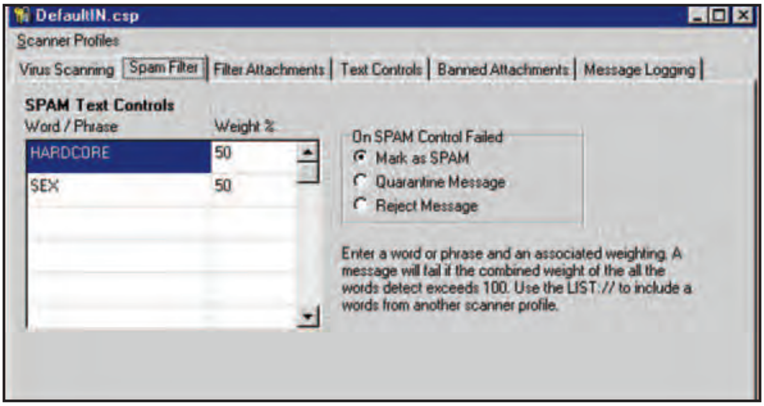
8. Click on the Save button to save any changes.

Content Control - Spam Filter

1. Select Add Content Rule from the Message Control menu.

2. Enter a name for the Content Rule if it doesn’t exist.

3. Click on the Spam Filter tab.



SPAM Text Controls

Word / Phrase	Weight %
HARDCORE	50
SEX	50

On SPAM Control Failed

● Mark as SPAM
○ Quarantine Message
○ Reject Message

Enter a word or phrase and an associated weighting. A message will fail if the combined weight of the all the words detect exceeds 100. Use the LIST:// to include a words from another scanner profile.

4. Enter the words or phrases and their weighted value. The words and their weighted values comprise the spam scanner profile.

Spam Content Scanner Profile

Spam filtering is set up by entering words or phrases in the Spam Text Control Table along with their associated weight.

The program scans messages for all the words and phrases entered in the text control box. If any of the words or phrases are present, the program totals the weighted percentage for each word or phrase. If the total meets or exceeds 100% the message is tagged as Spam.

For example, to filter messages containing the phrase “hardcore sex” you would enter the phrase and give it a weight of 100%.

You can also scan for the words separately by entering hardcore 50% and sex 50%. If the two words are present the weighted combination is 100% and the message is identified as Spam. This would allow a message containing the word “hardcore” alone to pass the Spam filter.

5. The program allows three action options if a Spam message is detected.

Default Setting - Mark as Spam

The message is delivered with a notification to the recipient that this message has been identified as Spam.

Quarantine Message

The message is routed to a quarantine file. (To view quarantined messages refer to the Viewing Quarantined Files section of this chapter.)

Reject Message

The message is rejected and is not delivered. No notification is given to the sender or recipient.

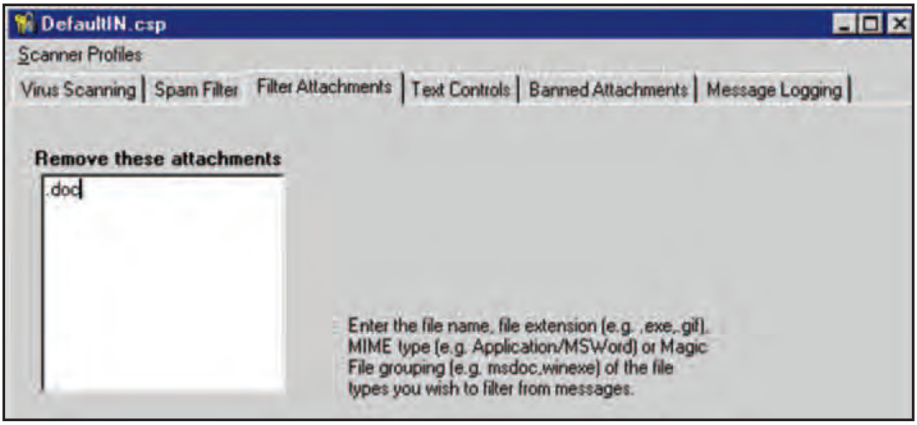
6. Click on the Save button to save any changes.

Content Control - Filter Attachments

1. Select Add Content Rule from the Message Control menu.

2. Enter a name for the Content Rule if it doesn’t exist.

3. Click on the Filter Attachments tab.



Remove these attachments

.doc

Enter the file name, file extension (e.g. ,exe,.gif), MIME type (e.g. Application/MSWord) or Magic File grouping (e.g. msdoc,winexe) of the file types you wish to filter from messages.

4. Enter the type of file attachments to be removed to create the filter attachments content scanner profile.

Filter Attachments Content Scanner Profile

Attachments to be removed are specified by type of file. Each file type is designated by one of three means of identification: file extension, Multipurpose Internet Mail Extension (MIME) and Magic File Grouping .

For example to filter MS/Word documents:

By extension “doc” would be entered.

By MIME “application/msword” would be entered. Most mail programs display the MIME type for file attachments allowing identification of other file types.

By Magic File Group “msdoc” would be entered.

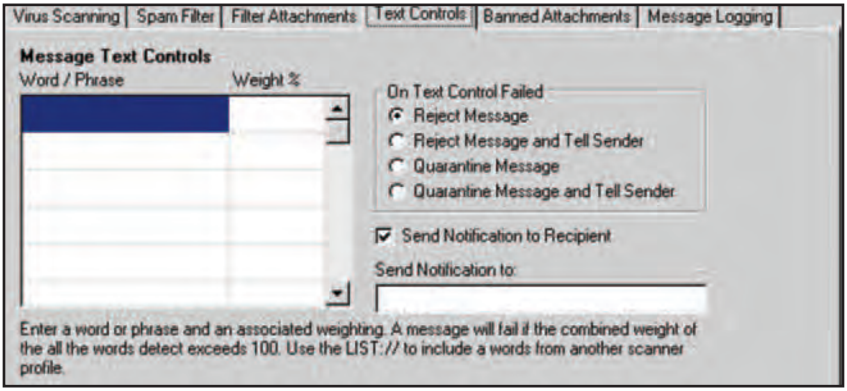
5. Click on the Save button to save any changes.

Content Control – Text Controls

1. Select Add Content Rule from the Message Control menu.

2. Enter a name for the Content Rule if it doesn't exist.

3. Click on the Text Controls tab.



On Text Control Failed
● Reject Message
○ Reject Message and Tell Sender
○ Quarantine Message
○ Quarantine Message and Tell Sender

☑ Send Notification to Recipient

Send Notification to:

Enter a word or phrase and an associated weighting. A message will fail if the combined weight of the all the words detect exceeds 100. Use the LIST:// to include a words from another scanner profile.

4. Enter the words or phrases and their weighted value that will comprise the text control content scanner profile.

Text Controls Content Scanner Profile

Text filtering is setup by entering words or phrases in the Message Text Control Table along with their associated weight.

The program scans messages for all the words and phrases entered in the text control box. If any of the words or phrases are present, the program totals the weighted percentage for each word or phrase. If the total equals or exceeds 100% the message is tagged as a hit.

For example, to filter messages containing the phrase "secret product", you would enter the phrase and give it a weight of 100%.

Text Controls Content Scanner Profile (cont)

You can also scan for the words separately by entering secret 50% and product 50%. If the two words are present the weighted combination is 100% and the message is identified as exceeding text parameters. This would allow a message containing the word “product” alone to pass the text filter.

5. The program allows four action options if the text in a message equals or exceeds a weighted value of 100%.

Default Setting - Reject Message

The message is rejected and is not delivered. No notification is given to the sender.

Reject Message and Tell Sender

The message is rejected and is not delivered. A message is generated informing the sender the message was rejected because of text context.

Quarantine Message

The message is routed to a quarantine file. No notification is given to the sender. (To view quarantined messages refer to the Viewing Quarantined Messages section of this chapter.)

Quarantine Message and Tell Sender

The message is routed to a quarantine file. A message is generated informing the sender the message was rejected because of text context. (To view quarantined messages refer to the Viewing Quarantined Messages section of this chapter.)

6. Notification to the recipient is turned on and off by clicking on the Send Notification to Recipient Box.

7. A third party can be notified by entering an e-mail address in the Send Notification to: text box.

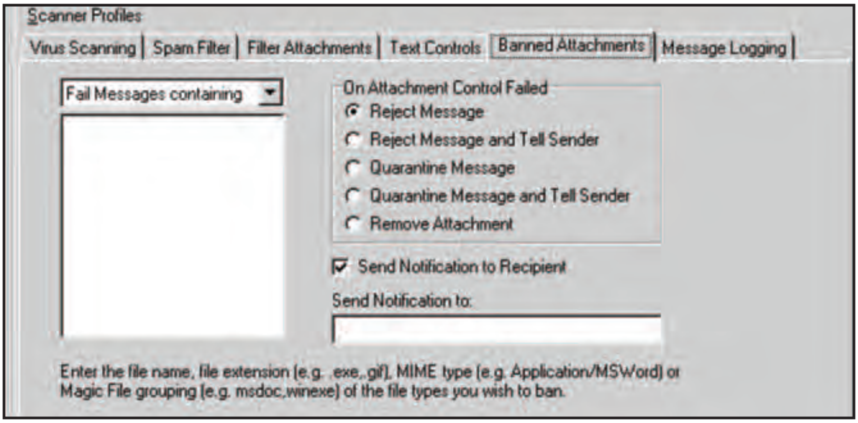
8. Click on the Save button to save any changes.

Content Control - Banned Attachments

1. Select Add Content Rule from the Message Control menu.

2. Enter a name for the Content Rule if it doesn't exist.

3. Click on the Banned Attachments tab.



Fail Messages containing

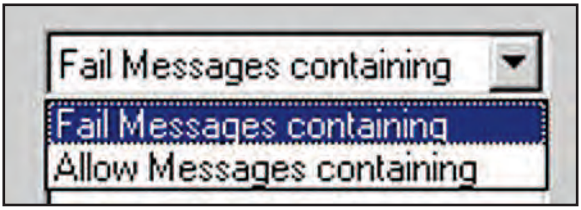
On Attachment Control Failed
● Reject Message
○ Reject Message and Tell Sender
○ Quarantine Message
○ Quarantine Message and Tell Sender
○ Remove Attachment

☑ Send Notification to Recipient

Send Notification to:

Enter the file name, file extension (e.g. .exe,.gif), MIME type (e.g. Application/MSWord) or Magic File grouping (e.g. msdoc,winexe) of the file types you wish to ban.

4. The program allow two types of filtering from the pull down menu.



Default Setting - Fail Messages Containing

This option will reject messages containing the listed attachments.

Allow Messages Containing

This option will allow messages with the listed attachments. All other attachments will not be allowed.

5. Enter the type of files which are banned as attachments.

Banned Attachments Content Scanner Profile

Attachments to be identified as banned are specified by type of file. Each file type is designated by one of three means of identification, file extension, Multipurpose Internet Mail Extension (MIME) and Magic File Grouping .

For example to filter MS/Word documents:

By extension "doc" would be entered.

By MIME "application/msword" would be entered. Most mail programs display the MIME type for file attachments allowing identification of other file types.

By Magic File Group "msdoc" would be entered.

6. The program allows five action options if a banned attachment is detected.

Default Setting - Reject Message

The message is rejected and is not delivered. No notification is given to the sender.

Quarantine Message

The message is routed to a quarantine file. No notification is given to the sender. (To view quarantined messages refer to the Viewing Quarantined Messages section of this chapter.)

Quarantine Message and Tell Sender

The message is routed to a quarantine file. A message is generated informing the sender the message was rejected because a banned attachment was detected. (To view quarantined messages refer to the Viewing Quarantined Messages section of this chapter.)

Remove Attachment

The message is delivered but the attachment is removed. No notification is given to the sender.

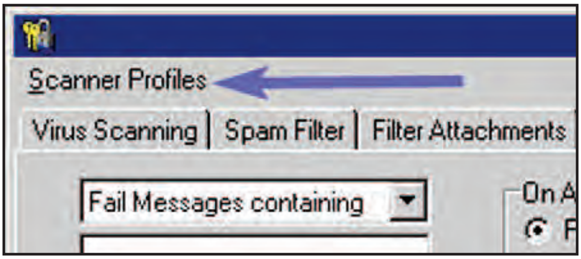
7. Notification to the recipient is turned on and off by clicking on the Send Notification to Recipient Box.

8. A third party can be notified by entering an e-mail address in the Send Notification to: text box.

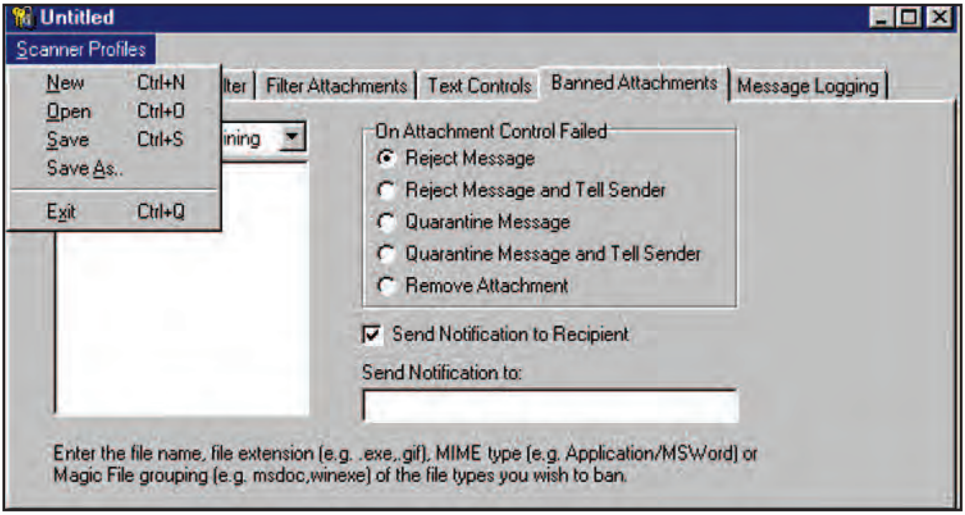
9. Click on the Save button to save any changes.

Making New Content Rules Effective

1. Click on the Scanner Profiles line immediately below the blue Untitled bar at the top of the screen.



2. Select Save As from the Scanner Profiles pulldown window.



On Attachment Control Failed

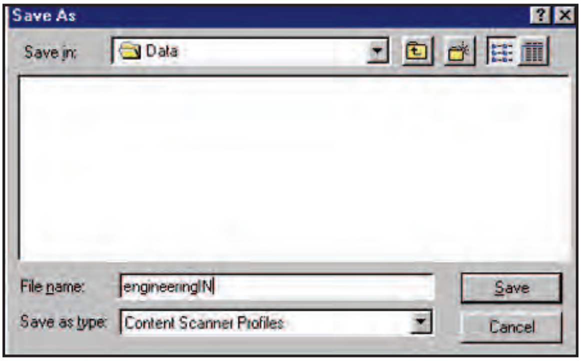
● Reject Message
○ Reject Message and Tell Sender
○ Quarantine Message
○ Quarantine Message and Tell Sender
○ Remove Attachment

☑ Send Notification to Recipient

Send Notification to:

Enter the file name, file extension (e.g. .exe,.gif), MIME type (e.g. Application/MSWord) or Magic File grouping (e.g. msdoc,winexe) of the file types you wish to ban.

3. Enter the inbound profile name associated with the new content rule. In this case the profile name may be 'engineeringIN'.

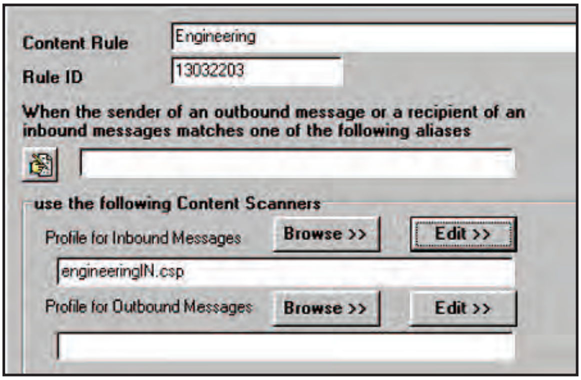


File name: engineeringIN

Save as type: Content Scanner Profiles

4. Click the Save button.

5. The Content Rule dialog screen reappears with the Profile Name for Inbound Messages shown in the space provided.



Content Rule: Engineering

Rule ID: 13032203

When the sender of an outbound message or a recipient of an inbound messages matches one of the following aliases

use the following Content Scanners

Profile for Inbound Messages: engineeringIN.csp

Profile for Outbound Messages:

Content Control - Message Logging

Message Logging

The Message Logging control is currently not provided in UbiQ*IDmail*.

Viewing the Quarantine File

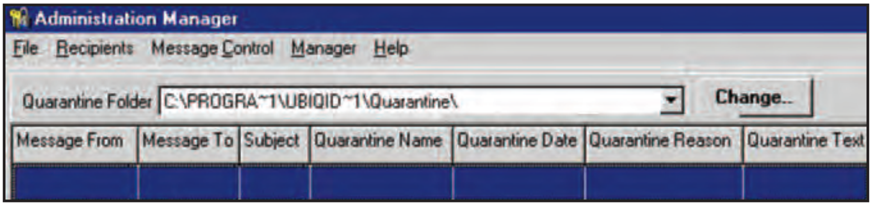
Quarantine File

The quarantine file consists of messages flagged by the content scanner. Reasons for quarantining a message are: a virus being detected, spam, specified text or banned attachments. The quarantine option must be selected in order to redirect messages to the quarantine file.

The quarantine file is only active with the UbiQ Fortress user software.

1. Select Quarantine Viewer from the Message Control menu.

2. The viewer will list the sender, recipient, message subject, type of quarantine, date quarantined, reason quarantined and the quarantined text.



Quarantine Folder C:\PROGRA~1\UBIQID~1\Quarantine\

Message From	Message To	Subject	Quarantine Name	Quarantine Date	Quarantine Reason	Quarantine Text

3. The viewer allows three action options.

View the Message

Clicking on the View button will bring up a window asking for a forwarding e-mail address. This will allow the user to view the entire message.

Warning

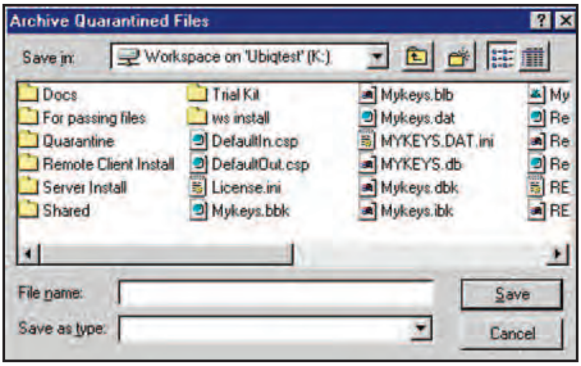
If a virus is detected it is not advisable to select the View option. The safest procedure is to delete the message.

Delete the Message

Clicking on the Delete button will erase the message.

Archive the Message

Clicking on the Archive button will bring up a window asking for a file location to save the message.



Archive Quarantined Files

Save in: Workspace on 'Ubiqtest' (K:)

UbiQIDmail®

Allowing a User to Download the User Database

6

This chapter covers how to allow users who travel the ability to download the system database to a portable computer.

In this chapter

- Authorizing a User to Download the User Database to a Portable Computer

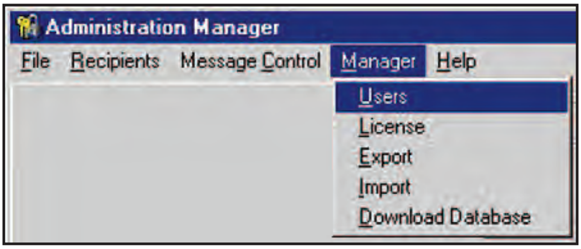
Users Who Don't Have Access to the User Database

In order to send encrypted messages, a user must have access to the recipient's public keys. Normally, a user accesses the database file located on a common network.

Some users, however, may not have access to the common network. For example, a person who travels as part of their job will not have access to the user database. To accommodate these situations, the UbiQ*IDmail* Administrative Manager allows the system administrator to authorize a user to download the database to a portable computer.

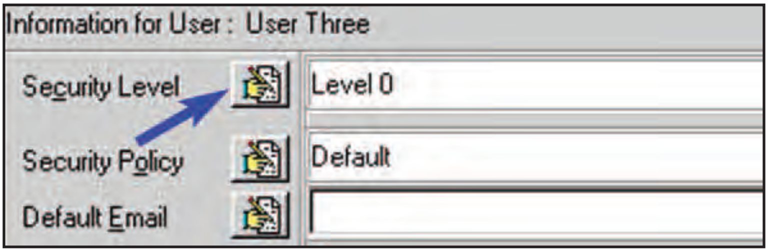
Authorizing a User to Download the User Database

1. Select Users from the Manager menu.



2. Highlight the user you wish to allow to download the database

3. Click on the Security Level Write icon.

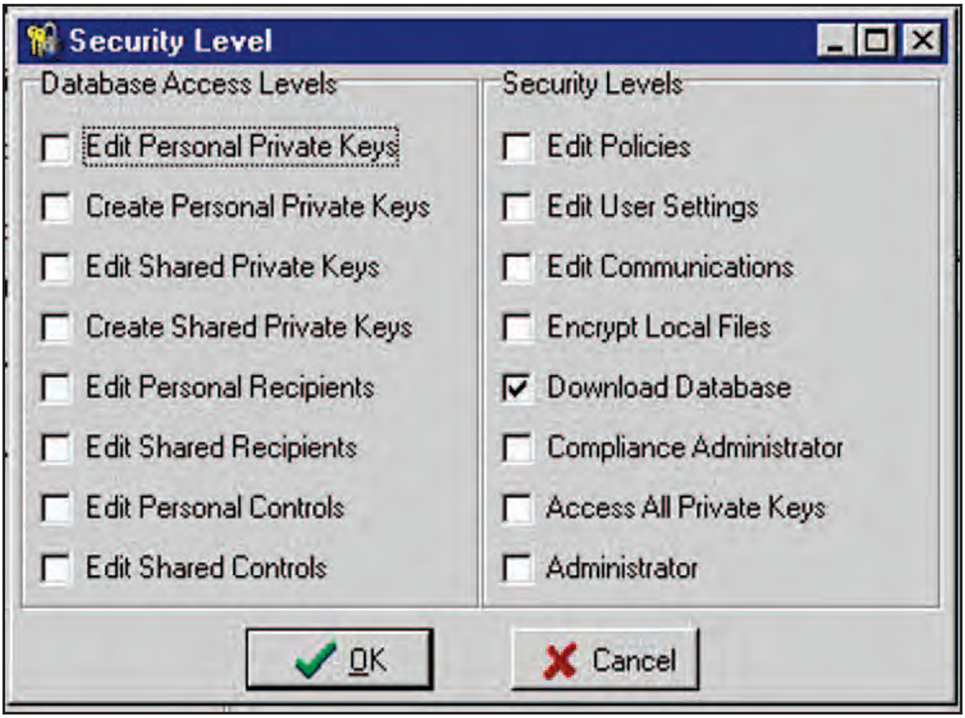

Information for User : User Three

Security Level: Level 0

Security Policy: Default

Default Email:

4. Click on the Download Database check box.



Security Level

Database Access Levels

☐ Edit Personal Private Keys

☐ Create Personal Private Keys

☐ Edit Shared Private Keys

☐ Create Shared Private Keys

☐ Edit Personal Recipients

☐ Edit Shared Recipients

☐ Edit Personal Controls

☐ Edit Shared Controls

Security Levels

☐ Edit Policies

☐ Edit User Settings

☐ Edit Communications

☐ Encrypt Local Files

☑ Download Database

☐ Compliance Administrator

☐ Access All Private Keys

☐ Administrator

5. Click on the OK button.

6. Click on the Update button.

Managing Databases in Multiple Facilities

7

This chapter cover how to synchronize user databases in two or more facilities.

In this chapter

Managing Databases in Multiple Facilities

This section covers situations where there are two or more UbiQ*IDmail* databases. The software allows the system administrator to export the primary database to remote enrollment servers and to synchronize the information in both databases allowing the consistent application of changes in security policy and updating new or deleted users.

This same export function is used to export that primary database to individual work stations that are remote form the primary enterprise facility.

The UbiQ*IDmail* system makes a distinction between two types of databases, primary and secondary.

Primary Database

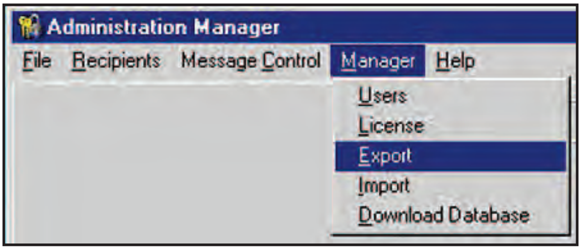
A primary database is the database which is modified when new users are added or deleted or when security policies are changed. If an enterprise has two facilities which issue user cards, both facilities would have a primary database.

Secondary Database

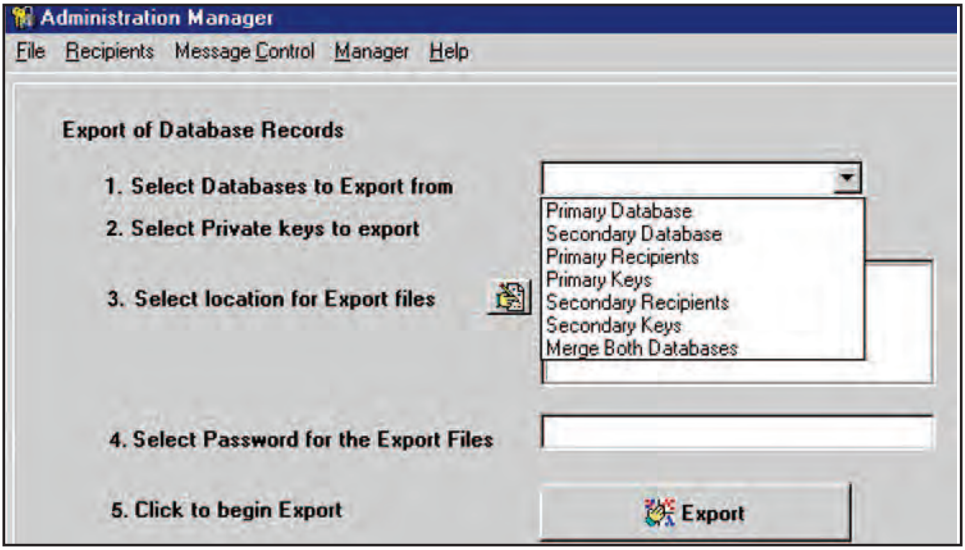
A UbiQ*IDmail* secondary database is only updated using the Import / Export functions. A secondary site might be a branch office or a regular business correspondent outside the enterprise.

Exporting a Primary Database

1. Select Export from the Manager menu.



2. Use the Select Databases to Export From pull down menu to select the Primary Database.



Export of Database Records

1. Select Databases to Export from
2. Select Private keys to export
3. Select location for Export files
4. Select Password for the Export Files
5. Click to begin Export

3. Select Private keys to export.

   - The default setting is All Private Keys.

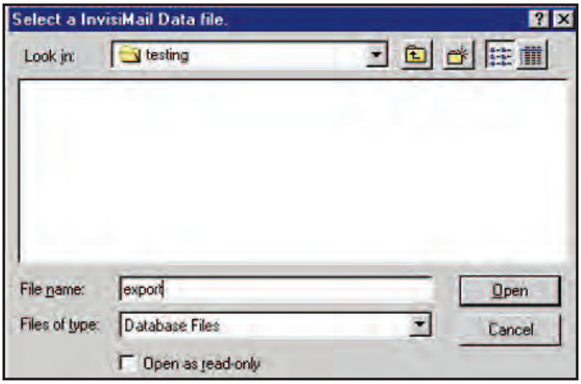
   - The optional setting is Private Keys for User Only. This exports only the private key of the an individual receiving the database.

Exporting the Private Keys

Each private key in the database is encrypted under a DES key. Private keys can only be recovered when the user's secret pass phase is combined with cryptograms on the user's badge card. This system ensures that only the specific user's private keys can be retrieved from the database. As a result, exporting the private keys does not represent a security risk.

4. Click on the Export Files Write icon.

5. Select a temporary file location for exported database.

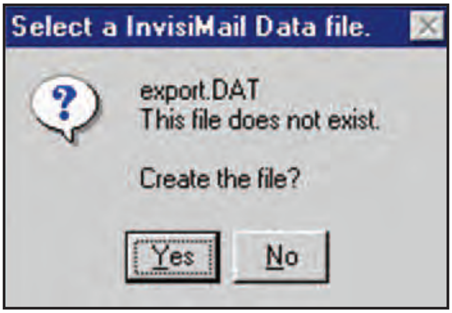


File name: export

Files of type: Database Files

6. Click on the Open button. This will create an export file.

   6.1 If a file does not exist, you will be prompted to create one.



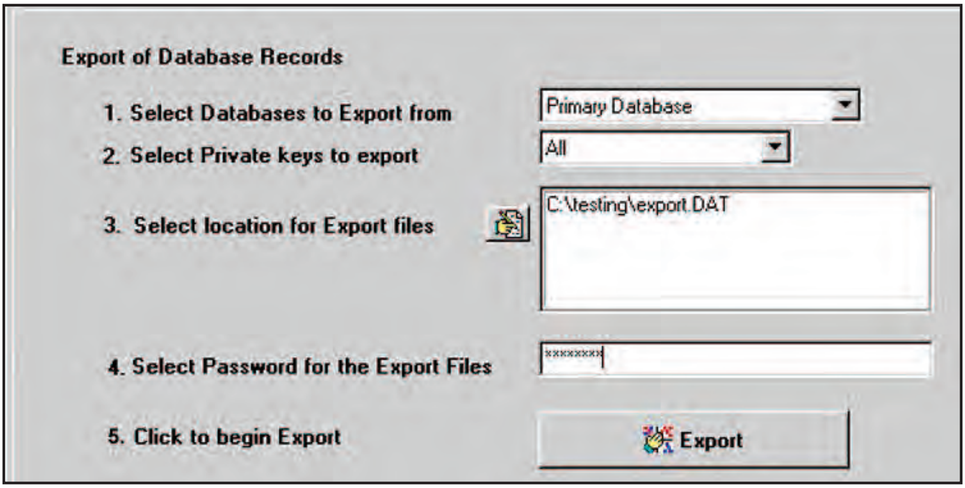
Select a InvisiMail Data file.

export.DAT
This file does not exist.

Create the file?

7. Enter the password for the export file.

   The password is used to derive an encryption key which will be used to encrypt the database.



Export of Database Records

1. Select Databases to Export from: Primary Database
2. Select Private keys to export: All
3. Select location for Export files: C:\testing\export.DAT
4. Select Password for the Export Files: ********
5. Click to begin Export

Important

This password should be established by the enterprise to facilitate the importing and exporting databases. Both the sender and receiver need to know the password. For additional security, an unique pass word (Minimum of 8 characters) can be used for each export / import of the database.

8. Click on the Export button. This will encrypt the selected database and place the encrypted result in the selected export file.

9. Send an e-mail message to the administrator of the remote facility and attach the export file created by the program.

   Alternately, the encrypted export file may be saved to a floppy disk or CD for physical transport to the remote site.

Importing a Primary Database to a Secondary Enterprise Site

Two separate scenarios exist for the import of a primary database to a remote location.

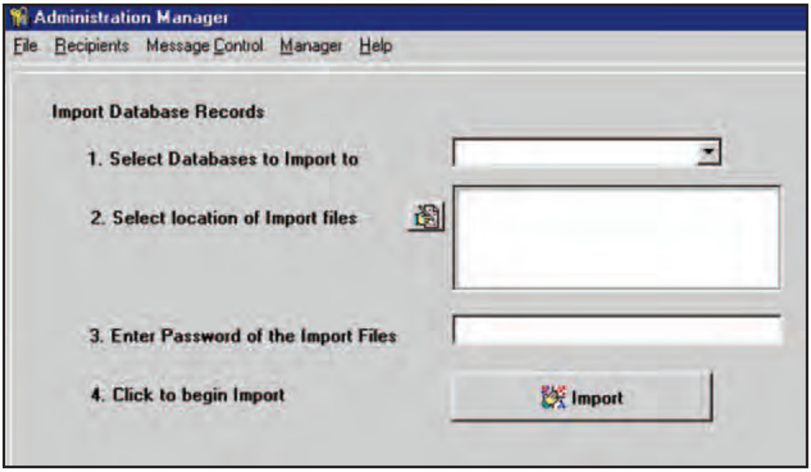
a. Another facility in the enterprise with its own enrollment server.

b. A remotely located client, either an enterprise employee or a frequent correspondent outside the enterprise.

This section addresses scenario a, above. Scenario b, import a primary database to a remote client is covered in the UbiQ*IDmail* Client User Guide.

1. Select Import from the Manager menu.

2. Use the Select Databases to Import pull down menu to select the Primary Database.

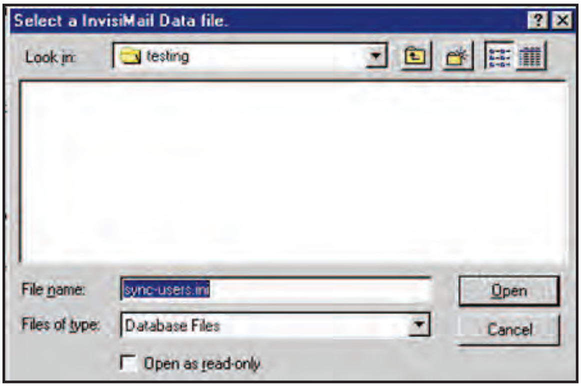


3. Identify the source of the input files. (Where the import files are stored)

   - A floppy disk or a CD
   - An attachment to an e-mail. The attachment must be saved as a separate file by you e-mail program.

4. Click on the write icon.

5. Select the location for the secondary database.

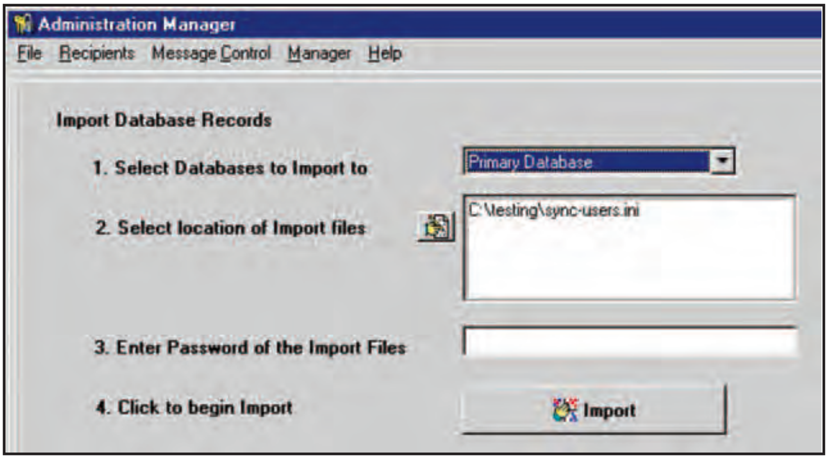


Look in: testing

File name: sync-users.ini

Files of type: Database Files

6. Enter the password for the import file.



Import Database Records

1. Select Databases to Import to: Primary Database

2. Select location of Import files: C:\testing\sync-users.ini

3. Enter Password of the Import Files

4. Click to begin Import

Important

This password should be established by the enterprise to facilitate the importing and exporting databases. Both the sender and receiver need to know the password.

7. Click on the Import button.

After the installation of the Ubiq*IDmail* Client and the importation of the client database, you are ready to communicate securely with any enrolled user in the enterprise.

Merging Two Primary Databases

Main Facility Administrator

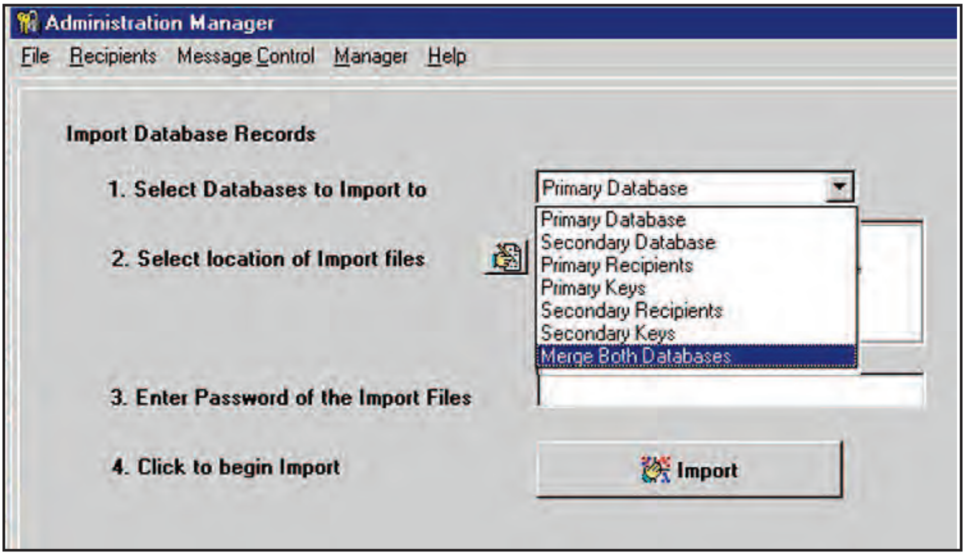
1. Export the main facility's primary database.

   - The exported database should include all private keys. (Refer to the Exporting the Primary Database section of this chapter.)

Remote Facility Administrator

2. Select Import from the Manager menu.

3. Use the pull down menu to select the Merge Databases.



Administration Manager

Import Database Records

1. Select Databases to Import to: Primary Database

2. Select location of Import files

3. Enter Password of the Import Files

4. Click to begin Import

4. Select All Private keys to import.

5. Click on the Import Files Write icon.

6. Select a temporary file location for the imported database.

7. Click on the Save button. This will create an import file.

8. Enter the password for the import file.

> **Important**
>
> This password should be established by the enterprise to facilitate the importing and exporting databases. Both the sender and receiver need to know the password.

9. Click on the Import button.

10. Send the merged database to the main facility.

    - The exported database should include all private keys. (Refer to the Exporting the Primary database section of this chapter.)

Main Facility Administrator

11. Import the merged primary database.

UbiQIDmail®

System Administration

8

It may be desirable for the Audit Manager to delegate system administration to other people in the enterprise.

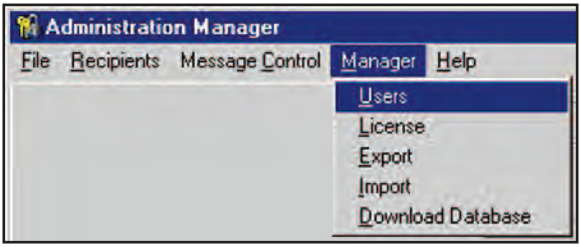
This chapter covers how to allow other users to gain access to various system administration tasks.

In this chapter

- Changing a User’s Security Settings
- Allowing a User Administrative Access to the System

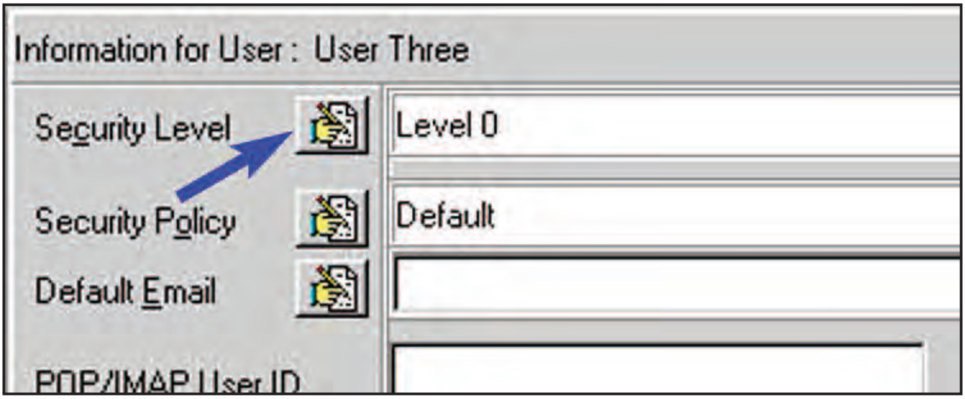
Changing a User's Security Level

1. Select Users from the Manager menu.



2. Highlight the user to be modified.

3. Click on the Security Level Write icon.


Information for User : User Three

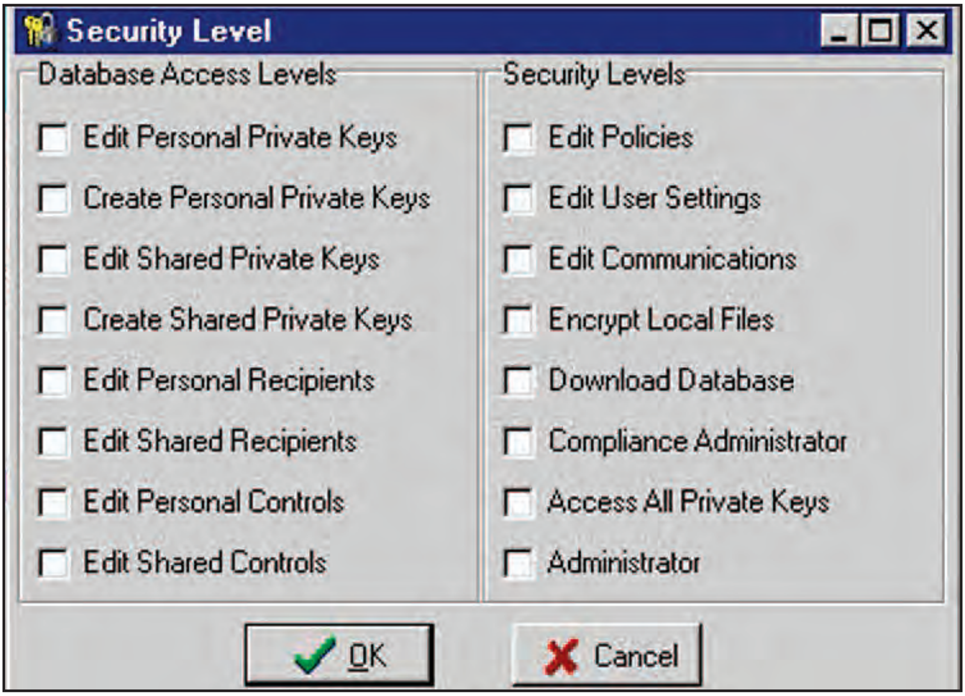
Security Level: Level 0

Security Policy: Default

Default Email:

POP/IMAP User ID:

4. A Security Level window will appear.



Security Level

Database Access Levels

□ Edit Personal Private Keys

□ Create Personal Private Keys

□ Edit Shared Private Keys

□ Create Shared Private Keys

□ Edit Personal Recipients

□ Edit Shared Recipients

□ Edit Personal Controls

□ Edit Shared Controls

Security Levels

□ Edit Policies

□ Edit User Settings

□ Edit Communications

□ Encrypt Local Files

□ Download Database

□ Compliance Administrator

□ Access All Private Keys

□ Administrator

Database Access Levels

The program does not allow the creation or editing of the private keys. This is done by the enrollment server. None of these check boxes will be checked for regular users.

Security Levels

The program allows the audit manger to delegate administrative access to the system. The most common privileges are:

Edit Policies - Allows the delegated user to create or modify security policies.
Edit User Setting - Allows the delegated user to modify the settings for individual users.
Edit Communications - Allows the delegated user access to the Diagnostic Manager on the Client Tray.
Download Database - Allows the delegated user to download the user database to a portable computer.

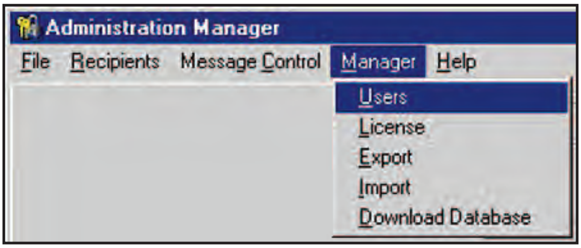
5. Click on the Update button.

Changing a User's Security Policy

Default Security Policy

When a user is enrolled into the system he or she is automatically assigned the default security policy. No other action is required unless the system administrator wishes to assign the user an alternate policy.

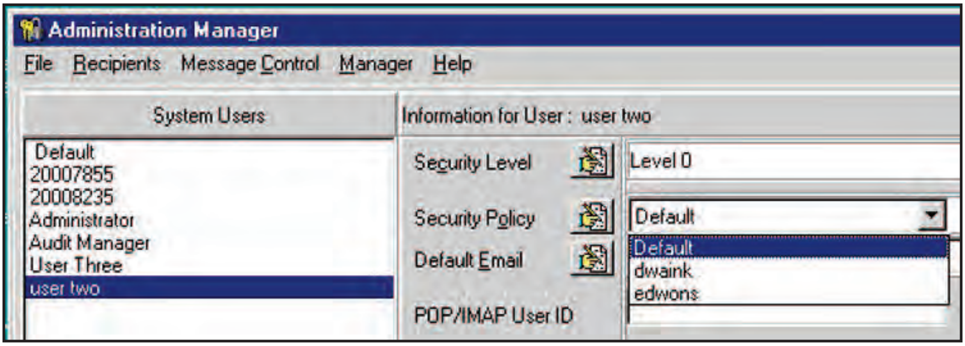
1. Select Users from the Manager menu.



2. Highlight the user to be modified.

3. Click on the Security Policy Write icon.

4. Use the popup box to select the desired security policy.



System Users

- Default
- 20007855
- 20008235
- Administrator
- Audit Manager
- User Three
- user two

Information for User : user two

Security Level: Level 0

Security Policy: Default

- Default
- dwaink
- edwons

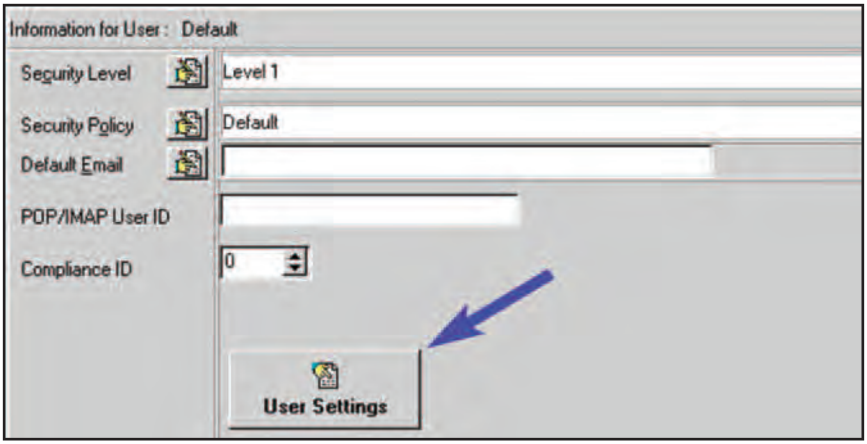
Default Email

POP/IMAP User ID

4. Click on the Update button.

User Setting Defaults

The user setting defaults are accessed by highlighting Default under System Users. The user settings defaults are accessed by clicking on the User Settings button.



Information for User : Default

Security Level: Level 1

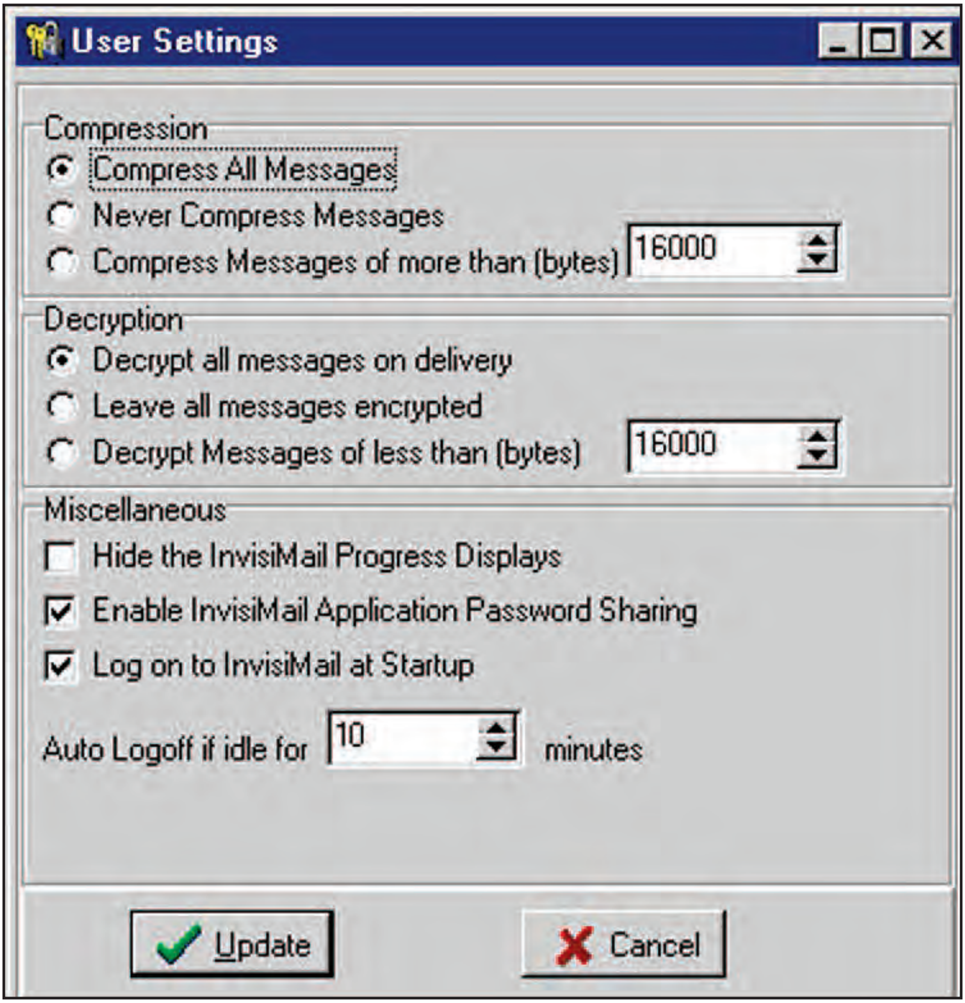
Security Policy: Default

Default Email

POP/IMAP User ID

Compliance ID: 0

User Settings



User Settings

Compression

● Compress All Messages

○ Never Compress Messages

○ Compress Messages of more than (bytes) 16000

Decryption

● Decrypt all messages on delivery

○ Leave all messages encrypted

○ Decrypt Messages of less than (bytes) 16000

Miscellaneous

□ Hide the InvisiMail Progress Displays

☑ Enable InvisiMail Application Password Sharing

☑ Log on to InvisiMail at Startup

Auto Logoff if idle for 10 minutes

Compression

This option determines under what conditions messages will be compressed. The default setting is Compress All Messages.

Decryption

This option determines when messages are decrypted. The default setting decrypts messages when the user inserts his or her card and enters the correct pass phrase.

Miscellaneous

These options control the operation of the client software. The hide mail progress displays is normally off. Password sharing and log on at startup are on.

The auto log off is typically set to 10 minutes. If the system has not been used for the specified period the user must reenter his or her pass phrase.

Glossary

Administration Manager Utility
A utility of the UbiQ*IDmail* system that allows the audit manger access to the enterprise's UbiQ*IDmail* security settings.

Attachment
A file or files that are separate from the text of the e-mail message.

Audit Manager
The senior person in the enterprise with responsibility for physical and information security.

Audit Manager's Card
Used in conjunction with the audit manager's pass phrase to personalize the security officer's card and to change the security parameters of the UbiQ*IDmail* system.

Badge Card Reader
A card reader used to enroll new client users on the enrollment server. It is also used on client station to allow users to access encrypted messages.

Client User Database
A file on a shared network drive containing the client users' public keys.

Client User
A person enrolled in the UbiQ*IDmail* system.

Content Scanning
A feature of the UbiQ*IDmail* system that filters messages for viruses, Spam, specific content and attachments. Content Scanning is active only for users using the Fortress software.

Crypto Card Reader
A card reader used on the enrollment server for the audit manager or security officer's card.

Digital Certificate
An authentication generated with a new card is issued.

Digital Signature
A feature of the UbiQ*IDmail* system that verifies the identity of the sender.

E-mail Address
The e-mail address of the users. (johnnyappleseed@apple.com)

Enrollment Server
A computer with access to an enterprise's network, a crypto card and badge card reader and the UbiQ*IDmail* software.

Enterprise
The company the purchased UbiQ*IDmail*.

Message Blocking
A feature of the UbiQ*IDmail* system that allows the enterprise to block incoming and / or outgoing messages to specific e-mail addresses.

Message Control Policy
The UbiQ*IDmail* security policy that controls incoming and outgoing messages, new recipients, key handling, warning text options, and access to IP addresses. The system options for the message control policy are access by the audit manger using the Administration Manger Utility.

Pass Phrase
A series of charters used with a smart card to gain access to the UbiQ*IDmail* system. The pass phrase for the audit manager and security officer is between 8 and 20 characters. The pass phrase for client users is between 8 and 40 characters.

Private Key
A cryptographic algorithm used to decrypt messages. The private key is a combination of the smart card and the user's pass phrase.

Public Key
A cryptographic algorithm used to encrypt a message to a specific client user.

Security Officer
One or more people in the enterprise with responsibility of the UbiQ*IDmail* system. The security officer manages the day-to-day operation of the UbiQ*IDmail* system.

Security Officer's Card
Used in conjunction with the security officer's pass phrase to enroll new client users.

User Name
Identifies the user's first and last name. Each user must have a unique user name.

User Profile
Determines the security settings for the user.