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

For Unified Contact Center Enterprise

Release 11.0(1)
August 2015

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
Preface

- About This Guide
- Obtaining Documentation and Submitting a Service Request
- Documentation Feedback
- Field Alerts and Field Notices
- Document Conventions
- Acronyms and Initialisms
- Other Learning Resources
Welcome to Cisco® Unified EIM & WIM™, 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 Unified EIM & WIM 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.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Field Alerts and Field Notices

Cisco products may be modified or key processes may be determined to be important. These are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field
Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Log into www.cisco.com and then access the tool at http://www.cisco.com/cisco/support/notifications.html

### Document Conventions

This guide uses the following typographical conventions.

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

**Document conventions**

### Acronyms and Initialisms

The following acronyms and initialisms are used in this document.

- ARM: Agent Reporting and Management
- CSA: Cisco Security Agent
- CTI: Computer Telephony Integration
- EAAS: External Agent Assignment Service
- ICM: Intelligent Contact Management
- 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: Simple Network Management Protocol
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.

<table>
<thead>
<tr>
<th>Use</th>
<th>To view</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help button</td>
<td>Topics in <em>Cisco Unified Web and E-Mail Interaction Manager Help</em>, the Help button appears in the console toolbar on every screen.</td>
</tr>
<tr>
<td>F1 keypad button</td>
<td>Context-sensitive information about the item selected on the screen.</td>
</tr>
</tbody>
</table>

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](http://www.cisco.com)


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 Offers Console
- 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
Email Basics

- Elements of the User Interface
- Key Terms and Concepts
- Configuring the System for Email
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.

### Elements of the User Interface

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

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).

### 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 16.

- **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 22.

- **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 25.

- **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 30.

  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 33.

### Configuring the System for Email

The following items must be configured before agents can begin replying to emails from customers.

- **Email aliases**: These map to email addresses to which customers send emails. For details, see “Aliases” on page 16.
- **Inbound workflows**: Process the emails. See the *Cisco Unified Web and E-mail Interaction Manager Administrator's Guide to Administration Console* for details.

- **Queues**: A holding location for emails waiting to be routed to agents. See the *Cisco Unified Web and E-mail Interaction Manager Administrator's Guide to Routing and Workflows* for details.

- **Users**: Agents who reply to emails, supervisors who monitor and manage agents, and administrators who create and administer workflow and routing. See the *Cisco Unified Web and E-mail Interaction Manager Administrator's Guide to Administration Console* for details.

**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.

**Data Masking for Email**

Data masking allows businesses to ensure that sensitive information, like credit card numbers, Social Security Numbers, bank account numbers, etc. is not transmitted from the system to the customers and vice versa. If the customer and agent do add any sensitive data in the email content and chat messages, all such data is masked before it is displayed to customers and agents and before it is stored in the application.

Data masking is the process of scanning the content for sensitive information and applying regular expressions to mask the sensitive information and hide the original data with characters, like, * ^ #. Data is masked using patterns, which are defined using Javascript and Java regular expressions.

Masking patterns are defined by the partition administrators and then are applied to the email and chat channel. The partition administrator can decide to manage the channels for all departments at the partition level, or can allow each department to manage their own configurations.

For email, you have the option to enable data masking for incoming and outgoing emails.
For details about setting up data masking, see the Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Administration Console.

**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): Gets incoming emails from configured aliases and parses them.
- Dispatcher service (For standalone and integrated emails): Sends outgoing emails out of the system.
- Workflow cache service: Maintains information about objects used in workflows.
- Workflow engine service: Applies workflows on emails to automate their routing and handling.
- **External Agent Assignment Service:** Routes activities to agents integrated with Unified CCE.
- **Listener:** Initiates and maintains the channel of communication with the Agent Peripheral Gateway (PG)/ARM interface of Unified CCE. Responsible for reporting all agent events.

**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
Aliases

- About Aliases
- Creating Aliases
- Deleting Aliases
- Changing the Status of Aliases
This chapter will assist you with setting 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 21.
   - **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. When an agent composes a new email, the default alias is selected as the From address for the email. The default email address is also used for activities transferred to this department from other departments, if the value of the setting ‘Set “From” email address for email activities transferred between departments’ is set to “Use default alias of destination department”. For details about the setting, see *Cisco Unified Web and E-Mail Interaction Manager Administrator’s Guide to Administration Console*.

**Important:** The default alias should be an active alias. Only one alias can be set as the default alias for each department.

- **Redirection Email Addresses:** If you are redirecting emails from other email addresses to this alias, then provide the list of those addresses. Separate the list of addresses using a semicolon. While replying to emails, in the From field, agents will by default see the redirection email address from where the email came in the system.

4. 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.
  - **Use SSL:** Select Yes, if you have enabled the retriever service to work with an SSL enabled mail server.
• **Port**: Provide the port used by the services server to connect to the IMAP or POP3 server. The field is pre-filled with a port number based on the type of server and SSL configuration selected. The default ports are:
  - POP3, with SSL disabled: 110
  - POP3, with SSL enabled: 995
  - IMAP, with SSL disabled: 143
  - IMAP, with SSL enabled: 993

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.
- **Use SSL**: Select Yes, if you have enabled the dispatcher service to work with an SSL enabled mail server.
- **Port**: Provide the port used by the services server to connect to the SMTP or ESMTP server. The field is pre-filled with a port number based on the type of server and SSL configuration selected. The default ports are:
  - SMTP, with SSL disabled: 25
  - SMTP, with SSL enabled: 587
  - ESMTP, with SSL disabled: 25
  - ESMTP, with SSL enabled: 587

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

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

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.

  ![Properties: <New>](image)

  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.

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 mailbox 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 33.

**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

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Phrase</th>
<th>Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>-MaiSer-</td>
<td>-MaiSer-</td>
<td>Temporary</td>
</tr>
<tr>
<td>Auto-reply</td>
<td>Auto-reply</td>
<td>Permanent</td>
</tr>
<tr>
<td>auto-sender</td>
<td>auto-sender</td>
<td>Permanent</td>
</tr>
<tr>
<td>Autoresponder</td>
<td>Autoresponder</td>
<td>Permanent</td>
</tr>
<tr>
<td>badaddress</td>
<td>badaddress</td>
<td>Temporary</td>
</tr>
<tr>
<td>ccmail_agent</td>
<td>ccmail_agent</td>
<td>Temporary</td>
</tr>
<tr>
<td>Mail-Gateway</td>
<td>Mail-Gateway</td>
<td>Temporary</td>
</tr>
<tr>
<td>Mail_master</td>
<td>Mail_master</td>
<td>Temporary</td>
</tr>
<tr>
<td>Mailer</td>
<td>Mailer</td>
<td>Temporary</td>
</tr>
<tr>
<td>mail-daemon</td>
<td>mail-daemon</td>
<td>Temporary</td>
</tr>
<tr>
<td>mdaemon</td>
<td>mdaemon</td>
<td>Temporary</td>
</tr>
<tr>
<td>postadm</td>
<td>postadm</td>
<td>Temporary</td>
</tr>
<tr>
<td>postmast</td>
<td>postmast</td>
<td>Temporary</td>
</tr>
<tr>
<td>postmaster</td>
<td>postmaster</td>
<td>Temporary</td>
</tr>
<tr>
<td>supervisor</td>
<td>supervisor</td>
<td>Permanent</td>
</tr>
<tr>
<td>unknown</td>
<td>unknown</td>
<td>Temporary</td>
</tr>
</tbody>
</table>
The following 112 phrases are checked in the subject of the email.

<table>
<thead>
<tr>
<th>Name</th>
<th>Phrase</th>
<th>Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abwesenheitsnotiz</td>
<td>Abwesenheitsnotiz</td>
<td>Permanent</td>
</tr>
<tr>
<td>Address Unavailable</td>
<td>Address Unavailable</td>
<td>Temporary</td>
</tr>
<tr>
<td>Admin</td>
<td>Admin</td>
<td>Permanent</td>
</tr>
<tr>
<td>Adressänderung</td>
<td>Adressänderung</td>
<td>Permanent</td>
</tr>
<tr>
<td>Auto answer</td>
<td>Auto answer</td>
<td>Permanent</td>
</tr>
<tr>
<td>Auto Reply</td>
<td>Auto Reply</td>
<td>Permanent</td>
</tr>
<tr>
<td>Auto response</td>
<td>Auto response</td>
<td>Permanent</td>
</tr>
<tr>
<td>Auto-Reply</td>
<td>Auto-Reply</td>
<td>Permanent</td>
</tr>
<tr>
<td>Auto-response</td>
<td>Auto-response</td>
<td>Permanent</td>
</tr>
<tr>
<td>Automated response</td>
<td>Automated response</td>
<td>Permanent</td>
</tr>
<tr>
<td>Automated Omnigate Message</td>
<td>Automated Omnigate Message</td>
<td>Permanent</td>
</tr>
<tr>
<td>Automatic reply</td>
<td>Automatic reply</td>
<td>Permanent</td>
</tr>
<tr>
<td>Automatic response</td>
<td>Automatic response</td>
<td>Permanent</td>
</tr>
<tr>
<td>Automaticcka odpoved</td>
<td>Automaticcka odpoved</td>
<td>Permanent</td>
</tr>
<tr>
<td>AUTOMATICKA ODPOVID</td>
<td>AUTOMATICKA ODPOVID</td>
<td>Permanent</td>
</tr>
<tr>
<td>Automatisch antwoord</td>
<td>Automatisch antwoord</td>
<td>Permanent</td>
</tr>
<tr>
<td>Automatisk_svar</td>
<td>Automatisk_svar</td>
<td>Permanent</td>
</tr>
<tr>
<td>Automatsvar</td>
<td>Automatsvar</td>
<td>Permanent</td>
</tr>
<tr>
<td>AutoReply</td>
<td>AutoReply</td>
<td>Permanent</td>
</tr>
<tr>
<td>AutoResp</td>
<td>AutoResp</td>
<td>Permanent</td>
</tr>
<tr>
<td>Autoresponse</td>
<td>Autoresponse</td>
<td>Permanent</td>
</tr>
<tr>
<td>Autosvar</td>
<td>Autosvar</td>
<td>Permanent</td>
</tr>
<tr>
<td>away from my email</td>
<td>away from my email</td>
<td>Permanent</td>
</tr>
<tr>
<td>away from the office</td>
<td>away from the office</td>
<td>Permanent</td>
</tr>
<tr>
<td>bad-style address</td>
<td>bad-style address</td>
<td>Temporary</td>
</tr>
<tr>
<td>Bevestiging Ontvangen</td>
<td>Bevestiging Ontvangen</td>
<td>Permanent</td>
</tr>
<tr>
<td>bounced message</td>
<td>bounced message</td>
<td>Permanent</td>
</tr>
<tr>
<td>Conversion fail</td>
<td>Conversion fail</td>
<td>Permanent</td>
</tr>
<tr>
<td>Name</td>
<td>Phrase</td>
<td>Failure</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>could not send message</td>
<td>could not send message</td>
<td>Permanent</td>
</tr>
<tr>
<td>Delivery Confirmation</td>
<td>Delivery Confirmation</td>
<td>Permanent</td>
</tr>
<tr>
<td>Delivery Error</td>
<td>Delivery Error</td>
<td>Temporary</td>
</tr>
<tr>
<td>Delivery Failed</td>
<td>Delivery Failed</td>
<td>Temporary</td>
</tr>
<tr>
<td>Delivery Failure</td>
<td>Delivery Failure</td>
<td>Temporary</td>
</tr>
<tr>
<td>Delivery notification</td>
<td>Delivery notification</td>
<td>Temporary</td>
</tr>
<tr>
<td>Delivery Problem Notification</td>
<td>Delivery Problem Notification</td>
<td>Permanent</td>
</tr>
<tr>
<td>Delivery Report</td>
<td>Delivery Report</td>
<td>Temporary</td>
</tr>
<tr>
<td>Delivery Returned</td>
<td>Delivery Returned</td>
<td>Temporary</td>
</tr>
<tr>
<td>Delivery Status Notification</td>
<td>Delivery Status Notification</td>
<td>Temporary</td>
</tr>
<tr>
<td>Delivery-Report</td>
<td>Delivery-Report</td>
<td>Permanent</td>
</tr>
<tr>
<td>Details of my business trips</td>
<td>Details of my business trips</td>
<td>Permanent</td>
</tr>
<tr>
<td>Dikuji za maila</td>
<td>Dikuji za maila</td>
<td>Permanent</td>
</tr>
<tr>
<td>E-mail Received!</td>
<td>E-mail Received!</td>
<td>Permanent</td>
</tr>
<tr>
<td>E-mail Unavailable</td>
<td>E-mail Unavailable</td>
<td>Permanent</td>
</tr>
<tr>
<td>Error Response</td>
<td>Error Response</td>
<td>Temporary</td>
</tr>
<tr>
<td>Error sending mail</td>
<td>Error sending mail</td>
<td>Temporary</td>
</tr>
<tr>
<td>Extended Absence Response</td>
<td>Extended Absence Response</td>
<td>Permanent</td>
</tr>
<tr>
<td>Failed mail</td>
<td>Failed mail</td>
<td>Temporary</td>
</tr>
<tr>
<td>failed message delivery</td>
<td>failed message delivery</td>
<td>Permanent</td>
</tr>
<tr>
<td>failure notice</td>
<td>failure notice</td>
<td>Temporary</td>
</tr>
<tr>
<td>Ihre Mail</td>
<td>Ihre Mail</td>
<td>Permanent</td>
</tr>
<tr>
<td>Inaccessible e-mail address</td>
<td>Inaccessible e-mail address</td>
<td>Temporary</td>
</tr>
<tr>
<td>INBOUND MESSAGE ERR</td>
<td>INBOUND MESSAGE ERR</td>
<td>Permanent</td>
</tr>
<tr>
<td>Invalid mailbox</td>
<td>Invalid mailbox</td>
<td>Temporary</td>
</tr>
<tr>
<td>Invalid user</td>
<td>Invalid user</td>
<td>Temporary</td>
</tr>
<tr>
<td>Keep more of what you make!</td>
<td>Keep more of what you make!</td>
<td>Permanent</td>
</tr>
<tr>
<td>Mail Did Not Get Through</td>
<td>Mail Did Not Get Through</td>
<td>Temporary</td>
</tr>
<tr>
<td>Mail error</td>
<td>Mail error</td>
<td>Temporary</td>
</tr>
<tr>
<td>Mail failed</td>
<td>Mail failed</td>
<td>Temporary</td>
</tr>
<tr>
<td>Mail failure</td>
<td>Mail failure</td>
<td>Temporary</td>
</tr>
<tr>
<td>Name</td>
<td>Phrase</td>
<td>Failure</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Mail recipient has left Enter-Net</td>
<td>Mail recipient has left Enter-Net</td>
<td>Permanent</td>
</tr>
<tr>
<td>Maternity Leave</td>
<td>Maternity Leave</td>
<td>Permanent</td>
</tr>
<tr>
<td>message failed</td>
<td>message failed</td>
<td>Permanent</td>
</tr>
<tr>
<td>message not sent</td>
<td>message not sent</td>
<td>Permanent</td>
</tr>
<tr>
<td>message rejected</td>
<td>message rejected</td>
<td>Permanent</td>
</tr>
<tr>
<td>message was not sent</td>
<td>message was not sent</td>
<td>Permanent</td>
</tr>
<tr>
<td>NDN:</td>
<td>NDN:</td>
<td>Temporary</td>
</tr>
<tr>
<td>No interest!!</td>
<td>No interest!!</td>
<td>Permanent</td>
</tr>
<tr>
<td>No such user</td>
<td>No such user</td>
<td>Temporary</td>
</tr>
<tr>
<td>Non-Delivery</td>
<td>Non-Delivery</td>
<td>Temporary</td>
</tr>
<tr>
<td>Non-existing employee</td>
<td>Non-existing employee</td>
<td>Permanent</td>
</tr>
<tr>
<td>Nondeliverable</td>
<td>Nondeliverable</td>
<td>Temporary</td>
</tr>
<tr>
<td>Not a WORLDPATH client</td>
<td>Not a WORLDPATH client</td>
<td>Permanent</td>
</tr>
<tr>
<td>Non deliverable</td>
<td>Non deliverable</td>
<td>Temporary</td>
</tr>
<tr>
<td>Not delivered</td>
<td>Not delivered</td>
<td>Temporary</td>
</tr>
<tr>
<td>not_a_jono_addy</td>
<td>not_a_jono_addy</td>
<td>Permanent</td>
</tr>
<tr>
<td>Odpoved na zpravu</td>
<td>Odpoved na zpravu</td>
<td>Permanent</td>
</tr>
<tr>
<td>Ontvangstbevestiging</td>
<td>Ontvangstbevestiging</td>
<td>Permanent</td>
</tr>
<tr>
<td>Out of email contact</td>
<td>Out of email contact</td>
<td>Permanent</td>
</tr>
<tr>
<td>Out of office</td>
<td>Out of office</td>
<td>Permanent</td>
</tr>
<tr>
<td>Out of the office</td>
<td>Out of the office</td>
<td>Permanent</td>
</tr>
<tr>
<td>ponse_automatique</td>
<td>ponse_automatique</td>
<td>Permanent</td>
</tr>
<tr>
<td>problem delivering your mail</td>
<td>problem delivering your mail</td>
<td>Permanent</td>
</tr>
<tr>
<td>Response from Administrator</td>
<td>Response from Administrator</td>
<td>Permanent</td>
</tr>
<tr>
<td>Response from bdbad</td>
<td>Response from bdbad</td>
<td>Permanent</td>
</tr>
<tr>
<td>Response from rlozano</td>
<td>Response from rlozano</td>
<td>Permanent</td>
</tr>
<tr>
<td>Resposta Automatica</td>
<td>Resposta Automatica</td>
<td>Permanent</td>
</tr>
<tr>
<td>Return message</td>
<td>Return message</td>
<td>Permanent</td>
</tr>
<tr>
<td>Returned Mail</td>
<td>Returned Mail</td>
<td>Permanent</td>
</tr>
<tr>
<td>Returned to Sender</td>
<td>Returned to Sender</td>
<td>Permanent</td>
</tr>
<tr>
<td>Réponse automatique</td>
<td>Réponse automatique</td>
<td>Permanent</td>
</tr>
<tr>
<td>Name</td>
<td>Phrase</td>
<td>Failure</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Service Message</td>
<td>Service Message</td>
<td>Temporary</td>
</tr>
<tr>
<td>SMS error response</td>
<td>SMS error response</td>
<td>Temporary</td>
</tr>
<tr>
<td>SMS message</td>
<td>SMS message</td>
<td>Permanent</td>
</tr>
<tr>
<td>system</td>
<td>system</td>
<td>Permanent</td>
</tr>
<tr>
<td>Thanks for writing ER!</td>
<td>Thanks for writing ER!</td>
<td>Permanent</td>
</tr>
<tr>
<td>Thanks for your e-mail message!!</td>
<td>Thanks for your e-mail message!!</td>
<td>Permanent</td>
</tr>
<tr>
<td>Troubles delivering the message</td>
<td>Troubles delivering the message</td>
<td>Permanent</td>
</tr>
<tr>
<td>Unable to deliver mail</td>
<td>Unable to deliver mail</td>
<td>Temporary</td>
</tr>
<tr>
<td>Undeliverable</td>
<td>Undeliverable</td>
<td>Temporary</td>
</tr>
<tr>
<td>unknown address</td>
<td>unknown address</td>
<td>Temporary</td>
</tr>
<tr>
<td>unknown domain</td>
<td>unknown domain</td>
<td>Temporary</td>
</tr>
<tr>
<td>unknown recipient</td>
<td>unknown recipient</td>
<td>Temporary</td>
</tr>
<tr>
<td>User Not at VISTA.COM Domain</td>
<td>User Not at VISTA.COM Domain</td>
<td>Permanent</td>
</tr>
<tr>
<td>user not found</td>
<td>user not found</td>
<td>Temporary</td>
</tr>
<tr>
<td>user unknown</td>
<td>user unknown</td>
<td>Temporary</td>
</tr>
<tr>
<td>vacation</td>
<td>vacation</td>
<td>Permanent</td>
</tr>
<tr>
<td>Warning - delayed mail</td>
<td>Warning - delayed mail</td>
<td>Permanent</td>
</tr>
<tr>
<td>X.400 Inter-Personal Notification</td>
<td>X.400 Inter-Personal Notification</td>
<td>Temporary</td>
</tr>
<tr>
<td>Your Message To Juno</td>
<td>Your Message To Juno</td>
<td>Permanent</td>
</tr>
<tr>
<td>Your message was received</td>
<td>Your message was received</td>
<td>Permanent</td>
</tr>
<tr>
<td>ZAZ Reply</td>
<td>ZAZ Reply</td>
<td>Temporary</td>
</tr>
</tbody>
</table>