



Enterprise Chat and Email Administrator's Guide to Email Resources, Release 12.5(1) ES3

For Unified Contact Center Enterprise

First Published: January, 2020

Last Updated: June, 2022

Americas Headquarters

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

First Published: January, 2020

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 NON-INFRINGEMENT 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.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned 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. (1110R)

Enterprise Chat and Email Administrator's Guide to Email Resources: For Unified Contact Center Enterprise. June 15, 2022

© 2016-2020, Cisco Systems, Inc. All rights reserved.

Contents

- Chapter 1: Preface6**
 - About This Guide 7
 - Change History 7
 - Obtaining Documentation and Submitting a Service Request 7
 - Documentation Feedback 8
 - Field Alerts and Field Notices 8
 - Document Conventions..... 8
 - Acronyms and Initialisms 8
 - Other Learning Resources..... 9
 - Online Help 9
 - Document Set 9

- Chapter 2: Email Basics11**
 - Elements of the User Interface 12
 - Key Terms and Concepts 13
 - Configuring the System for Email 13
 - Important Tasks on the Mail Server 14
 - Configuring Spam Filters on Mail Server 14
 - Data Masking for Email 14
 - Services for Emails 15
 - Settings for Emails 15
 - Settings for Delivery Exceptions..... 15

- Chapter 3: Aliases16**
 - About Aliases 17
 - Creating Aliases 17
 - Deleting Aliases 20
 - Changing the Status of Aliases 21

Chapter 4: Email Accounts.....22

- About Email Accounts 23
- Registering Applications with Azure Active Directory 23
 - Registering an Application 23
 - Adding Client Secret 24
 - Assigning API Permissions 25
- Configuring OAuth Applications 25
- Deleting OAuth Applications 26
- Configuring Email Accounts 27
 - Creating Email Accounts 27
 - Adding Email Aliases 28
 - Adding new email aliases 28
 - Adding existing email aliases 30
- Testing Connections for Email Accounts 30
- Removing linked Aliases from Email Accounts 31
- Deleting Email Accounts 31

Chapter 5: Blocked File Extensions32

- About Blocked File Extensions 33
- Configuring Blocked File Extensions 33
- Deleting Blocked File Extensions 34
- Blocking Attachments 34
 - Blocking Specific Types of Attachments for Inbound Emails 34
 - Blocking Specific Types of Attachments for Inbound and Outbound Emails 35
 - Blocking All Types of Attachments for Inbound Emails 35
 - Blocking All Types of Attachments for Inbound and Outbound Emails 35
- Viewing Blocked Attachments 35
- Restoring Blocked Attachments 36
- Deleting Blocked Attachments 36

Chapter 6: Delivery Exceptions.....37

- About Delivery Exceptions 38
- Configuring Delivery Exceptions 38

Deleting Delivery Exceptions	39
Appendix: Predefined Delivery Exceptions	41
Phrases Checked in Email Addresses	41
Phrases Checked in the Subject of Emails	42

1

Preface

- ▶ [About This Guide](#)
- ▶ [Change History](#)
- ▶ [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® Enterprise Chat and Email™, 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.

About This Guide

Enterprise Chat and Email 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.

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

Change	See	Date
Update of Document		June 2022
Listed requirements to configure email accounts.	“Configuring Email Accounts” on page 27	
Update of Document		April 2022
Note added in reference to adding specific URLs to communicate with mailboxes while configuring Email Accounts.	“About Email Accounts” on page 23	
Update of Document for Release 12.5(1) ES3		July 2021
Email Accounts chapter added	“Email Accounts” on page 22	

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.

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.

- ▶ 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
- ▶ 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 Enterprise Chat and Email 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 Enterprise Chat and Email 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>

- ▶ 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:

- ▶ *Cisco Enterprise Chat and Email Hardware and System Software Specification*
- ▶ *Cisco Enterprise Chat and Email Installation Guide*
- ▶ *Cisco Enterprise Chat and Email Browser Settings Guide*

User guides for agents and supervisors

- ▶ *Cisco Enterprise Chat and Email Agent's Guide*
- ▶ *Cisco Enterprise Chat and Email Supervisor's Guide*

User guides for Knowledge Base managers and authors

- ▶ *Cisco Enterprise Chat and Email Knowledge Base Author's Guide*

User guides for administrators

- ▶ *Cisco Enterprise Chat and Email Administrator's Guide to Administration Console*
- ▶ *Cisco Enterprise Email and Chat Administrator's Guide to Routing and Workflows*
- ▶ *Cisco Enterprise Chat and Email Administrator's Guide to Chat and Collaboration Resources*
- ▶ *Cisco Enterprise Chat and Email Administrator's Guide to Email Resources*
- ▶ *Cisco Enterprise Chat and Email Administrator's Guide to Reports Console*
- ▶ *Cisco Enterprise Chat and Email Administrator's Guide to System Console*
- ▶ *Cisco Enterprise Chat and Email Administrator's Guide to Tools Console*

1

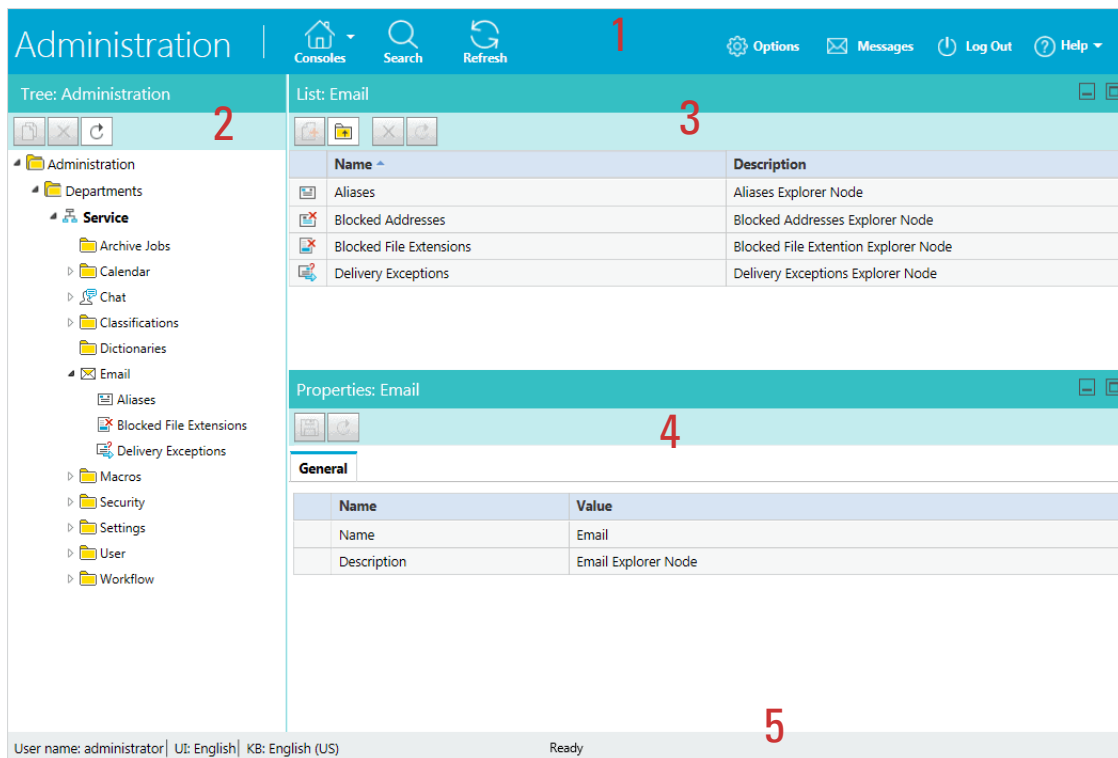
Email Basics

- ▶ [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.



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 into 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 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 32](#).

- ▶ **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 37](#).

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 41](#).

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 *Enterprise Chat and Email Administrator's Guide to Administration Console* for details.
- ▶ **Queues:** A holding location for emails waiting to be routed to agents. See *Enterprise Chat and Email 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 *Enterprise Chat and Email 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.

Configuring Spam Filters on Mail Server

You may wish to block emails from certain email addresses or domains from being processed by the system. To do this, spam filters must be established on the IMAP or POP3 mail server to handle spam emails coming in the system. Refer to your IT department for more information.

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 *Enterprise Chat and Email 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 *Enterprise Chat and Email Administrator's Guide to System Console*.

- ▶ **Retriever service:** Gets incoming emails from configured aliases and parses them.
- ▶ **Dispatcher service:** 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 *Enterprise Chat and Email Administrator's Guide to Administrator's Console*.

Settings for Delivery Exceptions

These settings are available at the partition level.

- ▶ Default SMTP Server Settings

2

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 *Enterprise Chat and Email Administrator's Guide to Routing and Workflows*.

Basic authenticated email aliases can be added to email accounts to convert them to OAuth authenticated aliases. For more information, see [“Email Accounts” on page 22](#).

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 the email. Only one BCC address may be used. Whenever an email is sent out from this alias, a BCC copy of that email is automatically sent to this address. You can use this option when you want to review later the replies sent out from a particular alias.
 - **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 *Enterprise Chat and Email 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.

Name	Value
Name *	Customer Support
Description	
Email address *	support@company.com
Status *	Active
Automatic BCC	
Send mail to	
Default alias *	Yes
Redirection Email Adres...	

Set the general properties

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.
 - **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 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
- **Folder:** The folder from which emails are fetched. By default, “inbox” is selected. This can be changed to a different folder if IMAP protocol is selected.

	Name	Value
Incoming	Server type	POP3
Outgoing	Server name *	Mail Server
	User name *	jdoe
	Password *	*****
	Verify password *	*****
	Use SSL	Yes
	Port *	995
	Folder *	inbox

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 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.

	Name	Value
Incoming		
Outgoing	Server type	SMTP
	Use SMTP	<Select>
	Server name *	Mail Server
	User name (ES...	
	Password *	
	Verify password *	
	Use SSL	No
	Port *	25

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. Now, use the alias in an inbound workflow. For more details on workflows, see *Enterprise Chat and Email 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 *Enterprise Chat and Email 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.

Email Accounts

- ▶ [About Email Accounts](#)
- ▶ [Registering Applications with Azure Active Directory](#)
- ▶ [Configuring OAuth Applications](#)
- ▶ [Deleting OAuth Applications](#)
- ▶ [Configuring Email Accounts](#)
- ▶ [Testing Connections for Email Accounts](#)
- ▶ [Removing linked Aliases from Email Accounts](#)
- ▶ [Deleting Email Accounts](#)

About Email Accounts

You can use the OAuth 2.0 authentication service (provided by Azure Active Directory) to enable your application to connect with IMAP, POP or SMTP protocols to send and receive emails in a more secure way. Email accounts allow you to create or add OAuth authenticated aliases. These email accounts are associated with the OAuth applications registered with Microsoft Azure Active Directory.

To use the OAuth 2.0 authentication for email, perform the following tasks:

1. Register your application with Azure Active Directory ([page 23](#)).
2. Configure an OAuth application in the Administration Console ([page 25](#)).
3. Configure an email account and add email aliases to it ([page 27](#)).



Important: While configuring an email account, in order to communicate to the mailbox, you need to ensure that the following URLs have been provided accessibility and connectivity from the Application server and Services server: *.office365.com and *login.microsoftonline.com.

4. Test connection for the email account ([page 30](#)).

Registering Applications with Azure Active Directory

Before using OAuth 2.0 authentication with your application, you must register your application with Azure Active Directory. Once the registration is complete, you will get the **client ID**, **tenant ID** and **Value** of the client secret. For more information, see [Register an application with the Microsoft identity platform](#).

You need to perform the following tasks:

- ▶ Register an application on the Azure portal ([page 23](#)).
- ▶ Add a client secret ([page 24](#)).
- ▶ Assign API permissions to the registered application ([page 25](#)).

Registering an Application

To register an application with Azure Active Directory:

1. Sign in to the [Azure portal](#).
2. Search for and select **Azure Active Directory**.
3. Under Manage, select **App registrations > New registration**.
4. In the Register an application page, provide the following details:
 - **Name:** Provide a user-facing display name for the application.
 - **Supported Account Types:** Select the **Accounts in this organizational directory only (Single tenant)** option.

- **Redirect URL:** Provide the **Redirect URL** in the following format:
`https://ECE_Web_Server_or_Load_Balancer_Server/Context_Name/web/view/mail/admin/account/showauthcode.jsp`. For example,
`https://sample.company.com/system/web/view/mail/admin/account/showauthcode.jsp`. This is the URL of the page where the authorization code is generated after successful authentication.

5. Click **Register**.

The Overview pane opens after the application is registered. The following information is displayed for the registered application:

- **Application (client) ID** (also called the **client ID**): This value uniquely identifies your application in the Microsoft identity platform.
- **Directory (tenant) ID** (also called the **tenant ID**)



Important: Record the client ID and tenant ID. This information is used while configuring the OAuth Application in the Administration Console (page 25).

Adding Client Secret

A client secret is a secret string that is used by the application to prove its identity when requesting a token.

To add a client secret:

1. Sign in to the [Azure portal](#).
2. Search for and select **Azure Active Directory**.
3. Under Manage, click **App registrations** and select the application that you registered with Azure Active Directory (page 23).
4. Now, under Manage, select **Certificates & secrets > New client secret**.
5. In the Add a client secret page, provide the following details:
 - **Description:** Add a description for your client secret.
 - **Expires:** From the dropdown, select an expiration for the secret or specify a custom lifetime. You can select from the following options:
 - **Recommended: 6 months**
 - **3 months**
 - **12 months**
 - **18 months**
 - **24 months**
 - **Custom:** You can provide a custom start and end date.



Important: Client secret lifetime is limited to two years (24 months) or less. You cannot specify a custom lifetime longer than 24 months.

6. Click the **Add** button.

The client secret **Value** and **Secret ID** is displayed.



Important: Record the Value of the client secret as it is masked after you leave the page. This information is used while configuring the OAuth Application in the Administration Console (page 25).

Assigning API Permissions


To assign API permissions:

1. Sign in to the [Azure portal](#).
2. Search for and select **Azure Active Directory**.
3. Under Manage, click **App registrations** and select the application that you registered with Azure Active Directory (page 23).
4. Now, under Manage, select **API Permissions > Microsoft Graph > Delegated permissions**.
5. In the Request API page, select the following delegated permissions:
 - `IMAP.AccessAsUser.All`
 - `Mail.Read`
 - `Mail.Read.Shared`
 - `Mail.ReadWrite`
 - `Mail.ReadWrite.Shared`
 - `Mail.Send`
 - `Mail.Send.Shared`
 - `offline_access`
 - `POP.AccessAsUser.All`
 - `SMTP.Send`
 - `User.Read`
6. Click the **Update Permissions** button.

Configuring OAuth Applications

After registering your application with the Azure Active Directory, configure your application details in the Administration Console.

To configure an OAuth application:

1. In the Tree pane, browse to **Administration > Partition: *Partition Name* > Email > OAuth Applications**.
2. In the List pane toolbar, click the **New**  button
3. In the Properties pane, provide the following details:

- **Name:** The name for the configuration.
- **Description:** Provide a brief description.
- **Provider:** Select **Microsoft Office 365**.
- **Endpoint:** Select **Worldwide**.
- **Tenant ID:** Provide the **tenant ID** assigned by Azure Active Directory. For more information see, [“Registering an Application” on page 23](#)
- **Client ID:** Provide the **client ID** assigned by Azure Active Directory. For more information see, [“Registering an Application” on page 23](#)
- **Client Secret:** Provide the **client secret Value**. For more information see, [“Adding Client Secret” on page 24](#)

Name	Value
Name *	oauth_app
Description	
Provider	Microsoft Office 365
Endpoint	Worldwide
Client ID *	26047cfe-0c27-47dc-843d-b9a188e10382
Tenant ID *	d60887ce-696b-4e9a-98db-a7266a25839f
Client Secret *	*****

Configure the general properties of the OAuth Application

4. Click the **Save** button.

Deleting OAuth Applications

You cannot delete an OAuth application, if it is used in email accounts.

To delete an email account:

1. In the Tree pane, browse to **Administration > Partition:** *Partition Name* **> Email > OAuth Applications**.
2. In the List pane, select the OAuth application you want to delete.
3. In the list pane toolbar, click the **Delete** button.
4. You are prompted to confirm the deletion. Click **OK** to delete the OAuth Application.

Configuring Email Accounts



After configuring the OAuth applications, you need to create email accounts ([page 27](#)) and add email aliases ([page 28](#)) to them.

Before configuring the email accounts, perform the following tasks:

- ▶ Configure the Web Server URL and Load Balancer URL partition setting to generate the authorization code.
- ▶ Ensure that the FQDN (Fully Qualified Domain Name) used in the Web Server URL must match the FQDN used in the Redirect URL configured in the Azure Active Directory.
- ▶ Administrator must log into the ECE Administration Console using the same FQDN as inputted in the Web Server URL.

Creating Email Accounts

To create an email account:

1. In the Tree pane, browse to **Administration > Department:** *Department Name* > **Email > Accounts**.
2. In the List pane toolbar, click the **New**  button
3. In the Properties pane, under the General tab, provide the following details:
 - **Account Name:** The name for the account.
 - **Account Description:** A brief description of the account.
 - **Status:** Select **Active** to make the account active. By default the status of an account is set as **Active**.
 - **OAuth Registered App:** Select the OAuth application, configured at the partition level. For more information, see “[Configuring OAuth Applications](#)” on [page 25](#). Note that you can map an OAuth application to multiple email accounts.
 - **Server Type:** Select the server type you want to use. The options available are: **POP3 and SMTP** and **IMAP and SMTP**.
 - **Address:** The value is set as **outlook.office365.com** when an **OAuth Registered App** is selected. This value cannot be changed.
 - **Authentication Type:** The value is set as **OAuth 2.0** and it cannot be changed.
 - **Authentication Token:** Click the **Assistance**  button to generate the authorization code. On the Microsoft Sign in page, log into the Microsoft account associated with the registered application and accept the permissions requested to generate the authorization code. Once the authorization is complete, a page is displayed with the authorization code.

- **Authorization code:** Paste the authorization code.

Name	Value
Account name *	support@customer.com
Account description	
Status	Active
OAuth Registered App *	email_app
Server type	IMAP and SMTP
Address	outlook.office365.com
Authentication type *	OAuth2.0
Authentication token	Click the Assistance button to generate the authentication token.
Authorization code	*****

Configure the general properties of the Email Account

4. Click the **Save**  button.

Once the account is saved, the Email Address (page 27) tab and the **Test Connection** (page 30) button in the Properties pane toolbar are enabled.

Adding Email Aliases

Under the Email Address tab, you can either create new email aliases (page 28) or you can add existing email aliases, under basic authentication, to email accounts to convert them into OAuth authentication (page 30). After the existing aliases are added to the email account, they are no longer available in the **Aliases** list. To know more about creating basic authenticated aliases, see “Aliases” on page 16.

Adding new email aliases

To add a new email alias:

1. In the Tree pane, browse to **Administration > Department:** *Department Name* > **Email > Accounts**.
2. In the List pane, select the account to which you want to add a new email alias.
3. In the Properties pane, under the Email Address tab, click the **New** button.
4. In the **Add a New Alias** window, provide the following details:
 - **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 **Active**.
 - **Automatic BCC:** Type the email address to which you want to send a BCC copy of the email. Only one BCC address may be used. Whenever an email is sent out from this alias, a BCC copy of that email is

automatically sent to this address. You can use this option when you want to review later the replies sent out from a particular alias.



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

- **Send Email To:** Specify the email address to which the outgoing emails from this alias should go. Whenever an agent replies to a customer email, the reply is sent only to the email address specified in the **Send Email To** field and not to the customer email address. You can use this option to test that the alias has been configured properly and to test workflows. Make sure that after testing the alias you make this field empty.
- **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**.



Important: A default alias should also be active and for each department only one alias can be the default alias.

- **Redirection Email Addresses:** List the email addresses from where you want to redirect the emails to this email address. Separate the list of email 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.
- **Folder:** The folder from which emails are fetched. By default, **inbox** is selected. This can be changed to a different folder if IMAP protocol is selected.
- **Shared Mailbox:** To add shared mailboxes as aliases to email accounts, select **Yes**. The default value is **No**.

Add a new alias

Name	Value
Email address *	support@company.com
Status *	Active <input type="checkbox"/>
Automatic BCC	
Send mail to	
Default alias *	Yes <input type="checkbox"/>
Redirection email addresses	
Shared mailbox	No <input type="checkbox"/>
Folder	inbox

Add a new alias to the Email Account

5. Click **Save**.

Adding existing email aliases

To add an existing alias:

1. In the Tree pane, browse to **Administration > Department:** *Department Name* > **Email > Accounts**.
2. In the List pane, select the account to which you want to add an existing basic authenticated email alias.
3. In the Properties pane, under the Email Address tab, click the **Add Existing Email Address** button.
4. In the **Add Existing Aliases** window, from the list of existing email aliases within the department, click the check boxes next to the email aliases you want to convert to OAuth authenticated aliases.
5. If the existing email alias belongs to a shared account, click the check box next to the **Add as Shared Mailbox** option.
6. Click **OK**. The aliases are validated and then added to the account. When an alias, which does not belong to the email account, is added, an error is shown.

Select	Existing Aliases
<input checked="" type="checkbox"/>	support@company.com
<input checked="" type="checkbox"/>	services@company.com

Add as shared mailbox

OK Cancel

Add an existing alias to the Email Account

Testing Connections for Email Accounts

After creating and saving an email account, the **Test Connection** button on the properties pane toolbar is enabled. It is used to test the validity of an email account.

An email account can become invalid due to the following reasons:

- ▶ When the generated authorization code is revoked or has expired.
- ▶ When the email aliases no longer belong to the account.
- ▶ When the permissions granted to the OAuth application are revoked.

To test the connection for an email account:

1. In the Tree pane, browse to **Administration > Department:** *Department Name* > **Email > Accounts**.

2. In the List pane, select an existing email account.
3. In the Properties pane toolbar, click the **Test Connection** button to test the validity of the account. If the email account is valid, the following message pops up: `Connection established successfully`. If the account is rendered invalid, an error message is shown.


Removing linked Aliases from Email Accounts

To delete an email account, it is imperative to remove linked email aliases. When email aliases are removed from an email account, any aliases that are moved from basic authentication to OAuth authentication, are converted back to basic authentication. These aliases become available in the Aliases list in an inactive state. The newly added OAuth authenticated aliases are deleted permanently.

You cannot delete an email account, if an alias added to the email account:

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


To remove an alias from an email account:

1. In the Tree pane, browse to **Administration > Department:** *Department Name* > **Email > Accounts**.
2. In the List pane, select the email account for which you want to remove the email aliases.
3. In the Properties pane, under the Email Address tab, click the **Delete**  button to delete the email aliases you want to remove.
4. You are prompted to confirm the deletion. Click **OK**.

Deleting Email Accounts

You can delete email accounts only after removing all linked email aliases from the account. For more information, see [“Removing linked Aliases from Email Accounts” on page 31](#)

To delete an email account:

1. In the Tree pane, browse to **Administration > Department:** *Department Name* > **Email > Accounts**.
2. In the List pane, select the email account you want to delete.
3. In the list pane toolbar, click the **Delete**  button.
4. You are prompted to confirm the deletion. Click **OK** to delete the email account.



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 department settings for this feature to work.


- ▶ Block all attachments
- ▶ Action on blocked attachments

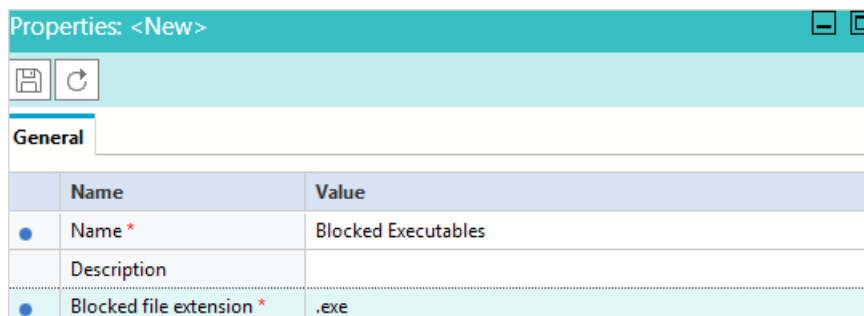
For more information on working with settings, see the Settings chapter in the *Enterprise Chat and Email Administrator's Guide to Administration Console*.

Be aware that any file types that are blocked or allowed in the Attachments settings at the partition level supercede the blocked file extension rules set at the department level. For more information, see the *Enterprise Chat and Email 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`.



	Name	Value
<input checked="" type="radio"/>	Name *	Blocked Executables
<input type="radio"/>	Description	
<input checked="" type="radio"/>	Blocked file extension *	.exe


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 extension.

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 *Enterprise Chat and Email 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 *Enterprise Chat and Email 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.

Address-type delivery exceptions work by checking the part of the email address before the “at” @ character and excludes the “at” @ character. For example, administrators can configure the term, ‘postmaster’ as an address-type delivery exception. This would then be compared against the from email address of the incoming email and checked. For example, email addresses such as `postmaster@abc.com` and `mail-postmaster.xyz@abc.com` would be confirmed as delivery exceptions while `exception@postmaster.com` would not.

The application 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 41](#).

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.



Important: The “at” @ character must not be included in the exception phrase.

- **Failure:** Select the type of failure from the dropdown list. The options available are:
 - Permanent
 - Temporary

	Name	Value
●	Name *	Automated Response
	Description	
●	Type *	Subject
●	Phrase *	Automated 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