Service Name

Amazon WorkSpaces Secure Browser

Service Overview

Amazon WorkSpaces Secure Browser is a fully managed, cloud-native, hosted browser service that enables secure access to private websites, software-as-a-service (SaaS) applications, and the public internet from a disposable container. Web content is streamed to users' existing web browsers while the actual browser session remains isolated in AWS. Each session launches with a fresh, fully patched Chrome browser, eliminating the need for IT to manage appliances, infrastructure, specialized client software, or VPN connections. The service reduces data exfiltration risk by streaming encrypted pixels without transmitting HTML, DOM, or sensitive company data to local devices.

Key Use Cases

- Empowering customer support and back-office workers: Secure access to internal applications and customer data without exposing sensitive information to local devices
- Enabling BYOD (Bring Your Own Device) initiatives: Allow employees to safely access company resources from personal devices without security risks
- Creating secure data and analytics environments: Provide controlled access to sensitive data and analytics tools while maintaining data isolation
- Isolating high-security networks from the public internet: Enable secure browsing for users in high-security environments without direct internet exposure
- Cost optimization: Replace expensive VPN infrastructure and traditional virtual desktops with a more cost-effective browser solution

Features

- **Ephemeral Sessions**: Each session launches with a fresh, fully patched Chrome browser that is wiped clean after use
- **Pixel Streaming**: Streams encrypted pixels from remote browser sessions without transmitting sensitive data to local devices
- **Enterprise Browser Policies**: Enforce URL allow/blocking, session-level controls for clipboard, file transfer, and printer access
- **IP Access Controls**: Restrict access to trusted networks or devices through IP-based access controls
- **SAML 2.0 Integration**: Single sign-on support with existing SAML 2.0 identity providers for authentication

- **Web Content Filtering**: Control and monitor web content access with granular policies and 25+ predefined categories
- **Session Monitoring**: Monitor sessions using CloudWatch and CloudTrail with detailed logging capabilities
- **Multiple Instance Types**: Support for standard.regular, standard.large, and standard.xlarge instances for different performance needs

Value Proposition

Amazon WorkSpaces Secure Browser offers significant advantages over traditional VPN solutions and virtual desktops. It eliminates the browser attack surface by isolating sessions in AWS, reduces data exfiltration risks through pixel streaming, and requires no specialized client software or VPN management:

- Starting at $7 per month, it provides cost-effective secure browsing compared to traditional virtual desktops
- The service simplifies IT management with fully managed infrastructure, automatic browser updates, and centralized policy enforcement
- Organizations benefit from enhanced security controls, simplified BYOD enablement, and the ability to provide secure access from any device without complex infrastructure management

Service Integration

WorkSpaces Secure Browser integrates deeply with core AWS services to provide secure, scalable browsing capabilities. It leverages Amazon EC2 for provisioning streaming instances and creating Cross-Account Elastic Network Interfaces for corporate network communication:

- The service uses Amazon VPC for network isolation, subnets, and security groups configuration
- Data protection is ensured through integration with AWS Key Management Service (KMS) for encryption, Amazon DynamoDB and S3 for secure data storage, and AWS Identity and Access Management (IAM) for access control
- Monitoring capabilities are provided through Amazon CloudWatch for metrics and AWS CloudTrail for audit logging
- Optional integration with Kinesis Data Streams enables advanced user access logging

Onboarding and Offboarding

Getting started with WorkSpaces Secure Browser involves creating a web portal in the desired AWS region, configuring VPC, subnets, and security groups for network connectivity. Administrators set up browser policies and user settings through the AWS

console, then federate their existing SAML 2.0 identity provider for user authentication and single sign-on:

- The setup process includes signing up for an AWS account, creating IAM users with appropriate permissions, and configuring networking prerequisites
- Once configured, users can access the browser through common web browsers from desktop, laptop, or thin client devices without requiring additional software installation

Getting Started Guide: https://docs.aws.amazon.com/workspaces-web/latest/adminguide/setting-up.html

Data Removal

WorkSpaces Secure Browser ensures data protection through ephemeral sessions that are automatically wiped at the end of each session. No HTML, DOM, or sensitive company data is transmitted to or stored on local devices. When offboarding, administrators can simply deactivate user access through their SAML identity provider and delete web portals through the AWS console. All session data, browser policies, and user preferences stored in AWS are encrypted and can be removed by deleting the associated resources.

Backup/Restore and Disaster Recovery

WorkSpaces Secure Browser provides inherent data protection through its ephemeral session model where no persistent data is stored in browser instances. The service automatically maintains fresh, fully patched browser sessions that are recreated for each use. Configuration data including portal settings, browser policies, and user preferences are stored in AWS managed services with built-in durability and availability features across multiple availability zones.

Backup Capabilities

The service does not require traditional backup capabilities as browser sessions are ephemeral and automatically wiped after use. Configuration data is stored in AWS managed services like DynamoDB and S3 with built-in durability. The service itself does not directly integrate with AWS Backup as there is no persistent session data to backup - each session starts fresh with applied policies and settings.

Disaster Recovery

WorkSpaces Secure Browser supports disaster recovery through its multi-region availability and stateless session architecture. Since sessions are ephemeral and configuration data is stored in AWS managed services, the service can be quickly restored in alternate regions. The service does not directly integrate with AWS Elastic Disaster Recovery as sessions are recreated on-demand rather than requiring instance-level recovery.

Recovery Objectives

WorkSpaces Secure Browser supports rapid recovery with minimal RPO and RTO through its ephemeral session model. Since no persistent data exists in browser sessions, RPO is effectively zero for session data. RTO is minimized through the service's ability to quickly provision new sessions and its multi-region availability, allowing rapid failover to alternate regions when needed.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/workspaces-web/latest/adminguide/request-service-quota.html

FAQ: https://aws.amazon.com/workspaces/secure-browser/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/workspaces-web/latest/adminguide/index.html

User Guide: https://docs.aws.amazon.com/workspaces-web/latest/adminguide/user-guide.html

API Reference: https://docs.aws.amazon.com/workspaces-web/latest/APIReference/Welcome.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/workspaces/secure-browser/pricing/

Cost Optimization

WorkSpaces Secure Browser offers several cost optimization features including pay-as-you-go pricing with no minimum fees or long-term contracts, starting at $7 per month for standard.regular instances. The service includes up to 200 streaming hours per user monthly, with additional hours charged at competitive rates:

- Organizations can optimize costs by selecting appropriate instance types based on workload requirements - standard.regular for static content, standard.large for improved performance, and standard.xlarge for resource-intensive applications
- The ephemeral session model eliminates storage costs and reduces infrastructure overhead compared to traditional virtual desktop solutions

Savings Considerations

Primary cost savings come from eliminating VPN infrastructure, reducing virtual desktop licensing costs, and minimizing IT management overhead. The service eliminates the need for specialized client software, appliances, or dedicated infrastructure management:

- Organizations save on hardware procurement, maintenance, and upgrade cycles typically associated with traditional remote access solutions
- The fully managed service model reduces operational costs through automated patching, scaling, and capacity management
- Additional savings result from improved security posture reducing potential breach-related costs and simplified BYOD implementation without additional security infrastructure investments