# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is Amazon WorkMail?</td>
<td>1</td>
</tr>
<tr>
<td>Amazon WorkMail system requirements</td>
<td>1</td>
</tr>
<tr>
<td>Amazon WorkMail concepts</td>
<td>1</td>
</tr>
<tr>
<td>Related AWS services</td>
<td>2</td>
</tr>
<tr>
<td>Amazon WorkMail pricing</td>
<td>3</td>
</tr>
<tr>
<td>Resources</td>
<td>3</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>4</td>
</tr>
<tr>
<td>Sign up for an AWS account</td>
<td>4</td>
</tr>
<tr>
<td>Create an administrative user</td>
<td>4</td>
</tr>
<tr>
<td>Grant IAM users permissions for Amazon WorkMail</td>
<td>5</td>
</tr>
<tr>
<td>Security</td>
<td>6</td>
</tr>
<tr>
<td>Data protection</td>
<td>6</td>
</tr>
<tr>
<td>How Amazon WorkMail uses AWS KMS</td>
<td>7</td>
</tr>
<tr>
<td>Identity and access management</td>
<td>13</td>
</tr>
<tr>
<td>Audience</td>
<td>14</td>
</tr>
<tr>
<td>Authenticating With identities</td>
<td>14</td>
</tr>
<tr>
<td>Managing access using policies</td>
<td>16</td>
</tr>
<tr>
<td>How Amazon WorkMail works with IAM</td>
<td>17</td>
</tr>
<tr>
<td>Identity-based policy examples</td>
<td>21</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>25</td>
</tr>
<tr>
<td>AWS managed policies</td>
<td>26</td>
</tr>
<tr>
<td>AmazonWorkMailFullAccess</td>
<td>27</td>
</tr>
<tr>
<td>AmazonWorkMailReadOnlyAccess</td>
<td>27</td>
</tr>
<tr>
<td>AmazonWorkMailEventsServiceRolePolicy</td>
<td>27</td>
</tr>
<tr>
<td>Policy updates</td>
<td>27</td>
</tr>
<tr>
<td>Using service-linked roles</td>
<td>27</td>
</tr>
<tr>
<td>Service-linked role permissions for Amazon WorkMail</td>
<td>28</td>
</tr>
<tr>
<td>Creating a service-linked role for Amazon WorkMail</td>
<td>28</td>
</tr>
<tr>
<td>Editing a service-linked role for Amazon WorkMail</td>
<td>28</td>
</tr>
<tr>
<td>Deleting a service-linked role for Amazon WorkMail</td>
<td>28</td>
</tr>
<tr>
<td>Supported Regions for Amazon WorkMail service-linked roles</td>
<td>29</td>
</tr>
<tr>
<td>Logging and monitoring</td>
<td>29</td>
</tr>
<tr>
<td>Monitoring with CloudWatch</td>
<td>30</td>
</tr>
<tr>
<td>Logging Amazon WorkMail API calls with AWS CloudTrail</td>
<td>37</td>
</tr>
<tr>
<td>Enabling event logging</td>
<td>40</td>
</tr>
<tr>
<td>Compliance validation</td>
<td>42</td>
</tr>
<tr>
<td>Resilience</td>
<td>43</td>
</tr>
<tr>
<td>Infrastructure security</td>
<td>43</td>
</tr>
<tr>
<td>Getting started</td>
<td>44</td>
</tr>
<tr>
<td>Getting started with Amazon WorkMail console</td>
<td>44</td>
</tr>
<tr>
<td>Step 1: Sign in to the Amazon WorkMail console</td>
<td>44</td>
</tr>
<tr>
<td>Step 2: Set up your Amazon WorkMail site</td>
<td>45</td>
</tr>
<tr>
<td>Step 3: Set up Amazon WorkMail user access</td>
<td>45</td>
</tr>
<tr>
<td>More resources</td>
<td>46</td>
</tr>
<tr>
<td>Migrating to Amazon WorkMail</td>
<td>46</td>
</tr>
<tr>
<td>Step 1: Create or enable users in Amazon WorkMail</td>
<td>46</td>
</tr>
<tr>
<td>Step 2: Migrate to Amazon WorkMail</td>
<td>46</td>
</tr>
<tr>
<td>Step 3: Complete the migration to Amazon WorkMail</td>
<td>46</td>
</tr>
<tr>
<td>Interoperability between Amazon WorkMail and Microsoft Exchange</td>
<td>47</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>47</td>
</tr>
<tr>
<td>Add domains and enable mailboxes</td>
<td>48</td>
</tr>
<tr>
<td>Enable interoperability</td>
<td>48</td>
</tr>
<tr>
<td>Create service accounts in Microsoft Exchange and Amazon WorkMail</td>
<td>48</td>
</tr>
<tr>
<td>Limitations in interoperability mode</td>
<td>49</td>
</tr>
</tbody>
</table>
Configure availability settings on Amazon WorkMail ................................................................. 49
 Configure an EWS-based availability provider ........................................................................ 49
 Configuring a Custom Availability Provider ............................................................................. 50
 Building a CAP Lambda function ................................................................................................ 51
 Configure availability settings in Microsoft Exchange ............................................................. 56
 Enable email routing between Microsoft Exchange and Amazon WorkMail users ..................... 57
 Enable email routing for a user ..................................................................................................... 57
 Post setup configuration ............................................................................................................... 58
 Mail client configuration ............................................................................................................. 58
 Disabling interoperability mode and decommissioning your mail server ..................................... 58
 Troubleshooting ......................................................................................................................... 59
 Amazon WorkMail quotas .......................................................................................................... 60
 Amazon WorkMail organization and user quotas ......................................................................... 60
 WorkMail organization setting quotas ........................................................................................ 61
 Per-user quotas ............................................................................................................................ 62
 Message quotas .......................................................................................................................... 62
 Working with organizations ........................................................................................................ 64
 Creating an organization ............................................................................................................ 64
 Creating an organization ............................................................................................................ 65
 Viewing an organization's details ................................................................................................. 66
 Integrating an Amazon WorkDocs or WorkSpaces directory ...................................................... 66
 Organization states and descriptions .............................................................................................. 66
 Deleting an organization ............................................................................................................ 67
 Working with organization settings ............................................................................................. 68
 Enabling mailbox migration ......................................................................................................... 68
 Enabling journaling ....................................................................................................................... 68
 Enabling interoperability .............................................................................................................. 68
 Enabling SMTP gateways ............................................................................................................. 68
 Managing email flows ............................................................................................................... 69
 Enforcing DMARC policies on incoming email .......................................................................... 84
 Tagging an organization ............................................................................................................. 85
 Working with access control rules ............................................................................................... 86
 Creating access control rules ....................................................................................................... 86
 Editing access control rules ......................................................................................................... 87
 Testing access control rules ......................................................................................................... 87
 Deleting access control rules ....................................................................................................... 88
 Setting mailbox retention policies ............................................................................................... 88
 Working with domains ............................................................................................................... 90
 Adding a domain ......................................................................................................................... 90
 Removing a domain .................................................................................................................... 93
 Choosing the default domain ...................................................................................................... 93
 Verifying domains ....................................................................................................................... 93
 Verifying TXT records and MX records with your DNS service .................................................. 94
 Troubleshooting domain verification .......................................................................................... 96
 Enabling AutoDiscover to configure endpoints .......................................................................... 97
 AutoDiscover phase 2 troubleshooting ...................................................................................... 99
 Editing domain identity policies ................................................................................................ 100
 Custom Amazon SES service-principal policy .......................................................................... 101
 Authenticating email with SPF .................................................................................................... 102
 Configuring a custom MAIL FROM domain .............................................................................. 102
 Working with users .................................................................................................................... 103
 Managing user accounts ........................................................................................................... 103
 Creating users ............................................................................................................................ 103
 Enabling existing users .............................................................................................................. 104
 Disabling user accounts ............................................................................................................. 104
 Editing user email addresses ...................................................................................................... 105
 Editing user details ..................................................................................................................... 105
Amazon WorkMail Administrator Guide

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resetting user passwords</td>
<td>107</td>
</tr>
<tr>
<td>Troubleshooting Amazon WorkMail password policies</td>
<td>107</td>
</tr>
<tr>
<td>Viewing email headers</td>
<td>108</td>
</tr>
<tr>
<td>Working with notifications</td>
<td>108</td>
</tr>
<tr>
<td>Enabling signed or encrypted email</td>
<td>111</td>
</tr>
<tr>
<td>Working with groups</td>
<td>112</td>
</tr>
<tr>
<td>Create a group</td>
<td>112</td>
</tr>
<tr>
<td>Enabling a group</td>
<td>113</td>
</tr>
<tr>
<td>Adding users as members to a group</td>
<td>113</td>
</tr>
<tr>
<td>Removing users from a group</td>
<td>114</td>
</tr>
<tr>
<td>Disable a group</td>
<td>114</td>
</tr>
<tr>
<td>Deleting a group</td>
<td>115</td>
</tr>
<tr>
<td>Working with resources</td>
<td>116</td>
</tr>
<tr>
<td>Creating a resource</td>
<td>116</td>
</tr>
<tr>
<td>Editing resource details</td>
<td>116</td>
</tr>
<tr>
<td>Disabling a resource</td>
<td>118</td>
</tr>
<tr>
<td>Enabling a resource</td>
<td>118</td>
</tr>
<tr>
<td>Deleting a resource</td>
<td>119</td>
</tr>
<tr>
<td>Working with mobile devices</td>
<td>120</td>
</tr>
<tr>
<td>Editing your organization's mobile device policy</td>
<td>120</td>
</tr>
<tr>
<td>Managing mobile devices</td>
<td>121</td>
</tr>
<tr>
<td>Remotely wiping mobile devices</td>
<td>121</td>
</tr>
<tr>
<td>Removing user devices from the devices list</td>
<td>121</td>
</tr>
<tr>
<td>Viewing mobile device details</td>
<td>122</td>
</tr>
<tr>
<td>Managing mobile device access rules</td>
<td>122</td>
</tr>
<tr>
<td>How mobile device access rules work</td>
<td>123</td>
</tr>
<tr>
<td>Using mobile device access rules</td>
<td>124</td>
</tr>
<tr>
<td>Managing mobile device access overrides</td>
<td>125</td>
</tr>
<tr>
<td>How mobile device access overrides work</td>
<td>125</td>
</tr>
<tr>
<td>Managing overrides</td>
<td>125</td>
</tr>
<tr>
<td>Integrating with mobile device management solutions</td>
<td>126</td>
</tr>
<tr>
<td>Mobile device management solutions overview</td>
<td>126</td>
</tr>
<tr>
<td>Configuring a WorkMail organization to integrate with a third-party MDM solution in direct mode</td>
<td>128</td>
</tr>
<tr>
<td>Working with mailbox permissions</td>
<td>130</td>
</tr>
<tr>
<td>About mailbox and folder permissions</td>
<td>130</td>
</tr>
<tr>
<td>Managing mailbox permissions for users</td>
<td>131</td>
</tr>
<tr>
<td>Adding permissions</td>
<td>131</td>
</tr>
<tr>
<td>Editing mailbox permissions for users</td>
<td>131</td>
</tr>
<tr>
<td>Managing mailbox permissions for groups</td>
<td>132</td>
</tr>
<tr>
<td>Programmatic access to mailboxes</td>
<td>134</td>
</tr>
<tr>
<td>Managing impersonation roles</td>
<td>134</td>
</tr>
<tr>
<td>Impersonation roles overview</td>
<td>134</td>
</tr>
<tr>
<td>Security considerations</td>
<td>135</td>
</tr>
<tr>
<td>Creating impersonation roles</td>
<td>135</td>
</tr>
<tr>
<td>Editing impersonation roles</td>
<td>136</td>
</tr>
<tr>
<td>Testing impersonation roles</td>
<td>136</td>
</tr>
<tr>
<td>Deleting impersonation roles</td>
<td>137</td>
</tr>
<tr>
<td>Using impersonation roles</td>
<td>137</td>
</tr>
<tr>
<td>Exporting mailbox content</td>
<td>140</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>140</td>
</tr>
<tr>
<td>IAM policy examples and role creation</td>
<td>140</td>
</tr>
<tr>
<td>Example: Exporting mailbox content</td>
<td>142</td>
</tr>
<tr>
<td>Considerations</td>
<td>143</td>
</tr>
<tr>
<td>Troubleshooting mail routing issues</td>
<td>99</td>
</tr>
<tr>
<td>Using email journaling with Amazon WorkMail</td>
<td>145</td>
</tr>
<tr>
<td>Using journaling</td>
<td>145</td>
</tr>
</tbody>
</table>

Version 1.0
What is Amazon WorkMail?

Amazon WorkMail is a secure, managed business email and calendaring service with support for existing desktop and mobile email clients. Amazon WorkMail users can access their email, contacts, and calendars using Microsoft Outlook, their browser, or their native iOS and Android email applications. You can integrate Amazon WorkMail with your existing corporate directory and control both the keys that encrypt your data and the location in which your data is stored.

For a list of supported AWS Regions and endpoints, see AWS Regions and Endpoints.

Topics

- Amazon WorkMail system requirements (p. 1)
- Amazon WorkMail concepts (p. 1)
- Related AWS services (p. 2)
- Amazon WorkMail pricing (p. 3)
- Amazon WorkMail resources (p. 3)

Amazon WorkMail system requirements

Amazon WorkMail works with all major mobile devices and operating systems that support the Exchange ActiveSync protocol. Supported mobile platforms include iOS, Android, and Windows Phone. Users of macOS can add their Amazon WorkMail account to their Mail, Calendar, and Contacts apps.

If you have a valid Microsoft Outlook license, you can access Amazon WorkMail using the following versions of Microsoft Outlook:

- Outlook 2010 and Outlook 2013 Click-to-Run
- Outlook for Mac 2011, Outlook 2016 for Mac, and Outlook 2019 for Mac

The Amazon WorkMail web application is accessed at https://alias.awsapps.com/mail. Amazon WorkMail can also be used with IMAP clients. For more information, see Setting up email clients for Amazon WorkMail in the Amazon WorkMail User Guide.

Amazon WorkMail concepts

The terminology and concepts that are central to your understanding and use of Amazon WorkMail are described below.

Organization

A tenant setup for Amazon WorkMail.

Alias

A globally unique name to identify your organization. The alias is used to access the Amazon WorkMail web application (https://alias.awsapps.com/mail).
Domain

The web address that comes after the @ symbol in an email address. You can add a domain that receives mail and delivers it to mailboxes in your organization.

Test mail domain

A domain is automatically configured during setup that can be used for testing Amazon WorkMail. The test mail domain is alias.awsapps.com and is used as the default domain if you don't configure your own domain. The test mail domain is subject to different limits. For more information, see Amazon WorkMail quotas (p. 60).

Directory

An AWS Simple AD, AWS Managed AD, or AD Connector created in AWS Directory Service. If you create an organization using the Amazon WorkMail Quick setup, we create a WorkMail directory for you. You can't view a WorkMail directory in AWS Directory Service.

User

A user created in the AWS Directory Service. The user can be created in an USER or REMOTE_USER role. When a user is created and enabled with an USER role, they receive their own mailbox to access. When a user is disabled, they can't access Amazon WorkMail.

User created and enabled with a REMOTE_USER role is listed in the address book but do not get a mailbox in Amazon WorkMail. The REMOTE_USER can have the mailbox hosted outside Amazon WorkMail but will still be listed as any other user with mailbox in the Amazon WorkMail address book and can look up each others calendar to find free or busy information.

Group

A group used in AWS Directory Service. A group can be used as a distribution list or a security group in Amazon WorkMail. Groups don't have their own mailboxes.

Resource

A resource represents a meeting room or equipment resource that can be booked by Amazon WorkMail users.

Mobile device policy

Various IT policy rules that control the security features and behavior of a mobile device.

Related AWS services

The following services are used along with Amazon WorkMail:

- AWS Directory Service—You can integrate Amazon WorkMail with an existing AWS Simple AD, AWS Managed AD, or AD Connector. Create a directory in the AWS Directory Service and then enable Amazon WorkMail for this directory. After you've configured this integration, you can choose which users you would like to enable for Amazon WorkMail from a list of users in your existing directory, and users can log in using their existing Active Directory credentials. For more information, see AWS Directory Service Administration Guide.

- Amazon Simple Email Service—Amazon WorkMail uses Amazon SES to send all outgoing email. The test mail domain and your domains are available for management in the Amazon SES console. There is no cost for outgoing email sent from Amazon WorkMail. For more information, see Amazon Simple Email Service Developer Guide.

- AWS Identity and Access Management—The AWS Management Console requires your user name and password so that any service you use can determine whether you have permission to access its resources. We recommend that you avoid using AWS account credentials to access AWS because AWS account credentials can't be revoked or limited in any way. Instead, we recommend that you create an
IAM user and add the user to an IAM group with administrative permissions. You can then access the console using the IAM user credentials.

If you signed up for AWS but have not created an IAM user for yourself, you can create one using the IAM console. For more information, see Create individual IAM users in the IAM User Guide.

- **AWS Key Management Service**—Amazon WorkMail is integrated with AWS KMS for encryption of customer data. Key management can be performed from the AWS KMS console. For more information, see What is the AWS Key Management Service in the AWS Key Management Service Developer Guide.

### Amazon WorkMail pricing

With Amazon WorkMail, there are no upfront fees or commitments. You pay only for active user accounts. For more specific information about pricing, see Pricing.

### Amazon WorkMail resources

The following related resources can help you as you work with this service.

- **Classes & Workshops** – Links to role-based and specialty courses, in addition to self-paced labs to help sharpen your AWS skills and gain practical experience.
- **AWS Developer Center** – Explore tutorials, download tools, and learn about AWS developer events.
- **AWS Developer Tools** – Links to developer tools, SDKs, IDE toolkits, and command line tools for developing and managing AWS applications.
- **Getting Started Resource Center** – Learn how to set up your AWS account, join the AWS community, and launch your first application.
- **Hands-On Tutorials** – Follow step-by-step tutorials to launch your first application on AWS.
- **AWS Whitepapers** – Links to a comprehensive list of technical AWS whitepapers, covering topics such as architecture, security, and economics and authored by AWS Solutions Architects or other technical experts.
- **AWS Support Center** – The hub for creating and managing your AWS Support cases. Also includes links to other helpful resources, such as forums, technical FAQs, service health status, and AWS Trusted Advisor.
- **AWS Support** – The primary webpage for information about AWS Support, a one-on-one, fast-response support channel to help you build and run applications in the cloud.
- **Contact Us** – A central contact point for inquiries concerning AWS billing, account, events, abuse, and other issues.
- **AWS Site Terms** – Detailed information about our copyright and trademark; your account, license, and site access; and other topics.
Prerequisites

To act as an Amazon WorkMail administrator, you need an AWS account. If you haven't signed up for AWS yet, complete the following tasks to get set up.

Topics
- Sign up for an AWS account (p. 4)
- Create an administrative user (p. 4)
- Grant IAM users permissions for Amazon WorkMail (p. 5)

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an AWS account root user is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to an administrative user, and use only the root user to perform tasks that require root user access.

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing My Account.

Create an administrative user

After you sign up for an AWS account, create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the AWS Management Console as the account owner by choosing Root user and entering your AWS account email address. On the next page, enter your password.

   For help signing in by using root user, see Signing in as the root user in the AWS Sign-In User Guide.

2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the IAM User Guide.
Create an administrative user

- For your daily administrative tasks, grant administrative access to an administrative user in AWS IAM Identity Center.
  
  For instructions, see Getting started in the AWS IAM Identity Center User Guide.

Sign in as the administrative user

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.
  
  For help signing in using an IAM Identity Center user, see Signing in to the AWS access portal in the AWS Sign-In User Guide.

Grant IAM users permissions for Amazon WorkMail

By default, IAM users don't have permissions to manage Amazon WorkMail resources. You must attach an AWS managed policy (AmazonWorkMailFullAccess or AmazonWorkMailReadOnlyAccess) or create a customer-managed policy that explicitly grants IAM users those permissions. You then attach the policy to the IAM users or groups that require those permissions. For more information, see Identity and access management for Amazon WorkMail (p. 13).
Security in Amazon WorkMail

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS compliance programs. To learn about the compliance programs that apply to Amazon WorkMail, see AWS Services in Scope by Compliance Program.

- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon WorkMail. The following topics show you how to configure Amazon WorkMail to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon WorkMail resources.

Topics

- Data protection in Amazon WorkMail (p. 6)
- Identity and access management for Amazon WorkMail (p. 13)
- AWS managed policies for Amazon WorkMail (p. 26)
- Using service-linked roles for Amazon WorkMail (p. 27)
- Logging and monitoring in Amazon WorkMail (p. 29)
- Compliance validation for Amazon WorkMail (p. 42)
- Resilience in Amazon WorkMail (p. 43)
- Infrastructure security in Amazon WorkMail (p. 43)

Data protection in Amazon WorkMail

The AWS shared responsibility model applies to data protection in Amazon WorkMail. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the AWS Security Blog.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:
• Use multi-factor authentication (MFA) with each account.
• Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
• Set up API and user activity logging with AWS CloudTrail.
• Use AWS encryption solutions, along with all default security controls within AWS services.
• Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
• If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a Name field. This includes when you work with Amazon WorkMail or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

How Amazon WorkMail uses AWS KMS

Amazon WorkMail transparently encrypts all messages in the mailboxes of all Amazon WorkMail organizations before the messages are written to disk, and it transparently decrypts the messages when users access them. You can't disable encryption. To protect the encryption keys that protect the messages, Amazon WorkMail is integrated with AWS Key Management Service (AWS KMS).

Amazon WorkMail also provides an option for enabling users to send signed or encrypted email. This encryption feature does not use AWS KMS. For more information, see Enabling signed or encrypted email (p. 111).

Topics
• Amazon WorkMail encryption (p. 7)
• Authorizing use of the CMK (p. 10)
• Amazon WorkMail encryption context (p. 11)
• Monitoring Amazon WorkMail interaction with AWS KMS (p. 12)

Amazon WorkMail encryption

In Amazon WorkMail, each organization can contain multiple mailboxes, one for each user in the organization. All messages, including email and calendar items, are stored in the user's mailbox.

To protect the contents of the mailboxes in your Amazon WorkMail organizations, Amazon WorkMail encrypts all mailbox messages before they are written to disk. No customer-provided information is stored in plaintext.

Each message is encrypted under a unique data encryption key. The message key is protected by a mailbox key, which is a unique encryption key that is used only for that mailbox. The mailbox key is encrypted under an AWS KMS customer master key (CMK) for the organization that never leaves AWS KMS unencrypted. The following diagram shows the relationship of the encrypted messages, encrypted message keys, encrypted mailbox key, and the CMK for the organization in AWS KMS.
Setting a CMK for the organization

When you create an Amazon WorkMail organization, you have the option to select an AWS KMS customer master key (CMK) for the organization. This CMK protects all mailbox keys in that organization.

You can select the default AWS managed CMK for Amazon WorkMail, or you can select an existing customer managed CMK that you own and manage. For more information, see customer master keys (CMKs) in the AWS Key Management Service Developer Guide. You can select the same CMK or a different CMK for each of your organizations, but you cannot change the CMK once you select it.

Important
Amazon WorkMail supports only symmetric CMKs. You cannot use an asymmetric CMK. For help determining whether a CMK is symmetric or asymmetric, see Identifying symmetric and asymmetric CMKs in the AWS Key Management Service Developer Guide.

To find the CMK for your organization, use the AWS CloudTrail log entry that records calls to AWS KMS.

A unique encryption key for each mailbox

When you create a mailbox, Amazon WorkMail generates a unique 256-bit Advanced Encryption Standard (AES) symmetric encryption key for the mailbox, known as its mailbox key, outside of AWS KMS. Amazon WorkMail uses the mailbox key to protect the encryption keys for each message in the mailbox.

To protect the mailbox key, Amazon WorkMail calls AWS KMS to encrypt the mailbox key under the CMK for the organization. Then it stores the encrypted mailbox key in the mailbox metadata.
Note
Amazon WorkMail uses a symmetric mailbox encryption key to protect message keys. Previously, Amazon WorkMail protected each mailbox with an asymmetric key pair. It used the public key to encrypt each message key and the private key to decrypt it. The private mailbox key was protected by the CMK for the organization. Older mailboxes may use an asymmetric mailbox key pair. This change does not affect the security of the mailbox or its messages.

Encrypting each message
When a user adds a message to a mailbox, Amazon WorkMail generates a unique 256-bit AES symmetric encryption key for the message outside of AWS KMS. It uses this message key to encrypt the message. Amazon WorkMail encrypts the message key under the mailbox key and stores the encrypted message key with the message. Then, it encrypts the mailbox key under the CMK for the organization.

Creating a new mailbox
When Amazon WorkMail creates a mailbox, it uses the following process to prepare the mailbox to hold encrypted messages.

- Amazon WorkMail generates a unique 256-bit AES symmetric encryption key for the mailbox outside of AWS KMS.
- Amazon WorkMail calls the AWS KMS Encrypt operation. It passes in the mailbox key and the identifier of the customer master key (CMK) for the organization. AWS KMS returns a ciphertext of the mailbox key encrypted under the CMK.
- Amazon WorkMail stores the encrypted mailbox key with the mailbox metadata.

Encrypting a mailbox message
To encrypt a message, Amazon WorkMail uses the following process.

1. Amazon WorkMail generates a unique 256-bit AES symmetric key for the message. It uses the plaintext message key and the Advanced Encryption Standard (AES) algorithm to encrypt the message outside of AWS KMS.
2. To protect the message key under the mailbox key, Amazon WorkMail needs to decrypt the mailbox key, which is always stored in its encrypted form.
   - Amazon WorkMail calls the AWS KMS Decrypt operation and passes in the encrypted mailbox key. AWS KMS uses the CMK for the organization to decrypt the mailbox key and it returns the plaintext mailbox key to Amazon WorkMail.
3. Amazon WorkMail uses the plaintext mailbox key and the Advanced Encryption Standard (AES) algorithm to encrypt the message key outside of AWS KMS.
4. Amazon WorkMail stores the encrypted message key in the metadata of the encrypted message so it is available to decrypt it.

Decrypting a mailbox message
To decrypt a message, Amazon WorkMail uses the following process.

1. Amazon WorkMail calls the AWS KMS Decrypt operation and passes in the encrypted mailbox key. AWS KMS uses the CMK for the organization to decrypt the mailbox key and it returns the plaintext mailbox key to Amazon WorkMail.
2. Amazon WorkMail uses the plaintext mailbox key and the Advanced Encryption Standard (AES) algorithm to decrypt the encrypted message key outside of AWS KMS.
3. Amazon WorkMail uses the plaintext message key to decrypt the encrypted message.
Caching mailbox keys

To improve performance and minimize calls to AWS KMS, Amazon WorkMail caches each plaintext mailbox key for each client locally for up to one minute. At the end of the caching period, the mailbox key is removed. If the mailbox key for that client is required during the caching period, Amazon WorkMail can get it from the cache instead of calling AWS KMS. The mailbox key is protected in the cache and is never written to disk in plaintext.

Authorizing use of the CMK

When Amazon WorkMail uses a customer master key (CMK) in cryptographic operations, it acts on behalf of the mailbox administrator.

To use the AWS KMS customer master key (CMK) for a secret on your behalf, the administrator must have the following permissions. You can specify these required permissions in an IAM policy or key policy.

- `kms:Encrypt`
- `kms:Decrypt`
- `kms:CreateGrant`

To allow the CMK to be used only for requests that originate in Amazon WorkMail, you can use the `kmsViaService` condition key with the `workmail.<region>.amazonaws.com` value.

You can also use the keys or values in the encryption context (p. 11) as a condition for using the CMK for cryptographic operations. For example, you can use a string condition operator in an IAM or key policy document or use a grant constraint in a grant.

Key policy for the AWS managed CMK

The key policy for the AWS managed CMK for Amazon WorkMail gives users permission to use the CMK for specified operations only when Amazon WorkMail makes the request on the user's behalf. The key policy does not allow any user to use the CMK directly.

This key policy, like the policies of all AWS managed keys, is established by the service. You can't change the key policy, but you can view it at any time. For details, see Viewing a key policy in the AWS Key Management Service Developer Guide.

The policy statements in the key policy have the following effect:

- Allow users in the account and Region to use the CMK for cryptographic operations and to create grants, but only when the request comes from Amazon WorkMail on their behalf. The `kms:ViaService` condition key enforces this restriction.
- Allows the AWS account to create IAM policies that allow users to view CMK properties and revoke grants.

The following is a key policy for an example AWS managed CMK for Amazon WorkMail.

```json
{
  "Version": "2012-10-17",
  "Id": "auto-workmail-1",
  "Statement": [
    {
      "Sid": "Allow access through WorkMail for all principals in the account that are authorized to use WorkMail",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      }
    }
  ]
}
```
How Amazon WorkMail uses AWS KMS

Using grants to authorize Amazon WorkMail

In addition to key policies, Amazon WorkMail uses grants to add permissions to the CMK for each organization. To view the grants on the CMK in your account, use the `ListGrants` operation.

Amazon WorkMail uses grants to add the following permissions to the CMK for the organization.

- Add the `kms:Encrypt` permission to allow Amazon WorkMail to encrypt the mailbox key.
- Add the `kms:Decrypt` permission to allow Amazon WorkMail to use the CMK to decrypt the mailbox key. Amazon WorkMail requires this permission in a grant because the request to read mailbox messages uses the security context of the user who is reading the message. The request does not use the credentials of the AWS account. Amazon WorkMail creates this grant when you select a CMK for the organization.

To create the grants, Amazon WorkMail calls `CreateGrant` on behalf of the user who created the organization. Permission to create the grant comes from the key policy. This policy allows account users to call `CreateGrant` on the CMK for the organization when Amazon WorkMail makes the request on an authorized user's behalf.

The key policy also allows the account root to revoke the grant on the AWS managed key. However, if you revoke the grant, Amazon WorkMail can't decrypt the encrypted data in your mailboxes.

Amazon WorkMail encryption context

An encryption context is a set of key-value pairs that contain arbitrary nonsecret data. When you include an encryption context in a request to encrypt data, AWS KMS cryptographically binds the encryption context to the encrypted data. To decrypt the data, you must pass in the same encryption context. For more information, see Encryption context in the AWS Key Management Service Developer Guide.

Amazon WorkMail uses the same encryption context format in all AWS KMS cryptographic operations. You can use the encryption context to identify a cryptographic operation in audit records and logs, such as AWS CloudTrail, and as a condition for authorization in policies and grants.

In its `Encrypt` and `Decrypt` requests to AWS KMS, Amazon WorkMail uses an encryption context where the key is `aws:workmail:arn` and the value is the Amazon Resource Name (ARN) of the organization.


For example, the following encryption context includes an example organization ARN in the Europe (Ireland) (eu-west-1) Region.
Monitoring Amazon WorkMail interaction with AWS KMS

You can use AWS CloudTrail and Amazon CloudWatch Logs to track the requests that Amazon WorkMail sends to AWS KMS on your behalf.

Encrypt

When you create a mailbox, Amazon WorkMail generates a mailbox key and calls AWS KMS to encrypt the mailbox key. Amazon WorkMail sends an `Encrypt` request to AWS KMS with the plaintext mailbox key and an identifier for the CMK of the Amazon WorkMail organization.

The event that records the `Encrypt` operation is similar to the following example event. The user is the Amazon WorkMail service. The parameters include the CMK ID (keyId) and the encryption context for the Amazon WorkMail organization. Amazon WorkMail also passes in the mailbox key, but that is not recorded in the CloudTrail log.

```json
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-19T10:01:09Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/m-a123b4c5de678fg9h0ij1k2lm234no56"
        },
        "keyId": "arn:aws:kms:eu-west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    },
    "responseElements": null,
    "requestId": "76e96b96-7e24-4faf-a2d6-08ded23ef6c",
    "eventID": "d5a59c78-128a-4082-aa5b-729f7734626a",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
        },
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "d08e60f1-097e-4a00-b7e9-10bc3872d50c"
}
```

Decrypt

When you add, view, or delete a mailbox message, Amazon WorkMail asks AWS KMS to decrypt the mailbox key. Amazon WorkMail sends a `Decrypt` request to AWS KMS with the encrypted mailbox key and an identifier for the CMK of the Amazon WorkMail organization.
The event that records the Decrypt operation is similar to the following example event. The user is the Amazon WorkMail service. The parameters include the encrypted mailbox key (as a ciphertext blob), which is not recorded in the log, and the encryption context for the Amazon WorkMail organization. AWS KMS derives the ID of the CMK from the ciphertext.

{  
  "eventVersion": "1.05",  
  "userIdentity": {  
    "type": "AWS:Service",  
    "invokedBy": "workmail.eu-west-1.amazonaws.com"  
  },  
  "eventTime": "2019-02-20T11:51:10Z",  
  "eventName": "Decrypt",  
  "awsRegion": "eu-west-1",  
  "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",  
  "userAgent": "workmail.eu-west-1.amazonaws.com",  
  "requestParameters": {  
    "encryptionContext": {  
      "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/m-a123b4c5de678f9h0ij1k2lm234no56"  
    }  
  },  
  "responseElements": null,  
  "requestID": "4a32dda1-34d9-4100-9718-674b8e0782c9",  
  "eventID": "ea9fd966-98e9-4b7b-b377-6e5a397a71de",  
  "readOnly": true,  
  "resources": [  
    {  
      "ARN": "arn:aws:kms:eu-west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",  
      "accountId": "111122223333",  
      "type": "AWS::KMS::Key"  
    }  
  ],  
  "eventType": "AwsApiCall",  
  "recipientAccountId": "111122223333",  
  "sharedEventID": "241e1e5b-ff64-427a-a5b3-7949164d0214"  
}

Identity and access management for Amazon WorkMail

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be authenticated (signed in) and authorized (have permissions) to use Amazon WorkMail resources. IAM is an AWS service that you can use with no additional charge.

Topics

- Audience (p. 14)
- Authenticating With identities (p. 14)
- Managing access using policies (p. 16)
- How Amazon WorkMail works with IAM (p. 17)
- Amazon WorkMail identity-based policy examples (p. 21)
- Troubleshooting Amazon WorkMail identity and access (p. 25)
Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Amazon WorkMail.

**Service user** – If you use the Amazon WorkMail service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon WorkMail features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Amazon WorkMail, see *Troubleshooting Amazon WorkMail identity and access* (p. 25).

**Service administrator** – If you're in charge of Amazon WorkMail resources at your company, you probably have full access to Amazon WorkMail. It's your job to determine which Amazon WorkMail features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon WorkMail, see *How Amazon WorkMail works with IAM* (p. 17).

**IAM administrator** – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon WorkMail. To view example Amazon WorkMail identity-based policies that you can use in IAM, see *Amazon WorkMail identity-based policy examples* (p. 21).

Authenticating With identities

Authentication is how you sign in to AWS using your identity credentials. You must be **authenticated** (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see *How to sign in to your AWS account* in the AWS Sign-In User Guide.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see *Signing AWS API requests* in the IAM User Guide.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see *Multi-factor authentication* in the AWS IAM Identity Center User Guide and *Using multi-factor authentication (MFA) in AWS* in the IAM User Guide.

AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see *Tasks that require root user credentials* in the IAM User Guide.
IAM users and groups

An **IAM user** is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the IAM User Guide.

An **IAM group** is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named IAMadmins and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to create an IAM user (instead of a role) in the IAM User Guide.

IAM roles

An **IAM role** is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM roles in the IAM User Guide.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Creating a role for a third-party Identity Provider in the IAM User Guide. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the AWS IAM Identity Center User Guide.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the IAM User Guide.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
- **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see Actions, Resources, and Condition Keys for Amazon WorkMail in the Service Authorization Reference.
- **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the IAM User Guide.
• **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

• **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](https://docs.aws.amazon.com/IAM/latest/UserGuide/id实例-profiles.html) in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see [When to create an IAM role (instead of a user)](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use.html) in the *IAM User Guide*.

### Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see [Overview of JSON policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_policies_overview.html) in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on **what resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the *iam:GetRole* action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

### Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_policies.html) in the *IAM User Guide*.

Identity-based policies can be further categorized as **inline policies** or **managed policies**. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see [Choosing between managed policies and inline policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_policies_createinline.html) in the *IAM User Guide*.

### Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM **role trust policies** and Amazon S3 **bucket policies**. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must **specify a principal** in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.
Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

**Access Control Lists (ACLs)**

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see [Access control list (ACL) overview](https://docs.aws.amazon.com/AmazonS3/latest/userguide/acl-overview.html) in the *Amazon Simple Storage Service Developer Guide*.

**Other policy types**

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the Principal field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see [Permissions boundaries for IAM entities](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_policies_permissions_boundaries.html) in the *IAM User Guide*.

- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see [How SCPs work](https://docs.aws.amazon.com/AWSOrganizations/latest/userguide/what-is-organization-control-policy.html) in the *AWS Organizations User Guide*.

- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see [Session policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_ses-prof-sessions.html) in the *IAM User Guide*.

**Multiple policy types**

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see [Policy evaluation logic](https://docs.aws.amazon.com/IAM/latest/UserGuide/evaluating-a-policy.html) in the *IAM User Guide*.

**How Amazon WorkMail works with IAM**

Before you use IAM to manage access to Amazon WorkMail, you should understand what IAM features are available to use with Amazon WorkMail. To get a high-level view of how Amazon WorkMail and other AWS services work with IAM, see [AWS services that work with IAM](https://docs.aws.amazon.com/IAM/latest/UserGuide/services-supported-iam-features.html) in the *IAM User Guide*.

**Topics**

- [Amazon WorkMail identity-based policies](https://docs.aws.amazon.com/workmail/latest/adminGuide/amazon-workmail-identity-based-policies.html) (p. 18)
- [Amazon WorkMail resource-based policies](https://docs.aws.amazon.com/workmail/latest/adminGuide/amazon-workmail-resource-based-policies.html) (p. 20)
- Authorization based on Amazon WorkMail tags (p. 20)
- [Amazon WorkMail IAM roles](https://docs.aws.amazon.com/workmail/latest/adminGuide/amazon-workmail-iam-roles.html) (p. 21)
Amazon WorkMail identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. Amazon WorkMail supports specific actions, resources, and condition keys. To learn about all of the elements that you use in a JSON policy, see IAM JSON Policy Elements Reference in the IAM User Guide.

Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

The Action element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as permission-only actions that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called dependent actions.

Include actions in a policy to grant permissions to perform the associated operation.

Policy actions in Amazon WorkMail use the following prefix before the action: workmail:. For example, to grant someone permission to retrieve a list of users with the Amazon WorkMail ListUsers API operation, you include the workmail:ListUsers action in their policy. Policy statements must include either an Action or NotAction element. Amazon WorkMail defines its own set of actions that describe tasks that you can perform with this service.

To specify multiple actions in a single statement, separate them with commas as follows:

```
"Action": [
   "workmail:ListUsers",
   "workmail:DeleteUser"
]
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word List, include the following action:

```
"Action": "workmail:List*"
```

To see a list of Amazon WorkMail actions, see Actions defined by Amazon WorkMail in the IAM User Guide.

Resources

Administrators can use AWS JSON policies to specify who has access to what. That is, which principal can perform actions on what resources, and under what conditions.

The Resource JSON policy element specifies the object or objects to which the action applies. Statements must include either a Resource or a NotResource element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as resource-level permissions.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

Amazon WorkMail supports resource-level permissions for Amazon WorkMail organizations.
The Amazon WorkMail organization resource has the following ARN:

```
arn:aws:workmail:${Region}:${Account}:organization/${OrganizationId}
```

For more information about the format of ARNs, see Amazon Resource Names (ARNs) and AWS service namespaces.

For example, to specify the m-n1pq2345678r901st2u3vx45x6789yza organization in your statement, use the following ARN.

```
"Resource": "arn:aws:workmail:us-east-1:111122223333:organization/m-n1pq2345678r901st2u3vx45x6789yza"
```

To specify all organizations that belong to a specific account, use the wildcard (*):

```
```

Some Amazon WorkMail actions, such as those for creating resources, can't be performed on a specific resource. In those cases, you must use the wildcard (*).

```
"Resource": "*
```

To see a list of Amazon WorkMail resource types and their ARNs, see Resources defined by Amazon WorkMail in the IAM User Guide. To learn with which actions you can specify for the ARN of each resource, see Actions, resources, and condition keys for Amazon WorkMail.

### Condition keys

Amazon WorkMail supports the following global condition keys.

- aws:CurrentTime
- aws:EpochTime
- aws:MultiFactorAuthAge
- aws:MultiFactorAuthPresent
- aws:PrincipalOrgID
- aws:PrincipalArn
- aws:RequestedRegion
- aws:SecureTransport
- aws:UserAgent

The following example policy grants access to the Amazon WorkMail console only from MFA authenticated IAM principals in the eu-west-1 AWS Region.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ses:Describe*",
                "ses:Get*",
                "workmail:Describe*",
                "workmail:Get*",
                "workmail:List*",
                "workmail:Search*"
            ]
        }
    ]
}
```
To see all AWS global condition keys, see [AWS global condition context keys](https://docs.aws.amazon.com/IAM/latest/UserGuide/aws-contextkeys.html) in the IAM User Guide.

`workmail:ImpersonationRoleId` is the only service-specific condition key supported by Amazon WorkMail.

The following example policy scopes-down `AssumeImpersonationRole` action to a particular WorkMail organization and impersonation role:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workmail:AssumeImpersonationRole"
      ],
      "Resource": "arn:aws:workmail:us-east-1:111122223333:organization/m-n1pq2345678r901st2u3vx45x6789yza",
      "Condition": {
        "StringEquals": {
          "workmail:ImpersonationRoleId": "12345678-1234-1234-1234-123456789012"
        }
      }
    }
  ]
}
```

**Examples**

To view examples of Amazon WorkMail identity-based policies, see [Amazon WorkMail identity-based policy examples](https://docs.aws.amazon.com/workmail/latest/identity-based-policy-reference.html) (p. 21).

**Amazon WorkMail resource-based policies**

Amazon WorkMail does not support resource-based policies.

**Authorization based on Amazon WorkMail tags**

You can attach tags to Amazon WorkMail resources or pass tags in a request to Amazon WorkMail. To control access based on tags, you provide tag information in the condition element of a policy using the
aws:ResourceTag/key-name, aws:RequestTag/key-name, or aws:TagKeys condition keys. For more information about tagging Amazon WorkMail resources, see Tagging an organization (p. 85).

Amazon WorkMail IAM roles

An IAM role is an entity within your AWS account that has specific permissions.

Using temporary credentials with Amazon WorkMail

You can use temporary credentials to sign in with federation, assume an IAM role, or to assume a cross-account role. You obtain temporary security credentials by calling AWS STS API operations such as AssumeRole or GetFederationToken.

Amazon WorkMail supports using temporary credentials.

Service-linked roles

Service-linked roles allow AWS services to access resources in other services to complete an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view but not edit the permissions for service-linked roles.

Amazon WorkMail supports service-linked roles. For details about creating or managing Amazon WorkMail service-linked roles, see Using service-linked roles for Amazon WorkMail (p. 27).

Service roles

This feature allows a service to assume a service role on your behalf. This role allows the service to access resources in other services to complete an action on your behalf. Service roles appear in your IAM account and are owned by the account. This means that an IAM administrator can change the permissions for this role. However, doing so might break the functionality of the service.

Amazon WorkMail supports service roles.

Amazon WorkMail identity-based policy examples

By default, IAM users and roles don’t have permission to create or modify Amazon WorkMail resources. They also can’t perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see Creating policies on the JSON tab in the IAM User Guide.

Topics

- Policy best practices (p. 21)
- Using the Amazon WorkMail console (p. 22)
- Allow users to view their own permissions (p. 24)
- Allow users read-only access to Amazon WorkMail resources (p. 24)

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Amazon WorkMail resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:
Amazon WorkMail Administrator Guide

Identity-based policy examples

• **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the **AWS managed policies** that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see [AWS managed policies](https://docs.aws.amazon.com/iam/latest/UserGuide/awsmanagedpolicies.html) or [AWS managed policies for job functions](https://docs.aws.amazon.com/iam/latest/UserGuide/aws-m南海g-policies-for-job-functions.html) in the IAM User Guide.

• **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as **least-privilege permissions**. For more information about using IAM to apply permissions, see [Policies and permissions in IAM](https://docs.aws.amazon.com/iam/latest/UserGuide/policies-and-permissions-in-iam.html) in the IAM User Guide.

• **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see [IAM JSON policy elements: Condition](https://docs.aws.amazon.com/iam/latest/UserGuide/iam-policies-conditions.html) in the IAM User Guide.

• **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see [IAM Access Analyzer policy validation](https://docs.aws.amazon.com/iam/latest/UserGuide/iam-access-analyzer-policy-validation.html) in the IAM User Guide.

• **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see [Configuring MFA-protected API access](https://docs.aws.amazon.com/iam/latest/UserGuide/configuring-mfa-protected-api-access.html) in the IAM User Guide.


**Using the Amazon WorkMail console**

To access the Amazon WorkMail console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon WorkMail resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won’t function as intended for entities (IAM users or roles) with that policy.

To ensure that those entities can still use the Amazon WorkMail console, also attach the following **AWS managed policy**, **AmazonWorkMailFullAccess**, to the entities. For more information, see [Adding permissions to a user](https://docs.aws.amazon.com/iam/latest/UserGuide/add-permissions-to-a-user.html) in the IAM User Guide.

The **AmazonWorkMailFullAccess** policy grants an IAM user full access to Amazon WorkMail resources. This policy gives the user access to all Amazon WorkMail, AWS Key Management Service, Amazon Simple Email Service, and AWS Directory Service operations. This also includes several Amazon EC2 operations that Amazon WorkMail needs to perform on your behalf. The logs and cloudwatch permissions are required for email event logging and viewing metrics in the Amazon WorkMail console. For more information, see [Logging and monitoring in Amazon WorkMail](https://docs.aws.amazon.com/workmail/latest/userguide/logging-monitoring.html) (p. 29).

```
{
  "Version": "2012-10-17",
  "Statement": [ 
    { 
      "Effect": "Allow",
      "Action": [ 
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
      ]
    }
  ]
}
```

Version 1.0

22
Identity-based policy examples

```
"ds:CreateIdentityPoolDirectory",
"ds:DeleteAlias",
"ds:DeleteDirectory",
"ds:DescribeDirectories",
"ds:GetDirectoryLimits",
"ds:ListAuthorizedApplications",
"ds:UnauthorizeApplication",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateNetworkInterface",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",
"ec2:CreateTags",
"ec2:CreateVpc",
"ec2:DeleteSecurityGroup",
"ec2:DeleteSubnet",
"ec2:DeleteVpc",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeRouteTables",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"kms:DescribeKey",
"kms:ListAliases",
"lambda:ListFunctions",
"route53:ChangeResourceRecordSets",
"route53:ListHostedZones",
"route53:ListResourceRecordSets",
"route53domains:CheckDomainAvailability",
"route53domains:ListDomains",
"ses:*",
"workmail:*",
"iam:ListRoles",
"logs:DescribeLogGroups",
"logs:CreateLogGroup",
"logs:Put RetentionPolicy",
"cloudwatch:GetMetricData"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "iam:CreateServiceLinkedRole",
"Resource": "*",
"Condition": {
"StringEquals": {
"iam:AWSServiceName": "events.workmail.amazonaws.com"
}
}
},
{
"Effect": "Allow",
"Action": [
"iam:DeleteServiceLinkedRole",
"iam:GetServiceLinkedRoleDeletionStatus"
],
"Resource": "arn:aws:iam::*:role/aws-service-role/events.workmail.amazonaws.com/AWSServiceRoleForAmazonWorkMailEvents*"
},
{
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::*:role/*workmail*",
"Condition": {
"StringLike": {
"iam:PolicyName": "*workmail*"
}
}
```

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that you're trying to perform.

### Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"],
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPoliciesVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

### Allow users read-only access to Amazon WorkMail resources

The following policy statement grants an IAM user read-only access to Amazon WorkMail resources. This policy gives the same level of access as the AWS managed policy `AmazonWorkMailReadOnlyAccess`. Either policy gives the user access to all of the Amazon WorkMail `Describe` operations. Access to the AWS Directory Service `DescribeDirectories` operation is needed to obtain information about your AWS Directory Service directories. Access to the Amazon SES service is needed to obtain information about the configured domains. Access to AWS Key Management Service is needed to obtain information about the used encryption keys. The logs and cloudwatch permissions are required for email event logging and viewing metrics in the Amazon WorkMail console. For more information, see [Logging and monitoring in Amazon WorkMail](p. 29).

Version 1.0
24
Troubleshooting Amazon WorkMail identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon WorkMail and IAM.

Topics

- I am not authorized to perform an action in Amazon WorkMail (p. 25)
- I am not authorized to perform iam:PassRole (p. 25)
- I want to allow people outside of my AWS account to access my Amazon WorkMail resources (p. 26)

I am not authorized to perform an action in Amazon WorkMail

If the AWS Management Console tells you that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password.

The following example error occurs when the mateojackson IAM user tries to use the console to view details about a group but does not have workmail:DescribeGroup permissions.

User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: workmail:DescribeGroup on resource: group

In this case, Mateo asks his administrator to update his policies to allow him to access the group resource using the workmail:DescribeGroup action.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the iam:PassRole action, your policies must be updated to allow you to pass a role to Amazon WorkMail.
Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named marymajor tries to use the console to perform an action in Amazon WorkMail. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

**I want to allow people outside of my AWS account to access my Amazon WorkMail resources**

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon WorkMail supports these features, see [How Amazon WorkMail works with IAM](p. 17).
- To learn how to provide access to your resources across AWS accounts that you own, see [Providing access to an IAM user in another AWS account that you own](in the [IAM User Guide](
- To learn how to provide access to your resources to third-party AWS accounts, see [Providing access to AWS accounts owned by third parties](in the [IAM User Guide](
- To learn how to provide access through identity federation, see [Providing access to externally authenticated users (identity federation)](in the [IAM User Guide](
- To learn the difference between using roles and resource-based policies for cross-account access, see [How IAM roles differ from resource-based policies](in the [IAM User Guide](

**AWS managed policies for Amazon WorkMail**

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see [AWS managed policies](in the [IAM User Guide](

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the [ReadOnlyAccess](AWS managed policy provides read-only access to all AWS services and resources.
When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the IAM User Guide.

**AWS managed policy: AmazonWorkMailFullAccess**

You can attach the AmazonWorkMailFullAccess policy to your IAM identities. This policy grants permissions that allow full access to Amazon WorkMail.

To view the permissions for this policy, see AmazonWorkMailFullAccess in the AWS Management Console.

**aws managed policy: AmazonWorkMailReadOnlyAccess**

You can attach the AmazonWorkMailReadOnlyAccess policy to your IAM identities. This policy grants permissions that allow read-only access to Amazon WorkMail.

To view the permissions for this policy, see AmazonWorkMailReadOnlyAccess in the AWS Management Console.

**AWS managed policy: AmazonWorkMailEventsServiceRolePolicy**

This policy is attached to the service-linked role named AmazonWorkMailEvents to allow access to AWS services and resources used or managed by Amazon WorkMail events. For more information, see Using service-linked roles for Amazon WorkMail (p. 27).

**Amazon WorkMail updates to AWS managed policies**

View details about updates to AWS managed policies for Amazon WorkMail since this service began tracking these changes.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon WorkMail started tracking changes</td>
<td>Amazon WorkMail started tracking changes for its AWS managed policies.</td>
<td>March 1, 2021</td>
</tr>
</tbody>
</table>

**Using service-linked roles for Amazon WorkMail**

Amazon WorkMail uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Amazon WorkMail. Service-linked roles are predefined by Amazon WorkMail and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Amazon WorkMail easier because you don’t have to manually add the necessary permissions. Amazon WorkMail defines the permissions of its service-linked roles, and unless defined otherwise, only Amazon WorkMail can assume its roles. The defined permissions include...
the trust policy and the permissions policy, and that permissions policy can't be attached to any other IAM entity.

You can delete a service-linked role only after first deleting the related resources. This protects your Amazon WorkMail resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS services that work with IAM and look for the services that have Yes in the Service-linked role column. Choose a Yes with a link to view the service-linked role documentation for that service.

**Service-linked role permissions for Amazon WorkMail**

Amazon WorkMail uses the service-linked role named AmazonWorkMailEvents – Amazon WorkMail uses this service-linked role to enable access to AWS services and resources used or managed by Amazon WorkMail events, such as monitoring email events logged by CloudWatch. For more information about enabling email event logging for Amazon WorkMail, see Enabling event logging (p. 40).

The AmazonWorkMailEvents service-linked role trusts the following services to assume the role:

- `events.workmail.amazonaws.com`

The role permissions policy allows Amazon WorkMail to complete the following actions on the specified resources:

- Action: logs:CreateLogGroup on all AWS resources
- Action: logs:CreateLogStream on all AWS resources
- Action: logs:PutLogEvents on all AWS resources

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the IAM User Guide.

**Creating a service-linked role for Amazon WorkMail**

You don't need to manually create a service-linked role. When you turn on Amazon WorkMail event logging and use the default settings in the Amazon WorkMail console, Amazon WorkMail creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you turn on Amazon WorkMail event logging and use the default settings, Amazon WorkMail creates the service-linked role for you again.

**Editing a service-linked role for Amazon WorkMail**

Amazon WorkMail does not allow you to edit the AmazonWorkMailEvents service-linked role. After you create a service-linked role, you can't change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the IAM User Guide.

**Deleting a service-linked role for Amazon WorkMail**

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored.
or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

**Note**

If the Amazon WorkMail service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

**To delete Amazon WorkMail resources used by AmazonWorkMailEvents**

1. Turn off Amazon WorkMail event logging.
   a. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
      
      If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
   b. In the navigation pane, choose Organizations, then choose the name of your organization.
   c. In the navigation pane, choose Organization settings, then choose Monitoring.
   d. For Log settings, choose Edit.
   e. Move the Enable mail events slider to the off position.
   f. Choose Save.

2. Delete the Amazon CloudWatch log group.
   b. Choose Logs.
   c. For Log Groups, select the log group to delete.
   d. For Actions, choose Delete log group.
   e. Choose Yes, Delete.

**To manually delete the service-linked role using IAM**

Use the IAM console, the AWS CLI, or the AWS API to delete the AmazonWorkMailEvents service-linked role. For more information, see Deleting a service-linked role in the IAM User Guide.

**Supported Regions for Amazon WorkMail service-linked roles**

Amazon WorkMail supports using service-linked roles in all of the Regions where the service is available. For more information, see Amazon WorkMail Regions and Endpoints.

**Logging and monitoring in Amazon WorkMail**

Monitoring your email flow is important for maintaining the health of your Amazon WorkMail organization. Monitoring the email sending activity for your organization helps protect your domain reputation. Monitoring can also help you track emails that are sent and received. For more information about how to enable email event logging, see Enabling event logging (p. 40).

AWS provides the following monitoring tools to watch Amazon WorkMail, report when something is wrong, and take automatic actions when appropriate:

- **Amazon CloudWatch** monitors your AWS resources and the applications you run on AWS in real time. For example, when you enable email event logging for Amazon WorkMail, CloudWatch can track emails sent and received for your organization. For more information about monitoring Amazon
WorkMail with CloudWatch, see Monitoring Amazon WorkMail with Amazon CloudWatch (p. 30). For more information about CloudWatch, see the Amazon CloudWatch User Guide.

- Amazon CloudWatch Logs enables you to monitor, store, and access your email event logs for Amazon WorkMail when email event logging is enabled in the Amazon WorkMail console. CloudWatch Logs can monitor information in the log files, and you can archive your log data in highly durable storage. For more information about tracking Amazon WorkMail messages using CloudWatch Logs, see Enabling event logging (p. 40). For more information about CloudWatch Logs, see the Amazon CloudWatch Logs User Guide.

- AWS CloudTrail captures API calls and related events made by or on behalf of your AWS account, and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see Logging Amazon WorkMail API calls with AWS CloudTrail (p. 37).

Topics
- Monitoring Amazon WorkMail with Amazon CloudWatch (p. 30)
- Logging Amazon WorkMail API calls with AWS CloudTrail (p. 37)
- Enabling event logging (p. 40)

Monitoring Amazon WorkMail with Amazon CloudWatch

You can monitor Amazon WorkMail using CloudWatch, which collects raw data and processes it into readable, near real-time metrics. The free metrics are stored for 15 months, so that you can access historical information and gain a better perspective on how your web application or service is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the Amazon CloudWatch User Guide.

CloudWatch metrics for Amazon WorkMail

Amazon WorkMail sends the following metrics and dimension information to CloudWatch.

The AWS/WorkMail namespace includes the following metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OrganizationEmailReceived</td>
<td>The number of emails received by your Amazon WorkMail organization. If 1 email is addressed to 10 recipients in your organization, the OrganizationEmailReceived count is 1. Units: Count</td>
</tr>
<tr>
<td>MailboxEmailDelivered</td>
<td>The number of emails delivered to individual mailboxes in your Amazon WorkMail organization. If 1 email is successfully delivered to 10 recipients in your organization, the MailboxEmailDelivered count is 10. Units: Count</td>
</tr>
<tr>
<td>IncomingEmailBounced</td>
<td>The number of incoming emails that bounced due to full mailboxes. This metric is counted for each</td>
</tr>
</tbody>
</table>
## Monitoring with CloudWatch

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IncomingEmailBounced</strong></td>
<td>The intended recipient. For example, if 1 email is sent to 10 recipients in your organization, and 2 of the recipients have full mailboxes resulting in a bounce response, the IncomingEmailBounced count is 2. Units: Count</td>
</tr>
<tr>
<td><strong>OutgoingEmailBounced</strong></td>
<td>The number of outgoing emails that could not be delivered, counted for each intended recipient. For example, if 1 email is sent to 10 recipients, and 2 emails could not be delivered, the OutgoingEmailBounced count is 2. Units: Count</td>
</tr>
<tr>
<td><strong>OutgoingEmailSent</strong></td>
<td>The number of emails successfully sent from your Amazon WorkMail organization. This metric is counted for each recipient of a successfully sent email. For example, if 1 email is sent to 10 recipients, and the email was successfully delivered to 8 of the recipients, the OutgoingEmailSent count is 8. Units: Count</td>
</tr>
</tbody>
</table>

### CloudWatch event logs for Amazon WorkMail

When you turn on email event logging for your Amazon WorkMail organization, Amazon WorkMail logs email events with CloudWatch. For more information about turning on email event logging, see [Enabling event logging](p. 40).

The following tables describe the events that Amazon WorkMail logs with CloudWatch, when the events are transmitted, and what the event fields contain.

**ORGANIZATION_EMAIL_RECEIVED**

This event is logged when your Amazon WorkMail organization receives an email message.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recipients</td>
<td>The intended recipients of the message.</td>
</tr>
<tr>
<td>sender</td>
<td>The email address of the user who sent the email message on behalf of another user. This field is set only when an email is sent on behalf of another user.</td>
</tr>
<tr>
<td>from</td>
<td>The From address, which is usually the email address of the user who sent the message. If the user sent the message as another user or on behalf of another user, this field returns the email address of the user on whose behalf the email was sent, not the email address of the actual sender.</td>
</tr>
<tr>
<td>subject</td>
<td>The email message subject.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
messageId | The SMTP message ID.
spamVerdict | Indicates whether the message is marked as spam by Amazon SES. For more information, see [Contents of Notifications for Amazon SES Email Receiving](https://docs.aws.amazon.com/AmazonSES/latest/DeveloperGuide/contents-of-notifications-for-amazon-ses-email-receiving.html) in the *Amazon Simple Email Service Developer Guide*.
dkimVerdict | Indicates whether the DomainKeys Identified Mail (DKIM) check passed. For more information, see [Contents of Notifications for Amazon SES Email Receiving](https://docs.aws.amazon.com/AmazonSES/latest/DeveloperGuide/contents-of-notifications-for-amazon-ses-email-receiving.html) in the *Amazon Simple Email Service Developer Guide*.
dmarcVerdict | Indicates whether the Domain-based Message Authentication, Reporting & Conformance (DMARC) check passed. For more information, see [Contents of Notifications for Amazon SES Email Receiving](https://docs.aws.amazon.com/AmazonSES/latest/DeveloperGuide/contents-of-notifications-for-amazon-ses-email-receiving.html) in the *Amazon Simple Email Service Developer Guide*.
dmarcPolicy | Appears only when the dmarcVerdict field contains "FAIL". Indicates the action to take on the email when the DMARC check fails (NONE, QUARANTINE, or REJECT). This is set by the owner of the sending email domain.
spfVerdict | Indicates whether the Sender Policy Framework (SPF) check passed. For more information, see [Contents of Notifications for Amazon SES Email Receiving](https://docs.aws.amazon.com/AmazonSES/latest/DeveloperGuide/contents-of-notifications-for-amazon-ses-email-receiving.html) in the *Amazon Simple Email Service Developer Guide*.
messageTimestamp | Indicates when the message is received.

**MAILBOX_EMAIL_DELIVERED**

This event is logged when a message is delivered to a mailbox in your organization. This is logged once for each mailbox to which a message is delivered, so a single ORGANIZATION_EMAIL_RECEIVED event can result in multiple MAILBOX_EMAIL_DELIVERED events.

| Field | Description |
--- | ---|
recipient | The mailbox to which the message is delivered. |
folder | The mailbox folder where the message is placed. |

**RULE_APPLIED**

This event is logged when an incoming or outgoing message triggers an email flow rule.

| Field | Description |
--- | ---|
ruleName | The name of the rule. |
# Field | Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ruleType</td>
<td>The type of rule applied (INBOUND_RULE, OUTBOUND_RULE, MAILBOX_RULE). Inbound and outbound rules apply to your Amazon WorkMail organization. Mailbox rules apply only to specified mailboxes. For more information, see Managing email flows (p. 69).</td>
</tr>
<tr>
<td>ruleActions</td>
<td>Actions taken based on the rule. Different recipients of the message might have different actions, such as a bounced email or a successfully delivered email.</td>
</tr>
<tr>
<td>targetFolder</td>
<td>Intended destination folder for a Move or Copy MAILBOX_RULE.</td>
</tr>
<tr>
<td>targetRecipient</td>
<td>Intended recipient of a Forward or Redirect MAILBOX_RULE.</td>
</tr>
</tbody>
</table>

### JOURNALING_INITIATED

This event is logged when Amazon WorkMail sends an email to the journaling address specified by your organization administrator. This is only transmitted if journaling is configured for your organization. For more information, see Using email journaling with Amazon WorkMail (p. 145).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>journalingAddress</td>
<td>The email address to which the journaling message is sent.</td>
</tr>
</tbody>
</table>

### INCOMING_EMAIL_BOUNCED

This event is logged when an incoming message can't be delivered to a target recipient. Emails can bounce for a number of reasons, such as a full target mailbox. The system logs this event once for each recipient that results in a bounced email. For example, if an incoming message is addressed to three recipients and two of them have full mailboxes, two INCOMING_EMAIL_BOUNCED events are logged.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bouncedRecipient</td>
<td>The intended recipient for which Amazon WorkMail bounced the message.</td>
</tr>
</tbody>
</table>

### OUTGOING_EMAIL_SUBMITTED

This event is logged when a user in your organization submits an email message for sending. This is logged before the message leaves Amazon WorkMail, so this event does not indicate whether the email is successfully delivered.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recipients</td>
<td>The recipients of the message as specified by the sender. Includes all recipients on the To, CC, and BCC lines.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>sender</td>
<td>The email address of the user who sent the email message on behalf of another user. This field is set only when an email is sent on behalf of another user.</td>
</tr>
<tr>
<td>from</td>
<td>The From address, which is usually the email address of the user who sent the message. If the user sent the message as another user or on behalf of another user, this field returns the email address of the user on whose behalf the email was sent, not the email address of the actual sender.</td>
</tr>
<tr>
<td>subject</td>
<td>The email message subject.</td>
</tr>
</tbody>
</table>

**OUTGOING_EMAIL_SENT**

This event is logged when an outgoing email is successfully delivered to a target recipient. This is logged once for each successful recipient, so a single OUTGOING_EMAIL_SUBMITTED can result in multiple OUTGOING_EMAIL_SENT entries.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>recipient</td>
<td>The recipient of the successfully delivered email.</td>
</tr>
<tr>
<td>sender</td>
<td>The email address of the user who sent the email message on behalf of another user. This field is set only when an email is sent on behalf of another user.</td>
</tr>
<tr>
<td>from</td>
<td>The From address, which is usually the email address of the user who sent the message. If the user sent the message as another user or on behalf of another user, this field returns the email address of the user on whose behalf the email was sent, not the email address of the actual sender.</td>
</tr>
<tr>
<td>messageId</td>
<td>The SMTP message ID.</td>
</tr>
</tbody>
</table>

**OUTGOING_EMAIL_BOUNCED**

This event is logged when an outgoing message can't be delivered to a target recipient. Emails can bounce for a number of reasons, such as a full target mailbox. The system logs a bounce for each recipient that results in a bounced email. For example, if an outgoing message is addressed to three recipients and two of them have full mailboxes, two OUTGOING_EMAIL_BOUNCED events are logged.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bouncedRecipient</td>
<td>The intended recipient for which the destination mail server bounced the message.</td>
</tr>
</tbody>
</table>

**DMARC_POLICY_APPLIED**

This event is logged when a DMARC policy is applied to an email sent to your organization.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>from</td>
<td>The From address, which is usually the email address of the user who sent the message. If the user sent the message as another user or on behalf of another user, this field returns the email address of the user on whose behalf the email was sent, not the email address of the actual sender.</td>
</tr>
<tr>
<td>recipients</td>
<td>The intended recipients of the message.</td>
</tr>
<tr>
<td>policy</td>
<td>The applied DMARC policy, indicating the action to take on the email when the DMARC check fails (NONE, QUARANTINE, or REJECT). This is the same as the dmarcPolicy field in the ORGANIZATION_EMAIL_RECEIVED event.</td>
</tr>
</tbody>
</table>

**Using CloudWatch Insights with Amazon WorkMail**

If you have turned on email event logging in the Amazon WorkMail console, you can use Amazon CloudWatch Logs Insights to query your event logs. For more information about turning on email event logging, see [Enabling event logging](#). For more information about CloudWatch Logs Insights, see [Analyze log data with CloudWatch Logs Insights](#) in the Amazon CloudWatch Logs User Guide.

The following examples demonstrate how to query CloudWatch Logs for common email events. You run these queries in the CloudWatch console. For instructions about how to run these queries, see [Tutorial: Run and modify a sample query](#) in the Amazon CloudWatch Logs User Guide.

**Example Example: See why User B did not receive an email sent by User A.**

The following code example demonstrates how to query for an outgoing email sent by User A to User B, sorted by timestamp.

```plaintext
fields @timestamp, traceId | sort @timestamp asc
| filter (event.from like /(?i)userA@example.com/ and event.eventName = "OUTGOING_EMAIL_SUBMITTED" and event.recipients.0 like /(?i)userB@example.com/)
```

This returns the sent message and trace ID. Use the trace ID in the following code example to query the event logs for the sent message.

```plaintext
fields @timestamp, event.eventName | sort @timestamp asc | filter traceId = "$TRACEID"
```

This returns the email message ID and the email events. OUTGOING_EMAIL_SENT indicates that the email was sent. OUTGOING_EMAIL_BOUNCED indicates that the email bounced. To see whether the email was received, query using the message ID in the following code example.

```plaintext
fields @timestamp, event.eventName | sort @timestamp asc | filter event.messageId like "$MESSAGEID"
```

This should also return the received message, because it has the same message ID. Use the trace ID in the following code example to query for delivery.
fields @timestamp, event.eventName
| sort @timestamp asc
| filter traceId = "$TRACEID"

This returns the delivery action and any applicable rule actions.

**Example Example: See all mail received from a user or domain**

The following code example demonstrates how to query for all mail received from a specified user.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter (event.from like '/(?i)user@example.com/' and event.eventName = "ORGANIZATION_EMAIL_RECEIVED")
```

The following code example demonstrates how to query for all mail received from a specified domain.

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter (event.from like "example.com" and event.eventName = "ORGANIZATION_EMAIL_RECEIVED")
```

**Example Example: See who sent bounced emails**

The following code example demonstrates how to query for outgoing emails that bounced, and also returns the reasons for bouncing.

```
fields @timestamp, event.destination, event.reason
| sort @timestamp desc
| filter event.eventName = "OUTGOING_EMAIL_BOUNCED"
```

The following code example demonstrates how to query for incoming emails that bounced, and also returns the bounced recipients' email addresses and the reasons for bouncing.

```
fields @timestamp, event.bouncedRecipient.emailAddress, event.bouncedRecipient.reason, event.bouncedRecipient.status
| sort @timestamp desc
| filter event.eventName = "INCOMING_EMAIL_BOUNCED"
```

**Example Example: See which domains are sending spam**

The following code example demonstrates how to query for recipients in your organization that are receiving spam.

```
stats count(*) as c by event.recipients.0
| filter (event.eventName = "ORGANIZATION_EMAIL_RECEIVED" and event.spamVerdict = "FAIL")
| sort c desc
```

The following code example demonstrates how to query for the sender of the spam emails.

```
fields @timestamp, event.recipients.0, event.sender, event.from
| sort @timestamp asc
| filter (event.spamVerdict = "FAIL")
```

**Example Example: See why an email was sent to a recipient's spam folder**

The following code example demonstrates how to query for emails identified as spam, filtered by subject.
Logging Amazon WorkMail API calls with AWS CloudTrail

Amazon WorkMail is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon WorkMail. CloudTrail captures all API calls for Amazon WorkMail as events, including calls from the Amazon WorkMail console and from code calls to the Amazon WorkMail APIs. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon WorkMail. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to Amazon WorkMail, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.
Amazon WorkMail information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Amazon WorkMail, that activity is recorded in a CloudTrail event along with other AWS service events in Event history. You can view, search, and download recent events in your AWS account. For more information, see Viewing events with CloudTrail event history.

For an ongoing record of events in your AWS account, including events for Amazon WorkMail, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple Regions
- Receiving CloudTrail log files from multiple accounts

All Amazon WorkMail actions are logged by CloudTrail and are documented in the Amazon WorkMail API Reference. For example, calls to the CreateUser, CreateAlias, and GetRawMessageContent API operations generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or IAM user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element.

Understanding Amazon WorkMail log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files are not an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the CreateUser action from the Amazon WorkMail API.

```json
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6G2EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/WMSDK",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "WMSDK"
    },
    "eventTime": "2017-12-12T17:49:59Z",
}```
Logging Amazon WorkMail API calls with AWS CloudTrail

The following example shows a CloudTrail log entry that demonstrates the CreateAlias action from the Amazon WorkMail API.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateAlias",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "alias": "aliasjamesdoe@testofconsole.awsapps.com",
    "organizationId": "m-5b1c980000EXAMPLE"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

The following example shows a CloudTrail log entry that demonstrates the GetRawMessageContent action from the Amazon WorkMail Message Flow API.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateAlias",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "alias": "aliasjamesdoe@testofconsole.awsapps.com",
    "organizationId": "m-5b1c980000EXAMPLE"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

The following example shows a CloudTrail log entry that demonstrates the GetRawMessageContent action from the Amazon WorkMail Message Flow API.

```
"eventSource": "workmail.amazonaws.com",
"eventName": "CreateUser",
"awsRegion": "us-west-2",
"sourceIPAddress": "203.0.113.12",
"userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-Bit_Server_VM/25.151-b12 java/1.8.0_151",
"requestParameters": {
  "name": "janedoe",
  "displayName": "Jane Doe",
  "organizationId": "m-5b1c980000EXAMPLE"
},
"responseElements": {
  "userId": "a3a9176d-EXAMPLE"
},
"requestID": "dec81e4a-EXAMPLE",
"eventID": "9f2f09c5-EXAMPLE",
"eventType": "AwsApiCall",
"recipientAccountId": "111111111111"
}
```

The following example shows a CloudTrail log entry that demonstrates the CreateAlias action from the Amazon WorkMail API.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateAlias",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "alias": "aliasjamesdoe@testofconsole.awsapps.com",
    "organizationId": "m-5b1c980000EXAMPLE"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

The following example shows a CloudTrail log entry that demonstrates the GetRawMessageContent action from the Amazon WorkMail Message Flow API.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateAlias",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "alias": "aliasjamesdoe@testofconsole.awsapps.com",
    "organizationId": "m-5b1c980000EXAMPLE"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```
Enabling event logging

You enable email event logging in the Amazon WorkMail console in order to track email messages for your organization. Email event logging uses an AWS Identity and Access Management service-linked role to grant permissions to publish the email event logs to Amazon CloudWatch. For more information about IAM service-linked roles, see Using service-linked roles for Amazon WorkMail (p. 27).

In the CloudWatch event logs, you can use CloudWatch search tools and metrics to track messages and troubleshoot email issues. For more information about the event logs that Amazon WorkMail sends to CloudWatch, see CloudWatch event logs for Amazon WorkMail (p. 31). For more information about CloudWatch Logs, see the Amazon CloudWatch Logs User Guide.

Topics

- Turning on email event logging (p. 40)
- Creating a custom log group and IAM role for email event logging (p. 41)
- Turning off email event logging (p. 42)

Turning on email event logging

When you turn on email event logging using the default settings, Amazon WorkMail:

- Creates an AWS Identity and Access Management service-linked role – AmazonWorkMailEvents.
- Creates a CloudWatch log group – /aws/workmail/emailevents/organization-alias.
- Sets CloudWatch log retention to 30 days.

To turn on email event logging

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, then choose the name of your organization.

3. In the navigation pane, choose Monitoring.

4. In the Log settings section, choose Edit.
5. Move the **Enable mail events** slider to the on position.
6. Do one of the following:
   - (Recommended) Choose **Use default settings**.
   - **OR**—
     - (Optional) Clear the **Use default settings**, and select a **Destination Log Group** and **IAM Role** from the lists that appear.

   **Note**
   Choose this option only if you have already created a log group and custom IAM role using the AWS CLI. For more information, see **Creating a custom log group and IAM role for email event logging** (p. 41).

7. Select **I authorize Amazon WorkMail to publish logs in my account using this configuration**.
8. Choose **Save**.

### Creating a custom log group and IAM role for email event logging

We recommend using the default settings when enabling email event logging for Amazon WorkMail. If you require a custom monitoring configuration, you can use the AWS CLI to create a dedicated log group and custom IAM role for email event logging.

#### To create a custom log group and IAM role for email event logging

1. Using the AWS CLI, create a log group in the same AWS Region as your Amazon WorkMail organization. For more information, see **create-log-group** in the **AWS CLI Command Reference**.
   ```bash
   aws --region us-east-1 logs create-log-group --log-group-name workmail-monitoring
   ```

2. Create a file containing the following policy:
   ```json
   {
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
   "Principal": {
   "Service": "events.workmail.amazonaws.com"
   },
   "Action": "sts:AssumeRole"
   }
   ]
   }
   ```

3. Using the AWS CLI, create an IAM role and attach this file as the role policy document. For more information, see **create-role** in the **AWS CLI Command Reference**.
   ```bash
   aws iam create-role --role-name workmail-monitoring-role --assume-role-policy-document file://trustpolicyforworkmail.json
   ```

   **Note**
   If you are a **WorkMailFullAccess** managed policy user, you must include the term `workmail` in the role name. This managed policy only allows you to configure email event logging using roles with workmail in the name. For more information, see **Granting a user permissions to pass a role to an AWS service** in the **IAM User Guide**.
4. Create a file containing the policy for the IAM role you created in the previous step. At minimum, the policy must grant permissions to the role to create log streams and put log events into the log group that you created in step 1.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
        }
    ]
}
```

5. Using the AWS CLI, attach the policy file to the IAM role. For more information, see `put-role-policy` in the `AWS CLI Command Reference`.

```
aws iam put-role-policy --role-name workmail-monitoring-role --policy-name workmail-permissions --policy-document file://rolepolicy.json
```

Follow the steps in the previous topic to turn on email event logging using the newly created log group and role. For more information, see Turning on email event logging (p. 40).

**Turning off email event logging**

Turn off email event logging from the Amazon WorkMail console. If you no longer need to use email event logging, we recommend that you delete the related CloudWatch log group and service-linked role as well. For more information, see Deleting a service-linked role for Amazon WorkMail (p. 28).

**To turn off email event logging**

1. Open the Amazon WorkMail console at `https://console.aws.amazon.com/workmail/`.
   
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, then choose the name of your organization.
3. In the navigation pane, choose Monitoring.
4. In the Log settings section, choose Edit.
5. Move the Enable mail events slider to the off position.
6. Choose Save.

**Compliance validation for Amazon WorkMail**

Third-party auditors assess the security and compliance of Amazon WorkMail as part of multiple AWS compliance programs. These include SOC, ISO, and C5.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.
You can download third-party audit reports using AWS Artifact. For more information, see [Downloading reports in AWS Artifact](#).

Your compliance responsibility when using Amazon WorkMail is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- **Security and Compliance Quick Start Guides** – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- **AWS Compliance Resources** – This collection of workbooks and guides might apply to your industry and location.
- **AWS Config** – This AWS service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- **AWS Security Hub** – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

### Resilience in Amazon WorkMail

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between Availability Zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see [AWS Global Infrastructure](#).

In addition to the AWS global infrastructure, Amazon WorkMail offers several features to help support your data resiliency and backup needs.

### Infrastructure security in Amazon WorkMail

**Note**

Amazon WorkMail discontinued support for Transport Layer Security (TLS) 1.0 and 1.1. If you are using TLS 1.0 or 1.1, you must upgrade the TLS version to 1.2. For more information, see [TLS 1.2 to become the minimum TLS protocol level for all AWS API endpoints](#).

As a managed service, Amazon WorkMail is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see [AWS Cloud Security](#). To design your AWS environment using the best practices for infrastructure security, see [Infrastructure Protection in Security Pillar AWS Well-Architected Framework](#).

You use AWS published API calls to access Amazon WorkMail through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.
Getting started with Amazon WorkMail

After you complete the Prerequisites (p. 4), you're ready to get started with Amazon WorkMail. For more information, see Getting started with Amazon WorkMail (p. 44).

You can learn more about migrating existing mailboxes to Amazon WorkMail, interoperability with Microsoft Exchange, and Amazon WorkMail quotas in the following sections.

Topics
- Getting started with Amazon WorkMail (p. 44)
- Migrating to Amazon WorkMail (p. 46)
- Interoperability between Amazon WorkMail and Microsoft Exchange (p. 47)
- Configure availability settings on Amazon WorkMail (p. 49)
- Configure availability settings in Microsoft Exchange (p. 56)
- Enable email routing between Microsoft Exchange and Amazon WorkMail users (p. 57)
- Enable email routing for a user (p. 57)
- Post setup configuration (p. 58)
- Mail client configuration (p. 58)
- Disabling interoperability mode and decommissioning your mail server (p. 58)
- Troubleshooting (p. 59)
- Amazon WorkMail quotas (p. 60)

Getting started with Amazon WorkMail

Whether you're a new Amazon WorkMail user or an existing user of Amazon WorkDocs or Amazon WorkSpaces, get started with Amazon WorkMail by completing the following steps.

Note
Complete the Prerequisites (p. 4) before getting started.

Topics
- Step 1: Sign in to the Amazon WorkMail console (p. 44)
- Step 2: Set up your Amazon WorkMail site (p. 45)
- Step 3: Set up Amazon WorkMail user access (p. 45)
- More resources (p. 46)

Step 1: Sign in to the Amazon WorkMail console

You must sign in to the Amazon WorkMail console before you can add users and manage their accounts and mailboxes.

To sign in to the Amazon WorkMail console

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
2. If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information about regions, see Regions and endpoints in the Amazon Web Services General Reference.

Step 2: Set up your Amazon WorkMail site

1. After you sign in to the Amazon WorkMail console, you set up your organization and add a domain. We recommend using a dedicated domain for your Amazon WorkMail organization. For more information, see Creating an organization (p. 64) and Adding a domain (p. 90).

2. (Optional) You can choose to use a free testing domain provided by Amazon WorkMail. If you choose to do this, skip to step 4.

   **Note**
   Test domains use this format: alias.awsapps.com. As you go, remember that you should only use test domains for testing. Don't use a test domain for a production environment. Also, you must have at least one enabled user in your Amazon WorkMail organization. If you don't have an enabled user, the domain can become available for registration and use by other customers.

3. If you use an external domain, verify that domain by adding the appropriate text (TXT) and mail exchange (MX) records to your Domain Name System (DNS) service. TXT records allow you to enter notes in the DNS. MX records specify the incoming mail servers. Make sure to set your domain as the default for your organization. For more information, see Verifying domains (p. 93) and Choosing the default domain (p. 93).

4. Create new users or enable your existing directory users for Amazon WorkMail. For more information, see Managing user accounts (p. 103).

5. (Optional) If you have existing Microsoft Exchange mailboxes, migrate them to Amazon WorkMail. For more information, see Migrating to Amazon WorkMail (p. 46).

After you've finished setting up your Amazon WorkMail site, you can access Amazon WorkMail using the web application URL.

**To locate your Amazon WorkMail web application URL**

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the AWS Region. To do so, open the Select a region list, located to the right of the search box, then choose the desired Region. For more information, see Region and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of your organization.

   The Organization settings page appears and displays the URL under User login. The URLs take this form: https://alias.awsapps.com/mail.

Step 3: Set up Amazon WorkMail user access

Choose from the following options to set up Amazon WorkMail user access:

- Set up user access from an existing desktop client using the Microsoft Outlook client. For more information, see Connect Microsoft Outlook to your Amazon WorkMail account.
- Set up user access from a mobile device, such as a Kindle, Android, iPad, or iPhone. For more information, see Getting started with a mobile device.
- To set up user access, use any client software compatible with the Internet Mail Access Protocol (IMAP) protocol. For more information, see Connect IMAP clients to Your Amazon WorkMail account.
More resources

- Migrating to Amazon WorkMail (p. 46)
- Interoperability between Amazon WorkMail and Microsoft Exchange (p. 47)
- Amazon WorkMail quotas (p. 60)

Migrating to Amazon WorkMail

You can migrate to Amazon WorkMail from Microsoft Exchange, Microsoft Office 365, G Suite Basic (formerly Google Apps for Work), and other platforms by working with one of our partners. For more information about our partners, see Amazon WorkMail Features.

Topics

- Step 1: Create or enable users in Amazon WorkMail (p. 46)
- Step 2: Migrate to Amazon WorkMail (p. 46)
- Step 3: Complete the migration to Amazon WorkMail (p. 46)

Step 1: Create or enable users in Amazon WorkMail

Before you migrate your users, you must add those users in Amazon WorkMail to provision their mailbox. For more information, see Creating users (p. 103).

Step 2: Migrate to Amazon WorkMail

You can work with any AWS migration partners to migrate to Amazon WorkMail. For information about these providers, see Amazon WorkMail features.

To migrate your mailboxes, create a dedicated Amazon WorkMail user to act as a migration administrator. The following procedure grants permission to that user to access all of the mailboxes in your organization.

To create a migration administrator

1. Do one of the following:

   - In the Amazon WorkMail console, create a new user to act as migration administrator. For more information, see Creating users (p. 103).
   - In your Active Directory, create a new user to act as migration administrator, and then enable the user for Amazon WorkMail. For more information, see Enabling existing users (p. 104).

2. In the Amazon WorkMail console navigation pane, choose Organizations, and then choose Migration, and then Edit.
3. Choose Organization settings, choose Migration, and then Edit.
4. Move the Migration enabled slider to the on position.
5. Open the Migration administrator and select a user.
6. Choose Save.

Step 3: Complete the migration to Amazon WorkMail

After you migrate your email accounts to Amazon WorkMail, you can verify your DNS records and configure your desktop and mobile clients.
To complete migration to Amazon WorkMail

1. Verify that all DNS records are updated and that they point to Amazon WorkMail. For more information about the required DNS records, see Adding a domain (p. 90).

Note
The DNS record update process can take several hours. If any new items appear in a source mailbox while the MX records are being changed, run the migration tool again to migrate new items after the DNS records are updated.

2. For more information about configuring your desktop or mobile clients to use Amazon WorkMail, see Connect Microsoft Outlook to your Amazon WorkMail account in the Amazon WorkMail User Guide.

Interoperability between Amazon WorkMail and Microsoft Exchange

Interoperability between Amazon WorkMail and Microsoft Exchange Server allows you to minimize disruption to your users as you migrate mailboxes to Amazon WorkMail, or use Amazon WorkMail for a subset of your corporate mailboxes.

This interoperability allows you to use the same corporate domain for mailboxes across both environments. This way, your users can schedule meetings with bidirectional sharing of calendar free/busy status information.

Prerequisites

Before you enable interoperability with Microsoft Exchange, do the following:

- Make sure you have at least one user enabled for Amazon WorkMail. This is required to configure availability settings for Microsoft Exchange. To enable a user, follow the steps in Enable email routing for a user (p. 57).
- Set up an Active Directory (AD) Connector. Setting up an AD Connector with your on-premises directory allows users to continue using their existing corporate credentials. For more information, see Set up AD Connector and Integrate Amazon WorkMail with your on-premises directory.
- Set up your Amazon WorkMail organization. Create an Amazon WorkMail organization that uses the AD Connector that you set up.
- Add your corporate domains to your Amazon WorkMail organization and then verify them in the Amazon WorkMail console. Otherwise, emails sent to this alias will bounce. For more information, see Working with domains.
- Migrate mailboxes to Amazon WorkMail. Enable users to provision and migrate mailboxes from your on-premises environment to Amazon WorkMail. For more information, see Enable existing users and Migrating to Amazon WorkMail.

Note
Do not update DNS records to point to Amazon WorkMail. This ensures that Microsoft Exchange remains the primary server for incoming email for as long as you want interoperability between the two environments.

- Make sure that the User Principal Names (UPNs) in Active Directory match the users' primary SMTP addresses.

Amazon WorkMail makes HTTPS requests to the Exchange Web Services (EWS) URL on Microsoft Exchange to obtain calendar free/busy information.
For EWS-based availability providers, Amazon WorkMail makes HTTPS requests to the Exchange Web Services (EWS) URL on Microsoft Exchange to obtain calendar free/busy information. Hence, the following prerequisites only apply to EWS-based availability providers.

- **Ensure that the relevant firewall settings are set up to allow access from the internet. The default port for HTTPS requests is port 443.**
- **Amazon WorkMail can only make successful HTTPS requests to the EWS URL on Microsoft Exchange when a certificate signed by a valid certificate authority (CA) is available in your Microsoft Exchange environment. For more information, see Create an Exchange Server certificate request for a certification authority on the Microsoft Exchange Documentation website.**
- **You must enable Basic Authentication for EWS in Microsoft Exchange. For more information, see Virtual directories: Exchange 2013 on the Microsoft MVP Award Program Blog.**

**Add domains and enable mailboxes**

Add your corporate domains to Amazon WorkMail so that they can be used in email addresses. Ensure that the domains added to Amazon WorkMail are verified, and then enable users and groups to provision mailboxes on Amazon WorkMail. Resources can't be enabled in Amazon WorkMail while in interoperability mode, and should be re-created in Amazon WorkMail after you disable interoperability mode. However, you can still use them to schedule meetings while in interoperability mode. Resources from Microsoft Exchange are always shown in the **Users** tab in Amazon WorkMail.

- **For more information, see Add domains, Enable existing users, and Enable an existing group.**

  **Note**
  To ensure interoperability with Microsoft Exchange, don’t update the DNS records to point to Amazon WorkMail records. Microsoft Exchange remains the primary server for incoming email as long as you want interoperability between the two environments.

**Enable interoperability**

If you have not created an Amazon WorkMail organization, you can use the public API to create a new WorkMail Organization with interoperability mode enabled.

If you already have an Amazon WorkMail organization with an AD Connector linked to Active Directory, and you also have Microsoft Exchange, contact AWS Support for assistance with enabling Microsoft Exchange interoperability for an existing Amazon WorkMail organization.

**Create service accounts in Microsoft Exchange and Amazon WorkMail**

  **Note**
  Creating a service account in Exchange is not required when Exchange is not used as a back-end for custom availability provider.

To access calendar free/busy information, create a service account on both Microsoft Exchange and Amazon WorkMail. The Microsoft Exchange service account is any user on Microsoft Exchange that has access to the calendar free/busy information of other Exchange users. Access is granted by default; so no special permissions are required.

Similarly, the Amazon WorkMail service account is any user on Amazon WorkMail that has access to calendar free/busy information of other Amazon WorkMail users. This is also granted by default. You
must create the Amazon WorkMail user in your on-premises directory, and then enable that user for Amazon WorkMail, to integrate Amazon WorkMail with AD Connector into your directory.

Limitations in interoperability mode

When your organization is in interoperability mode, you must use the Exchange admin center to manage all users, groups, and resources. To enable Amazon WorkMail users and groups, use the AWS Management Console. For more information, see Enable existing users and Enable an existing group.

When enabling a user or group for Amazon WorkMail, you can't edit the email addresses or aliases of those users and groups. Those must also be configured via the Exchange admin center. Amazon WorkMail synchronizes changes in your directory every four hours.

Resources can't be created or enabled in Amazon WorkMail while in interoperability mode. However, all of your Exchange resources are available in the Amazon WorkMail address book and can be used for scheduling meetings as usual.

Configure availability settings on Amazon WorkMail

Configure availability settings on Amazon WorkMail to enable querying external systems, offering calendaring functionality, and to get calendar free/busy information. Amazon WorkMail supports two modes of obtaining free/busy information from a remote system:

- **Exchange Web Services (EWS)** — In this configuration, Amazon WorkMail will query an Exchange server or another WorkMail organization for availability information using the EWS protocol. This is the simplest configuration but requires the Exchange server's EWS endpoint to be accessible through the public internet.

- **Custom Availability Provider (CAP)** — In this configuration, an administrator can configure an AWS Lambda function to obtain user availability information for a given email domain. Depending on your email server platform, using CAP with Amazon WorkMail offers the following benefits:
  - Get user availability from internal EWS without the need to open up their firewall for WorkMail.
  - Get user availability from non-Exchange or non-EWS systems, like Google Workspace (formerly known as G Suite).

**Topics**

- Configure an EWS-based availability provider (p. 49)
- Configuring a Custom Availability Provider (p. 50)
- Building a Custom Availability Provider Lambda function (p. 51)

Configure an EWS-based availability provider

To configure an EWS-based availability settings on the console, complete the following procedure:

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   
   If necessary, change the AWS Region. To do so, open the Select a region list, located to the right of the search box, then choose the desired Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of an organization.
3. In the navigation pane, choose **Organization settings**, and then choose the **Interoperability** tab.

4. Choose **Add availability configuration**, and then enter the following information:
   - **Type** — Select EWS.
   - **Domain** — The domain for which WorkMail will attempt to query availability information using this configuration.
   - **EWS URL** — Amazon WorkMail will query this URL to the EWS endpoint. See the **Getting the EWS URL** section of this guide.
   - **User email address** — The email address of the user that WorkMail will use to authenticate with the EWS endpoint.
   - **Password** — The password that WorkMail will use to authenticate with the EWS endpoint.

5. Choose **Save**.

---

**Getting the EWS URL**

To get the EWS URL for Exchange using Microsoft Outlook, complete the following procedure:

1. Log in to Microsoft Outlook on Windows for any user on your Exchange environment.
2. Hold the **Ctrl** key and open the context (right-click) menu on the Microsoft Outlook icon in the task bar.
3. Choose **Test E-mail AutoConfiguration**.
4. Enter the Microsoft Exchange user’s email address and password, and choose **Test**.
5. From the Results window, copy the value for the **Availability Service URL**.

To get the EWS URL for exchange using PowerShell, at the PowerShell prompt, execute the following command:

```
Get-WebServicesVirtualDirectory | Select name, *url* | fl
```

To get the EWS URL for Amazon WorkMail, first, find the EWS domain under Amazon WorkMail endpoints and quotas. Enter the EWS URL — `https://"EWS domain"/EWS/Exchange.asmx` and replace “EWS domain” with your EWS domain.

---

**Configuring a Custom Availability Provider**

To configure a Custom Availability Provider (CAP), complete the following procedure:

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
   - If necessary, change the AWS Region. To do so, open the **Select a Region** list, located to the right of the search box, then choose the desired Region.
2. In the navigation pane, choose **Organizations**, and then choose the name of an organization.
3. In the navigation panel, choose **Organization settings** and then choose **Interoperability**.
4. Choose **Add availability configuration**, and then enter the following information:
   - **Type** — Select CAP Lambda.
   - **Domain** — The domain for which WorkMail will attempt to query availability information using this configuration.
   - **ARN** — The ARN of the Lambda function that will provide the availability information.

To build a CAP Lambda function, see [Building a Custom Availability Provider Lambda function](p. 51).
Building a Custom Availability Provider Lambda function

Custom Availability Providers (CAPs) are configured with a JSON-based request and response protocol that is written in a well-defined JSON schema. A Lambda function will parse the request and provide a valid response.

Topics

- Request and response elements (p. 51)
- Granting access (p. 55)
- Example of Amazon WorkMail using a CAP Lambda function (p. 56)

Request and response elements

Request elements

The following is a sample request used to configure a CAP for an Amazon WorkMail user:

```json
{
  "requester": {
    "email": "user1@internal.example.com",
    "username": "user1",
    "organization": "m-0123456789abcdef0123456789abcdef",
    "userId": "S-1-5-18",
    "origin": "127.0.0.1"
  },
  "mailboxes": [
    "user2@external.example.com",
    "unknown@internal.example.com"
  ],
  "window": {
    "startDate": "2021-05-04T00:00:00.000Z",
    "endDate": "2021-05-06T00:00:00.000Z"
  }
}
```

A request is composed of three sections: requester, mailboxes, and window. These are described in the following Requester (p. 51), Mailboxes (p. 52), and Window (p. 52) sections of this guide.

Requester

The requester section provides information about the user who made the original request to Amazon WorkMail. CAPs use this information to change the behavior of the provider. For instance, this data can be used to impersonate the same user on the backend availability provider or certain details can be omitted from the response.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>The primary email address of the requester.</td>
<td>Yes</td>
</tr>
<tr>
<td>Username</td>
<td>The user name of the requester.</td>
<td>Yes</td>
</tr>
<tr>
<td>Organization</td>
<td>The organization ID of the requester.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Building a CAP Lambda function

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserID</td>
<td>The requester ID.</td>
<td>Yes</td>
</tr>
<tr>
<td>Origin</td>
<td>The remote address of the request.</td>
<td>No</td>
</tr>
<tr>
<td>Bearer</td>
<td>Reserved for future use.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Mailboxes**

The *mailboxes* section contains a comma separated list of email addresses of users for which availability information is requested.

**Window**

The *window* section contains the time window which the availability information is requested for. Both startDate and endDate are specified in UTC and are formatted according to [RFC 3339](https://tools.ietf.org/html/rfc3339). Events aren't expected to be truncated. In other words, if an event starts before the defined *StartDate*, the original start will be used.

**Response elements**

Amazon WorkMail will wait for 25 seconds to get a response from the CAP Lambda function. After 25 seconds, Amazon WorkMail will assume the function has failed and generate failures for the associated mailboxes in the EWS GetUserAvailability response. This will not cause the entire GetUserAvailability operation to fail.

The following is a sample response from the configuration defined at the beginning of this section:

```
{
  "mailboxes": [
    {
      "mailbox": "user2@external.example.com",
      "events": [
        {
          "startTime": "2021-05-03T23:00:00.000Z",
          "endTime": "2021-05-04T03:00:00.000Z",
          "busyType": "BUSY"|"FREE"|"TENTATIVE",
          "details": {  // optional
            "subject": "Late meeting",
            "location": "Chime",
            "instanceType": "SINGLE_INSTANCE"|"RECURRING_INSTANCE"|"EXCEPTION",
            "isMeeting": true,
            "isReminderSet": true,
            "isPrivate": false
          }
        }
      ],
      "workingHours": {
        "timezone": {
          "name": "W. Europe Standard Time",
          "bias": 60,
          "standardTime": {  // optional (not needed for fixed offsets)
            "offset": 60,
            "time": "02:00:00",
            "month": "JAN"|"FEB"|"MAR"|"APR"|"JUN"|"JUL"|"AUG"|"SEP"|"OCT"|"NOV"|"DEC",
            "week": "FIRST"|"SECOND"|"THIRD"|"FOURTH"|"LAST",
            "dayOfWeek": "SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"
          },
          "daylightTime": {  // optional (not needed for fixed offsets)
            "offset": 0,
            "time": "03:00:00",
          }
        }
      }
    }
  ]
}
```
A response is composed of a single `mailboxes` section which consists of a list of mailboxes. Each mailbox for which availability is successfully obtained is composed of three sections: mailbox, events, and workinghours. If the availability provider has failed to obtain availability information for a mailbox, the section is composed of two sections: mailbox and error. These are described in the following Mailbox (p. 53), Events (p. 53), Working Hours (p. 54), Timezone (p. 54), Working Periods (p. 55), and Error (p. 55) sections of this guide.

**Mailbox**

The `mailbox` section is the email address of the user found in the `mailboxes` section of the request.

**Events**

The `events` section is a list of events that occur in the requested window. Each event is defined with the following parameters:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>startTime</td>
<td>The start time of the event in UTC and formatted according to RFC 3339.</td>
<td>Yes</td>
</tr>
<tr>
<td>endTime</td>
<td>The end time of the event in UTC and formatted according to RFC 3339.</td>
<td>Yes</td>
</tr>
<tr>
<td>busyType</td>
<td>The busy type of the event. Can be Busy, Free, or Tentative.</td>
<td>Yes</td>
</tr>
<tr>
<td>details</td>
<td>The details of the event.</td>
<td>No</td>
</tr>
<tr>
<td>details.subject</td>
<td>The subject of the event.</td>
<td>Yes</td>
</tr>
<tr>
<td>details.location</td>
<td>The location of the event.</td>
<td>Yes</td>
</tr>
<tr>
<td>details.instanceType</td>
<td>The instance type of the event. Can be Single_Instance, Recurring_Instance, or Exception.</td>
<td>Yes</td>
</tr>
<tr>
<td>details.isMeeting</td>
<td>A Boolean to indicate if the event has attendees.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Field | Description | Required
---|---|---
`details.isReminderSet` | A Boolean to indicate if the event has a reminder set. | Yes
`details.isPrivate` | A Boolean to indicate if the event is set to private. | Yes

#### Working Hours

The `workingHours` section contains information about the mailbox owner's working hours. It contains two sections: `timezone` and `workingPeriods`.

#### Timezone

The `timezone` subsection describes the mailbox owner's time zone. It's important to correctly render the user's working hours when the requester works in a different time zone. The availability provider is required to explicitly describe the time zone, rather than using a name. Using the standarized time zone description helps avoid time zone mismatches.

| Field | Description | Required |
---|---|---|
`name` | The time zone's name. | Yes |
`bias` | The default offset from GMT in minutes. | Yes |
`standardTime` | The start of standard time for the specified time zone. | No |
`daylightTime` | The start of daylight savings time for the specified time zone. | No |

You must either define both `standardTime` and `daylightTime`, or omit both. Fields in the `standardTime` and `daylightTime` object are:

| Field | Description | Allowed Values |
---|---|---|
`offset` | The offset relative to the default offset in minutes. | NA |
`time` | The time at which the transition between standard time and daylight savings time happens, specified as `hh:mm:ss`. | NA |
`month` | The month that the transition between standard time and daylight savings time happens. | JAN, FEB, MAR, APR, JUN, JUL, AUG, SEP, OCT, NOV, DEC |
`week` | The week within the specified month that the transition between standard time and daylight savings time happens. | FIRST, SECOND, THIRD, FOURTH, LAST |
`dayOfWeek` | The day within the specified week that the transition happens. | SUN, MON, TUE, WED, THU, FRI, SAT |
### Working Periods

The `workingPeriods` section contains one or more working period objects. Each period defines a start and end of working day for one or more days.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>startMinutes</td>
<td>The start of the working day in minutes from midnight.</td>
<td>NA</td>
</tr>
<tr>
<td>endMinutes</td>
<td>The end of the working day in minutes from midnight.</td>
<td>NA</td>
</tr>
<tr>
<td>days</td>
<td>The days that this period applies to.</td>
<td>SUN, MON, TUE, WED, THU, FRI, SAT</td>
</tr>
</tbody>
</table>

### Error

The `error` field can contain arbitrary error messages. The following table lists a mapping of well known codes to EWS error codes. All other messages will be mapped to `ERROR_FREE_BUSY_GENERATION_FAILED`.

<table>
<thead>
<tr>
<th>Value</th>
<th>EWS Error code</th>
</tr>
</thead>
<tbody>
<tr>
<td>MailboxNotFound</td>
<td>ERROR_MAIL_RECIPIENT_NOT_FOUND</td>
</tr>
<tr>
<td>ErrorAvailabilityConfigNotFound</td>
<td>ERROR.AvailabilityConfigNotFound</td>
</tr>
<tr>
<td>ErrorServerBusy</td>
<td>ERROR_SERVER_BUSY</td>
</tr>
<tr>
<td>ErrorTimeoutExpired</td>
<td>ERROR_TIMEOUT_EXPIRED</td>
</tr>
<tr>
<td>ErrorFreeBusyGenerationFailed</td>
<td>ERROR.FreeBusyGenerationFailed</td>
</tr>
<tr>
<td>ErrorResponseSchemaValidation</td>
<td>ERROR_RESPONSE_SCHEMA_VALIDATION</td>
</tr>
</tbody>
</table>

### Granting access

Run the following Lambda command from the AWS Command Line Interface (AWS CLI). This command adds a resource policy to the Lambda function that parses the CAP. This function allows the Amazon WorkMail availability service to invoke your Lambda function.

```bash
aws lambda add-permission
--region LAMBDA_REGION
--function-name CAP_FUNCTION_NAME
--statement-id AllowWorkMail
--action "lambda:InvokeFunction"
--principal availability.workmail.WM_REGION.amazonaws.com
--source-account WM_ACCOUNT_ID
```
Configure availability settings in Microsoft Exchange

To redirect all calendar free/busy information requests for enabled users to Amazon WorkMail, set up an availability address space in Microsoft Exchange.

Use the following PowerShell command to create the address space:

```powershell
$credentials = Get-Credential
Add-AvailabilityAddressSpace -ForestName orgname.awsapps.com -AccessMethod OrgWideFB -Credentials $credentials
```

At the prompt, enter the credentials of the Amazon WorkMail service account. The username should be entered as `domain\username` (that is, `orgname.awsapps.com\workmail_service_account_username`). Here, `orgname` represents the name of the Amazon WorkMail organization. For more information, see [Create service accounts in Microsoft Exchange and Amazon WorkMail](p. 48).

For more information, see [Add-AvailabilityAddressSpace](on Microsoft Docs).
Enable email routing between Microsoft Exchange and Amazon WorkMail users

With email routing between Microsoft Exchange Server and Amazon WorkMail, users can keep their existing email addresses after they migrate to Amazon WorkMail. Email routing lets you keep Microsoft Exchange Server as the primary Simple Mail Transfer Protocol (SMTP) server for incoming email for your organization.

Before using email routing, you'll need to complete the following prerequisites:

- Enable interoperability mode for your organization. For more information, see Enable interoperability (p. 48).
- Ensure that you see your domain in the Amazon WorkMail console.
- Verify that your Microsoft Exchange Server can send email to the internet. You might need to configure a Send connector. For more information about Send connectors, see Create a Send connector in Exchange Server to send mail to the internet in the Microsoft documentation.

Enable email routing for a user

We recommend that you complete the following steps first for test users before applying any changes to your organization.

1. Enable the user account that you are migrating to Amazon WorkMail. For more information, see Enable existing users.
2. In the Amazon WorkMail console, ensure that there are at least two email addresses associated with the enabled user.
   - `<workmailuser@orgname.awsapps.com>` (this is added automatically and can be used for tests without your Microsoft Exchange.)
   - `<workmailuser@yourdomain.com>` (this is added automatically and is the primary Microsoft Exchange address.)
   For more information, see Edit user email addresses.
3. Ensure that you migrate all data from the mailbox in Microsoft Exchange to the mailbox in Amazon WorkMail. For more information, see Migrating to Amazon WorkMail.
4. After all of the data is migrated, disable the mailbox for the user on Microsoft Exchange. Then, create a mail user (or mail-enabled user) that has the external SMTP address pointed to Amazon WorkMail. To do this, use the following commands in the Exchange Management Shell:

   **Important**
   The following steps erase the contents of the mailbox. Ensure that your data has been migrated to Amazon WorkMail before you attempt to enable email routing. Some mail clients don’t seamlessly switch to Amazon WorkMail when you run this command. For more information, see Mail client configuration (p. 58).

```
$old_mailbox = Get-Mailbox exchangeuser

Disable-Mailbox $old_mailbox

$new_mailuser = Enable-MailUser $old_mailbox.Identity -ExternalEmailAddress workmailuser@orgname.awsapps.com -PrimarySmtpAddress $old_mailbox.PrimarySmtpAddress
```

Version 1.0
In the above commands, `orgname` represents the name of your Amazon WorkMail organization. For more information, see Disabling mailbox and Enabling mail users on Microsoft TechNet.

5. Send a test email to the user (in the example above, `workmailuser@yourdomain.com`). If email routing has been enabled correctly, the user should be able to log in to their Amazon WorkMail mailbox and receive the email.

**Note**

Microsoft Exchange remains the primary server for incoming email as long as you would like to have interoperability between the two environments. To ensure interoperability with Microsoft Exchange, the DNS records shouldn't be updated to point to Amazon WorkMail until later.

**Post setup configuration**

The above steps move a user mailbox from Microsoft Exchange Server to Amazon WorkMail, while keeping the user in Microsoft Exchange as a contact. Because the migrated user is now an external mail user, Microsoft Exchange Server imposes additional constraints. There may also be additional configuration requirements to complete the migration.

- The user might not be able to send emails to groups by default. To enable this functionality, you must add the user to a safe sender list for all groups. For more information, see Delivery management on Microsoft TechNet.
- The user might not be able to book resources. To enable this functionality, you must set the `ProcessExternalMeetingMessages` of all of the resources that the user needs to access. For more information, see Set-CalendarProcessing on Microsoft TechNet.

**Mail client configuration**

Some mail clients don't switch seamlessly to Amazon WorkMail. These clients require the user to perform additional setup steps. Different mail clients require different actions to be taken.

- Microsoft Outlook on Windows – Requires Outlook to be restarted. At startup, you are required to choose whether to keep using the old mailbox or use a temporary mailbox. Choose the temporary mailbox option. Then, reconfigure the Microsoft Exchange mailbox.
- Microsoft Outlook on MacOS – When Outlook is restarted, it will prompt the following message: *Outlook was redirected to server orgname.awsapps.com. Do you want this server to configure your settings?* Accept the suggestion.
- Mail on iOS – The mail app stops receiving emails and generates a can't get mail error. Recreate and reconfigure the Microsoft Exchange mailbox.

**Disabling interoperability mode and decommissioning your mail server**

After you configure your Microsoft Exchange mailboxes for Amazon WorkMail, you can disable interoperability mode. If you haven't migrated any users or records, disabling interoperability mode does not affect any of your configurations.
Warning
Before disabling interoperability mode, ensure that you complete all the required steps. Failure to do so can result in bounced emails or unintended behavior. If you have not completed migration, disabling interoperability may cause disruptions to your organization. You can't undo this operation.

To disable interoperability mode support
1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, and then choose the organization for which you want to disable interoperability mode.
3. Under Organization settings, choose Disable interoperability mode.
4. In the Disable interoperability mode dialog box, enter the name of the organization and choose Disable interoperability mode.

After disabling interoperability support, users and groups that are not enabled for Amazon WorkMail are removed from the address book. You can still enable any missing user or group using the Amazon WorkMail console, and they are added to the address book. Resources from Microsoft Exchange can't be enabled and do not appear in the address book until you complete the step below.

- **Create resources in Amazon WorkMail** – You can create resources in Amazon WorkMail and then configure delegates and booking options for these resources. For more information, see Working with resources.
- **Create an AutoDiscover DNS record** – Configure an AutoDiscover DNS record for all mail domains in the organization. This enables users to connect to their Amazon WorkMail mailboxes from their Microsoft Outlook and mobile clients. For more information, see Use AutoDiscover to configure endpoints.
- **Switch your MX DNS record to Amazon WorkMail** – To deliver all incoming emails to Amazon WorkMail, you must switch your MX DNS record to Amazon WorkMail. Changes to DNS records can take up to 72 hours to propagate to all DNS servers.
- **Decommission your mail server** – After you've verified that all email is being routed directly to Amazon WorkMail, you can decommission your mail server if you don't intend to use it going forward.

Troubleshooting

Solutions to the most commonly encountered Amazon WorkMail interoperability and migration errors are listed below.

**Exchange Web Services (EWS) URL is invalid or unreachable** – Check that you have the correct EWS URL. For more information, see Configure availability settings on Amazon WorkMail (p. 49).

**Connection failure during EWS validation** – This is a general error and can be caused by:

- No internet connection in Microsoft Exchange.
- Your firewall is not configured to allow access from the internet. Ensure that port 443 (the default port for HTTPS requests) is open.

If you've confirmed the internet connection and firewall settings, but the error persists, contact AWS Support.
Invalid username and password when configuring Microsoft Exchange interoperability – This is a general error and can be caused by:

- The username is not in the expected form. Use the following pattern:

  DOMAIN\username

- Your Microsoft Exchange server is not configured for Basic Authentication for EWS. For more information, see Virtual directories: Exchange 2013 on the Microsoft MVP Award Program Blog.

User receives emails with winmail.dat attachment – This might happen when encrypted S/MIME email is sent from Exchange to Amazon WorkMail and received in Outlook 2016 for Mac or an IMAP client. The solution is to run the following command in the Exchange Management Shell.

  Set-RemoteDomain -Identity "Default" -TNEFEnabled $false

If you’ve confirmed the points above but the error persists, contact AWS Support.

Amazon WorkMail quotas

Amazon WorkMail can be used by both enterprise customers and small business owners. Although we support most use cases without the need to configure any changes in quotas, we also protect our users and the internet against abuse of the product. Therefore, some customers may run into quotas that we have set. This section describes these quotas and how to change them.

Some quota values can be changed, and some are hard quotas that can’t be changed. For more information about requesting a quota increase, see AWS Service quotas in the Amazon Web Services General Reference.

Amazon WorkMail organization and user quotas

You can add up to 25 users to your Amazon WorkMail organization for a 30-day free trial. After this period ends, you are charged for all active users unless you remove them or close your Amazon WorkMail account.

All messages that are sent to another user are considered when evaluating these quotas. These include emails, meeting requests, meeting responses, task requests, and messages that are forwarded or redirected automatically as the result of a rule.

Note

When requesting a quota increase for a specific organization, you must include the organization name in your request.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default quota</th>
<th>Upper bound for change requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon WorkMail organizations per AWS account</td>
<td>100</td>
<td>Can be increased based on an organization’s directory type. You can view AWS Directory Service quotas and request increases from the AWS Directory Service console. For more information, see Service quotas in the AWS General Reference.</td>
</tr>
</tbody>
</table>
WorkMail organization setting quotas

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default quota</th>
<th>Upper bound for change requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users per Amazon WorkMail organization</td>
<td>1,000</td>
<td>Can be increased depending on the organization's directory type, as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Amazon WorkMail directory: up to 10 million users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Simple AD or AD Connector, large: up to 5,000 users*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Simple AD or AD Connector, small: up to 500 users*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Microsoft AD, hosted by AWS Directory Service: up to 10 million users depending on your setup and configuration,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*If you are using Simple AD or AD Connector, see <a href="https://aws.amazon.com/ams/directory-service/">AWS Directory Service</a> for additional information.</td>
</tr>
<tr>
<td>Free trial users</td>
<td>Up to 25 users in the first 30 days</td>
<td>The free trial period is only applicable for the first 25 users in any organization. Any additional users are not included in the free trial offer.</td>
</tr>
<tr>
<td>Recipients addressed per AWS account per day</td>
<td>100,000 recipients external to the organization, with no hard quota on recipients internal to the organization</td>
<td>There is no upper bound. However, Amazon WorkMail is a business email service and not intended to be used for bulk email services. For bulk email services, see <a href="https://aws.amazon.com/ses/">Amazon SES</a> or <a href="https://aws.amazon.com/pinpoint/">Amazon Pinpoint</a>.</td>
</tr>
<tr>
<td>Recipients addressed per AWS account per day using any of the test domains</td>
<td>200 recipients, regardless of destination</td>
<td>The test mail domain is not intended for long-term usage. We recommend that you add your own domain and use it as the default domain.</td>
</tr>
</tbody>
</table>

Quotas for groups are set by the underlying directory.

**WorkMail organization setting quotas**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of domains per Amazon WorkMail organization</td>
<td>1,000</td>
</tr>
<tr>
<td></td>
<td>This is a hard quota and can't be changed.</td>
</tr>
<tr>
<td>Number of sender patterns in email flow rules per rule</td>
<td>250</td>
</tr>
</tbody>
</table>
Per-user quotas

All messages that are sent to another user are considered when evaluating these quotas. These include emails, meeting requests, meeting responses, task requests, and messages that are forwarded or redirected automatically as the result of a rule.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size of mailbox</td>
<td>50 GB</td>
</tr>
<tr>
<td></td>
<td>This is a hard quota and can't be changed.</td>
</tr>
<tr>
<td>Maximum number of aliases per user</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>This is a hard quota and can't be changed.</td>
</tr>
<tr>
<td>Recipients addressed per user per day using the domain that you own</td>
<td>10,000 recipients external to the organization, with no hard quota on recipients internal to the organization.</td>
</tr>
<tr>
<td></td>
<td>There is no upper bound. However, Amazon WorkMail is a business email service and not intended to be used for bulk email services. For bulk email services, see Amazon SES or Amazon Pinpoint.</td>
</tr>
</tbody>
</table>

Message quotas

All messages that are sent to another user are considered when evaluating these quotas. These include emails, meeting requests, meeting responses, task requests, and messages that are forwarded or redirected automatically as the result of a rule.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size of incoming message</td>
<td>29 MB of unencoded data.</td>
</tr>
<tr>
<td></td>
<td>Messages are received in a MIME format.</td>
</tr>
<tr>
<td></td>
<td>Maximum size of incoming MIME message is 40 MB.</td>
</tr>
<tr>
<td></td>
<td>This is a hard quota and can't be changed.</td>
</tr>
<tr>
<td>Maximum size of outgoing message</td>
<td>29 MB of unencoded data.</td>
</tr>
<tr>
<td></td>
<td>Messages are sent in a MIME format.</td>
</tr>
<tr>
<td></td>
<td>Maximum size of outgoing MIME message is 40 MB.</td>
</tr>
<tr>
<td>Resource</td>
<td>Default quota</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>Maximum number of recipients per message</td>
<td>500</td>
</tr>
<tr>
<td></td>
<td>This is a hard quota and can't be changed.</td>
</tr>
<tr>
<td>Maximum number of attachments per message</td>
<td>500</td>
</tr>
<tr>
<td></td>
<td>This is a hard quota and can't be changed.</td>
</tr>
</tbody>
</table>
Creating an organization

To use Amazon WorkMail, you must first create an organization. One AWS account can have multiple Amazon WorkMail organizations. When you create an organization, you also select a domain for the organization and set up user directory and encryption settings.

You can create a new user directory, or integrate Amazon WorkMail with an existing directory. You can use Amazon WorkMail with an on-premises Microsoft Active Directory, AWS Managed Active Directory, or Simple AD. By integrating with your on-premises directory, you can use your existing users and groups in Amazon WorkMail and users can sign in with their existing credentials. If you're using an on-premises directory, you must first set up an AD Connector in AWS Directory Service. The AD Connector synchronizes your users and groups with the Amazon WorkMail address book and performs user authentication requests. For more information, see Active Directory Connector in the AWS Directory Service Administration Guide.

You also have the option of selecting a AWS KMS key that Amazon WorkMail uses to encrypt the mailbox content. You can either select the default AWS managed master key for Amazon WorkMail, or use an existing KMS key in AWS Key Management Service (AWS KMS). For information about creating a new KMS key, see Creating keys in the AWS Key Management Service Developer Guide. If you are signed in as an AWS Identity and Access Management (IAM) user, make yourself a key administrator on the KMS key. For more information, see Enabling and disabling keys in the AWS Key Management Service Developer Guide.

Considerations

Remember the following when creating an Amazon WorkMail organization:

- Amazon WorkMail doesn't currently support managed Microsoft Active Directory services that you share with multiple accounts.
- If you have an on-premises Active Directory with Microsoft Exchange and an AD Connector, we recommend configuring interoperability settings for your organization. This allows you to minimize disruption to your users as you migrate mailboxes to Amazon WorkMail, or use Amazon WorkMail for a subset of your corporate mailboxes. For more information, see Interoperability between Amazon WorkMail and Microsoft Exchange (p. 47).
If you select the **Free test domain** option, you can start using your Amazon WorkMail organization with the provided test domain. The test domain uses this format: `example.awsapps.com`. You can use the test mail domain with Amazon WorkMail and other supported AWS services as long as you maintain enabled users in your Amazon WorkMail organization. However, you can't use the test domain for other purposes. The test domain might become available for registration and use by other customers if your Amazon WorkMail organization does not maintain at least one enabled user.

Amazon WorkMail does not support multi-Region directories.

**Topics**
- Creating an organization (p. 65)
- Viewing an organization's details (p. 66)
- Integrating an Amazon WorkDocs or WorkSpaces directory (p. 66)
- Organization states and descriptions (p. 66)

## Creating an organization

Create a new organization in the Amazon WorkMail console.

### To create an organization

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
   
   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see [Region and endpoints](https://docs.aws.amazon.com/AmazonWorkMail/latest/WorkMailReference/region-and-endpoints.html) in the Amazon Web Services General Reference.

2. In the navigation bar, select **Organization**.

   The **Organizations** page appears and displays your organizations, if any.

3. Choose **Create organization**.

4. Under **Email domain**, select the domain to use for the email addresses in your organization:

   - **Existing Route 53 domain** – Select an existing domain that you manage with an Amazon Route 53 (Route 53) hosted zone.
   - **New Route 53 domain** – Register a new Route 53 domain name to use with Amazon WorkMail.
   - **External domain** – Enter an existing domain that you manage with an external domain name system (DNS) provider.
   - **Free test domain** – Use a free test domain provided by Amazon WorkMail. You can explore Amazon WorkMail using a test domain, and then add a domain to your organization later.

5. (Optional) If your domain is managed through Amazon Route 53, for **Route 53 hosted zone**, select your Route 53 domain.

6. For **Alias**, enter a unique alias for your organization.

7. Choose **Advanced settings**, and for **User directory**, select one of the following options:

   - **Create new Amazon WorkMail directory** – Creates a new directory for adding and managing your users.
   - **Use existing directory** – Uses an existing directory to manage your users, such as an on-premises Microsoft Active Directory, AWS Managed Active Directory, or Simple AD.

8. For **Encryption**, select one of the following options:

   - **Use an Amazon WorkMail managed key** – Creates a new encryption key in your account.
   - **Use existing KMS key** – Uses an existing KMS key that you have already created in AWS KMS.
9. Choose **Create organization**.

If you use an external domain, verify it by adding the appropriate text (TXT) and mail exchanger (MX) records to your DNS service. TXT records allow you to enter notes about the DNS service. MX records specify the incoming mail server.

Be sure to set your domain as the default for your organization. For more information, see [Verifying domains](p. 93) and [Choosing the default domain](p. 93).

When your organization is **Active**, you can add users to it and set up their email clients. For more information, see [Managing user accounts](p. 103) and [Setting up email clients for Amazon WorkMail](p. 103).

**Viewing an organization's details**

Each of your Amazon WorkMail organizations can display an organization details page. The page shows you information about their organization, including IDs that you can use with the AWS Command Line Interface. Messages on the page can also show you any steps needed to finish setting up and organization, such as an unverified domain or a lack of users. The messages also provide the first step that you follow to set up a given email client.

**To view organization details**

1. In the navigation bar, choose **Organization**.
   - The **Organizations** page appears and displays your organizations.
2. Choose the organization that you want to view.

**Integrating an Amazon WorkDocs or WorkSpaces directory**

To use Amazon WorkMail with Amazon WorkDocs or WorkSpaces, create a compatible directory by using the following steps.

**To add a compatible Amazon WorkDocs or WorkSpaces directory**

1. Create a compatible directory using Amazon WorkDocs or WorkSpaces.
   a. For Amazon WorkDocs instructions, see [Getting started with Quick Start](in the Amazon WorkDocs Administration Guide).
   b. For WorkSpaces instructions, see [Get started with Amazon WorkSpaces Quick Setup](in the Amazon WorkSpaces Administration Guide).
2. In the Amazon WorkMail console, create your Amazon WorkMail organization and choose to use your existing directory for it. For more information, see [Creating an organization](p. 65).

**Organization states and descriptions**

After you create an organization, it can have one of the following states.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Your organization is healthy and ready for use.</td>
</tr>
</tbody>
</table>
Deleting an organization

If you no longer want to use Amazon WorkMail for your organization's email, you can delete your organization from Amazon WorkMail.

**Note**
This operation can't be undone. You won't be able to recover your mailbox data after an organization is deleted.

**To delete an organization**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see [Regions and endpoints](https://aws.amazon.com/about-aws/global-infrastructure/regions-endpoints/) in the [Amazon Web Services General Reference](https://docs.aws.amazon.com/).  

2. On the Organizations screen, in the list of organizations, select the organization to delete and choose **Delete**.

3. For **Delete organization**, choose whether to delete or keep the existing user directory, and then enter the name of the organization.

4. Choose **Delete organization**.

**Note**
If you didn't provide your own directory for Amazon WorkMail, we'll create one for you. If you keep this existing directory when you delete the organization, you will be charged for it unless it is being used by Amazon WorkMail, Amazon WorkDocs, or WorkSpaces. For pricing information, see [Other directory types pricing](https://aws.amazon.com/aws/pricing/).  
In order to delete the directory, it can't have any other AWS applications enabled. For more information, see [Deleting a Simple AD directory](https://docs.aws.amazon.com/directoryservice/latest/adminGuide/ad-delete.html) or [Deleting an AD Connector directory](https://docs.aws.amazon.com/directoryservice/latest/adminGuide/ad-connector-delete.html) in the [AWS Directory Service Administration Guide](https://docs.aws.amazon.com/directoryservice/latest/adminGuide/).  

You may get an invalid Amazon Simple Email Service (Amazon SES) rule set error message when you attempt to delete an organization. If you receive this error, edit the Amazon SES rule in the Amazon SES console and remove the invalid rule set. The rule that you edit should have your Amazon WorkMail organization ID in the rule name. For more information about editing Amazon SES rules, see [Creating receipt rules](https://docs.aws.amazon.com/ses/latest/dg/sending-email-receipts.html) in the [Amazon Simple Email Service Developer Guide](https://docs.aws.amazon.com/ses/latest/dg/index.html).

If you need to figure out which rule set is not valid, save the rule first. An error message appears for the rule set.
Working with organization settings

The following sections explain how to use the settings available for Amazon WorkMail organizations. Settings that you choose will apply to the entire organization.

Topics

- Enabling mailbox migration (p. 68)
- Enabling journaling (p. 68)
- Enabling interoperability (p. 68)
- Enabling SMTP gateways (p. 68)
- Managing email flows (p. 69)
- Enforcing DMARC policies on incoming email (p. 84)

Enabling mailbox migration

You enable mailbox migration when you want to transfer mailboxes from a source, such as Microsoft Exchange or G Suite Basic, to Amazon WorkMail. You enable migration as part of a larger migration process. For more information, including how-to steps, see Migrating to Amazon WorkMail (p. 46) in the Getting started section of this guide.

Enabling journaling

You enable journaling to record your email communication. When using journaling, you typically use integrated third-party archiving and eDiscovery tools. Journaling helps ensure that you meet compliance regulations for data storage, privacy protection, and information protection.

For more information, including how-to steps, see Using email journaling with Amazon WorkMail (p. 145) in the Getting started section of this guide.

Enabling interoperability

Interoperability allows you to migrate from Microsoft Exchange and to use Amazon WorkMail as a subset of your corporate mailboxes. For more information, including how-to steps, see Configure availability settings on Amazon WorkMail (p. 49) in the Getting started section of this guide.

Enabling SMTP gateways

You enable Simple Mail Transfer Protocol (SMTP) gateways for use with outbound email flow rules. Outbound email flow rules let you route email messages sent from your Amazon WorkMail organization through an SMTP gateway. For more information, see Outbound email rule actions (p. 71).

Note

SMTP gateways configured for outbound email flow rules must support Transport Layer Security (TLS) v1.2 using certificates from major certificate authorities. Only basic authentication is supported.

To configure an SMTP gateway

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, then choose the name of an organization.
3. In the navigation pane, choose Organization settings.

   The Organization settings page appears and displays a set of tabs.
4. Choose the SMTP gateways tab, then choose Create gateway.
5. Enter the following:
   • Gateway name — Enter a unique name.
   • Gateway address — Enter the gateway's host name or IP address.
   • Port number — Enter the gateway's port number.
   • User name — Enter a user name.
   • Password — Enter a strong password.
6. Choose Create.

   The SMTP gateway is available for use with outbound email flow rules.

When you configure an SMTP gateway for use with an outbound email flow rule, outbound messages attempt to match the rule with an SMTP gateway. The message that match the rule are routed to the corresponding SMTP gateway, which then handles the rest of the email delivery.

If Amazon WorkMail is unable to reach the SMTP gateway, the system bounces the email message back to the sender. If this occurs, follow the previous steps to correct the gateway settings.

Managing email flows

To help manage email, you can set up email flow rules. Email flow rules can take one or more actions on email messages based on their addresses or domains. You can use email flow rules on senders' and recipients' email addresses or domains.

When you create an email flow rule, you specify a rule action (p. 69) that applies to an email when a specified rule pattern (p. 71) is matched.

Topics
• Inbound email rule actions (p. 69)
• Outbound email rule actions (p. 71)
• Sender and recipient patterns (p. 71)
• Creating email flow rules (p. 72)
• Editing email flow rules (p. 73)
• Configuring AWS Lambda for Amazon WorkMail (p. 73)
• Managing access to the Amazon WorkMail Message Flow API (p. 81)
• Testing an email flow rule (p. 83)
• Removing an email flow rule (p. 83)

Inbound email rule actions

Inbound email flow rules help prevent undesirable email from reaching your users' mailboxes. Inbound email flow rules, also called rule actions, automatically apply to all email messages sent to anyone inside of your Amazon WorkMail organization. This differs from email rules for individual mailboxes.

Note
Optionally, you can use rules with an AWS Lambda function to process incoming email before it is delivered to your users' mailboxes. For more information about using Lambda with Amazon
WorkMail, see Configuring AWS Lambda for Amazon WorkMail (p. 73). For more information about Lambda, see the AWS Lambda Developer Guide.

Inbound email flow rules, also called rule actions, automatically apply to all email messages sent to anyone inside of the Amazon WorkMail organization. This differs from email rules for individual mailboxes.

The following rule actions define how inbound email is handled. For each rule, you specify sender and recipient patterns (p. 71) together with one of the following actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop email</td>
<td>The email message is ignored. It is not delivered, and the sender is not notified of the non-delivery.</td>
</tr>
<tr>
<td>Send bounce response</td>
<td>The email message is not delivered, and the sender is notified of the non-delivery in a bounce message.</td>
</tr>
<tr>
<td>Deliver to junk folder</td>
<td>The email message is delivered to users' spam or junk folders, even if it is not originally identified as spam by the Amazon WorkMail spam detection system.</td>
</tr>
<tr>
<td>Default</td>
<td>The email message is delivered after being checked by the Amazon WorkMail spam detection system. Spam email is delivered to the junk folder. All other email messages are delivered to the inbox. Other email flow rules with a less specific sender pattern are ignored. To add exceptions to domain-based email flow rules, configure the Default action with a more specific sender pattern. For more information, see Sender and recipient patterns (p. 71).</td>
</tr>
<tr>
<td>Never deliver to junk folder</td>
<td>The email message is always delivered to users' inboxes, even if it is identified as spam by the Amazon WorkMail spam detection system.</td>
</tr>
</tbody>
</table>
| Important               | **Important**  
By not using the default spam detection system, you could expose your users to high-risk content from the addresses that you specify. |
| Run AWS Lambda          | Passes the email message to a Lambda function for processing before or while it is delivered to users' inboxes.                           |

**Note**  
Inbound email is first delivered to Amazon SES, and then to Amazon WorkMail. If Amazon SES blocks an incoming email message, then rule actions won't apply. For example, Amazon SES blocks an email message when a known virus is detected or because of explicit IP filtering rules. Specifying a rule action, such as Default, Deliver to junk folder, or Never deliver to junk folder has no effect.
Outbound email rule actions

You use outbound email flow rules to direct email messages via SMTP gateways, or to block senders from sending email messages to specified recipients. For more information about SMTP gateways, see Enabling SMTP gateways (p. 68).

You can also use outbound email flow rules to pass the email message to an AWS Lambda function for processing after the email is sent. For more information about Lambda, see the AWS Lambda Developer Guide.

The following rule actions define how outbound email is handled. For each rule, you specify sender and recipient patterns (p. 71) together with one of the following actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>The email message is sent via the normal flow.</td>
</tr>
<tr>
<td>Drop email</td>
<td>The email message is dropped. It is not sent, and the sender is not notified.</td>
</tr>
<tr>
<td>Send bounce response</td>
<td>The email message is not sent, and the sender is notified with a message that the administrator blocked the email message.</td>
</tr>
<tr>
<td>Route to SMTP gateway</td>
<td>The email message is sent via a configured SMTP gateway.</td>
</tr>
<tr>
<td>Run Lambda</td>
<td>Passes the email message to a Lambda function for processing before or while the email message is sent.</td>
</tr>
</tbody>
</table>

Sender and recipient patterns

An email flow rule can apply to a specific email address, or all email addresses under a specific domain or set of domains. You define a pattern to determine the email addresses that a rule applies to.

Both sender and recipient patterns take one of the following forms:

- An **email address** matches a single email address; for example:

  mailbox@example.com

- A **domain name** matches all email addresses under that domain; for example:

  example.com

- A **wildcard domain** matches all email addresses under that domain and all of its subdomains. A wildcard appears only at the front of a domain; for example:

  *.example.com

- A **star** matches any email addresses under any domain.

  *
**Note**  
The + symbol is not valid inside of sender or recipient patterns.

Multiple patterns can be specified for one rule. For more information, see Inbound email rule actions (p. 69) and Outbound email rule actions (p. 71).

Inbound email flow rules are applied if either the Sender or From header in an inbound email message matches any patterns. If present, the Sender address is matched first. The From address is matched if there is no Sender header or if the Sender header doesn't match any rule. If there are multiple recipients for the email message that match different rules, each rule applies for the matched recipients.

Outbound email flow rules are applied if the recipient and either the Sender or From header in an outbound email message matches any patterns. If there are multiple recipients for the email message that match different rules, each rule applies for the matched recipients.

If multiple rules match, the action of the most specific rule is applied. An example is when a rule for a specific email address takes precedence over a rule for an entire domain. If multiple rules have the same specificity, the most restrictive action is applied. An example is when a Drop action takes precedence over a Bounce action. The order of precedence for actions is the same as the order in which they are listed in Inbound email rule actions (p. 69) and Outbound email rule actions (p. 71).

**Note**  
Take care when creating rules with overlapping sender patterns with Drop or Bounce actions. Unexpected precedence ordering could result in many inbound email messages not being delivered.

**Creating email flow rules**

Email flow rules apply rule actions (p. 69) to incoming and outgoing email messages. The actions apply when messages match a specified pattern (p. 71). New email flow rules take effect immediately.

**To create email flow rules**

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, then choose the name of an organization.
3. In the navigation pane, choose Organization settings.
   
   The Organization settings page appears and displays a set of tabs. From this page, you can create inbound or outbound rules. The following steps explain how to create both types.

**To create inbound rules**

1. Choose the Inbound rules tab and then choose Create.
2. In the Rule name box, enter a unique name.
3. Under Action, open the list and select an action. Each item in the list contains a description, and some provide Learn more links.
   
   **Note**  
   If you choose the Run Lambda action, additional controls appear: For information about using those controls, see the next section, Configuring AWS Lambda for Amazon WorkMail (p. 73).
4. Under Sender domains or addresses, enter the sender domains or addresses to which you want the rule to apply.
5. Under Destination domains or addresses, enter any combination of destination domains and email addresses.
6. Choose **Create**.

**To create outbound rules**

1. Choose the **Outbound rules** tab and choose **Create**.
2. In the **Rule name** box, enter a unique name.
3. Under **Action**, open the list and select an action. Each item in the list contains a description, and some provide **Learn more** links.

   **Note**
   If you choose the **Run Lambda** action, additional controls appear. For information about using those controls, see the next section, *Configuring AWS Lambda for Amazon WorkMail* (p. 73).
4. Under **Sender domains or addresses**, enter any combination of valid sender domains and email addresses.
5. Under **Destination domains or addresses**, enter any combination of valid destinations domains and email addresses.
6. Choose **Create**.

You can test the new email flow rule that you created. For more information, see Testing an email flow rule (p. 83).

**Editing email flow rules**

You edit email flow rules whenever you need to change one or more **rule actions** (p. 69) for email messages. The steps in this section apply to incoming and outgoing email messages.

**To edit email flow rules**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose **Organizations**, then choose the name of an organization.
3. In the navigation pane, choose **Organization settings**.
   The **Organization settings** page appears and displays a set of tabs.
4. Choose the **Inbound rules** or **Outbound rules** tabs.
5. Choose the radio button next to the rule that you want to change, then choose **Edit**.
6. Change the action or actions in the rule as needed, then choose **Save**.

**Configuring AWS Lambda for Amazon WorkMail**

Use the **Run Lambda** action in inbound and outbound email flow rules to pass email messages that match the rules to an AWS Lambda function for processing.

Choose from the following configurations for a **Run Lambda** action in Amazon WorkMail.

**Synchronous Run Lambda configuration**

Email messages that match the flow rule are passed to a Lambda function for processing before they are sent or delivered. Use this configuration to modify email content. You can also control inbound
or outbound email flow for different use cases. For example, a rule passed to a Lambda function can block delivery of sensitive email messages, remove attachments, or add disclaimers.

**Asynchronous Run Lambda configuration**

Email messages that match the flow rule are passed to a Lambda function for processing while they are sent or delivered. This configuration does not affect email delivery and is used for tasks such as collecting metrics for inbound or outbound email messages.

Whether you choose a synchronous or asynchronous configuration, the event object passed to your Lambda function contains metadata for the inbound or outbound email event. You can also use the message ID in the metadata to access the full content of the email message. For more information, see [Retrieving message content with AWS Lambda](p. 79). For more information about email events, see [Lambda event data](p. 75).

For more information about inbound and outbound email flow rules, see [Managing email flows](p. 69). For more information about Lambda, see the [AWS Lambda Developer Guide](p. 75).

**Note**

Currently, Lambda email flow rules reference only Lambda functions in the same AWS Region and AWS account as the Amazon WorkMail organization being configured.

**Getting started with AWS Lambda for Amazon WorkMail**

To start using AWS Lambda with Amazon WorkMail, we recommend deploying the [WorkMail Hello World Lambda function](p. 79) from the AWS Serverless Application Repository to your account. The function has all the necessary resources, and the permissions configured for you. For more examples, see the [amazon-workmail-lambda-templates](p. 79) repository on GitHub.

If you choose to create your own Lambda function, you must configure permissions using the AWS Command Line Interface (AWS CLI). In the following example command, do the following:

- Replace `MY_FUNCTION_NAME` with the name of your Lambda function.
- Replace `REGION` with your Amazon WorkMail AWS Region. Available Amazon WorkMail Regions include `us-east-1` (US East (N. Virginia)), `us-west-2` (US West (Oregon)), and `eu-west-1` (Europe (Ireland)).
- Replace `AWS_ACCOUNT_ID` with your 12-digit AWS account ID.
- Replace `WORKMAIL_ORGANIZATION_ID` with your Amazon WorkMail organization ID. You can find it on the card for your organization on the [Organizations](p. 79) page.

```
```

For more information about using the AWS CLI, see the [AWS Command Line Interface User Guide](p. 79).

**Configuring synchronous Run Lambda rules**

To configure a synchronous Run Lambda rule, create an email flow rule with the Run Lambda action and select the Run synchronously check box. For more information about creating mail flow rules, see [Creating email flow rules](p. 72).

To finish creating the synchronous rule, add the Lambda Amazon Resource Name (ARN) and configure the following options.
Fallback action

The action Amazon WorkMail applies if the Lambda function fails to run. This action also applies to any recipients that are omitted from the Lambda response if the allRecipients flag is not set. The Fallback action can't be another Lambda action.

Rule timeout (in minutes)

The time period during which the Lambda function is retried if Amazon WorkMail fails to invoke it. The Fallback action is applied at the end of this time period.

Note

Synchronous Run Lambda rules support the * destination condition only.

Lambda event data

The Lambda function is triggered using the following event data. The presentation of the data varies depending on which programming language is used for the Lambda function.

```json
{
    "summaryVersion": "2018-10-10",
    "envelope": {
        "mailFrom": {
            "address": "from@example.com"
        },
        "recipients": [
            { "address": "recipient1@example.com" },
            { "address": "recipient2@example.com" }
        ]
    },
    "sender": {
        "address": "sender@example.com"
    },
    "subject": "Hello From Amazon WorkMail!",
    "messageId": "00000000-0000-0000-0000-000000000000",
    "invocationId": "00000000000000000000000000000000",
    "flowDirection": "INBOUND",
    "truncated": false
}
```

The event JSON includes the following data.

**summaryVersion**

The version number for LambdaEventData. This only updates when you make a backwards incompatible change in LambdaEventData.

**envelope**

The envelope of the email message, which includes the following: fields.

**mailFrom**

The From address, which is usually the email address of the user who sent the email message. If the user sent the email message as another user or on behalf of another user, the mailFrom field returns the email address of the user on whose behalf the email message was sent, not the email address of the actual sender.

**recipients**

A list of recipient email addresses. Amazon WorkMail doesn't distinguish between To, CC, or BCC.
Note
For inbound email flow rules, this list includes recipients in all the domains in the Amazon WorkMail organization in which you create the rule. The Lambda function is invoked separately for each SMTP conversation from the sender, and the recipients field lists the recipients from that SMTP conversation. Recipients with external domains are not included.

sender
The email address of the user who sent the email message on behalf of another user. This field is set only when an email message is sent on behalf of another user.

subject
The email subject line. Truncated when it exceeds the 256 character limit.

messageId
A unique ID used to access the full content of the email message when using the Amazon WorkMail Message Flow SDK.

invocationId
The ID for a unique Lambda invocation. This ID remains the same when a Lambda function is called more than once for the same LambdaEvent. Use to detect retries and avoid duplication.

flowDirection
Indicates the direction of the email flow, either INBOUND or OUTBOUND.

truncated
Applies to the payload size, not the subject line length. When true, the payload size exceeds the 128 KB limit, so the list of recipients is truncated in order to meet the limit.

Synchronous Run Lambda response schema
When an email flow rule with a synchronous Run Lambda action matches an inbound or outbound email message, Amazon WorkMail calls the configured Lambda function and waits for the response before taking action on the email message. The Lambda function returns a response according to a pre-defined schema that lists the actions, action types, applicable parameters, and recipients that the action applies to.

The following example shows a synchronous Run Lambda response. Responses vary based on the programming language used for the Lambda function.

```json
{
    "actions": [
        {
            "action": {
                "type": "string",
                "parameters": { various }
            },
            "recipients": [list of strings],
            "allRecipients": boolean
        }
    ]
}
```

The response JSON includes the following data.

action
The action to take for the recipients.
type

The action type. Action types are not returned for asynchronous Run Lambda actions.

Inbound rule action types include BOUNCE, DROP, DEFAULT, BYPASS_SPAM_CHECK, and MOVE_TO_JUNK. For more information, see Inbound email rule actions (p. 69).

Outbound rule action types include BOUNCE, DROP, and DEFAULT. For more information, see Outbound email rule actions (p. 71).

parameters

Additional action parameters. Supported for the BOUNCE action type as a JSON object with the key bounceMessage and value string. This bounce message is used to create the bounce email message.

recipients

List of email addresses on which the action should be taken. You can add new recipients to the response even if they were not included in the original recipients list. This field is not required if allRecipients is true for an action.

Note

When a Lambda action is called for inbound email, you can only add new recipients that are from your organization. The new recipients are added to the response as BCC.

allRecipients

When true, applies the action to all the recipients that are not subject to another specific action in the Lambda response.

Synchronous Run Lambda action limits

The following limits apply when Amazon WorkMail invokes Lambda functions for synchronous Run Lambda actions:

- Lambda functions must respond within 15 seconds, or be treated as failed invocations.
  
  Note
  
  The system retries the invocation for the Rule timeout interval that you specify.

- Lambda function responses up to 256 KB are allowed.

- Up to 10 unique actions are allowed in the response. Actions greater than 10 are subject to the configured Fallback action.

- Up to 500 recipients are allowed for outbound Lambda functions.

- The maximum value for Rule timeout is 240 minutes. If the minimum value of 0 is configured, there are no retries before Amazon WorkMail applies the fallback action.

Synchronous Run Lambda action failures

If Amazon WorkMail can’t invoke your Lambda function due to an error, invalid response, or Lambda timeout, Amazon WorkMail retries the invocation with exponential backoff that decreases the processing rate until the Rule timeout period completes. Then, the Fallback action is applied to all recipients of the email message. For more information, see Configuring synchronous Run Lambda rules (p. 74).

Example synchronous Run Lambda responses

The following examples demonstrate the structure of common synchronous Run Lambda responses.

Example : Remove specified recipients from an email message

The following example demonstrates the structure of a synchronous Run Lambda response for removing recipients from an email message.
Example: Bounce with a custom email message

The following example demonstrates the structure of a synchronous Run Lambda response for bouncing with a custom email message.

```
{
  "actions": [
    {
      "action": {
        "type": "BOUNCE",
        "parameters": {
          "bounceMessage": "Email in breach of company policy."
        }
      },
      "allRecipients": true
    }
  ]
}
```

Example: Add recipients to an email message

The following example demonstrates the structure of a synchronous Run Lambda response for adding recipients to the email message. This does not update the To or CC fields of the email message.

```
{
  "actions": [
    {
      "action": {
        "type": "DEFAULT"
      },
      "recipients": [
        "new-recipient@example.com"
      ]
    },
    {
      "action": {
        "type": "DEFAULT"
      },
      "allRecipients": true
    }
  ]
}
```
For more code examples to use when creating Lambda functions for Run Lambda actions, see Amazon WorkMail Lambda templates.

More information about using Lambda with Amazon WorkMail

You can also access the full content of the email message that triggers the Lambda function. For more information, see Retrieving message content with AWS Lambda (p. 79).

Retrieving message content with AWS Lambda

After you configure an AWS Lambda function to manage email flows for Amazon WorkMail, you can access the full content of the email messages that are processed using Lambda. For more information about getting started with Lambda for Amazon WorkMail, see Configuring AWS Lambda for Amazon WorkMail (p. 73).

To access the full content of email messages, use the GetRawMessageContent action in the Amazon WorkMail Message Flow API. The email message ID that is passed to your Lambda function upon invocation sends a request to the API. Then, the API responds with the full MIME content of the email message. For more information, see Amazon WorkMail Message Flow in the Amazon WorkMail API Reference.

The following example shows how a Lambda function using the Python runtime environment can retrieve the full message content.

```
import boto3
import email
import os

def email_handler(event, context):
    workmail = boto3.client('workmailmessageflow', region_name=os.environ['AWS_REGION'])
    msg_id = event['messageId']
    raw_msg = workmail.get_raw_message_content(messageId=msg_id)
    parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())
    print(parsed_msg)
```

For more detailed examples of ways to analyze the content of messages that are in transit, see the amazon-workmail-lambda-templates repository on GitHub.

Note

You only use the Amazon WorkMail Message Flow API to access email messages in transit. You can only access the messages within 24 hours of being sent or received. To programmatically access messages in a user's mailbox, use one of the other protocols supported by Amazon WorkMail, such as IMAP or Exchange Web Services (EWS).

Updating message content with AWS Lambda

After you configure a synchronous AWS Lambda function to manage email flows, you can use the PutRawMessageContent action in the Amazon WorkMail Message flow API to update the content of in-transit email messages. For more information about getting started with Lambda functions for Amazon WorkMail, see Configuring synchronous Run Lambda rules (p. 74). For more information about the API, see PutRawMessageContent.
Note
The PutRawMessageContent API requires boto3 1.17.8, or you can add a layer to your Lambda function. To download the correct boto3 version, see the boto page on GitHub. For more information about adding layers, see Configure a function to use layers.
Here's an example layer: "LayerArn":"arn:aws:lambda: ${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2". In this example, substitute ${AWS::Region} with an appropriate aws region, such as us-east-1.

Tip
If you start by deploying the Amazon WorkMail Hello World Lambda function from the AWS Serverless Application Repository to your account, the system creates a Lambda function in your account with the necessary resources and permissions. You can then add business logic to the lambda function, based on your use cases.

As you go, remember the following:

- Use the GetRawMessageContent API to retrieve the original message content. For more information see Retrieving message content with AWS Lambda (p. 79).
- Once you have the original message, change the MIME content. When you finish, upload the message to an Amazon Simple Storage Service (Amazon S3) bucket in your account. Ensure that the S3 bucket uses the same AWS account as your Amazon WorkMail operations, and that it uses the same AWS Region as your API calls.
- For Amazon WorkMail to process requests, your S3 bucket must have the correct policy in order to access the S3 object. For more information, see Example S3 policy.
- Use the PutRawMessageContent API to send the updated message content back to Amazon WorkMail.

Note
The PutRawMessageContent API ensures that the MIME content of the updated message meets RFC standards, as well as the criteria mentioned in the RawMessageContent data type. Emails inbound to your Amazon WorkMail organization don't always meet those standards, so the PutRawMessageContent API may reject them. In such cases, you can consult the error message returned for more information on how to fix any issues.

Example Example S3 policy

```json
{
   "Version": "2008-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {"Service": "workmail.REGION.amazonaws.com"}
      },
      "Action": [
         "s3:GetObject",
         "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::My-Test-S3-Bucket/**",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "AWS_ACCOUNT_ID"
         },
         "Bool": {
            "aws:SecureTransport": "true"
         },
         "ArnLike": {
         }
      }
   ]
}```
The following example shows how a Lambda function uses the Python runtime to update the subject of an in-transit email message.

```python
import boto3
import os
import uuid
import email

def email_handler(event, context):
    workmail = boto3.client('workmailmessageflow', region_name=os.environ['AWS_REGION'])
    s3 = boto3.client('s3', region_name=os.environ['AWS_REGION'])

    msg_id = event['messageId']
    raw_msg = workmail.get_raw_message_content(messageId=msg_id)
    parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())

    # Updating subject. For more examples, see https://github.com/aws-samples/amazon-workmail-lambda-templates.
    parsed_msg.replace_header('Subject', 'New Subject Updated From Lambda')

    # Store updated email in S3
    key = str(uuid.uuid4());
    s3.put_object(Body=parsed_msg.as_bytes(), Bucket='Your-S3-Bucket', Key=key)

    # Update the email in WorkMail
    s3_reference = {
        'bucket': 'Your-S3-Bucket',
        'key': key
    }
    content = {
        's3Reference': s3_reference
    }
    workmail.put_raw_message_content(messageId=msg_id, content=content)
```

For more examples of ways to analyze the content of in-transit messages, see the [amazon-workmail-lambda-templates](https://github.com/aws-samples/amazon-workmail-lambda-templates) repository on GitHub.

**Managing access to the Amazon WorkMail Message Flow API**

Use AWS Identity and Access Management (IAM) policies to manage access to the Amazon WorkMail Message Flow API.

The Amazon WorkMail Message Flow API works with a single resource type, an email message in transit. Each email message in transit has a unique Amazon Resource Name (ARN) associated with it.

The following example shows the syntax of an ARN associated with an email message in transit.

```
arn:aws:workmailmessageflow:region:account:message/organization/context/messageID
```

Changeable fields in the preceding example include the following:

- **Region** – The AWS Region for your Amazon WorkMail organization.
- **Account** – The AWS account ID for your Amazon WorkMail organization.
• **Organization** – Your Amazon WorkMail organization ID.
• **Context** – Indicates whether the message is incoming to your organization, or outgoing from it.
• **Message ID** – The unique email message ID that is passed as input to your Lambda function.

The following example includes example IDs for an ARN associated with an incoming email message in transit.

```
arn:aws:workmailmessageflow:us-east-1:111122223333:message/m-n1pq2345678r901st2u3vx45x6789yza/incoming/d1234567-8e90-1f23-456g-hjk7lmnop8q9
```

You can use these ARNs as resources in the Resource section of your IAM user policies in order to manage access to Amazon WorkMail messages in transit.

**Example IAM policies for Amazon WorkMail message flow access**

The following example policy grants an IAM entity full read access to all inbound and outbound messages for every Amazon WorkMail organization in your AWS account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": ["workmailmessageflow:GetRawMessageContent"],
            "Effect": "Allow"
        }
    ]
}
```

If you have multiple organizations in your AWS account, you can also limit access to one or more organizations. This is useful if certain Lambda functions should only be used for certain organizations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": ["workmailmessageflow:GetRawMessageContent"],
            "Effect": "Allow"
        }
    ]
}
```

You can also choose to grant access to messages depending on whether they are incoming to your organization, or outgoing from it. To do this, use the qualifier incoming or outgoing in the ARN.

The following example policy grants access only to messages that are incoming to your organization.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

Version 1.0
82
Managing email flows

The following example policy grants an IAM entity full read and update access to all inbound and outbound messages for every Amazon WorkMail organization in your AWS accounts.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workmailmessageflow:GetRawMessageContent",
        "workmailmessageflow:PutRawMessageContent"
      ],
      "Effect": "Allow"
    }
  ]
}
```

**Testing an email flow rule**

To check your current rule configuration, you can test how the configuration behaves against specific email addresses.

**To test an email flow rule**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, and then choose the name of your organization.
3. In the navigation pane, choose Organization settings, Inbound/Outbound rules.
4. Next to Test configuration, enter the full email addresses of both the sender and recipient that you want to test.
5. Choose Test. The action to be taken for the provided email address is displayed.

**Removing an email flow rule**

When you remove an email flow rule, the changes are applied immediately.

**To remove an email flow rule**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, and then choose the name of your organization.
3. In the navigation pane, choose **Organization settings, Inbound/Outbound rules**.
4. Select the rule and choose **Remove**.
5. At the confirmation prompt, choose **Remove**.

**Enforcing DMARC policies on incoming email**

Email domains use Domain Name System (DNS) records for security. They protect your users from common attacks such as spoofing or phishing. DNS records often include Domain-based Message Authentication, Reporting, and Conformance (DMARC) records, which are set by the domain owner that sends the email. DMARC records include policies that specify actions to take when an email fails a DMARC check. You can choose whether to enforce the DMARC policy on emails being sent to your organization.

New Amazon WorkMail organizations have DMARC enforcement turned on by default.

**To turn on DMARC enforcement**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
   
   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see [Regions and endpoints](https://docs.aws.amazon.com/AmazonWorkMail/latestDeveloperGuide/regions-endpoints.html) in the Amazon WorkMail Service Reference.
2. In the navigation pane, choose **Organizations**, then choose the name of your organization.
3. In the navigation pane, choose **Organization settings**. The **Organization settings** page appears and displays a set of tabs.
4. Choose the **DMARC** tab, then choose **Edit**.
5. Move the **DMARC enforcement** slider to the on position.
6. Select the checkbox next to **I acknowledge that turning on DMARC enforcement may result in inbound emails being dropped or quarantined based on the sender's domain configuration**.
7. Choose **Save**.

**To turn off DMARC enforcement**

- Follow the steps in the previous section, but move the **DMARC enforcement** slider to the off position.

**Using email event logging to track DMARC enforcement**

Turning on DMARC enforcement might result in inbound emails being dropped or marked as spam, depending on how the sender configured their domain. If a sender misconfigures their email domain, your users might stop receiving legitimate emails. To check for emails that aren't being delivered to your users, you can enable email event logging for your Amazon WorkMail organization. Then, you can query your email event logs for inbound emails that are filtered out based on the sender’s DMARC policies.

Before you use email event logging to track DMARC enforcement, enable email event logging in the Amazon WorkMail console. To get the most out of your log data, allow some time to pass while email events are logged. For more information and instructions, see the section called “Turning on email event logging” (p. 40).

**To use email event logging to track DMARC enforcement**

1. In the CloudWatch Insights console, under **Logs**, choose **Insights**.
2. For **Select log group(s)**, select your Amazon WorkMail organization's log group. For example, /aws/workmail/events/organization-alias.
3. Select a time period to query.
4. Run the following query: \texttt{stats count()} by event.dmarcPolicy | filter event.dmarcVerdict == "FAIL"
5. Choose \texttt{Run query}.

You can also set up custom metrics for these events. For more information, see Creating metric filters.

Tagging an organization

Tagging an Amazon WorkMail organization resource allows you to:

- Differentiate between organizations in the AWS Billing and Cost Management console.
- Control access to Amazon WorkMail organization resources by adding them to the Resource element of AWS Identity and Access Management (IAM) permission policy statements.

For more information about Amazon WorkMail resource-level permissions, see Resources (p. 18). For more information about controlling access based on tags, see Authorization based on Amazon WorkMail tags (p. 20).

Amazon WorkMail administrators can tag organizations using the Amazon WorkMail console.

\textbf{To add tags to an Amazon WorkMail organization}

1. Open the Amazon WorkMail console at \url{https://console.aws.amazon.com/workmail/}.
   
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of your organization.
3. Choose Tags.
4. For Organization tags, choose Add new tag.
5. For Key, enter a name that identifies the tag.
6. (Optional) For Value, enter a value for the tag.
7. (Optional) Repeat steps 4-6 to add more tags to your organization. You can add up to 50 tags.
8. Choose Save to save your changes.

You can view your organization tags in the Amazon WorkMail console.

Developers can also tag organizations using the AWS SDK or AWS Command Line Interface (AWS CLI). For more information, see the TagResource, ListTagsForResource, and UntagResource commands in the Amazon WorkMail API Reference or the AWS CLI Command Reference.

You can remove tags from an organization at any time, using the Amazon WorkMail console.

\textbf{To remove tags from an Amazon WorkMail organization}

1. Open the Amazon WorkMail console at \url{https://console.aws.amazon.com/workmail/}.
   
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of your organization.
3. Choose Tags.
4. For Organization tags, choose Remove next to the tag to remove.
5. Choose Submit to save your changes.

Working with access control rules

Access control rules for Amazon WorkMail allow administrators to control how their organization's users and impersonation roles are granted access to Amazon WorkMail. Each Amazon WorkMail organization has a default access control rule that grants mailbox access to all users and impersonation roles added to the organization, no matter which access protocol or IP address they use. Administrators can edit or replace the default rule with one of their own, add a new rule, or delete a rule.

Warning
If an administrator deletes all access control rules for an organization, Amazon WorkMail blocks all access to the organization's mailboxes.

Administrators can apply access control rules that allow or deny access based on the following criteria:

- **Protocols** – The protocol used to access the mailbox. Examples include Autodiscover, EWS, IMAP, SMTP, ActiveSync, Outlook for Windows, and Webmail.
- **IP addresses** – The IPv4 CIDR ranges used to access the mailbox.
- **Amazon WorkMail users** – The users in your organization that are used to access the mailbox.
- **Impersonation roles** – The impersonation roles in your organization that are used to access the mailbox. For more information, see Managing impersonation roles (p. 134).

Administrators apply access control rules in addition to the user's mailbox and folder permissions. For more information, see Working with mailbox permissions (p. 130) and Sharing folders and folder permissions in the Amazon WorkMail User Guide.

Note
- When you are enabling access for Outlook for Windows, it is recommended to also enable access for Autodiscover and EWS.
- Access control rules do not apply to Amazon WorkMail console or SDK access. Use AWS Identity and Access Management (IAM) roles or policies instead. For more information, see Identity and access management for Amazon WorkMail (p. 13).

Creating access control rules

Create new access control rules from the Amazon WorkMail console.

To create a new access control rule

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of your organization.


4. Choose Create rule.

5. For Description, enter a description for the rule.
6. For **Effect**, choose **Allow** or **Deny**. This allows or denies access based on the conditions that you select in the following step.

7. For **This rule applies to requests that** ..., select the conditions to apply to the rule, such as whether to include or exclude specific protocols, IP addresses, or users, or impersonation roles.

8. (Optional) If you enter IP address ranges, users, or impersonation roles, choose **Add** to add them to the rule.

9. Choose **Create rule**.

# Editing access control rules

Edit new and default access control rules from the Amazon WorkMail console.

**To edit an access control rule**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).

   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see [Regions and endpoints](https://docs.aws.amazon.com/AmazonWorkMail/latest/DeveloperGuide/regions.html) in the **Amazon Web Services General Reference**.

2. In the navigation pane, choose **Organizations**, and then choose the name of your organization.

3. Choose **Access control rules**.

4. Select the rule to edit.

5. Choose **Edit rule**.

6. Edit the description, effect, and conditions, as needed.

7. Choose **Save changes**.

**Important**

When you change an access rule, the affected mailboxes can take five minutes to follow the updated rule. Clients that access the affected mailboxes may show inconsistent behavior during that time. However, you will immediately see correct behavior when you test your rules. For more information about testing rules, see the steps in the next section.

# Testing access control rules

To see how your organization's access control rules are applied, test the rules from the Amazon WorkMail console.

**To test access control rules for your organization**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).

   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see [Regions and endpoints](https://docs.aws.amazon.com/AmazonWorkMail/latest/DeveloperGuide/regions.html) in the **Amazon Web Services General Reference**.

2. In the navigation pane, choose **Organizations**, and then choose the name of your organization.

3. Choose **Access control rules**.

4. Choose **Test rules**.

5. For **Request context**, select the protocol to test for.

6. For **Source IP address**, enter the IP address to test for.

7. For **Request performed by**, choose **User** or **Impersonation role** to test for.

8. Select **User** or **Impersonation role** to test for.
9. Choose Test.

The test results appear under Effect.

Deleting access control rules

Delete access control rules that you no longer require from the Amazon WorkMail console.

**Warning**
If an administrator deletes all access control rules for an organization, Amazon WorkMail blocks all access to the organization's mailboxes.

**To delete an access control rule**

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of your organization.


4. Select the rule to delete.

5. Choose Delete rule.

6. Choose Delete.

Setting mailbox retention policies

You can set mailbox retention policies for your Amazon WorkMail organization. Retention policies automatically delete email messages from user mailboxes after a time period that you choose. You can choose which mailbox folders to apply retention policies to. Also, you can choose whether to set different retention policies for different folders. Mailbox retention policies apply to the selected folders in all of the user mailboxes in your organization. Users can't override the retention policies.

**To set a mailbox retention policy**

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of your organization.

3. Choose Retention policy.

4. For Folder actions, next to each mailbox folder that you want to include in the policy, select Delete or Permanently delete.

5. Enter the number of days to keep the email messages in each mailbox folder before deleting them.

6. Choose Save.

Allow 48 hours to apply the retention policies for your organization. If you choose the Delete folder action, users can recover deleted email messages from the Amazon WorkMail web application and supported clients. If you choose the Permanently delete folder action, email messages can't be recovered after they are deleted.
The number of days a retention policy keeps an item is based on when it was created, modified, or moved. For example, if a retention policy deletes items after a year, the policy counts retention days from the date you created or last took action on that item. It is not affected by the date you implemented the retention policy.
Working with domains

You can configure Amazon WorkMail to use a custom domain. You can also make a domain the default for your organization, and enable AutoDiscover for Microsoft Outlook.

Topics
- Adding a domain (p. 90)
- Removing a domain (p. 93)
- Choosing the default domain (p. 93)
- Verifying domains (p. 93)
- Enabling AutoDiscover to configure endpoints (p. 97)
- Editing domain identity policies (p. 100)
- Authenticating email with SPF (p. 102)
- Configuring a custom MAIL FROM domain (p. 102)

Adding a domain

You can add up to 100 domains to your Amazon WorkMail organization. When you add a new domain, an Amazon Simple Email Service (Amazon SES) sending authorization policy is automatically added to the domain identity policy. This provides Amazon WorkMail with access to all Amazon SES sending actions for your domain and allows you to redirect email to your domain. You can also redirect email to external domains.

Note
As a best practice, you should add aliases for <postmaster@> and <abuse@> to all your domains. You can create distribution groups for these aliases if you want specific users in your organization to receive mail sent to these aliases.

When you configure your Amazon WorkMail organization with a custom domain, remember the following about your domain's DNS records:

- For MX and autodiscover CNAME records, we recommend setting the Time to Live (TTL) value to 3600. Reducing the TTL ensures that your mail servers don't use outdated or invalid MX records after you update those records or migrate your mailboxes.
- After you create your users and distribution groups, and then successfully migrate your mailboxes, you should update the MX record to start forwarding emails to Amazon WorkMail. Updates to DNS records can take up to 48 hours to process.
- Some DNS providers automatically append domain names to the ends of DNS records. Adding a record that already contains the domain name, such as _amazonses.example.com, might result in the duplication of the domain name, resulting in _amazonses.example.com.example.com. To avoid duplicating the domain name in the record name, add a period to the end of the domain name in the DNS record. This indicates to your DNS provider that the record name is fully qualified and no longer relative to the domain name. It also prevents the DNS provider from appending an additional domain name.
- Copied record names include the domain name. Depending on which DNS service you use, the domain name might already be added to the domain's DNS record.
- After you create a DNS record, choose the refresh icon on the Amazon WorkMail console to see the verification status and record value. For more information about verifying domains, see Verifying domains (p. 93).
• We recommend that you configure your domain as the MAIL FROM domain. To enable AutoDiscover for iOS devices, you must configure your domain as the MAIL FROM domain. You can see the status of your MAIL FROM domain in the Enhance deliverability section of the console. For more information, see Configuring a custom MAIL FROM domain (p. 102).

To add a domain

1. Sign in to the AWS Management Console and open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

2. If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

3. In the navigation pane, choose Organizations, and then choose the name of the organization that you want to add a domain to.

4. In the navigation pane, choose Domains, and then choose Add domain.

5. On the Add domain screen, enter a domain name. Domain names can contain only Basic Latin (ASCII) characters.

   Note
   If you have a domain that is managed in an Amazon Route 53 public hosted zone, you can choose it from the dropdown menu that appears as you enter a domain name.

6. Choose Add domain.

A page appears and lists the DNS records for the new domain. The page groups the records into the following sections:

• Domain ownership
• WorkMail configuration
• Improved security
• Improved email delivery

Each of these sections contains one or more DNS records, and each record displays a Status value. The following list shows the records and their available status values.

**TXT ownership**

_{Verified}_ – Record resolved and verified.

_{Pending}_ – Record not verified yet.

_{Failed}_ – Unable to verify ownership. Record mismatched or unreachable.

**MX WorkMail configuration**

_{Verified}_ – Record resolved and verified.

_{Missing}_ – Unable to resolve record.

_{Inconsistent}_ – Value does not match expected record.

**AutoDiscover**

_{Verified}_ – Record resolved and verified.

_{Missing}_ – Unable to resolve record.

_{Inconsistent}_ – Value does not match expected record.
Note
The AutoDiscover verification process also checks for correct AutoDiscover setup. The process verifies the configuration settings for each phase. A green check mark appears next to Verified in the Status column when verification finishes. You can hover over Verified and see which of the phases was verified by the process. For more information about the AutoDiscover phases, see Enabling AutoDiscover to configure endpoints (p. 97).

DKIM CNAME
- Verified – Record resolved and verified.
- Pending – Record not verified yet
- Failed – Unable to verify ownership. Record mismatched or unreachable.

For more information about DKIM signing, see Authenticating email with DKIM in Amazon SES in the Amazon Simple Email Service Developer Guide.

SPF TXT
- Verified – Record resolved and verified.
- Missing – Unable to resolve record.
- Inconsistent – Value does not match expected record.

For more information about SPF verification, see Authenticating email with SPF (p. 102).

DMARC TXT
- Verified – Record resolved and verified.
- Missing – Unable to resolve record.
- Inconsistent – Value does not match expected record.

For more information about DMARC records in Amazon WorkMail, see Complying with DMARC using Amazon SES in the Amazon Simple Email Service Developer Guide.

TXT MAIL FROM domain
- Verified – Record resolved and verified.
- Pending – Record not verified yet.
- Failed – Unable to verify ownership. Record mismatched or unreachable.

MX MAIL FROM domain
- Verified – Record resolved and verified.
- Missing – Unable to resolve record.
- Inconsistent – Value does not match expected record.

7. For the next step, choose the appropriate action based on the DNS provider you use.

If you use a Route 53 domain
- At the top of the page, choose Update all in Route 53.
If you use another DNS provider

- Copy the records and paste them into your DNS provider. You can copy the records in bulk or one at a time. To copy records in bulk, choose Copy all. That creates a file zone that you can import into your DNS provider. To copy records one at a time, choose the overlapping squares next to the record name, and then paste each one into your DNS provider.

8. Choose the refresh icon update the Status for each record. This verifies domain ownership and proper configuration of your domain with Amazon WorkMail.

Removing a domain

When you no longer need a domain, you can delete it. However, you must first delete any individuals or groups that use the domain as their email address.

To remove a domain

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Region Name and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, and then choose the name of your organization.
3. In the list of domains, select the check box next to the domain name and choose Remove.
4. In the Remove domain dialog box, enter the name of the domain to remove and choose Remove.

Choosing the default domain

You can make a domain associated with your organization the default for users and groups in that organization. Making a domain the default does not change existing email addresses.

To make a domain the default

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Region Name and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, and then choose the name of your organization.
3. In the list of domains, select the check box next to the domain name you want to use and choose Set as default.

Verifying domains

You must verify your domain after you add it in the Amazon WorkMail console. Verifying the domain confirms that you own the domain and will use Amazon WorkMail as the email service for the domain.

You verify a domain by adding TXT and MX records to it in your DNS service. TXT records enable you to add notes to your DNS service. MX records specify the incoming mail server.

You use the Amazon SES console to create the TXT and MX records, and then you use the Amazon WorkMail console to add the records to your DNS service. Follow these steps.
To create TXT and MX records

1. Open the Amazon SES console at https://console.aws.amazon.com/ses/.
2. In the navigation pane, choose Domains, and then choose Verify a New Domain.
   
   The Verify a New Domain dialog box appears.
3. In the Domain box, enter the name of the domain that you created in the Adding a domain (p. 90) section.
4. (Optional) If you want to use DomainKeys Identified Mail (DKIM), select the Generate DKIM Settings checkbox.
5. Choose Verify This Domain.
   
   The console displays a list of TXT and MX records.
6. Choose the Download Record Set as CSV link, located under the TXT listing.
   
   The Save As dialog box appears. Choose a location for the download, and then choose Save.
7. Open the downloaded CSV file and copy all of its contents.

Once your create the TXT and MX records, you then add them to your DNS provider. The following steps use Route 53. If you use a different DNS provider and you don't know how to add records, consult your provider's documentation.

2. In the navigation pane, choose Hosted Zones. Then, choose the radio button next to the domain that you want to verify.
3. From the list of DNS records for your domain, choose Import zone file.
4. Under Zone file, paste the copied records into the text box. A list of the files appears below the text box.
5. Scroll down to the end of the list and choose Import.

Note
Allow up to 72 hours to complete the verification process.

Verifying TXT records and MX records with your DNS service

Confirm that the TXT record that verifies that you own the domain is added correctly to your DNS service. This procedure uses the nslookup tool, which is available for Windows and Linux. On Linux, you can also use dig.

To use the nslookup tool, you must first find the DNS servers that serve your domain. Then, you query those servers to view the TXT records. You can query the DNS servers for your domain because those servers contain the most up-to-date information for your domain. This information can take time to propagate to other DNS servers.

Use nslookup to verify that your TXT record is added to your DNS service

1. Find your domain's name servers:
   
   a. Open a command prompt (Windows) or terminal (Linux).
Verifying TXT records and MX records with your DNS service

1. Run the following command to list all of the name servers that serve your domain. Replace *example.com* with your domain.

   ```bash
   nslookup -type=NS example.com
   ```

   You'll query one of these name servers in the next step.

2. Verify that the Amazon WorkMail TXT record is correctly added.
   a. Run the following command, replacing *example.com* with your domain, and *ns1.name-server.net* with a name server from Step 1.

   ```bash
   nslookup -type=TXT _amazonses.example.com ns1.name-server.net
   ```

   b. Review the "text =" string shown in the output from `nslookup`. Confirm that this string matches the TXT value for your domain in the **Verified Senders** list in the Amazon WorkMail console.

   In the following example, you want to see a TXT record for _amazonses.example.com with a value of fmxqxT/icOYx4aA/bEUzDPMeax9/s3frbl5+niixmqk=. If you update the record correctly, the command has the following output:

   ```
   _amazonses.example.com text = "fmxqxT/icOYx4aA/bEUzDPMeax9/s3frbl5+niixmqk="
   ```

   Use dig to verify that your TXT record is added to your DNS service

   1. Open a terminal session.
   2. Run the following command to list the TXT records for your domain. Replace *example.com* with your domain.

   ```bash
   dig +short example.com txt
   ```

   3. Verify that the string that follows TXT in the command's output matches the TXT value you see when you select the domain in the **Verified Senders** list of the Amazon WorkMail console.

To use nslookup to verify that your MX record is added to your DNS service

1. Find the name servers for your domain:
   a. Open a command prompt.
   b. Run the following command to list all of the name servers for your domain.

   ```bash
   nslookup -type=NS example.com
   ```

   You'll query one of these name servers in the next step.

2. Verify that the MX record is correctly added:
   a. Run the following command, replacing *example.com* with your domain and *ns1.name-server.net* with one of the name servers you identified in the previous step.

   ```bash
   nslookup -type=MX example.com ns1.name-server.net
   ```

   b. In the output of the command, verify that the string that follows mail exchange = matches one of the following values:
US East (N. Virginia) Region – 10 inbound-smtp.us-east-1.amazonaws.com

US West (Oregon) Region – 10 inbound-smtp.us-west-2.amazonaws.com

Europe (Ireland) Region – 10 inbound-smtp.eu-west-1.amazonaws.com

Note
10 represents the MX preference number or priority.

Use dig to verify that your MX record is added to your DNS service

1. Open a terminal session.
2. Run the following command to list the MX records for your domain.
   
   ```
   dig +short example.com mx
   ```
3. Verify that the string that follows MX matches one of the following values:
   
   US East (N. Virginia) Region – 10 inbound-smtp.us-east-1.amazonaws.com

   US West (Oregon) Region – 10 inbound-smtp.us-west-2.amazonaws.com

   Europe (Ireland) Region – 10 inbound-smtp.eu-west-1.amazonaws.com

   Note
   10 represents the MX preference number or priority.

Troubleshooting domain verification

To troubleshoot common issues with domain verification, see the following suggestions:

Your DNS service does not allow underscores in TXT record names

   Omit _amazonses from the TXT record name.

You want to verify the same domain multiple times but can't have multiple TXT records with the same name

   If your DNS service does not allow you to have multiple TXT records with the same name, use either of the following workarounds:
   
   - (Recommended) If your DNS service allows it, assign multiple values to the TXT record. For example, if your DNS is managed by Amazon Route 53, you can set up multiple values for the same TXT record as follows:
     1. In the Route 53 console, choose the _amazonses TXT record that you added when you verified your domain in the first Region.
     2. For Value, press Enter after the first value.
     3. Add the value for the additional Region, and save the record set.
   - If you only need to verify your domain twice, you can verify it once by creating a TXT record with _amazonses in the name, and then create another record without _amazonses in the record name.

The Amazon WorkMail console reports that domain verification has failed

   Amazon WorkMail can't find the necessary TXT record for your DNS service. Verify that the required TXT record is correctly added to your DNS service by following the procedure in Verifying TXT records and MX records with your DNS service (p. 94).
Your DNS provider appended the domain name to the end of the TXT record

Adding a TXT record that already contains the domain name, such as _amazonses.example.com, can result in the duplication of the domain name, such as _amazonses.example.com.example.com. To avoid duplicating the domain name in the record name, add a period to the end of the domain name in the TXT record. This indicates to your DNS provider that the record name is fully qualified and already has the domain name included in the TXT record.

Amazon WorkMail reports that the MX record is Inconsistent

When migrating from existing mail servers, the MX record might return a status of Inconsistent. Update your MX record to point to Amazon WorkMail instead of pointing to your previous mail server. The MX record is also returned as Inconsistent when a third-party email proxy is used along with Amazon WorkMail. If this is the case, it is safe to ignore the Inconsistent warning.

Enabling AutoDiscover to configure endpoints

AutoDiscover enables you to configure Microsoft Outlook and mobile clients by using only your email address and password. The service maintains a connection to Amazon WorkMail and updates local settings whenever you change endpoints or settings. In addition, AutoDiscover enables your client to use additional Amazon WorkMail features, such as the Offline Address Book, Out-of-Office Assistant, and the ability to view free/busy time in Calendar.

The client performs the following AutoDiscover phases to detect the server endpoint URLs:

- **Phase 1** – The client performs a Secure Copy Protocol (SCP) lookup against the local Active Directory. If your client isn't domain-joined, AutoDiscover skips this step.
- **Phase 2** – The client sends a request to the following URLs and validates the results. These endpoints are only available using HTTPS.
  - https://company.tld/autodiscover/autodiscover.xml
  - https://autodiscover.company.tld/autodiscover/autodiscover.xml
- **Phase 3** – The client performs a DNS lookup to autodiscover.company.tld and sends an unauthenticated GET request to the derived endpoint from the user's email address. If the server returns a 302 redirect, the client resends the AutoDiscover request against the returned HTTPS endpoint.

If all of these phases fail, the client can’t be configured automatically. For information about manually configuring mobile devices, see Manually connect your device.

You are prompted to add the AutoDiscover DNS record to your provider when you add your domain to Amazon WorkMail. This enables the client to perform phase 3 of the AutoDiscover process. However, these steps don't work for all mobile devices, such as the stock Android email app. As a result, you may need to set up AutoDiscover phase 2 manually.

You can use the following methods to set up AutoDiscover phase 2 for your domain:

**Recommended** Use Route 53 and Amazon CloudFront

**Note**
The following steps explain how to create a proxy for https://autodiscover.company.tld/autodiscover/autodiscover.xml. To create a proxy for https://company.tld/autodiscover/autodiscover.xml, remove the autodiscover prefix from the domains in the following steps. Using CloudFront and Route 53 may incure charges. For more information about applicable pricing, see Amazon CloudFront pricing and Amazon Route 53 pricing.
To enable AutoDiscover phase 2 with Route 53 and CloudFront

1. Get an SSL certificate for autodiscover.company.tld and upload it to AWS Identity and Access Management (IAM) or AWS Certificate Manager. For more information, see Working with server certificates in the IAM User Guide, or Getting started in the AWS Certificate Manager User Guide.

2. Create a new CloudFront distribution:
   2. In the navigation pane, choose Distributions.
   3. Choose Create Distribution.
   5. In Origin Settings, enter the following values:
      - Origin Domain Name – The appropriate domain name for your Region:
        - US East (N. Virginia) — autodiscover-service.mail.us-east-1.awsapps.com
        - US West (Oregon) — autodiscover-service.mail.us-west-2.awsapps.com
        - Europe (Ireland) — autodiscover-service.mail.eu-west-1.awsapps.com
      - Origin Protocol Policy – The desired policy: Match Viewer
        Note
        Leave Origin path blank. Don't change the auto-populated value for Origin ID.
      6. In Default Cache Behavior Settings, select the following values for the listed settings:
        - Viewer Protocol Policy: HTTPS Only
        - Allowed HTTP Methods: GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
        - Cache Based on Selected Request Headers: All
        - Forward Cookies: All
        - Query String Forwarding and Caching: None (Improves Caching)
        - Smooth Streaming: No
        - Restrict Viewer Access: No
      7. Select the following values for Distribution Settings:
        - Price Class: Use only US, Canada, and Europe
        - For Alternate Domain Names (CNAMEs), enter autodiscover.company.tld or company.tld, where company.tld is your domain name.
        - SSL Certificate: Custom SSL Certificate (stored in IAM)
        - Custom SSL Client Support: Choose All Clients or Only Clients that Support Server Name Indication (SNI). Older versions of Android might not work with the latter option.
        Note
        If you choose All Clients, leave Default Root Object blank.
        - Logging: Choose On or Off. On enables logging.
        - For Comment, enter AutoDiscover type2 for autodiscover.company.tld
        - Distribution State: choose Enabled.
      8. Choose Create Distribution.
   3. In the Route 53 console, create a record that routes internet traffic for your domain name to your CloudFront distribution.
      Note
      These steps assume that the DNS record for example.com is hosted on Route 53. If you don't use Route 53, follow the procedures in your DNS provider's management console.
      1. In the console's navigation pane, choose Hosted Zones. and then choose a domain.
      2. In the list of domains, choose the domain name that you want to use.
3. In Records, choose Create record.
4. Under Quick create record, set the following parameters:
   • Under Record Name, enter a name for the record.
   • Under Routing policy, select Simple routing.
   • Choose the Alias slider to turn it on. The slider turns blue when in the on state.
   • In the Record type list, choose A - Routes traffic to an IPv4 address and some AWS resources.
   • In the Route traffic to list, choose Alias to CloudFront distribution.
   • A search box will appear beneath the Route traffic to list. Enter your CloudFront distribution's name into the text box. You can also select your distribution from the list that appears when you select the search box.
5. Choose Create record.

Use an Apache web server

The following steps explain how to use an Apache web server to create a proxy for https://autodiscover.company.tld/autodiscover/autodiscover.xml. To create a proxy for https://company.tld/autodiscover/autodiscover.xml, remove the “autodiscover.” prefix from the domains in the following steps.

To enable AutoDiscover phase 2 with an Apache web server

1. Run the following directives on an SSL-enabled Apache server:

SSLProxyEngine on
ProxyPass /autodiscover/autodiscover.xml https://autodiscover-service.mail.REGION.awsapps.com/autodiscover/autodiscover.xml

2. As needed, enable the following Apache modules. If you don’t know how, refer to the Apache help:
   • proxy
   • proxy_http
   • socache_shmcb
   • ssl

See the following section for information about testing and troubleshooting AutoDiscover.

AutoDiscover phase 2 troubleshooting

Once you’ve configured your DNS provider for AutoDiscover, you can test your AutoDiscover endpoint configuration. If you’ve configure your endpoint correctly, it responds with an unauthorized request message.

To make a basic unauthorized request

1. From a terminal, create an unauthenticated POST request to the AutoDiscover endpoint.

   $ curl -X POST -v https://autodiscover.''company.tld'''/autodiscover/autodiscover.xml

   If your endpoint is configured correctly, it should return a 401 unauthorized message, as shown in the following example:

   $ curl -X POST -v https://autodiscover.''company.tld'''/autodiscover/autodiscover.xml
HTTP/1.1 401 Unauthorized

2. Next, test a real AutoDiscover request. Create a request.xml file with the following XML content:

```xml
<?xml version="1.0" encoding="utf-8"?>
  <Request>
    <EMailAddress>testuser@company.tld</EMailAddress>
    <AcceptableResponseSchema>
    </AcceptableResponseSchema>
  </Request>
</Autodiscover>
```

3. Use the request.xml file you created and make an authenticated AutoDiscover request to the endpoint. Remember to replace testuser@company.tld with a valid email address:

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/autodiscover/autodiscover.xml
```

The response will look similar to the following example if the endpoint is configured correctly:

```
Enter host password for user 'testuser@company.tld':
<?xml version="1.0" encoding="UTF-8"?>
    <Culture>en:us</Culture>
    <User>
      <DisplayName>User1</DisplayName>
      <EMailAddress>testuser@company.tld</EMailAddress>
    </User>
    <Action>
      <Settings>
        <Server>
          <Type>MobileSync</Type>
          <Url>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-ActiveSync</Url>
          <Name>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-ActiveSync</Name>
        </Server>
      </Settings>
    </Action>
  </Response>
</Autodiscover>
```

## Editing domain identity policies

Domain identity policies specify permissions for email actions, such as redirecting email messages. For example, you can redirect emails to any email address in your Amazon WorkMail organization.
Note

As of April 1, 2022, Amazon WorkMail began using service principals for authorization instead of AWS account principals. If you added a domain prior to April 1, 2022 you may have an older policy that uses an AWS account principal for authorization. If so, we recommend updating to the latest policy. The steps in this section explain how. Your organization continues to send emails normally during the update.

You only follow these steps if you don't use a custom Amazon SES policy. If you use a custom Amazon SES policy, you must update it yourself. For more information, see Custom Amazon SES service-principal policy (p. 101), later in this topic.

Important

Don't remove your existing domains. If you do, you'll disrupt mail service. All you need to do is re-enter your existing domains.

To update a domain identity policy

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the AWS Region. To do so, open the Select a region list, located to the right of the search box, then choose the desired region. For more information about regions, see Regions and endpoints in the Amazon Web Services General Reference.

2. In navigation pane, choose Organizations, and then choose name of your organization.

3. In the navigation pane, choose Domains.

4. Highlight and copy the name of the domain that you want to re-enter, and then choose Add Domain.

   The Add domain dialog box appears.

5. Paste the copied name into the Domain name box, and then choose Add domain.

6. Repeat steps 3-5 for the remaining domains in your organization.

Custom Amazon SES service-principal policy

If you use a custom Amazon SES policy, adapt this example for use in your domain.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuthorizeWorkMail",
      "Effect": "Allow",
      "Principal": {
        "Service": "workmail.REGION.amazonaws.com"
      },
      "Action": [
        "ses:*"
      ],
      "Condition": {
        " ArnEquals": {
          "aws:SourceArn":
          "arn:aws:workmail:REGION:AWS_ACCOUNT_ID:organization/WORKMAIL_ORGANIZATION_ID"
        }
      }
    }
  ]
}
```
Authenticating email with SPF

The Sender Policy Framework (SPF) is an email validation standard designed to combat email spoofing. Spoofing is the act of making an email sent by a malicious actor look like one sent by a legitimate user. For information about configuring SPF for your Amazon WorkMail-enabled domain, see Authenticating email with SPF in Amazon SES.

Configuring a custom MAIL FROM domain

By default, Amazon WorkMail uses a subdomain of amazonses.com as the MAIL FROM domain for your outgoing email. This can cause delivery failure if the DMARC policy on your domain is only set up for SPF. To resolve this, configure your own domain as the MAIL FROM domain. To learn how to set up your email domain as the MAIL FROM domain, see Setting up a custom MAIL FROM domain in the Amazon Simple Email Service Developer Guide.

**Important**
A custom MAIL FROM domain is required when you enable AutoDiscover for iOS devices.

For more information about custom MAIL FROM domains, see Amazon SES now supports custom MAIL FROM domains.
Working with users

You can create and remove users from Amazon WorkMail. In addition, you can reset their email passwords, manage their mailbox quotas and device access, and control their mailbox permissions.

Topics
- Managing user accounts (p. 103)
- Viewing email headers (p. 108)
- Working with notifications (p. 108)
- Enabling signed or encrypted email (p. 111)

Managing user accounts

Amazon WorkMail includes tools and options for managing user accounts. You can create users, enable existing users, edit email addresses and create email aliases, edit user details, and reset user passwords.

Topics
- Creating users (p. 103)
- Enabling existing users (p. 104)
- Disabling user accounts (p. 104)
- Editing user email addresses (p. 105)
- Editing user details (p. 105)
- Resetting user passwords (p. 107)
- Troubleshooting Amazon WorkMail password policies (p. 107)

Creating users

When you create users, Amazon WorkMail automatically creates mailboxes for them. Users can log in and access their mail from the Amazon WorkMail web application, their mobile device, or by using Microsoft Outlook on macOS or PC.

To create a user

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the organization to which you want to add users.

3. In the navigation pane, choose Users, and then choose Create User.

   The Create a user screen appears.
4. Under **User details**, in the **User name** field, enter the user's name. The name also appears in the **Email address** box. If you want the user to have a different email address from their user name, you can edit the **Email address** field.

5. (Optional) Enter the user's first and last name in the **First name** and **Last name** boxes.

6. In the **Display name** box, enter the user's display name.

7. Under **Email setup**, accept the email alias in the **Email address** box or enter another one. Then, enter the user's password in the **Password** and **Repeat password** boxes. Finally, choose **Create user**.

### Enabling existing users

When you integrate Amazon WorkMail with your corporate Active Directory, or you already have users available in your Simple AD directory, you can enable those users in Amazon WorkMail. You also follow these steps to reenable a user whose account was disabled.

**To enable an existing directory user**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).

   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see **Regions and endpoints** in the **Amazon Web Services General Reference**.

2. In the navigation pane, choose **Organizations**, then choose the organization for which you want to enable users.

3. In the navigation pane, choose **Users**.

   A list of the group’s users appears. User accounts in the enabled, disabled, and system user states are shown in the list.

4. From the list of users with disabled accounts, select the checkboxes for the users that you want to enable, and then choose **Enable**.

   The **Enable users** dialog box appears.

5. As needed, review and change the primary email address for each user, and then choose **Enable**.

### Disabling user accounts

You can disable any user account in a group at any time. When you disable an account, it immediately becomes inaccessible. User accounts that have been disabled for longer than 30 days will have their inbox deleted from Amazon WorkMail.

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).

   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see **Regions and endpoints** in the **Amazon Web Services General Reference**.

2. In the navigation pane, choose **Organizations**, then choose the organization that contains the users that you want to disable.

3. In the navigation pane, choose **Users**.

   A list of all users appears, showing accounts that are in the enabled, disabled, and system user states.

4. From the list of enabled users, select the checkboxes for the accounts that you want to disable, and then choose **Disable**.
The **Disable users** dialog box appears.

5. Choose Disable.

### Editing user email addresses

When you edit a user email address, you can do the following:

- Assign email addresses to a user
- Assign email aliases to a user
- Set a new default email address for the user

When you assign addresses to a user, Amazon WorkMail uses the default email address to send outgoing email. When you assign email aliases, the user can send and receive email from a different address or domain. For more information, refer to [Send as an alias](#).

#### To edit email addresses

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
   
   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see [Regions and endpoints](#) in the Amazon Web Services General Reference.

2. In the navigation pane, choose **Organizations**, then choose the organization that you want to use.

3. In the navigation pane, choose **Users**, and then choose the desired user name.
   
   **Note**
   Be sure to choose the name, and not select the checkbox next to the name. You must choose the name to open the **User details** page.

   The **User details** page appears.

4. Choose **Edit**.

   The **Edit user** screen appears.

5. Under **Email address**, choose **Add alias**, and then do one of the following:
   
   - To add an email address, enter an alias in the left-hand box. Then choose a domain from the list of available domains.
   - To add an alias, enter the alias in the left-hand box. Don't change the domain.
   - To set a new email address, enter the desired address in the **Primary email address to be used for this user** box.

6. Repeat step 5 as needed to enter more addresses or aliases. When you are finished, choose **Save changes**.

### Editing user details

When you edit a user's details, you can change the following:

- **Personal data** – Names, email addresses, phone numbers, and other personal details.
- **Mailbox quotas (sizes)** – Quotas can range from 1 MB to 51,200 MB (50 GB). Amazon WorkMail notifies users when they reach 90 percent of their quota. Also, changing a user's mailbox quota won't affect pricing. For more information about pricing, refer to [Amazon WorkMail Pricing](#).
- **Mobile device access** – Remove and wipe devices, and view device details.
• **Mailbox access permissions** – Grant users permission to use a mailbox, and grant users different levels of access to the mailbox.

**Note**
If you integrate Amazon WorkMail with an AD Connector directory, you can’t edit these details from the AWS Management Console. Instead, you must edit them using your Active Directory management tools. Limitations apply when your organization is in interoperability mode. For more information, see [Limitations in interoperability mode](p. 49).

**To edit a user’s details**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
   
   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see [Regions and endpoints](https://aws.amazon.com/about-aws/whats-new/) in the *Amazon Web Services General Reference*.

2. In the navigation pane, choose **Organizations**, then choose the organization that you want to use.

3. In the navigation pane, choose **Organizations**, and then choose the organization that you want to use.

4. In the navigation pane, choose **Users**, and then choose the name of the user to edit.

5. Do any of the following:

   **To edit personal data**
   1. In the **User details** section, choose **Edit**.
   2. Under **User details**, enter or change the user's personal information as needed.
   3. When finished, choose **Save changes**.

   **To edit mailbox quotas**
   1. Under **User details**, choose the **Quota** tab, and then choose **Edit**.
   2. In the **Update mailbox quota** box, enter a size for the mailbox. You can enter values from 1 to 51200.
   3. Choose **Save**.

   **To manage mobile device data**
   
   **Note**
   To manage mobile devices, your users first need to connect their devices to your instance of Amazon WorkMail. For information about connecting mobile devices, refer to [Setting up mobile device clients for Amazon WorkMail](https://docs.aws.amazon.com/workmail/latest/userguide/setting-up-mobile-devices.html).

   1. Under **User details**, choose the **Mobile devices** tab.
   2. To see a current list of devices, choose **Refresh**.
   3. To view a device's details, choose the device name from the **Device ID** column.
   4. To remove or wipe the device, choose the radio button next to the device name, and then choose **Remove** or **Wipe** as needed.
   5. In the dialog box that appears, confirm the removal or wipe operation. Remember that users will reappear when they sync their devices with Amazon WorkMail again.

   **To edit mailbox permissions**
   1. Choose the **Permissions** tab.
2. Do one of the following:
   a. To add permissions, choose Add permissions. Open the Add new permissions list and choose a user or group, choose the permission settings for the user or group, and then choose Save.
   b. To edit a user's permissions, choose the button next to the user's name. Choose Edit, select the desired options, and then choose Save.

   For more information about the permission options, refer to Working with mailbox permissions (p. 130).

3. To remove all permissions, choose Remove, then confirm the removal.

### Resetting user passwords

If a user forgets their password or has trouble signing in to Amazon WorkMail, you can reset their password.

**Note**

If you've integrated Amazon WorkMail with an AD Connector directory, you must reset the user password in Active Directory.

**To reset a user password**

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, then choose the name of your organization.

3. In the navigation pane, choose Users.

4. In the list of users, select the checkbox next to the name of the user, and then choose Reset password.

5. In the Reset Password dialog box, enter the new password, and then choose Reset.

### Troubleshooting Amazon WorkMail password policies

If resetting the password is unsuccessful, verify that the new password meets the password policy requirements.

The password policy requirements depend on which directory type your Amazon WorkMail organization uses.

**Amazon WorkMail directory and Simple AD directory password policy**

By default, passwords for an Amazon WorkMail directory or Simple AD directory must be:

- Non-empty
- At least eight characters
- Less than 64 characters
- Composed of Basic Latin or Latin-1 supplement characters

Passwords must also contain characters from three out of five of the following groups:

- Uppercase characters
• Lowercase characters
• Numerical digits (0 through 9)
• Special characters (for example, <, ~, or !)
• Latin-1 supplement characters (for example, é, ü, or ñ)

Amazon WorkMail directory password policies can't be changed.

To change a Simple AD password policy, use the AD administration tools on an Amazon Elastic Compute Cloud (Amazon EC2) Windows instance of your Simple AD directory. For more information, see Installing the Active Directory administration tools in the AWS Directory Service Administration Guide.

AWS Managed Microsoft AD Directory password policy

For information about the default password policy for an AWS Managed Microsoft AD directory, see Manage Password Policies for AWS Managed Microsoft AD in the AWS Directory Service Administration Guide.

AD Connector password policy

AD Connector uses the password policy of the Active Directory domain that it is connected to. See the documentation for your Active Directory domain for more information on password policy settings.

Viewing email headers

The information in email headers can help you troubleshoot common user email issues. Amazon WorkMail allows you to view the header information for any message.

To view email headers in Amazon WorkMail

1. In the Amazon WorkMail web application, double-click on the email message to open.
2. Choose Message options (the gear and envelope icon) located in the upper-right corner of the message, next to the Sent on date.

The email headers appear under Internet Headers.

Working with notifications

With the Amazon WorkMail Push Notifications API, you can receive push notifications about changes in your mailbox, including new email and calendar updates. You must register the URLs (or push notification responders) to receive notifications. With this feature, developers can create responsive applications for Amazon WorkMail users, as applications are quickly notified about changes from a user's mailbox.

For more information, see Notification subscriptions, mailbox events, and EWS in Exchange.

You can subscribe to specific folders, such as Inbox or Calendar, or to all folders for mailbox change events (including New Mail, Created, and Modified).

You can use client libraries such as the EWS Java API or the Managed EWS C# API to access this feature. A complete sample application of a push responder, developed using AWS Lambda and API Gateway (using the AWS Serverless framework), is available on the AWS GitHub page. It uses the EWS Java API.

The following is a sample push subscription request:
Working with notifications

```xml
  <Header xmlns="http://schemas.xmlsoap.org/soap/envelope/">
  </Header>
  <soap:Body>
    <m:Subscribe xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
      <m:PushSubscriptionRequest>
        <t:FolderIds>
          <t:DistinguishedFolderId Id="inbox" />
        </t:FolderIds>
        <t:EventTypes>
          <t:EventType>NewMailEvent</t:EventType>
          <t:EventType>CopiedEvent</t:EventType>
          <t:EventType>CreatedEvent</t:EventType>
          <t:EventType>DeletedEvent</t:EventType>
          <t:EventType>ModifiedEvent</t:EventType>
          <t:EventType>MovedEvent</t:EventType>
        </t:EventTypes>
        <t:StatusFrequency>1</t:StatusFrequency>
        <t:URL>https://YOUR_PUSH_RESPONDER_URL</t:URL>
      </m:PushSubscriptionRequest>
    </m:Subscribe>
  </soap:Body>
</soap:Envelope>
```

The following is a successful subscription request result:

```xml
  <Header xmlns="http://schemas.xmlsoap.org/soap/envelope/">
  </Header>
  <soap:Body>
      <m:ResponseMessages>
        <m:SubscribeResponseMessage ResponseClass="Success">
          <m:ResponseCode>NoError</m:ResponseCode>
          <m:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</m:SubscriptionId>
          <m:Watermark>AAAAAAA=</m:Watermark>
        </m:SubscribeResponseMessage>
      </m:ResponseMessages>
    </m:SubscribeResponse>
  </soap:Body>
</soap:Envelope>
```

Afterwards, notifications are sent to the URL specified in the subscription request. The following is a sample notification:

```xml
<soap:Envelope
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
  <t:RequestServerVersion Version="Exchange2010_SP2" />
  <soap:Header>
    <m:SendNotification
      xmlns="http://schemas.microsoft.com/exchange/services/2006/types"/>
  </soap:Header>
  <soap:Body>
    <m:SendNotificationRequest
      xmlns="http://schemas.microsoft.com/exchange/services/2006/messages">
      <m:MessageIds>
        <t:MessageId>
          <t:PrimarySmtpAddress>primary_smtp_address@example.com</t:PrimarySmtpAddress>
          <t:UniqueInstance>unique_instance</t:UniqueInstance>
        </t:MessageId>
      </m:MessageIds>
    </m:SendNotificationRequest>
  </soap:Body>
</soap:Envelope>
```
Working with notifications

To acknowledge that the push notification responder has received the notification, it must reply with the following:

```xml
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
  <soap:Header></soap:Header>
  <m:SendNotificationResponseMessage ResponseClass="Success">
    <m:ResponseCode>NoError</m:ResponseCode>
    <m:Notification>
      <t:SubscriptionId>hKJETtoAdi9PPWtZDQ4MTmhMDoYVY</t:SubscriptionId>
      <t:PreviousWatermark>ygwAAAAAAA=</t:PreviousWatermark>
      <t:MoreEvents>false</t:MoreEvents>
      <t:ModifiedEvent>
        <t:Watermark>ywwAAAAAAA=</t:Watermark>
        <t:TimeStamp>2018-02-02T15:15:14Z</t:TimeStamp>
        <t:FolderId Id="AAB2L089bS1kNDgxOGYwOGE5OTQ0="></t:FolderId>
        <t:ParentFolderId Id="AAB2L089bS1kNDgxOGYwOGE5OTQ0="></t:ParentFolderId>
      </t:ModifiedEvent>
    </m:Notification>
  </m:SendNotificationResponseMessage>
</soap:Envelope>
```

To unsubscribe from receiving push notifications, clients must send an unsubscribe response in the `SubscriptionStatus` field, similar to the following:

```xml
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
  <soap:Header></soap:Header>
  <m:SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/services/2006/messages">
    <SubscriptionStatus>Unsubscribe</SubscriptionStatus>
  </m:SendNotificationResult>
</soap:Envelope>
```

To verify the health of your push notification responder, Amazon WorkMail sends a “heartbeat” (also called a `StatusEvent`). The frequency with which they are sent is determined by the `StatusFrequency` parameter provided in the initial subscription request. For example, if `StatusFrequency` equals 1, a `StatusEvent` is sent every 1 minute. This value can range between 1 and 1440 minutes. This `StatusEvent` looks like the following:

```xml
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
  <soap:Header></soap:Header>
</soap:Envelope>
```
If a client push notification responder fails to respond with the same OK status as before, the notification is retried for a maximum of StatusFrequency minutes. For example, if StatusFrequency equals 5, and the first notification fails, it is retried for a maximum of 5 minutes with an exponential backoff between each retry. If the notification is not delivered after the retry time has expired, the subscription is invalidated and no new notifications are delivered. You must create a new subscription to continue to receive notifications about mailbox events. Currently, you can subscribe for a maximum of three subscriptions per mailbox.

### Enabling signed or encrypted email

You can use S/MIME to enable users to send signed or encrypted email both inside and outside of the organization.

**Note**
User certificates in the Global Address List (GAL) are supported only in a connected Active Directory setup.

**To enable users to send signed or encrypted emails**

1. Set up an Active Directory (AD) Connector. Setting up an AD Connector with your on-premises directory allows users to continue to use their existing corporate credentials.
2. Configure Certificate Autoenrollment to issue and store user certificates automatically in the Active Directory. Amazon WorkMail receives user certificates from the Active Directory and publishes them to the GAL. For more information, see Configure Certificate Autoenrollment.
3. Distribute the generated certificates to users by exporting the certificates from the server running Microsoft Exchange and mailing them.
4. Each user installs the certificate to their email program (such as Windows Outlook) and mobile devices.
Working with groups

You can use groups as distribution lists in Amazon WorkMail for receiving emails for generic email addresses, such as <sales@example.com> or <support@example.com>. You can create multiple email aliases for a group.

You can also use groups as security groups to share a mailbox or calendar with a certain team.

Groups don't have their own mailboxes, and that affects the mailbox permissions that you can grant to a group. For information about setting up mailbox permissions for a group, see Managing mailbox permissions for groups (p. 132).

Note
It can take up to 2 hours before newly added groups appear in your Microsoft Outlook offline address book.

Topics
- Create a group (p. 112)
- Enabling a group (p. 113)
- Adding users as members to a group (p. 113)
- Removing users from a group (p. 114)
- Disable a group (p. 114)
- Deleting a group (p. 115)

Create a group

You can create groups from the Amazon WorkMail console. You can also create aliases for your groups.

To create a group

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   If necessary, change the AWS Region In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, then choose the name of your organization.
3. In the navigation pane, choose Organizations, and then choose the name of your organization.
4. In the navigation pane, choose Groups, and then choose Create group.
   The Create a group page appears.
5. Under Group name, enter a name for the group.
6. Under Email address, enter the primary email address for the group.
7. Choose Create group.

To create a group alias

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   If necessary, change the AWS Region In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose **Organizations**, and then choose the name of your organization.
3. In the navigation pane, choose **Groups**, choose the name of the group that you want to change, and then choose **Edit**.

   The Create a group page appears.
4. Choose **Add alias**.

   The Group details page appears and displays the group's primary email address.
5. Choose **Add alias** again. In the **Email aliases** box, enter the group's alias.
6. Choose **Save changes**.

---

### Enabling a group

When you integrate Amazon WorkMail with your corporate Active Directory, or you already have groups available in your simple Active Directory, you can use those groups as security groups or distribution lists in Amazon WorkMail.

#### To enable an existing directory group

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).

   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see [Regions and endpoints](https://docs.aws.amazon.com/en_us/sts/latest/developerguide/regions-endpoints.html) in the Amazon Web Services General Reference.
2. In the navigation pane, choose **Organizations**, and then choose the name of your organization.
3. In the navigation pane, choose **Groups**.
4. Choose the checkbox next to the the group that you want to enable, and then choose **Enable**.

   The Enable groups dialog box appears and asks you to confirm the operation.
5. If needed, enter a different email address, then choose **Enable**.

---

### Adding users as members to a group

After you create and enable an Amazon WorkMail group, use the Amazon WorkMail console to add members to that group.

#### Note

If Amazon WorkMail is integrated with a connected Active Directory service or Microsoft Active Directory, you can use Active Directory to manage your group members. However, changes can take longer to propagate to Amazon WorkMail.

The following steps explain how to add up to 100 users at a time.

#### To add users to a group

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).

   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see [Regions and endpoints](https://docs.aws.amazon.com/en_us/sts/latest/developerguide/regions-endpoints.html) in the Amazon Web Services General Reference.
2. In the navigation pane, choose **Organizations**, then choose the name of your organization.
3. In the navigation pane, choose **Groups**.
Removing users from a group

Use the Amazon WorkMail console to remove users from a group.

**Note**
If Amazon WorkMail is integrated with a connected Active Directory or Microsoft Active Directory, you can use Active Directory to manage your group members. However, doing so can create the time needed to propagate your changes to Amazon WorkMail.

**To remove users from a group**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
2. In the navigation pane, choose Organizations, then choose the name of your organization.
3. In the navigation pane, choose Groups, then choose the name of the group.
4. On the **Group details** page, choose Members.
5. Choose Edit.
6. Under **Group members**, search for the users to add to the group, and select them.
7. Choose <<. The users no longer appear under **Group members**.
8. Choose Save.

Your changes can take a few minutes to propagate.

Disable a group

When you no longer need a group, you can disable it.

**To disable a group**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).
2. In the navigation pane, choose Organizations, then choose the name of your organization.
3. In the navigation pane, choose Groups.
4. In the list of groups, select the group to disable, and then choose Disable group.
5. In the Disable group(s) dialog box, choose Disable.

**Note**
To permanently delete a group, use the DeleteGroup API action for Amazon WorkMail. For more information, see DeleteGroup in the Amazon WorkMail API Reference.

### Deleting a group

Before you can delete a group, you must first disable that group. For information about disabling groups, see Disable a group (p. 114).

**To delete a group**

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, then choose the name of your organization.
3. In the navigation pane, choose Groups.
4. Select the checkbox next to the disabled group that you want to delete and choose **Delete**.
   The Delete group dialog box appears.
5. In the Enter the group name to confirm deletion box, enter the name of the group, then choose **Delete group**.
Creating a resource

You can add a new resource to your organization and allow your users to reserve it.

To add a resource

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of your organization.

3. In the navigation pane, choose Resources, and then Create resource.

   The Create resource page appears.

4. In the Resource name box, enter a name for the resource.

5. Optionally, in the Resource description box, enter a description for the resource.

6. Under Resource type, choose an option.

7. Verify the resource’s email address, change it as needed, then choose Create resource.

Editing resource details

You can edit a resource’s general details, including name, description, type, and email address, as well as booking options and delegates.

To edit general resource details

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   
   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, then choose the name of your organization.

3. In the navigation pane, choose Resources, and then select the resource to edit.
4. On the **General** tab, update the **Resource name**, **Description**, **Resource Type**, or **Email address** details as needed.

5. Choose **Save**.

You can configure a resource to accept or decline booking requests automatically.

**To enable or disable automatic processing of booking requests**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).

   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see **Regions and endpoints** in the **Amazon Web Services General Reference**.

2. In the navigation pane, choose **Organizations**, and then choose the name of your organization.

3. In the navigation pane, choose **Resources**, and then select the resource to edit. A page appears and displays **Resource details** and two tabs, **Booking options** and **Delegates**.

Do any of the following:

**To change a resource's details**

1. In the **Resource details** section, choose **Edit**.
2. As needed, change the resource's name, description, or type.

**To add an email alias to a resource**

1. In the **Resource details** section, choose **Edit**.
2. Under **Email address**, choose **Add alias**.
3. In the **Email aliases** box, enter an alias.
4. Repeat steps 2 and 3 as desired to enter more aliases.
5. Choose **Save changes**.

**To change a resource's booking options**

1. In the **Booking options** section, choose **Edit**.
2. As desired, select or clear the checkbox next to an option to enable or disable the option.

   **Note**
   When you disable any of the automatic booking options, you must create a delegate to handle the booking requests. The next steps explain how to create delegate.

3. Choose **Save**.

You can add a delegate to control booking requests for a resource that doesn't have automatic booking options configured. Resource delegates automatically receive copies of all booking requests and have full access to the resource calendar. In addition, they must accept all booking requests for a resource.

**To add a resource delegate**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).

   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see **Regions and endpoints** in the **Amazon Web Services General Reference**.
Disabling a resource

When you disable a resource, you make it unavailable for booking. For example, you can disable a conference room while it's being remodeled, then enable the room once it's available for use.

To disable a resource

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information about regions, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the organization which contains the resource that you want to disable.

3. In the navigation pane, choose Resources.

4. In the list of resources, select the button next to the resource that you want to disable, and then choose Disable.

   The Disable resource dialog box appears.

5. Choose Disable.

Enabling a resource

By default, Amazon WorkMail enables all resources when you create them. If you or someone else disables a resource, you can enable it at any time.

To enable a resource

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information about regions, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the organization which contains the resource that you want to enable.

3. In the navigation pane, choose Resources.

4. In the list of resources, select the button next to the resource that you want to enable, and then choose Enable.

   The Enable resource dialog box appears.
5. Choose **Enable**.

# Deleting a resource

You can remove unneeded resources at any time.

**To remove a resource**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).

   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information, see [Regions and endpoints](https://docs.aws.amazon.com/general/latest/grRegions.html) in the *Amazon Web Services General Reference*.

2. In the navigation pane, choose **Organizations**, and then choose the name of your organization.

When you no longer need a resource, you can delete it. However, you must first disable the resource. For information about disabling a resource, see the steps in the previous section.

**To remove a resource**

1. Open the Amazon WorkMail console at [https://console.aws.amazon.com/workmail/](https://console.aws.amazon.com/workmail/).

   If necessary, change the AWS Region. In the bar at the top of the console window, open the **Select a Region** list and choose a Region. For more information about regions, see [Regions and endpoints](https://docs.aws.amazon.com/general/latest/grRegions.html) in the *Amazon Web Services General Reference*.

2. In the navigation pane, choose **Organizations**, then choose the desired organization.

3. In the navigation pane, choose **Resources**.

4. In the list of resources, select the button next to the disabled resource that you want to remove, and then choose **Delete**.

   The **Delete resource** dialog box appears.

5. In the **Enter the resource name to confirm deletion** box, enter the name of the resource that you want to delete, and then choose **Delete resource**.
Working with mobile devices

The topics in this section explain how to manage mobile devices connected to Amazon WorkMail.

Topics

- Editing your organization's mobile device policy (p. 120)
- Managing mobile devices (p. 121)
- Managing mobile device access rules (p. 122)
- Managing mobile device access overrides (p. 125)
- Integrating with mobile device management solutions (p. 126)

Editing your organization's mobile device policy

You can edit your organization's mobile device policy to change the way that mobile devices interact with Amazon WorkMail.

To edit your organization's mobile device policy

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a region list and choose a Region. For more information, see Region Name and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of your organization.

3. In the navigation pane, choose Mobile Policies, and then on the Mobile policy screen, choose Edit.

4. Update any of the following as necessary:

   a. **Require encryption on device**: Encrypt email data on the mobile device.
   b. **Require encryption on storage card**: Encrypt email data on the mobile device's removable storage.
   c. **Password required**: Require a password to unlock a mobile device.
   d. **Allow simple password**: Use the device's PIN as the password.
   e. **Minimal password length**: Set the number of characters required for a valid password.
   f. **Require alphanumeric password**: Require passwords that consist of letters and numbers.
   g. **Number of failed attempts allowed**: Specify the number of failed login attempts that are allowed before the user is locked out of their account.
   h. **Password expiration**: Specify the number of days before a password expires and must be changed.
   i. **Enable screen lock**: Specify the number of seconds that must elapse without user input to lock the user's screen.
   j. **Enforce password history**: Specify the number of passwords that can be entered before repeating the same password.

5. Choose Save.
Managing mobile devices

The topics in this section explain how to remotely wipe mobile devices, remove devices from your organization, and view the details for devices. For information about editing your organization’s mobile device policy, see Editing your organization’s mobile device policy (p. 120).

Topics

• Remotely wiping mobile devices (p. 121)
• Removing user devices from the devices list (p. 121)
• Viewing mobile device details (p. 122)

Remotely wiping mobile devices

The steps in this section explain how to remotely wipe mobile devices. Remember the following:

• Devices must be online and connected to Amazon WorkMail. If someone disconnects the device, the wipe operation resumes when the user reconnects the device.
• Wipe operations can take five minutes to propagate.

Important

For most mobile devices, a remote wipe resets the device to factory defaults. All data, including personal files, can be removed when you perform this procedure.

To remotely wipe a user’s mobile device

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
2. If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a region list and choose a Region. For more information, see Region Name and endpoints in the Amazon Web Services General Reference.
3. In the navigation pane, choose Organizations, and then choose the name of your organization.
4. In the navigation pane, choose Users, and in the list of users, select the name of the user whose device you need to wipe.
5. Choose the Mobile devices tab.
6. In the list of devices, choose the button next to the device, and then choose Wipe.
7. Check the status in the overview to see whether the wipe is requested.
8. After the device is wiped, remove it from the devices list. The steps in the next section explain how.

Important

To return a wiped device to a user’s list of devices, make sure you first remove it from the devices list. Otherwise, the system wipes the device again.

Removing user devices from the devices list

If someone stops using a specific mobile device, or you’ve remotely wiped the device, you can remove the device from the devices list. When the user configures the device again, it shows up in the list.

To remove a user’s mobile devices from the devices list

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
If necessary, change the AWS Region. In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of your organization.
3. In the navigation pane, choose Users, and then select the user's name.
4. Choose the Mobile devices tab.
5. In the list of devices, select the button next to the device and choose Remove.

**Viewing mobile device details**

You can view the details of a user's mobile device.

*Note*
Some devices don't send all their details to the server. You may not see all available device details.

**To view device details**

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the Region. From the navigation bar, select the Region that meets your needs. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of your organization.
3. In the navigation pane, choose Users, and then choose the Mobile devices tab.
4. In the list of devices, select the ID of the device for which you want to view details.

The following table lists the device status codes.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROVISIONING_REQUIRED</td>
<td>A user or administrator has requested that the device be provisioned for use with Amazon WorkMail. Devices are also set to this status if the current policy for that device is modified in the Amazon WorkMail console.</td>
</tr>
<tr>
<td>PROVISIONING_SUCCEEDED</td>
<td>The device has been successfully provisioned. The device has enforced the given policy.</td>
</tr>
<tr>
<td>WIPE_REQUIRED</td>
<td>An administrator requested a wipe in the Amazon WorkMail console.</td>
</tr>
<tr>
<td>WIPE_SUCCEEDED</td>
<td>The device has been successfully wiped.</td>
</tr>
</tbody>
</table>

**Managing mobile device access rules**

Mobile device access rules for Amazon WorkMail allow administrators to control mailbox access for certain types of mobile devices. By default, each Amazon WorkMail organization uses a rule that grants mailbox access to any devices, regardless of type, model, operating system, or user agent. You can edit or replace that default rule with one of your own. You can also add, change, and delete rules.
Warning
If you delete all the mobile device access rules for an organization, Amazon WorkMail blocks all mobile device access.

You can create rules that allow or deny access based on the following device properties:

- **Device type**—"iPhone", "iPad", or "Android."
- **Device model**—"iPhone10C1", "iPad5C1", or "HTCOneX."
- **Device operating system**—"iOS 12.3.1 16F203", or "Android 8.1.0."
- **Device user agent**—"iOS/14.2 (18B92) exchangesyncd/1.0," or "Android-Mail/7.7.16.163886392.release."

To view device properties on the AWS Management Console, see Viewing mobile device details.

Note
Some devices and clients may not report properties for all fields. For information about working around those cases, see Dealing with empty fields.

Important
Amazon WorkMail mobile device access rules only apply to devices that use the Microsoft Exchange ActiveSync protocol. Mobile clients that use a different protocol, such as IMAP, don’t report the device properties listed here, so these rules won't apply. If you need to restrict access for devices that use other protocols, you can create access control rules. For more information about them, see Working with access control rules. As an example, you can restrict access to other protocols and webmail to just a range of corporate IP addresses, but allow Microsoft ActiveSync from elsewhere, and then use Mobile Device Access Rules to further limit the types and versions of allowed clients.

Topics
- How mobile device access rules work (p. 123)
- Using mobile device access rules (p. 124)

How mobile device access rules work

Mobile device access rules only apply to devices that use the Microsoft Exchange ActiveSync protocol. Each rule has a set of conditions that specify when the rule applies, plus an access effect of ALLOW or DENY for the device. A rule applies to an access request only if all of the conditions of the rule match properties of the user's mobile device. Rules with no conditions apply to all requests. Each condition uses a case-insensitive prefix match against the device's reported properties.

Amazon WorkMail evaluates rules as follows:

- If any DENY rule matches a device property, the policy blocks the device. DENY rules take precedence over ALLOW rules.
- If at least one ALLOW rule matches, and no DENY rule matches, the policy allows the device.
- If no rule applies, the device is blocked.

Important
Mobile devices report the properties that the rules use to operate. The devices report their properties during the Microsoft ActiveSync device provisioning process. Amazon WorkMail cannot independently verify that mobile clients report correct or up-to-date information.
Using mobile device access rules

You can use APIs or the AWS Command Line Interface (CLI) to create and manage mobile device access rules. For more information about the AWS CLI, see the [AWS Command Line Interface User Guide](https://docs.aws.amazon.com/cli/latest/userguide/)

**Important**

When you change an access rule for an Amazon WorkMail organization, the affected devices can take five minutes to follow the updated rule, and devices may show inconsistent behavior during that time. However, you immediately see correct behavior when you test rules. For more information, see [Testing mobile device access rules](#).

**Listing mobile device access rules**

The following example shows how to list mobile device access rules.

```bash
aws workmail list-mobile-device-access-rules --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56
```

**Creating mobile device access rules**

The following example creates a rule that blocks all Android devices from accessing mailboxes.

```bash
aws workmail create-mobile-device-access-rule --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types "android"
```

The following example creates a rule that only allows a specific version of iOS. Be sure to remove the default ALLOW-all rule.

```bash
aws workmail create-mobile-device-access-rule --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56 --name AllowLatestiOS --effect ALLOW --device-operating-systems "iOS 14.3"
```

**Updating mobile device access rules**

The following example updates a device rule by adding an identifier.

```bash
aws workmail update-mobile-device-access-rule --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d --name AllowLatestiOS --effect ALLOW --device-operating-systems "iOS 14.4"
```

**Deleting a mobile device access rule**

The following example deletes the mobile device access rule with the given identifier.

```bash
aws workmail delete-mobile-device-access-rule --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

**Testing mobile device access rules**

To test access rules, you can use the `GetMobileDeviceAccessEffect` API, or the `get-mobile-device-access-effect` command in the AWS CLI. For more information about the AWS CLI, see the [AWS Command Line Interface User Guide](https://docs.aws.amazon.com/cli/latest/userguide/).

When you test, you pass in the properties of a simulated mobile device, and the API or CLI returns the access effect—ALLOW or DENY—that a real mobile device with those properties would receive. For
example, this command tests whether an iPhone running iOS 14.2, plus the default mail app, can access a mailbox.

```bash
aws workmail get-mobile-device-access-effect
  --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56
  --device-type "iPhone" --device-model "iPhone10C1"
  --device-operating-system "iOS 14.2.1 16F203"
  --device-user-agent "iOS/14.2 (18B92) exchangesyncd/1.0"
```

Dealing with empty fields

Some mobile devices or clients may not report information for one or more fields, leaving the values empty. Rules can match against these devices by using the special value `$NONE` in a condition. For example, a rule with `DeviceTypes=["iphone", "ipad", "$NONE"]` will match devices that report a device type of "iphone" or "ipad", or don't report a device type at all.

Negative conditions such as `NotDeviceTypes` or `NotDeviceUserAgents` won't match these empty values. For example, a rule with `NotDeviceTypes=["android"]` will match devices that report a device type other than "android". However, the rule won't match devices that don't report a device type at all.

Managing mobile device access overrides

You use mobile device access overrides to override the results of mobile device access rules. The overrides apply to specific users and devices, and it reverses the default access rule. You can also use overrides to create one-off exceptions to access rules and allow or deny specific user and device pairs. In addition, you can use overrides with a `DefaultDenyAll` mobile device access rule. That defers access decisions to a third-party mobile device management (MDM) solution. For more information, see Managing overrides (p. 125) and Integrating with mobile device management solutions (p. 126)

Topics
- How mobile device access overrides work (p. 125)
- Managing overrides (p. 125)

How mobile device access overrides work

You create mobile device access overrides for a specific user and device pair. The override reverses the default access result when evaluating mobile device access rules for a given user and device. For example, if an access rule normally denies access, an access override allows that user and device to synchronize their email. Conversely, if an access rule normally allows access, you can create an override that prevents the user and device from synchronizing their mail. When you delete a mobile device access override, Amazon WorkMail again respects the result of the current mobile device access rules when deciding whether to grant access for that user and device.

Important
When you change a mobile device access override for an Amazon WorkMail organization, the affected devices can take five minutes to follow the updated override.

Managing overrides

Mobile device access overrides can be created, updated, or deleted using the API or AWS Command Line Interface. For more information about the AWS CLI, see the AWS Command Line Interface User Guide.

To find device ID, use the AWS Management Console. For more information, see Viewing mobile device details.
Integrating with mobile device management solutions

Amazon WorkMail supports some basic mobile device management capabilities through mobile device policies and mobile device access rules. However, those features can only interact with mobile devices through the Microsoft Exchange ActiveSync (EAS) protocol, so they have limited ability to introspect and enforce device security posture. Administrators who need greater control over device security and compliance can use a third-party mobile device management (MDM) solution.

Mobile device management solutions overview

You can configure your MDM solution in two modes, proxy or direct. Consult your MDM documentation to see which modes your solution supports.

In proxy mode, mobile devices use the Exchange Active Sync (EAS) protocol via your MDM solution to access Amazon WorkMail. The MDM solution uses device posture to allow or deny access to Amazon WorkMail data. On the Amazon WorkMail side, use an Access Control Rule that allows EAS access only
from the MDM solution's IP address or addresses. For more information, refer to Working with access control rules.

The following image shows a typical proxy mode configuration.

In direct mode, mobile devices use EAS to access Amazon WorkMail directly. Your MDM solution receives device posture changes and continually assesses whether each device meets those requirements. When the MDM solution detects a posture changes, such as a device going out of compliance, it can take several actions and typically emits notifications or events. An Amazon WorkMail administrator can set up a system to listen to these compliance status events and automatically create mobile device access overrides that allow or deny access to devices when they go in or out of compliance with the MDM device requirements.

The following image shows a typical direct mode configuration.
Configuring a WorkMail organization to integrate with a third-party MDM solution in direct mode

To integrate with a third-party mobile device management (MDM) solution in direct mode, you must meet these requirements:

- Create access control rules that restrict access to user devices to only the ActiveSync protocol.
- Create a default "deny-to-all" mobile device access rule to ensure that all unknown or unmanaged mobile devices are denied by default.
- Adopt a mobile device management solution that emits custom notifications or events when a device changes security posture, meaning it goes in or out of compliance.
- Create a custom software component to listen to those notifications and call the Amazon WorkMail SDK to create mobile device access overrides.

These components ensure that all user devices meet their MDM compliance requirements before being allowed to access their Amazon WorkMail mailboxes.

**Use access control rules to restrict mobile device access to ActiveSync**

You must ensure that all devices use only the ActiveSync protocol, and you can use access control rules to do so. For example, you can grant access to other mail protocols only from an internal corporate IP address range, and then allow only ActiveSync when accessing email from outside the corporate firewall. You must do this because only ActiveSync allows you to identify devices using a device ID. You can't use protocols such as the Internet Message Access Protocol (IMAP) or Exchange Web Services. For more information, see Working with access control rules (p. 86).

**Create a default 'deny to all' access rule**
To defer all mobile device access decisions to the third-party mobile device management solution, create an access rule that automatically denies all devices unless overridden on a per-user or per-device basis. For more information, refer to Managing mobile device access rules (p. 122).

This example shows a ‘deny to all’ rule.

```bash
aws workmail create-mobile-device-access-rule --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

React to device posture changes and create mobile device access overrides

You must configure your MDM solution to send notifications for device posture changes. These notifications must be consumed by a component that can use the Amazon WorkMail SDK to create or update mobile device access overrides. By default, Amazon WorkMail denies access to unmanaged or newly provisioned devices because of the default "deny to all" mobile device access rule shown earlier in this topic. When the MDM solution determines that the device meets all requirements and emits a notification indicating that the device is compliant, this component can react to this notification by creating a mobile device access override with an effect of ALLOW for the specified user and device. If the device later goes out of compliance, the mobile device management solution emits another notification, and the access override can be deleted or modified to deny access for that device. For more information, see Managing mobile device access overrides (p. 125).

For an example of Amazon WorkMail integrated with MDM, see this AWS sample application.
Working with mailbox permissions

You can use mailbox permissions in Amazon WorkMail to grant users and groups the right to work in other users' mailboxes. Mailbox permissions apply to an entire mailbox. They enable multiple users to access the same mailbox without sharing that mailbox's credentials. Users with mailbox permissions can read and modify mailbox data and send email from the shared mailbox.

Note
Users with permissions to a mailbox belonging to a user hidden from the global address list can still access the hidden user's mailbox.

The following list shows the permissions that you can grant:

- **Full Access** – Enables full read and write access to the mailbox, including permissions to modify folder-level permissions.
  
  **Note**
  
  This option is only available for users. Groups can't be granted full access rights.

- **Send On Behalf** – Enables a user or group to send email on behalf of another user. The mailbox owner appears in the *From:* header, and the sender appears in the *Sender:* header.

- **Send As** – Enables a user or group to send email as the mailbox owner, without showing the actual sender of the message. The mailbox owner appears in both the *From:* and *Sender:* headers.

- **None** – Prevents a user or group from sending emails.

  **Note**
  
  Granting mailbox permissions to a group extends those permissions to all the members of that group, including members of nested groups.

When you grant mailbox permissions, the Amazon WorkMail AutoDiscover service automatically updates access to those mailboxes for the users or groups you added.

For the Microsoft Outlook client in Windows, users with full access permissions can automatically access the shared mailboxes. Allow up to 60 minutes for the changes to propagate, and then restart Microsoft Outlook.

For the Amazon WorkMail web application and in other email clients, users with full access permissions can manually open the shared mailboxes. Opened mailboxes stay open, even between sessions, unless the user closes them.

**Topics**

- [About mailbox and folder permissions](#)
- [Managing mailbox permissions for users](#)
- [Managing mailbox permissions for groups](#)

About mailbox and folder permissions

Mailbox permissions apply to all folders within a mailbox. These permissions can only be enabled by the AWS account holder or an IAM user authorized to call the Amazon WorkMail management API. To set and change permissions for mailboxes, or for groups as a whole, use the AWS Management Console or the Amazon WorkMail API. You can manage up to 100 mailbox and group permissions from the console. To manage permissions for more users and groups, use the Amazon WorkMail API.
Managing mailbox permissions for users

You can use the Amazon WorkMail console to manage mailbox permissions for users, as well as groups. The following sections explain how to manage permissions for users. For information about managing permissions for groups, refer to Managing mailbox permissions for groups (p. 132).

Topics
- Adding permissions (p. 131)
- Editing mailbox permissions for users (p. 131)

Adding permissions

When you add permissions, you grant one user the right to perform one or more tasks in another user's mailbox. For example, say that Employee A needs to send messages on behalf of his supervisor, Employee B. To grant that permission, you go to Employee B's mailbox settings and grant Employee A permission to do the requested task.

To add mailbox permissions

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the Region. From the navigation bar, choose the Region that meets your needs. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of the organization for which you want to manage permissions.

3. In the navigation pane, choose Users, and then select the name of the user for whom you want to manage permissions.

4. Choose the Permissions tab, and then choose Add permissions.

   The Add permissions dialog box appears.

5. Open the Add new permissions list and select the user or group that needs access to the mailbox.

6. Under Mailbox permissions and Send permissions, choose the desired options.

7. Choose Add.

New permissions can take up to five minutes to propagate to users.

Editing mailbox permissions for users

When you edit mailbox permissions for a user, you change the access that others have to that user's mailbox. Editing mailbox permissions doesn't change access for the mailbox's original user.

To edit mailbox permissions

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the Region. From the navigation bar, choose the Region that meets your needs. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, and then choose the name of the organization for which you want to manage permissions.
3. In the navigation pane, choose Users, and then select the name of the user whose permissions you want to edit.
4. Choose the Permissions tab.
   A list of the users and groups that have access to the mailbox appears.
5. Select the radio button next to the user or group that you want to change, then do any of the following:

   **To remove a user’s permissions**
   1. Choose Remove.
      The Remove permissions dialog box appears.
   2. In the Remove permissions dialog box, choose Remove.

   **To edit a user’s permissions**
   1. Choose Edit.
      The Edit permissions dialog box appears.
   2. Set the permissions as needed, and then choose Save.

   **To grant another user permissions to the mailbox**
   1. Choose Add permissions.
      The Add permissions dialog box appears.
   2. Open the Add new permissions list and select the user that you want to add.
   3. Set the permissions as needed, and then choose Add.

Changes to permissions can take up to five minutes to propagate to users.

## Managing mailbox permissions for groups

You can add or remove group permissions for Amazon WorkMail.

### Note
You can’t apply Full Access permissions to a group, because groups don’t have a mailbox to access.

### To manage group permissions
1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   If necessary, change the AWS Region In the bar at the top of the console window, open the Select a Region list and choose a Region. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, then choose the name of the organization for which you want to manage permissions.
3. In the navigation pane, choose Groups, and then select the name of the group for which you want to set permissions.
4. Choose the **Permissions** tab, then choose **Add permissions**.

   The **Add permissions** dialog box appears.

5. Open the **Add new permissions** list and select the user or group to grant permissions for the mailbox.

6. Under **Mailbox permissions** and **Send permissions**, choose the desired options.

7. Choose **Add**.

Changes to permissions can take up to five minutes to propagate to users.
Programmatic access to mailboxes

To programmatically access Amazon WorkMail mailboxes, use the Exchange Web Services (EWS) protocol. With EWS, you can access all item types in a mailbox. Here are some EWS libraries that you can use with Amazon WorkMail:

- Java – EWS Java API
- .Net – EWS Managed API
- Python – Exchangelib

Amazon WorkMail also supports IMAP and SMTP protocols, which you can use to send and receive emails. You can see the URLs supported for Amazon WorkMail protocols under Amazon WorkMail endpoints and quotas.

When using the EWS protocol, Amazon WorkMail supports the following authentication methods:

- **Basic Authentication** – With basic authentication, you enter an email address and password.
- **Impersonation roles** – With impersonation roles, you access users' mailboxes without entering the user's credentials.

Topics

- Managing impersonation roles (p. 134)
- Using impersonation roles (p. 137)

Managing impersonation roles

With impersonation roles, administrators configure programmatic access to user's mailboxes without entering the user's credentials. Services and tools can assume an impersonation role to perform actions in user's mailboxes. Impersonation is only supported with the EWS protocol.

Impersonation roles overview

To allow impersonation, administrators must create an impersonation role with the following properties:

- **Role type** – Choose either Full access or Read only. The role type limits the kind of operations a role can perform.
- **Rules** – A list of rules that define which users the impersonation role can impersonate.

Amazon WorkMail evaluates the rules on the following conditions:

- If any DENY rule matches, the policy denies impersonation. DENY rules take precedence over any ALLOW rules.
- If at least one ALLOW rule matches, and no DENY rule matches, the policy allows impersonation.
- If no rule applies, impersonation is denied.

**Note**

To allow impersonation for all users in an Amazon WorkMail organization, create a rule with the ALLOW effect and with no conditions.
Warning
You must create rules to allow an impersonation role to impersonate a user. If you do not specify rules, an impersonation role can't assume a user's access rights.

After the impersonation role is created, you can use it to get access to users' mailboxes. For more information, see Using impersonation roles (p. 137).

Security considerations

The use of impersonation roles creates the potential for security issues within your Amazon WorkMail organization and AWS account. Here are some of the potential issues to consider when you create an impersonation role:

- **Transitive permissions** – If user A has access to user B’s mailbox, and an impersonation role is allowed to impersonate user A, then this impersonation role can impersonate user A's access permissions and access user’s B mailbox.

- **Access control** – You can use access control rules to limit impersonation role access. For more information, see Working with access control rules (p. 86).

- **IAM policy** – You can assign an AssumeImpersonationRole action to a particular Amazon WorkMail organization and impersonation role by using the workmail:ImpersonationRoleId condition. To see an IAM policy example, see How Amazon WorkMail works with IAM (p. 17).

Creating impersonation roles

You can create impersonation roles from the Amazon WorkMail console.

To create an impersonation role

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   
   If necessary, change the Region. From the navigation bar, choose the Region that meets your needs. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of the organization.

3. Choose Impersonation roles, and then choose Create role.

4. The Create impersonation role dialog box appears. Under Role, enter the following information:
   
   - **Name** – Enter a unique name for the impersonation role.
   - **(Optional) Description** – Enter a description for the impersonation role.
   - **Role type** – Choose Read only or Full access.

5. Under Rules, choose Add rule.

6. The Add rule dialog box appears. Enter the following information:
   
   - **Name** – Enter a unique name for the rule.
   - **(Optional) Description** – Enter a description for the rule.
   - **Under Effect**, choose Allow or Deny. This allows or denies access based on the conditions you select in the following step.
   - **(Optional) Under This rule**, choose Matches requests that impersonate the selected users to include specific users. Choose Matches requests that impersonate users other than the selected users to add users other than the selected users.

7. Choose Add rule.

   **Note**
   Rules are only saved when you save the corresponding role.
8. Choose Create role.

Editing impersonation roles

You can edit impersonation roles from the Amazon WorkMail console.

To edit an impersonation role

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the Region. From the navigation bar, choose the Region that meets your needs. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of the organization.

3. Choose Impersonation roles.

4. Select the impersonation role name you want to edit, then choose Edit.

5. The Edit impersonation role dialog box appears. Under Role, enter the following information:

   • Name – Enter a unique name for the impersonation role.
   • (Optional) Description – Enter a description for the impersonation role.
   • Role type – To give the impersonation role read only access to a user’s mailbox, choose Read only. To give the impersonation role rights to read and modify items in a user’s mailbox, choose Full access.

6. Under Rules, select the rule that you want to edit and choose Edit.

7. The Edit rule dialog box appears. Enter the following information:

   • Name – Edit the name of the rule.
   • (Optional) Description – Update or enter a description for the rule.
   • Under Effect, choose Allow to allow access when the conditions set in the rules are met. To deny access, choose Deny.
   • (Optional) Under This rule, choose Matches requests that impersonate the selected users to include specific users. Choose Matches requests that impersonate users other than the selected users to add users other than the selected users.

8. Choose Save.

9. Choose Save changes.

Important
When you change an impersonation rule, the affected mailboxes can take up to five minutes to update. During the rule update process, you may observe inconsistent behavior in your mailbox. However, if you test a role, Amazon WorkMail responds as expected based on the updated rule. For more information, see Testing impersonation roles (p. 136).

Testing impersonation roles

You can test an impersonation role from the Amazon WorkMail console.

To test an impersonation role

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

   If necessary, change the Region. From the navigation bar, choose the Region that meets your needs. For more information, see Regions and endpoints in the Amazon Web Services General Reference.

2. In the navigation pane, choose Organizations, and then choose the name of the organization.
Deleting impersonation roles

You can delete an impersonation role from the Amazon WorkMail console.

To delete an impersonation role

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.
   - If necessary, change the Region. From the navigation bar, choose the Region that meets your needs. For more information, see Regions and endpoints in the Amazon Web Services General Reference.
2. In the navigation pane, choose Organizations, and then choose the name of the organization.
3. Choose Impersonation roles.
4. Select the impersonation role name you want to delete.
5. Choose Delete.
6. The Delete role dialog box appears. To confirm deletion, enter the role's name into the dialog box and choose Delete.

Using impersonation roles

To access mailbox data, use the Amazon WorkMail API action AssumeImpersonationRole. For more details on Amazon WorkMail APIs, see API Reference.

AssumeImpersonationRole returns a Token. This Token must be passed within 15 minutes to the EWS protocol through the HTTP header Authorization.

The following examples demonstrate how to use impersonation roles with the EWS protocol. The constants used in the examples specify the following details unique to your organization and account:

- WORKMAIL_ORGANIZATION_ID – Amazon WorkMail organization ID
- IMPersonation_ROLE_ID – Impersonation role ID
- WORKMAIL_EWS_URL – EWS endpoint available at Amazon WorkMail endpoints and quotas
- EMAIL_ADDRESS – Email address of the user mailbox

Example Java – EWS Java API

```java
import software.amazon.awssdk.services.workmail.WorkMailClient;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleRequest;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleResponse;

import microsoft.exchange.webservices.data.core.ExchangeService;
import microsoft.exchange.webservices.data.core.enumeration.misc.ExchangeVersion;
import microsoft.exchange.webservices.data.misc.ImpersonatedUserId;
import microsoft.exchange.webservices.data.core.enumeration.misc.ConnectingIdType;
```
AssumeImpersonationRoleResponse response = workMailClient.assumeImpersonationRole(  
    AssumeImpersonationRoleRequest.builder()
    .organizationId(WORKMAIL_ORGANIZATION_ID)
    .impersonationRoleId(IMPERSONATION_ROLE_ID)
    .build());

ExchangeService exchangeService = new ExchangeService(ExchangeVersion.Exchange2010_SP2);
exchangeService.setUrl(URI.create(WORKMAIL_EWS_URL));
exchangeService.getHttpHeaders().put("Authorization", "Bearer " + response.token());
exchangeService.setImpersonatedUserId(new ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS));

Example .Net – EWS Managed API

using Amazon.WorkMail;
using Amazon.WorkMail.Model;

AssumeImpersonationRoleRequest request = new AssumeImpersonationRoleRequest();
request.OrganizationId = WORKMAIL_ORGANIZATION_ID;
request.ImpersonationRoleId = IMPERSION_ROLE_ID;
AssumeImpersonationRoleResponse response = workMailClient.AssumeImpersonationRole(request);

ExchangeService service = new ExchangeService(ExchangeVersion.Exchange2010_SP2);
service.Url = new Uri(WORKMAIL_EWS_URL);
service.HttpHeaders.Add("Authorization", "Bearer " + response.Token);
service.ImpersonatedUserId = new ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS);

Example Python – Exchangelib

import boto3
from requests.auth import AuthBase
from exchangelib.transport import AUTH_TYPE_MAP
from exchangelib import Configuration, Account, Version, IMPERSION
from exchangelib.version import EXCHANGE_2010_SP2

work_mail_client = boto3.client("workmail")

class ImpersonationRoleAuth(AuthBase):
    def __init__(self):
        self.token = work_mail_client.assume_impersonation_role(  
            OrganizationId=WORKMAIL_ORGANIZATION_ID,
            ImpersonationRoleId=IMPERSONATION_ROLE_ID)
            ]["Token"]

    def __call__(self, r):
        r.headers["Authorization"] = "Bearer " + self.token
        return r

AUTH_TYPE_MAP["ImpersonationRoleAuth"] = ImpersonationRoleAuth

ews_config = Configuration(  
    service_endpoint=WORKMAIL_EWS_URL,
    version=Version(build=EXCHANGE_2010_SP2),
    auth_type="ImpersonationRoleAuth"
ews_account = Account(
    config=ews_config,
    primary_smtp_address=EMAIL_ADDRESS,
    access_type=IMPERSONATION
)
Exporting mailbox content

Use the StartMailboxExportJob API action in the Amazon WorkMail API Reference to export Amazon WorkMail mailbox content to an Amazon Simple Storage Service (Amazon S3) bucket. This action exports all email messages and calendar items from the specified mailbox to a .zip file in the Amazon S3 bucket, in MIME format. Other items, such as contacts and tasks, are not exported.

The time it takes for the mailbox export job to finish is dependent on the size and number of items in the mailbox. Because the mailbox export job takes place over a period of time, it does not represent a snapshot of the mailbox content at a single point in time. To see the status of an export job, use the DescribeMailboxExportJob or ListMailboxExportJobs API actions in the Amazon WorkMail API Reference.

When a mailbox export job is completed, the .zip file in the Amazon S3 bucket is encrypted using the symmetric AWS Key Management Service (AWS KMS) customer master key (CMK) that you provide. Because AWS KMS encryption is integrated with Amazon S3, the decrypted data is visible to the user who downloads it, as long as the user has access to the AWS KMS CMK.

Prerequisites

The following are prerequisites for exporting mailbox content:

- The ability to program.
- An Amazon WorkMail administrator account.
- An Amazon S3 bucket that does not allow public access. For more information, see Using Amazon S3 block public access in the Amazon Simple Storage Service User Guide and the Amazon Simple Storage Service User Guide.
- A symmetric AWS KMS CMK. For more information, see Getting started in the AWS Key Management Service Developer Guide.
- An AWS Identity and Access Management (IAM) role with a policy that grants permission to write to the Amazon S3 bucket and encrypt the sent files with the AWS KMS CMK. For more information, see How Amazon WorkMail works with IAM (p. 17).

IAM policy examples and role creation

The following example shows an IAM policy that grants permission to write to the Amazon S3 bucket and encrypt the sent files with the AWS KMS CMK. To use this example policy in the following Example: Exporting mailbox content (p. 142) procedure, save the policy as a JSON file with file name mailbox-export-policy.json.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
      ],
    },
  ],
}
```
The following example shows an IAM trust policy that is attached to the IAM role you create. To use this example policy in the following Example: Exporting mailbox content (p. 142) procedure, save the policy as a JSON file with file name mailbox-export-trust-policy.json.

You don't have to use the aws:SourceArn and aws:SourceAccount conditions at the same time. For example, you can remove aws:SourceArn from the policy if you need to use the same role to export messages from different Amazon WorkMail organizations under the same AWS account. For more information about condition keys, refer to the AWS global condition context keys in the AWS Identity and Access Management user guide.

You can use the AWS CLI to create the IAM role in your account by running the following commands.
Example: Exporting mailbox content

After you create the IAM role and policies in the preceding section, complete the following steps to export your mailbox content. You must have your Amazon WorkMail organization ID and user ID (entity ID), which you can access in the Amazon WorkMail console or by using the Amazon WorkMail API.

Example: To export mailbox content

1. Use the AWS CLI to start the mailbox export job.

   ```bash
   aws workmail start-mailbox-export-job --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56 --entity-id S-1-1-1111111111-2222222222-3333333333-3333 --kms-key-arn:aws:kms:us-east-1:111122223333:key/KEY-ID --role-arn arn:aws:iam::111122223333:role/WorkmailMailboxExportRole --s3-bucket-name AWSDOC-EXAMPLE-BUCKET --s3-prefix S3-PREFIX
   ```

2. Use the AWS CLI to monitor the state of the mailbox export jobs for your Amazon WorkMail organization.

   ```bash
   aws workmail list-mailbox-export-jobs --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56
   ```

   Alternatively, use the job ID generated by the `start-mailbox-export-job` command to monitor the state of that mailbox export job only.

   ```bash
   aws workmail describe-mailbox-export-job --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
   ```

When the mailbox export job state is **COMPLETED**, the exported mailbox items are available in a `.zip` file in the specified Amazon S3 bucket.

The following is an example of the output log from the exported mailbox:

```json
{
   "totalNonExportableItems" : "13",
   "totalMessages" : "76",
   "sha384Hash" : "Ade93a***96a1dd",
   "totalBytes" : "161892",
   "totalFolders" : "15",
   "startTime" : "168***380",
   "endTime" : "168***384"
}
```
Note

totalNonExportableItems are unsupported items like notes and contacts.

Considerations

The following considerations apply when exporting mailbox jobs for Amazon WorkMail:

• You can run up to 10 concurrent mailbox export jobs for a given Amazon WorkMail organization.
• You can run a mailbox export job for a given mailbox as often as once every 24 hours.
• The following resources must all be in the same AWS Region:
  • Amazon WorkMail organization
  • AWS KMS CMK
  • Amazon S3 bucket
Troubleshooting mail routing issues

If a user stops receiving emails, your Amazon WorkMail organization may be experiencing a mail routing issue. The steps in this section explain common ways to resolve delivery and routing issues.

Inbound mail issues:

• Check the MX record for the domain associated with your Amazon WorkMail organization. WorkMail should be the only entry and should have the lowest priority. Multiple MX records can lead to the wrong service receiving messages. For more information about MX records, see Verifying domains (p. 93).

• Check the Domain-based Message Authentication, Reporting, and Conformance (DMARC) settings for your organization in the Amazon WorkMail console. DMARC records are used to protect against common attacks, such as spoofing or phishing, that can compromise a user’s account credentials. For more information about DMARC, see Enforcing DMARC policies on incoming email (p. 84).

• Check the Amazon Simple Email Service inbound rule. If the rule contains actions other than Amazon WorkMail, those actions can fail and cause Amazon WorkMail to stop receiving mail. For more information about Amazon SES rules, see Integrate with Amazon WorkMail action in the Amazon Simple Email Service Developer Guide.

• Enable message tracking in Amazon WorkMail, and then check the logs for delivery problems. For more information about message tracking, see Enabling event logging (p. 40).

Outbound mail issues

• Ensure your SPF record includes Amazon SES. Check the domains page in the Amazon WorkMail console to verify. For more information about SPF, see Authenticating email with SPF (p. 102).

• Ensure Amazon WorkMail has permissions to use the domain. If not, add the domain again. Adding a domain (p. 90) in this guide provides the how-to steps.
Using email journaling with Amazon WorkMail

You can set up journaling to record your email communication, using integrated third-party archiving and eDiscovery tools. This ensures that email storage compliance regulations for privacy protection, data storage, and information protection are met.

Using journaling

Amazon WorkMail journals all email messages that are sent to any user in the specified organization, as well as all email messages sent by users in that organization. A copy of all email messages is sent to an address specified by the system administrator, in a format called journal record. This format is compatible with Microsoft email programs. There is no additional charge for email journaling.

Two email addresses are used for email journaling—a journaling email address and a report email address. The journaling email address is the address of a dedicated mailbox or third-party device that is integrated with your account, where journal reports are sent. The report email address is the address of your system administrator, where notifications of failed journal reports are sent.

All journal records are sent from an email address that is automatically added to your domain and looks like the following.

amazonjournaling@yourorganization.awsapps.com

There is no mailbox associated with this address, and you won't be able to create one using this name or address.

**Note**
don't delete the following domain record from the Amazon Simple Email Service (Amazon SES) console, or email journaling stops functioning.

yourorganization.awsapps.com

Every incoming or outgoing email message generates one journal record, regardless of the number of recipients or user groups. Email that fails to generate a journal record generates an error notification, which is sent to the report email address.

To enable email journaling

1. Open the Amazon WorkMail console at https://console.aws.amazon.com/workmail/.

2. In the navigation pane, choose Organizations, then choose the name of your organization.

3. In the navigation pane, Organization settings, choose the Journaling tab, and then choose Edit.

4. Move the Journaling status slider to the on position.

5. in the Journaling email address box, enter the email address given by your email journaling provider.
Note
We recommend using a dedicated journaling provider.

6. In the **Report email address**, enter the email administrator’s address.
7. Choose **Save**. The changes apply immediately.
# Document history

The following table describes important changes in each release of the *Amazon WorkMail Administrator Guide*. For notification about updates to this documentation, you can subscribe to an RSS feed.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Layer Security (TLS) support (p. 147)</td>
<td>Amazon WorkMail discontinued support for Transport Layer Security (TLS) 1.0 and 1.1. If you are using TLS 1.0 or 1.1, you must upgrade the TLS version to 1.2.</td>
<td>November 2, 2023</td>
</tr>
<tr>
<td>Remote users (p. 147)</td>
<td>Remote users are Amazon WorkMail users hosted outside the Amazon WorkMail organization or hosted on a different email domain. For more information, see <em>Users</em> in the <em>Amazon WorkMail Administrator Guide</em>.</td>
<td>September 18, 2023</td>
</tr>
<tr>
<td>Programmatic access to mailboxes (p. 147)</td>
<td>Amazon WorkMail now offers Impersonation Roles to grant programmatic access to mailboxes. For more information, see <em>Programmatic access to mailboxes</em> in the <em>Amazon WorkMail Administrator Guide</em>.</td>
<td>October 4, 2022</td>
</tr>
<tr>
<td>Configure Custom Availability Providers on Amazon WorkMail (p. 147)</td>
<td>Amazon WorkMail supports the use of Custom Availability Providers (CAPs). For more information, see <em>Configuring a Custom Availability Provider</em> in the <em>Amazon WorkMail Administrator Guide</em>.</td>
<td>June 30, 2022</td>
</tr>
<tr>
<td>Console changes for creating an organization (p. 147)</td>
<td>The Amazon WorkMail console experience for creating an organization is updated. For more information, see <em>Creating an organization</em> in the <em>Amazon WorkMail Administrator Guide</em>.</td>
<td>October 23, 2020</td>
</tr>
<tr>
<td>Exporting mailbox content (p. 147)</td>
<td>Use the StartMailboxExportJob API action to export Amazon WorkMail mailbox content to an Amazon Simple Storage Service (Amazon S3) bucket. For more information, see <em>Exporting mailbox content</em> in the <em>Amazon WorkMail Administrator Guide</em>.</td>
<td>September 22, 2020</td>
</tr>
<tr>
<td><strong>Mailbox retention policies (p. 147)</strong></td>
<td>Set mailbox retention policies for your Amazon WorkMail organization that automatically delete email messages after a time period that you choose. For more information, see Setting mailbox retention policies in the Amazon WorkMail Administrator Guide.</td>
<td>May 28, 2020</td>
</tr>
<tr>
<td><strong>Synchronous and asynchronous Run Lambda actions (p. 147)</strong></td>
<td>Choose synchronous or asynchronous configurations for Run Lambda actions in Amazon WorkMail email flow rules. For more information, see Configuring AWS Lambda for Amazon WorkMail in the Amazon WorkMail Administrator Guide.</td>
<td>May 11, 2020</td>
</tr>
<tr>
<td><strong>Working with access control rules (p. 147)</strong></td>
<td>Access control rules allow Amazon WorkMail administrators to control how their organization's mailboxes are accessed. For more information, see Working with access control rules in the Amazon WorkMail Administrator Guide.</td>
<td>February 12, 2020</td>
</tr>
<tr>
<td><strong>Tagging an organization (p. 147)</strong></td>
<td>Tag an Amazon WorkMail organization to differentiate between organizations in the AWS Billing and Cost Management console, or to control access to organization resources. For more information, see Tagging an organization in the Amazon WorkMail Administrator Guide.</td>
<td>January 23, 2020</td>
</tr>
<tr>
<td><strong>Enforce DMARC policies on incoming email (p. 147)</strong></td>
<td>For more information, see Enforcing DMARC policies on incoming email in the Amazon WorkMail Administrator Guide.</td>
<td>October 17, 2019</td>
</tr>
<tr>
<td><strong>Retrieving message content with Lambda (p. 147)</strong></td>
<td>Use the Amazon WorkMail Message Flow API with AWS Lambda to retrieve message content. For more information, see Retrieving message content with Lambda in the Amazon WorkMail Administrator Guide.</td>
<td>September 12, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>Logging Amazon WorkMail email events (p. 147)</td>
<td>Enable email event logging in the Amazon WorkMail console to track email messages for your organization. For more information, see Tracking messages in the Amazon WorkMail Administrator Guide.</td>
<td>May 13, 2019</td>
</tr>
<tr>
<td>Route 53 DNS record insertion (p. 147)</td>
<td>When setting up a domain that is managed in a Route 53 public hosted zone, Amazon WorkMail automatically inserts the DNS records for you. For more information, see Adding a domain in the Amazon WorkMail Administrator Guide.</td>
<td>February 13, 2019</td>
</tr>
<tr>
<td>Configuring Lambda for inbound email rule actions (p. 147)</td>
<td>Amazon WorkMail supports configuring Lambda functions to use with inbound email flow rules. For more information, see Managing email flows in the Amazon WorkMail Administrator Guide.</td>
<td>January 24, 2019</td>
</tr>
<tr>
<td>Configuring Lambda for Amazon WorkMail (p. 147)</td>
<td>Amazon WorkMail supports configuring Lambda functions to use with outbound email flow rules. For more information, see Configuring Lambda for Amazon WorkMail in the Amazon WorkMail Administrator Guide.</td>
<td>November 19, 2018</td>
</tr>
<tr>
<td>SMTP routing (p. 147)</td>
<td>Amazon WorkMail supports configuring SMTP gateways to use with outbound email flow rules. For more information, see Configuring SMTP gateways in the Amazon WorkMail Administrator Guide.</td>
<td>November 1, 2018</td>
</tr>
<tr>
<td>Debugging tools for custom domains (p. 147)</td>
<td>Amazon WorkMail has added debugging tools for custom domains. For more information, see Adding a domain in the Amazon WorkMail Administrator Guide.</td>
<td>October 15, 2018</td>
</tr>
<tr>
<td>Support for Outlook 2019 (p. 147)</td>
<td>Amazon WorkMail supports Outlook 2019 for Windows and macOS. For more information, see Amazon WorkMail system requirements in the Amazon WorkMail Administrator Guide.</td>
<td>October 1, 2018</td>
</tr>
<tr>
<td>Various updates (p. 147)</td>
<td>Various updates to topic layout and organization.</td>
<td>July 12, 2018</td>
</tr>
<tr>
<td>Feature Description</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Mailbox permissions (p. 147)</td>
<td>You can use mailbox permissions in Amazon WorkMail to grant users or groups the right to work in other users' mailboxes. For more information, see Working with mailbox permissions in the Amazon WorkMail Administrator Guide.</td>
<td>April 9, 2018</td>
</tr>
<tr>
<td>Support for AWS CloudTrail (p. 147)</td>
<td>Amazon WorkMail is integrated with AWS CloudTrail. For more information, see Logging Amazon WorkMail API calls with AWS CloudTrail in the Amazon WorkMail Administrator Guide.</td>
<td>December 12, 2017</td>
</tr>
<tr>
<td>Support for email flows (p. 147)</td>
<td>You can set up email flow rules for handling incoming email based on a sender's email address or domain. For more information, see Managing email flows in the Amazon WorkMail Administrator Guide.</td>
<td>July 5, 2017</td>
</tr>
<tr>
<td>Updates to Quick Setup (p. 147)</td>
<td>Quick Setup now creates an Amazon WorkMail directory for you. For more information, see Set up Amazon WorkMail with Quick Setup in the Amazon WorkMail Administrator Guide.</td>
<td>May 10, 2017</td>
</tr>
<tr>
<td>Support for a wider range of email clients (p. 147)</td>
<td>You can now use Amazon WorkMail with Microsoft Outlook 2016 for Mac and IMAP email clients. For more information, see System requirements for Amazon WorkMail in the Amazon WorkMail Administrator Guide.</td>
<td>January 9, 2017</td>
</tr>
<tr>
<td>Support for SMTP journaling (p. 147)</td>
<td>You can set up journaling to record your email communication. For more information, see Using email journaling with Amazon WorkMail in the Amazon WorkMail Administrator Guide.</td>
<td>November 25, 2016</td>
</tr>
<tr>
<td>Support for email redirection to external email addresses (p. 147)</td>
<td>You can set up email redirection rules by updating the Amazon SES identity policy for your domain. For more information, see Edit domain identity policies in the Amazon WorkMail Administrator Guide.</td>
<td>October 26, 2016</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Support for interoperability (p. 147)</td>
<td>You can enable interoperability between Amazon WorkMail and Microsoft Exchange. For more information, see <a href="#">Interoperability between Amazon WorkMail and Microsoft Exchange</a> in the <em>Amazon WorkMail Administrator Guide</em>.</td>
<td>October 25, 2016</td>
</tr>
<tr>
<td>Support for reserving resources (p. 147)</td>
<td>Support for reserving resources, such as meeting rooms and equipment. For more information, see <a href="#">Working with resources</a> in the <em>Amazon WorkMail Administrator Guide</em>.</td>
<td>October 19, 2015</td>
</tr>
<tr>
<td>Support for the email migration tool (p. 147)</td>
<td>Support for the email migration tool. For more information, see <a href="#">Migrating to Amazon WorkMail</a> in the <em>Amazon WorkMail Administrator Guide</em>.</td>
<td>August 16, 2015</td>
</tr>
<tr>
<td>Preview release of Amazon WorkMail (p. 147)</td>
<td>The preview release of Amazon WorkMail.</td>
<td>January 28, 2015</td>
</tr>
</tbody>
</table>