aws

Panduan Administrasi

Browser WorkSpaces Aman Amazon

Browser WorkSpaces Aman Amazon: Panduan Administrasi

Table of Contents

Apa itu Amazon WorkSpaces Secure Browser? 1
Riwayat rilis 1
Ketentuan untuk mengetahui 2
Layanan terkait 4
Arsitektur 4
Akses 5
Menyiapkan 6
Mendaftar dan membuat pengguna 6
Mendaftar untuk Akun AWS 6
Buat pengguna dengan akses administratif 7
Memberikan akses terprogram 8
Jaringan 10
Pengaturan VPC 11
Koneksi pengguna 25
Memulai 28
Pembuatan portal web 28
Pengaturan jaringan 29
Pengaturan portal 29
Pengaturan pengguna 32
Konfigurasi penyedia identitas 33
Luncurkan 44
Pengujian portal web 45
Distribusi portal web 45
Mengelola portal web Anda 47
Melihat detail portal web 48
Mengedit portal web 48
Menghapus portal web 48
Mengelola kuota layanan 49
Meminta peningkatan kuota layanan 50
Meminta peningkatan portal 50
Meminta peningkatan sesi bersamaan maksimum 51
Batasi contoh 52
Kuota layanan lainnya 52
Mengautentikasi ulang token IDP SAMP 53

Menyiapkan pencatatan aktivitas pengguna 54
Menyiapkan Session Logger 55
Menyiapkan pencatatan Akses Pengguna 58
Mengelola kebijakan browser 58
Tutorial: Mengatur kebijakan browser khusus 59
Mengedit kebijakan browser dasar 65
Mengkonfigurasi Editor Metode Input 67
Mengkonfigurasi lokalisasi dalam sesi 69
Kode bahasa yang didukung 69
Pengaturan browser pengguna 71
Mengelola kontrol akses IP 72
Membuat grup kontrol akses IP 73
Mengaitkan pengaturan akses IP 74
Mengedit grup kontrol akses IP 75
Menghapus grup kontrol akses IP 75
Mengelola ekstensi masuk tunggal 76
Mengidentifikasi domain untuk ekstensi masuk tunggal 77
Menambahkan ekstensi masuk tunggal ke portal web baru 77
Menambahkan ekstensi masuk tunggal ke portal web yang ada 78
Mengedit atau menghapus ekstensi masuk tunggal 78
Pemfilteran konten web 78
Membatasi penelusuran ke spesifik URLs 79
Memblokir spesifik URLs 80
Kategori pemblokiran 80
Contoh dari URLs 83
Mentransfer kebijakan Chrome 83
Deep link 84
Menyiapkan tautan dalam 84
Menggunakan pemfilteran URL untuk deep link 85
Dasbor manajemen sesi 85
Akses dasbor 85
Filter dasbor 86
Mengakhiri sesi 86
Riwayat sesi 86
Melindungi data bergerak 87
Pengaturan perlindungan data 88

Redaksi data sebaris 88
Konfigurasi redaksi default 90
Redaksi sebaris dasar 91
Redaksi inline kustom 93
Buat pengaturan perlindungan data 94
Mengaitkan pengaturan perlindungan data 95
Edit pengaturan perlindungan data 96
Hapus pengaturan perlindungan data 96
Penyesuaian branding 97
Mengkonfigurasi kustomisasi branding untuk portal Anda 98
Pedoman kustomisasi 101
Pengalihan otentikasi web 114
WebAuthn Aktifkan pengalihan di pengaturan portal 115
Konfigurasikan kebijakan browser lokal 115
WebAuthn penggunaan pengalihan 116
WebAuthn pemecahan masalah pengalihan 116
Kontrol bilah alat 117
Domain kustom 118
Mengkonfigurasi domain khusus untuk portal Anda 119
Pemecahan masalah domain khusus 130
Keamanan 132
Perlindungan data 133
Enkripsi data 134
Privasi lalu lintas antar jaringan 143
Pencatatan akses pengguna 144
Identity and Access Management 144
Audiens 144
Mengautentikasi dengan identitas 145
Mengelola akses menggunakan kebijakan 146
Bagaimana Amazon WorkSpaces Secure Browser bekerja dengan IAM 148
Contoh kebijakan berbasis identitas 154
AWS kebijakan terkelola 157
Pemecahan masalah 167
Menggunakan Peran Terkait Layanan 169
Respons insiden 173
Validasi kepatuhan 173

Ketahanan 174
Keamanan infrastruktur 174
Konfigurasi dan analisis kerentanan 175
Antarmuka VPC titik akhir ()AWS PrivateLink 175
Pertimbangan untuk Amazon WorkSpaces Secure Browser 176
Membuat titik akhir VPC antarmuka untuk Amazon Secure Browser WorkSpaces 176
Membuat kebijakan endpoint untuk titik akhir VPC antarmuka Anda 177
Pemecahan masalah 177
Praktik terbaik keamanan 178
Pemantauan 180
Pemantauan CloudWatch dengan 181
CloudTrail log 184
Informasi di CloudTrail 185
Entri berkas log 186
Pencatatan aktivitas pengguna 187
Acara sesi di Session Logger 188
Peristiwa sesi dalam pencatatan Akses Pengguna 195
Panduan pengguna 197
Kompatibilitas browser dan perangkat 197
Akses portal web 198
Panduan sesi 198
Memulai sesi 198
Menggunakan toolbar 199
Menggunakan browser 202
Mengakhiri sesi 202
Memecahkan masalah pengguna 203
Ekstensi masuk tunggal 204
Kompatibilitas ekstensi masuk tunggal 205
Memasang ekstensi masuk tunggal 205
Memecahkan masalah ekstensi masuk tunggal 206
Riwayat dokumen 207
..... ccxii

Apa itu Amazon WorkSpaces Secure Browser?

> **Note**
>
> Amazon WorkSpaces Secure Browser sebelumnya dikenal sebagai Amazon WorkSpaces Web.

Amazon WorkSpaces Secure Browser adalah layanan browser yang dikelola sepenuhnya, cloud-native, dan dihosting yang digunakan untuk mengakses situs web pribadi dan aplikasi web (software-as-a-serviceSaaS) dengan aman, berinteraksi dengan sumber daya online, dan menjelajahi internet dari wadah sekali pakai. WorkSpaces Secure Browser bekerja dengan browser web pengguna yang ada, tanpa membebani TI dengan mengelola peralatan, infrastruktur, perangkat lunak klien khusus, atau koneksi jaringan pribadi virtual (VPN). Konten web dialirkan ke browser web pengguna, sedangkan browser dan konten web yang sebenarnya diisolasi. AWS Dengan menggunakan teknologi dasar yang sama yang mendukung layanan AWS End User Computing seperti Amazon WorkSpaces dan Amazon WorkSpaces Applications, WorkSpaces Secure Browser dapat lebih hemat biaya daripada desktop virtual tradisional, dan mengurangi kompleksitas dibandingkan dengan menyediakan perangkat lunak manajemen milik perusahaan. WorkSpaces Browser Aman mengurangi risiko eksfiltrasi data dengan streaming konten web. Tidak ada HTML, model objek dokumen (DOM), atau data perusahaan sensitif yang ditransmisikan ke mesin lokal. Dengan mengisolasi perangkat, jaringan perusahaan, dan internet dari satu sama lain, permukaan serangan browser hampir dihilangkan.

Anda dapat menerapkan kebijakan browser perusahaan (termasuk pengizinan/pemblokiran URL) pada semua sesi, dan menyertakan kontrol tingkat sesi untuk clipboard, transfer file, dan printer. Anda juga dapat membatasi akses ke jaringan atau perangkat tepercaya dengan menggunakan Kontrol Akses IP. WorkSpaces Browser Aman mudah diatur dan dioperasikan. Setiap sesi diluncurkan dengan versi Browser Chrome yang baru dan sepenuhnya ditambal, dengan kebijakan dan pengaturan perusahaan diterapkan.

Riwayat rilis untuk Amazon WorkSpaces Secure Browser

Pada 20 Mei 2024, Amazon WorkSpaces Web diubah namanya menjadi Amazon WorkSpaces Secure Browser. Untuk pelanggan yang sudah ada, tidak ada perubahan pada cara mereka mengelola pengguna atau sumber daya dengan layanan. Daftar berikut menjelaskan pembaruan yang berlaku yang juga terjadi sebagai akibat dari penggantian nama ini.

Namespace API web ruang kerja tetap tidak berubah untuk kompatibilitas mundur. Akibatnya, sumber daya berikut masih sama:

- Perintah CLI.
- CloudWatch Metrik Amazon. Untuk informasi selengkapnya, lihat the section called “Pemantauan CloudWatch dengan”.
- Titik akhir layanan. Untuk informasi selengkapnya, lihat titik akhir dan kuota Amazon WorkSpaces Secure Browser.
- AWS CloudFormation sumber daya. Untuk informasi selengkapnya, lihat referensi jenis sumber daya Amazon WorkSpaces Secure Browser.
- Peran terkait layanan yang berisi ruang kerja-web. Untuk informasi selengkapnya, lihat the section called “Menggunakan Peran Terkait Layanan”.
- Konsol URLs yang berisi ruang kerja-web.
- Dokumentasi URLs yang berisi ruang kerja-web. Untuk informasi selengkapnya, lihat Dokumentasi Browser WorkSpaces Aman Amazon.
- Peran ReadOnly terkelola yang ada. Untuk informasi selengkapnya, lihat the section called “AWS kebijakan terkelola”.
- Nama hibah KMS.
- UAL (Pencatatan Aktivitas Pengguna) Awalan aliran Kinesis.

Selain itu, portal yang ada URLs tetap sama. URLs <UUID>untuk portal yang dibuat sebelum 20 Mei 2024 menggunakan format .workspaces-web.com. WorkSpaces Portal Browser Aman terus menggunakan format ini dan domain workspaces-web.com.

Ketentuan yang perlu diketahui saat menggunakan Amazon WorkSpaces Secure Browser

Untuk membantu Anda memulai dengan Browser WorkSpaces Aman, Anda harus terbiasa dengan konsep-konsep berikut.

Penyedia identitas (iDP)

> Penyedia identitas memverifikasi kredensi pengguna Anda. Kemudian mengeluarkan pernyataan otentikasi untuk menyediakan akses ke penyedia layanan. Anda dapat mengonfigurasi IDP yang ada untuk bekerja dengan Browser WorkSpaces Aman.

Proses untuk mengonfigurasi penyedia identitas Anda (iDP) bervariasi, tergantung pada IDP Anda.

Anda harus mengunggah file metadata penyedia layanan ke IDP Anda. Jika tidak, pengguna Anda tidak akan dapat masuk. Anda juga harus memberikan akses bagi pengguna Anda untuk menggunakan Browser WorkSpaces Aman di IDP Anda.

Dokumen metadata penyedia identitas (iDP)

WorkSpaces Browser Aman memerlukan metadata khusus dari penyedia identitas Anda (IDP) untuk membangun kepercayaan. Anda dapat menambahkan metadata ini ke Browser WorkSpaces Aman dengan mengunggah file pertukaran metadata yang diunduh dari IDP Anda.

Penyedia layanan (SP)

Penyedia layanan menerima pernyataan otentikasi dan menyediakan layanan kepada pengguna. WorkSpaces Secure Browser bertindak sebagai penyedia layanan untuk pengguna yang telah diautentikasi oleh IDP mereka.

Dokumen metadata penyedia layanan (SP)

Anda perlu menambahkan detail metadata penyedia layanan ke antarmuka konfigurasi penyedia identitas (IDP) Anda. Rincian proses konfigurasi ini bervariasi antar penyedia.

SAML 2.0

Standar untuk bertukar data otentikasi dan otorisasi antara IDP dan penyedia layanan.

Cloud Privat Virtual (VPC)

Anda dapat menggunakan VPC yang sudah ada atau baru, subnet yang sesuai, dan grup keamanan untuk menautkan konten Anda dengan WorkSpaces Browser Aman.

Subnet harus dengan koneksi yang stabil ke internet, dan VPC dan subnet juga harus memiliki koneksi yang stabil ke situs web internal dan Perangkat Lunak sebagai Layanan (SaaS) bagi pengguna untuk mengakses sumber daya ini.

Grup VPCs, subnet, dan keamanan yang terdaftar diambil dari wilayah yang sama dengan konsol Browser WorkSpaces Aman Anda.

Toko kepercayaan

Jika pengguna yang mengakses situs web melalui Browser WorkSpaces Aman menerima kesalahan privasi, seperti NET: :ERR_CERT_INVALID, situs tersebut mungkin menggunakan sertifikat yang ditandatangani oleh otoritas sertifikat pribadi (PCA). Anda mungkin perlu

menambahkan atau mengubah PCAs di toko kepercayaan Anda. Selain itu, jika perangkat pengguna mengharuskan Anda untuk menginstal sertifikat tertentu untuk memuat situs web, Anda perlu menambahkan sertifikat itu ke toko kepercayaan Anda untuk memungkinkan pengguna mengakses situs tersebut di Browser WorkSpaces Aman.

Situs web yang dapat diakses publik biasanya tidak memerlukan perubahan apa pun ke toko kepercayaan.

Portal web

Portal web memberi pengguna Anda akses ke situs web internal dan SaaS dari browser mereka. Anda dapat membuat satu portal web di setiap wilayah yang didukung per akun. Untuk meminta peningkatan batas untuk lebih dari satu portal, hubungi dukungan.

Titik akhir portal web

Titik akhir portal web adalah titik akses pengguna Anda akan meluncurkan portal web Anda setelah masuk dengan penyedia identitas yang dikonfigurasi untuk portal.

Titik akhir tersedia untuk umum di internet dan dapat disematkan ke jaringan Anda.

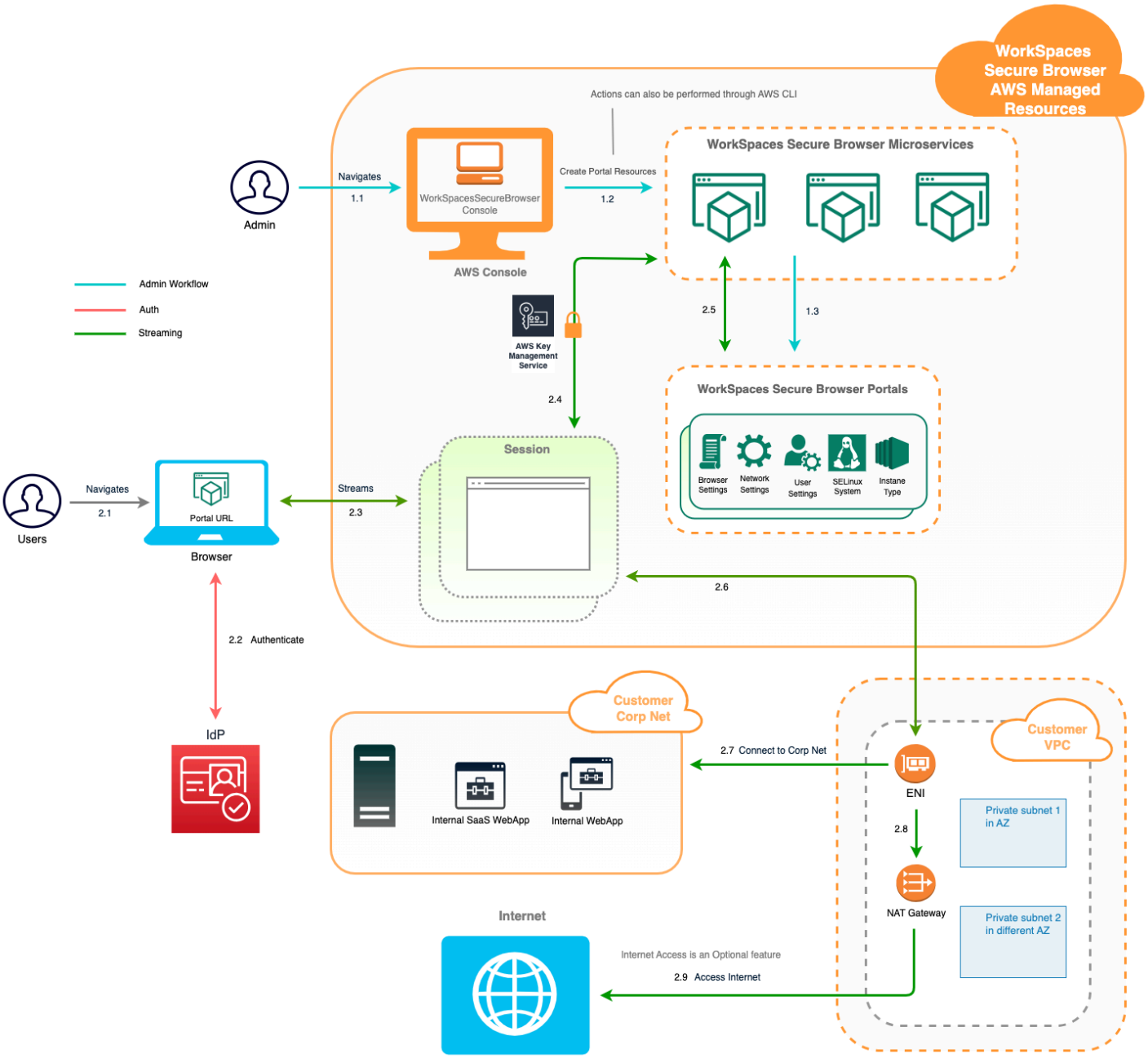
AWS layanan yang terkait dengan Amazon WorkSpaces Secure Browser

Ada beberapa AWS layanan yang terkait dengan Browser WorkSpaces Aman.

WorkSpaces Secure Browser adalah kemampuan dari Amazon WorkSpaces dalam portofolio AWS End User Computing. Dibandingkan dengan WorkSpaces dan AppStream 2.0, WorkSpaces Secure Browser dibangun khusus untuk memfasilitasi beban kerja berbasis web yang aman. WorkSpaces Browser Aman dikelola secara otomatis, dengan kapasitas, penskalaan, dan gambar disediakan dan diperbarui sesuai permintaan oleh AWS. Misalnya, Anda dapat memilih untuk menawarkan Desktop Ruang Kerja persisten kepada pengembang perangkat lunak Anda yang memerlukan akses ke sumber daya desktop, dan Browser WorkSpaces Aman ke pengguna pusat kontak yang hanya memerlukan akses ke beberapa situs web internal dan SaaS (termasuk yang dihosting di luar jaringan Anda) di komputer desktop.

Arsitektur Amazon WorkSpaces Secure Browser

Diagram berikut menunjukkan arsitektur WorkSpaces Secure Browser.



Mengakses Browser WorkSpaces Aman Amazon

Anda dapat mengakses Browser WorkSpaces Aman dengan beberapa cara.

Administrator mengakses Browser WorkSpaces Aman melalui WorkSpaces Secure Browser Console, SDK, CLI, atau API. Pengguna Anda mengaksesnya melalui titik akhir Browser WorkSpaces Aman.

Menyiapkan Browser WorkSpaces Aman Amazon

Sebelum Anda dapat mengonfigurasi Browser WorkSpaces Aman untuk menjangkau situs web internal dan aplikasi SaaS Anda, Anda harus menyelesaikan prasyarat berikut.

Topik

- Mendaftar dan membuat pengguna
- Memberikan akses terprogram
- Jaringan untuk Amazon WorkSpaces Secure Browser

Mendaftar dan membuat pengguna

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke Konsol Manajemen AWSsebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Memberikan akses terprogram

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. Konsol Manajemen AWS Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Disarankan) Gunakan kredenal konsol sebagai kredensional sementara untuk menandatangani permintaan terprogram ke,, atau. AWS CLI AWS SDKs AWS APIs	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk itu AWS CLI, lihat Login untuk pengembangan AWS lokal di Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDKs, lihat Login untuk pengembangan AWS lokal di Panduan Referensi Alat AWS SDKs dan Alat.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredensyal sementara untuk menandatangani permintaan terprogram ke AWS CLI,, AWS SDKs atau. AWS APIs	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDKs, alat, dan AWS APIs, lihat Autentikasi Pusat Identitas IAM di Panduan Referensi Alat AWS SDKs dan Alat.
IAM	Gunakan kredensyal sementara untuk menandatangani permintaan terprogram ke AWS CLI,, AWS SDKs atau. AWS APIs	Mengikuti petunjuk dalam Menggunakan kredensi sementara dengan AWS sumber daya di Panduan Pengguna IAM.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Tidak direkomendasikan) Gunakan kredensyal jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI,, AWS SDKs atau. AWS APIs	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensyal pengguna IAM di Panduan Pengguna.AWS Command Line Interface • Untuk AWS SDKs dan alat, lihat Mengautentikasi menggunakan kredensi jangka panjang di Panduan Referensi Alat AWS SDKs dan Alat. • Untuk AWS APIs, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Jaringan untuk Amazon WorkSpaces Secure Browser

Topik berikut menjelaskan cara mengatur instance streaming Browser WorkSpaces Aman sehingga pengguna dapat terhubung dengannya. Ini juga menjelaskan cara mengaktifkan instance streaming Browser WorkSpaces Aman Anda untuk mengakses sumber daya VPC, serta internet.

Topik

- Menyiapkan VPC untuk Amazon WorkSpaces Secure Browser
- Mengaktifkan koneksi pengguna untuk Amazon WorkSpaces Secure Browser

Menyiapkan VPC untuk Amazon WorkSpaces Secure Browser

Untuk mengatur dan mengkonfigurasi VPC untuk Browser WorkSpaces Aman, selesaikan langkah-langkah berikut.

Topik

- Persyaratan VPC untuk Amazon Secure Browser WorkSpaces
- Membuat VPC baru untuk Amazon WorkSpaces Secure Browser
- Mengaktifkan penjelajahan internet untuk Amazon WorkSpaces Secure Browser
- Praktik terbaik VPC untuk WorkSpaces Browser Aman
- Zona Ketersediaan yang Didukung untuk Amazon WorkSpaces Secure Browser

Persyaratan VPC untuk Amazon Secure Browser WorkSpaces

Selama pembuatan portal Browser WorkSpaces Aman, Anda akan memilih VPC di akun Anda. Anda juga akan memilih setidaknya dua subnet di dua Availability Zone yang berbeda. Ini VPCs dan subnet harus memenuhi persyaratan berikut:

- VPC harus memiliki tenancy default. VPCs dengan penyewaan khusus tidak didukung.
- Untuk pertimbangan ketersediaan, kami memerlukan setidaknya dua subnet yang dibuat di dua Availability Zone yang berbeda. Subnet Anda harus memiliki alamat IP yang cukup untuk mendukung lalu lintas Browser WorkSpaces Aman yang diharapkan. Konfigurasikan setiap subnet Anda dengan subnet mask yang memungkinkan alamat IP klien yang cukup untuk memperhitungkan jumlah maksimum sesi bersamaan. Untuk informasi selengkapnya, lihat Membuat VPC baru untuk Amazon WorkSpaces Secure Browser.
- Semua subnet harus memiliki koneksi yang stabil ke konten internal apa pun, baik yang terletak di AWS Cloud atau di tempat, yang akan diakses pengguna dengan Browser WorkSpaces Aman.

Kami menyarankan Anda memilih tiga subnet di Availability Zone yang berbeda untuk pertimbangan ketersediaan dan penskalaan. Untuk informasi selengkapnya, lihat Membuat VPC baru untuk Amazon WorkSpaces Secure Browser.

WorkSpaces Browser Aman tidak menetapkan alamat IP publik apa pun ke instans streaming untuk mengaktifkan akses internet. Ini akan membuat instance streaming Anda dapat diakses dari internet. Oleh karena itu, instans streaming apa pun yang terhubung ke subnet publik Anda tidak

akan memiliki akses internet. Jika Anda ingin portal Browser WorkSpaces Aman Anda memiliki akses ke konten internet publik dan konten VPC pribadi, selesaikan langkah-langkahnya. Mengaktifkan penjelajahan internet tanpa batas untuk Amazon WorkSpaces Secure Browser (disarankan)

Membuat VPC baru untuk Amazon WorkSpaces Secure Browser

Bagian ini menjelaskan cara menggunakan wizard VPC untuk membuat VPC dengan cepat dengan subnet publik dan pribadi. Wizard secara otomatis membuat gateway internet, gateway NAT, dan mengonfigurasi tabel rute untuk subnet Anda.

Untuk informasi selengkapnya tentang konfigurasi ini, lihat VPC dengan subnet publik dan pribadi (NAT).

Topik

- Pengaturan VPC Cepat (1 menit)
- Memverifikasi tabel rute subnet Anda (opsional)

Pengaturan VPC Cepat (1 menit)

Selesaikan langkah-langkah berikut untuk membuat VPC khusus untuk Browser WorkSpaces Aman dengan cepat dengan subnet publik dan pribadi untuk akses internet. Jika Anda ingin menggunakan VPC yang ada, lihat Persyaratan VPC untuk Amazon Secure Browser WorkSpaces untuk memverifikasi bahwa VPC memenuhi persyaratan.

> **Note**
>
> Pastikan Anda berada dalam keinginan Anda Wilayah AWS. Anda dapat mengubah wilayah di konsol jika diperlukan.

Untuk mengatur VPC dengan cepat

1. Buka wizard pembuatan VPC: Buat VPC dengan sumber daya. Simpan semua pengaturan sebagai default kecuali ditentukan di bawah ini:
   - Agar Sumber Daya dapat dibuat, pilih VPC dan lainnya.
   - Untuk tag Nama, pilih auto-generate dan masukkan nama deskriptif untuk VPC Anda (mis.,). **WSB-VPC**

- Untuk blok IPv4 CIDR, secara default, **`10.0.0.0/16`** VPC menggunakan. Anda dapat menentukan blok IPv4 CIDR yang berbeda jika diperlukan.
- Untuk Penyewaan, pilih Default (VPCs dengan penyewaan khusus tidak didukung).
- Untuk Jumlah Availability Zones (AZs), pilih 2.
  - Perluas Kustomisasi AZs dan pilih 2 Availability Zone berbeda yang didukung oleh WorkSpaces Secure Browser. Untuk daftar yang didukung AZs, lihatZona Ketersediaan yang Didukung untuk Amazon WorkSpaces Secure Browser.
- Untuk Jumlah subnet publik, pilih 2.
- Untuk Jumlah subnet pribadi, pilih 2.
- Untuk blok CIDR Subnet, jika Anda perlu menyesuaikan blok CIDR di subnet Anda, perluas Sesuaikan subnet blok CIDR. Pastikan setiap subnet memiliki alamat IP yang cukup untuk lalu lintas yang Anda harapkan.
- Untuk gateway NAT, pilih Regional untuk mengaktifkan akses internet untuk subnet pribadi di semua Availability Zone.
- Untuk titik akhir VPC, pilih Tidak Ada. Jika Anda memerlukan akses S3 langsung tanpa melalui gateway NAT, pilih S3 Gateway.
- Untuk opsi DNS, biarkan opsi DNS diaktifkan (default) untuk memastikan resolusi nama yang tepat dalam VPC Anda.

2. Tinjau panel Pratinjau, lalu pilih Buat VPC.

> **Note**
>
> Biaya tambahan berlaku untuk gateway NAT dan titik akhir VPC. Untuk informasi selengkapnya, lihat halaman harga VPC.

Memverifikasi tabel rute subnet Anda (opsional)

Wizard VPC secara otomatis mengonfigurasi tabel rute untuk Anda. Jika Anda membuat VPC secara manual atau ingin mengonfirmasi konfigurasi, Anda dapat memverifikasi bahwa detail berikut ini benar untuk tabel rute Anda:

- Tabel rute yang terkait dengan subnet tempat gateway NAT Anda berada harus menyertakan rute yang mengarahkan lalu lintas internet ke gateway internet. Ini memastikan bahwa gateway NAT Anda dapat mengakses internet.

- Tabel rute yang terkait dengan subnet pribadi Anda harus dikonfigurasi untuk mengarahkan lalu lintas internet ke gateway NAT. Ini memungkinkan contoh streaming di subnet pribadi Anda untuk berkomunikasi dengan internet.

Untuk memverifikasi dan memberi nama tabel rute subnet Anda

1. Di panel navigasi, pilih Subnet, lalu pilih subnet publik. Misalnya, WSB-VPC-Subnet-Public1-US-East-1a.
2. Pada tab Tabel rute, pilih ID tabel rute. Misalnya, rtb-12345678.
3. Pilih tabel rute. Di bawah Nama, pilih ikon edit (pensil), dan masukkan nama untuk tabel. Misalnya, masukkan nama**`workspacesweb-public-routetable`**. Kemudian pilih tanda centang untuk menyimpan nama.
4. Dengan tabel rute publik masih dipilih, pada tab Rute, verifikasi bahwa ada dua rute: satu untuk lalu lintas lokal, dan satu yang mengirim semua lalu lintas lainnya melalui gateway internet VPC. Tabel berikut menjelaskan dua rute ini:

Destinasi	Target	Deskripsi
Blok IPv4 CIDR subnet publik (misalnya, 10.0.0/20)	Lokal:	Semua lalu lintas dari sumber daya yang ditujukan untuk IPv4 alamat dalam blok IPv4 CIDR subnet publik. Lalu lintas ini diarahkan secara lokal di dalam VPC.
Lalu lintas ditujukan ke semua IPv4 alamat lain (misalnya, 0.0.0.0/0)	Keluar (IGW-ID)	Lalu lintas yang ditujukan untuk semua IPv4 alamat lain diarahkan ke gateway internet (diidentifikasi oleh IGW-ID) yang dibuat oleh wizard VPC.

5. Di panel navigasi, pilih Pengguna. Kemudian, pilih subnet pribadi (misalnya,**`WSB-VPC-subnet-private1-us-east-1a`**).
6. Pada tab Route Table, pilih ID tabel rute.

7. Pilih tabel rute. Di bawah Nama, pilih ikon edit (pensil), dan masukkan nama untuk tabel. Misalnya, masukkan nama**`WSB-VPC-private-routetable`**. Kemudian pilih tanda centang untuk menyimpan nama.
8. Pada tab Rute, verifikasi bahwa tabel rute menyertakan rute berikut:

Destinasi	Target	Deskripsi
Blok IPv4 CIDR subnet publik (misalnya, 10.0.0/20)	Lokal:	Semua lalu lintas dari sumber daya yang ditujukan untuk IPv4 alamat dalam blok IPv4 CIDR subnet publik dirutekan secara lokal di dalam VPC.
Lalu lintas ditujukan ke semua IPv4 alamat lain (misalnya, 0.0.0.0/0)	Keluar (Nat-ID)	Lalu lintas yang ditujukan untuk semua IPv4 alamat lain diarahkan ke gateway NAT (diidentifikasi oleh NAT-ID).
Lalu lintas yang ditujukan untuk bucket S3 (berlaku jika Anda menentukan titik akhir S3) [PL-ID (com.amazonaws.region.s3)]	Penyimpanan (VPCE-ID)	Lalu lintas yang ditujukan untuk bucket S3 dialihkan ke titik akhir S3 (diidentifikasi oleh VPCE-ID).

9. Di panel navigasi, pilih Pengguna. Kemudian pilih subnet pribadi kedua yang Anda buat (misalnya,**`WorkSpaces Secure Browser Private Subnet2`**).
10. Pada tab Route Table, verifikasi bahwa tabel rute yang dipilih adalah tabel rute pribadi (misalnya,**`workspacesweb-private-routetable`**). Jika tabel rute berbeda, pilih Edit dan pilih tabel rute pribadi Anda.

Mengaktifkan penjelajahan internet untuk Amazon WorkSpaces Secure Browser

Anda dapat memilih untuk mengaktifkan penjelajahan internet tanpa batas (opsi yang disarankan) atau penjelajahan internet terbatas.

Topik

- Mengaktifkan penjelajahan internet tanpa batas untuk Amazon WorkSpaces Secure Browser (disarankan)
- Mengaktifkan penjelajahan internet terbatas untuk Amazon WorkSpaces Secure Browser
- Port konektivitas internet untuk Amazon WorkSpaces Secure Browser

Mengaktifkan penjelajahan internet tanpa batas untuk Amazon WorkSpaces Secure Browser (disarankan)

Ikuti langkah-langkah ini untuk mengonfigurasi VPC dengan gateway NAT untuk penjelajahan internet tanpa batas. Ini memberikan akses Browser WorkSpaces Aman ke situs di internet publik, dan situs pribadi yang dihosting di atau dengan koneksi ke VPC Anda.

Untuk mengonfigurasi VPC dengan gateway NAT untuk penjelajahan internet tanpa batas

Jika Anda ingin portal Browser WorkSpaces Aman Anda memiliki akses ke konten internet publik dan konten VPC pribadi, ikuti langkah-langkah berikut:

> **Note**
>
> Jika Anda sudah mengonfigurasi VPC, selesaikan langkah-langkah berikut untuk menambahkan gateway NAT ke VPC Anda. Jika Anda perlu membuat VPC baru, lihat. Membuat VPC baru untuk Amazon WorkSpaces Secure Browser

1. Untuk membuat gateway NAT Anda, selesaikan langkah-langkah di Buat gateway NAT. Pastikan gateway NAT ini memiliki konektivitas publik, dan berada di subnet publik di VPC Anda.
2. Anda harus menentukan setidaknya dua subnet pribadi dari Availability Zone yang berbeda. Menetapkan subnet Anda ke Availability Zone yang berbeda membantu memastikan ketersediaan dan toleransi kesalahan yang lebih baik. Untuk informasi tentang cara membuat VPC dengan subnet pribadi, lihat. the section called “Pengaturan VPC Cepat”

   > **Note**
   >
   > Untuk memastikan setiap instans streaming memiliki akses internet, jangan lampirkan subnet publik ke portal Browser WorkSpaces Aman Anda.

3. Perbarui tabel rute yang terkait dengan subnet pribadi Anda untuk mengarahkan lalu lintas ke internet ke gateway NAT. Ini memungkinkan contoh streaming di subnet pribadi Anda untuk berkomunikasi dengan internet. Untuk informasi tentang cara mengaitkan tabel rute dengan subnet pribadi, selesaikan langkah-langkah di Konfigurasi tabel rute.

Mengaktifkan penjelajahan internet terbatas untuk Amazon WorkSpaces Secure Browser

Pengaturan jaringan yang direkomendasikan dari portal Browser WorkSpaces Aman adalah menggunakan subnet pribadi dengan gateway NAT, sehingga portal dapat menelusuri internet publik dan konten pribadi. Untuk informasi selengkapnya, lihat the section called “Penjelajahan internet tanpa batas”. Namun, Anda mungkin diminta untuk mengontrol komunikasi keluar dari portal Browser WorkSpaces Aman ke internet dengan menggunakan proxy web. Misalnya, jika Anda menggunakan proxy web sebagai gateway ke internet, Anda dapat menerapkan kontrol keamanan preventif, seperti daftar izin domain dan pemfilteran konten. Ini juga dapat mengurangi penggunaan bandwidth dan meningkatkan kinerja jaringan dengan menyimpan sumber daya yang sering diakses, seperti halaman web atau pembaruan perangkat lunak secara lokal. Untuk beberapa kasus penggunaan, Anda mungkin memiliki konten pribadi yang hanya dapat diakses dengan menggunakan proxy web.

Anda mungkin sudah terbiasa dengan mengonfigurasi pengaturan proxy pada perangkat terkelola, atau pada gambar lingkungan virtual Anda. Tetapi ini menimbulkan tantangan jika Anda tidak mengendalikan perangkat (misalnya, ketika pengguna menggunakan perangkat yang tidak dimiliki atau dikelola oleh perusahaan), atau jika Anda perlu mengelola gambar untuk lingkungan virtual Anda. Dengan Browser WorkSpaces Aman, Anda dapat mengatur pengaturan proxy menggunakan kebijakan Chrome yang ada di browser web. Anda dapat melakukan ini dengan menyiapkan proxy keluar HTTP untuk Browser WorkSpaces Aman.

Solusi ini didasarkan pada pengaturan proxy VPC keluar yang direkomendasikan. Solusi proxy didasarkan pada open source HTTP proxy Squid. Kemudian, ia menggunakan pengaturan browser Browser WorkSpaces WorkSpaces Aman untuk mengkonfigurasi portal Browser Aman untuk terhubung ke titik akhir proxy. Untuk informasi selengkapnya, lihat Cara mengatur proxy VPC keluar dengan daftar putih domain dan pemfilteran konten.

Solusi ini memberi Anda manfaat berikut:

- Proxy keluar yang menyertakan grup instans auto-scaling Amazon EC2, yang dihosting oleh penyeimbang beban jaringan. Instans proxy hidup di subnet publik, dan masing-masing terpasang dengan IP Elastis, sehingga mereka dapat memiliki akses ke internet.

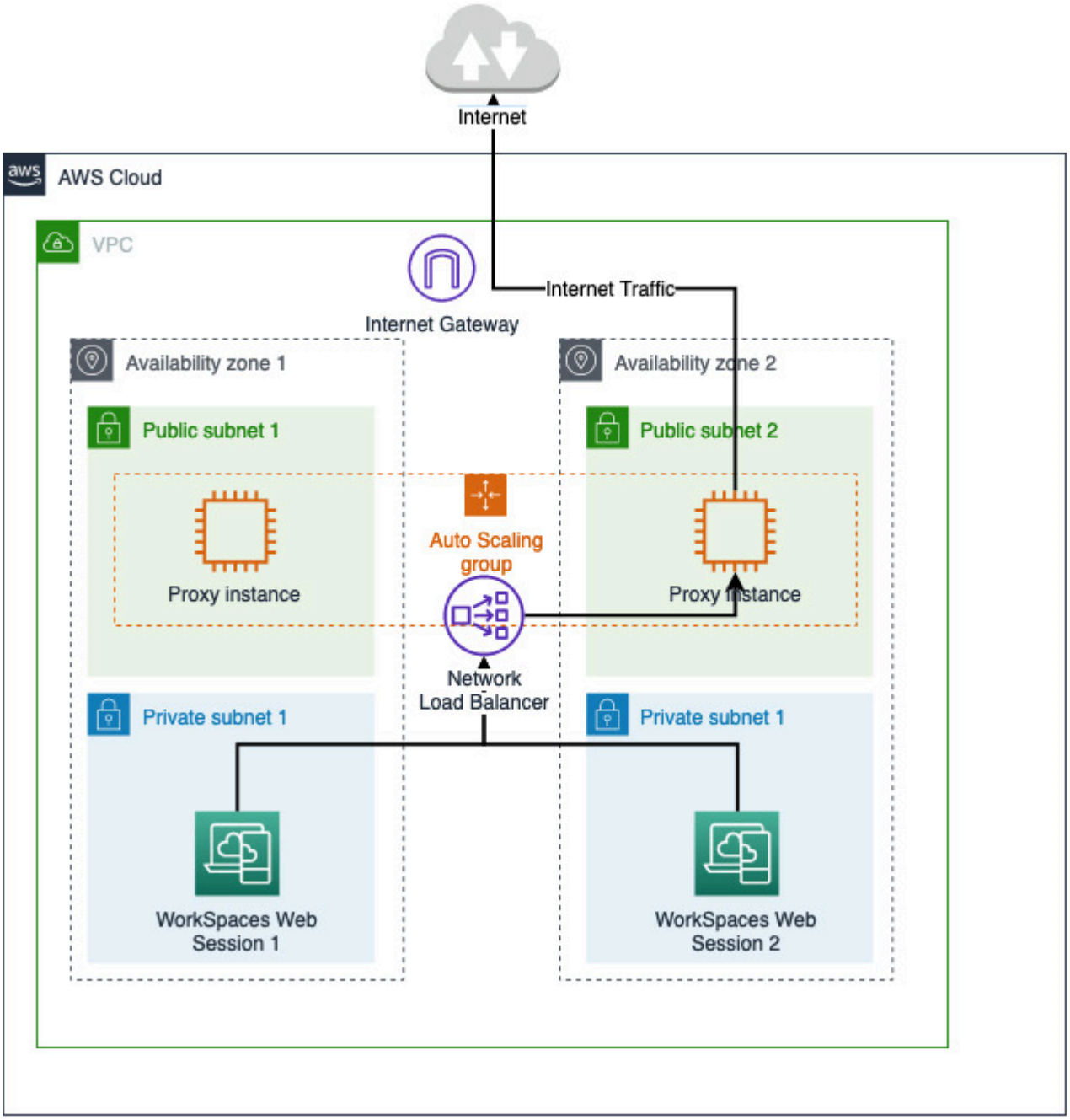
- Portal Browser WorkSpaces Aman digunakan untuk subnet pribadi. Anda tidak perlu mengkonfigurasi gateway NAT untuk mengaktifkan akses internet. Sebagai gantinya, Anda mengonfigurasi kebijakan browser Anda, sehingga semua lalu lintas internet melewati proxy keluar. Jika Anda ingin menggunakan proxy Anda sendiri, pengaturan portal Browser WorkSpaces Aman akan serupa.

Topik

- Arsitektur penjelajahan internet terbatas untuk Amazon WorkSpaces Secure Browser
- Prasyarat penjelajahan internet terbatas untuk Amazon Secure Browser WorkSpaces
- Proxy keluar HTTP untuk Amazon WorkSpaces Secure Browser
- Memecahkan masalah penjelajahan internet terbatas untuk Amazon WorkSpaces Secure Browser

Arsitektur penjelajahan internet terbatas untuk Amazon WorkSpaces Secure Browser

Berikut ini adalah contoh pengaturan proxy tipikal di VPC Anda. Instans proxy Amazon EC2 ada di subnet publik dan terkait dengan Elastic IP, sehingga mereka memiliki akses ke internet. Penyeimbang beban jaringan menjadi tuan rumah grup penskalaan otomatis dari instance proxy. Ini memastikan bahwa instance proxy dapat ditingkatkan secara otomatis, dan penyeimbang beban jaringan adalah titik akhir proxy tunggal, yang dapat dikonsumsi oleh sesi Browser WorkSpaces Aman.



Prasyarat penjelajahan internet terbatas untuk Amazon Secure Browser WorkSpaces

Sebelum memulai, pastikan Anda memenuhi prasyarat berikut:

- Anda memerlukan VPC yang sudah digunakan, dengan subnet publik dan pribadi yang tersebar di beberapa Availability Zones (). AZs Untuk informasi selengkapnya tentang cara mengatur lingkungan VPC, lihat Default. VPCs

- Anda memerlukan satu titik akhir proxy tunggal yang dapat diakses dari subnet pribadi, tempat sesi Browser WorkSpaces Aman hidup (misalnya, nama DNS penyeimbang beban jaringan). Jika Anda ingin menggunakan proxy yang ada, pastikan juga memiliki satu titik akhir yang dapat diakses dari subnet pribadi Anda.

Proxy keluar HTTP untuk Amazon WorkSpaces Secure Browser

Untuk menyiapkan proxy keluar HTTP untuk Browser WorkSpaces Aman, ikuti langkah-langkah berikut.

1. Untuk menerapkan contoh proksi keluar ke VPC Anda, ikuti langkah-langkah di Cara mengatur proxy VPC keluar dengan daftar putih domain dan pemfilteran konten.
   a. Ikuti langkah-langkah di “Instalasi (pengaturan satu kali)” untuk menyebarkan CloudFormation template ke akun Anda. Pastikan untuk memilih VPC dan subnet yang tepat sebagai parameter template. CloudFormation
   b. Setelah penerapan, temukan parameter CloudFormation output OutboundProxyDomaindan OutboundProxyPort. Ini adalah nama dan port DNS proxy Anda.
   c. Jika Anda sudah memiliki proxy sendiri, lewati langkah ini dan gunakan nama dan port DNS proxy Anda.
2. Di Browser WorkSpaces Aman, konsol, pilih portal Anda dan kemudian pilih Edit.
   a. Dalam detail koneksi Jaringan, pilih VPC dan subnet pribadi yang memiliki akses ke proxy.
   b. Di Pengaturan kebijakan, tambahkan ProxySettings kebijakan berikut menggunakan editor JSON. `ProxyServer`Bidang harus berupa nama dan port DNS proxy Anda. Untuk detail selengkapnya tentang ProxySettings kebijakan, lihat ProxySettings.

```
{
    "chromePolicies":
    {
        ...
        "ProxySettings": {
            "value": {
                "ProxyMode": "fixed_servers",
                "ProxyServer": "OutboundProxyLoadBalancer-0a01409a46943c47.elb.us-
west-2.amazonaws.com:3128",
                "ProxyBypassList": "https://www.example1.com,https://
www.example2.com,https://internalsite/"
            }
        },
```

```
    }
}
```

3. Dalam sesi Browser WorkSpaces Aman Anda, Anda akan melihat proxy diterapkan ke pengaturan Chrome menggunakan pengaturan proxy dari administrator Anda.
4. Buka chrome: //policy dan tab Kebijakan Chrome untuk mengonfirmasi bahwa kebijakan tersebut diterapkan.
5. Verifikasi bahwa sesi Browser WorkSpaces Aman Anda berhasil menelusuri konten internet tanpa gateway NAT. Di CloudWatch Log, verifikasi bahwa log akses proxy Squid direkam.

Memecahkan masalah penjelajahan internet terbatas untuk Amazon WorkSpaces Secure Browser

Setelah kebijakan Chrome diterapkan, jika sesi Browser WorkSpaces Aman Anda masih tidak dapat mengakses internet, ikuti langkah-langkah berikut untuk mencoba menyelesaikan masalah Anda:

- Verifikasi bahwa titik akhir proxy dapat diakses dari subnet pribadi tempat portal Browser WorkSpaces Aman Anda tinggal. Untuk melakukan ini, buat instans EC2 di subnet pribadi, dan uji koneksi dari instans EC2 pribadi ke titik akhir proxy Anda.
- Verifikasi bahwa proxy memiliki akses internet.
- Verifikasi bahwa kebijakan Chrome sudah benar.
  - Konfirmasikan pemformatan berikut untuk `ProxyServer` bidang kebijakan:`<Proxy DNS name>:<Proxy port>`. Seharusnya tidak ada `http://` atau `https://` di awalan.
  - Dalam sesi Browser WorkSpaces Aman, gunakan Chrome untuk menavigasi ke chrome: //policy, dan pastikan ProxySettings kebijakan tersebut berhasil diterapkan.

Port konektivitas internet untuk Amazon WorkSpaces Secure Browser

Setiap instance streaming Browser WorkSpaces Aman memiliki antarmuka jaringan pelanggan yang menyediakan konektivitas ke sumber daya dalam VPC Anda, serta ke internet jika subnet pribadi dengan gateway NAT diatur.

Untuk konektivitas internet, port berikut harus terbuka untuk semua tujuan. Jika Anda menggunakan grup keamanan yang dimodifikasi atau kustom, Anda harus menambahkan aturan yang diperlukan secara manual. Untuk informasi selengkapnya, lihat Aturan grup keamanan.

> **Note**
>
> Ini berlaku untuk lalu lintas jalan keluar.

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 8433

Praktik terbaik VPC untuk WorkSpaces Browser Aman

Rekomendasi berikut dapat membantu Anda mengonfigurasi VPC Anda dengan lebih efektif dan aman.

Konfigurasi VPC Keseluruhan

- Pastikan konfigurasi VPC Anda dapat mendukung kebutuhan penskalaan Anda.
- Pastikan bahwa kuota layanan Browser WorkSpaces Aman Anda (juga disebut sebagai batas) cukup untuk mendukung permintaan Anda yang diantisipasi. Untuk meminta peningkatan kuota, Anda dapat menggunakan konsol Service Quotas di. https://console.aws.amazon.com/servicequotas/ Untuk informasi tentang kuota Browser WorkSpaces Aman default, lihatthe section called “Mengelola kuota layanan”.
- Jika Anda berencana untuk menyediakan sesi streaming Anda dengan akses ke internet, kami sarankan Anda mengonfigurasi VPC dengan gateway NAT di subnet publik.

Antarmuka Jaringan Elastis

- Setiap sesi WorkSpaces Secure Browser memerlukan elastic network interface sendiri selama durasi streaming. WorkSpaces Secure Browser menciptakan antarmuka jaringan elastis (ENIs) sebanyak kapasitas maksimum yang diinginkan dari armada Anda. Secara default, batas untuk ENIs per Wilayah adalah 5000. Untuk informasi selengkapnya, lihat Antarmuka jaringan.

  Saat merencanakan kapasitas untuk penyebaran yang sangat besar, misalnya, ribuan sesi streaming bersamaan, pertimbangkan jumlah ENIs yang mungkin diperlukan untuk penggunaan puncak Anda. Kami menyarankan Anda menjaga batas ENI Anda pada atau di atas batas penggunaan bersamaan maksimum yang Anda konfigurasi untuk portal web Anda.

Subnet

- Saat Anda mengembangkan rencana untuk meningkatkan pengguna, ingatlah bahwa setiap sesi Browser WorkSpaces Aman memerlukan alamat IP klien unik dari subnet yang dikonfigurasi. Oleh karena itu, ukuran ruang alamat IP klien yang dikonfigurasi pada subnet Anda menentukan jumlah pengguna yang dapat melakukan streaming secara bersamaan.
- Kami merekomendasikan setiap subnet dikonfigurasi dengan subnet mask yang memungkinkan alamat IP klien yang cukup untuk memperhitungkan jumlah maksimum pengguna bersamaan yang diharapkan. Selain itu, pertimbangkan untuk menambahkan alamat IP tambahan ke akun untuk pertumbuhan yang diantisipasi. Untuk informasi selengkapnya, lihat Ukuran VPC dan Subnet untuk. IPv4
- Kami menyarankan Anda mengonfigurasi subnet di setiap Availability Zone unik yang didukung WorkSpaces Secure Browser di wilayah yang Anda inginkan untuk pertimbangan ketersediaan dan penskalaan. Untuk informasi selengkapnya, lihat the section called “Membuat VPC baru”.
- Pastikan bahwa sumber daya jaringan yang diperlukan untuk aplikasi web Anda dapat diakses melalui subnet Anda.

Grup Keamanan

- Gunakan grup keamanan untuk memberikan kontrol akses tambahan ke VPC Anda.

  Grup keamanan yang termasuk dalam VPC Anda memungkinkan Anda mengontrol lalu lintas jaringan antara instance streaming Browser WorkSpaces Aman dan sumber daya jaringan yang diperlukan oleh aplikasi web. Pastikan bahwa grup keamanan menyediakan akses ke sumber daya jaringan yang dibutuhkan aplikasi web Anda.

Zona Ketersediaan yang Didukung untuk Amazon WorkSpaces Secure Browser

Saat Anda membuat cloud pribadi virtual (VPC) untuk digunakan dengan Browser WorkSpaces Aman, subnet VPC Anda harus berada di Zona Ketersediaan yang berbeda di Wilayah tempat Anda meluncurkan Browser Aman. WorkSpaces Availability Zone berada di lokasi yang berjauhan yang ditata sedemikian rupa agar terisolasi dari kegagalan Availability Zone lain. Dengan meluncurkan instans dalam Availability Zone yang terpisah, Anda dapat melindungi aplikasi Anda dari kegagalan di satu lokasi. Setiap subnet harus berada sepenuhnya dalam satu Availability Zone dan tidak dapat memperluas zona. Sebaiknya konfigurasi subnet untuk setiap AZ yang didukung di wilayah yang Anda inginkan untuk ketahanan maksimum

Availability Zone diwakili oleh kode Wilayah yang diikuti oleh pengidentifikasi huruf; misalnya, `us-east-1a`. Untuk memastikan bahwa sumber daya didistribusikan di seluruh Availability Zone untuk suatu Wilayah, kami secara independen memetakan Availability Zone ke nama untuk setiap akun AWS . Misalnya, Availability Zone `us-east-1a` untuk akun AWS Anda mungkin tidak memiliki lokasi yang sama karena `us-east-1a` untuk akun AWS lainnya.

Untuk mengoordinasikan Availability Zone di seluruh akun, Anda harus menggunakan AZ ID, yang merupakan pengenal unik dan konsisten untuk Availability Zone. Misalnya, `use1-az2` adalah ID AZ untuk `us-east-1` Wilayah dan memiliki lokasi yang sama di setiap AWS akun.

Melihat AZ IDs memungkinkan Anda untuk menentukan lokasi sumber daya dalam satu akun relatif terhadap sumber daya di akun lain. Misalnya, jika Anda membagikan subnet di Availability Zone dengan ID AZ `use1-az2` dengan akun lain, subnet ini tersedia untuk akun tersebut di Availability Zone yang juga memiliki ID AZ yang juga `use1-az2`. ID AZ untuk setiap VPC dan subnet ditampilkan di konsol Amazon VPC.

WorkSpaces Browser Aman tersedia dalam subset Availability Zones untuk setiap Wilayah yang didukung. Tabel berikut mencantumkan AZ IDs yang dapat Anda gunakan untuk setiap Wilayah. Untuk melihat pemetaan AZ IDs ke Availability Zones di akun Anda, lihat AZ IDs untuk Sumber Daya Anda di Panduan AWS RAM Pengguna.

Nama wilayah	Kode Wilayah	AZ yang didukung IDs
AS Timur (Virginia Utara)	`us-east-1`	`use1-az1`, `use1-az2`, `use1-az4`, `use1-az5`, `use1-az6`
US West (Oregon)	`us-west-2`	`usw2-az1`, `usw2-az2`, `usw2-az3`
Asia Pasifik (Mumbai)	`ap-south-1`	`aps1-az1`, `aps1-az3`
Asia Pasifik (Singapura)	`ap-southeast-1`	`apse1-az1` , `apse1-az2` , `apse1-az3`
Asia Pasifik (Sydney)	`ap-southeast-2`	`apse2-az1` , `apse2-az2` , `apse2-az3`
Asia Pasifik (Tokyo)	`ap-northeast-1`	`apne1-az1` , `apne1-az2` , `apne1-az4`

Nama wilayah	Kode Wilayah	AZ yang didukung IDs
Kanada (Pusat)	`ca-central-1`	`cac1-az1`, `cac1-az2`, `cac1-az4`
Eropa (Frankfurt)	`eu-central-1`	`euc1-az2`, `euc1-az2`, `euc1-az3`
Eropa (Irlandia)	`eu-west-1`	`euw1-az1`, `euw1-az2`, `euw1-az3`
Eropa (London)	`eu-west-2`	`euw2-az1`, `euw2-az2`

Untuk informasi selengkapnya tentang Availability Zone dan AZ IDs, lihat Wilayah, Availability Zone, dan Local Zones di Panduan Pengguna Amazon EC2.

Mengaktifkan koneksi pengguna untuk Amazon WorkSpaces Secure Browser

WorkSpaces Browser Aman dikonfigurasi untuk merutekan koneksi streaming melalui internet publik. Konektivitas internet diperlukan untuk mengautentikasi pengguna dan mengirimkan aset web yang dibutuhkan WorkSpaces Secure Browser agar berfungsi. Untuk mengizinkan lalu lintas ini, Anda harus mengizinkan domain yang tercantum di dalamnyaDomain yang diizinkan untuk Amazon WorkSpaces Secure Browser.

Topik berikut memberikan informasi tentang cara mengaktifkan koneksi pengguna ke Browser WorkSpaces Aman.

Topik

- Alamat IP dan persyaratan port untuk Amazon WorkSpaces Secure Browser
- Domain yang diizinkan untuk Amazon WorkSpaces Secure Browser

Alamat IP dan persyaratan port untuk Amazon WorkSpaces Secure Browser

Untuk mengakses instance Browser WorkSpaces Aman, perangkat pengguna memerlukan akses keluar pada port berikut:

- Port 443 (TCP)

  - Port 443 digunakan untuk komunikasi HTTPS antara perangkat pengguna dan instance streaming saat menggunakan titik akhir internet. Biasanya, ketika pengguna akhir menjelajah web selama sesi streaming, browser web secara acak memilih port sumber dalam kisaran tinggi untuk lalu lintas streaming. Anda harus memastikan bahwa lalu lintas kembali ke port ini diizinkan.
  - Port ini harus terbuka untuk domain yang diperlukan yang tercantum diDomain yang diizinkan untuk Amazon WorkSpaces Secure Browser.
  - AWS menerbitkan rentang alamat IP saat ini, termasuk rentang yang dapat diselesaikan oleh Session Gateway dan CloudFront domain, dalam format JSON. Untuk informasi tentang cara mengunduh file.json dan melihat rentang saat ini, lihat rentang alamat AWS IP. Atau, jika Anda menggunakan AWS Tools for Windows PowerShell, Anda dapat mengakses informasi yang sama dengan menggunakan Get-AWSPublicIpAddressRange PowerShell perintah. Untuk informasi selengkapnya, lihat Menanyakan Rentang Alamat IP Publik untuk AWS.
- (Opsional) Port 53 (UDP)
  - Port 53 digunakan untuk komunikasi antara perangkat pengguna dan server DNS Anda.
  - Port ini opsional jika Anda tidak menggunakan server DNS untuk resolusi nama domain.
  - Port harus terbuka ke alamat IP untuk server DNS Anda sehingga nama domain publik dapat diselesaikan.

Domain yang diizinkan untuk Amazon WorkSpaces Secure Browser

Agar pengguna dapat mengakses portal web dari browser lokal mereka, Anda harus menambahkan domain berikut ke daftar izinkan di jaringan tempat pengguna mencoba mengakses layanan tersebut.

Dalam tabel berikut, ganti *{region}* dengan kode Wilayah portal web operasi. Misalnya, s3. *{region}*.amazonaws.com harus s3.eu-west-1.amazonaws.com untuk portal web wilayah Eropa (Irlandia). Untuk daftar kode Wilayah, lihat titik akhir dan kuota Amazon WorkSpaces Secure Browser.

Kategori	Domain atau Alamat IP
WorkSpaces Aset streaming Browser yang aman	s3. *{region}*.amazonaws.com s3.amazonaws.com appstream2. *{region}*.aws.amazon.com

Kategori	Domain atau Alamat IP
	*.amazonappstream.com *.shortbread.aws.dev
WorkSpaces Amankan aset statis Browser	*.workspaces-web.com di5ry4hb4263e.cloudfront.net
WorkSpaces Otentikasi Browser Aman	*.auth. *{region}*.amazoncognito.com kognito-identitas. *{region}*.amazonaws.com kognito-idp. *{region}*.amazonaws.com *.cloudfront.net
WorkSpaces Metrik dan pelaporan Browser yang aman	*.eksekusi api. *{region}*.amazonaws.com unagi-id.amazon.com

Bergantung pada penyedia identitas yang dikonfigurasi, Anda mungkin juga perlu mengizinkan daftar domain tambahan. Tinjau dokumentasi IDP Anda untuk mengidentifikasi domain mana yang Anda perlukan untuk mengizinkan daftar agar Browser WorkSpaces Aman dapat menggunakan penyedia tersebut. Jika Anda menggunakan Pusat Identitas IAM, lihat prasyarat Pusat Identitas IAM untuk informasi lebih lanjut.

Memulai dengan Amazon WorkSpaces Secure Browser

Ikuti langkah-langkah ini untuk membuat portal web Browser WorkSpaces Aman dan memberi pengguna akses ke situs web internal dan SaaS dari browser yang ada. Anda dapat membuat satu portal web di wilayah mana pun yang didukung per akun.

> **Note**
>
> Untuk meminta peningkatan batas untuk lebih dari satu portal, silakan hubungi dukungan dengan Akun AWS ID Anda, jumlah portal yang akan diminta, dan Wilayah AWS.

Proses ini biasanya memakan waktu lima menit dengan wizard pembuatan portal web, dan hingga 15 menit tambahan agar portal menjadi Aktif.

Tidak ada biaya yang terkait dengan pengaturan portal web. WorkSpaces Secure Browser menawarkan pay-as-you-go harga, termasuk harga bulanan yang rendah untuk pengguna yang secara aktif menggunakan layanan ini. Tidak ada biaya di muka, lisensi, atau komitmen jangka panjang.

> **Important**
>
> Sebelum Anda mulai, Anda harus menyelesaikan prasyarat yang diperlukan untuk portal web. Untuk informasi lebih lanjut tentang prasyarat portal web, lihat. Menyiapkan Browser WorkSpaces Aman Amazon

Topik

- Membuat portal web untuk Amazon WorkSpaces Secure Browser
- Menguji portal web Anda di Amazon WorkSpaces Secure Browser
- Mendistribusikan portal web Anda di Amazon WorkSpaces Secure Browser

Membuat portal web untuk Amazon WorkSpaces Secure Browser

Ikuti langkah-langkah ini untuk membuat portal web.

Topik

- Mengkonfigurasi pengaturan jaringan untuk Amazon WorkSpaces Secure Browser
- Mengkonfigurasi pengaturan portal untuk Amazon WorkSpaces Secure Browser
- Mengkonfigurasi pengaturan pengguna untuk Amazon WorkSpaces Secure Browser
- Mengonfigurasi penyedia identitas Anda untuk Amazon WorkSpaces Secure Browser
- Meluncurkan portal web dengan Amazon WorkSpaces Secure Browser

Mengkonfigurasi pengaturan jaringan untuk Amazon WorkSpaces Secure Browser

Untuk mengonfigurasi pengaturan jaringan untuk Browser WorkSpaces Aman ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman di https://console.aws.amazon.com/workspaces-web/rumah.
2. Pilih Browser WorkSpaces Aman, lalu portal Web, lalu pilih Buat portal web.
3. Pada Langkah 1: Tentukan halaman koneksi jaringan, selesaikan langkah-langkah berikut untuk menghubungkan VPC Anda ke portal web Anda dan konfigurasikan VPC dan subnet Anda.
    1. Untuk detail Jaringan, pilih VPC dengan koneksi ke konten yang ingin diakses pengguna dengan WorkSpaces Secure Browser.
    2. Pilih hingga tiga subnet pribadi yang memenuhi persyaratan berikut. Untuk informasi selengkapnya, lihat Jaringan untuk Amazon WorkSpaces Secure Browser.
        - Anda harus memilih minimal dua subnet pribadi untuk membuat portal.
        - Untuk memastikan ketersediaan yang tinggi untuk portal web Anda, kami sarankan Anda menyediakan jumlah maksimum subnet pribadi di zona ketersediaan unik untuk VPC Anda.
    3. Pilih grup keamanan.

Mengkonfigurasi pengaturan portal untuk Amazon WorkSpaces Secure Browser

Pada Langkah 2: Konfigurasikan halaman pengaturan portal web, selesaikan langkah-langkah berikut untuk menyesuaikan pengalaman penjelajahan pengguna Anda saat mereka memulai sesi.

1. Di bawah detail portal Web, untuk nama Tampilan, masukkan nama yang dapat diidentifikasi untuk portal web Anda.
2. Di bawah Jenis Instance, pilih jenis instans untuk portal web Anda dari menu tarik-turun. Kemudian, masukkan batas pengguna bersamaan Max Anda untuk portal web. Untuk informasi selengkapnya, lihat the section called “Mengelola kuota layanan”.

> **Note**
>
> Memilih jenis instans baru akan mengubah biaya untuk setiap pengguna aktif bulanan. Untuk informasi selengkapnya, lihat Harga Amazon WorkSpaces Secure Browser.

3. Di bawah Domain Kustom, Anda dapat mengonfigurasi domain khusus untuk portal Anda untuk mengaktifkan akses melalui nama domain Anda sendiri, bukan titik akhir portal default. Untuk informasi selengkapnya, lihat the section called “Domain kustom”. Ini opsional.
4. Di bawah Session Logger, Anda dapat menentukan bucket S3 untuk menyimpan file log sesi. Untuk informasi selengkapnya, lihat the section called “Menyiapkan Session Logger”. Ini opsional.
5. Di bawah Pencatatan akses pengguna, untuk ID aliran Kinesis, pilih aliran data Amazon Kinesis yang ingin Anda kirimi file log. Untuk informasi selengkapnya, lihat the section called “Menyiapkan pencatatan aktivitas pengguna”. Ini opsional.
6. Di bawah Kontrol Akses IP, pilih apakah akan membatasi akses ke jaringan tepercaya. Untuk informasi selengkapnya, lihat the section called “Mengelola kontrol akses IP”. Ini opsional.
7. Di bawah Pengaturan Perlindungan Data, Anda dapat membuat kebijakan untuk Browser WorkSpaces Aman untuk menyunting informasi sensitif. Untuk informasi selengkapnya, lihat the section called “Pengaturan perlindungan data”. Ini opsional.
8. Di bawah pemfilteran URL, Anda dapat menentukan pengguna URLs akhir mana yang diizinkan mengakses atau memblokir kategori tertentu URLs atau domain untuk membatasi akses. Untuk informasi selengkapnya, lihat the section called “Pemfilteran konten web”. Ini opsional.

    1. Untuk membatasi penjelajahan sesi ke beberapa domain yang dipilih, aktifkan sakelar Blokir semua URLs dan klik tambahkan URL untuk memberikan daftar pengguna akhir URLs Anda yang diizinkan untuk mengakses.
    2. Untuk membuat daftar URLs untuk memblokir pengguna akhir, klik Tambahkan URL untuk mencantumkan single URLs yang akan diblokir atau klik Tambahkan kategori untuk memilih kategori domain yang diblokir (mis., Jejaring Sosial).

9. Di bawah Pengaturan kebijakan, Anda dapat menyetel kebijakan browser apa pun menggunakan kebijakan Chrome yang tersedia untuk versi stabil terbaru ke portal web. Untuk informasi selengkapnya, lihat the section called “Mengelola kebijakan browser”. Ini opsional.

    1. Anda dapat dengan cepat memilih beberapa kebijakan yang paling umum di editor Visual
        - Untuk URL Startup - opsional, masukkan domain untuk digunakan sebagai beranda saat pengguna meluncurkan browser mereka. VPC Anda harus memiliki koneksi yang stabil ke URL ini.
        - Pilih atau hapus Penjelajahan pribadi dan penghapusan Riwayat untuk mengaktifkan atau menonaktifkan fitur ini selama sesi pengguna

        > **Note**
        >
        > URLs dikunjungi saat menjelajah secara pribadi, atau sebelum pengguna menghapus riwayat browser mereka, tidak dapat direkam dalam pencatatan akses pengguna. Untuk informasi selengkapnya, lihat the section called “Menyiapkan pencatatan aktivitas pengguna”.

        - Untuk bookmark Browser - opsional, masukkan nama Tampilan, Domain, dan Folder untuk setiap bookmark yang Anda ingin pengguna Anda lihat di browser mereka. Kemudian, pilih Tambahkan bookmark.

        > **Note**
        >
        > Domain adalah bidang wajib untuk bookmark browser.
        > Di Chrome, pengguna dapat menemukan bookmark terkelola di folder Bookmark terkelola pada bilah alat bookmark.

    2. Anda juga dapat langsung menambahkan atau mengedit kebijakan dengan menggunakan editor JSON alih-alih editor visual. Untuk format kebijakan tertentu, silakan lihat daftar kebijakan Chrome Enterprise.
    3. Anda juga dapat mengimpor kebijakan Chrome yang digunakan di organisasi Anda dengan mengunggah file JSON ke portal web. Untuk detailnya, silakan lihat the section called “Tutorial: Mengatur kebijakan browser khusus”

        Saat mengunggah file kebijakan, Anda dapat melihat kebijakan yang tersedia di file di konsol. Namun, Anda tidak dapat mengedit semua kebijakan di editor visual. Konsol mencantumkan

kebijakan dalam file JSON yang tidak dapat Anda edit dengan editor visual di bawah kebijakan JSON Tambahan. Untuk membuat perubahan pada kebijakan ini, Anda harus mengeditnya secara manual.

10. Tambahkan Tag ke portal Anda. Anda dapat menggunakan tag untuk mencari atau memfilter AWS sumber daya Anda. Tag terdiri dari kunci dan nilai opsional dan dikaitkan dengan sumber daya portal Anda. Ini opsional.
11. Pilih Next untuk melanjutkan.

Mengkonfigurasi pengaturan pengguna untuk Amazon WorkSpaces Secure Browser

Pada Langkah 3: Pilih halaman pengaturan pengguna, selesaikan langkah-langkah berikut untuk memilih fitur mana yang dapat diakses pengguna Anda dari bilah navigasi atas selama sesi mereka, lalu pilih Berikutnya:

1. Di bawah kustomisasi Branding, Anda dapat menyesuaikan layar masuk dan memuat yang muncul untuk pengguna akhir Anda dengan memodifikasi elemen visual, konten teks, dan persyaratan layanan. Untuk informasi selengkapnya, lihat the section called “Penyesuaian branding”. Ini opsional.
2. Di bawah Izin, pilih apakah akan mengaktifkan ekstensi untuk sistem masuk tunggal. Untuk informasi selengkapnya, lihat the section called “Mengelola ekstensi masuk tunggal”.
3. Untuk Izinkan pengguna mencetak ke perangkat lokal dari portal web mereka, pilih Diizinkan atau Tidak diizinkan.
4. Untuk Izinkan pengguna melakukan deeplink ke portal web mereka, pilih Diizinkan atau Tidak Diizinkan. Untuk informasi lebih lanjut tentang deep link, lihatthe section called “Deep link”.
5. Untuk Izinkan pengguna menggunakan otentikasi lokal di sesi portal mereka, pilih Diizinkan atau Tidak Diizinkan. Untuk informasi selengkapnya tentang otentikasi web, lihatthe section called “Pengalihan otentikasi web”.
6. Di bawah kontrol Toolbar, pilih pengaturan yang Anda inginkan di bawah Fitur.
7. Di bawah Pengaturan, kelola tampilan presentasi bilah alat di awal sesi termasuk status bilah alat (berlabuh atau terlepas), tema (mode gelap atau terang), visibilitas ikon, dan resolusi tampilan maksimum untuk sesi. Biarkan pengaturan ini tidak dikonfigurasi untuk memberikan pengguna akhir kontrol penuh atas opsi ini. Untuk informasi selengkapnya, lihat the section called “Kontrol bilah alat”.

8. Untuk batas waktu Sesi, tentukan yang berikut ini:

   - Untuk Putuskan batas waktu dalam hitungan menit, pilih jumlah waktu sesi streaming tetap aktif setelah pengguna memutuskan sambungan. Jika pengguna mencoba menyambung kembali ke sesi streaming setelah pemutusan atau gangguan jaringan dalam interval waktu ini, mereka terhubung ke sesi sebelumnya. Jika tidak, mereka terhubung ke sesi baru dengan instans streaming baru.

     Jika pengguna mengakhiri sesi, batas waktu pemutusan tidak berlaku. Sebagai gantinya, pengguna diminta untuk menyimpan dokumen yang terbuka, dan kemudian segera terputus dari instance streaming. Contoh yang digunakan pengguna kemudian dihentikan.
   - Untuk batas waktu pemutusan Idle dalam hitungan menit, pilih jumlah waktu pengguna dapat menganggur (tidak aktif) sebelum mereka terputus dari sesi streaming mereka dan batas waktu Putuskan sambungan dalam interval waktu menit dimulai. Pengguna akan diberi tahu sebelum koneksi mereka terputus karena tidak ada aktivitas. Jika mereka mencoba menyambung kembali ke sesi streaming sebelum interval waktu yang ditentukan dalam batas waktu Putuskan sambungan dalam menit telah berlalu, mereka terhubung ke sesi sebelumnya. Jika tidak, mereka terhubung ke sesi baru dengan instans streaming baru. Menyetel nilai ini ke 0 menonaktifkannya. Ketika nilai ini dinonaktifkan, pengguna tidak terputus karena tidak aktif.

     > **Note**
     >
     > Pengguna dianggap dalam keadaan diam ketika mereka berhenti memberikan input keyboard atau mouse selama sesi streaming mereka. Unggahan dan unduhan file, audio masuk, audio keluar, dan perubahan piksel tidak memenuhi syarat sebagai aktivitas pengguna. Jika pengguna terus menganggur setelah interval waktu di batas waktu pemutusan Idle dalam beberapa menit berlalu, mereka terputus.

Mengonfigurasi penyedia identitas Anda untuk Amazon WorkSpaces Secure Browser

Gunakan langkah-langkah berikut untuk mengonfigurasi penyedia identitas Anda (iDP).

Topik

- Memilih jenis penyedia identitas untuk Amazon WorkSpaces Secure Browser
- Mengubah jenis penyedia identitas untuk Amazon WorkSpaces Secure Browser

Memilih jenis penyedia identitas untuk Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser menawarkan dua jenis otentikasi: Standar dan AWS IAM Identity Center. Anda memilih jenis otentikasi yang akan digunakan dengan portal Anda di halaman Konfigurasi penyedia identitas.

- Untuk Standar (opsi default), gabungkan penyedia identitas SAMP 2.0 pihak ketiga Anda (seperti Okta atau Ping) langsung dengan portal Anda. Untuk informasi selengkapnya, lihat the section called “Jenis otentikasi standar”. Tipe standar mendukung alur otentikasi yang diprakarsai SP dan yang diprakarsai IDP.
- Untuk Pusat Identitas IAM (opsi lanjutan), gabungkan Pusat Identitas IAM dengan portal Anda. Untuk menggunakan jenis otentikasi ini, Pusat Identitas IAM dan portal Browser WorkSpaces Aman Anda harus berada di tempat yang sama. Wilayah AWS Untuk informasi selengkapnya, lihat the section called “Jenis otentikasi Pusat Identitas IAM”.

Topik

- Mengonfigurasi jenis otentikasi standar untuk Amazon Secure Browser WorkSpaces
- Mengonfigurasi jenis autentikasi Pusat Identitas IAM untuk Amazon Secure Browser WorkSpaces

Mengonfigurasi jenis otentikasi standar untuk Amazon Secure Browser WorkSpaces

Jenis otentikasi standar adalah jenis otentikasi default. Ini dapat mendukung alur masuk yang dimulai oleh penyedia layanan (dimulai SP) dan yang diprakarsai oleh penyedia identitas (diprakarsai IDP) dengan IDP yang sesuai dengan SAMP 2.0 Anda. Untuk mengonfigurasi jenis otentikasi standar, ikuti langkah-langkah di bawah ini untuk menggabungkan IDP SAMP 2.0 pihak ketiga Anda (seperti Okta atau Ping) secara langsung dengan portal Anda.

Topik

- Mengonfigurasi penyedia identitas Anda di Amazon WorkSpaces Secure Browser
- Mengkonfigurasi IDP Anda di IDP Anda sendiri
- Menyelesaikan konfigurasi IDP di Amazon Secure Browser WorkSpaces
- Panduan untuk menggunakan khusus IdPs dengan Amazon WorkSpaces Secure Browser

Mengonfigurasi penyedia identitas Anda di Amazon WorkSpaces Secure Browser

Selesaikan langkah-langkah berikut untuk mengonfigurasi penyedia identitas Anda:

1. Pada halaman Configure identity provider dari wizard pembuatan, pilih Standard.
2. Pilih Lanjutkan dengan IDP Standar.
3. Unduh file metadata SP, dan biarkan tab tetap terbuka untuk nilai metadata individual.
   - Jika file metadata SP tersedia, pilih Unduh file metadata untuk mengunduh dokumen metadata penyedia layanan (SP), dan unggah file metadata penyedia layanan ke IDP Anda di langkah berikutnya. Tanpa ini, pengguna tidak akan dapat masuk.
   - Jika penyedia Anda tidak mengunggah file metadata SP, masukkan nilai metadata secara manual.
4. Di bawah Pilih tipe login SAMP, pilih antara pernyataan SAMP yang diprakarsai SP dan yang diprakarsai IDP, atau hanya pernyataan SAMP yang diprakarsai SP.
   - Pernyataan SAMP yang diprakarsai SP dan yang diprakarsai IDP memungkinkan portal Anda mendukung kedua jenis alur masuk. Portal yang mendukung alur yang diprakarsai IDP memungkinkan Anda untuk menyajikan pernyataan SAMP ke titik akhir federasi identitas layanan tanpa mengharuskan pengguna untuk meluncurkan sesi dengan mengunjungi URL portal.
     - Pilih ini untuk memungkinkan portal menerima pernyataan SAMP yang diprakarsai IDP yang tidak diminta.
     - Opsi ini memerlukan Status Relay default untuk dikonfigurasi di Penyedia Identitas SAMP 2.0 Anda. Parameter status Relay untuk portal Anda ada di konsol di bawah login SAMP yang dimulai IDP, atau Anda dapat menyalinnya dari file metadata SP di bawah. `<md:IdPInitRelayState>`
     - Catatan
       - Berikut ini adalah format status relai:`redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com %2Fsso&response_type=code&client_id=1example23456789&identity_provider=Ex Identity-Provider`.
       - Jika Anda menyalin dan menempelkan nilai dari file metadata SP, pastikan Anda mengubahnya`&` . & `&`adalah karakter pelarian XHTML.
   - Pilih pernyataan SAMP yang diprakarsai SP hanya agar portal hanya mendukung alur masuk yang diprakarsai SP. Opsi ini akan menolak pernyataan SAMP yang tidak diminta dari alur masuk yang diprakarsai IDP.

> **Note**
>
> Beberapa pihak ketiga IdPs memungkinkan Anda membuat aplikasi SAMP kustom yang dapat memberikan pengalaman otentikasi yang diprakarsai IDP dengan memanfaatkan alur yang diprakarsai SP. Misalnya, lihat Menambahkan aplikasi bookmark Okta.

5. Pilih apakah Anda ingin mengaktifkan permintaan Sign SAMP ke penyedia ini. Otentikasi yang dimulai SP memungkinkan IDP Anda untuk memvalidasi bahwa permintaan otentikasi berasal dari portal, yang mencegah penerimaan permintaan pihak ketiga lainnya.
   a. Unduh sertifikat penandatanganan dan unggah ke IDP Anda. Sertifikat penandatanganan yang sama dapat digunakan untuk logout tunggal.
   b. Aktifkan permintaan yang ditandatangani di IDP Anda. Namanya mungkin berbeda, tergantung pada IDP.

   > **Note**
   >
   > RSA- SHA256 adalah satu-satunya permintaan dan algoritma penandatanganan permintaan default yang didukung.

6. Pilih apakah Anda ingin mengaktifkan Perlukan pernyataan SAMP terenkripsi. Ini memungkinkan Anda untuk mengenkripsi pernyataan SAMP yang berasal dari IDP Anda. Hal ini dapat mencegah data dari dicegat dalam pernyataan SAMP antara IDP dan Secure Browser. WorkSpaces

   > **Note**
   >
   > Sertifikat enkripsi tidak tersedia pada langkah ini. Ini akan dibuat setelah portal Anda diluncurkan. Setelah Anda meluncurkan portal, unduh sertifikat enkripsi dan unggah ke IDP Anda. Kemudian, aktifkan enkripsi pernyataan di IDP Anda (namanya mungkin berbeda, tergantung pada IDP.

7. Pilih apakah Anda ingin mengaktifkan Single Logout. Single logout memungkinkan pengguna akhir Anda untuk keluar dari sesi IDP WorkSpaces dan Secure Browser mereka dengan satu tindakan.
   a. Unduh sertifikat penandatanganan dari WorkSpaces Secure Browser dan unggah ke IDP Anda. Ini adalah sertifikat penandatanganan yang sama yang digunakan untuk Penandatanganan Permintaan pada langkah sebelumnya.

b. Menggunakan Single Logout mengharuskan Anda untuk mengonfigurasi URL Logout Tunggal di penyedia identitas SAMP 2.0 Anda. Anda dapat menemukan URL Logout Tunggal untuk portal Anda di konsol di bawah Detail penyedia layanan (SP) - Tampilkan nilai metadata individual, atau dari file metadata SP di bawah. `<md:SingleLogoutService>`

c. Aktifkan Single Logout di IDP Anda. Namanya mungkin berbeda, tergantung pada IDP.

Mengkonfigurasi IDP Anda di IDP Anda sendiri

Untuk mengonfigurasi iDP Anda di IDP Anda sendiri, ikuti langkah-langkah berikut.

1. Buka tab baru di browser Anda.
2. Tambahkan metadata portal Anda ke IDP SAMP Anda.

   Unggah dokumen metadata SP yang Anda unduh di langkah sebelumnya ke iDP Anda, atau salin dan tempel nilai metadata ke bidang yang benar di iDP Anda. Beberapa penyedia tidak mengizinkan pengunggahan file.

   Rincian proses ini dapat bervariasi antar penyedia. Temukan dokumentasi penyedia Anda the section called “Bimbingan untuk spesifik IdPs” untuk mendapatkan bantuan tentang cara menambahkan detail portal ke konfigurasi iDP Anda.
3. Konfirmasikan NameID untuk pernyataan SAMP Anda.

   Pastikan IDP SAMP Anda mengisi nameID di pernyataan SAMP dengan bidang email pengguna. NameID dan email pengguna digunakan untuk mengidentifikasi pengguna federasi SAMP Anda secara unik dengan portal. Gunakan format ID Nama SAMP persisten.
4. Opsional: Konfigurasikan Status Relay untuk otentikasi yang dimulai IDP.

   Jika Anda memilih Accept SP-initiated dan IDP-initiated SAMP assertions pada langkah sebelumnya, ikuti langkah-langkah di langkah 2 untuk the section called “Konfigurasi IDP pada WorkSpaces Browser Aman” mengatur Status Relay default untuk aplikasi IDP Anda.
5. Opsional: Konfigurasikan penandatanganan Permintaan. Jika Anda memilih Menandatangani permintaan SAMP ke penyedia ini pada langkah sebelumnya, ikuti langkah-langkah di langkah 3 the section called “Konfigurasi IDP pada WorkSpaces Browser Aman” untuk mengunggah sertifikat penandatanganan ke IDP Anda dan mengaktifkan penandatanganan permintaan. Beberapa IdPs seperti Okta mungkin mengharuskan NameID Anda termasuk dalam tipe “persisten” untuk menggunakan penandatanganan Permintaan. Pastikan untuk mengonfirmasi NameID Anda untuk pernyataan SAMP Anda dengan mengikuti langkah-langkah di atas.

6. Opsional: Konfigurasikan enkripsi Assertion. Jika Anda memilih Memerlukan pernyataan SAMP terenkripsi dari penyedia ini, tunggu hingga pembuatan portal selesai, lalu ikuti langkah 4 di “Unggah metadata” di bawah ini untuk mengunggah sertifikat enkripsi ke IDP Anda dan mengaktifkan enkripsi pernyataan.
7. Opsional: Konfigurasikan Single Logout. Jika Anda memilih Single Logout, ikuti langkah-langkah di langkah 5 the section called “Konfigurasi IDP pada WorkSpaces Browser Aman” untuk mengunggah sertifikat penandatanganan ke IDP Anda, isi URL Logout Tunggal, dan aktifkan Single Logout.
8. Berikan akses ke pengguna Anda di IDP Anda untuk menggunakan Browser WorkSpaces Aman.
9. Unduh file pertukaran metadata dari IDP Anda. Anda akan mengunggah metadata ini ke WorkSpaces Secure Browser di langkah berikutnya.

Menyelesaikan konfigurasi IDP di Amazon Secure Browser WorkSpaces

Untuk menyelesaikan konfigurasi IDP di Browser WorkSpaces Aman ikuti langkah-langkah ini.

1. Kembali ke WorkSpaces Secure Browserconsole. Pada halaman Konfigurasi penyedia identitas dari panduan pembuatan, di bawah metadata iDP, unggah file metadata, atau masukkan URL metadata dari iDP Anda. Portal menggunakan metadata ini dari IDP Anda untuk membangun kepercayaan.
2. Untuk mengunggah file metadata, di bawah dokumen metadata iDP, pilih Pilih file. Unggah file metadata berformat XML dari IDP yang Anda unduh pada langkah sebelumnya.
3. Untuk menggunakan URL metadata, buka IDP yang Anda atur pada langkah sebelumnya dan dapatkan URL Metadata-nya. Kembali ke konsol Browser WorkSpaces Aman, dan di bawah URL metadata iDP, masukkan url metadata yang Anda peroleh dari iDP Anda.
4. Setelah selesai, pilih Berikutnya.
5. Untuk portal di mana Anda telah mengaktifkan Perlukan pernyataan SAMP terenkripsi dari opsi penyedia ini, Anda perlu mengunduh sertifikat enkripsi dari bagian detail iDP portal dan mengunggahnya ke IDP Anda. Kemudian, Anda dapat mengaktifkan opsi di sana.

> **Note**
>
> WorkSpaces Browser Aman memerlukan subjek atau nameID untuk dipetakan dan disetel dalam pernyataan SAMP dalam pengaturan IDP Anda. IDP Anda dapat membuat pemetaan ini secara otomatis. Jika pemetaan ini tidak dikonfigurasi dengan benar, pengguna Anda tidak dapat masuk ke portal web dan memulai sesi.

WorkSpaces Browser Aman mengharuskan klaim berikut hadir dalam respons SAMP. Anda dapat menemukan *<Your SP Entity ID>* dan *<Your SP ACS URL>* dari detail penyedia layanan portal atau dokumen metadata Anda, baik melalui konsol atau CLI.

- `AudienceRestriction`Klaim dengan `Audience` nilai yang menetapkan ID Entitas SP Anda sebagai target respons. Contoh:

```
<saml:AudienceRestriction>
    <saml:Audience><Your SP Entity ID></saml:Audience>
</saml:AudienceRestriction>
```

- `Response`Klaim dengan `InResponseTo` nilai ID permintaan SAMP asli. Contoh:

```
<samlp:Response ... InResponseTo="<originalSAMLrequestId>">
```

- `SubjectConfirmationData`Klaim dengan `Recipient` nilai URL SP ACS Anda, dan `InResponseTo` nilai yang cocok dengan ID permintaan SAMP asli. Contoh:

```
<saml:SubjectConfirmation>
    <saml:SubjectConfirmationData ...
        Recipient="<Your SP ACS URL>"
        InResponseTo="<originalSAMLrequestId>"
        />
</saml:SubjectConfirmation>
```

WorkSpaces Browser Aman memvalidasi parameter permintaan dan pernyataan SAMP Anda. Untuk pernyataan SAMP yang diprakarsai IDP, rincian permintaan Anda harus diformat sebagai `RelayState` parameter di badan permintaan HTTP POST. Badan permintaan juga harus berisi pernyataan SAMP Anda sebagai parameter. `SAMLResponse` Keduanya harus ada jika Anda telah mengikuti langkah sebelumnya.
Berikut ini adalah contoh `POST` badan untuk penyedia SAMP yang diprakarsai IDP.

```
SAMLResponse=<Base64-encoded SAML assertion>&RelayState=<RelayState>
```

Panduan untuk menggunakan khusus IdPs dengan Amazon WorkSpaces Secure Browser

Untuk memastikan Anda mengonfigurasi federasi SAMP dengan benar untuk portal Anda, lihat tautan di bawah ini untuk dokumentasi dari yang umum digunakan IdPs.

IdP	Pengaturan aplikasi SAMP	Manajemen pengguna	Autentikasi yang diprakarsai IDP	Permintaan penandatanganan	Enkripsi pernyataan	Keluar tunggal
Okta	Buat integrasi aplikasi SAMP	Manajemen pengguna	Referensi bidang Wizard Integrasi Aplikasi SAMP	Referensi bidang Wizard Integrasi Aplikasi SAMP	Referensi bidang Wizard Integrasi Aplikasi SAMP	Referensi bidang Wizard Integrasi Aplikasi SAMP
Entra	Buat aplikasi Anda sendiri	Mulai cepat: Buat dan tetapkan akun pengguna	Aktifkan sistem masuk tunggal untuk aplikasi perusahaan	SAMP Minta Verifikasi Tanda Tangan	Konfigurasikan enkripsi token Microsoft Entra SAMP	Protokol SAMP Keluar Tunggal
Ping	Tambahkan aplikasi SAMP	Pengguna	Mengaktifkan SSO yang diprakarsai IDP	Mengkonfigurasi permintaan otentikasi masuk untuk Enterprise PingOne	Apakah PingOne untuk Enterprise mendukung enkripsi?	SAMP 2.0 logout tunggal
Satu Login	Konektor Kustom SAMP (Lanjutan) (4266907)	Tambahkan Pengguna ke OneLogin Secara Manual	Konektor Kustom SAMP (Lanjutan) (4266907)	Konektor Kustom SAMP (Lanjutan) (4266907)	Konektor Kustom SAMP (Lanjutan) (4266907)	Konektor Kustom SAMP (Lanjutan) (4266907)

IdP	Pengaturan aplikasi SAMP	Manajemen pengguna	Autentikasi yang diprakarsai IDP	Permintaan penandatanganan	Enkripsi pernyataan	Keluar tunggal
Pusat Identitas IAM	Siapkan aplikasi SAMP 2.0 Anda sendiri	Siapkan aplikasi SAMP 2.0 Anda sendiri	Siapkan aplikasi SAMP 2.0 Anda sendiri	N/A	N/A	N/A

Mengonfigurasi jenis autentikasi Pusat Identitas IAM untuk Amazon Secure Browser WorkSpaces

Untuk tipe Pusat Identitas IAM (lanjutan), Anda menggabungkan Pusat Identitas IAM dengan portal Anda. Hanya pilih opsi ini jika hal berikut berlaku untuk Anda:

- Pusat Identitas IAM Anda dikonfigurasi dalam hal yang sama Akun AWS dan Wilayah AWS sebagai portal web Anda.
- Jika Anda menggunakan AWS Organizations, Anda menggunakan akun manajemen.

Sebelum membuat portal web dengan tipe autentikasi IAM Identity Center, Anda harus menyiapkan IAM Identity Center sebagai penyedia mandiri. Untuk informasi selengkapnya, lihat Memulai tugas umum di Pusat Identitas IAM. Atau, Anda dapat menghubungkan SAMP 2.0 IDP Anda ke IAM Identity Center. Untuk informasi selengkapnya, lihat Connect ke penyedia identitas eksternal. Jika tidak, Anda tidak akan memiliki pengguna atau grup untuk ditetapkan ke portal web Anda.

Jika Anda sudah menggunakan IAM Identity Center, Anda dapat memilih IAM Identity Center sebagai jenis penyedia dan ikuti langkah-langkah di bawah ini untuk menambah, melihat, atau menghapus pengguna atau grup dari portal web Anda.

> **Note**
>
> Untuk menggunakan jenis otentikasi ini, Pusat Identitas IAM Anda harus sama Akun AWS dan Wilayah AWS sebagai portal Browser WorkSpaces Aman Anda. Jika Pusat Identitas IAM Anda terpisah Akun AWS atau Wilayah AWS, ikuti petunjuk untuk jenis otentikasi Standar. Untuk informasi selengkapnya, lihat the section called “Jenis otentikasi standar”.

Jika Anda menggunakan AWS Organizations, Anda hanya dapat membuat portal Browser WorkSpaces Aman yang terintegrasi dengan IAM Identity Center menggunakan akun manajemen.

Topik

- Membuat portal web dengan IAM Identity Center
- Mengelola portal web Anda dengan IAM Identity Center
- Menambahkan pengguna dan grup tambahan ke portal web
- Melihat atau menghapus pengguna dan grup untuk portal web Anda

Membuat portal web dengan IAM Identity Center

Untuk membuat portal web dengan IAM Identity Center, ikuti langkah-langkah ini.

Untuk membuat portal web dengan IAM Identity Center

1. Selama pembuatan portal pada Langkah 4: Konfigurasikan penyedia identitas, pilih AWS IAM Identity Center.
2. Pilih Lanjutkan dengan Pusat Identitas IAM.
3. Pada halaman Tetapkan pengguna dan grup, pilih tab and/or Grup Pengguna.
4. Centang kotak di samping pengguna atau grup yang ingin Anda tambahkan ke portal.
5. Setelah Anda membuat portal, pengguna yang terkait dapat masuk ke Browser WorkSpaces Aman dengan nama pengguna dan kata sandi Pusat Identitas IAM mereka.

Mengelola portal web Anda dengan IAM Identity Center

Untuk mengelola portal web Anda dengan IAM Identity Center, ikuti langkah-langkah ini.

Untuk mengelola portal web Anda dengan IAM Identity Center

1. Setelah Anda membuat portal Anda, itu terdaftar di konsol Pusat Identitas IAM sebagai aplikasi yang dikonfigurasi.
2. Untuk mengakses konfigurasi aplikasi ini, pilih Aplikasi di sidebar, dan cari aplikasi yang dikonfigurasi dengan nama yang cocok dengan nama tampilan untuk portal web Anda.

> **Note**
>
> Jika Anda belum memasukkan nama tampilan, GUID portal Anda ditampilkan sebagai gantinya. GUID adalah ID yang diawali dengan URL endpoint portal web Anda.

Menambahkan pengguna dan grup tambahan ke portal web

Untuk menambahkan pengguna dan grup tambahan ke portal web yang ada, ikuti langkah-langkah ini.

Untuk menambahkan pengguna dan grup tambahan ke portal web yang ada

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Edit.
3. Pilih Pengaturan penyedia identitas dan Tetapkan pengguna dan grup tambahan. Dari sini, Anda dapat menambahkan pengguna dan grup ke portal web Anda.

> **Note**
>
> Anda tidak dapat menambahkan pengguna atau grup dari konsol Pusat Identitas IAM. Anda harus melakukan ini dari halaman edit portal Browser WorkSpaces Aman Anda.

Melihat atau menghapus pengguna dan grup untuk portal web Anda

Untuk melihat atau menghapus pengguna dan grup untuk portal web Anda, gunakan tindakan yang tersedia di tabel Pengguna yang ditugaskan. Untuk informasi selengkapnya, lihat Mengelola akses ke aplikasi

> **Note**
>
> Anda tidak dapat melihat atau menghapus pengguna dan grup dari halaman edit Portal Browser WorkSpaces Aman. Anda harus melakukan ini dari halaman edit konsol Pusat Identitas IAM Anda.

Mengubah jenis penyedia identitas untuk Amazon WorkSpaces Secure Browser

Anda dapat mengubah jenis otentikasi portal Anda kapan saja. Untuk melakukan ini, ikuti langkah-langkah ini.

- Untuk mengubah dari IAM Identity Center ke Standard, ikuti langkah-langkah dithe section called "Jenis otentikasi standar".
- Untuk mengubah dari Standard ke IAM Identity Center, ikuti langkah-langkah dithe section called "Jenis otentikasi Pusat Identitas IAM".

Perubahan pada jenis penyedia identitas dapat memakan waktu hingga 15 menit untuk diterapkan, dan tidak akan secara otomatis mengakhiri sesi yang sedang berlangsung.

Anda dapat melihat perubahan jenis penyedia identitas ke portal Anda AWS CloudTrail dengan memeriksa `UpdatePortal` peristiwa. Jenis ini terlihat dalam muatan permintaan dan respons acara.

Meluncurkan portal web dengan Amazon WorkSpaces Secure Browser

Setelah selesai mengonfigurasi portal web Anda, Anda dapat mengikuti langkah-langkah ini untuk meluncurkannya.

1. Pada Langkah 5: Tinjau dan luncurkan halaman, tinjau pengaturan yang Anda pilih untuk portal web Anda. Anda dapat memilih Edit untuk mengubah pengaturan dalam bagian tertentu. Anda juga dapat mengubah pengaturan ini nanti dari tab portal Web konsol.
2. Setelah selesai, pilih Luncurkan portal web.
3. Untuk melihat status portal web Anda, pilih portal Web, pilih portal Anda, lalu pilih Lihat detail.

   Portal web memiliki salah satu status berikut:

   - Tidak lengkap - Konfigurasi portal web tidak memiliki pengaturan penyedia identitas yang diperlukan.
   - Menunggu - Portal web sedang menerapkan perubahan pada pengaturannya.
   - Aktif - Portal web sudah siap dan tersedia untuk digunakan.
4. Tunggu hingga 15 menit hingga portal Anda menjadi Aktif.

Menguji portal web Anda di Amazon WorkSpaces Secure Browser

Setelah membuat portal web, Anda dapat masuk ke titik akhir Browser WorkSpaces Aman untuk menelusuri situs web yang terhubung seperti yang dilakukan pengguna akhir.

Jika Anda sudah menyelesaikan langkah-langkah inithe section called “Konfigurasi penyedia identitas”, Anda dapat melewati bagian ini dan pergi keMendistribusikan portal web Anda di Amazon WorkSpaces Secure Browser.

1. Buka konsol Browser WorkSpaces Aman di https://console.aws.amazon.com/workspaces-web/rumah? wilayah=us-timur-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Lihat detail
3. Di bawah titik akhir portal Web, buka URL yang ditentukan untuk portal Anda. Titik akhir portal web adalah titik akses yang akan digunakan oleh pengguna untuk meluncurkan portal web Anda setelah masuk dengan penyedia identitas yang dikonfigurasi untuk portal. Ini tersedia untuk umum di internet dan dapat disematkan ke jaringan Anda.
4. Pada halaman login Browser WorkSpaces Aman, pilih Masuk, SAMP, dan masukkan kredensi SAMP Anda.
5. Saat Anda melihat halaman Sesi Anda sedang disiapkan, sesi Browser WorkSpaces Aman Anda diluncurkan. Jangan menutup atau keluar dari halaman ini.
6. Browser web diluncurkan, menampilkan URL startup Anda dan perilaku tambahan lainnya yang dikonfigurasi melalui pengaturan kebijakan browser Anda.
7. Anda sekarang dapat menelusuri situs web yang terhubung dengan memilih tautan atau URLs masuk ke bilah alamat.

Mendistribusikan portal web Anda di Amazon WorkSpaces Secure Browser

Ketika Anda siap untuk pengguna Anda untuk mulai menggunakan Browser WorkSpaces Aman, Anda memilih dari opsi berikut untuk mendistribusikan portal:

- Tambahkan portal Anda ke gateway aplikasi SAMP Anda untuk memungkinkan pengguna meluncurkan sesi dari IDP mereka secara langsung. Anda dapat melakukan ini melalui alur masuk yang diprakarsai IDP dengan IDP yang sesuai dengan SAMP 2.0 Anda. Untuk informasi selengkapnya, lihat pernyataan SAMP yang diprakarsai SP dan yang diprakarsai IDP di. the

section called “Jenis otentikasi standar” Atau, Anda dapat membuat aplikasi SAMP kustom yang dapat memberikan pengalaman otentikasi yang diprakarsai IDP dengan menggunakan alur yang diprakarsai SP. Untuk informasi selengkapnya, lihat Membuat integrasi Aplikasi Bookmark.

- Tambahkan URL portal ke situs web yang Anda miliki, dan gunakan pengalihan browser untuk mengarahkan pengguna ke portal web.
- Email URL portal ke pengguna Anda, atau tekan ke perangkat yang Anda kelola sebagai halaman beranda browser atau bookmark.
- Gunakan domain khusus jika Anda telah menyiapkannya untuk portal Anda, bukan URL portal untuk pengalaman branding yang lebih terintegrasi bagi pengguna Anda. Lihat informasi yang lebih lengkap di the section called “Domain kustom”.

Mengelola portal web Anda di Amazon WorkSpaces Secure Browser

Setelah Anda mengatur portal web Anda, Anda dapat melakukan tindakan berikut untuk mengelolanya.

Topik

- Melihat detail portal web di Amazon WorkSpaces Secure Browser
- Mengedit portal web di Amazon WorkSpaces Secure Browser
- Menghapus portal web di Amazon WorkSpaces Secure Browser
- Mengelola kuota layanan untuk portal Anda di Amazon WorkSpaces Secure Browser
- Mengontrol interval untuk mengautentikasi ulang token IDP SAMP di Amazon Secure Browser WorkSpaces
- Menyiapkan pencatatan aktivitas pengguna di Amazon WorkSpaces Secure Browser
- Mengelola kebijakan browser di Amazon WorkSpaces Secure Browser
- Mengkonfigurasi Editor Metode Input untuk Amazon WorkSpaces Secure Browser
- Mengonfigurasi pelokalan dalam sesi untuk Amazon Secure Browser WorkSpaces
- Mengelola kontrol akses IP di Amazon WorkSpaces Secure Browser
- Mengelola ekstensi masuk tunggal di Amazon WorkSpaces Secure Browser
- Pemfilteran konten web di Amazon WorkSpaces Secure Browser
- Tautan dalam di Amazon WorkSpaces Secure Browser
- Menggunakan dasbor manajemen sesi di Amazon WorkSpaces Secure Browser
- Melindungi data dalam perjalanan dengan titik akhir FIPS dan Amazon WorkSpaces Secure Browser
- Mengelola pengaturan perlindungan data di Amazon WorkSpaces Secure Browser
- Kustomisasi branding di Amazon WorkSpaces Secure Browser
- Mengaktifkan dukungan WebAuthn pengalihan di Amazon WorkSpaces Secure Browser
- Mengelola kontrol toolbar di Amazon WorkSpaces Secure Browser
- Mengkonfigurasi domain khusus untuk portal Anda

Melihat detail portal web di Amazon WorkSpaces Secure Browser

Untuk melihat detail portal web, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Lihat detail.

Mengedit portal web di Amazon WorkSpaces Secure Browser

Untuk mengedit portal web, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Edit.

> **Note**
>
> Perubahan pada pengaturan jaringan atau pengaturan batas waktu segera mengakhiri sesi portal aktif apa pun. Pengguna terputus dan harus terhubung kembali untuk memulai sesi baru. Perubahan pada izin Clipboard, Izin transfer file, atau Cetak ke perangkat lokal berlaku dimulai dengan sesi baru pertama. Saat ini sesi aktif tidak terputus. Pengguna yang terhubung ke sesi aktif tidak terpengaruh oleh perubahan hingga mereka memutuskan sambungan dan terhubung ke sesi baru.

Menghapus portal web di Amazon WorkSpaces Secure Browser

Untuk menghapus portal web, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Hapus.

Mengelola kuota layanan untuk portal Anda di Amazon WorkSpaces Secure Browser

Saat Anda membuat Akun AWS, kami secara otomatis menetapkan kuota layanan default (juga disebut sebagai batas) untuk penggunaan sumber daya dengan Layanan AWS. Administrator harus mengetahui dua kuota yang mungkin perlu ditingkatkan untuk mendukung kasus penggunaannya. Kedua kuota ini adalah jumlah portal web yang dapat Anda buat di setiap wilayah, dan jumlah sesi bersamaan maksimum yang dapat Anda dukung dengan setiap jenis instans yang tersedia di setiap wilayah. Anda dapat meminta peningkatan untuk ini dari halaman Service Quotas di Konsol. AWS

Tabel berikut mencantumkan batas kuota layanan default.

Kuota default dalam akun Wilayah AWS menurut	Nilai
Portal web	3
Sesi bersamaan maksimum - standard.regular	25
Sesi bersamaan maksimum - standard.large	10
Sesi bersamaan maksimum - standard.xlarge	5

Untuk melihat kuota layanan yang dialokasikan ke akun Anda untuk setiap wilayah kapan saja, lihat halaman Service Quotas.

> **Important**
>
> Kuota layanan mempengaruhi satu Wilayah AWS per satu. Anda harus meminta peningkatan kuota layanan di setiap Wilayah AWS tempat Anda membutuhkan lebih banyak sumber daya. Untuk informasi selengkapnya, titik akhir dan kuota Amazon WorkSpaces Secure Browser.

Topik

- Meminta peningkatan kuota layanan di Amazon WorkSpaces Secure Browser
- Meminta peningkatan portal di Amazon WorkSpaces Secure Browser
- Meminta peningkatan sesi bersamaan maksimum di Amazon WorkSpaces Secure Browser

- Batasi contoh untuk Amazon WorkSpaces Secure Browser
- Kuota layanan lainnya di Amazon WorkSpaces Secure Browser

Meminta peningkatan kuota layanan di Amazon WorkSpaces Secure Browser

Untuk meminta peningkatan kuota layanan ikuti langkah-langkah berikut.

1. Buka dasbor AWS Support.
2. Pilih Peningkatan Batas Layanan.

> **Important**
>
> WorkSpaces Kuota layanan Browser Aman memengaruhi satu Wilayah pada satu waktu. Anda harus meminta peningkatan kuota layanan di setiap Wilayah AWS di mana Anda membutuhkan lebih banyak sumber daya. Untuk informasi selengkapnya, lihat titik akhir layanan AWS.

3. Di bawah Use case description, masukkan informasi berikut:
   - Jika Anda meminta peningkatan jumlah portal web, tentukan jenis sumber daya ini, dan sertakan ID Akun AWS Anda, wilayah tempat Anda ingin kenaikan, dan nilai batas baru.
   - Jika Anda meminta peningkatan untuk sesi bersamaan maksimum, tentukan jenis sumber daya ini, dan sertakan ID Akun AWS Anda, wilayah tempat Anda ingin kenaikan, ARN portal web, dan nilai batas baru.
4. (Opsional) Untuk meminta peningkatan kuota beberapa layanan secara bersamaan, lengkapi satu permintaan peningkatan kuota di bagian Permintaan, lalu pilih Tambahkan permintaan lain.

Meminta peningkatan portal di Amazon WorkSpaces Secure Browser

Portal adalah sumber daya dasar layanan. Setiap portal adalah asosiasi antara penyedia identitas SAMP 2.0 Anda dan koneksi jaringan Anda ke internet dan konten web pribadi apa pun. Setiap portal dapat memiliki kebijakan browser portal dan pengaturan pengguna yang terpisah, sehingga administrator biasanya akan membuat beberapa portal di wilayah yang sama untuk mengatasi kasus penggunaan yang berbeda. Misalnya, Anda dapat memberikan Grup A akses ke situs web tertentu dengan kebijakan terbatas (misalnya, Clipboard dan transfer File dinonaktifkan), dan Grup B dengan

akses ke internet umum tanpa pemfilteran URL. Anda dapat membuat portal di mana pun yang didukung Wilayah AWS. Untuk melihat ketersediaan layanan saat ini, lihat AWS Services by Region.

Meminta peningkatan kuota layanan

1. Buka halaman Service Quotas di wilayah yang Anda inginkan.
2. Pilih Jumlah Portal Web.
3. Pilih Minta kenaikan di tingkat akun.
4. Di bawah Tingkatkan nilai kuota, masukkan jumlah total kuota yang Anda inginkan.

Meminta peningkatan sesi bersamaan maksimum di Amazon WorkSpaces Secure Browser

Kuota sesi konkuren maksimum adalah jumlah pengguna tertinggi yang dapat dihubungkan secara bersamaan ke portal. Jika batas kuota layanan untuk sesi bersamaan maksimum tidak ditetapkan dengan tepat, pengguna mungkin menemukan bahwa sesi tidak tersedia saat mereka masuk. Selain meningkatkan kuota layanan ini, pelanggan juga harus memastikan bahwa VPC dan subnet mereka memiliki ruang IP yang cukup untuk mendukung sesi konkuren maksimum.

Untuk meminta peningkatan sesi bersamaan maksimum

1. Buka halaman Service Quotas di wilayah yang Anda inginkan.
2. Pilih Jumlah Sesi Serentak Maksimum per Portal untuk jenis instans yang ingin Anda tingkatkan.
3. Pilih Minta kenaikan di tingkat akun.
4. Di bawah Tingkatkan nilai kuota, masukkan jumlah total kuota yang Anda inginkan.

> **Note**
>
> Untuk peningkatan besar atau mendesak, buka halaman riwayat Service Quotas Anda, pilih tautan di kolom status permintaan Anda, tautkan ke kasus dukungan Anda, dan tambahkan balasan dengan detail tentang kasus penggunaan Anda and/or yang mendesak. Informasi ini membantu tim layanan memprioritaskan permintaan dan memastikan kapasitas yang cukup dialokasikan untuk akun Anda.

Batasi contoh untuk Amazon WorkSpaces Secure Browser

Sebagai contoh, asumsikan administrator mengkonfigurasi dua portal web di US East (Virginia N.) untuk 125 total pengguna. Sebelum membuat portal web, administrator mengidentifikasi portal web pertama (Portal A) akan mendukung 100 pengguna. Saat menguji alur kerja untuk pengguna ini, administrator menentukan bahwa mereka memerlukan jenis instans XL untuk mendukung streaming audio dan video selama sesi berlangsung. Portal web kedua (Portal B) harus tersedia hingga 25 pengguna untuk mendukung akses ke satu halaman web statis yang dihosting di VPC pelanggan. Saat menguji kasus penggunaan ini, administrator menentukan bahwa tipe instans standar dapat mendukung kasus penggunaan ini.

Untuk portal A, administrator harus mengirimkan permintaan peningkatan kuota layanan untuk menaikkan batas instans XL dari default wilayah (yaitu, 5) menjadi 100. Setelah terpenuhi, administrator dapat mengalokasikan kapasitas dengan mengedit portal web. Untuk portal B, administrator dapat bergerak maju tanpa meminta peningkatan kuota (yaitu, karena wilayah memiliki kuota default 25 untuk tipe instans standar).

Kuota layanan lainnya di Amazon WorkSpaces Secure Browser

Anda dapat melihat dan meminta kenaikan kuota lain yang tercantum di halaman Service Quotas. Dalam praktiknya, sebagian besar pelanggan akan merasa tidak perlu meminta kenaikan untuk batasan ini. Kuota ini secara luas dikelompokkan menjadi dua jenis: Number dan Rate.

Untuk kuota Nomor, ketika Anda mengirimkan peningkatan kuota layanan untuk Jumlah portal web, Anda akan secara otomatis menerima peningkatan jumlah sub-sumber daya yang diperlukan untuk membuat portal unik. Ini akan tercermin pada halaman Service Quotas. Misalnya, jika Anda meminta peningkatan portal dari 3 menjadi 5, Anda akan secara otomatis menerima peningkatan kuota layanan dari 3 menjadi 5 untuk pengaturan browser dan pengguna. Anda memiliki opsi untuk menggunakan kembali atau membuat sub-sumber daya baru sesuai keinginan.

Pada kesempatan langka, pelanggan mungkin menemukan kasus penggunaan untuk meningkatkan jumlah atau tingkat kuota sumber daya lainnya. Misalnya, administrator mungkin ingin meningkatkan jumlah pengaturan browser untuk menguji konfigurasi portal tambahan. Permintaan kuota layanan ini akan ditinjau dan dipenuhi secara case-by-case dasar.

Untuk kuota Harga, batas tarif yang terekspos dalam Service Quotas tidak perlu disesuaikan, terlepas dari batas portal akun.

Mengontrol interval untuk mengautentikasi ulang token IDP SAMP di Amazon Secure Browser WorkSpaces

Saat pengguna mengunjungi portal Browser WorkSpaces Aman, mereka dapat masuk untuk meluncurkan sesi streaming. Setiap sesi dimulai di halaman awal, kecuali mereka masuk kurang dari 5 menit yang lalu. Portal memeriksa token penyedia identitas (iDP) untuk menentukan apakah akan meminta kredensi pengguna saat meluncurkan sesi. Pengguna tanpa token iDP yang valid harus memasukkan nama pengguna, kata sandi, dan (otentikasi multifaktor opsional (MFA) untuk meluncurkan sesi streaming. Jika pengguna telah membuat token IDP SAMP dengan masuk ke iDP mereka atau aplikasi yang dilindungi oleh iDP yang sama, mereka tidak akan diminta untuk kredensialnya masuk.

Jika pengguna memiliki token IDP SAMP yang valid, mereka dapat WorkSpaces mengakses Browser Aman. Anda dapat mengontrol interval yang diperlukan untuk mengautentikasi ulang token IDP SAMP.

Untuk mengontrol interval untuk mengautentikasi ulang token IDP SAMP

1. Tetapkan durasi batas waktu iDP dengan penyedia IDP SAMP Anda. Kami menyarankan untuk mengonfigurasi durasi waktu tunggu IDP Anda dengan jumlah waktu terpendek yang diperlukan pengguna untuk menyelesaikan tugasnya.

   - Untuk informasi selengkapnya tentang Okta, lihat Menegakkan masa pakai sesi terbatas untuk semua kebijakan.
   - Untuk informasi selengkapnya tentang Azure AD, lihat Mengonfigurasi kontrol sesi autentikasi.
   - Untuk informasi selengkapnya tentang Ping, lihat Sesi.
   - Untuk informasi selengkapnya AWS IAM Identity Center, lihat Mengatur durasi sesi.
2. Tetapkan ketidakaktifan portal WorkSpaces Secure Browser dan nilai batas waktu idle Anda. Nilai-nilai ini mengontrol jumlah waktu antara interaksi terakhir pengguna dan ketika sesi Browser WorkSpaces Aman berakhir karena tidak aktif. Ketika sesi berakhir, pengguna akan kehilangan status sesi mereka (termasuk tab terbuka, konten web yang belum disimpan, dan riwayat), dan kembali ke keadaan baru pada awal sesi berikutnya. Untuk informasi selengkapnya, lihat langkah 5 di the section called “Pembuatan portal web”.

> **Note**
>
> Jika waktu sesi pengguna habis tetapi pengguna masih memiliki token SAMP iDP yang valid, mereka tidak perlu memasukkan nama pengguna dan kata sandi mereka untuk memulai sesi Browser Aman yang WorkSpaces baru. Untuk mengontrol bagaimana token diautentikasi ulang, ikuti panduan di langkah sebelumnya.

Menyiapkan pencatatan aktivitas pengguna di Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser menawarkan dua opsi untuk mencatat aktivitas pengguna dan peristiwa terkait keamanan:

- Session Logger menangkap berbagai acara sesi. Log ini dikirimkan ke bucket Amazon S3 di akun Anda, memungkinkan integrasi yang mudah dengan platform SIEM pilihan Anda.
- User Access Logging menangkap peristiwa sesi yang paling penting. Log ini dialirkan ke aliran Amazon Kinesis untuk pemrosesan dan analisis waktu nyata.

Kedua opsi logging dikonfigurasi di tingkat portal. Anda harus mengatur setiap opsi satu per satu untuk setiap portal tempat Anda ingin log aktif. Anda dapat mengaktifkan salah satu opsi atau keduanya, tergantung pada kebutuhan Anda untuk setiap portal.

Anda bertanggung jawab untuk mematuhi persyaratan apa pun yang berlaku untuk pencatatan atau pemantauan aktivitas pengguna saat menggunakan fitur ini, termasuk pencatatan atau pemantauan aktivitas karyawan.

Topik

- Menyiapkan Session Logger untuk Amazon WorkSpaces Secure Browser
- Menyiapkan pencatatan Akses Pengguna untuk Amazon WorkSpaces Secure Browser

Menyiapkan Session Logger untuk Amazon WorkSpaces Secure Browser

Warning

Mengaktifkan Session Logger menonaktifkan fitur Chrome berikut:

- Mode penyamaran
- Alat Pengembang
- Pengalihan Profil Chrome

Untuk mengaktifkan pencatat sesi untuk portal Browser WorkSpaces Aman, Anda harus terlebih dahulu mengidentifikasi bucket Amazon S3 tempat acara sesi akan dikumpulkan. Anda dapat menggunakan bucket yang sudah ada yang sudah menyimpan log serupa atau membuat yang baru khusus untuk tujuan ini.

Bucket Amazon S3 harus memiliki kebijakan bucket yang memberikan izin Browser WorkSpaces Aman untuk menulis log ke dalamnya. Sebaiknya tempatkan bucket Amazon S3 di wilayah yang sama Akun AWS dan sesuai dengan portal Browser WorkSpaces Aman Anda.

Tidak ada persyaratan penamaan untuk bucket Amazon S3. Untuk membuat bucket baru, ikuti langkah-langkah di bawah ini atau lihat Membuat bucket tujuan umum di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Untuk panduan cara mengonfigurasi izin, lihat Kebijakan Bucket untuk Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Di bawah ini adalah contoh kebijakan untuk bucket Amazon S3 Anda. Pastikan untuk memperbarui kebijakan dengan nama bucket Amazon S3 Anda. Perhatikan bahwa Principal adalah “workspaces-web.amazonaws.com”.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "AllowSessionLogger",
          "Effect": "Allow",
          "Principal": {
              "Service": "workspaces-web.amazonaws.com"
          },
          "Action": [
```

```
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

Mengaktifkan Session Logger di portal Browser WorkSpaces Aman Anda dapat mengakibatkan biaya dari Amazon S3. Untuk informasi, lihat Harga Amazon S3.

Untuk informasi selengkapnya tentang peristiwa terkait sesi yang ditangkap Session Logger, lihat. the section called “Acara sesi di Session Logger”

Bucket S3 dengan enkripsi KMS (opsional)

WorkSpaces Secure Browser Session Logger sepenuhnya mendukung bucket AWS KMS Amazon S3 dengan enkripsi diaktifkan. Untuk memastikan fungsionalitas pencatatan yang tepat dengan bucket Amazon S3 terenkripsi, Anda harus memberikan Session Logger izin yang diperlukan untuk menggunakan kunci Anda. AWS KMS

Tambahkan kebijakan berikut ke konfigurasi AWS KMS kunci Anda:

```
{
  "Sid": "Session Logger",
  "Effect": "Allow",
  "Principal": {
    "Service": "workspaces-web.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
},
```

Di AWS konsol, pilih portal Browser WorkSpaces Aman tempat Anda akan mengumpulkan acara, dan pilih tab Session logger dan Edit.

Masukkan informasi berikut untuk mengkonfigurasi Session Logger untuk portal:

- Lokasi S3 (wajib): Nama bucket Amazon S3 Anda tempat acara akan dikirimkan.
- Awalan Kunci (opsional): Folder tempat acara dikirimkan. Jika folder tidak ada, itu akan dibuat. Jika bidang dibiarkan kosong, Session Logger akan menulis peristiwa di root bucket Amazon S3.

Di bawah Advanced, Anda dapat mengonfigurasi bidang berikut:

- Filter acara: Ini adalah daftar acara yang dipantau oleh Session Logger.
  - Semua: Memilih opsi ini berarti semua peristiwa saat ini dan masa depan akan dipantau
  - Sertakan: Ini memungkinkan Anda memilih acara tertentu secara manual untuk dipantau. Hanya peristiwa yang dipilih secara eksplisit yang akan dicatat. Peristiwa baru yang diperkenalkan di pembaruan masa depan tidak akan dipantau, kecuali jika ditambahkan secara manual ke pilihan.
- Format berkas
  - JSON (default): Ini adalah format file di mana setiap file log disajikan sebagai array peristiwa. Kami merekomendasikan format ini untuk sebagian besar kasus penggunaan.
  - JSONLines: Ini adalah format file yang dioptimalkan untuk Amazon Athena.
- Struktur folder: Ini menentukan bagaimana file log disimpan.
  - Flat (default): Semua file log berada dalam satu folder.
  - Bersarang Berdasarkan tanggal: File log diatur ke dalam folder berdasarkan tanggal dan waktu. Dipartisi untuk Amazon Athena, dan dioptimalkan untuk kueri Amazon Athena.

Anda dapat menguji pengaturan Session Logger dan memastikan bahwa session logger berfungsi dengan benar. Setelah konfigurasi selesai, sistem mencoba menulis file pengujian yang diberi nama `_workspaces_secure_browser.tmp` ke bucket dan folder Amazon S3 yang ditentukan. Ini berfungsi sebagai validasi fungsionalitas logging dan pengaturan izin.

Anda juga dapat menjalankan sesi pengujian dengan memulai sesi Browser Aman di portal dan menggunakan browser seperti biasa. Session Logger menulis file log ke bucket Amazon S3 yang dikonfigurasi setiap 15 menit selama sesi aktif, atau saat sesi berakhir.

Setelah mengakhiri sesi atau menunggu interval logging berikutnya, periksa bucket Amazon S3 untuk mengonfirmasi bahwa file log untuk sesi Anda telah dibuat dan disimpan seperti yang diharapkan.

Menyiapkan pencatatan Akses Pengguna untuk Amazon WorkSpaces Secure Browser

Untuk mengaktifkan login akses pengguna di konsol Browser WorkSpaces Aman, di bawah Pencatatan akses pengguna, pilih ID Kinesis Stream yang ingin Anda gunakan untuk menerima data. Data yang direkam akan dikirimkan langsung ke stream tersebut.

Untuk informasi selengkapnya tentang cara membuat Aliran Data Amazon Kinesis, lihat Apa itu Amazon Kinesis Data Streams?

Untuk menerima log dari Browser WorkSpaces Aman, Anda harus memiliki Aliran Data Kinesis Amazon yang dimulai dengan "amazon-workspaces-web-*". Aliran data Amazon Kinesis Anda harus menonaktifkan enkripsi sisi server, atau harus digunakan untuk enkripsi sisi server. Kunci yang dikelola AWS

Untuk informasi selengkapnya tentang menyetel enkripsi sisi server di Amazon Kinesis, lihat Bagaimana Saya Memulai Enkripsi Sisi Server? .

Mengelola kebijakan browser di Amazon WorkSpaces Secure Browser

Anda dapat menyetel kebijakan browser khusus apa pun menggunakan kebijakan Chrome yang tersedia untuk versi stabil terbaru ke Browser WorkSpaces Aman. Saat Anda menetapkan kebijakan di portal Browser WorkSpaces Aman, kebijakan tersebut akan berlaku untuk semua sesi yang dikelola oleh portal web tersebut.

Ada lebih dari 300 kebijakan yang dapat Anda terapkan ke portal web. Untuk informasi selengkapnya, termasuk daftar lengkap kebijakan Chrome, lihat daftar kebijakan Chrome Enterprise.

Anda memiliki tiga cara untuk menetapkan kebijakan Chrome:

1. Menggunakan editor visual di portal web

   Dengan menggunakan tampilan konsol untuk membuat portal web, Anda dapat menerapkan beberapa kebijakan paling umum di editor visual:

   - `StartURL`
   - Mengaktifkan dan menonaktifkan penjelajahan pribadi
   - Penghapusan sejarah

- Bookmark dan folder bookmark

2. Menggunakan editor JSON di portal web

   Anda juga dapat langsung menambahkan atau mengedit kebijakan dengan menggunakan editor JSON alih-alih editor visual.

   Untuk format kebijakan tertentu, silakan lihat daftar kebijakan Chrome Enterprise.

3. Mengunggah file JSON ke portal web

   Anda juga dapat mengimpor kebijakan Chrome yang digunakan di organisasi Anda dengan mengunggah file JSON ke portal web.

   Untuk detailnya, silakan lihat the section called “Tutorial: Mengatur kebijakan browser khusus”

WorkSpaces Browser Aman menerapkan konfigurasi kebijakan browser dasar ke semua portal beserta kebijakan apa pun yang Anda tentukan. Anda dapat mengedit beberapa kebijakan ini dengan file JSON kustom Anda. Untuk informasi selengkapnya, lihat the section called “Mengedit kebijakan browser dasar”.

Topik

- Tutorial: Menyetel kebijakan browser khusus di Amazon WorkSpaces Secure Browser
- Mengedit kebijakan browser dasar di Amazon WorkSpaces Secure Browser

Tutorial: Menyetel kebijakan browser khusus di Amazon WorkSpaces Secure Browser

Anda dapat menyetel kebijakan Chrome apa pun yang didukung untuk Linux dengan mengunggah file JSON. Untuk mempelajari selengkapnya tentang kebijakan Chrome, lihat daftar kebijakan Chrome Enterprise dan pilih platform Linux. Kemudian, cari dan tinjau kebijakan untuk versi stabil terbaru.

Dalam tutorial berikut, Anda membuat portal web dengan kontrol kebijakan berikut:

- Siapkan bookmark
- Siapkan halaman startup default
- Mencegah pengguna menginstal ekstensi lain

- Mencegah pengguna menghapus riwayat
- Mencegah pengguna mengakses mode penyamaran
- Pra-instal ekstensi plug-in Okta untuk semua sesi.

Topik

- Langkah 1: Buat portal web
- Langkah 2: Kumpulkan kebijakan
- Langkah 3: Buat file kebijakan JSON kustom
- Langkah 4: Tambahkan kebijakan Anda ke template
- Langkah 5: Unggah file JSON kebijakan Anda ke portal web Anda

Langkah 1: Buat portal web

Untuk mengunggah file JSON kebijakan Chrome Anda, Anda harus membuat portal Browser WorkSpaces Aman. Untuk informasi selengkapnya, lihat the section called “Pembuatan portal web”.

Langkah 2: Kumpulkan kebijakan

Cari dan temukan kebijakan yang Anda inginkan dari Kebijakan Chrome. Anda kemudian menggunakan kebijakan untuk membuat file JSON di langkah berikutnya.

1. Buka daftar kebijakan Chrome Enterprise.
2. Pilih platform Linux, lalu pilih versi Chrome terbaru.
3. Cari kebijakan yang ingin Anda tetapkan. Untuk contoh ini, cari ekstensi untuk menemukan kebijakan untuk mengelolanya. Setiap kebijakan mencakup deskripsi, nama preferensi Linux, dan nilai sampel.
4. Dari hasil pencarian, ada 3 kebijakan yang memenuhi persyaratan bisnis jika digunakan bersama:
   - ExtensionSettings— Menginstal ekstensi di awal browser.
   - ExtensionInstallBlocklist— Mencegah ekstensi tertentu agar tidak diinstal.
   - ExtensionInstallAllowlist— Memungkinkan ekstensi tertentu untuk diinstal.
5. Kebijakan tambahan memenuhi persyaratan yang tersisa;
   - ManagedBookmarks— Menambahkan bookmark ke halaman web.
   - RestoreOnStartupURLs— Mengkonfigurasi halaman web mana yang dibuka setiap kali jendela browser baru diluncurkan.

- AllowDeletingBrowserHistory— Mengkonfigurasi apakah pengguna dapat menghapus riwayat penjelajahan mereka.
- IncognitoModeAvailability— Mengkonfigurasi apakah pengguna dapat mengakses mode penyamaran.

Langkah 3: Buat file kebijakan JSON kustom

Buat file JSON menggunakan editor teks, templat, dan kebijakan yang Anda temukan di langkah sebelumnya.

1. Buka editor teks.
2. Salin dan tempel template berikut ke editor teks Anda:

```
{
  "chromePolicies":
    {
        "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Bookmark 1",
                    "url": "bookmark-url-1"
                },
                {
                    "name": "Bookmark 2",
                    "url": "bookmark-url-2"
                },
            ]
        },
        "RestoreOnStartup":
        {
            "value": 4
        },
        "RestoreOnStartupURLs":
        {
            "value":
            [
                "startup-url"
            ]
```

```
        },
        "ExtensionInstallBlocklist": {
            "value": [
                "insert-extensions-value-to-block",
            ]
        },
        "ExtensionInstallAllowlist": {
            "value": [
                "insert-extensions-value-to-allow",
            ]
        },
        "ExtensionSettings":
        {
            "value":
            {
                "insert-extension-value-to-force-install":
                {
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
                },
            }
        },
        "AllowDeletingBrowserHistory":
        {
            "value": should-allow-history-deletion
        },
        "IncognitoModeAvailability":
        {
            "value": incognito-mode-availability
        }
    }
}
```

Langkah 4: Tambahkan kebijakan Anda ke template

Tambahkan kebijakan kustom Anda ke template untuk setiap kebutuhan bisnis.

1. Siapkan bookmark URLs.

a. Di bawah `value` tombol, tambahkan pasangan `name` dan `url` kunci untuk setiap bookmark yang ingin Anda tambahkan.

b. Atur `bookmark-url-1` ke `https://www.amazon.com`.

c. Atur `bookmark-url-2` ke `https://docs.aws.amazon.com/workspaces-web/latest/adminguide/`.

```
    "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Amazon",
                    "url": "https//www.amazon.com"
                },
                {
                    "name": "Bookmark 2",
                    "url": "https://docs.aws.amazon.com/workspaces-web/latest/
adminguide/"
                },
            ]
        },
```

2. Siapkan startup URLs. Kebijakan ini memungkinkan administrator untuk menyetel halaman web yang ditampilkan saat pengguna meluncurkan jendela browser baru.

a. Atur `RestoreOnStartup` ke `4` . Ini menetapkan `RestoreOnStartup` tindakan untuk membuka daftar URLs . Anda juga dapat menggunakan tindakan lain pada startup Anda URLs. Untuk informasi selengkapnya, lihat daftar kebijakan Chrome Enterprise.

b. Setel `RestoreOnStartupURLs` ke https://www.aboutamazon.com /news.

```
     "RestoreOnStartup":
        {
            "value": 4
        },
    "RestoreOnStartupURLs":
        {
            "value":
            [
```

```
            "https://www.aboutamazon.com/news"
        ]
    },
```

3. Untuk mencegah pengguna menghapus riwayat browser mereka, atur `AllowDeletingBrowserHistory` kefalse.

```
"AllowDeletingBrowserHistory":
   {
       "value": false
   },
```

4. Untuk menonaktifkan akses ke akses mode Penyamaran bagi pengguna Anda, setel `IncognitoModeAvailability` ke. 1

```
"IncognitoModeAvailability":
   {
       "value": 1
   }
```

5. Tetapkan dan terapkan plug-in Okta dengan kebijakan berikut:

   - `ExtensionSettings`— Menginstal ekstensi di awal browser. Nilai ekstensi tersedia dari halaman bantuan plug-in Okta.
   - `ExtensionInstallBlocklist`— Mencegah ekstensi tertentu agar tidak diinstal. Gunakan * nilai untuk mencegah semua ekstensi secara default. Administrator dapat mengontrol ekstensi mana yang akan diizinkan pada file. `ExtensionInstallAllowlist`
   - `ExtensionInstallAllowlist`memungkinkan Anda untuk menginstal ekstensi tertentu. Karena `ExtensionInstallBlocklist` diatur ke*, tambahkan nilai plug-in Okta di sini untuk mengizinkannya.

   Berikut ini menunjukkan contoh kebijakan untuk mengaktifkan plug-in Okta:

```
"ExtensionInstallBlocklist": {
    "value": [
```

```
                "*",
                ]
        },
        "ExtensionInstallAllowlist": {
            "value": [
                "glnpjglilkicbckjpbgcfkogebgllemb",
               ]
        },
        "ExtensionSettings": {
            "value": {
                "glnpjglilkicbckjpbgcfkogebgllemb": {
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
            }
        }
```

Langkah 5: Unggah file JSON kebijakan Anda ke portal web Anda

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, lalu pilih Portal Web.
3. Pilih portal web Anda, lalu pilih Edit.
4. Pilih Pengaturan kebijakan, lalu pilih Unggah file JSON.
5. Pilih Pilih File. Arahkan ke, pilih, dan unggah file JSON Anda.
6. Pilih Simpan.

Mengedit kebijakan browser dasar di Amazon WorkSpaces Secure Browser

Untuk memberikan layanan, WorkSpaces Secure Browser menerapkan kebijakan browser dasar ke semua portal. Kebijakan dasar ini diterapkan selain kebijakan yang Anda tentukan dari tampilan konsol atau unggahan JSON. Berikut ini adalah daftar kebijakan yang diterapkan oleh layanan dalam format JSON:

```
{
    "chromePolicies":
```

```
    {
        "DefaultDownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadRestrictions": {
            "value": 1
        },
        "URLBlocklist": {
            "value": [
                "file://",
                "http://169.254.169.254",
                "http://[fd00:ec2::254]",
            ]
        },
        "URLAllowlist": {
            "value": [
                "file:///home/as2-streaming-user/MyFiles/TemporaryFiles",
                "file:///opt/appstream/tmp/TemporaryFiles",
            ]
        }
    }
}
```

Pelanggan tidak dapat melakukan perubahan pada kebijakan berikut:

- `DefaultDownloadDirectory`Kebijakan ini tidak dapat diedit. Layanan menimpa setiap perubahan pada kebijakan ini.
- `DownloadDirectory`Kebijakan ini tidak dapat diedit. Layanan menimpa setiap perubahan pada kebijakan ini.

Dasar `URLAllowlist` dan `URLBlocklist` kebijakan tidak dapat ditimpa. Perhatikan bahwa file kebijakan browser JSON yang terkait dengan portal web Anda tidak akan berisi kebijakan dasar ini. Untuk melihat daftar lengkap semua kebijakan yang diterapkan dan nilainya, navigasikan ke “chrome: //policy” dari dalam sesi penjelajahan jarak jauh.

Pelanggan dapat memperbarui kebijakan berikut untuk portal web mereka:

- `DownloadRestrictions`— Default diatur `1` untuk mencegah unduhan yang diidentifikasi sebagai berbahaya oleh Penjelajahan Aman Chrome. Untuk informasi selengkapnya, lihat Mencegah pengguna mengunduh file berbahaya. Anda dapat mengatur nilai dari `0` ke`4`.

Mengkonfigurasi Editor Metode Input untuk Amazon WorkSpaces Secure Browser

Input Method Editor (IME) adalah utilitas yang menyediakan opsi kepada pengguna akhir untuk memasukkan teks dalam bahasa yang menggunakan tata letak keyboard selain keyboard QWERTY. IMEs membantu pengguna memasukkan teks dalam bahasa dengan set bahasa yang lebih besar dan lebih kompleks, seperti Jepang, Mandarin, dan Korea. WorkSpaces Sesi Browser Aman menyertakan dukungan IME secara default. Pengguna dapat memilih bahasa alternatif dari toolbar IME dalam sesi atau dengan menggunakan pintasan keyboard.

Bahasa berikut saat ini didukung oleh IME Browser WorkSpaces Aman:

- Bahasa Inggris
- Bahasa Mandarin Sederhana (Pinyin)
- Tionghoa Tradisional (Bopomofo)
- Bahasa Jepang
- Bahasa Korea

Untuk memilih bahasa dari toolbar IME, lakukan hal berikut:

1. Pilih drop-down pemilih bahasa yang terletak di sisi kanan bilah panel atas hitam. Secara default, pemilih akan menampilkan en, untuk bahasa Inggris.
2. Di menu tarik-turun, pilih bahasa yang diinginkan.
3. Di submenu yang muncul setelah memilih bahasa, pilih detail bahasa tambahan.

Untuk memilih bahasa menggunakan pintasan keyboard, gunakan yang berikut ini:

- Semua Bahasa
  - Untuk memajukan IME (atau pindah ke tata letak keyboard kanan), tekanShift+Control+Left Alt.
  - Untuk mengakses pengaturan bahasa dan input, gunakan pemilih bahasa di bilah panel atas. Jika tidak terlihat, aktifkan melalui Toolbar → Preferensi → Umum → Metode input keyboard.

- Bahasa Jepang
  - Untuk pengguna macOS: Jika Anda menggunakan sumber input AS, Anda mungkin mengalami masalah input. Untuk mengatasi ini:
    1. Pilih sumber input Jepang (misalnya, Jepang - Kana atau Jepang - Romaji) alih-alih sumber input AS di macOS Anda.
    2. Dalam sesi Browser WorkSpaces Aman, buka Toolbar → Preferences → Keyboard → Pengaturan tombol Option dan pilih Use Option () sebagai tombol Alt jarak jauh (Mac) untuk memastikan pintasan keyboard berfungsi dengan baik.
  - Mengonversi karakter masukan
    - Untuk mengonversi karakter ke Hiragana, tekan. F6
    - Untuk mengonversi karakter ke Katakana, tekan. F7
    - Untuk mengonversi karakter ke Hankaku Katakana (Katakana setengah lebar), tekan F8
    - Untuk mengonversi karakter ke bahasa Latin, tekanF10.
    - Untuk mengonversi karakter ke Wide Latin, tekanF9.
  - Mengalihkan mode input
    - Untuk beralih dari Hiragana ke Katakana, tekan. Alt/Option+K
    - Untuk beralih dari Katakana ke Hankaku Katakana, tekan. Alt/Option+K
    - Untuk beralih dari Hankaku Katakana (Katakana setengah lebar) kembali ke Hiragana, tekan. Alt/Option+K
    - Untuk beralih dari mode Jepang atau Wide Latin ke Latin, tekanAlt/Option+L.
    - Untuk beralih dari Latin ke Wide Latin, tekanAlt/Option+L.
    - Untuk beralih dari mode apa pun ke Input Langsung, tekanHenkaku/Zenkaku key.
    - Untuk beralih dari Input Langsung kembali ke Hiragana, tekan. Henkaku/Zenkaku key
- Bahasa Korea
  - Untuk memilih Hangul, tekanShift+Space.
  - Untuk memilih Hanja, tekanF9.

Untuk mematikan keyboard di layar dari sesi Browser WorkSpaces Aman Anda, hubungi Dukungan.

Mengonfigurasi pelokalan dalam sesi untuk Amazon Secure Browser WorkSpaces

Ketika pengguna memulai sesi, WorkSpaces Secure Browser mendeteksi bahasa browser lokal pengguna dan pengaturan zona waktu dan menerapkannya ke sesi. Ini memengaruhi bahasa tampilan selama sesi, dan membantu memastikan bahwa waktu yang ditampilkan cocok dengan waktu saat ini di lokasi pengguna.

Bahasa sesi ditentukan dalam urutan prioritas berikut:

1. ForcedLanguagesKebijakan dalam pengaturan browser portal web. Untuk informasi selengkapnya, lihat ForcedLanguages.
2. Pengaturan bahasa browser lokal pengguna akhir.
3. Nilai default, Bahasa Inggris (en-US).

Zona waktu ditentukan oleh pengaturan zona waktu lokal yang ditentukan di browser pengguna akhir. Jika pengaturan zona waktu tidak valid, UTC digunakan.

Komponen berikut di WorkSpaces Secure Browser mendukung lokalisasi:

- WorkSpaces Halaman masuk Browser Aman
- WorkSpaces Pesan status portal Browser Aman (termasuk memuat pesan dan kesalahan)
- Browser Chrome
- Menu Konteks Sistem dan Simpan sebagai jendela

Topik

- Kode bahasa yang didukung untuk Amazon WorkSpaces Secure Browser
- Memilih bahasa di pengaturan browser pengguna

Kode bahasa yang didukung untuk Amazon WorkSpaces Secure Browser

Daftar berikut menunjukkan kode bahasa yang saat ini didukung oleh WorkSpaces Secure Browser. Jika browser lokal pengguna diatur untuk menggunakan kode bahasa yang tidak didukung, sesi default ke bahasa Inggris (en-US).

- Bahasa Jerman

  - de — Jerman
  - De-at — Jerman (Austria)
  - De-de — Jerman (Jerman)
  - De-ch — Jerman (Swiss)
  - De-li — Jerman (Liechtenstein)
- Bahasa Inggris
  - en — Bahasa Inggris
  - En-au — Inggris (Australia)
  - En-CA — Inggris (Kanada)
  - En-in — Inggris (India)
  - en-NZ — Inggris (Selandia Baru)
  - En-za — Inggris (Afrika Selatan)
  - en-GB - Inggris (Britania Raya)
  - en-US — Inggris (Amerika Serikat)
- Bahasa Spanyol
  - es — Spanyol
  - Es-AR — Spanyol (Argentina)
  - Es-Cl - Spanyol (Cile)
  - Es-co — Spanyol (Kolombia)
  - es-CR - Spanyol (Kosta Rika)
  - Es-hn — Spanyol (Honduras)
  - es-419 — Spanyol (Amerika Latin)
  - es-MX — Spanyol (Meksiko)
  - es-PE - Spanyol (Peru)
  - ES-es — Spanyol (Spanyol)
  - es-US - Spanyol (Amerika Serikat)
  - es-UY - Spanyol (Uruguay)
  - Es-ve - Spanyol (Venezuela)
- Prancis
  - fr — Prancis

  - fr-Ca — Prancis (Kanada)
  - FR-fr - Prancis (Prancis)
  - FR-ch — Prancis (Swiss)
- orang Indonesia
  - id — Indonesia
  - ID-ID — Bahasa Indonesia (Indonesia)
- Bahasa Italia
  - itu — Italia
  - IT-it - Italia (Italia)
  - IT-ch — Italia (Swiss)
- Bahasa Jepang
  - ja — Jepang
  - Ja-jp - Jepang (Jepang)
- Bahasa Korea
  - ko — Korea
  - Ko-kr — Korea (Korea)
- Bahasa Portugis
  - pt — Portugis
  - Pt-BR - Portugis (Brasil)
  - Pt-PT — Portugis (Portugal)
- Mandarin
  - zh — Bahasa Mandarin
  - Zh-CN - Mandarin (Tiongkok)
  - Zh-HK - Tionghoa (Hong Kong)
  - Zh-TW - Bahasa Mandarin (Taiwan)

Memilih bahasa di pengaturan browser pengguna

Untuk mengatur pengaturan browser lokal pengguna, ikuti langkah-langkah yang sesuai.

- Di Chrome, pilih Pengaturan, pilih Bahasa, lalu urutkan bahasa berdasarkan preferensi.

- Di Firefox, pilih Pengaturan, Umum, Bahasa, dan pilih bahasa dari menu tarik-turun.
- Di Edge, pilih Pengaturan, pilih Bahasa, lalu urutkan bahasa berdasarkan preferensi.

Mengelola kontrol akses IP di Amazon WorkSpaces Secure Browser

Important

Kontrol akses IP hanya mendukung IPv4. Pengguna yang terhubung dari jaringan IPv6 -only akan diblokir.

WorkSpaces Secure Browser memungkinkan Anda mengontrol alamat IP mana portal web Anda dapat diakses. Dengan menggunakan pengaturan akses IP, Anda dapat menentukan dan mengelola grup alamat IP tepercaya, dan hanya mengizinkan pengguna untuk mengakses portal mereka ketika mereka terhubung ke jaringan tepercaya.

Secara default, WorkSpaces Secure Browser memungkinkan pengguna untuk mengakses portal web mereka dari mana saja. Grup kontrol akses IP bertindak sebagai firewall virtual yang memfilter alamat IP mana yang dapat digunakan pengguna untuk terhubung ke portal web. Saat dikaitkan dengan portal web Anda, pengaturan akses IP akan mendeteksi IP pengguna sebelum autentikasi untuk menentukan apakah mereka memenuhi syarat untuk terhubung. Setelah terhubung, WorkSpaces Secure Browser terus memantau alamat IP pengguna untuk memastikan mereka tetap terhubung dari jaringan tepercaya. Jika IP pengguna berubah, WorkSpaces Secure Browser akan mendeteksi dan mengakhiri sesi.

Untuk menentukan rentang alamat CIDR, tambahkan aturan ke grup kontrol akses IP Anda, lalu kaitkan grup ini dengan portal web Anda. Anda dapat mengaitkan setiap pengaturan akses IP dengan satu atau beberapa portal web. Untuk menentukan alamat IP publik dan rentang alamat IP untuk jaringan terpercaya Anda, tambahkan aturan ke grup kontrol akses IP. Jika pengguna Anda mengakses portal web mereka melalui gateway NAT atau VPN, Anda harus membuat aturan yang memungkinkan lalu lintas dari alamat IP publik untuk gateway NAT atau VPN.

Note

Pelanggan bertanggung jawab untuk memahami potensi masalah hukum yang timbul dengan penggunaan Browser WorkSpaces Aman mereka, dan harus memastikan bahwa

penggunaan Browser WorkSpaces Aman mematuhi semua hukum dan peraturan yang berlaku. Ini termasuk undang-undang yang mengatur kemampuan pemberi kerja untuk memantau penggunaan Browser WorkSpaces Aman oleh karyawan, termasuk aktivitas yang dilakukan dalam aplikasi.

Topik

- Membuat grup kontrol akses IP di Amazon WorkSpaces Secure Browser
- Mengaitkan pengaturan akses IP dengan portal web di Amazon WorkSpaces Secure Browser
- Mengedit grup kontrol akses IP di Amazon WorkSpaces Secure Browser
- Menghapus grup kontrol akses IP di Amazon WorkSpaces Secure Browser

Membuat grup kontrol akses IP di Amazon WorkSpaces Secure Browser

Important

Kontrol akses IP hanya mendukung IPv4. Pengguna yang terhubung dari jaringan IPv6 -only akan diblokir.

Untuk membuat grup kontrol akses IP, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Di panel navigasi, pilih kontrol akses IP.
3. Pilih Buat grup kontrol akses IP.
4. Dalam kotak dialog Buat grup kontrol akses IP, masukkan nama (wajib) dan deskripsi (opsional) untuk grup.
5. Masukkan alamat IP atau rentang IP CIDR yang akan dikaitkan dengan Sumber, dan Deskripsi (opsional).
6. Di bawah Tag, pilih apakah akan menandai pasangan nilai kunci untuk setiap grup kontrol akses IP.
7. Setelah selesai menambahkan aturan dan tag, pilih Simpan.

Mengaitkan pengaturan akses IP dengan portal web di Amazon WorkSpaces Secure Browser

> **Important**
>
> Kontrol akses IP hanya mendukung IPv4. Pengguna yang terhubung dari jaringan IPv6 -only akan diblokir.

Untuk mengaitkan grup kontrol akses IP dengan portal web yang ada, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Di panel navigasi, pilih Portal Web.
3. Pilih portal web, dan pilih Edit.
4. Di bawah grup kontrol akses IP, dan pilih grup kontrol akses IP untuk portal web.
5. Pilih Simpan.

Untuk mengaitkan grup kontrol akses IP saat membuat portal web baru, ikuti langkah-langkah ini.

1. Selesaikan langkah 1 hingga 4 the section called “Pengaturan portal” untuk mengakses Kontrol Akses IP (opsional).
2. Pilih Buat kontrol akses IP.
3. Dalam Buat Grup IP kotak dialog, masukkan nama (wajib) dan deskripsi (opsional) untuk grup.
4. Masukkan alamat IP atau rentang IP CIDR yang akan dikaitkan dengan Sumber, dan Deskripsi (opsional).
5. Di bawah Tag, pilih apakah akan menandai pasangan nilai kunci untuk setiap grup kontrol akses IP.
6. Setelah selesai menambahkan aturan dan tag, pilih Buat kontrol akses IP.
7. Grup kontrol akses IP Anda akan dikaitkan dengan portal web ini saat diluncurkan.

Mengedit grup kontrol akses IP di Amazon WorkSpaces Secure Browser

Anda dapat menghapus aturan dari pengaturan akses IP kapan saja. Jika Anda menghapus aturan yang digunakan untuk mengizinkan koneksi ke portal web, setiap pengguna dengan sesi saat ini akan terputus dari portal web.

Untuk mengedit grup kontrol akses IP, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Di panel navigasi, pilih kontrol akses IP.
3. Pilih grup target Anda dan pilih Edit.
4. Edit aturan yang ada Sumber dan Deskripsi (opsional), atau tambahkan aturan tambahan.
5. Di bawah Tag, pilih apakah akan menandai pasangan nilai kunci untuk setiap grup kontrol akses IP.
6. Setelah selesai menambahkan aturan dan tag, pilih Simpan.
7. Jika Anda memperbarui setelan akses IP yang ada, tunggu hingga 15 menit agar aturan baru atau yang telah diedit berlaku.

Menghapus grup kontrol akses IP di Amazon WorkSpaces Secure Browser

Anda dapat menghapus aturan dari grup kontrol akses IP kapan saja. Jika Anda menghapus aturan yang digunakan untuk mengizinkan koneksi ke portal web, setiap pengguna dengan sesi saat ini akan terputus dari portal web.

Untuk menghapus grup kontrol akses IP, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Di panel navigasi, pilih grup kontrol akses IP.
3. Pilih grup dan pilih Hapus.

Mengelola ekstensi masuk tunggal di Amazon WorkSpaces Secure Browser

Anda dapat mengaktifkan ekstensi agar pengguna akhir Anda memiliki pengalaman masuk portal yang lebih baik. Misalnya, jika Anda menggunakan Okta sebagai penyedia identitas SAMP 2.0 portal Anda (IDP), dan Anda juga menggunakannya sebagai idP untuk situs web yang ingin dikunjungi pengguna selama sesi, Anda dapat meneruskan cookie masuk Okta ke sesi dengan ekstensi. Setelah itu, ketika pengguna mengunjungi situs web yang memerlukan cookie domain Okta, mereka dapat mengakses situs web tanpa harus masuk selama sesi berlangsung.

Ekstensi ini didukung di browser Chrome dan Firefox. Ekstensi ini memungkinkan sinkronisasi cookie untuk domain yang diizinkan dari pengguna yang masuk ke sesi. Ekstensi tidak mengharuskan pengguna untuk masuk, dan berfungsi di belakang layar untuk mengaktifkan sinkronisasi cookie tanpa mengharuskan pengguna untuk mengambil tindakan apa pun setelah instalasi. Tidak ada data yang disimpan oleh ekstensi.

Secara default, ekstensi tidak diaktifkan di Chrome di jendela Penyamaran atau jendela Penjelajahan Pribadi Firefox. Pengguna dapat mengaktifkannya secara manual. Untuk informasi selengkapnya tentang Chrome, lihat Ekstensi dalam mode Penyamaran. Untuk informasi selengkapnya tentang Firefox, lihat Ekstensi di Penjelajahan Pribadi.

Pengguna diminta untuk menginstal ekstensi ketika mereka masuk ke portal. Untuk detail tentang pengalaman pengguna dengan ekstensi, lihatthe section called “Ekstensi masuk tunggal”.

Topik

- Mengidentifikasi domain untuk ekstensi masuk tunggal di Amazon Secure Browser WorkSpaces
- Menambahkan ekstensi masuk tunggal ke portal web baru di Amazon WorkSpaces Secure Browser
- Menambahkan ekstensi masuk tunggal ke portal web yang ada di Amazon WorkSpaces Secure Browser
- Mengedit atau menghapus ekstensi masuk tunggal di Amazon WorkSpaces Secure Browser

Mengidentifikasi domain untuk ekstensi masuk tunggal di Amazon Secure Browser WorkSpaces

Pertama, tentukan domain mana yang Anda butuhkan untuk IDP dan situs web SAMP Anda. Anda dapat menambahkan hingga 10 domain.

Anda bertanggung jawab untuk menguji dan mengidentifikasi domain yang sesuai untuk cookie yang akan disinkronkan. Perubahan mungkin diperlukan di iDP atau tingkat otentikasi situs web untuk memastikan sistem masuk tunggal berfungsi seperti yang diharapkan.

Untuk melihat domain mana yang akan digunakan dengan iDP yang paling umum, lihat tabel berikut:

IDP dan domain

IdP	Domain
Okta	okta.com
ID Entra	microsoftonline.com
Pusat Identitas AWS	awsapps.com
Satu Login	onelogin.com
duet	duosecurity.com

Menambahkan ekstensi masuk tunggal ke portal web baru di Amazon WorkSpaces Secure Browser

Untuk mengizinkan ekstensi saat membuat portal web baru, ikuti langkah-langkah ini.

1. Ikuti langkah-langkahnya the section called “Pembuatan portal web” sampai Anda tibathe section called “Pengaturan pengguna”.
2. Untuk langkah 1the section called “Pengaturan pengguna”, di bawah Izin pengguna, pilih Diizinkan untuk mengaktifkan ekstensi untuk portal web Anda.
3. Masukkan domain untuk sinkronisasi cookie, dan pilih Tambahkan domain baru.
4. Selesaikan langkah-langkah di the section called “Pengaturan pengguna” dan bagian yang tersisa the section called “Pembuatan portal web” untuk membuat portal web Anda.

Menambahkan ekstensi masuk tunggal ke portal web yang ada di Amazon WorkSpaces Secure Browser

Untuk menambahkan ekstensi ke portal web yang ada, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman di https://console.aws.amazon.com/workspaces-web/rumah.
2. Pilih portal web yang akan diedit.
3. Pilih Pengaturan pengguna, Izin pengguna, dan Diizinkan untuk mengaktifkan ekstensi untuk portal web Anda.
4. Masukkan domain untuk sinkronisasi cookie, pilih Tambahkan domain baru.
5. Simpan perubahan portal Anda. Portal akan meminta pengguna untuk menginstal ekstensi dalam waktu 15 menit.

Mengedit atau menghapus ekstensi masuk tunggal di Amazon WorkSpaces Secure Browser

Untuk mengedit domain atau menghapus ekstensi, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman di https://console.aws.amazon.com/workspaces-web/rumah.
2. Pilih portal web yang akan diedit.
3. Pilih Pengaturan pengguna, Izin pengguna, dan Tidak diizinkan untuk menghapus ekstensi untuk portal web Anda.
4. Hapus atau edit domain individual.
5. Setelah dihapus, sesi tidak akan lagi menyinkronkan cookie, bahkan jika pengguna memiliki ekstensi Browser WorkSpaces Aman yang diinstal di browser mereka.

Pemfilteran konten web di Amazon WorkSpaces Secure Browser

Penyaringan Konten Web adalah fitur keamanan dan kepatuhan yang memungkinkan organisasi Anda menentukan kebijakan dan mengatur akses konten dalam Browser WorkSpaces Aman. Dengan Pemfilteran Konten Web, Anda dapat menentukan pengguna URLs akhir mana yang

diizinkan mengakses atau memblokir kategori tertentu URLs atau domain untuk membatasi akses, menangani persyaratan keamanan dan kepatuhan terhadap peraturan yang penting.

> **Note**
>
> Meskipun Anda dapat menyiapkan kebijakan pemfilteran URL melalui kebijakan Chrome untuk memblokir atau mengizinkan domain tertentu, kami tidak menyarankan pendekatan ini karena tindakan dari kebijakan Chrome tidak akan diambil sebagai bagian dari kemampuan pencatatan layanan. Untuk pemantauan komprehensif dan pelaporan kepatuhan, gunakan kebijakan Pemfilteran Konten Web yang dijelaskan di halaman ini.

Topik

- Membatasi penelusuran ke spesifik URLs
- Memblokir spesifik URLs
- Kategori pemblokiran
- Contoh dari URLs
- Mentransfer kebijakan Chrome

Membatasi penelusuran ke spesifik URLs

Anda dapat menerapkan kebijakan “penolakan default” di mana hanya situs web yang disetujui secara eksplisit dan dapat URLs diakses. Ini ideal untuk lingkungan dengan keamanan tinggi di mana akses internet harus dikontrol dengan ketat dan setiap situs yang diizinkan telah diperiksa untuk kebutuhan bisnis dan kepatuhan keamanan.

Di AWS konsol, di bawah pemfilteran URL:

- Arahkan ke daftar Blokir dan pilih sakelar Blokir semua URLs
- Di bawah daftar Izinkan, klik Tambahkan URL untuk menambahkan URL yang akan diizinkan terdaftar untuk pengguna akhir Anda. Tambahkan satu entri per URL.
- Klik Simpan

Memblokir spesifik URLs

Anda dapat menyeimbangkan keamanan dengan produktivitas dengan mempertahankan akses internet terbuka sambil memblokir situs bermasalah yang diketahui. Ini cocok untuk organisasi yang mempercayai penggunanya tetapi ingin mencegah akses ke ancaman tertentu atau konten yang tidak pantas tanpa terlalu membatasi aktivitas bisnis yang sah.

Di AWS konsol Anda, di bawah Pemfilteran URL:

- Arahkan ke Diblokir URLs
- Pilih Tambahkan URL, dan masukkan URL yang akan diblokir. Tambahkan satu entri per URL yang ingin Anda blokir
- Klik Simpan

Kategori pemblokiran

Selain memblokir spesifik URLs, Anda juga dapat secara otomatis memblokir grup URLs berdasarkan kategori konten. Ini berguna untuk organisasi yang membutuhkan cakupan komprehensif terhadap berbagai jenis konten yang tidak pantas atau berisiko tanpa harus mengidentifikasi dan memblokir situs individual secara manual.

Di AWS konsol Anda, di bawah Pemfilteran URL:

- Arahkan ke kategori yang diblokir dan klik Tambahkan kategori
- Pilih kategori yang ingin Anda blokir
- Anda dapat pengecualian untuk kategori ini dengan menambahkan URLs ke Daftar Izinkan. Untuk ini klik Tambahkan URL dan masukkan entry/ies yang ingin URLs Anda izinkan. Bahkan jika mereka termasuk dalam kategori, pengguna akhir akan dapat mengunjungi URLs.
- Klik Simpan

Kategori berikut dapat dipilih. Anda dapat memilih satu, banyak, atau semua kategori.

Kategori penyaringan yang tersedia

Tema	Kategori	Deskripsi
Konten Dewasa & Tidak Pantas	Ketelanjangan	Situs yang berisi gambar telanjang non-seksual atau karya seni.
Konten Dewasa & Tidak Pantas	Pornografi	Situs dengan konten seksual eksplisit atau materi telanjang provokatif.
Konten Dewasa & Tidak Pantas	Pendidikan Seks	Sumber daya kesehatan dan seksualitas yang sesuai dengan usia, ditinjau secara medis.
Konten Dewasa & Tidak Pantas	hambar	Konten yang tidak pantas untuk anak-anak yang tidak tercakup dalam kategori lain.
Komunikasi dan Sosial	Obrolan	Grup waktu nyata dan platform pesan pribadi.
Komunikasi dan Sosial	Pesan Instan	Layanan pesan pribadi.
Komunikasi dan Sosial	Jaringan Profesional	Platform membangun hubungan yang berfokus pada bisnis.
Komunikasi dan Sosial	Jejaring Sosial	Platform interaksi pengguna untuk berbagi konten dan pengalaman pribadi.
Komunikasi dan Sosial	Email Berbasis Web	Layanan pesan yang dapat diakses browser, termasuk e-card dan sistem ucapan.
Hiburan	Permainan	Sumber daya permainan rekreasi, termasuk video game, teka-teki, dan aktivitas non-perjudian.
Hiburan	Berbagi Gambar	Platform konten visual yang menawarkan kemampuan hosting, pencarian, dan berbagi.
Hiburan	Peer To Peer	Penyedia aplikasi berbagi file dan alat perangkat lunak terkait.

Tema	Kategori	Deskripsi
Konten Berbahaya & Ilegal	Kegiatan Kriminal	Instruksi atau materi yang mempromosikan tindakan ilegal.
Konten Berbahaya & Ilegal	Peretasan	Alat akses sistem yang tidak sah dan sumber daya eksploitasi jaringan.
Konten Berbahaya & Ilegal	Narkoba Ilegal	Konten yang mempromosikan penggunaan narkoba rekreasi atau penyalahgunaan zat.
Konten Berbahaya & Ilegal	Perangkat Lunak Ilegal	Materi berhak cipta yang tidak sah dan distribusi perangkat lunak berbahaya.
Konten Berbahaya & Ilegal	Kekerasan	Konten yang mempromosikan kerusakan fisik atau menampilkan materi grafis.
Konten Berbahaya & Ilegal	Senjata	Sumber daya olahraga dan rekreasi yang sah menggunakan senjata api.
Perilaku Berisiko Tinggi	Kultus	Konten spiritual dan metafisik non-arus utama.
Perilaku Berisiko Tinggi	Judi	Kegiatan dan informasi terkait taruhan.
Perilaku Berisiko Tinggi	Kebencian dan Intoleransi	Konten mempromosikan bias terhadap karakteristik yang dilindungi.
Perilaku Berisiko Tinggi	Kecurangan Sekolah	Bantuan akademik yang tidak sah dan layanan penyelesaian pekerjaan rumah.

Tema	Kategori	Deskripsi
Perilaku Berisiko Tinggi	Menyakiti Diri Sendiri	Mempromosikan konten atau mendiskusikan perilaku merusak diri sendiri.
Teknologi & AI	Situs Unduhan	Perangkat lunak, aplikasi, dan platform hosting aset digital.
Teknologi & AI	AI Generatif	AI dan sumber daya teknologi pembelajaran mesin.
Teknologi & AI	Domain yang diparkir	Domain konten minimal yang digunakan untuk iklan atau penjualan domain.
Teknologi & AI	Media Streaming dan Unduhan	Platform konten audio/video termasuk musik, video, dan radio internet.

Contoh dari URLs

Jenis-jenis berikut URLs dapat disediakan di AllowedUrls atau BlockedUrls

Tipe	Contoh
Domain	contoh.com
Subdomain	login.example.com
Jalan	example.com/myvideos
Parameter kueri	example.com/? parameter=123

Mentransfer kebijakan Chrome

Jika Anda sudah menyiapkan kebijakan Chrome untuk mengizinkan atau memblokir domain tertentu, sebaiknya Anda mentransfernya ke fitur Pemfilteran Konten Web.

Fitur Pemfilteran Konten Web akan mendeteksi setiap URLAllow atau URLBlock kebijakan yang berlaku untuk sesi Browser WorkSpaces Aman dan akan memberi sinyal di AWS Konsol.

Untuk mentransfer kebijakan Chrome untuk URLAllowlist dan/atau URLBlocklist:

- Di AWS Konsol Anda, di bawah Pemfilteran URL, klik Tinjau Kebijakan Chrome (jika Anda tidak melihat tombol Tinjau Kebijakan Chrome, ini berarti kebijakan Chrome saat ini tidak berlaku untuk Izinkan URL atau URLBlock)
- Di bawah overlay, tinjau kebijakan Chrome
- Klik Transfer

Kebijakan Chrome akan dihapus dari Editor JSON di bawah Pengaturan Kebijakan dan baru URLs akan secara otomatis ditambahkan ke fitur Pemfilteran Konten Web.

Tautan dalam di Amazon WorkSpaces Secure Browser

Saat pengguna masuk ke Browser WorkSpaces Aman, mereka memulai sesi di halaman beranda yang ditetapkan oleh administrator. Anda juga dapat mengizinkan portal menerima tautan dalam yang menghubungkan pengguna ke situs web tertentu selama sesi. Saat deep link dipilih, portal menampilkan URL yang ditentukan di deep link. Tautan ditampilkan di samping halaman beranda yang dikonfigurasi untuk memulai sesi, atau dengan sendirinya jika sesi sudah berlangsung. Fitur ini memungkinkan administrator untuk membuat pengalaman pengguna yang lebih dinamis dengan Browser WorkSpaces Aman.

Deep link membuka halaman dalam sesi Browser WorkSpaces Aman. Jika sesi sudah berjalan, itu akan membuka deep link di tab baru. Jika sesi belum berjalan, itu akan membuka URL tautan dalam di tab baru, dan halaman beranda default portal di tab terpisah. Jika deep link berisi lebih dari satu URL, itu akan menampilkan URL tautan dalam yang terdaftar pertama dalam fokus, dengan setiap URL berikutnya (termasuk halaman beranda default) dibuka di tab terpisah.

Topik

- Menyiapkan tautan dalam di Amazon WorkSpaces Secure Browser
- Menggunakan pemfilteran URL untuk deep link di Amazon WorkSpaces Secure Browser

Menyiapkan tautan dalam di Amazon WorkSpaces Secure Browser

Untuk mengizinkan izin tautan dalam, pilih Diizinkan saat membuat pengaturan pengguna. Situs yang ingin Anda tautkan dalam harus dikodekan URL. Misalnya, untuk menautkan pengguna ke “https://www.example.com/? query=true”, perbarui link ke %2F%3Fquery%3Dtrue. https%3A%2F %2Fwww.example.com

Deeplink dapat berisi hingga 10 URLs, digambarkan dengan koma. Contoh:

https://<uuid>.workspaces-web.com/? https%3A%2F%2Fwww.example.com DeepLinks= %2F %3Fquery%3Dtrue, %2F%3Fquery%3Dtrue2, %2F%3Fquery%3Dtrue3, %2F%3Fquery%3Dtrue4. https%3A%2F%2Fwww.example.com https%3A%2F%2Fwww.example.com https%3A%2F %2Fwww.example.com

Untuk informasi selengkapnya tentang mengizinkan deep link, lihatthe section called “Pengaturan pengguna”.

Menggunakan pemfilteran URL untuk deep link di Amazon WorkSpaces Secure Browser

Setiap pengguna yang Anda bagikan tautan portal ini dapat memanipulasi nilai tautan dalam untuk mengunjungi situs web, jika domain tersebut dapat dijangkau dari portal dan bukan pada daftar blokir URL. Untuk membuat daftar izin atau daftar blokir yang membatasi untuk mencegah pengguna mengunjungi domain yang tidak diinginkan dengan portal Anda, gunakan pemfilteran URL.

Daftar yang diizinkan dan daftar blokir untuk portal dapat diedit dengan pemfilteran URL di pengaturan browser portal Anda. <uuid>Untuk melakukan ini, tambahkan URL ke URL portal allow-listed dalam format berikut, di mana UUID adalah id portal: https://.workspaces-web.com/? deepLinks= %2F%3Fquery%3Dtrue https%3A%2F%2Fwww.example.com

Untuk informasi selengkapnya, lihat the section called “Pemfilteran konten web” dan Izinkan atau blokir akses ke situs web.

Menggunakan dasbor manajemen sesi di Amazon WorkSpaces Secure Browser

Gunakan dasbor manajemen sesi di konsol Browser WorkSpaces Aman Anda untuk memantau dan mengelola sesi aktif dan lengkap.

Akses dasbor

Untuk mengakses dasbor, ikuti langkah-langkah ini.

Untuk mengakses dasbor

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, dan pilih portal web Anda.

3. Pilih tab Sesi atau pilih Lihat sesi untuk membuka dasbor di panel terpisah di bawah ini.

Filter dasbor

Di panel sesi, Anda dapat memfilter sesi berdasarkan properti atau nilai berikut:

- Status
  - Aktif - Menunjukkan sesi sedang berjalan. Untuk mengakhiri sesi, lihat di bawah.
  - Dihentikan - Menunjukkan sesi tidak lagi aktif.
- ID Sesi
- Nama Pengguna
- Waktu mulai sesi

Mengakhiri sesi

Untuk mengakhiri sesi, ikuti langkah-langkah ini.

Untuk mengakhiri sesi

1. Di dasbor sesi, pilih sesi yang ingin Anda hentikan.
2. Pilih Akhiri.
3. Pengguna yang terputus kehilangan semua status dari sesi. Semua tab terbuka, riwayat browser, dan file yang diunduh ke browser aman didaur ulang.

Riwayat sesi

Dasbor berisi sesi dari 35 hari terakhir. Anda dapat menggunakan CLI untuk membuat daftar sesi, dengan atau tanpa filter. Riwayat sesi disampaikan sebagai JSON, yang administrator dapat memproses, mengelola, dan menyimpan dalam repositori terpisah.

Berikut ini adalah contoh perintah CLI untuk mengelola sesi di wilayah AS-Barat-2 (Oregon).

Untuk membuat daftar semua sesi untuk portal web, jalankan perintah berikut:

aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId>

Untuk membuat daftar semua sesi untuk pengguna tertentu dari portal web, jalankan perintah berikut:

aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId> --username <username>

Melindungi data dalam perjalanan dengan titik akhir FIPS dan Amazon WorkSpaces Secure Browser

Secara default, saat Anda berkomunikasi dengan layanan Browser WorkSpaces Aman sebagai administrator menggunakan konsol, Antarmuka Baris AWS Perintah (AWS CLI), atau AWS SDK, atau selama sesi pengguna, semua data dalam perjalanan dienkripsi menggunakan TLS 1.2.

Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Saat Anda menggunakan titik akhir FIPS, semua data dalam perjalanan dienkripsi menggunakan standar kriptografi yang sesuai dengan Federal Information Processing Standard (FIPS) 140-3. Untuk informasi tentang titik akhir FIPS, termasuk daftar titik akhir Browser WorkSpaces Aman, lihat. https://aws.amazon.com/compliance/fips

Setelah portal dibuat dengan titik akhir FIPS, semua sesi pengguna dan perubahan administratif dibuat secara otomatis menggunakan titik akhir FIPS 140-3. Anda dapat menggunakan variabel `AWS_USE_FIPS_ENDPOINT=true` lingkungan untuk menemukan titik akhir FIPS dan mengirim permintaan dengan SDK. Berikut adalah contohnya.

```
$ export AWS_USE_FIPS_ENDPOINT=true
$ aws workspaces-web list-portal
```

Anda juga dapat menggunakan `–endpoint-url` opsi untuk mengirim permintaan langsung ke titik akhir FIPS. Berikut ini adalah contoh portal daftar panggilan di Wilayah AS-Barat-2 (Oregon):

```
$ aws workspaces-web list-portal --endpoint-url https://workspaces-web-fips.us-west-2.amazonaws.com
```

Mengelola pengaturan perlindungan data di Amazon WorkSpaces Secure Browser

Pengaturan Perlindungan Data digunakan untuk membantu melindungi data agar tidak dibagikan selama sesi. Pengaturan dapat dibuat dan diterapkan ke beberapa portal.

Topik

- Redaksi data sebaris di Amazon WorkSpaces Secure Browser
- Konfigurasi redaksi default di Amazon WorkSpaces Secure Browser
- Redaksi sebaris dasar di Amazon WorkSpaces Secure Browser
- Redaksi sebaris khusus di Amazon WorkSpaces Secure Browser
- Buat pengaturan perlindungan data di Amazon WorkSpaces Secure Browser
- Mengaitkan pengaturan perlindungan data di Amazon WorkSpaces Secure Browser
- Mengedit pengaturan perlindungan data di Amazon WorkSpaces Secure Browser
- Hapus pengaturan perlindungan data di Amazon WorkSpaces Secure Browser

Redaksi data sebaris di Amazon WorkSpaces Secure Browser

Dengan menambahkan redaksi data sebaris ke portal, Anda dapat secara otomatis memprediksi dan menyunting data tertentu dari serangkaian teks yang ditampilkan di halaman web. Anda dapat membuat kebijakan redaksi dengan memilih dari pola bawaan (seperti nomor jaminan sosial atau nomor kartu kredit), atau membuat tipe data kustom mereka sendiri menggunakan ekspresi reguler dan kata kunci. Kebijakan mencakup tingkat penegakan dan kontrol yang dapat dikonfigurasi untuk URLs tempat redaksi harus ditegakkan.

Komponen berikut menentukan kapan data disunting:

- Pengaturan Perlindungan Data - Pengaturan Perlindungan Data adalah nama sumber daya yang mencakup tipe data dan kriteria penegakan. Untuk menggunakan sumber daya ini, pertama-tama buat pengaturan Anda, lalu kaitkan ke portal. Saat pengguna meluncurkan sesi, pengaturan Anda diberlakukan selama sesi berlangsung.
- Ekstensi browser dalam sesi - Saat Anda mengaitkan pengaturan redaksi dengan portal Anda, browser sesi akan diluncurkan dengan ekstensi browser yang diberlakukan sistem yang memberlakukan pengaturan Anda. Pengaturan Perlindungan Data menerapkan redaksi melalui pencocokan pola (Ekspresi Reguler) dan pencarian kata kunci mengikuti tingkat kepercayaan

dan konfigurasi penegakan URL Anda. Konten diprediksi dari string teks dan disunting sebelum ditampilkan di layar. Ekstensi ini juga menetapkan kebijakan browser terkait yang mengatur kemampuan pengguna untuk melewati redaksi (seperti penjelajahan pribadi yang dinonaktifkan, akses ke alat pengembang, dan inspeksi jaringan).

Perubahan kebijakan browser Chrome berikut diberlakukan oleh ekstensi browser dalam sesi. Untuk informasi selengkapnya, lihat daftar kebijakan Chrome Enterprise.

- Menerapkan kebijakan browser untuk mencegah pengguna melihat sesi tanpa redaksi:
  - IncognitoModeAvailability= 1
  - DeveloperToolsAvailability= 2
  - BrowserAddPersonEnabled= salah
  - BrowserGuestModeEnabled= salah
- Ekstensi ini juga mencegah pengguna mengunduh file HTML dari URLs yang menerapkan pengaturan perlindungan data dengan membatalkan acara unduhan.

Secara umum, Anda harus menggunakan redaksi dengan situs web pribadi dan terstruktur (seperti alat manajemen pelanggan, sistem tiket, atau wiki), dan bukan untuk penjelajahan publik yang tidak terstruktur (seperti Facebook atau Google). Anda dapat memilih dari tipe data bawaan (lihat di bawah untuk daftar lengkapnya), atau menentukan tipe data khusus menggunakan nilai ekspresi reguler dan kata kunci Anda sendiri. Administrator bertanggung jawab untuk menguji dan memvalidasi bahwa setiap tipe data, tingkat kepercayaan, dan penegakan URL berfungsi seperti yang diharapkan. AWS tidak dapat menjamin kompatibilitas dengan situs web atau aplikasi khusus yang disediakan oleh pihak ketiga.

WorkSpaces Browser Aman saat ini tidak mendukung redaksi tipe data yang didukung atau kustom dalam format non-teks, termasuk teks dalam format berikut:

- Gambar, seperti JPEG, PNG, atau GIF
- Halaman web yang memungkinkan pengguna untuk menggunakan pengolah kata dinamis atau pengeditan, seperti Google Documents atau Sheets
- Streaming audio atau video diakses di browser, seperti video YouTube
- PDFs dilihat oleh browser Chrome

Jangan gunakan redaksi untuk konten dalam format yang tidak didukung. Administrator bertanggung jawab untuk memvalidasi kompatibilitas situs dan konten sebelum memberikan pengguna akses ke konten yang ingin mereka edit.

Konfigurasi redaksi default di Amazon WorkSpaces Secure Browser

Konfigurasi redaksi default akan secara otomatis menerapkan tingkat kepercayaan dan penegakan URL untuk semua tipe data bawaan dalam pengaturan perlindungan data. Anda memiliki opsi untuk mengganti konfigurasi default saat menambahkan tipe data bawaan.

Tingkat kepercayaan memungkinkan Anda untuk menyempurnakan logika redaksi untuk tipe data bawaan menggunakan kombinasi format, kata kunci, dan teks yang tidak diformat. Pilih tingkat keketatan untuk bagaimana redaksi diterapkan, termasuk Tinggi, Sedang, atau Rendah. Nilai default akan berlaku untuk semua tipe data, kecuali penggantian diterapkan pada tingkat tipe data. Secara umum, mulailah dengan konfigurasi default Medium, dan perbaiki dengan memvalidasi bahwa redaksi diberlakukan seperti yang diharapkan di situs Anda.

Tingkat kepercayaan	Deskripsi	Contoh
Tinggi	Memerlukan kecocokan pola teks yang diformat agar konten dapat disunting.	SSN dari 123-45-6798 akan disunting, sedangkan 123456789 tidak.
Sedang	Redaksi mempertimbangkan teks yang diformat dan tidak diformat, dan menambahkan asosiasi kata kunci ke logika.	SSN dari 123-45-6798 akan disunting. 123456789 akan disunting jika terdeteksi di dekat kata kunci (seperti “nomor jaminan sosial”).
Rendah	Redaksi diberlakukan untuk kedua pola yang diformat+pola yang tidak diformat tanpa kata kunci.	SSN dalam format apa pun - 123-45-6798 dan 123456789 - disunting tanpa memerlukan kata kunci.

Anda harus mengatur konfigurasi redaksi default untuk semua tipe data. Anda dapat memilih dari opsi berikut:

- Semua URLs

- Spesifik URLs
- Konfigurasi lanjutan

Nilai default akan berlaku untuk semua tipe data, kecuali penggantian diterapkan pada tingkat tipe data. Penegakan URL menggunakan logika serupa dengan kebijakan Chrome untuk mengelola izin dan daftar blokir. Untuk panduan menggunakan blokir dan izinkan URLs, lihat Mengizinkan atau memblokir akses ke situs web. Untuk hasil terbaik, tambahkan URLs ke daftar ini mengikuti format filter daftar blokir Chrome. Untuk informasi selengkapnya, lihat format filter daftar blokir URL.

Redaksi sebaris dasar di Amazon WorkSpaces Secure Browser

Redaksi data inline memiliki dukungan untuk pola bawaan (seperti nomor jaminan sosial dan nomor kartu kredit), yang dapat Anda temukan tercantum di bawah Redaksi inline Base. Pilih tipe data dari menu tarik-turun, dan tentukan nilai pengganti untuk setiap tipe data. Semua tipe data mengikuti pola penegakan konfigurasi default di atas, tetapi Anda dapat memilih untuk mengganti tingkat kepercayaan, dan menyempurnakan pola penegakan domain untuk setiap tipe data.

Untuk memasukkan nilai alternatif dari konfigurasi default, pilih Confidence level override. Misalnya, dengan konfigurasi default disetel ke Medium, Anda mungkin memperhatikan selama pengujian bahwa salah satu tipe data Anda tidak disunting secara andal. Anda dapat mengatur override ke Low untuk meningkatkan kemungkinan redaksi, tanpa menyesuaikan logika yang digunakan untuk tipe data Anda yang lain.

Untuk menyempurnakan cara redaksi diterapkan URLs tanpa mengubah konfigurasi default, terapkan penggantian penegakan URL. Misalnya, Anda dapat mengatur penggantian URL penggunaan untuk menerapkan redaksi alamat email dalam sistem manajemen hubungan pelanggan Anda, tanpa merusak akses pengguna ke alamat email di situs web direktori perusahaan atau email berbasis web.

Berikut ini adalah daftar tipe data dan pola bawaannya yang sesuai IDs:

builtInPatternId	Jenis data
awsAccessKey:	Kunci Akses AWS
awsSecretKey:	Kunci Rahasia AWS
Nomor kartu:	Nomor Kartu Kredit
kripto:	Alamat Cryptocurrency

builtInPatternId	Jenis data
CusiPnum:	Nomor CUSIP
tanggal:	Date
DeAnum:	Nomor DEA AS
dob:	Tanggal Lahir
Lisensi DriversLicense:	Surat Izin Mengemudi AS
Alamat email:	Alamat Email
ein:	Nomor Identifikasi Majikan AS
Tanggal kedaluwarsa:	Tanggal Kedaluwarsa Kartu Kredit
healthInsuranceNum:	Nomor Klaim Asuransi Kesehatan Medicare
HipaaCode:	Kode HIPAA ICD-10
indivTaxId:	ID Pajak Perorangan AS
iPaddr:	Alamat IP
isin:	Nomor Identifikasi Sekuritas Internasional
jwt:	Token Web JSON
LocationCoord:	Koordinat Lokasi
MacAddr:	Alamat MAC
medicareBeneficiaryId:	Nomor Penerima Medicare
npi:	Nomor Identifikasi Penyedia Nasional
NDC:	Kode Obat Nasional (NDC)
PassportNUM:	Nomor Paspor AS

builtInPatternId	Jenis data
PhoneNum:	Nomor Telepon
RoutingNumber:	Nomor Perutean ABA
ssn:	Nomor Jaminan Sosial AS
Kode Swift:	Kode SWIFT
waktu:	Waktu
vin:	Nomor Identifikasi Kendaraan AS

Redaksi sebaris khusus di Amazon WorkSpaces Secure Browser

Pelanggan dapat menentukan pola mereka sendiri menggunakan ekspresi reguler, seperti aplikasi internal khusus IDs. Untuk membuat pola redaksi inline kustom Anda, ikuti langkah-langkah ini:

1. Buka pengaturan perlindungan data Anda.
2. Pilih Custom inline redaction dan tambahkan.
3. Masukkan nama untuk tipe data kustom.
4. Masukkan nilai ekspresi reguler Anda.
   - Nilai ekspresi reguler harus sesuai dengan sintaks literal ekspresi JavaScript reguler. Untuk informasi selengkapnya, lihat Ekspresi reguler. Contoh ekspresi reguler adalah`/ex[am]+ple/i`.
   - Pastikan untuk menguji pola kustom Anda di situs web yang Anda rencanakan untuk didukung. Jika pola kustom ditulis dengan kesalahan, mereka dapat menimbulkan masalah kinerja yang tidak diinginkan.
5. Tentukan nilai penggantian.
6. Pilih Opsi lainnya untuk penyesuaian opsional lainnya, termasuk yang berikut ini:
   - Tambahkan kata kunci untuk menyempurnakan logika redaksi. Kata kunci dapat meningkatkan akurasi penegakan hukum. Tambahkan kata kunci dalam sintaks literal ekspresi reguler Javascript. Untuk informasi selengkapnya, lihat Ekspresi reguler.

Misalnya, jika Anda membuat pola redaksi khusus untuk klien yang IDs digunakan dalam sistem internal, Anda dapat menambahkan `/client name/i` ke bidang kata kunci untuk menginformasikan logika pemindaian dan deteksi.

- Terapkan penggantian penegakan URL untuk menyempurnakan cara redaksi diterapkan URLs, tanpa mengubah konfigurasi default.

  Misalnya, Anda dapat mengatur penggantian URL penggunaan untuk menerapkan redaksi alamat email dalam sistem manajemen hubungan pelanggan Anda, tanpa merusak akses pengguna ke alamat email di situs web direktori perusahaan atau email berbasis web.

- Masukkan deskripsi (opsional) untuk tipe data.

Buat pengaturan perlindungan data di Amazon WorkSpaces Secure Browser

Anda dapat membuat pengaturan perlindungan data di Browser WorkSpaces Aman.

Untuk membuat pengaturan perlindungan data

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Di panel navigasi sebelah kiri, pilih Pengaturan Perlindungan Data.
3. Pilih Buat Pengaturan Perlindungan Data.
4. Masukkan nama tampilan (wajib) dan deskripsi (opsional) untuk pengaturan.
5. Pilih pengaturan default untuk redaksi sebaris. Anda dapat mengatur yang berikut ini:
   - Tingkat keketatan semua tipe data
   - Domain tempat redaksi harus ditegakkan
6. Pilih tipe data redaksi sebaris dasar Anda dari tipe yang didukung, atau buat tipe data kustom. Anda dapat mengatur penggantian untuk setiap tipe data, termasuk tingkat keketatan dan pengecualian domain.
7. Tambahkan Tag apa pun (opsional) untuk pelaporan.
8. Jika Anda sudah selesai, pilih Simpan.

Mengaitkan pengaturan perlindungan data di Amazon WorkSpaces Secure Browser

Anda dapat mengaitkan pengaturan perlindungan data di Browser WorkSpaces Aman.

Untuk mengaitkan pengaturan perlindungan data dengan portal yang ada

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Di panel navigasi sebelah kiri, pilih Portal Web.
3. Pilih portal web, dan pilih Edit.
4. Di bawah Pengaturan perlindungan data, pilih pengaturan untuk portal Anda.
5. Pilih Simpan.

Untuk mengaitkan pengaturan perlindungan data saat membuat portal baru, ikuti langkah-langkah ini.

Untuk mengaitkan pengaturan perlindungan data saat membuat portal baru

1. Ikuti petunjuk the section called “Pembuatan portal web” untuk membuat portal, sampai Anda mendapatkan pengaturan perlindungan data.
2. Pilih pengaturan perlindungan data Anda dari menu tarik-turun.
3. Selesaikan langkah-langkah the section called “Pembuatan portal web” untuk menyelesaikan pembuatan portal Anda.

Untuk membuat pengaturan perlindungan data saat membuat portal baru, ikuti langkah-langkah ini.

Untuk membuat pengaturan perlindungan data saat membuat portal baru

1. Ikuti petunjuk the section called “Pembuatan portal web” untuk membuat portal, sampai Anda mendapatkan pengaturan perlindungan data.
2. Pilih pengaturan perlindungan data dari menu tarik-turun.
3. Masukkan nama tampilan (wajib) dan deskripsi (opsional) untuk pengaturan.
4. Pilih pengaturan default untuk redaksi sebaris. Anda dapat mengatur yang berikut ini:
   - Tingkat keketatan semua tipe data
   - Domain tempat redaksi harus ditegakkan

5. Pilih tipe data redaksi sebaris dasar Anda dari tipe yang didukung, atau buat tipe data kustom. Anda dapat mengatur penggantian untuk setiap tipe data, termasuk tingkat keketatan dan pengecualian domain.
6. Tambahkan Tag apa pun (opsional) untuk pelaporan.
7. Jika Anda sudah selesai, pilih Simpan.
8. Pilih tombol refresh di bawah pengaturan perlindungan data, lalu pilih pengaturan perlindungan data Anda dari menu tarik-turun.
9. Terus ikuti instruksi buat portal untuk menyelesaikan pembuatan portal Anda.

Mengedit pengaturan perlindungan data di Amazon WorkSpaces Secure Browser

Anda dapat mengedit pengaturan perlindungan data di Browser WorkSpaces Aman.

Untuk mengedit pengaturan perlindungan data

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih pengaturan perlindungan data dan pengaturan perlindungan data yang ingin Anda edit dari tampilan daftar.
3. Anda dapat memperbarui nama, deskripsi, pengaturan default, tipe data (didukung atau kustom), dan menerapkan tingkat kepercayaan atau penggantian domain.
4. Pilih Simpan.

Hapus pengaturan perlindungan data di Amazon WorkSpaces Secure Browser

Anda dapat menghapus pengaturan perlindungan data di Browser WorkSpaces Aman.

Untuk menghapus pengaturan perlindungan data

1. Jika Anda memiliki portal yang terkait dengan pengaturan perlindungan data, Anda harus terlebih dahulu menghapus asosiasi sebelum menghapus pengaturan perlindungan data.
2. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.

3. Pilih pengaturan perlindungan data dan pengaturan perlindungan data yang ingin Anda hapus dari tampilan daftar.
4. Pilih Hapus.

Kustomisasi branding di Amazon WorkSpaces Secure Browser

Anda dapat menyesuaikan layar masuk dan memuat yang muncul untuk pengguna akhir Anda dengan memodifikasi elemen visual, konten teks, dan persyaratan layanan. Kustomisasi branding membantu menciptakan pengalaman yang konsisten yang selaras dengan identitas organisasi Anda.

Ikhtisar

Kustomisasi branding memungkinkan Anda untuk mempersonalisasi aspek-aspek berikut dari pengalaman pengguna:

- Elemen visual - Unggah logo, favicon, dan wallpaper, dan pilih tema warna yang sesuai dengan identitas merek Anda.
- Konten teks - Sesuaikan pesan selamat datang, judul tab browser, dan bidang teks opsional lainnya untuk mempertahankan suara merek Anda di seluruh alur masuk. Jika Anda tidak menentukan teks kustom untuk bidang tertentu, teks default akan digunakan. Lihat perinciannya di the section called “Pedoman kustomisasi”.
- Ketentuan Layanan (opsional) - Tambahkan persyaratan layanan organisasi Anda yang harus diakui pengguna sebelum memulai sesi.

> **Note**
>
> Anda juga dapat menyesuaikan nama domain untuk portal Anda. Lihat perinciannya di the section called “Domain kustom”.

Topik

- Mengkonfigurasi kustomisasi branding untuk portal Anda
- Pedoman kustomisasi

Mengkonfigurasi kustomisasi branding untuk portal Anda

Cara kerjanya

Saat Anda mengonfigurasi kustomisasi branding:

- Elemen visual dan teks diterapkan ke layar masuk dan layar pemuatan.
- Tab browser menampilkan favicon dan judul kustom Anda.
- Pengguna akhir akan melihat perubahan penyesuaian Anda saat memulai sesi baru. Dalam beberapa kasus, mungkin diperlukan beberapa menit sebelum perubahan Anda terlihat.
- Jika persyaratan layanan dikonfigurasi, pengguna akhir harus menerima persyaratan layanan Anda sebelum memulai sesi streaming mereka. Perhatikan bahwa mereka akan ditanya di awal setiap sesi.

Prasyarat

Sebelum Anda memulai:

- Pastikan Anda memiliki izin yang diperlukan untuk mengubah pengaturan portal, lihatthe section called “AWS kebijakan terkelola”.
- Siapkan aset branding Anda (logo, favicon, wallpaper) sesuai spesifikasi di. the section called “Pedoman kustomisasi”

Memulai

Untuk mengonfigurasi kustomisasi branding, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, dan pilih portal web Anda.
3. Pilih portal Anda dan pilih tab Pengaturan pengguna.
4. Di bagian Kustomisasi merek, pilih Edit.
5. Konfigurasikan bagian berikut sesuai kebutuhan:

    - Di editor Konten - Unggah semua elemen visual (logo perusahaan Anda, favicon Anda, dan wallpaper opsional) dan pilih tema warna. Anda dapat mengunggah file baik dari komputer

lokal Anda atau dari ember S3. Untuk informasi tentang menyiapkan izin bucket S3, lihat. the section called “Menyiapkan izin bucket S3”

- Di Editor teks - Sesuaikan teks yang muncul di layar masuk.
- Dalam editor Ketentuan Layanan - Secara opsional, tambahkan persyaratan yang harus diakui pengguna.

6. Pilih Simpan perubahan.

Untuk petunjuk terperinci tentang setiap opsi penyesuaian, lihatthe section called “Pedoman kustomisasi”.

Menyiapkan izin bucket S3

Anda dapat mengunggah file branding langsung dari komputer Anda atau memilih objek yang ada dari bucket S3 Anda. Jika Anda memilih untuk mengunggah file untuk elemen visual (logo perusahaan, favicon, dan wallpaper) dari bucket S3, pastikan Anda menyiapkan izin yang tepat untuk bucket S3.

Memilih objek S3 di akun yang sama

Jika pengguna atau peran IAM Anda sudah memiliki `s3:GetObject` izin untuk bucket yang berisi aset branding Anda, konfigurasi tambahan tidak diperlukan.

Memilih objek S3 di akun lain

Untuk memilih bucket S3 di AWS akun lain, Anda perlu mengonfigurasi kebijakan bucket di akun sumber dan kebijakan IAM di akun admin Anda.

Contoh kebijakan bucket (di akun sumber):

Terapkan kebijakan ini ke bucket S3 di akun sumber. Ganti *123456789012* dengan ID akun admin Anda dan *source-account-bucket-name* dengan nama bucket Anda yang sebenarnya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountAccess",
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
      ]
    }
  ]
}
```

Contoh kebijakan IAM (di akun admin Anda):

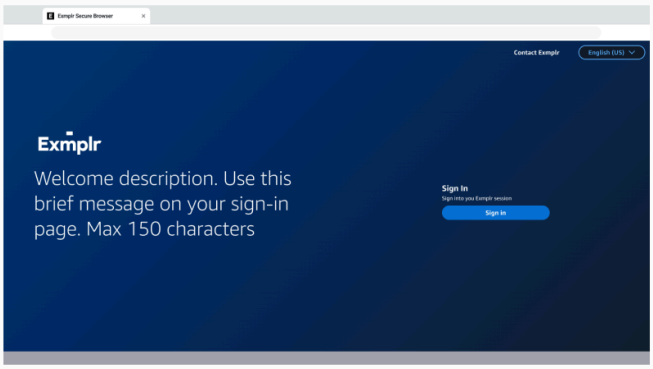
Lampirkan kebijakan ini ke pengguna IAM atau peran di akun admin Anda. Ganti *source-account-bucket-name* dengan nama bucket yang sebenarnya dari akun sumber.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountS3Access",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
      ]
    }
  ]
}
```

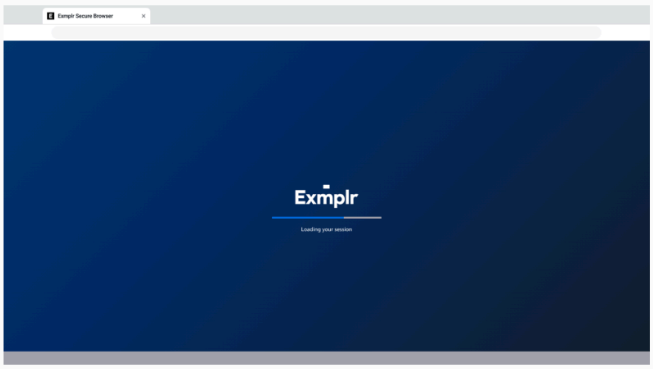
Untuk informasi selengkapnya tentang akses lintas akun, lihat Akses S3 Memberikan akses lintas akun.

Pedoman kustomisasi

Sesuaikan pengalaman masuk dan pemuatan untuk pengguna akhir Anda dengan memperbarui elemen branding dan teks saat masuk dan memuat halaman. Anda dapat memodifikasi elemen visual seperti logo dan wallpaper, mengedit elemen teks seperti pesan selamat datang dan header, dan secara opsional mengonfigurasi perjanjian Ketentuan Layanan yang harus diterima pengguna sebelum memulai sesi mereka.



Sign in Page

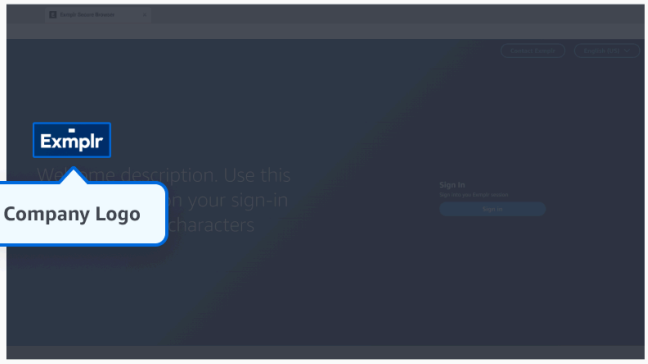


Loading Page

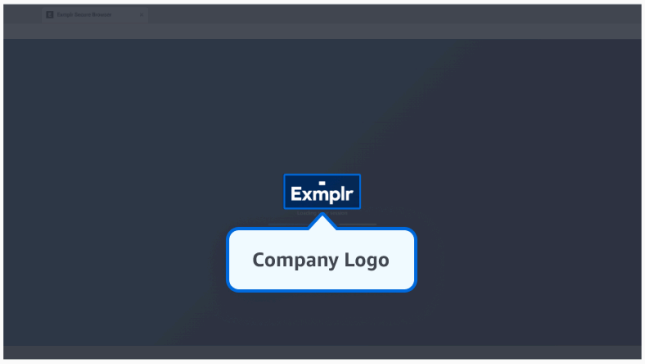
Editor konten

Logo perusahaan

Logo muncul di layar masuk dan layar pemuatan, sehingga memberikan branding yang konsisten sepanjang pengalaman pengguna.



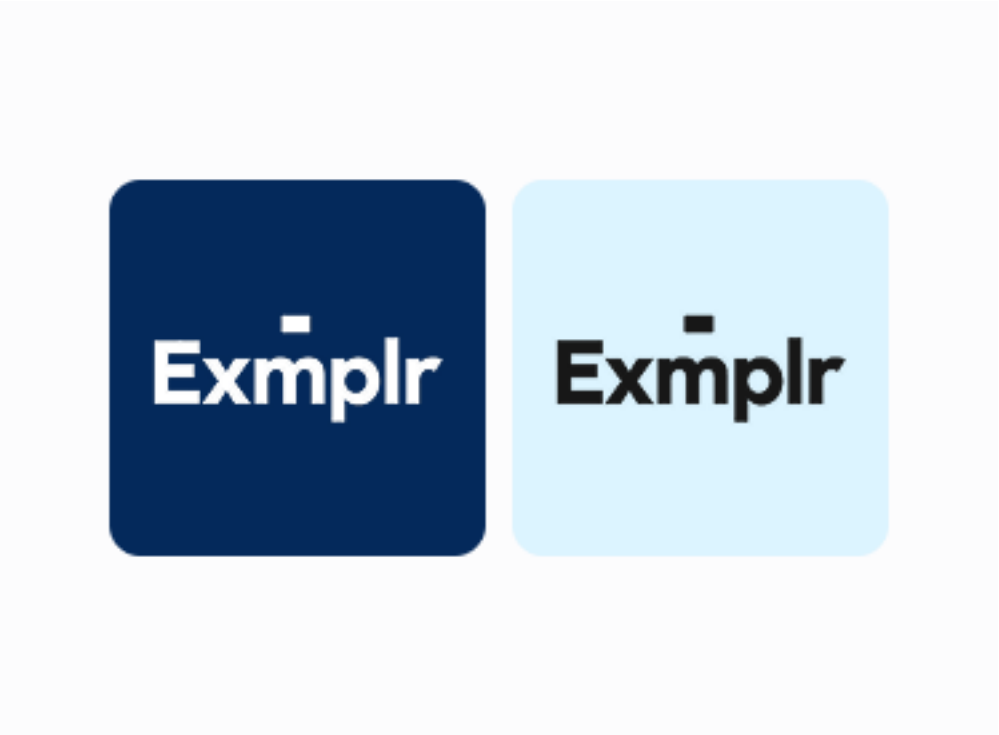
Sign in page



Loading page

- Format yang didukung: JPG, ICO, atau PNG
- Ukuran file maksimum: 100 KB

Lakukan



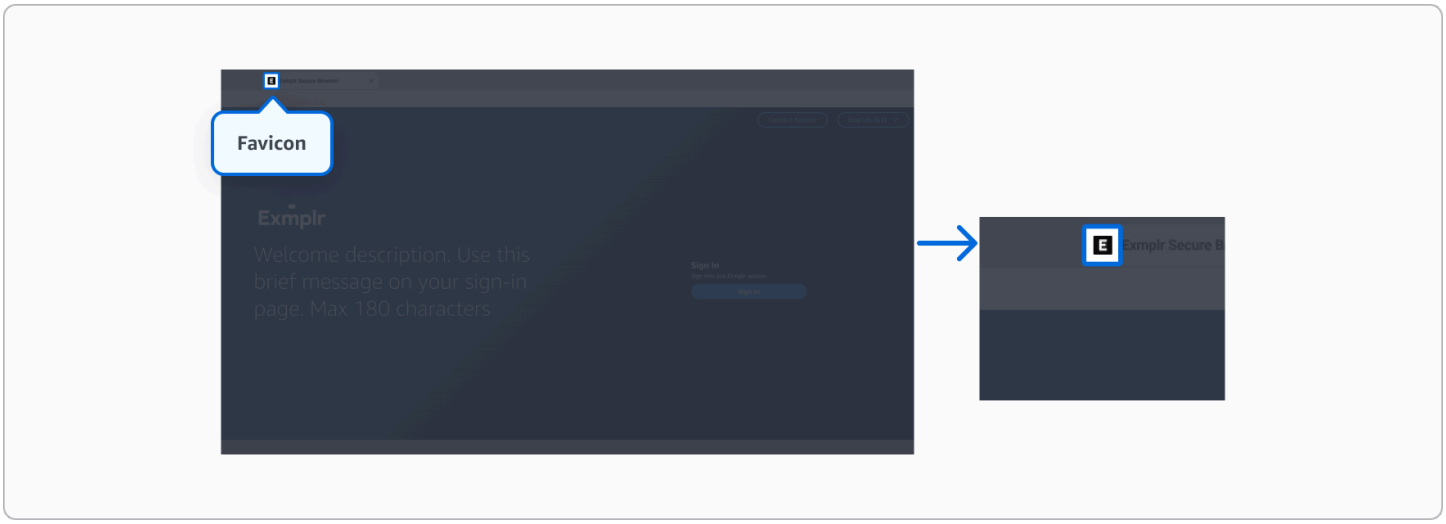
- Jika Anda memiliki variasi logo yang berbeda (seperti warna atau gaya yang berbeda), pilih salah satu yang memberikan kontras terbaik dengan latar belakang wallpaper pilihan Anda.

Jangan

- Jangan abaikan rasio aspek saat mengubah ukuran logo Anda.
- Jangan gunakan logo yang tidak berukuran benar sebelumnya karena mungkin terlihat terdistorsi.

Favicon

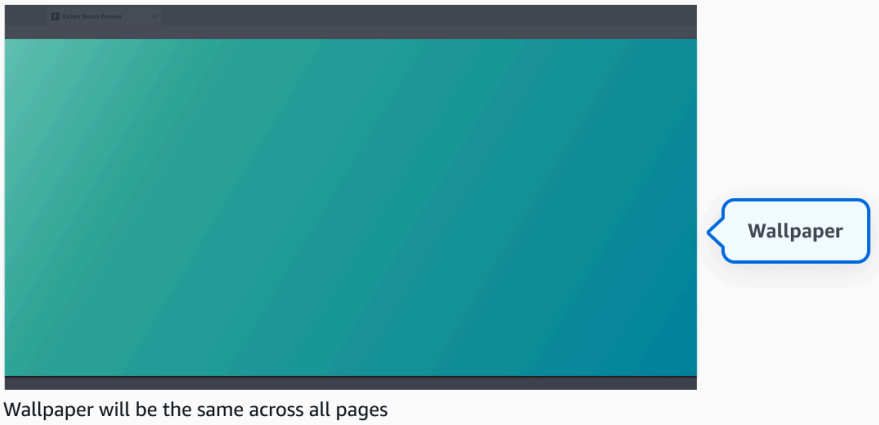
Favicon adalah ikon kecil yang muncul di tab browser, membantu pengguna mengidentifikasi aplikasi Anda di antara beberapa tab yang terbuka.



- Format yang didukung: JPG, ICO, atau PNG
- Ukuran file maksimum: 100 KB
- Rasio aspek yang disarankan: 1:1

Wallpaper - opsional

Wallpaper berfungsi sebagai gambar latar belakang di semua layar, yang menciptakan pengalaman visual yang padu. Jika Anda tidak mengunggah wallpaper khusus, wallpaper default yang ditunjukkan di bawah ini akan digunakan. Pilih gambar yang melengkapi branding Anda tanpa mengganggu keterbacaan konten.



Wallpaper will be the same across all pages

- Format yang didukung: JPG atau PNG
- Ukuran file maksimum: 5 MB
- Rasio aspek yang disarankan: 16:9
- Resolusi minimum yang disarankan: 1920 x 1080

Lakukan

- Gunakan wallpaper halus, kontras rendah atau gambar buram yang tidak mengganggu konten latar depan.
- Pertimbangkan penempatan teks prasetel untuk menghindari area sibuk di belakang teks.
- Manfaatkan warna merek dan gunakan overlay untuk menciptakan kontras dan keterbacaan yang lebih baik.

Jangan

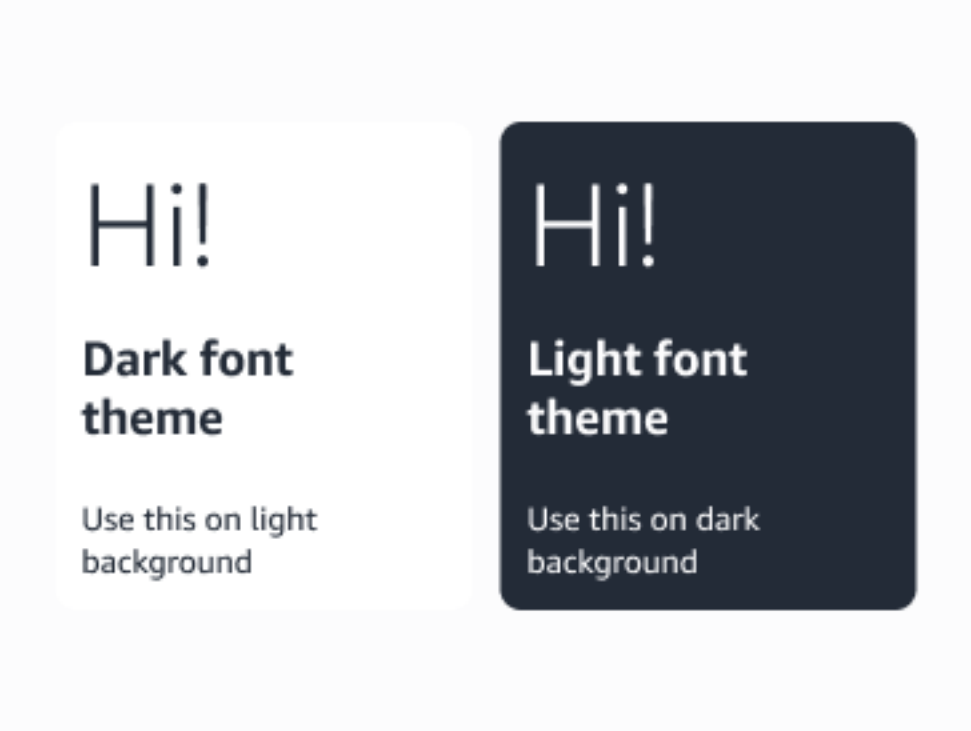
- Jangan gunakan gambar yang sibuk, jenuh, atau detail tinggi tepat di belakang teks penting.
- Jangan gunakan gambar atau gambar yang kompleks secara visual dengan transisi tajam yang akan menyebabkan keterbatasan keterbacaan dengan lokasi teks yang telah ditetapkan sebelumnya.
- Jangan hanya mengandalkan warna untuk memisahkan teks dari latar belakang tanpa kontras yang cukup.

Tema warna

Pilih antara tema terang atau gelap yang mencerminkan font, tombol, dan modals.

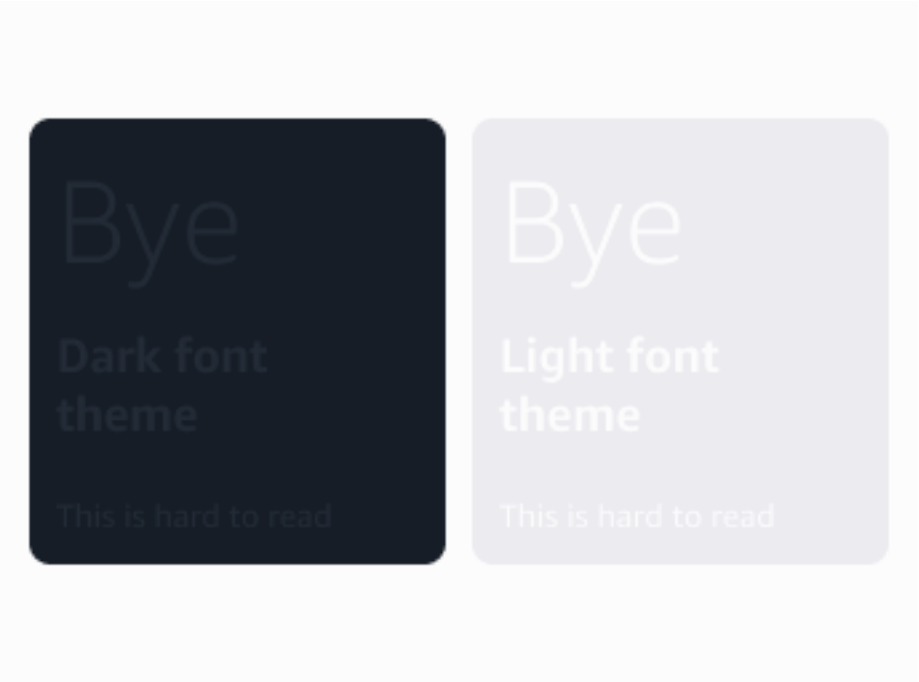
- Tema terang - Paling ideal untuk latar belakang yang lebih gelap, sehingga memberikan kontras yang jelas dan lebih nyaman untuk mata saat bekerja di lingkungan dengan minim cahaya.
- Tema gelap - Optimal untuk latar belakang berwarna terang, sehingga memberikan tampilan yang nyaman dan mengurangi silau dalam lingkungan yang terang.

Lakukan



- Pastikan kontras yang kuat dengan elemen latar belakang/wallpaper.
- Gunakan tema warna gelap pada latar belakang terang.
- Gunakan tema warna terang pada latar belakang gelap.

Jangan



- Jangan letakkan font terang atau gelap di atas gambar atau wallpaper kompleks.

Editor teks

Editor teks memungkinkan Anda menyesuaikan teks yang muncul di layar masuk pengguna akhir Anda. Untuk mengaktifkan kustomisasi branding, Anda harus menambahkan setidaknya satu bahasa.

Untuk pengguna baru: Kami mendeteksi preferensi bahasa browser Anda dan menampilkan halaman portal dalam bahasa tersebut jika Anda mengonfigurasinya dalam bahasa branding Anda. Jika bahasa browser Anda tidak dalam bahasa yang Anda konfigurasi, kami akan menggunakan bahasa Inggris (en-US) jika tersedia. Jika Anda tidak mengonfigurasi bahasa Inggris, kami akan menggunakan bahasa pertama dalam urutan abjad dari bahasa-bahasa yang Anda konfigurasi.

Untuk pengguna yang kembali: Kami menyimpan preferensi bahasa Anda dari sesi sebelumnya di dalam cookie browser. Jika bahasa tersebut ada dalam bahasa branding yang Anda konfigurasi, kami akan menggunakannya. Jika tidak, kami akan mengikuti logika fallback yang sama: bahasa Inggris (en-US) jika tersedia, atau bahasa yang dikonfigurasi pertama dalam urutan abjad.

Bahasa (kode bahasa) berikut ini didukung:

- Jerman (de-DE)
- Inggris (en-US)

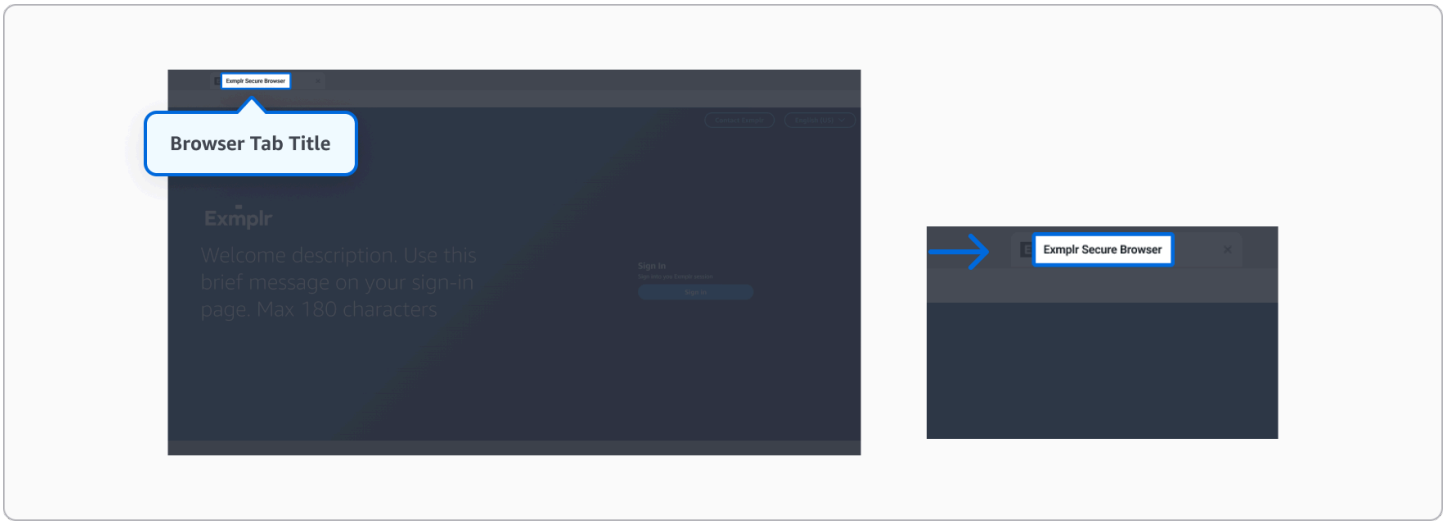
- Spanyol (es-ES)
- Prancis (fr-FR)
- Indonesia (id-ID)
- Italia (it-IT)
- Jepang (ja-JP)
- Korea (ko-KR)
- Portugis (pt-BR)
- Mandarin - Disederhanakan (zh-CN)
- Mandarin - Tradisional (zh-TW)

Untuk alasan keamanan, karakter berikut ini diblokir di semua bidang teks:

- < (kurang dari)
- > (lebih dari)
- & (ampersan)
- ' (apostrof lurus)
- ` (aksen nontirus/apostrof terbalik)
- ~ (tilde)
- \ (garis miring terbalik)

Judul tab browser

Teks yang ditampilkan di tab browser. Maksimum 25 karakter.

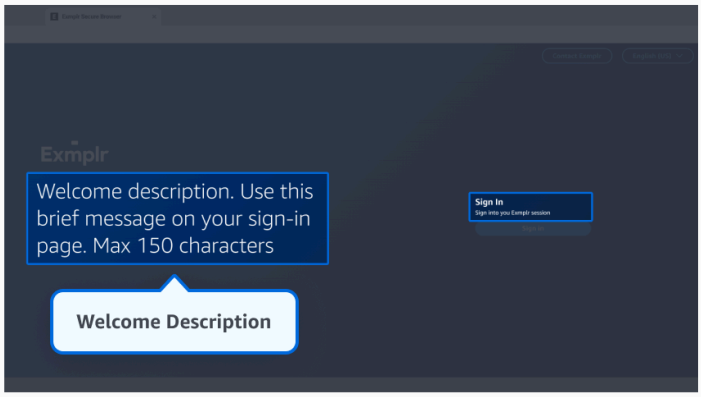


Rekomendasi

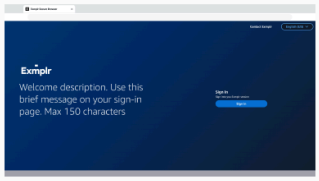
Pertimbangkan untuk menggunakan judul pendek dan jelas sehingga tetap dapat dibaca bahkan ketika beberapa tab terbuka.

Deskripsi selamat datang

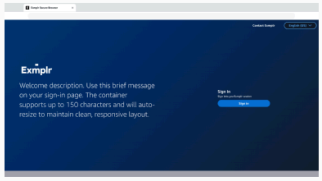
Deskripsi singkat yang menyertai logo perusahaan Anda di layar masuk. Maksimum 150 karakter.



Welcome description



Starting font sizing



Adapted sizing to Max characters

Rekomendasi

Jaga agar teks tetap ringkas untuk keterbacaan yang lebih baik. Perhatikan bahwa teks yang lebih panjang akan secara otomatis menskalakan ke ukuran font yang lebih kecil, sementara pesan yang lebih pendek ditampilkan lebih menonjol.

Bagian kontak

Tombol kontak - opsional

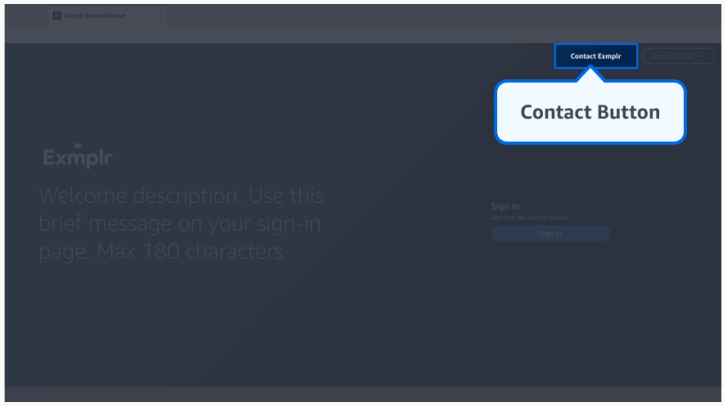
Teks tombol kontak di layar masuk. Jika dibiarkan kosong, “Hubungi kami” akan ditampilkan. Maksimum 30 karakter.

Tautan kontak - opsional

Tautan tombol kontak di layar masuk. Anda dapat menggunakan:

- URL HTTPS untuk mengarahkan pengguna ke halaman web
- Tautan mailto: untuk membuka klien email pengguna

Jika dikosongkan, tombol kontak akan disembunyikan dari layar.



Rekomendasi

Jaga agar teks tetap pendek, idealnya 2-3 kata.

Masuk bagian

Header masuk - opsional

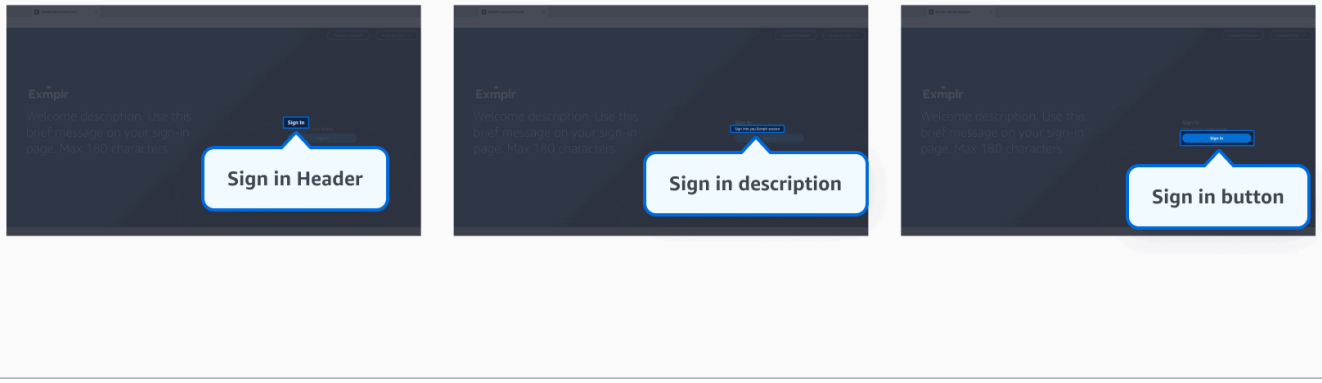
Header untuk bagian masuk di halaman login. Jika dikosongkan, teks “Masuk” akan ditampilkan. Maksimum 100 karakter.

Deskripsi masuk - opsional

Teks deskripsi untuk bagian login. Jika dibiarkan kosong, “Masuk ke Sesi Browser WorkSpaces Aman Anda” akan ditampilkan. Maksimum 250 karakter.

Tombol masuk - opsional

Teks yang ditampilkan pada tombol masuk. Jika dikosongkan, teks “Masuk” akan ditampilkan. Maksimum 30 karakter.

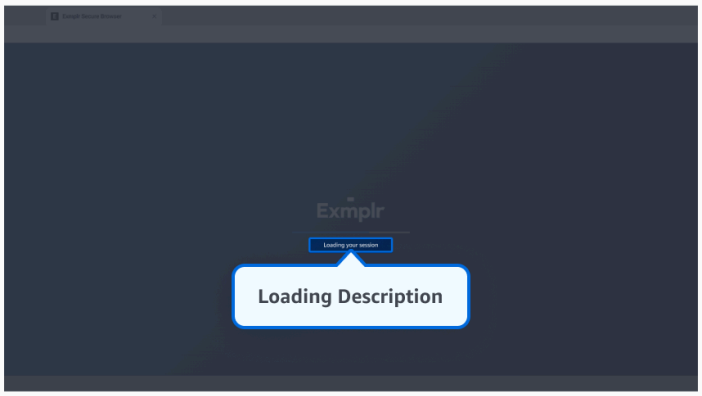


Rekomendasi

- Jaga agar teks tetap pendek.
- Pertimbangkan bahwa tombol masuk mengarahkan pengguna ke penyedia identitas yang dikonfigurasi untuk portal Anda. Anda dapat menyesuaikan teks tombol untuk mencerminkan penyedia identitas spesifik Anda.

Memuat deskripsi

Teks yang ditampilkan selama koneksi pada layar pemuatan. Jika dikosongkan, “Menghubungkan...” akan ditampilkan. Maksimum 300 karakter.



Loading screen

Rekomendasi

Pesan ini hanya ditampilkan saat sesi sedang dimuat, sehingga pengguna akhir mungkin tidak punya waktu untuk membacanya. Cobalah untuk menghindari membuatnya terlalu lama.

Ketentuan layanan - opsional

Anda dapat menyesuaikan ketentuan layanan yang harus ditinjau dan diterima oleh pengguna akhir sebelum mereka memulai sesi streaming. Konten ini dapat ditambahkan dengan mengunggah file Markdown atau menggunakan editor Markdown bawaan.

Pengguna akan melihat ketentuan layanan setelah berhasil masuk. Mereka harus menggulir dokumen sampai bawah lalu mengklik tombol “Terima” untuk melanjutkan ke sesi Secure Browser mereka. Jika pengguna mengklik “Tolak”, mereka akan diarahkan kembali ke halaman masuk.

Perhatikan bahwa ini adalah pengaturan opsional - jika Anda tidak menambahkan ketentuan layanan, pengguna akan langsung melanjutkan ke sesi mereka setelah masuk.

Pemformatan yang didukung:

- Gaya teks dasar (tebal, miring)
- Judul
- Daftar yang diurutkan dan tidak diurutkan
- Blockquote
- Aturan horizontal
- Paragraf sederhana dan jeda baris

Untuk keamanan, elemen-elemen berikut diblokir:

- Skrip dan eksekusi kode
- Elemen interaktif seperti bentuk dan iframe
- Protokol dan jalur file yang tidak aman
- Atribut dan penggayaan HTML
- Tabel dan tautan eksternal

Perlu diingat bahwa ukuran file ketentuan layanan Anda tidak boleh lebih dari 150 KB.

Mengaktifkan dukungan WebAuthn pengalihan di Amazon WorkSpaces Secure Browser

> **Warning**
>
> WebAuthn pengalihan hanya berfungsi di sesi browser dengan akses internet diaktifkan. Pastikan pengaturan jaringan portal Anda memungkinkan akses internet agar WebAuthn fungsionalitas berfungsi dengan baik.

WorkSpaces Dukungan Browser Aman WebAuthn (Otentikasi Web) untuk situs web yang diakses dalam sesi browser jarak jauh. Ini memungkinkan pengguna untuk mengautentikasi ke situs web menggunakan kunci FIDO2 keamanan lokal, otentikator biometrik, dan otentikator platform saat menjelajah di sesi Browser Aman mereka. WorkSpaces

> **Note**
>
> WebAuthn Pengalihan tersedia untuk pengguna akhir yang menggunakan Google Chrome 136 (atau yang lebih baru) atau Microsoft Edge 137 (atau yang lebih baru). Fitur ini tidak tersedia untuk browser non-Chromium seperti Safari atau Firefox.
> Untuk mengaktifkan fungsionalitas WebAuthn pengalihan, administrator harus mengonfigurasi keduanya:
>
> 1. Pengaturan Pengguna Portal - Aktifkan WebAuthn pengalihan di pengaturan portal
> 2. Kebijakan browser lokal pengguna akhir - Konfigurasikan kebijakan WebAuthenticationRemoteDesktopAllowedOrigins browser pada perangkat pengguna untuk memungkinkan pengalihan WebAuthn

Topik

- Mengaktifkan WebAuthn pengalihan dalam pengaturan portal
- Mengkonfigurasi kebijakan browser lokal untuk WebAuthn
- Menggunakan WebAuthn pengalihan dalam sesi browser jarak jauh
- Memecahkan masalah pengalihan WebAuthn

Mengaktifkan WebAuthn pengalihan dalam pengaturan portal

Untuk mengaktifkan WebAuthn pengalihan situs web yang diakses dalam sesi browser jarak jauh, ikuti langkah-langkah ini.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Pilih Browser WorkSpaces Aman, portal Web, pilih portal web Anda, lalu pilih Edit.
3. Arahkan ke bagian Pengaturan pengguna.
4. Di bawah Izin pengguna, setel Izinkan pengguna menggunakan otentikasi lokal di sesi portal mereka ke Diizinkan.
5. Pilih Simpan untuk menerapkan konfigurasi.

Mengkonfigurasi kebijakan browser lokal untuk WebAuthn

Selain mengaktifkan WebAuthn pengalihan di pengaturan portal Anda, kebijakan browser lokal harus dikonfigurasi untuk memungkinkan WebAuthn pengalihan antara perangkat lokal pengguna dan sesi browser jarak jauh dan sebaliknya. Konfigurasi ini biasanya dikelola oleh administrator TI untuk lingkungan perusahaan, atau oleh pengguna individu untuk skenario BYOD.

Kebijakan browser harus menyertakan domain konten Browser WorkSpaces Aman untuk wilayah Anda. Tambahkan asal berikut ke `WebAuthenticationRemoteDesktopAllowedOrigins` kebijakan berdasarkan wilayah Anda:

`https://<region>.content.workspaces-web.com`

Misalnya, di us-west-2: `https://us-west-2.content.workspaces-web.com`

Metode konfigurasi spesifik bergantung pada apakah Anda mengelola browser di lingkungan perusahaan atau mengonfigurasi perangkat individual untuk pengguna BYOD. Untuk informasi selengkapnya tentang kebijakan browser, lihat dokumentasi kebijakan Chrome Enterprise dan dokumentasi kebijakan Microsoft Edge.

> **Note**
>
> Mulai ulang peramban mungkin diperlukan agar kebijakan diterapkan.

Menggunakan WebAuthn pengalihan dalam sesi browser jarak jauh

Setelah WebAuthn pengalihan diaktifkan di pengaturan portal dan kebijakan browser lokal dikonfigurasi, pengguna dapat menggunakan WebAuthn otentikasi pada situs web dalam sesi browser jarak jauh Browser WorkSpaces Aman mereka.

Pengguna dapat mengautentikasi ke situs web menggunakan:

- FIDO2 kunci keamanan yang terhubung ke perangkat lokal mereka
- Kunci Sandi
- Autentikator platform seperti Windows Hello atau Touch ID

Proses WebAuthn otentikasi diteruskan dengan mulus dari sesi browser jarak jauh ke perangkat lokal pengguna, memberikan otentikasi tanpa kata sandi yang aman sambil mempertahankan manfaat keamanan dari lingkungan penjelajahan jarak jauh.

Memecahkan masalah pengalihan WebAuthn

Jika pengguna mengalami masalah dengan WebAuthn pengalihan dalam sesi browser jarak jauh mereka, gunakan langkah-langkah pemecahan masalah berikut untuk mengidentifikasi dan menyelesaikan masalah umum.

Topik

- WebAuthn pengalihan tidak berfungsi
- Pesan kesalahan umum

WebAuthn pengalihan tidak berfungsi

Jika permintaan WebAuthn otentikasi tidak muncul atau gagal berfungsi:

1. Verifikasi WebAuthn diaktifkan di pengaturan portal di bawah Izin pengguna.
2. Periksa apakah kebijakan browser lokal dikonfigurasi dengan benar dengan menavigasi ke `chrome://policy` atau `edge://policy` dan mengonfirmasi `WebAuthenticationRemoteDesktopAllowedOrigins` menyertakan URL konten wilayah Anda.
3. Pastikan versi browser memenuhi persyaratan: Chrome 136+ atau Edge 137+.
4. Uji dengan autentikator yang berbeda (kunci keamanan vs. platform authenticator).

Pesan kesalahan umum

Berikut ini adalah pesan kesalahan umum dan resolusinya:

WebAuthn pesan kesalahan dan resolusi

Pesan kesalahan	Resolusi
WebAuthn Pengalihan Amazon DCV gagal menyelesaikan permintaan pendaftaran: Pengalihan Webauthn tidak didukung oleh klien	Periksa apakah Anda menggunakan browser dan versi yang didukung (Chrome 136+ atau Edge 137+).
Prompt muncul tetapi tidak dapat berinteraksi dengan autentikator lokal	Periksa apakah ekstensi WebAuthn pengalihan Amazon DCV diinstal dan diaktifkan di browser jarak jauh Anda.
WebAuthn Pengalihan Amazon DCV gagal menyelesaikan permintaan pendaftaran: ID pihak yang bergantung bukanlah akhiran domain yang dapat didaftarkan, atau sama dengan domain saat ini. Selanjutnya, upaya untuk mengambil sumber daya.well-known/webauthn dari ID RP yang diklaim gagal.	Ini berarti bahwa kebijakan browser WebAuthenticationRemoteDesktopAllowedOrigins lokal tidak diterapkan. Periksa kebijakan dan perbarui untuk mengizinkan domain konten. Pastikan browser dimulai ulang. Anda mungkin harus memulai sesi baru agar perubahan diterapkan.
Operasi habis waktu atau tidak diizinkan. Lihat: https://www.w3. org/TR/webauthn-2/#sctn-privacy-considerations-client.	Kesalahan ini dapat terjadi jika: (1) Ekstensi WebAuthn pengalihan DCV tidak diinstal atau diaktifkan, (2) Pengguna membatalkan prompt otentikasi, (3) Pengguna memasukkan PIN yang salah untuk kunci keamanan mereka, atau (4) Pengguna tidak berinteraksi dengan prompt dan waktu permintaan habis.

Mengelola kontrol toolbar di Amazon WorkSpaces Secure Browser

Dengan kontrol Toolbar, Anda dapat mengonfigurasi presentasi bilah alat untuk sesi pengguna akhir, termasuk opsi berikut:

- Fitur

- Clipboard: Saat diaktifkan, memungkinkan copy/paste dengan kontrol granular (hanya salin, tempel saja, atau keduanya). Saat dinonaktifkan, menyembunyikan ikon dan mencegah penggunaan dari bilah alat.
- Transfer file: Ketika diaktifkan, memungkinkan operasi file dengan kontrol granular (hanya unggah, unduh saja, atau keduanya). Saat dinonaktifkan, menyembunyikan ikon dan mencegah transfer.
- Mikrofon: Saat diaktifkan, memungkinkan penggunaan mikrofon. Saat dinonaktifkan, menyembunyikan ikon.
- Webcam: Saat diaktifkan, memungkinkan penggunaan kamera. Saat dinonaktifkan, menyembunyikan ikon.
- Monitor ganda: Saat diaktifkan, memungkinkan penggunaan monitor ganda. Saat dinonaktifkan, menyembunyikan ikon.
- Layar penuh: Saat diaktifkan, memungkinkan mode layar penuh. Saat dinonaktifkan, menyembunyikan ikon.
- Windows: Saat diaktifkan, memungkinkan bergerak antar jendela. Saat dinonaktifkan, menyembunyikan ikon.

- Pengaturan
  - Tema bilah alat: Mengontrol tampilan mode terang atau gelap. Konfigurasi menghapus kontrol tema pengguna akhir.
  - Status toolbar: Menetapkan status docked atau terpisah dari toolbar. Konfigurasi menghapus kontrol pengguna akhir atas status bilah alat.
  - Resolusi maks: Mendefinisikan resolusi tampilan tertinggi yang diizinkan. Pengguna hanya dapat memilih resolusi hingga batas yang ditentukan ini.

Mengkonfigurasi domain khusus untuk portal Anda

Anda dapat mengonfigurasi domain khusus untuk portal Browser WorkSpaces Aman untuk mengaktifkan akses melalui nama domain Anda sendiri, bukan URL portal default. Fitur ini memungkinkan Anda untuk memberikan pengalaman yang lebih terintegrasi kepada pengguna menggunakan domain yang selaras dengan branding organisasi Anda.

Ikhtisar

Domain khusus memungkinkan Anda untuk mempersonalisasi aspek-aspek berikut dari pengalaman pengguna:

- Akses portal bermerek - Pengguna mengakses portal Anda melalui domain organisasi Anda, bukan titik akhir AWS default.
- Pengalaman pengguna yang konsisten - Pertahankan konsistensi merek dengan menggunakan nama domain yang sudah dikenal yang selaras dengan organisasi Anda.

> **Note**
>
> Untuk menyesuaikan tampilan visual dan elemen branding portal Anda, lihatthe section called "Penyesuaian branding".

Topik

- Mengkonfigurasi domain khusus untuk portal Anda
- Memecahkan masalah domain kustom

Mengkonfigurasi domain khusus untuk portal Anda

Cara kerjanya

Saat Anda mengonfigurasi domain khusus:

- Anda membuat dan mengonfigurasi proxy terbalik dengan domain kustom Anda untuk merutekan lalu lintas ke titik akhir portal.
- Pengguna mengakses portal Anda melalui domain khusus Anda, bukan titik akhir portal default.
- Sertifikat SSL memastikan koneksi aman selama proses berlangsung.

Prasyarat

Sebelum menyiapkan domain khusus, pastikan Anda memiliki:

- Nama domain yang Anda kelola melalui penyedia layanan DNS seperti Amazon Route53.
- Portal Browser WorkSpaces Aman. Untuk informasi selengkapnya tentang membuat portal, lihatthe section called "Pembuatan portal web".
- Pastikan Anda memiliki izin yang diperlukan untuk mengelola AWS Certificate Manager CloudFront, dan konfigurasi DNS.

> **Important**
>
> Pengguna harus mengaktifkan cookie pihak ketiga untuk domain khusus di browser mereka untuk memastikan fungsionalitas portal yang tepat.
> Pastikan Anda memiliki dan mengelola domain kustom dan catatan DNS-nya dengan benar untuk menjaga keamanan dan fungsionalitas portal Anda.

> **Note**
>
> Untuk mengaktifkan ekstensi masuk tunggal untuk domain khusus, pengguna harus menginstal ekstensi di browser mereka dengan versi yang lebih lambat dari 1.0.2505.6608. Pengguna diminta untuk menginstal ekstensi ketika mereka masuk ke portal. Untuk detail tentang pengalaman pengguna dengan ekstensi, lihatthe section called “Ekstensi masuk tunggal”.

Memulai

Anda dapat mengonfigurasi domain kustom Anda sebagai atribut pengaturan portal baik saat membuat portal baru atau saat mengedit portal yang ada. Ini dapat dilakukan dengan menggunakan perintah AWS Console, SDK, CloudFormation atau AWS CLI.

Sebaiknya siapkan CloudFront distribusi Amazon sebagai proxy terbalik yang merutekan lalu lintas dari domain kustom Anda ke titik akhir portal Browser WorkSpaces Aman.

> **Note**
>
> Meskipun Amazon CloudFront direkomendasikan sebagai solusi proxy terbalik, Anda dapat menggunakan konfigurasi proxy terbalik alternatif. Pastikan Anda memenuhi pengaturan konfigurasi asal dan cache yang diperlukan seperti yang dijelaskan dalam langkah-langkah CloudFront penyiapan Amazon.

Menyiapkan CloudFront sebagai proxy terbalik

Untuk menyelesaikan pengaturan proxy terbalik, Anda perlu:

- Sertifikat SSL melalui AWS Certificate Manager (ACM)

- CloudFront Distribusi Amazon
- Catatan DNS
- Portal dikonfigurasi dengan domain kustom Anda

Sertifikat SSL

Jika Anda belum memilikinya, ikuti langkah-langkah berikut untuk memintanya melalui ACM:

1. Arahkan ke konsol ACM dihttps://console.aws.amazon.com/acm.

   > **Important**
   >
   > Gunakan Wilayah AS Timur (Virginia N.), karena CloudFront memerlukan sertifikat untuk disimpan di sana.

2. Minta sertifikat:

   - Untuk pengguna ACM baru: Pilih Memulai di bawah Sertifikat ketentuan
   - Untuk pengguna ACM yang ada: Pilih Minta sertifikat

3. Pilih Minta sertifikat publik dan kemudian pilih Minta sertifikat.

   > **Note**
   >
   > Anda juga dapat mengimpor sertifikat yang ada. Untuk informasi selengkapnya, lihat Mengimpor sertifikat ke ACM di Panduan Pengguna ACM.

4. Masukkan nama domain utama Anda (misalnya,**`myportal.example.com`**).
5. Pilih metode validasi:

   - Validasi DNS (Direkomendasikan untuk pengguna Route 53) - Memungkinkan pembuatan set rekaman otomatis di zona yang dihosting. Untuk informasi selengkapnya, lihat Validasi DNS di Panduan Pengguna ACM.
   - Validasi Email — Untuk informasi selengkapnya, lihat Validasi email di Panduan Pengguna ACM.

6. Tinjau pengaturan Anda dan pilih Konfirmasi dan minta.

CloudFront distribusi

Buat CloudFront distribusi ke permintaan proxy dari domain kustom Anda ke titik akhir portal.

1. Arahkan ke CloudFront konsol dihttps://console.aws.amazon.com/cloudfront.
2. Pilih Buat Distribusi.
   - Nama distribusi: Masukkan nama untuk distribusi
   - Jenis distribusi: Situs web atau aplikasi tunggal

   > **Note**
   >
   > Jika domain kustom Anda dikelola di Route 53 di akun AWS yang sama, CloudFront dapat secara otomatis mengelola DNS Anda untuk Anda. Masukkan domain khusus Anda dan klik “Periksa domain”. Jika Anda memiliki domain dari penyedia DNS yang berbeda, lewati langkah ini dan konfigurasikan domain Anda nanti.

3. Konfigurasikan pengaturan asal:
   - Tipe Asal: Lain
   - Asal Kustom: Masukkan titik akhir *<portalId>* portal .workspaces-web.com
   - Jalur Asal: Biarkan kosong (default)
4. Sesuaikan pengaturan asal:
   - Tambahkan header kustom

     > **Important**
     >
     > Akses portal melalui domain khusus hanya akan berfungsi jika header ini ada dalam permintaan proksi. Pastikan nama dan nilai header ditentukan persis seperti yang disebutkan.

     - Nama Header: workspacessecurebrowser-custom-domain
     - Nilai: Domain kustom Anda (misalnya,**myportal.example.com**)
   - Protokol: HTTPS saja
   - Port HTTPS: 443 (tetap default)
   - Protokol SSL Asli Minimum: TLSv1 .2 (default)

- Jenis alamat IP asal: IPv4 hanya (Amazon WorkSpaces Secure Browser tidak mendukung IPv6 pada saat menulis panduan administrasi ini.)

5. Sesuaikan pengaturan cache:

   - Kebijakan protokol penampil: Alihkan HTTP ke HTTPS
   - Metode HTTP yang diizinkan: GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
   - Kebijakan Cache: CachingDisabled
   - Kebijakan permintaan asal: AllViewerExceptHostHeader

   > **Important**
   >
   > Akses portal melalui domain khusus hanya akan berfungsi jika kebijakan permintaan asal disetel ke AllViewerExceptHostHeader. Seperti namanya, kebijakan ini hanya menyaring header host dari header permintaan dan meneruskan semua header yang tersisa ke asal.

6. Anda dapat mengonfigurasi WAF jika Anda mau tetapi tidak diperlukan untuk tujuan pengaturan ini.
7. Di Dapatkan sertifikat TLS, pilih Sertifikat TLS yang dibuat di Langkah 1.
8. Tinjau pengaturan dan pilih Buat Distribusi.

Catatan DNS

Cloudfront dapat memperbarui catatan DNS Anda di Route 53 untuk merutekan lalu lintas dari domain yang ditentukan ke distribusi yang dibuat di Langkah 2, jika zona yang dihosting berada di akun AWS yang sama.

1. Arahkan ke CloudFront pengaturan
2. Klik “Rute domain ke CloudFront”
3. Klik “Siapkan perutean secara otomatis”

Jika Anda telah mengonfigurasi DNS untuk domain kustom di penyedia layanan lain atau akun AWS lain, konfigurasikan penyedia DNS Anda untuk merutekan lalu lintas domain Anda ke distribusi. Langkah-langkah berikut menjelaskan cara melakukannya menggunakan Route 53.

1. Buka konsol Amazon Route 53 dihttps://console.aws.amazon.com/route53.

2. Akses manajemen DNS:
   - Jika Anda baru menggunakan Route 53 dengan AWS akun ini, halaman ikhtisar Amazon Route 53 akan terbuka. Di bawah manajemen DNS, pilih Mulai sekarang.
   - Jika Anda telah menggunakan Route 53 sebelumnya dengan AWS akun ini, lanjutkan ke langkah berikutnya.
3. Pada panel navigasi, pilih Zona yang di-hosting.
4. Buat zona yang dihosting jika Anda belum memilikinya:
   - Untuk merutekan lalu lintas internet ke sumber daya Anda, lihat Membuat Zona Hosting Publik di Panduan Pengembang Amazon Route 53.
   - Untuk merutekan lalu lintas di VPC, lihat Membuat Zona Dihosting Pribadi di Panduan Pengembang Amazon Route 53.
5. Pada halaman Zona yang Dihosting, pilih nama zona yang dihosting yang ingin Anda kelola.
6. Pilih Buat Set Catatan.
7. Buat entri untuk domain Anda (misalnya,**`myportal.example.com`**):
   - Tipe: A — IPv4 alamat
   - Alias: Ya
   - Alias Target: URL CloudFront Distribusi

   Simpan nilai default untuk semua pengaturan lainnya.

> **Note**
>
> Jika Anda tidak menggunakan Route 53 untuk mengelola DNS untuk domain Anda, gunakan penyedia layanan DNS Anda dan tambahkan entri DNS yang mengarah ke domain Anda ke URL distribusi Anda. CloudFront

Atau, Anda dapat menggunakan CloudFormation template berikut untuk membuat CloudFront distribusi Anda:

CloudFormation Template ini secara otomatis membuat CloudFront distribusi, mengonfigurasi pengaturan proxy terbalik, dan secara opsional membuat catatan DNS Route53:

Example workspaces-web-custom-domain-template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'CloudFront Distribution for custom domain configuration with existing AWS
 WorkSpaces Secure Browser Portal'

Parameters:
  PortalEndpoint:
    Type: String
    Description: 'The endpoint of your existing WorkSpaces Web Portal (e.g.,
 abc123.workspaces-web.com)'
    AllowedPattern: '^[a-zA-Z0-9-]+(\.[a-zA-Z0-9-]+)?\.workspaces-web\.com$'
    ConstraintDescription: 'Must be a valid WorkSpaces Web portal endpoint'

  CustomDomainName:
    Type: String
    Description: 'Custom domain name for the portal (e.g., myportal.example.com)'
    AllowedPattern: '^([a-zA-Z0-9]?((?!-)([A-Za-z0-9-]*[A-Za-z0-9])\.)+[a-zA-Z0-9]+)$'
    ConstraintDescription: 'Must be a valid domain name'

  CertificateArn:
    Type: String
    Description: 'ARN of the validated SSL certificate in ACM (must be in us-east-1
 region for CloudFront)'
    AllowedPattern: 'arn:aws:acm:us-east-1:[0-9]{12}:certificate/[a-f0-9]{8}-[a-f0-9]
{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}'
    ConstraintDescription: 'Must be a valid ACM certificate ARN in us-east-1 region'

  CreateRoute53Record:
    Type: String
    Description: 'Create Route53 record for custom domain (requires existing hosted
 zone)'
    Default: 'No'
    AllowedValues:
      - 'Yes'
      - 'No'

  HostedZoneId:
    Type: String
    Description: 'Route53 Hosted Zone ID for the custom domain (required if creating
 Route53 record)'
    Default: ''
```

```
Conditions:
  ShouldCreateRoute53Record: !And
    - !Equals [!Ref CreateRoute53Record, 'Yes']
    - !Not [!Equals [!Ref HostedZoneId, '']]

Resources:
  # CloudFront Distribution
  CloudFrontDistribution:
    Type: AWS::CloudFront::Distribution
    Properties:
      DistributionConfig:
        Aliases:
          - !Ref CustomDomainName
        Comment: !Sub 'CloudFront distribution for WorkSpaces Web Portal -
 ${CustomDomainName}'
        Enabled: true
        HttpVersion: http2
        IPV6Enabled: false  # WorkSpaces Secure Browser does not support IPv6
        PriceClass: PriceClass_All

        # Origin Configuration
        Origins:
          - Id: WorkSpacesWebOrigin
            DomainName: !Ref PortalEndpoint
            CustomOriginConfig:
              HTTPSPort: 443
              OriginProtocolPolicy: https-only
              OriginSSLProtocols:
                - TLSv1.2
            OriginCustomHeaders:
              - HeaderName: workspacessecurebrowser-custom-domain
                HeaderValue: !Ref CustomDomainName

        # Default Cache Behavior
        DefaultCacheBehavior:
          TargetOriginId: WorkSpacesWebOrigin
          ViewerProtocolPolicy: https-only
          AllowedMethods:
            - GET
            - HEAD
            - OPTIONS
            - PUT
            - POST
            - PATCH
```

```
            - DELETE
          Compress: false
          # Cache Policy: CachingDisabled (using predefined managed policy)
          CachePolicyId: 4135ea2d-6df8-44a3-9df3-4b5a84be39ad
          # Origin Request Policy: AllViewerExceptHostHeader (using predefined managed
 policy)
          OriginRequestPolicyId: b689b0a8-53d0-40ab-baf2-68738e2966ac

        # SSL Configuration
        ViewerCertificate:
          AcmCertificateArn: !Ref CertificateArn
          SslSupportMethod: sni-only
          MinimumProtocolVersion: TLSv1.2_2021

      Tags:
        - Key: Name
          Value: !Sub '${AWS::StackName}-cloudfront'

  # Route 53 Record (optional - requires hosted zone to exist)
  Route53Record:
    Type: AWS::Route53::RecordSet
    Condition: ShouldCreateRoute53Record
    Properties:
      HostedZoneId: !Ref HostedZoneId
      Name: !Ref CustomDomainName
      Type: A
      AliasTarget:
        DNSName: !GetAtt CloudFrontDistribution.DomainName
        HostedZoneId: Z2FDTNDATAQYW2  # CloudFront Hosted Zone ID
        EvaluateTargetHealth: false

Outputs:
  PortalEndpoint:
    Description: 'WorkSpaces Web Portal endpoint used as origin'
    Value: !Ref PortalEndpoint
    Export:
      Name: !Sub '${AWS::StackName}-PortalEndpoint'

  CustomDomainEndpoint:
    Description: 'Custom domain endpoint for the portal'
    Value: !Sub 'https://${CustomDomainName}'
    Export:
      Name: !Sub '${AWS::StackName}-CustomDomainEndpoint'
```

```
  CloudFrontDistributionId:
    Description: 'CloudFront Distribution ID'
    Value: !Ref CloudFrontDistribution
    Export:
      Name: !Sub '${AWS::StackName}-CloudFrontDistributionId'

  CloudFrontDomainName:
    Description: 'CloudFront Distribution Domain Name'
    Value: !GetAtt CloudFrontDistribution.DomainName
    Export:
      Name: !Sub '${AWS::StackName}-CloudFrontDomainName'

  CertificateArn:
    Description: 'SSL Certificate ARN used by CloudFront'
    Value: !Ref CertificateArn
    Export:
      Name: !Sub '${AWS::StackName}-CertificateArn'

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: "Existing Portal Configuration"
        Parameters:
          - PortalEndpoint
      - Label:
          default: "Custom Domain Configuration"
        Parameters:
          - CustomDomainName
          - CertificateArn
          - CreateRoute53Record
          - HostedZoneId
    ParameterLabels:
      PortalEndpoint:
        default: "Portal Endpoint"
      CustomDomainName:
        default: "Custom Domain Name"
      CertificateArn:
        default: "SSL Certificate ARN"
      CreateRoute53Record:
        default: "Create Route53 Record"
      HostedZoneId:
        default: "Hosted Zone ID"
```

Untuk menggunakan template ini:

1. Simpan template di atas sebagai `workspaces-web-custom-domain-template.yaml`
2. Terapkan menggunakan AWS Konsol, AWS CLI, AWS atau SDK dengan nilai parameter spesifik Anda
3. Setelah penerapan, konfigurasikan portal Anda dengan domain kustom seperti yang dijelaskan pada Langkah 4 di bawah

Konfigurasi portal

Daftarkan domain kustom Anda sebagai atribut pengaturan portal menggunakan perintah AWS CLI AWS Console, UpdatePortal API, atau update-portal.

1. Buka konsol Browser WorkSpaces Aman dihttps://console.aws.amazon.com/workspaces-web/home.
2. Di panel navigasi, pilih Portal Web.
3. Pilih portal web yang ingin Anda konfigurasikan dan pilih Edit.
4. Di pengaturan portal, tambahkan domain khusus Anda.
5. Simpan konfigurasi portal.

Uji konfigurasi Anda

Untuk menguji konfigurasi Anda, ikuti langkah-langkah berikut:

1. Buka browser web dan arahkan ke URL untuk domain kustom Anda (misalnya,**`https://myportal.example.com`**).
2. Jika semuanya diatur dengan benar, Anda akan melihat halaman masuk untuk portal Anda.
3. Selanjutnya, masukkan URL portal di browser Anda, Anda harus diarahkan ke domain khusus setelah masuk ke IDP Anda.
4. Terakhir, masuk ke IDP Anda dan klik ubin aplikasi untuk portal Anda. Anda harus diarahkan ke domain khusus.

Memecahkan masalah domain kustom

Jika pengguna mengalami masalah dengan akses portal melalui domain khusus dalam sesi browser jarak jauh mereka, gunakan langkah-langkah pemecahan masalah berikut untuk mengidentifikasi dan menyelesaikan masalah umum.

Topik

- Pesan kesalahan umum

Pesan kesalahan umum

Berikut ini adalah pesan kesalahan umum dan resolusinya saat menyiapkan domain khusus:

Kesalahan Token CSRF tidak valid

Kesalahan ini terjadi ketika Browser Aman tidak menerima permintaan Anda dengan benar melalui CloudFront pengaturan.

Untuk menyelesaikan masalah ini:

- Periksa pengaturan asal kustom pada CloudFront distribusi Anda.
- Verifikasi bahwa nama header kustom sama persis `workspacessecurebrowser-custom-domain` dan nilainya sama persis dengan domain kustom Anda (tanpa https://atau parameter kueri apa pun).
- Bersihkan cache di browser lokal Anda.
- Membatalkan cache pada. CloudFront

502 Kesalahan Gateway Buruk

Kesalahan ini biasanya menunjukkan masalah konfigurasi cache.

Untuk menyelesaikan masalah ini:

- Periksa pengaturan cache pada CloudFront distribusi Anda.
- Verifikasi bahwa kebijakan Cache disetel ke`CachingDisabled`.
- Verifikasi bahwa kebijakan permintaan Origin disetel ke`AllViewerExceptHostHeader`.
- Bersihkan cache di browser lokal Anda.

- Membatalkan cache pada. CloudFront

Kesalahan Akses Ditolak

Kesalahan ini dapat terjadi jika domain kustom Anda tidak dikonfigurasi dengan benar.

Untuk menyelesaikan masalah ini:

- Periksa pengaturan asal pada CloudFront distribusi Anda.
- Verifikasi bahwa asal diatur ke URL portal yang benar.
- Verifikasi bahwa portal dikonfigurasi dengan domain kustom yang benar.
- Bersihkan cache di browser lokal Anda.
- Membatalkan cache pada. CloudFront

Keamanan di Amazon WorkSpaces Secure Browser

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 menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam 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. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon WorkSpaces Secure Browser, lihat AWS Services in Scope by Compliance Program .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor-faktor lain, termasuk sensitivitas data Anda, persyaratan perusahaan Anda, dan undang-undang dan peraturan yang berlaku yang berlaku untuk data Anda.

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

Konten

- Perlindungan data di Amazon WorkSpaces Secure Browser
- Identity and Access Management untuk Amazon WorkSpaces Secure Browser
- Respons insiden di Amazon WorkSpaces Secure Browser
- Validasi kepatuhan untuk Amazon WorkSpaces Secure Browser
- Ketahanan di Browser Aman Amazon WorkSpaces
- Keamanan infrastruktur di Amazon WorkSpaces Secure Browser
- Analisis konfigurasi dan kerentanan di Amazon WorkSpaces Secure Browser
- Akses APIs menggunakan antarmuka VPC endpoint ()AWS PrivateLink

- Praktik terbaik keamanan untuk Amazon WorkSpaces Secure Browser

Perlindungan data di Amazon WorkSpaces Secure Browser

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon WorkSpaces Secure Browser. 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. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil 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 Browser WorkSpaces Aman atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. 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.

Topik

- Enkripsi data di Amazon WorkSpaces Secure Browser
- Privasi lalu lintas antar jaringan di Amazon Secure Browser WorkSpaces
- Masuk akses pengguna di Amazon WorkSpaces Secure Browser

Enkripsi data di Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser mengumpulkan data kustomisasi portal, seperti pengaturan browser, pengaturan pengguna, pengaturan jaringan, informasi penyedia identitas, data penyimpanan kepercayaan, dan data sertifikat penyimpanan kepercayaan. WorkSpaces Secure Browser juga mengumpulkan data kebijakan browser, preferensi pengguna (untuk pengaturan browser), dan log sesi. Data yang dikumpulkan disimpan di Amazon DynamoDB dan Amazon S3. WorkSpaces Browser Aman digunakan AWS Key Management Service untuk enkripsi.

Untuk mengamankan konten Anda, ikuti panduan ini:

- Terapkan akses hak istimewa paling sedikit dan buat peran khusus yang akan digunakan untuk tindakan Browser WorkSpaces Aman. Gunakan templat IAM untuk membuat peran Akses Penuh atau peran Hanya Baca. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk Browser WorkSpaces Aman.
- Lindungi data dari ujung ke ujung dengan menyediakan kunci yang dikelola pelanggan, sehingga WorkSpaces Secure Browser dapat mengenkripsi data Anda saat istirahat dengan kunci yang Anda berikan.
- Hati-hati dengan berbagi domain portal dan kredensyal pengguna:
  - Admin diminta untuk masuk ke WorkSpaces konsol Amazon, dan pengguna diharuskan masuk ke portal Browser WorkSpaces Aman.
  - Siapa pun di internet dapat mengakses portal web, tetapi mereka tidak dapat memulai sesi kecuali mereka memiliki kredensi pengguna yang valid ke portal.

- Pengguna dapat secara eksplisit mengakhiri sesi mereka dengan memilih End Session. Ini membuang instance yang menghosting sesi browser, dan menghasilkan isolasi browser.

WorkSpaces Secure Browser mengamankan konten dan metadata secara default dengan mengenkripsi semua data sensitif. AWS KMS Ini mengumpulkan kebijakan browser dan preferensi pengguna untuk menegakkan kebijakan dan pengaturan selama sesi Browser WorkSpaces Aman. Jika ada kesalahan saat menerapkan pengaturan yang ada, pengguna tidak dapat mengakses sesi baru dan tidak dapat mengakses situs internal perusahaan dan aplikasi SaaS.

Enkripsi saat istirahat untuk Amazon WorkSpaces Secure Browser

Enkripsi saat istirahat dikonfigurasi secara default dan semua data pelanggan (misalnya, pernyataan kebijakan browser, nama pengguna, logging, atau alamat IP) yang digunakan di Browser WorkSpaces Aman dienkripsi menggunakan. AWS KMS Secara default, WorkSpaces Secure Browser memungkinkan enkripsi dengan kunci yang AWS dimiliki. Anda juga dapat menggunakan Customer Managed Key (CMK) dengan menentukan CMK Anda pada pembuatan sumber daya. Ini saat ini hanya didukung melalui CLI.

Jika Anda memilih untuk meneruskan CMK, kunci yang diberikan harus berupa AWS KMS kunci enkripsi simetris dan Anda, sebagai administrator, harus memiliki izin berikut:

```
kms:DescribeKey

kms:GenerateDataKey

kms:GenerateDataKeyWithoutPlaintext

kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

Jika Anda menggunakan CMK, Anda harus mengizinkan prinsipal layanan eksternal Browser WorkSpaces Aman untuk mengakses kunci tersebut.
Untuk informasi selengkapnya, lihat Contoh Kebijakan Kunci CMK Tercakup dengan aws: SourceAccount

Jika memungkinkan, WorkSpaces Secure Browser akan menggunakan kredensyal Forward Access Sessions (FAS) untuk mengakses kunci Anda. Untuk informasi selengkapnya tentang FAS, lihat Teruskan sesi akses.

Ada kasus di mana Browser WorkSpaces Aman mungkin perlu mengakses kunci Anda secara asinkron. Dengan mengizinkan prinsipal layanan eksternal WorkSpaces Secure Browser dalam kebijakan kunci Anda, WorkSpaces Secure Browser akan dapat melakukan serangkaian operasi kriptografi yang diizinkan dengan kunci Anda.

Setelah sumber daya dibuat, kunci tidak dapat lagi dihapus atau diubah. Jika Anda menggunakan CMK, Anda, sebagai administrator yang mengakses sumber daya, harus memiliki izin berikut:

```
kms:GenerateDataKey
kms:GenerateDataKeyWithoutPlaintext
kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

Jika Anda melihat kesalahan Akses Ditolak saat menggunakan konsol, kemungkinan pengguna yang mengakses konsol tidak memiliki izin yang diperlukan untuk menggunakan CMK pada kunci yang sedang digunakan.

Contoh kebijakan dan pelingkupan utama untuk WorkSpaces Browser Aman

CMKs memerlukan kebijakan kunci berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
```

```
      }
    ]
}
```

Izin berikut diperlukan oleh Browser WorkSpaces Aman:

- `kms:DescribeKey`— Memvalidasi bahwa AWS KMS kunci yang disediakan dikonfigurasi dengan benar.
- `kms:GenerateDataKeyWithoutPlaintext`dan `kms:GenerateDataKey` — Permintaan AWS KMS kunci untuk membuat kunci data yang digunakan untuk mengenkripsi objek.
- `kms:Decrypt`— Meminta AWS KMS kunci untuk mendekripsi kunci data terenkripsi. Kunci data ini digunakan untuk mengenkripsi data Anda.
- `kms:ReEncryptTo`dan `kms:ReEncryptFrom` — Meminta AWS KMS kunci untuk mengizinkan enkripsi ulang dari atau ke kunci KMS.

Mencakup izin Browser WorkSpaces Aman pada kunci Anda AWS KMS

Ketika prinsipal dalam pernyataan kebijakan kunci adalah prinsip AWS layanan, kami sangat menyarankan Anda menggunakan kunci kondisi SourceAccount global aws: SourceArn atau aws:, selain Konteks Enkripsi.

Konteks Enkripsi yang digunakan untuk sumber daya akan selalu berisi entri dalam format `aws:workspaces-web:RESOURCE_TYPE:id` dan ID sumber daya yang sesuai.

Sumber ARN dan nilai akun sumber disertakan dalam konteks otorisasi hanya ketika permintaan datang AWS KMS dari layanan lain. AWS Kombinasi kondisi ini mengimplementasikan izin yang paling tidak memiliki hak istimewa dan menghindari skenario wakil yang berpotensi membingungkan. Untuk informasi selengkapnya, lihat Izin untuk layanan AWS dalam kebijakan utama.

```
  "Condition": {
       "StringEquals": {
         "aws:SourceAccount": "AccountId",
         "kms:EncryptionContext:aws:workspaces-web:resourceType:id": "resourceId"
       },
       "ArnEquals": {
         "aws:SourceArn": [
           "arn:aws:workspaces-web:Region:AccountId:resourceType/resourceId"
         ]
       },
```

```
      }
```

> **Note**
>
> Sebelum pembuatan sumber daya, kebijakan kunci sebaiknya hanya menggunakan `aws:SourceAccount` Condition, karena arn sumber daya lengkap belum ada. Setelah pembuatan sumber daya, kebijakan utama dapat diperbarui untuk menyertakan `aws:SourceArn` dan `kms:EncryptionContext` Ketentuan.

Contoh kebijakan kunci CMK Cakupan dengan **`aws:SourceAccount`**

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "<AccountId>"
        }
      }
    }
  ]
}
```

Contoh kebijakan kunci CMK cakupan dengan **`aws:SourceArn`** dan wildcard sumber daya

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workspaces-web:<Region>:<AccountId>:*/*"
        }
      }
    }
  ]
}
```

Contoh kebijakan kunci CMK tercakup dengan **`aws:SourceArn`**

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
```

```
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:<Region>:<AccountId>:portal/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:browserSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:userSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:ipAccessSettings/*"
          ]
        }
    }
  ]
}
```

> **Note**
>
> Setelah Anda membuat sumber daya, Anda dapat memperbarui wildcard `SourceArn` untuk itu. Jika Anda menggunakan Browser WorkSpaces Aman untuk membuat sumber daya baru yang memerlukan akses CMK, pastikan Anda memperbarui kebijakan utamanya.

Contoh kebijakan kunci CMK tercakup dengan dan spesifik sumber daya **`aws:SourceArn`** **`EncryptionContext`**

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt portal",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
```

```
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:portal:id": "<portalId>>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt userSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:userSetttings:id":
"<userSetttingsId>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt browserSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
```

```
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:browserSettings:id":
 "<browserSettingsId>"
         }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt ipAccessSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:ipAccessSettings:id":
 "<ipAccessSettingsId>"
         }
      }
    },
  ]
}
```

> **Note**
>
> Pastikan Anda membuat pernyataan terpisah saat menyertakan sumber daya spesifik `EncryptionContext` pada kebijakan kunci yang sama. Untuk informasi selengkapnya, lihat bagian Menggunakan beberapa pasangan konteks enkripsi di bawah kms:EncryptionContext: context-key.

Enkripsi dalam perjalanan untuk Amazon WorkSpaces Secure Browser

WorkSpaces Browser Aman mengenkripsi data dalam perjalanan melalui HTTPS dan TLS 1.2. Anda dapat mengirim permintaan WorkSpaces dengan menggunakan konsol atau panggilan API langsung. Data permintaan yang ditransfer dienkripsi dengan mengirimkan semuanya melalui koneksi HTTPS atau TLS. Data permintaan dapat ditransfer dari AWS Konsol, AWS Command Line Interface, atau AWS SDK ke Browser WorkSpaces Aman.

Enkripsi dalam perjalanan dikonfigurasi secara default, dan koneksi aman (HTTPS, TLS) dikonfigurasi secara default.

Manajemen kunci untuk Amazon WorkSpaces Secure Browser

Anda dapat menyediakan Customer Managed AWS KMS Key Anda sendiri untuk mengenkripsi informasi pelanggan Anda. Jika Anda tidak menyediakannya, Browser WorkSpaces Aman akan menggunakan Kunci yang AWS Dimiliki. Anda dapat mengatur kunci Anda menggunakan AWS SDK.

Privasi lalu lintas antar jaringan di Amazon Secure Browser WorkSpaces

Untuk mengamankan koneksi antara WorkSpaces Secure Browser dan aplikasi on-premise, Anda menggunakan WorkSpaces Secure Browser untuk meluncurkan sesi browser di dalam VPC Anda sendiri. Koneksi ke aplikasi on-premise dikonfigurasi di VPC Anda sendiri, dan tidak dikontrol oleh Secure Browser. WorkSpaces

Untuk mengamankan koneksi antar akun, WorkSpaces Secure Browser menggunakan peran terkait layanan untuk terhubung dengan aman ke akun pelanggan dan menjalankan operasi atas nama pelanggan. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Amazon WorkSpaces Secure Browser.

Masuk akses pengguna di Amazon WorkSpaces Secure Browser

Administrator dapat merekam acara sesi Browser WorkSpaces Aman, termasuk mulai, berhenti, dan kunjungan URL. Log ini dienkripsi dan dikirimkan dengan aman ke pelanggan melalui Amazon Kinesis Data Stream. Informasi penjelajahan dari pencatatan akses pengguna tidak disimpan oleh AWS, atau tersedia dari sesi tanpa pencatatan yang dikonfigurasi. Kunjungan URL dalam mode penyamaran, atau dihapus URLs dari riwayat browser, tidak direkam dalam pencatatan akses pengguna.

Identity and Access Management untuk Amazon WorkSpaces Secure Browser

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 diberi wewenang (memiliki izin) untuk menggunakan WorkSpaces sumber daya Browser Aman. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Amazon WorkSpaces Secure Browser bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces
- AWS kebijakan terkelola untuk Browser WorkSpaces Aman
- Memecahkan masalah identitas dan akses Amazon WorkSpaces Secure Browser
- Menggunakan peran terkait layanan untuk Amazon WorkSpaces Secure Browser

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 identitas dan akses Amazon WorkSpaces Secure Browser)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Bagaimana Amazon WorkSpaces Secure Browser bekerja dengan IAM)
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces)

Mengautentikasi dengan identitas

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

Anda dapat masuk sebagai identitas federasi menggunakan kredensional dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensional. 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.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensi dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

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 kredensi 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 melakukan operasinya.

Kebijakan berbasis identitas

Kebijakan berbasis identitas 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.

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya 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.

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

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 (SCPs) — Tentukan 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 (RCPs) — Tetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- 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 WorkSpaces Secure Browser bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Browser WorkSpaces Aman, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Browser WorkSpaces Aman.

Fitur IAM yang dapat Anda gunakan dengan Amazon WorkSpaces Secure Browser

Fitur IAM	WorkSpaces Dukungan Browser Aman
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya
Izin principal	Ya

Fitur IAM	WorkSpaces Dukungan Browser Aman
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Browser WorkSpaces Aman dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Topik

- Kebijakan berbasis identitas untuk Browser Aman WorkSpaces
- Kebijakan berbasis sumber daya dalam Secure Browser WorkSpaces
- Tindakan kebijakan untuk Browser WorkSpaces Aman
- Sumber daya kebijakan untuk Browser WorkSpaces Aman
- Kunci kondisi kebijakan untuk Browser WorkSpaces Aman
- Daftar kontrol akses (ACLs) di Browser WorkSpaces Aman
- Kontrol akses berbasis atribut (ABAC) dengan Browser Aman WorkSpaces
- Menggunakan kredensi sementara dengan WorkSpaces Browser Aman
- Izin utama lintas layanan untuk WorkSpaces Browser Aman
- Peran layanan untuk Browser WorkSpaces Aman
- Peran terkait layanan untuk WorkSpaces Browser Aman

Kebijakan berbasis identitas untuk Browser Aman WorkSpaces

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

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. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Browser Aman WorkSpaces

Untuk melihat contoh kebijakan berbasis identitas Browser WorkSpaces Aman, lihat. Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Kebijakan berbasis sumber daya dalam Secure Browser WorkSpaces

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah 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. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk Browser WorkSpaces Aman

Mendukung tindakan kebijakan: Ya

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.

Untuk melihat daftar tindakan Browser WorkSpaces Aman, lihat Tindakan yang ditentukan oleh Amazon WorkSpaces Secure Browser di Referensi Otorisasi Layanan.

Tindakan kebijakan di Browser WorkSpaces Aman menggunakan awalan berikut sebelum tindakan:

```
workspaces-web
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "workspaces-web:action1",
      "workspaces-web:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Browser WorkSpaces Aman, lihat. Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Sumber daya kebijakan untuk Browser WorkSpaces Aman

Mendukung sumber daya kebijakan: Ya

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": "*"
```

Untuk melihat daftar jenis sumber daya Browser WorkSpaces Aman dan jenisnya ARNs, lihat Sumber daya yang ditentukan oleh Amazon WorkSpaces Secure Browser di Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh Amazon WorkSpaces Secure Browser.

Untuk melihat contoh kebijakan berbasis identitas Browser WorkSpaces Aman, lihat. Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Kunci kondisi kebijakan untuk Browser WorkSpaces Aman

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Browser WorkSpaces Aman, lihat Kunci kondisi untuk Browser WorkSpaces Aman Amazon di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon WorkSpaces Secure Browser.

Untuk melihat contoh kebijakan berbasis identitas Browser WorkSpaces Aman, lihat. Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Daftar kontrol akses (ACLs) di Browser WorkSpaces Aman

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Kontrol akses berbasis atribut (ABAC) dengan Browser Aman WorkSpaces

Mendukung ABAC (tag dalam kebijakan): Sebagian

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut tanda. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

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`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensi sementara dengan WorkSpaces Browser Aman

Mendukung kredensial sementara: Ya

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Izin utama lintas layanan untuk WorkSpaces Browser Aman

Mendukung sesi akses terusan (FAS): Ya

Sesi akses teruskan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

Peran layanan untuk Browser WorkSpaces Aman

Mendukung peran layanan: Tidak

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas Browser WorkSpaces Aman. Edit peran layanan hanya jika Browser WorkSpaces Aman memberikan panduan untuk melakukannya.

Peran terkait layanan untuk WorkSpaces Browser Aman

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Browser WorkSpaces Aman. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Browser WorkSpaces Aman, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk Browser WorkSpaces Aman Amazon di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces
- Menggunakan konsol Amazon WorkSpaces Secure Browser
- Memungkinkan pengguna untuk melihat izin mereka sendiri untuk Amazon WorkSpaces Secure Browser

Praktik terbaik kebijakan berbasis identitas untuk Amazon Secure Browser WorkSpaces

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Browser WorkSpaces Aman 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 konsol Amazon WorkSpaces Secure Browser

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

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

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Browser WorkSpaces Aman, lampirkan juga Browser WorkSpaces Aman `ConsoleAccess` atau kebijakan `ReadOnly` AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Memungkinkan pengguna untuk melihat izin mereka sendiri untuk Amazon WorkSpaces Secure Browser

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:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola untuk Browser WorkSpaces Aman

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 AWS akun 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 dapat menambahkan izin tambahan ke

kebijakan AWS terkelola untuk mendukung 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.

Topik

- AWS kebijakan terkelola: AmazonWorkSpacesWebServiceRolePolicy
- AWS kebijakan terkelola: AmazonWorkSpacesSecureBrowserReadOnly
- AWS kebijakan terkelola: AmazonWorkSpacesWebReadOnly
- WorkSpaces Mengamankan pembaruan Browser ke kebijakan AWS terkelola

AWS kebijakan terkelola: AmazonWorkSpacesWebServiceRolePolicy

Anda tidak dapat melampirkan kebijakan `AmazonWorkSpacesWebServiceRolePolicy` ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Browser WorkSpaces Aman melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat the section called “Menggunakan Peran Terkait Layanan”.

Kebijakan ini memberikan izin administratif yang memungkinkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh Browser WorkSpaces Aman.

Detail izin

Kebijakan ini mencakup izin berikut:

- `workspaces-web`— Memungkinkan akses ke AWS layanan dan sumber daya yang digunakan atau dikelola oleh Browser WorkSpaces Aman.
- `ec2`— Memungkinkan prinsipal untuk mendeskripsikan VPCs, subnet, dan zona ketersediaan; membuat, menandai, mendeskripsikan, dan menghapus antarmuka jaringan; mengaitkan atau memisahkan alamat; dan menjelaskan tabel rute, grup keamanan, dan titik akhir VPC.
- `CloudWatch`— Memungkinkan kepala sekolah untuk menempatkan data metrik.
- `Kinesis`- Memungkinkan prinsipal untuk menjelaskan ringkasan aliran data Kinesis dan memasukkan catatan ke dalam aliran data Kinesis untuk pencatatan akses pengguna. Untuk informasi selengkapnya, lihat the section called “Menyiapkan pencatatan aktivitas pengguna”.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "WorkSpacesWebManaged"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/WorkSpacesWeb",
                        "AWS/Usage"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:PutRecord",
                "kinesis:PutRecords",
                "kinesis:DescribeStreamSummary"
            ],
            "Resource": "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
        }
    ]
}
```

AWS kebijakan terkelola: AmazonWorkSpacesSecureBrowserReadOnly

Anda dapat melampirkan kebijakan `AmazonWorkSpacesSecureBrowserReadOnly` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan akses ke Browser WorkSpaces Aman dan dependensinya melalui AWS Management Console, SDK, dan CLI. Kebijakan ini tidak menyertakan izin yang diperlukan untuk berinteraksi dengan portal yang digunakan `IAM_Identity_Center` sebagai jenis autentikasi. Untuk mendapatkan izin ini, gabungkan kebijakan ini dengan`AWSSSOReadOnly`.

Detail izin

Kebijakan ini mencakup izin berikut.

- `workspaces-web`— Menyediakan akses read-only ke WorkSpaces Secure Browser dan dependensinya melalui AWS Management Console, SDK, dan CLI.

- `ec2`— Memungkinkan kepala sekolah untuk mendeskripsikan VPCs, subnet, dan kelompok keamanan. Ini digunakan di Konsol AWS Manajemen di Browser WorkSpaces Aman untuk menunjukkan kepada Anda VPCs, subnet, dan grup keamanan yang tersedia untuk digunakan dengan layanan.
- `Kinesis`- Memungkinkan kepala sekolah untuk daftar aliran data Kinesis. Ini digunakan di Konsol AWS Manajemen di Browser WorkSpaces Aman untuk menunjukkan aliran data Kinesis yang tersedia untuk digunakan dengan layanan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
```

```
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AmazonWorkSpacesWebReadOnly

Anda dapat melampirkan kebijakan `AmazonWorkSpacesWebReadOnly` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan akses ke Browser WorkSpaces Aman dan dependensinya melalui AWS Management Console, SDK, dan CLI. Kebijakan ini tidak menyertakan izin yang diperlukan untuk berinteraksi dengan portal yang digunakan `IAM_Identity_Center` sebagai jenis autentikasi. Untuk mendapatkan izin ini, gabungkan kebijakan ini dengan`AWSSSOReadOnly`.

> **Note**
>
> Jika saat ini Anda menggunakan kebijakan ini, beralihlah ke `AmazonWorkSpacesSecureBrowserReadOnly` kebijakan baru.

Detail izin

Kebijakan ini mencakup izin berikut.

- `workspaces-web`— Menyediakan akses read-only ke WorkSpaces Secure Browser dan dependensinya melalui AWS Management Console, SDK, dan CLI.
- `ec2`— Memungkinkan kepala sekolah untuk mendeskripsikan VPCs, subnet, dan kelompok keamanan. Ini digunakan di Konsol AWS Manajemen di Browser WorkSpaces Aman untuk menunjukkan kepada Anda VPCs, subnet, dan grup keamanan yang tersedia untuk digunakan dengan layanan.
- `Kinesis`- Memungkinkan kepala sekolah untuk daftar aliran data Kinesis. Ini digunakan di Konsol AWS Manajemen di Browser WorkSpaces Aman untuk menunjukkan aliran data Kinesis yang tersedia untuk digunakan dengan layanan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

WorkSpaces Mengamankan pembaruan Browser ke kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Browser WorkSpaces Aman sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan ke umpan RSS pada halaman Riwayat dokumen.

Perubahan	Deskripsi	Date
AmazonWorkSpacesSecureBrowserReadOnly – Kebijakan baru	WorkSpaces Secure Browser menambahkan kebijakan baru untuk menyediakan akses hanya-baca ke WorkSpaces Secure Browser dan dependensinya melalui AWS Management Console, SDK, dan CLI.	24 Juni 2024
AmazonWorkSpacesWebServiceRolePolicy— Kebijakan yang diperbarui	WorkSpaces Secure Browser memperbarui kebijakan CreateNetworkInterface untuk membatasi tag dengan aws:RequestTag/WorkSpacesWebManaged: true and act on subnet and security group resources, as well as restrict DeleteNetworkInterface to ENIs tagged with aws:ResourceTag/WorkSpacesWebManaged: true.	15 Desember 2022
AmazonWorkSpacesWebReadOnly— Kebijakan yang diperbarui	WorkSpaces Browser Aman memperbarui kebijakan untuk menyertakan izin baca untuk pencatatan akses pengguna dan daftar aliran data Kinesis. Untuk informasi selengkap	2 November 2022

Perubahan	Deskripsi	Date
	nya, lihat the section called “Menyiapkan pencatatan aktivitas pengguna”.	
AmazonWorkSpacesWebServiceRolePolicy— Kebijakan yang diperbarui	WorkSpaces Secure Browser memperbarui kebijakan untuk menjelaskan ringkasan aliran data Kinesis dan memasukkan catatan ke dalam aliran data Kinesis untuk pencatatan akses pengguna. Untuk informasi selengkapnya, lihat the section called “Menyiapkan pencatatan aktivitas pengguna”.	Oktober 17, 2022
AmazonWorkSpacesWebServiceRolePolicy— Kebijakan yang diperbarui	WorkSpaces Secure Browser memperbarui kebijakan untuk membuat tag selama pembuatan ENI.	September 6, 2022
AmazonWorkSpacesWebServiceRolePolicy— Kebijakan yang diperbarui	WorkSpaces Secure Browser memperbarui kebijakan untuk menambahkan AWS/Usage namespace ke izin PutMetricData API.	April 6, 2022
AmazonWorkSpacesWebReadOnly – Kebijakan baru	WorkSpaces Secure Browser menambahkan kebijakan baru untuk menyediakan akses hanya-baca ke WorkSpaces Secure Browser dan dependensinya melalui AWS Management Console, SDK, dan CLI.	30 November 2021

Perubahan	Deskripsi	Date
AmazonWorkSpacesWebServiceRolePolicy – Kebijakan baru	WorkSpaces Secure Browser menambahkan kebijakan baru untuk mengizinkan akses ke layanan AWS dan sumber daya yang digunakan atau dikelola oleh WorkSpaces Secure Browser.	30 November 2021
WorkSpaces Browser Aman mulai melacak perubahan	WorkSpaces Browser Aman mulai melacak perubahan untuk kebijakan yang AWS dikelola.	30 November 2021

Memecahkan masalah identitas dan akses Amazon WorkSpaces Secure Browser

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan WorkSpaces Secure Browser dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Browser WorkSpaces Aman
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses sumber daya Browser WorkSpaces Aman saya

Saya tidak berwenang untuk melakukan tindakan di Browser WorkSpaces Aman

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `workspaces-web:`*`GetWidget`* rekaan.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-web:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `workspaces-web:`*`GetWidget`*.

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

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 Browser WorkSpaces Aman.

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 Browser WorkSpaces Aman. 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 AWS akun saya untuk mengakses sumber daya Browser WorkSpaces Aman 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 (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Browser WorkSpaces Aman mendukung fitur-fitur ini, lihatBagaimana Amazon WorkSpaces Secure Browser 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.

Menggunakan peran terkait layanan untuk Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke WorkSpaces Browser Aman. Peran terkait layanan telah ditentukan sebelumnya oleh Browser WorkSpaces Aman dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Browser WorkSpaces Aman lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. WorkSpaces Secure Browser mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya WorkSpaces Secure Browser yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan izin. Kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah terlebih dahulu menghapus sumber dayanya yang terkait. Ini melindungi sumber daya Browser WorkSpaces Aman 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 bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Topik

- Izin peran terkait layanan untuk Browser Aman WorkSpaces
- Membuat peran terkait layanan untuk WorkSpaces Browser Aman
- Mengedit peran terkait layanan untuk WorkSpaces Browser Aman
- Menghapus peran terkait layanan untuk Browser Aman WorkSpaces
- Wilayah yang didukung untuk peran WorkSpaces terkait layanan Browser Aman

Izin peran terkait layanan untuk Browser Aman WorkSpaces

WorkSpaces Secure Browser menggunakan peran terkait layanan bernama `AWSServiceRoleForAmazonWorkSpacesWeb` — WorkSpaces Secure Browser menggunakan peran terkait layanan ini untuk mengakses sumber daya Amazon EC2 dari akun pelanggan untuk streaming instans dan metrik. CloudWatch

Peran tertaut layanan `AWSServiceRoleForAmazonWorkSpacesWeb` memercayai layanan berikut untuk mengambil peran tersebut:

- `workspaces-web.amazonaws.com`

Kebijakan izin peran bernama `AmazonWorkSpacesWebServiceRolePolicy` memungkinkan Browser WorkSpaces Aman untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan. Untuk informasi selengkapnya, lihat the section called “AmazonWorkSpacesWebServiceRolePolicy”.

- Tindakan: `ec2:DescribeVpcs` pada `all AWS resources`
- Tindakan: `ec2:DescribeSubnets` pada `all AWS resources`
- Tindakan: `ec2:DescribeAvailabilityZones` pada `all AWS resources`
- Tindakan: `ec2:CreateNetworkInterface` dengan `aws:RequestTag/WorkSpacesWebManaged: true` sumber daya subnet dan grup keamanan
- Tindakan: `ec2:DescribeNetworkInterfaces` pada `all AWS resources`

- Tindakan: `ec2:DeleteNetworkInterface` pada antarmuka jaringan dengan `aws:ResourceTag/WorkSpacesWebManaged: true`
- Tindakan: `ec2:DescribeSubnets` pada `all AWS resources`
- Tindakan: `ec2:AssociateAddress` pada `all AWS resources`
- Tindakan: `ec2:DisassociateAddress` pada `all AWS resources`
- Tindakan: `ec2:DescribeRouteTables` pada `all AWS resources`
- Tindakan: `ec2:DescribeSecurityGroups` pada `all AWS resources`
- Tindakan: `ec2:DescribeVpcEndpoints` pada `all AWS resources`
- Tindakan: `ec2:CreateTags` pada `ec2:CreateNetworkInterface` Operasi dengan `aws:TagKeys: ["WorkSpacesWebManaged"]`
- Tindakan: `cloudwatch:PutMetricData` pada `all AWS resources`
- Tindakan: `kinesis:PutRecord` pada aliran data Kinesis dengan nama yang dimulai dengan `amazon-workspaces-web-`
- Tindakan: `kinesis:PutRecords` pada aliran data Kinesis dengan nama yang dimulai dengan `amazon-workspaces-web-`
- Tindakan: `kinesis:DescribeStreamSummary` pada aliran data Kinesis dengan nama yang dimulai dengan `amazon-workspaces-web-`

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, silakan lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk WorkSpaces Browser Aman

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat portal pertama di, API Konsol Manajemen AWS, atau AWS API AWS CLI, WorkSpaces Secure Browser akan membuat peran terkait layanan untuk Anda.

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini.

Jika Anda menghapus peran terkait layanan ini dan kemudian perlu membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran di akun Anda. Saat Anda membuat portal pertama, WorkSpaces Secure Browser akan membuat peran terkait layanan untuk Anda lagi.

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaan Browser WorkSpaces Aman. Di AWS CLI atau AWS API, buat peran terkait layanan dengan nama `workspaces-web.amazonaws.com` layanan. Untuk informasi lebih lanjut, lihat Membuat Peran yang Terhubung dengan Layanan di Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Mengedit peran terkait layanan untuk WorkSpaces Browser Aman

WorkSpaces Browser Aman tidak memungkinkan Anda mengedit peran `AWSServiceRoleForAmazonWorkSpacesWeb` 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 Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Browser Aman WorkSpaces

Jika Anda tidak lagi perlu menggunakan fitur atau layanan yang memerlukan peran tertaut 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 layanan Browser WorkSpaces Aman 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 sumber daya Browser WorkSpaces Aman yang digunakan oleh AWSService RoleForAmazonWorkSpacesWeb

- Pilih dari salah satu opsi berikut:
  - Jika Anda menggunakan konsol, hapus semua portal Anda di konsol.

- Jika Anda menggunakan CLI atau API, lepaskan semua sumber daya Anda (termasuk pengaturan browser, pengaturan jaringan, pengaturan pengguna, penyimpanan kepercayaan, dan pengaturan pencatatan akses pengguna) dari portal Anda, hapus sumber daya ini, lalu hapus portal.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSService RoleForAmazonWorkSpacesWeb terkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang didukung untuk peran WorkSpaces terkait layanan Browser Aman

WorkSpaces Secure Browser mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat Wilayah dan Titik Akhir AWS.

Respons insiden di Amazon WorkSpaces Secure Browser

Anda dapat mendeteksi insiden dengan memantau CloudWatch metrik `SessionFailure` Amazon. Untuk menerima peringatan untuk insiden, gunakan CloudWatch alarm untuk metrik. `SessionFailure` Untuk informasi selengkapnya, lihat Memantau Browser WorkSpaces Aman Amazon dengan Amazon CloudWatch.

Validasi kepatuhan untuk Amazon WorkSpaces Secure Browser

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program 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 Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat Dokumentasi AWS Keamanan.

Ketahanan di Browser Aman Amazon WorkSpaces

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS 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 serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Berikut ini saat ini tidak didukung oleh Browser WorkSpaces Aman:

- Mencadangkan konten di seluruh AZs atau wilayah
- Cadangan terenkripsi
- Mengenkripsi konten dalam perjalanan antar atau wilayah AZs
- Pencadangan default atau otomatis

Untuk mengonfigurasi ketersediaan internet yang tinggi, Anda dapat menyetel konfigurasi VPC Anda. Untuk ketersediaan API yang tinggi, Anda dapat meminta jumlah TPS yang tepat.

Keamanan infrastruktur di Amazon WorkSpaces Secure Browser

Sebagai layanan terkelola, Amazon WorkSpaces Secure Browser 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 WorkSpaces Secure Browser melalui jaringan. Klien harus mendukung hal-hal berikut:

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

WorkSpaces Browser Aman mengisolasi lalu lintas layanan dengan menerapkan Otentikasi dan Otorisasi AWS SigV4 Standar ke semua layanan. Titik akhir sumber daya pelanggan (atau titik akhir portal web) dilindungi oleh penyedia identitas Anda. Anda dapat mengisolasi lalu lintas lebih lanjut dengan menggunakan Otorisasi Multi-faktor dan mekanisme keamanan lainnya di penyedia identitas Anda (IDP).

Semua akses internet dapat dikontrol dengan mengkonfigurasi pengaturan jaringan, seperti VPC, subnet, atau grup keamanan. Multi-tenancy dan titik akhir VPC (PrivateLink) saat ini tidak didukung.

Analisis konfigurasi dan kerentanan di Amazon WorkSpaces Secure Browser

WorkSpaces Pembaruan Browser Aman dan tambalan aplikasi dan platform sesuai kebutuhan atas nama Anda, termasuk Chrome dan Linux. Anda tidak diharuskan untuk menambal atau membangun kembali. Namun, Anda bertanggung jawab untuk mengonfigurasi Browser WorkSpaces Aman sesuai dengan spesifikasi dan pedoman, dan untuk memantau penggunaan Browser WorkSpaces Aman oleh pengguna Anda. Semua konfigurasi terkait layanan dan analisis kerentanan adalah tanggung jawab Secure Browser. WorkSpaces

Anda dapat meminta peningkatan batas untuk sumber daya Browser WorkSpaces Aman, seperti jumlah portal web dan jumlah pengguna. WorkSpaces Browser Aman memastikan ketersediaan layanan dan SLA.

Akses APIs menggunakan antarmuka VPC endpoint ()AWS PrivateLink

Anda dapat langsung memanggil titik akhir Amazon WorkSpaces Secure Browser API dari dalam cloud pribadi (VPC), alih-alih terhubung melalui internet. Anda dapat melakukan ini tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau Direct Connect koneksi.

Anda membuat koneksi pribadi ini dengan membuat titik akhir VPC antarmuka yang didukung oleh. AWS PrivateLink Untuk setiap subnet yang Anda tentukan dari VPC Anda, kami membuat antarmuka jaringan endpoint di subnet. Antarmuka jaringan endpoint adalah antarmuka jaringan yang dikelola pemohon yang berfungsi sebagai titik masuk untuk lalu lintas API Amazon WorkSpaces Secure Browser.

Untuk informasi selengkapnya, lihat Akses AWS layanan melalui AWS PrivateLink.

Topik

- Pertimbangan untuk Amazon WorkSpaces Secure Browser
- Membuat titik akhir VPC antarmuka untuk Amazon Secure Browser WorkSpaces
- Membuat kebijakan endpoint untuk titik akhir VPC antarmuka Anda
- Pemecahan masalah

Pertimbangan untuk Amazon WorkSpaces Secure Browser

Sebelum Anda menyiapkan titik akhir VPC antarmuka untuk Amazon WorkSpaces Secure Browser APIs, pastikan untuk meninjau “Prasyarat” di layanan Access melalui. AWSAWS PrivateLink Amazon WorkSpaces Secure Browser mendukung panggilan ke semua tindakan API-nya melalui titik akhir VPC antarmuka.

Secara default, akses penuh ke Amazon WorkSpaces Secure Browser diizinkan melalui titik akhir. Untuk informasi selengkapnya, lihat Mengontrol Akses ke Layanan dengan titik akhir VPC dalam Panduan Pengguna Amazon VPC.

Membuat titik akhir VPC antarmuka untuk Amazon Secure Browser WorkSpaces

Anda dapat membuat titik akhir VPC antarmuka untuk layanan Amazon WorkSpaces Secure Browser menggunakan konsol VPC Amazon atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka dalam Panduan Pengguna Amazon VPC.

Buat titik akhir VPC antarmuka untuk Amazon WorkSpaces Secure Browser menggunakan nama layanan berikut:

- com.amazonaws. *region*.workspace-web

Untuk wilayah yang didukung FIPS, buat titik akhir VPC antarmuka untuk WorkSpaces Amazon Secure Browser menggunakan nama layanan berikut:

- com.amazonaws. *region*. workspaces-web-fips

Membuat kebijakan endpoint untuk titik akhir VPC antarmuka Anda

Kebijakan endpoint adalah sumber daya IAM yang dapat Anda lampirkan ke titik akhir VPC antarmuka. Kebijakan endpoint default memberi Anda akses penuh ke Amazon WorkSpaces Secure Browser APIs melalui titik akhir VPC antarmuka. Untuk mengontrol akses yang diberikan ke Amazon WorkSpaces Secure Browser dari VPC Anda, lampirkan kebijakan endpoint khusus ke titik akhir VPC antarmuka.

kebijakan titik akhir mencantumkan informasi berikut:

- Prinsipal yang dapat melakukan tindakan (Akun AWS, pengguna IAM, dan peran IAM).
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat Mengontrol Akses ke Layanan dengan titik akhir VPC dalam Panduan Pengguna Amazon VPC.

Contoh: Kebijakan titik akhir VPC untuk tindakan Amazon WorkSpaces Secure Browser

Berikut ini adalah contoh kebijakan endpoint kustom. Saat Anda melampirkan kebijakan ini ke titik akhir VPC antarmuka Anda, kebijakan ini memberikan akses ke tindakan Amazon WorkSpaces Secure Browser yang terdaftar untuk semua prinsipal di semua sumber daya.

```
{
    "Statement": [
        {
            "Action": "workspaces-web:*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        }
    ]
}
```

Pemecahan masalah

Jika panggilan Anda ke Amazon WorkSpaces Secure Browser APIs macet, kemungkinan ada kesalahan konfigurasi di grup keamanan Layanan VPC Endpoint Service atau pengaturan peran IAM. Untuk mengatasi ini, coba yang berikut ini:

- Saat membuat titik akhir VPC antarmuka Anda, itu mungkin secara otomatis terpasang ke grup keamanan default Anda Akun AWS. Coba gunakan grup keamanan yang berbeda, dan pastikan izin masuk dan keluar memungkinkan Anda mentransfer data dengan tepat.
- Pastikan Anda menggunakan peran IAM yang memungkinkan Anda memanggil Amazon WorkSpaces Secure Browser APIs.

Untuk informasi lebih lanjut, lihat Apa itu AWS PrivateLink? di Panduan Pengguna Amazon VPC.

Praktik terbaik keamanan untuk Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser menyediakan sejumlah fitur keamanan yang dapat Anda gunakan saat mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

Praktik terbaik untuk Amazon WorkSpaces Secure Browser mencakup hal-hal berikut:

- Untuk mendeteksi potensi peristiwa keamanan yang terkait dengan penggunaan Browser WorkSpaces Aman, gunakan AWS CloudTrail atau Amazon CloudWatch untuk mendeteksi dan melacak riwayat akses dan log proses. Untuk informasi selengkapnya, silakan lihat Memantau Browser WorkSpaces Aman Amazon dengan Amazon CloudWatch dan Mencatat panggilan API Browser WorkSpaces Aman menggunakan AWS CloudTrail.
- Untuk menerapkan kontrol detektif dan mengidentifikasi anomali, gunakan CloudTrail log dan metrik. CloudWatch Untuk informasi selengkapnya, silakan lihat Memantau Browser WorkSpaces Aman Amazon dengan Amazon CloudWatch dan Mencatat panggilan API Browser WorkSpaces Aman menggunakan AWS CloudTrail.
- Anda dapat mengatur pencatatan akses pengguna untuk merekam peristiwa pengguna. Untuk informasi selengkapnya, lihat the section called “Menyiapkan pencatatan aktivitas pengguna”.

Untuk mencegah potensi peristiwa keamanan yang terkait dengan penggunaan Browser WorkSpaces Aman oleh Anda, ikuti praktik terbaik berikut ini:

- Terapkan akses hak istimewa paling sedikit dan buat peran khusus yang akan digunakan untuk tindakan Browser WorkSpaces Aman. Gunakan templat IAM untuk membuat peran Akses Penuh

atau Hanya Baca. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk Browser WorkSpaces Aman.

- Hati-hati dengan berbagi domain portal dan kredensi pengguna. Siapa pun di internet dapat mengakses portal web, tetapi mereka tidak dapat memulai sesi kecuali mereka memiliki kredensi pengguna yang valid ke portal. Berhati-hatilah tentang bagaimana, kapan, dan kepada siapa Anda berbagi kredensi portal web.

Memantau Peramban WorkSpaces Aman Amazon

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Amazon WorkSpaces Secure Browser dan AWS solusi Anda lainnya. AWS menyediakan alat pemantauan berikut untuk menonton portal Browser WorkSpaces Aman Anda dan sumber dayanya, 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. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan menyetel alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat CloudWatch melacak penggunaan CPU atau metrik lain untuk EC2 instans Amazon Anda dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.
- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses file log Anda dari EC2 instans Amazon CloudTrail, dan sumber lainnya. CloudWatch Log dapat memantau informasi dalam file log dan memberi tahu Anda ketika ambang batas tertentu terpenuhi. Anda juga dapat mengarsipkan data log dalam penyimpanan yang sangat durabel. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon CloudWatch Logs.
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda 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, silakan lihat Panduan Pengguna AWS CloudTrail.

Topik

- Memantau Browser WorkSpaces Aman Amazon dengan Amazon CloudWatch
- Mencatat panggilan API Browser WorkSpaces Aman menggunakan AWS CloudTrail
- Login aktivitas pengguna di Amazon WorkSpaces Secure Browser

Memantau Browser WorkSpaces Aman Amazon dengan Amazon CloudWatch

Anda dapat memantau Amazon WorkSpaces Secure Browser menggunakan CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca, mendekati real-time. Statistik ini disimpan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa 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.

Namespace `AWS/WorkSpacesWeb` mencakup metrik berikut.

CloudWatch metrik untuk Amazon WorkSpaces Secure Browser

Metrik	Deskripsi	Dimensi	Statistik	Unit
`SessionAttempt`	Jumlah upaya sesi Amazon WorkSpaces Secure Browser.	`[PortalId]`	Rata-rata, Jumlah, Maksimum, Minimum	Hitungan
`SessionSuccess`	Jumlah sesi Amazon WorkSpaces Secure Browser yang sukses dimulai.	`[PortalId]`	Rata-rata, Jumlah, Maksimum, Minimum	Hitungan
`SessionFailure`	Jumlah sesi Amazon WorkSpaces Secure Browser yang gagal dimulai.	`[PortalId]`	Rata-rata, Jumlah, Maksimum, Minimum	Hitungan

Metrik	Deskripsi	Dimensi	Statistik	Unit
`SessionIdleDisconnect`	Jumlah koneksi yang ditutup karena pengguna tidak aktif.	`[PortalId]`	Rata-rata	Hitungan
`ActiveSession`	Jumlah sesi aktif di portal.	`[PortalId]`	Rata-rata	Hitungan
`GlobalCpuPercent`	Penggunaan CPU dari instance sesi Amazon WorkSpaces Secure Browser.	`[PortalId]` `[PortalId, UserName]`	Rata-rata, Jumlah, Maksimum, Minimum	Persen
`GlobalMemoryPercent`	Penggunaan memori (RAM) dari instance sesi Amazon WorkSpaces Secure Browser.	`[PortalId]` `[PortalId, UserName]`	Rata-rata, Jumlah, Maksimum, Minimum	Persen
`DisplayLatency`	Waktu rata-rata dalam milidetik antara frame capture dan presentasi.	`[PortalId]` `[PortalId, UserName]`	Rata-rata, Maksimum, Minimum	Milidetik
`InputLatency`	Latensi input antara klien dan server. Misalnya, latensi antara klik mouse klien dan klik mouse server.	`[PortalId]` `[PortalId, UserName]`	Rata-rata, Maksimum, Minimum	Milidetik

Metrik	Deskripsi	Dimensi	Statistik	Unit
`SessionLoggerEventDelivered`	Jumlah acara yang dimiliki setiap file Session Logger yang dikirimkan.	`[PortalId]`	Rata-rata, Jumlah, Maksimum, Minimum	Hitungan
`SessionLoggerTargetNotFoundError`	Jumlah pengiriman file log yang mengakibatkan bucket tidak ditemukan.	`[PortalId]`	Rata-rata, Jumlah, Maksimum, Minimum	Hitungan
`SessionLoggerAccessDeniedError`	Jumlah pengiriman file log yang mengakibatkan izin ditolak.	`[PortalId]`	Rata-rata, Jumlah, Maksimum, Minimum	Hitungan

> **Note**
>
> Titik data metrik dikumpulkan oleh setiap sesi sekali per menit dan dipublikasikan setiap 5 menit CloudWatch sekali. Metrik Session Logger segera dipancarkan, untuk setiap pengiriman File Log.

Dimensi untuk metrik Amazon WorkSpaces Secure Browser

Dimensi	Deskripsi
PortalId	Memfilter data metrik untuk Amazon WorkSpaces Secure Browser untuk portal tertentu.

Dimensi	Deskripsi
UserName	Memfilter data metrik untuk Amazon WorkSpaces Secure Browser untuk portal dan pengguna tertentu.

Anda dapat menggunakan SessionLoggerEventDeliveredmetrik untuk memantau jumlah agregat peristiwa dari portal Anda, atau melihat jumlah file log yang dikirimkan dengan menghitung jumlah titik data daripada menjumlahkan nilai. Sebaiknya konfigurasi alarm pada SessionLoggerAccessDeniedErrormetrik SessionLoggerTargetNotFoundErrordan untuk mendeteksi penghapusan sumber daya atau izin yang tidak disengaja.

Mencatat panggilan API Browser WorkSpaces Aman menggunakan AWS CloudTrail

WorkSpaces Secure Browser terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon WorkSpaces Secure Browser. CloudTrail menangkap semua panggilan API untuk Amazon WorkSpaces Secure Browser sebagai peristiwa. Ini termasuk panggilan dari konsol Amazon WorkSpaces Secure Browser dan panggilan kode ke operasi Amazon WorkSpaces Secure Browser API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Amazon WorkSpaces Secure Browser. 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 mengidentifikasi permintaan yang dibuat ke Amazon WorkSpaces Secure Browser, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, serta detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Topik

- WorkSpaces Amankan informasi Browser di CloudTrail
- Memahami entri file log Browser WorkSpaces Aman

WorkSpaces Amankan informasi Browser di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Saat aktivitas terjadi di Amazon WorkSpaces Secure Browser, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Dalam riwayat acara, Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Amazon WorkSpaces Secure Browser, Anda dapat membuat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi 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 selengkapnya, lihat berikut:

- Gambaran umum 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 tindakan Amazon WorkSpaces Secure Browser dicatat oleh CloudTrail dan didokumentasikan dalam Referensi WorkSpaces API Amazon. Misalnya, panggilan ke`CreatePortal`, `DeleteUserSettings` dan `ListBrowserSettings` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang siapa 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 log Browser WorkSpaces Aman

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. Peristiwa mewakili permintaan tunggal dari sumber mana pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan detail lainnya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `ListBrowserSettings` tindakan.


```
{
   "Records": [{
       "eventVersion": "1.08",
       "userIdentity": {
           "type": "IAMUser",
           "principalId": "111122223333",
           "arn": "arn:aws:iam::111122223333:user/myUserName",
           "accountId": "111122223333",
           "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
           "userName": "myUserName"
       },
       "eventTime": "2021-11-17T23:44:51Z",
       "eventSource": "workspaces-web.amazonaws.com",
       "eventName": "ListBrowserSettings",
       "awsRegion": "us-west-2",
       "sourceIPAddress": "127.0.0.1",
       "userAgent": "[]",
       "requestParameters": null,
       "responseElements": null,
       "requestID": "159d5c4f-c8c8-41f1-9aee-b5b1b632e8b2",
       "eventID": "d8237248-0090-4c1e-b8f0-a6e8b18d63cb",
       "readOnly": true,
       "eventType": "AwsApiCall",
       "managementEvent": true,
       "recipientAccountId": "111122223333",
       "eventCategory": "Management"
   },
   {
       "eventVersion": "1.08",
```

```
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2021-11-17T23:55:51Z",
        "eventSource": "workspaces-web.amazonaws.com",
        "eventName": "CreateUserSettings",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "5127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "clientToken": "some-token",
            "copyAllowed": "Enabled",
            "downloadAllowed": "Enabled",
            "pasteAllowed": "Enabled",
            "printAllowed": "Enabled",
            "uploadAllowed": "Enabled"
        },
        "responseElements": "arn:aws:workspaces-web:us-
west-2:111122223333:userSettings/04a35a2d-f7f9-4b22-af08-8ec72da9c2e2",
        "requestID": "6a4aa162-7c1b-4cf9-a7ac-e0c8c4622117",
        "eventID": "56f1fbee-6a1d-4fc6-bf35-a3a71f016fcb",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    }]
}
```


Login aktivitas pengguna di Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser memungkinkan pelanggan untuk mencatat peristiwa sesi yang terkait dengan aktivitas pengguna di sesi browser Aman.

WorkSpaces Secure Browser menawarkan dua opsi untuk mencatat aktivitas pengguna dan peristiwa terkait keamanan:

- Session Logger menangkap berbagai acara sesi. Log ini dikirimkan ke bucket Amazon S3 di akun Anda, memungkinkan integrasi yang mudah dengan platform SIEM pilihan Anda.
- User Access Logging menangkap peristiwa sesi yang paling penting. Log ini dialirkan ke aliran Amazon Kinesis untuk pemrosesan dan analisis waktu nyata.

Untuk informasi selengkapnya tentang cara mengatur opsi ini, lihat the section called “Menyiapkan Session Logger” danthe section called “Menyiapkan pencatatan Akses Pengguna”.

Topik

- Acara sesi di Session Logger untuk Amazon WorkSpaces Secure Browser
- Peristiwa sesi dalam pencatatan Akses Pengguna untuk Amazon WorkSpaces Secure Browser

Acara sesi di Session Logger untuk Amazon WorkSpaces Secure Browser

Session Logger menangkap berbagai acara terkait sesi untuk tujuan pemantauan dan audit.

Anda dapat mengonfigurasi Session Logger untuk mengumpulkan semua acara sesi atau subset yang dipilih, tergantung pada kebutuhan portal Browser WorkSpaces Aman. Untuk informasi selengkapnya tentang konfigurasi, lihatthe section called “Menyiapkan Session Logger”.

Untuk menjaga privasi pengguna, Session Logger tidak merekam konten sensitif, seperti data clipboard, atau konten file yang diunggah atau diunduh.

Bidang berikut termasuk dalam semua acara:

- Waktu
- Nama Pengguna
- ID Portal
- Portal IP
- IP Klien
- ID Sesi

Nama	Penjelasan	Bidang tambahan termasuk dalam acara
SessionStart	Sesi browser aman diluncurkan, tetapi pengguna belum terhubung.	
SessionConnect	Pengguna terhubung ke sesi browser aman.	
TabOpen	Dalam sesi browser aman mereka, pengguna membuka tab baru, atau mereka membuka tautan di tab baru.	Nama host, jalur, URL (jika pengguna membuka tautan di tab baru), tidak ada (jika pengguna membuka tab baru)
UrlVisit	Dalam sesi browser mereka, pengguna menavigasi ke URL.	Nama host, jalur, URL
WebsiteInteract	Pengguna mengubah elemen HTML standar di situs web (misalnya, mengklik kotak centang, tombol radio, atau tombol, atau memilih item di drop-down).	Nama host, jalur, URL
TabClose	Dalam sesi browser mereka, pengguna menutup tab.	Nama host, jalur, URL (jika pengguna menutup tab yang mereka navigasikan), tidak ada (jika pengguna menutup tab baru)
ContentTransferFromLocalToRemoteClipboard	Pengguna memperbarui clipboard dalam browser aman menggunakan konten dari browser lokal mereka (di luar lingkungan yang aman). Pembaruan ini dapat terjadi baik dengan menyalin konten	

Nama	Penjelasan	Bidang tambahan termasuk dalam acara
	melalui toolbar dalam sesi atau dengan mentransfer data melalui pintasan keyboard (Ctrl+C/ Ctrl+V).	
ContentCopyFromWebsite	Pengguna memperbarui clipboard dalam browser aman menggunakan konten dari browser aman (di dalam lingkungan yang aman).	Nama host, jalur, URL
ContentPasteToWebsite	Konten clipboard disisipkan ke halaman web di dalam browser. (Peristiwa ini tidak menangkap contoh di mana konten clipboard ditempelkan ke bilah URL browser.)	Nama host, jalur, URL
PrintJobSubmit	Pengguna mengirimkan pekerjaan permintaan ke printer virtual browser (“Printer DCV”). Konten disimpan sebagai PDF di mesin lokal pengguna.	Nama file, ukuran, ekstensi
FileDownloadFromSecureBrowserToRemoteDisk	Sebuah file disimpan dari sesi ke disk lokal instans jarak jauh.	Nama host, jalur, URLfilename, ukuran, ekstensi
FileTransferFromRemoteToLocalDisk	File diunduh dari disk instans jarak jauh ke perangkat lokal pengguna.	Nama file, ukuran, ekstensi

Nama	Penjelasan	Bidang tambahan termasuk dalam acara
FileUploadFromRemoteDiskToSecureBrowser	File yang disimpan di disk lokal instans jarak jauh diunggah ke platform SaaS berbagi file (misalnya, Google Drive, Box, atau File.io) melalui sesi browser.	
FileTransferFromLocalToRemoteDisk	File diunggah dari perangkat pengguna ke sesi browser aman.	Nama file, ukuran, dan ekstensi
SessionDisconnection	Pengguna terputus dari sesi browser aman.	
SessionEnd	Sesi browser aman telah dihentikan. Pengakhiran dapat terjadi dengan salah satu dari tiga cara: administrator mengakhiri sesi melalui Pengelola Sesi Pengguna di konsol, pengguna secara manual mengakhiri sesi menggunakan Sesi Akhir di bilah alat, atau waktu sesi habis setelah melebihi durasi yang ditetapkan oleh administrator.	

Setiap acara mengikuti standar OCSF dan menyertakan daftar atribut yang umum untuk semua acara:

```
{
    activity_name : String | A human readable name of the event | eg. UrlLoad
```

```
   activity_id : Integer | OCSF standard value 99 for 'others'
   category_name : "WorkSpacesSecureBrowser" | The category name where the event
belongs to.
   category_id : 2 | Numerical identifier for category,
   metadata : link | Required {
       product : link {
           vendor_name : "wsb",
           name : "WorkSpacesSecureBrowser"
       }
       version : String | Version of the schema | eg. 1.0.0
   },
   severity_id : 1 | The severity of the event. All events will have a severity of 1,
meaning 'Informational',
   type_id : class_uid * 100 + activity_id
   time : The time the event happened (RFC3339 format),
   observables : link [
       {
           name : "session_detail.portal_id",
           type_id : 10 //Resource UID
           value : //Generated value
       },
       {
           name : "session_detail.session_id",
           type_id : 10 //Resource UID
           value : //Generated value
       },
       {
           name : "session_detail.client_ip",
           type_id : 2 //IP Address
           value : //Generated value
       },
       {
           name : "session_detail.portal_ip",
           type_id : 2 //IP Address
           value : //Generated value
       },
       {
           name : "session_detail.username",
           type_id : 10 //Resource UID
           value : //Generated value
       }
   ],

   // New Events
```

```
    session_detail : {
        portal_id : String | UUID of the Portal | eg.
 1ebe42de-86bb-4073-88a4-34284bc5bcbb,
        session_id : String | SessionId of the user session | eg. 17be80fa-7bc2-4675-
b17a-791243938cdf
        client_ip : String | IP Address from which user LoggedIn From | eg. 31.65.180.9
        portal_ip : String | IP Address of the AWS AppStream Instance that is running
 the Portal | eg.240.62.100.169
        username : String | The logged-in username | eg. bobross
    }
}
```

Di bawah ini adalah contoh URLVisit acara:

```
{
    activity_id : 99,
    activity_name : "URLVisit",
    ...
    observables : [
        ...
        {
            name : "url",
            type_id : 23 //Unified Resource Locator
        }
    ]
    ...
    url : {
        url_string : String | Full URL path,
        hostname : String | The hostname in the URL
        path : String | Path in the domain
    }
}
```

Di bawah ini adalah contoh PrintJobSubmit acara:

```
{
    activity_id : 99,
    activity_name : "PrintJobSubmitted",
    observable : [
```

```
        ...
        {
            name : "file.name",
            type_id : 24 // File
        }
    ]
    ...
    file : {
        name : String | The file name,
        type_id : 1 //Regular file
        size : Long | Size in bytes
        ext : String | File extension
    }
}
```

Metrik Session Logger untuk Amazon Secure Browser WorkSpaces

Session Logger memancarkan metrik berikut Amazon CloudWatch .

Anda dapat menggunakan SessionLoggerEventDeliveredmetrik untuk memantau jumlah agregat peristiwa dari portal Anda, atau melihat jumlah file log yang dikirimkan dengan menghitung jumlah titik data daripada menjumlahkan nilai. Sebaiknya konfigurasi alarm pada SessionLoggerAccessDeniedErrormetrik SessionLoggerTargetNotFoundErrordan untuk mendeteksi penghapusan sumber daya atau izin yang tidak disengaja.

> **Note**
>
> Titik data metrik dikumpulkan oleh setiap sesi sekali per menit dan dipublikasikan setiap 5 menit Amazon CloudWatch sekali. Metrik Session Logger segera dipancarkan, untuk setiap pengiriman File Log.

Metrik Session Logger

Metrik	Deskripsi	Dimensi	Statistik	Unit
SessionLoggerEvent Delivered	Jumlah acara yang dimiliki setiap file	[PortalId]	Rata-rata , Jumlah, Maksimum, Minimum	Hitungan

Metrik	Deskripsi	Dimensi	Statistik	Unit
	Session Logger yang dikirimkan.			
SessionLoggerTargetNotFoundError	Jumlah pengiriman file log yang mengakibatkan bucket tidak ditemukan.	[PortalId]	Rata-rata, Jumlah, Maksimum, Minimum	Hitungan
SessionLoggerAccessDeniedError	Jumlah pengiriman file log yang mengakibatkan izin ditolak.	[PortalId]	Rata-rata, Jumlah, Maksimum, Minimum	Hitungan

Peristiwa sesi dalam pencatatan Akses Pengguna untuk Amazon WorkSpaces Secure Browser

Acara sesi berikut tersedia untuk pencatatan User Acess:

- Validasi: Acara ini berhasil dimasukkan ke aliran data Kinesis.
- StartSession: Pengguna telah memulai sesi dan terhubung ke sesi browser aman.
- VisitPage: Pengguna mengunjungi halaman dalam sesi.
- EndSession: Pengguna telah mengakhiri sesi.

Log navigasi URL direkam dari riwayat browser. URLs tidak direkam dalam riwayat browser (baik dikunjungi dalam mode penyamaran atau dihapus dari riwayat browser) tidak direkam dalam log. Terserah pelanggan untuk menentukan apakah akan mematikan mode penyamaran atau penghapusan riwayat dengan kebijakan browser mereka.

Di bawah ini adalah contoh dari setiap acara yang tersedia. Bidang berikut selalu disertakan untuk setiap acara:

- stempel waktu disertakan sebagai waktu epoch dalam milidetik.

- EventType disertakan sebagai string.
- detail disertakan sebagai objek json lain.
- PortaLarn dan UserName disertakan untuk setiap acara kecuali untuk Validasi.

```
{
  "timestamp": "1665430373875",
  "eventType": "Validation",
  "details": {
    "permission": "Kinesis:PutRecord",
    "userArn": "userArn",
    "operation": "AssociateUserAccessLoggingSettings",
    "userAccessLoggingSettingsArn": "userAccessLoggingSettingsArn"
  }
}

{
  "timestamp": "1665179071723",
  "eventType": "StartSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179084578",
  "eventType": "VisitPage",
  "details": {
    "title": "Amazon",
    "url": "https://www.amazon.com/"
  },
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179155953",
  "eventType": "EndSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}
```

Panduan untuk pengguna Amazon WorkSpaces Secure Browser

Administrator menggunakan Browser WorkSpaces Aman untuk membuat portal web yang terhubung ke situs web perusahaan, seperti situs web internal, aplikasi web software-as-a-service (SAAS), atau internet. Pengguna akhir menggunakan browser web mereka yang ada untuk mengakses portal web ini untuk meluncurkan sesi dan mengakses konten.

Konten berikut membantu memandu pengguna akhir yang ingin mempelajari lebih lanjut tentang mengakses Browser WorkSpaces Aman, meluncurkan dan mengonfigurasi sesi, serta menggunakan bilah alat dan browser web.

Topik

- Kompatibilitas browser dan perangkat untuk Amazon WorkSpaces Secure Browser
- Akses portal web untuk Amazon WorkSpaces Secure Browser
- Panduan sesi untuk Amazon WorkSpaces Secure Browser
- Memecahkan masalah pengguna di Amazon WorkSpaces Secure Browser
- Ekstensi masuk tunggal untuk Amazon WorkSpaces Secure Browser

Kompatibilitas browser dan perangkat untuk Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser didukung oleh klien browser web Amazon DCV, yang berjalan di dalam browser web, jadi tidak diperlukan instalasi. Klien browser web didukung oleh browser web umum, seperti Chrome dan Firefox, dan oleh sistem operasi desktop utama, seperti Windows, macOS, dan Linux.

Untuk up-to-date detail paling detail tentang dukungan klien browser web, lihat Klien browser Web.

> **Note**
>
> Support untuk webcam saat ini hanya tersedia di browser berbasis Chromium, seperti Google Chrome dan Microsoft Edge. Saat ini, Apple Safari dan Mozilla FireFox tidak mendukung webcam.

Akses portal web untuk Amazon WorkSpaces Secure Browser

Administrator Anda dapat memberikan akses ke portal web Anda dengan opsi berikut:

- Anda dapat memilih tautan dari email atau situs web, lalu masuk dengan kredensil identitas SAMP Anda.
- Anda dapat masuk ke penyedia identitas SAMP Anda (seperti Okta, Ping, atau Azure), dan meluncurkan sesi dengan satu klik dari halaman beranda aplikasi penyedia SAMP Anda (seperti Okta End User Dashboard atau portal Azure Myapps).

Panduan sesi untuk Amazon WorkSpaces Secure Browser

Setelah Anda masuk ke portal web, Anda dapat meluncurkan sesi dan melakukan berbagai tindakan selama sesi Anda.

Topik

- Memulai sesi di Amazon WorkSpaces Secure Browser
- Menggunakan toolbar di Amazon WorkSpaces Secure Browser
- Menggunakan browser di Amazon WorkSpaces Secure Browser
- Mengakhiri sesi di Amazon WorkSpaces Secure Browser

Memulai sesi di Amazon WorkSpaces Secure Browser

Setelah Anda masuk untuk meluncurkan sesi, Anda akan melihat pesan sesi peluncuran dan bilah kemajuan. Ini menunjukkan bahwa Amazon WorkSpaces Secure Browser membuat sesi untuk Anda. Di belakang layar, Amazon WorkSpaces Secure Browser membuat instance, meluncurkan browser web terkelola, dan menerapkan pengaturan administrator dan kebijakan browser.

Jika ini adalah pertama kalinya Anda masuk ke portal web Anda, Anda akan melihat ikon biru + di bilah alat. Ikon ini menunjukkan bahwa tutorial tersedia, yang akan memandu melalui fitur yang tersedia di toolbar. Anda dapat menggunakan ikon ini untuk mempelajari cara:

- Izinkan izin browser untuk mikrofon, webcam, dan clipboard, dengan memilih ikon kunci di sebelah browser lokal Anda, dan mengatur sakelar ke Aktif di sebelah clipboard, mikrofon, dan kamera.

> **Note**
>
> Saat Anda mengaktifkan izin webcam di awal sesi pertama Anda, webcam diaktifkan sebentar dan lampu di komputer Anda akan berkedip. Ini memberikan akses browser lokal ke webcam Anda.

- Aktifkan Amazon WorkSpaces Secure Browser untuk meluncurkan jendela monitor tambahan, dengan memilih ikon kunci di browser Anda dan pengaturan untuk Selalu izinkan pop-up.

Jika Anda ingin meluncurkan kembali tutorial, Anda dapat memilih Profil dari toolbar, Help, dan Launch tutorial.

Menggunakan toolbar di Amazon WorkSpaces Secure Browser

Untuk mempelajari cara menggunakan bilah alat, ikuti langkah-langkah ini.

Untuk memindahkan bilah alat, pilih bilah yang lebih ringan di bagian atas bilah alat, seret ke lokasi yang Anda inginkan, lalu lepaskan untuk menjatuhkannya.

Untuk menutup bilah alat, arahkan kursor ke atasnya, dan pilih tombol panah atas, atau klik dua kali bilah yang lebih ringan di bagian atas. Tampilan yang diciutkan memberi Anda lebih banyak real estat layar, dan akses satu klik ke ikon yang paling umum digunakan.

Untuk menambah ukuran layar, pilih jendela browser dan perbesar. Untuk meningkatkan ukuran tampilan ikon bilah alat dan teks, pilih bilah alat dan perbesar.

Untuk memperbesar atau memperkecil perangkat Windows, ikuti langkah-langkah berikut:

1. Pilih toolbar atau konten web.
2. Tekan Ctrl++ untuk memperbesar, atau tekan Ctrl + - untuk memperkecil.

Untuk memperbesar atau memperkecil perangkat Mac, ikuti langkah-langkah berikut:

1. Pilih toolbar atau konten web.
2. Tekan Cmd ++ untuk memperbesar, atau tekan Cmd + - untuk memperkecil.

Untuk memasang toolbar ke bagian atas layar, pilih Preferences, General, dan Docked di bawah mode Toolbar.

Tabel berikut mencakup deskripsi semua ikon yang tersedia di toolbar:

Icon	Title	Description
	**Windows**	Move between windows or launch additional browser windows.
	**Launch additional monitor window**	Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor.
	**Full screen**	Launch a full screen experience view.
	**Microphone**	Activate mic input for the session. Use the down arrow to select from a list of available microphones.
	**Webcam**	Activate webcam for the session. Use the down arrow to select from a list of available webcams.
	**Preferences**	Access the **General** and **Keyboard** menus. From the **General** menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below).
	**Profile**	End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session. **Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service. **Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team. **Help** provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide. **About** provides more information about Amazon WorkSpaces Web.
	**Notifications**	Get one-click access to session notifications.
	**Clipboard**	Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administator.
	**Files**	From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in **Files** are deleted at the end of the session. This icon only displays if **Files** permission is granted by your administator.

> **Note**
>
> Ikon Clipboard dan File disembunyikan secara default, kecuali administrator Anda memberikan izin ini. Hanya administrator yang dapat mengaktifkan atau menonaktifkan clipboard dan file di portal web. Jika ikon ini disembunyikan dan Anda perlu mengaksesnya, hubungi administrator Anda.

Menggunakan browser di Amazon WorkSpaces Secure Browser

Ketika Anda memulai sesi Anda, browser menampilkan URL Startup, yang merupakan URL yang dipilih oleh administrator Anda. Jika administrator belum memilih URL Startup, Anda akan melihat pengalaman tab baru default dari Google Chrome.

Dari browser, Anda dapat membuka tab, meluncurkan jendela browser tambahan (dari ikon toolbar Windows atau menu triple dot browser), memasukkan URL atau mencari di bilah URL, atau pergi ke situs web dari bookmark terkelola. Untuk mengakses bookmark untuk portal web, buka folder Bookmark Terkelola di bilah bookmark (di bawah bilah URL), atau buka pengelola bookmark dari menu titik tiga di sisi kanan bilah URL.

Untuk mengubah ukuran atau memindahkan jendela browser, seret ke bawah strip tab Chrome. Ini memungkinkan lebih banyak real estat layar untuk beberapa jendela browser selama sesi.

> **Note**
>
> Fitur browser, seperti mode Penyamaran, mungkin tidak tersedia selama sesi Anda jika administrator Anda telah mematikannya.

Mengakhiri sesi di Amazon WorkSpaces Secure Browser

Untuk mengakhiri sesi, pilih Profil dan Akhir sesi. Setelah sesi berakhir, Amazon WorkSpaces Secure Browser menghapus semua data dari sesi. Tidak ada data browser, seperti situs web terbuka atau riwayat, atau file atau data dari File Explorer yang tersedia setelah sesi berakhir.

Jika Anda menutup tab selama sesi aktif, sesi berakhir setelah periode waktu yang ditetapkan oleh administrator Anda. Jika Anda menutup tab dan mengunjungi kembali portal web sebelum batas waktu ini berlaku, Anda dapat bergabung dengan sesi saat ini dan melihat semua data sesi Anda sebelumnya, seperti membuka situs web dan file.

Memecahkan masalah pengguna di Amazon WorkSpaces Secure Browser

Jika Anda mengalami salah satu masalah berikut saat menggunakan Browser WorkSpaces Aman, coba resolusi berikut.

Portal Browser WorkSpaces Aman Amazon saya tidak mengizinkan saya masuk. Saya menerima pesan kesalahan yang mengatakan "Portal web Anda belum diatur. Hubungi administrator TI Anda untuk bantuan. “

Administrator Anda harus menyelesaikan pembuatan portal dengan penyedia identitas SAMP 2.0 agar Anda dapat masuk. Hubungi administrator Anda untuk bantuan.

Portal saya tidak akan meluncurkan sesi. Saya menerima pesan kesalahan yang mengatakan” Gagal memesan sesi. Ada kesalahan internal. Silakan coba lagi. “

Ada masalah dengan peluncuran sesi portal web Anda. Coba luncurkan sesi lagi. Jika ini berlanjut, hubungi administrator Anda untuk bantuan.

Saya tidak bisa menggunakan clipboard, mikrofon, atau webcam.

Untuk mengizinkan izin browser, pilih ikon kunci di sebelah URL, dan alihkan sakelar biru di sebelah Clipboard, Mikrofon, Kamera, dan Pop-up dan pengalihan untuk mengaktifkan fitur ini.

> **Note**
>
> Jika browser web Anda tidak mendukung input video atau audio, opsi ini tidak akan muncul di bilah alat.

Amazon WorkSpaces Secure Browser real-time audio-video (AV) mengalihkan video webcam lokal dan input audio mikrofon ke sesi streaming browser. Dengan cara ini, Anda dapat menggunakan perangkat lokal Anda untuk konferensi video dan audio dalam sesi streaming Anda dengan browser web berbasis Chromium, seperti Google Chrome atau Microsoft Edge. Webcam saat ini tidak didukung di browser non-Chromium.

Untuk informasi tentang cara mengonfigurasi Google Chrome, lihat Menggunakan kamera & mikrofon.

Portal web saya tidak akan meluncurkan jendela monitor tambahan.

Jika Anda mencoba meluncurkan monitor ganda dan melihat ikon Pop-up diblokir di akhir bilah alamat di browser atas, pilih ikon dan tombol radio di sebelah Selalu izinkan pop-up dan pengalihan. Dengan pop-up yang diizinkan, pilih ikon Monitor ganda pada bilah alat untuk meluncurkan jendela baru, memposisikan ulang jendela pada monitor Anda, dan seret tab browser ke jendela.

Ketika saya mencoba mengunduh file dari panel File, tidak ada yang terjadi.

Jika Anda mencoba mengunduh file dari panel File dan melihat ikon Pop-up diblokir di akhir bilah alamat di browser atas, pilih ikon dan tombol radio di samping Selalu izinkan pop-up dan pengalihan. Dengan pop-up diizinkan, coba unduh file lagi.

Bagaimana saya bisa tahu and/or webcam mikrofon mana yang digunakan, dan bagaimana saya bisa mengubahnya?

Klik ikon panah bawah di sebelah mikrofon atau kamera. Menu menampilkan perangkat yang tersedia, dengan tanda centang yang menunjukkan perangkat Anda saat ini. Pilih perangkat lain untuk mengubah perangkat yang ingin Anda gunakan untuk sesi Anda.

Portal web saya tidak akan diluncurkan saat diakses langsung dari domain khusus perusahaan

Jika Anda mencoba meluncurkan sesi menggunakan nama domain non-workspaces-web.com seperti`acme.secureportal.mycompany.com`, pastikan browser Anda mengaktifkan cookie pihak ketiga untuk domain perusahaan yang Anda akses.

Ekstensi masuk tunggal untuk Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser menawarkan ekstensi untuk sistem masuk tunggal dengan browser Chrome dan Firefox di komputer desktop. Jika administrator Anda telah mengaktifkan ekstensi, portal web akan meminta Anda untuk menginstal ekstensi saat Anda masuk.

Amazon WorkSpaces Secure Browser membuat ekstensi untuk mengaktifkan sistem masuk tunggal ke situs web selama sesi Anda. Misalnya, jika Anda masuk ke portal web Anda menggunakan penyedia identitas SAMP 2.0 (seperti Okta atau Ping), dan Anda mengunjungi situs web selama sesi Anda yang menggunakan penyedia identitas yang sama, ekstensi dapat mempermudah akses situs web dengan menghapus permintaan masuk tambahan.

Anda tidak diharuskan untuk menginstal ekstensi untuk mengakses portal web Anda, tetapi dapat meningkatkan pengalaman Anda dengan mengurangi berapa kali Anda diminta untuk memasukkan nama pengguna dan kata sandi Anda.

Saat Anda masuk, ekstensi akan menempatkan cookie yang terdaftar administrator Anda untuk sesi Anda. Semua data yang ditempatkan ekstensi dienkripsi saat istirahat dan selama transit. Tak satu pun dari data ini disimpan di browser lokal Anda. Saat Anda mengakhiri sesi, semua data sesi Anda (seperti tab terbuka, file yang diunduh, dan cookie yang dikirimkan ke atau dibuat selama sesi) dihapus.

Topik

- Kompatibilitas ekstensi masuk tunggal untuk Amazon Secure Browser WorkSpaces
- Menginstal ekstensi masuk tunggal untuk Amazon WorkSpaces Secure Browser
- Memecahkan masalah ekstensi masuk tunggal untuk Amazon Secure Browser WorkSpaces

Kompatibilitas ekstensi masuk tunggal untuk Amazon Secure Browser WorkSpaces

Ekstensi masuk tunggal berfungsi dengan perangkat dan browser berikut:

- Perangkat
  - Laptop
  - Komputer desktop
- Browser
  - Google Chrome
  - Mozilla Firefox

Menginstal ekstensi masuk tunggal untuk Amazon WorkSpaces Secure Browser

Untuk menginstal ekstensi masuk tunggal, ikuti langkah-langkah ini.

Saat Anda masuk ke portal, ikuti prompt untuk menginstal ekstensi untuk browser Chrome atau Firefox Anda. Anda hanya perlu melakukan ini satu kali untuk setiap browser web.

Jika Anda beralih perangkat, beralih ke browser lain di perangkat yang sama, atau menghapus ekstensi dari browser lokal, Anda akan melihat prompt untuk menginstal ekstensi saat memulai sesi berikutnya.

Untuk memastikan bahwa ekstensi berfungsi seperti yang diharapkan, gunakan ekstensi di jendela penelusuran normal, bukan Incognito (Chrome) atau Penjelajahan Pribadi (Firefox).

Memecahkan masalah ekstensi masuk tunggal untuk Amazon Secure Browser WorkSpaces

Saat menggunakan ekstensi masuk tunggal, Anda mungkin mengalami masalah berikut.

Jika ekstensi telah diinstal, tetapi Anda masih diminta untuk masuk selama sesi, ikuti langkah-langkah berikut:

1. Pastikan bahwa Anda memiliki ekstensi Amazon WorkSpaces Secure Browser diinstal pada browser Anda. Jika Anda menghapus data browser Anda, Anda mungkin telah menghapus ekstensi secara tidak sengaja.
2. Pastikan Anda bukan Incognito (Chrome) atau Private Browsing (Firefox). Mode ini dapat menyebabkan masalah dengan ekstensi.
3. Jika masalah berlanjut, hubungi administrator portal Anda untuk bantuan tambahan.

Riwayat dokumen untuk Panduan Administrasi Browser WorkSpaces Aman Amazon

Tabel berikut menjelaskan rilis dokumentasi untuk Amazon WorkSpaces Secure Browser.

Perubahan	Deskripsi	Tanggal
Session Logger	Siapkan Session Logger untuk menangkap berbagai acara sesi.	Agustus 1, 2025
CloudWatch metrik	CloudWatch Metrik yang diperbarui.	Juli 21, 2025
Kontrol bilah alat	Dengan kontrol toolbar, Anda dapat mengonfigurasi presentasi toolbar untuk sesi pengguna akhir.	Februari 21, 2025
Akses APIs menggunakan antarmuka VPC endpoint ()AWS PrivateLink	Panggil langsung titik akhir Amazon WorkSpaces Secure Browser API dari dalam cloud pribadi (VPC), alih-alih terhubung melalui internet.	Januari 10, 2025
Pengaturan Perlindungan Data	Tambahkan Pengaturan Perlindungan Data untuk membantu melindungi data agar tidak dibagikan selama sesi.	November 20, 2024
Titik akhir FIPS	Lindungi data dalam perjalanan dengan titik akhir FIPS.	Oktober 7, 2024
Dasbor manajemen sesi	Gunakan dasbor manajemen sesi untuk memantau dan	September 19, 2024

	mengelola sesi aktif dan lengkap.	
Izinkan tautan dalam	Izinkan portal menerima tautan dalam yang menghubungkan pengguna ke situs web tertentu selama sesi berlangsung.	Juni 25, 2024
Pembaruan kebijakan terkelola	Ditambahkan kebijakan AmazonWorkSpacesSecureBrowserReadOnly terkelola	Juni 24, 2024
Gunakan bilah alat untuk memperbesar	Anda dapat meningkatkan ukuran tampilan, ikon, dan teks dengan bilah alat.	1 Mei 2024
Pengaturan portal web baru	Anda sekarang dapat menentukan jenis Instance dan batas pengguna bersamaan Max untuk portal web Anda.	April 22, 2024
CloudWatch metrik	Ditambahkan GlobalCpuPercent dan GlobalMemoryPercent metrik.	Februari 26, 2024
Mengatur pemfilteran URL	Anda dapat menggunakan Kebijakan Chrome untuk memfilter URLs pengguna mana yang dapat diakses dari browser jarak jauh mereka.	Februari 21, 2024
Jenis otentikasi IDP	Anda dapat memilih jenis otentikasi standar atau IAM Identity Center.	Februari 5, 2024

Aktifkan ekstensi untuk sistem masuk tunggal	Anda dapat mengaktifkan ekstensi agar pengguna akhir Anda memiliki pengalaman masuk portal yang lebih baik.	28 Agustus 2023
Panduan pengguna untuk Amazon WorkSpaces Secure Browser	Menambahkan konten untuk membantu memandu pengguna akhir, yang ingin mempelajari lebih lanjut tentang mengakses Amazon WorkSpaces Secure Browser, meluncurkan dan mengonfig urasi sesi, serta menggunakan bilah alat dan browser web.	Juli 17, 2023
Kontrol akses IP	WorkSpaces Secure Browser memungkinkan Anda mengontrol alamat IP mana portal web Anda dapat diakses.	31 Mei 2023
Pembaruan kebijakan terkelola	Kebijakan AmazonWor kSpacesWebReadOnly terkelola yang diperbarui	15 Mei 2023
Konfigurasikan pembaruan penyedia identitas	WorkSpaces Secure Browser menawarkan dua jenis otentikasi: Standar dan AWS IAM Identity Center	15 Maret 2023
Pembaruan kebijakan browser	Bagian kebijakan browser yang diperbarui dan direstruk turisasi	31 Januari 2023
Pembaruan kebijakan terkelola	Kebijakan AmazonWor kSpacesWebServiceR olePolicy terkelola yang diperbarui	15 Desember 2022

Daftar Izinkan dan Daftar Blokir	Tentukan Allowlist dan Blocklist untuk menentukan daftar domain yang dapat atau tidak dapat diakses oleh pengguna Anda.	November 14, 2022
Pembaruan kebijakan terkelola	Kebijakan AmazonWorkSpacesWebReadOnly terkelola yang diperbarui	2 November 2022
Pembaruan kebijakan terkelola	Kebijakan AmazonWorkSpacesWebServiceRolePolicy terkelola yang diperbarui	24 Oktober 2022
Pencatatan akses pengguna	Siapkan pencatatan akses pengguna untuk merekam peristiwa pengguna	Oktober 17, 2022
Pembaruan jaringan	Berbagai pembaruan ke bagian “Jaringan dan akses”	September 22, 2022
Pembaruan kebijakan terkelola	Kebijakan AmazonWorkSpacesWebServiceRolePolicy terkelola yang diperbarui	September 6, 2022
Konfigurasikan sesi pengguna	Konfigurasikan Input Method Editor (IME) dan lokalisasi dalam sesi	28 Juli 2022
Pembaruan jaringan	Berbagai pembaruan ke bagian “Jaringan dan akses”	Juli 7, 2022

Nilai batas waktu	Tentukan batas waktu Putuskan sambungan dalam hitungan menit dan batas waktu putuskan sambungan Idle dalam hitungan menit	Mei 16, 2022
Kebijakan terkelola yang diperbarui	Memperbarui kebijakan AmazonWorkSpacesWebServiceRolePolicy terkelola untuk menambahkan AWS/Usage namespace ke izin API PutMetricData	April 6, 2022
Peran terkait layanan	AWSServiceRoleForAmazonWorkSpacesWeb Peran terkait layanan baru	30 November 2021
Kebijakan terkelola	Kebijakan AmazonWorkSpacesWebReadOnly terkelola baru	30 November 2021
Kebijakan terkelola	Kebijakan AmazonWorkSpacesWebServiceRolePolicy terkelola baru	30 November 2021
Rilis awal	Rilis awal Panduan Administrasi Browser WorkSpaces Aman	30 November 2021

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