



Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Email Resources

For Unified Contact Center Enterprise and Hosted and Unified ICM

Release 4.3(1)
September 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Email Resources: For Unified Contact Center Enterprise and Hosted and Unified ICM
© 2009 Cisco Systems, Inc. All rights reserved.

Contents

- Preface5**
 - About This Guide 6
 - Document Conventions..... 6
 - Acronyms and Initialisms 6
 - Other Learning Resources..... 7
 - Online Help 7
 - Document Set 7

- Chapter 1: Email Basics9**
 - Key Terms and Concepts 10
 - Important Tasks on the Mail Server 11
 - Services for Emails 11
 - Settings for Emails 12
 - Settings for Blocked Addresses..... 12
 - Settings for Blocked Attachments..... 12
 - Settings for Delivery Exceptions..... 12
 - Elements of the User Interface 13

- Chapter 2: Aliases14**
 - About Aliases 15
 - Creating Aliases 15
 - Deleting Aliases 17
 - Changing the Status of Aliases 18

- Chapter 3: Blocked Addresses.....19**
 - About Blocked Addresses..... 20
 - Configuring Blocked Addresses 20
 - Deleting Blocked Addresses 21

Chapter 4: Blocked File Extensions	22
About Blocked File Extensions.	23
Configuring Blocked File Extensions.	23
Deleting Blocked File Extensions.	24
Blocking Attachments.	24
Blocking Specific Types of Attachments for Inbound Emails	24
Blocking Specific Types of Attachments for Inbound and Outbound Emails	24
Blocking All Types of Attachments for Inbound Emails	25
Blocking All Types of Attachments for Inbound and Outbound Emails	25
Viewing Blocked Attachments	25
Restoring Blocked Attachments	25
Deleting Blocked Attachments	26
 Chapter 5: Delivery Exceptions.....	 27
About Delivery Exceptions.	28
Configuring Delivery Exceptions	28
Deleting Delivery Exceptions	29
 Appendix: Predefined Delivery Exceptions	 30
Phrases Checked in Email Addresses	30
Phrases Checked in the Subject of Emails	31

Preface

- ▶ [About This Guide](#)
- ▶ [Document Conventions](#)
- ▶ [Acronyms and Initialisms](#)
- ▶ [Other Learning Resources](#)

Welcome to Cisco® Interaction Manager™, multichannel interaction software used by businesses all over the world to build and sustain customer relationships. A unified suite of the industry's best applications for web and email interaction management, it is the backbone of many innovative contact center and customer service helpdesk organizations.

Cisco Interaction Manager includes a common platform and one or both of the following applications:

- ▶ Cisco Unified Web Interaction Manager (Unified WIM)
- ▶ Cisco Unified E-Mail Interaction Manager (Unified EIM)

About This Guide

Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Email Resources introduces you to the email infrastructure within the application. It includes instructions on how to set up aliases, block unwanted emails and files from entering the system, and handle delivery exceptions.

Document Conventions

This guide uses the following typographical conventions.

Convention	Indicates
<i>Italic</i>	Emphasis. Or the title of a published document.
Bold	Labels of items on the user interface, such as buttons, boxes, and lists. Or text that must be typed by the user.
Monospace	The name of a file or folder, a database table column or value, or a command.
<i>Variable</i>	User-specific text; varies from one user or installation to another.

Document conventions

Acronyms and Initialisms

The following acronyms and initialisms are used in this document.

- ▶ ACD: Automatic Call Distributor
- ▶ ARM: Agent Reporting and Management
- ▶ CSA: Cisco Security Agent
- ▶ CTI: Computer Telephony Integration
- ▶ EAAS: External Agent Assignment Service


- ▶ ICM: Intelligent Contact Manager
- ▶ IPCC: Internet Protocol Contact Center
- ▶ IPTA: ICM-picks-the-agent
- ▶ JDBC: Java Database Connectivity
- ▶ MR: Media Routing
- ▶ MRD: Media Routing Domain
- ▶ ODBC: Open Database Connectivity
- ▶ PG: Peripheral Gateway
- ▶ PIM: Peripheral Interface Manager
- ▶ SNMP: Standard Network Management Protocol
- ▶ UI: User Interface

Other Learning Resources

Various learning tools are available within the product, as well as on the product CD and our web site. You can also request formal end-user or technical training.

Online Help

The product includes topic-based as well as context-sensitive help.

Use	To view
 Help button	Topics in <i>Cisco Unified Web and E-Mail Interaction Manager Help</i> ; the Help button appears in the console toolbar on every screen.
F1 keypad button	Context-sensitive information about the item selected on the screen.

Online help options

Document Set

The Cisco Unified Web and E-Mail Interaction Manager documentation is available in the `Documents` folder on the product CD. The latest versions of all Cisco documentation can be found online at <http://www.cisco.com>

- ▶ All Unified EIM documentation can be found online at http://www.cisco.com/en/US/products/ps7236/tsd_products_support_series_home.html
- ▶ All Unified WIM documentation can be found online at http://www.cisco.com/en/US/products/ps7233/tsd_products_support_series_home.html
- ▶ In particular, Release Notes for these products can be found at http://www.cisco.com/en/US/products/ps7236/prod_release_notes_list.html

- ▶ For general access to Cisco Voice and Unified Communications documentation, go to http://www.cisco.com/en/US/products/sw/voicesw/tsd_products_support_category_home.html

The document set contains the following guides:

- ▶ *Hardware and System Software Specification for Cisco Unified Web and E-Mail Interaction Manager*
- ▶ *Cisco Unified Web and E-Mail Interaction Manager Installation Guide*
- ▶ *Cisco Unified Web and E-Mail Interaction Manager Browser Settings Guide*

User guides for agents and supervisors

- ▶ *Cisco Unified Web and E-Mail Interaction Manager Agent's Guide*
- ▶ *Cisco Unified Web and E-Mail Interaction Manager Supervisor's Guide*

User guides for Knowledge Base managers and authors

- ▶ *Cisco Unified Web and E-Mail Interaction Manager Knowledge Base Author's Guide*

User guides for administrators

- ▶ *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Administration Console*
- ▶ *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Routing and Workflows*
- ▶ *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Chat and Collaboration Resources*
- ▶ *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Email Resources*
- ▶ *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Data Adapters*
- ▶ *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Reports Console*
- ▶ *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to System Console*
- ▶ *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Tools Console*

1

Email Basics

- ▶ [Key Terms and Concepts](#)
- ▶ [Important Tasks on the Mail Server](#)
- ▶ [Services for Emails](#)
- ▶ [Settings for Emails](#)
- ▶ [Elements of the User Interface](#)

This chapter introduces the basics of using the Administration Console to set up email resources. It defines key terms and concepts, and outlines the tasks that have to be completed on the mail server before email resources can be configured. It also lists the services and settings that are required for processing emails through the system.

Key Terms and Concepts

- ▶ **Aliases:** Aliases are mapped to email addresses that customers use to contact your company—for example, support@yourcompany.com or sales@yourcompany.com. They function as entry and exit points for emails processed by the system. Administrators configure aliases in the Administration Console. Once an alias is configured and made active, the Retriever Service retrieves emails from the mail server on which the email address is configured. For more details, see [“Aliases” on page 14](#).

- ▶ **Blocked addresses:** Administrators can block emails from certain email addresses or domains from being processed by the system by creating a list of blocked addresses and domains. Any email from a blocked address or domain is treated as spam and directly deleted, stored in a separate file, or redirected to another address.

This feature should supplement any spam or security software that may be running on your corporate email server. For more details, see [“Blocked Addresses” on page 19](#).

- ▶ **Blocked file extensions:** This is a security feature that allows you to selectively prevent certain types of attachments, which may contain viruses, from entering the system. For example, files with extensions like .exe, .vbs, .js, etc.

This feature works in conjunction with department settings for email attachments. Using settings, the system can be configured to block all attachments, block incoming and outgoing attachments, and delete or quarantine blocked attachments. For more information, see [“Blocked File Extensions” on page 22](#).

- ▶ **Delivery exceptions:** This feature allows you to handle emails that bounce back to the system. Administrators can create a list of words and phrases that may appear in the email subjects and email addresses of incoming emails. If any of these words or phrases are found in the subject or email address of emails, they are treated as bounce backs, permanent or temporary. A permanent bounceback indicates that an irreparable reason (such as invalid email address) caused the email to bounce back. A temporary bounceback indicates that a temporary reason (such as out of office reply, destination server down, etc.) caused the email to bounce back. For more details, see [“Delivery Exceptions” on page 27](#).

The application includes 144 common delivery exception scenarios. Other exceptions can be created as needed. The predefined exception scenarios are listed in [“Appendix: Predefined Delivery Exceptions” on page 30](#).

Important Tasks on the Mail Server

Before you start configuring aliases, make sure that the following objects have been configured and are ready to be used.

- ▶ An email address with credentials on the company mail server.

Along with the email address, make sure you have the following details. You would need this information to configure the alias from the Administration Console.

For the incoming email server:

- The server type, either POP3 (Post Office Protocol 3) or IMAP4 (Internet Message Access Protocol).
- The server name or IP (Internet Protocol) address.
- A user name and password for the server.

For the outgoing email server:

- The server type, either SMTP (Simple Mail Transfer Protocol) or ESMTP (Extended Simple Mail Transfer Protocol).
- The outgoing server name or IP address.
- A user name and password for the outgoing server (only if using ESMTP).

Refer to your IT department's policies and decide whether or not to use SMTP if ESMTP authentication fails.

Services for Emails

Make sure the following services in the System Console are configured properly and are running. For details on setting up these services, see *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to System Console*.

- ▶ Retriever service (For standalone and integrated emails)
- ▶ Dispatcher service (For standalone and integrated emails)
- ▶ Listener service (For integrated emails only)
- ▶ External Agent Assignment Service (EAAS) (For integrated emails only)

Settings for Emails

Make sure that the following partition and department level settings are configured properly. For more information about these settings, see *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Administrator's Console*.

Settings for Blocked Addresses

These settings are available at the partition level.

- ▶ Action on spam mails
- ▶ Spam mail maximum file size (megabyte)
- ▶ Spam mail redirection SMTP preference
- ▶ Spam mail redirection from address
- ▶ Spam mail redirection to address
- ▶ Spam mails SMTP server
- ▶ Spam mails SMTP protocol
- ▶ Spam mails SMTP user name
- ▶ Spam mails SMTP password
- ▶ Spam mails auto bcc

Settings for Blocked Attachments

These settings are available at the department level.

- ▶ Block all attachments
- ▶ Action on blocked attachments
- ▶ Email for scan

Settings for Delivery Exceptions

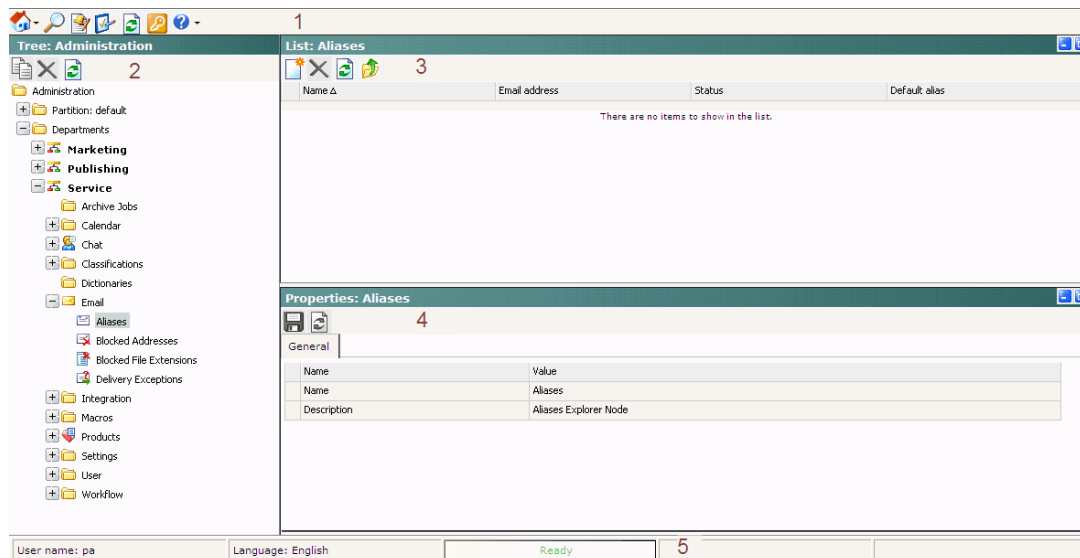
These settings are available at the partition level.

- ▶ Action on exception mails
- ▶ Exception mail maximum file size (megabyte)
- ▶ Exception mail redirection SMTP preference
- ▶ Exception mail redirection from address
- ▶ Exception mail redirection to address
- ▶ Exception mails SMTP server
- ▶ Exception mails SMTP protocol

- ▶ Exception mails SMTP user name
- ▶ Exception mails SMTP password
- ▶ Exception mails auto bcc

Elements of the User Interface

The Administration Console user interface can be divided into five functional areas.



Elements of the Administration Console user interface

1. **Console toolbar:** The main toolbar of the console appears at the top of the screen. Each button on this toolbar allows you to perform a specific function. Some of these are: navigate to other consoles, send and receive internal messages, log out of the system, and access the online help for the Administration Console.
2. **Tree pane:** The Tree pane lists all the business objects in the application, allowing you to select the node (folder) that you wish to work in. When you select a folder, its first-level contents are displayed in the List pane. To expand all first and second level nodes with a single click, press SHIFT and click the plus [+] button next to the topmost node. The contents of all first and second level nodes are displayed in the Tree pane.
3. **List pane:** The List pane displays first-level contents of the folder selected in the Tree pane. You can view the name, description, date of creation, etc., of the displayed items. In this pane, you can create items, or select existing ones, to modify or delete.
4. **Properties pane:** The Properties pane displays the contents of the business object selected in the List pane. In this pane, you can edit the properties of the selected item.
5. **Status bar:** The status bar is present at the bottom of every screen. It displays the following information:
 - The user name with which the user has logged in the system.
 - The language currently in use.
 - The status of the system (Loading, Ready, etcetera).

2

Aliases

- ▶ [About Aliases](#)
- ▶ [Creating Aliases](#)
- ▶ [Deleting Aliases](#)
- ▶ [Changing the Status of Aliases](#)

This chapter will assist you to set up aliases.

About Aliases


Aliases are business objects in the application that map to email addresses that customers use to contact your company. They function as entry and exit points for emails processed by the system, and are configured almost like an email client. Design your aliases in such a way that they become the first step in meaningfully separating the different types of inquiries received by your company. For example, a bank may decide to create separate email addresses for inquiries about the different kinds of services they provide, such as accounts, home loans, car loans, mutual funds, etc. This bank would create the following email addresses, and corresponding aliases: accounts@yourbank.com, loans@yourbank.com, mfunds@yourbank.com and so on.

Once an alias is configured, the Retriever Service is set up to retrieve emails that arrive at the email server, and bring them into the system. Workflows then act on them to create activities, send auto-responses, set service levels and route activities to queues and agents. For more information about workflows and routing, refer to the *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Routing and Workflows*.

Creating Aliases

Before you create an alias, verify that the corresponding email address has been created on the email server. You will require the server type, server name, and user name and password for the email account, while creating the alias.

To create an alias:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Aliases**.
2. In the List pane toolbar, click the **New**  button.
3. In the Properties pane, go to the General tab and provide the following details.
 - **Name:** Type the name of the alias. This is required information.
 - **Description:** Type a brief description of the alias.
 - **Email address:** Type the email address for the alias. This is required information. The email address you provide here should be first created on the incoming email server.
 - **Status:** Select the status of the alias. By default the status of an alias is set as active. For more details, see [“Changing the Status of Aliases” on page 18](#).
 - **Automatic BCC:** Type the email address to which you want to send a BCC copy of all emails that go out from this alias. You can provide multiple addresses separated by semicolons. Whenever an email is sent out from this alias, a BCC copy of that email is automatically sent to this address.
 - **Send mail to:** Use this field to specify an email address to which all outgoing emails from this alias should be sent. If a value is entered in this field, no outgoing email from this alias will reach its original intended recipient. When an agent replies to a customer email, the reply is sent to the email address specified in this field, and not to the customer's email address. Enter values in this field only while testing the system. Make sure that after testing the alias, you clear the values in this field.



Important: If you provide email addresses in both the Automatic BCC and Send mail to fields, the email is sent only to the address given in the Send mail to field.

- **Default alias:** Select **Yes** to make this alias the default alias for the department. This field can be edited only after the alias is saved. When an agent composes a new email, the default alias is selected as the **From** address for the email.



Important: The default alias should be an active alias. For each department only one alias can be set as the default alias.

Name	Value
Name *	Customer support
Description	
Email address *	Customersupport@yourcompany.com
Status *	Active
Automatic BCC	
Send mail to	
Default alias *	No

Set the general properties

- In the Properties pane, go to the Servers tab and provide the details of the incoming and outgoing servers to be used for the alias.
 - In the Incoming section, provide the following details. All the fields are required.
 - **Server type:** Select the server type you want to use. By default **POP3** is selected. The options available are **POP3** and **IMAP**.
 - **Server name:** Type the name of the server.
 - **User name:** Type the user name of the email account.
 - **Password:** Type the password of the email account.
 - **Verify password:** Verify the password.

	Name	Value
Incoming	Server type	POP3
Outgoing	Server name *	Server name
	User name *	jdoe
	Password *	*****
	Verify password *	*****

Configure the incoming server for the alias

- Next, in the Outgoing section, provide the following details.
 - **Server type:** Select the server type you want to use. By default **SMTP** is selected. The options available are **SMTP** and **ESMTP**.

- **Use SMTP:** If your server type is ESMTP, then you can optionally use the SMTP server when the ESMTP server authentication fails. Select **Never** if you do not want to use the SMTP server. The options available are **Never** and **When authorization fails**. This field is enabled only if the server type is set as ESMTP in the **Server type** field.
- **Server name:** Type the name of the server.

The following three options are enabled only if the server type is set as ESMTP.

- **User name (ESMTP):** Type the user name.
- **Password:** Type the password.
- **Verify password:** Verify the password.

Name	Value
Server type	SMTP
Use SMTP	<Select>
Server name *	Server Name
User name (ESMTP) *	
Password *	
Verify password *	

Configure the outgoing server for the alias

5. Click the **Save**  button.

After creating an alias, add the new alias to a retriever service instance in the System Console. Then, restart the retriever service instance and restart all dispatcher instances. Now, use the alias in an inbound workflow. For more details on workflows, see *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Routing and Workflows*.

Deleting Aliases

Messages sent to a deleted alias are not received by the system even if the email address to which it maps continues to exist on the mail server.

You cannot delete an alias, if:

- ▶ It is configured as the default alias.
- ▶ It is associated with a retriever service instance.
- ▶ It is used in an inbound workflow.


If any replies are sent out from a deleted alias, they go out using the default SMTP preferences. For this, make sure you have set the following six default SMTP settings at the partition level. For more information about working with settings, see the Settings chapter in the *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Administration Console*.

- ▶ Default SMTP Server
- ▶ Default SMTP protocol
- ▶ Default SMTP Port

- ▶ SMTP Flag
- ▶ Default SMTP user name
- ▶ Default SMTP password

If these settings are not configured, replies from deleted aliases are not sent out to customers.

To delete an alias:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Aliases**.
2. In the List pane, select the alias you want to delete.
3. In the List pane toolbar, click the **Delete**  button.
4. A message appears asking to confirm the deletion. Click **Yes** to delete the alias.

When you delete an alias, the Retriever Service and Dispatcher Service instances associated with that alias need to be restarted for the changes to take effect.

Changing the Status of Aliases

Administrators can change the status of an alias from the Administration Console. The system can also automatically set an alias to be active or inactive. The retriever tries to connect to an alias three times, and after the third failed attempt, it makes the alias inactive.


For the following two conditions, the retriever makes an alias inactive and then tries to connect to the alias after ten minutes. If it is able to connect, the retriever makes the alias active again and starts retrieving emails.

- ▶ POP3 server is not available because of a problem with the network, or if the server appears to be stopped.
- ▶ A user is logged in to the mailbox through telnet or through another external email client.

For the following two conditions, the retriever makes the alias inactive and does not try to connect again. The administrator has to manually fix the problem, and make the alias active from the Administration Console.

- ▶ POP3 or IMAP service is not started on the POP3 or IMAP servers.
- ▶ The authentication details provided for the alias are incorrect.

To change the status of an alias:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Aliases**.
2. In the List pane, select an alias.
3. In the Properties pane, go to the General tab and change the status of the alias. The options available are:
 - **Active:** If set to active, the retriever retrieves incoming emails from this alias and the dispatcher dispatches outgoing emails from the alias. By default the status of an alias is set as active.
 - **Inactive:** If you make an alias inactive, the retriever does not retrieve incoming emails from this alias, but the dispatcher dispatches outgoing emails from the alias.
4. Click the **Save**  button.

3 Blocked Addresses

- ▶ [About Blocked Addresses](#)
- ▶ [Configuring Blocked Addresses](#)
- ▶ [Deleting Blocked Addresses](#)

This chapter will assist you in understanding how to set up blocked addresses to prevent emails from specific email addresses and domains from being processed by the system.

About Blocked Addresses


Administrators may wish to block emails from certain email addresses or domains from being processed by the system. This is done by creating a list of blocked addresses and domains. Any incoming email from a blocked address or domain is treated as spam and directly deleted, stored in a separate file, or redirected to another address.

When the retriever retrieves emails for processing, it checks if the From address of the emails matches addresses or domains specified in the blocked addresses list. If a match is found, the email is blocked and the action specified in the Action on spam emails setting is performed. For an email to be blocked, there must be an exact match between the email address and the address specified in the blocked addresses list. For example, if you have blocked the domain address “yahoo.com”, an email from “john@yahoo.com” is blocked, but emails from “john@yahoo.co.uk” are not. Blocked addresses are used only for incoming emails. Outgoing emails are not blocked based on the items in the blocked address list.

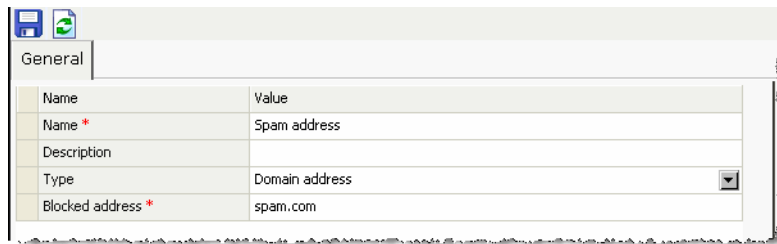
This feature should supplement any spam or security software that is running on your corporate email server. If spam is a major issue or concern, corporate email filtering software is recommended as a more permanent solution.

Configuring Blocked Addresses

To configure a blocked addresses:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Blocked Addresses**.
2. In the List pane toolbar, click the **New**  button.
3. In the Properties pane, on the General tab, provide the following details.
 - **Name:** Type the name for the blocked address.
 - **Description:** Type a brief description.
 - **Type:** Select the type of address you want to block. The options available are:
 - Email address
 - Domain address

- **Blocked address:** Specify the address you want to block. For example, `spam@spam.com` for an email address and `spam.com` for a domain address.



Name	Value
Name *	Spam address
Description	
Type	Domain address
Blocked address *	spam.com


Set the general properties

4. Click the **Save**  button.

When you configure a blocked address, the Retriever Service instances need to be restarted for the changes to take effect.

Deleting Blocked Addresses

To delete a blocked address:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Blocked Addresses**.
2. In the List pane, select the blocked address you want to delete.
3. In the List pane toolbar, click the **Delete**  button.
4. A message appears asking to confirm the deletion. Click **Yes** to delete the blocked address.

When you delete a blocked address, the Retriever Service instances need to be restarted for the changes to take effect.



Blocked File Extensions

- ▶ [About Blocked File Extensions](#)
- ▶ [Configuring Blocked File Extensions](#)
- ▶ [Deleting Blocked File Extensions](#)
- ▶ [Blocking Attachments](#)
- ▶ [Viewing Blocked Attachments](#)
- ▶ [Restoring Blocked Attachments](#)
- ▶ [Deleting Blocked Attachments](#)

This chapter will assist you in understanding how to block specific file types from being processed by the system.

About Blocked File Extensions

This is a security feature that allows you to selectively block certain types of attachments, which may contain viruses, from entering the system. (For example, `.exe`, `.vbs`, `.js`, etc.) This feature works in conjunction with department settings for email attachments. Using settings, the system can be configured to block all attachments, block incoming and outgoing attachments, and delete or quarantine blocked attachments.


Along with setting the file extensions for blocking, you need to configure the following three department settings for this feature to work.

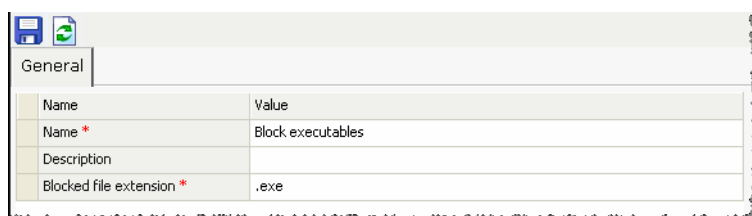
- ▶ Email for scan
- ▶ Block all attachments
- ▶ Action on blocked attachments

For more information on working with settings, see the Settings chapter in the *Cisco Unified Web and E-Mail Interaction Manager Administrator's Guide to Administration Console*.

Configuring Blocked File Extensions

To configure a blocked file extension:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Blocked File Extensions**.
2. In the List pane toolbar, click the **New**  button.
3. In the Properties pane, on the General tab, provide the following details.
 - **Name:** Type a name for the blocked file extension.
 - **Description:** Type a brief description.
 - **Blocked file extension:** Type the file extension you want to block such as `.exe`, `.vbs`, `.js`.




Set the general properties

4. Click the **Save**  button.

When you configure a blocked file extension, the Retriever Service instances need to be restarted for the changes to take effect.

Deleting Blocked File Extensions

To delete a blocked file extension:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Blocked File Extensions**.
2. In the List pane, select the blocked file extension you want to delete.
3. In the List pane toolbar, click the **Delete**  button.
4. A message appears asking to confirm the deletion. Click **Yes** to delete the blocked address.

When you delete a blocked file extension, the Retriever Service instances need to be restarted for the changes to take effect.

Blocking Attachments

You can block:

- ▶ All incoming attachments
- ▶ All incoming and outgoing attachments
- ▶ Specific incoming attachments
- ▶ Specific incoming and outgoing attachments

You cannot block only the outgoing attachments.

Blocking Specific Types of Attachments for Inbound Emails

To block specific types of attachments for inbound emails:

1. In the **Email > Blocked File Extensions** node, configure the file extensions you want to block.
2. In the department level setting, **Email for scan**, select **Inbound emails only**.
3. In the department level setting, **Block all attachments**, select **No**.
4. In the department level setting, **Action on blocked attachments**, select **Quarantine** or **Delete**.

Blocking Specific Types of Attachments for Inbound and Outbound Emails

To block specific types of attachments for inbound and outbound emails:

1. In the **Email > Blocked File Extensions** node, configure the file extensions you want to block.
2. In the department level setting, **Email for scan**, select **Both inbound and outbound emails**.
3. In the department level setting, **Block all attachments**, select **No**.

4. In the department level setting, **Action on blocked attachments**, select **Quarantine** or **Delete**.

Blocking All Types of Attachments for Inbound Emails

To block all types of attachments for inbound emails:

1. In the department level setting, **Email for scan**, select **Inbound emails only**.
2. In the department level setting, **Block all attachments**, select **Yes**.
3. In the department level setting, **Action on blocked attachments**, select **Quarantine** or **Delete**.

If you configure the setting, **Block all attachments**, to **Yes**, all attachments are blocked. Configuring file extensions in the **Email > Blocked File Extensions** node, will not override this setting.

Blocking All Types of Attachments for Inbound and Outbound Emails

To block all types of attachments for inbound and outbound emails:


1. In the department level setting, **Email for scan**, select **Both inbound and outbound emails**.
2. In the department level setting, **Block all attachments**, select **Yes**.
3. In the department level setting, **Action on blocked attachments**, select **Quarantine** or **Delete**.

If you configure the setting, **Block all attachments**, to **Yes**, all attachments are blocked. Configuring file extensions in the **Email > Blocked File Extensions** node, will not override this setting.

Viewing Blocked Attachments

Blocked attachments are available for viewing, only if the system is configured to quarantine blocked attachments. This is configured through the **Action on blocked attachments** department level setting.

To view a blocked attachment:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Blocked File Extensions**.
2. In the List pane toolbar, click the **Blocked attachments**  button.



The View blocked file extension window opens. Here you can see a list of attachments that have been blocked with the activity ID to which they belong.

Restoring Blocked Attachments

You can restore blocked attachments from the Administration Console and the Agent Console. Only agents with the “Restore blocked attachment” action can restore blocked attachments from the Agent Console. This section

talks about restoring attachments from the Administration Console only. For details about the Agent Console, see *Cisco Unified Web and E-Mail Interaction Manager Agent's Guide*.



To restore a blocked attachment:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Blocked File Extensions**.
2. In the List pane toolbar, click the **Blocked attachments**  button.
3. In the View blocked file extension window, select the attachment you want to restore and click the **Restore**  button.

Deleting Blocked Attachments

You can delete blocked attachments from the Administration Console and the Agent Console. Only agents with the “Delete blocked attachment” action can delete blocked attachments from the Agent Console. This section talks about deleting attachments from the Administration Console only. For details about the Agent Console, see *Cisco Unified Web and E-Mail Interaction Manager Agent's Guide*.

To delete a blocked attachment:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Blocked File Extensions**.
2. In the List pane toolbar, click the **Blocked attachments**  button.
3. In the View blocked file extension window, select the attachment you want to delete and click the **Delete**  button.



Delivery Exceptions

- ▶ [About Delivery Exceptions](#)
- ▶ [Configuring Delivery Exceptions](#)
- ▶ [Deleting Delivery Exceptions](#)

This chapter will assist you in understanding how to set up delivery exceptions.

About Delivery Exceptions

This feature allows you to handle emails that bounce back to the system because the original outgoing email could not be delivered to the intended recipient. Emails can bounce back for a number of reasons, like an incorrect email address, a customer mail box that has exceeded its storage limit, or network connectivity issues. Such emails are processed using the delivery exception feature of the application.

Administrators create a list of delivery exception words and phrases, like `Out of office`, `Auto-Reply`, `mail-daemon`, etc., that may appear in the email subject line or email addresses which indicate that an email is a bounce back. If the system finds any of these phrases, it treats the email as a bounced back email. Regular emails that contain phrases configured for delivery exception are also categorized as bounced back emails, and treated as such. Bouncebacks are of two types:


- ▶ **Permanent:** Indicates that an irreparable reason, such as an invalid email address, caused the email to bounce back. These are permanent failure conditions and any email sent to such email address would always bounce back.
- ▶ **Temporary:** Indicates that a temporary reason, such as an out of office reply or a temporary unavailability of the destination server caused the email to bounce back. The inference here is that should the emails be sent again, there is a chance that they may be delivered.

When the retriever picks up an email, it checks it for delivery exception words and phrases configured in the system. If the email address or subject contains any of those words, the activity subtype is changed to **Email-permanent undeliverable** or **Email-temporary undeliverable**, based on the failure type configured for that word or phrase, and the email activity is sent to the exception queue by the standard start workflow. These activities can be processed from the exception queue by a user with the appropriate permissions. Workflows can also be configured to process activities that are routed to the exception queue.

Cisco Unified Web and E-Mail Interaction Manager comes with some default delivery exception instances. Should you need to create other instances of delivery exception, you can easily do so from the **Delivery Exceptions** node in the Administration Console. For a list of default delivery exceptions, see [“Appendix: Predefined Delivery Exceptions”](#) on page 30.

Configuring Delivery Exceptions

To configure a delivery exception:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Delivery Exceptions**.
2. In the List pane toolbar, click the **New**  button.
3. In the Properties pane, on the General tab, and provide the following details.
 - **Name:** Type a name for the delivery exception.
 - **Description:** Provide a brief description.
 - **Type:** Select the type from the dropdown list. The options available are:

- Address
- Subject
- **Phrase:** Type the phrase you want the system to check for.
- **Failure:** Select the type of failure from the dropdown list. The options available are:
 - **Permanent**
 - **Temporary**

Name	Value
Name *	Auto-response
Description	
Type *	Subject
Phrase *	Auto-response
Failure *	Permanent

Set the general properties

4. Click the **Save**  button.


After configuring the delivery exception phrases, you need to stop and restart the email Retriever instance from the System Console to update the system accordingly.

Deleting Delivery Exceptions



Important: If you delete a system provided delivery exception phrase, it gets deleted from all departments in the system.

To delete a delivery exception:

1. In the Tree pane, browse to **Administration > Departments > *Department_Name* > Email > Delivery Exceptions**.
2. In the List pane, select the delivery exception you want to delete.
3. In the List pane toolbar, click the **Delete**  button.
4. A message appears asking to confirm the deletion. Click **Yes** to delete the delivery exception.

When you delete a delivery exception, the Retriever Service instances need to be restarted for the changes to take effect.

Appendix: Predefined Delivery Exceptions

This appendix contains a list of predefined delivery exception phrases available in the system.

Phrases Checked in Email Addresses

The following 16 phrases are checked in email addresses.

Name	Phrase	Failure
-MaiSer-	-MaiSer-	Temporary
Auto-reply	Auto-reply	Permanent
auto-sender	auto-sender	Permanent
Autoresponder	Autoresponder	Permanent
badaddress	badaddress	Temporary
ccmail_agent	ccmail_agent	Temporary
Mail-Gateway	Mail-Gateway	Temporary
Mail_master	Mail_master	Temporary
Mailer	Mailer	Temporary
mail-daemon	mail-daemon	Temporary
mdaemon	mdaemon	Temporary
postadm	postadm	Temporary
postmast	postmast	Temporary
postmaster	postmaster	Temporary
supervisor	supervisor	Permanent
unknown	unknown	Temporary

Phrases Checked in the Subject of Emails

The following 112 phrases are checked in the subject of the email.

Name	Phrase	Failure
Abwesenheitsnotiz	Abwesenheitsnotiz	Permanent
Address Unavailable	Address Unavailable	Temporary
Admin	Admin	Permanent
Adressänderung	Adressänderung	Permanent
Auto answer	Auto answer	Permanent
Auto Reply	Auto Reply	Permanent
Auto response	Auto response	Permanent
Auto-Reply	Auto-Reply	Permanent
Auto-response	Auto-response	Permanent
Automated response	Automated response	Permanent
Automated Omnigate Message	Automated Omnigate Message	Permanent
Automatic reply	Automatic reply	Permanent
Automatic response	Automatic response	Permanent
Automaticka odpoved	Automaticka odpoved	Permanent
AUTOMATICKA ODPOVID	AUTOMATICKA ODPOVID	Permanent
Automatisch antwoord	Automatisch antwoord	Permanent
Automatisk_svar	Automatisk_svar	Permanent
Automatsvar	Automatsvar	Permanent
AutoReply	AutoReply	Permanent
AutoResp	AutoResp	Permanent
Autoresponse	Autoresponse	Permanent
Autosvar	Autosvar	Permanent
away from my email	away from my email	Permanent
away from the office	away from the office	Permanent
bad-style address	bad-style address	Temporary
Bevestiging Ontvangen	Bevestiging Ontvangen	Permanent
bounced message	bounced message	Permanent
Conversion fail	Conversion fail	Permanent

Name	Phrase	Failure
could not send message	could not send message	Permanent
Delivery Confirmation	Delivery Confirmation	Permanent
Delivery Error	Delivery Error	Temporary
Delivery Failed	Delivery Failed	Temporary
Delivery Failure	Delivery Failure	Temporary
Delivery notification	Delivery notification	Temporary
Delivery Problem Notification	Delivery Problem Notification	Permanent
Delivery Report	Delivery Report	Temporary
Delivery Returned	Delivery Returned	Temporary
Delivery Status Notification	Delivery Status Notification	Temporary
Delivery-Report	Delivery-Report	Permanent
Details of my business trips	Details of my business trips	Permanent
Dikuji za maila	Dikuji za maila	Permanent
E-mail Received!	E-mail Received!	Permanent
E-mail Unavailable	E-mail Unavailable	Permanent
Error Response	Error Response	Temporary
Error sending mail	Error sending mail	Temporary
Extended Absence Response	Extended Absence Response	Permanent
Failed mail	Failed mail	Temporary
failed message delivery	failed message delivery	Permanent
failure notice	failure notice	Temporary
Ihre Mail	Ihre Mail	Permanent
Inaccessible e-mail address	Inaccessible e-mail address	Temporary
INBOUND MESSAGE ERR	INBOUND MESSAGE ERR	Permanent
Invalid mailbox	Invalid mailbox	Temporary
Invalid user	Invalid user	Temporary
Keep more of what you make!	Keep more of what you make!	Permanent
Mail Did Not Get Through	Mail Did Not Get Through	Temporary
Mail error	Mail error	Temporary
Mail failed	Mail failed	Temporary
Mail failure	Mail failure	Temporary

Name	Phrase	Failure
Mail recipient has left Enter-Net	Mail recipient has left Enter-Net	Permanent
Maternity Leave	Maternity Leave	Permanent
message failed	message failed	Permanent
message not sent	message not sent	Permanent
message rejected	message rejected	Permanent
message was not sent	message was not sent	Permanent
NDN:	NDN:	Temporary
No interest!!	No interest!!	Permanent
No such user	No such user	Temporary
Non-Delivery	Non-Delivery	Temporary
Non-existing employee	Non-existing employee	Permanent
Nondeliverable	Nondeliverable	Temporary
Not a WORLDPATH client	Not a WORLDPATH client	Permanent
Non deliverable	Non deliverable	Temporary
Not delivered	Not delivered	Temporary
not_a_jono_addy	not_a_jono_addy	Permanent
Odpoved na zpravu	Odpoved na zpravu	Permanent
Ontvangstbevestiging	Ontvangstbevestiging	Permanent
Out of email contact	Out of email contact	Permanent
Out of office	Out of office	Permanent
Out of the office	Out of the office	Permanent
ponse_automatique	ponse_automatique	Permanent
problem delivering your mail	problem delivering your mail	Permanent
Response from Administrator	Response from Administrator	Permanent
Response from bdbad	Response from bdbad	Permanent
Response from rlozano	Response from rlozano	Permanent
Resposta Automatica	Resposta Automatica	Permanent
Return message	Return message	Permanent
Returned Mail	Returned Mail	Permanent
Returned to Sender	Returned to Sender	Permanent
Réponse automatique	Réponse automatique	Permanent

Name	Phrase	Failure
Service Message	Service Message	Temporary
SMS error response	SMS error response	Temporary
SMS message	SMS message	Permanent
system	system	Permanent
Thanks for writing ER!	Thanks for writing ER!	Permanent
Thanks for your e-mail message!!	Thanks for your e-mail message!!	Permanent
Troubles delivering the message	Troubles delivering the message	Permanent
Unable to deliver mail	Unable to deliver mail	Temporary
Undeliverable	Undeliverable	Temporary
unknown address	unknown address	Temporary
unknown domain	unknown domain	Temporary
unknown recipient	unknown recipient	Temporary
User Not at VISTA.COM Domain	User Not at VISTA.COM Domain	Permanent
user not found	user not found	Temporary
user unknown	user unknown	Temporary
vacation	vacation	Permanent
Warning - delayed mail	Warning - delayed mail	Permanent
X.400 Inter-Personal Notification	X.400 Inter-Personal Notification	Temporary
Your Message To Juno	Your Message To Juno	Permanent
Your message was received	Your message was received	Permanent
ZAZ Reply	ZAZ Reply	Temporary