



Panduan Administrator

Amazon WorkMail



Versi 1.0

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon WorkMail: Panduan Administrator

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

.....	ix
Apa itu Amazon WorkMail?	1
Persyaratan WorkMail sistem Amazon	1
WorkMail Konsep Amazon	2
Layanan AWS terkait	3
WorkMail Harga Amazon	4
Sumber daya	4
Amazon WorkMail Akhir Dukungan	6
Solusi alternatif	6
Mengekspor data	6
Butuh bantuan atau punya pertanyaan?	6
Prasyarat	7
Mendaftar untuk Akun AWS	7
Berikan izin kepada pengguna IAM untuk Amazon WorkMail	7
Keamanan	8
Perlindungan data	9
Bagaimana Amazon WorkMail menggunakan AWS KMS	10
Manajemen identitas dan akses	19
Audiens	20
Mengautentikasi Dengan identitas	20
Mengelola akses menggunakan kebijakan	21
Bagaimana Amazon WorkMail bekerja dengan IAM	23
Identity-based contoh kebijakan	29
Pemecahan masalah	36
AWS kebijakan terkelola	38
AmazonWorkMailFullAccess	39
AmazonWorkMailReadOnlyAccess	39
AmazonWorkMailEventsServiceRolePolicy	39
Pembaruan kebijakan	40
Menggunakan Peran Terkait Layanan	40
Service-linked izin peran untuk Amazon WorkMail	41
Membuat peran terkait layanan untuk Amazon WorkMail	41
Mengedit peran terkait layanan untuk Amazon WorkMail	42
Menghapus peran terkait layanan untuk Amazon WorkMail	42

Wilayah yang Didukung untuk peran WorkMail terkait layanan Amazon	43
Pencatatan log dan pemantauan	43
Pemantauan dengan CloudWatch metrik	45
Memantau log peristiwa WorkMail email Amazon	48
Memantau log WorkMail audit Amazon	54
Menggunakan CloudWatch Wawasan dengan Amazon WorkMail	61
Mencatat panggilan WorkMail API Amazon dengan AWS CloudTrail	65
Mengaktifkan pencatatan peristiwa email	69
Mengaktifkan pencatatan audit	73
Validasi kepatuhan	88
Ketahanan	88
Keamanan infrastruktur	89
Memulai	90
Memulai dengan Amazon WorkMail	90
Langkah 1: Masuk ke WorkMail konsol Amazon	91
Langkah 2: Siapkan WorkMail situs Amazon Anda	91
Langkah 3: Siapkan akses WorkMail pengguna Amazon	92
Sumber daya lainnya	93
Migrasi ke Amazon WorkMail	93
Langkah 1: Buat atau aktifkan pengguna di Amazon WorkMail	93
Langkah 2: Migrasi ke Amazon WorkMail	93
Langkah 3: Selesaikan migrasi ke Amazon WorkMail	94
Interoperabilitas antara Amazon dan WorkMail Microsoft Exchange	95
Prasyarat	95
Menambahkan domain dan mengaktifkan kotak pesan	96
Aktifkan interoperabilitas	97
Buat akun layanan di Microsoft Exchange dan Amazon WorkMail	97
Keterbatasan dalam mode interoperabilitas	97
Konfigurasi setelan ketersediaan di Amazon WorkMail	98
Konfigurasi penyedia EWS-based ketersediaan	98
Mengkonfigurasi Penyedia Ketersediaan Kustom	100
Membangun fungsi CAP Lambda	100
Konfigurasi pengaturan ketersediaan di Microsoft Exchange	109
Aktifkan perutean email antara pengguna Microsoft Exchange dan Amazon WorkMail	109
Aktifkan perutean email untuk pengguna	110
Konfigurasi pengaturan pos	112

Konfigurasi klien email	112
Menonaktifkan mode interoperabilitas dan menonaktifkan server email Anda	113
Pemecahan masalah	114
WorkMail Kuota Amazon	115
WorkMail Organisasi Amazon dan kuota pengguna	115
WorkMail kuota pengaturan organisasi	118
Per-user kuota	118
Kuota pesan	119
Bekerja dengan organisasi	121
Membuat organisasi	121
Perubahan penting untuk AD Terkelola	123
Membuat organisasi	123
Integrasi AD Terkelola	125
Melihat detail organisasi	126
Mengintegrasikan direktori WorkSpaces	126
Status dan deskripsi organisasi	127
Menghapus organisasi	127
Menemukan alamat email	129
Bekerja dengan pengaturan organisasi	129
Mengaktifkan migrasi kotak pesan	130
Mengaktifkan penjurnalan	130
Mengaktifkan interoperabilitas	130
Mengaktifkan gateway SMTP	130
Mengelola alur email	131
Memberlakukan kebijakan DMARC pada email masuk	156
Penandaan sebuah organisasi	157
Bekerja dengan aturan kontrol akses	159
Membuat aturan kontrol akses	160
Mengedit aturan kontrol akses	161
Menguji aturan kontrol akses	161
Menghapus aturan kontrol akses	162
Mengatur kebijakan penyimpanan kotak pesan	163
Bekerja dengan domain	165
Menambahkan domain	165
Menghapus domain	170
Memilih domain default	170

Memverifikasi domain	171
Memverifikasi catatan TXT dan catatan MX dengan layanan DNS	172
Pemecahan masalah verifikasi domain	175
Mengaktifkan AutoDiscover untuk mengkonfigurasi titik akhir	176
AutoDiscover pemecahan masalah fase 2	180
Mengedit kebijakan identitas domain	182
Kebijakan utama layanan Amazon SES khusus	183
Mengautentikasi Email dengan SPF	184
Mengkonfigurasi domain PESAN DARI kustom	184
Bekerja dengan pengguna	186
Melihat daftar pengguna	186
Menambahkan pengguna	187
Mengaktifkan pengguna	188
Mengelola alias pengguna	188
Menonaktifkan pengguna	189
Mengedit detail pengguna	190
Mengatur ulang kata sandi pengguna	193
Memecahkan masalah kebijakan kata sandi Amazon WorkMail	194
Bekerja dengan notifikasi	195
Mengaktifkan email yang ditandatangani atau dienkripsi	199
Bekerja dengan grup	201
Melihat daftar grup	201
Menambahkan grup	202
Mengaktifkan grup	203
Menambahkan anggota ke grup	203
Mengedit detail grup	204
Menghapus anggota dari grup	205
Mengelola alias grup	205
Menonaktifkan grup	206
Menghapus grup	207
Bekerja dengan sumber daya	208
Melihat daftar sumber daya	208
Menambahkan sumber daya	209
Mengedit detail sumber daya	209
Mengelola alias sumber daya	212
Mengaktifkan sumber daya	213

Menonaktifkan sumber daya	214
Menghapus sumber daya	214
Bekerja dengan IAM Identity Center	216
Mengaktifkan Pusat Identitas IAM di Amazon WorkMail	218
Menetapkan pengguna dan grup Pusat Identitas IAM ke aplikasi Amazon WorkMail	218
Mengaitkan WorkMail pengguna Amazon dengan pengguna IAM Identity Center	221
Mode autentikasi	222
Mengkonfigurasi token akses pribadi	223
Menonaktifkan Pusat Identitas IAM	225
Bekerja dengan perangkat seluler	226
Mengedit kebijakan perangkat seluler organisasi	226
Mengelola perangkat seluler	227
Menghapus perangkat seluler dari jarak jauh	227
Menghapus perangkat pengguna dari daftar perangkat	228
Melihat detail perangkat seluler	229
Mengelola aturan akses perangkat seluler	230
Cara kerja aturan akses perangkat seluler	231
Menggunakan aturan akses perangkat seluler	232
Mengelola penggantian akses perangkat seluler	234
Cara kerja penggantian akses perangkat seluler	235
Mengelola penggantian	235
Mengintegrasikan dengan solusi manajemen perangkat seluler	236
Ikhtisar solusi manajemen perangkat seluler	236
Mengkonfigurasi WorkMail organisasi untuk berintegrasi dengan solusi MDM pihak ketiga dalam mode langsung	238
Bekerja dengan izin kotak pesan	240
Tentang izin kotak pesan dan folder	241
Mengelola izin kotak pesan untuk pengguna	241
Menambahkan izin	242
Mengedit izin kotak pesan untuk pengguna	242
Mengelola izin kotak pesan untuk grup	244
Akses terprogram ke kotak surat	245
Mengelola peran peniruan	245
Ikhtisar peran peniruan	245
Pertimbangan keamanan	246
Membuat peran peniruan	247

Mengedit peran peniruan	248
Menguji peran peniruan	249
Menghapus peran peniruan	250
Menggunakan peran peniruan	250
Mengekspor konten kotak pesan	253
Prasyarat	253
Contoh kebijakan IAM dan pembuatan peran	254
Contoh: Mengekspor konten kotak surat	256
Pertimbangan-pertimbangan	257
Pemecahan Masalah	180
Melihat header email	258
Perutean surat	258
Menggunakan jurnal email dengan Amazon WorkMail	260
Menggunakan penjurnalan	260
Riwayat dokumen	262

Pemberitahuan akhir dukungan: Pada 31 Maret 2027, AWS akan mengakhiri dukungan untuk Amazon WorkMail. Setelah 31 Maret 2027, Anda tidak akan lagi dapat mengakses WorkMail konsol Amazon atau WorkMail sumber daya Amazon. Untuk informasi selengkapnya, lihat [dukungan WorkMail akhir Amazon](#).

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.

Apa itu Amazon WorkMail?

Amazon WorkMail adalah layanan email dan kalender bisnis yang aman dan terkelola dengan dukungan untuk klien email desktop dan seluler yang ada. WorkMail Pengguna Amazon dapat mengakses email, kontak, dan kalender mereka menggunakan Microsoft Outlook, browser mereka, atau aplikasi email iOS dan Android asli mereka. Anda dapat mengintegrasikan Amazon WorkMail dengan direktori perusahaan yang ada dan mengontrol kunci yang mengenkripsi data Anda dan lokasi penyimpanan data Anda.

Untuk daftar Wilayah titik akhir AWS yang didukung saat ini, lihat [Wilayah dan Titik Akhir](#).

Topik

- [Persyaratan WorkMail sistem Amazon](#)
- [WorkMail Konsep Amazon](#)
- [Layanan AWS terkait](#)
- [WorkMail Harga Amazon](#)
- [WorkMail Sumber daya Amazon](#)

Persyaratan WorkMail sistem Amazon

Saat WorkMail administrator Amazon mengundang Anda untuk masuk ke WorkMail akun Amazon, Anda dapat masuk menggunakan klien WorkMail web Amazon.

Amazon WorkMail juga bekerja dengan semua perangkat seluler utama dan sistem operasi yang mendukung ActiveSync protokol Exchange. Perangkat ini mencakup iPad, iPhone, Android, dan Windows Phone. Pengguna macOS dapat menambahkan WorkMail akun Amazon mereka ke aplikasi Mail, Kalender, dan Kontak mereka.

Amazon WorkMail mendukung versi sistem operasi berikut:

- Windows - Windows 7 SP1 atau yang lebih baru
- macOS — macOS 10.12 (Sierra) atau versi lebih baru
- Android — Android 5.0 atau yang lebih baru
- iPhone - iOS 5 atau versi lebih baru
- Windows Phone — Windows 8.1 atau yang lebih baru
- Blackberry — Blackberry OS 10.3.3.3216

Jika Anda memiliki lisensi Microsoft Outlook yang valid, Anda dapat mengakses Amazon WorkMail menggunakan versi Microsoft Outlook berikut:

- Outlook 2013 atau yang lebih baru
- Outlook 2013 Click-to-Run atau yang lebih baru
- Outlook untuk Mac 2016 atau versi lebih baru

Anda dapat mengakses klien WorkMail web Amazon menggunakan versi browser berikut:

- Google Chrome - Versi 22 atau yang lebih baru
- Mozilla Firefox — Versi 27 atau yang lebih baru
- Safari - Versi 7 atau yang lebih baru
- Internet Explorer - Versi 11
- Microsoft Edge

Anda juga dapat menggunakan Amazon WorkMail dengan klien IMAP pilihan Anda.

WorkMail Konsep Amazon

Terminologi dan konsep yang menjadi pusat pemahaman dan penggunaan Amazon Anda WorkMail dijelaskan di bawah ini.

Organisasi

Pengaturan penyewa untuk Amazon WorkMail.

Alias

Nama yang unik secara global untuk mengidentifikasi organisasi Anda. Alias digunakan untuk mengakses aplikasi WorkMail web Amazon (<https://alias.awsapps.com/mail>).

Domain

Alamat web yang muncul setelah @ simbol di alamat email. Anda dapat menambahkan domain yang menerima email dan mengirimkannya ke kotak pesan di organisasi Anda.

Domain pesan uji

Domain secara otomatis dikonfigurasi selama penyiapan yang dapat digunakan untuk menguji Amazon WorkMail. Domain email uji adalah *alias*.awsapps.com dan digunakan sebagai domain

default jika Anda tidak mengonfigurasi domain Anda sendiri. Domain pesan uji tunduk pada batas yang berbeda. Untuk informasi selengkapnya, lihat [WorkMail Kuota Amazon](#).

Direktori

AWS Simple AD, AWS Managed AD, atau AD Connector yang dibuat di AWS Directory Service. Jika Anda membuat organisasi menggunakan penyiapan Amazon WorkMail Quick, kami membuat WorkMail direktori untuk Anda. Anda tidak dapat melihat WorkMail direktori di AWS Directory Service.

Pengguna

Pengguna yang dibuat di AWS Directory Service. Pengguna dapat dibuat dalam peran USER atau REMOTE_USER. Saat pengguna dibuat dan diaktifkan dengan peran USER, pengguna akan menerima kotak pesan sendiri untuk diakses. Ketika pengguna dinonaktifkan, mereka tidak dapat mengakses Amazon WorkMail.

Pengguna yang dibuat dan diaktifkan dengan peran REMOTE_USER tercantum dalam buku alamat tetapi tidak mendapatkan kotak pesan di Amazon. WorkMail REMOTE_USER dapat memiliki kotak surat yang dihosting di luar Amazon WorkMail tetapi masih akan terdaftar sebagai pengguna lain dengan kotak surat di buku alamat WorkMail Amazon dan dapat mencari kalender satu sama lain untuk menemukan informasi gratis atau sibuk.

Kelompok

Kelompok yang digunakan dalam AWS Directory Service Grup dapat digunakan sebagai daftar distribusi atau grup keamanan di Amazon WorkMail. Grup tidak memiliki kotak pesan sendiri.

Sumber daya

Sumber daya mewakili ruang rapat atau sumber daya peralatan yang dapat dipesan oleh WorkMail pengguna Amazon.

Kebijakan perangkat seluler

Berbagai aturan kebijakan IT yang mengontrol fitur keamanan dan perilaku perangkat mobile.

Layanan AWS terkait

Layanan berikut digunakan bersama dengan Amazon WorkMail:

- AWS Directory Service—Anda dapat mengintegrasikan Amazon WorkMail dengan AWS Simple AD, AWS Managed AD, atau AD Connector yang ada. Buat direktori di AWS Directory Service

dan kemudian aktifkan Amazon WorkMail untuk direktori ini. Setelah mengonfigurasi integrasi ini, Anda dapat memilih pengguna mana yang ingin Anda aktifkan untuk Amazon WorkMail dari daftar pengguna di direktori yang ada, dan pengguna dapat masuk menggunakan kredensial Direktori Aktif yang ada. Untuk informasi selengkapnya, lihat [Panduan Administrasi AWS Directory Service](#).

- Layanan Email Sederhana Amazon —Amazon WorkMail menggunakan Amazon SES untuk mengirim semua email keluar. Domain pesan uji dan domain Anda tersedia untuk dikelola di konsol Amazon SES. Tidak ada biaya untuk email keluar yang dikirim dari Amazon WorkMail. Untuk informasi selengkapnya lihat [Panduan Developer Amazon Simple Email Service](#).
- AWS Identity and Access Management Konsol Manajemen AWS Memerlukan nama pengguna dan kata sandi Anda sehingga layanan apa pun yang Anda gunakan dapat menentukan apakah Anda memiliki izin untuk mengakses sumber dayanya. Kami menyarankan Anda menghindari penggunaan kredensial akun AWS untuk mengakses AWS karena kredensial AWS akun tidak dapat dicabut atau dibatasi dengan cara apa pun. Sebagai gantinya, kami sarankan Anda membuat pengguna IAM dan menambahkan pengguna ke grup IAM dengan izin administratif. Anda kemudian dapat mengakses konsol menggunakan kredensial pengguna IAM.

Jika Anda mendaftar ke AWS tetapi belum membuat pengguna IAM untuk Anda sendiri, Anda dapat membuatnya menggunakan konsol IAM. Untuk informasi selengkapnya, lihat [Buat pengguna IAM individual](#) dalam Panduan Pengguna IAM.

- AWS Key Management Service—Amazon WorkMail terintegrasi dengan AWS KMS enkripsi data pelanggan. Manajemen kunci dapat dilakukan dari AWS KMS konsol. Untuk informasi selengkapnya, [Apa itu AWS Key Management Service](#) dalam Panduan Developer AWS Key Management Service .

WorkMail Harga Amazon

Dengan Amazon WorkMail, tidak ada biaya atau komitmen di muka. Anda hanya membayar untuk akun pengguna aktif. Untuk informasi lebih lanjut tentang harga, lihat [Harga](#).

WorkMail Sumber daya Amazon

Sumber daya terkait berikut dapat membantu Anda ketika bekerja dengan layanan ini.

- [Kelas & Lokakarya](#) - Tautan ke kursus berbasis peran dan khusus, selain laboratorium mandiri untuk membantu mempertajam keterampilan Anda AWS dan mendapatkan pengalaman praktis.

- [AWS Pusat Pengembang](#) — Jelajahi tutorial, unduh alat, dan pelajari tentang acara AWS pengembang.
- [AWS Alat Pengembang](#) - Tautan ke alat pengembang, SDK, toolkit IDE, dan alat baris perintah untuk mengembangkan dan mengelola aplikasi. AWS
- [Memulai Pusat Sumber Daya](#) — Pelajari cara menyiapkan Akun AWS, bergabung dengan AWS komunitas, dan meluncurkan aplikasi pertama Anda.
- [Hands-On Tutorial](#) — Ikuti tutorial langkah demi langkah untuk meluncurkan aplikasi pertama Anda AWS.
- [AWS Whitepaper](#) — Tautan ke daftar lengkap AWS whitepaper teknis, yang mencakup topik-topik seperti arsitektur, keamanan, dan ekonomi dan ditulis oleh AWS Solutions Architects atau pakar teknis lainnya.
- [AWS Dukungan Pusat](#) — Hub untuk membuat dan mengelola AWS Dukungan kasus Anda. Juga termasuk tautan ke sumber daya bermanfaat lainnya, seperti forum, FAQ teknis, status kesehatan layanan, dan. AWS Trusted Advisor
- [Dukungan](#)— Halaman web utama untuk informasi tentang Dukungan, saluran dukungan satu-satu, respon cepat untuk membantu Anda membangun dan menjalankan aplikasi di cloud.
- [Hubungi Kami](#) – Titik kontak pusat untuk pertanyaan tentang tandaihan AWS , akun, peristiwa, penyalahgunaan, dan masalah lainnya.
- [AWS Ketentuan Situs](#) — Informasi terperinci tentang hak cipta dan merek dagang kami; akun, lisensi, dan akses situs Anda; dan topik lainnya.

Amazon WorkMail Akhir Dukungan

Setelah mempertimbangkan dengan cermat, kami memutuskan untuk mengakhiri dukungan untuk Amazon WorkMail, efektif 31 Maret 2027. Amazon tidak WorkMail akan lagi menerima pelanggan baru mulai 30 April 2026. Sebagai pelanggan lama dengan akun yang mendaftar untuk layanan sebelum 30 April 2026, Anda dapat terus menggunakan WorkMail fitur Amazon. Setelah 31 Maret 2027, Anda tidak akan lagi dapat menggunakan Amazon WorkMail.

Solusi alternatif

Amazon WorkMail merekomendasikan pelanggan untuk bermigrasi ke solusi pihak ketiga seperti [Kopano Cloud](#), [Zoho Mail](#), dan [Zoom Mail](#), masing-masing menyediakan WorkMail-comparable kemampuan dan alat Amazon untuk memudahkan migrasi. Anda juga dapat bermigrasi ke solusi pihak ketiga di pasar lainnya.

Mengekspor data

Anda dapat mengikuti [panduan ekspor kotak pesan](#) untuk mengekspor konten kotak pesan Anda.

Butuh bantuan atau punya pertanyaan?

Jika Anda memerlukan bantuan atau memiliki umpan balik, hubungi [AWS Support](#).

Prasyarat

Untuk bertindak sebagai WorkMail administrator Amazon, Anda memerlukan akun AWS. Jika Anda belum mendaftar untuk AWS, selesaikan tugas-tugas berikut untuk melakukan pengaturan.

Topik

- [Mendaftar untuk Akun AWS](#)
- [Berikan izin kepada pengguna IAM untuk Amazon WorkMail](#)

Mendaftar untuk Akun AWS

Untuk memulai AWS, Anda membutuhkan Akun AWS. Untuk informasi tentang membuat Akun AWS, lihat [Memulai dengan Akun AWS](#) di Panduan AWS Account Management Referensi.

Berikan izin kepada pengguna IAM untuk Amazon WorkMail

Secara default, pengguna IAM tidak memiliki izin untuk mengelola sumber daya Amazon WorkMail . Anda harus melampirkan kebijakan terkelola AWS (AmazonWorkMailFullAccessatau AmazonWorkMailReadOnlyAccess) atau membuat kebijakan yang dikelola pelanggan yang secara eksplisit memberikan izin tersebut kepada pengguna IAM. Anda kemudian melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut. Lihat informasi yang lebih lengkap di [Manajemen identitas dan akses untuk Amazon WorkMail](#).

Keamanan di Amazon WorkMail

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-party Auditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [program AWS kepatuhan](#). Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon WorkMail, lihat [AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan](#).
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Amazon WorkMail. Topik berikut menunjukkan cara mengonfigurasi Amazon WorkMail untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan layanan AWS lain yang membantu Anda memantau dan mengamankan WorkMail sumber daya Amazon Anda.

Topik

- [Perlindungan data di Amazon WorkMail](#)
- [Manajemen identitas dan akses untuk Amazon WorkMail](#)
- [AWS kebijakan terkelola untuk Amazon WorkMail](#)
- [Menggunakan peran terkait layanan untuk Amazon WorkMail](#)
- [Pencatatan dan pemantauan di Amazon WorkMail](#)
- [Validasi kepatuhan untuk Amazon WorkMail](#)
- [Ketahanan di Amazon WorkMail](#)
- [Keamanan infrastruktur di Amazon WorkMail](#)

Perlindungan data di Amazon WorkMail

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di Amazon WorkMail. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat [FAQ Privasi Data AWS](#). Untuk informasi tentang perlindungan data di Eropa, lihat [Pusat Peraturan Perlindungan Data Umum \(GDPR\)](#).

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon WorkMail atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan

supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Bagaimana Amazon WorkMail menggunakan AWS KMS

Amazon WorkMail secara transparan mengenkripsi semua pesan di kotak surat semua WorkMail organisasi Amazon sebelum pesan ditulis ke disk, dan secara transparan mendekripsi pesan saat pengguna mengaksesnya. Anda tidak dapat menonaktifkan enkripsi. Untuk melindungi kunci enkripsi yang melindungi pesan, Amazon WorkMail terintegrasi dengan AWS Key Management Service (AWS KMS).

Amazon WorkMail juga menyediakan opsi untuk memungkinkan pengguna mengirim email yang ditandatangani atau dienkripsi. Fitur enkripsi ini tidak menggunakan AWS KMS. Untuk informasi selengkapnya, lihat [Mengaktifkan email yang ditandatangani atau dienkripsi](#).

Topik

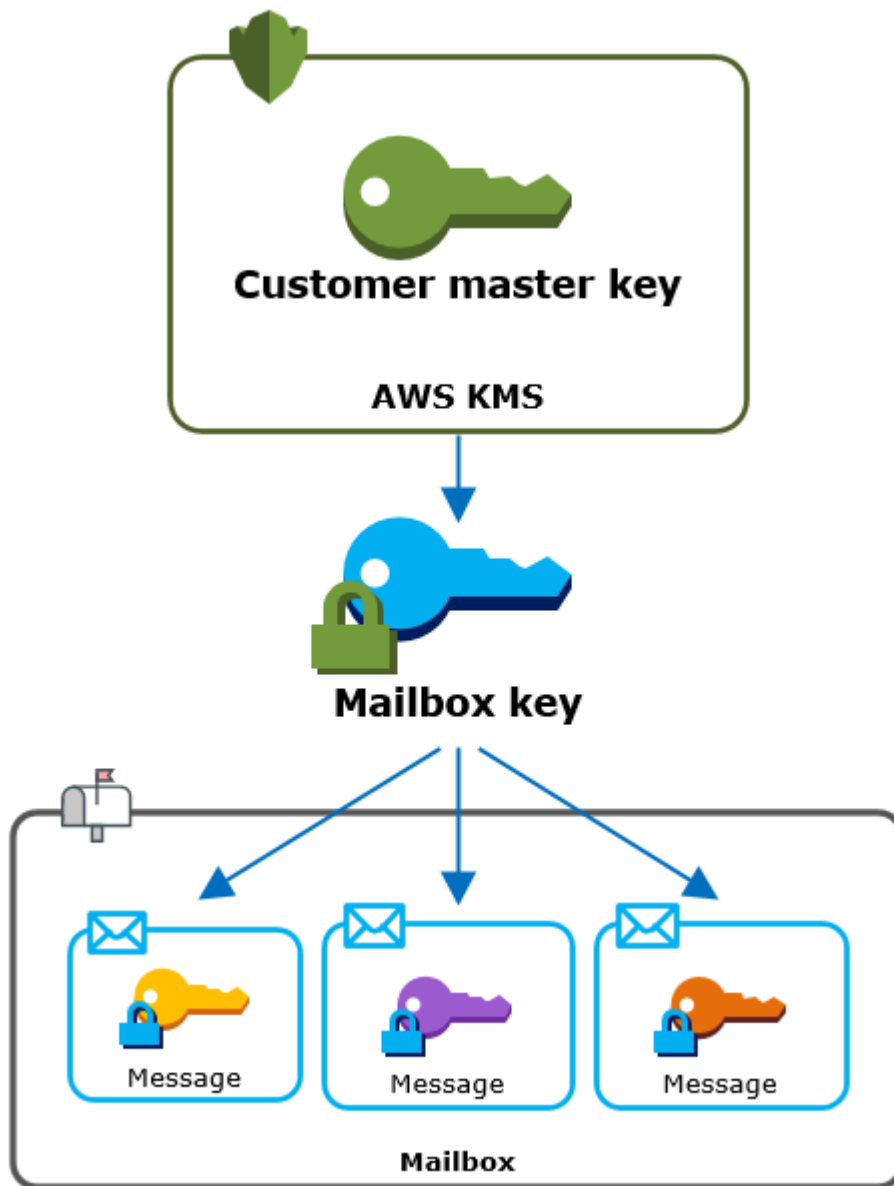
- [WorkMail Enkripsi Amazon](#)
- [Mengotorisasi penggunaan CMK](#)
- [Konteks WorkMail enkripsi Amazon](#)
- [Memantau WorkMail interaksi Amazon dengan AWS KMS](#)

WorkMail Enkripsi Amazon

Di Amazon WorkMail, setiap organisasi dapat berisi beberapa kotak pesan, satu untuk setiap pengguna di organisasi. Semua pesan, termasuk item email dan kalender, disimpan di kotak pesan pengguna.

Untuk melindungi konten kotak pesan di WorkMail organisasi Amazon Anda, Amazon WorkMail mengenkripsi semua pesan kotak pesan sebelum ditulis ke disk. Tidak ada informasi yang disediakan pelanggan disimpan dalam plaintext.

Setiap pesan dienkripsi di bawah kunci enkripsi data yang unik. Kunci pesan dilindungi oleh kunci kotak pesan, yang merupakan kunci enkripsi unik yang hanya digunakan untuk kotak pesan tersebut. Kunci kotak pesan dienkripsi di bawah kunci master AWS KMS pelanggan (CMK) untuk organisasi yang tidak pernah dibiarkan tidak terenkripsi. AWS KMS Diagram berikut menunjukkan hubungan pesan terenkripsi, kunci pesan terenkripsi, kunci kotak pesan terenkripsi, dan CMK untuk organisasi di AWS KMS.



Menetapkan CMK untuk organisasi

Saat membuat WorkMail organisasi Amazon, Anda memiliki opsi untuk memilih kunci master AWS KMS pelanggan (CMK) untuk organisasi. CMK ini melindungi semua kunci kotak pesan di organisasi tersebut.

Anda dapat memilih CMK AWS terkelola default untuk Amazon WorkMail, atau Anda dapat memilih CMK terkelola pelanggan yang sudah ada yang Anda miliki dan kelola. Untuk informasi selengkapnya, lihat [kunci utama pelanggan \(CMK\)](#) dalam Panduan Developer AWS Key Management Service . Anda dapat memilih CMK yang sama atau CMK yang berbeda untuk setiap organisasi Anda, tetapi Anda tidak dapat mengubah CMK setelah Anda memilihnya.

⚠ Important

Amazon hanya WorkMail mendukung CMK simetris. Anda tidak dapat menggunakan CMK asimetris. Untuk bantuan menentukan apakah kunci CMK simetris atau asimetris, lihat [Mengidentifikasi CMK simetris dan asimetris](#) dalam AWS Key Management Service Panduan Developer.

Untuk menemukan CMK untuk organisasi Anda, gunakan entri AWS CloudTrail log yang merekam panggilan. AWS KMS

Kunci enkripsi unik untuk setiap kotak pesan

Saat Anda membuat kotak pesan, Amazon WorkMail menghasilkan kunci enkripsi simetris [Advanced Encryption Standard](#) (AES) 256-bit yang unik untuk kotak pesan, yang dikenal sebagai kunci kotak pesan, di luar kotak pesan. AWS KMS Amazon WorkMail menggunakan kunci kotak pesan untuk melindungi kunci enkripsi untuk setiap pesan di kotak pesan.

Untuk melindungi kunci kotak pesan, Amazon WorkMail memanggil AWS KMS untuk mengenkripsi kunci kotak pesan di bawah CMK untuk organisasi. Kemudian ini menyimpan kunci kotak pesan yang dienkripsi dalam metadata kotak pesan.

ℹ Note

Amazon WorkMail menggunakan kunci enkripsi kotak pesan simetris untuk melindungi kunci pesan. Sebelumnya, Amazon WorkMail melindungi setiap kotak surat dengan key pair asimetris. Ini menggunakan kunci publik untuk mengenkripsi setiap kunci pesan dan kunci pribadi untuk mendekripsinya. Kunci kotak pesan privat dilindungi oleh CMK untuk organisasi. Kotak pesan lama dapat menggunakan key pair kotak pesan asimetris. Perubahan ini tidak memengaruhi keamanan kotak surat atau pesannya.

Mengenkripsi setiap pesan

Saat pengguna menambahkan pesan ke kotak pesan, Amazon WorkMail menghasilkan kunci enkripsi simetris AES 256-bit yang unik untuk pesan di luar. AWS KMS Ini menggunakan kunci pesan ini untuk mengenkripsi pesan. Amazon WorkMail mengenkripsi kunci pesan di bawah kunci kotak surat dan menyimpan kunci pesan terenkripsi dengan pesan. Kemudian, ini mengenkripsi kunci kotak pesan di bawah CMK untuk organisasi.

Membuat kotak pesan baru

Saat Amazon WorkMail membuat kotak pesan, Amazon menggunakan proses berikut untuk menyiapkan kotak pesan untuk menyimpan pesan terenkripsi.

- Amazon WorkMail menghasilkan kunci enkripsi simetris AES 256-bit yang unik untuk kotak surat di luar AWS KMS.
- Amazon WorkMail menyebut operasi AWS KMS [Enkripsi](#). Ini melewati kunci kotak surat dan pengidentifikasi kunci master pelanggan (CMK) untuk organisasi. AWS KMS mengembalikan ciphertext dari kunci kotak surat yang dienkripsi di bawah CMK.
- Amazon WorkMail menyimpan kunci kotak surat terenkripsi dengan metadata kotak surat.

Mengenkripsi pesan kotak pesan

Untuk mengenkripsi pesan, Amazon WorkMail menggunakan proses berikut.

1. Amazon WorkMail menghasilkan kunci simetris AES 256-bit yang unik untuk pesan tersebut. Ini menggunakan kunci pesan teks biasa dan algoritma Advanced Encryption Standard (AES) untuk mengenkripsi pesan di luar AWS KMS
2. Untuk melindungi kunci pesan di bawah kunci kotak surat, Amazon WorkMail perlu mendekripsi kunci kotak surat, yang selalu disimpan dalam bentuk terenkripsi.

Amazon WorkMail memanggil operasi AWS KMS [Dekripsi](#) dan meneruskan kunci kotak surat terenkripsi. AWS KMS menggunakan CMK untuk organisasi untuk mendekripsi kunci kotak pesan dan mengembalikan kunci kotak pesan teks biasa ke Amazon WorkMail

3. Amazon WorkMail menggunakan kunci kotak pesan teks biasa dan algoritma Advanced Encryption Standard (AES) untuk mengenkripsi kunci pesan di luar AWS KMS
4. Amazon WorkMail menyimpan kunci pesan terenkripsi dalam metadata pesan terenkripsi sehingga tersedia untuk mendekripsi.

Mendekripsi pesan kotak pesan

Untuk mendekripsi pesan, Amazon WorkMail menggunakan proses berikut.

1. Amazon WorkMail memanggil operasi AWS KMS [Dekripsi](#) dan meneruskan kunci kotak surat terenkripsi. AWS KMS menggunakan CMK untuk organisasi untuk mendekripsi kunci kotak pesan dan mengembalikan kunci kotak pesan teks biasa ke Amazon WorkMail

2. Amazon WorkMail menggunakan kunci kotak pesan teks biasa dan algoritma Advanced Encryption Standard (AES) untuk mendekripsi kunci pesan terenkripsi di luar. AWS KMS
3. Amazon WorkMail menggunakan kunci pesan teks biasa untuk mendekripsi pesan terenkripsi.

Melakukan cache tombol kotak pesan

Untuk meningkatkan kinerja dan meminimalkan panggilan ke AWS KMS, Amazon WorkMail menyimpan setiap kunci kotak pesan teks biasa untuk setiap klien secara lokal hingga satu menit. Pada akhir periode caching, kunci kotak pesan akan dihapus. Jika kunci kotak surat untuk klien tersebut diperlukan selama periode caching, Amazon WorkMail bisa mendapatkannya dari cache alih-alih menelepon. AWS KMS Kunci kotak pesan dilindungi dalam cache dan tidak pernah ditulis ke disk dalam plaintext.

Mengotorisasi penggunaan CMK

Saat Amazon WorkMail menggunakan kunci master pelanggan (CMK) dalam operasi kriptografi, Amazon bertindak atas nama administrator kotak pesan.

Untuk menggunakan kunci master AWS KMS pelanggan (CMK) untuk rahasia atas nama Anda, administrator harus memiliki izin berikut. Anda dapat menentukan izin yang diperlukan ini dalam kebijakan IAM atau kebijakan kunci.

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

Untuk mengizinkan CMK hanya digunakan untuk permintaan yang berasal dari Amazon WorkMail, Anda dapat menggunakan kunci ViaService kondisi [kms:](#) dengan nilainya. `workmail.<region>.amazonaws.com`

Anda juga dapat menggunakan kunci atau nilai dalam [konteks enkripsi](#) sebagai syarat untuk menggunakan CMK untuk operasi kriptografi. Misalnya, Anda dapat menggunakan operator ketentuan string di IAM atau dokumen kebijakan kunci atau menggunakan batasan hibah dalam hibah.

Kebijakan utama untuk AWS managed CMK

Kebijakan utama untuk CMK AWS terkelola untuk Amazon WorkMail memberi pengguna izin untuk menggunakan CMK untuk operasi tertentu hanya ketika Amazon WorkMail membuat permintaan

atas nama pengguna. Kebijakan kunci tidak mengizinkan setiap pengguna untuk menggunakan CMK secara langsung.

Kebijakan kunci ini, seperti kebijakan dari semua [kunci yang dikelola AWS](#), ditetapkan oleh layanan. Anda tidak dapat mengubah kebijakan kunci, tetapi Anda dapat melihatnya kapan saja. Untuk detailnya, lihat [Menampilkan kebijakan kunci](#) di Panduan Developer AWS Key Management Service .

Pernyataan kebijakan dalam kebijakan kunci memiliki efek sebagai berikut:

- Izinkan pengguna di akun dan Wilayah untuk menggunakan CMK untuk operasi kriptografi dan untuk membuat hibah, tetapi hanya ketika permintaan datang dari Amazon WorkMail atas nama mereka. Kunci kondisi `kms:ViaService` memberlakukan pembatasan ini.
- Memungkinkan AWS akun untuk membuat kebijakan IAM yang memungkinkan pengguna untuk melihat properti CMK dan mencabut hibah.

Berikut ini adalah kebijakan utama untuk contoh CMK AWS terkelola untuk 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": "*"
    },
    "Action": [ "kms:Decrypt", "kms:CreateGrant", "kms:ReEncrypt*", "kms:DescribeKey", "kms:Encrypt" ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "workmail.us-east-1.amazonaws.com",
        "kms:CallerAccount": "111122223333"
      }
    }
  }, {
    "Sid": "Allow direct access to key metadata to the account",
    "Effect": "Allow",
```

```
"Principal" : {
  "AWS" : "arn:aws:iam::111122223333:root"
},
"Action" : [ "kms:Describe*", "kms:List*", "kms:Get*", "kms:RevokeGrant" ],
"Resource" : "*"
} ]
}
```

Menggunakan hibah untuk mengotorisasi Amazon WorkMail

Selain kebijakan utama, Amazon WorkMail menggunakan hibah untuk menambahkan izin ke CMK untuk setiap organisasi. Untuk melihat hibah pada CMK di akun Anda, gunakan operasi. [ListGrants](#)

Amazon WorkMail menggunakan hibah untuk menambahkan izin berikut ke CMK untuk organisasi.

- Tambahkan `kms:Encrypt` izin untuk mengizinkan Amazon WorkMail mengenkripsi kunci kotak surat.
- Tambahkan `kms:Decrypt` izin untuk mengizinkan Amazon menggunakan CMK WorkMail untuk mendekripsi kunci kotak pesan. Amazon WorkMail memerlukan izin ini dalam hibah karena permintaan untuk membaca pesan kotak pesan menggunakan konteks keamanan pengguna yang membaca pesan. Permintaan tidak menggunakan kredensial akun. AWS Amazon WorkMail membuat hibah ini saat Anda memilih CMK untuk organisasi.

Untuk membuat hibah, Amazon WorkMail memanggil [CreateGrant](#) atas nama pengguna yang membuat organisasi. Izin untuk membuat hibah berasal dari kebijakan kunci. Kebijakan ini memungkinkan pengguna akun untuk memanggil `CreateGrant` CMK untuk organisasi saat Amazon WorkMail membuat permintaan atas nama pengguna yang berwenang.

Kebijakan kunci juga memungkinkan root akun untuk mencabut hibah pada kunci yang AWS dikelola. Namun, jika Anda mencabut hibah, Amazon tidak WorkMail dapat mendekripsi data terenkripsi di kotak pesan Anda.

Konteks WorkMail enkripsi Amazon

Konteks enkripsi adalah seperangkat pasangan nilai kunci yang berisi data non-rahasia yang berubah-ubah. Ketika Anda menyertakan konteks enkripsi dalam permintaan untuk mengenkripsi data, secara AWS KMS kriptografis mengikat konteks enkripsi ke data terenkripsi. Untuk mendekripsi data, Anda harus meneruskan konteks enkripsi yang sama. Untuk informasi lebih lanjut, lihat [Konteks enkripsi](#) di Panduan Developer AWS Key Management Service .

Amazon WorkMail menggunakan format konteks enkripsi yang sama di semua operasi AWS KMS kriptografi. Anda dapat menggunakan konteks enkripsi untuk mengidentifikasi operasi kriptografi ini dalam catatan audit dan log, seperti [AWS CloudTrail](#), dan sebagai syarat untuk otorisasi dalam kebijakan dan bantuan.

Dalam permintaan [Enkripsi](#) dan [Dekripsi](#) ke, AWS KMS Amazon WorkMail menggunakan konteks enkripsi di mana kuncinya berada `aws:workmail:arn` dan nilainya adalah Nama Sumber Daya Amazon (ARN) organisasi.

```
"aws:workmail:arn":"arn:aws:workmail:region:account ID:organization/organization-ID"
```

Sebagai contoh, konteks enkripsi berikut mencakup contoh organisasi ARN di Wilayah Europe (Ireland) (`eu-west-1`).

```
"aws:workmail:arn":"arn:aws:workmail:eu-west-1:111122223333:organization/m-  
a123b4c5de678fg9h0ij1k2lm234no56"
```

Memantau WorkMail interaksi Amazon dengan AWS KMS

Anda dapat menggunakan AWS CloudTrail dan Amazon CloudWatch Logs untuk melacak permintaan yang WorkMail dikirimkan AWS KMS Amazon atas nama Anda.

Enkripsi

Saat Anda membuat kotak pesan, Amazon akan membuat WorkMail kunci kotak pesan dan panggilan AWS KMS untuk mengenkripsi kunci kotak pesan. Amazon WorkMail mengirimkan permintaan [Enkripsi](#) AWS KMS dengan kunci kotak pesan teks biasa dan pengenal untuk CMK organisasi Amazon. WorkMail

Peristiwa yang mencatat operasi Encrypt serupa dengan peristiwa contoh berikut. Pengguna adalah WorkMail layanan Amazon. Parameter termasuk ID CMK (`keyId`) dan konteks enkripsi untuk WorkMail organisasi Amazon. Amazon WorkMail juga melewati kunci kotak surat, tetapi itu tidak dicatat dalam CloudTrail log.

```
{  
  "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-a2d6-08ded2eaf63c",
"eventID": "d5a59c18-128a-4082-aa5b-729f7734626a",
"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": "d08e60f1-097e-4a00-b7e9-10bc3872d50c"
}
```

Dekripsi

Saat menambahkan, melihat, atau menghapus pesan kotak pesan, Amazon WorkMail meminta AWS KMS untuk mendekripsi kunci kotak pesan. Amazon WorkMail mengirimkan permintaan [Dekripsi](#) AWS KMS dengan kunci kotak surat terenkripsi dan pengenal untuk CMK organisasi Amazon WorkMail.

Peristiwa yang mencatat operasi Decrypt serupa dengan peristiwa contoh berikut. Pengguna adalah WorkMail layanan Amazon. Parameter termasuk kunci kotak surat terenkripsi (sebagai gumpalan ciphertext), yang tidak direkam dalam log, dan konteks enkripsi untuk organisasi Amazon. WorkMail AWS KMS mendapatkan ID CMK dari ciphertext.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "workmail.eu-west-1.amazonaws.com"
  },
  "eventTime": "2019-02-20T11:51:10Z",
  "eventSource": "kms.amazonaws.com",
  "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-a123b4c5de678fg9h0ij1k2lm234no56"
    }
  },
  "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"
}
```

Manajemen identitas dan akses untuk Amazon WorkMail

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya Amazon. WorkMail IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi Dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana Amazon WorkMail bekerja dengan IAM](#)
- [Contoh WorkMail kebijakan berbasis identitas Amazon](#)
- [Memecahkan masalah WorkMail identitas dan akses Amazon](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat [Memecahkan masalah WorkMail identitas dan akses Amazon](#))
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Bagaimana Amazon WorkMail bekerja dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [Contoh WorkMail kebijakan berbasis identitas Amazon](#))

Mengautentikasi Dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensial identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensial dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensial. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat [Cara masuk ke Akun AWS Anda](#) dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat [Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensial sementara](#) di Panduan Pengguna IAM.

[Grup IAM](#) menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan [beralih dari pengguna ke peran IAM \(konsol\)](#) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukannya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan](#) dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih antara kebijakan terkelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar Kontrol Akses (ACL)

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat [Gambaran umum daftar kontrol akses \(ACL\)](#) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol sumber daya \(RCP\)](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

Bagaimana Amazon WorkMail bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Amazon WorkMail, Anda harus memahami fitur IAM apa yang tersedia untuk digunakan dengan Amazon WorkMail. Untuk mendapatkan tampilan tingkat tinggi tentang cara Amazon WorkMail dan AWS layanan lainnya bekerja dengan IAM, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Topik

- [Kebijakan WorkMail berbasis identitas Amazon](#)
- [Kebijakan berbasis WorkMail sumber daya Amazon](#)
- [Otorisasi berdasarkan tag Amazon WorkMail](#)
- [Peran Amazon WorkMail IAM](#)

Kebijakan WorkMail berbasis identitas Amazon

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Amazon WorkMail mendukung tindakan, sumber daya, dan kunci kondisi tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat [Referensi Elemen Kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan di Amazon WorkMail menggunakan awalan berikut sebelum tindakan: `workmail:`. Misalnya, untuk memberikan izin kepada seseorang untuk mengambil daftar pengguna dengan operasi Amazon WorkMail `ListUsers` API, Anda menyertakan `workmail:ListUsers` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Amazon WorkMail mendefinisikan serangkaian tindakannya sendiri yang menggambarkan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma seperti berikut:

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

Anda dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `List`, sertakan tindakan berikut:

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

Untuk melihat daftar tindakan Amazon, lihat WorkMail [Tindakan yang ditentukan oleh Amazon WorkMail](#) di Panduan Pengguna IAM.

Sumber daya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Amazon WorkMail mendukung izin tingkat sumber daya untuk organisasi Amazon. WorkMail

Sumber daya WorkMail organisasi Amazon memiliki ARN berikut:

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

Untuk informasi selengkapnya tentang format ARN, lihat [Amazon Resource Names \(ARN\) dan ruang nama AWS layanan](#).

Misalnya, untuk menentukan organisasi `m-n1pq2345678r901st2u3vx45x6789yza` dalam pernyataan Anda, gunakan ARN berikut.

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

Untuk menentukan semua organisasi milik akun tertentu, gunakan wildcard (*):

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

Beberapa WorkMail tindakan Amazon, seperti untuk membuat sumber daya, tidak dapat dilakukan pada sumber daya tertentu. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

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

Untuk melihat daftar jenis WorkMail sumber daya Amazon dan ARNnya, lihat [Sumber daya yang ditentukan oleh Amazon WorkMail](#) di Panduan Pengguna IAM. Untuk mempelajari tindakan yang

dapat Anda tentukan untuk ARN setiap sumber daya, lihat [Tindakan, sumber daya, dan kunci kondisi untuk Amazon](#). WorkMail

Kunci syarat

Amazon WorkMail mendukung kunci kondisi global berikut.

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

Contoh kebijakan berikut memberikan akses ke WorkMail konsol Amazon hanya dari prinsipal IAM yang diautentikasi MFA di Wilayah AWS. eu-west-1

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "cloudwatch:GetMetricData"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestedRegion": [
          "eu-west-1"
        ]
      },
      "Bool": {
        "aws:MultiFactorAuthPresent": true
      }
    }
  }
]
}

```

Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

`workmail:ImpersonationRoleId` adalah satu-satunya kunci kondisi khusus layanan yang didukung oleh Amazon WorkMail.

Contoh kebijakan berikut mencakup `AssumeImpersonationRole` tindakan ke bawah untuk WorkMail organisasi tertentu dan peran peniruan identitas.

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"
        }
      }
    }
  ]
}

```

```
}  
  }  
] }  
}
```

Contoh

Untuk melihat contoh kebijakan WorkMail berbasis identitas Amazon, lihat. [Contoh WorkMail kebijakan berbasis identitas Amazon](#)

Kebijakan berbasis WorkMail sumber daya Amazon

Amazon WorkMail tidak mendukung kebijakan berbasis sumber daya.

Otorisasi berdasarkan tag Amazon WorkMail

Anda dapat melampirkan tag ke WorkMail sumber daya Amazon atau meneruskan tag dalam permintaan ke Amazon WorkMail. Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`. Untuk informasi selengkapnya tentang menandai WorkMail sumber daya Amazon, lihat [Penandaan sebuah organisasi](#).

Peran Amazon WorkMail IAM

[Peran IAM](#) adalah entitas dalam AWS akun Anda yang memiliki izin tertentu.

Menggunakan kredensial sementara dengan Amazon WorkMail

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensial keamanan sementara dengan memanggil operasi AWS STS API seperti [AssumeRole](#) atau [GetFederationToken](#)

Amazon WorkMail mendukung penggunaan kredensial sementara.

Service-linked peran

[Service-linked peran](#) memungkinkan AWS layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Service-linked peran muncul di akun IAM Anda dan dimiliki oleh layanan. Administrator IAM dapat melihat tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Amazon WorkMail mendukung peran terkait layanan. Untuk detail tentang membuat atau mengelola peran WorkMail terkait layanan Amazon, lihat. [Menggunakan peran terkait layanan untuk Amazon WorkMail](#)

Peran layanan

Fitur ini memungkinkan layanan untuk menerima [peran layanan](#) atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti administrator IAM dapat mengubah izin untuk peran ini. Namun, melakukan hal itu dapat merusak fungsionalitas layanan.

Amazon WorkMail mendukung peran layanan.

Contoh WorkMail kebijakan berbasis identitas Amazon

Secara default, pengguna dan peran IAM tidak memiliki izin untuk membuat atau memodifikasi WorkMail sumber daya Amazon. Mereka juga tidak dapat melakukan tugas menggunakan Konsol Manajemen AWS, AWS CLI, atau AWS API. Administrator IAM harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan di tab JSON](#) dalam Panduan Pengguna IAM.

Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan WorkMail konsol Amazon](#)
- [Izinkan para pengguna untuk melihat izin mereka sendiri](#)
- [Izinkan pengguna akses hanya-baca ke sumber daya Amazon WorkMail](#)

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus WorkMail sumber daya Amazon di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

Menggunakan WorkMail konsol Amazon

Untuk mengakses WorkMail konsol Amazon, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang WorkMail sumber daya Amazon di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tersebut tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna IAM atau peran) dengan kebijakan tersebut.

Untuk memastikan bahwa entitas tersebut masih dapat menggunakan WorkMail konsol Amazon, lampirkan juga kebijakan AWS terkelola berikut AmazonWorkMailFullAccess, ke entitas. Untuk informasi selengkapnya, lihat [Menambah izin untuk pengguna](#) dalam Panduan Pengguna IAM.

AmazonWorkMailFullAccessKebijakan ini memberi pengguna IAM akses penuh ke sumber daya Amazon WorkMail . Kebijakan ini memberi pengguna akses ke semua Amazon WorkMail AWS Key Management Service, Layanan Email Sederhana Amazon, dan AWS Directory Service operasi. Ini juga mencakup beberapa operasi Amazon EC2 yang WorkMail perlu dilakukan Amazon atas nama Anda. Izin logs dan ccloudwatch izin diperlukan untuk pencatatan peristiwa email, dan melihat metrik di konsol Amazon WorkMail . Pencatatan audit menggunakan CloudWatch Log, Amazon S3, dan Data Amazon FireHose untuk disimpan. Logs Untuk informasi selengkapnya, lihat [Pencatatan dan pemantauan di Amazon WorkMail](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailAdministration",
      "Effect": "Allow",
      "Action": [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "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",
"route53:GetHostedZone",
"route53domains:CheckDomainAvailability",
"route53domains:ListDomains",
"ses:*",
"workmail:*",
"iam:ListRoles",
"logs:DescribeLogGroups",
"logs:CreateLogGroup",
"logs:PutRetentionPolicy",
"logs>DeleteDeliveryDestination",
"logs>DeleteDeliveryDestinationPolicy",
"logs:DescribeDeliveryDestinations",
"logs:GetDeliveryDestination",
"logs:GetDeliveryDestinationPolicy",
"logs:PutDeliveryDestination",
"logs:PutDeliveryDestinationPolicy",
"logs:CreateDelivery",
"logs>DeleteDelivery",
"logs:DescribeDeliveries",
"logs:GetDelivery",
"logs>DeleteDeliverySource",
"logs:DescribeDeliverySources",
```

```
"logs:GetDeliverySource",
"logs:PutDeliverySource",
"logs:DescribeResourcePolicies",
"cloudwatch:GetMetricData",
"firehose:DescribeDeliveryStream",
"firehose:ListDeliveryStreams",
"s3:ListAllMyBuckets"
],
"Resource": "*"
},
{
  "Sid": "AuditLogDeliveryThroughCWLogs",
  "Effect": "Allow",
  "Action": [
    "firehose:TagDeliveryStream",
    "logs:PutResourcePolicy",
    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:CalledViaLast": "logs.amazonaws.com"
    }
  }
},
{
  "Sid": "InboundOutboundEmailEventsLink",
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": "events.workmail.amazonaws.com"
    }
  }
},
{
  "Sid": "AuditLoggingLink",
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
```

```

        "iam:AWSServiceName": "delivery.logs.amazonaws.com"
    }
}
},
{
    "Sid": "InboundOutboundEmailEventsUnlink",
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/
events.workmail.amazonaws.com/AWSServiceRoleForAmazonWorkMailEvents*"
},
{
    "Sid": "InboundOutboundEmailEventsAuth",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/*workmail*",
    "Condition": {
        "StringLike": {
            "iam:PassedToService": "events.workmail.amazonaws.com"
        }
    }
}
]
}

```

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai alternatif, hanya izinkan akses ke tindakan yang cocok dengan operasi API yang sedang Anda coba lakukan.

Izinkan para pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```

{
    "Version": "2012-10-17",

```

```

"Statement": [
  {
    "Sid": "ViewOwnUserInfo",
    "Effect": "Allow",
    "Action": [
      "iam:GetUserPolicy",
      "iam:ListGroupsWithUser",
      "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:ListPolicyVersions",
      "iam:ListPolicies",
      "iam:ListUsers"
    ],
    "Resource": "*"
  }
]
}

```

Izinkan pengguna akses hanya-baca ke sumber daya Amazon WorkMail

Pernyataan kebijakan berikut memberikan akses hanya-baca pengguna IAM ke sumber daya Amazon. WorkMail Kebijakan ini memberikan tingkat akses yang sama dengan kebijakan yang dikelola AWS AmazonWorkMailReadOnlyAccess. Kebijakan mana pun memberi pengguna akses ke semua WorkMail Describe operasi Amazon. Akses ke AWS Directory Service DescribeDirectories operasi diperlukan untuk mendapatkan informasi tentang Directory Service direktori Anda. Akses ke layanan Amazon SES diperlukan untuk mendapatkan informasi tentang domain yang dikonfigurasi. Akses ke AWS Key Management Service diperlukan untuk mendapatkan informasi tentang kunci enkripsi yang digunakan. Izin logs dan cloudwatch izin diperlukan untuk pencatatan peristiwa email dan metrik tampilan di konsol Amazon WorkMail. Pencatatan audit

menggunakan CloudWatch Log, Amazon S3, dan Data Amazon FireHose untuk disimpan. Logs Untuk informasi selengkapnya, lihat [Pencatatan dan pemantauan di Amazon WorkMail](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailReadOnly",
      "Effect": "Allow",
      "Action": [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeDeliveryDestinations",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliverySources",
        "logs:GetDelivery",
        "logs:GetDeliverySource",
        "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
    }
  ]
}
```

Memecahkan masalah WorkMail identitas dan akses Amazon

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Amazon WorkMail dan IAM.

Topik

- [Saya tidak berwenang untuk melakukan tindakan di Amazon WorkMail](#)
- [Saya tidak berwenang untuk melakukan iam: PassRole](#)
- [Saya ingin mengizinkan orang di luar saya AWS akun untuk mengakses WorkMail sumber daya Amazon saya](#)

Saya tidak berwenang untuk melakukan tindakan di Amazon WorkMail

Jika Konsol Manajemen AWS memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberikan nama pengguna dan kata sandi Anda.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu grup, tetapi tidak memiliki izin `workmail:DescribeGroup`.

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

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya `group` menggunakan tindakan `workmail:DescribeGroup`.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Amazon WorkMail.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Amazon WorkMail. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

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

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya AWS akun untuk mengakses WorkMail sumber daya Amazon saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Amazon WorkMail mendukung fitur-fitur ini, lihat [Bagaimana Amazon WorkMail bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM](#).

AWS kebijakan terkelola untuk Amazon WorkMail

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk [membuat kebijakan yang dikelola pelanggan IAM](#) yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini

mencakup kasus penggunaan umum dan tersedia di Akun AWS Anda. Untuk informasi selengkapnya tentang kebijakan AWS [AWS terkelola](#), lihat [kebijakan terkelola](#) di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan `ReadOnlyAccess` AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat [kebijakan yang dikelola AWS untuk fungsi tugas](#) di Panduan Pengguna IAM.

AWS kebijakan terkelola: `AmazonWorkMailFullAccess`

Anda dapat melampirkan kebijakan `AmazonWorkMailFullAccess` ke identitas IAM Anda. Kebijakan ini memberikan izin yang memungkinkan akses penuh ke Amazon. WorkMail

Untuk menampilkan izin untuk kebijakan ini, lihat [AmazonWorkMailFullAccess](#) di Konsol Manajemen AWS.

AWS kebijakan terkelola: `AmazonWorkMailReadOnlyAccess`

Anda dapat melampirkan kebijakan `AmazonWorkMailReadOnlyAccess` ke identitas IAM Anda. Kebijakan ini memberikan izin yang memungkinkan akses hanya-baca ke Amazon. WorkMail

Untuk menampilkan izin untuk kebijakan ini, lihat [AmazonWorkMailReadOnlyAccess](#) di Konsol Manajemen AWS.

AWS kebijakan terkelola: `AmazonWorkMailEventsServiceRolePolicy`

Kebijakan ini dilampirkan ke peran terkait layanan yang diberi nama `AmazonWorkMailEvents` untuk mengizinkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh peristiwa Amazon WorkMail. Untuk informasi selengkapnya, lihat [Menggunakan peran terkait layanan untuk Amazon WorkMail](#).

Amazon WorkMail memperbarui ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon WorkMail sejak layanan ini mulai melacak perubahan ini.

Ubah	Deskripsi	Date
Pembaruan kebijakan terkelola AWS - Pembaruan ke kebijakan yang ada	AmazonWorkMailFull Access Izin AmazonWorkMailReadOnlyAccess dan telah diperbarui untuk Amazon WorkMail untuk mendukung pencatatan audit. Untuk informasi selengkapnya tentang izin yang diperbarui, lihat Contoh WorkMail kebijakan berbasis identitas Amazon dan untuk informasi tentang pencatatan audit, lihat Mengaktifkan pencatatan audit .	Februari 14, 2024
Amazon WorkMail mulai melacak perubahan	Amazon WorkMail mulai melacak perubahan untuk kebijakan yang AWS dikelola.	1 Maret 2021

Menggunakan peran terkait layanan untuk Amazon WorkMail

Amazon WorkMail menggunakan peran AWS Identity and Access Management [terkait layanan](#) (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Amazon. WorkMail Service-linked peran telah ditentukan sebelumnya oleh Amazon WorkMail dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Amazon WorkMail lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Amazon WorkMail mendefinisikan izin peran terkait layanannya, dan kecuali ditentukan lain, hanya Amazon yang WorkMail dapat mengambil

perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi WorkMail sumber daya Amazon Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [layanan AWS yang bekerja dengan IAM](#) dan cari layanan yang memiliki Ya di kolom peran. Service-linked Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Service-linked izin peran untuk Amazon WorkMail

Amazon WorkMail menggunakan peran terkait layanan bernama — AmazonWorkMailEventsAmazon WorkMail menggunakan peran terkait layanan ini untuk mengaktifkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh WorkMail peristiwa Amazon, seperti memantau peristiwa email yang dicatat oleh CloudWatch Untuk informasi selengkapnya tentang mengaktifkan pencatatan peristiwa email untuk Amazon WorkMail, lihat [Mengaktifkan pencatatan peristiwa email](#).

Peran AmazonWorkMailEvents terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `events.workmail.amazonaws.com`

Kebijakan izin peran memungkinkan Amazon WorkMail menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `logs:CreateLogGroup` pada `all AWS resources`
- Tindakan: `logs:CreateLogStream` pada `all AWS resources`
- Tindakan: `logs:PutLogEvents` pada `all AWS resources`

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, menyunting, atau menghapus peran tertaut layanan. Untuk informasi selengkapnya, lihat [izin Service-linked peran](#) di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Amazon WorkMail

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda mengaktifkan pencatatan WorkMail peristiwa Amazon dan menggunakan pengaturan default di WorkMail konsol Amazon, Amazon akan WorkMail membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda mengaktifkan pencatatan WorkMail peristiwa Amazon dan menggunakan pengaturan default, Amazon akan WorkMail membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Amazon WorkMail

Amazon WorkMail tidak mengizinkan Anda mengedit peran AmazonWorkMailEvents terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit Service-Linked Peran](#) di Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Amazon WorkMail

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

Note

Jika WorkMail layanan Amazon menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus WorkMail sumber daya Amazon yang digunakan oleh AmazonWorkMailEvents

1. Matikan pencatatan WorkMail peristiwa Amazon.

- a. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

- b. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.

- c. Di panel navigasi, pilih Pengaturan organisasi, lalu pilih Pemantauan.

- d. Untuk Pengaturan pencatatan, pilih Edit.
 - e. Pindahkan penggeser Aktifkan acara email ke posisi mati.
 - f. Pilih Simpan.
2. Hapus grup CloudWatch log Amazon.
 - a. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
 - b. Pilih Log.
 - c. Untuk Grup log, pilih grup log yang akan dihapus.
 - d. Pilih Tindakan, Hapus grup log.
 - e. Pilih Yes, Delete (Ya, Hapus).

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AmazonWorkMailEvents terkait layanan. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk peran WorkMail terkait layanan Amazon

Amazon WorkMail mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat [WorkMail Wilayah dan Titik Akhir Amazon](#).

Pencatatan dan pemantauan di Amazon WorkMail

Memantau dan mengaudit email dan log Anda penting untuk menjaga kesehatan WorkMail organisasi Amazon Anda. Amazon WorkMail mendukung dua jenis pemantauan:

- Pencatatan peristiwa — Memantau aktivitas pengiriman email untuk organisasi Anda membantu melindungi reputasi domain Anda. Pemantauan juga dapat membantu Anda melacak email yang dikirim dan diterima. Untuk informasi selengkapnya tentang cara mengaktifkan pencatatan peristiwa email, lihat [Mengaktifkan pencatatan peristiwa email](#).
- Pencatatan audit — Anda dapat menggunakan log audit untuk menangkap informasi terperinci tentang penggunaan WorkMail organisasi Amazon Anda seperti memantau akses pengguna ke kotak pesan, mengaudit aktivitas mencurigakan, dan men-debug kontrol akses dan konfigurasi penyedia ketersediaan. Untuk informasi selengkapnya, lihat [Mengaktifkan pencatatan audit](#).

AWS menyediakan alat pemantauan berikut untuk menonton Amazon WorkMail, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- Amazon CloudWatch memantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time. Misalnya, ketika Anda mengaktifkan pencatatan peristiwa email untuk Amazon WorkMail, CloudWatch dapat melacak email yang dikirim dan diterima untuk organisasi Anda. Untuk informasi selengkapnya tentang memantau Amazon WorkMail dengan CloudWatch, lihat [Memantau Amazon WorkMail dengan CloudWatch metrik](#). Untuk informasi selengkapnya CloudWatch, lihat [Panduan CloudWatch Pengguna Amazon](#).
- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses peristiwa email dan log audit untuk Amazon WorkMail saat pencatatan email dan audit diaktifkan di WorkMail konsol Amazon. CloudWatch Log dapat memantau informasi dalam file log, dan Anda dapat mengarsipkan data log Anda dalam penyimpanan yang sangat tahan lama. Untuk informasi selengkapnya tentang melacak WorkMail pesan Amazon menggunakan CloudWatch Log, lihat [Mengaktifkan pencatatan peristiwa email](#) dan [Mengaktifkan pencatatan audit](#). Untuk informasi selengkapnya tentang CloudWatch Log, lihat [Panduan Pengguna CloudWatch Log Amazon](#).
- AWS CloudTrail menangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama Anda Akun AWS, dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, lihat [Mencatat panggilan WorkMail API Amazon dengan AWS CloudTrail](#).
- Amazon S3 memungkinkan Anda untuk menyimpan dan mengakses WorkMail acara Amazon Anda dengan cara yang hemat biaya. [Amazon S3 menyediakan mekanisme untuk mengelola siklus hidup data peristiwa, memungkinkan Anda mengonfigurasi penghapusan otomatis peristiwa lama, atau mengonfigurasi arsip otomatis ke Amazon S3 Glacier](#). Catatan, pengiriman Amazon S3 hanya tersedia untuk peristiwa pencatatan audit. Untuk informasi selengkapnya tentang Amazon S3, lihat Panduan Pengguna [Amazon S3](#).
- Amazon Data Firehose memungkinkan Anda mengalirkan data peristiwa Anda ke layanan AWS lainnya seperti Amazon Simple Storage Service (Amazon S3), Amazon Redshift, Amazon Service, Amazon Serverless, Splunk OpenSearch , dan titik akhir HTTP kustom atau titik akhir HTTP apa pun yang dimiliki oleh penyedia OpenSearch layanan pihak ketiga yang didukung, termasuk Datadog LogicMonitor, Dynatrace,, MongoDB, Relik Baru, Coralogix, dan Elastic. Pengiriman ke Firehose hanya tersedia untuk peristiwa pencatatan audit. Untuk informasi selengkapnya tentang Firehose, lihat panduan developer [Amazon Data Firehose](#).

Topik

- [Memantau Amazon WorkMail dengan CloudWatch metrik](#)
- [Memantau log peristiwa WorkMail email Amazon](#)
- [Memantau log WorkMail audit Amazon](#)
- [Menggunakan CloudWatch Wawasan dengan Amazon WorkMail](#)
- [Mencatat panggilan WorkMail API Amazon dengan AWS CloudTrail](#)
- [Mengaktifkan pencatatan peristiwa email](#)
- [Mengaktifkan pencatatan audit](#)

Memantau Amazon WorkMail dengan CloudWatch metrik

Anda dapat memantau WorkMail penggunaan Amazon CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati waktu nyata. Metrik tanpa biaya disimpan selama 15 bulan sehingga Anda dapat mengakses informasi historis untuk melihat kinerja aplikasi atau layanan web Anda. Anda juga dapat mengatur alarm yang memperhatikan ambang batas tertentu dan mengirim notifikasi atau mengambil tindakan saat ambang batas tersebut terpenuhi. Untuk informasi selengkapnya, lihat [Panduan CloudWatch Pengguna Amazon](#).

CloudWatch metrik untuk Amazon WorkMail

Amazon WorkMail mengirimkan metrik dan informasi dimensi berikut ke CloudWatch.

Namespace `AWS/WorkMail` mencakup metrik berikut.

Metrik	Deskripsi
<code>OrganizationEmailReceived</code>	<p>Jumlah email yang diterima oleh WorkMail organisasi Amazon Anda. Jika satu email ditujukan ke 10 penerima di organisasi Anda, <code>OrganizationEmailReceived</code> hitungannya adalah satu.</p> <p>Unit: Hitungan</p>
<code>MailboxEmailDelivered</code>	<p>Jumlah email yang dikirimkan ke kotak pesan individual di WorkMail organisasi Amazon Anda. Jika satu email berhasil dikirim ke 10</p>

Metrik	Deskripsi
	<p>penerima di organisasi Anda, <code>MailboxEmailDelivered</code> hitungannya adalah 10.</p> <p>Unit: Hitungan</p>
<code>IncomingEmailBounced</code>	<p>Jumlah email masuk yang memental karena kotak pesan penuh. Metrik ini dihitung untuk setiap penerima yang dituju. Misalnya, jika satu email dikirim ke 10 penerima di organisasi Anda, dan dua penerima memiliki kotak pesan penuh yang menghasilkan respons pentalan, jumlahnya adalah dua. <code>IncomingEmailBounced</code></p> <p>Unit: Hitungan</p>
<code>OutgoingEmailBounced</code>	<p>Jumlah email keluar yang tidak dapat dikirimkan. Metrik ini dihitung untuk setiap penerima yang dituju. Misalnya, jika satu email dikirim ke 10 penerima, dan dua email tidak dapat dikirim, <code>OutgoingEmailBounced</code> hitungannya adalah 2.</p> <p>Unit: Hitungan</p>
<code>OutgoingEmailSent</code>	<p>Jumlah email yang berhasil dikirim dari WorkMail organisasi Amazon Anda. Metrik ini dihitung untuk setiap penerima email yang berhasil dikirim. Misalnya, jika 1 email dikirim ke 10 penerima, dan email berhasil dikirim ke 8 penerima, jumlah <code>OutgoingEmailSent</code> adalah 8.</p> <p>Unit: Hitungan</p>

Metrik	Deskripsi
AuthenticationFailure	<p>Metrik ini menghitung jumlah upaya otentikasi. Ketika otentikasi berhasil, hitungannya adalah 0 dan ketika otentikasi tidak berhasil, hitungannya adalah 1. Gunakan Sum statistik untuk memantau jumlah upaya otentikasi yang gagal. Gunakan Sample count statistik untuk memantau jumlah total peristiwa otentikasi. Gunakan Average statistik untuk memantau rasio peristiwa otentikasi yang gagal dan berhasil.</p> <p>Unit: Hitungan</p>
AccessDenied	<p>Metrik ini menghitung jumlah evaluasi kontrol akses. Ketika tindakan ditolak oleh kontrol akses, hitungannya adalah 1 dan ketika tindakan diberikan, hitungannya adalah 0. Gunakan Sum statistik untuk memantau volume tindakan yang ditolak, Sample count statistik untuk memantau jumlah total tindakan yang dicoba, dan Average statistik untuk memantau rasio tindakan yang diizinkan dan ditolak.</p> <p>Unit: Hitungan</p>

Metrik	Deskripsi
ActionDenied	<p>Metrik ini dihitung ketika ada tindakan pada data kotak pesan. Ketika tindakan ditolak, hitungannya adalah 1 dan jika tindakan diberikan, hitungannya adalah 0. Gunakan Sum statistik untuk memantau volume tindakan kotak pesan yang ditolak, Sample count statistik untuk memantau jumlah total tindakan kotak pesan yang dicoba, dan Average statistik untuk memantau rasio tindakan yang diizinkan dan ditolak.</p> <p>Unit: Hitungan</p>
AvailabilityProviderFailure	<p>Metrik ini dihitung untuk setiap permintaan penyedia ketersediaan yang WorkMail dijalankan Amazon untuk mengambil ketersediaan kalender dari sumber eksternal. Untuk informasi selengkapnya tentang Penyedia Ketersediaan, lihat Panduan WorkMail Administrator Amazon.</p>

Memantau log peristiwa WorkMail email Amazon

Saat Anda mengaktifkan pencatatan peristiwa email untuk WorkMail organisasi Amazon Anda, Amazon WorkMail mencatat peristiwa email dengan CloudWatch. Untuk informasi selengkapnya tentang mengaktifkan pencatatan peristiwa email, lihat [Mengaktifkan pencatatan peristiwa email](#).

Tabel berikut menjelaskan peristiwa yang digunakan Amazon untuk WorkMail log CloudWatch, kapan peristiwa ditransmisikan, dan isi bidang peristiwa.

ORGANISASI_EMAIL_RECEIVED

Peristiwa ini dicatat ketika WorkMail organisasi Amazon Anda menerima pesan email.

Bidang	Deskripsi
penerima	Penerima pesan yang dimaksud.
pengirim	Alamat email pengguna yang mengirim pesan email atas nama pengguna lain. Bidang ini diatur hanya jika suatu email dikirim atas nama pengguna lain.
From	Alamat Dari, yang biasanya alamat email dari pengguna yang mengirim pesan. Jika pengguna mengirim pesan sebagai pengguna lain atau atas nama pengguna lain, bidang ini mengembalikan alamat email pengguna atas nama siapa email dikirim, bukan alamat email pengirim sebenarnya.
subjek	Subjek pesan email.
messageId	ID pesan SMTP.
SpamVerdict	Menunjukkan apakah pesan ditandai sebagai spam oleh Amazon SES. Untuk informasi selengkapnya, lihat Konten Notifikasi untuk Penerimaan Email Amazon SES dalam Panduan Developer Amazon Simple Email Service.
dkimVerdict	Menunjukkan apakah cek DomainKeys Identified Mail (DKIM) lulus. Untuk informasi selengkapnya, lihat Konten Notifikasi untuk Penerimaan Email Amazon SES dalam Panduan Developer Amazon Simple Email Service.
DmarcVerdict	Menunjukkan apakah pemeriksaan Domain-based Message Authentication, Reporting and Conformance (DMARC) lulus. Untuk informasi selengkapnya, lihat Konten Notifikas

Bidang	Deskripsi
	i untuk Penerimaan Email Amazon SES dalam Panduan Developer Amazon Simple Email Service.
dmarcPolicy	Muncul hanya ketika bidang dmarcVerdict berisi "FAIL". Menunjukkan tindakan yang harus dilakukan terhadap email ketika pemeriksaan DMARC gagal (NONE, QUARANTINE, atau REJECT). Tindakan ini diatur oleh pemilik domain email pengiriman.
spfVerdict	Menunjukkan apakah pemeriksaan Kerangka Kebijakan Pengirim (SPF) lulus. Untuk informasi selengkapnya, lihat Konten Notifikasi i untuk Penerimaan Email Amazon SES dalam Panduan Developer Amazon Simple Email Service.
MessageTimestamp	Menunjukkan kapan pesan diterima.

MAILBOX_EMAIL_DELIVERED

Peristiwa ini dicatat saat pesan dikirim ke kotak pesan di organisasi Anda. Ini dicatat satu kali untuk setiap kotak surat yang menjadi tujuan pengiriman pesan, sehingga satu peristiwa ORGANIZATION_EMAIL_RECEIVED dapat mengakibatkan beberapa peristiwa MAILBOX_EMAIL_DELIVERED.

Bidang	Deskripsi
penerima	Kotak pesan yang menjadi tujuan pengiriman pesan.
folder	Folder kotak pesan tempat pesan ditempatkan.

RULE_APPLIED

Peristiwa ini dicatat ketika pesan masuk atau keluar memulai aturan alur email.

Bidang	Deskripsi
ruleName	Nama aturan.
ruleType	Jenis aturan yang diterapkan (INBOUND_RULE, OUTBOUND_RULE, atau MAILBOX_RULE). Aturan masuk dan keluar berlaku untuk organisasi Amazon WorkMail Anda. Aturan kotak pesan hanya berlaku untuk kotak pesan yang ditentukan. Untuk informasi selengkapnya, lihat Mengelola alur email .
RuleAction	Tindakan yang diambil berdasarkan aturan. Penerima pesan yang berbeda mungkin memiliki tindakan yang berbeda, seperti email yang dipantulkan atau email yang berhasil dikirim.
targetFolder	Folder tujuan yang dimaksudkan untuk Move atau Copy MAILBOX_RULE.
targetRecipient	Penerima yang dimaksudkan dari Forward atau Redirect MAILBOX_RULE.

JOURNALING_INITIATED

Peristiwa ini dicatat saat Amazon WorkMail mengirim email ke alamat penjurnalan yang ditentukan oleh administrator organisasi Anda. Ini hanya ditransmisikan jika penjurnalan dikonfigurasi untuk organisasi Anda. Untuk informasi selengkapnya, lihat [Menggunakan jurnal email dengan Amazon WorkMail](#).

Bidang	Deskripsi
journalingAddress	Alamat email yang menjadi tujuan pengiriman pesan penjurnalan.

MASUK_EMAIL_MEMANTUL

Peristiwa ini dicatat ketika pesan masuk tidak dapat dikirim ke penerima target. Email dapat memental karena sejumlah alasan, seperti kotak pesan target penuh. Sistem mencatat peristiwa ini sekali untuk setiap penerima yang menghasilkan email yang dipentalkan. Misalnya, jika pesan masuk ditujukan ke tiga penerima dan dua di antaranya memiliki kotak pesan penuh, dua peristiwa INCOMING_EMAIL_BOUNCED akan dicatat.

Bidang	Deskripsi
bouncedRecipient	Penerima yang dituju di mana Amazon WorkMail memantulkan pesan.

OUTGOING_EMAIL_SUBMIT

Peristiwa ini dicatat ketika pengguna di organisasi Anda mengirimkan pesan email untuk mengirim. Ini dicatat sebelum pesan meninggalkan Amazon WorkMail, jadi acara ini tidak menunjukkan apakah email berhasil dikirim.

Bidang	Deskripsi
penerima	Penerima pesan seperti yang ditentukan oleh pengirim. Mencakup semua penerima pada baris Kepada, CC, dan BCC.
pengirim	Alamat email pengguna yang mengirim pesan email atas nama pengguna lain. Bidang ini diatur hanya jika suatu email dikirim atas nama pengguna lain.
From	Alamat Dari, yang biasanya alamat email dari pengguna yang mengirim pesan. Jika pengguna mengirim pesan sebagai pengguna lain atau atas nama pengguna lain, bidang ini mengembalikan alamat email pengguna atas nama siapa email dikirim, bukan alamat email pengirim sebenarnya.

Bidang	Deskripsi
subjek	Subjek pesan email.

OUTGOING_EMAIL_SENT

Peristiwa ini dicatat ketika email keluar berhasil dikirim ke penerima target. Ini dicatat satu kali untuk setiap penerima sukses, sehingga satu OUTGOING_EMAIL_SUBMITTED dapat mengakibatkan beberapa entri OUTGOING_EMAIL_SENT.

Bidang	Deskripsi
penerima	Penerima email yang berhasil dikirim.
pengirim	Alamat email pengguna yang mengirim pesan email atas nama pengguna lain. Bidang ini diatur hanya jika suatu email dikirim atas nama pengguna lain.
From	Alamat Dari, yang biasanya alamat email dari pengguna yang mengirim pesan. Jika pengguna mengirim pesan sebagai pengguna lain atau atas nama pengguna lain, bidang ini mengembalikan alamat email pengguna atas nama siapa email dikirim, bukan alamat email pengirim sebenarnya.
messageid	ID pesan SMTP.

OUTGOING_EMAIL_BOUNCE

Peristiwa ini dicatat ketika pesan keluar tidak dapat dikirim ke penerima target. Email dapat memental karena sejumlah alasan, seperti kotak pesan target penuh. Sistem mencatat pentalan untuk setiap penerima yang menghasilkan email yang dipentalkan. Misalnya, jika pesan keluar ditujukan ke tiga penerima dan dua di antaranya memiliki kotak pesan penuh, dua peristiwa OUTGOING_EMAIL_BOUNCED akan dicatat.

Bidang	Deskripsi
bouncedRecipient	Penerima yang dimaksudkan yang menjadi tujuan server surat mementalkan pesan.

DMARC_POLICY_APPLIED

Peristiwa ini dicatat ketika kebijakan DMARC diterapkan pada email yang dikirim ke organisasi Anda.

Bidang	Deskripsi
From	Alamat Dari, yang biasanya alamat email dari pengguna yang mengirim pesan. Jika pengguna mengirim pesan sebagai pengguna lain atau atas nama pengguna lain, bidang ini mengembalikan alamat email pengguna atas nama siapa email dikirim, bukan alamat email pengirim sebenarnya.
penerima	Penerima pesan yang dimaksud.
kebijakan	Kebijakan DMARC yang diterapkan, yang menunjukkan tindakan yang harus dilakukan terhadap email ketika pemeriksaan DMARC gagal (NONE, QUARANTINE, atau REJECT). Ini adalah sama dengan bidang dmarcPolicy dalam peristiwa ORGANIZATION_EMAIL_RECEIVED.

Memantau log WorkMail audit Amazon

Anda dapat menggunakan log audit untuk memantau akses ke kotak pesan WorkMail Organisasi Amazon Anda. Amazon WorkMail mencatat lima jenis peristiwa audit dan peristiwa ini dapat dipublikasikan ke CloudWatch Log, Amazon S3, atau Amazon Firehouse. Anda dapat menggunakan log audit untuk memantau interaksi pengguna dengan kotak pesan Organisasi, upaya autentikasi, evaluasi aturan kontrol akses, dan melakukan panggilan penyedia ketersediaan ke sistem eksternal

dan memantau peristiwa dengan token akses pribadi. Untuk informasi tentang mengonfigurasi pencatatan audit, lihat [Mengaktifkan pencatatan audit](#).

Bagian berikut menjelaskan peristiwa audit yang dicatat oleh Amazon WorkMail, saat peristiwa ditransmisikan, dan informasi tentang bidang acara.

Log akses kotak surat

Peristiwa akses kotak pesan memberikan informasi tentang tindakan apa yang diambil (atau dicoba) pada objek kotak pesan mana. Peristiwa akses kotak pesan dibuat untuk setiap operasi yang Anda coba jalankan pada item atau folder di kotak pesan. Peristiwa ini berguna untuk mengaudit akses ke data kotak pesan.

Bidang	Deskripsi
event_timestamp	Ketika peristiwa itu terjadi, dalam milidetik sejak zaman Unix.
request_id	ID yang secara unik mengidentifikasi permintaan.
organisasi_arn	ARN dari WorkMail Organisasi & Amazon tempat pengguna yang diautentikasi berada.
user_id	ID pengguna yang diautentikasi.
impersonator_id	ID peniru. Hadir hanya jika fitur peniruan digunakan untuk permintaan.
protokol	Protokol yang digunakan. Protokolnya dapat berupa: AutoDiscover, EWS, IMAP, Windows Outlook, ActiveSync, SMTP, WebMail, IncomingEmail, atau OutgoingEmail.
source_ip	Alamat IP sumber permintaan.
user_agent	Agen pengguna yang membuat permintaan.

Bidang	Deskripsi
tindakan	Tindakan yang diambil pada objek, yang dapat berupa:read,read_hierarchy ,read_summary ,read_attachment ,read_permissions ,create,update,update_permissions ,update_read_state delete,submit_email_for_sending ,abort_sending_email ,move,move_to,copy, ataucopy_to.
owner_id	ID pengguna yang memiliki objek yang ditindaklanjuti.
object_type	Jenis objek, yang dapat berupa: Folder, Pesan, atau Lampiran.
item_id	ID yang secara unik mengidentifikasi pesan yang menjadi subjek acara atau yang berisi lampiran yang menjadi subjek acara.
folder_path	Jalur folder yang ditindaklanjuti atau jalur folder yang berisi item yang ditindaklanjuti.
folder_id	ID yang secara unik mengidentifikasi folder yang menjadi subjek acara atau berisi objek yang menjadi subjek acara.
attachment_path	Jalur nama tampilan ke lampiran yang terpengaruh.
action_allowed	Apakah tindakan itu diizinkan. Bisa benar atau salah.

Log kontrol akses

Peristiwa kontrol akses dihasilkan setiap kali aturan kontrol akses dievaluasi. Log ini berguna untuk mengaudit akses terlarang, atau men-debug konfigurasi kontrol akses.

Bidang	Deskripsi
event_timestamp	Ketika peristiwa itu terjadi, dalam milidetik sejak zaman Unix.
request_id	ID yang secara unik mengidentifikasi permintaan.
organisasi_arn	ARN WorkMail Organisasi tempat pengguna yang diautentikasi berada.
user_id	ID pengguna yang diautentikasi.
impersonator_id	ID peniru. Hadir hanya jika fitur peniruan digunakan untuk permintaan.
protokol	Protokol yang digunakan, yang dapat berupa:AutoDiscover ,EWS,IMAP,WindowsOutlook ,ActiveSync ,SMTP,WebMail,IncomingEmail , atauOutgoingEmail .
source_ip	Alamat IP sumber permintaan.
cakupan	Ruang lingkup aturan, yang dapat berupa:AccessControl ,DeviceAccessControl , atauImpersonationAccessControl .
rule_id	ID dari aturan kontrol akses yang cocok. Bila tidak ada aturan yang cocok, rule_id tidak tersedia.
access_granted	Apakah akses diizinkan. Bisa benar atau salah.

Log otentikasi

Peristiwa otentikasi berisi informasi tentang upaya otentikasi.

Note

Peristiwa otentikasi tidak dibuat untuk peristiwa otentikasi melalui aplikasi Amazon WorkMail WebMail .

Bidang	Deskripsi
event_timestamp	Ketika peristiwa itu terjadi, dalam milidetik sejak zaman Unix.
request_id	ID yang secara unik mengidentifikasi permintaan.
organisasi_arn	ARN WorkMail Organisasi tempat pengguna yang diautentikasi berada.
user_id	ID pengguna yang diautentikasi.
user	Nama pengguna yang dicoba dengan otentikasi.
protokol	Protokol yang digunakan, yang dapat berupa:AutoDiscover ,EWS,IMAP,WindowsOutlook ,ActiveSync ,SMTP,WebMail,IncomingEmail , atauOutgoingEmail .
source_ip	Alamat IP sumber permintaan.
user_agent	Agen pengguna yang membuat permintaan.
metode	Metode autentikasi. Saat ini, hanya dasar yang didukung.

Bidang	Deskripsi
auth_successful	Apakah upaya autentikasi berhasil. Bisa benar atau salah.
auth_failed_reason	Alasan kegagalan autentikasi. Hadir hanya jika autentikasi gagal.
personal_access_token_id	ID token akses pribadi yang digunakan untuk otentikasi.

Log token akses pribadi

Peristiwa token akses pribadi (PAT) dibuat untuk setiap upaya dalam membuat atau menghapus token akses pribadi. Acara token akses pribadi memberikan informasi tentang apakah pengguna berhasil membuat token akses pribadi. Log token akses pribadi berguna untuk mengaudit pengguna akhir yang membuat dan menghapus PAT mereka sendiri. Login pengguna dengan token akses pribadi akan menghasilkan peristiwa di log Otentikasi yang ada. Untuk informasi selengkapnya, lihat [Log otentikasi](#).

Bidang	Deskripsi
event_timestamp	Ketika peristiwa itu terjadi, dalam milidetik sejak zaman Unix.
request_id	ID yang secara unik mengidentifikasi permintaan.
organisasi_arn	ARN WorkMail Organisasi tempat pengguna yang diautentikasi berada.
user_id	ID pengguna yang diautentikasi.
user	Nama pengguna pengguna yang mengambil tindakan ini.
protokol	Protokol yang digunakan melalui tindakan berlangsung, yang dapat berupa: webapp

Bidang	Deskripsi
source_ip	Alamat IP sumber permintaan.
user_agent	Agen pengguna yang membuat permintaan.
tindakan	Tindakan token akses pribadi, yang dapat berupa: membuat atau menghapus.
name	Nama token akses pribadi.
kadaluarsa_waktu	Tanggal ketika token akses pribadi kedaluwarsa.
ruang_lingkup	Cakupan izin token akses pribadi di kotak surat.

Log penyedia ketersediaan

Acara penyedia ketersediaan dibuat untuk setiap permintaan ketersediaan yang WorkMail dilakukan Amazon atas nama Anda kepada penyedia ketersediaan yang dikonfigurasi. Peristiwa ini berguna untuk men-debug konfigurasi penyedia ketersediaan Anda.

Bidang	Deskripsi
event_timestamp	Ketika peristiwa itu terjadi, dalam milidetik sejak zaman Unix.
request_id	ID yang secara unik mengidentifikasi permintaan.
organisasi_arn	ARN WorkMail Organisasi tempat pengguna yang diautentikasi berada.
user_id	ID pengguna yang diautentikasi.
jenis	Jenis penyedia ketersediaan yang dipanggil, yang dapat berupa: EWS atau LAMBDA.
domain	Domain yang ketersediaannya diperoleh.

Bidang	Deskripsi
function_arn	ARN dari Lambda yang dipanggil, jika jenisnya adalah LAMBDA. Jika tidak, bidang ini tidak ada.
ews_titik_akhir	Endpoint EWS adalah tipe EWS. Jika tidak, bidang ini tidak ada.
error_message	Pesan yang menggambarkan penyebab kegagalan. Jika permintaan berhasil, bidang ini tidak ada.
availability_event_successful	Apakah permintaan ketersediaan berhasil dilayani.

Menggunakan CloudWatch Wawasan dengan Amazon WorkMail

Jika mengaktifkan pencatatan peristiwa email di WorkMail konsol Amazon atau mengaktifkan pengiriman log audit ke Log, Anda dapat menggunakan Amazon CloudWatch CloudWatch Logs Insights untuk menanyakan log peristiwa Anda. Untuk informasi selengkapnya tentang mengaktifkan pencatatan peristiwa email, lihat [Mengaktifkan pencatatan peristiwa email](#). Untuk informasi selengkapnya tentang Wawasan CloudWatch Log, lihat [Menganalisis data CloudWatch log dengan Wawasan Log](#) di Panduan Pengguna CloudWatch Log Amazon.

Contoh berikut menunjukkan cara kueri CloudWatch Log untuk acara email umum. Anda menjalankan kueri ini di CloudWatch konsol. Untuk petunjuk tentang cara menjalankan kueri ini, lihat [Tutorial: Menjalankan dan memodifikasi contoh kueri](#) di Panduan Pengguna Amazon CloudWatch Logs.

Example Lihat mengapa Pengguna B tidak menerima email yang dikirim oleh Pengguna A.

Contoh kode berikut menunjukkan bagaimana untuk meminta email keluar yang dikirim oleh Pengguna A ke Pengguna B, diurutkan berdasarkan timestamp.

```
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/)
```

Ini mengembalikan pesan yang dikirim dan ID jejak. Gunakan ID jejak dalam contoh kode berikut untuk meminta pencatatan peristiwa untuk pesan terkirim.

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

Ini mengembalikan ID pesan email dan peristiwa email. `OUTGOING_EMAIL_SENT` menunjukkan bahwa email telah dikirim. `OUTGOING_EMAIL_BOUNCED` menunjukkan bahwa email terpental. Untuk melihat apakah email diterima, kueri menggunakan ID pesan dalam contoh kode berikut.

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

Ini juga seharusnya mengembalikan pesan yang diterima, karena memiliki ID pesan yang sama. Gunakan ID jejak dalam contoh kode berikut untuk kueri untuk pengiriman.

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

Ini mengembalikan tindakan pengiriman dan tindakan aturan yang berlaku.

Example Melihat semua email yang diterima dari pengguna atau domain

Contoh kode berikut mendemonstrasikan cara meminta semua surat yang diterima dari pengguna tertentu.

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

Contoh kode berikut mendemonstrasikan cara meminta semua surat yang diterima dari domain tertentu.

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

Example Lihat siapa yang mengirim email yang memantul

Contoh kode berikut menunjukkan bagaimana meminta email keluar yang terpental, dan juga mengembalikan alasan untuk pementalan.

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

Contoh kode berikut menunjukkan bagaimana untuk query untuk email masuk yang memantul. Ini juga mengembalikan alamat email penerima yang terpental dan alasan memantul.

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

Example Lihat domain mana yang mengirim spam

Contoh kode berikut mendemonstrasikan cara meminta penerima di organisasi Anda yang menerima spam.

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

Contoh kode berikut mendemonstrasikan cara meminta pengirim email spam.

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

Example Lihat mengapa email dikirim ke folder spam penerima

Contoh kode berikut mendemonstrasikan cara meminta email yang diidentifikasi sebagai spam, disaring berdasarkan subjek.

```
fields @timestamp, event.recipients.0, event.spamVerdict, event.spfVerdict,
  event.dkimVerdict, event.dmarcVerdict
| sort @timestamp asc
| filter event.subject like /(?!i)$SUBJECT/ and event.eventName =
  "ORGANIZATION_EMAIL_RECEIVED"
```

Anda juga dapat meminta berdasarkan ID jejak email untuk melihat semua peristiwa untuk email.

Example Lihat email yang cocok dengan aturan alur email

Contoh kode berikut mendemonstrasikan cara meminta email yang cocok dengan aturan aliran email keluar.

```
fields @timestamp, event.ruleName, event.ruleActions.0.action
| sort @timestamp desc
| filter event.ruleType = "OUTBOUND_RULE"
```

Contoh kode berikut mendemonstrasikan cara meminta email yang cocok dengan aturan aliran email masuk.

```
fields @timestamp, event.ruleName, event.ruleActions.0.action,
  event.ruleActions.0.recipients.0
| sort @timestamp desc
| filter event.ruleType = "INBOUND_RULE"
```

Example Lihat berapa banyak email yang diterima atau dikirim oleh organisasi Anda

Contoh kode berikut mendemonstrasikan cara meminta jumlah email yang diterima oleh setiap penerima di organisasi Anda.

```
stats count(*) as c by event.recipient
| filter event.eventName = "MAILBOX_EMAIL_DELIVERED"
| sort c desc
```

Contoh kode berikut mendemonstrasikan cara meminta jumlah email yang dikirim oleh masing-masing pengirim di organisasi Anda.

```
stats count(*) as c by event.from
| filter event.eventName = "OUTGOING_EMAIL_SUBMITTED"
| sort c desc
```

Mencatat panggilan WorkMail API Amazon dengan AWS CloudTrail

Amazon WorkMail terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS di Amazon WorkMail. CloudTrail menangkap semua panggilan API untuk Amazon WorkMail sebagai peristiwa, termasuk panggilan dari WorkMail konsol Amazon dan dari panggilan kode ke WorkMail API Amazon. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail secara berkala ke bucket Amazon S3, termasuk acara untuk Amazon WorkMail. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Amazon WorkMail, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

WorkMail Informasi Amazon di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Amazon WorkMail, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan Layanan AWS peristiwa lain dalam riwayat Peristiwa. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan riwayat CloudTrail acara](#).

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Amazon WorkMail, Anda harus membuat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi lebih lanjut, lihat:

- [Ikhtisar untuk membuat jejak](#)

- [CloudTrail layanan dan integrasi yang didukung](#)
- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima file CloudTrail log dari beberapa Wilayah](#) dan [Menerima file CloudTrail log dari beberapa akun](#)

Semua WorkMail tindakan Amazon dicatat oleh CloudTrail dan didokumentasikan dalam [Referensi WorkMail API Amazon](#). Misalnya, panggilan ke `CreateUserCreateAlias`, dan operasi `GetRawMessageContent` API menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan tersebut dibuat dengan kredensial root atau pengguna IAM.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#).

Memahami entri file WorkMail log Amazon

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Sebuah kejadian mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. Berkas log CloudTrail bukan merupakan jejak tumpukan terurut dari panggilan API publik, sehingga tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `CreateUser` tindakan dari 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": "2017-12-12T17:49:59Z",
  "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"
}

```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan CreateAlias tindakan dari 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"
  "entityId": "a3a9176d-EXAMPLE"
},
"responseElements": null,
"requestID": "dec81e4a-EXAMPLE",
"eventID": "9f2f09c5-EXAMPLE",
"eventType": "AwsApiCall",
"recipientAccountId": "111111111111"
}

```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan GetRawMessageContent tindakan dari 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": "workmailMessageFlow.amazonaws.com",
  "eventName": "GetRawMessageContent",
  "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": {
    "messageId": "123A4A5A-67B8-90C1-D23E-45FG67H890J1"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}

```

}

Mengaktifkan pencatatan peristiwa email

Anda mengaktifkan pencatatan peristiwa email di WorkMail konsol Amazon untuk melacak pesan email untuk organisasi Anda. Pencatatan peristiwa email menggunakan peran AWS Identity and Access Management terkait layanan (SLR) untuk memberikan izin untuk mempublikasikan log peristiwa email ke Amazon CloudWatch. Untuk informasi selengkapnya tentang peran terkait layanan IAM, lihat [Menggunakan peran terkait layanan untuk Amazon WorkMail](#).

Dalam log CloudWatch peristiwa, Anda dapat menggunakan alat CloudWatch pencarian dan metrik untuk melacak pesan dan memecahkan masalah email. Untuk informasi selengkapnya tentang log peristiwa yang dikirimkan Amazon CloudWatch, lihat [Memantau log peristiwa WorkMail email Amazon](#). Untuk informasi selengkapnya tentang CloudWatch Log, lihat [Panduan Pengguna CloudWatch Log Amazon](#).

Topik

- [Mengaktifkan pencatatan peristiwa email](#)
- [Membuat grup log kustom dan IAM role untuk pencatatan peristiwa email](#)
- [Mematikan pencatatan peristiwa email](#)
- [Cross-service pencegahan wakil bingung](#)

Mengaktifkan pencatatan peristiwa email

Berikut ini terjadi ketika Anda mengaktifkan pencatatan peristiwa email menggunakan pengaturan default, Amazon WorkMail:


- Menciptakan peran AWS Identity and Access Management terkait layanan — `AmazonWorkMailEvents`
- Membuat grup CloudWatch log `—/aws/workmail/emailevents/organization-alias`.
- Menetapkan retensi CloudWatch log ke 30 hari.

Cara mengaktifkan pencatatan peristiwa email

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Pengaturan logging.
4. Pilih tab Pengaturan log alur email.
5. Di bagian Pengaturan log alur email, pilih Edit.
6. Pindahkan slider Aktifkan acara email ke posisi aktif.
7. Lakukan salah satu tindakan berikut:
 - (Disarankan) Pilih Gunakan pengaturan default.
 - (Opsional) Hapus pengaturan default Gunakan, dan pilih Grup Log Tujuan dan Peran IAM dari daftar yang muncul.

 Note

Pilih opsi ini hanya jika Anda telah membuat grup log dan IAM role kustom menggunakan AWS CLI. Untuk informasi selengkapnya, lihat [Membuat grup log kustom dan IAM role untuk pencatatan peristiwa email](#).

8. Pilih Saya mengotorisasi Amazon WorkMail untuk menerbitkan log di akun saya menggunakan konfigurasi ini.
9. Pilih Simpan.

Membuat grup log kustom dan IAM role untuk pencatatan peristiwa email

Sebaiknya gunakan pengaturan default saat mengaktifkan pencatatan peristiwa email untuk Amazon WorkMail. Jika Anda memerlukan konfigurasi pemantauan khusus, Anda dapat menggunakannya AWS CLI untuk membuat grup log khusus dan peran IAM khusus untuk pencatatan peristiwa email.

Untuk membuat grup log dan IAM role kustom untuk pencatatan peristiwa email

1. Gunakan AWS CLI perintah berikut untuk membuat grup log di AWS Wilayah yang sama dengan WorkMail organisasi Amazon Anda. Untuk informasi lebih lanjut, lihat [create-log-group](#) dalam Referensi Perintah AWS CLI .

```
aws --region us-east-1 logs create-log-group --log-group-name workmail-monitoring
```

2. Buat file yang berisi kebijakan berikut ini:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "events.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. Gunakan AWS CLI perintah berikut untuk membuat peran IAM dan lampirkan file ini sebagai dokumen kebijakan peran. Untuk informasi lebih lanjut, lihat [create-role](#) dalam Referensi Perintah AWS CLI .

```
aws iam create-role --role-name workmail-monitoring-role --assume-role-policy-document file://trustpolicyforworkmail.json
```

Note

Jika Anda pengguna kebijakan WorkMailFullAccess terkelola, Anda harus menyertakan istilah `workmail` dalam nama peran. Kebijakan terkelola ini hanya memungkinkan Anda mengkonfigurasi pencatatan peristiwa email menggunakan peran dengan `workmail` dalam nama tersebut. Untuk informasi selengkapnya, lihat [Memberikan izin pengguna untuk meneruskan peran ke AWS layanan](#) di Panduan Pengguna IAM.

4. Buat file yang berisi kebijakan untuk peran IAM yang Anda buat di langkah sebelumnya. Minimal, kebijakan harus memberikan izin untuk peran untuk membuat pengaliran log dan menempatkan peristiwa log ke grup log yang Anda buat pada langkah 1.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:us-east-1:111122223333:log-
group:example-log-group*"
    }
  ]
}
```

5. Gunakan AWS CLI perintah berikut untuk melampirkan file kebijakan ke peran IAM. Untuk informasi selengkapnya, lihat [put-role-policy](#) dalam Referensi Perintah AWS CLI .

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

Mematikan pencatatan peristiwa email

Matikan pencatatan peristiwa email dari WorkMail konsol Amazon. Jika Anda tidak perlu lagi menggunakan pencatatan peristiwa email, sebaiknya hapus grup CloudWatch log terkait dan peran terkait layanan juga. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan untuk Amazon WorkMail](#).

Untuk mematikan pencatatan peristiwa email

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.

3. Di panel navigasi, pilih Pemantauan.
4. Di bagian Pengaturan log, pilih Edit.
5. Pindahkan penggeser Aktifkan acara email ke posisi mati.
6. Pilih Simpan.

Cross-service pencegahan wakil bingung

Masalah "confused deputy" adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memengaruhi entitas yang memiliki hak akses lebih tinggi untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Cross-service peniruan identitas dapat terjadi ketika satu layanan (layanan panggilan) memanggil layanan lain (layanan yang disebut).

Layanan panggilan dapat dimanipulasi untuk menggunakan izinnya untuk bertindak atas sumber daya pelanggan lain yang tidak akan memiliki izin untuk mengaksesnya.

Untuk mencegah hal ini, AWS sediakan alat yang membantu Anda melindungi data Anda untuk semua layanan dengan prinsip layanan yang telah diberikan akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi [aws:SourceAccount](#) global [aws:SourceArn](#) dan global dalam kebijakan sumber daya untuk membatasi izin yang diberikan CloudWatch Log dan Amazon S3 ke layanan yang menghasilkan log. Jika Anda menggunakan kedua kunci konteks kondisi global, nilai harus menggunakan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama.

Nilai `aws:SourceArn` harus berupa ARN dari sumber pengiriman yang menghasilkan log.

Cara paling efektif untuk melindungi dari masalah "confused deputy" adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci konteks kondisi `aws:SourceArn` global dengan wildcard (*) untuk bagian ARN yang tidak diketahui.

Mengaktifkan pencatatan audit

Anda dapat menggunakan log audit untuk menangkap informasi terperinci tentang penggunaan WorkMail organisasi Amazon Anda. Log audit dapat digunakan untuk memantau akses pengguna ke kotak pesan, mengaudit aktivitas mencurigakan, dan men-debug kontrol akses dan konfigurasi penyedia ketersediaan.

Note

Kebijakan AmazonWorkMailFullAccesssterkelola tidak mencakup semua izin yang diperlukan untuk mengelola pengiriman log. Jika Anda menggunakan kebijakan ini untuk mengelola WorkMail, pastikan prinsipal (misalnya, peran yang diasumsikan) yang digunakan untuk mengonfigurasi pengiriman log juga memiliki semua izin yang diperlukan.

Amazon WorkMail mendukung tiga tujuan pengiriman untuk log audit: CloudWatch Log, Amazon S3, dan Amazon Data Firehose. Untuk informasi selengkapnya, lihat [Logging yang memerlukan izin tambahan \[V2\]](#) di [Panduan Pengguna Amazon CloudWatch Logs](#).

Selain izin yang tercantum dalam [Logging yang memerlukan izin tambahan \[V2\]](#), Amazon WorkMail memerlukan izin tambahan untuk mengonfigurasi pengiriman log:
`workmail:AllowVendedLogDeliveryForResource`


Pengiriman log kerja terdiri dari tiga elemen:

- `DeliverySource`, objek logis yang mewakili sumber daya atau sumber daya yang mengirim log. Untuk Amazon WorkMail, ini adalah WorkMail Organisasi Amazon.
- `DeliveryDestination`, yang merupakan objek logis yang mewakili tujuan pengiriman yang sebenarnya.
- Pengiriman, yang menghubungkan sumber pengiriman ke tujuan pengiriman.

Untuk mengonfigurasi pengiriman log antara Amazon WorkMail dan tujuan, Anda dapat melakukan hal berikut:

- Buat sumber pengiriman dengan [PutDeliverySource](#).
- Buat tujuan pengiriman dengan [PutDeliveryDestination](#).
- Jika Anda mengirimkan log lintas akun, Anda harus menggunakan [PutDeliveryDestinationPolicy](#) di akun tujuan untuk menetapkan kebijakan IAM ke tujuan. Kebijakan ini mengizinkan pembuatan pengiriman dari sumber pengiriman di akun A ke tujuan pengiriman di akun B.
- Buat pengiriman dengan memasang tepat satu sumber pengiriman dan satu tujuan pengiriman dengan menggunakan [CreateDelivery](#).

Bagian berikut memberikan rincian izin yang harus Anda miliki saat masuk untuk menyiapkan pengiriman log ke setiap jenis tujuan. Izin ini dapat diberikan ke peran IAM yang Anda gunakan untuk masuk.

 Important

Anda bertanggung jawab untuk menghapus sumber daya pengiriman log setelah menghapus sumber daya penghasil log.

Untuk menghapus sumber daya pengiriman log setelah menghapus sumber daya penghasil log, ikuti langkah-langkah berikut.

1. Hapus Pengiriman dengan menggunakan [DeleteDelivery](#) operasi.
2. Hapus DeliverySource dengan menggunakan [DeleteDeliverySource](#) operasi.
3. Jika yang DeliveryDestination terkait dengan DeliverySource yang baru saja Anda hapus hanya digunakan untuk spesifik ini DeliverySource, maka Anda dapat menghapusnya dengan menggunakan [DeleteDeliveryDestinations](#) operasi.

Mengonfigurasi pencatatan audit menggunakan konsol Amazon WorkMail

Anda dapat mengonfigurasi pencatatan audit di WorkMail konsol Amazon:

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Pilih pengaturan Logging.
4. Pilih tab Pengaturan log audit.
5. Konfigurasi pengiriman untuk jenis log yang diperlukan menggunakan widget yang sesuai.
6. Pilih Simpan.

Log dikirim ke CloudWatch Log

Izin pengguna

Untuk mengaktifkan pengiriman CloudWatch log ke Log, Anda harus masuk dengan izin berikut.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadWriteAccessForLogDeliveryActions",
      "Effect": "Allow",
      "Action": [
        "logs:GetDelivery",
        "logs:GetDeliverySource",
        "logs:PutDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs>DeleteDeliverySource",
        "logs:PutDeliveryDestinationPolicy",
        "logs>CreateDelivery",
        "logs:GetDeliveryDestination",
        "logs:PutDeliverySource",
        "logs>DeleteDeliveryDestination",
        "logs>DeleteDeliveryDestinationPolicy",
        "logs>DeleteDelivery"
      ],
      "Resource": [
        "arn:aws:logs:us-east-1:111122223333:delivery:*",
        "arn:aws:logs:us-east-1:111122223333:delivery-source:*",
        "arn:aws:logs:us-east-1:111122223333:delivery-destination:*"
      ]
    },
    {
      "Sid": "ListAccessForLogDeliveryActions",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDeliveries",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowUpdatesToResourcePolicyCWL",
```

```

    "Effect": "Allow",
    "Action": [
      "logs:PutResourcePolicy",
      "logs:DescribeResourcePolicies",
      "logs:DescribeLogGroups"
    ],
    "Resource": [
      "arn:aws:logs:us-east-1:111122223333:*"
    ]
  },
  {
    "Sid": "AllowLogDeliveryForWorkMail",
    "Effect": "Allow",
    "Action": [
      "workmail:AllowVendedLogDeliveryForResource"
    ],
    "Resource": [
      "arn:aws:workmail:us-east-1:111122223333:organization/organization-id"
    ]
  }
]
}

```

Kebijakan sumber daya grup log

Grup log tempat log dikirim harus memiliki kebijakan sumber daya yang mencakup izin tertentu. Jika grup log saat ini tidak memiliki kebijakan sumber daya, dan pengguna yang mengatur logging memiliki `logs:PutResourcePolicy`, `logs:DescribeResourcePolicies`, dan `logs:DescribeLogGroups` izin untuk grup log, maka AWS secara otomatis membuat kebijakan berikut untuk itu ketika Anda mulai mengirim CloudWatch log ke Log.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite20150319",
      "Effect": "Allow",
      "Principal": {

```

```

        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:us-east-1:111122223333:log-group:my-log-group:log-
stream:*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": [
                "111122223333"
            ]
        },
        "ArnLike": {
            "aws:SourceArn": [
                "arn:aws:logs:us-east-1:111122223333:*"
            ]
        }
    }
}

```

Pertimbangan batas ukuran kebijakan sumber daya grup log

Layanan ini harus mencantumkan setiap grup log tempat mereka mengirim log ke dalam kebijakan sumber daya. CloudWatch Kebijakan sumber daya log dibatasi hingga 5.120 karakter. Layanan yang mengirimkan log ke sejumlah besar grup log mungkin mengalami batas ini.

Untuk mengurangi hal ini, CloudWatch Log memantau ukuran kebijakan sumber daya yang digunakan oleh layanan yang mengirim log. Ketika mendeteksi bahwa kebijakan mendekati batas ukuran 5.120 karakter, CloudWatch Log secara otomatis mengaktifkan `/aws/vendedlogs/*` kebijakan sumber daya untuk layanan tersebut. Anda kemudian dapat mulai menggunakan grup log dengan nama yang dimulai dengan `/aws/vendedlogs/` sebagai tujuan log dari layanan-layanan ini.

Log yang dikirim ke Amazon S3

Izin pengguna

Untuk mengaktifkan pengiriman log ke Amazon S3, Anda harus masuk dengan izin berikut.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadWriteAccessForLogDeliveryActions",
      "Effect": "Allow",
      "Action": [
        "logs:GetDelivery",
        "logs:GetDeliverySource",
        "logs:PutDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs>DeleteDeliverySource",
        "logs:PutDeliveryDestinationPolicy",
        "logs>CreateDelivery",
        "logs:GetDeliveryDestination",
        "logs:PutDeliverySource",
        "logs>DeleteDeliveryDestination",
        "logs>DeleteDeliveryDestinationPolicy",
        "logs>DeleteDelivery"
      ],
      "Resource": [
        "arn:aws:logs:us-east-1:111122223333:delivery:*",
        "arn:aws:logs:us-east-1:111122223333:delivery-source:*",
        "arn:aws:logs:us-east-1:111122223333:delivery-destination:*"
      ]
    },
    {
      "Sid": "ListAccessForLogDeliveryActions",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDeliveries",
        "logs:DescribeLogGroups"
      ]
    }
  ]
}
```

```

        "Resource": "*"
    },
    {
        "Sid": "AllowUpdatesToResourcePolicyS3",
        "Effect": "Allow",
        "Action": [
            "s3:PutBucketPolicy",
            "s3:GetBucketPolicy"
        ],
        "Resource": "arn:aws:s3::bucket-name"
    },
    {
        "Sid": "AllowLogDeliveryForWorkMail",
        "Effect": "Allow",
        "Action": [
            "workmail:AllowVendedLogDeliveryForResource"
        ],
        "Resource": [
            "arn:aws:workmail:us-east-1:111122223333:organization/organization-id"
        ]
    }
]
}

```

Bucket S3 tempat log dikirim harus memiliki kebijakan sumber daya yang mencakup izin tertentu. Jika bucket saat ini tidak memiliki kebijakan sumber daya dan pengguna yang menyiapkan logging memiliki izin `S3:GetBucketPolicy` dan `S3:PutBucketPolicy` izin untuk bucket, maka AWS secara otomatis membuat kebijakan berikut untuk itu saat Anda mulai mengirim log ke Amazon S3.

JSON

```

{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            }
        }
    ]
}

```

```

    },
    "Action": "s3:GetBucketAcl",
    "Resource": "arn:aws:s3:::my-bucket",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": [
          "123456789012"
        ]
      },
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:logs:us-east-1:111122223333:delivery-source:*"
        ]
      }
    }
  },
  {
    "Sid": "AWSLogDeliveryWrite",
    "Effect": "Allow",
    "Principal": {
      "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::my-bucket/AWSLogs/111122223333/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceAccount": [
          "123456789012"
        ]
      },
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:logs:us-east-1:111122223333:delivery-source:*"
        ]
      }
    }
  }
]
}

```

Dalam kebijakan sebelumnya, untuk `aws:SourceAccount`, tentukan daftar ID akun tempat log dikirimkan ke bucket ini. Untuk `aws:SourceArn`, tentukan daftar ARN dari sumber daya yang menghasilkan log, dalam formulir `arn:aws:logs:source-region:source-account-id:*`.

Jika bucket memiliki kebijakan sumber daya, tetapi kebijakan tersebut tidak berisi pernyataan yang ditampilkan di kebijakan sebelumnya, dan pengguna yang menyiapkan logging memiliki `S3:PutBucketPolicy` izin `S3:GetBucketPolicy` dan untuk bucket, pernyataan tersebut akan ditambahkan ke kebijakan sumber daya bucket.

Note

Dalam beberapa kasus, Anda mungkin melihat `AccessDenied` kesalahan AWS CloudTrail jika `s3:ListBucket` izin belum diberikandelivery.logs.amazonaws.com. Untuk menghindari kesalahan ini di CloudTrail log Anda, Anda harus memberikan `s3:ListBucket` izin untukdelivery.logs.amazonaws.com. Anda juga harus menyertakan `Condition` parameter yang ditampilkan dengan `s3:GetBucketAcl` izin yang ditetapkan dalam kebijakan bucket sebelumnya. Untuk merampingkan ini, alih-alih membuat yang baruStatement, Anda dapat langsung memperbarui `AWSLogDeliveryAclCheck` menjadi `"Action": ["s3:GetBucketAcl", "s3:ListBucket"]`.

Enkripsi sisi server bucket Amazon S3

Anda dapat melindungi data di bucket Amazon S3 dengan mengaktifkan enkripsi sisi server dengan S3-managed Amazon keys SSE-S3 () atau enkripsi sisi server dengan kunci yang disimpan di (). AWS KMS AWS Key Management Service SSE-KMS Untuk informasi selengkapnya, silakan lihat [Melindungi data menggunakan enkripsi sisi server](#).

Jika Anda memilih SSE-S3, tidak diperlukan konfigurasi tambahan. Amazon S3 menangani kunci enkripsi.

Warning

Jika Anda memilih SSE-KMS, Anda harus menggunakan kunci yang dikelola pelanggan, karena menggunakan Kunci yang dikelola AWS tidak didukung untuk skenario ini. Jika Anda mengatur enkripsi menggunakan kunci AWS terkelola, log akan dikirimkan dalam format yang tidak dapat dibaca.

Saat menggunakan AWS KMS kunci terkelola pelanggan, Anda dapat menentukan Nama Sumber Daya Amazon (ARN) kunci terkelola pelanggan saat mengaktifkan enkripsi bucket. Tambahkan hal berikut ke kebijakan kunci untuk kunci terkelola pelanggan Anda (bukan ke kebijakan bucket untuk bucket S3 Anda), sehingga akun pengiriman log dapat menulis ke bucket S3 Anda.

Jika Anda memilih SSE-KMS, Anda harus menggunakan kunci yang dikelola pelanggan, karena menggunakan kunci AWS terkelola tidak didukung untuk skenario ini. Saat menggunakan AWS KMS kunci terkelola pelanggan, Anda dapat menentukan Nama Sumber Daya Amazon (ARN) kunci terkelola pelanggan saat mengaktifkan enkripsi bucket. Tambahkan hal berikut ke kebijakan kunci untuk kunci terkelola pelanggan Anda (bukan ke kebijakan bucket untuk bucket S3 Anda), sehingga akun pengiriman log dapat menulis ke bucket S3 Anda.

```
{
  "Sid":"Allow Logs Delivery to use the key",
  "Effect":"Allow",
  "Principal":{
    "Service":[
      "delivery.logs.amazonaws.com"
    ]
  },
  "Action":[
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource":"*",
  "Condition":{
    "StringEquals":{
      "aws:SourceAccount":[
        "account-id"
      ]
    },
    "ArnLike":{
      "aws:SourceArn":[
        "arn:aws:logs:region:account-id:delivery-source:*"
      ]
    }
  }
}
```

Untuk `aws:SourceAccount`, tentukan daftar ID akun tempat log dikirimkan ke bucket ini.

Untuk `aws:SourceArn`, tentukan daftar ARN dari sumber daya yang menghasilkan log, dalam formulir `arn:aws:logs:source-region:source-account-id:*`.

Log dikirim ke Firehose

Izin pengguna

Untuk mengaktifkan pengiriman log ke Firehose, Anda harus masuk dengan izin berikut.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadWriteAccessForLogDeliveryActions",
      "Effect": "Allow",
      "Action": [
        "logs:GetDelivery",
        "logs:GetDeliverySource",
        "logs:PutDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs>DeleteDeliverySource",
        "logs:PutDeliveryDestinationPolicy",
        "logs>CreateDelivery",
        "logs:GetDeliveryDestination",
        "logs:PutDeliverySource",
        "logs>DeleteDeliveryDestination",
        "logs>DeleteDeliveryDestinationPolicy",
        "logs>DeleteDelivery"
      ],
      "Resource": [
        "arn:aws:logs:us-east-1:111122223333:delivery:*",
        "arn:aws:logs:us-east-1:111122223333:delivery-source:*",
        "arn:aws:logs:us-east-1:111122223333:delivery-destination:*"
      ]
    },
    {
      "Sid": "ListAccessForLogDeliveryActions",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeDeliveryDestinations",
```

```

        "logs:DescribeDeliverySources",
        "logs:DescribeDeliveries",
        "logs:DescribeLogGroups"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowUpdatesToResourcePolicyFH",
    "Effect": "Allow",
    "Action": [
        "firehose:TagDeliveryStream"
    ],
    "Resource": [
        "arn:aws:firehose:us-east-1:111122223333:deliverystream/*"
    ]
},
{
    "Sid": "CreateServiceLinkedRole",
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam:111122223333:role/aws-service-role/
delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery"
},
{
    "Sid": "AllowLogDeliveryForWorkMail",
    "Effect": "Allow",
    "Action": [
        "workmail:AllowVendedLogDeliveryForResource"
    ],
    "Resource": [
        "arn:aws:workmail:us-
east-1:111122223333:organization/organization-id"
    ]
}
]
}

```

Peran IAM yang digunakan untuk izin sumber daya

Karena Firehose tidak menggunakan kebijakan sumber daya, AWS menggunakan peran IAM saat menyiapkan log ini untuk dikirim ke Firehose. AWS membuat peran terkait layanan bernama `AWSServiceRoleForLogDelivery`. Peran terkait layanan ini mencakup izin berikut.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource": "arn:aws:firehose:us-east-1:111122223333:deliverystream/workmail-*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/LogDeliveryEnabled": "true"
        }
      },
      "Effect": "Allow"
    }
  ]
}
```

Peran terkait layanan ini memberikan izin untuk semua aliran pengiriman Firehose yang memiliki tag yang disetel ke `LogDeliveryEnabled true`. AWS memberikan tag ini ke aliran pengiriman tujuan saat Anda mengatur logging.

Peran terkait layanan ini juga memiliki kebijakan kepercayaan yang memungkinkan layanan `delivery.logs.amazonaws.com` utama untuk mengasumsikan peran yang terhubung dengan layanan yang diperlukan. Kebijakan kepercayaan tersebut adalah sebagai berikut:

JSON

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

```

"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "delivery.logs.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
]
}

```

Console-specific izin

Selain izin yang tercantum di bagian sebelumnya, jika Anda menyiapkan pengiriman log menggunakan konsol alih-alih API, Anda juga memerlukan izin berikut:

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLogDeliveryActions",
      "Effect": "Allow",
      "Action": [
        "firehose:DescribeDeliveryStream",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:logs:us-east-1:111122223333:log-group:*",
        "arn:aws:firehose:us-east-1:111122223333:deliverystream/*",
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "ListAccessForDeliveryDestinations",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogGroups",
        "firehose:ListDeliveryStreams",

```

```
    "s3:ListAllMyBuckets"  
  ],  
  "Resource": "*" ]  
}  
]
```

Validasi kepatuhan untuk Amazon WorkMail

Third-party Auditor menilai keamanan dan kepatuhan Amazon WorkMail sebagai bagian dari beberapa program AWS kepatuhan. Ini mencakup SOC, ISO, dan C5.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat [AWS Services in Scope by Compliance Program](#). Untuk informasi umum, lihat [Program Kepatuhan AWS](#).

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#).

Tanggung jawab kepatuhan Anda saat menggunakan Amazon WorkMail ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta undang-undang dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- [Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan](#) penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS
- [AWS Sumber Daya Kepatuhan](#) — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [AWS Config](#) AWS Layanan ini menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub CSPM](#)— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di Amazon WorkMail

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung

dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat [Infrastruktur AWS Global](#).

Selain infrastruktur AWS global, Amazon WorkMail menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Keamanan infrastruktur di Amazon WorkMail

Note

Amazon WorkMail menghentikan dukungan untuk Transport Layer Security (TLS) 1.0 dan 1.1. Jika Anda menggunakan TLS 1.0 atau 1.1, Anda harus memutakhirkan versi TLS ke 1.2. Untuk informasi selengkapnya, lihat [TLS 1.2 untuk menjadi level protokol TLS minimum untuk semua titik akhir AWS API](#).

Sebagai layanan terkelola, Amazon WorkMail dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan Infrastruktur dalam Kerangka Kerja](#) yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Amazon WorkMail melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Cipher suite dengan perfect forward secrecy (PFS) seperti DHE (Ephemeral) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Memulai dengan Amazon WorkMail

Setelah Anda menyelesaikan [Prasyarat](#), Anda siap untuk memulai dengan Amazon WorkMail. Untuk informasi selengkapnya, lihat [Memulai dengan Amazon WorkMail](#).

Anda dapat mempelajari lebih lanjut tentang memigrasi kotak pesan yang ada ke Amazon WorkMail, interoperabilitas dengan Microsoft Exchange, dan kuota WorkMail Amazon di bagian berikut.

Topik

- [Memulai dengan Amazon WorkMail](#)
- [Migrasi ke Amazon WorkMail](#)
- [Interoperabilitas antara Amazon dan WorkMail Microsoft Exchange](#)
- [Konfigurasi setelah ketersediaan di Amazon WorkMail](#)
- [Konfigurasi pengaturan ketersediaan di Microsoft Exchange](#)
- [Aktifkan perutean email antara pengguna Microsoft Exchange dan Amazon WorkMail](#)
- [Aktifkan perutean email untuk pengguna](#)
- [Konfigurasi pengaturan pos](#)
- [Konfigurasi klien email](#)
- [Menonaktifkan mode interoperabilitas dan menonaktifkan server email Anda](#)
- [Pemecahan masalah](#)
- [WorkMail Kuota Amazon](#)

Memulai dengan Amazon WorkMail

Baik Anda WorkMail pengguna Amazon baru atau pengguna Amazon yang sudah ada WorkSpaces, mulailah dengan Amazon WorkMail dengan menyelesaikan langkah-langkah berikut.

Note

Menyelesaikan [Prasyarat](#) sebelum memulai.

Topik

- [Langkah 1: Masuk ke WorkMail konsol Amazon](#)

- [Langkah 2: Siapkan WorkMail situs Amazon Anda](#)
- [Langkah 3: Siapkan akses WorkMail pengguna Amazon](#)
- [Sumber daya lainnya](#)

Langkah 1: Masuk ke WorkMail konsol Amazon

Anda harus masuk ke WorkMail konsol Amazon sebelum dapat menambahkan pengguna dan mengelola akun dan kotak pesan mereka.

Untuk masuk ke WorkMail konsol Amazon

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.
2. Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya tentang wilayah, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

Langkah 2: Siapkan WorkMail situs Amazon Anda

1. Setelah masuk ke WorkMail konsol Amazon, Anda menyiapkan organisasi dan menambahkan domain. Sebaiknya gunakan domain khusus untuk WorkMail organisasi Amazon Anda. Untuk informasi selengkapnya, lihat [Membuat organisasi](#) dan [Menambahkan domain](#).
2. (Opsional) Anda dapat memilih untuk menggunakan domain pengujian gratis yang disediakan oleh Amazon WorkMail. Jika Anda memilih untuk melakukan ini, lompat ke langkah 4.

Note

Domain uji menggunakan format ini: *alias*.awsapps.com. Saat Anda pergi, ingatlah bahwa Anda hanya boleh menggunakan domain pengujian untuk pengujian. Jangan gunakan domain pengujian untuk lingkungan produksi. Selain itu, Anda harus memiliki setidaknya satu pengguna yang diaktifkan di WorkMail organisasi Amazon Anda. Jika Anda tidak memiliki pengguna yang diaktifkan, domain dapat menjadi tersedia untuk pendaftaran dan digunakan oleh pelanggan lain.

3. Jika Anda menggunakan domain eksternal, verifikasi domain tersebut dengan menambahkan catatan teks (TXT) dan pertukaran surat (MX) yang sesuai ke layanan Sistem Nama Domain (DNS) Anda. Catatan TXT memungkinkan Anda memasukkan catatan di DNS. Catatan MX

menentukan server email masuk. Pastikan untuk menetapkan domain sebagai default untuk organisasi Anda. Untuk informasi selengkapnya, lihat [Memverifikasi domain](#) dan [Memilih domain default](#).

4. Buat pengguna baru atau aktifkan pengguna direktori Anda yang ada untuk Amazon WorkMail. Untuk informasi selengkapnya, lihat [Menambahkan pengguna](#).
5. (Opsional) Jika Anda memiliki kotak pesan Microsoft Exchange yang sudah ada, migrasi ke Amazon WorkMail. Untuk informasi selengkapnya, lihat [Migrasi ke Amazon WorkMail](#).

Setelah selesai menyiapkan WorkMail situs Amazon, Anda dapat mengakses Amazon WorkMail menggunakan URL aplikasi web.

Untuk menemukan URL aplikasi WorkMail web Amazon Anda

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Untuk melakukannya, buka daftar Pilih wilayah, yang terletak di sebelah kanan kotak pencarian, lalu pilih Wilayah yang diinginkan. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di. Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.

Halaman pengaturan Organisasi muncul dan menampilkan URL di bawah Login pengguna. URL mengambil formulir ini: <https://alias.awsapps.com/mail>.

Langkah 3: Siapkan akses WorkMail pengguna Amazon

Pilih dari opsi berikut untuk mengatur akses WorkMail pengguna Amazon:

- Mengatur akses pengguna dari klien desktop yang ada menggunakan klien Microsoft Outlook. Untuk informasi selengkapnya, lihat [Connect Microsoft Outlook ke WorkMail akun Amazon Anda](#).
- Atur akses pengguna dari perangkat seluler, seperti Kindle, Android, iPad, atau iPhone. Untuk informasi selengkapnya, lihat Memulai [Memulai dengan perangkat seluler](#).
- Untuk mengatur akses pengguna, gunakan perangkat lunak klien apa pun yang kompatibel dengan protokol Internet Mail Access Protocol (IMAP). Untuk informasi selengkapnya, lihat [Connect klien IMAP ke WorkMail akun Amazon Anda](#).

Sumber daya lainnya

- [Migrasi ke Amazon WorkMail](#)
- [Interoperabilitas antara Amazon dan WorkMail Microsoft Exchange](#)
- [WorkMail Kuota Amazon](#)

Migrasi ke Amazon WorkMail

Anda dapat bermigrasi ke Amazon WorkMail dari Microsoft Exchange, Microsoft Office 365, G Suite Basic (sebelumnya Google Apps for Work), dan platform lainnya dengan bekerja sama dengan salah satu mitra kami. Untuk informasi selengkapnya tentang mitra kami, lihat [WorkMail Fitur Amazon](#).

Topik

- [Langkah 1: Buat atau aktifkan pengguna di Amazon WorkMail](#)
- [Langkah 2: Migrasi ke Amazon WorkMail](#)
- [Langkah 3: Selesaikan migrasi ke Amazon WorkMail](#)

Langkah 1: Buat atau aktifkan pengguna di Amazon WorkMail

Sebelum memigrasi pengguna, Anda harus menambahkan pengguna tersebut di Amazon WorkMail untuk menyediakan kotak pesan mereka. Untuk informasi selengkapnya, lihat [Menambahkan pengguna](#).

Langkah 2: Migrasi ke Amazon WorkMail

Anda dapat bekerja dengan mitra AWS migrasi mana pun untuk bermigrasi ke Amazon WorkMail. Untuk informasi tentang penyedia ini, lihat [WorkMailfitur Amazon](#).

Untuk memigrasi kotak pesan, buat WorkMail pengguna Amazon khusus untuk bertindak sebagai administrator migrasi. Prosedur berikut memberikan izin kepada pengguna tersebut untuk mengakses semua kotak pesan di organisasi Anda.

Untuk membuat administrator migrasi

1. Lakukan salah satu tindakan berikut:

- Di WorkMail konsol Amazon, buat pengguna baru untuk bertindak sebagai administrator migrasi. Untuk informasi selengkapnya, lihat [Menambahkan pengguna](#).
 - Di Active Directory, buat pengguna baru untuk bertindak sebagai administrator migrasi, lalu aktifkan pengguna untuk Amazon WorkMail. Untuk informasi selengkapnya, lihat [Mengaktifkan pengguna](#).
2. Di panel navigasi WorkMail konsol Amazon, pilih Organizations, lalu pilih nama organisasi Anda.
 3. Pilih Pengaturan organisasi, pilih Migrasi, lalu Edit.
 4. Pindahkan penggeser berkemampuan Migrasi ke posisi aktif.
 5. Buka administrator Migrasi dan pilih pengguna.
 6. Pilih Simpan.

Langkah 3: Selesaikan migrasi ke Amazon WorkMail

Setelah memigrasikan akun email ke Amazon WorkMail, Anda dapat memverifikasi catatan DNS dan mengonfigurasi klien desktop dan seluler Anda.

Untuk menyelesaikan migrasi ke Amazon WorkMail

1. Verifikasi bahwa semua catatan DNS diperbarui dan mengarah ke Amazon WorkMail. Untuk informasi lebih lanjut tentang catatan DNS yang diperlukan, lihat [Menambahkan domain](#).

Note

Proses pembaruan catatan DNS dapat memakan waktu beberapa jam. Jika item baru muncul di kotak pesan sumber saat catatan MX diubah, jalankan lagi alat migrasi untuk memigrasi item baru setelah catatan DNS diperbarui.

2. Untuk informasi selengkapnya tentang mengonfigurasi klien desktop atau seluler agar menggunakan Amazon WorkMail, lihat [Connect Microsoft Outlook ke WorkMail akun Amazon Anda](#) di Panduan WorkMail Pengguna Amazon.

Interoperabilitas antara Amazon dan WorkMail Microsoft Exchange

Interoperabilitas antara Amazon dan WorkMail Microsoft Exchange Server memungkinkan Anda meminimalkan gangguan pada pengguna saat memigrasi kotak pesan ke Amazon, WorkMail atau menggunakan Amazon WorkMail untuk subset kotak pesan perusahaan Anda.

Interoperabilitas ini memungkinkan Anda untuk menggunakan domain perusahaan yang sama untuk kotak pesan di kedua lingkungan. Dengan cara ini, pengguna Anda dapat menjadwalkan rapat dengan berbagi dua arah informasi free/busy status kalender.

Prasyarat

Sebelum Anda mengaktifkan interoperabilitas dengan Microsoft Exchange, lakukan hal berikut:

- Pastikan Anda memiliki setidaknya satu pengguna yang diaktifkan untuk Amazon WorkMail. Ini diperlukan untuk mengonfigurasi pengaturan ketersediaan untuk Microsoft Exchange. Untuk mengaktifkan pengguna, ikuti langkah-langkah di [Aktifkan perutean email untuk pengguna](#).
- Mengatur Direktori Aktif (AD) Connector. Menyiapkan AD Connector dengan direktori lokal memungkinkan pengguna untuk terus menggunakan kredensial perusahaan yang ada. Untuk informasi selengkapnya, lihat [Membuat Konektor AD](#) dan [Mengintegrasikan Amazon WorkMail dengan direktori lokal](#).
- Siapkan WorkMail organisasi Amazon Anda. Buat WorkMail organisasi Amazon yang menggunakan AD Connector yang Anda atur.
- Tambahkan domain perusahaan Anda ke WorkMail organisasi Amazon Anda, lalu verifikasi di WorkMail konsol Amazon. Jika tidak, email yang dikirim ke alias ini akan terpenjal. Untuk informasi lebih lanjut, lihat [Bekerja dengan domain](#).
- Memigrasi kotak pesan ke WorkMail. Enable pengguna Amazon untuk menyediakan dan memigrasi kotak pesan dari lingkungan lokal ke Amazon. WorkMail Untuk informasi selengkapnya, lihat [Mengaktifkan pengguna yang ada](#) dan lihat [Memigrasi ke Amazon WorkMail](#).

Note

Jangan perbarui catatan DNS untuk menunjuk ke Amazon WorkMail. Hal ini memastikan bahwa Microsoft Exchange tetap menjadi server primer untuk email masuk selama Anda menginginkan interoperabilitas antara kedua lingkungan tersebut.

- Pastikan bahwa User Principal Names (UPNs) di Direktori Aktif sesuai dengan alamat SMTP primer pengguna.

Amazon WorkMail membuat permintaan HTTPS ke URL Exchange Web Services (EWS) di Microsoft Exchange untuk mendapatkan free/busy informasi kalender.

Untuk penyedia EWS-based ketersediaan, Amazon WorkMail membuat permintaan HTTPS ke URL Exchange Web Services (EWS) di Microsoft Exchange untuk mendapatkan free/busy informasi kalender. Oleh karena itu, prasyarat berikut hanya berlaku untuk penyedia ketersediaan. EWS-based

- Pastikan bahwa pengaturan firewall yang relevan diatur untuk mengizinkan akses dari internet. Port default untuk permintaan HTTPS adalah port 443.
- Amazon hanya WorkMail dapat membuat permintaan HTTPS yang berhasil ke URL EWS di Microsoft Exchange jika sertifikat yang ditandatangani oleh otoritas sertifikat (CA) yang valid tersedia di lingkungan Microsoft Exchange Anda. Untuk informasi selengkapnya, lihat [Buat permintaan sertifikat Exchange Server untuk otoritas sertifikasi \(CA\)](#) di situs web Dokumentasi Microsoft Exchange.
- Anda harus mengaktifkan Autentikasi Basic untuk EWS di Microsoft Exchange. Untuk informasi lebih lanjut, lihat [Direktori virtual: Exchange 2013](#) pada Blog Program Penghargaan Microsoft MVP.

Menambahkan domain dan mengaktifkan kotak pesan

Tambahkan domain perusahaan Anda ke Amazon WorkMail sehingga dapat digunakan di alamat email. Pastikan domain yang ditambahkan ke Amazon WorkMail diverifikasi, lalu aktifkan pengguna dan grup untuk menyediakan kotak pesan di Amazon. WorkMail Sumber daya tidak dapat diaktifkan di Amazon WorkMail saat dalam mode interoperabilitas, dan harus dibuat ulang di Amazon WorkMail setelah Anda menonaktifkan mode interoperabilitas. Namun, Anda masih dapat menggunakannya untuk menjadwalkan pertemuan saat dalam mode interoperabilitas. Sumber daya dari Microsoft Exchange selalu ditampilkan di tab Pengguna di Amazon WorkMail.

- Untuk informasi lebih lanjut, lihat [Tambahkan domain](#), [Aktifkan pengguna yang ada](#), dan [Aktifkan grup yang ada](#).

Note

Untuk memastikan interoperabilitas dengan Microsoft Exchange, jangan perbarui catatan DNS untuk menunjuk ke catatan Amazon. WorkMail Microsoft Exchange tetap menjadi

server primer untuk email masuk selama Anda menginginkan interoperabilitas antara kedua lingkungan tersebut.

Aktifkan interoperabilitas

Jika Anda belum membuat WorkMail organisasi Amazon, Anda dapat menggunakan API publik untuk membuat WorkMail Organisasi baru dengan mode interoperabilitas diaktifkan.

Jika Anda sudah memiliki WorkMail organisasi Amazon dengan Konektor AD yang ditautkan ke Active Directory, dan Anda juga memiliki Microsoft Exchange, hubungi [AWS Support](#) untuk mendapatkan bantuan dengan mengaktifkan interoperabilitas Microsoft Exchange untuk organisasi Amazon yang ada. WorkMail

Buat akun layanan di Microsoft Exchange dan Amazon WorkMail

Note

Membuat akun layanan di Exchange tidak diperlukan saat Exchange tidak digunakan sebagai back-end untuk penyedia ketersediaan kustom.

Untuk mengakses free/busy informasi kalender, buat akun layanan di Microsoft Exchange dan Amazon WorkMail. Akun layanan Microsoft Exchange adalah setiap pengguna di Microsoft Exchange yang memiliki akses ke free/busy informasi kalender pengguna Exchange lainnya. Akses diberikan secara default; sehingga tidak ada izin khusus yang diperlukan.

Demikian pula, akun WorkMail layanan Amazon adalah setiap pengguna di Amazon WorkMail yang memiliki akses ke free/busy informasi kalender WorkMail pengguna Amazon lainnya. Ini juga diberikan secara default. Anda harus membuat WorkMail pengguna Amazon di direktori lokal, lalu mengaktifkan pengguna tersebut untuk Amazon WorkMail, untuk mengintegrasikan Amazon WorkMail dengan AD Connector ke direktori Anda.

Keterbatasan dalam mode interoperabilitas

Saat organisasi Anda dalam mode interoperabilitas, Anda harus menggunakan pusat admin Exchange untuk mengelola semua pengguna, grup, dan sumber daya. Untuk mengaktifkan WorkMail pengguna dan grup Amazon, gunakan file Konsol Manajemen AWS. Untuk informasi lebih lanjut, lihat [Aktifkan pengguna yang ada](#) dan [Aktifkan grup yang ada](#).

Saat mengaktifkan pengguna atau grup untuk Amazon WorkMail, Anda tidak dapat mengedit alamat email atau alias pengguna dan grup tersebut. Dan juga harus dikonfigurasi melalui admincenter Exchange. Amazon WorkMail menyinkronkan perubahan di direktori Anda setiap empat jam.

Sumber daya tidak dapat dibuat atau diaktifkan di Amazon WorkMail saat dalam mode interoperabilitas. Namun, semua sumber daya Exchange Anda tersedia di buku WorkMail alamat Amazon dan dapat digunakan untuk menjadwalkan rapat seperti biasa.

Konfigurasi setelah ketersediaan di Amazon WorkMail

Konfigurasi pengaturan ketersediaan di Amazon WorkMail untuk mengaktifkan kueri sistem eksternal, menawarkan fungsionalitas kalender, dan untuk mendapatkan informasi kalender. free/busy Amazon WorkMail mendukung dua mode untuk memperoleh free/busy informasi dari sistem jarak jauh:

- Exchange Web Services (EWS) — Dalam konfigurasi ini, Amazon WorkMail akan meminta server Exchange atau WorkMail organisasi lain untuk informasi ketersediaan menggunakan protokol EWS. Ini adalah konfigurasi yang paling sederhana tetapi membutuhkan endpoint EWS server Exchange agar dapat diakses melalui internet publik.
- Penyedia Ketersediaan Khusus (CAP) — Dalam konfigurasi ini, administrator dapat mengonfigurasi fungsi AWS Lambda untuk mendapatkan informasi ketersediaan pengguna untuk domain email tertentu. Bergantung pada platform server email Anda, menggunakan CAP dengan Amazon WorkMail menawarkan manfaat berikut:
 - Dapatkan ketersediaan pengguna dari EWS internal tanpa perlu membuka firewall mereka. WorkMail
 - Dapatkan ketersediaan pengguna dari sistem non-Exchange atau non-EWS, seperti Google Workspace (sebelumnya dikenal sebagai G Suite).

Topik

- [Konfigurasi penyedia EWS-based ketersediaan](#)
- [Mengkonfigurasi Penyedia Ketersediaan Kustom](#)
- [Membangun fungsi Lambda Penyedia Ketersediaan Kustom](#)

Konfigurasi penyedia EWS-based ketersediaan

Untuk mengonfigurasi pengaturan EWS-based ketersediaan di konsol, selesaikan prosedur berikut:

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Untuk melakukannya, buka daftar Pilih wilayah, yang terletak di sebelah kanan kotak pencarian, lalu pilih Wilayah yang diinginkan. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi.
3. Di panel navigasi, pilih Pengaturan organisasi, lalu pilih tab Interoperabilitas.
4. Pilih Tambahkan konfigurasi ketersediaan, lalu masukkan informasi berikut:
 - Jenis - Pilih EWS.
 - Domain — Domain yang WorkMail akan mencoba menanyakan informasi ketersediaan menggunakan konfigurasi ini.
 - URL EWS - Amazon WorkMail akan menanyakan URL ini ke titik akhir EWS. Lihat bagian [Mendapatkan URL EWS](#) dari panduan ini.
 - Alamat email pengguna — Alamat email pengguna yang WorkMail akan digunakan untuk mengautentikasi ke titik akhir EWS.
 - Kata sandi — Kata sandi yang WorkMail akan digunakan untuk mengautentikasi ke titik akhir EWS.
5. Pilih Simpan.

Mendapatkan URL EWS

Untuk mendapatkan URL EWS untuk Exchange menggunakan Microsoft Outlook, selesaikan prosedur berikut:

1. Masuk ke Microsoft Outlook pada Windows untuk setiap pengguna di lingkungan Exchange Anda.
2. Tekan dan tahan tombol Ctrl dan buka menu konteks (klik kanan) di ikon Microsoft Outlook di bilah tugas.
3. Pilih Uji E-mail AutoConfiguration.
4. Masukkan alamat email dan kata sandi pengguna Microsoft Exchange, lalu pilih Uji.
5. Dari jendela Hasil, salin nilai untuk URL Layanan Ketersediaan.

Untuk mendapatkan URL EWS untuk pertukaran menggunakan PowerShell, pada PowerShell prompt, jalankan perintah berikut:

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

Untuk mendapatkan URL EWS untuk Amazon WorkMail, pertama-tama, temukan domain EWS di bawah [WorkMail titik akhir dan kuota Amazon](#). Masukkan URL EWS — `https://"EWS domain"/EWS/Exchange.asmx` dan ganti “domain EWS” dengan domain EWS Anda.

Mengkonfigurasi Penyedia Ketersediaan Kustom

Untuk mengonfigurasi Penyedia Ketersediaan Kustom (CAP), selesaikan prosedur berikut:

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Untuk melakukannya, buka daftar Pilih Wilayah, yang terletak di sebelah kanan kotak pencarian, lalu pilih Wilayah yang diinginkan.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi.
3. Di panel navigasi, pilih Pengaturan organisasi dan kemudian pilih Interoperabilitas.
4. Pilih Tambahkan konfigurasi ketersediaan, lalu masukkan informasi berikut:
 - Jenis — Pilih CAP Lambda.
 - Domain — Domain yang WorkMail akan mencoba menanyakan informasi ketersediaan menggunakan konfigurasi ini.
 - ARN — ARN dari fungsi Lambda yang akan memberikan informasi ketersediaan.

Untuk membangun fungsi CAP Lambda, lihat. [Membangun fungsi Lambda Penyedia Ketersediaan Kustom](#)

Membangun fungsi Lambda Penyedia Ketersediaan Kustom

Penyedia Ketersediaan Kustom (CAP) dikonfigurasi dengan protokol JSON-based permintaan dan respons yang ditulis dalam skema JSON yang terdefinisi dengan baik. Fungsi Lambda akan mengurai permintaan dan memberikan respons yang valid.

Topik

- [Elemen permintaan dan respons](#)
- [Memberi Akses](#)
- [Contoh Amazon WorkMail menggunakan fungsi CAP Lambda](#)

Elemen permintaan dan respons

Elemen permintaan

Berikut ini adalah contoh permintaan yang digunakan untuk mengonfigurasi CAP untuk WorkMail pengguna Amazon:

```
{
  "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"
  }
}
```

Permintaan terdiri dari tiga bagian: pemohon, kotak surat, dan jendela. Ini dijelaskan dalam berikut [Pemohon](#), [Kotak surat](#), dan [Jendela](#) bagian dari panduan ini.

Pemohon

Bagian pemohon memberikan informasi tentang pengguna yang membuat permintaan asli ke Amazon WorkMail. CAP menggunakan informasi ini untuk mengubah perilaku penyedia. Misalnya, data ini dapat digunakan untuk meniru pengguna yang sama di penyedia ketersediaan backend atau detail tertentu dapat dihilangkan dari respons.

Bidang	Deskripsi	Diperlukan
Email	Alamat email utama pemohon.	Ya
Username	Nama pengguna pemohon.	Ya
Organization	ID organisasi pemohon.	Ya

Bidang	Deskripsi	Diperlukan
UserID	ID pemohon.	Ya
Origin	Alamat jarak jauh dari permintaan.	Tidak
Bearer	Terpesan untuk digunakan di masa mendatang.	Tidak

Kotak surat

Bagian kotak pesan berisi daftar alamat email pengguna yang dipisahkan koma yang meminta informasi ketersediaannya.

Jendela

Bagian jendela berisi jendela waktu yang diminta informasi ketersediaan. Keduanya `startDate` dan `endDate` ditentukan dalam UTC dan diformat sesuai dengan [RFC 3339](#). Acara tidak diharapkan terpotong. Dengan kata lain, jika suatu peristiwa dimulai sebelum yang ditentukan `startDate`, awal asli akan digunakan.

Elemen jawaban

Amazon WorkMail akan menunggu selama 25 detik untuk mendapatkan respons dari fungsi CAP Lambda. Setelah 25 detik, Amazon WorkMail akan menganggap fungsi tersebut gagal dan menghasilkan kegagalan untuk kotak pesan terkait dalam respons EWS `GetUserAvailability`. Ini tidak akan menyebabkan seluruh `GetUserAvailability` operasi gagal.

Berikut ini adalah contoh respons dari konfigurasi yang ditentukan di awal bagian ini:

```
{
  "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",
            "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"
        },
    },
    "workingPeriods":[
        {
            "startMinutes": 480,
            "endMinutes": 1040,
            "days": ["SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"]
        }
    ]
},
{
    "mailbox": "unknown@internal.example.com",
    "error": "MailboxNotFound"
}
}

```

Respons terdiri dari satu bagian kotak pesan yang terdiri dari daftar kotak pesan. Setiap kotak pesan yang ketersediaannya berhasil diperoleh terdiri dari tiga bagian: kotak surat, acara, dan jam kerja.

Jika penyedia ketersediaan gagal mendapatkan informasi ketersediaan untuk kotak pesan, bagian ini

terdiri dari dua bagian: kotak pesan dan kesalahan. Ini dijelaskan dalam bagian berikut [Kotak surat](#), [Peristiwa](#), [Jam Kerja](#), [Zona waktu](#), [Periode Kerja](#), dan [Kesalahan](#) bagian dari panduan ini.

Kotak surat

Bagian kotak pesan adalah alamat email pengguna yang ditemukan di bagian kotak pesan permintaan.

Peristiwa

Bagian peristiwa adalah daftar peristiwa yang terjadi di jendela yang diminta. Setiap peristiwa didefinisikan dengan parameter berikut:

Bidang	Deskripsi	Diperlukan
<code>startTime</code>	Waktu mulai acara di UTC dan diformat sesuai dengan RFC 3339 .	Ya
<code>endTime</code>	Waktu akhir acara di UTC dan diformat sesuai dengan RFC 3339 .	Ya
<code>busyType</code>	Jenis acara yang sibuk. Dapat berupa <code>Busy</code> , <code>Free</code> , atau <code>Tentative</code> .	Ya
<code>details</code>	Detail acara.	Tidak
<code>details.subject</code>	Subjek acara.	Ya
<code>details.location</code>	Lokasi acara.	Ya
<code>details.instanceType</code>	Jenis instance dari acara tersebut. Dapat berupa <code>Single_Instance</code> , <code>Recurring_Instance</code> , atau <code>Exception</code> .	Ya

Bidang	Deskripsi	Diperlukan
<code>details.isMeeting</code>	Sebuah Boolean untuk menunjukkan apakah acara memiliki peserta.	Ya
<code>details.isReminderSet</code>	Sebuah Boolean untuk menunjukkan jika acara memiliki set pengingat.	Ya
<code>details.isPrivate</code>	Sebuah Boolean untuk menunjukkan jika acara diatur ke pribadi.	Ya

Jam Kerja

Bagian `WorkingHours` berisi informasi tentang jam kerja pemilik kotak pesan. Ini berisi dua bagian: zona waktu dan `WorkingPeriod`.

Zona waktu

Subbagian zona waktu menjelaskan zona waktu pemilik kotak pesan. Penting untuk merender jam kerja pengguna dengan benar saat pemohon bekerja di zona waktu yang berbeda. Penyedia ketersediaan diharuskan untuk menjelaskan zona waktu secara eksplisit, daripada menggunakan nama. Menggunakan deskripsi zona waktu standar membantu menghindari ketidakcocokan zona waktu.

Bidang	Deskripsi	Diperlukan
<code>name</code>	Nama zona waktu.	Ya
<code>bias</code>	Offset default dari GMT dalam hitungan menit.	Ya
<code>standardTime</code>	Awal waktu standar untuk zona waktu yang ditentukan.	Tidak

Bidang	Deskripsi	Diperlukan
<code>daylightTime</code>	Awal waktu penghematan siang hari untuk zona waktu yang ditentukan.	Tidak

Anda harus mendefinisikan keduanya `standardTime` dan `daylightTime`, atau menghilangkan keduanya. Bidang dalam `standardTime` dan `daylightTime` objek adalah:

Bidang	Deskripsi	Nilai yang Diizinkan
<code>offset</code>	Offset relatif terhadap offset default dalam hitungan menit.	TA
<code>time</code>	Waktu di mana transisi antara waktu standar dan waktu musim panas terjadi, ditentukan sebagai <code>hh:mm:ss</code> .	TA
<code>month</code>	Bulan di mana transisi antara waktu standar dan waktu musim panas terjadi.	JAN, FEB, MAR, APR, JUN, JUL, AUG, SEP, OCT, NOV, DEC
<code>week</code>	Minggu dalam bulan yang ditentukan bahwa transisi antara waktu standar dan waktu musim panas terjadi.	FIRST, SECOND, THIRD, FOURTH, LAST
<code>dayOfWeek</code>	Hari dalam minggu yang ditentukan bahwa transisi antara waktu standar dan waktu musim panas terjadi.	SUN, MON, TUE, WED, THU, FRI, SAT

Periode Kerja

Bagian `WorkingPeriod` berisi satu atau lebih objek periode kerja. Setiap periode menentukan awal dan akhir hari kerja selama satu hari atau lebih.

Bidang	Deskripsi	Nilai yang Diizinkan
<code>startMinutes</code>	Awal hari kerja dalam hitungan menit dari tengah malam.	TA
<code>endMinutes</code>	Akhir hari kerja dalam hitungan menit dari tengah malam.	TA
<code>days</code>	Hari-hari di mana periode ini berlaku.	SUN, MON, TUE, WED, THU, FRI, SAT

Kesalahan

Bidang kesalahan dapat berisi pesan kesalahan arbitrer. Tabel berikut mencantumkan pemetaan kode terkenal untuk kode kesalahan EWS. Semua pesan lainnya akan dipetakan ke `ERROR_FREE_BUSY_GENERATION_FAILED`.

Nilai	Kode kesalahan EWS
<code>MailboxNotFound</code>	<code>ERROR_MAIL_RECIPIENT_NOT_FOUND</code>
<code>ErrorAvailabilityConfigNotFound</code>	<code>ERROR_AVAILABILITY_CONFIG_NOT_FOUND</code>
<code>ErrorServerBusy</code>	<code>ERROR_SERVER_BUSY</code>
<code>ErrorTimeoutExpired</code>	<code>ERROR_TIMEOUT_EXPIRED</code>
<code>ErrorFreeBusyGenerationFailed</code>	<code>ERROR_FREE_BUSY_GENERATION_FAILED</code>
<code>ErrorResponseSchemaValidation</code>	<code>ERROR_RESPONSE_SCHEMA_VALIDATION</code>

Memberi Akses

Jalankan perintah Lambda berikut dari AWS Command Line Interface (AWS CLI). Perintah ini menambahkan kebijakan sumber daya ke fungsi Lambda yang mem-parsing CAP. Fungsi ini memungkinkan layanan WorkMail ketersediaan Amazon untuk menjalankan fungsi Lambda Anda.

```
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 \  
  --source-arn arn:aws:workmail:WM_REGION:WM_ACCOUNT_ID:organization/ORGANIZATION_ID
```

Dalam perintah, tambahkan parameter berikut di mana ditunjukkan:

- *LAMBDA_REGION*— Nama wilayah tempat CAP Lambda dikerahkan. Misalnya, us-east-1.
- *CAP_FUNCTION_NAME*— Nama fungsi CAP Lambda.

Note

Ini bisa berupa nama, alias, atau ARN sebagian atau penuh dari fungsi CAP Lambda.

- *WM_REGION*— Nama wilayah tempat WorkMail organisasi Amazon memanggil fungsi Lambda.

Note

Hanya Wilayah berikut yang tersedia untuk digunakan dengan CAP:

- AS Timur (Virginia Utara)
 - US West (Oregon)
 - Eropa (Irlandia)
- *WM_ACCOUNT_ID*— ID akun Organisasi.
 - *ORGANIZATION_ID*— ID Organisasi yang memanggil CAP Lambda. Misalnya, ID Org: m-934ebb9eb57145d0a6cab566ca81a21f.

Note

LAMBDA_REGION dan *WM_REGION* akan berbeda hanya jika panggilan lintas wilayah diperlukan. Jika panggilan lintas wilayah tidak diperlukan, mereka akan sama.

Contoh Amazon WorkMail menggunakan fungsi CAP Lambda

Untuk contoh Amazon yang WorkMail menggunakan fungsi CAP Lambda untuk menanyakan titik akhir EWS, lihat [AWS contoh aplikasi ini di aplikasi](#) Tanpa Server untuk repositori Amazon. WorkMail GitHub

Konfigurasi pengaturan ketersediaan di Microsoft Exchange

Untuk mengalihkan semua permintaan free/busy informasi kalender untuk pengguna yang diaktifkan ke Amazon WorkMail, siapkan ruang alamat ketersediaan di Microsoft Exchange.

Gunakan PowerShell perintah berikut untuk membuat ruang alamat:

```
$credentials = Get-Credential
```

Pada prompt, masukkan kredensial akun WorkMail layanan Amazon. Nama pengguna harus dimasukkan sebagai **domain\username** (yaitu, **orgname.awsapps.com\workmail_service_account_username**). Di sini, **orgname** mewakili nama WorkMail organisasi Amazon. Untuk informasi selengkapnya, lihat [Buat akun layanan di Microsoft Exchange dan Amazon WorkMail](#).

```
Add-AvailabilityAddressSpace -ForestName orgname.awsapps.com -AccessMethod OrgWideFB -  
Credentials $credentials
```

Untuk informasi selengkapnya, lihat [Add-AvailabilityAddressSpace](#) di Microsoft Docs.

Aktifkan perutean email antara pengguna Microsoft Exchange dan Amazon WorkMail

Dengan perutean email antara Microsoft Exchange Server dan Amazon WorkMail, pengguna dapat menyimpan alamat email yang ada setelah mereka bermigrasi ke Amazon. WorkMail Perutean email

memungkinkan Anda menyimpan Microsoft Exchange Server sebagai server Simple Mail Transfer Protocol (SMTP) utama untuk email masuk untuk organisasi Anda.

Sebelum menggunakan perutean email, Anda harus menyelesaikan prasyarat berikut:

- Aktifkan mode interoperabilitas untuk organisasi Anda. Untuk informasi selengkapnya, lihat [Aktifkan interoperabilitas](#).
- Pastikan Anda melihat domain Anda di WorkMail konsol Amazon.
- Verifikasi bahwa Microsoft Exchange Server kami dapat mengirim email ke internet. Anda mungkin harus mengonfigurasi konektor Kirim. Untuk informasi selengkapnya tentang Kirim konektor, lihat [Membuat konektor Kirim di Exchange Server untuk mengirim email ke internet](#) dalam dokumentasi Microsoft.

Aktifkan perutean email untuk pengguna

Kami menyarankan Anda menyelesaikan langkah-langkah berikut terlebih dahulu untuk menguji pengguna sebelum menerapkan perubahan apa pun pada organisasi Anda.

1. Aktifkan akun pengguna yang Anda migrasi ke Amazon WorkMail. Untuk informasi lebih lanjut, lihat [Aktifkan pengguna yang ada](#).
2. Di WorkMail konsol Amazon, pastikan setidaknya ada dua alamat email yang terkait dengan pengguna yang diaktifkan.
 - `<workmailuser@ orgname .awsapps .com>` (ini ditambahkan secara otomatis dan dapat digunakan untuk pengujian tanpa Microsoft Exchange Anda.)
 - `<workmailuser@ yourdomain .com>` (ini ditambahkan secara otomatis dan merupakan alamat Microsoft Exchange utama.)

Untuk informasi lebih lanjut, lihat [Edit alamat email pengguna](#).

3. Pastikan Anda memigrasi semua data dari kotak pesan di Microsoft Exchange ke kotak pesan di Amazon. WorkMail Untuk informasi selengkapnya, lihat [Migrasi ke Amazon WorkMail](#).
4. Setelah semua data dimigrasi, nonaktifkan kotak pesan untuk pengguna di Microsoft Exchange. Kemudian, buat pengguna email (atau pengguna yang mendukung email) yang memiliki alamat SMTP eksternal yang mengarah ke Amazon. WorkMail Untuk melakukan ini, gunakan perintah berikut di Exchange Management Shell:

⚠ Important

Langkah-langkah berikut menghapus isi kotak pesan. Pastikan data Anda telah dimigrasikan ke Amazon WorkMail sebelum Anda mencoba mengaktifkan perutean email. Beberapa klien email tidak beralih ke Amazon dengan mulus WorkMail saat Anda menjalankan perintah ini. Untuk informasi selengkapnya, lihat [Konfigurasi klien email](#).

```
$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
```

```
Set-MailUser $new_mailuser -EmailAddresses $old_mailbox.EmailAddresses -  
HiddenFromAddressListsEnabled $old_mailbox.HiddenFromAddressListsEnabled
```

Dalam perintah di atas, *orgname* mewakili nama WorkMail organisasi Amazon Anda. Untuk selengkapnya, lihat [Menonaktifkan kotak pesan](#) dan [Mengaktifkan pengguna](#) e-mail di Microsoft TechNet

5. Kirim email pengujian ke pengguna (dalam contoh di atas, **workmailuser@yourdomain.com**). Jika perutean email telah diaktifkan dengan benar, pengguna harus dapat masuk ke WorkMail kotak surat Amazon mereka dan menerima email.

ℹ Note

Microsoft Exchange tetap menjadi server primer untuk email masuk selama Anda ingin memiliki interoperabilitas antara kedua lingkungan. Untuk memastikan interoperabilitas dengan Microsoft Exchange, catatan DNS tidak boleh diperbarui untuk mengarah ke Amazon WorkMail hingga nanti.

Konfigurasi pengaturan pos

Langkah-langkah di atas memindahkan kotak pesan pengguna dari Microsoft Exchange Server ke Amazon WorkMail, sambil menjaga pengguna di Microsoft Exchange sebagai kontak. Karena pengguna yang dimigrasi sekarang adalah pengguna email eksternal, Microsoft Exchange Server memberlakukan batasan tambahan. Mungkin juga ada persyaratan konfigurasi tambahan untuk menyelesaikan migrasi.

- Pengguna mungkin tidak dapat mengirim email ke grup secara default. Untuk mengaktifkan fungsi ini, Anda harus menambahkan pengguna ke daftar pengirim aman untuk semua grup. Untuk informasi selengkapnya, lihat [Manajemen pengiriman](#) di Microsoft TechNet.
- Pengguna mungkin tidak dapat memesan sumber daya. Untuk mengaktifkan fungsi ini, Anda harus mengatur semua sumber daya yang perlu diakses pengguna. `ProcessExternalMeetingMessages` Untuk informasi selengkapnya, lihat [Set-CalendarProcessing](#) di Microsoft TechNet.

Konfigurasi klien email

Beberapa klien email tidak beralih dengan mulus ke Amazon WorkMail. Klien ini mengharuskan pengguna untuk melakukan langkah-langkah pengaturan tambahan. Klien email yang berbeda memerlukan tindakan yang berbeda untuk diambil.

- Microsoft Outlook di Windows - Memerlukan Outlook untuk dimulai ulang. Saat penyalaan, Anda harus memilih apakah akan tetap menggunakan kotak surat lama atau menggunakan kotak surat sementara. Pilih opsi kotak surat sementara. Kemudian, konfigurasi ulang kotak surat Microsoft Exchange.
- Microsoft Outlook di macOS - Ketika Outlook dimulai ulang, itu akan meminta pesan berikut: Outlook dialihkan ke server `.awsapps.com`. **orgname** Apakah Anda ingin server ini mengonfigurasi pengaturan Anda? Terima saran.
- Mail di iOS — Aplikasi email berhenti menerima email dan menghasilkan kesalahan email tidak bisa mendapatkan. Membuat ulang dan mengkonfigurasi ulang kotak pesan Microsoft Exchange.

Menonaktifkan mode interoperabilitas dan menonaktifkan server email Anda

Setelah mengonfigurasi kotak pesan Microsoft Exchange untuk Amazon WorkMail, Anda dapat menonaktifkan mode interoperabilitas. Jika Anda belum memigrasikan pengguna atau catatan apa pun, menonaktifkan mode interoperabilitas tidak memengaruhi konfigurasi apa pun.

Warning

Sebelum menonaktifkan mode interoperabilitas, pastikan Anda menyelesaikan semua langkah yang diperlukan. Kegagalan untuk melakukannya dapat mengakibatkan email terpental atau perilaku yang tidak diinginkan. Jika Anda belum menyelesaikan migrasi, menonaktifkan interoperabilitas dapat menyebabkan gangguan pada organisasi Anda. Anda tidak dapat membatalkan operasi ini.

Untuk menonaktifkan dukungan mode interoperabilitas

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih organisasi yang ingin Anda nonaktifkan mode interoperabilitasnya.
3. Di bawah Pengaturan organisasi, pilih Nonaktifkan mode interoperabilitas.
4. Dalam kotak dialog Nonaktifkan mode interoperabilitas, masukkan nama organisasi dan pilih Nonaktifkan mode interoperabilitas.

Setelah menonaktifkan dukungan interoperabilitas, pengguna dan grup yang tidak diaktifkan untuk Amazon akan WorkMail dihapus dari buku alamat. Anda masih dapat mengaktifkan pengguna atau grup yang hilang menggunakan WorkMail konsol Amazon, dan mereka ditambahkan ke buku alamat. Sumber daya dari Microsoft Exchange tidak dapat diaktifkan dan tidak muncul di buku alamat sampai Anda menyelesaikan langkah di bawah ini.

- Buat sumber daya di Amazon WorkMail — Anda dapat membuat sumber daya di Amazon WorkMail dan kemudian mengonfigurasi delegasi dan opsi pemesanan untuk sumber daya ini. Untuk informasi selengkapnya, lihat [Bekerja dengan sumber daya](#).
- Buat catatan AutoDiscover DNS — Konfigurasi catatan AutoDiscover DNS untuk semua domain email di organisasi. Ini memungkinkan pengguna untuk terhubung ke WorkMail kotak surat Amazon mereka dari Microsoft Outlook dan klien seluler mereka. Untuk informasi selengkapnya, lihat [Menggunakan AutoDiscover untuk mengonfigurasi titik akhir](#).
- Alihkan data DNS MX Anda ke Amazon WorkMail — Untuk mengirimkan semua email masuk ke Amazon WorkMail, Anda harus mengalihkan data DNS MX Anda ke Amazon. WorkMail Perubahan pada catatan DNS dapat memakan waktu hingga 72 jam untuk menyebar ke semua server DNS.
- Nonaktifkan server email Anda — Setelah Anda memverifikasi bahwa semua email sedang dirutekan langsung ke Amazon WorkMail, Anda dapat menonaktifkan server email Anda jika Anda tidak bermaksud menggunakannya ke depan.

Pemecahan masalah

Solusi untuk WorkMail interoperabilitas Amazon dan kesalahan migrasi yang paling sering ditemui tercantum di bawah ini.

URL Exchange Web Services (EWS) tidak valid atau tidak terjangkau — Periksa apakah Anda memiliki URL EWS yang benar. Untuk informasi selengkapnya, lihat [Konfigurasi setelah ketersediaan di Amazon WorkMail](#).

Kegagalan koneksi selama validasi EWS — Ini adalah kesalahan umum dan dapat disebabkan oleh:

- Tidak ada koneksi internet di Microsoft Exchange.
- Firewall Anda tidak dikonfigurasi untuk mengizinkan akses dari internet. Pastikan bahwa port 443 (port default untuk permintaan HTTPS) terbuka.

Jika Anda telah mengkonfirmasi koneksi internet dan pengaturan firewall, namun kesalahan tetap ada, hubungi [AWS Support](#).

Nama pengguna dan kata sandi tidak valid saat mengonfigurasi interoperabilitas Microsoft Exchange — Ini adalah kesalahan umum dan dapat disebabkan oleh:

- Nama pengguna tidak dalam bentuk yang diharapkan. Gunakan pola berikut:

```
DOMAIN\username
```

- Server Microsoft Exchange Anda tidak dikonfigurasi untuk Autentikasi Basic untuk EWS. Untuk informasi lebih lanjut, lihat [Direktori virtual: Exchange 2013](#) pada Blog Program Penghargaan Microsoft MVP.

Pengguna menerima email dengan lampiran winmail.dat - Ini mungkin terjadi ketika S/MIME email terenkripsi dikirim dari Exchange ke Amazon WorkMail dan diterima di Outlook 2016 untuk Mac atau klien IMAP. Solusinya adalah dengan menjalankan perintah berikut di Exchange Management Shell.

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

Jika Anda telah mengonfirmasi poin di atas tetapi kesalahan tetap ada, hubungi [AWS Support](#).

WorkMail Kuota Amazon


Amazon WorkMail dapat digunakan oleh pelanggan perusahaan dan pemilik usaha kecil. Meskipun kami mendukung sebagian besar kasus penggunaan tanpa perlu mengkonfigurasi perubahan kuota, kami juga melindungi pengguna kami dan internet dari penyalahgunaan produk. Oleh karena itu, beberapa pelanggan mungkin mengalami kuota yang telah kami tetapkan. Bagian ini menjelaskan kuota ini dan cara mengubahnya.

Beberapa nilai kuota dapat diubah, dan beberapa adalah kuota keras yang tidak dapat diubah. Untuk informasi selengkapnya tentang meminta peningkatan kuota, lihat [Kuota AWS layanan](#) di Referensi Umum Amazon Web

WorkMail Organisasi Amazon dan kuota pengguna

Anda dapat menambahkan hingga 25 pengguna ke WorkMail organisasi Amazon Anda untuk uji coba gratis 30 hari. Setelah periode ini berakhir, Anda akan dikenakan biaya untuk semua pengguna aktif kecuali Anda menghapusnya atau menutup WorkMail akun Amazon Anda.

Semua pesan yang dikirim ke pengguna lain dipertimbangkan saat mengevaluasi kuota ini. Ini mencakup email, permintaan pertemuan, respons pertemuan, permintaan tugas, dan pesan yang diteruskan atau dialihkan secara otomatis sebagai hasil dari aturan.

 Note

Saat meminta peningkatan kuota untuk organisasi tertentu, Anda harus menyertakan nama organisasi dalam permintaan Anda.

Sumber daya	Kuota bawaan	Batas atas untuk permintaan perubahan
WorkMail Organisasi Amazon per AWS akun	100	Dapat ditingkatkan berdasarkan jenis direktori organisasi. Anda dapat melihat Directory Service kuota dan meminta kenaikan dari AWS Directory Service konsol . Untuk informasi selengkapnya, lihat Kuota layanan di. Referensi Umum AWS
Pengguna per WorkMail organisasi Amazon	1.000	Dapat ditingkatkan tergantung pada jenis direktori organisasi, sebagai berikut: <ul style="list-style-type: none"> • WorkMail Direktori Amazon: hingga 10 juta pengguna • Simple AD atau AD Connector, besar: hingga 5.000 pengguna* • Simple AD atau AD Connector, kecil: hingga 500 pengguna* • Microsoft AD, dihosting oleh Directory Service: hingga 10 juta pengguna tergantung pada pengaturan dan konfigurasi Anda,

Sumber daya	Kuota bawaan	Batas atas untuk permintaan perubahan
		*Jika Anda menggunakan Simple AD atau AD Connector, lihat AWS Directory Service untuk informasi tambahan.
Pengguna uji coba gratis	Hingga 25 pengguna dalam 30 hari pertama	Masa uji coba gratis hanya berlaku untuk 25 pengguna pertama di organisasi manapun. Setiap pengguna tambahan tidak termasuk dalam penawaran uji coba gratis.
Penerima yang dialamatkan per AWS akun per hari	100.000 penerima eksternal organisasi, tanpa kuota keras pada penerima internal organisasi	Tidak ada batas atas. Namun, Amazon WorkMail adalah layanan email bisnis dan tidak dimaksudkan untuk digunakan untuk layanan email massal. Untuk layanan email masal, lihat Amazon SES atau Amazon Pinpoint .
Penerima yang dialamatkan per AWS akun per hari menggunakan salah satu domain pengujian	200 penerima, terlepas dari tujuannya	Domain email uji tidak dimaksudkan untuk penggunaan jangka panjang. Kami menyarankan Anda menambahkan domain Anda sendiri dan menggunakannya sebagai domain default.

Kuota untuk grup ditetapkan oleh direktori yang mendasari.

WorkMail kuota pengaturan organisasi

Sumber daya	Kuota bawaan
Jumlah domain per organisasi Amazon WorkMail	1.000 Ini adalah kuota yang sulit dan tidak dapat diubah.
Jumlah pola pengirim dalam aturan aliran email per aturan	250 Ini adalah kuota yang sulit dan tidak dapat diubah.
Jumlah pola pengirim dalam aturan aliran email per organisasi	1.000 Ini adalah kuota yang sulit dan tidak dapat diubah.

Per-user kuota

Semua pesan yang dikirim ke pengguna lain dipertimbangkan saat mengevaluasi kuota ini. Ini mencakup email, permintaan pertemuan, respons pertemuan, permintaan tugas, dan pesan yang diteruskan atau dialihkan secara otomatis sebagai hasil dari aturan.

Sumber daya	Kuota bawaan	Kuota atas untuk permintaan perubahan
Ukuran maksimum kotak pesan	50 GB Ini adalah kuota yang sulit dan tidak dapat diubah.	Tidak berlaku
Jumlah maksimum alias per pengguna	100 Ini adalah kuota yang sulit dan tidak dapat diubah.	Tidak berlaku

Sumber daya	Kuota bawaan	Kuota atas untuk permintaan perubahan
Penerima yang dialamatkan per pengguna per hari yang menggunakan domain yang Anda miliki	10.000 penerima eksternal organisasi, tanpa kuota keras pada penerima internal organisasi.	Tidak ada batas atas. Namun, Amazon WorkMail adalah layanan email bisnis dan tidak dimaksudkan untuk digunakan untuk layanan email massal. Untuk layanan email masal, lihat Amazon SES atau Amazon Pinpoint .

Kuota pesan

Semua pesan yang dikirim ke pengguna lain dipertimbangkan saat mengevaluasi kuota ini. Ini mencakup email, permintaan pertemuan, respons pertemuan, permintaan tugas, dan pesan yang diteruskan atau dialihkan secara otomatis sebagai hasil dari aturan.

Sumber daya	Kuota bawaan
Ukuran maksimum pesan masuk	<p>29 MB data yang tidak dikodekan.</p> <p>Pesan diterima dalam format MIME. Ukuran maksimum pesan MIME yang masuk adalah 40 MB.</p> <p>Ini adalah kuota yang sulit dan tidak dapat diubah.</p>
Ukuran maksimum pesan keluar	<p>29 MB data yang tidak dikodekan.</p> <p>Pesan dikirim dalam format MIME. Ukuran maksimum pesan MIME keluar adalah 40 MB.</p> <p>Ini adalah kuota yang sulit dan tidak dapat diubah.</p>
Jumlah maksimum penerima per pesan	500

Sumber daya	Kuota bawaan
	Ini adalah kuota yang sulit dan tidak dapat diubah.
Jumlah maksimum lampiran per pesan	500 Ini adalah kuota yang sulit dan tidak dapat diubah.

Bekerja dengan organisasi

Di Amazon WorkMail, organisasi Anda mewakili pengguna di perusahaan Anda. Di WorkMail konsol Amazon, Anda melihat daftar organisasi yang tersedia. Jika Anda tidak memiliki yang tersedia, Anda harus membuat organisasi untuk menggunakan Amazon WorkMail.

Topik

- [Membuat organisasi](#)
- [Menghapus organisasi](#)
- [Menemukan alamat email](#)
- [Bekerja dengan pengaturan organisasi](#)
- [Penandaan sebuah organisasi](#)
- [Bekerja dengan aturan kontrol akses](#)
- [Mengatur kebijakan penyimpanan kotak pesan](#)

Membuat organisasi

Untuk menggunakan Amazon WorkMail, Anda harus terlebih dahulu membuat organisasi. Satu AWS akun dapat memiliki beberapa WorkMail organisasi Amazon. Saat Anda membuat organisasi, Anda juga memilih domain untuk organisasi dan mengatur pengaturan direktori pengguna dan enkripsi.

Anda dapat membuat WorkMail direktori Amazon baru untuk digunakan dengan WorkMail organisasi Anda, atau mengintegrasikan Amazon WorkMail dengan direktori yang ada. Anda dapat menggunakan Amazon WorkMail dengan direktori yang ada dari jenis berikut:

- Direktori Aktif Microsoft lokal
- AWS Managed Active Directory (yang merupakan [Microsoft AD yang dikelola oleh AWS Directory Service](#))
- Simple AD

Dengan mengintegrasikan dengan direktori lokal, Anda dapat menggunakan pengguna dan grup yang ada di Amazon WorkMail dan pengguna dapat masuk dengan kredensialnya yang ada. Jika Anda menggunakan direktori lokal, Anda harus terlebih dahulu menyiapkan AD Connector. AWS Directory Service AD Connector menyinkronkan pengguna dan grup Anda dengan buku WorkMail

alamat Amazon dan melakukan permintaan otentikasi pengguna. Untuk informasi lebih lanjut, lihat [Konektor Direktori Aktif](#) dalam Panduan Administrasi Directory Service .

Anda juga memiliki opsi untuk memilih AWS KMS key yang WorkMail digunakan Amazon untuk mengenkripsi konten kotak surat. Anda dapat memilih kunci master AWS terkelola default untuk Amazon WorkMail, atau menggunakan kunci KMS yang ada di AWS Key Management Service (AWS KMS). Untuk informasi tentang membuat kunci KMS baru, lihat [Membuat kunci](#) di Panduan AWS Key Management Service Pengembang. Jika Anda masuk sebagai pengguna AWS Identity and Access Management (IAM), jadikan diri Anda administrator kunci pada kunci KMS. Untuk informasi selengkapnya, lihat [Mengaktifkan dan menonaktifkan kunci](#) di Panduan Developer AWS Key Management Service .

Pertimbangan-pertimbangan

Ingat hal berikut saat membuat WorkMail organisasi Amazon:

- Amazon saat ini WorkMail tidak mendukung layanan Microsoft Active Directory terkelola yang Anda bagikan dengan beberapa akun.
- Jika Anda memiliki Direktori Aktif on-premise dengan Microsoft Exchange dan AD Connector, kami sarankan Anda mengonfigurasi pengaturan interoperabilitas untuk organisasi Anda. Hal ini memungkinkan Anda meminimalkan gangguan pada pengguna saat memigrasi kotak pesan ke Amazon WorkMail, atau menggunakan Amazon WorkMail untuk subset kotak pesan perusahaan Anda. Untuk informasi selengkapnya, lihat [Interoperabilitas antara Amazon dan WorkMail Microsoft Exchange](#).
- Jika Anda memilih opsi Domain uji gratis, Anda dapat mulai menggunakan WorkMail organisasi Amazon Anda dengan domain pengujian yang disediakan. Domain pengujian menggunakan format ini: *example*.awsapps.com. Anda dapat menggunakan domain email uji dengan Amazon WorkMail dan AWS layanan lain yang didukung selama Anda mempertahankan pengguna yang diaktifkan di WorkMail organisasi Amazon Anda. Namun, Anda tidak dapat menggunakan domain pengujian untuk tujuan lain. Domain pengujian mungkin tersedia untuk pendaftaran dan digunakan oleh pelanggan lain jika WorkMail organisasi Amazon Anda tidak mempertahankan setidaknya satu pengguna yang diaktifkan.
- Amazon WorkMail tidak mendukung direktori Multi-region.
- Amazon WorkMail menyinkronkan data direktori dengan AWS Managed Active Directory, Simple AD, dan AD Connector setiap empat jam.

Perubahan penting untuk menggunakan AWS Direktori Aktif Terkelola

Amazon WorkMail memperbarui model otorisasi untuk organisasi yang menggunakan AWS Managed Active Directory (Managed AD). Perubahan ini memengaruhi cara Amazon WorkMail berinteraksi dengan data direktori dan mengharuskan Anda mengambil tindakan spesifik untuk memastikan fungsionalitas yang berkelanjutan.

Sebelumnya, ketika WorkMail organisasi Amazon dibuat dengan Direktori Aktif AWS Terkelola, Amazon WorkMail menggunakan izin tingkat layanan untuk berinteraksi dengan Managed AD. Untuk memberikan fleksibilitas tambahan bagi pelanggan untuk memisahkan peran manajemen direktori dan administrasi kotak pesan, WorkMail API dan konsol sekarang akan menggunakan AWS Directory Service Data (DS-Data) API untuk membuat atau memperbarui pengguna dan grup di AWS Managed Active Directory. Prinsipal IAM yang menjalankan operasi ini melalui WorkMail konsol atau API juga akan memerlukan otorisasi untuk menggunakan DS-Data tindakan yang setara terhadap AD Terkelola yang terkait dengan WorkMail organisasi mereka, memberikan kontrol yang lebih terperinci dan integrasi yang lebih baik dengan kebijakan IAM.

Baik Anda membuat organisasi baru dengan Managed AD, atau memiliki organisasi yang sudah ada yang menggunakan Managed AD, jika Anda ingin terus dapat membuat, memperbarui, atau menghapus pengguna dan grup melalui WorkMail konsol atau API, Anda harus menyelesaikan langkah-langkah konfigurasi tambahan untuk memastikan fungsionalitas yang tepat dengan model otorisasi yang diperbarui. Hal ini dijelaskan dalam [the section called "Integrasi AD Terkelola"](#).

Topik

- [Membuat organisasi](#)
- [Mengkonfigurasi integrasi AWS Managed Active Directory](#)
- [Melihat detail organisasi](#)
- [Mengintegrasikan direktori WorkSpaces](#)
- [Status dan deskripsi organisasi](#)

Membuat organisasi

Buat organisasi baru di WorkMail konsol Amazon.

Untuk membuat organisasi

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

2. Di bilah navigasi, pilih Organisasi.

Halaman Organizations muncul dan menampilkan organisasi Anda, jika ada.

3. Pilih Buat organisasi.
4. Di bawah Domain email, pilih domain yang akan digunakan untuk alamat email di organisasi Anda:
 - Domain Route 53 yang ada — Pilih domain yang ada yang Anda kelola dengan zona yang di-hosting Amazon Route 53 (Route 53).
 - Domain Route 53 Baru — Daftarkan nama domain Route 53 baru untuk digunakan dengan Amazon WorkMail.
 - Domain eksternal — Masukkan domain yang sudah ada yang Anda kelola dengan penyedia sistem nama domain eksternal (DNS).
 - Domain uji gratis — Gunakan domain uji gratis yang disediakan oleh Amazon WorkMail. Anda dapat menjelajahi Amazon WorkMail menggunakan domain pengujian, lalu menambahkan domain ke organisasi Anda nanti.
5. (Opsional) Jika domain Anda dikelola melalui Amazon Route 53, untuk zona yang dihosting Route 53, pilih domain Route 53 Anda.
6. Untuk Alias, masukkan alias unik untuk organisasi Anda.
7. Pilih Pengaturan lanjutan, dan untuk direktori Pengguna, pilih salah satu opsi berikut:
 - Buat WorkMail direktori Amazon baru — Membuat direktori baru untuk menambahkan dan mengelola pengguna Anda.
 - Gunakan direktori yang ada — Menggunakan direktori yang ada untuk mengelola pengguna Anda, seperti Direktori Aktif Microsoft on-premise, Direktori Aktif yang Dikelola AWS, atau Simple AD.
8. Untuk Enkripsi, pilih salah satu opsi berikut:
 - Gunakan kunci WorkMail terkelola Amazon — Membuat kunci enkripsi baru di akun Anda.
 - Gunakan kunci KMS yang ada — Menggunakan kunci KMS yang sudah ada yang telah Anda buat. AWS KMS
9. Pilih Buat organisasi.

Jika Anda menggunakan domain eksternal, verifikasi dengan menambahkan catatan teks (TXT) dan mail exchanger (MX) yang sesuai ke layanan DNS Anda. Catatan TXT memungkinkan Anda memasukkan catatan tentang layanan DNS. Catatan MX menentukan server email masuk.

Pastikan untuk menetapkan domain Anda sebagai default untuk organisasi Anda. Untuk informasi selengkapnya, lihat [Memverifikasi domain](#) dan [Memilih domain default](#).

Saat organisasi Anda Aktif, Anda dapat menambahkan pengguna ke organisasi Anda dan mengatur klien email mereka. Untuk informasi selengkapnya, lihat [Menambahkan pengguna](#) dan [Menyiapkan klien email untuk Amazon WorkMail](#).

Mengkonfigurasi integrasi AWS Managed Active Directory

Saat menggunakan AWS Managed Active Directory dengan WorkMail organisasi Amazon Anda, langkah-langkah konfigurasi tambahan memastikan fungsionalitas yang tepat dengan model otorisasi yang diperbarui.

Untuk mengonfigurasi integrasi AD Terkelola untuk organisasi baru

1. Di Directory Service konsol, navigasikan ke iklan terkelola (Microsoft AD), atau dari WorkMail konsol Amazon, pilih Pengguna atau Grup di panel navigasi kiri, lalu klik tautan direktori di kotak catatan di bagian atas halaman.
2. Pilih Aktifkan untuk Pengguna dan manajemen grup. Pengaturan ini dinonaktifkan secara default dan harus diaktifkan untuk melakukan operasi tulis pada pengguna dan grup.
3. Pastikan kepala sekolah IAM Anda memiliki izin yang diperlukan dengan melampirkan kebijakan dengan tindakan berikut:

```
ds:AccessDSData
ds:ResetUserPassword
ds-data:CreateGroup
ds-data>DeleteGroup
ds-data:AddGroupMember
ds-data:RemoveGroupMember
ds-data:CreateUser
ds-data>DeleteUser
ds-data:UpdateUser
```

Untuk memigrasikan organisasi AD Terkelola yang ada

1. Pantau halaman Pengguna atau Grup di WorkMail konsol Amazon untuk pemberitahuan migrasi.
2. Saat pemberitahuan muncul, aktifkan Aktifkan operasi direktori yang diperbarui untuk bermigrasi ke Directory Service API yang baru.
3. Terakhir, pastikan bahwa Anda telah mengaktifkan Manajemen pengguna dan grup di Directory Service konsol dan telah memperbarui kebijakan IAM Anda dengan DS-Data izin yang diperlukan seperti yang dijelaskan di bagian sebelumnya.

Penggunaan AWS Directory Service Data (DS-Data) API untuk membuat, memperbarui, dan menghapus pengguna akan diaktifkan untuk WorkMail organisasi Amazon yang tersisa menggunakan Managed AD yang sebelumnya tidak diaktifkan.

Melihat detail organisasi

Setiap WorkMail organisasi Amazon Anda dapat menampilkan halaman detail organisasi. Halaman ini menampilkan informasi tentang organisasi mereka, termasuk ID yang dapat Anda gunakan dengan AWS Command Line Interface. Pesan di halaman juga dapat menunjukkan kepada Anda langkah-langkah apa pun yang diperlukan untuk menyelesaikan pengaturan dan pengorganisasian, seperti domain yang tidak diverifikasi atau kurangnya pengguna. Pesan juga memberikan langkah pertama yang Anda ikuti untuk mengatur klien email tertentu.

Untuk melihat detail organisasi

1. Di bilah navigasi, pilih Organisasi.

Halaman Organizations muncul dan menampilkan organisasi Anda.

2. Pilih organisasi yang ingin Anda lihat.

Mengintegrasikan direktori WorkSpaces

Untuk menggunakan Amazon WorkMail WorkSpaces, buat direktori yang kompatibel dengan menggunakan langkah-langkah berikut.

Untuk menambahkan WorkSpaces direktori yang kompatibel

1. Buat direktori yang kompatibel menggunakan WorkSpaces. Untuk WorkSpaces petunjuknya, lihat [Memulai Penyiapan WorkSpaces Cepat Amazon](#) di Panduan WorkSpaces Administrasi Amazon.
2. Di WorkMail konsol Amazon, buat WorkMail organisasi Amazon Anda dan pilih untuk menggunakan direktori yang ada untuk itu. Untuk informasi selengkapnya, lihat [Membuat organisasi](#).

Status dan deskripsi organisasi

Setelah Anda membuat organisasi, organisasi tersebut dapat memiliki salah satu status berikut.

Status	Deskripsi
Aktif	Organisasi Anda sehat dan siap digunakan.
Creating	Alur kerja berjalan untuk membuat organisasi Anda.
Gagal	Organisasi Anda tidak dapat dibuat.
Terganggu	Organisasi Anda tidak berfungsi atau masalah telah terdeteksi.
Tidak aktif	Organisasi Anda tidak aktif.
Diminta	Permintaan pembuatan organisasi Anda ada dalam antrian dan menunggu untuk dibuat.
Memvalidasi	Semua pengaturan untuk organisasi sedang diperiksa kesehatannya.

Menghapus organisasi

Jika Anda tidak lagi ingin menggunakan Amazon WorkMail untuk email organisasi Anda, Anda dapat menghapus organisasi Anda dari Amazon WorkMail.

Note

Operasi ini tidak dapat dibatalkan. Anda tidak akan dapat memulihkan data kotak pesan setelah organisasi dihapus.

Untuk menghapus organisasi

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Pada layar Organizations, dalam daftar organisasi, pilih organisasi yang akan dihapus dan dipilih Hapus.
3. Untuk Menghapus organisasi, pilih apakah akan menghapus atau menyimpan direktori pengguna yang ada, dan kemudian masukkan nama organisasi.
4. Pilih Hapus organisasi.

Note

Jika Anda tidak menyediakan direktori Anda sendiri untuk Amazon WorkMail, kami akan membuatnya untuk Anda. Jika Anda menyimpan direktori yang ada ini saat menghapus organisasi, Anda akan dikenakan biaya untuk itu kecuali jika digunakan oleh Amazon WorkMail, WorkDocs, atau WorkSpaces. Untuk informasi harga, lihat [Harga Jenis direktori Lainnya](#).

Untuk menghapus direktori, itu tidak dapat mengaktifkan AWS aplikasi lain. Untuk informasi selengkapnya, lihat [Menghapus direktori Simple AD](#) atau [Menghapus direktori AD Connector](#) di Panduan Administrasi AWS Directory Service .

Anda mungkin mendapatkan pesan galat set aturan Amazon Simple Email Service (Amazon SES) yang tidak valid saat mencoba menghapus organisasi. Jika Anda menerima kesalahan ini, edit aturan Amazon SES di konsol Amazon SES dan hapus kumpulan aturan yang tidak valid. Aturan yang Anda edit harus memiliki ID WorkMail organisasi Amazon Anda di nama aturan. Untuk informasi

selengkapnya tentang mengedit aturan Amazon SES, lihat [Membuat aturan tanda terima](#) di Panduan Pengembang Layanan Email Sederhana Amazon.

Jika Anda perlu mencari tahu set aturan mana yang tidak valid, simpan aturan terlebih dahulu. Pesan kesalahan muncul untuk set aturan.

Menemukan alamat email

Anda dapat menemukan jika alamat email digunakan di Organisasi menurut pengguna, sumber daya, atau grup.

Untuk menemukan alamat email

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi.
3. Di halaman Organisasi, pilih Temukan alamat email.
4. Pilih Cari.

Bekerja dengan pengaturan organisasi

Bagian berikut menjelaskan cara menggunakan pengaturan yang tersedia untuk WorkMail organisasi Amazon. Pengaturan yang Anda pilih akan berlaku untuk seluruh organisasi.

Topik

- [Mengaktifkan migrasi kotak pesan](#)
- [Mengaktifkan penjurnalan](#)
- [Mengaktifkan interoperabilitas](#)
- [Mengaktifkan gateway SMTP](#)
- [Mengelola alur email](#)
- [Memberlakukan kebijakan DMARC pada email masuk](#)

Mengaktifkan migrasi kotak pesan

Anda mengaktifkan migrasi kotak pesan saat ingin mentransfer kotak pesan dari sumber, seperti Microsoft Exchange atau G Suite Basic, ke Amazon WorkMail Anda mengaktifkan migrasi sebagai bagian dari proses migrasi yang lebih besar. Untuk informasi selengkapnya, termasuk langkah-langkah caranya, lihat [Migrasi ke Amazon WorkMail](#) di bagian Memulai panduan ini.

Mengaktifkan penjurnalan

Anda mengaktifkan jurnal untuk merekam komunikasi email Anda. Saat menggunakan penjurnalan, Anda biasanya menggunakan alat pengarsipan dan eDiscovery pihak ketiga yang terintegrasi. Jurnal membantu memastikan bahwa Anda memenuhi peraturan kepatuhan untuk penyimpanan data, perlindungan privasi, dan perlindungan informasi.

Untuk informasi selengkapnya, termasuk langkah-langkah caranya, lihat [Menggunakan jurnal email dengan Amazon WorkMail](#) di bagian Memulai panduan ini.

Mengaktifkan interoperabilitas

Interoperabilitas memungkinkan Anda untuk bermigrasi dari Microsoft Exchange dan menggunakan Amazon WorkMail sebagai bagian dari kotak pesan perusahaan Anda. Untuk informasi selengkapnya, termasuk langkah-langkah caranya, lihat [Konfigurasi setelah ketersediaan di Amazon WorkMail](#) di bagian Memulai panduan ini.

Mengaktifkan gateway SMTP

Anda mengaktifkan gateway Simple Mail Transfer Protocol (SMTP) untuk digunakan dengan aturan alur email keluar. Aturan alur email keluar memungkinkan Anda merutekan pesan email yang dikirim dari WorkMail organisasi Amazon Anda melalui gateway SMTP. Untuk informasi selengkapnya, lihat [Tindakan aturan email keluar](#).

Note

Gateway SMTP yang dikonfigurasi untuk aturan alur email keluar harus mendukung Transport Layer Security (TLS) v1.2 menggunakan sertifikat dari otoritas sertifikat utama. Hanya autentikasi dasar yang didukung.

Untuk mengkonfigurasi gateway SMTP

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi.
3. Di panel navigasi, pilih Pengaturan organisasi.

Halaman pengaturan Organisasi muncul dan menampilkan satu set tab.

4. Pilih tab gateway SMTP, lalu pilih Buat gateway.
5. Masukkan yang berikut ini:

- Nama gateway — Masukkan nama unik.
- Alamat gateway — Masukkan nama host atau alamat IP gateway.
- Nomor port — Masukkan nomor port gateway.
- Nama pengguna — Masukkan nama pengguna.
- Kata sandi — Masukkan kata sandi yang kuat.

6. Pilih Buat.

Gateway SMTP tersedia untuk digunakan dengan aturan alur email keluar.

Saat Anda mengonfigurasi gateway SMTP untuk digunakan dengan aturan alur email keluar, pesan keluar mencoba mencocokkan aturan dengan gateway SMTP. Pesan yang cocok dengan aturan dirutekan ke gateway SMTP yang sesuai, yang kemudian menangani sisa pengiriman email.

Jika Amazon WorkMail tidak dapat mencapai gateway SMTP, sistem akan memantulkan pesan email kembali ke pengirim. Jika ini terjadi, ikuti langkah-langkah sebelumnya untuk memperbaiki pengaturan gateway.

Mengelola alur email

Untuk membantu mengelola email, Anda dapat mengatur aturan alur email. Aturan alur email dapat mengambil satu atau beberapa tindakan pada pesan email berdasarkan alamat atau domainnya. Anda dapat menggunakan aturan alur email pada alamat email atau domain pengirim dan penerima.

Saat membuat aturan alur email, Anda menentukan [tindakan aturan](#) yang berlaku untuk email saat [pola](#) aturan tertentu dicocokkan.

Topik

- [Tindakan aturan email masuk](#)
- [Tindakan aturan email keluar](#)
- [Pola pengirim dan penerima](#)
- [Membuat aturan alur email](#)
- [Mengedit aturan alur email](#)
- [Melakukan konfigurasi AWS Lambda untuk Amazon WorkMail](#)
- [Mengelola akses ke Amazon WorkMail Message Flow API](#)
- [Menguji aturan alur email](#)
- [Menghapus aturan alur email](#)

Tindakan aturan email masuk


Aturan alur email masuk membantu mencegah email yang tidak diinginkan masuk ke kotak pesan pengguna. Aturan alur email masuk, juga disebut tindakan aturan, secara otomatis berlaku untuk semua pesan email yang dikirim ke siapa pun di dalam WorkMail organisasi Amazon Anda. Ini berbeda dari aturan email untuk masing-masing kotak pesan.

Note

Secara opsional, Anda dapat menggunakan aturan dengan AWS Lambda fungsi untuk memproses email masuk sebelum dikirimkan ke kotak pesan pengguna. Untuk informasi selengkapnya tentang penggunaan Lambda dengan Amazon WorkMail, lihat [Melakukan konfigurasi AWS Lambda untuk Amazon WorkMail](#) Untuk informasi tentang Lambda, lihat [Panduan Developer AWS Lambda](#) .

Aturan alur email masuk, juga disebut tindakan aturan, secara otomatis berlaku untuk semua pesan email yang dikirim ke siapa pun di dalam WorkMail organisasi Amazon. Ini berbeda dari aturan email untuk masing-masing kotak pesan.

Tindakan aturan berikut menentukan bagaimana email masuk ditangani. Untuk setiap aturan, Anda tentukan [pola pengirim dan penerima](#) bersama-sama dengan salah satu tindakan berikut.

Tindakan	Deskripsi
Jatuhkan email	Pesan email diabaikan. Email ini tidak disampaikan, dan pengirim tidak diberitahu tentang kegagalan pengiriman.
Kirim respon pentalan	Pesan email tidak terkirim, dan pengirim diberitahu tentang kegagalan pengiriman dalam pesan pentalan.
Kirim ke folder sampah	Pesan email dikirim ke folder spam atau sampah pengguna, bahkan jika itu awalnya tidak diidentifikasi sebagai spam oleh sistem deteksi WorkMail spam Amazon.
Default	<p>Pesan email dikirimkan setelah diperiksa oleh sistem deteksi WorkMail spam Amazon. Email spam dikirim ke folder sampah. Semua pesan email lainnya dikirim ke kotak masuk.</p> <p>Aturan alur email lainnya dengan pola pengirim yang kurang spesifik akan diabaikan. Untuk menambahkan pengecualian ke aturan alur email berbasis domain, konfigurasi tindakan Default dengan pola pengirim yang lebih spesifik. Untuk informasi selengkapnya, lihat Pola pengirim dan penerima.</p>
Jangan pernah mengirim ke folder sampah	<p>Pesan email selalu dikirim ke kotak masuk pengguna, bahkan jika itu diidentifikasi sebagai spam oleh sistem deteksi WorkMail spam Amazon.</p> <div data-bbox="829 1640 1507 1864" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>Dengan tidak menggunakan sistem deteksi spam default, Anda dapat membuat pengguna Anda dalam</p></div>

Tindakan	Deskripsi
	bahaya karena berpotensi menerima konten berisiko tinggi dari alamat yang Anda tentukan.
Jalankan AWS Lambda	Menyampaikan pesan email ke fungsi Lambda untuk diproses sebelum atau saat dikirim ke kotak masuk pengguna.

Note

Email masuk pertama kali dikirim ke Amazon SES, dan kemudian ke Amazon WorkMail. Jika Amazon SES memblokir pesan email yang masuk, maka tindakan aturan tidak akan berlaku. Sebagai contoh, Amazon SES memblokir pesan email ketika virus yang diketahui terdeteksi atau karena aturan penyaringan IP eksplisit. Menentukan tindakan aturan, seperti Default, Kirim ke folder sampah, atau Jangan pernah mengirim ke folder sampah tidak berpengaruh.

Tindakan aturan email keluar

Anda menggunakan aturan alur email keluar untuk mengarahkan pesan email melalui gateway SMTP, atau untuk memblokir pengirim agar tidak mengirim pesan email ke penerima tertentu. Untuk informasi selengkapnya tentang gateway SMTP, lihat [Mengaktifkan gateway SMTP](#).

Anda juga dapat menggunakan aturan alur email keluar untuk meneruskan pesan email ke AWS Lambda fungsi untuk diproses setelah email dikirim. Untuk informasi tentang Lambda, lihat [Panduan Developer AWS Lambda](#).

Tindakan aturan berikut menentukan bagaimana email keluar ditangani. Untuk setiap aturan, Anda tentukan [pola pengirim dan penerima](#) bersama-sama dengan salah satu tindakan berikut.

Tindakan	Deskripsi
Default	Pesan email dikirim melalui aliran normal.

Tindakan	Deskripsi
Jatuhkan email	Pesan email dijatuhkan. Email tidak dikirim, dan pengirim tidak diberitahu.
Kirim respon pentalan	Pesan email tidak dikirim, dan pengirim akan diberitahu dengan pesan bahwa administrator memblokir pesan email.
Rute ke gateway SMTP	Pesan email dikirim melalui gateway SMTP yang dikonfigurasi.
Jalankan Lambda	Menyampaikan pesan email ke fungsi Lambda untuk diproses sebelum atau saat pesan email dikirim.

Pola pengirim dan penerima

Aturan alur email dapat diterapkan ke alamat email tertentu, atau semua alamat email di bawah domain atau kumpulan domain tertentu. Anda menentukan pola untuk menentukan alamat email yang diberlakukan aturan.

Pola pengirim dan penerima mengambil salah satu bentuk berikut:

- Alamat email cocok dengan satu alamat email; misalnya:

mailbox@example.com

- Nama domain cocok dengan semua alamat email di bawah domain tersebut; misalnya:

example.com

- Domain wildcard cocok dengan semua alamat email di bawah domain itu dan semua subdomainnya. Wildcard hanya muncul di bagian depan domain; misalnya:

*.example.com

- Bintang cocok dengan alamat email apa pun di bawah domain apa pun.

*

Note

Simbol + tidak valid dalam pola pengirim atau penerima.

Beberapa pola dapat ditentukan untuk satu aturan. Untuk informasi selengkapnya, lihat [Tindakan aturan email masuk](#) dan [Tindakan aturan email keluar](#).

Aturan alur email masuk diterapkan jika header `Sender` atau `From` dalam pesan email masuk cocok dengan pola apapun. Jika ada, alamat `Sender` dicocokkan terlebih dahulu. Parameter `From` alamat dicocokkan jika tidak ada header `Sender` atau jika header `Sender` tidak cocok dengan aturan apapun. Jika ada beberapa penerima pesan email yang sesuai dengan aturan yang berbeda, setiap aturan akan berlaku untuk penerima yang cocok.

Aturan alur email keluar diterapkan jika penerima dan header `Sender` atau `From` dalam pesan email keluar cocok dengan pola apapun. Jika ada beberapa penerima untuk pesan email yang cocok dengan aturan yang berbeda, setiap aturan akan berlaku untuk penerima yang cocok.

Jika beberapa aturan cocok, tindakan aturan yang paling spesifik diterapkan. Contohnya adalah ketika aturan untuk alamat email tertentu diutamakan daripada aturan untuk seluruh domain. Jika beberapa aturan memiliki kekhususan yang sama, tindakan yang paling ketat diterapkan. Contohnya adalah ketika tindakan Jatuhkan lebih diutamakan daripada tindakan Pentalan. Urutan prioritas untuk tindakan adalah sama dengan urutan di mana mereka tercantum dalam [Tindakan aturan email masuk](#) dan [Tindakan aturan email keluar](#).

Note

Berhati-hatilah saat membuat aturan dengan pola pengirim yang tumpang tindih dengan tindakan Jatuhkan atau Pentalan. Urutan prioritas tak terduga dapat mengakibatkan banyak pesan email masuk tidak terkirim.

Membuat aturan alur email

Aturan alur email menerapkan [tindakan aturan](#) ke pesan email masuk dan keluar. Tindakan berlaku ketika pesan cocok dengan [pola](#) tertentu. Aturan alur email baru segera berlaku.

Untuk membuat aturan alur email

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi.
3. Di panel navigasi, pilih Pengaturan organisasi.

Halaman pengaturan Organisasi muncul dan menampilkan satu set tab. Dari halaman ini, Anda dapat membuat aturan masuk atau keluar. Langkah-langkah berikut menjelaskan cara membuat kedua jenis.

Untuk membuat aturan masuk

1. Pilih tab Aturan masuk dan kemudian pilih Buat.
2. Di kotak Nama aturan, masukkan nama unik.
3. Di bawah Tindakan, buka daftar dan pilih tindakan. Setiap item dalam daftar berisi deskripsi, dan beberapa menyediakan Pelajari lebih lanjut tautan.

Note

Jika Anda memilih tindakan Jalankan Lambda, kontrol tambahan akan muncul: Untuk informasi tentang penggunaan kontrol tersebut, lihat bagian selanjutnya. [Melakukan konfigurasi AWS Lambda untuk Amazon WorkMail](#)

4. Di bawah Domain atau alamat Pengirim, masukkan domain atau alamat pengirim yang Anda inginkan aturan untuk diterapkan.
5. Di bawah Domain atau alamat tujuan, masukkan kombinasi domain tujuan dan alamat email apa pun.
6. Pilih Buat.

Untuk membuat aturan keluar

1. Pilih tab Aturan keluar dan pilih Buat.
2. Di kotak Nama aturan, masukkan nama unik.
3. Di bawah Tindakan, buka daftar dan pilih tindakan. Setiap item dalam daftar berisi deskripsi, dan beberapa menyediakan Pelajari lebih lanjut tautan.

Note

Jika Anda memilih tindakan Jalankan Lambda, kontrol tambahan akan muncul. Untuk informasi tentang menggunakan kontrol tersebut, lihat bagian selanjutnya [Melakukan konfigurasi AWS Lambda untuk Amazon WorkMail](#).

4. Di bawah domain atau alamat Pengirim, masukkan kombinasi domain pengirim dan alamat email yang valid.
5. Di bawah Domain atau alamat tujuan, masukkan kombinasi domain tujuan dan alamat email yang valid.
6. Pilih Buat.

Anda dapat menguji aturan alur email baru yang Anda buat. Untuk informasi selengkapnya, lihat [Menguji aturan alur email](#).

Mengedit aturan alur email

Anda mengedit aturan alur email kapan pun Anda perlu mengubah satu atau beberapa [tindakan aturan](#) untuk pesan email. Langkah-langkah di bagian ini berlaku untuk pesan email masuk dan keluar.

Untuk mengedit aturan alur email

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi.

3. Di panel navigasi, pilih Pengaturan organisasi.

Halaman pengaturan Organisasi muncul dan menampilkan satu set tab.

4. Pilih tab Aturan masuk atau Aturan keluar.
5. Pilih tombol radio di sebelah aturan yang ingin Anda ubah, lalu pilih Edit.
6. Ubah tindakan atau tindakan dalam aturan sesuai kebutuhan, lalu pilih Simpan.

Melakukan konfigurasi AWS Lambda untuk Amazon WorkMail

Gunakan tindakan Jalankan Lambda dalam aturan alur email masuk dan keluar untuk meneruskan pesan email yang cocok dengan aturan ke fungsi untuk diproses. AWS Lambda

Pilih dari konfigurasi berikut untuk tindakan Jalankan Lambda di Amazon. WorkMail

Konfigurasi Jalankan Lambda yang sinkron

Pesan email yang cocok dengan aturan aliran disampaikan ke fungsi Lambda untuk diproses sebelum mereka dikirim atau diserahkan. Gunakan konfigurasi ini untuk mengubah konten email. Anda juga dapat mengontrol aliran email masuk atau keluar untuk kasus penggunaan yang berbeda. Misalnya, aturan yang diteruskan ke fungsi Lambda dapat memblokir pengiriman pesan email sensitif, menghapus lampiran, atau menambahkan penafian.

Konfigurasi Jalankan Lambda yang tidak sinkron

Pesan email yang cocok dengan aturan aliran disampaikan ke fungsi Lambda untuk diproses saat mereka dikirim atau diserahkan. Konfigurasi ini tidak mempengaruhi pengiriman email dan digunakan untuk tugas-tugas seperti mengumpulkan metrik untuk pesan email masuk atau keluar.

Baik Anda memilih konfigurasi sinkron atau asinkron, objek peristiwa yang diteruskan ke fungsi Lambda berisi metadata untuk peristiwa email masuk atau keluar. Anda juga dapat menggunakan ID pesan dalam metadata untuk mengakses konten lengkap pesan email. Untuk informasi selengkapnya, lihat [Mengambil konten pesan dengan AWS Lambda](#). Untuk informasi selengkapnya tentang peristiwa email, lihat [Data peristiwa Lambda](#).

Untuk informasi selengkapnya tentang aturan alur email masuk dan keluar, lihat [Mengelola alur email](#). Untuk informasi tentang Lambda, lihat [Panduan Developer AWS Lambda](#).

Note

Saat ini, aturan aliran email Lambda hanya mereferensikan fungsi Lambda di Wilayah AWS yang sama dan sebagai organisasi Amazon Akun AWS WorkMail yang sedang dikonfigurasi.

Memulai dengan AWS Lambda untuk Amazon WorkMail

Untuk mulai menggunakan AWS Lambda dengan Amazon WorkMail, sebaiknya gunakan fungsi [WorkMail Hello World Lambda](#) dari AWS Serverless Application Repository akun Anda ke akun Anda. Fungsi ini memiliki semua sumber daya yang diperlukan, dan izin yang dikonfigurasi untuk Anda. Untuk contoh lainnya, lihat repositori [amazon-workmail-lambda-templates](#) di GitHub

Jika Anda memilih untuk membuat fungsi Lambda Anda sendiri, Anda harus mengonfigurasi izin menggunakan (). AWS Command Line Interface AWS CLI Dalam contoh perintah berikut, lakukan hal berikut:

- Ganti MY_FUNCTION_NAME dengan nama fungsi Lambda Anda.
- Ganti REGION dengan Amazon WorkMail AWS Region Anda. WorkMail Wilayah Amazon yang tersedia termasuk us-east-1 (AS Timur (Virginia N.)), us-west-2 (AS Barat (Oregon)), dan eu-west-1 (Eropa (Irlandia)).
- Ganti AWS_ACCOUNT_ID dengan Akun AWS ID 12 digit Anda.
- Ganti WORKMAIL_ORGANIZATION_ID dengan ID WorkMail organisasi Amazon Anda. Anda dapat menemukannya di kartu untuk organisasi Anda di halaman Organizations.

```
aws --region REGION lambda add-permission --function-name MY_FUNCTION_NAME  
--statement-id AllowWorkMail  
--action "lambda:InvokeFunction"  
--principal workmail.REGION.amazonaws.com  
--source-arn  
arn:aws:workmail:REGION:AWS_ACCOUNT_ID:organization/WORKMAIL_ORGANIZATION_ID
```

Untuk informasi selengkapnya tentang menggunakan AWS CLI, lihat [Panduan AWS Command Line Interface Pengguna](#).

Mengkonfigurasi sinkron Jalankan Lambda aturan

Untuk mengkonfigurasi aturan Jalankan Lambda yang sinkron, buat aturan alur email dengan tindakan Jalankan Lambda dan pilih kotak centang Jalankan secara sinkron. Untuk informasi selengkapnya tentang membuat aturan alur pesan, lihat [Membuat aturan alur email](#).

Untuk menyelesaikan pembuatan aturan sinkron, tambahkan Amazon Resource Name (ARN) Lambda dan konfigurasi opsi berikut.

Aksi mundur

Tindakan Amazon WorkMail berlaku jika fungsi Lambda gagal dijalankan. Tindakan ini juga berlaku untuk setiap penerima yang dihilangkan dari respon Lambda jika bendera allRecipients tidak diatur. Aksi Fallback tidak bisa menjadi aksi Lambda lain.

Waktu habis (dalam menit)

Periode waktu di mana fungsi Lambda dicoba lagi jika Amazon WorkMail gagal memanggilnya. Tindakan mundur diterapkan pada akhir jangka waktu ini.

Note

Aturan Jalankan Lambda Sinkron hanya support syarat tujuan *.

Data peristiwa Lambda

Fungsi Lambda dipicu menggunakan data peristiwa berikut. Presentasi data bervariasi tergantung pada bahasa pemrograman yang digunakan untuk fungsi Lambda.

```
{
  "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
}
```

JSON peristiwa mencakup data peristiwa berikut.

summaryVersion

Nomor versi untuk `LambdaEventData`. Ini hanya diperbarui ketika Anda membuat perubahan yang tidak kompatibel ke belakang. `LambdaEventData`

amplop

Amplop pesan email, yang meliputi: bidang berikut.

mailFrom

Alamat Dari, yang biasanya alamat email dari pengguna yang mengirim pesan. Jika pengguna mengirim pesan email sebagai pengguna lain atau atas nama pengguna lain, bidang `mailFrom` mengembalikan alamat email pengguna yang atas namanya pesan email tersebut dikirim, bukan alamat email pengirim sebenarnya.

penerima

Daftar alamat email penerima. Amazon WorkMail tidak membedakan antara To, CC, atau BCC.

Note

Untuk aturan alur email masuk, daftar ini menyertakan penerima di semua domain di WorkMail organisasi Amazon tempat Anda membuat aturan. Fungsi Lambda diminta secara terpisah untuk setiap percakapan SMTP dari pengirim, dan bidang penerima mencantumkan penerima dari percakapan SMTP tersebut. Penerima dengan domain eksternal tidak disertakan.

pengirim

Alamat email pengguna yang mengirim pesan email atas nama pengguna lain. Bidang ini diatur hanya jika suatu pesan email dikirim atas nama pengguna lain.

subjek

Baris subjek email. Dipotong ketika melebihi batas 256 karakter.

messageId

ID unik yang digunakan untuk mengakses konten lengkap pesan email saat menggunakan Amazon WorkMail Message Flow SDK.

InvocationId

ID untuk invokasi Lambda yang unik. ID ini tetap sama ketika fungsi Lambda dipanggil lebih dari sekali untuk hal yang sama. `LambdaEventData` Gunakan untuk mendeteksi percobaan ulang dan menghindari duplikasi.

flowDirection

Menunjukkan arah alur email, baik INBOUND atau OUTBOUND.

terpotong

Berlaku untuk ukuran muatan, bukan panjang baris subjek. Saat `true`, ukuran muatan melebihi batas 128 KB, sehingga daftar penerima dipotong untuk memenuhi batas.

Sinkron Jalankan Lambda skema respon

Jika aturan alur email dengan tindakan Jalankan Lambda sinkron cocok dengan pesan email masuk atau keluar, Amazon WorkMail memanggil fungsi Lambda yang dikonfigurasi dan menunggu respons sebelum mengambil tindakan pada pesan email. Fungsi Lambda mengembalikan respon sesuai dengan skema yang telah ditetapkan yang berisi tindakan, jenis tindakan, parameter yang berlaku, dan penerima yang diberlakukan tindakan terhadapnya.

Contoh berikut menunjukkan respon Run Lambda sinkron. Respon bervariasi berdasarkan bahasa pemrograman yang digunakan untuk fungsi Lambda.

```
{
  "actions": [
    {
      "action" : {
```

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

Respon JSON meliputi data berikut.

tindakan

Tindakan yang harus dilakukan untuk penerima.

jenis

Jenis tindakan. Jenis tindakan tidak dikembalikan untuk tindakan Jalankan Lambda yang tidak sinkron.

Jenis tindakan aturan masuk termasuk BOUNCE, DROP, DEFAULT, BYPASS_SPAM_CHECK, dan MOVE_TO_JUNK. Untuk informasi selengkapnya, lihat [Tindakan aturan email masuk](#).

Jenis tindakan aturan keluar termasuk BOUNCE, DROP, dan DEFAULT. Untuk informasi selengkapnya, lihat [Tindakan aturan email keluar](#).

parameter

Parameter tindakan tambahan. Support untuk jenis tindakan BOUNCE sebagai objek JSON dengan kunci bouncemessage dan nilai string. Pesan pentalan ini digunakan untuk membuat pesan email pentalan.

penerima

Daftar alamat email tempat tindakan harus dilakukan. Anda dapat menambahkan penerima baru ke respon meskipun mereka tidak disertakan dalam daftar penerima semula. Bidang ini tidak diperlukan jika allRecipients benar untuk sebuah tindakan.

Note

Ketika tindakan Lambda dipanggil untuk email masuk, Anda hanya dapat menambahkan penerima baru yang berasal dari organisasi Anda. Penerima baru ditambahkan ke respon sebagai BCC.

allRecipients

Jika benar, berlaku tindakan untuk semua penerima yang tidak tunduk pada tindakan spesifik lain dalam respon Lambda.

Sinkron Jalankan Lambda batas tindakan

Batasan berikut berlaku saat Amazon WorkMail memanggil fungsi Lambda untuk tindakan Jalankan Lambda yang sinkron:

- Fungsi Lambda harus merespon dalam waktu 15 detik, atau diperlakukan sebagai permintaan yang gagal.

Note

Sistem mencoba ulang permintaan untuk interval Batas waktu habis yang Anda tentukan.

- Respon fungsi Lambda hingga 256 KB diperbolehkan.
- Hingga 10 tindakan unik diperbolehkan dalam respon. Tindakan yang lebih besar dari 10 tunduk pada konfigurasi Tindakan mundur.
- Hingga 500 penerima diperbolehkan untuk fungsi Lambda keluar.
- Nilai maksimum untuk Batas waktu habis adalah 240 menit. Jika nilai minimum 0 dikonfigurasi, tidak ada percobaan ulang sebelum Amazon WorkMail menerapkan tindakan fallback.

Sinkron Jalankan Lambda kegagalan tindakan

Jika Amazon tidak WorkMail dapat menjalankan fungsi Lambda karena kesalahan, respons tidak valid, atau batas waktu Lambda, WorkMail Amazon akan mencoba ulang pemanggilan dengan backoff eksponensial yang mengurangi laju pemrosesan hingga periode batas waktu Aturan selesai. Kemudian, Tindakan mundur diterapkan ke semua penerima pesan email. Untuk informasi selengkapnya, lihat [Mengkonfigurasi sinkron Jalankan Lambda aturan](#).

Contoh sinkron Jalankan Lambda tanggapan

Contoh berikut menunjukkan struktur respon umum Jalankan Lambda sinkron.

Example: Hapus penerima yang ditentukan dari pesan email

Contoh berikut menunjukkan struktur respon Jalankan Lambda sinkron untuk menghapus penerima dari pesan email.

```
{
  "actions": [
    {
      "action": {
        "type": "DEFAULT"
      },
      "allRecipients": true
    },
    {
      "action": {
        "type": "DROP"
      },
      "recipients": [
        "drop-recipient@example.com"
      ]
    }
  ]
}
```

Example: Pentalkan dengan pesan email kustom

Contoh berikut menunjukkan struktur respon Jalankan Lambda yang tidak sinkron untuk mementalkan pesan email kustom.

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

Example: Tambahkan penerima ke pesan email

Contoh berikut menunjukkan struktur respon Jalankan Lambda sinkron untuk menambahkan penerima ke pesan email. Tindakan ini tidak memperbarui bidang Kepada atau CC pesan email.

```
{
  "actions": [
    {
      "action": {
        "type": "DEFAULT"
      },
      "recipients": [
        "new-recipient@example.com"
      ]
    },
    {
      "action": {
        "type": "DEFAULT"
      },
      "allRecipients": true
    }
  ]
}
```

[Untuk contoh kode lainnya yang akan digunakan saat membuat fungsi Lambda untuk tindakan Jalankan Lambda, lihat templat Amazon Lambda. WorkMail](#)

Informasi lebih lanjut tentang menggunakan Lambda dengan Amazon WorkMail

Anda juga dapat mengakses konten lengkap pesan email yang memicu fungsi Lambda. Untuk informasi selengkapnya, lihat [Mengambil konten pesan dengan AWS Lambda](#).

Mengambil konten pesan dengan AWS Lambda

Setelah mengonfigurasi AWS Lambda fungsi untuk mengelola alur email Amazon WorkMail, Anda dapat mengakses konten lengkap pesan email yang diproses menggunakan Lambda. Untuk informasi selengkapnya tentang memulai dengan Lambda untuk Amazon WorkMail, lihat [Melakukan konfigurasi AWS Lambda untuk Amazon WorkMail](#)

Untuk mengakses konten lengkap pesan email, gunakan GetRawMessageContent tindakan di Amazon WorkMail Message Flow API. ID pesan email yang diteruskan ke fungsi Lambda Anda

setelah invokasi mengirimkan permintaan ke API. Kemudian, API merespon dengan konten MIME penuh dari pesan email. Untuk informasi selengkapnya, lihat [Alur WorkMail Pesan Amazon](#) di Referensi Amazon WorkMail API.

Contoh berikut menunjukkan bagaimana fungsi Lambda menggunakan lingkungan waktu aktif Python dapat mengambil isi pesan lengkap.

Tip

Jika Anda mulai dengan menerapkan fungsi Amazon WorkMail [Hello World Lambda](#) dari AWS Serverless Application Repository ke akun Anda, sistem membuat fungsi Lambda di akun Anda dengan semua sumber daya dan izin yang diperlukan. Anda kemudian dapat menambahkan logika bisnis Anda ke fungsi lambda berdasarkan kasus penggunaan Anda.

```
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)
```

Untuk contoh lebih rinci tentang cara menganalisis konten pesan yang sedang transit, lihat repositori [amazon-workmail-lambda-templates](#) di GitHub

Note

Anda hanya menggunakan Amazon WorkMail Message Flow API untuk mengakses pesan email dalam perjalanan. Anda hanya dapat mengakses pesan dalam waktu 24 jam setelah dikirim atau diterima. Untuk mengakses pesan secara terprogram di kotak pesan pengguna, gunakan salah satu protokol lain yang didukung oleh WorkMail Amazon, seperti IMAP atau Exchange Web Services (EWS).

Memperbarui konten pesan dengan AWS Lambda

Setelah mengonfigurasi AWS Lambda fungsi sinkron untuk mengelola alur email, Anda dapat menggunakan `PutRawMessageContent` tindakan di Amazon WorkMail Message flow API untuk memperbarui konten pesan email dalam perjalanan. Untuk informasi selengkapnya tentang memulai fungsi Lambda untuk Amazon WorkMail, lihat [Mengkonfigurasi sinkron Jalankan Lambda aturan](#). Untuk informasi selengkapnya tentang API, lihat [PutRawMessageContent](#).

Note

`PutRawMessageContent` API membutuhkan boto3 1.17.8, atau Anda dapat menambahkan lapisan ke fungsi Lambda Anda. Untuk mengunduh versi boto3 yang benar, lihat halaman [boto](#) di GitHub. Untuk informasi lebih lanjut tentang menambahkan lapisan, lihat [Konfigurasi fungsi untuk menggunakan lapisan](#).

Berikut ini adalah contoh lapisan: `"LayerArn": "arn:aws:lambda:`

`${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2"`. Dalam contoh ini, gantikan `${AWS::Region}` dengan wilayah aws yang sesuai, seperti `us-east-1`.

Tip

Jika Anda memulai dengan menerapkan fungsi Amazon WorkMail [Hello World Lambda](#) dari AWS Serverless Application Repository ke akun Anda, sistem akan membuat fungsi Lambda di akun Anda dengan sumber daya dan izin yang diperlukan. Anda kemudian dapat menambahkan logika bisnis ke fungsi lambda berdasarkan kasus penggunaan Anda.

Saat Anda pergi, ingat hal berikut:

- Gunakan [GetRawMessageContent](#) API untuk mengambil konten pesan asli. Untuk informasi lebih lanjut, lihat [Mengambil konten pesan dengan AWS Lambda](#).
- Setelah Anda memiliki pesan asli, ubah konten MIME. Setelah selesai, unggah pesan ke bucket Amazon Simple Storage Service (Amazon S3) di akun Anda. Pastikan bucket S3 menggunakan hal yang Akun AWS sama dengan WorkMail operasi Amazon Anda, dan bucket tersebut menggunakan Wilayah AWS yang sama dengan panggilan API Anda.
- WorkMail Agar Amazon dapat memproses permintaan, bucket S3 Anda harus memiliki kebijakan yang benar untuk mengakses objek S3. Untuk informasi selengkapnya, lihat [Example S3 policy](#).

- Gunakan [PutRawMessageContent](#) API untuk mengirim konten pesan yang diperbarui kembali ke Amazon WorkMail.

Note

PutRawMessageContent API memastikan bahwa konten MIME dari pesan yang diperbarui memenuhi standar RFC, serta kriteria yang disebutkan dalam tipe [RawMessageContent](#) data. Email yang masuk ke WorkMail organisasi Amazon Anda tidak selalu memenuhi standar tersebut, sehingga PutRawMessageContent API dapat menolaknya. Dalam kasus tersebut, Anda dapat berkonsultasi tentang pesan kesalahan yang dikembalikan untuk mendapatkan informasi selengkapnya tentang cara memperbaiki masalah.

Example Contoh kebijakan S3

JSON

```
{
  "Version": "2012-10-17",
  "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": "111122223333"
        },
        "Bool": {
          "aws:SecureTransport": "true"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workmailmessageflow:us-east-1:111122223333:message/WORKMAIL_ORGANIZATION_ID/*"
        }
      }
    }
  ]
}
```

```
}  
    }  
  }  
]
```

Contoh berikut menunjukkan bagaimana fungsi Lambda menggunakan waktu aktif Python untuk memperbarui subjek pesan email di transit.

```
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="amzn-s3-demo-bucket",  
Key=key)  
  
    # Update the email in WorkMail  
    s3_reference = {  
        'bucket': "amzn-s3-demo-bucket",  
        'key': key  
    }  
    content = {  
        's3Reference': s3_reference  
    }  
    workmail.put_raw_message_content(messageId=msg_id, content=content)
```

Untuk lebih banyak contoh cara menganalisis konten pesan dalam transit, lihat repositori [amazon-workmail-lambda-templates](#) aktif. GitHub

Mengelola akses ke Amazon WorkMail Message Flow API

Gunakan kebijakan AWS Identity and Access Management (IAM) untuk mengelola akses ke Amazon WorkMail Message Flow API.

Amazon WorkMail Message Flow API bekerja dengan satu jenis sumber daya, pesan email dalam perjalanan. Setiap pesan email di transit memiliki Amazon Resource Name (ARN) yang unik terkait dengannya.

Contoh berikut menunjukkan sintaks ARN terkait dengan pesan email di transit.

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

Bidang yang dapat diubah dalam contoh sebelumnya meliputi:

- Wilayah — Wilayah AWS untuk WorkMail organisasi Amazon Anda.
- Akun — Akun AWS ID untuk WorkMail organisasi Amazon Anda.
- Organisasi — ID WorkMail organisasi Amazon Anda.
- Konteks — Menunjukkan apakah pesan incoming ke organisasi Anda, atau outgoing darinya.
- ID Pesan — ID pesan email unik yang disampaikan sebagai masukan ke fungsi Lambda Anda.

Contoh berikut termasuk contoh ID untuk ARN terkait dengan pesan email masuk di transit.

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

Anda dapat menggunakan ARN ini sebagai sumber daya di Resource bagian kebijakan pengguna IAM Anda untuk mengelola akses ke WorkMail pesan Amazon dalam perjalanan.

Contoh kebijakan IAM untuk akses aliran WorkMail pesan Amazon

Contoh kebijakan berikut memberikan entitas IAM akses baca penuh ke semua pesan masuk dan keluar untuk setiap organisasi Amazon WorkMail di Anda. Akun AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workmailmessageflow:GetRawMessageContent"
      ],
      "Resource": "arn:aws:workmailmessageflow:us-  
east-1:111122223333:message/*",
      "Effect": "Allow"
    }
  ]
}
```

Jika Anda memiliki beberapa organisasi di Akun AWS, Anda juga dapat membatasi akses ke satu atau beberapa organisasi. Hal ini berguna jika fungsi Lambda tertentu hanya boleh digunakan untuk organisasi tertentu.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workmailmessageflow:GetRawMessageContent"
      ],
      "Resource": "arn:aws:workmailmessageflow:us-  
east-1:111122223333:message/organization/*",
      "Effect": "Allow"
    }
  ]
}
```

Anda juga dapat memilih untuk memberikan akses ke pesan tergantung pada apakah pesan tersebut `incoming` ke organisasi Anda, atau `outgoing` darinya. Untuk melakukannya, gunakan pengkualifikasi `incoming` atau `outgoing` di ARN.

Kebijakan contoh berikut memberikan akses hanya ke pesan yang masuk ke organisasi Anda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workmailmessageflow:GetRawMessageContent"
      ],
      "Resource": "arn:aws:workmailmessageflow:us-east-1:111122223333:message/organization/incoming/*",
      "Effect": "Allow"
    }
  ]
}
```

Contoh kebijakan berikut memberikan akses baca dan pembaruan lengkap kepada entitas IAM ke semua pesan masuk dan keluar untuk setiap organisasi Amazon WorkMail di Anda. Akun AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workmailmessageflow:GetRawMessageContent",
        "workmailmessageflow:PutRawMessageContent"
      ],
      "Resource": "arn:aws:workmailmessageflow:us-east-1:111122223333:message/*",
      "Effect": "Allow"
    }
  ]
}
```

}

Menguji aturan alur email

Untuk memeriksa konfigurasi aturan Anda saat ini, Anda dapat menguji bagaimana konfigurasi berperilaku terhadap alamat email tertentu.

Untuk menguji aturan alur email

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Pengaturan organisasi, Inbound/Outboundaturan.
4. Di samping Konfigurasi pengujian, masukkan alamat email lengkap pengirim dan penerima yang ingin Anda uji.
5. Pilih Uji. Tindakan yang akan diambil untuk alamat email yang disediakan akan ditampilkan.

Menghapus aturan alur email

Bila Anda menghapus aturan alur email, perubahan tersebut akan segera diterapkan.

Untuk menghapus aturan alur email

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Pengaturan organisasi, Inbound/Outboundaturan.
4. Pilih aturan dan pilih Hapus.
5. Pada prompt konfirmasi, pilih Hapus.

Memberlakukan kebijakan DMARC pada email masuk

Domain email menggunakan catatan Sistem Nama Domain (DNS) untuk keamanan. Mereka melindungi pengguna Anda dari serangan umum seperti spoofing atau phishing. Catatan DNS sering menyertakan catatan Domain-based Message Authentication, Reporting, and Conformance (DMARC), yang ditetapkan oleh pemilik domain yang mengirim email. Catatan DMARC termasuk kebijakan yang menentukan tindakan untuk dilakukan ketika email gagal melewati pemeriksaan DMARC. Anda dapat memilih apakah akan memberlakukan kebijakan DMARC pada email yang dikirim ke organisasi Anda.

WorkMail Organisasi Amazon baru mengaktifkan penegakan DMARC secara default.

Untuk mengaktifkan pemberlakuan DMARC

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Pengaturan organisasi. Halaman pengaturan Organisasi muncul dan menampilkan satu set tab.
4. Pilih tab DMARC, lalu pilih Edit.
5. Pindahkan slider penegakan DMARC ke posisi on.
6. Pilih kotak centang di sebelah Saya mengakui bahwa mengaktifkan penegakan DMARC dapat mengakibatkan email masuk dijatuhkan atau dikarantina berdasarkan konfigurasi domain pengirim.
7. Pilih Simpan.

Untuk mematikan pemberlakuan DMARC

- Ikuti langkah-langkah di bagian sebelumnya, tetapi pindahkan slider penegakan DMARC ke posisi mati..

Menggunakan pencatatan peristiwa email untuk melacak pemberlakuan DMARC

Mengaktifkan pemberlakuan DMARC dapat mengakibatkan email masuk dijatuhkan atau ditandai sebagai spam, tergantung pada cara pengirim mengonfigurasi domain mereka. Jika pengirim salah mengonfigurasi domain email mereka, pengguna mungkin berhenti menerima email yang sah. Untuk memeriksa email yang tidak dikirimkan ke pengguna, Anda dapat mengaktifkan pencatatan peristiwa email untuk WorkMail organisasi Amazon Anda. Kemudian, Anda dapat meminta pencatatan peristiwa email Anda untuk email masuk yang disaring berdasarkan kebijakan DMARC pengirim.

Sebelum Anda menggunakan pencatatan peristiwa email untuk melacak penegakan DMARC, aktifkan pencatatan peristiwa email di konsol Amazon WorkMail . Untuk mendapatkan hasil maksimal dari data log Anda, biarkan beberapa waktu menunggu peristiwa email dicatat. Untuk informasi dan petunjuk selengkapnya, silakan lihat [the section called “Mengaktifkan pencatatan peristiwa email”](#).

Untuk menggunakan pencatatan peristiwa email untuk melacak pemberlakuan DMARC

1. Di konsol CloudWatch Insights, di bawah Log, pilih Insights.
2. Untuk Pilih grup log, pilih grup log WorkMail organisasi Amazon Anda. Misalnya, /aws/workmail/events/organization-alias.
3. Pilih jangka waktu untuk kueri.
4. Jalankan kueri berikut: stats count() by event.dmarcPolicy | filter event.dmarcVerdict == "FAIL"
5. Pilih Run query (Jalankan kueri).

Anda juga dapat mengatur metrik khusus untuk peristiwa ini. Untuk informasi lebih lanjut, lihat [Membuat konfigurasi metrik](#).

Penandaan sebuah organisasi

Menandai sumber daya WorkMail organisasi Amazon memungkinkan Anda untuk:

- Bedakan antar organisasi di AWS Manajemen Penagihan dan Biaya konsol.
- Kontrol akses ke sumber daya WorkMail organisasi Amazon dengan menambahkannya ke Resource elemen pernyataan kebijakan izin AWS Identity and Access Management (IAM).

Untuk informasi selengkapnya tentang izin WorkMail tingkat sumber daya Amazon, lihat [Sumber daya](#) Untuk informasi lebih lanjut tentang mengendalikan akses berdasarkan tanda, lihat [Otorisasi berdasarkan tag Amazon WorkMail](#).

WorkMail Administrator Amazon dapat menandai organisasi menggunakan WorkMail konsol Amazon.

Untuk menambahkan tag ke WorkMail organisasi Amazon

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Pilih Tanda.
4. Untuk Tanda Organisasi, pilih Tambahkan tanda baru.
5. Untuk Key, masukkan nama yang mengidentifikasi tag.
6. (Opsional) Untuk Nilai, masukkan nilai untuk tanda tersebut.
7. (Opsional) Ulangi langkah 4-6 untuk menambahkan lebih banyak tanda ke organisasi Anda. Anda dapat menambahkan hingga 50 tag.
8. Pilih Simpan untuk menyimpan perubahan Anda.

Anda dapat melihat tag organisasi Anda di WorkMail konsol Amazon.

Pengembang juga dapat menandai organisasi menggunakan AWS SDK atau AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat `UntagResource` perintah `TagResourceListTagsForResource`, dan di [Referensi WorkMail API Amazon atau Referensi AWS CLI Perintah](#).

Anda dapat menghapus tag dari organisasi kapan saja, menggunakan WorkMail konsol Amazon.

Untuk menghapus tag dari WorkMail organisasi Amazon

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Pilih Tanda.
4. Untuk Tag organisasi, pilih Hapus di sebelah tanda yang akan dihapus.

5. Pilih Kirim untuk menyimpan perubahan Anda.

Bekerja dengan aturan kontrol akses

Aturan kontrol akses untuk Amazon WorkMail memungkinkan administrator mengontrol cara pengguna dan peran peniruan identitas organisasi mereka diberikan akses ke Amazon WorkMail. Setiap WorkMail organisasi Amazon memiliki aturan kontrol akses default yang memberikan akses kotak pesan ke semua pengguna dan peran peniruan identitas yang ditambahkan ke organisasi, apa pun protokol akses atau alamat IP yang mereka gunakan. Administrator dapat mengedit atau mengganti aturan default dengan yang mereka miliki, menambahkan aturan baru, atau menghapus aturan.


Warning

Jika administrator menghapus semua aturan kontrol akses untuk organisasi, Amazon WorkMail memblokir semua akses ke kotak pesan organisasi.

Administrator dapat menerapkan aturan kontrol akses yang mengizinkan atau menolak akses berdasarkan kriteria berikut:

- Protokol — Protokol yang digunakan untuk mengakses kotak surat. Contohnya termasuk Autodiscover, EWS, IMAP, SMTP, Outlook untuk Windows ActiveSync, dan Webmail.
- Alamat IP — rentang IPv4 CIDR yang digunakan untuk mengakses kotak pesan.
- WorkMail Pengguna Amazon — Pengguna di organisasi Anda yang digunakan untuk mengakses kotak pesan.
- Peran peniruan identitas — Peran peniruan identitas di organisasi Anda yang digunakan untuk mengakses kotak pesan. Untuk informasi selengkapnya, lihat [Mengelola peran peniruan](#).

Administrator menerapkan aturan kontrol akses selain izin kotak pesan dan folder pengguna. Untuk informasi selengkapnya, lihat [Bekerja dengan izin kotak pesan](#) dan [Berbagi folder dan izin folder](#) di Panduan WorkMail Pengguna Amazon.

 Note

- Saat Anda mengaktifkan akses untuk Outlook untuk Windows, disarankan untuk juga mengaktifkan akses untuk Autodiscover dan EWS.
- Aturan kontrol akses tidak berlaku untuk WorkMail konsol Amazon atau akses SDK. Gunakan AWS Identity and Access Management (IAM) role atau kebijakan sebagai gantinya. Untuk informasi selengkapnya, lihat [Manajemen identitas dan akses untuk Amazon WorkMail](#).

Membuat aturan kontrol akses

Buat aturan kontrol akses baru dari WorkMail konsol Amazon.

Untuk membuat aturan kontrol akses baru

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Pilih Aturan kontrol akses.
4. Pilih Buat aturan.
5. Di Deskripsi, masukkan deskripsi untuk aturan.
6. Untuk Efek, pilih Izinkan atau Tolak. Pilihan ini mengizinkan atau menolak akses berdasarkan syarat yang Anda pilih pada langkah berikut.
7. Untuk Aturan ini berlaku untuk permintaan yang... , pilih kondisi yang akan diterapkan pada aturan, seperti apakah akan menyertakan atau mengecualikan protokol tertentu, alamat IP, atau pengguna, atau peran peniruan identitas.
8. (Opsional) Jika Anda memasukkan rentang alamat IP, pengguna, atau peran peniruan identitas, pilih Tambahkan untuk menambahkannya ke aturan.
9. Pilih Buat aturan.

Mengedit aturan kontrol akses

Edit aturan kontrol akses baru dan default dari WorkMail konsol Amazon.

Untuk mengedit aturan kontrol akses

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Pilih Aturan kontrol akses.
4. Pilih aturan untuk diedit.
5. Pilih Edit aturan.
6. Mengedit deskripsi, efek, dan syarat, sesuai kebutuhan.
7. Pilih Simpan perubahan.

Important

Bila Anda mengubah aturan akses, kotak pesan yang terpengaruh dapat memakan waktu lima menit untuk mengikuti aturan yang diperbarui. Klien yang mengakses kotak pesan yang terpengaruh mungkin menunjukkan perilaku yang tidak konsisten selama waktu tersebut. Namun, Anda akan segera melihat perilaku yang benar ketika Anda menguji aturan Anda. Untuk informasi selengkapnya tentang aturan pengujian, lihat langkah-langkah di bagian berikutnya.

Menguji aturan kontrol akses

Untuk melihat bagaimana aturan kontrol akses organisasi Anda diterapkan, uji aturan dari WorkMail konsol Amazon.

Untuk menguji aturan kontrol akses untuk organisasi Anda

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Pilih Aturan kontrol akses.
4. Pilih Aturan pengujian.
5. Untuk Konteks permintaan, pilih protokol yang akan diuji.
6. Untuk Alamat IP sumber, masukkan alamat IP yang akan diuji.
7. Untuk Permintaan yang dilakukan oleh, pilih peran Pengguna atau Peniruan Identitas yang akan diuji.
8. Pilih peran Pengguna atau Peniruan identitas yang akan diuji.
9. Pilih Uji.

Hasil pengujian muncul di bawah Efek.

Menghapus aturan kontrol akses

Hapus aturan kontrol akses yang tidak lagi Anda perlukan dari WorkMail konsol Amazon.

Warning

Jika administrator menghapus semua aturan kontrol akses untuk organisasi, Amazon WorkMail memblokir semua akses ke kotak pesan organisasi.

Untuk menghapus aturan kontrol akses

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Pilih Aturan kontrol akses.
4. Pilih aturan yang akan dihapus.

5. Pilih Hapus aturan.
6. Pilih Hapus.

Mengatur kebijakan penyimpanan kotak pesan

Anda dapat menyetel kebijakan penyimpanan kotak pesan untuk WorkMail organisasi Amazon Anda. Kebijakan penyimpanan otomatis menghapus pesan e-mail dari kotak pesan pengguna setelah jangka waktu yang Anda pilih. Anda dapat memilih folder kotak pesan mana yang akan diterapkan kebijakan penyimpanan. Selain itu, Anda dapat memilih apakah akan menetapkan kebijakan penyimpanan yang berbeda untuk folder yang berbeda. Kebijakan penyimpanan kotak pesan berlaku untuk folder yang dipilih di semua kotak pesan pengguna di organisasi Anda. Pengguna tidak dapat mengganti kebijakan retensi.

Untuk menyetel kebijakan penyimpanan kotak pesan

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Pilih Kebijakan penyimpanan.
4. Untuk Tindakan folder, di samping setiap folder kotak pesan yang ingin Anda sertakan dalam kebijakan, pilih Hapus atau Hapus permanen.
5. Masukkan jumlah hari untuk menyimpan pesan email di setiap folder kotak pesan sebelum menghapusnya.
6. Pilih Simpan.

Biarkan 48 jam untuk menerapkan kebijakan penyimpanan untuk organisasi Anda. Jika Anda memilih tindakan Hapus folder, pengguna dapat memulihkan pesan email yang dihapus dari aplikasi WorkMail web Amazon dan klien yang didukung. Jika Anda memilih tindakan Hapus folder secara permanen, pesan email tidak dapat dipulihkan setelah dihapus.

Jumlah hari kebijakan penyimpanan menyimpan item didasarkan pada saat item dibuat, dimodifikasi, atau dipindahkan. Misalnya, jika kebijakan penyimpanan menghapus item setelah satu tahun, kebijakan tersebut menghitung hari penyimpanan sejak tanggal Anda membuat atau terakhir

mengambil tindakan pada item tersebut. Hal ini tidak terpengaruh oleh tanggal Anda menerapkan kebijakan retensi.

Bekerja dengan domain

Anda dapat mengonfigurasi Amazon WorkMail untuk menggunakan domain khusus. Anda juga dapat menjadikan domain sebagai default untuk organisasi Anda, dan mengaktifkan AutoDiscover untuk Microsoft Outlook.

Topik

- [Menambahkan domain](#)
- [Menghapus domain](#)
- [Memilih domain default](#)
- [Memverifikasi domain](#)
- [Mengaktifkan AutoDiscover untuk mengkonfigurasi titik akhir](#)
- [Mengedit kebijakan identitas domain](#)
- [Mengautentikasi Email dengan SPF](#)
- [Mengkonfigurasi domain PESAN DARI kustom](#)

Menambahkan domain

Anda dapat menambahkan hingga 100 domain ke WorkMail organisasi Amazon Anda. Ketika Anda menambahkan domain baru, Amazon Simple Email Service (Amazon SES) yang mengirim kebijakan otorisasi secara otomatis ditambahkan ke kebijakan identitas domain. Ini WorkMail memberi Amazon akses ke semua tindakan pengiriman Amazon SES untuk domain Anda dan memungkinkan Anda mengarahkan email ke domain Anda. Anda juga dapat mengarahkan email ke domain eksternal.

Note

Sebagai praktik terbaik, Anda harus menambahkan alias untuk <postmaster@> dan <abuse@> ke semua domain Anda. Anda dapat membuat grup distribusi untuk alias ini jika Anda ingin pengguna tertentu di organisasi Anda menerima email yang dikirim ke alias ini.


Saat mengonfigurasi WorkMail organisasi Amazon dengan domain khusus, ingatlah hal berikut tentang catatan DNS domain Anda:

- Untuk data MX dan autodiscover CNAME, sebaiknya atur nilai Time to Live (TTL) ke 3600. Mengurangi TTL memastikan bahwa server email Anda tidak menggunakan data MX yang sudah ketinggalan zaman atau tidak valid setelah memperbarui catatan tersebut atau memigrasi kotak pesan Anda.
- Setelah membuat pengguna dan grup distribusi, lalu berhasil memigrasi kotak pesan, Anda harus memperbarui data MX untuk mulai meneruskan email ke Amazon. WorkMail Pembaruan catatan DNS dapat memakan waktu hingga 48 jam untuk diproses.
- Beberapa penyedia DNS secara otomatis menambahkan nama domain ke ujung catatan DNS. Menambahkan catatan yang sudah berisi nama domain, seperti `_amazonses.example.com`, dapat mengakibatkan duplikasi nama domain, menghasilkan `_amazonses.example.com.example.com`. Untuk menghindari duplikasi nama domain, tambahkan titik di akhir nama domain di catatan DNS. Ini menunjukkan kepada penyedia DNS Anda bahwa nama rekaman sepenuhnya memenuhi syarat dan tidak lagi relatif terhadap nama domain. Hal ini juga mencegah penyedia DNS menambahkan nama domain tambahan.
- Nama rekaman yang disalin termasuk nama domain. Tergantung pada layanan DNS yang Anda gunakan, nama domain mungkin sudah ditambahkan ke catatan DNS domain.
- Setelah Anda membuat catatan DNS, pilih ikon penyegaran di WorkMail konsol Amazon untuk melihat status verifikasi dan nilai rekaman. Untuk informasi selengkapnya tentang memverifikasi domain, lihat [Memverifikasi domain](#).
- Kami menyarankan Anda mengonfigurasi domain Anda sebagai MAIL FROM domain. AutoDiscover Untuk mengaktifkan perangkat iOS, Anda harus mengonfigurasi domain Anda sebagai MAIL FROM domain. Anda dapat melihat status MAIL FROM domain Anda di bagian Tingkatkan kemampuan pengiriman konsol. Untuk informasi selengkapnya, lihat [Mengkonfigurasi domain PESAN DARI kustom](#).

Untuk menambahkan domain

1. Masuk ke Konsol Manajemen AWS dan buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.
2. Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

3. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi yang ingin Anda tambahkan domain.
4. Di panel navigasi, pilih Domain, lalu pilih Tambah domain.
5. Pada layar Tambahkan domain, masukkan nama domain. Nama domain hanya dapat berisi karakter Latin Dasar (ASCII).

 Note

Jika Anda memiliki domain yang dikelola di zona host publik Amazon Route 53, Anda dapat memilihnya dari menu tarik-turun yang muncul saat Anda memasukkan nama domain.

6. Pilih Tambahkan domain.

Sebuah halaman muncul dan mencantumkan catatan DNS untuk domain baru. Halaman mengelompokkan catatan ke dalam bagian berikut:

- Kepemilikan domain
- WorkMail konfigurasi
- Keamanan yang ditingkatkan
- Peningkatan pengiriman email

Masing-masing bagian ini berisi satu atau beberapa catatan DNS, dan setiap catatan menampilkan nilai Status. Daftar berikut menunjukkan catatan dan nilai status yang tersedia.

Kepemilikan TXT

Terverifikasi - Rekam diselesaikan dan diverifikasi.

Tertunda — Rekam belum diverifikasi.

Gagal — Tidak dapat memverifikasi kepemilikan. Catatan tidak cocok atau tidak terjangkau.

Konfigurasi MX WorkMail

Terverifikasi - Rekam diselesaikan dan diverifikasi.

Hilang - Tidak dapat menyelesaikan catatan.

Tidak konsisten — Nilai tidak sesuai dengan catatan yang diharapkan.

AutoDiscover

Terverifikasi - Rekam diselesaikan dan diverifikasi.

Hilang - Tidak dapat menyelesaikan catatan.

Tidak konsisten — Nilai tidak sesuai dengan catatan yang diharapkan.

Note

Proses AutoDiscover verifikasi juga memeriksa AutoDiscover pengaturan yang benar. Proses memverifikasi pengaturan konfigurasi untuk setiap fase. Tanda centang hijau muncul di samping Terverifikasi di kolom Status saat verifikasi selesai. Anda dapat mengarahkan kursor ke Verified dan melihat fase mana yang telah diverifikasi oleh proses. Untuk informasi lebih lanjut tentang AutoDiscover fase, lihat [Mengaktifkan AutoDiscover untuk mengkonfigurasi titik akhir](#).

DKIM CNAME

Terverifikasi - Rekam diselesaikan dan diverifikasi.

Tertunda - Rekam belum diverifikasi

Gagal — Tidak dapat memverifikasi kepemilikan. Catatan tidak cocok atau tidak terjangkau.

Untuk informasi selengkapnya tentang penandatanganan DKIM, lihat [Mengautentikasi email dengan DKIM di Amazon SES](#) di Panduan Pengembang Layanan Email Sederhana Amazon.

SPF TXT

Terverifikasi - Rekam diselesaikan dan diverifikasi.

Hilang - Tidak dapat menyelesaikan catatan.

Tidak konsisten — Nilai tidak sesuai dengan catatan yang diharapkan.

Untuk informasi selengkapnya tentang verifikasi SPF, lihat [Mengautentikasi Email dengan SPF](#).

DMARC TXT

Terverifikasi - Rekam diselesaikan dan diverifikasi.

Hilang - Tidak dapat menyelesaikan catatan.

Tidak konsisten — Nilai tidak sesuai dengan catatan yang diharapkan

Untuk informasi selengkapnya tentang catatan DMARC di Amazon WorkMail, lihat [Mematuhi DMARC menggunakan Amazon SES](#) di Panduan Pengembang Layanan Email Sederhana Amazon.

TXT MAIL DARI domain

Terverifikasi - Rekam diselesaikan dan diverifikasi.

Tertunda — Rekam belum diverifikasi.

Gagal — Tidak dapat memverifikasi kepemilikan. Catatan tidak cocok atau tidak terjangkau.

MX MAIL DARI domain

Terverifikasi - Rekam diselesaikan dan diverifikasi.

Hilang - Tidak dapat menyelesaikan catatan.

Tidak konsisten — Nilai tidak sesuai dengan catatan yang diharapkan.

7. Untuk langkah selanjutnya, pilih tindakan yang sesuai berdasarkan penyedia DNS yang Anda gunakan.

Jika Anda menggunakan domain Route 53

- Di bagian atas halaman, pilih Perbarui semua di Rute 53.

Jika Anda menggunakan penyedia DNS lain

- Salin catatan dan tempel ke penyedia DNS Anda. Anda dapat menyalin catatan dalam jumlah besar atau satu per satu. Untuk menyalin catatan secara massal, pilih Salin semua. Itu membuat zona file yang dapat Anda impor ke penyedia DNS Anda. Untuk menyalin catatan satu per satu, pilih kotak yang tumpang tindih di sebelah nama rekaman, lalu tempel masing-masing ke penyedia DNS Anda.

8. Pilih ikon penyegaran, perbarui Status untuk setiap rekaman. Ini memverifikasi kepemilikan domain dan konfigurasi domain Anda yang tepat dengan Amazon WorkMail.

Menghapus domain

Bila Anda tidak lagi memerlukan domain, Anda dapat menghapusnya. Namun, Anda harus terlebih dahulu menghapus setiap individu atau grup yang menggunakan domain sebagai alamat email mereka.

Untuk menghapus domain

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Nama Wilayah dan titik akhir](#) di. Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Dalam daftar domain, pilih kotak centang di samping nama domain, lalu pilih Hapus.
4. Dalam kotak dialog Hapus domain, masukkan nama domain yang akan dihapus dan pilih Hapus.

Memilih domain default

Anda dapat menjadikan domain yang terkait dengan organisasi Anda sebagai default untuk pengguna dan grup di organisasi tersebut. Membuat domain default tidak mengubah alamat email yang ada.

Untuk menjadikan domain sebagai default

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Nama Wilayah dan titik akhir](#) di. Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Dalam daftar domain, pilih kotak centang di sebelah nama domain yang ingin Anda gunakan dan pilih Tetapkan sebagai default.

Memverifikasi domain

Anda harus memverifikasi domain Anda setelah menambahkannya di WorkMail konsol Amazon. Memverifikasi domain mengonfirmasi bahwa Anda memiliki domain dan akan menggunakan Amazon WorkMail sebagai layanan email untuk domain tersebut.

Anda memverifikasi domain dengan menambahkan data TXT dan MX ke dalam layanan DNS Anda. Catatan TXT memungkinkan Anda menambahkan catatan ke layanan DNS Anda. Catatan MX menentukan server email masuk.

Anda menggunakan konsol Amazon SES untuk membuat catatan TXT dan MX, lalu Anda menggunakan WorkMail konsol Amazon untuk menambahkan catatan ke layanan DNS Anda. Ikuti langkah-langkah ini.

Untuk membuat catatan TXT dan MX

1. Buka konsol Amazon SES di <https://console.aws.amazon.com/ses/>.
2. Di panel navigasi, pilih Domain, lalu pilih Verifikasi Domain Baru.

Kotak dialog Verifikasi Domain Baru muncul.

3. Di kotak Domain, masukkan nama domain yang Anda buat di [Menambahkan domain](#) bagian tersebut.
4. (Opsional) Jika Anda ingin menggunakan DomainKeys Identified Mail (DKIM), pilih kotak centang Hasilkan Pengaturan DKIM.
5. Pilih Verifikasi Domain Ini.

Konsol menampilkan daftar catatan TXT dan MX.

6. Pilih tautan Unduh Rekam Set sebagai CSV, yang terletak di bawah daftar TXT.

Kotak dialog Save As muncul. Pilih lokasi untuk unduhan, lalu pilih Simpan.

7. Buka file CSV yang diunduh dan salin semua isinya.

Setelah Anda membuat catatan TXT dan MX, Anda kemudian menambahkannya ke penyedia DNS Anda. Langkah-langkah berikut menggunakan Route 53. Jika Anda menggunakan penyedia DNS yang berbeda dan Anda tidak tahu cara menambahkan catatan, lihat dokumentasi penyedia Anda.

1. Masuk ke Konsol Manajemen AWS dan buka konsol Route 53 di <https://console.aws.amazon.com/route53/>.
2. Pada panel navigasi, pilih Zona yang Di-hosting. Kemudian, pilih tombol radio di sebelah domain yang ingin Anda verifikasi.
3. Dari daftar catatan DNS untuk domain Anda, pilih Impor file zona.
4. Di bawah file Zone, tempel catatan yang disalin ke dalam kotak teks. Daftar file muncul di bawah kotak teks.
5. Gulir ke bawah ke akhir daftar dan pilih Impor.

Note

Biarkan hingga 72 jam untuk menyelesaikan proses verifikasi.

Memverifikasi catatan TXT dan catatan MX dengan layanan DNS

Mengkonfirmasi bahwa catatan TXT yang memverifikasi bahwa Anda memiliki domain ditambahkan dengan benar ke layanan DNS Anda. Prosedur ini menggunakan alat [nslookup](#), yang tersedia untuk Windows dan Linux. Di Linux, Anda juga dapat menggunakan [dig](#).

Untuk menggunakan nslookup alat ini, Anda harus terlebih dahulu menemukan server DNS yang melayani domain Anda. Kemudian, Anda menanyakan server tersebut untuk melihat catatan TXT. Anda dapat menanyakan server DNS untuk domain Anda karena server tersebut berisi informasi terbaru untuk domain Anda. Informasi ini dapat membutuhkan waktu lama untuk disebarkan ke server DNS lainnya.

Gunakan nslookup untuk memverifikasi bahwa catatan TXT Anda ditambahkan ke layanan DNS Anda

1. Temukan server nama domain Anda:
 - a. Buka prompt perintah (Windows) atau terminal (Linux).
 - b. Jalankan perintah berikut untuk mencantumkan semua server nama yang melayani domain Anda. Ganti *example.com* dengan domain Anda.

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

Anda akan menanyakan salah satu server nama ini di langkah berikutnya.

2. Verifikasi bahwa catatan Amazon WorkMail TXT ditambahkan dengan benar.
 - a. Jalankan perintah berikut, ganti *example.com* dengan domain Anda, dan *ns1.name-server.net* dengan server nama dari Langkah 1.

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

- b. Tinjau "text =" string yang ditunjukkan pada output darinslookup. Konfirmasikan bahwa string ini cocok dengan nilai TXT untuk domain Anda dalam daftar Pengirim Terverifikasi di konsol Amazon. WorkMail

Dalam contoh berikut, Anda ingin melihat catatan TXT untuk `_amazonses.example.com` dengan nilai `fmxqxT/ic0Yx4aA/bEUrDPMeax9/s3friblS+niixmqk=`. Jika Anda memperbarui catatan dengan benar, perintah memiliki output berikut:

```
_amazonses.example.com text = "fmxqxT/ic0Yx4aA/bEUrDPMeax9/s3friblS+niixmqk="
```

Gunakan `dig` untuk memverifikasi bahwa catatan TXT Anda ditambahkan ke layanan DNS Anda

1. Buka sesi terminal.
2. Jalankan perintah berikut untuk menampilkan daftar catatan TXT untuk domain Anda. Ganti *example.com* dengan domain Anda.

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

3. Verifikasi bahwa string yang mengikuti TXT output perintah cocok dengan nilai TXT yang Anda lihat saat memilih domain dalam daftar Pengirim Terverifikasi di konsol Amazon. WorkMail

Untuk menggunakan `nslookup` untuk memverifikasi bahwa catatan MX Anda ditambahkan ke layanan DNS

1. Temukan server nama untuk domain Anda:
 - a. Buka prompt perintah.
 - b. Jalankan perintah berikut untuk mencantumkan semua server nama untuk domain Anda.

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

Anda akan menanyakan salah satu server nama ini di langkah berikutnya.

2. Verifikasi bahwa catatan MX ditambahkan dengan benar:
 - a. Jalankan perintah berikut, ganti *example.com* dengan domain Anda dan *ns1.name-server.net* dengan salah satu server nama yang Anda identifikasi pada langkah sebelumnya..


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

- b. Dalam output perintah, verifikasi bahwa string yang mengikuti `mail exchange =` cocok dengan salah satu nilai berikut:

Wilayah AS Timur (Virginia N.) — `10 inbound-smtp.us-east-1.amazonaws.com`

Wilayah AS Barat (Oregon) — `10 inbound-smtp.us-west-2.amazonaws.com`

Wilayah Eropa (Irlandia) — `10 inbound-smtp.eu-west-1.amazonaws.com`

 Note

`10` mewakili nomor preferensi MX atau prioritas.

Gunakan `dig` untuk memverifikasi bahwa data MX Anda ditambahkan ke layanan DNS Anda

1. Buka sesi terminal.
2. Jalankan perintah berikut untuk menampilkan catatan MX untuk domain yang tepat.

```
dig +short example.com mx
```

3. Verifikasi bahwa string yang mengikuti MX cocok dengan salah satu nilai berikut:

Wilayah AS Timur (Virginia N.) — `10 inbound-smtp.us-east-1.amazonaws.com`

Wilayah AS Barat (Oregon) — `10 inbound-smtp.us-west-2.amazonaws.com`

Wilayah Eropa (Irlandia) — `10 inbound-smtp.eu-west-1.amazonaws.com`

 Note

10 mewakili nomor preferensi MX atau prioritas.

Pemecahan masalah verifikasi domain

Untuk memecahkan masalah umum dengan verifikasi domain, lihat saran berikut:

Layanan DNS Anda tidak mengizinkan garis bawah dalam nama catatan TXT

Hilangkan `_amazonses` dari nama catatan TXT.

Anda ingin memverifikasi domain yang sama beberapa kali tetapi tidak dapat memiliki beberapa catatan TXT dengan nama yang sama

Jika layanan DNS Anda tidak mengizinkan Anda memiliki beberapa catatan TXT dengan nama yang sama, gunakan salah satu solusi berikut:

- (Disarankan) Jika layanan DNS Anda mengizinkannya, tetapkan beberapa nilai ke catatan TXT. Misalnya, jika DNS Anda dikelola oleh Amazon Route 53, Anda dapat mengatur beberapa nilai untuk catatan TXT yang sama sebagai berikut:
 1. Di konsol Route 53, pilih catatan TXT `_amazonses` yang ditambahkan saat Anda memverifikasi domain di Wilayah pertama.
 2. Untuk Nilai, tekan Masukkan setelah nilai pertama.
 3. Tambahkan nilai untuk Wilayah tambahan, dan simpan kumpulan catatan.
- Jika Anda hanya perlu memverifikasi domain Anda dua kali, Anda dapat memverifikasinya sekali dengan membuat catatan TXT dengan `_amazonses` nama, dan kemudian membuat catatan lain tanpa `_amazonses` nama rekaman.

WorkMail Konsol Amazon melaporkan bahwa verifikasi domain telah gagal

Amazon tidak WorkMail dapat menemukan catatan TXT yang diperlukan untuk layanan DNS Anda. Verifikasi bahwa catatan TXT yang diperlukan ditambahkan dengan benar ke layanan DNS Anda dengan mengikuti prosedur di [Memverifikasi catatan TXT dan catatan MX dengan layanan DNS](#)

Penyedia DNS Anda menambahkan nama domain ke akhir catatan TXT

Menambahkan catatan TXT yang sudah berisi nama domain, seperti `_amazonses.example.com`, dapat mengakibatkan duplikasi nama domain, seperti `_amazonses.example.com.example.com`. Untuk menghindari duplikasi nama domain dalam nama catatan, tambahkan periode ke akhir nama domain dalam catatan TXT. Ini menunjukkan kepada penyedia DNS Anda bahwa nama rekaman sepenuhnya memenuhi syarat dan sudah memiliki nama domain yang disertakan dalam catatan TXT.

Amazon WorkMail melaporkan bahwa catatan MX tidak konsisten

Saat bermigrasi dari server email yang ada, data MX mungkin menampilkan status Inconsistent. Perbarui data MX Anda untuk menunjuk ke Amazon WorkMail alih-alih menunjuk ke server email Anda sebelumnya. Catatan MX juga dikembalikan sebagai tidak konsisten ketika proxy email pihak ketiga digunakan bersama dengan Amazon. WorkMail Jika hal ini terjadi, aman untuk mengabaikan peringatan Tidak konsisten.

Mengaktifkan AutoDiscover untuk mengkonfigurasi titik akhir

AutoDiscover memungkinkan Anda untuk mengkonfigurasi Microsoft Outlook dan klien seluler dengan hanya menggunakan alamat email dan kata sandi Anda. Layanan ini mempertahankan koneksi ke Amazon WorkMail dan memperbarui pengaturan lokal setiap kali Anda mengubah titik akhir atau pengaturan. Selain itu, AutoDiscover memungkinkan klien Anda untuk menggunakan WorkMail fitur Amazon tambahan, seperti Buku Alamat Offline, Out-of-Office Asisten, dan kemampuan untuk melihat free/busy waktu di Kalender.

Klien melakukan AutoDiscover tahapan berikut untuk mendeteksi URL endpoint server:

- Fase 1 — Klien melakukan pencarian Secure Copy Protocol (SCP) terhadap Active Directory lokal. Jika klien Anda tidak bergabung dengan domain, AutoDiscover lewati langkah ini.
- Fase 2 — Klien mengirimkan permintaan ke URL berikut dan memvalidasi hasilnya. Endpoint ini hanya tersedia menggunakan HTTPS.
 - `https://company.tld/autodiscover/autodiscover.xml`
 - `https://autodiscover.company.tld/autodiscover/autodiscover.xml`
- Fase 3 - Klien melakukan pencarian DNS ke `autodiscover.company.tld` dan mengirimkan permintaan GET yang tidak diautentikasi ke titik akhir turunan dari alamat email pengguna. Jika

server mengembalikan pengalihan 302, klien mengirim ulang AutoDiscover permintaan terhadap titik akhir HTTPS yang dikembalikan.

Jika semua fase ini gagal, klien tidak dapat dikonfigurasi secara otomatis. Untuk informasi tentang mengonfigurasi perangkat seluler secara manual, lihat [Menyambungkan perangkat secara manual](#).

Anda diminta untuk menambahkan data AutoDiscover DNS ke penyedia Anda ketika Anda menambahkan domain Anda ke Amazon. WorkMail Hal ini memungkinkan klien untuk melakukan fase 3 dari AutoDiscover proses. Namun, langkah-langkah ini tidak berfungsi untuk semua perangkat seluler, seperti aplikasi email Android stok. Akibatnya, Anda mungkin perlu mengatur AutoDiscover fase 2 secara manual.

Anda dapat menggunakan metode berikut untuk menyiapkan AutoDiscover fase 2 untuk domain Anda:

(Disarankan) Gunakan Route 53 dan Amazon CloudFront

Note


Langkah-langkah berikut menjelaskan cara membuat proxy untuk `https://autodiscover.company.tld/autodiscover/.xml`. Untuk membuat proxy untuk `https://company.tld/autodiscover/autodiscover.xml`, hapus `autodiscover.` awalan dari domain dalam langkah-langkah berikut.

Menggunakan CloudFront dan Rute 53 dapat dikenakan biaya. Untuk informasi selengkapnya tentang harga yang berlaku, lihat [CloudFront harga Amazon dan harga Amazon Route 53](#).

Untuk mengaktifkan AutoDiscover fase 2 dengan Route 53 dan CloudFront


1. Dapatkan sertifikat SSL untuk penemuan otomatis. *company.tld* dan mengunggahnya ke AWS Identity and Access Management (IAM) atau AWS Certificate Manager. Untuk informasi selengkapnya, lihat [Bekerja dengan sertifikat server](#) di Panduan Pengguna IAM, atau [Memulai](#) di Panduan Pengguna AWS Certificate Manager .
2. Buat CloudFront distribusi baru:
 1. Buka CloudFront konsol di <https://console.aws.amazon.com/cloudfront/v4/home>.
 2. Di panel navigasi, pilih Distribusi.

3. Pilih Buat Distribusi.
4. Di bawah Web, pilih Memulai.
5. Di Pengaturan Asal, masukkan nilai berikut:
 - Nama Domain Asal — Nama domain yang sesuai untuk Wilayah Anda:
 - AS Timur (Virginia N.) - **autodiscover-service.mail.us-east-1.awsapps.com**
 - AS Barat (Oregon) — **autodiscover-service.mail.us-west-2.awsapps.com**
 - Eropa (Irlandia) — **autodiscover-service.mail.eu-west-1.awsapps.com**
 - Kebijakan Protokol Asal — Kebijakan yang diinginkan: **Match Viewer**

 Note

Biarkan jalur Origin kosong. Jangan ubah nilai yang diisi otomatis untuk Origin ID.

6. Di Pengaturan Perilaku Cache Default, pilih nilai berikut untuk pengaturan yang tercantum:
 - Kebijakan Protokol Penampil: HTTPS Saja
 - Metode HTTP yang diizinkan: GET, HEAD, OPTIONS, PUT, PATCH, POST dan DELETE
 - Cache Berdasarkan Header Permintaan yang Dipilih: Semua
 - Teruskan Cookies: Semua
 - Pencarian String Forwarding dan Caching: Tidak ada (Tingkatkan Caching)
 - Streaming yang Lancar: Tidak
 - Batasi Akses Penampil: Tidak
7. Pilih nilai berikut untuk Pengaturan Distribusi:
 - Kelas Harga: Gunakan hanya AS, Kanada, dan Eropa
 - Untuk Nama Domain Alternatif (CNames), masukkan **autodiscover.company.tld** atau **company.tld**, di **company.tld** mana nama domain Anda.
 - Sertifikat SSL: Sertifikat SSL Kustom (disimpan dalam IAM)
 - Support Klien SSL Kustom: Pilih Semua Klien atau Hanya Klien yang Support Indikasi Nama Server (SNI). Versi Android yang lebih lama mungkin tidak berfungsi dengan pilihan yang kedua.


 Note

Jika Anda memilih Semua Klien, kosongkan Objek Root Default.

- Pencatatan: Pilih Hidup atau Mati. Aktif memungkinkan pencatatan.
- Untuk Komentar, masukkan **AutoDiscover type2 for autodiscover.company.tld**
- Status Distribusi: pilih Diaktifkan.

8. Pilih Buat Distribusi.

3. Di konsol Route 53, buat catatan yang merutekan lalu lintas internet untuk nama domain Anda ke CloudFront distribusi Anda.

 Note

Langkah-langkah ini mengasumsikan bahwa catatan DNS untuk example.com di-host di Route 53. Jika Anda tidak menggunakan Route 53, ikuti prosedur di konsol manajemen penyedia DNS Anda.

1. Di panel navigasi konsol, pilih Zona yang Dihosting. Lalu pilih domain.
2. Dalam daftar domain, pilih nama domain yang ingin Anda gunakan.
3. Di Rekaman, pilih Buat catatan.
4. Di bawah Quick create record, atur parameter berikut:
 - Di bawah Nama Rekam, masukkan nama untuk catatan.
 - Di bawah Kebijakan perutean, pilih Perutean sederhana.
 - Pilih slider Alias untuk menyalakannya. Slider berubah menjadi biru saat dalam keadaan aktif.
 - Dalam daftar jenis Rekam, pilih A - Rute lalu lintas ke alamat IPv4 dan beberapa sumber daya AWS.
 - Dalam Rute lalu lintas ke daftar, pilih Alias untuk CloudFront didistribusikan.
 - Sebuah kotak pencarian akan muncul di bawah Rute lalu lintas ke daftar. Masukkan nama CloudFront distribusi Anda ke dalam kotak teks. Anda juga dapat memilih distribusi Anda dari daftar yang muncul ketika Anda memilih kotak pencarian.

5. Pilih Buat catatan.

Menggunakan server web Apache

Langkah-langkah berikut menjelaskan cara menggunakan server web Apache untuk membuat proxy `https://autodiscover.company.tld/autodiscover/autodiscover.xml`. Untuk membuat proxy untuk `https://company.tld/autodiscover/autodiscover.xml`, hapus "autodiscover." Prefiks dari domain di langkah-langkah berikut.

Untuk mengaktifkan AutoDiscover fase 2 dengan server web Apache

1. Jalankan arahan berikut di server SSL-enabled Apache:

```
SSLProxyEngine on ProxyPass /autodiscover/autodiscover.xml https://autodiscover-  
service.mail.REGION.awsapps.com/autodiscover/autodiscover.xml
```

2. Sesuai kebutuhan, aktifkan modul Apache berikut. Jika Anda tidak tahu caranya, lihat bantuan Apache:

- `proxy`
- `proxy_http`
- `socache_shmcb`
- `ssl`

Lihat bagian berikut untuk informasi tentang pengujian dan pemecahan masalah AutoDiscover.

AutoDiscover pemecahan masalah fase 2

Setelah mengonfigurasi penyedia DNS Anda AutoDiscover, Anda dapat menguji konfigurasi AutoDiscover titik akhir Anda. Jika Anda telah mengonfigurasi titik akhir dengan benar, titik akhir akan merespons dengan pesan permintaan yang tidak sah.

Untuk membuat permintaan dasar yang tidak sah

1. Dari terminal, buat permintaan POST yang tidak diautentikasi ke titik akhir. AutoDiscover

```
$ curl -X POST -v https://autodiscover.'company.tld'/autodiscover/  
autodiscover.xml
```

Jika titik akhir Anda dikonfigurasi dengan benar, itu akan mengembalikan 401 unauthorized pesan, seperti yang ditunjukkan pada contoh berikut:

```
$ curl -X POST -v https://autodiscover.'company.tld'/autodiscover/autodiscover.xml
...
HTTP/1.1 401 Unauthorized
```

2. Selanjutnya, uji AutoDiscover permintaan nyata. Buat request.xml file dengan konten XML-berikut:

```
<?xml version="1.0" encoding="utf-8"?>

<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/requestschemata/2006">
  <Request>
    <EmailAddress>testuser@company.tld</EmailAddress>
    <AcceptableResponseSchema>
      http://schemas.microsoft.com/exchange/autodiscover/mobilesync/responseschemata/2006
    </AcceptableResponseSchema>
  </Request>
</Autodiscover>
```

3. Gunakan request.xml file yang Anda buat dan buat AutoDiscover permintaan yang diautentikasi ke titik akhir. Ingatlah untuk mengganti *testuser@company.tld* dengan alamat email yang valid:

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/autodiscover/autodiscover.xml
```

Respons akan terlihat mirip dengan contoh berikut jika titik akhir dikonfigurasi dengan benar:

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/autodiscover/autodiscover.xml

Enter host password for user 'testuser@company.tld':
<?xml version="1.0" encoding="UTF-8"?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschemata/2006" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/responseschema/2006">
  <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>
```

Mengedit kebijakan identitas domain

Kebijakan identitas domain menentukan izin untuk tindakan email, seperti mengarahkan pesan email. Misalnya, Anda dapat mengarahkan email ke alamat email apa pun di WorkMail organisasi Amazon Anda.

Note

Pada 1 April 2022, Amazon WorkMail mulai menggunakan prinsip layanan untuk otorisasi alih-alih kepala sekolah akun. AWS Jika Anda menambahkan domain sebelum 1 April 2022, Anda mungkin memiliki kebijakan lama yang menggunakan prinsipal AWS akun untuk otorisasi. Jika demikian, kami sarankan memperbarui ke kebijakan terbaru. Langkah-langkah di bagian ini menjelaskan caranya. Organisasi Anda terus mengirim email secara normal selama pembaruan.

Anda hanya mengikuti langkah-langkah ini jika Anda tidak menggunakan kebijakan Amazon SES khusus. Jika Anda menggunakan kebijakan Amazon SES khusus, Anda harus memperbaruinya

sendiri. Untuk informasi lebih lanjut, lihat [Kebijakan utama layanan Amazon SES khusus](#), nanti dalam topik ini.

Important

Jangan hapus domain yang ada. Jika Anda melakukannya, Anda akan mengganggu layanan email. Yang perlu Anda lakukan adalah memasukkan kembali domain yang ada.

Untuk memperbarui kebijakan identitas domain

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Untuk melakukannya, buka daftar Pilih wilayah, yang terletak di sebelah kanan kotak pencarian, lalu pilih wilayah yang diinginkan. Untuk informasi selengkapnya tentang wilayah, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Domain.
4. Sorot dan salin nama domain yang ingin Anda masukkan kembali, lalu pilih Tambah Domain.

Kotak dialog Add domain muncul.

5. Rekatkan nama yang disalin ke dalam kotak Nama domain, lalu pilih Tambah domain.
6. Ulangi langkah 3-5 untuk domain yang tersisa di organisasi Anda.

Kebijakan utama layanan Amazon SES khusus

Jika Anda menggunakan kebijakan Amazon SES khusus, sesuaikan contoh ini untuk digunakan di domain Anda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuthorizeWorkMail",
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "workmail.REGION.amazonaws.com"
    },
    "Action": [
        "ses:*"
    ],
    "Resource": "arn:aws:ses:us-east-1:111122223333:identity/WORKMAIL-
DOMAIN-NAME",
    "Condition": {
        "ArnEquals": {
            "aws:SourceArn": "arn:aws:workmail:us-
east-1:111122223333:organization/WORKMAIL_ORGANIZATION_ID"
        }
    }
}
]
```

Mengautentikasi Email dengan SPF

Kerangka Kerja Kebijakan Pengirim (SPF) adalah standar validasi email yang dirancang untuk memerangi pemalsuan email. Spoofing adalah tindakan membuat email yang dikirim oleh aktor jahat terlihat seperti yang dikirim oleh pengguna yang sah. Untuk informasi tentang mengonfigurasi SPF untuk WorkMail-enabled domain Amazon Anda, lihat [Mengautentikasi email dengan SPF di Amazon SES](#).

Mengkonfigurasi domain PESAN DARI kustom

Secara default, Amazon WorkMail menggunakan subdomain amazonses.com sebagai MAIL FROM domain untuk email keluar Anda. Hal ini dapat menyebabkan kegagalan pengiriman jika kebijakan DMARC pada domain Anda hanya diatur untuk SPF. Untuk mengatasi hal ini, konfigurasi domain Anda sendiri sebagai domain MAIL FROM. Untuk mempelajari cara mengatur domain email Anda sebagai domain MAIL FROM, lihat [Mengatur domain PESAN DARI kustom](#) di Panduan Developer Amazon Simple Email Service.

Important

Domain MAIL FROM kustom diperlukan saat Anda mengaktifkan AutoDiscover untuk perangkat iOS.

Untuk informasi selengkapnya tentang MAIL FROM domain kustom, lihat [Amazon SES sekarang mendukung domain MAIL FROM kustom](#).

Bekerja dengan pengguna

Anda dapat membuat dan menghapus pengguna dari Amazon WorkMail. Selain itu, Anda dapat mengatur ulang kata sandi email, mengelola kuota kotak pesan dan akses perangkat, serta mengontrol izin kotak pesan mereka.

Topik

- [Melihat daftar pengguna](#)
- [Menambahkan pengguna](#)
- [Mengaktifkan pengguna](#)
- [Mengelola alias pengguna](#)
- [Menonaktifkan pengguna](#)
- [Mengedit detail pengguna](#)
- [Mengatur ulang kata sandi pengguna](#)
- [Memecahkan masalah kebijakan kata sandi Amazon WorkMail](#)
- [Bekerja dengan notifikasi](#)
- [Mengaktifkan email yang ditandatangani atau dienkripsi](#)


Melihat daftar pengguna

Untuk melihat daftar pengguna

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Users (Pengguna).
4. Selain itu, Anda dapat memfilter pengguna berdasarkan Nama Pengguna, Nama tampilan, atau alamat email utama.

 Note

Pencarian peka huruf besar/kecil.

Menambahkan pengguna

Saat Anda menambahkan pengguna, Amazon WorkMail secara otomatis membuat kotak pesan untuk mereka. Pengguna dapat masuk dan mengakses email mereka dari aplikasi WorkMail web Amazon, perangkat seluler mereka, atau dengan menggunakan Microsoft Outlook di macOS atau PC.

Untuk menambahkan pengguna

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih organisasi yang ingin Anda tambahkan pengguna.
3. Di panel navigasi, pilih Pengguna, lalu pilih Tambah Pengguna.

Layar Tambahkan pengguna muncul.

4. Di bawah Rincian pengguna, di bidang Nama pengguna, masukkan nama pengguna. Nama juga muncul di kotak Alamat email. Jika Anda ingin pengguna memiliki alamat email yang berbeda dari nama pengguna mereka, Anda dapat mengedit bidang Alamat email.
5. (Opsional) Masukkan nama depan dan belakang pengguna di kotak Nama depan dan Nama belakang.
6. Di kotak Nama tampilan, masukkan nama tampilan pengguna.
7. Di kotak Alamat email, terima alias email atau masukkan yang lain.
8. Secara default, pengguna ditampilkan dalam daftar alamat global. Untuk menyembunyikan pengguna dari daftar alamat global, kosongkan kotak centang Tampilkan di daftar alamat global.
9. Pilih Jangan buat kotak pesan untuk menambahkan pengguna sebagai pengguna jarak jauh ke organisasi.

10. Di bawah Pengaturan kata sandi, masukkan kata sandi pengguna di kotak Kata Sandi dan Ulangi kata sandi.
11. Pilih Tambahkan pengguna.

Mengaktifkan pengguna

Ketika Anda mengintegrasikan Amazon WorkMail dengan Active Directory perusahaan Anda, atau Anda sudah memiliki pengguna yang tersedia di direktori Simple AD Anda, Anda dapat mengaktifkan pengguna tersebut di Amazon WorkMail. Anda juga mengikuti langkah-langkah ini untuk mengaktifkan kembali pengguna yang akunnya dinonaktifkan.

Untuk mengaktifkan pengguna

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih organisasi yang ingin Anda aktifkan pengguna.
3. Di panel navigasi, pilih Users (Pengguna).

Daftar pengguna muncul. Akun pengguna dalam status pengguna yang diaktifkan, dinonaktifkan, dan sistem ditampilkan dalam daftar.

4. Dari daftar pengguna dengan akun yang dinonaktifkan, pilih kotak centang untuk pengguna yang ingin Anda aktifkan, lalu pilih Aktifkan.

Kotak dialog Aktifkan pengguna muncul.

5. Jika diperlukan, tinjau dan ubah alamat email utama untuk setiap pengguna, lalu pilih Aktifkan.

Mengelola alias pengguna

Anda dapat menambahkan atau menghapus alias email ke pengguna.

Untuk menambahkan alias email ke pengguna

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi yang ingin Anda tambahkan pengguna.
3. Di panel navigasi, pilih Pengguna, lalu pilih nama pengguna yang ingin Anda tambahkan alias.
4. Di bagian Detail pengguna, pilih tab Alias.
5. Di bawah tab Alias, pilih Tambah alias.
6. Di kotak Alias, masukkan alias.
7. Pilih domain untuk alias.
8. Pilih Tambahkan.

Untuk menghapus alias email dari pengguna

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi tempat Anda ingin menghapus pengguna.
3. Di panel navigasi, pilih Pengguna, lalu pilih nama pengguna yang ingin Anda hapus aliasnya.
4. Di bagian Detail pengguna, pilih tab Alias.
5. Di bawah tab Alias, pilih kotak centang terhadap alias yang ingin Anda hapus.
6. Verifikasi alias yang akan dihapus.
7. Pada jendela Hapus alias, pilih Hapus.

Menonaktifkan pengguna

Anda dapat menonaktifkan pengguna mana pun di organisasi kapan saja. Ketika Anda menonaktifkan pengguna, itu segera menjadi tidak dapat diakses. Pengguna yang dinonaktifkan selama lebih dari 30 hari akan menghapus kotak masuk mereka dari Amazon WorkMail.

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih organisasi yang berisi pengguna yang ingin Anda nonaktifkan.
3. Di panel navigasi, pilih Users (Pengguna).

Daftar semua pengguna muncul, menampilkan akun yang berada dalam status pengguna yang diaktifkan, dinonaktifkan, dan sistem.

4. Dari daftar pengguna yang diaktifkan, pilih kotak centang untuk akun yang ingin Anda nonaktifkan, lalu pilih Nonaktifkan.

Kotak dialog Nonaktifkan pengguna muncul.

5. Pilih Disable (Nonaktifkan).

Mengedit detail pengguna

Saat Anda mengedit detail pengguna, Anda dapat mengubah yang berikut ini:

- Data pribadi — Nama, alamat email, nomor telepon, dan detail pribadi lainnya.
- Kuota kotak surat (ukuran) - Kuota dapat berkisar dari 1 MB hingga 51.200 MB (50 GB). Amazon WorkMail memberi tahu pengguna ketika mereka mencapai 90 persen dari kuota mereka. Selain itu, mengubah kuota kotak pesan pengguna tidak akan memengaruhi harga. Untuk informasi selengkapnya tentang harga, lihat [WorkMail Harga Amazon](#).
- Akses perangkat seluler — Hapus dan hapus perangkat, dan lihat detail perangkat.
- Izin akses kotak pesan — Berikan izin kepada pengguna untuk menggunakan kotak pesan, dan berikan pengguna tingkat akses yang berbeda ke kotak pesan.
- Token akses pribadi (ketika Pusat Identitas IAM diaktifkan) — Lihat dan hapus token akses pribadi.

Note

Jika Anda mengintegrasikan Amazon WorkMail dengan direktori AD Connector, Anda tidak dapat mengedit detail ini dari direktori Konsol Manajemen AWS. Sebaliknya, Anda harus

mengeditnya menggunakan alat pengelolaan Direktori Aktif. Batasan berlaku bila organisasi Anda berada dalam mode interoperabilitas. Untuk informasi selengkapnya, lihat [Keterbatasan dalam mode interoperabilitas](#).

Untuk mengedit detail pengguna

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih organisasi yang ingin Anda gunakan.
3. Di panel navigasi, pilih Pengguna, lalu pilih nama pengguna yang akan diedit.

Untuk mengedit data pribadi

1. Di bagian Detail pengguna, pilih Edit.
2. Di bawah rincian Pengguna, masukkan atau ubah informasi pribadi pengguna sesuai kebutuhan.
3. Setelah selesai, pilih Simpan perubahan.

Untuk bergaul dengan pengguna IAM Identity Center

1. Di bawah Detail pengguna, pilih Edit.
2. Masukkan ID pengguna Pusat Identitas IAM yang ingin Anda kaitkan. Anda dapat melihat informasi ini di bawah tabel Pengguna yang Ditugaskan di halaman Pusat Identitas IAM atau di konsol Pusat Identitas IAM.
3. Pilih Simpan perubahan.

Untuk mengedit kuota kotak surat

1. Di bawah Detail pengguna, pilih tab Kuota, lalu pilih Edit.
2. Di kotak Perbarui kuota kotak pesan, masukkan ukuran kotak pesan. Anda dapat memasukkan nilai dari **1** ke**51200**.
3. Pilih Simpan perubahan.

Untuk mengelola data perangkat seluler

Note

Untuk mengelola perangkat seluler, pengguna Anda harus terlebih dahulu menghubungkan perangkat mereka ke instans Amazon Anda WorkMail. Untuk informasi tentang menghubungkan perangkat seluler, lihat [Menyiapkan klien perangkat seluler untuk Amazon WorkMail](#).

1. Di bawah Detail pengguna, pilih tab Perangkat seluler.
2. Untuk melihat daftar perangkat saat ini, pilih Segarkan.
3. Untuk melihat detail perangkat, pilih nama perangkat dari kolom ID Perangkat.
4. Untuk menghapus atau menghapus perangkat, pilih tombol radio di sebelah nama perangkat, lalu pilih Hapus atau Hapus sesuai kebutuhan.
5. Di kotak dialog yang muncul, konfirmasi operasi penghapusan atau penghapusan. Ingat bahwa pengguna akan muncul kembali ketika mereka menyinkronkan perangkat mereka dengan Amazon WorkMail lagi.

Untuk mengedit izin kotak pesan

1. Pilih tab Izin.
2. Lakukan salah satu tindakan berikut:
 1. Untuk menambahkan izin, pilih Tambahkan izin. Buka daftar Tambahkan izin baru dan pilih pengguna atau grup, pilih pengaturan izin untuk pengguna atau grup, lalu pilih Simpan.
 2. Untuk mengedit izin pengguna, pilih tombol di sebelah nama pengguna. Pilih Edit, pilih opsi yang diinginkan, lalu pilih Simpan.

Untuk informasi selengkapnya tentang opsi izin, lihat [Bekerja dengan izin kotak pesan](#).

3. Untuk menghapus semua izin, pilih Hapus, lalu konfirmasi penghapusan.

Untuk menghapus token akses pribadi

Note

Pastikan token yang Anda hapus tidak digunakan secara aktif oleh klien email mana pun. Menghapus token saat digunakan akan merusak otentikasi untuk klien yang menggunakan token.

1. Pilih tab Token Akses Pribadi.
2. Dari daftar token akses pribadi, pilih token akses pribadi untuk dihapus.
3. Pilih Hapus token.
4. Masukkan Ketik di kotak teks konfirmasi.

Mengatur ulang kata sandi pengguna

Jika pengguna lupa kata sandi mereka atau mengalami masalah saat masuk ke Amazon WorkMail, Anda dapat mengatur ulang kata sandi mereka.

Note

- Jika Anda telah mengintegrasikan Amazon WorkMail dengan direktori AD Connector, Anda harus mengatur ulang kata sandi pengguna di Active Directory.
- Jika Anda telah mengintegrasikan Amazon WorkMail dengan IAM Identity Center, Anda dapat memilih untuk mengatur ulang kata sandi pengguna. Untuk informasi selengkapnya, lihat [Mengatur ulang kata sandi pengguna Pusat Identitas IAM untuk pengguna akhir](#) di Panduan AWS IAM Identity Center Pengguna.

Cara mengatur ulang kata sandi pengguna

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Users (Pengguna).
4. Dalam daftar pengguna, pilih kotak centang di sebelah nama pengguna, lalu pilih Atur ulang kata sandi.
5. Di kotak dialog Reset Password, masukkan kata sandi baru, lalu pilih Reset.

Memecahkan masalah kebijakan kata sandi Amazon WorkMail

Jika mengatur ulang sandi tidak berhasil, pastikan bahwa kata sandi baru memenuhi persyaratan kebijakan kata sandi.

Persyaratan kebijakan kata sandi bergantung pada jenis direktori yang digunakan WorkMail organisasi Amazon Anda.

WorkMail Direktori Amazon dan kebijakan kata sandi direktori Simple AD

Secara default, kata sandi untuk WorkMail direktori Amazon atau direktori Simple AD harus:

- Non-empty
- Setidaknya delapan karakter
- Kurang dari 64 karakter
- Terdiri dari bahasa Latin Dasar atau karakter Latin-1 suplemen

Kata sandi juga harus berisi karakter dari tiga dari lima kelompok berikut:

- Karakter huruf besar
- Karakter huruf kecil
- Digit numerik (0 hingga 9)
- Karakter khusus (misalnya, <, ~, atau !)
- Latin-1 karakter tambahan (misalnya, é, ü, atau ñ)

Kebijakan kata sandi WorkMail direktori Amazon tidak dapat diubah.

Untuk mengubah kebijakan kata sandi Simple AD, gunakan alat administrasi AD pada Instans Amazon Elastic Compute Cloud (Amazon EC2) Windows direktori Simple AD Anda. Untuk informasi

selengkapnya, lihat [Menginstal alat administrasi Direktori Aktif](#) dalam Panduan Administrasi AWS Directory Service .

AWS Managed Microsoft AD Kebijakan kata sandi direktori

Untuk informasi tentang kebijakan kata sandi default untuk direktori AWS Managed Microsoft AD , lihat [Kelola Kebijakan Kata Sandi untuk AWS Managed Microsoft AD](#) di Panduan Administrasi AWS Directory Service .

Kebijakan kata sandi AD Connector

AD Connector menggunakan kebijakan kata sandi domain Direktori Aktif yang terkoneksi ke. Lihat dokumentasi untuk domain Active Directory Anda untuk informasi selengkapnya tentang pengaturan kebijakan kata sandi.

Bekerja dengan notifikasi

Dengan API Pemberitahuan WorkMail Push Amazon, Anda dapat menerima pemberitahuan push tentang perubahan di kotak pesan, termasuk pembaruan email dan kalender baru. Anda harus mendaftarkan URL (atau penjawab pemberitahuan push) untuk menerima pemberitahuan. Dengan fitur ini, pengembang dapat membuat aplikasi responsif untuk WorkMail pengguna Amazon, karena aplikasi dengan cepat diberitahu tentang perubahan dari kotak surat pengguna.

Untuk informasi selengkapnya, lihat [Langganan notifikasi, peristiwa kotak pesan, dan EWS di Exchange](#).

Anda dapat berlangganan folder tertentu, seperti Kotak Masuk atau Kalender, atau ke semua folder untuk peristiwa perubahan kotak pesan (termasuk Mail Baru, Dibuat, dan Dimodifikasi).

Anda dapat menggunakan perpustakaan klien seperti [EWS Java API](#) atau [EWS C# API terkelola](#) untuk mengakses fitur ini. [Contoh aplikasi lengkap dari push responder, yang dikembangkan menggunakan AWS Lambda dan API Gateway \(menggunakan kerangka AWS Serverless\), tersedia di halaman. AWS GitHub](#) Menggunakan API EWS Java.

Berikut ini adalah contoh permintaan langganan push:

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types">
  <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>

```

Berikut ini adalah hasil permintaan berlangganan yang berhasil:

```

<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
  <Header xmlns="http://schemas.xmlsoap.org/soap/envelope/">
    <ServerVersionInfo xmlns="http://schemas.microsoft.com/exchange/
services/2006/types" MajorVersion="14" MinorVersion="2" MajorBuildNumber="390"
  Version="Exchange2010_SP2" MinorBuildNumber="3" />
  </Header>
  <soap:Body>
    <m:SubscribeResponse xmlns:m="http://schemas.microsoft.com/exchange/
services/2006/messages" xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types">
      <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>

```

```

    </m:SubscribeResponse>
  </soap:Body>
</soap:Envelope>

```

Setelah itu, notifikasi dikirim ke URL yang ditentukan dalam permintaan langganan. Berikut ini adalah contoh pemberitahuan:

```

<soap:Envelope
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
    <t:RequestServerVersion
      xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
      xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"
      Version="Exchange2010_SP2">
    </t:RequestServerVersion>
  </soap:Header>
  <soap:Body>
    <m:SendNotification
      xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
      xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
      <m:ResponseMessages>
        <m:SendNotificationResponseMessage ResponseClass="Success">
          <m:ResponseCode>NoError</m:ResponseCode>
          <m:Notification>
            <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</
t:SubscriptionId>
            <t:PreviousWatermark>ygwAAAAAAAAA=</t:PreviousWatermark>
            <t:MoreEvents>>false</t:MoreEvents>
            <t:ModifiedEvent>
              <t:Watermark>ywwAAAAAAAAA=</t:Watermark>
              <t:TimeStamp>2018-02-02T15:15:14Z</t:TimeStamp>
              <t:FolderId Id="AAB2L089bS1kNDgx0GYw0GE50TQ0="></
t:FolderId>
              <t:ParentFolderId Id="AAB2L089bS1kNDgx0GYw0GE="></
t:ParentFolderId>
            </t:ModifiedEvent>
          </m:Notification>
        </m:SendNotificationResponseMessage>
      </m:ResponseMessages>
    </m:SendNotification>
  </soap:Body>
</soap:Envelope>

```

Untuk mengetahui bahwa responden pemberitahuan push telah menerima pemberitahuan, ia harus membalas dengan yang berikut:

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>OK</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

Untuk berhenti berlangganan menerima pemberitahuan push, klien harus mengirim respons berhenti berlangganan di SubscriptionStatus bidang, mirip dengan yang berikut ini:

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>Unsubscribe</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

Untuk memverifikasi kesehatan responden pemberitahuan push Anda, Amazon WorkMail mengirimkan “detak jantung” (juga disebut aStatusEvent). Frekuensi yang dikirim bersamanya ditentukan oleh parameter StatusFrequency yang disediakan dalam permintaan langganan semula. Misalnya, jika StatusFrequency sama 1, a StatusEvent dikirim setiap 1 menit. Nilai ini dapat berkisar antara 1 dan 1440 menit. Ini StatusEvent terlihat seperti berikut:

```
<?xml version="1.0 (http://www.w3.org/TR/REC-xml/)" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>
  <t:RequestServerVersion xmlns:t="http://schemas.microsoft.com/exchange/
services/2006/types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages" Version="Exchange2010_SP2"/>
</soap:Header>
<soap:Body>
```

```
<m:SendNotification xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
  <m:ResponseMessages>
    <m:SendNotificationResponseMessage ResponseClass="Success">
      <m:ResponseCode>NoError</m:ResponseCode>
      <m:Notification>
        <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</t:SubscriptionId>
        <t:PreviousWatermark>AAAAAAAAAAAA=</t:PreviousWatermark>
        <t:MoreEvents>false</t:MoreEvents>
        <t:StatusEvent>
          <t:Watermark>AAAAAAAAAAAA=</t:Watermark>
        </t:StatusEvent>
      </m:Notification>
    </m:SendNotificationResponseMessage>
  </m:ResponseMessages>
</m:SendNotification>
</soap:Body>
</soap:Envelope>
```

Jika responden notifikasi push klien gagal merespons dengan OK status yang sama seperti sebelumnya, notifikasi akan dicoba ulang selama maksimal beberapa menit. StatusFrequency Misalnya, jika StatusFrequency sama dengan 5, dan notifikasi pertama gagal, itu dicoba maksimum selama 5 menit dengan backoff eksponensial antara setiap percobaan kembali. Jika notifikasi tidak dikirimkan setelah waktu coba lagi berakhir, langganan tidak valid dan tidak ada pemberitahuan baru yang dikirimkan. Anda harus membuat langganan baru untuk terus menerima notifikasi tentang peristiwa kotak pesan. Saat ini, Anda dapat berlangganan maksimal tiga langganan per kotak surat.

Mengaktifkan email yang ditandatangani atau dienkripsi

Anda dapat menggunakan S/MIME untuk memungkinkan pengguna mengirim email yang ditandatangani atau dienkripsi baik di dalam maupun di luar organisasi.

Note

Sertifikat pengguna dalam Daftar Alamat Global (GAL) didukung hanya dalam pengaturan Direktori Aktif terkoneksi.

Untuk mengizinkan pengguna mengirim email yang ditandatangani atau dienkripsi

1. Mengatur Direktori Aktif (AD) Connector. Menyiapkan AD Connector dengan direktori on-premise memungkinkan pengguna untuk terus menggunakan kredensial perusahaannya yang ada.
2. Mengkonfigurasi Pendaftaran Otomatis Sertifikat untuk menerbitkan dan menyimpan sertifikat pengguna secara otomatis di Direktori Aktif. Amazon WorkMail menerima sertifikat pengguna dari Active Directory dan menerbitkannya ke GAL. Untuk informasi selengkapnya, lihat [Mengkonfigurasi Pendaftaran Otomatis Sertifikat](#).
3. Mendistribusikan sertifikat yang dihasilkan untuk pengguna dengan mengekspor sertifikat dari server yang menjalankan Microsoft Exchange dan mengirimkannya melalui email.
4. Setiap pengguna menginstal sertifikat untuk program email mereka (seperti Windows Outlook) dan perangkat seluler.

Bekerja dengan grup

Anda dapat menggunakan grup sebagai daftar distribusi di Amazon WorkMail untuk menerima email untuk alamat email umum, seperti <sales@example.com> atau <support@example.com>. Anda dapat membuat beberapa alias email untuk suatu grup.

Anda juga dapat menggunakan grup sebagai grup keamanan untuk berbagi kotak pesan atau kalender dengan tim tertentu.

Grup tidak memiliki kotak pesan sendiri, dan hal itu memengaruhi izin kotak pesan yang dapat Anda berikan ke grup. Untuk informasi tentang mengatur izin kotak pesan untuk grup, lihat [Mengelola izin kotak pesan untuk grup](#)

Note

Ini dapat memakan waktu hingga 2 jam sebelum grup yang baru ditambahkan muncul di buku alamat offline Microsoft Outlook.

Topik

- [Melihat daftar grup](#)
- [Menambahkan grup](#)
- [Mengaktifkan grup](#)
- [Menambahkan anggota ke grup](#)
- [Mengedit detail grup](#)
- [Menghapus anggota dari grup](#)
- [Mengelola alias grup](#)
- [Menonaktifkan grup](#)
- [Menghapus grup](#)


Melihat daftar grup

Untuk melihat daftar grup

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Grup.
4. Selain itu, Anda dapat memfilter grup berdasarkan nama Grup atau Alamat email utama.

 Note

Pencarian peka huruf besar/kecil.

Menambahkan grup

Anda dapat menambahkan grup dari WorkMail konsol Amazon.

Untuk menambahkan grup

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Grup, lalu pilih Tambah grup.

Halaman Tambah grup muncul.

4. Di bawah Nama grup, masukkan nama untuk grup.
5. Di bawah Alamat email, masukkan alamat email utama untuk grup.
6. Verifikasi alamat email grup, perbarui sesuai kebutuhan.
7. Secara default, grup ditampilkan dalam daftar alamat global. Untuk menyembunyikan grup dari daftar alamat global, kosongkan kotak centang Tampilkan di daftar alamat global.
8. Pilih Tambah grup.

Mengaktifkan grup

Ketika Anda mengintegrasikan Amazon WorkMail dengan Active Directory perusahaan Anda, atau Anda sudah memiliki grup yang tersedia di Active Directory sederhana Anda, Anda dapat menggunakan grup tersebut sebagai grup keamanan atau daftar distribusi di Amazon WorkMail.

Untuk mengaktifkan grup direktori yang ada

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Grup.
4. Pilih kotak centang di samping grup yang ingin Anda aktifkan, lalu pilih Aktifkan.

Kotak dialog Aktifkan grup muncul dan meminta Anda untuk mengonfirmasi operasi.

5. Jika diperlukan, tinjau dan ubah alamat email utama untuk setiap grup, lalu pilih Aktifkan.

Menambahkan anggota ke grup

Setelah Anda membuat dan mengaktifkan WorkMail grup Amazon, gunakan WorkMail konsol Amazon untuk menambahkan anggota ke grup tersebut.

Note

Jika Amazon WorkMail terintegrasi dengan layanan Active Directory yang terhubung atau Microsoft Active Directory, Anda dapat menggunakan Active Directory untuk mengelola anggota grup Anda. Namun, perubahan bisa memakan waktu lebih lama untuk menyebar ke Amazon WorkMail.

Untuk menambahkan anggota ke grup

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Grup.
4. Nama dari grup keamanan.
5. Pada halaman Detail grup, pilih tab Anggota.
6. Pilih grup atau pengguna untuk ditambahkan di bawah Grup atau Pengguna.
7. Pilih pengguna atau grup dari drop-down.
8. Pilih Simpan.

Perubahan Anda dapat memakan waktu beberapa menit untuk disebar.

Mengedit detail grup

Anda dapat mengedit detail grup.

Untuk mengedit detail grup

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Grup, lalu pilih grup yang akan diedit.
4. Pada halaman Detail grup, perbarui alamat Email sesuai kebutuhan.
5. Secara default, grup ditampilkan dalam daftar alamat global. Untuk menyembunyikan grup dari daftar alamat global, kosongkan kotak centang Tampilkan di daftar alamat global.
6. Pilih Simpan perubahan.

Menghapus anggota dari grup

Gunakan WorkMail konsol Amazon untuk menghapus anggota dari grup.

Note

Jika Amazon WorkMail terintegrasi dengan Active Directory atau Microsoft Active Directory yang terhubung, Anda dapat menggunakan Active Directory untuk mengelola anggota grup Anda. Namun, hal itu dapat menciptakan waktu yang dibutuhkan untuk menyebarkan perubahan Anda ke Amazon WorkMail.

Untuk menghapus anggota dari grup

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Grup, lalu pilih nama grup.
4. Pada halaman Detail grup, pilih tab Anggota.
5. Pilih anggota yang akan dihapus dari grup.
6. Pilih Hapus.

Perubahan Anda dapat memakan waktu beberapa menit untuk disebarkan.

Mengelola alias grup

Anda dapat menambahkan atau menghapus alias email ke grup.

Untuk menambahkan alias email ke grup.

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi yang ingin Anda tambahkan alias.
3. Di panel navigasi, pilih Grup, lalu pilih nama grup yang ingin Anda tambahkan alias.
4. Di bagian Detail grup, pilih Alias.
5. Di bawah Alias, pilih Tambahkan alias.
6. Di kotak Alias, masukkan alias.
7. Pilih domain untuk alias.
8. Pilih Tambahkan.

Untuk menghapus alias email dari grup.

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi tempat Anda ingin menghapus alias.
3. Di panel navigasi, pilih Grup, lalu pilih pilih nama grup tempat Anda ingin menghapus aliasnya.
4. Di bagian Detail grup, pilih Alias.
5. Di bawah Alias, pilih kotak centang terhadap alias yang ingin Anda hapus.
6. Pilih Hapus.
7. Verifikasi alias yang akan dihapus.
8. Pada jendela Hapus alias, pilih Hapus.

Menonaktifkan grup

Bila Anda tidak lagi memerlukan sebuah grup, Anda dapat menonaktifkannya.

Menonaktifkan grup

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Grup.
4. Di bawah Nama grup, pilih grup yang akan dinonaktifkan, lalu pilih Nonaktifkan.
5. Di kotak dialog Nonaktifkan grup, pilih Nonaktifkan.

Menghapus grup

Sebelum Anda dapat menghapus grup, Anda harus menonaktifkan grup itu terlebih dahulu. Untuk informasi tentang menonaktifkan grup, lihat [Menonaktifkan grup](#)

Untuk menghapus grup

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Grup.
4. Pilih kotak centang di samping grup yang dinonaktifkan yang ingin Anda hapus dan pilih Hapus.

Kotak dialog Hapus muncul.

5. Di kotak Masukkan nama grup untuk mengonfirmasi penghapusan, masukkan nama grup, lalu pilih Hapus.

Note

Untuk menghapus grup secara permanen, gunakan tindakan DeleteGroup API untuk Amazon WorkMail. Untuk informasi selengkapnya, lihat [DeleteGroup](#) di Referensi Amazon WorkMail API.

Bekerja dengan sumber daya

Amazon WorkMail dapat membantu pengguna Anda memesan sumber daya. Misalnya, pengguna dapat memesan ruang rapat, atau peralatan seperti proyektor, telepon, atau mobil. Untuk memesan sumber daya, pengguna menambahkan sumber daya ke undangan rapat.

Topik

- [Melihat daftar sumber daya](#)
- [Menambahkan sumber daya](#)
- [Mengedit detail sumber daya](#)
- [Mengelola alias sumber daya](#)
- [Mengaktifkan sumber daya](#)
- [Menonaktifkan sumber daya](#)
- [Menghapus sumber daya](#)

Melihat daftar sumber daya

Untuk melihat daftar sumber daya

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Pada panel navigasi, silakan pilih Sumber Daya.
4. Selain itu, Anda dapat memfilter sumber daya berdasarkan nama Sumber Daya atau Alamat email utama.

Note

Pencarian peka huruf besar/kecil.

Menambahkan sumber daya

Anda dapat menambahkan sumber daya baru ke organisasi Anda dan memungkinkan pengguna untuk memesannya.

Untuk menambahkan sumber daya

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Sumber Daya, lalu Tambahkan sumber daya.

Halaman Tambah sumber daya muncul.

4. Di kotak Nama sumber daya, masukkan nama untuk sumber daya.
5. Secara opsional, di kotak Deskripsi sumber daya, masukkan deskripsi untuk sumber daya.
6. Di bawah Jenis sumber daya, pilih opsi.
7. Verifikasi alamat email sumber daya, perbarui sesuai kebutuhan.
8. Secara default, sumber daya ditampilkan dalam daftar alamat global. Untuk menyembunyikan sumber daya dari daftar alamat global, kosongkan kotak centang Tampilkan di daftar alamat global.
9. Pilih Tambahkan sumber daya.

Mengedit detail sumber daya

Anda dapat mengedit detail umum sumber daya, termasuk nama, deskripsi, jenis, dan alamat email, opsi pemesanan, dan delegasi.

Untuk mengedit detail sumber daya umum

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Sumber Daya, lalu pilih sumber daya yang akan diedit.
4. Pada halaman Detail sumber daya, perbarui nama Sumber Daya, Deskripsi, Jenis Sumber Daya, atau alamat Email sesuai kebutuhan.
5. Secara default, sumber daya ditampilkan dalam daftar alamat global. Untuk menyembunyikan sumber daya dari daftar alamat global, kosongkan kotak centang Tampilkan di daftar alamat global.
6. Pilih Simpan perubahan.

Anda dapat mengkonfigurasi sumber daya untuk menerima atau menolak permintaan pemesanan secara otomatis.


Anda dapat mengedit opsi pemesanan sumber daya.

Untuk mengubah opsi pemesanan sumber daya

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Sumber Daya, lalu pilih sumber daya yang akan diedit. Halaman muncul dan menampilkan detail Sumber Daya.
4. Di bawah Opsi pemesanan pilih Edit.
5. Seperti yang diperlukan, pilih atau kosongkan kotak centang di sebelah opsi untuk mengaktifkan atau menonaktifkan opsi.

 Note

Ketika Anda menonaktifkan salah satu opsi pemesanan otomatis, Anda harus membuat delegasi untuk menangani permintaan pemesanan. Langkah selanjutnya menjelaskan cara membuat delegasi.

Anda dapat menambahkan delegasi untuk mengontrol permintaan pemesanan untuk sumber daya yang tidak memiliki opsi pemesanan otomatis yang dikonfigurasi. Delegasi sumber daya secara otomatis menerima salinan semua permintaan pemesanan dan memiliki akses penuh ke kalender sumber daya. Selain itu, mereka harus menerima semua permintaan pemesanan untuk suatu sumber daya.

Untuk menambahkan delegasi sumber daya

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Sumber daya, lalu pilih nama sumber daya yang ingin Anda tambahkan delegasi.
4. (Opsional) Di tab Opsi pemesanan, pilih Edit, kosongkan kotak centang Terima semua permintaan sumber daya secara otomatis, lalu pilih Simpan.
5. Pilih tab Delegasi, lalu pilih Tambah delegasi.

Kotak dialog Add delegate muncul.

6. Buka daftar delegasi Cari dan pilih delegasi, lalu pilih Simpan.

Untuk menghapus delegasi sumber daya

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi tempat Anda ingin menghapus delegasi.
3. Di panel navigasi, pilih Sumber daya, lalu pilih nama sumber daya dari mana Anda ingin menghapus delegasi.
4. Pilih Delegasi, lalu pilih delegasi yang akan dihapus.
5. Choose Hapus.

Mengelola alias sumber daya

Anda dapat menambahkan atau menghapus alias email ke sumber daya.

Untuk menambahkan alias email ke sumber daya

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi yang ingin Anda tambahkan alias.
3. Di panel navigasi, pilih Resources, lalu pilih nama sumber daya yang ingin Anda tambahkan alias.
4. Di bagian Rincian sumber daya, pilih Alias.
5. Di bawah Alias, pilih Tambahkan alias.
6. Di kotak Alias, masukkan alias.
7. Pilih domain untuk alias.
8. Pilih Tambahkan.

Untuk menghapus alias email dari sumber daya

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi tempat Anda ingin menghapus aliasnya.
3. Di panel navigasi, pilih Sumber daya, lalu pilih nama sumber daya yang ingin Anda hapus aliasnya.
4. Di bagian Rincian sumber daya, pilih Alias.
5. Di bawah Alias, pilih kotak centang terhadap alias yang ingin Anda hapus.
6. Pilih Hapus.
7. Verifikasi alias yang akan dihapus.
8. Pada jendela Hapus alias, pilih Hapus.

Mengaktifkan sumber daya

Secara default, Amazon WorkMail membuat sumber daya. Jika Anda atau orang lain menonaktifkan sumber daya, Anda dapat mengaktifkan kembali sumber daya dalam waktu 30 hari.

Untuk mengaktifkan sumber daya

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya tentang wilayah, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih organisasi yang berisi sumber daya yang ingin Anda aktifkan.
3. Pada panel navigasi, silakan pilih Sumber Daya.
4. Dalam daftar sumber daya, pilih tombol di sebelah sumber daya yang ingin Anda aktifkan, lalu pilih Aktifkan.

Kotak dialog Aktifkan sumber daya muncul.

5. Pilih Aktifkan.

Menonaktifkan sumber daya

Ketika Anda menonaktifkan sumber daya, Anda membuatnya tidak tersedia untuk pemesanan. Misalnya, Anda dapat menonaktifkan ruang konferensi saat sedang direnovasi, lalu mengaktifkan ruangan setelah tersedia untuk digunakan.

Untuk menonaktifkan sumber daya

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya tentang wilayah, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih organisasi yang berisi sumber daya yang ingin Anda nonaktifkan.
3. Pada panel navigasi, silakan pilih Sumber Daya.
4. Dalam daftar sumber daya, pilih tombol di sebelah sumber daya yang ingin Anda nonaktifkan, lalu pilih Nonaktifkan.

Kotak dialog Nonaktifkan sumber daya muncul.

5. Pilih Disable (Nonaktifkan).

Menghapus sumber daya

Ketika Anda tidak lagi membutuhkan sumber daya, Anda dapat menghapusnya. Namun, Anda harus menonaktifkan sumber daya terlebih dahulu. Untuk informasi tentang menonaktifkan sumber daya, lihat langkah-langkah di bagian sebelumnya.

Warning

Setelah sumber daya dihapus, itu tidak dapat dipulihkan.

Untuk menghapus sumber daya

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya tentang wilayah, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih organisasi yang diinginkan.
3. Pada panel navigasi, silakan pilih Sumber Daya.
4. Dalam daftar sumber daya, pilih tombol di sebelah sumber daya yang dinonaktifkan yang ingin Anda hapus, lalu pilih Hapus.

Kotak dialog Hapus sumber daya muncul.

5. Di kotak Masukkan nama sumber daya untuk mengonfirmasi penghapusan, masukkan nama sumber daya yang ingin Anda hapus, lalu pilih Hapus sumber daya.

Bekerja dengan IAM Identity Center

Anda dapat mengaktifkan otentikasi multi-faktor (MFA) di Amazon dengan WorkMail mengaitkan WorkMail pengguna Amazon Anda dengan IAM Identity Center. Untuk informasi selengkapnya, lihat [Apa itu Pusat Identitas IAM](#).

Tabel di bawah ini menjelaskan langkah-langkah untuk mengatasi skenario yang berbeda.

Skenario	Langkah-langkah
Mengaitkan WorkMail pengguna Amazon ke Pusat Identitas IAM	<ol style="list-style-type: none">1. Mengaktifkan Pusat Identitas IAM di Amazon WorkMail2. Menetapkan pengguna dan grup Pusat Identitas IAM ke aplikasi Amazon WorkMail3. Mengaitkan WorkMail pengguna Amazon dengan pengguna IAM Identity Center
WorkMail Pengguna Amazon yang ada	<ol style="list-style-type: none">1. Buat pengguna IAM Identity Center dengan nama pengguna yang sama, kelompokkan pengguna bersama-sama dan tetapkan grup ke aplikasi Amazon WorkMail .2. Kaitkan WorkMail pengguna Amazon dengan pengguna Pusat Identitas IAM.
Pengguna Pusat Identitas IAM yang ada	<ol style="list-style-type: none">1. Buat WorkMail pengguna Amazon dengan nama pengguna yang sama dengan pengguna IAM Identity Center.2. Tetapkan pengguna atau grup Pusat Identitas IAM ke aplikasi Amazon WorkMail.3. Kaitkan WorkMail pengguna Amazon dengan pengguna IAM Identity Center.
Menghubungkan direktori eksternal ke IAM Identity Center	<ol style="list-style-type: none">1. Sinkronkan pengguna direktori eksternal ke grup Pusat Identitas IAM. Untuk informasi lebih lanjut, lihat tutorial sumber Identitas Pusat Identitas IAM

Skenario	Langkah-langkah
	<ol style="list-style-type: none">2. Tetapkan grup Pusat Identitas IAM ke aplikasi Amazon WorkMail .3. Connect direktori eksternal ke Amazon WorkMail dan pastikan nama pengguna cocok4. Kaitkan WorkMail pengguna Amazon dengan pengguna Pusat Identitas IAM.

Setelah langkah-langkah di atas selesai, Anda dapat melihat status Pusat Identitas IAM, tautan ke Pusat Identitas AWS IAM untuk mengelola pengguna dan grup, MFA mengaktifkan URL aplikasi web WorkMail Amazon, mode otentikasi, status token akses pribadi, dan garis waktu di bawah Pusat Identitas IAM di bawah Pengaturan di konsol Amazon. WorkMail Untuk informasi selengkapnya tentang mengelola MFA di konsol Pusat Identitas IAM, lihat [Multi-factor autentikasi untuk pengguna Pusat Identitas IAM](#).

Note

Pastikan konfigurasi antara Amazon WorkMail dan IAM Identity Center diuji dan diverifikasi dengan baik. Pengguna dapat kehilangan akses ke kotak pesan mereka ketika konfigurasi tidak benar dan lengkap.

Topik

- [Mengaktifkan Pusat Identitas IAM di Amazon WorkMail](#)
- [Menetapkan pengguna dan grup Pusat Identitas IAM ke aplikasi Amazon WorkMail](#)
- [Mengaitkan WorkMail pengguna Amazon dengan pengguna IAM Identity Center](#)
- [Mode autentikasi](#)
- [Mengkonfigurasi token akses pribadi](#)
- [Menonaktifkan Pusat Identitas IAM](#)

Mengaktifkan Pusat Identitas IAM di Amazon WorkMail

Saat Anda mengaktifkan IAM Identity Center, ia bertindak sebagai lapisan otentikasi untuk pengguna Amazon WorkMail. Pengguna IAM Identity Center dikelola secara terpisah dari WorkMail direktori Amazon. Disarankan untuk menggunakan nama pengguna yang sama di IAM Identity Center dan Amazon WorkMail.

Note

Pastikan Amazon WorkMail dan IAM Identity Center disiapkan di wilayah yang sama.

Untuk mengaktifkan Pusat Identitas IAM, ikuti langkah-langkah ini.

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

2. Di panel navigasi, pilih Pusat Identitas.

Halaman Pengaturan Pusat Identitas IAM muncul.

3. Pilih Aktifkan.

Jendela Enable IAM Identity Center muncul.

4. Pilih Aktifkan.

Halaman Pengaturan Pusat Identitas muncul dengan Status Pusat Identitas ditampilkan.

5. Untuk menambahkan pengguna dan grup Pusat Identitas IAM ke WorkMail Organisasi Amazon Anda, ikuti tautan di bawah status Pusat Identitas. Untuk informasi tentang cara menambahkan pengguna dan grup, lihat [Mengelola identitas di Pusat Identitas IAM](#).

Menetapkan pengguna dan grup Pusat Identitas IAM ke aplikasi Amazon WorkMail

Saat Anda mengaktifkan Pusat Identitas IAM di Amazon WorkMail, WorkMail buat aplikasi di Pusat Identitas IAM atas nama Anda. Secara default, pengguna Pusat Identitas IAM harus ditetapkan ke

aplikasi ini atau termasuk dalam grup yang ditetapkan ke aplikasi ini untuk mengakses kotak surat di organisasi Amazon WorkMail. Untuk informasi selengkapnya, lihat [aplikasi AWS terkelola](#) di Panduan AWS IAM Identity Center Pengguna.

Anda dapat menetapkan pengguna dan grup Pusat Identitas IAM ke Amazon dengan WorkMail cara berikut:

- Oleh pengguna IAM Identity Center - Anda dapat menetapkan pengguna IAM Identity Center ke Amazon. WorkMail
- Dengan grup Pusat Identitas IAM - Anda dapat menetapkan grup Pusat Identitas IAM ke Amazon. WorkMail Dengan menambahkan grup, semua pengguna di bawah grup akan memiliki akses ke Amazon WorkMail.

Untuk informasi selengkapnya tentang menambahkan pengguna dan grup, lihat [Pengguna, grup, dan penyediaan di Pusat Identitas IAM](#).

Note

Jika Anda menghubungkan sumber identitas yang ada dengan IAM Identity Center, tinjau hal berikut sebelum mengubah sumber direktori Anda.

- Otentikasi Anda sedang dikelola oleh IAM Identity Center.
- Amazon WorkMail akan mempertahankan semua WorkMail pengguna dan grup Amazon.
- IAM Identity Center akan mempertahankan semua pengguna, grup, dan tugas IAM Identity Center.
- Anda harus mengelola WorkMail pengguna dan grup Amazon di WorkMail konsol Amazon.
- Anda harus mengelola pengguna dan grup Pusat Identitas IAM di Pusat Identitas IAM.
- Pengguna tanpa penetapan Pusat Identitas IAM atau asosiasi pengguna tidak dapat mengakses Amazon. WorkMail
- Anda harus mengelola kontrol kebijakan MFA di Pusat Identitas IAM.
- Saat Anda mengubah sumber Pusat Identitas IAM ke dan dari Kelola Direktori Aktif di Pusat Identitas IAM, Anda harus menonaktifkan konfigurasi Pusat Identitas IAM yang ada di Amazon dan mengonfigurasi ulang untuk mengaitkan pengguna WorkMail WorkMail Amazon Anda dengan Pusat Identitas IAM.

Pengguna dan grup yang disinkronkan dengan direktori Pusat Identitas IAM Anda tersedia untuk ditetapkan ke aplikasi Amazon Anda. WorkMail Untuk informasi selengkapnya tentang pengguna IAM Identity Center dan manajemen grup, lihat [Memulai tugas umum di Pusat Identitas IAM](#). .

Untuk menetapkan pengguna dan grup Pusat Identitas IAM ke Amazon WorkMail, ikuti langkah-langkah ini.

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di. Referensi Umum Amazon Web

2. Di panel navigasi, pilih Pusat Identitas.

Halaman Pengaturan Pusat Identitas IAM muncul.

3. Pilih Tetapkan pengguna dan grup.

Anda dapat menambahkan dan menetapkan pengguna baru atau menetapkan pengguna dan grup yang ada.

- Tetapkan Pengguna - Anda dapat menetapkan pengguna Pusat Identitas IAM individual ke Amazon. WorkMail Anda dapat membuat pengguna Pusat Identitas IAM baru atau mencari pengguna yang sudah ada.
- Tetapkan Grup - Anda juga dapat menetapkan grup Pusat Identitas IAM ke Amazon. WorkMail Semua anggota grup kemudian akan ditugaskan ke Amazon WorkMail.

Note

Semua pengguna IAM Identity Center baru diaktifkan secara default di IAM Identity Center. Untuk memberikan akses ke Amazon WorkMail, Anda harus mengatur kata sandi mereka di Pusat Identitas IAM dan menetapkannya ke Amazon. WorkMail Untuk informasi selengkapnya, lihat [Menambahkan pengguna ke direktori Pusat Identitas Anda](#).

Mengaitkan WorkMail pengguna Amazon dengan pengguna IAM Identity Center

Saat pengguna masuk ke klien WorkMail web Amazon dengan kredensi pengguna Pusat Identitas IAM mereka, klien akan membuka kotak pesan pengguna Amazon terkait. WorkMail Jika tidak ada pengguna dalam WorkMail organisasi yang dikaitkan dengan pengguna Pusat Identitas IAM, WorkMail akan membuat asosiasi antara pengguna Pusat Identitas IAM yang masuk dan pengguna yang memiliki nama WorkMail pengguna yang sama, jika WorkMail pengguna tersebut ada. Jika tidak, klien akan menampilkan pesan kesalahan kepada pengguna.

Note

Anda disarankan untuk menggunakan nama pengguna yang sama untuk pengguna di Amazon WorkMail dan Pusat Identitas IAM karena WorkMail akan membuat asosiasi secara otomatis ketika pengguna pertama kali masuk ke klien WorkMail web Amazon dengan kredensi pengguna Pusat Identitas IAM mereka. Ketika nama pengguna berbeda, Anda bertanggung jawab untuk membuat asosiasi.

Untuk mengaitkan pengguna, ikuti langkah-langkah ini.

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

2. Di panel navigasi, pilih Pusat Identitas.

Halaman Pengaturan Pusat Identitas IAM muncul.

3. Pilih Rekanan pengguna.
4. Di bawah Pilih WorkMail pengguna, pilih WorkMail pengguna Amazon yang ingin Anda kaitkan.
5. Di bawah Masukkan ID pengguna Pusat Identitas IAM, masukkan ID pengguna Pusat Identitas IAM yang ingin Anda kaitkan. Anda dapat menyalin ID dari tab Pengguna yang Ditugaskan pada halaman Pusat Identitas.

Note

Pengguna IAM Identity Center harus diberi wewenang untuk mengakses WorkMail aplikasi Amazon.

6. Pilih Rekanan pengguna.

Setelah asosiasi berhasil, WorkMail pengguna Amazon dapat masuk ke Amazon WorkMail menggunakan kredensial Pusat Identitas IAM MFA.

Note

Anda juga dapat mengaitkan WorkMail pengguna Amazon dengan pengguna IAM Identity Center saat Anda mengedit detail WorkMail pengguna Amazon. Untuk informasi selengkapnya, lihat [Mengedit detail pengguna](#).

Mode autentikasi

Anda dapat menggunakan mode otentikasi untuk memungkinkan pengguna masuk menggunakan kredensial WorkMail direktori Amazon mereka, kredensial Pusat Identitas IAM mereka, atau membatasi login hanya ke kredensial Pusat Identitas IAM.

Ada dua mode otentikasi yang tersedia di Amazon WorkMail.

Note

Pilihan mode otentikasi tergantung pada persyaratan keamanan organisasi Anda dan preferensi pengalaman pengguna. Disarankan untuk menggunakan mode IAM Identity Center saja karena memberikan keamanan yang ditingkatkan dengan menegakkan kredensial IAM Identity Center dan MFA. Namun, sebelum beralih dari mode WorkMail Direktori Amazon dan Pusat Identitas IAM, pastikan untuk menguji proses MFA dengan semua pengguna Anda untuk memastikan transisi yang lancar dan menghindari dampak apa pun pada akses klien email yang ada.

- WorkMail Direktori Amazon dan Pusat Identitas IAM (disarankan untuk pengujian) — Ini adalah opsi default bagi Anda untuk menguji asosiasi Pusat Identitas IAM sebelum beralih ke mode produksi. Mode pengujian memungkinkan pengguna untuk masuk ke klien WorkMail web Amazon menggunakan WorkMail direktori Amazon dan kredensial Pusat Identitas IAM. Saat Anda membagikan URL aplikasi WorkMail web Amazon dari pengaturan Organisasi, pengguna dapat masuk menggunakan kredensial WorkMail direktori Amazon mereka. Saat Anda membagikan MFA-enabled URL dari pengaturan Pusat Identitas IAM, pengguna dapat masuk menggunakan kredensial IAM mereka.
- Hanya Pusat Identitas IAM (disarankan untuk produksi) - Mode otentikasi ini hanya memungkinkan Anda untuk masuk ke kotak surat WorkMail klien Amazon menggunakan kredensial Pusat Identitas IAM. Untuk setiap WorkMail pengguna Amazon yang ada, kredensial WorkMail direktori Amazon tidak lagi berlaku untuk aplikasi WorkMail web Amazon dan klien email yang ada. Anda dapat meminta token akses pribadi untuk mengakses kotak surat menggunakan klien email apa pun. Untuk menghindari kehilangan akses ke kotak surat, pastikan MFA diaktifkan untuk semua pengguna Amazon WorkMail .

Untuk mengaktifkan mode otentikasi, ikuti langkah-langkah ini.

1. Di bawah halaman Pengaturan Pusat Identitas, pilih tab Mode Otentikasi.
2. Pilih Edit.


Halaman mode Edit otentikasi muncul.

3. Pilih salah satu dari berikut ini:
 - Pusat Identitas IAM saja
 - WorkMail Direktori Amazon dan Pusat Identitas IAM
4. Pilih Simpan.

Mengkonfigurasi token akses pribadi

Anda dapat mengaktifkan token akses pribadi bagi WorkMail pengguna Amazon untuk mengakses kotak surat mereka menggunakan klien email desktop dan seluler. Setelah Pusat Identitas IAM diaktifkan, secara default, status token akses pribadi diatur ke aktif dan berlaku selama 365 hari. Setelah mengaktifkan IAM Identity Center, kredensial pengguna Anda yang ada tidak lagi valid untuk masuk ke klien email mereka. Pengguna Anda dapat menghasilkan token akses pribadi dari aplikasi WorkMail web Amazon dan menggunakannya untuk masuk ke klien email apa pun. Anda dapat

mengedit kedaluwarsa token akses pribadi dan ketika token kedaluwarsa, pengguna Anda dapat membuat yang baru.

 Note

- Pengguna Anda hanya dapat melihat dan menyalin token akses pribadi Anda sekali saat Anda membuatnya di Amazon WorkMail. Jika Anda kehilangan token akses pribadi Anda, Anda perlu membuat yang baru untuk alasan keamanan.
- Amazon WorkMail hanya mengizinkan token akses pribadi untuk akses kotak surat ketika WorkMail pengguna Amazon dikaitkan dengan pengguna Pusat Identitas IAM yang berwenang untuk mengakses aplikasi Amazon WorkMail.

Konfigurasi token akses pribadi tercantum di bawah ini:

- Aktif — Ketika status token akses pribadi disetel ke Aktif, pengguna Anda dapat membuat token akses pribadi dari Amazon WorkMail dan menggunakannya untuk masuk ke klien email mana pun dalam masa pakai token.
- Tidak Aktif — Ketika status token akses pribadi disetel ke Tidak Aktif, pengguna Anda tidak akan dapat membuat atau menggunakan token akses pribadi untuk mengakses kotak pesan.
- Token seumur hidup — Secara default, token akses pribadi berlaku selama 365 hari. Anda memiliki opsi untuk mengubah masa pakai token akses pribadi. Saat Anda membiarkan pengaturan seumur hidup kosong, token akan memiliki masa pakai yang tidak terbatas dan tidak pernah kedaluwarsa.

Untuk mengonfigurasi token akses pribadi, ikuti langkah-langkah ini.

1. Di bawah halaman Pengaturan Pusat Identitas, pilih tab konfigurasi token akses pribadi.
2. Pilih Edit.

Halaman konfigurasi Edit token pribadi muncul.

3. Di bawah status Token, geser tombol Aktif untuk mengaktifkan token akses pribadi.
4. Dalam kotak teks Token seumur hidup (dalam hari), masukkan jumlah hari token akses pribadi dapat diaktifkan.
5. Pilih Simpan.

Menonaktifkan Pusat Identitas IAM

Anda dapat menonaktifkan Pusat Identitas IAM dari WorkMail konsol Amazon. Setelah dinonaktifkan, Anda tidak dapat mengakses kotak pesan menggunakan kredensial Pusat Identitas IAM atau token akses pribadi. Disarankan untuk mengatur ulang semua kata sandi pengguna dan WorkMail pengguna Amazon akan kembali menggunakan kredensial WorkMail Direktori Amazon.

Note

Periksa hal-hal berikut:

- Setelah menonaktifkan Pusat Identitas IAM, pengguna dan grup Pusat Identitas Amazon WorkMail dan IAM Anda akan tetap tidak berubah.
- Asosiasi pengguna yang ada akan terus ada.
- Otentikasi Anda akan kembali dikelola oleh WorkMail direktori Amazon, bukan IAM Identity Center.

Untuk menonaktifkan Pusat Identitas IAM, ikuti langkah-langkah ini.

1. Di bawah halaman Pengaturan Pusat Identitas, pilih Nonaktifkan.

Halaman Disable IAM Identity Center muncul.

2. Pilih Konfirmasi.

Bekerja dengan perangkat seluler

Topik di bagian ini menjelaskan cara mengelola perangkat seluler yang terhubung ke Amazon WorkMail.

Topik

- [Mengedit kebijakan perangkat seluler organisasi](#)
- [Mengelola perangkat seluler](#)
- [Mengelola aturan akses perangkat seluler](#)
- [Mengelola penggantian akses perangkat seluler](#)
- [Mengintegrasikan dengan solusi manajemen perangkat seluler](#)

Mengedit kebijakan perangkat seluler organisasi

Anda dapat mengedit kebijakan perangkat seluler organisasi Anda untuk mengubah cara perangkat seluler berinteraksi dengan Amazon WorkMail.

Cara mengedit kebijakan perangkat seluler organisasi

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Nama Wilayah dan titik akhir](#) di Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Kebijakan Seluler, dan kemudian pada layar Kebijakan seluler, pilih Edit.
4. Perbarui yang berikut sebagaimana yang diperlukan:
 - a. Wajibkan enkripsi pada perangkat: Enkripsi data email di perangkat seluler.
 - b. Wajibkan enkripsi pada kartu penyimpanan: Enkripsi data email pada penyimpanan yang dapat dilepas pada perangkat seluler.
 - c. Diperlukan kata sandi: Memerlukan kata sandi untuk membuka kunci perangkat seluler.
 - d. Izinkan kata sandi sederhana: Gunakan PIN perangkat sebagai kata sandi.
 - e. Panjang kata sandi minimal: Atur jumlah karakter yang diperlukan untuk kata sandi yang valid.

- f. Memerlukan kata sandi alfanumerik: Memerlukan kata sandi yang terdiri dari huruf dan angka.
 - g. Jumlah upaya gagal yang diizinkan: Tentukan jumlah upaya membuka kunci perangkat yang gagal yang diizinkan sebelum perangkat pengguna dihapus. Semua data, termasuk file pribadi akan dihapus ketika perangkat dihapus.
 - h. Kedaluwarsa kata sandi: Tentukan jumlah hari sebelum kata sandi kedaluwarsa dan harus diubah.
 - i. Aktifkan kunci layar: Tentukan jumlah detik untuk membiarkan layar aktif tanpa input pengguna hingga layar pengguna terkunci.
 - j. Berlakukan riwayat kata sandi: Tentukan jumlah kata sandi yang dapat dimasukkan sebelum mengulangi kata sandi yang sama.
5. Pilih Simpan.

Mengelola perangkat seluler

Topik di bagian ini menjelaskan cara menghapus perangkat seluler dari jarak jauh, menghapus perangkat dari organisasi, dan melihat detail untuk perangkat. Untuk informasi tentang mengedit kebijakan perangkat seluler organisasi Anda, lihat [Mengedit kebijakan perangkat seluler organisasi](#).

Topik

- [Menghapus perangkat seluler dari jarak jauh](#)
- [Menghapus perangkat pengguna dari daftar perangkat](#)
- [Melihat detail perangkat seluler](#)

Menghapus perangkat seluler dari jarak jauh

Langkah-langkah dalam bagian ini menjelaskan cara menghapus perangkat seluler dari jarak jauh. Ingat hal berikut:

- Perangkat harus online dan terhubung ke Amazon WorkMail. Jika seseorang memutuskan koneksi perangkat, operasi penghapusan akan dilanjutkan saat pengguna mengkoneksikan kembali perangkat.
- Operasi penghapusan bisa memakan waktu lima menit untuk menyebar.

⚠ Important

Untuk sebagian besar perangkat seluler, penghapusan jarak jauh akan menyetel ulang perangkat ke setelah default pabrik. Semua data, termasuk file pribadi, dapat dihapus saat Anda melakukan prosedur ini.

Menghapus perangkat seluler pengguna dari jarak jauh

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Nama Wilayah dan titik akhir](#) di. Referensi Umum Amazon Web

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Pengguna, dan dalam daftar pengguna, pilih nama pengguna yang perangkatnya perlu Anda hapus.
4. Pilih tab Perangkat seluler.
5. Dalam daftar perangkat, pilih tombol di sebelah perangkat, lalu pilih Wipe.
6. Periksa status dalam ikhtisar untuk melihat apakah penghapusan diminta.
7. Setelah perangkat dihapus, hapus dari daftar perangkat. Langkah-langkah di bagian selanjutnya menjelaskan caranya.

⚠ Important

Untuk mengembalikan perangkat yang dihapus ke daftar perangkat pengguna, pastikan Anda menghapusnya terlebih dahulu dari daftar perangkat. Jika tidak, sistem akan menghapus perangkat lagi.

Menghapus perangkat pengguna dari daftar perangkat

Jika seseorang berhenti menggunakan perangkat seluler tertentu, atau Anda telah menghapus perangkat dari jarak jauh, Anda dapat menghapus perangkat dari daftar perangkat. Saat pengguna mengonfigurasi perangkat lagi, perangkat tersebut akan muncul di daftar.

Menghapus perangkat seluler pengguna dari daftar perangkat

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Pengguna, lalu pilih nama pengguna.
4. Pilih tab Perangkat seluler.
5. Dalam daftar perangkat, pilih tombol di sebelah perangkat dan pilih Hapus.

Melihat detail perangkat seluler

Anda dapat melihat detail perangkat seluler pengguna.

Note

Beberapa perangkat tidak mengirim semua detailnya ke server. Anda mungkin tidak melihat semua detail perangkat yang tersedia.

Untuk melihat detail perangkat

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah . Dari bilah navigasi, pilih Wilayah yang memenuhi kebutuhan Anda. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, pilih Pengguna, lalu pilih tab Perangkat seluler.
4. Dalam daftar perangkat, pilih ID perangkat yang ingin Anda lihat detailnya.

Tabel berikut mencantumkan kode status perangkat.

Status	Deskripsi
PROVISIONING_REQUIRED	Pengguna atau administrator telah meminta agar perangkat disediakan untuk digunakan dengan Amazon. WorkMail Perangkat juga disetel ke status ini jika kebijakan saat ini untuk perangkat tersebut diubah di WorkMail konsol Amazon.
PROVISIONING_SUCCEEDED	Perangkat telah berhasil disediakan. Perangkat telah memberlakukan kebijakan yang diberikan.
WIPE_REQUIRED	Administrator meminta penghapusan di WorkMail konsol Amazon.
WIPE_SUCCEEDED	Perangkat telah berhasil dihapus.

Mengelola aturan akses perangkat seluler

Aturan akses perangkat seluler untuk Amazon WorkMail memungkinkan administrator mengontrol akses kotak pesan untuk jenis perangkat seluler tertentu. Secara default, setiap WorkMail organisasi Amazon menggunakan aturan yang memberikan akses kotak pesan ke perangkat apa pun, terlepas dari jenis, model, sistem operasi, atau agen pengguna. Anda dapat mengedit atau mengganti aturan default dengan salah satu aturan Anda sendiri. Anda juga dapat menambahkan, mengubah, dan menghapus aturan.

Warning

Jika Anda menghapus semua aturan akses perangkat seluler untuk suatu organisasi, Amazon WorkMail memblokir semua akses perangkat seluler.

Anda dapat membuat aturan yang mengizinkan atau menolak akses berdasarkan properti perangkat berikut ini:

- Jenis perangkat —"iPhone", "iPad", atau "Android."
- Model perangkat —"iPhone10C1", "iPad5C1", atau "HTConeX."
- Sistem operasi perangkat —"iOS 12.3.1 16F203", atau "Android 8.1.0."
- Agen pengguna perangkat — "iOS/14.2 (18B92) exchangesyncd/1 .0," atau "." Android-Mail/7.7.16.163886392.release

Untuk melihat properti perangkat di Konsol AWS Manajemen, lihat [Melihat detail perangkat seluler](#).

Note

Beberapa perangkat dan klien mungkin tidak melaporkan properti untuk semua bidang. Untuk informasi tentang cara menangani kasus tersebut, lihat [Dealing with empty fields](#)

Important

Aturan akses perangkat WorkMail seluler Amazon hanya berlaku untuk perangkat yang menggunakan ActiveSync protokol Microsoft Exchange. Klien seluler yang menggunakan protokol berbeda, seperti IMAP, tidak melaporkan properti perangkat yang tercantum di sini, sehingga aturan ini tidak akan berlaku.

Jika Anda perlu membatasi akses untuk perangkat yang menggunakan protokol lain, Anda dapat membuat aturan kontrol akses. Untuk informasi selengkapnya tentang mereka, lihat [Bekerja dengan aturan kontrol akses](#). Sebagai contoh, Anda dapat membatasi akses ke protokol dan webmail lain hanya untuk berbagai alamat IP perusahaan, tetapi mengizinkan Microsoft ActiveSync dari tempat lain, dan kemudian menggunakan Aturan Akses Perangkat Seluler untuk lebih membatasi jenis dan versi klien yang diizinkan.

Topik

- [Cara kerja aturan akses perangkat seluler](#)
- [Menggunakan aturan akses perangkat seluler](#)

Cara kerja aturan akses perangkat seluler

Aturan akses perangkat seluler hanya berlaku untuk perangkat yang menggunakan ActiveSync protokol Microsoft Exchange. Setiap aturan memiliki seperangkat kondisi yang menentukan kapan

aturan berlaku, ditambah efek akses ALLOW atau DENY untuk perangkat tersebut. Aturan berlaku untuk permintaan akses hanya jika semua kondisi aturan cocok dengan properti perangkat seluler pengguna. Aturan tanpa syarat berlaku untuk semua permintaan. Setiap kondisi menggunakan kecocokan prefiks peka huruf besar kecil terhadap properti yang dilaporkan perangkat.

Amazon WorkMail mengevaluasi aturan sebagai berikut:

- Jika aturan DENY cocok dengan properti perangkat, kebijakan memblokir perangkat tersebut. Aturan DENY diutamakan atas aturan ALLOW.
- Jika setidaknya satu aturan ALLOW cocok, dan tidak ada aturan DENY yang cocok, kebijakan mengizinkan perangkat.
- Jika tidak ada aturan yang berlaku, perangkat diblokir.

Important

Perangkat seluler melaporkan properti yang digunakan aturan untuk beroperasi. Perangkat melaporkan propertinya selama proses penyediaan ActiveSync perangkat Microsoft. Amazon WorkMail tidak dapat memverifikasi secara independen bahwa klien seluler melaporkan informasi yang benar atau terkini.

Menggunakan aturan akses perangkat seluler

Anda dapat menggunakan API atau Antarmuka Baris Perintah (CLI) AWS untuk membuat dan mengelola aturan akses perangkat seluler. Untuk informasi selengkapnya tentang ini AWS CLI, lihat [Panduan Pengguna Antarmuka Baris Perintah AWS](#).

Important

Bila Anda mengubah aturan akses untuk WorkMail organisasi Amazon, perangkat yang terpengaruh dapat memakan waktu lima menit untuk mengikuti aturan yang diperbarui, dan perangkat mungkin menunjukkan perilaku yang tidak konsisten selama waktu tersebut. Namun, Anda segera melihat perilaku yang benar ketika Anda menguji aturan. Untuk informasi selengkapnya, lihat [Testing mobile device access rules](#).

Membuat daftar aturan akses perangkat seluler

Contoh berikut menunjukkan cara membuat daftar aturan akses perangkat seluler.

```
aws workmail list-mobile-device-access-rules --organization-id  
m-a123b4c5de678fg9h0ij1k2lm234no56
```

Membuat aturan akses perangkat seluler

Contoh berikut membuat aturan yang memblokir semua perangkat Android agar tidak dapat mengakses kotak pesan.

```
aws workmail create-mobile-device-access-rule --organization-id  
m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types  
"android"
```

Contoh berikut membuat aturan yang hanya mengizinkan iOS versi tertentu. Pastikan untuk menghapus aturan ALLOW-all default.

```
aws workmail create-mobile-device-access-rule --organization-id  
m-a123b4c5de678fg9h0ij1k2lm234no56 --name AllowLatestiOS --effect ALLOW --device-  
operating-systems "iOS 14.3"
```

Memperbarui aturan akses perangkat seluler

Contoh berikut memperbarui aturan perangkat dengan menambahkan pengenalan.

```
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"
```

Menghapus aturan akses perangkat seluler

Contoh berikut menghapus aturan akses perangkat seluler dengan pengenalan yang diberikan.

```
aws workmail delete-mobile-device-access-rule --organization-id  
m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

Menguji aturan akses perangkat seluler

Untuk menguji aturan akses, Anda dapat menggunakan [GetMobileDeviceAccessEffectAPI](#), atau perintah `get-mobile-device-access-effect` di AWS CLI Untuk informasi selengkapnya tentang AWS CLI, lihat [Panduan Pengguna Antarmuka Baris AWS Perintah](#).

Ketika Anda menguji, Anda meloloskan properti perangkat seluler simulasi, dan API atau CLI mengembalikan efek akses—ALLOW atau DENY—bahwa perangkat seluler nyata dengan properti tersebut akan menerima. Misalnya, perintah ini menguji apakah iPhone yang menjalankan iOS 14.2, ditambah aplikasi email default, dapat mengakses kotak pesan.

```
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"
```

Berurusan dengan bidang kosong

Beberapa perangkat seluler atau klien mungkin tidak melaporkan informasi untuk satu atau lebih bidang, membiarkan nilai kosong. Aturan dapat cocok dengan perangkat ini dengan menggunakan nilai khusus \$NONE dalam suatu kondisi. Misalnya, aturan dengan DeviceTypes=["iphone", "ipad", "\$NONE"] akan cocok dengan perangkat yang melaporkan jenis perangkat "iphone" atau "ipad", atau tidak melaporkan jenis perangkat sama sekali.

Kondisi negatif seperti NotDeviceTypes atau tidak NotDeviceUserAgents akan cocok dengan nilai kosong ini. Misalnya, aturan dengan NotDeviceTypes=["android"] akan cocok dengan perangkat yang melaporkan jenis perangkat selain "android". Namun, aturan tidak akan cocok dengan perangkat yang tidak melaporkan jenis perangkat sama sekali.

Mengelola penggantian akses perangkat seluler

Anda menggunakan penggantian akses perangkat seluler untuk mengganti hasil aturan akses perangkat seluler. Penggantian berlaku untuk pengguna dan perangkat tertentu, dan membalikkan aturan akses default. Anda juga dapat menggunakan penggantian untuk membuat pengecualian satu kali untuk mengakses aturan dan mengizinkan atau menolak pasangan pengguna dan perangkat tertentu. Selain itu, Anda dapat menggunakan penggantian dengan aturan akses perangkat DefaultDenyAll seluler. Itu menunda keputusan akses ke solusi manajemen perangkat seluler (MDM) pihak ketiga. Untuk informasi selengkapnya, lihat [Mengelola penggantian](#) dan [Mengintegrasikan dengan solusi manajemen perangkat seluler](#)

Topik

- [Cara kerja penggantian akses perangkat seluler](#)
- [Mengelola penggantian](#)

Cara kerja penggantian akses perangkat seluler

Anda membuat penggantian akses perangkat seluler untuk pengguna dan pasangan perangkat tertentu. Penggantian membalikkan hasil akses default saat mengevaluasi aturan akses perangkat seluler untuk pengguna dan perangkat tertentu. Misalnya, jika aturan akses biasanya menolak akses, penggantian akses memungkinkan pengguna dan perangkat untuk menyinkronkan email mereka. Sebaliknya, jika aturan akses biasanya mengizinkan akses, Anda dapat membuat penggantian yang mencegah pengguna dan perangkat menyinkronkan email mereka. Saat Anda menghapus penggantian akses perangkat seluler, Amazon WorkMail kembali menghormati hasil aturan akses perangkat seluler saat ini saat memutuskan apakah akan memberikan akses untuk pengguna dan perangkat tersebut.

Important

Saat Anda mengubah penggantian akses perangkat seluler untuk WorkMail organisasi Amazon, perangkat yang terpengaruh dapat memakan waktu lima menit untuk mengikuti penggantian yang diperbarui.

Mengelola penggantian

Penggantian akses perangkat seluler dapat dibuat, diperbarui, atau dihapus menggunakan API atau AWS Command Line Interface Untuk informasi selengkapnya tentang ini AWS CLI, lihat [Panduan Pengguna Antarmuka Baris Perintah AWS](#).

Untuk menemukan ID perangkat, gunakan file Konsol Manajemen AWS. Untuk informasi selengkapnya, lihat [Melihat detail perangkat seluler](#).

Daftar penggantian akses perangkat seluler

Contoh ini menunjukkan cara mencantumkan semua penggantian akses perangkat seluler untuk organisasi Amazon WorkMail tertentu.

```
aws workmail list-mobile-device-access-overrides --organization-id  
m-a123b4c5de678fg9h0ij1k2lm234no56
```

Membuat dan memperbarui penggantian akses perangkat seluler

Ini akan membuat penggantian akses perangkat seluler untuk menolak akses ke WorkMail organisasi Amazon, pengguna, dan ID perangkat yang ditentukan.

```
aws workmail put-mobile-device-access-override --organization-id  
m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-  
id 6APMEKPHCP2ND42VIJ4BR8ECDO --effect DENY
```

Penggantian akses perangkat seluler yang ada dapat dimodifikasi untuk memiliki efek yang berbeda. Ini akan memperbarui penggantian akses perangkat seluler yang dibuat sebelumnya untuk mengizinkan akses alih-alih menyangkal.

```
aws workmail put-mobile-device-access-override --organization-id  
m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-  
id 6APMEKPHCP2ND42VIJ4BR8ECDO --effect ALLOW
```

Menghapus penggantian akses perangkat seluler

Ini akan menghapus penggantian akses perangkat seluler untuk WorkMail organisasi Amazon, pengguna, dan ID perangkat yang ditentukan.

```
aws workmail delete-mobile-device-access-override --organization-id  
m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-  
id 6APMEKPHCP2ND42VIJ4BR8ECDO
```

Mengintegrasikan dengan solusi manajemen perangkat seluler

Amazon WorkMail mendukung beberapa kemampuan manajemen perangkat seluler dasar melalui kebijakan perangkat seluler dan aturan akses perangkat seluler. Namun, fitur tersebut hanya dapat berinteraksi dengan perangkat seluler melalui protokol Microsoft Exchange ActiveSync (EAS), sehingga mereka memiliki kemampuan terbatas untuk introspeksi dan menegakkan postur keamanan perangkat. Administrator yang membutuhkan kontrol lebih besar atas keamanan dan kepatuhan perangkat dapat menggunakan solusi manajemen perangkat seluler (MDM) pihak ketiga.

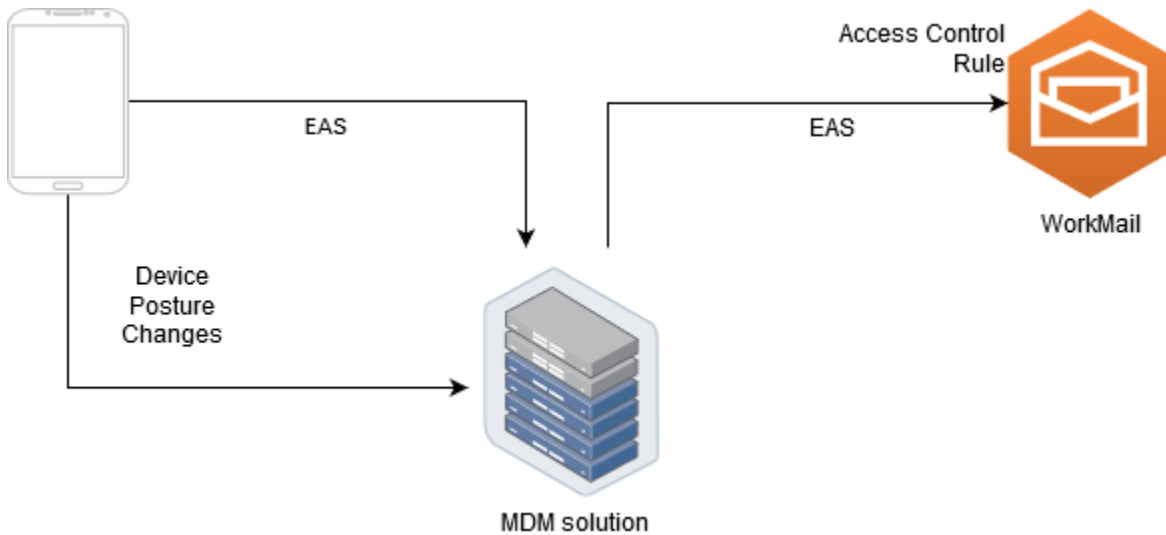
Ikhtisar solusi manajemen perangkat seluler

Anda dapat mengonfigurasi solusi MDM Anda dalam dua mode, proxy atau langsung. Konsultasikan dokumentasi MDM Anda untuk melihat mode mana yang didukung solusi Anda.

Dalam mode proxy, perangkat seluler menggunakan protokol Exchange Active Sync (EAS) melalui solusi MDM Anda untuk mengakses Amazon. WorkMail Solusi MDM menggunakan postur perangkat untuk mengizinkan atau menolak akses ke WorkMail data Amazon. Di WorkMail sisi Amazon,

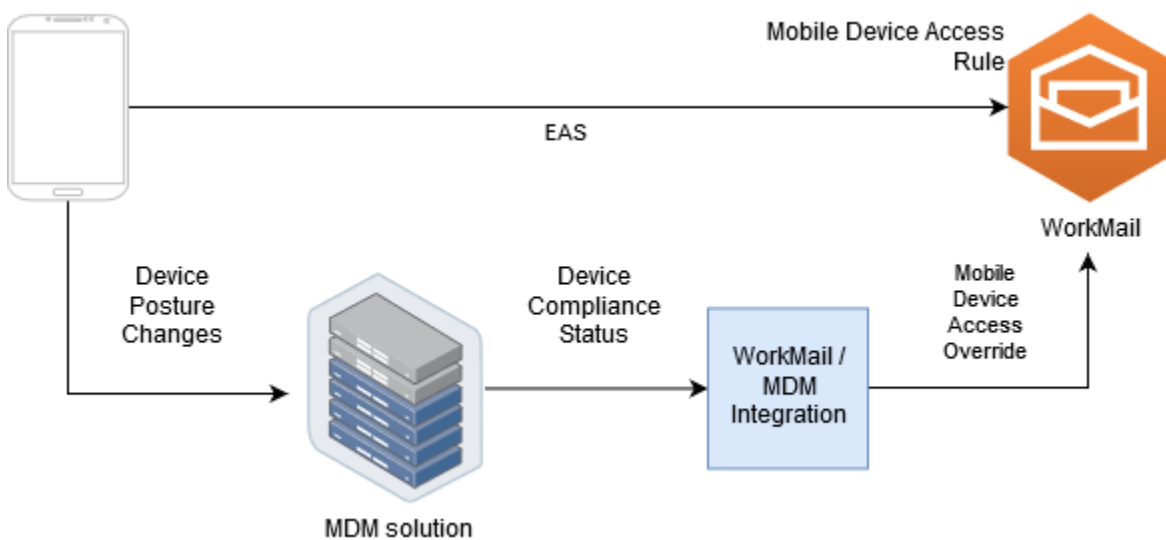
gunakan Aturan Kontrol Akses yang memungkinkan akses EAS hanya dari alamat IP atau alamat solusi MDM. Untuk informasi selengkapnya, lihat [Bekerja dengan aturan kontrol akses](#).

Gambar berikut menunjukkan konfigurasi mode proxy yang khas.



Dalam mode langsung, perangkat seluler menggunakan EAS untuk mengakses Amazon WorkMail secara langsung. Solusi MDM Anda menerima perubahan postur perangkat dan terus menilai apakah setiap perangkat memenuhi persyaratan tersebut. Ketika solusi MDM mendeteksi perubahan postur, seperti perangkat yang tidak sesuai, solusi MDM dapat mengambil beberapa tindakan dan biasanya memancarkan pemberitahuan atau peristiwa. WorkMail Administrator Amazon dapat menyiapkan sistem untuk mendengarkan peristiwa status kepatuhan ini dan secara otomatis membuat penggantian akses perangkat seluler yang mengizinkan atau menolak akses ke perangkat saat masuk atau tidak sesuai dengan persyaratan perangkat MDM.

Gambar berikut menunjukkan konfigurasi mode langsung yang khas.



Mengkonfigurasi WorkMail organisasi untuk berintegrasi dengan solusi MDM pihak ketiga dalam mode langsung

Untuk berintegrasi dengan solusi manajemen perangkat seluler (MDM) pihak ketiga dalam mode langsung, Anda harus memenuhi persyaratan ini:

- Buat aturan kontrol akses yang membatasi akses ke perangkat pengguna hanya pada ActiveSync protokol.
- Buat aturan akses perangkat seluler “tolak-ke-semua” default untuk memastikan bahwa semua perangkat seluler yang tidak dikenal atau tidak dikelola ditolak secara default.
- Mengadopsi solusi manajemen perangkat seluler yang memancarkan pemberitahuan atau peristiwa khusus saat perangkat mengubah postur keamanan, yang berarti perangkat masuk atau keluar dari kepatuhan.
- Buat komponen perangkat lunak khusus untuk mendengarkan notifikasi tersebut dan hubungi Amazon WorkMail SDK untuk membuat penggantian akses perangkat seluler.

Komponen ini memastikan bahwa semua perangkat pengguna memenuhi persyaratan kepatuhan MDM mereka sebelum diizinkan mengakses WorkMail kotak surat Amazon mereka.

Gunakan aturan kontrol akses untuk membatasi akses perangkat seluler ActiveSync

Anda harus memastikan bahwa semua perangkat hanya menggunakan ActiveSync protokol, dan Anda dapat menggunakan aturan kontrol akses untuk melakukannya. Misalnya, Anda dapat memberikan akses ke protokol email lain hanya dari rentang alamat IP perusahaan internal, dan kemudian mengizinkan hanya ActiveSync ketika mengakses email dari luar firewall perusahaan. Anda harus melakukan ini karena hanya ActiveSync memungkinkan Anda mengidentifikasi perangkat menggunakan ID perangkat. Anda tidak dapat menggunakan protokol seperti Internet Message Access Protocol (IMAP) atau Exchange Web Services. Untuk informasi selengkapnya, lihat [Bekerja dengan aturan kontrol akses](#).

Buat aturan akses 'tolak semua' default

Untuk menunda semua keputusan akses perangkat seluler ke solusi manajemen perangkat seluler pihak ketiga, buat aturan akses yang secara otomatis menolak semua perangkat kecuali diganti berdasarkan per pengguna atau per perangkat. Untuk informasi lebih lanjut, lihat [Mengelola aturan akses perangkat seluler](#).

Contoh ini menunjukkan aturan 'tolak semua'.

```
aws workmail create-mobile-device-access-rule --organization-id  
m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

Bereaksi terhadap perubahan postur perangkat dan buat penggantian akses perangkat seluler

Anda harus mengonfigurasi solusi MDM Anda untuk mengirim pemberitahuan perubahan postur perangkat. Pemberitahuan ini harus dikonsumsi oleh komponen yang dapat menggunakan Amazon WorkMail SDK untuk membuat atau memperbarui penggantian akses perangkat seluler. Secara default, Amazon WorkMail menolak akses ke perangkat yang tidak dikelola atau yang baru disediakan karena aturan akses perangkat seluler “tolak untuk semua” default yang ditampilkan sebelumnya dalam topik ini. Ketika solusi MDM menentukan bahwa perangkat memenuhi semua persyaratan dan mengeluarkan pemberitahuan yang menunjukkan bahwa perangkat tersebut sesuai, komponen ini dapat bereaksi terhadap pemberitahuan ini dengan membuat penggantian akses perangkat seluler dengan efek ALLOW untuk pengguna dan perangkat yang ditentukan. Jika perangkat nantinya tidak sesuai, solusi manajemen perangkat seluler akan mengeluarkan pemberitahuan lain, dan penggantian akses dapat dihapus atau dimodifikasi untuk menolak akses perangkat tersebut. Untuk informasi selengkapnya, lihat [Mengelola penggantian akses perangkat seluler](#).

Untuk contoh Amazon yang WorkMail terintegrasi dengan MDM, lihat [AWS contoh aplikasi](#) ini.

Bekerja dengan izin kotak pesan

Anda dapat menggunakan izin kotak pesan di Amazon WorkMail untuk memberi pengguna dan grup hak untuk bekerja di kotak pesan pengguna lain. Izin kotak pesan berlaku untuk seluruh kotak pesan. Mereka memungkinkan beberapa pengguna mengakses kotak pesan yang sama tanpa membagikan kredensi kotak pesan tersebut. Pengguna dengan izin kotak pesan dapat membaca dan mengubah data kotak pesan serta mengirim email dari kotak pesan bersama.

Note

Pengguna dengan izin ke kotak pesan milik pengguna yang disembunyikan dari daftar alamat global masih dapat mengakses kotak pesan pengguna tersebut.

Daftar berikut menunjukkan izin yang dapat Anda berikan:

- **Akses Penuh** — Memungkinkan akses baca dan tulis penuh ke kotak pesan, termasuk izin untuk mengubah izin tingkat folder.

Note

Opsi ini hanya tersedia untuk pengguna. Grup tidak dapat diberikan hak akses penuh.

- **Kirim Atas Nama** - Memungkinkan pengguna atau grup untuk mengirim email atas nama pengguna lain. Pemilik kotak pesan muncul di header Dari:, dan pengirim muncul di header Pengirim:.
- **Kirim Sebagai** — Memungkinkan pengguna atau grup untuk mengirim email sebagai pemilik kotak pesan, tanpa menunjukkan pengirim pesan yang sebenarnya. Pemilik kotak pesan muncul di header Dari: dan header Pengirim:.
- **Tidak ada** - Mencegah pengguna atau grup mengirim email.

Note

Pemberian izin kotak pesan ke grup memperluas izin tersebut ke semua anggota grup, termasuk anggota grup bersarang.

Saat Anda memberikan izin kotak pesan, WorkMail AutoDiscover layanan Amazon secara otomatis memperbarui akses ke kotak pesan tersebut untuk pengguna atau grup yang Anda tambahkan.

Untuk klien Microsoft Outlook di Windows, pengguna dengan izin akses penuh dapat secara otomatis mengakses kotak pesan bersama. Biarkan hingga 60 menit agar perubahan menyebar, lalu restart Microsoft Outlook.

Untuk aplikasi WorkMail web Amazon dan klien email lainnya, pengguna dengan izin akses penuh dapat membuka kotak surat bersama secara manual. Kotak pesan yang dibuka akan tetap terbuka, bahkan di antara sesi, kecuali pengguna menutupnya.

Topik

- [Tentang izin kotak pesan dan folder](#)
- [Mengelola izin kotak pesan untuk pengguna](#)
- [Mengelola izin kotak pesan untuk grup](#)

Tentang izin kotak pesan dan folder

Izin kotak pesan berlaku untuk semua folder dalam kotak pesan. Izin ini hanya dapat diaktifkan oleh pemegang AWS akun atau pengguna IAM yang berwenang untuk memanggil API WorkMail manajemen Amazon. Untuk mengatur dan mengubah izin kotak pesan, atau untuk grup secara keseluruhan, gunakan API Amazon Konsol Manajemen AWS atau Amazon WorkMail . Anda dapat mengelola hingga 100 kotak pesan dan izin grup dari konsol. Untuk mengelola izin bagi lebih banyak pengguna dan grup, gunakan Amazon WorkMail API.

Izin folder hanya berlaku untuk satu folder. Pengguna akhir dapat mengatur izin folder dengan menggunakan klien email, atau dengan menggunakan aplikasi WorkMail web Amazon. Untuk informasi selengkapnya tentang menggunakan aplikasi WorkMail web Amazon untuk berbagi folder, lihat [Berbagi folder dan izin folder](#) di Panduan WorkMail Pengguna Amazon.

Mengelola izin kotak pesan untuk pengguna

Anda dapat menggunakan WorkMail konsol Amazon untuk mengelola izin kotak pesan bagi pengguna, serta grup. Bagian berikut menjelaskan cara mengelola izin untuk pengguna. Untuk informasi tentang mengelola izin untuk grup, lihat. [Mengelola izin kotak pesan untuk grup](#)

Topik

- [Menambahkan izin](#)
- [Mengedit izin kotak pesan untuk pengguna](#)

Menambahkan izin

Saat menambahkan izin, Anda memberi satu pengguna hak untuk melakukan satu atau beberapa tugas di kotak pesan pengguna lain. Misalnya, katakan bahwa Karyawan A perlu mengirim pesan atas nama atasannya, Karyawan B. Untuk memberikan izin tersebut, Anda pergi ke pengaturan kotak pesan Karyawan B dan memberikan izin kepada Karyawan A untuk melakukan tugas yang diminta.

Untuk menambahkan izin kotak pesan

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah . Dari bilah navigasi, pilih Wilayah yang memenuhi kebutuhan Anda. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi yang ingin Anda kelola izinnya.
3. Di panel navigasi, pilih Pengguna, lalu pilih nama pengguna yang ingin Anda kelola izin.
4. Pilih tab Izin, lalu pilih Tambahkan izin.

Kotak dialog Add Permissions muncul.

5. Buka daftar Tambahkan izin baru dan pilih pengguna atau grup yang memerlukan akses ke kotak pesan.
6. Di bawah Izin kotak surat dan izin Kirim, pilih opsi yang diinginkan.
7. Pilih Tambahkan.

Izin baru dapat memakan waktu hingga lima menit untuk disebarkan ke pengguna.

Mengedit izin kotak pesan untuk pengguna

Saat mengedit izin kotak pesan untuk pengguna, Anda mengubah akses yang dimiliki orang lain ke kotak pesan pengguna tersebut. Mengedit izin kotak pesan tidak mengubah akses untuk pengguna asli kotak pesan.

Untuk mengedit izin kotak pesan

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah . Dari bilah navigasi, pilih Wilayah yang memenuhi kebutuhan Anda. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi yang ingin Anda kelola izinnnya.
3. Di panel navigasi, pilih Pengguna, lalu pilih nama pengguna yang izinnnya ingin Anda edit.
4. Pilih tab Izin.

Daftar pengguna dan grup yang memiliki akses ke kotak pesan muncul.

5. Pilih tombol radio di sebelah pengguna atau grup yang ingin Anda ubah, lalu lakukan salah satu hal berikut:

Untuk menghapus izin pengguna

1. Pilih Hapus.

Kotak dialog Hapus izin muncul.

2. Dalam kotak dialog Hapus izin, pilih Hapus.

Untuk mengedit izin pengguna

1. Pilih Edit.

Kotak dialog Edit izin muncul.

2. Tetapkan izin sesuai kebutuhan, lalu pilih Simpan.

Untuk memberikan izin pengguna lain ke kotak pesan

1. Pilih Tambahkan izin.

Kotak dialog Add Permissions muncul.

2. Buka daftar Tambahkan izin baru dan pilih pengguna yang ingin Anda tambahkan.
3. Tetapkan izin sesuai kebutuhan, lalu pilih Tambah.

Perubahan izin dapat memakan waktu hingga lima menit untuk disebarakan ke pengguna.

Mengelola izin kotak pesan untuk grup

Anda dapat menambah atau menghapus izin grup untuk Amazon WorkMail.

Note

Anda tidak dapat menerapkan izin Akses Penuh ke grup, karena grup tidak memiliki kotak pesan untuk diakses.

Untuk mengelola izin grup

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah AWS Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi yang ingin Anda kelola izinnya.
3. Di panel navigasi, pilih Grup, lalu pilih nama grup yang ingin Anda tetapkan izinnya.
4. Pilih tab Izin, lalu pilih Tambahkan izin.

Kotak dialog Add Permissions muncul.

5. Buka daftar Tambahkan izin baru dan pilih pengguna atau grup untuk memberikan izin untuk kotak pesan.
6. Di bawah Izin kotak surat dan izin Kirim, pilih opsi yang diinginkan.
7. Pilih Tambahkan.

Perubahan izin dapat memakan waktu hingga lima menit untuk disebarkan ke pengguna.

Akses terprogram ke kotak surat

Untuk mengakses WorkMail kotak surat Amazon secara terprogram, gunakan protokol Exchange Web Services (EWS). Dengan EWS, Anda dapat mengakses semua jenis item di kotak pesan. Berikut adalah beberapa pustaka EWS yang dapat Anda gunakan dengan Amazon: WorkMail

- Java - [EWS Java API](#)
- .Net - API [Terkelola EWS](#)
- Python — [Exchangelib](#)

Amazon WorkMail juga mendukung protokol IMAP dan SMTP, yang dapat Anda gunakan untuk mengirim dan menerima email. Anda dapat melihat URL yang didukung untuk WorkMail protokol Amazon di bawah titik [WorkMailakhir dan kuota Amazon](#).

Saat menggunakan protokol EWS, Amazon WorkMail mendukung metode otentikasi berikut:

- Otentikasi Dasar — Dengan otentikasi dasar, Anda memasukkan alamat email dan kata sandi.
- Peran peniruan identitas — Dengan peran peniruan identitas, Anda mengakses kotak pesan pengguna tanpa memasukkan kredensial pengguna.

Topik

- [Mengelola peran peniruan](#)
- [Menggunakan peran peniruan](#)

Mengelola peran peniruan

Dengan peran peniruan identitas, administrator mengonfigurasi akses terprogram ke kotak pesan pengguna tanpa memasukkan kredensial pengguna. Layanan dan alat dapat mengambil peran peniruan identitas untuk melakukan tindakan di kotak pesan pengguna. Peniruan identitas hanya didukung dengan protokol EWS.

Ikhtisar peran peniruan

Untuk mengizinkan peniruan identitas, administrator harus membuat peran peniruan identitas dengan properti berikut:

- Jenis peran — Pilih Akses penuh atau Hanya Baca. Jenis peran membatasi jenis operasi yang dapat dilakukan peran.
- Aturan — Daftar aturan yang menentukan pengguna mana yang dapat ditiru oleh peran peniruan identitas.

Amazon WorkMail mengevaluasi aturan pada kondisi berikut:

- Jika ada aturan DENY yang cocok, kebijakan tersebut menolak peniruan identitas. Aturan DENY lebih diutamakan daripada aturan ALLOW.
- Jika setidaknya satu aturan ALLOW cocok, dan tidak ada aturan DENY yang cocok, kebijakan tersebut mengizinkan peniruan identitas.
- Jika tidak ada aturan yang berlaku, peniruan identitas ditolak.

Note

Untuk mengizinkan peniruan identitas untuk semua pengguna di WorkMail organisasi Amazon, buat aturan dengan efek ALLOW dan tanpa kondisi.

Warning

Anda harus membuat aturan untuk mengizinkan peran peniruan identitas untuk meniru pengguna. Jika Anda tidak menentukan aturan, peran peniruan identitas tidak dapat mengambil hak akses pengguna.

Setelah peran peniruan identitas dibuat, Anda dapat menggunakannya untuk mendapatkan akses ke kotak pesan pengguna. Untuk informasi selengkapnya, lihat [Menggunakan peran peniruan](#).

Pertimbangan keamanan

Penggunaan peran peniruan identitas menciptakan potensi masalah keamanan dalam WorkMail organisasi Amazon Anda dan. Akun AWS Berikut adalah beberapa masalah potensial yang perlu dipertimbangkan saat Anda membuat peran peniruan:

- Izin transitif — Jika pengguna A memiliki akses ke kotak pesan pengguna B, dan peran peniruan identitas diizinkan untuk menyamar sebagai pengguna A, maka peran peniruan identitas ini dapat meniru izin akses pengguna A dan mengakses kotak pesan B pengguna.
- Kontrol akses — Anda dapat menggunakan aturan kontrol akses untuk membatasi akses peran peniruan identitas. Untuk informasi selengkapnya, lihat [Bekerja dengan aturan kontrol akses](#).
- Kebijakan IAM — Anda dapat menetapkan `AssumeImpersonationRole` tindakan ke WorkMail organisasi Amazon tertentu dan peran peniruan dengan menggunakan kondisi tersebut. `workmail:ImpersonationRoleId` Untuk melihat contoh kebijakan IAM, lihat [Bagaimana Amazon WorkMail bekerja dengan IAM](#).

Membuat peran peniruan


Anda dapat membuat peran peniruan identitas dari konsol Amazon WorkMail .

Untuk membuat peran peniruan

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.
Jika perlu, ubah Wilayah . Dari bilah navigasi, pilih Wilayah yang memenuhi kebutuhan Anda. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.
2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi.
3. Pilih Peran peniruan identitas, lalu pilih Buat peran.
4. Kotak dialog Create impersonation role muncul. Di bawah Peran, masukkan informasi berikut:
 - Nama — Masukkan nama unik untuk peran peniruan identitas.
 - (Opsional) Deskripsi — Masukkan deskripsi untuk peran peniruan identitas.
 - Jenis peran — Pilih Hanya Baca atau Akses penuh.
5. Di bawah Aturan, pilih Tambahkan aturan.
6. Kotak dialog Tambah aturan muncul. Masukkan informasi berikut:
 - Nama — Masukkan nama unik untuk aturan.
 - (Opsional) Deskripsi — Masukkan deskripsi untuk aturan.
 - Di bawah Efek, pilih Izinkan atau Tolak. Ini memungkinkan atau menolak akses berdasarkan kondisi yang Anda pilih pada langkah berikut.
 - (Opsional) Di bawah Aturan ini:, pilih Permintaan kecocokan yang meniru pengguna yang dipilih untuk menyertakan pengguna tertentu. Pilih permintaan Cocokkan yang meniru

pengguna selain pengguna yang dipilih untuk menambahkan pengguna selain pengguna yang dipilih.

7. Pilih Tambahkan aturan.

 Note

Aturan hanya disimpan ketika Anda menyimpan peran yang sesuai.

8. Pilih Buat peran.

Mengedit peran peniruan

Anda dapat mengedit peran peniruan identitas dari konsol Amazon WorkMail .

Untuk mengedit peran peniruan

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah . Dari bilah navigasi, pilih Wilayah yang memenuhi kebutuhan Anda. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi.
3. Pilih peran peniruan identitas.
4. Pilih nama peran peniruan identitas yang ingin Anda edit, lalu pilih Edit.
5. Kotak dialog Edit peran peniruan muncul. Di bawah Peran, masukkan informasi berikut:
 - Nama — Masukkan nama unik untuk peran peniruan identitas.
 - (Opsional) Deskripsi — Masukkan deskripsi untuk peran peniruan identitas.
 - Jenis peran — Untuk memberikan akses hanya membaca peran peniruan ke kotak pesan pengguna, pilih Hanya baca. Untuk memberikan hak peran peniruan identitas untuk membaca dan mengubah item di kotak pesan pengguna, pilih Akses penuh.
6. Di bawah Aturan, pilih aturan yang ingin Anda edit dan pilih Edit.
7. Kotak dialog Edit rule muncul. Masukkan informasi berikut:
 - Nama — Edit nama aturan.
 - (Opsional) Deskripsi - Perbarui atau masukkan deskripsi untuk aturan.

- Di bawah Efek, pilih Izinkan untuk mengizinkan akses ketika kondisi yang ditetapkan dalam aturan terpenuhi. Untuk menolak akses, pilih Tolak.
 - (Opsional) Di bawah Aturan ini:, pilih Permintaan kecocokan yang meniru pengguna yang dipilih untuk menyertakan pengguna tertentu. Pilih permintaan Cocokkan yang meniru pengguna selain pengguna yang dipilih untuk menambahkan pengguna selain pengguna yang dipilih.
8. Pilih Simpan.
 9. Pilih Simpan perubahan.

Important

Bila Anda mengubah aturan peniruan identitas, kotak pesan yang terpengaruh dapat memakan waktu hingga lima menit untuk diperbarui. Selama proses pembaruan aturan, Anda dapat mengamati perilaku yang tidak konsisten di kotak pesan. Namun, jika Anda menguji peran, Amazon WorkMail merespons seperti yang diharapkan berdasarkan aturan yang diperbarui. Untuk informasi selengkapnya, lihat [Menguji peran peniruan](#).

Menguji peran peniruan

Anda dapat menguji peran peniruan identitas dari konsol Amazon WorkMail .

Untuk menguji peran peniruan

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah . Dari bilah navigasi, pilih Wilayah yang memenuhi kebutuhan Anda. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi.
3. Pilih peran peniruan identitas.
4. Pilih peran peniruan identitas yang ingin Anda uji.
5. Pilih Peran uji.
6. Kotak dialog Test impersonation role muncul. Di bawah Target pengguna, pilih pengguna yang ingin Anda uji akses peniruan identitas.
7. Pilih Uji.

Menghapus peran peniruan

Anda dapat menghapus peran peniruan identitas dari konsol Amazon WorkMail .

Untuk menghapus peran peniruan identitas

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah Wilayah . Dari bilah navigasi, pilih Wilayah yang memenuhi kebutuhan Anda. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi.
3. Pilih peran peniruan identitas.
4. Pilih nama peran peniruan identitas yang ingin Anda hapus.
5. Pilih Hapus.
6. Kotak dialog Hapus peran muncul. Untuk mengonfirmasi penghapusan, masukkan nama peran ke dalam kotak dialog dan pilih Hapus.

Menggunakan peran peniruan

Untuk mengakses data kotak pesan, gunakan tindakan `AssumeImpersonationRole` Amazon WorkMail API. Untuk detail selengkapnya tentang Amazon WorkMail API, lihat [Referensi API](#).

`AssumeImpersonationRole` mengembalikan `aToken`. Ini Token harus diteruskan dalam waktu 15 menit ke protokol EWS melalui header `Authorization` HTTP.

Contoh berikut menunjukkan cara menggunakan peran peniruan dengan protokol EWS. Konstanta yang digunakan dalam contoh menentukan detail berikut yang unik untuk organisasi dan akun Anda:

- `WORKMAIL_ORGANIZATION_ID`— ID WorkMail organisasi Amazon
- `IMPERSONATION_ROLE_ID`— ID peran peniruan identitas
- `WORKMAIL_EWS_URL`— Titik akhir EWS tersedia di titik akhir dan [kuota Amazon WorkMail](#)
- `EMAIL_ADDRESS`— Alamat email kotak pesan pengguna

Example Jawa — [EWS Java API](#)

```
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 — API Terkelola EWS

```
using Amazon.WorkMail;
using Amazon.WorkMail.Model;

using Microsoft.Exchange.WebServices.Data;

// ...

AssumeImpersonationRoleRequest request = new AssumeImpersonationRoleRequest();
request.OrganizationId = WORKMAIL_ORGANIZATION_ID;
request.ImpersonationRoleId = IMPERSONATION_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, IMPERSONATION
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
)
```

Mengekspor konten kotak pesan

Gunakan tindakan [StartMailboxExportJob](#) API di Referensi Amazon WorkMail API untuk mengekspor konten WorkMail kotak pesan Amazon ke bucket Amazon Simple Storage Service (Amazon S3). Tindakan ini mengekspor semua pesan email dan item kalender dari kotak pesan yang ditentukan ke file .zip di bucket Amazon S3, dalam format MIME. Item lain, seperti kontak dan tugas, tidak diekspor.

Waktu yang diperlukan untuk menyelesaikan tugas ekspor kotak pesan tergantung pada ukuran dan jumlah item di kotak pesan. Karena tugas ekspor kotak pesan berlangsung selama periode waktu tertentu, itu tidak mewakili snapshot konten kotak pesan pada satu titik waktu. Untuk melihat status pekerjaan ekspor, gunakan tindakan [DescribeMailboxExportJob](#) atau [ListMailboxExportJobs](#) API di Referensi WorkMail API Amazon.

Saat tugas ekspor kotak pesan selesai, .zip file di bucket Amazon S3 dienkripsi menggunakan AWS Key Management Service symmetric AWS KMS() customer master key (CMK) yang Anda berikan. Karena AWS KMS enkripsi terintegrasi dengan Amazon S3, data yang didekripsi terlihat oleh pengguna yang mengunduhnya, selama pengguna memiliki akses ke CMK. AWS KMS

Prasyarat

Berikut ini adalah prasyarat untuk mengekspor konten kotak pesan:

- Kemampuan untuk memprogram.
- Akun WorkMail administrator Amazon.
- Sebuah bucket Amazon S3 yang tidak mengizinkan akses publik. Untuk informasi selengkapnya, lihat [Menggunakan Amazon S3 memblokir akses publik](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon dan Panduan Pengguna [Layanan Penyimpanan Sederhana Amazon](#).
- CMK simetris AWS KMS . Untuk informasi lebih lanjut, lihat [Memulai](#) di Panduan Developer.AWS Key Management Service
- Peran AWS Identity and Access Management (IAM) dengan kebijakan yang memberikan izin untuk menulis ke bucket Amazon S3 dan mengenkripsi file yang dikirim dengan CMK. AWS KMS Untuk informasi selengkapnya, lihat [Bagaimana Amazon WorkMail bekerja dengan IAM](#).

Contoh kebijakan IAM dan pembuatan peran

Contoh berikut menunjukkan kebijakan IAM yang memberikan izin untuk menulis ke bucket Amazon S3 dan mengenkripsi file yang dikirim dengan CMK. AWS KMS Untuk menggunakan kebijakan contoh ini berikut: prosedur [Contoh: Mengekspor konten kotak surat](#), menyimpan kebijakan sebagai file JSON dengan nama file `mailbox-export-policy.json`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetBucketPolicyStatus"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/KEY-ID"
      ],
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "s3.us-east-1.amazonaws.com"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-
demo-bucket/S3-PREFIX*"
        }
      }
    }
  ]
}
```

```

    }
  ]
}

```

Contoh berikut adalah kebijakan kepercayaan IAM yang melekat pada IAM role yang Anda buat. Untuk menggunakan kebijakan contoh ini berikut: prosedur [Contoh: Mengekspor konten kotak surat](#), menyimpan kebijakan sebagai file JSON dengan nama file `mailbox-export-trust-policy.json`.

Anda tidak harus menggunakan `aws:SourceArn` dan `aws:SourceAccount` kondisi secara bersamaan. Misalnya, Anda dapat menghapus `aws:SourceArn` dari kebijakan jika Anda perlu menggunakan peran yang sama untuk mengeksport pesan dari WorkMail organisasi Amazon yang berbeda di bawah AWS akun yang sama. Untuk informasi selengkapnya tentang kunci kondisi, lihat [kunci konteks kondisi AWS global](#) di panduan pengguna AWS Identity and Access Management.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "export.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workmail:us-east-1:111122223333:organization/m-a123b4c5de678fg9h0ij1k2lm234no56"
        }
      }
    }
  ]
}

```

Anda dapat menggunakan AWS CLI untuk membuat peran IAM di akun Anda dengan menjalankan perintah berikut.

```
aws iam create-role --role-name WorkmailMailboxExportRole --assume-role-policy-document file://mailbox-export-trust-policy.json --region us-east-1
```

```
aws iam put-role-policy --role-name WorkmailMailboxExportRole --policy-name MailboxExport --policy-document file://mailbox-export-policy.json
```

Untuk informasi selengkapnya tentang AWS CLI, lihat [Panduan AWS Command Line Interface Pengguna](#).

Contoh: Mengekspor konten kotak surat

Setelah Anda membuat IAM role dan kebijakannya di bagian sebelumnya, selesaikan langkah-langkah berikut untuk mengekspor konten kotak pesan. Anda harus memiliki ID WorkMail organisasi Amazon dan ID pengguna (ID entitas), yang dapat Anda akses di WorkMail konsol Amazon atau dengan menggunakan Amazon WorkMail API.

Contoh: Untuk mengekspor konten kotak pesan

1. Gunakan tombol AWS CLI untuk memulai pekerjaan ekspor kotak pesan.

```
aws workmail start-mailbox-export-job --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56 --entity-id S-1-1-11-1111111111-222222222-3333333333-3333 --kms-key-arn arn:aws:kms:us-east-1:111122223333:key/KEY-ID --role-arn arn:aws:iam::111122223333:role/WorkmailMailboxExportRole --s3-bucket-name amzn-s3-demo-bucket --s3-prefix S3-PREFIX
```

2. Gunakan AWS CLI untuk memantau status pekerjaan ekspor kotak pesan untuk WorkMail organisasi Amazon Anda.

```
aws workmail list-mailbox-export-jobs --organization-id m-a123b4c5de678fg9h0ij1k2lm234no56
```

Atau, gunakan ID tugas yang dihasilkan oleh perintah **start-mailbox-export-job** untuk memantau status tugas ekspor kotak pesan itu saja.

```
aws workmail describe-mailbox-export-job --organization-id m-  
a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
```

Ketika satu tugas ekspor kotak pesan SELESAI, item kotak pesan yang diekspor tersedia di file .zip di bucket Amazon S3 yang ditentukan.

Berikut ini adalah contoh log keluaran dari kotak surat yang diekspor:

```
{  
  "totalNonExportableItems" : "13",  
  "totalMessages" : "76",  
  "sha384Hash" : "4de93a***96a1dd",  
  "totalBytes" : "161892",  
  "totalFolders" : "15",  
  "startTime" : "168***380",  
  "endTime" : "168***384"  
}
```

Note

total NonExportableItems adalah item yang tidak didukung seperti catatan dan kontak.

Pertimbangan-pertimbangan

Pertimbangan berikut berlaku saat mengekspor pekerjaan kotak surat untuk Amazon: WorkMail

- Anda dapat menjalankan hingga 10 pekerjaan ekspor kotak pesan bersamaan untuk organisasi Amazon WorkMail tertentu.
- Anda dapat menjalankan tugas ekspor kotak pesan untuk kotak pesan tertentu sesering setiap 24 jam sekali.
- Semua sumber daya berikut harus berada di AWS Wilayah yang sama:
 - WorkMail Organisasi Amazon
 - AWS KMS CMK
 - Buket Amazon S3

Pemecahan Masalah

Topik di bagian ini menjelaskan cara memecahkan masalah di Amazon WorkMail

Topik

- [Melihat header email](#)
- [Perutean surat](#)

Melihat header email

Informasi dalam header email dapat membantu Anda memecahkan masalah email pengguna yang umum. Amazon WorkMail memungkinkan Anda untuk melihat informasi header untuk pesan apa pun.

Untuk melihat header email di Amazon WorkMail

1. Di aplikasi WorkMail web Amazon, klik dua kali pada pesan email untuk membuka.
2. Pilih Opsi pesan (ikon roda gigi dan amplop) yang terletak di sudut kanan atas pesan, di sebelah Terkirim pada tanggal.

Header email muncul di bawah Header Internet.

Perutean surat

Jika pengguna berhenti menerima email, WorkMail organisasi Amazon Anda mungkin mengalami masalah perutean email. Langkah-langkah di bagian ini menjelaskan cara-cara umum untuk menyelesaikan masalah pengiriman dan perutean.

Masalah surat masuk:

- Periksa data MX untuk domain yang terkait dengan WorkMail organisasi Amazon Anda. WorkMail harus menjadi satu-satunya entri dan harus memiliki prioritas terendah. Beberapa catatan MX dapat menyebabkan layanan yang salah menerima pesan. Untuk informasi selengkapnya tentang catatan MX, lihat [Memverifikasi domain](#).
- Periksa pengaturan Otentikasi Domain-based Pesan, Pelaporan, dan Kesesuaian (DMARC) untuk organisasi Anda di konsol Amazon WorkMail. Catatan DMARC digunakan untuk melindungi terhadap serangan umum, seperti spoofing atau phishing, yang dapat membahayakan kredensi

akun pengguna. Untuk informasi lebih lanjut tentang DMARC, lihat. [Memberlakukan kebijakan DMARC pada email masuk](#)

- Periksa aturan masuk Layanan Email Sederhana Amazon. Jika aturan berisi tindakan selain Amazon WorkMail, tindakan tersebut dapat gagal dan WorkMail menyebabkan Amazon berhenti menerima email. Untuk informasi selengkapnya tentang aturan Amazon SES, lihat [Mengintegrasikan dengan WorkMail tindakan Amazon](#) di Panduan Pengembang Layanan Email Sederhana Amazon.
- Aktifkan pelacakan pesan di Amazon WorkMail, lalu periksa log untuk masalah pengiriman. Untuk informasi selengkapnya tentang pelacakan pesan, lihat [Mengaktifkan pencatatan peristiwa email](#).

Masalah surat keluar

- Pastikan catatan SPF Anda termasuk Amazon SES. Periksa halaman domain di WorkMail konsol Amazon untuk memverifikasi. Untuk informasi lebih lanjut tentang SPF, lihat [Mengautentikasi Email dengan SPF](#).
- Pastikan Amazon WorkMail memiliki izin untuk menggunakan domain. Jika tidak, tambahkan domain lagi. [Menambahkan domain](#) dalam panduan ini memberikan langkah-langkah cara.

Menggunakan jurnal email dengan Amazon WorkMail

Anda dapat mengatur penjurnalan untuk merekam komunikasi email, menggunakan alat pengarsipan pihak ketiga dan eDiscovery yang terintegrasi. Hal ini memastikan bahwa peraturan kepatuhan penyimpanan email untuk perlindungan privasi, penyimpanan data, dan perlindungan informasi terpenuhi.

Menggunakan penjurnalan

Amazon membuat WorkMail jurnal semua pesan email yang dikirim ke pengguna mana pun di organisasi tertentu, serta semua pesan email yang dikirim oleh pengguna di organisasi tersebut. Salinan semua pesan email dikirim ke alamat yang ditentukan oleh administrator sistem, dalam format yang disebut `journal record`. Format ini kompatibel dengan program email Microsoft. Tidak ada biaya tambahan untuk penjurnalan email.

Dua alamat email digunakan untuk penjurnalan email—alamat email penjurnalan dan alamat email laporan. Alamat email penjurnalan adalah alamat kotak pesan khusus atau perangkat pihak ketiga yang terintegrasi dengan akun Anda, tempat laporan jurnal dikirim. Alamat email laporan adalah alamat administrator sistem Anda, di mana pemberitahuan laporan jurnal gagal dikirim.

Semua catatan jurnal dikirim dari alamat email yang secara otomatis ditambahkan ke domain Anda dan terlihat seperti berikut ini.

```
amazonjournaling@yourorganization.awsapps.com
```

Tidak ada kotak pesan yang terkait dengan alamat ini, dan Anda tidak akan dapat membuatnya menggunakan nama atau alamat ini.

Note

Jangan hapus catatan domain berikut dari konsol Amazon Simple Email Service (Amazon SES), atau penjurnalan email berhenti berfungsi.

```
yourorganization.awsapps.com
```


Setiap pesan email masuk atau keluar menghasilkan satu catatan jurnal, terlepas dari jumlah penerima atau grup pengguna. Email yang gagal menghasilkan catatan jurnal menghasilkan notifikasi galat, yang dikirim ke alamat email laporan.

Untuk mengaktifkan penjurnalan email

1. Buka WorkMail konsol Amazon di <https://console.aws.amazon.com/workmail/>.

Jika perlu, ubah AWS Wilayah. Di bilah di bagian atas jendela konsol, buka daftar Pilih Wilayah dan pilih Wilayah. Untuk informasi selengkapnya, lihat [Wilayah dan titik akhir](#) di Referensi Umum Amazon Web.

2. Di panel navigasi, pilih Organizations, lalu pilih nama organisasi Anda.
3. Di panel navigasi, Pengaturan organisasi, pilih tab Jurnal, lalu pilih Edit.
4. Pindahkan slider status Journaling ke posisi on.
5. di kotak Jurnal alamat email, masukkan alamat email yang diberikan oleh penyedia jurnal email Anda.

 Note

Kami merekomendasikan penggunaan penyedia penjurnalan khusus.

6. Di alamat email Laporkan, masukkan alamat administrator email.
7. Pilih Simpan. Perubahan berlaku segera.

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting dalam setiap rilis Panduan WorkMail Administrator Amazon. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Pemberitahuan akhir dukungan	Pemberitahuan akhir dukungan: Pada 31 Maret 2027, AWS akan mengakhiri dukungan untuk Amazon WorkMail. Setelah 31 Maret 2027, Anda tidak akan lagi dapat mengakses WorkMail konsol Amazon atau WorkMail sumber daya Amazon. Untuk informasi selengkapnya, lihat dukungan WorkMail akhir Amazon .	Maret 31, 2026
Dukungan pencatatan audit	Log audit dapat digunakan untuk memantau akses pengguna ke kotak pesan, mengaudit aktivitas mencurigakan, dan men-debug kontrol akses dan konfigurasi penyedia ketersediaan. Untuk informasi selengkapnya, lihat Mengaktifkan pencatatan audit dan Pencatatan dan pemantauan di Amazon WorkMail di Panduan WorkMail Administrator Amazon.	Maret 20, 2024

[Dukungan Transport Layer Security \(TLS\)](#)

Amazon WorkMail menghentikan dukungan untuk Transport Layer Security (TLS) 1.0 dan 1.1. Jika Anda menggunakan TLS 1.0 atau 1.1, Anda harus memutakhirkan versi TLS ke 1.2.

November 2, 2023

[Pengguna jarak jauh](#)

Pengguna jarak jauh adalah WorkMail pengguna Amazon yang dihosting di luar WorkMail organisasi Amazon atau dihosting di domain email yang berbeda. Untuk informasi selengkapnya, lihat [Pengguna](#) di Panduan WorkMail Administrator Amazon.

18 September 2023

[Akses terprogram ke kotak surat](#)

Amazon WorkMail sekarang menawarkan Peran Peniruan untuk memberikan akses terprogram ke kotak pesan. Untuk selengkapnya, lihat [Akses terprogram ke kotak pesan](#) di Panduan WorkMail Administrator Amazon.

4 Oktober 2022

[Konfigurasi Penyedia Ketersediaan Kustom di Amazon WorkMail](#)

Amazon WorkMail mendukung penggunaan Custom Availability Providers (CAP). Untuk informasi selengkapnya, lihat [Mengonfigurasi Penyedia Ketersediaan Khusus](#) di Panduan WorkMail Administrator Amazon.

30 Juni 2022

[Perubahan konsol untuk membuat organisasi](#)

Pengalaman WorkMail konsol Amazon untuk membuat organisasi diperbarui. Untuk informasi selengkapnya, lihat [Membuat organisasi](#) di Panduan WorkMail Administrator Amazon.

23 Oktober 2020

[Mengekspor konten kotak surat](#)

Gunakan tindakan `StartMailboxExport Job` API untuk mengekspor konten WorkMail kotak pesan Amazon ke bucket Amazon Simple Storage Service (Amazon S3). Untuk selengkapnya, lihat [Mengekspor konten kotak pesan](#) di Panduan WorkMail Administrator Amazon.

22 September 2020

[Kebijakan penyimpanan kotak pesan](#)

Tetapkan kebijakan penyimpanan kotak pesan untuk WorkMail organisasi Amazon Anda yang secara otomatis menghapus pesan email setelah jangka waktu yang Anda pilih. Untuk selengkapnya, lihat [Menyetel kebijakan penyimpanan kotak pesan](#) di Panduan WorkMail Administrator Amazon.

28 Mei 2020

[Tindakan Jalankan Lambda sinkron dan asinkron](#)

Pilih konfigurasi sinkron atau asinkron untuk tindakan Jalankan Lambda dalam aturan alur email Amazon. WorkMail Untuk informasi selengkapnya, lihat [Mengonfigurasi AWS Lambda Amazon WorkMail](#) di Panduan WorkMail Administrator Amazon.

11 Mei 2020

[Bekerja dengan aturan kontrol akses](#)

Aturan kontrol akses memungkinkan WorkMail administrator Amazon mengontrol cara mengakses kotak pesan organisasi mereka. Untuk informasi selengkapnya, lihat [Bekerja dengan aturan kontrol akses](#) di Panduan WorkMail Administrator Amazon.

12 Februari 2020

[Menandai organisasi](#)

Tandai WorkMail organisasi Amazon untuk membedakan antara organisasi di AWS Manajemen Penagihan dan Biaya konsol, atau untuk mengontrol akses ke sumber daya organisasi. Untuk informasi selengkapnya, lihat [Menandai organisasi](#) di Panduan WorkMail Administrator Amazon.

23 Januari 2020

Menegakkan kebijakan DMARC tentang incoming email	Untuk informasi selengkapnya, lihat Menegakkan kebijakan DMARC tentang email masuk di Panduan Administrator Amazon WorkMail	17 Oktober 2019
Mengambil konten pesan dengan Lambda	Gunakan Amazon WorkMail Message Flow API AWS Lambda untuk mengambil konten pesan. Untuk informasi selengkapnya, lihat Mengambil konten pesan dengan Lambda di Panduan Administrator WorkMail Amazon .	12 September 2019
Mencatat peristiwa WorkMail email Amazon	Aktifkan pencatatan peristiwa email di WorkMail konsol Amazon untuk melacak pesan email untuk organisasi Anda. Untuk informasi selengkapnya, lihat Melacak pesan di Panduan WorkMail Administrator Amazon .	13 Mei 2019
Rute 53 penyisipan catatan DNS	Saat menyiapkan domain yang dikelola di zona host publik Route 53, Amazon WorkMail secara otomatis menyisipkan catatan DNS untuk Anda. Untuk informasi selengkapnya, lihat Menambahkan domain di Panduan WorkMail Administrator Amazon .	13 Februari 2019

Mengonfigurasi Lambda untuk tindakan aturan email masuk	Amazon WorkMail mendukung konfigurasi fungsi Lambda untuk digunakan dengan aturan alur email masuk. Untuk informasi selengkapnya, lihat Mengelola alur email di Panduan WorkMail Administrator Amazon.	24 Januari 2019
Mengkonfigurasi Lambda untuk Amazon WorkMail	Amazon WorkMail mendukung konfigurasi fungsi Lambda untuk digunakan dengan aturan alur email keluar. Untuk informasi selengkapnya, lihat Mengonfigurasi Lambda untuk WorkMail Amazon di Panduan Administrator WorkMail Amazon.	19 November 2018
Perutean SMTP	Amazon WorkMail mendukung konfigurasi gateway SMTP untuk digunakan dengan aturan alur email keluar. Untuk informasi selengkapnya, lihat Mengonfigurasi gateway SMTP di Panduan Administrator Amazon. WorkMail	1 November 2018
Alat debugging untuk domain khusus	Amazon WorkMail telah menambahkan alat debugging untuk domain khusus. Untuk informasi selengkapnya, lihat Menambahkan domain di Panduan WorkMail Administrator Amazon.	15 Oktober 2018

Support untuk Outlook 2019	Amazon WorkMail mendukung Outlook 2019 untuk Windows dan macOS. Untuk informasi selengkapnya, lihat Persyaratan WorkMail sistem Amazon di Panduan WorkMail Administrator Amazon.	1 Oktober 2018
Berbagai pembaruan	Berbagai pembaruan untuk tata letak topik dan organisasi.	12 Juli 2018
Izin kotak surat	Anda dapat menggunakan izin kotak pesan di Amazon WorkMail untuk memberi pengguna atau grup hak untuk bekerja di kotak pesan pengguna lain. Untuk selengkapnya, lihat Bekerja dengan izin kotak pesan di Panduan WorkMail Administrator Amazon.	9 April 2018
Support untuk AWS CloudTrail	Amazon WorkMail terintegrasi dengan AWS CloudTrail. Untuk informasi selengkapnya, lihat Mencatat panggilan Amazon WorkMail API dengan AWS CloudTrail di Panduan WorkMail Administrator Amazon.	12 Desember 2017

Support untuk alur email	Anda dapat mengatur aturan alur email untuk menangani email masuk berdasarkan alamat email atau domain pengirim. Untuk informasi selengkapnya, lihat Mengelola alur email di Panduan WorkMail Administrator Amazon.	5 Juli 2017
Pembaruan untuk Pengaturan Cepat	Pengaturan Cepat sekarang membuat WorkMail direktori Amazon untuk Anda. Untuk informasi selengkapnya, lihat Mengatur Amazon WorkMail dengan Pengaturan Cepat di Panduan WorkMail Administrator Amazon.	10 Mei 2017
Support untuk klien email yang lebih luas	Anda sekarang dapat menggunakan Amazon WorkMail dengan Microsoft Outlook 2016 untuk klien email Mac dan IMAP. Untuk informasi selengkapnya, lihat Persyaratan sistem untuk Amazon WorkMail di Panduan WorkMail Administrator Amazon.	9 Januari 2017

Support untuk SMTP journaling	Anda dapat mengatur penjurnalan untuk merekam komunikasi email. Untuk informasi selengkapnya, lihat Menggunakan penjurnalan email dengan Amazon WorkMail di Panduan WorkMail Administrator Amazon.	25 Nopember 2016
Support untuk pengalihan email ke alamat email eksternal	Anda dapat mengatur aturan pengalihan email dengan memperbarui kebijakan identitas Amazon SES untuk domain Anda. Untuk informasi selengkapnya, lihat Mengedit kebijakan identitas domain di Panduan WorkMail Administrator Amazon.	26 Oktober 2016
Support untuk interoperabilitas	Anda dapat mengaktifkan interoperabilitas antara Amazon dan WorkMail Microsoft Exchange. Untuk informasi selengkapnya, lihat Interoperabilitas antara Amazon dan WorkMail Microsoft Exchange di Panduan WorkMail Administrator Amazon.	25 Oktober 2016
Ketersediaan umum	Rilis ketersediaan umum Amazon WorkMail.	4 Januari 2016

Support untuk memesan sumber daya	Support untuk menyimpan sumber daya, seperti ruang pertemuan dan peralatan. Untuk informasi selengkapnya, lihat Bekerja dengan sumber daya di Panduan WorkMail Administrator Amazon.	19 Oktober 2015
Support untuk alat migrasi email	Support untuk alat migrasi email. Untuk informasi selengkapnya, lihat Migrasi ke Amazon WorkMail di Panduan WorkMail Administrator Amazon.	16 Agustus 2015
Pratinjau rilis Amazon WorkMail	Rilis pratinjau Amazon WorkMail.	28 Januari 2015