aws

管理指南

Amazon WorkSpaces 安全瀏覽器

Amazon WorkSpaces 安全瀏覽器: 管理指南

Table of Contents

什麼是 Amazon WorkSpaces 安全瀏覽器？

> **Note**
>
> Amazon WorkSpaces 安全瀏覽器先前稱為 Amazon WorkSpaces Web。

Amazon WorkSpaces 安全瀏覽器是一種全受管的雲端原生託管瀏覽器服務，用於安全地存取私有網站和software-as-a-service(SaaS) Web 應用程式、與線上資源互動，以及從一次性容器瀏覽網際網路。WorkSpaces 安全瀏覽器可與使用者現有的 Web 瀏覽器搭配使用，而無須負擔 IT 管理設備、基礎設施、專用用戶端軟體或虛擬私有網路 (VPN) 連線的負擔。Web 內容會串流到使用者的 Web 瀏覽器，而實際的瀏覽器和 Web 內容會隔離在其中 AWS。透過使用支援 AWS Amazon WorkSpaces 和 Amazon WorkSpaces 應用程式等最終使用者運算服務的相同基礎技術，WorkSpaces 安全瀏覽器可以比傳統虛擬桌面更具成本效益，並且相較於使用管理軟體為公司擁有的裝置降低複雜性。WorkSpaces 安全瀏覽器透過串流 Web 內容來降低資料外洩的風險。不會將 HTML、文件物件模型 (DOM) 或敏感的公司資料傳輸至本機電腦。透過將裝置、公司網路和網際網路彼此隔離，幾乎消除了瀏覽器攻擊面。

您可以在所有工作階段上強制執行企業瀏覽器政策（包括 URL 允許/封鎖），並包含剪貼簿、檔案傳輸和印表機的工作階段層級控制項。您也可以使用 IP 存取控制來限制對受信任網路或裝置的存取。WorkSpaces 安全瀏覽器易於設定和操作。每個工作階段都會以全新且完全修補的 Chrome 瀏覽器版本啟動，並套用公司政策和設定。

Amazon WorkSpaces 安全瀏覽器的版本歷史記錄

2024 年 5 月 20 日，Amazon WorkSpaces Web 重新命名為 Amazon WorkSpaces 安全瀏覽器。對於現有客戶，他們使用 服務管理使用者或資源的方式沒有變更。下列清單說明由於此重新命名而發生的適用更新。

workspaces-web API 命名空間在回溯相容性方面保持不變。因此，下列資源仍然相同：

- CLI 命令。
- Amazon CloudWatch 指標。如需詳細資訊，請參閱the section called “使用 CloudWatch 進行監控”。
- 服務端點。如需詳細資訊，請參閱 Amazon WorkSpaces 安全瀏覽器端點和配額。
- AWS CloudFormation 資源。如需詳細資訊，請參閱 Amazon WorkSpaces 安全瀏覽器資源類型參考。

- 包含 workspaces-web 的服務連結角色。如需詳細資訊，請參閱the section called “使用服務連結角色”。
- 包含 workspaces-web URLs。
- 包含 workspaces-web 的文件 URLs。如需詳細資訊，請參閱 Amazon WorkSpaces 安全瀏覽器文件。
- 現有的 ReadOnly 受管角色。如需詳細資訊，請參閱the section called “AWS 受管政策”。
- KMS 授予名稱。
- UAL（使用者活動記錄） Kinesis 串流字首。

此外，現有的入口網站 URLs保持不變。在 2024 年 5 月 20 日之前建立的入口網站 URLs 使用格式 <UUID>.workspaces-web.com。WorkSpaces 安全瀏覽器入口網站會繼續使用此格式和 workspaces-web.com 網域。

使用 Amazon WorkSpaces 安全瀏覽器時應注意的術語

為了協助您開始使用 WorkSpaces 安全瀏覽器，您應該熟悉下列概念。

Identity provider (IdP) (身分提供者 (IdP))

身分提供者會驗證您的使用者的登入資料。然後會發出身分驗證聲明，以提供存取權給服務提供者。您可以設定現有的 IdP 以使用 WorkSpaces 安全瀏覽器。

根據您的 IdP，會有不同的設定身分提供者 (IdP) 程序。

您必須將服務提供者中繼資料檔案上傳至您的 IdP。否則您的使用者將無法登入。您還必須授予使用者在 IdP 中使用 WorkSpaces 安全瀏覽器的存取權。

身分提供者 (IdP) 中繼資料文件

WorkSpaces 安全瀏覽器需要身分提供者 (IdP) 的特定中繼資料，才能建立信任。您可以透過上傳從 IdP 下載的中繼資料交換檔案，將此中繼資料新增至 WorkSpaces 安全瀏覽器。

服務供應商 (SP)

服務提供者接受身分驗證聲明並向使用者提供服務。WorkSpaces 安全瀏覽器可做為已透過其 IdP 驗證之使用者的服務提供者。

服務供應商 (SP) 中繼資料文件

您需要將服務提供者中繼資料詳細資訊加入身分提供者 (IdP) 的組態介面。各提供者會有不同的組態流程詳細資訊。

SAML 2.0

用在 IdP 與服務提供者之間的身分驗證和授權資料交換的標準。

Virtual Private Cloud (VPC)

您可以使用現有或新的 VPC、對應的子網路和安全群組，將您的內容連結至 WorkSpaces 安全瀏覽器。

子網路必須與網際網路保持穩定連線，並且 VPC 和子網路也必須與任何內部網站和軟體即服務 (SaaS) 網站有穩定連線，才能存取這些資源。

列出的 VPCs、子網路和安全群組來自 WorkSpaces 安全瀏覽器主控台所在的相同區域。

Trust store (信任存放區)

如果透過 WorkSpaces 安全瀏覽器存取網站的使用者收到隱私權錯誤，例如 NET：：ERR_CERT_INVALID，則該網站可能正在使用私有憑證授權單位 (PCA) 簽署的憑證。您可能需要在信任存放區中新增或變更 PCA。此外，如果使用者的裝置要求您安裝特定憑證以載入網站，您將需要將該憑證新增至您的信任存放區，以允許使用者在 WorkSpaces 安全瀏覽器中存取該網站。

可公開存取的網站通常無需對信任存放區進行任何變更。

Web 入口網站

Web 入口網站可讓您的使用者從其瀏覽器存取內部和 SaaS 網站。您可以在每個帳戶的任何支援區域建立一個 Web 入口網站。若要請求提高多個入口網站的限制，請連絡支援人員。

Web 入口網站端點

Web 入口網站端點是您的使用者在使用針對入口網站設定的身分提供者登入後，啟動 Web 入口網站的存取點。

可在網際網路上公開使用端點，且可以嵌入您的網路。

AWS 與 Amazon WorkSpaces 安全瀏覽器相關的 服務

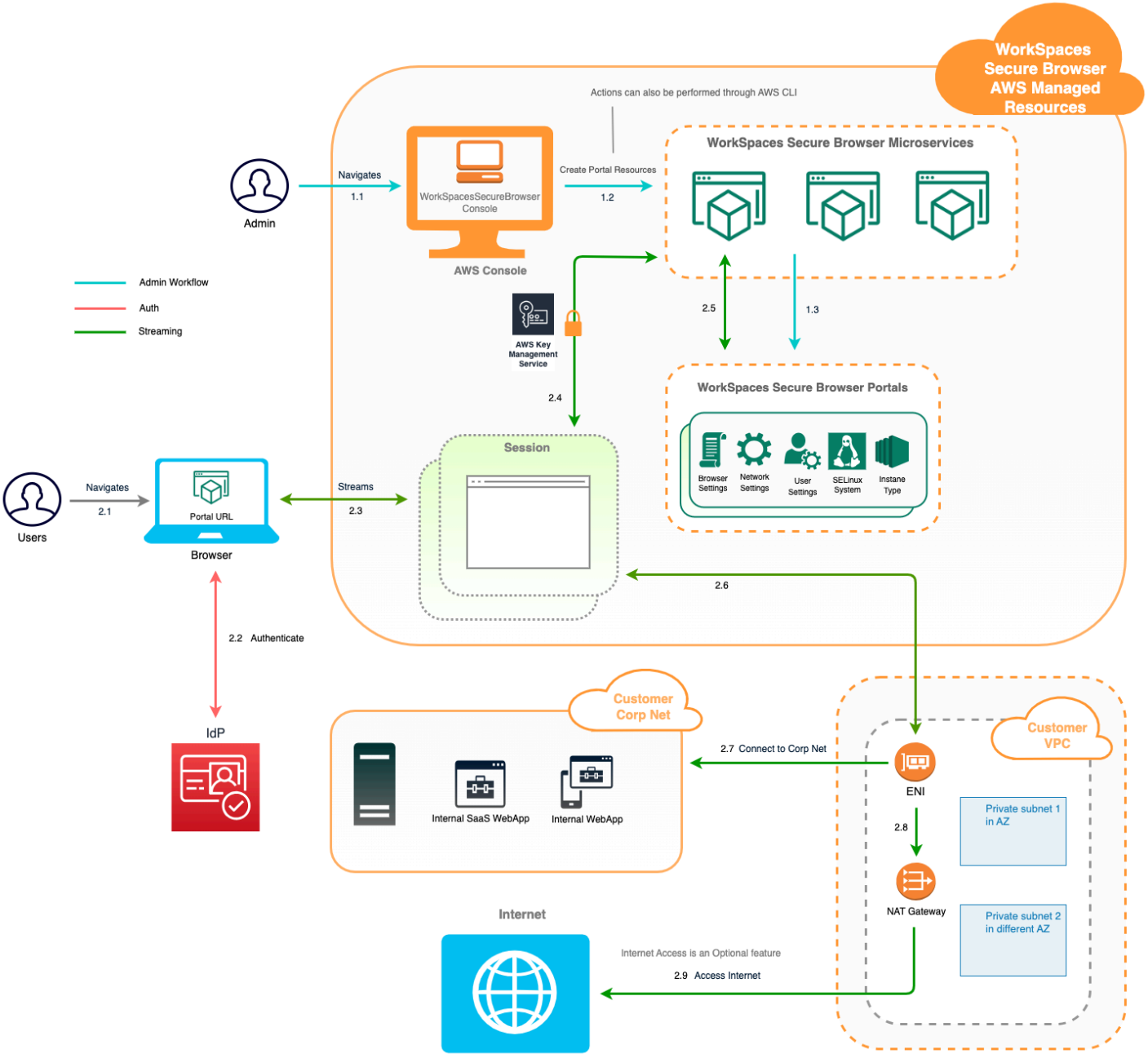
有數個 AWS 服務與 WorkSpaces 安全瀏覽器相關。

WorkSpaces 安全瀏覽器是 AWS 最終使用者運算產品組合中 Amazon WorkSpaces 的功能。與 WorkSpaces 和 AppStream 2.0 相比，WorkSpaces 安全瀏覽器專為促進安全的 Web 型工作負載而建

置。WorkSpaces 安全瀏覽器會自動受管，由 AWS 隨需佈建和更新容量、擴展和映像。例如，您可以選擇將持久性工作區桌面提供給需要存取桌面資源的軟體開發人員，以及將 WorkSpaces 安全瀏覽器提供給只需要存取桌上型電腦上少數內部和 SaaS 網站（包括網路外部託管的網站）的聯絡中心使用者。

Amazon WorkSpaces 安全瀏覽器的架構

下圖顯示 WorkSpaces 安全瀏覽器的架構。



存取 Amazon WorkSpaces 安全瀏覽器

您可以透過多種方式存取 WorkSpaces 安全瀏覽器。

管理員可透過 WorkSpaces 安全瀏覽器主控台、SDK、CLI 或 API 存取 WorkSpaces 安全瀏覽器。您的使用者透過 WorkSpaces 安全瀏覽器端點存取它。

設定 Amazon WorkSpaces 安全瀏覽器

您必須先完成下列先決條件，才能將 WorkSpaces 安全瀏覽器設定為連接內部網站和 SaaS 應用程式。

主題

註冊和建立使用者

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 在註冊程序完成後， 會傳送確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS 管理主控台身分登入 。在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需說明，請參閱《IAM 使用者指南》中的為您的 AWS 帳戶 根使用者 （主控台） 啟用虛擬 MFA 裝置。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的啟用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center 《 使用者指南》中的使用預設值設定使用者存取 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《 使用者指南》中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

授予程式設計存取權

如果使用者想要與 AWS 外部互動，則需要程式設計存取 AWS 管理主控台。授予程式設計存取權的方式取決於正在存取的使用者類型 AWS。

若要授予使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	根據
IAM	（建議）使用主控台登入資料做為臨時登入資料，以簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	請依照您要使用的介面所提供的指示操作。 • 如需 AWS CLI，請參閱AWS Command Line Interface 《使用者指南》中的登入以進行 AWS 本機開發。 • AWS SDKs，請參閱 AWS SDKs 和工具參考指南中的登入以進行 AWS 本機開發。
人力資源身分 (IAM Identity Center 中管理的使用者)	使用暫時登入資料簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	請依照您要使用的介面所提供的指示操作。 • 如需 AWS CLI，請參閱AWS Command Line Interface 《使用者指南》中的設定 AWS CLI 要使用 AWS IAM Identity Center的 。 • AWS SDKs、工具和 AWS APIs，請參閱 AWS SDKs 和工具參考指南中的 IAM Identity Center 身分驗證。
IAM	使用暫時登入資料簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	遵循《IAM 使用者指南》中將臨時登入資料與 AWS 資源搭配使用的指示。

哪個使用者需要程式設計存取權？	到	根據
IAM	(不建議使用) 使用長期憑證簽署對 AWS CLI、 AWS SDKs程式設計請求。 AWS APIs	請依照您要使用的介面所提供的指示操作。 • 如需 AWS CLI，請參閱AWS Command Line Interface 《 使用者指南》中的使用 IAM 使用者憑證進行身分驗證。 • AWS SDKs和工具，請參閱 AWS SDKs和工具參考指南中的使用長期憑證進行身分驗證。 • 對於 AWS APIs，請參閱《 IAM 使用者指南》中的管理 IAM 使用者的存取金鑰。

Amazon WorkSpaces 安全瀏覽器的網路

下列主題說明如何設定 WorkSpaces 安全瀏覽器串流執行個體，讓使用者可以與其連線。它還說明如何讓您的 WorkSpaces 安全瀏覽器串流執行個體存取 VPC 資源以及網際網路。

主題

- 設定 Amazon WorkSpaces 安全瀏覽器的 VPC
- 啟用 Amazon WorkSpaces 安全瀏覽器的使用者連線

設定 Amazon WorkSpaces 安全瀏覽器的 VPC

若要為 WorkSpaces 安全瀏覽器設定 VPC，請完成下列步驟。

主題

- Amazon WorkSpaces 安全瀏覽器的 VPC 需求
- 為 Amazon WorkSpaces 安全瀏覽器建立新的 VPC

- 啟用 Amazon WorkSpaces 安全瀏覽器的網際網路瀏覽
- WorkSpaces 安全瀏覽器的 VPC 最佳實務
- Amazon WorkSpaces 安全瀏覽器支援的可用區域

Amazon WorkSpaces 安全瀏覽器的 VPC 需求

在建立 WorkSpaces 安全瀏覽器入口網站期間，您將在帳戶中選取 VPC。您也將選擇位於不同可用區域的至少兩個子網路。這些 VPC 和子網路必須符合下列要求：

- VPC 必須具有預設硬體租用。不支援具有專用租用的 VPC。
- 有鑑於可用性，我們至少需要在兩個不同可用區域中建立的子網路。您的子網路必須有足夠的 IP 地址，以支援預期的 WorkSpaces 安全瀏覽器流量。請為各個子網路設定子網路遮罩，該遮罩必須具備足夠的用戶端 IP 地址來應付最大同時工作階段數量。如需詳細資訊，請參閱為 Amazon WorkSpaces 安全瀏覽器建立新的 VPC。
- 所有子網路都必須與位於 AWS 雲端 或內部部署的任何內部內容有穩定的連線，使用者將使用 WorkSpaces 安全瀏覽器存取該子網路。

在考量到可用性和擴展的情況下我們建議您在不同的可用區域中選擇三個子網路。如需詳細資訊，請參閱為 Amazon WorkSpaces 安全瀏覽器建立新的 VPC。

WorkSpaces 安全瀏覽器不會將任何公有 IP 地址指派給串流執行個體，以啟用網際網路存取。這將使得使用者可以從網際網路存取您的串流執行個體。因此，任何連接到您公用子網路的串流執行個體都無法存取網際網路。如果您希望 WorkSpaces 安全瀏覽器入口網站同時存取公有網際網路內容和私有 VPC 內容，請完成 中的步驟啟用 Amazon WorkSpaces 安全瀏覽器的無限制網際網路瀏覽 （ 建議 ）。

為 Amazon WorkSpaces 安全瀏覽器建立新的 VPC

本節說明如何使用 VPC 精靈快速建立具有公有和私有子網路的 VPC。精靈會自動建立網際網路閘道、NAT 閘道，並設定子網路的路由表。

如需此組態的詳細資訊，請參閱具有公有和私有子網路 (NAT) 的 VPC。

主題

- 快速 VPC 設定 (1 分鐘)
- 驗證子網路路由表 （ 選用 ）

快速 VPC 設定 (1 分鐘)

請完成下列步驟，以透過公有和私有子網路快速建立 WorkSpaces 安全瀏覽器的專用 VPC 進行網際網路存取。如果您想要使用現有的 VPC，請參閱 Amazon WorkSpaces 安全瀏覽器的 VPC 需求 驗證是否符合需求。

> **Note**
>
> 確定您在所需的 中 AWS 區域。如有需要，您可以在 主控台中變更區域。

快速設定 VPC

1. 開啟 VPC 建立精靈：使用 資源建立 VPC。除非以下指定，否則將所有設定保留為預設值：
   - 針對要建立的資源，選取 VPC 等。
   - 針對名稱標籤，選取自動產生並輸入 VPC 的描述性名稱 （ 例如 **WSB-VPC**)。
   - 對於 IPv4 CIDR 區塊，VPC 預設會使用 **10.0.0.0/16**。如有需要，您可以指定不同的 IPv4 CIDR 區塊。
   - 對於租用，選取預設 （ 不支援具有專用租用VPCs)。
   - 針對可用區域 (AZs) 的數量，選取 2。
     - 展開自訂可用AZs，然後選取 WorkSpaces 安全瀏覽器支援的 2 個不同可用區域。如需支援的 AZs清單，請參閱 Amazon WorkSpaces 安全瀏覽器支援的可用區域。
   - 針對公有子網路數量，選取 2。
   - 針對私有子網路的數量，選取 2。
   - 對於子網路 CIDR 區塊，如果您需要自訂子網路中的 CIDR 區塊，請展開自訂子網路 CIDR 區塊。確保每個子網路都有足夠的 IP 地址可供您預期流量使用。
   - 針對 NAT 閘道，選取區域以啟用所有可用區域的私有子網路網際網路存取。
   - 對於 VPC 端點，選取無。如果您需要直接存取 S3 而不經過 NAT 閘道，請選取 S3 Gateway。
   - 對於 DNS 選項，請保持啟用 DNS 選項 （ 預設 ），以確保 VPC 內的正確名稱解析。
2. 檢閱預覽窗格，然後選擇建立 VPC。

> **Note**
>
> NAT 閘道和 VPC 端點需支付額外費用。如需詳細資訊，請參閱 VPC 定價頁面。

驗證子網路路由表（選用）

VPC 精靈會自動為您設定路由表。如果您手動建立 VPC 或想要確認組態，您可以驗證路由表的下列詳細資訊是否正確：

- 與您 NAT 閘道所在之子網路關聯的路由表必須包含將網際網路流量指向網際網路閘道的路由。這可確保您的 NAT 閘道可以存取網際網路。
- 與您私有子網路建立關聯的路由表，必須設定為將網際網路流量指向 NAT 閘道。這可讓您私有子網路中的串流執行個體與網際網路通訊。

確認並為您的子網路路由表命名

1. 在導覽窗格中，選擇子網路，然後選取公有子網路。例如，WSB-VPC-subnet-public1-us-east-1a。
2. 在 Route Table (路由表) 標籤上，請選擇路由表的 ID。例如，rtb-12345678。
3. 選取 路由表。在名稱下，選擇編輯 (鉛筆) 圖示，然後輸入路由表的名稱。例如，輸入名稱 **workspacesweb-public-routetable**。選取打勾記號以儲存名稱。
4. 在已選取公有路由表的情況下，於路由標籤確認本機端流量有兩個路由，且有一個路由會將所有其他流量傳送到 VPC 網際網路閘道。下表說明這兩種路由：

目標	Target	Description
公有子網路 IPv4 CIDR 區塊 (例如 10.0.0.0/20)	區域	公有子網路 IPv4 CIDR 區塊中，以 IPv4 地址為目標的資源流量。此流量會在 VPC 內進行本機路由傳送。
以所有其他 IPv4 地址 (例如 0.0.0.0/0) 為目標的流量	流出 (igw-ID)	以所有其他 IPv4 地址為目標的流量，都會路由至 VPC 精靈所建立的網際網路閘道 (以 igw-ID 識別)。

5. 在導覽窗格中，選擇 Subnets (子網)。然後，選取私有子網路（例如 **WSB-VPC-subnet-private1-us-east-1a**)。
6. 在路由表標籤上，請選擇路由表的 ID。
7. 選取 路由表。在名稱下，選擇編輯 (鉛筆) 圖示，然後輸入路由表的名稱。例如，輸入名稱 **WSB-VPC-private-routetable**。若要儲存名稱，請選擇核取記號。

8. 在 Routes (路由) 標籤上，請確認路由表包含以下路由：

目標	Target	Description
公有子網路 IPv4 CIDR 區塊 (例如 10.0.0.0/20)	區域	公有子網路 IPv4 CIDR 區塊中，以 IPv4 地址為目標的資源流量都會在 VPC 內進行本機路由。
以所有其他 IPv4 地址 (例如 0.0.0.0/0) 為目標的流量	流出 (nat-ID)	以所有其他 IPv4 地址為目標的流量，都會路由至 NAT 閘道 (以 nat-ID 識別)。
以 S3 儲存貯體為目標的流量 (如果您指定 S3 端點，則適用)[pl-ID (com.amazonaws.region.s3)]	儲存裝置 (vpce-ID)	以 S3 儲存貯體為目標的流量會路由至 S3 端點 (以 vpce-ID 識別)。

9. 在導覽窗格中，選擇 Subnets (子網)。然後選取您建立的第二個私有子網路 (例如，**WorkSpaces Secure Browser Private Subnet2**)。
10. 在路由表標籤上，請確認選定的路由表為私有路由表 (例如，**workspacesweb-private-routetable**)。如果路由表不同，請選擇編輯改為選取您的私有路由表。

啟用 Amazon WorkSpaces 安全瀏覽器的網際網路瀏覽

您可以選擇啟用不受限制的網際網路瀏覽 （ 建議選項 ） 或受限制的網際網路瀏覽。

主題

- 啟用 Amazon WorkSpaces 安全瀏覽器的無限制網際網路瀏覽 （ 建議 ）
- 啟用 Amazon WorkSpaces 安全瀏覽器的限制網際網路瀏覽
- Amazon WorkSpaces 安全瀏覽器的網際網路連線連接埠

啟用 Amazon WorkSpaces 安全瀏覽器的無限制網際網路瀏覽 （ 建議 ）

請依照下列步驟設定具有 NAT 閘道的 VPC，以進行不受限制的網際網路瀏覽。這可讓 WorkSpaces 安全瀏覽器存取公有網際網路上的網站，以及在 VPC 中託管或與 VPC 連線的私有網站。

設定具有 NAT 閘道的 VPC，以進行不受限制的網際網路瀏覽

如果您希望 WorkSpaces 安全瀏覽器入口網站同時存取公有網際網路內容和私有 VPC 內容，請遵循下列步驟：

> **Note**
>
> 如果您已經設定好 VPC，請完成以下步驟來將 NAT 閘道新增至 VPC。如果您需要建立新的 VPC，請參閱為 Amazon WorkSpaces 安全瀏覽器建立新的 VPC。

1. 若要建立 NAT 閘道，請完成建立 NAT 閘道中的步驟。請確定此 NAT 閘道具有公用連線，且位於 VPC 中的公用子網路中。
2. 您必須在不同的可用區域內指定至少兩個私有子網路。將子網路指派給不同的可用區域，有助於確保更好的可用性和容錯能力。如需如何使用私有子網路建立 VPC 的詳細資訊，請參閱 the section called “快速 VPC 設定”。

   > **Note**
   >
   > 為了確保每個串流執行個體都能存取網際網路，請勿將公有子網路連接至 WorkSpaces 安全瀏覽器入口網站。

3. 更新與您的私有子網路關聯的路由表，將網際網路的流量指向 NAT 閘道。這可讓您私有子網路中的串流執行個體與網際網路通訊。如需有關如何將路由表與私有子網路產生關聯的資訊，請完成設定路由表中的步驟。

啟用 Amazon WorkSpaces 安全瀏覽器的限制網際網路瀏覽

WorkSpaces 安全瀏覽器入口網站的建議網路設定是使用具有 NAT 閘道的私有子網路，以便入口網站可以瀏覽公有網際網路和私有內容。如需詳細資訊，請參閱the section called “不受限制的網際網路瀏覽”。不過，您可能需要使用 Web 代理控制從 WorkSpaces 安全瀏覽器入口網站到網際網路的傳出通訊。例如，如果您使用 Web 代理做為網際網路的閘道，您可以實作預防性安全控制，例如網域允許清單和內容篩選。這也可以透過快取經常存取的資源來減少頻寬使用量並改善網路效能，例如本機的網頁或軟體更新。對於某些使用案例，您可能擁有只能使用 Web 代理存取的私有內容。

您可能已經熟悉在受管裝置或虛擬環境的映像上設定代理設定。但是，如果您無法控制裝置（例如，當使用者位於非由企業擁有或管理的裝置上時），或者如果您需要管理虛擬環境的映像，這會構成挑

戰。使用 WorkSpaces 安全瀏覽器，您可以使用 Web 瀏覽器中內建的 Chrome 政策來設定代理設定。您可以透過設定 WorkSpaces 安全瀏覽器的 HTTP 傳出代理來執行此操作。

此解決方案是以建議的傳出 VPC 代理設定為基礎。代理解決方案是以開放原始碼 HTTP Proxy Squid 為基礎。然後，它會使用 WorkSpaces 安全瀏覽器瀏覽器設定來設定 WorkSpaces 安全瀏覽器入口網站以連線至代理端點。如需詳細資訊，請參閱如何使用網域白名單和內容篩選來設定傳出 VPC 代理。

此解決方案為您提供下列優點：

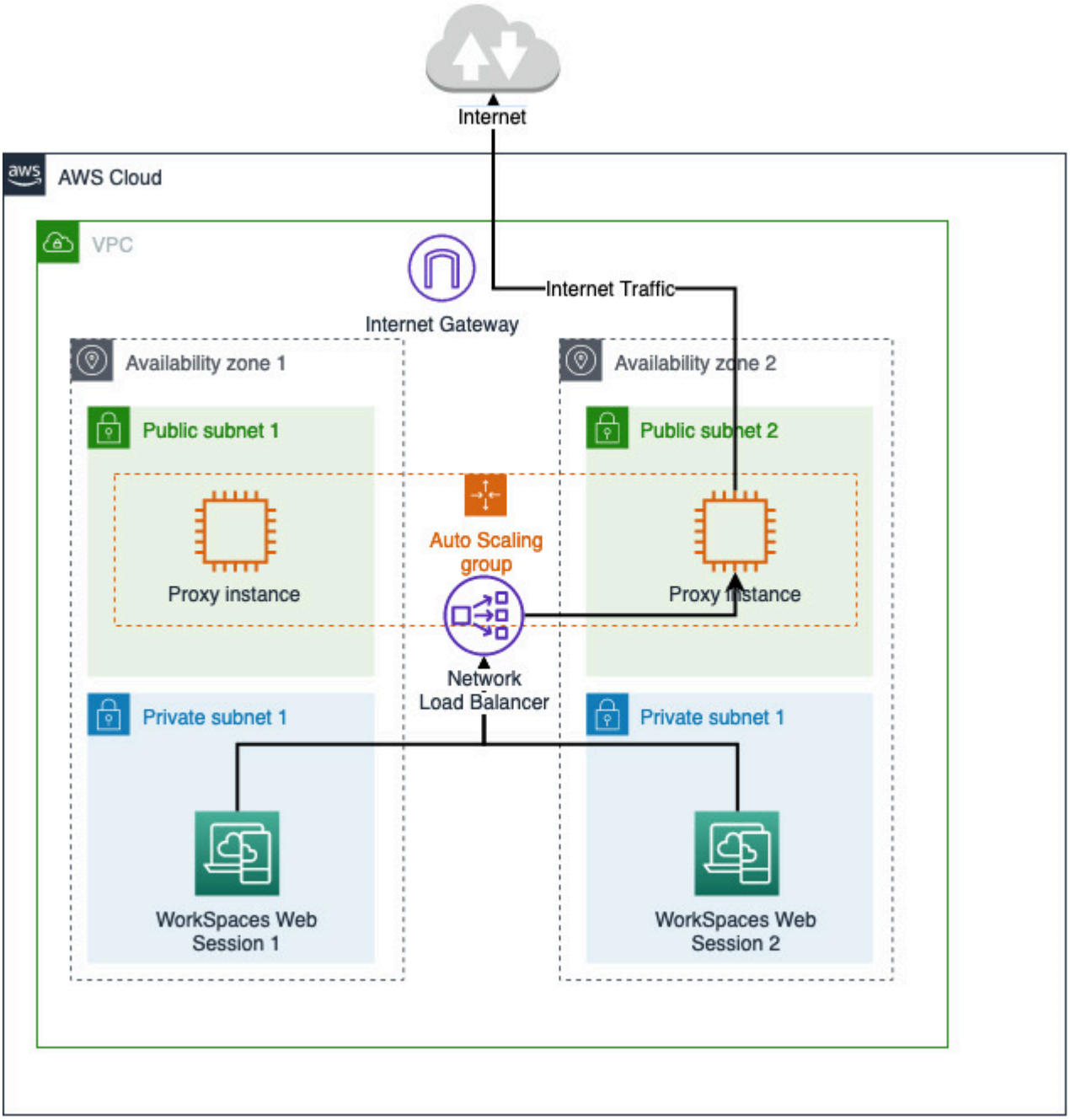
- 傳出代理，其中包含一組由網路負載平衡器託管的自動擴展 Amazon EC2 執行個體。Proxy 執行個體位於公有子網路中，且每個執行個體都連接彈性 IP，因此可以存取網際網路。
- 部署至私有子網路的 WorkSpaces 安全瀏覽器入口網站。您不需要設定 NAT 閘道來啟用網際網路存取。相反地，您可以設定瀏覽器政策，因此所有網際網路流量都會通過傳出代理。如果您想要使用自己的代理，WorkSpaces 安全瀏覽器入口網站設定將相似。

主題

- Amazon WorkSpaces 安全瀏覽器的受限網際網路瀏覽架構
- Amazon WorkSpaces 安全瀏覽器的受限網際網路瀏覽先決條件
- Amazon WorkSpaces 安全瀏覽器的 HTTP 傳出代理
- 對 Amazon WorkSpaces 安全瀏覽器的限制網際網路瀏覽進行故障診斷

Amazon WorkSpaces 安全瀏覽器的受限網際網路瀏覽架構

以下是 VPC 中典型代理設定的範例。代理 Amazon EC2 執行個體位於公有子網路中並與彈性 IP 相關聯，因此可以存取網際網路。網路負載平衡器託管代理執行個體的自動擴展群組。這可確保代理執行個體可以自動擴展，而網路負載平衡器是單一代理端點，可供 WorkSpaces 安全瀏覽器工作階段使用。



Amazon WorkSpaces 安全瀏覽器的受限網際網路瀏覽先決條件

開始之前，請確定您符合下列先決條件：

- 您需要已部署的 VPC，其中公有和私有子網路分散在數個可用區域 (AZs) 上。如需如何設定 VPC 環境的詳細資訊，請參閱預設 VPCs。

- 您需要一個可從私有子網路存取的單一代理端點，其中 WorkSpaces 安全瀏覽器工作階段為即時（例如網路負載平衡器 DNS 名稱）。如果您想要使用現有的代理，請確定它也具有可從私有子網路存取的單一端點。

Amazon WorkSpaces 安全瀏覽器的 HTTP 傳出代理

若要設定 WorkSpaces 安全瀏覽器的 HTTP 傳出代理，請遵循下列步驟。

1. 若要將範例傳出代理部署到您的 VPC，請遵循如何使用網域白名單和內容篩選來設定傳出 VPC 代理中的步驟。
   a. 請依照「安裝（一次性設定）」中的步驟，將 CloudFormation 範本部署至您的帳戶。請務必選擇正確的 VPC 和子網路做為 CloudFormation 範本參數。
   b. 部署之後，請尋找 CloudFormation 輸出參數 OutboundProxyDomain 和 OutboundProxyPort。這是代理的 DNS 名稱和連接埠。
   c. 如果您已有自己的代理，請略過此步驟，並使用代理的 DNS 名稱和連接埠。
2. 在 WorkSpaces 安全瀏覽器、主控台中，選取您的入口網站，然後選擇編輯。
   a. 在網路連線詳細資訊中，選擇可存取代理的 VPC 和私有子網路。
   b. 在政策設定中，使用 JSON 編輯器新增下列 ProxySettings 政策。`ProxyServer` 欄位應該是代理的 DNS 名稱和連接埠。如需 ProxySettings 政策的詳細資訊，請參閱 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. 在 WorkSpaces 安全瀏覽器工作階段中，您會看到代理套用到 Chrome 設定 Chrome 使用管理員的代理設定。

4. 前往 chrome：//policy 和 Chrome 政策索引標籤，確認政策已套用。
5. 確認您的 WorkSpaces 安全瀏覽器工作階段可以在沒有 NAT 閘道的情況下成功瀏覽網際網路內容。在 CloudWatch Logs 中，確認已記錄 Squid 代理存取日誌。

對 Amazon WorkSpaces 安全瀏覽器的限制網際網路瀏覽進行故障診斷

套用 Chrome 政策後，如果您的 WorkSpaces 安全瀏覽器工作階段仍然無法存取網際網路，請依照下列步驟嘗試解決您的問題：

- 確認代理端點可從 WorkSpaces 安全瀏覽器入口網站所在的私有子網路存取。若要這樣做，請在私有子網路中建立 EC2 執行個體，並測試從私有 EC2 執行個體到代理端點的連線。
- 確認代理具有網際網路存取。
- 驗證 Chrome 政策是否正確。
  - 確認政策 `ProxyServer` 欄位的下列格式：`<Proxy DNS name>:<Proxy port>`。字首`https://`中應該沒有 `http://`或 。
  - 在 WorkSpaces 安全瀏覽器工作階段中，使用 Chrome 導覽至 chrome：//policy，並確保成功套用 ProxySettings 政策。

Amazon WorkSpaces 安全瀏覽器的網際網路連線連接埠

每個 WorkSpaces 安全瀏覽器串流執行個體都有一個客戶網路介面，可讓您連線至 VPC 內的資源，以及設定具有 NAT 閘道的私有子網路時連線至網際網路。

針對網際網路連線，下列連接埠必須對所有目的地開放。如果您使用修改過或自訂的安全群組，則需要手動新增所需規則。如需詳細資訊，請參閱安全群組規則。

> **Note**
>
> 這適用於出口流量。

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

WorkSpaces 安全瀏覽器的 VPC 最佳實務

下列建議可協助您更有效率且安全地設定 VPC，

整體 VPC 組態

- 請確定您的 VPC 組態能夠支援擴展需求。
- 請確定您的 WorkSpaces 安全瀏覽器服務配額（也稱為限制）足以支援您的預期需求。若要請求增加配額，您可以使用 Service Quotas 主控台，位於 https://console.aws.amazon.com/servicequotas/。如需預設 WorkSpaces 安全瀏覽器配額的相關資訊，請參閱 the section called “管理服務配額”。
- 如果您打算提供串流工作階段存取網際網路的權限，建議您在公有子網路中設定具有 NAT 閘道的 VPC。

彈性網路界面

- 每個 WorkSpaces 安全瀏覽器工作階段在串流期間都需要自己的彈性網路界面。WorkSpaces 安全瀏覽器會建立與機群所需容量上限一樣多的彈性網路介面 (ENIs)。每個區域的 ENI 限制預設為 5000。如需詳細資訊，請參閱網路介面。

  規劃大型部署的容量 (例如，數千個同時串流的工作階段) 時，請考慮尖峰使用量可能需要的 ENI 數量。我們建議您將 ENI 限制保持在或高於您為 Web 入口網站設定的最大同時使用量限制。

子網路

- 當您制定擴展使用者的計劃時，請記住，每個 WorkSpaces 安全瀏覽器工作階段都需要您設定的子網路中唯一的用戶端 IP 地址。因此，子網路上設定的用戶端 IP 地址空間大小會決定可同時串流的使用者數量。
- 我們建議為各個子網路設定子網路遮罩，該遮罩必須具備足夠的用戶端 IP 地址來應付預期的最大同時上線使用者數量，此外也要考慮加入額外的 IP 地址來因應帳戶的預期成長。如需詳細資訊，請參閱 VPC 和 IPv4 的子網路大小調整。
- 我們建議您在 WorkSpaces 安全瀏覽器在所需區域中支援的每個唯一可用區域中設定子網路，以考慮可用性和擴展。如需詳細資訊，請參閱the section called “建立新的 VPC”。
- 請確保可透過您的子網路存取網路應用程式所需的網路資源。

安全群組

- 使用安全群組來為 VPC 提供額外的存取控制。

  屬於 VPC 的安全群組可讓您控制 WorkSpaces 安全瀏覽器串流執行個體與 Web 應用程式所需的網路資源之間的網路流量。確認安全群組可提供您網路應用程式所需的網路資源存取權。

Amazon WorkSpaces 安全瀏覽器支援的可用區域

當您建立虛擬私有雲端 (VPC) 以搭配 WorkSpaces 安全瀏覽器使用時，VPC 的子網路必須位於您啟動 WorkSpaces 安全瀏覽器的區域中的不同可用區域。可用區域是代表不同的位置，旨在隔離其他可用區域的故障。藉由在個別的可用區域中啟動執行個體，您就可以保護應用程式免於發生單點故障。各個子網必須完全位於某一可用區域內，不得跨越多個區域。我們建議您為所需區域中每個有支援的可用區域設定子網路，以獲得最大的恢復能力

可用區域以區域代碼加上字母識別符表示；例如 `us-east-1a`。為確保資源分配至區域中的所有可用區域，可用區域會獨立映射至各個 AWS 帳戶的名稱。例如，您 `us-east-1a` 帳戶的可用區域 AWS 與其他 `us-east-1a` 帳戶的 AWS 可能不在同一位置。

為協調各帳戶的可用區域，您必須使用 AZ ID，這是可用區域唯一且一致的識別符。例如， `use1-az2` 是 `us-east-1` 區域的 AZ ID，而且在每個 AWS 帳戶中都有相同的位置。

檢視 AZ ID 能讓您判斷某個帳戶資源在另一個帳戶中的相對位置。例如，如果您與另一個帳戶共享 AZ ID 為 `use1-az2` 的可用區域子網路，則 AZ ID 也是 `use1-az2` 之可用區域中的該帳戶就可以使用此子網路。Amazon VPC 主控台會顯示各 VPC 和子網路的 AZ ID。

WorkSpaces 安全瀏覽器可在每個支援區域的可用區域子集中使用。下表列出您可用於每個區域的 AZ ID。若要查看帳戶中 AZ ID 與可用區域的對應，請參閱《AWS RAM 使用者指南》中的資源適用的 AZ ID。

區域名稱	區域代碼	支援的 AZ ID
美國東部 (維吉尼亞北部)	`us-east-1`	`use1-az1`, `use1-az2`, `use1-az4`, `use1-az5`, `use1-az6`
美國西部 (奧勒岡)	`us-west-2`	`usw2-az1`, `usw2-az2`, `usw2-az3`
亞太地區 (孟買)	`ap-south-1`	`aps1-az1`, `aps1-az3`

區域名稱	區域代碼	支援的 AZ ID
亞太地區 (新加坡)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
亞太地區 (雪梨)	ap-southeast-2	apse2-az1 , apse2-az2 , apse2-az3
亞太區域 (東京)	ap-northeast-1	apne1-az1 , apne1-az2 , apne1-az4
加拿大 (中部)	ca-central-1	cac1-az1, cac1-az2, cac1-az4
歐洲 (法蘭克福)	eu-central-1	euc1-az2, euc1-az2, euc1-az3
歐洲 (愛爾蘭)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
歐洲 (倫敦)	eu-west-2	euw2-az1, euw2-az2

如需可用區域和可用區域 IDs 的詳細資訊，請參閱《Amazon EC2 使用者指南》中的區域、可用區域和本機區域。

啟用 Amazon WorkSpaces 安全瀏覽器的使用者連線

WorkSpaces 安全瀏覽器設定為透過公有網際網路路由串流連線。需要網際網路連線才能驗證使用者，並提供 WorkSpaces 安全瀏覽器運作所需的 Web 資產。若要允許此流量，您必須允許 Amazon WorkSpaces 安全瀏覽器的允許網域 中所列的網域。

下列主題提供如何啟用 WorkSpaces 安全瀏覽器使用者連線的相關資訊。

主題

- Amazon WorkSpaces 安全瀏覽器的 IP 地址和連接埠需求
- Amazon WorkSpaces 安全瀏覽器的允許網域

Amazon WorkSpaces 安全瀏覽器的 IP 地址和連接埠需求

若要存取 WorkSpaces 安全瀏覽器執行個體，使用者裝置需要在下列連接埠上進行傳出存取：

- 連接埠 443 (TCP)
  - 連接埠 443 用於在使用網際網路端點時，使用者裝置和串流執行個體之間的 HTTPS 通訊。一般而言，最終使用者在串流工作階段期間瀏覽 Web 時，網頁瀏覽器會隨機選取串流流量高範圍的來源連接埠。您必須確保允許對此連接埠的傳回流量。
  - 此連接埠必須開啟，才能使用 Amazon WorkSpaces 安全瀏覽器的允許網域 所列的必要網域。
  - AWS 會以 JSON 格式發佈其目前的 IP 地址範圍，包括 Session Gateway 和 CloudFront 網域可能解析的範圍。如需如何下載 .json 檔案及檢視目前範圍的詳細資訊，請參閱 AWS IP 地址範圍。或者，如果您使用的是 AWS Tools for Windows PowerShell，您可以使用 Get-AWSPublicIpAddressRange PowerShell 命令存取相同的資訊。如需詳細資訊，請參閱查詢 AWS 的公有 IP 地址範圍相關文章。
- (選用) 連接埠 53 (UDP)
  - 連接埠 53 用於使用者裝置和您 DNS 伺服器間的通訊。
  - 如果您未使用 DNS 伺服器進行網域名稱解析，則此連接埠為選用。
  - 連接埠必須開放給 DNS 伺服器的 IP 地址，以便解析公有網域名稱。

Amazon WorkSpaces 安全瀏覽器的允許網域

若要讓使用者能夠從本機瀏覽器存取 Web 入口網站，您必須將下列網域新增至使用者嘗試存取服務之網路上的允許清單。

在下表中，將 *{region}* 取代為操作 Web 入口網站區域的程式碼。例如，歐洲（愛爾蘭）區域的 Web 入口網站的 s3.*{region}*.amazonaws.com 應為 s3.eu-west-1.amazonaws.com。如需區域代碼清單，請參閱 Amazon WorkSpaces 安全瀏覽器端點和配額。

Category	網域或 IP 地址
WorkSpaces 安全瀏覽器串流資產	s3.*{region}*.amazonaws.com s3.amazonaws.com appstream2.*{region}*.aws.amazon.com *.amazonappstream.com

Category	網域或 IP 地址
	*.shortbread.aws.dev
WorkSpaces 安全瀏覽器靜態資產	*.workspaces-web.com di5ry4hb4263e.cloudfront.net
WorkSpaces 安全瀏覽器身分驗證	*.auth.*{region}*.amazoncognito.com cognito-identity.*{region}*.amazonaws.com cognito-idp.*{region}*.amazonaws.com *.cloudfront.net
WorkSpaces 安全瀏覽器指標和報告	*.execute-api.*{region}*.amazonaws.com unagi-na.amazon.com

根據您設定的身分提供者，您可能也需要允許列出其他網域。檢閱 IdP 的文件，以識別您需要允許清單的網域，以便 WorkSpaces 安全瀏覽器使用該提供者。如果您使用的是 IAM Identity Center，請參閱 IAM Identity Center 先決條件以取得更詳細的資訊。

Amazon WorkSpaces 安全瀏覽器入門

請依照下列步驟建立 WorkSpaces 安全瀏覽器 Web 入口網站，並提供使用者從其現有瀏覽器存取內部和 SaaS 網站的權限。您可以在每個帳戶的任何支援區域建立一個 Web 入口網站。

> **Note**
>
> 若要請求提高多個入口網站的限制，請使用您的 AWS 帳戶 ID、要請求的入口網站數量和 聯絡支援 AWS 區域。

這個作業使用 Web 入口網站建立精靈，通常要 5 分鐘的時間，而入口網站最多還要 15 分鐘的時間才能成為作用中狀態。

設定 Web 入口網站不會產生任何相關費用。WorkSpaces 安全瀏覽器提供pay-as-you-go的定價，包括主動使用服務的使用者低廉的每月價格。您將無需先預付成本、授權或簽訂長期合約。

> **Important**
>
> 您必須在開始前先完成 Web 入口網站的先決條件。如需 Web 入口網站先決條件的詳細資訊，請參閱 設定 Amazon WorkSpaces 安全瀏覽器。

主題

為 Amazon WorkSpaces 安全瀏覽器建立 Web 入口網站

請執行下列步驟以建立 Web 入口網站：

主題

- 設定 Amazon WorkSpaces 安全瀏覽器的使用者設定
- 為 Amazon WorkSpaces 安全瀏覽器設定您的身分提供者
- 使用 Amazon WorkSpaces 安全瀏覽器啟動 Web 入口網站

設定 Amazon WorkSpaces 安全瀏覽器的網路設定

若要設定 WorkSpaces 安全瀏覽器的網路設定，請遵循下列步驟。

1. 在 https：//https://console.aws.amazon.com/workspaces-web/home 開啟 WorkSpaces 安全瀏覽器主控台。
2. 選擇 WorkSpaces 安全瀏覽器，然後選擇 Web 入口網站，然後選擇建立 Web 入口網站。
3. 在步驟 1：指定網路連線頁面上，完成下列步驟，將您的 VPC 連線到 Web 入口網站，並且設定您的 VPC 和子網路。
    1. 如需聯網詳細資訊，請選擇連線至您希望使用者使用 WorkSpaces 安全瀏覽器存取之內容的 VPC。
    2. 選擇最多三個符合下列需求的私有子網路。如需詳細資訊，請參閱Amazon WorkSpaces 安全瀏覽器的網路。
        - 您必須選擇最少兩個私有子網路，才能建立入口網站。
        - 建議您為 VPC 提供唯一可用區域中最大數量的私有子網路，以確保入口網站的高可用性。
    3. 選擇安全群組。

設定 Amazon WorkSpaces 安全瀏覽器的入口網站設定

在步驟 2：進行 Web 入口網站設定頁面上，完成下列步驟，以自訂使用者啟動工作階段時的瀏覽體驗。

1. 在 Web 入口網站詳細資訊底下，針對顯示名稱輸入可識別您入口網站的名稱。
2. 在執行個體類型下，從下拉式功能表中選取 Web 入口網站的執行個體類型。然後，輸入 Web 入口網站的最大並行使用者限制。如需詳細資訊，請參閱the section called “管理服務配額”。

> **Note**
>
> 選取新的執行個體類型會變更每個每月作用中使用者的成本。如需詳細資訊，請參閱 Amazon WorkSpaces 安全瀏覽器定價。

3. 在自訂網域下，您可以設定入口網站的自訂網域，以透過您自己的網域名稱啟用存取，而不是預設入口網站端點。如需詳細資訊，請參閱the section called “自訂網域”。這是選用的。
4. 在工作階段記錄器下，您可以指定用於儲存工作階段日誌檔案的 S3 儲存貯體。如需詳細資訊，請參閱the section called “設定工作階段記錄器”。這是選用的。
5. 在使用者存取記錄下，針對 Kinesis 串流 ID，選取您要傳送日誌檔案的 Amazon Kinesis 資料串流。如需詳細資訊，請參閱the section called “設定使用者活動記錄”。這是選用的。
6. 在 IP 存取控制下，選擇是否限制對受信任網路的存取。如需詳細資訊，請參閱the section called “管理 IP 存取控制”。這是選用的。
7. 在資料保護設定下，您可以為 WorkSpaces 安全瀏覽器建立政策，以修訂敏感資訊。如需詳細資訊，請參閱the section called “資料保護設定”。這是選用的。
8. 在 URL 篩選下，您可以指定 URLs 最終使用者可以存取或封鎖特定 URL 或網域類別以限制存取的 URLs。如需詳細資訊，請參閱the section called “Web 內容篩選”。這是選用的。

    1. 若要限制工作階段瀏覽到幾個選取的網域，請啟用切換封鎖所有 URLs然後按一下新增 URL，以提供最終使用者可存取的 URLs清單。
    2. 若要為最終使用者建立要封鎖的 URLs 清單，請按一下新增 URL 以列出要封鎖URLs，或按一下新增類別以選取封鎖的網域類別（例如社交網路）。
9. 在政策設定下，您可以使用適用於 Web 入口網站最新穩定版本的 Chrome 政策來設定任何瀏覽器政策。如需詳細資訊，請參閱the section called “管理瀏覽器政策”。這是選用的。

    1. 您可以在視覺化編輯器中快速選取一些最常見的政策
        - 對於啟動 URL - 選用，輸入當使用者啟動瀏覽器時要用作首頁的網域。您的 VPC 必須與此 URL 保持穩定連線。
        - 選取或清除隱私瀏覽和刪除歷程記錄，以在使用者工作階段期間開啟或關閉這些功能

        > **Note**
        >
        > 在使用者存取日誌記錄中無法記錄使用隱私瀏覽功能，或在使用者刪除瀏覽器歷程記錄之前造訪的 URL。如需詳細資訊，請參閱the section called “設定使用者活動記錄”。

        - 對於瀏覽器書籤 - 選用，輸入您希望使用者在其瀏覽器中看到的任何書籤的顯示名稱、網域和資料夾。然後，選擇新增書籤。

> **Note**
>
> 網域是瀏覽器書籤的必填欄位。
> Chrome 的使用者可以在書籤工具列的受管理的書籤資料夾中找到受管理的書籤。

2. 您也可以使用 JSON 編輯器而非視覺化編輯器，直接新增或編輯政策。如需政策的特定格式，請參閱 Chrome Enterprise 政策清單。
3. 您也可以將 JSON 檔案上傳至 Web 入口網站，匯入組織中使用的 Chrome 政策。如需詳細資訊，請參閱 the section called “教學課程：設定自訂瀏覽器政策”

   上傳政策檔案時，您可以在主控台中看到可用的政策檔案。但是，您無法在視覺化編輯器中編輯所有政策。主控台會列出您無法在其他 JSON 政策下使用視覺化編輯器編輯的 JSON 檔案政策。您必須用手動編輯的方式，才能更動這些政策。

10. 將標籤新增至您的入口網站。您可以使用標籤來搜尋或篩選 AWS 資源。標籤由金鑰和選用值組成，且與您的入口網站資源相關聯。這是選用的。
11. 選擇 Next (下一步) 繼續。

設定 Amazon WorkSpaces 安全瀏覽器的使用者設定

在步驟 3：選取使用者設定頁面上完成下列步驟，選擇使用者在工作階段期間可從頂端導覽列存取的功能，然後選擇下一步：

1. 在品牌自訂下，您可以透過修改視覺元素、文字內容和服務條款，自訂顯示給最終使用者的登入和載入畫面。如需詳細資訊，請參閱the section called “品牌自訂”。這是選用的。
2. 在許可下，選擇是否啟用單一登入的延伸。如需詳細資訊，請參閱the section called “管理單一登入延伸模組”。
3. 對於允許使用者從其 Web 入口網站列印到本機裝置，請選擇允許或不允許。
4. 針對允許使用者深層連結至其 Web 入口網站，選擇允許或不允許。如需深度連結的詳細資訊，請參閱 the section called “深層連結”。
5. 針對允許使用者在其入口網站工作階段中使用本機身分驗證，選擇允許或不允許。如需 Web 身分驗證的詳細資訊，請參閱 the section called “Web 身分驗證重新導向”。
6. 在工具列控制項下，選擇您要在功能下進行的設定。
7. 在設定下，管理工作階段開始時的工具列呈現檢視，包括工具列狀態（停駐或分離）、佈景主題（深色或淺色模式）、圖示可見性和工作階段的最大顯示解析度。未設定這些設定，以授予最終使用者對這些選項的完全控制權。如需詳細資訊，請參閱the section called “工具列控制項”。

8. 對於工作階段逾時，請指定下列項目：

   - 針對 Disconnect timeout in minutes (中斷連線逾時 (以分鐘為單位))，選擇在使用者中斷連線之後，串流工作階段會保持作用中的時間長度。如果在這個時間間隔內，使用者於中斷連線或網路中斷後仍嘗試重新連線到此串流工作階段，則會連線到上一個工作階段。否則，它們會連接到具有新串流執行個體的新工作階段。

     如果使用者結束工作階段，則不會套用中斷連線逾時。反之，系統會提示使用者儲存任何開啟的文件，然後立即從串流執行個體中斷連線。接著會終止使用者正在使用的執行個體。

   - 針對 Idle disconnect timeout in minutes (閒置中斷連線逾時 (以分鐘為單位))，選擇要等使用者閒置 (非作用中) 多久後，才讓使用者與其串流工作階段中斷連線，並開始計算 Disconnect timeout in minutes (中斷連線逾時 (以分鐘為單位)) 時間間隔。使用者會在因閒置而中斷連線之前收到通知。如果使用者在 Disconnect timeout in minutes (中斷連線逾時 (以分鐘為單位)) 中指定的時間間隔過去之前就嘗試重新連線至串流工作階段，系統會將使用者連線至其先前的工作階段。否則，它們會連接到具有新串流執行個體的新工作階段。將此值設定為 0 便可加以停用。當此值停用時，使用者就不會由於未活動而導致中斷連線。

     > **Note**
     >
     > 使用者在串流工作階段期間停止提供鍵盤或滑鼠輸入時，會被視為閒置。檔案上傳和下載、音訊輸入、音訊輸出和像素變更無法作為使用者活動。如果使用者在 Idle disconnect timeout in minutes (閒置中斷連線逾時 (以分鐘為單位)) 中的時間間隔過後仍保持閒置狀態，系統便會將其中斷連線。

為 Amazon WorkSpaces 安全瀏覽器設定您的身分提供者

使用下列步驟來設定您的身分提供者 (IdP)。

主題

選擇 Amazon WorkSpaces 安全瀏覽器的身分提供者類型

WorkSpaces 安全瀏覽器提供兩種身分驗證類型：標準 和 AWS IAM Identity Center。您可以在設定身分提供者頁面上選擇要與入口網站搭配使用的身分驗證類型。

- 對於標準（預設選項），請直接將第三方 SAML 2.0 身分提供者（例如 Okta 或 Ping) 與您的入口網站聯合。如需詳細資訊，請參閱the section called “標準身分驗證類型”。標準類型支援 SP 起始和 IdP 起始的身分驗證流程。
- 對於 IAM Identity Center（進階選項），請將 IAM Identity Center 與您的入口網站聯合。若要使用此身分驗證類型，您的 IAM Identity Center 和 WorkSpaces 安全瀏覽器入口網站必須位於相同的 中 AWS 區域。如需詳細資訊，請參閱the section called “IAM Identity Center 身分驗證類型”。

主題

- 設定 Amazon WorkSpaces 安全瀏覽器的標準身分驗證類型
- 設定 Amazon WorkSpaces 安全瀏覽器的 IAM Identity Center 身分驗證類型

設定 Amazon WorkSpaces 安全瀏覽器的標準身分驗證類型

標準身分驗證類型是預設身分驗證類型。它可以支援服務提供者啟動 (SP 啟動） 和身分提供者啟動 (IdP 啟動） 的登入流程，搭配您的 SAML 2.0 相容 IdP。若要設定標準身分驗證類型，請依照下列步驟直接與入口網站聯合第三方 SAML 2.0 IdP（例如 Okta 或 Ping)。

主題

- 在 Amazon WorkSpaces 安全瀏覽器上設定您的身分提供者
- 在您自己的 IdP 上設定 IdP
- 在 Amazon WorkSpaces 安全瀏覽器上完成 IdP 組態
- 搭配 Amazon WorkSpaces 安全瀏覽器使用特定 IdPs 的指引

在 Amazon WorkSpaces 安全瀏覽器上設定您的身分提供者

完成下列步驟以設定您的身分提供者：

1. 在建立精靈的設定身分提供者頁面上，選擇標準。
2. 選擇使用標準 IdP 繼續。
3. 下載 SP 中繼資料檔案，並保持個別中繼資料值的索引標籤開啟。
   - 如果 SP 中繼資料檔案可用，請選擇下載中繼資料檔案以下載服務提供者 (SP) 中繼資料文件，然後在下一個步驟中將服務提供者中繼資料檔案上傳到您的 IdP。如果沒有此項目，使用者將無法登入。
   - 如果您的提供者未上傳 SP 中繼資料檔案，請手動輸入中繼資料值。

4. 在選擇 SAML 登入類型下，選擇 SP 起始和 IdP 起始的 SAML 聲明，或僅 SP 起始的 SAML 聲明。
   - SP 起始和 IdP 起始的 SAML 聲明可讓您的入口網站支援這兩種類型的登入流程。支援 IdP 起始流程的入口網站可讓您向服務聯合身分端點呈現 SAML 聲明，而不需要使用者透過造訪入口網站 URL 來啟動工作階段。
     - 選擇此選項，以允許入口網站接受未經請求的 IdP 起始的 SAML 聲明。
     - 此選項需要在 SAML 2.0 Identity Provider 中設定預設轉送狀態。入口網站的轉送狀態參數位於 IdP 起始的 SAML 登入下的主控台中，或者您可以從 下的 SP 中繼資料檔案複製`<md:IdPInitRelayState>`。
     - 注意
       - 以下是轉送狀態的格式：`redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=Ex Identity-Provider`。
       - 如果您從 SP 中繼資料檔案複製並貼上值，請務必`&` 變更為 `&`。 `&` 是 XML 逸出字元。
   - 僅為入口網站選擇 SP 起始的 SAML 聲明，僅支援 SP 起始的登入流程。此選項將從 IdP 起始的登入流程拒絕未經請求的 SAML 聲明。

   > **Note**
   >
   > 某些第三方 IdPs 可讓您建立自訂 SAML 應用程式，以利用 SP 起始的流程提供 IdP 起始的身分驗證體驗。例如，請參閱新增 Okta 書籤應用程式。

5. 選擇是否要啟用對此提供者的 Sign SAML 請求。SP 啟動的身分驗證可讓您的 IdP 驗證身分驗證請求是否來自入口網站，以防止接受其他第三方請求。
   a. 下載簽署憑證並上傳至您的 IdP。相同的簽署憑證可用於單一登出。
   b. 在 IdP 中啟用已簽署的請求。根據 IdP，名稱可能不同。

   > **Note**
   >
   > RSA-SHA256 是唯一支援請求和預設請求簽署演算法。

6. 選擇是否要啟用需要加密的 SAML 聲明。這可讓您加密來自 IdP 的 SAML 聲明。它可以防止 IdP 和 WorkSpaces 安全瀏覽器之間的 SAML 聲明攔截資料。

> **Note**
>
> 此步驟不提供加密憑證。它會在您的入口網站啟動後建立。啟動入口網站後，請下載加密憑證並將其上傳至您的 IdP。然後，在您的 IdP 中啟用聲明加密（名稱可能不同，取決於 IdP。

7. 選擇是否要啟用單一登出。單一登出可讓您的最終使用者透過單一動作登出其 IdP 和 WorkSpaces 安全瀏覽器工作階段。
   a. 從 WorkSpaces 安全瀏覽器下載簽署憑證，並將其上傳至您的 IdP。這是上一個步驟中用於請求簽署的相同簽署憑證。
   b. 使用單一登出需要在 SAML 2.0 身分提供者中設定單一登出 URL。您可以在 主控台的服務供應商 (SP) 詳細資訊 - 顯示個別中繼資料值，或從 下的 SP `<md:SingleLogoutService>` 中繼資料檔案找到入口網站的單一登出 URL。
   c. 在 IdP 中啟用單一登出。根據 IdP，名稱可能不同。

在您自己的 IdP 上設定 IdP

若要在您自己的 IdP 上設定 IdP，請遵循下列步驟。

1. 在瀏覽器中開啟新的分頁。
2. 將入口網站中繼資料新增至 SAML IdP。

   您可以將您在上一個步驟中下載的 SP 中繼資料文件上傳至 IdP，或將中繼資料值複製並貼到 IdP 中的正確欄位中。有些供應商不允許檔案上傳。

   此程序的詳細資訊可能因供應商而異。在 中尋找供應商的文件the section called “特定 IdPs 的指引”，以取得如何將入口網站詳細資訊新增至 IdP 組態的說明。
3. 確認您的 SAML 聲明的 NameID。

   請確定您的 SAML IdP 將使用者電子郵件欄位填入 SAML 聲明中的 NameID。NameID 和使用者電子郵件用於透過 入口網站唯一識別您的 SAML 聯合身分使用者。使用持久性 SAML 名稱 ID 格式。
4. 選用：設定 IdP 起始身分驗證的轉送狀態。

   如果您在上一個步驟中選擇接受 SP 起始和 IdP 起始的 SAML 聲明，請遵循 的步驟 2the section called “WorkSpaces 安全瀏覽器上的 IdP 組態”，為您的 IdP 應用程式設定預設轉送狀態。

5. 選用：設定請求簽署。如果您在上一個步驟中選擇簽署 SAML 請求給此提供者，請遵循 的步驟 3，將簽署憑證the section called “WorkSpaces 安全瀏覽器上的 IdP 組態”上傳到您的 IdP 並啟用請求簽署。某些 IdPs，例如 Okta，可能需要您的 NameID 屬於「持久性」類型才能使用請求簽署。請務必遵循上述步驟，確認 SAML 聲明的 NameID。
6. 選用：設定宣告加密。如果您選擇需要此提供者的加密 SAML 聲明，請等待入口網站建立完成，然後遵循以下「上傳中繼資料」中的步驟 4，將加密憑證上傳到您的 IdP 並啟用聲明加密。
7. 選用：設定單一登出。如果您選擇單一登出，請遵循 的步驟 5，將簽署憑證the section called “WorkSpaces 安全瀏覽器上的 IdP 組態”上傳到您的 IdP、填寫單一登出 URL，並啟用單一登出。
8. 將存取權授予 IdP 中的使用者，以使用 WorkSpaces 安全瀏覽器。
9. 從您的 IdP 下載中繼資料交換檔案。您將在下一個步驟中將此中繼資料上傳至 WorkSpaces 安全瀏覽器。

在 Amazon WorkSpaces 安全瀏覽器上完成 IdP 組態

若要在 WorkSpaces 安全瀏覽器上完成 IdP 組態，請遵循下列步驟。

1. 返回 WorkSpaces 安全瀏覽器。在建立精靈的設定身分提供者頁面的 IdP 中繼資料下，上傳中繼資料檔案，或從 IdP 輸入中繼資料 URL。入口網站會從您的 IdP 使用此中繼資料來建立信任。
2. 若要上傳中繼資料檔案，請在 IdP 中繼資料文件下，選擇選擇檔案。上傳您在上一個步驟中從 IdP 下載的 XML 格式中繼資料檔案。
3. 若要使用中繼資料 URL，請前往您在上一個步驟中設定的 IdP，並取得其中繼資料 URL。返回 WorkSpaces 安全瀏覽器主控台，然後在 IdP 中繼資料 URL 下，輸入您從 IdP 取得的中繼資料 URL。
4. 完成時請選擇 Next (下一步)。
5. 對於您已啟用此提供者要求加密 SAML 聲明選項的入口網站，您需要從入口網站 IdP 詳細資訊區段下載加密憑證，並將其上傳至您的 IdP。然後，您可以在該處啟用 選項。

> **Note**
>
> WorkSpaces 安全瀏覽器要求在 IdP 設定中的 SAML 聲明中映射和設定主體或 NameID。您的 IdP 可以自動建立這些對映。如果未正確設定這些對映，您的使用者將無法登入 Web 入口網站和啟動工作階段。
>
> WorkSpaces 安全瀏覽器要求 SAML 回應中存在下列宣告。您可以透過主控台或 CLI，從入口網站的服務提供者詳細資訊或中繼資料文件找到 *<## SP ## ID>* 和 *<## SP ACS URL>*。

- 具有 Audience值的AudienceRestriction宣告，可將 SP 實體 ID 設定為回應的目標。範例：

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

- InResponseTo 值為原始 SAML 請求 ID 的 Response 宣告。範例：

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

- 具有 SP ACS URL Recipient值的SubjectConfirmationData宣告，以及符合原始 SAML 請求 ID InResponseTo的值。範例：

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

WorkSpaces 安全瀏覽器會驗證您的請求參數和 SAML 聲明。對於 IdP 起始的 SAML 聲明，請求的詳細資訊必須格式化為 HTTP POST 請求內文中的RelayState參數。請求內文也必須包含您的 SAML 聲明做為SAMLResponse參數。如果您已遵循上一個步驟，這兩者都應該存在。
以下是 IdP 起始 SAML 提供者的範例POST內文。

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

搭配 Amazon WorkSpaces 安全瀏覽器使用特定 IdPs 的指引

為了確保您正確設定入口網站的 SAML 聯合，請參閱以下連結以取得常用 IdPs 的文件。

IdP	SAML 應用程式設定	使用者管理	IdP 起始的身分驗證	請求簽署	宣告加密	單一登出
Okta	建立 SAML 應用程式整合	使用者管理	應用程式整合精靈 SAML 欄位參考	應用程式整合精靈 SAML 欄位參考	應用程式整合精靈 SAML 欄位參考	應用程式整合精靈 SAML 欄位參考
Entra	建立您自己的應用程式	快速入門：建立和指派使用者帳戶	啟用企業應用程式的單一登入	SAML 請求簽章驗證	設定 Microsoft Entra SAML 字符加密	單一登出 SAML 通訊協定
Ping	新增 SAML 應用程式	使用者	啟用 IdP 起始的 SSO	在 PingOne for Enterprise 中設定身分驗證請求簽署	PingOne for Enterprise 是否支援加密？	SAML 2.0 單一登出
一次登入	SAML Custom Connector （進階） (4266907)	手動將使用者新增至 OneLogin	SAML Custom Connector （進階） (4266907)	SAML Custom Connector （進階） (4266907)	SAML Custom Connector （進階） (4266907)	SAML Custom Connector （進階） (4266907)
IAM Identity Center	設定您自己的 SAML 2.0 應用程式	設定您自己的 SAML 2.0 應用程式	設定您自己的 SAML 2.0 應用程式	N/A	N/A	N/A

設定 Amazon WorkSpaces 安全瀏覽器的 IAM Identity Center 身分驗證類型

對於 IAM Identity Center 類型 （進階），您可以將 IAM Identity Center 與入口網站聯合。只有在下列條件適用於您時，才選取此選項：

- 您的 IAM Identity Center 是在與 Web 入口網站相同的 AWS 帳戶 和 AWS 區域 中設定。
- 如果您使用的是 AWS Organizations，則會使用 管理帳戶。

使用 IAM Identity Center 身分驗證類型建立 Web 入口網站之前，您必須將 IAM Identity Center 設定為獨立提供者。如需詳細資訊，請參閱 IAM Identity Center 中的常見任務入門。或者，您可以將 SAML 2.0 IdP 連接到 IAM Identity Center。如需詳細資訊，請參閱連線至外部身分提供者。否則，您將不會有任何使用者或群組可指派給您的 Web 入口網站。

如果您已經在使用 IAM Identity Center，您可以選擇 IAM Identity Center 做為提供者類型，並依照下列步驟從 Web 入口網站新增、檢視或移除使用者或群組。

> **Note**
>
> 若要使用此身分驗證類型，IAM Identity Center 必須與 WorkSpaces 安全瀏覽器入口網站位於相同 AWS 帳戶 和 AWS 區域 。如果您的 IAM Identity Center 位於不同的 AWS 帳戶 或 中 AWS 區域，請遵循標準身分驗證類型的指示。如需詳細資訊，請參閱the section called “標準身分驗證類型”。
>
> 如果您使用的是 AWS Organizations，您只能使用管理帳戶建立與 IAM Identity Center 整合的 WorkSpaces 安全瀏覽器入口網站。

主題

使用 IAM Identity Center 建立 Web 入口網站

若要使用 IAM Identity Center 建立 Web 入口網站，請遵循下列步驟。

使用 IAM Identity Center 來建立 Web 入口網站

1. 在步驟 4：設定身分提供者的入口網站建立期間，選擇 AWS IAM Identity Center。
2. 選擇使用 IAM Identity Center 繼續。
3. 在指派使用者和群組頁面上，選擇使用者和/或群組索引標籤。

4. 勾選您要新增至入口網站的 user(s) 或 group(s) 旁的方塊。
5. 建立入口網站之後，您相關聯的使用者可以使用其 IAM Identity Center 使用者名稱和密碼登入 WorkSpaces 安全瀏覽器。

使用 IAM Identity Center 管理您的 Web 入口網站

若要使用 IAM Identity Center 管理您的 Web 入口網站，請遵循下列步驟。

使用 IAM Identity Center 來管理 Web 入口網站

1. 建立入口網站之後，它會在 IAM Identity Center 主控台中列為已設定的應用程式。
2. 若要存取此應用程式的組態設定，請在側邊欄中選擇應用程式，然後尋找名稱與 Web 入口網站顯示名稱相符的已設定應用程式。

> **Note**
>
> 如果您尚未輸入顯示名稱，則會改為顯示入口網站的 GUID。GUID 是您入口網站端點 URL 前置詞的 ID。

將其他使用者和群組新增至 Web 入口網站

若要將其他使用者和群組新增至現有的 Web 入口網站，請遵循下列步驟。

將其他使用者和群組新增至現有的 Web 入口網站

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 WorkSpaces 安全瀏覽器、Web 入口網站、選擇您的 Web 入口網站，然後選擇編輯。
3. 選擇身分提供者設定和指派其他使用者和群組。從這裡，您可以將使用者和群組新增至您的 Web 入口網站。

> **Note**
>
> 您無法從 IAM Identity Center 主控台新增使用者或群組。您必須從 WorkSpaces 安全瀏覽器入口網站的編輯頁面執行此操作。

檢視或移除 Web 入口網站的使用者和群組

若要檢視或移除 Web 入口網站的使用者和群組，請使用指派的使用者資料表中可用的動作。如需詳細資訊，請參閱管理對應用程式的存取

> **Note**
>
> 您無法從 WorkSpaces 安全瀏覽器的編輯頁面檢視或移除使用者和群組。您必須從 IAM Identity Center 主控台的編輯頁面執行這個操作。

變更 Amazon WorkSpaces 安全瀏覽器的身分提供者類型

您可以隨時變更入口網站的身分驗證類型。若要執行此操作，請遵循下列步驟。

- 若要從 IAM Identity Center 變更為標準，請遵循 中的步驟the section called “標準身分驗證類型”。
- 若要從標準變更為 IAM Identity Center，請遵循 中的步驟the section called “IAM Identity Center 身分驗證類型”。

身分提供者類型的變更最多可能需要 15 分鐘才能部署，而且不會自動終止進行中工作階段。

您可以檢查`UpdatePortal`事件 AWS CloudTrail ，透過 檢視入口網站的身分提供者類型變更。類型會顯示在事件的請求和回應承載中。

使用 Amazon WorkSpaces 安全瀏覽器啟動 Web 入口網站

完成 Web 入口網站的設定後，您可以依照下列步驟啟動入口網站。

1. 在步驟 5：檢閱和啟動頁面上，檢閱您為 Web 入口網站選取的設定。您可以選擇 編輯，以變更指定部分中的設定。您也可以稍後從主控台的 Web 入口網站標籤變更這些設定。
2. 完成時，請選擇啟動 Web 入口網站。
3. 若要檢視 Web 入口網站的狀態，請選擇 Web 入口網站，選擇您的入口網站，然後選擇檢視詳細資訊。

   Web 入口網站有下列其中一個狀態：

   - 未完成 – Web 入口網站的組態缺少必要的身分提供者設定。
   - 擱置中 – Web 入口網站正在將變更套用至其設定。

- 作用中 – Web 入口網站已準備就緒且可供使用。

4. 請等待最多 15 分鐘，讓您的入口網站變為作用中狀態。

在 Amazon WorkSpaces 安全瀏覽器中測試您的 Web 入口網站

建立 Web 入口網站後，您可以登入 WorkSpaces 安全瀏覽器端點，像最終使用者一樣瀏覽連線的網站。

如果您已在 the section called “身分提供者組態” 中完成這些步驟，可跳過本部分並且前往 在 Amazon WorkSpaces 安全瀏覽器中分發 Web 入口網站。

1. 在 https：//https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/ 開啟 WorkSpaces 安全瀏覽器主控台。
2. 選擇 WorkSpaces 安全瀏覽器、Web 入口網站、選擇您的 Web 入口網站，然後選擇檢視詳細資訊
3. 在 Web 入口網站端點下，前往入口網站的指定 URL。Web 入口網站端點是您的使用者在使用針對入口網站設定的身分提供者登入後，啟動 Web 入口網站的存取點。它在網際網路上公開提供，且能夠嵌入到您的網路中。
4. 在 WorkSpaces 安全瀏覽器登入頁面上，選擇登入、SAML，然後輸入您的 SAML 憑證。
5. 當您看到您的工作階段正在準備頁面時，WorkSpaces 安全瀏覽器工作階段正在啟動。請勿關閉或離開此頁面。
6. 此時會啟動網頁瀏覽器，並顯示您的啟動 URL，以及透過瀏覽器政策設定所設定的任何其他行為。
7. 您現在可以選擇連結或在網址欄中輸入 URL，以瀏覽已連接的網站。

在 Amazon WorkSpaces 安全瀏覽器中分發 Web 入口網站

當您準備好讓使用者開始使用 WorkSpaces 安全瀏覽器時，您可以從下列選項中選擇分發入口網站：

- 將您的入口網站新增至 SAML 應用程式閘道，讓使用者能夠直接從其 IdP 啟動工作階段。您可以使用符合 SAML 2.0 標準的 IdP，透過 IdP 起始的登入流程執行此操作。如需詳細資訊，請參閱 中的 SP 起始和 IdP 起始的 SAML 聲明the section called “標準身分驗證類型”。或者，您可以建立自訂 SAML 應用程式，透過使用 SP 起始的流程來提供 IdP 起始的身分驗證體驗。如需詳細資訊，請參閱建立書籤應用程式整合。
- 將入口網站 URL 新增至您擁有的網站，然後使用瀏覽器重新導向，將使用者導向 Web 入口網站。

- 透過電子郵件傳送入口網站 URL 給您的使用者，或向下推送至您管理的裝置，當成瀏覽器首頁或書籤。
- 如果您已為入口網站設定自訂網域，而非入口網站 URL，即可為使用者提供更整合的品牌體驗。如需詳細資訊，請參閱the section called “自訂網域”。

在 Amazon WorkSpaces 安全瀏覽器中管理您的 Web 入口網站

設定 Web 入口網站之後，您可以執行下列動作來管理入口網站。

主題

在 Amazon WorkSpaces 安全瀏覽器中檢視 Web 入口網站詳細資訊

若要檢視 Web 入口網站詳細資訊，請遵循下列步驟。

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 WorkSpaces 安全瀏覽器、Web 入口網站、選擇您的 Web 入口網站，然後選擇檢視詳細資訊。

在 Amazon WorkSpaces 安全瀏覽器中編輯 Web 入口網站

若要編輯 Web 入口網站，請遵循下列步驟。

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 WorkSpaces 安全瀏覽器、Web 入口網站、選擇您的 Web 入口網站，然後選擇編輯。

> **Note**
>
> 變更網路設定或逾時設定，會立即結束任何作用中的入口網站工作階段。使用者中斷連線，必須重新連線才能開始新的工作階段。剪貼簿許可、檔案傳輸許可或列印至本機端裝置的變更，會從第一個新的工作階段開始套用。目前作用中的工作階段未中斷連線。連接到作用中工作階段的使用者，在中斷連線並連接到新的工作階段之前不會受到變更的影響。

在 Amazon WorkSpaces 安全瀏覽器中刪除 Web 入口網站

若要刪除 Web 入口網站，請遵循下列步驟。

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 WorkSpaces 安全瀏覽器、Web 入口網站、選擇您的 Web 入口網站，然後選擇刪除。

在 Amazon WorkSpaces 安全瀏覽器中管理入口網站的服務配額

當您建立 時 AWS 帳戶，我們會自動設定資源使用的預設服務配額 （ 也稱為限制 ） AWS 服務。管理員必須知道可能需要增加兩個配額，以支援其使用案例。這兩個配額是您可以在每個區域中建立的 Web 入口網站數量，以及每個區域中每個可用執行個體類型可支援的最大並行工作階段數量。您可以從 AWS 主控台的 Service Quotas 頁面請求提高這些配額。

下表列出預設的服務配額限制。

AWS 區域 依帳戶區分 內的預設配額	Value
Web 入口網站	3
並行工作階段上限 - standard.regular	25
並行工作階段上限 - standard.large	10
並行工作階段上限 - standard.xlarge	5

若要隨時檢視分配給您帳戶的每個區域的服務配額，請參閱 Service Quotas 頁面。

> **Important**
>
> 服務配額 AWS 區域 一次影響一個。您必須在需要更多資源 AWS 區域 的每個 中請求增加服務配額。如需詳細資訊，請參閱 Amazon WorkSpaces 安全瀏覽器端點和配額。

主題

在 Amazon WorkSpaces 安全瀏覽器中請求提高服務配額

若要請求提高服務配額，請遵循下列步驟。

1. 開啟 AWS Support 儀表板。
2. 選擇服務限制提高。

> **Important**
>
> WorkSpaces 安全瀏覽器服務配額一次會影響一個區域。您必須在需要更多資源的每個 AWS 區域申請增加服務配額。如需詳細資訊，請參閱 AWS 服務端點。

3. 在使用案例說明底下輸入下列資訊：
   - 如果您請求增加 Web 入口網站的數量，請指定此資源類型，並且包含您的 AWS 帳戶 ID、要增加的區域及新的限制值。
   - 如果您請求增加同時發生工作階段數量上限，請指定此資源類型，並且包含您的 AWS 帳戶 ID、您想要增加的區域、Web 入口網站 ARN 及新的限制值。
4. (選用) 若要同時請求增加多個服務配額，請完成請求部分中的一個配額增加請求，然後選擇新增其他請求。

在 Amazon WorkSpaces 安全瀏覽器中請求入口網站增加

入口網站是服務的基礎資源。每個入口網站都是 SAML 2.0 身分提供者與網際網路網路連線與任何私有 Web 內容之間的關聯。每個入口網站都可以有個別的入口網站瀏覽器政策和使用者設定，因此管理員通常會在相同區域中建立多個入口網站，以解決不同的使用案例。例如，您可以為群組 A 提供具有限制性政策（例如，剪貼簿和檔案傳輸已停用）的特定網站的存取權，以及群組 B 在沒有 URL 篩選的情況下存取一般網際網路。您可以在任何支援的 中建立入口網站 AWS 區域。若要檢視目前的服務可用性，請參閱依區域的 AWS 服務。

請求增加服務配額

1. 開啟所需區域中Service Quotas頁面。
2. 選擇 Web 入口網站的數量。
3. 選擇請求提高帳戶層級。
4. 在增加配額值下，輸入您想要配額的總量。

在 Amazon WorkSpaces 安全瀏覽器中請求增加並行工作階段上限

並行工作階段配額上限是可同時連線到入口網站的最高使用者數量。如果未適當設定並行工作階段上限的服務配額限制，使用者可能會在登入時發現工作階段無法使用。除了提高此服務配額之外，客戶還必須確保其 VPC 和子網路有足夠的 IP 空間來支援最大並行工作階段。

請求增加最大並行工作階段

1. 在所需區域中開啟 Service Quotas 頁面。
2. 針對您要增加的執行個體類型，選擇每個入口網站的最大並行工作階段數量。
3. 選擇請求提高帳戶層級。
4. 在增加配額值下，輸入您想要配額的總量。

> **Note**
>
> 對於大幅或緊急增加，請前往您的 Service Quotas 歷史記錄頁面，選取請求狀態欄中的連結，連結到您的支援案例，並新增包含使用案例和/或緊急性詳細資訊的回覆。此資訊可協助服務團隊排定請求的優先順序，並確保為您的 帳戶配置足夠的容量。

Amazon WorkSpaces 安全瀏覽器的限制範例

例如，假設管理員在美國東部（維吉尼亞北部）為 125 個使用者設定兩個 Web 入口網站。在建立 Web 入口網站之前，管理員會識別第一個 Web 入口網站（入口網站 A) 將支援 100 個使用者。為這些使用者測試工作流程時，管理員會判斷他們需要 XL 執行個體類型，才能在工作階段期間支援音訊和視訊串流。第二個 Web 入口網站（入口網站 B) 需要可供最多 25 位使用者存取客戶 VPC 中託管的單一靜態網頁。測試此使用案例時，管理員會判斷標準執行個體類型可支援此使用案例。

對於入口網站 A，管理員必須提交服務配額增加請求，將 XL 執行個體的限制從區域預設值（即 5) 提高到 100。完成後，管理員可以透過編輯 Web 入口網站來配置容量。對於入口網站 B，管理員可以繼續前進，而無需請求增加配額（即，因為標準執行個體類型的區域預設配額為 25)。

Amazon WorkSpaces 安全瀏覽器中的其他服務配額

您可以檢視和請求增加 Service Quotas 頁面上列出的其他配額。實際上，大多數客戶會發現不需要請求提高這些限制。這些配額大致分為兩種類型：數字和速率。

對於數量配額，當您提交 Web 入口網站數量的服務配額增加時，您將自動收到建立唯一入口網站所需的子資源數量增加。這將反映在 Service Quotas 頁面上。例如，如果您請求將入口網站從 3 增加到 5，則瀏覽器和使用者設定的服務配額將自動從 3 增加到 5。您可以選擇視需要重複使用或建立新的子資源。

在極少數情況下，客戶可能會發現增加其他資源配額數量或速率的使用案例。例如，管理員可能想要增加瀏覽器設定的數量，以測試其他入口網站組態。這些服務配額請求將根據case-by-case進行審核和履行。

對於費率配額，無論帳戶入口網站限制為何，都不需要調整 Service Quotas 中公開的費率限制。

在 Amazon WorkSpaces 安全瀏覽器中控制重新驗證 SAML IdP 權杖的間隔

當使用者造訪 WorkSpaces 安全瀏覽器入口網站時，他們可以登入以啟動串流工作階段。每個工作階段都會從開始頁面開始，除非他們在不到 5 分鐘前登入。入口網站會檢查身分提供者 (IdP) 權杖，以判斷是否在啟動工作階段時提示使用者輸入憑證。未持有有效 IdP 權杖的使用者必須輸入使用者名稱、密碼和選用的多重要素驗證 (MFA)，才能啟動串流工作階段。如果使用者已透過登入其 IdP 或受相同 IdP 保護的應用程式來產生 SAML IdP 權杖，則不會要求他們提供登入憑證。

如果使用者具有有效的 SAML IdP 字符，他們可以存取 WorkSpaces 安全瀏覽器。您可以控制重新驗證 SAML IdP 權杖所需的間隔。

控制重新驗證 SAML IdP 權杖的間隔

1. 使用您的 SAML IdP 提供者設定 IdP 逾時持續時間。我們建議以使用者完成其工作所需的最短時間來設定 IdP 逾時持續時間。

   - 如需關於 Okta 的詳細資訊，請參閱對所有政策強制執行有限的工作階段存留期。
   - 如需關於 Azure AD 的詳細資訊，請參閱設定驗證工作階段控制項。
   - 如需關於 Ping 的詳細資訊，請參閱工作階段。
   - 如需 的詳細資訊 AWS IAM Identity Center，請參閱設定工作階段持續時間。

2. 設定 WorkSpaces 安全瀏覽器入口網站的閒置和閒置逾時值。這些值控制使用者上次互動到 WorkSpaces 安全瀏覽器工作階段因閒置而結束之間的時間量。當工作階段結束時，使用者將失去其工作階段狀態 (包括開啟的分頁、未儲存的網頁內容和歷程記錄)，並在下一個工作階段開始時回到最新狀態。如需詳細資訊，請參閱 the section called “Web 入口網站建立” 中的步驟 5。

   > **Note**
   >
   > 如果使用者的工作階段逾時，但使用者仍有有效的 SAML IdP 字符，則不需要輸入其使用者名稱和密碼，即可啟動新的 WorkSpaces 安全瀏覽器工作階段。請按照上一個步驟中的指南，以控制重新驗證權杖的方式。

在 Amazon WorkSpaces 安全瀏覽器中設定使用者活動記錄

WorkSpaces 安全瀏覽器提供兩種記錄使用者活動和安全性相關事件的選項：

- 工作階段記錄器會擷取各種工作階段事件。這些日誌會傳送到您帳戶中的 Amazon S3 儲存貯體，以便與您偏好的 SIEM 平台輕鬆整合。
- 使用者存取記錄會擷取最重要的工作階段事件。這些日誌會串流至 Amazon Kinesis 串流，以進行即時處理和分析。

這兩個記錄選項都是在入口網站層級設定。您必須針對要啟用記錄的每個入口網站個別設定每個選項。您可以啟用選項或兩者，視每個入口網站的需求而定。

使用此功能時，您有責任遵守適用於記錄或監控使用者活動的任何要求，包括記錄或監控員工活動。

主題

設定 Amazon WorkSpaces 安全瀏覽器的工作階段記錄器

> **Warning**
>
> 啟用工作階段記錄器會停用下列 Chrome 功能：
>
> - Incognito 模式
> - 開發人員工具
> - Chrome 設定檔切換

若要啟用 WorkSpaces 安全瀏覽器入口網站的工作階段記錄器，您必須先識別要收集工作階段事件的 Amazon S3 儲存貯體。您可以使用已存放類似日誌的現有儲存貯體，或專門為此目的建立新的日誌。

Amazon S3 儲存貯體必須有儲存貯體政策，授予 WorkSpaces 安全瀏覽器寫入日誌的許可。我們建議您將 Amazon S3 儲存貯體放在與 WorkSpaces 安全瀏覽器入口網站相同的 AWS 帳戶 和 區域。

Amazon S3 儲存貯體沒有命名需求。若要建立新的儲存貯體，請依照下列步驟操作，或參閱《Amazon Simple Storage Service 使用者指南》中的建立一般用途儲存貯體。如需設定許可的指引，請參閱《Amazon Simple Storage Service 使用者指南》中的 Amazon S3 儲存貯體政策。

以下是 Amazon S3 儲存貯體的政策範例。請務必使用 Amazon S3 儲存貯體的名稱更新政策。請注意，委託人是 "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/*"
          ]
      }
  ]
}
```

在 WorkSpaces 安全瀏覽器入口網站上啟用工作階段記錄器可能會導致 Amazon S3 產生費用。如需詳細資訊，請參閱 Amazon S3 定價。

如需工作階段記錄器擷取之工作階段相關事件的詳細資訊，請參閱 the section called “工作階段記錄器中的工作階段事件”。

具有 KMS 加密的 S3 儲存貯體 （選用）

WorkSpaces 安全瀏覽器工作階段記錄器完全支援啟用 AWS KMS 加密的 Amazon S3 儲存貯體。為了確保您的加密 Amazon S3 儲存貯體具有適當的記錄功能，您必須授予工作階段記錄器使用 AWS KMS 金鑰的必要許可。

將下列政策新增至您的 AWS KMS 金鑰組態：

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

在 AWS 主控台中，選取您要從中收集事件的 WorkSpaces 安全瀏覽器入口網站，然後選擇工作階段記錄器索引標籤和編輯。

輸入下列資訊以設定入口網站的工作階段記錄器：

- S3 位置 （必要）：交付事件的 Amazon S3 儲存貯體名稱。
- 金鑰字首 （選用）：交付事件的資料夾。如果資料夾不存在，則會建立資料夾。如果欄位保留空白，工作階段記錄器會在 Amazon S3 儲存貯體的根目錄寫入事件。

在進階下，您可以設定下列欄位：

- 事件篩選條件：這是工作階段記錄器監控的事件清單。
  - 全部：選取此選項表示將監控所有目前和未來的事件
  - 包含：這可讓您手動選取要監控的特定事件。只會記錄明確選取的事件。除非手動將新事件新增至選取項目，否則未來更新中引入的新事件將不會受到監控。
- 檔案格式
  - JSON （預設）：這是將每個日誌檔案顯示為事件陣列的檔案格式。對於大多數使用案例，我們建議使用此格式。
  - JSONLines：這是針對 Amazon Athena 最佳化的檔案格式。
- 資料夾結構：這會決定日誌檔案的儲存方式。
  - 一般 （預設）：所有日誌檔案都在單一資料夾中。

- 巢狀依據日期：日誌檔案會依日期和時間組織成資料夾。針對 Amazon Athena 進行分割，並針對 Amazon Athena 查詢進行最佳化。

您可以測試工作階段記錄器設定，並確保工作階段記錄器正常運作。組態完成後，系統會嘗試將名為的測試檔案寫入指定的 Amazon S3 `_workspaces_secure_browser.tmp` 儲存貯體和資料夾。這可做為記錄功能和許可設定的驗證。

您也可以在入口網站中啟動安全瀏覽器工作階段，並像平常一樣使用瀏覽器，以執行測試工作階段。工作階段記錄器會在作用中工作階段期間或工作階段結束時，每 15 分鐘將日誌檔案寫入您設定的 Amazon S3 儲存貯體。

結束工作階段或等待下一個記錄間隔後，請檢查 Amazon S3 儲存貯體，確認工作階段的日誌檔案已如預期產生並儲存。

設定 Amazon WorkSpaces 安全瀏覽器的使用者存取記錄

若要在 WorkSpaces 安全瀏覽器主控台中啟用使用者存取記錄，請在使用者存取記錄下，選取您要用來接收資料的 Kinesis 串流 ID。記錄的資料將直接傳送到該串流。

如需建立 Amazon Kinesis Data Stream 的詳細資訊，請參閱什麼是 Amazon Kinesis Data Streams？。

若要從 WorkSpaces 安全瀏覽器接收日誌，您必須擁有開頭為「amazon-workspaces-web-*」的 Amazon Kinesis Data Stream。您的 Amazon Kinesis 資料串流必須關閉伺服器端加密，或必須使用 AWS 受管金鑰 進行伺服器端加密。

如需在 Amazon Kinesis 中設定伺服器端加密的詳細資訊，請參閱如何開始使用伺服器端加密？。

在 Amazon WorkSpaces 安全瀏覽器中管理瀏覽器政策

您可以使用適用於最新穩定版本的 Chrome 政策，將任何自訂瀏覽器政策設定為 WorkSpaces 安全瀏覽器。當您在 WorkSpaces 安全瀏覽器入口網站中設定政策時，該政策將套用到該 Web 入口網站管理的所有工作階段。

您可以在 Web 入口網站套用 300 多項政策。如需詳細資訊，包括 Chrome 政策的完整清單，請參閱 Chrome Enterprise 政策清單。

設定 Chrome 政策有三種方式：

1. 在 Web 入口網站中使用視覺化編輯器

透過使用主控台檢視來建立 Web 入口網站，您可以在視覺化編輯器中套用一些最常見的政策：

- `StartURL`
- 開啟和關閉隱私瀏覽
- 刪除歷程記錄
- 書籤和書籤資料夾

2. 在 Web 入口網站中使用 JSON 編輯器

   您也可以使用 JSON 編輯器而非視覺化編輯器，直接新增或編輯政策。

   如需政策的特定格式，請參閱 Chrome Enterprise 政策清單。

3. 將 JSON 檔案上傳至 Web 入口網站

   您也可以將 JSON 檔案上傳至 Web 入口網站，匯入組織中使用的 Chrome 政策。

   如需詳細資訊，請參閱 the section called “教學課程：設定自訂瀏覽器政策”

WorkSpaces 安全瀏覽器會將基準瀏覽器政策組態套用至所有入口網站，以及您指定的任何政策。您可以使用自訂的 JSON 檔案編輯其中部分政策。如需詳細資訊，請參閱the section called “編輯基準瀏覽器政策”。

主題

- 教學課程：在 Amazon WorkSpaces 安全瀏覽器中設定自訂瀏覽器政策
- 在 Amazon WorkSpaces 安全瀏覽器中編輯基準瀏覽器政策

教學課程：在 Amazon WorkSpaces 安全瀏覽器中設定自訂瀏覽器政策

您可以上傳 JSON 檔案以設定任何支援用於 Linux 的 Chrome 政策。如要進一步了解 Chrome 政策，請參閱 Chrome Enterprise 政策清單，然後選取 Linux 平台。然後，搜尋並檢閱最新穩定版本的政策。

在下列教學課程中，您會使用下列政策控制來建立 Web 入口網站：

- 設定書籤
- 設定預設啟動頁面
- 防止使用者安裝其他擴充功能
- 防止使用者刪除歷程記錄

- 防止使用者使用無痕模式
- 為所有工作階段預先安裝 Okta 外掛程式擴充功能。

主題

步驟 1：建立 Web 入口網站

若要上傳 Chrome 政策 JSON 檔案，您必須建立 WorkSpaces 安全瀏覽器入口網站。如需詳細資訊，請參閱the section called “Web 入口網站建立”。

步驟 2：收集政策

在 Chrome 政策中搜尋並找出您要使用的政策。然後，您可以在下一個步驟中使用政策來建立 JSON 檔案。

1. 前往 Chrome Enterprise 政策清單。
2. 選擇平台 Linux，然後選擇最新的 Chrome 版本。
3. 搜尋您要設定的政策。在此例中，搜尋擴充功能以尋找管理擴充功能的政策。每個政策都包含說明、Linux 偏好設定名稱和範例值。
4. 在搜尋結果中，如果一起使用，則有 3 個符合業務需求的政策：
   - ExtensionSettings – 在啟動瀏覽器時安裝擴充功能。
   - ExtensionInstallBlocklist – 防止安裝特定的擴充功能。
   - ExtensionInstallAllowlist – 允許安裝某些擴充功能。
5. 其他政策滿足其餘要求；
   - ManagedBookmarks – 將書籤加入網頁。
   - RestoreOnStartupURLs – 設定每當啟動新的瀏覽器視窗時，會開啟哪些網頁。
   - AllowDeletingBrowserHistory – 設定使用者是否可以刪除其瀏覽歷程記錄。
   - IncognitoModeAvailability – 設定使用者是否可以使用無痕模式。

步驟 3：建立自訂的 JSON 政策檔案

使用文字編輯器、範本和您在先前步驟中找到的政策來建立 JSON 檔案。

1. 開啟文字編輯器。
2. 複製下列範本並貼至文字編輯器：

```
{
  "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
        }
    }
}
```

步驟 4：將政策加入範本

針對每個業務需求，將您的自訂政策加入範本。

1. 設定書籤 URL。
   a. 為您要加入的每個書籤在 value 金鑰下方加入成對的 name 和 url 金鑰。
   b. 將 bookmark-url-1 設定為 https://www.amazon.com。
   c. 將 bookmark-url-2 設定為 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. 設定啟動 URL。此政策可讓系統管理員設定使用者啟動新瀏覽器視窗時要顯示的網頁。

   a. 將 RestoreOnStartup 設定為 4。這會設定開啟 URL 清單的 RestoreOnStartup 動作。您還可以在啟動 URL 上使用其他動作。如需詳細資訊，請參閱 Chrome Enterprise 政策清單。

   b. 設定 RestoreOnStartupURLs 為 https://www.aboutamazon.com/news。

```
    "RestoreOnStartup":
       {
           "value": 4
       },
   "RestoreOnStartupURLs":
       {
           "value":
           [
               "https://www.aboutamazon.com/news"
           ]
       },
```

3. 若要防止使用者刪除其瀏覽器歷程記錄，請將 AllowDeletingBrowserHistory 設定為 false。

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

4. 若要關閉使用者使用無痕模式的權限，請將設定 IncognitoModeAvailability 為 1。

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

5. 使用下列政策設定及強制執行 Okta 外掛程式：

   - ExtensionSettings – 在啟動瀏覽器時安裝擴充功能。可從 Okta 外掛程式說明頁面取得擴充功能值。
   - ExtensionInstallBlocklist – 防止安裝特定的擴充功能。預設使用一個 * 值來防止所有擴充功能。管理員可以控制允許在 ExtensionInstallAllowlist 上使用哪些擴充功能。
   - ExtensionInstallAllowlist 允許您安裝某些擴充功能。由於將 ExtensionInstallBlocklist 設定為 *，請在此處加入 Okta 外掛程式值以允許使用它。

   以下顯示開啟 Okta 外掛程式的範例政策：

```
"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"
    }
}
```

步驟 5：將您的政策 JSON 檔案上傳到您的 Web 入口網站

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 WorkSpaces 安全瀏覽器，然後選擇 Web 入口網站。
3. 選擇您的 Web 入口網站，然後選擇編輯。
4. 選擇 政策設定，然後選擇 JSON 檔案上傳。
5. 選擇選擇檔案。導覽至、選取並上傳您的 JSON 檔案。
6. 選擇儲存。

在 Amazon WorkSpaces 安全瀏覽器中編輯基準瀏覽器政策

為了提供服務，WorkSpaces 安全瀏覽器會將基準瀏覽器政策套用至所有入口網站。除了您從主控台檢視畫面或 JSON 上傳指定的政策之外，還會套用此基準政策。以下是服務套用的 JSON 格式政策清單：

```
{
    "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",
```

```
            ]
        }
    }
}
```

客戶無法變更下列政策：

- `DefaultDownloadDirectory` – 無法編輯此政策。此服務會覆寫此政策的任何變更。
- `DownloadDirectory` – 無法編輯此政策。此服務會覆寫此政策的任何變更。

基準`URLAllowlist`和`URLBlocklist`政策無法覆寫。請注意，與您的 Web 入口網站相關聯的 JSON 瀏覽器政策檔案不會包含這些基準政策。若要查看所有套用政策及其值的完整清單，請從遠端瀏覽工作階段導覽至「chrome：//policy」。

客戶可以更新其 Web 入口網站的下列政策：

- `DownloadRestrictions` – 預設是設定成 1，防止 Chrome Safe Browsing 將下載內容辨識成惡意的內容。如需詳細資訊，請參閱防止使用者下載有害檔案。您可以將值從 0 設定成 4。

設定 Amazon WorkSpaces 安全瀏覽器的輸入方法編輯器

終端使用者可以透過輸入法編輯器 (IME) 這項公用工具，選擇使用非 QWERTY 鍵盤的鍵盤配置來輸入語言文字。IME 可以協助使用者用更為龐大複雜的語言集 (例如，日文、中文和韓文) 來輸入文字。WorkSpaces 安全瀏覽器工作階段預設包含 IME 支援。使用者可以從工作階段的 IME 工具列或使用鍵盤快速鍵來選取其他語言。

WorkSpaces 安全瀏覽器的 IME 目前支援下列語言：

- 英文
- 簡體中文 (拼音)
- 繁體中文 (注音符號)
- 日文
- 韓文

請執行下列動作，以從 IME 工具列選取語言：

1. 選取黑色頂端面板列右側的語言選取器下拉清單。選擇器預設顯示英文的 en。

2. 在下拉選單中選擇要使用的語言。
3. 在選擇語言後出現的子選單中，選擇其他語言詳細資訊。

請使用下列鍵盤快速鍵來選取語言：

- 所有語言
  - 若要向前循環 IME (或向右移動鍵盤配置)，請按 Shift+Control+Left Alt。
  - 若要存取語言和輸入設定，請使用頂端面板列上的語言選擇器。如果看不到，請透過工具列 → 偏好設定 → 一般 → 鍵盤輸入方法將其啟用。
- 日文
  - 對於 macOS 使用者：如果您使用的是美國輸入來源，您可能會遇到輸入問題。若要解決此問題：
    1. 選取日文輸入來源 （例如日文 - Kana 或日文 - Romaji)，而不是 macOS 上的美國輸入來源。
    2. 在 WorkSpaces 安全瀏覽器工作階段中，前往工具列 → 偏好設定 → 鍵盤 → 選項金鑰設定，然後選取使用選項 (⌥) 做為遠端 Alt 金鑰 (Mac)，以確保鍵盤快速鍵正常運作。
  - 轉換輸入字元
    - 若要將字元轉換為 Hiragana，請按 F6。
    - 若要將字元轉換為 Katakana，請按 F7。
    - 若要將字元轉換為 Hankaku Katakana (Half-width Katakana)，請按 F8
    - 若要將字元轉換為拉丁文，請按 F10。
    - 若要將字元轉換為寬拉丁文，請按 F9。
  - 切換輸入模式
    - 若要從 Hiragana 切換到 Katakana，請按 Alt/Option+K。
    - 若要從 Katakana 切換到 Hankaku Katakana，請按 Alt/Option+K。
    - 若要從 Hankaku Katakana (Half-width Katakana) 切換回 Hiragana，請按 Alt/Option+K。
    - 若要從任何日文模式或寬拉丁轉換為拉丁文，請按 Alt/Option+L。
    - 若要從拉丁文切換至寬拉丁文，請按 Alt/Option+L。
    - 若要從任何模式切換到直接輸入，請按 Henkaku/Zenkaku key。
    - 若要從直接輸入切換回 Hiragana，請按 Henkaku/Zenkaku key。
- 韓文
  - 若要選擇韓文，請按 Shift+Space。
  - 若要選擇漢字，請按 F9。

若要從 WorkSpaces 安全瀏覽器工作階段關閉螢幕鍵盤，請聯絡 支援。

設定 Amazon WorkSpaces 安全瀏覽器的工作階段內當地語系化

當使用者啟動工作階段時，WorkSpaces 安全瀏覽器會偵測使用者的本機瀏覽器語言和時區設定，並將其套用至工作階段。這會影響工作階段期間的顯示語言，且有助於確保顯示的時間符合使用者所在位置的當前時間。

按以下優先順序確定工作階段語言：

1. Web 入口網站瀏覽器設定中的 ForcedLanguages 政策。如需詳細資訊，請參閱 ForcedLanguages。
2. 終端使用者的本機端瀏覽器語言設定。
3. 預設值為 English (en-US)。

由終端使用者瀏覽器中指定的本地時區設定來確定時區。如果時區設定無效，會使用 UTC。

WorkSpaces 安全瀏覽器中的下列元件支援當地語系化：

- WorkSpaces 安全瀏覽器登入頁面
- WorkSpaces 安全瀏覽器入口網站狀態訊息（包括載入訊息和錯誤）
- Chrome 瀏覽器
- 系統內容選單和另存為視窗

主題

- Amazon WorkSpaces 安全瀏覽器支援的語言代碼
- 在使用者瀏覽器設定中選取語言

Amazon WorkSpaces 安全瀏覽器支援的語言代碼

下列清單顯示 WorkSpaces 安全瀏覽器目前支援的語言代碼。如果使用者的本機端瀏覽器設定為使用未支援的語言代碼，工作階段會預設為英文 (en-US)。

- 德文
  - de – 德文
  - de-AT – 德文 (奧地利)

- de-DE – 德文 (德國)
- de-CH – 德文 (瑞士)
- de-LI – 德文 (列支敦士登)

- 英文
  - en – 英文
  - en-AU – 英文 (澳洲)
  - en-CA – 英文 (加拿大)
  - en-IN – 英文 (印度)
  - en-NZ – 英文 (紐西蘭)
  - en-ZA – 英文 (非洲南部)
  - en-GB – 英文 (英國)
  - en-US – 英文 (美國)
- 西班牙文
  - es – 西班牙文
  - es-AR – 西班牙文 (阿根廷)
  - es-CL – 西班牙文 (智利)
  - es-CO – 西班牙文 (哥倫比亞)
  - es-CR – 西班牙文 (哥斯大黎加)
  - es-HN – 西班牙文 (洪都拉斯)
  - es-419 – 西班牙文 (拉丁美洲)
  - es-MX – 西班牙文 (墨西哥)
  - es-PE – 西班牙文 (秘魯)
  - es-ES – 西班牙文 (西班牙)
  - es-US – 西班牙文 (美國)
  - es-UY – 西班牙文 (烏拉圭)
  - es-VE – 西班牙文 (委內瑞拉)
- 法文
  - fr – 法文
  - fr-CA – 法文 (加拿大)
  - fr-FR – 法文 (法國)

  - fr-CH – 法文 (瑞士)
- 印尼文
  - id – 印尼文
  - id-ID – 印尼文 (印尼)
- 義大利文
  - it – 義大利文
  - it-IT – 義大利文 (義大利)
  - it-CH – 義大利文 (瑞士)
- 日文
  - ja – 日文
  - ja-JP – 日文 (日本)
- 韓文
  - ko – 韓文
  - ko-KR – 韓文 (韓國)
- 葡萄牙文
  - pt – 葡萄牙文
  - pt-BR – 葡萄牙文 (巴西)
  - pt-PT – 葡萄牙文 (葡萄牙)
- 中文
  - zh – 中文
  - zh-CN – 中文 (中國)
  - zh-HK – 中文 (香港)
  - zh-TW – 中文 (台灣)

在使用者瀏覽器設定中選取語言

若要設定使用者的本機瀏覽器設定，請遵循適當的步驟。

- 在 Chrome 中，選擇設定，選擇語言，然後根據喜好設定語言順序。
- 在 Firefox 中，選擇設定、一般、語言，然後從下拉選單選擇語言。
- 在 Edge 中，選擇設定、選擇語言，然後根據喜好設定語言順序。

在 Amazon WorkSpaces 安全瀏覽器中管理 IP 存取控制

> **Important**
>
> IP 存取控制僅支援 IPv4。從IPv6-only 網路連線的使用者將被封鎖。

WorkSpaces 安全瀏覽器可讓您控制 Web 入口網站可從哪些 IP 地址存取。使用 IP 存取設定可以定義和管理受信任 IP 地址的群組，並且只允許使用者在連線至受信任網路時存取其入口網站。

根據預設，WorkSpaces 安全瀏覽器允許使用者從任何地方存取其 Web 入口網站。IP 存取控制群組可作為虛擬防火牆，來篩選使用者可用於連線至 Web 入口網站的 IP 位址。當與您的 Web 入口網站建立關聯時，IP 存取設定會在驗證前偵測使用者 IP，以判斷它們是否有資格進行連線。連線後，WorkSpaces 安全瀏覽器會持續監控使用者的 IP 地址，以確保他們從信任的網路保持連線。如果使用者的 IP 變更，WorkSpaces 安全瀏覽器會偵測並終止工作階段。

若要指定 CIDR 地址範圍，請將規則加入 IP 存取控制群組，然後將群組與您的 Web 入口網站建立關聯。您可以將每個 IP 存取設定與一或多個 Web 入口網站建立關聯。若要指定受信任網路的公用 IP 地址和 IP 地址範圍，請將規則加入您的 IP 存取控制群組。如果您的使用者透過 NAT 閘道或 VPN 存取其 Web 入口網站，您必須建立規則，以允許來自 NAT 閘道或 VPN 的公用 IP 地址流量。

> **Note**
>
> 客戶有責任了解使用 WorkSpaces 安全瀏覽器時產生的潛在法律問題，並且必須確保其使用 WorkSpaces 安全瀏覽器時符合所有適用的法律和法規。這包括規範雇主監控員工使用 WorkSpaces 安全瀏覽器之能力的法律，包括在應用程式中執行的活動。

主題

在 Amazon WorkSpaces 安全瀏覽器中建立 IP 存取控制群組

> **Important**
>
> IP 存取控制僅支援 IPv4。從IPv6-only 網路連線的使用者將被封鎖。

請按照下列步驟來建立 IP 存取控制群組。

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在導覽窗格中，選擇 IP 存取控制。
3. 選擇建立 IP 存取控制群組。
4. 在建立 IP 存取控制群組對話方塊中，輸入群組名稱 (必要) 和描述 (選用)。
5. 輸入將與來源建立關聯的 IP 地址或 CIDR IP 範圍，以及說明 (選用)。
6. 在標籤底下，選擇是否為每個 IP 存取控制群組標記金鑰值配對。
7. 新增規則和標籤完成後，選擇儲存。

將 IP 存取設定與 Amazon WorkSpaces 安全瀏覽器中的 Web 入口網站建立關聯

> **Important**
>
> IP 存取控制僅支援 IPv4。從IPv6-only 網路連線的使用者將被封鎖。

若要建立 IP 存取控制群組與現有 Web 入口網站的關聯，請依照下列步驟執行。

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在導覽窗格中，選擇 Web 入口網站。
3. 選取 Web 入口網站，然後選擇編輯。
4. 在 IP 存取控制群組底下，選取 Web 入口網站的 IP 存取控制群組。
5. 選擇儲存。

請依照下列步驟，以便在建立新的 Web 入口網站時建立 IP 存取控制群組的關聯。

1. 完成 the section called “入口網站設定” 中的步驟 1 到 4，以存取 IP 存取控制 (選用)。
2. 選擇建立 IP 存取控制。
3. 在建立 IP 群組對話方塊中，輸入群組名稱 (必要) 和描述 (選用)。
4. 輸入將與來源建立關聯的 IP 地址或 CIDR IP 範圍，以及說明 (選用)。
5. 在標籤底下，選擇是否為每個 IP 存取控制群組標記金鑰值配對。
6. 新增規則和標籤完成後，選擇建立 IP 存取控制。
7. 啟動時您的 IP 存取控制群組將與此 Web 入口網站建立關聯。

在 Amazon WorkSpaces 安全瀏覽器中編輯 IP 存取控制群組

您可以隨時刪除 IP 存取設定中的規則。如果您刪除用來允許連線至 Web 入口網站的規則，任何具有目前工作階段的使用者都會與 Web 入口網站中斷連線。

請按照下列步驟編輯 IP 存取控制群組。

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在導覽窗格中，選擇 IP 存取控制。
3. 選取群組與選擇編輯。
4. 編輯現有規則的來源和說明 (選用)，或加入其他規則。
5. 在標籤底下，選擇是否為每個 IP 存取控制群組標記金鑰值配對。
6. 新增規則和標籤完成後，選擇儲存。
7. 如果您已更新現有的 IP 存取設定，請等待最多 15 分鐘，讓新規則或編輯過的規則生效。

在 Amazon WorkSpaces 安全瀏覽器中刪除 IP 存取控制群組

您可以隨時刪除 IP 存取控制群組中的規則。如果您刪除用來允許連線至 Web 入口網站的規則，任何具有目前工作階段的使用者都會與 Web 入口網站中斷連線。

請按照下列步驟以刪除 IP 存取控制群組。

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。

2. 在導覽窗格中，選擇 IP 存取控制群組。
3. 選取群組並選擇刪除。

在 Amazon WorkSpaces 安全瀏覽器中管理單一登入擴充功能

您可以為終端使用者啟用擴充功能，以獲得更好的入口網站登入體驗。例如，如果您使用 Okta 當成入口網站的 SAML 2.0 身分提供者 (IdP)，並且也將它當成您希望使用者在工作階段期間造訪之網站的 IdP，則可以將 Okta 登入 cookie 傳給具有擴充功能的工作階段。之後使用者造訪需要 Okta 網域 cookie 的網站時，他們無需在工作連線期間登入，便能存取該網站。

Chrome 和 Firefox 瀏覽器支援擴充功能。擴充功能會針對從使用者登入到工作階段所允許的網域啟用 cookie 同步處理。擴充功能無需使用者登入，會在幕後運作以啟用 cookie 同步處理，使用者不用在安裝後採取任何動作。擴充功能不會儲存任何資料。

根據預設，在 Incognito 視窗或 Firefox Private Browsing 視窗中的 Chrome 中不會啟用擴充功能。使用者可以手動啟用它們。如需 Chrome 的詳細資訊，請參閱 Incognito 模式中的延伸模組。如需 Firefox 的詳細資訊，請參閱私有瀏覽中的延伸模組。

當使用者登入入口網站時，系統會提示他們安裝擴充功能。如需有關擴充功能使用者體驗的詳細資訊，請參閱 the section called “單一登入延伸”。

主題

- 在 Amazon WorkSpaces 安全瀏覽器中識別單一登入延伸模組的網域
- 將單一登入延伸模組新增至 Amazon WorkSpaces 安全瀏覽器中的新 Web 入口網站
- 將單一登入延伸模組新增至 Amazon WorkSpaces 安全瀏覽器中的現有 Web 入口網站
- 編輯或移除 Amazon WorkSpaces 安全瀏覽器中的單一登入擴充功能

在 Amazon WorkSpaces 安全瀏覽器中識別單一登入延伸模組的網域

先確定您的 SAML IdP 和網站需要哪些網域。您最多可以加入 10 個網域。

您負責測試和識別要同步之 Cookie 的適當網域。可能要在 IdP 或網站驗證層級進行變更，以確保單一登入如預期般運作。

若要查看要搭配最常見 IdP 使用的網域，請參閱下表：

IdP 和網域

IdP	網域
Okta	okta.com
Entra ID	microsoftonline.com
AWS 身分中心	awsapps.com
一次登入	onelogin.com
Duo	duosecurity.com

將單一登入延伸模組新增至 Amazon WorkSpaces 安全瀏覽器中的新 Web 入口網站

若要在建立新的 Web 入口網站時允許 延伸模組，請遵循下列步驟。

1. 請按照 the section called “Web 入口網站建立” 中的步驟操作，直到到達 the section called “使用者設定” 為止。
2. 針對 the section called “使用者設定” 的步驟 1，在使用者許可底下選擇允許，以啟用 Web 入口網站的擴充功能。
3. 輸入 cookie 同步的網域，然後選擇新增網域。
4. 完成 the section called “使用者設定” 中的步驟和 the section called “Web 入口網站建立” 的其餘部分，以建立您的 Web 入口網站。

將單一登入延伸模組新增至 Amazon WorkSpaces 安全瀏覽器中的現有 Web 入口網站

若要將擴充功能新增至現有的 Web 入口網站，請遵循下列步驟。

1. 在 https：//https://console.aws.amazon.com/workspaces-web/home 開啟 WorkSpaces 安全瀏覽器主控台。
2. 選取要編輯的 Web 入口網站。
3. 選擇使用者設定、使用者許可和允許，以啟用 Web 入口網站的擴充功能。

4. 輸入 cookie 同步的網域，選擇新增網域。
5. 儲存入口網站變更內容。入口網站會在 15 分鐘內提示使用者安裝擴充功能。

編輯或移除 Amazon WorkSpaces 安全瀏覽器中的單一登入擴充功能

若要編輯網域或移除擴充功能，請遵循下列步驟。

1. 在 https：//https://console.aws.amazon.com/workspaces-web/home 開啟 WorkSpaces 安全瀏覽器主控台。
2. 選取要編輯的 Web 入口網站。
3. 選擇使用者設定、使用者許可和不允許以移除 Web 入口網站的擴充功能。
4. 移除或編輯個別網域。
5. 移除後，即使使用者在其瀏覽器中已安裝 WorkSpaces 安全瀏覽器延伸模組，工作階段也不會再同步 Cookie。

Amazon WorkSpaces 安全瀏覽器中的 Web 內容篩選

Web 內容篩選是一項安全與合規功能，可讓您的組織定義政策和規範 WorkSpaces 安全瀏覽器中的內容存取。透過 Web 內容篩選，您可以指定 URLs 最終使用者可以存取或封鎖特定 URLs或網域類別，以限制存取，並解決重要的安全性和法規合規要求。

> **Note**
>
> 雖然您可以透過 Chrome 政策設定 URL 篩選政策來封鎖或允許特定網域，但我們不建議使用此方法，因為不會擷取來自 Chrome 政策的動作做為服務記錄功能的一部分。如需全面監控和合規報告，請使用此頁面所述的 Web 內容篩選政策。

主題

限制瀏覽至特定 URLs

您可以實作「預設拒絕」政策，其中只能存取明確核准的網站和 URLs。它非常適合需要嚴格控制網際網路存取的高度安全環境，並且每個允許的網站都已經過業務必要性和安全合規的審核。

在 AWS 主控台的 URL 篩選下：

- 導覽至封鎖清單，然後選取切換 封鎖所有 URLs
- 在允許清單下，按一下新增 URL 以新增將允許為您的最終使用者列出的 URL。每個 URL 新增一個項目。
- 按一下儲存

封鎖特定 URLs

您可以透過保持開放網際網路存取，同時封鎖已知有問題的網站，來平衡安全性與生產力。它適用於信任其使用者但想要防止存取特定威脅或不適當內容的組織，而不會過度限制合法的商業活動。

在 AWS 主控台的 URL 篩選下：

- 導覽至封鎖URLs
- 選取新增 URL，然後輸入要封鎖的 URL。為每個要封鎖的 URL 新增一個項目
- 按一下儲存

封鎖類別

除了封鎖特定 URLs之外，您也可以根據內容類別自動封鎖 URLs 群組。這適用於需要全面涵蓋各種不適當或風險內容的組織，而不需要手動識別和封鎖個別網站。

在 AWS 主控台的 URL 篩選下：

- 導覽至封鎖類別，然後按一下新增類別
- 選取您要封鎖的任何類別
- 您可以將 URLs 新增至允許清單，以例外處理這些類別。針對此操作，按一下新增 URL 並輸入您要允許的 URLs項目。即使它們包含在類別中，最終使用者可以造訪 URLs。
- 按一下儲存

您可以選取下列類別。您可以選取一個、多個或所有類別。

可用的篩選類別

佈景主題	類別	描述
成人和不適當的內容	裸露	包含非性裸影像或美術的站台。
成人和不適當的內容	色情	具有明確性內容或挑逗裸露材料的網站。
成人和不適當的內容	性教育	適齡、經過醫學審查的運作狀態和性向資源。
成人和不適當的內容	無味	內容不適合其他類別未涵蓋的子項。
通訊和社交	聊天	即時群組和私有傳訊平台。
通訊和社交	即時傳訊	私有傳訊服務。
通訊和社交	專業網路	以業務為重心的關係建置平台。
通訊和社交	社交網路	用於分享個人內容和體驗的使用者互動平台。
通訊和社交	Web 型電子郵件	瀏覽器可存取的簡訊服務，包括電子卡片和問候語系統。
娛樂	遊戲	娛樂遊戲資源，包括影片遊戲、拼圖和非博彩活動。
娛樂	影像共用	提供託管、搜尋和共用功能的視覺化內容平台。
娛樂	對等對等	檔案共用應用程式提供者和相關軟體工具。
有害和非法的內容	犯罪活動	提升非法行為的說明或資料。
有害和非法的內容	駭客入侵	未經授權的系統存取工具和網路利用資源。
有害和非法的內容	非法藥物	提升娛樂性藥物使用或濫用藥物的內容。

佈景主題	類別	描述
有害和非法的內容	非法軟體	未經授權的著作權資料和惡意軟體分發。
有害和非法的內容	暴力	提升物理傷害或顯示圖形材料的內容。
有害和非法的內容	武器	合法的運動和娛樂槍支使用資源。
高風險行為	ults	非主流精神和中繼物理內容。
高風險行為	賭博	投注相關活動和資訊。
高風險行為	仇恨與不容忍	內容提升對受保護特性的偏差。
高風險行為	學校作弊	未經授權的學術協助和家庭作業完成服務。
高風險行為	自我傷害	內容提升或討論自我破壞行為。
技術與 AI	下載網站	軟體、應用程式和數位資產託管平台。
技術與 AI	生成式 AI	AI 和機器學習技術資源。
技術與 AI	停駐網域	用於廣告或網域銷售的最低內容網域。
技術與 AI	串流媒體和下載	音訊/視訊內容平台，包括音樂、影片和網際網路廣播。

URLs範例

您可以在 AllowedUrls 或 BlockedUrls URLs 中提供下列 URL 類型

Type	範例
網域	example。com
子網域	login.example.com
路徑	example.com/myvideos

Type	範例
查詢參數	example.com/?parameter=123

轉移 Chrome 政策

如果您已設定 Chrome 政策來允許或封鎖特定網域，建議您將它們轉移到 Web 內容篩選功能。

Web 內容篩選功能會偵測任何適用於 WorkSpaces 安全瀏覽器工作階段的 URLAllow 或 URLBlock 政策，並在 AWS 主控台中發出訊號。

若要轉移 URLAllowlist 和/或 URLBlocklist 的 Chrome 政策：

- 在 AWS 主控台的 URL 篩選下，按一下檢閱 Chrome 政策（如果您沒有看到檢閱 Chrome 政策按鈕，這表示目前不適用於 URL 允許或 URLBlock 的 Chrome 政策）
- 在浮水印下，檢閱 Chrome 政策
- 按一下轉接

Chrome 政策將從政策設定下的 JSON 編輯器中移除，新的 URLs將自動新增至 Web 內容篩選功能。

Amazon WorkSpaces 安全瀏覽器中的深層連結

當使用者登入 WorkSpaces 安全瀏覽器時，他們會在管理員設定的首頁上啟動工作階段。您也可以允許入口網站接收深層連結，以在工作階段期間將使用者連線至特定網站。選取深層連結時，入口網站會顯示深層連結中指定的 URL。連結會與為工作階段開始設定的首頁一起顯示，或者如果工作階段已在進行中，則單獨顯示。此功能可讓管理員使用 WorkSpaces 安全瀏覽器建立更動態的使用者體驗。

深層連結會在 WorkSpaces 安全瀏覽器工作階段中開啟頁面。如果工作階段已在執行中，則會在新索引標籤中開啟深層連結。如果工作階段尚未執行，則會在新索引標籤中開啟深層連結 URL，並在個別索引標籤中開啟入口網站預設首頁。如果深層連結包含多個 URL，它會先顯示焦點列出的深層連結 URL，並在個別標籤中開啟每個後續 URL（包括預設首頁）。

主題

- 在 Amazon WorkSpaces 安全瀏覽器中設定深層連結
- 對 Amazon WorkSpaces 安全瀏覽器中的深層連結使用 URL 篩選

在 Amazon WorkSpaces 安全瀏覽器中設定深層連結

若要允許深層連結的許可，請在建立使用者設定時選擇允許。您想要深層連結的網站必須使用 URL 編碼。例如，若要將使用者連結至「https://www.example.com/?query=true」，請將連結更新為 https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue。

深層連結最多可包含 10 URLs，以逗號表示。例如：

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

如需允許深層連結的詳細資訊，請參閱 the section called “使用者設定”。

對 Amazon WorkSpaces 安全瀏覽器中的深層連結使用 URL 篩選

如果您與 共用此入口網站連結的任何使用者都可以操作深層連結值來造訪網站，前提是該網域可從入口網站存取，而不是在 URL 封鎖清單中。若要建立限制性允許清單或封鎖清單，以防止使用者使用您的入口網站來造訪意外網域，請使用 URL 篩選。

您可以在入口網站的瀏覽器設定中使用 URL 篩選來編輯入口網站的允許清單和封鎖清單。若要這樣做，請以下列格式將 URL 附加至允許清單的入口網站 URL，其中 UUID 是入口網站 ID：https：//https://<uuid>.workspaces-web.com/?deepLinks=https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue

如需詳細資訊，請參閱 the section called “Web 內容篩選”和允許或封鎖對網站的存取。

在 Amazon WorkSpaces 安全瀏覽器中使用工作階段管理儀表板

使用 WorkSpaces 安全瀏覽器主控台上的工作階段管理儀表板來監控和管理作用中和完整的工作階段。

儀表板存取

若要存取儀表板，請遵循下列步驟。

存取儀表板

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。

2. 選擇 WorkSpaces 安全瀏覽器、Web 入口網站，然後選擇您的 Web 入口網站。
3. 選擇工作階段索引標籤，或選擇檢視工作階段，以在下方的分割面板中開啟儀表板。

儀表板篩選條件

在工作階段面板中，您可以依下列屬性或值篩選工作階段：

- 狀態
  - 作用中 – 表示工作階段目前正在執行。若要終止工作階段，請參閱下列內容。
  - 已終止 – 表示工作階段不再處於作用中狀態。
- 工作階段 ID
- 使用者名稱
- 工作階段開始時間

終止工作階段

若要終止工作階段，請遵循下列步驟。

終止工作階段

1. 在工作階段儀表板上，選取您要停止的工作階段。
2. 選擇終止。
3. 中斷連線的使用者會從工作階段失去所有狀態。所有開啟的索引標籤、瀏覽器歷史記錄和下載到安全瀏覽器的檔案都會回收。

工作階段歷史記錄

儀表板包含過去 35 天的工作階段。您可以使用 CLI 列出具有或沒有篩選條件的工作階段。工作階段歷史記錄會以 JSON 的形式交付，管理員可以處理、管理和存放在不同的儲存庫中。

以下是用於管理 US-West-2 （奧勒岡） 區域中工作階段的 CLI 命令範例。

若要列出 Web 入口網站的所有工作階段，請執行下列命令：

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

若要列出 Web 入口網站特定使用者的所有工作階段，請執行下列命令：

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

使用 FIPS 端點和 Amazon WorkSpaces 安全瀏覽器保護傳輸中的資料

根據預設，當您使用主控台、 AWS 命令列界面 (AWS CLI) 或 AWS SDK 以管理員身分與 WorkSpaces 安全瀏覽器服務通訊時，或在使用者的工作階段期間，傳輸中的所有資料都會使用 TLS 1.2 加密。

如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-3 驗證的加密模組，請使用 FIPS 端點。當您使用 FIPS 端點時，傳輸中的所有資料都會使用符合聯邦資訊處理標準 (FIPS) 140-3 的密碼編譯標準進行加密。如需 FIPS 端點的資訊，包括 WorkSpaces 安全瀏覽器端點清單，請參閱 https://aws.amazon.com/compliance/fips。

使用 FIPS 端點建立入口網站後，所有使用者工作階段和管理變更都會使用 FIPS 140-3 端點自動進行。您可以使用 `AWS_USE_FIPS_ENDPOINT=true`環境變數來尋找 FIPS 端點，並使用 SDK 傳送請求。下列是 範例。

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

您也可以使用 `–endpoint-url`選項，將請求直接傳送到 FIPS 端點。以下是 US-West-2 （奧勒岡）區域中的呼叫清單入口網站範例：

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

在 Amazon WorkSpaces 安全瀏覽器中管理資料保護設定

資料保護設定用於協助保護資料免於在工作階段期間共用。設定可以建立並套用到多個入口網站。

主題

Amazon WorkSpaces 安全瀏覽器中的內嵌資料修訂

透過將內嵌資料修訂新增至入口網站，您可以自動從網頁中顯示的文字字串預測和修訂特定資料。您可以從內建模式（例如社會安全號碼或信用卡號碼）中選擇，或使用規則表達式和關鍵字建立自己的自訂資料類型，來建立修訂政策。政策包含可設定的強制執行層級，以及應強制執行修訂URLs 的控制。

下列元件決定何時修訂資料：

- 資料保護設定 - 資料保護設定是資源的名稱，其中包含您的資料類型和強制執行條件。若要使用此資源，請先建立您的設定，然後將設定與入口網站建立關聯。當使用者啟動工作階段時，您的設定會在工作階段期間強制執行。
- 工作階段內瀏覽器擴充功能 - 當您將修訂設定與入口網站建立關聯時，工作階段瀏覽器將啟動為系統強制執行的瀏覽器擴充功能，以強制執行您的設定。資料保護設定會透過模式比對（規則表達式）和關鍵字搜尋，依照您的可信度等級和 URL 強制執行組態來強制執行修訂。從文字字串預測內容，並在畫面上顯示之前進行修訂。延伸項目也會設定相關的瀏覽器政策，以控管使用者繞過修訂（例如停用私有瀏覽、存取開發人員工具和網路檢查）的能力。

工作階段中的瀏覽器延伸模組會強制執行下列 Chrome 瀏覽器政策變更。如需詳細資訊，請參閱 Chrome Enterprise 政策清單。

- 強制執行瀏覽器政策，以防止使用者在不修訂的情況下檢視工作階段：
  - IncognitoModeAvailability = 1
  - DeveloperToolsAvailability = 2
  - BrowserAddPersonEnabled = false

  - BrowserGuestModeEnabled = false
- 擴充功能也會防止使用者透過取消下載事件，從強制執行資料保護設定的 URLs 下載 HTML 檔案。

一般而言，您應該對私有、結構化網站（例如您的客戶管理工具、票證系統或 Wiki) 使用修訂，而不是用於非結構化的公開瀏覽（例如 Facebook 或 Google)。您可以選擇內建資料類型（完整清單請參閱下方），或使用您自己的規則表達式值和關鍵字定義自訂資料類型。管理員負責測試和驗證每種資料類型、可信度層級和 URL 強制執行是否如預期般運作。 AWS 無法保證與第三方提供的自訂網站或應用程式的相容性。

WorkSpaces 安全瀏覽器目前不支援以非文字格式修訂支援或自訂資料類型，包括以下格式的文字：

- 影像，例如 JPEG、PNG 或 GIF
- 讓使用者能夠使用動態文字處理或編輯的網頁，例如 Google Docs 或 Sheets
- 在瀏覽器中存取的音訊或影片串流，例如 YouTube 影片
- Chrome 瀏覽器檢視的 PDFs

請勿對不支援格式的內容使用修訂。管理員負責驗證網站和內容相容性，然後再授予使用者對他們打算修訂之內容的存取權。

Amazon WorkSpaces 安全瀏覽器中的預設修訂組態

預設修訂組態會自動為資料保護設定中的所有內建資料類型套用可信度層級和 URL 強制執行。您可以選擇在新增內建資料類型時覆寫預設組態。

可信度等級可讓您使用格式、關鍵字和未格式化文字的組合，微調內建資料類型的修訂邏輯。選擇修改套用方式的嚴格程度，包括高、中或低。除非在資料類型層級套用覆寫，否則預設值會套用至所有資料類型。一般而言，請從預設的 Medium 組態開始，並驗證修訂是否如預期在網站上強制執行。

可信度層級	Description	範例
高	需要格式化的文字模式比對，才能編輯內容。	123-45-6798 的 SSN 將會修訂，而 123456789 不會修訂。
中	修訂會同時考慮格式化和未格式化的文字，並將關鍵字關聯新增至邏輯。	123-45-6798 的 SSN 將會修訂。如果偵測到關鍵字附近（例如「社會安全號碼」），則會修訂 123456789。

可信度層級	Description	範例
低	針對格式化模式 + 不含關鍵字的未格式化模式強制執行修訂。	SSN 採用任一格式 - 123-45-6798 和 123456789 - 進行修訂，而不需要關鍵字。

您必須為所有資料類型設定預設修訂組態。您可從下列選項擇一使用：

- 所有 URLs
- 特定 URLs
- 進階組態

除非在資料類型層級套用覆寫，否則預設值會套用至所有資料類型。URL 強制執行使用與 Chrome 政策類似的邏輯來管理允許和封鎖清單。如需使用封鎖和允許 URLs的指引，請參閱允許或封鎖對網站的存取。為了獲得最佳結果，請依照 Chrome 的封鎖清單篩選條件格式，將 URLs 新增至這些清單。如需詳細資訊，請參閱 URL 封鎖清單篩選條件格式。

Amazon WorkSpaces 安全瀏覽器中的基本內嵌修訂

內嵌資料修訂支援內建模式（例如社會安全號碼和信用卡號碼），您可以在基本內嵌修訂下找到這些模式。從下拉式功能表中選擇資料類型，並指定每個資料類型的取代值（替代值）。所有資料類型都遵循上面的預設組態強制執行模式，但您可以選擇覆寫可信度層級，並微調每個資料類型的網域強制執行模式。

若要從預設組態輸入替代值，請選擇可信度層級覆寫。例如，在預設組態設為 Medium 的情況下，您可能會在測試期間注意到其中一個資料類型未可靠地修訂。您可以設定覆寫為低，以增加修訂的機會，而無需調整用於其他資料類型的邏輯。

若要微調在 URLs 之間套用修訂的方式，而不變更預設組態，請套用 URL 強制執行覆寫。例如，您可以設定使用 URL 覆寫，在客戶關係管理系統中強制執行電子郵件地址修訂，而不會中斷使用者存取公司目錄網站或 Web 型電子郵件中的電子郵件地址。

以下是資料類型及其對應的內建模式 IDs的清單：

builtInPatternId	資料類型
awsAccessKey：	AWS Access Key (AWS 存取金鑰)

builtInPatternId	資料類型
awsSecretKey：	AWS Secret Key (AWS 秘密金鑰)
cardNumbers：	信用卡號碼
加密：	加密貨幣地址
cusipNum：	CUSIP 號碼
日期：	Date
deaNum：	美國 DEA 號碼
dob：	出生日期
driversLicense：	美國駕照
emailAddress：	電子郵件地址
ein：	美國雇主識別號碼
expDate：	信用卡過期日期
healthInsuranceNum：	聯邦醫療保險健康保險申請號碼
hipaaCode：	HIPAA ICD-10 程式碼
indivTaxId：	美國個人稅務 ID
ipAddr：	IP Address (IP 地址)
isin：	國際股票識別號碼
jwt：	JSON Web Token
locationCoord：	位置座標
macAddr：	MAC 地址
medicareBeneficiaryId：	聯邦醫療保險受益人號碼

builtInPatternId	資料類型
npi：	國家供應商識別號碼
ndc：	國家藥物代碼 (NDC)
passportNum：	美國護照號碼
phoneNum：	電話號碼
routingNumber：	ABA 路由號碼
ssn：	美國社會安全號碼
swiftCode：	SWIFT 程式碼
時間：	時間
vin：	美國車輛識別號碼

Amazon WorkSpaces 安全瀏覽器中的自訂內嵌修訂

客戶可以使用規則表達式定義自己的模式，例如自訂內部應用程式 IDs。若要建立自訂內嵌修訂模式，請遵循下列步驟：

1. 前往您的資料保護設定。
2. 選擇自訂內嵌修訂並新增。
3. 輸入自訂資料類型的名稱。
4. 輸入您的規則表達式值。
   - 規則表達式值必須符合 JavaScript 規則表達式常值語法。如需詳細資訊，請參閱規則表達式。範例規則表達式為 `/ex[am]+ple/i`。
   - 請務必在您計劃支援的網站上測試您的自訂模式。如果自訂模式寫入錯誤，可能會導致意外的效能問題。
5. 指定替代值。
6. 為更多選用自訂選擇更多選項，包括下列項目：
   - 新增關鍵字以微調修訂邏輯。關鍵字可以提高強制執行的準確性。在 Javascript 規則表達式常值語法中新增關鍵字。如需詳細資訊，請參閱規則表達式。

例如，如果您要為內部系統中使用的用戶端 IDs 建立自訂修訂模式，您可以將 `/client name/i`新增至關鍵字欄位，以通知掃描和偵測邏輯。

- 套用 URL 強制執行覆寫來微調在 URLs 之間套用修訂的方式，而不變更預設組態。

  例如，您可以設定使用 URL 覆寫，在客戶關係管理系統中強制執行電子郵件地址修訂，而不會中斷使用者存取公司目錄網站或 Web 型電子郵件中的電子郵件地址。

- 輸入 資料類型的描述 （選用）。

在 Amazon WorkSpaces 安全瀏覽器中建立資料保護設定

您可以在 WorkSpaces 安全瀏覽器中建立資料保護設定。

建立資料保護設定

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在左側導覽窗格中，選擇資料保護設定。
3. 選擇建立資料保護設定。
4. 輸入 設定的顯示名稱 （必要） 和描述 （選用）。
5. 選取內嵌修訂的預設設定。您可以設定下列項目：
   - 所有資料類型的嚴格程度
   - 應強制執行修訂的網域
6. 從支援的類型中選擇基本內嵌修訂資料類型，或建立自訂資料類型。您可以為每個資料類型設定覆寫，包括嚴格程度和網域例外狀況。
7. 為報告新增任何標籤 （選用）。
8. 完成後，選擇 Save (儲存)。

關聯 Amazon WorkSpaces 安全瀏覽器中的資料保護設定

您可以在 WorkSpaces 安全瀏覽器中關聯資料保護設定。

將資料保護設定與現有入口網站建立關聯

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在左側導覽窗格中，選擇 Web 入口網站。
3. 選取 Web 入口網站，然後選擇編輯。
4. 在資料保護設定下，選取入口網站的設定。
5. 選擇儲存。

若要在建立新入口網站時關聯資料保護設定，請遵循下列步驟。

在建立新入口網站時關聯資料保護設定

1. 遵循 中的指示來the section called “Web 入口網站建立”建立入口網站，直到您取得資料保護設定為止。
2. 從下拉式選單中選擇您的資料保護設定。
3. 完成 中的步驟the section called “Web 入口網站建立”，以完成建立您的入口網站。

若要在建立新入口網站時建立資料保護設定，請遵循下列步驟。

在建立新入口網站時建立資料保護設定

1. 遵循 中的指示來the section called “Web 入口網站建立”建立入口網站，直到您取得資料保護設定為止。
2. 從下拉式選單中選擇資料保護設定。
3. 輸入 設定的顯示名稱 （ 必要 ） 和描述 （ 選用 ）。
4. 選取內嵌修訂的預設設定。您可以設定下列項目：
   - 所有資料類型的嚴格程度
   - 應強制執行修訂的網域
5. 從支援的類型中選擇基本內嵌修訂資料類型，或建立自訂資料類型。您可以為每個資料類型設定覆寫，包括嚴格程度和網域例外狀況。
6. 為報告新增任何標籤 （ 選用 ）。
7. 完成後，選擇 Save (儲存)。
8. 選取資料保護設定下的重新整理按鈕，然後從下拉式選單中選擇您的資料保護設定。

9. 繼續遵循建立入口網站的指示來完成建立入口網站。

在 Amazon WorkSpaces 安全瀏覽器中編輯資料保護設定

您可以在 WorkSpaces 安全瀏覽器中編輯資料保護設定。

編輯資料保護設定

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 從清單檢視中選擇資料保護設定和您要編輯的資料保護設定。
3. 您可以更新名稱、描述、預設設定、資料類型 （支援或自訂），並套用可信度層級或網域覆寫。
4. 選擇儲存。

在 Amazon WorkSpaces 安全瀏覽器中刪除資料保護設定

您可以在 WorkSpaces 安全瀏覽器中刪除資料保護設定。

刪除資料保護設定

1. 如果您有與資料保護設定相關聯的入口網站，您必須先移除關聯，才能刪除資料保護設定。
2. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
3. 選擇資料保護設定和您要從清單檢視中刪除的資料保護設定。
4. 選擇 刪除。

Amazon WorkSpaces 安全瀏覽器中的品牌自訂

您可以修改視覺元素、文字內容和服務條款，自訂最終使用者出現的登入和載入畫面。品牌自訂有助於建立與組織身分一致的體驗。

概觀

品牌自訂可讓您個人化使用者體驗的下列層面：

- 視覺元素 - 上傳標誌、favicon 和桌布，然後選取顏色主題以符合您的品牌身分。

- 文字內容 - 自訂歡迎訊息、瀏覽器索引標籤標題和其他選用的文字欄位，在整個登入流程中維持您的品牌聲音。如果您未針對特定欄位指定自訂文字，則會使用預設文字。如需詳細資訊，請參閱the section called “自訂準則”。
- 服務條款 （選用） - 新增您組織的服務條款，使用者必須先確認才能開始工作階段。

> **Note**
>
> 您也可以自訂入口網站的網域名稱。如需詳細資訊，請參閱the section called “自訂網域”。

主題

為您的入口網站設定品牌自訂

運作方式

當您設定品牌自訂時：

- 視覺化和文字元素會同時套用至登入畫面和載入畫面。
- 瀏覽器索引標籤會顯示您的自訂 favicon 和標題。
- 最終使用者會在啟動新的工作階段時看到您的自訂變更。在某些情況下，可能需要幾分鐘的時間才能顯示您的變更。
- 如果已設定服務條款，最終使用者必須先接受您的服務條款，才能開始串流工作階段。請注意，系統會在每個工作階段開始時詢問這些問題。

先決條件

開始之前：

- 確保您擁有修改入口網站設定的必要許可，請參閱 the section called “AWS 受管政策”。
- 根據 中的規格準備您的品牌資產 （標誌、favicon、桌布）the section called “自訂準則”。

開始使用

若要設定品牌自訂，請依照下列步驟進行。

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 WorkSpaces 安全瀏覽器、Web 入口網站，然後選擇您的 Web 入口網站。
3. 選取您的入口網站，然後選擇使用者設定索引標籤。
4. 在品牌自訂區段中，選擇編輯。
5. 視需要設定下列區段：
   - 在內容編輯器 - 上傳所有視覺元素（您的公司標誌、Favicon 和選用桌布），然後選取顏色主題。您可以從本機電腦或從 S3 儲存貯體上傳檔案。如需設定 S3 儲存貯體許可的資訊，請參閱 the section called “設定 S3 儲存貯體許可”。
   - 在文字編輯器 - 自訂顯示在登入畫面上的文字。
   - 在服務條款編輯器 - 或者，新增使用者必須確認的詞彙。
6. 選擇儲存變更。

如需每個自訂選項的詳細說明，請參閱 the section called “自訂準則”。

設定 S3 儲存貯體許可

您可以直接從電腦上傳品牌檔案，或從 S3 儲存貯體中選取現有的物件。如果您選擇從 S3 儲存貯體上傳視覺化元素（您的公司標誌、Favicon 和桌布）的檔案，請確定您已設定 S3 儲存貯體的適當許可。

選取相同帳戶中的 S3 物件

如果您的 IAM 使用者或角色已具有包含品牌資產之儲存貯體的`s3:GetObject`許可，則不需要額外的組態。

選取另一個帳戶中的 S3 物件

若要選取不同 AWS 帳戶中的 S3 儲存貯體，您需要同時設定來源帳戶中的儲存貯體政策和管理員帳戶中的 IAM 政策。

儲存貯體政策範例（在來源帳戶中）：

將此政策套用至來源帳戶中的 S3 儲存貯體。將 *123456789012* 取代為您的管理員帳戶 ID，並將 *source-account-bucket-name* 取代為您的實際儲存貯體名稱。

```
{
  "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/*"
      ]
    }
  ]
}
```

範例 IAM 政策（在您的管理員帳戶中）：

將此政策連接至管理員帳戶中的 IAM 使用者或角色。將 *source-account-bucket-name* 取代為來源帳戶的實際儲存貯體名稱。

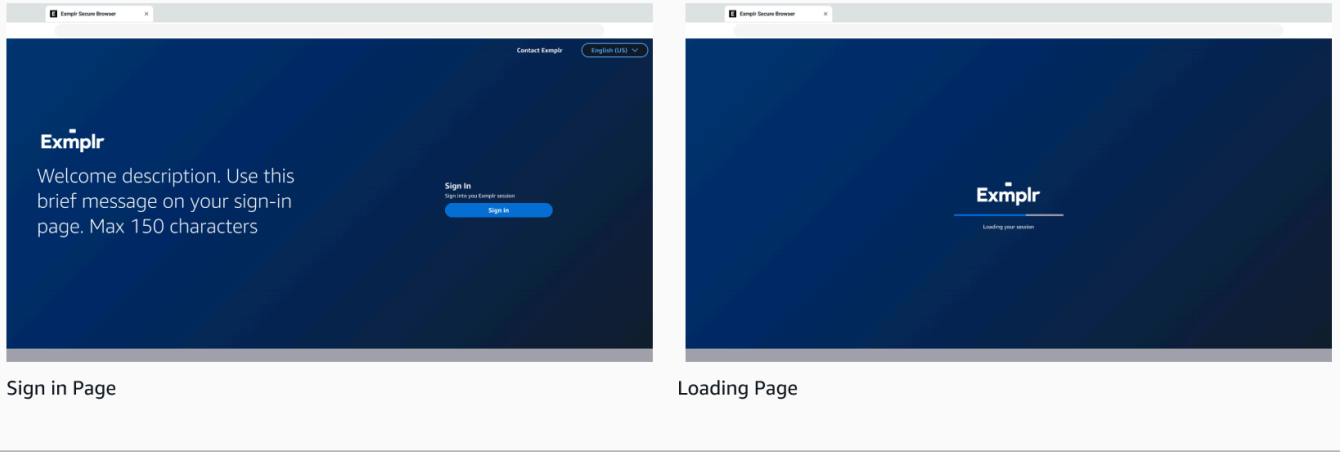
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountS3Access",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
```

```
        ]
      }
    ]
}
```

如需跨帳戶存取的詳細資訊，請參閱 S3 Access Grants 跨帳戶存取。

自訂準則

透過更新登入和載入頁面上的品牌元素和文字，為您的最終使用者自訂登入和載入體驗。您可以修改標誌和桌布等視覺化元素、編輯歡迎訊息和標頭等文字元素，以及選擇性地設定使用者在開始工作階段之前必須接受的服務條款協議。



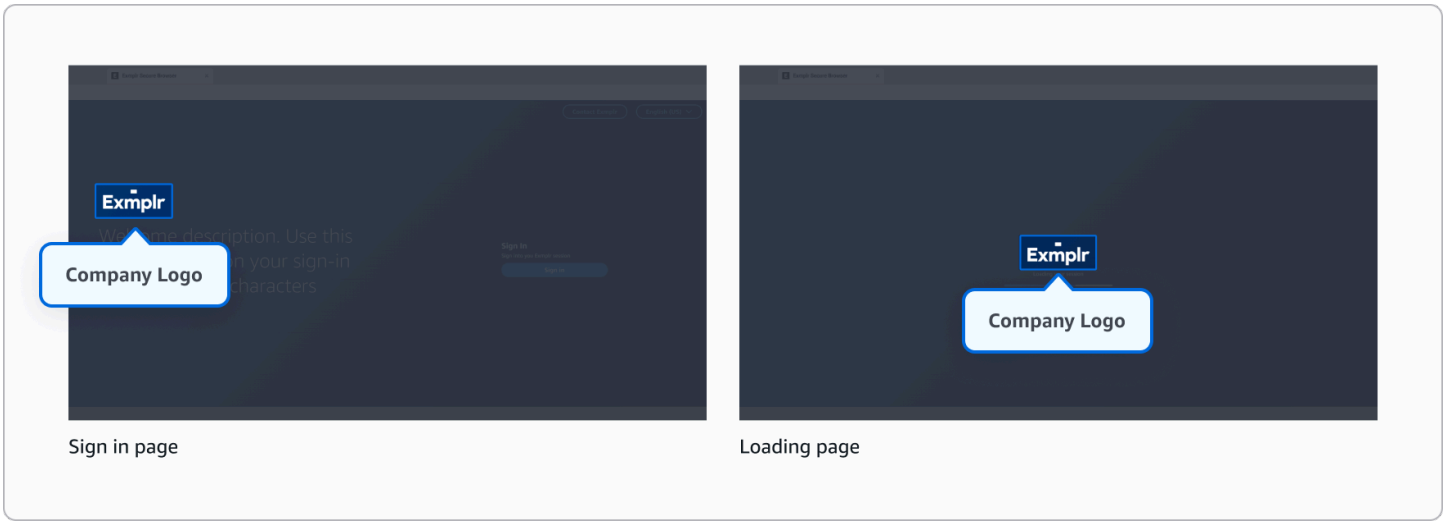
Sign in Page

Loading Page

內容編輯器

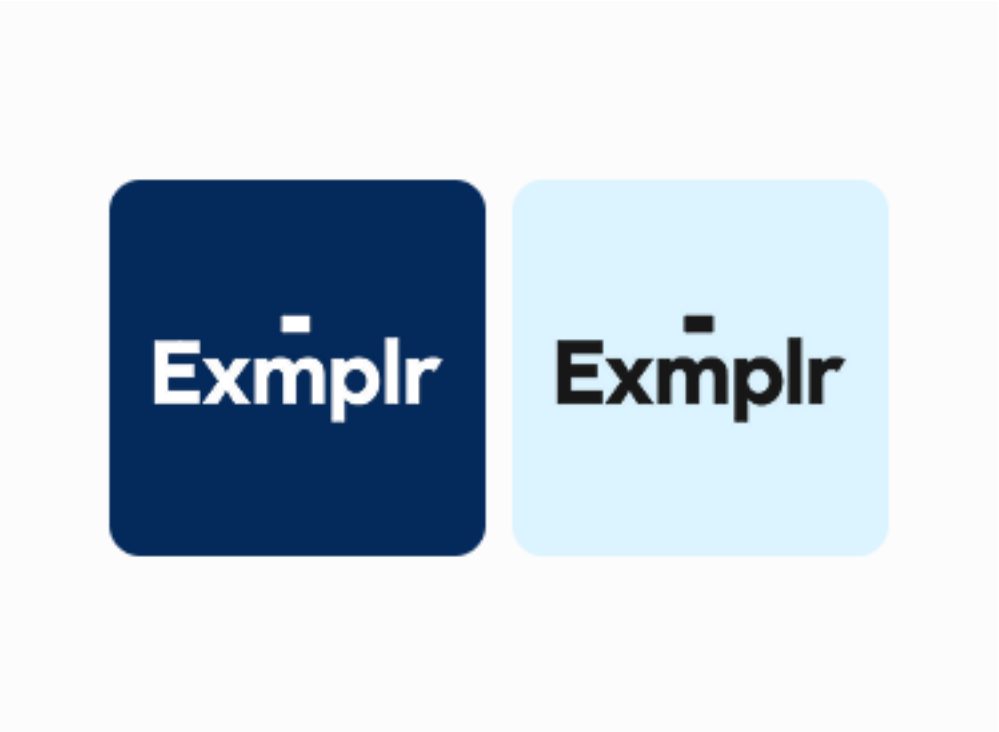
公司標誌

標誌會顯示在登入畫面和載入畫面上，在整個使用者體驗中提供一致的品牌形象。



- 支援的格式：JPG 或 ICO 或 PNG
- 檔案大小上限：100 KB

執行



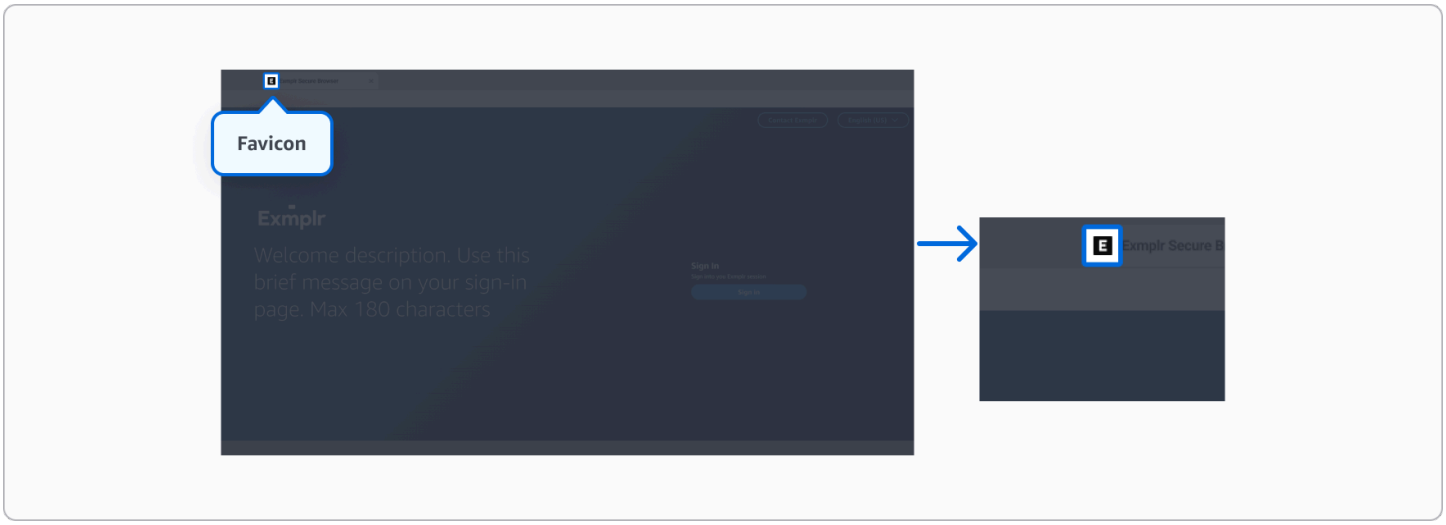
- 如果您有不同的標誌變化（例如不同的顏色或樣式），請選擇與所選桌布背景提供最佳對比的選項。

不要

- 調整標誌大小時，請勿忽略長寬比。
- 請勿使用未事先正確調整大小的標誌，因為它們看起來可能會扭曲。

網頁圖示

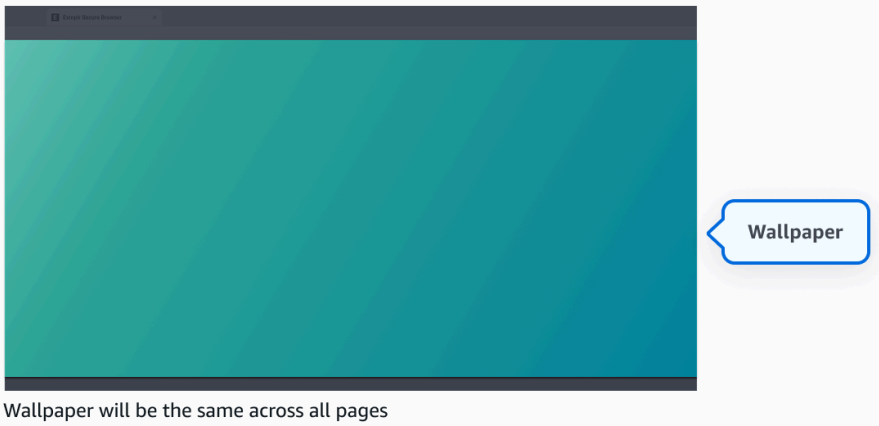
favicon 是出現在瀏覽器索引標籤中的小型圖示，可協助使用者在多個開啟的索引標籤中識別您的應用程式。



- 支援的格式：JPG 或 ICO 或 PNG
- 檔案大小上限：100 KB
- 建議的長寬比：1:1

桌布 - 選用

桌布可做為所有畫面的背景影像，建立有凝聚力的視覺化體驗。如果您未上傳自訂桌布，則會使用下方顯示的預設桌布。選擇一張既能與品牌形象相得益彰，又不影響內容可讀性的影像。



- 支援的格式：JPG 或 PNG
- 檔案大小上限：5 MB
- 建議的長寬比：16:9
- 建議的最低解析度：1920 x 1080

執行

- 使用不干擾前景內容的細微、低對比度桌布或模糊影像。
- 考慮預設文字置放，以避免文字後面的忙碌區域。
- 利用品牌顏色並使用浮水印來建立更好的對比和可讀性。

不要

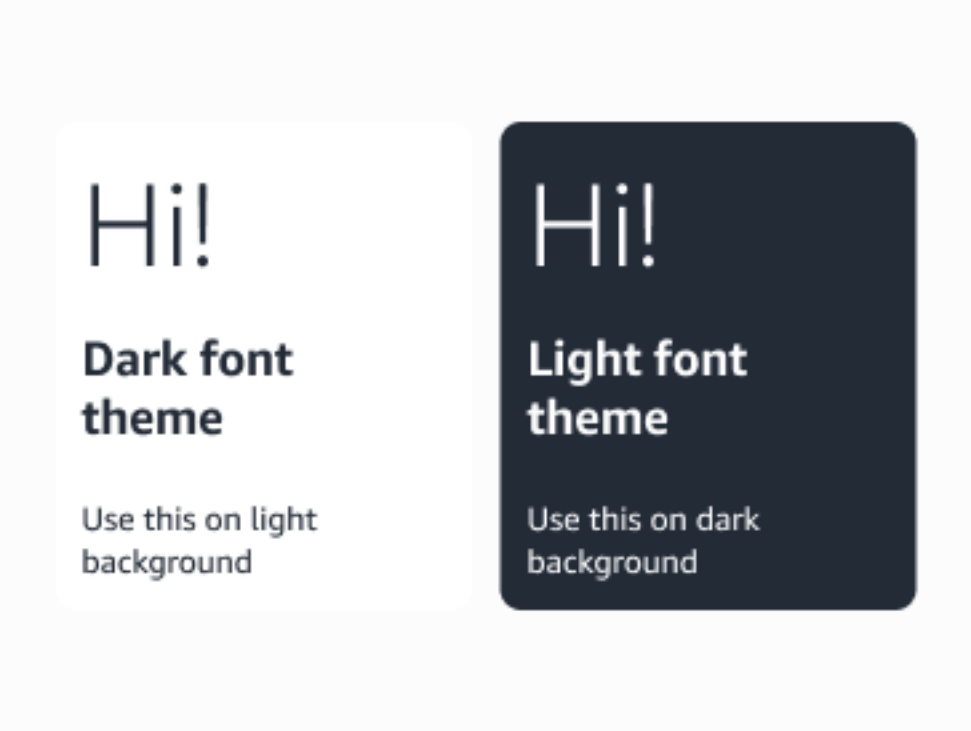
- 請勿在重要文字後面直接使用忙碌、飽和或高細節影像。
- 請勿使用視覺上複雜的影像或具有銳利轉換的影像，這些轉換會導致預設文字位置的可讀性限制。
- 如果沒有足夠的對比度，請勿僅倚賴顏色將文字與背景分隔。

彩色佈景主題

在反映字型、按鈕和模態的淺色或深色佈景主題之間進行選擇。

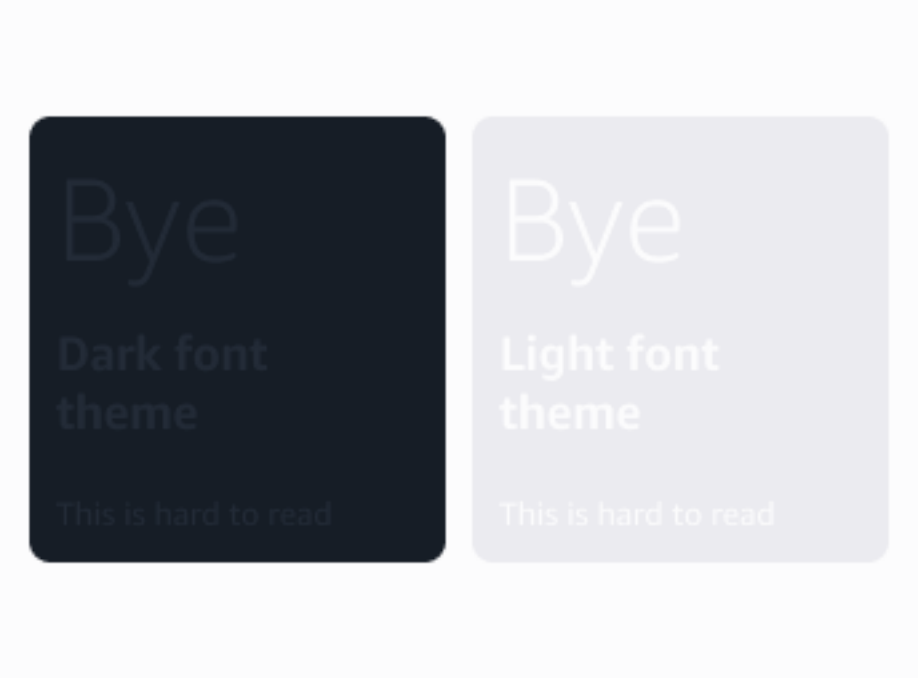
- 淺色佈景主題 - 最適合深色背景，在低光源環境中工作時提供清晰的對比，減少眼睛疲勞。
- 深色佈景主題 - 最適合淺色背景，在明亮環境中提供輕鬆的檢視，減少眩光。

執行



- 確保與背景元素/桌布形成強烈對比。
- 在淺色背景上使用深色佈景主題。
- 在深色背景上使用淺色佈景主題。

不要



- 請勿將淺色或深色字型放在影像或複雜的桌布上。

文字編輯器

文字編輯器可讓您自訂最終使用者登入畫面上顯示的文字。若要啟用品牌自訂，您必須至少新增一種語言。

對於新使用者：如果您使用品牌語言設定入口網站頁面，我們會偵測您的瀏覽器語言偏好設定，並以該語言顯示入口網站頁面。如果您的瀏覽器語言不是您設定的語言，我們會預設為英文 (en-US) (如果有)。如果您未設定英文，我們會依您設定的語言字母順序使用排列第一的語言。

對於傳回的使用者：我們會將您先前工作階段的語言偏好設定，儲存在瀏覽器 Cookie 中。如果該語言使用您設定的品牌語言，我們會使用該語言。否則，我們會遵循相同的備用方案邏輯：英文 (en-US)，或依字母順序設定的第一個語言。

支援下列地區設定 (語言代碼)：

- 德文 (de-DE)
- 英文 (en-US)
- 西班牙文 (es-ES)
- 法文 (fr-FR)
- 印尼文 (id-ID)

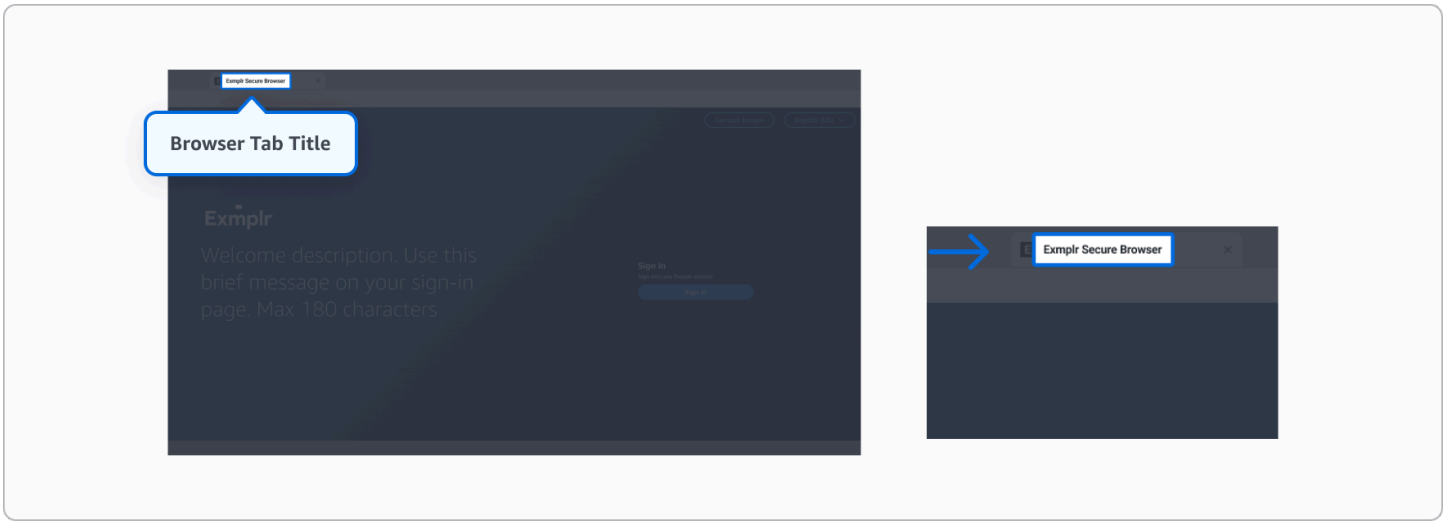
- 義大利文 (it-IT)
- 日文 (ja-JP)
- 韓文 (ko-KR)
- 葡萄牙文 (pt-BR)
- 簡體中文 (zh-CN)
- 繁體中文 (zh-TW)

基於安全考量，下列字元在所有文字欄位中會遭到封鎖：

- < (小於)
- > (大於)
- &(與符)
- ' (一般撇號)
- ` (反引號/重音符)
- ~ (波狀符號)
- \ (反斜線)。

瀏覽器索引標籤標題

瀏覽器索引標籤中顯示的文字。最多 25 個字元。

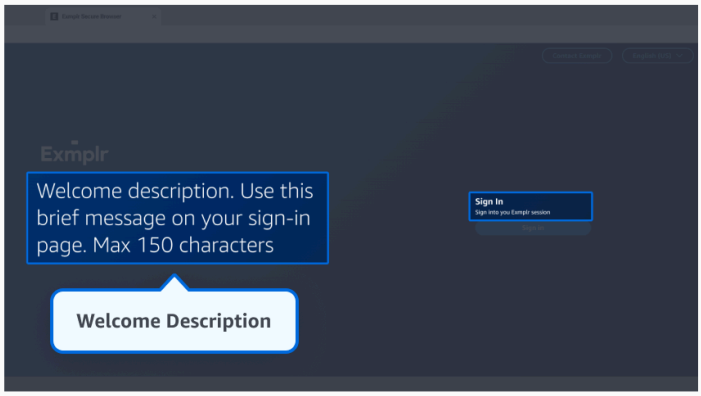


建議

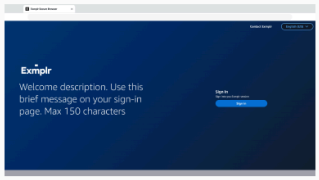
考慮使用簡短且清晰的標題，即使開啟多個索引標籤，它們仍保持可讀狀態。

歡迎描述

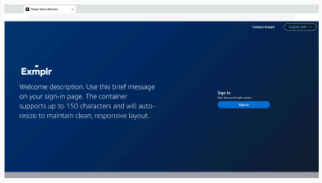
登入畫面上公司標誌的簡短描述。最多 150 個字元。



Welcome description



Starting font sizing



Adapted sizing to Max characters

建議

保持文字簡潔，以提高可讀性。請注意，較長的文字會自動擴展為較小的字型大小，而較短的訊息則會更明顯顯示。

聯絡區段

聯絡按鈕 - 選用

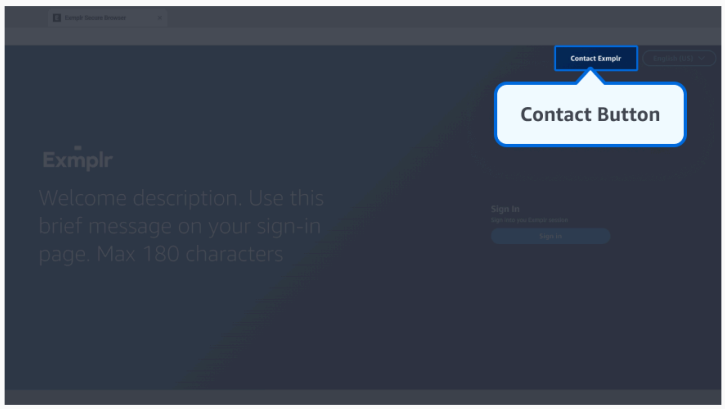
登入畫面上的聯絡按鈕文字。如果保留空白，則會顯示「聯絡我們」。最多 30 個字元。

聯絡連結 - 選用

登入畫面上的聯絡按鈕連結。您可以使用：

- 將使用者導向網頁的 HTTPS URL
- mailto：開啟使用者電子郵件用戶端的連結

如果保留空白，畫面中會隱藏聯絡人按鈕。



建議

讓文字保持簡短，最好是 2-3 個字。

登入區段

登入標頭 - 選用

登入頁面的登入區段標頭。如果保留空白，則會顯示「登入」。最多 100 個字元。

登入描述 - 選用

登入區段的描述文字。如果保留空白，則會顯示「登入 WorkSpaces 安全瀏覽器工作階段」。最多 250 個字元。

登入按鈕 - 選用

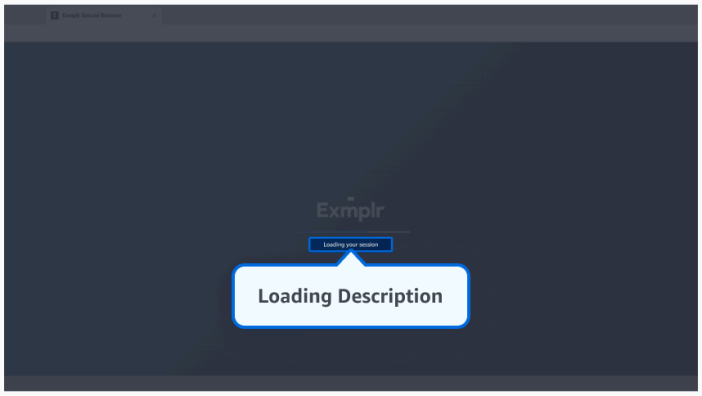
顯示在登入按鈕上的文字。如果保留空白，則會顯示「登入」。最多 30 個字元。

建議

- 讓文字保持簡短。
- 請考慮登入按鈕會將使用者導向至為您的入口網站設定的身分提供者。您可以自訂按鈕文字，以反映您的特定身分提供者。

載入描述

載入畫面連線期間顯示的文字。如果保留空白，則會顯示「連線中...」。最多 300 個字元。



Loading screen

建議

此訊息只會在工作階段載入時顯示，因此最終使用者可能沒有時間讀取。盡量避免讓它過長。

服務條款 - 選用

您可以自訂最終使用者在開始串流工作階段之前必須檢閱和接受的服務條款。您可以上傳 Markdown 檔案，或使用內建 Markdown 編輯器來新增此內容。

成功登入後，使用者會收到服務條款。他們必須捲動整個文件，然後按一下「接受」按鈕，以繼續他們的安全瀏覽器工作階段。如果使用者按一下「拒絕」，則會將其重新導向回登入頁面。

請注意，這是選用設定 - 如果您未新增服務條款，使用者會在登入後直接前往其工作階段。

支援的格式設定：

- 基本文字樣式 (粗體、斜體)
- 標題
- 已排序和未排序的清單
- 區塊引用
- 水平規則
- 簡單段落和換行

為了安全起見，會封鎖下列元素：

- 指令碼和程式碼執行
- 互動式元素，例如表單和 iframe
- 不安全的通訊協定和檔案路徑
- HTML 屬性和樣式
- 外部連結和資料表

請記住，您的服務條款檔案的大小不得超過 150KB。

在 Amazon WorkSpaces 安全瀏覽器中啟用 WebAuthn 重新導向支援

> **Warning**
>
> WebAuthn 重新導向僅適用於已啟用網際網路存取的瀏覽器工作階段。確保您的入口網站的網路設定允許 WebAuthn 功能的網際網路存取正常運作。

WorkSpaces 安全瀏覽器支援遠端瀏覽器工作階段中存取之網站的 WebAuthn (Web 身分驗證）。這允許使用者在瀏覽其 WorkSpaces 安全瀏覽器工作階段時，使用其本機 FIDO2 安全金鑰、生物識別驗證器和平台驗證器對網站進行身分驗證。

> **Note**
>
> WebAuthn 重新導向適用於使用 Google Chrome 136（或更新版本）或 Microsoft Edge 137（或更新版本）的最終使用者。此功能不適用於非 Chromium 瀏覽器，例如 Safari 或 Firefox。
>
> 若要啟用 WebAuthn 重新導向功能，管理員必須設定兩者：
>
> 1. 入口網站使用者設定 - 在入口網站設定中啟用 WebAuthn 重新導向
> 2. 最終使用者本機瀏覽器政策 - 在使用者裝置上設定 WebAuthenticationRemoteDesktopAllowedOrigins 瀏覽器政策，以允許 WebAuthn 重新導向

主題

在入口網站設定中啟用 WebAuthn 重新導向

若要為在遠端瀏覽器工作階段中存取的網站啟用 WebAuthn 重新導向，請遵循下列步驟。

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 WorkSpaces 安全瀏覽器、Web 入口網站、選擇您的 Web 入口網站，然後選擇編輯。
3. 導覽至使用者設定區段。
4. 在使用者許可下，將允許使用者在其入口網站工作階段中使用本機身分驗證設為允許。
5. 選擇儲存以套用組態。

設定 WebAuthn 的本機瀏覽器政策

除了在入口網站設定中啟用 WebAuthn 重新導向之外，還必須設定本機瀏覽器政策，以允許使用者本機裝置和遠端瀏覽器工作階段之間的 WebAuthn 重新導向，反之亦然。此組態通常由企業環境的 IT 管理員管理，或由 BYOD 案例的個別使用者管理。

瀏覽器政策必須包含您所在區域的 WorkSpaces 安全瀏覽器內容網域。根據您的區域，將下列原始伺服器新增至`WebAuthenticationRemoteDesktopAllowedOrigins`政策：

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

例如，在 us-west-2 中： `https://us-west-2.content.workspaces-web.com`

特定組態方法取決於您是管理企業環境中的瀏覽器，還是為 BYOD 使用者設定個別裝置。如需瀏覽器政策的詳細資訊，請參閱 Chrome Enterprise 政策文件和 Microsoft Edge 政策文件。

> **Note**
>
> 可能需要重新啟動瀏覽器，政策才會生效。

在遠端瀏覽器工作階段中使用 WebAuthn 重新導向

在入口網站設定中啟用 WebAuthn 重新導向並設定本機瀏覽器政策後，使用者可以在其 WorkSpaces 安全瀏覽器遠端瀏覽器工作階段內的網站上使用 WebAuthn 身分驗證。

使用者可以使用下列方式向網站進行身分驗證：

- 連接到其本機裝置的 FIDO2 安全金鑰
- 通行密鑰
- 平台驗證程式，例如 Windows Hello 或 Touch ID

WebAuthn 身分驗證程序會從遠端瀏覽器工作階段無縫轉送至使用者的本機裝置，提供安全的無密碼身分驗證，同時維護遠端瀏覽環境的安全優勢。

針對 WebAuthn 重新導向問題進行故障診斷

如果使用者在遠端瀏覽器工作階段中遇到 WebAuthn 重新導向問題，請使用下列疑難排解步驟來識別和解決常見問題。

主題

WebAuthn 重新導向無法運作

如果 WebAuthn 身分驗證提示未顯示或無法運作：

1. 確認已在使用者許可下的入口網站設定中啟用 WebAuthn。
2. 導覽至 `chrome://policy`或 `edge://policy`並確認 `WebAuthenticationRemoteDesktopAllowedOrigins` 包含您區域的內容 URL，以檢查本機瀏覽器政策是否已正確設定。
3. 確保瀏覽器版本符合要求：Chrome 136+ 或 Edge 137+。
4. 使用不同的驗證器進行測試（安全金鑰與平台驗證器）。

常見錯誤訊息

以下是常見的錯誤訊息及其解決方法：

WebAuthn 錯誤訊息和解決方案

錯誤訊息	Resolution
Amazon DCV WebAuthn 重新導向無法完成註冊請求：用戶端不支援 Webauthn 重新導向	檢查您是否使用支援的瀏覽器和版本 (Chrome 136+ 或 Edge 137+)。
提示出現，但無法與本機驗證者互動	檢查遠端瀏覽器中是否已安裝並啟用 Amazon DCV WebAuthn 重新導向延伸模組。
Amazon DCV WebAuthn 重新導向無法完成註冊請求：依賴方 ID 不是可註冊網域尾碼，也不等於目前的網域。之後，嘗試擷取所宣告 RP ID 的 .well-known/webauthn 資源失敗。	這表示不會套用 WebAuthenticationRemoteDesktopAllowedOrigins 本機瀏覽器政策。檢查政策並更新以允許內容網域。確定瀏覽器已重新啟動。您可能需要啟動新的工作階段，才能套用變更。
操作已逾時或不允許。請參閱：https：//https://www.w3.org/TR/webauthn-2/#sctn-privacy-considerations-client。	如果出現下列情況，可能會發生此錯誤：(1) 未安裝或啟用 DCV WebAuthn 重新導向延伸模組，(2) 使用者取消身分驗證提示，(3) 使用者輸

錯誤訊息	Resolution
	入不正確的安全金鑰 PIN，或 (4) 使用者未與提示互動，且請求逾時。

在 Amazon WorkSpaces 安全瀏覽器中管理工具列控制項

使用工具列控制項，您可以為最終使用者工作階段設定工具列呈現，包括下列選項：

- 功能
  - 剪貼簿：啟用時，允許使用精細控制項複製/貼上（僅複製、僅貼上或兩者）。停用時， 隱藏圖示並防止工具列使用。
  - 檔案傳輸：啟用時，允許使用精細控制進行檔案操作（僅上傳、僅下載或兩者）。停用時， 隱藏圖示並防止傳輸。
  - 麥克風：啟用時，允許麥克風使用。停用時， 隱藏圖示。
  - 網路攝影機：啟用時，允許使用攝影機。停用時， 隱藏圖示。
  - 雙監視器：啟用時，允許雙監視器用量。停用時， 隱藏圖示。
  - 全螢幕：啟用時，允許全螢幕模式。停用時， 隱藏圖示。
  - Windows：啟用時，允許在視窗之間移動。停用時， 隱藏圖示。
- 設定
  - 工具列主題：控制淺色或深色模式顯示。組態會移除最終使用者佈景主題控制。
  - 工具列狀態：設定工具列的停駐或分離狀態。組態會移除最終使用者對工具列狀態的控制。
  - 最大解析度：定義允許的最高顯示解析度。使用者最多只能選取此定義限制的解析度。

為您的入口網站設定自訂網域

您可以設定 WorkSpaces 安全瀏覽器入口網站的自訂網域，以透過您自己的網域名稱啟用存取，而非預設入口網站 URL。此功能可讓您使用與您組織品牌相符的網域，為使用者提供更整合的體驗。

概觀

自訂網域可讓您個人化使用者體驗的下列層面：

- 品牌入口網站存取 - 使用者透過組織的網域存取您的入口網站，而不是預設的 AWS 端點。
- 一致的使用者體驗 - 使用與您的組織一致的熟悉網域名稱來維持品牌一致性。

> **Note**
>
> 若要自訂入口網站的視覺效果和品牌元素，請參閱 the section called “品牌自訂”。

主題

為您的入口網站設定自訂網域

運作方式

當您設定自訂網域時：

- 您可以使用自訂網域建立和設定反向代理，將流量路由到入口網站端點。
- 使用者透過您的自訂網域存取您的入口網站，而不是預設入口網站端點。
- SSL 憑證可確保整個程序的安全連線。

先決條件

在設定自訂網域之前，請確定您有：

- 您透過 DNS 服務提供者管理的網域名稱，例如 Amazon Route53。
- WorkSpaces 安全瀏覽器入口網站。如需建立入口網站的詳細資訊，請參閱 the section called “Web 入口網站建立”。
- 確保您擁有管理 AWS Certificate Manager、CloudFront 和 DNS 組態的必要許可。

> **Important**
>
> 使用者必須在其瀏覽器中為自訂網域啟用第三方 Cookie，以確保適當的入口網站功能。
> 確保您擁有並正確管理自訂網域及其 DNS 記錄，以維護入口網站的安全性和功能。

> **Note**
>
> 若要啟用自訂網域的單一登入擴充功能，使用者必須在瀏覽器中安裝 擴充功能，版本必須高於 1.0.2505.6608。
> 當使用者登入入口網站時，系統會提示他們安裝擴充功能。如需有關擴充功能使用者體驗的詳細資訊，請參閱 the section called “單一登入延伸”。

開始使用

您可以在建立新入口網站或編輯現有入口網站時，將自訂網域設定為入口網站設定屬性。這可以使用 AWS 主控台、 SDK、CloudFormation 或 AWS CLI 命令來完成。

我們建議將 Amazon CloudFront 分佈設定為反向代理，將流量從您的自訂網域路由到 WorkSpaces 安全瀏覽器入口網站端點。

> **Note**
>
> 雖然建議使用 Amazon CloudFront 做為反向代理解決方案，但您可以使用替代的反向代理組態。請確定您符合 Amazon CloudFront 設定步驟中詳述的必要原始伺服器和快取組態設定。

將 CloudFront 設定為反向代理

若要完成設定反向代理，您需要：

- 透過 AWS Certificate Manager (ACM) 的 SSL 憑證
- Amazon CloudFront 分佈
- DNS 記錄
- 使用自訂網域設定的入口網站

SSL 憑證

如果您還沒有，請依照下列步驟透過 ACM 請求一個：

1. 導覽至位於 的 ACM 主控台https://console.aws.amazon.com/acm。

> **Important**
>
> 使用美國東部（維吉尼亞北部）區域，因為 CloudFront 需要將憑證存放在該區域。

2. 請求憑證：
   - 對於新的 ACM 使用者：選擇佈建憑證下的入門
   - 對於現有的 ACM 使用者：選擇請求憑證
3. 選擇請求公有憑證，然後選擇請求憑證。

> **Note**
>
> 您也可以匯入現有的憑證。如需詳細資訊，請參閱《ACM 使用者指南》中的將憑證匯入 ACM。

4. 輸入您的主要網域名稱（例如 **`myportal.example.com`**）。
5. 選擇驗證方法：
   - DNS 驗證（建議 Route 53 使用者使用）– 允許在您的託管區域中自動建立記錄集。如需詳細資訊，請參閱《ACM 使用者指南》中的 DNS 驗證。
   - 電子郵件驗證 – 如需詳細資訊，請參閱《ACM 使用者指南》中的電子郵件驗證。
6. 檢閱您的設定，然後選擇確認和請求。

CloudFront 分佈

建立 CloudFront 分佈，將請求從自訂網域代理到入口網站端點。

1. 導覽至位於 的 CloudFront 主控台https://console.aws.amazon.com/cloudfront。
2. 選擇 Create Distribution (建立分佈)。
   - 分佈名稱：輸入分佈的名稱
   - 分佈類型：單一網站或應用程式

> **Note**
>
> 如果您的自訂網域是在相同 AWS 帳戶中的 Route 53 中管理，CloudFront 可以自動為您管理您的 DNS。輸入您的自訂網域，然後按一下「檢查網域」。如果您有來自不同 DNS 供應商的網域，請略過此步驟，稍後再設定您的網域。

3. 設定原始伺服器設定：

   - 原始伺服器類型：其他
   - 自訂原始伺服器：輸入入口網站端點 *<portalId>*.workspaces-web.com
   - 原始路徑：保留空白（預設）

4. 自訂原始伺服器設定：

   - 新增自訂標頭

   > **Important**
   >
   > 只有在代理請求中存在此標頭時，才能透過自訂網域存取入口網站。確定標頭名稱和值的指定與上述完全相同。

     - 標頭名稱：workspacessecurebrowser-custom-domain
     - 值：您的自訂網域（例如 **myportal.example.com**）
   - 通訊協定：僅限 HTTPS
   - HTTPS 連接埠：443（保留預設值）
   - 最低原始 SSL 通訊協定：TLSv1.2（預設）
   - 原始 IP 地址類型：僅限 IPv4（撰寫此管理指南時，Amazon WorkSpaces 安全瀏覽器不支援 IPv6。）

5. 自訂快取設定：

   - 檢視器通訊協定政策：將 HTTP 重新導向至 HTTPS
   - 允許 HTTP 方法：GET、HEAD、OPONS、PUT、POST、PATCH、DELETE
   - 快取政策：CachingDisabled
   - 原始伺服器請求政策：AllViewerExceptHostHeader

> **Important**
>
> 只有在原始伺服器請求政策設定為 AllViewerExceptHostHeader 時，才能透過自訂網域存取入口網站。顧名思義，此政策只會從請求標頭篩選出主機標頭，並將所有剩餘的標頭傳遞至原始伺服器。

6. 您可以視需要設定 WAF，但此設定不需要。
7. 在取得 TLS 憑證中，選取在步驟 1 中建立的 TLS 憑證。
8. 檢閱設定，然後選擇建立分佈。

DNS 記錄

如果您的託管區域位於相同的 AWS 帳戶中，Cloudfront 可以更新 Route 53 中的 DNS 記錄，將流量從指定的網域路由到步驟 2 中建立的分佈。

1. 導覽至 CloudFront 設定
2. 按一下「將網域路由到 CloudFront」
3. 按一下「自動設定路由」

如果您已為另一個服務提供者或其他 AWS 帳戶中的自訂網域設定 DNS，請設定您的 DNS 提供者，將網域的流量路由至 分佈。下列步驟說明如何使用 Route 53 執行此操作。

1. 在 開啟 Amazon Route 53 主控台https://console.aws.amazon.com/route53。
2. 存取 DNS 管理：
   - 如果您不熟悉搭配此 AWS 帳戶使用 Route 53，則會開啟 Amazon Route 53 概觀頁面。在 DNS 管理下，選擇立即開始使用。
   - 如果您之前已使用此 AWS 帳戶使用 Route 53，請繼續下一個步驟。
3. 在導覽窗格中，選擇 Hosted zones (託管區域)。
4. 如果您還沒有託管區域，請建立託管區域：
   - 若要將網際網路流量路由到您的 資源，請參閱《Amazon Route 53 開發人員指南》中的建立公有託管區域。
   - 若要路由 VPC 中的流量，請參閱《Amazon Route 53 開發人員指南》中的建立私有託管區域。
5. 在託管區域頁面上，選擇您要管理的託管區域名稱。

6. 選擇 Create Record Set (建立記錄集)。
7. 為您的網域建立項目 （ 例如 **myportal.example.com**) ：

   - 類型：A – IPv4 地址
   - Alias (別名)：是
   - 別名目標：CloudFront 分佈 URL

   保留所有其他設定的預設值。

> **Note**
>
> 如果您不是使用 Route 53 來管理網域的 DNS，請使用 DNS 服務提供者，並將指向網域的 DNS 項目新增至 CloudFront 分佈的 URL。

或者，您可以使用下列 CloudFormation 範本來建立 CloudFront 分佈：

此 CloudFormation 範本會自動建立 CloudFront 分佈、設定反向代理設定，以及選擇性地建立 Route53 DNS 記錄：

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"
```

若要使用此範本：

1. 將上述範本儲存為 `workspaces-web-custom-domain-template.yaml`
2. 使用 AWS 主控台、 AWS CLI 或 AWS SDK 搭配特定參數值進行部署
3. 部署之後，請使用自訂網域設定您的入口網站，如以下步驟 4 所述

入口網站組態

使用 AWS 主控台、UpdatePortal API 或 update-portal CLI AWS 命令，將您的自訂網域註冊為入口網站設定屬性。

1. 在 開啟 WorkSpaces 安全瀏覽器主控台https://console.aws.amazon.com/workspaces-web/home。
2. 在導覽窗格中，選擇 Web 入口網站。
3. 選取您要設定的 Web 入口網站，然後選擇編輯。

4. 在入口網站設定中，新增您的自訂網域。
5. 儲存入口網站組態。

測試您的組態

若要測試您的組態，請依照下列步驟進行：

1. 開啟 Web 瀏覽器並導覽至自訂網域的 URL （例如 **https://myportal.example.com**)。
2. 如果一切設定正確，您應該會看到入口網站的登入頁面。
3. 接著，在瀏覽器中輸入入口網站 URL，您應該會在登入 IdP 之後重新導向至自訂網域。
4. 最後，登入您的 IdP，然後按一下入口網站的應用程式圖磚。您應該重新導向至自訂網域。

對自訂網域問題進行故障診斷

如果使用者在遠端瀏覽器工作階段中遇到透過自訂網域存取入口網站的問題，請使用下列疑難排解步驟來識別和解決常見問題。

主題

常見錯誤訊息

以下是設定自訂網域時常見的錯誤訊息及其解決方法：

無效的 CSRF 字符錯誤

當安全瀏覽器無法透過 CloudFront 設定正確接收您的請求時，就會發生此錯誤。

若要解決此問題：

- 檢查 CloudFront 分佈上的自訂原始伺服器設定。
- 確認自訂標頭的名稱完全相符，`workspacessecurebrowser-custom-domain`且值完全符合您的自訂網域（不含 https：// 或任何查詢參數）。
- 清除本機瀏覽器上的快取。
- 使 CloudFront 上的快取失效。

502 錯誤的閘道錯誤

此錯誤通常表示快取組態問題。

若要解決此問題：

- 檢查 CloudFront 分佈上的快取設定。
- 確認快取政策設定為 `CachingDisabled`。
- 確認原始伺服器請求政策設定為 `AllViewerExceptHostHeader`。
- 清除本機瀏覽器上的快取。
- 使 CloudFront 上的快取失效。

存取遭拒錯誤

如果您的自訂網域設定不正確，可能會發生此錯誤。

若要解決此問題：

- 檢查 CloudFront 分佈上的原始伺服器設定。
- 確認原始伺服器已設定為正確的入口網站 URL。
- 確認入口網站已設定正確的自訂網域。
- 清除本機瀏覽器上的快取。
- 使 CloudFront 上的快取失效。

Amazon WorkSpaces 安全瀏覽器的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。 AWS 也為您提供可安全使用的服務。在AWS 合規計劃中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 Amazon WorkSpaces 安全瀏覽器的合規計劃，請參閱合規計劃的 AWS 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用於您資料的法律和法規。

本文件可協助您了解如何在使用 Amazon WorkSpaces 安全瀏覽器時套用共同責任模型。其中說明如何設定 Amazon WorkSpaces 安全瀏覽器以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Amazon WorkSpaces 安全瀏覽器資源。

目錄

Amazon WorkSpaces 安全瀏覽器中的資料保護

AWS 共同責任模型適用於 Amazon WorkSpaces 安全瀏覽器中的資料保護。如此模型所述， AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常

見問答集。如需有關歐洲資料保護的相關資訊，請參閱AWS 安全性部落格上的AWS 共同責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 WorkSpaces 安全瀏覽器或使用主控台 AWS CLI、API 或 AWS SDKs的其他 AWS 服務 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

主題

Amazon WorkSpaces 安全瀏覽器中的資料加密

Amazon WorkSpaces 安全瀏覽器會收集入口網站自訂資料，例如瀏覽器設定、使用者設定、網路設定、身分提供者資訊、信任存放區資料和信任存放區憑證資料。WorkSpaces 安全瀏覽器也會收集瀏覽器政策資料、使用者偏好設定 （適用於瀏覽器設定） 和工作階段日誌。收集到的資料存放在 Amazon DynamoDB 和 Amazon S3 中。WorkSpaces 安全瀏覽器使用 AWS Key Management Service 進行加密。

若要保護您的內容，請遵循下列指示：

- 實作最低權限存取，並建立要用於 WorkSpaces 安全瀏覽器動作的特定角色。使用 IAM 範本建立完整存取角色或唯讀角色。如需詳細資訊，請參閱AWS WorkSpaces 安全瀏覽器的 受管政策。
- 提供客戶受管金鑰來保護端對端資料，因此 WorkSpaces 安全瀏覽器可以使用您提供的金鑰加密靜態資料。
- 請謹慎共享入口網域和使用者憑證：
  - 管理員必須登入 Amazon WorkSpaces 主控台，而使用者必須登入 WorkSpaces 安全瀏覽器入口網站。
  - 網際網路上的任何人都可以存取 Web 入口網站，但除非擁有入口網站的有效使用者憑證，否則他們無法啟動工作階段。
- 使用者可以選擇結束工作階段，明確結束工作階段。這會捨棄託管瀏覽器工作階段的執行個體，造成瀏覽器隔離。

WorkSpaces 安全瀏覽器預設會使用 加密所有敏感資料，以保護內容和中繼資料 AWS KMS。它會收集瀏覽器政策和使用者偏好設定，以在 WorkSpaces 安全瀏覽器工作階段期間強制執行政策和設定。如果在套用現有設定時發生錯誤，使用者將無法存取新的工作階段，也無法存取公司的內部網站和 SaaS 應用程式。

Amazon WorkSpaces 安全瀏覽器的靜態加密

根據預設，靜態加密是設定，而 WorkSpaces 安全瀏覽器中使用的所有客戶資料 （例如瀏覽器政策陳述式、使用者名稱、記錄或 IP 地址） 都會使用 加密 AWS KMS。根據預設，WorkSpaces 安全瀏覽器會使用 AWS擁有的金鑰啟用加密。您也可以在資源建立時指定 CMK，以使用客戶受管金鑰 (CMK)。這目前僅透過 CLI 支援。

如果您選擇傳遞 CMK，提供的金鑰必須是對稱加密 AWS KMS 金鑰，而且身為管理員的您必須具有下列許可：

```
kms:DescribeKey

kms:GenerateDataKey

kms:GenerateDataKeyWithoutPlaintext

kms:Decrypt

kms:ReEncryptTo
```

```
kms:ReEncryptFrom
```

如果您使用 CMK，則需要允許列出 WorkSpaces 安全瀏覽器外部服務主體以存取金鑰。
如需詳細資訊，請參閱 aws：SourceAccount 的 CMK 金鑰政策範圍範例

WorkSpaces 安全瀏覽器會盡可能使用轉送存取工作階段 (FAS) 登入資料來存取您的金鑰。如需 FAS 的詳細資訊，請參閱轉送存取工作階段。
在某些情況下，WorkSpaces 安全瀏覽器可能需要以非同步方式存取您的金鑰。透過在金鑰政策中允許列出 WorkSpaces 安全瀏覽器外部服務主體，WorkSpaces 安全瀏覽器將能夠使用金鑰執行允許列出的一組密碼編譯操作。

建立資源之後，就無法再移除或變更金鑰。如果您使用 CMK，身為存取資源的管理員，您必須擁有下列許可：

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

kms:ReEncryptTo
kms:ReEncryptFrom
```

如果您在使用主控台時看到存取遭拒錯誤，則存取主控台的使用者可能沒有在正在使用的金鑰上使用 CMK 所需的許可。

WorkSpaces 安全瀏覽器的金鑰政策和範圍範例

CMKs需要下列金鑰政策：

```
{
  "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": "*",
      }
    ]
}
```

WorkSpaces 安全瀏覽器需要下列許可：

- `kms:DescribeKey` — 驗證提供的 AWS KMS 金鑰已正確設定。
- `kms:GenerateDataKeyWithoutPlaintext` 和 `kms:GenerateDataKey` — 請求 AWS KMS 金鑰建立用於加密物件的資料金鑰。
- `kms:Decrypt` — 請求 AWS KMS 金鑰以解密加密的資料金鑰。這些資料金鑰用於加密您的資料。
- `kms:ReEncryptTo` 和 `kms:ReEncryptFrom` — 請求 AWS KMS 金鑰允許從 KMS 金鑰重新加密或重新加密至 KMS 金鑰。

在 AWS KMS 金鑰上擴展 WorkSpaces 安全瀏覽器許可

當金鑰政策陳述式中的委託人是AWS 服務委託人時，我們強烈建議您在加密內容之外，使用 aws：SourceArn 或 aws：SourceAccount 全域條件金鑰。

用於資源的加密內容一律會包含 格式的項目，`aws:workspaces-web:RESOURCE_TYPE:id`以及對應的資源 ID。

只有在 AWS KMS 請求來自其他服務時，來源 ARN 和來源帳戶值才會包含在授權內容中 AWS 。這個條件組合會實作最低權限許可，並避免潛在的混淆代理人案例。如需詳細資訊，請參閱金鑰政策中 AWS 服務的許可。

```
  "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**
>
> 在建立資源之前，金鑰政策應該僅使用 aws:SourceAccount 條件，因為完整的資源 ARN 尚不存在。建立資源後，可以更新金鑰政策以包含 aws:SourceArn和 kms:EncryptionContext條件。

使用 的範圍 CMK 金鑰政策範例 **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>"
        }
      }
    }
  ]
}
```

使用 **aws:SourceArn**和資源萬用字元的範圍 CMK 金鑰政策範例

```
{
```

```
  "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>:*/*"
        }
      }
    }
  ]
}
```

使用 的範圍 CMK 金鑰政策範例 **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**
>
> 建立資源之後，您可以在 中SourceArn更新資源的萬用字元。如果您使用 WorkSpaces 安全瀏覽器建立需要 CMK 存取的新資源，請務必相應地更新其金鑰政策。

具有 **aws:SourceArn**和資源特定的範圍 CMK 金鑰政策範例 **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**
>
> 在相同金鑰政策EncryptionContext中包含特定資源時，請務必建立個別的陳述式。如需詳細資訊，請參閱 kms:EncryptionContext：context-key 下的使用多個加密內容對一節。

Amazon WorkSpaces 安全瀏覽器的傳輸中加密

WorkSpaces 安全瀏覽器會透過 HTTPS 和 TLS 1.2 加密傳輸中的資料。您可以使用主控台或直接 API 呼叫，將請求傳送至 WorkSpaces。傳輸的請求資料會透過 HTTPS 或 TLS 連線傳送所有資料來進行加密。請求資料可以從 AWS 主控台 AWS Command Line Interface或 AWS SDK 傳輸到 WorkSpaces 安全瀏覽器。

預設會設定對傳輸中的資料進行加密，預設會設定安全連線 (HTTPS、TLS)。

Amazon WorkSpaces 安全瀏覽器的金鑰管理

您可以提供自己的客戶受管 AWS KMS 金鑰來加密您的客戶資訊。如果您不提供，WorkSpaces 安全瀏覽器將使用 AWS 擁有的金鑰。您可以使用 AWS SDK 設置金鑰。

Amazon WorkSpaces 安全瀏覽器中的網路流量隱私權

為了保護 WorkSpaces 安全瀏覽器與內部部署應用程式之間的連線，您可以使用 WorkSpaces 安全瀏覽器在您自己的 VPC 內啟動瀏覽器工作階段。內部部署應用程式的連線是在您自己的 VPC 中設定，且不受 WorkSpaces 安全瀏覽器控制。

為了保護帳戶之間的連線，WorkSpaces 安全瀏覽器會使用服務連結角色安全地連線至客戶帳戶，並代表客戶執行操作。如需詳細資訊，請參閱使用 Amazon WorkSpaces 安全瀏覽器的服務連結角色。

Amazon WorkSpaces 安全瀏覽器中的使用者存取記錄

管理員能夠記錄 WorkSpaces 安全瀏覽器工作階段事件，包括開始、停止和 URL 造訪。這些日誌經過加密，並且透過 Amazon Kinesis Data Stream 安全交給客戶。使用者存取記錄的瀏覽資訊不會由 儲存 AWS，也不會在未設定記錄的情況下從工作階段中取得。在無痕模式下造訪 URL，或從瀏覽器歷程記錄中刪除的 URL，不會記錄在使用者存取日誌記錄中。

Amazon WorkSpaces 安全瀏覽器的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ），以使用 WorkSpaces 安全瀏覽器資源。IAM 是您可以免費使用 AWS 服務 的 。

主題

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 對 Amazon WorkSpaces 安全瀏覽器身分和存取進行故障診斷)
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 Amazon WorkSpaces 安全瀏覽器如何與 IAM 搭配使用)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 Amazon WorkSpaces 安全瀏覽器的身分型政策範例)

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須驗證為 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的AWS 第 4 版簽署程序。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分可完整存取所有 AWS 服務 和 資源。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務 使用臨時憑證存取 。

聯合身分是您企業目錄、Web 身分提供者的使用者，或是 AWS 服務 使用身分來源的憑證 Directory Service 存取的使用者。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色 （主控台） 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS ， 會評估這些政策。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中指定主體。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。
- 服務控制政策 (SCP) — 為 AWS Organizations中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的資源控制政策 (RCP)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的工作階段政策。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 決定是否在涉及多個政策類型時允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon WorkSpaces 安全瀏覽器如何與 IAM 搭配使用

在您使用 IAM 管理 WorkSpaces 安全瀏覽器的存取權之前，請先了解哪些 IAM 功能可與 WorkSpaces 安全瀏覽器搭配使用。

您可以搭配 Amazon WorkSpaces 安全瀏覽器使用的 IAM 功能

IAM 功能	WorkSpaces 安全瀏覽器支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC(政策中的標籤)	部分
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	是

若要全面了解 WorkSpaces 安全瀏覽器和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS 與 IAM 搭配使用的 服務。

主題

- WorkSpaces 安全瀏覽器的身分型政策
- WorkSpaces 安全瀏覽器中的資源型政策
- WorkSpaces 安全瀏覽器的政策動作

- WorkSpaces 安全瀏覽器的政策資源
- WorkSpaces 安全瀏覽器的政策條件索引鍵
- WorkSpaces 安全瀏覽器中的存取控制清單 (ACLs)
- 使用 WorkSpaces 安全瀏覽器的屬性型存取控制 (ABAC)
- 搭配 WorkSpaces 安全瀏覽器使用臨時登入資料
- WorkSpaces 安全瀏覽器的跨服務主體許可
- WorkSpaces 安全瀏覽器的服務角色
- WorkSpaces 安全瀏覽器的服務連結角色

WorkSpaces 安全瀏覽器的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

WorkSpaces 安全瀏覽器的身分型政策範例

若要檢視 WorkSpaces 安全瀏覽器身分型政策的範例，請參閱 Amazon WorkSpaces 安全瀏覽器的身分型政策範例。

WorkSpaces 安全瀏覽器中的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

WorkSpaces 安全瀏覽器的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

若要查看 WorkSpaces 安全瀏覽器動作的清單，請參閱服務授權參考中的 Amazon WorkSpaces 安全瀏覽器定義的動作。

WorkSpaces 安全瀏覽器中的政策動作在動作之前使用以下字首：

```
workspaces-web
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視 WorkSpaces 安全瀏覽器身分型政策的範例，請參閱 Amazon WorkSpaces 安全瀏覽器的身分型政策範例。

WorkSpaces 安全瀏覽器的政策資源

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

若要查看 WorkSpaces 安全瀏覽器資源類型及其 ARNs的清單，請參閱服務授權參考中的 Amazon WorkSpaces 安全瀏覽器定義的資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon WorkSpaces 安全瀏覽器定義的動作。

若要檢視 WorkSpaces 安全瀏覽器身分型政策的範例，請參閱 Amazon WorkSpaces 安全瀏覽器的身分型政策範例。

WorkSpaces 安全瀏覽器的政策條件索引鍵

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Condition` 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看 WorkSpaces 安全瀏覽器條件索引鍵的清單，請參閱服務授權參考中的 Amazon WorkSpaces 安全瀏覽器的條件索引鍵。若要了解您可以使用條件索引鍵的動作和資源，請參閱 Amazon WorkSpaces 安全瀏覽器定義的動作。

若要檢視 WorkSpaces 安全瀏覽器身分型政策的範例，請參閱 Amazon WorkSpaces 安全瀏覽器的身分型政策範例。

WorkSpaces 安全瀏覽器中的存取控制清單 (ACLs)

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

使用 WorkSpaces 安全瀏覽器的屬性型存取控制 (ABAC)

支援 ABAC (政策中的標籤)：部分

屬性型存取控制 (ABAC) 是一種授權策略，根據稱為標籤的屬性定義許可權。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的使用 ABAC 授權定義許可。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

搭配 WorkSpaces 安全瀏覽器使用臨時登入資料

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，並在您使用聯合或切換角色時自動建立。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

WorkSpaces 安全瀏覽器的跨服務主體許可

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

WorkSpaces 安全瀏覽器的服務角色

支援服務角色：否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷 WorkSpaces 安全瀏覽器的功能。只有在 WorkSpaces 安全瀏覽器提供指引時，才能編輯服務角色。

WorkSpaces 安全瀏覽器的服務連結角色

支援服務連結角色：是

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在資料表中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

Amazon WorkSpaces 安全瀏覽器的身分型政策範例

根據預設，使用者和角色沒有建立或修改 WorkSpaces 安全瀏覽器資源的許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

如需 WorkSpaces 安全瀏覽器定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱服務授權參考中的 Amazon WorkSpaces 安全瀏覽器的動作、資源和條件索引鍵。

主題

- Amazon WorkSpaces 安全瀏覽器的身分型政策最佳實務
- 使用 Amazon WorkSpaces 安全瀏覽器主控台
- 允許使用者檢視自己的 Amazon WorkSpaces 安全瀏覽器許可

Amazon WorkSpaces 安全瀏覽器的身分型政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 WorkSpaces 安全瀏覽器資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作

AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。

- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 IAM 安全最佳實務。

使用 Amazon WorkSpaces 安全瀏覽器主控台

若要存取 Amazon WorkSpaces 安全瀏覽器主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 WorkSpaces 安全瀏覽器資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保使用者和角色仍然可以使用 WorkSpaces 安全瀏覽器主控台，請將 WorkSpaces 安全瀏覽器`ConsoleAccess`或`ReadOnly` AWS 受管政策連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

允許使用者檢視自己的 Amazon WorkSpaces 安全瀏覽器許可

此範例會示範如何建立政策，允許 IAM 使用者檢視連接到他們使用者身分的內嵌及受管政策。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
    "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 WorkSpaces 安全瀏覽器的 受管政策

若要新增許可給使用者、群組和角色，使用 AWS 受管政策比自行撰寫政策更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並且可在您的帳戶中使用 AWS 。如需 AWS 受管政策的詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 服務會維護和更新 AWS 受管政策。您無法變更 AWS 受管政策中的許可。服務可能會偶爾將其他許可新增至 AWS 受管政策，以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

此外， AWS 支援跨多個 服務之任務函數的受管政策。例如， `ReadOnlyAccess` AWS 受管政策提供所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時， 會為新操作和資源 AWS 新增唯讀許可。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

主題

- AWS 受管政策：AmazonWorkSpacesWebServiceRolePolicy
- AWS 受管政策：AmazonWorkSpacesSecureBrowserReadOnly
- AWS 受管政策：AmazonWorkSpacesWebReadOnly
- AWS 受管政策的 WorkSpaces 安全瀏覽器更新

AWS 受管政策：AmazonWorkSpacesWebServiceRolePolicy

您無法將 AmazonWorkSpacesWebServiceRolePolicy 政策附加至 IAM 實體。此政策會連接到服務連結角色，允許 WorkSpaces 安全瀏覽器代表您執行動作。如需詳細資訊，請參閱the section called “使用服務連結角色”。

此政策授予管理許可，允許存取 WorkSpaces 安全瀏覽器使用或管理 AWS 的服務和資源。

許可詳細資訊

此政策包含以下許可：

- workspaces-web – 允許存取 WorkSpaces 安全瀏覽器使用或管理 AWS 的服務和資源。
- ec2 – 允許主體描述 VPC、子網路和可用區域；建立、標記、描述和刪除網路介面；關聯或取消關聯地址；以及描述路由表、安全群組和 VPC 端點。
- CloudWatch – 允許主體放置指標資料。
- Kinesis - 允許主體描述 Kinesis 資料串流的摘要，並將紀錄放入 Kinesis 資料串流中以供使用者存取日誌記錄。如需詳細資訊，請參閱the section called “設定使用者活動記錄”。

```
{
    "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 受管政策：AmazonWorkSpacesSecureBrowserReadOnly

您可將 AmazonWorkSpacesSecureBrowserReadOnly 政策連接到 IAM 身分。

此政策授予唯讀許可，允許透過 AWS 管理主控台、 SDK 和 CLI 存取 WorkSpaces 安全瀏覽器及其相依性。此政策不包括使用 IAM_Identity_Center 當成驗證類型與入口網站進行互動所需的許可。若要取得這些許可，請將此政策加上 AWSSSOReadOnly。

許可詳細資訊

此政策包含以下許可。

- workspaces-web – 透過 AWS 管理主控台、 SDK 和 CLI 提供 WorkSpaces 安全瀏覽器及其相依性的唯讀存取權。
- ec2：允許主體描述 VPC、子網路與安全群組。這在 WorkSpaces 安全瀏覽器的 AWS 管理主控台中使用，以顯示可供與服務搭配使用VPCs、子網路和安全群組。
- Kinesis – 允許主體取得 Kinesis 資料串流的清單。這是在 WorkSpaces 安全瀏覽器的 AWS 管理主控台中用來顯示可用於 服務的 Kinesis 資料串流。

```
{
    "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 受管政策：AmazonWorkSpacesWebReadOnly

您可將 AmazonWorkSpacesWebReadOnly 政策連接到 IAM 身分。

此政策授予唯讀許可，允許透過 AWS 管理主控台、 SDK 和 CLI 存取 WorkSpaces 安全瀏覽器及其相依性。此政策不包括使用 IAM_Identity_Center 當成驗證類型與入口網站進行互動所需的許可。若要取得這些許可，請將此政策加上 AWSSSOReadOnly。

> **Note**
>
> 如果您目前正在使用此政策，請切換到新AmazonWorkSpacesSecureBrowserReadOnly政策。

許可詳細資訊

此政策包含以下許可。

- workspaces-web – 透過 AWS 管理主控台、 SDK 和 CLI 提供 WorkSpaces 安全瀏覽器及其相依性的唯讀存取權。
- ec2：允許主體描述 VPC、子網路與安全群組。這在 WorkSpaces 安全瀏覽器的 AWS 管理主控台中使用，以顯示可供與服務搭配使用VPCs、子網路和安全群組。
- Kinesis – 允許主體取得 Kinesis 資料串流的清單。這是在 WorkSpaces 安全瀏覽器的 AWS 管理主控台中用來顯示可用於 服務的 Kinesis 資料串流。

```
{
    "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 受管政策的 WorkSpaces 安全瀏覽器更新

檢視自此服務開始追蹤這些變更以來WorkSpaces 安全瀏覽器的 AWS 受管政策更新詳細資訊。如需有關此頁面變更的自動提醒，請訂閱 文件歷史紀錄 頁面的 RSS 摘要。

變更	描述	Date
AmazonWorkSpacesSecureBrowserReadOnly – 新政策	WorkSpaces 安全瀏覽器新增了新政策，透過 AWS 管理主控台、 SDK 和 CLI 提供 WorkSpaces 安全瀏覽器及其相依性的唯讀存取權。	2024 年 6 月 24 日
AmazonWorkSpacesWebServiceRolePolicy – 更新的政策	WorkSpaces 安全瀏覽器已更新政策，限制 CreateNetworkInterface 使用 aws：RequestTag/WorkSpacesWebManaged： true 並對子網路和安全群組資源採取行動，以及限制 DeleteNetworkInterface 使用 aws：ResourceTag/WorkSpacesWebManaged：true 標記的 ENIs。	2022 年 12 月 15 日

變更	描述	Date
AmazonWorkSpacesWebReadOnly – 更新的政策	WorkSpaces 安全瀏覽器已更新政策，以包含使用者存取記錄和列出 Kinesis 資料串流的讀取許可。如需詳細資訊，請參閱the section called “設定使用者活動記錄”。	2022 年 11 月 2 日
AmazonWorkSpacesWebServiceRolePolicy – 更新的政策	WorkSpaces 安全瀏覽器已更新政策，以描述 Kinesis 資料串流的摘要，並將記錄放入 Kinesis 資料串流，以供使用者存取記錄。如需詳細資訊，請參閱the section called “設定使用者活動記錄”。	2022 年 10 月 17 日
AmazonWorkSpacesWebServiceRolePolicy – 更新的政策	WorkSpaces 安全瀏覽器已更新政策，以在 ENI 建立期間建立標籤。	2022 年 9 月 6 日
AmazonWorkSpacesWebServiceRolePolicy – 更新的政策	WorkSpaces 安全瀏覽器已更新政策，將 AWS/Usage 命名空間新增至 PutMetricData API 許可。	2022 年 4 月 6 日
AmazonWorkSpacesWebReadOnly – 新政策	WorkSpaces 安全瀏覽器新增了新政策，透過 AWS 管理主控台、 SDK 和 CLI 提供 WorkSpaces 安全瀏覽器及其相依性的唯讀存取權。	2021 年 11 月 30 日
AmazonWorkSpacesWebServiceRolePolicy – 新政策	WorkSpaces 安全瀏覽器新增了新的政策，以允許存取 WorkSpaces 安全瀏覽器使用或管理的 AWS 服務和資源。	2021 年 11 月 30 日

變更	描述	Date
WorkSpaces 安全瀏覽器已開始追蹤變更	WorkSpaces 安全瀏覽器開始追蹤其 AWS 受管政策的變更。	2021 年 11 月 30 日

對 Amazon WorkSpaces 安全瀏覽器身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 WorkSpaces 安全瀏覽器和 IAM 時可能遇到的常見問題。

主題

- 我無權在 WorkSpaces 安全瀏覽器中執行動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 AWS 帳戶外的人員存取我的 WorkSpaces 安全瀏覽器資源

我無權在 WorkSpaces 安全瀏覽器中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 workspaces-web:*GetWidget* 許可時發生。

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

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 workspaces-web:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 iam:PassRole動作，您的政策必須更新，以允許您將角色傳遞至 WorkSpaces 安全瀏覽器。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 的 IAM `marymajor` 使用者嘗試使用主控台在 WorkSpaces 安全瀏覽器中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

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

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 AWS 帳戶外的人員存取我的 WorkSpaces 安全瀏覽器資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 WorkSpaces 安全瀏覽器是否支援這些功能，請參閱 Amazon WorkSpaces 安全瀏覽器如何與 IAM 搭配使用。
- 若要了解如何提供您擁有 AWS 帳戶 的資源存取權，請參閱《IAM 使用者指南》中的在您 AWS 帳戶擁有的另一個 中為 IAM 使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

使用 Amazon WorkSpaces 安全瀏覽器的服務連結角色

Amazon WorkSpaces 安全瀏覽器使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 WorkSpaces 安全瀏覽器的唯一 IAM 角色類型。服務連結角色由 WorkSpaces 安全瀏覽器預先定義，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 WorkSpaces 安全瀏覽器，因為您不必手動新增必要的許可。WorkSpaces 安全瀏覽器會定義其服務連結角色的許可，除非另有定義，否則只有 WorkSpaces

安全瀏覽器才能擔任其角色。已定義的許可包括信任和許可政策。許可政策無法附加到其他任何 IAM 實體。

您必須先刪除角色的相關資源，才能刪除服務連結角色。這可保護您的 WorkSpaces 安全瀏覽器資源，因為您不會不小心移除存取資源的許可。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

主題

- WorkSpaces 安全瀏覽器的服務連結角色許可
- 為 WorkSpaces 安全瀏覽器建立服務連結角色
- 編輯 WorkSpaces 安全瀏覽器的服務連結角色
- 刪除 WorkSpaces 安全瀏覽器的服務連結角色
- WorkSpaces 安全瀏覽器服務連結角色支援的區域

WorkSpaces 安全瀏覽器的服務連結角色許可

WorkSpaces 安全瀏覽器使用名為 的服務連結角色 AWSServiceRoleForAmazonWorkSpacesWeb – WorkSpaces 安全瀏覽器使用此服務連結角色來存取客戶帳戶的 Amazon EC2 資源，以進行串流執行個體和 CloudWatch 指標。

AWSServiceRoleForAmazonWorkSpacesWeb 服務連結角色信任下列服務以擔任角色：

- workspaces-web.amazonaws.com

名為 的角色許可政策AmazonWorkSpacesWebServiceRolePolicy允許 WorkSpaces 安全瀏覽器對指定的資源完成下列動作。如需詳細資訊，請參閱the section called “AmazonWorkSpacesWebServiceRolePolicy”。

- 動作：all AWS resources 上的 ec2:DescribeVpcs
- 動作：all AWS resources 上的 ec2:DescribeSubnets
- 動作：all AWS resources 上的 ec2:DescribeAvailabilityZones
- 動作：在子網路和安全群組資源上具有 aws:RequestTag/WorkSpacesWebManaged: true 的 ec2:CreateNetworkInterface

- 動作：all AWS resources 上的 ec2:DescribeNetworkInterfaces
- 動作：在網路介面上具有 aws:ResourceTag/WorkSpacesWebManaged: true 的 ec2:DeleteNetworkInterface
- 動作：all AWS resources 上的 ec2:DescribeSubnets
- 動作：all AWS resources 上的 ec2:AssociateAddress
- 動作：all AWS resources 上的 ec2:DisassociateAddress
- 動作：all AWS resources 上的 ec2:DescribeRouteTables
- 動作：all AWS resources 上的 ec2:DescribeSecurityGroups
- 動作：all AWS resources 上的 ec2:DescribeVpcEndpoints
- 動作：ec2:CreateNetworkInterface 上的 ec2:CreateTags 使用 aws:TagKeys: ["WorkSpacesWebManaged"] 進行操作
- 動作：all AWS resources 上的 cloudwatch:PutMetricData
- 動作：在名稱開頭為 amazon-workspaces-web- 之 Kinesis 資料串流上的 kinesis:PutRecord
- 動作：在名稱開頭為 amazon-workspaces-web- 之 Kinesis 資料串流上的 kinesis:PutRecords
- 動作：在名稱開頭為 amazon-workspaces-web- 之 Kinesis 資料串流上的 kinesis:DescribeStreamSummary

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

為 WorkSpaces 安全瀏覽器建立服務連結角色

您不需要手動建立服務連結角色，當您在 AWS 管理主控台、 AWS CLI或 AWS API 中建立第一個入口網站時，WorkSpaces 安全瀏覽器會為您建立服務連結角色。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立第一個入口網站時，WorkSpaces 安全瀏覽器會再次為您建立服務連結角色。

您也可以使用 IAM 主控台，透過 WorkSpaces 安全瀏覽器使用案例建立服務連結角色。在 AWS CLI 或 AWS API 中，使用服務名稱建立`workspaces-web.amazonaws.com`服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立服務連結角色。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

編輯 WorkSpaces 安全瀏覽器的服務連結角色

WorkSpaces 安全瀏覽器不允許您編輯`AWSServiceRoleForAmazonWorkSpacesWeb`服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 WorkSpaces 安全瀏覽器的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 如果您嘗試刪除資源時WorkSpaces 安全瀏覽器服務正在使用 角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除 WorkSpaces 所使用的 WorkSpaces 安全瀏覽器資源 AWSServiceRoleForAmazonWorkSpacesWeb

- 選擇下列任一選項：
  - 如果您使用主控台，請刪除主控台上的所有入口網站。
  - 如果您使用 CLI 或 API，請取消所有資源 (包括瀏覽器設定、網路設定、使用者設定、信任存放區和使用者存取日誌記錄設定) 與入口網站的關聯，刪除這些資源，然後刪除入口網站。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除 AWSServiceRoleForAmazonWorkSpacesWeb 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

WorkSpaces 安全瀏覽器服務連結角色支援的區域

WorkSpaces 安全瀏覽器支援在提供服務的所有區域中使用服務連結角色。如需詳細資訊，請參閱 AWS 區域與端點。

Amazon WorkSpaces 安全瀏覽器中的事件回應

您可以監控 SessionFailure Amazon CloudWatch 指標以偵測事件。請使用 SessionFailure 指標的 CloudWatch 警示，以接收事件警示。如需詳細資訊，請參閱使用 Amazon CloudWatch 監控 Amazon WorkSpaces 安全瀏覽器 Amazon CloudWatch。

Amazon WorkSpaces 安全瀏覽器的合規驗證

若要了解 是否 AWS 服務 在特定合規計劃範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱AWS 合規計劃。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 AWS 安全文件。

Amazon WorkSpaces 安全瀏覽器中的彈性

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體隔離和隔離的可用區域，這些區域與低延遲、高輸送量和高度備援聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和 可用區域的詳細資訊，請參閱AWS 全球基礎設施。

WorkSpaces 安全瀏覽器目前不支援下列項目：

- 跨可用區域或區域備份內容
- 加密備份
- 加密可用區域或區域之間的傳輸中內容
- 預設或自動備份

若要設定高網際網路可用性，您可以調整 VPC 組態。您可以請求適量的 TPS，以獲得高 API 可用性。

Amazon WorkSpaces 安全瀏覽器中的基礎設施安全

Amazon WorkSpaces 安全瀏覽器是受管服務，受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 Amazon WorkSpaces 安全瀏覽器。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

WorkSpaces 安全瀏覽器會將 Standard AWS SigV4 身分驗證和授權套用至所有 服務，以隔離服務流量。由您的身分提供者保護客戶資源端點 (或 Web 入口網站端點)。您可以使用身分提供者 (IdP) 中的多重要素授權和其他安全機制，進一步隔離流量。

您可以透過設定 VPC、子網路或安全群組等網路設定值，以控制所有網際網路存取。目前不支援多租戶及 VPC 端點 (PrivateLink)。

Amazon WorkSpaces 安全瀏覽器中的組態和漏洞分析

WorkSpaces 安全瀏覽器會視需要更新和修補應用程式和平台，包括 Chrome 和 Linux。您無需進行修補或重建。不過，您有責任根據規格和指導方針設定 WorkSpaces Secure Browser，並監控使用者對 WorkSpaces Secure Browser 的使用。所有服務相關的組態和漏洞分析都是 WorkSpaces Secure Browser 的責任。

您可以請求提高 WorkSpaces Secure Browser 資源的限制，例如 Web 入口網站數量和使用者數量。WorkSpaces 安全瀏覽器可確保服務和 SLA 的可用性。

使用界面 VPC 端點存取 APIs (AWS PrivateLink)

您可以從私有雲端 (VPC) 直接呼叫 Amazon WorkSpaces 安全瀏覽器 API 端點，而不是透過網際網路連線。您可以在不使用網際網路閘道、NAT 裝置、VPN 連線或 Direct Connect 連線的情況下執行此操作。

您可以透過建立採用 技術的介面 VPC 端點來建立此私有連線AWS PrivateLink。針對您從 VPC 指定的每個子網路，我們會在子網路中建立端點網路介面。端點網路介面是請求者管理的網路介面，可做為 Amazon WorkSpaces 安全瀏覽器 API 流量的進入點。

如需詳細資訊，請參閱透過 存取 AWS 服務 AWS PrivateLink。

主題

Amazon WorkSpaces 安全瀏覽器的考量事項

在您設定 Amazon WorkSpaces 安全瀏覽器 APIs的介面 VPC 端點之前，請務必檢閱 Access AWS 服務 AWS PrivateLink中的「先決條件」。Amazon WorkSpaces 安全瀏覽器支援透過介面 VPC 端點呼叫其所有 API 動作。

根據預設，允許透過端點完整存取 Amazon WorkSpaces 安全瀏覽器。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用 VPC 端點控制對服務的存取。

為 Amazon WorkSpaces 安全瀏覽器建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 () 為 Amazon WorkSpaces 安全瀏覽器服務建立介面 VPC 端點 AWS CLI。 AWS Command Line Interface 如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的建立介面端點。

使用下列服務名稱建立 Amazon WorkSpaces 安全瀏覽器的介面 VPC 端點：

- com.amazonaws.*region*.workspaces-web

對於支援 FIPS 的區域，請使用下列服務名稱為 Amazon WorkSpaces 安全瀏覽器建立介面 VPC 端點：

- com.amazonaws.*region*.workspaces-web-fips

為您的介面 VPC 端點建立端點政策

端點政策是您可以連接到介面 VPC 端點的 IAM 資源。預設端點政策可讓您透過介面 VPC 端點完整存取 Amazon WorkSpaces 安全瀏覽器 APIs。若要控制從您的 VPC 授予 Amazon WorkSpaces 安全瀏覽器的存取權，請將自訂端點政策連接至介面 VPC 端點。

端點政策會指定以下資訊：

- 可執行動作 (AWS 帳戶、IAM 使用者和 IAM 角色) 的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的使用 VPC 端點控制對服務的存取。

範例：Amazon WorkSpaces 安全瀏覽器動作的 VPC 端點政策

以下是自訂端點政策的範例。當您將此政策連接到介面 VPC 端點時，它會授予所有資源上所有主體的所列 Amazon WorkSpaces 安全瀏覽器動作的存取權。

```
{
     "Statement": [
         {
             "Action": "workspaces-web:*",
             "Effect": "Allow",
             "Resource": "*",
             "Principal": "*"
         }
     ]
}
```

疑難排解

如果您對 Amazon WorkSpaces 安全瀏覽器 APIs呼叫正在暫停，則 VPC Endpoint Service 安全群組或 IAM 角色設定中可能會有設定錯誤的情況。若要解決此問題，請嘗試下列動作：

- 建立介面 VPC 端點時，它可能已自動連接到 AWS 帳戶您預設的安全群組。嘗試使用不同的安全群組，並確保傳入和傳出許可允許您適當地傳輸資料。
- 請確定您使用的 IAM 角色可讓您呼叫 Amazon WorkSpaces 安全瀏覽器 APIs。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的什麼是 AWS PrivateLink？。

Amazon WorkSpaces 安全瀏覽器的安全最佳實務

Amazon WorkSpaces Secure Browser 提供多種安全功能，供您在開發和實作自己的安全政策時使用。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

Amazon WorkSpaces 安全瀏覽器的最佳實務包括下列項目：

- 若要偵測與您使用 WorkSpaces Secure Browser 相關聯的潛在安全事件，請使用 AWS CloudTrail 或 Amazon CloudWatch 來偵測和追蹤存取歷史記錄和程序日誌。如需詳細資訊，請參閱 使用 Amazon CloudWatch 監控 Amazon WorkSpaces 安全瀏覽器 Amazon CloudWatch 和 使用 記錄 WorkSpaces 安全瀏覽器 API 呼叫 AWS CloudTrail。
- 若要執行偵測控制項與識別異常情況，請使用 CloudTrail 日誌和 CloudWatch 指標。如需詳細資訊，請參閱 使用 Amazon CloudWatch 監控 Amazon WorkSpaces 安全瀏覽器 Amazon CloudWatch 和 使用 記錄 WorkSpaces 安全瀏覽器 API 呼叫 AWS CloudTrail。
- 您可以設定使用者存取日誌記錄來記錄使用者事件。如需詳細資訊，請參閱the section called “設定使用者活動記錄”。

若要防止與您使用 WorkSpaces Secure Browser 相關聯的潛在安全事件，請遵循下列最佳實務：

- 實作最低權限存取，並建立要用於 WorkSpaces Secure Browser 動作的特定角色。使用 IAM 範本建立完整存取或唯讀角色。如需詳細資訊，請參閱AWS WorkSpaces 安全瀏覽器的 受管政策。
- 請謹慎共享入口網域和使用者憑證。網際網路上的任何人都能存取 Web 入口網站，但除非擁有入口網站的有效使用者憑證，否則他們無法啟動工作階段。請注意您如何、何時以及與誰共用 Web 入口網站憑證。

監控 Amazon WorkSpaces 安全瀏覽器

監控是維護 Amazon WorkSpaces 安全瀏覽器和其他 AWS 解決方案可靠性、可用性和效能的重要部分。 AWS 提供下列監控工具來監看 WorkSpaces 安全瀏覽器入口網站及其資源、在發生錯誤時回報，並在適當時自動採取動作：

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。您可以收集和追蹤指標、建立自訂儀表板，以及設定警示，在您指定的指標達到您指定的閾值時通知您或採取動作。例如，您可以讓 CloudWatch 追蹤 CPU 使用量或其他 Amazon EC2 執行個體指標，在需要時自動啟動新的執行個體。如需更多資訊，請參閱 Amazon CloudWatch 使用者指南。
- Amazon CloudWatch Logs 可讓您監控、存放和存取來自 Amazon EC2 執行個體、CloudTrail 及其他來源的日誌檔案。CloudWatch Logs 可監控日誌檔案中的資訊，並在達到特定閾值時通知您。您也可以將日誌資料存檔在高耐用性的儲存空間。如需詳細資訊，請參閱 Amazon CloudWatch Logs 使用者指南。
- AWS CloudTrail 會擷取由您的帳戶或代表 AWS 您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」。

主題

使用 Amazon CloudWatch 監控 Amazon WorkSpaces 安全瀏覽器 Amazon CloudWatch

您可以使用 CloudWatch 監控 Amazon WorkSpaces 安全瀏覽器，該瀏覽器會收集原始資料並將其處理為可讀且幾近即時的指標。這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚 Web 應用程式或服務的執行效能。您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

AWS/WorkSpacesWeb 命名空間包含下列指標。

Amazon WorkSpaces 安全瀏覽器的 CloudWatch 指標

指標	描述	維度	統計資料	單位
SessionAttempt	Amazon WorkSpaces 安全瀏覽器工作階段嘗試次數。	[PortalId]	平均數、總和、上限、下限	計數
SessionSuccess	成功啟動 Amazon WorkSpaces 安全瀏覽器工作階段的數量。	[PortalId]	平均數、總和、上限、下限	計數
SessionFailure	失敗的 Amazon WorkSpaces 安全瀏覽器工作階段數目開始。	[PortalId]	平均數、總和、上限、下限	計數
SessionIdleDisconnect	由於使用者閒置而關閉的連線數。	[PortalId]	平均數	計數
ActiveSession	入口網站上的作用中工作階段數目。	[PortalId]	平均數	計數
GlobalCpuPercent	Amazon WorkSpaces 安全瀏覽器工作階段執行個體的 CPU 用量。	[PortalId] [PortalId, UserName]	平均數、總和、上限、下限	百分比
GlobalMemoryPercent	Amazon WorkSpaces 安全瀏覽器工作階段執行個體的記	[PortalId] [PortalId, UserName]	平均數、總和、上限、下限	百分比

指標	描述	維度	統計資料	單位
	憶體 (RAM) 用量。			
DisplayLatency	影格擷取和呈現之間的平均時間，以毫秒為單位。	[PortalId] [PortalId, UserName]	平均值、最大值、最小值	毫秒
InputLatency	用戶端和伺服器之間的輸入延遲。例如，用戶端滑鼠點選和伺服器滑鼠點選之間的延遲。	[PortalId] [PortalId, UserName]	平均值、最大值、最小值	毫秒
SessionLoggerEventDelivered	每個交付的工作階段記錄器檔案擁有的事件數量。	[PortalId]	平均數、總和、上限、下限	計數
SessionLoggerTargetNotFoundError	找不到導致儲存貯體的日誌檔案交付數量。	[PortalId]	平均數、總和、上限、下限	計數
SessionLoggerAccessDeniedError	導致許可遭拒的日誌檔案交付數量。	[PortalId]	平均數、總和、上限、下限	計數

> **Note**
>
> 每個工作階段每分鐘收集一次指標資料點，每 5 分鐘發佈一次到 CloudWatch。工作階段記錄器指標會針對每個日誌檔案交付立即發出。

Amazon WorkSpaces 安全瀏覽器指標的維度

維度	描述
PortalId	篩選指定入口網站的 Amazon WorkSpaces 安全瀏覽器指標資料。
UserName	篩選指定入口網站和使用者的 Amazon WorkSpaces 安全瀏覽器指標資料。

您可以使用 SessionLoggerEventDelivered 指標來監控入口網站中的事件彙總數量，或是透過計算資料點數而非加總值來查看已交付的日誌檔案數量。我們建議在 SessionLoggerTargetNotFoundError 和 SessionLoggerAccessDeniedError 指標上設定警示，以偵測意外的資源或許可刪除。

使用 記錄 WorkSpaces 安全瀏覽器 API 呼叫 AWS CloudTrail

WorkSpaces Secure Browser 已與 整合 AWS CloudTrail，此服務提供 Amazon WorkSpaces Secure Browser AWS 中使用者、角色或服務所採取動作的記錄。CloudTrail 會將 Amazon WorkSpaces Secure Browser 的所有 API 呼叫擷取為事件。這包括從 Amazon WorkSpaces Secure Browser 主控台呼叫，以及對 Amazon WorkSpaces Secure Browser API 操作的程式碼呼叫。如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Amazon WorkSpaces Secure Browser 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以識別對 Amazon WorkSpaces Secure Browser 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

主題

- CloudTrail 中的 WorkSpaces 安全瀏覽器資訊
- 了解 WorkSpaces 安全瀏覽器日誌檔案項目

CloudTrail 中的 WorkSpaces 安全瀏覽器資訊

建立 AWS 帳戶時，會在您的帳戶上啟用 CloudTrail。當活動在 Amazon WorkSpaces 安全瀏覽器中發生時，該活動會記錄於 CloudTrail 事件，以及事件歷史記錄中的其他服務 AWS 事件。在事件歷史記錄中，您可以檢視、搜尋和下載 AWS 帳戶中的最新事件。如需詳細資訊，請參閱「使用 CloudTrail 事件歷史記錄檢視事件」。

若要持續記錄您 AWS 帳戶中的事件，包括 Amazon WorkSpaces Secure Browser 的事件，您可以建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS區域。追蹤會記錄 AWS 分割區中所有 區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

所有 Amazon WorkSpaces 安全瀏覽器動作都會由 CloudTrail 記錄，並記錄在 Amazon WorkSpaces API 參考中。例如，對 `CreatePortal`、`DeleteUserSettings` 和 `ListBrowserSettings` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用根或 IAM 使用者憑證提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解 WorkSpaces 安全瀏覽器日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。事件即為來自任何來源的單一請求，其中包含請求動作、動作日期和時間，以及請求參數和其他細節的相關資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例顯示的是展示 `ListBrowserSettings` 動作的 CloudTrail 日誌項目。

```
{
   "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"
    }]
}
```

Amazon WorkSpaces 安全瀏覽器中的使用者活動記錄

Amazon WorkSpaces 安全瀏覽器可讓客戶在安全瀏覽器工作階段中記錄與使用者活動相關的工作階段事件。

WorkSpaces 安全瀏覽器提供兩種記錄使用者活動和安全相關事件的選項：

- 工作階段記錄器會擷取各種工作階段事件。這些日誌會傳送到您帳戶中的 Amazon S3 儲存貯體，以便與您偏好的 SIEM 平台輕鬆整合。
- 使用者存取記錄會擷取最重要的工作階段事件。這些日誌會串流到 Amazon Kinesis 串流，以進行即時處理和分析。

如需如何設定這些選項的詳細資訊，請參閱 the section called “設定工作階段記錄器”和 the section called “設定使用者存取記錄”。

主題

- Amazon WorkSpaces 安全瀏覽器的工作階段記錄器中的工作階段事件
- Amazon WorkSpaces 安全瀏覽器的使用者存取日誌中的工作階段事件

Amazon WorkSpaces 安全瀏覽器的工作階段記錄器中的工作階段事件

工作階段記錄器會擷取各種工作階段相關事件，以用於監控和稽核。

您可以設定工作階段記錄器，根據 WorkSpaces 安全瀏覽器入口網站的需求收集所有工作階段事件或選取的子集。如需組態的詳細資訊，請參閱 the section called “設定工作階段記錄器”。

為了維護使用者隱私權，工作階段記錄器不會記錄敏感內容，例如剪貼簿資料，或上傳或下載檔案的內容。

下列欄位包含在所有事件中：

- Time (時間)
- 使用者名稱
- 入口網站 ID
- 入口網站 IP
- 用戶端 IP
- 工作階段 ID

名稱	描述	事件中包含的其他欄位
SessionStart	已啟動安全瀏覽器工作階段，但使用者尚未連線。	
SessionConnect	使用者已連線至安全瀏覽器工作階段。	
TabOpen	在其安全瀏覽器工作階段中，使用者開啟了新標籤，或在新標籤中開啟了連結。	主機名稱、路徑、URL（如果使用者在新標籤中開啟連結）、無（如果使用者開啟新標籤）
UrlVisit	在瀏覽器工作階段中，使用者導覽至 URL。	主機名稱、路徑、URL
WebsiteInteract	使用者變更了網站上的標準 HTML 元素（例如，按一下核取方塊、選項按鈕或按鈕，或在下拉式清單中選取項目）。	主機名稱、路徑、URL
TabClose	在瀏覽器工作階段中，使用者已關閉索引標籤。	主機名稱、路徑、URL（如果使用者關閉導覽至的索引標

名稱	描述	事件中包含的其他欄位
		籤）、無（如果使用者關閉新索引標籤）
ContentTransferFromLocalToRemoteClipboard	使用者使用來自其本機瀏覽器（安全環境之外）的內容，在安全瀏覽器中更新剪貼簿。透過工作階段中工具列複製內容，或透過鍵盤快速鍵 (Ctrl+C/Ctrl+V) 傳輸資料，即可進行此更新。	
ContentCopyFromWebsite	使用者使用來自安全瀏覽器（在安全環境中）的內容，在安全瀏覽器中更新剪貼簿。	主機名稱、路徑、URL
ContentPasteToWebsite	剪貼簿內容已貼入瀏覽器中的網頁。（此事件不會擷取剪貼簿內容貼入瀏覽器 URL 列的執行個體。）	主機名稱、路徑、URL
PrintJobSubmit	使用者將請求任務提交至瀏覽器的虛擬印表機（「DCV 印表機」）。內容會在使用者的本機電腦上儲存為 PDF。	檔案名稱、大小、副檔名
FileDownloadFromSecureBrowserToRemoteDisk	檔案已從工作階段儲存至遠端執行個體的本機磁碟。	主機名稱、路徑、URLfilename、大小、延伸
FileTransferFromRemoteToLocalDisk	檔案已從遠端執行個體的磁碟下載到使用者的本機裝置。	檔案名稱、大小、副檔名
FileUploadFromRemoteDiskToSecureBrowser	存放在遠端執行個體本機磁碟上的檔案已透過瀏覽器工作階段上傳至檔案共用 SaaS 平台（例如 Google Drive、Box 或 File.io)。	

名稱	描述	事件中包含的其他欄位
FileTransferFromLocalToRemoteDisk	檔案已從使用者裝置上傳到安全瀏覽器工作階段。	檔案名稱、大小和副檔名
SessionDisconnection	使用者與安全瀏覽器工作階段中斷連線。	
SessionEnd	安全瀏覽器工作階段已終止。終止可以透過以下三種方式之一發生：管理員透過主控台中的使用者工作階段管理員結束工作階段、使用者使用工具列中的結束工作階段手動結束工作階段，或在超過管理員設定的持續時間之後工作階段逾時。	

每個事件都遵循 OCSF 標準，並包含所有事件通用的屬性清單：

```
{
    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
    }
}
```

以下是 URLVisit 事件的範例：

```
{
    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
    }
}
```

以下是 PrintJobSubmit 事件的範例：

```
{
    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
    }
}
```

Amazon WorkSpaces 安全瀏覽器的工作階段記錄器指標

Session Logger 會發出下列 Amazon CloudWatch 指標。

您可以使用 SessionLoggerEventDelivered 指標來監控入口網站的事件彙總數量，或是透過計算資料點的數量來查看已交付的日誌檔案數量，而不是加總值。我們建議在 SessionLoggerTargetNotFoundError 和 SessionLoggerAccessDeniedError 指標上設定警示，以偵測意外的資源或許可刪除。

> **Note**
>
> 每個工作階段每分鐘收集一次指標資料點，每 5 分鐘發佈 Amazon CloudWatch 一次。工作階段記錄器指標會針對每個日誌檔案交付立即發出。

工作階段記錄器指標

指標	描述	維度	統計資料	單位
SessionLoggerEventDelivered	每個交付的工作階段記錄器檔案擁有的事件數量。	【PortalId】	平均數、總和、上限、下限	計數
SessionLoggerTargetNotFoundError	找不到導致儲存貯體的日誌檔案交付數量。	【PortalId】	平均數、總和、上限、下限	計數
SessionLoggerAccessDeniedError	導致許可遭拒的日誌檔案交付數量。	【PortalId】	平均數、總和、上限、下限	計數

Amazon WorkSpaces 安全瀏覽器的使用者存取日誌中的工作階段事件

下列工作階段事件可用於使用者許可記錄：

- 驗證：事件已成功放入 Kinesis 資料串流。
- StartSession：使用者已啟動工作階段，並連線至安全瀏覽器工作階段。

- VisitPage：使用者正在瀏覽工作階段中的頁面。
- EndSession：使用者已終止工作階段。

從瀏覽器歷程記錄記錄 URL 導航日誌。未在瀏覽器歷史記錄中記錄URLs（以無痕模式造訪或從瀏覽器歷史記錄中刪除）不會記錄在日誌中。客戶可自行決定是否要使用瀏覽器政策關閉不熟悉模式或刪除歷史記錄。

以下是每個可用事件的範例。每個事件都一定有以下欄位：

- timestamp，包含為 epoch 時間 (以毫秒為單位)。
- eventType，為字串。
- details，為另一個 json 物件。
- 除 Validation 外，每個事件都有 portalArn 和 userName。

```
{
  "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"
}
```

Amazon WorkSpaces 安全瀏覽器使用者指南

管理員使用 WorkSpaces 安全瀏覽器來建立連線至公司網站的 Web 入口網站，例如內部網站、software-as-a-service(SAAS) Web 應用程式或網際網路。終端使用者會使用其現有的網頁瀏覽器存取這些入口網站，以啟動工作階段和存取內容。

下列內容有助於引導想要進一步了解如何存取 WorkSpaces 安全瀏覽器、啟動和設定工作階段，以及使用工具列和 Web 瀏覽器的最終使用者。

主題

Amazon WorkSpaces 安全瀏覽器的瀏覽器和裝置相容性

Amazon WorkSpaces 安全瀏覽器由在 Web 瀏覽器中執行的 Amazon DCV Web 瀏覽器用戶端提供支援，因此不需要安裝。網頁瀏覽器用戶端受到 Chrome 和 Firefox 等常見的網頁瀏覽器，以及 Windows、macOS 和 Linux 等主要桌面作業系統的支援。

如需網頁瀏覽器用戶端支援情況的最新詳細資訊，請參閱網頁瀏覽器用戶端。

> **Note**
>
> 目前僅 Google Chrome 和 Microsoft Edge 等採用 Chromium 架構的瀏覽器有支援網路攝影機。Apple Safari 和 Mozilla FireFox 現不支援網路攝影機。

Amazon WorkSpaces 安全瀏覽器的 Web 入口網站存取

您的管理員可以透過下列選項提供您存取 Web 入口網站的權限：

- 您可以從電子郵件或網站選取連結，然後使用您的 SAML 身分憑證登入。

- 您可以登入 SAML 身分提供者 (例如，Okta、Ping 或 Azure)，並且從 SAML 提供者的應用程式首頁 (例如 Okta 終端使用者儀表板或 Azure Myapps 入口網站) 按一下啟動工作階段。

Amazon WorkSpaces 安全瀏覽器的工作階段指導

登入 Web 入口網站之後，您可以啟動工作階段並且在工作階段期間執行各種動作。

主題

在 Amazon WorkSpaces 安全瀏覽器中啟動工作階段

登入以啟動工作階段後，您會看到啟動工作階段的訊息和進度列。這表示 Amazon WorkSpaces 安全瀏覽器正在為您建立工作階段。在幕後，Amazon WorkSpaces 安全瀏覽器正在建立執行個體、啟動受管 Web 瀏覽器，以及套用管理員設定和瀏覽器政策。

如果這是您第一次登入 Web 入口網站，您會在工具列中看到藍色的 + 圖示。此圖示表示有提供教學課程，它將帶領說明工具列裡可使用的功能。您可以使用這些圖示以瞭解如何：

- 選取本機端瀏覽器旁邊的鎖定圖示，並將剪貼簿、麥克風和攝影機旁邊的開關切換為開啟，以授予瀏覽器使用麥克風、網路攝影機和剪貼簿的權限。

> **Note**
>
> 當您在第一個工作階段開始時啟用網路攝影機權限，會短暫啟用網路攝影機，且電腦上的指示燈會閃爍。這將使得本機端瀏覽器可以使用網路攝影機。

- 啟用 Amazon WorkSpaces 安全瀏覽器以啟動其他監控視窗，方法是選取瀏覽器中的鎖定圖示，並將 設定為一律允許快顯視窗。

如果您想要重新啟動教學課程，可以從工具列、說明和啟動教學課程中選擇設定檔。

使用 Amazon WorkSpaces 安全瀏覽器中的工具列

若要了解如何使用工具列，請遵循下列步驟。

若要移動工具列，請選取工具列頂部的淺色條，將其拖曳至您想要的位置，然後放開它以放下。

若要收合工具列，請將滑鼠游標暫留在工具列上，然後選取向上箭頭按鈕，或按兩下頂端區段中的淺色列。收合檢視畫面提供更多螢幕空間，按一下即可存取最常用的圖示。

若要增加顯示的大小，請選取瀏覽器視窗並放大。若要增加工具列圖示和文字的顯示大小，請選取工具列並放大。

若要在 Windows 裝置上放大或縮小，請遵循下列步驟：

1. 選取工具列或 Web 內容。
2. 按 Ctrl + + 以放大，或按 Ctrl + - 以縮小。

若要在 Mac 裝置上放大或縮小，請遵循下列步驟：

1. 選取工具列或 Web 內容。
2. 按 Cmd + + 以放大，或按 Cmd + - 以縮小。

若要將工具列停駐至畫面頂端，請在工具列模式下選擇偏好設定、一般和停駐。

下表說明工具列中的所有可用圖示：

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**
>
> 除非您的管理員授與這些權限，否則預設隱藏 Clipboard 剪貼簿和 Files 檔案圖示。只有管理員可以啟用或停用 Web 入口網站上的剪貼簿和檔案功能。如果已經隱藏這些圖示，而您需要存取這些圖示，請聯絡您的管理員。

在 Amazon WorkSpaces 安全瀏覽器中使用瀏覽器

當您啟動工作階段時，瀏覽器會顯示啟動 URL，這是您的管理員所選擇的 URL。如果管理員尚未選擇啟動 URL，您將看到 Google Chrome 瀏覽器中的預設新分頁體驗。

您可以在瀏覽器中開啟分頁、啟動其他瀏覽器視窗 (從 Windows 工具列圖示或瀏覽器的三點功能表)、在 URL 列中輸入 URL 或搜尋 URL，或從受管理的書籤開啟網站。若要存取 Web 入口網站的書籤，請開啟書籤列上的受管理的書籤資料夾 (位於 URL 列下方)，或是從 URL 列右側的三點功能表開啟書籤管理員。

若要調整瀏覽器視窗大小或移動瀏覽器視窗，請向下拖曳 Chrome 分頁列。這樣可以在工作階段期間有更多螢幕空間顯示多個瀏覽器視窗。

> **Note**
>
> 如果您的管理員已經關閉無痕模式等瀏覽器的功能，您的工作階段期間可能無法使用這些功能。

在 Amazon WorkSpaces 安全瀏覽器中結束工作階段

若要結束工作階段，請選擇設定檔和結束工作階段。工作階段結束後，Amazon WorkSpaces 安全瀏覽器會從工作階段中刪除所有資料。工作階段結束後，將無法使用任何瀏覽器資料，例如開啟的網站或歷程記錄，或是檔案總管裡的檔案或資料。

如果您在使用中的工作階段期間關閉分頁，會在管理員設定的一段時間後結束工作階段。如果您在此逾時生效之前關閉分頁且重新造訪 Web 入口網站，您可以加入目前的工作階段及查看所有先前的工作階段資料，例如開啟的網站和檔案。

對 Amazon WorkSpaces 安全瀏覽器中的使用者問題進行故障診斷

如果您在使用 WorkSpaces 安全瀏覽器時遇到以下任何問題，請嘗試以下解決方案。

我的 Amazon WorkSpaces 安全瀏覽器入口網站不會讓我登入。我收到錯誤訊息，指出「尚未設定您的 Web 入口網站。如需進一步協助，請聯絡您的管理員。」

您的管理員必須使用 SAML 2.0 身分提供者來完成建立入口網站，才能讓您登入。如需進一步協助，請聯絡您的管理員。

我的入口網站不會啟動工作階段。我收到錯誤訊息，指出「無法保留工作階段。發生內部錯誤。請再試一次。」

您的 Web 入口網站在啟動工作階段時發生問題。請嘗試再次啟動工作階段。如果繼續發生這個情況，請聯絡您的管理員以尋求協助。

我無法使用剪貼簿、麥克風或網路攝影機。

請選取 URL 旁的鎖定圖示，然後切換剪貼簿、麥克風、攝影機和快顯視窗旁的藍色開關，然後重新導向來開啟這些功能，以允許瀏覽器可以使用這些功能。

> **Note**
>
> 如果您的網頁瀏覽器不支援輸入視訊或音訊，在工具列上將不會出現這些選項。

Amazon WorkSpaces 安全瀏覽器即時音訊視訊 (AV) 會將本機網路攝影機視訊和麥克風音訊輸入重新導向至瀏覽器串流工作階段。如此一來，您便能在使用 Google Chrome 或 Microsoft Edge 等 Chromium 架構網頁瀏覽器進行串流工作階段時，透過本機端裝置進行視訊和音訊會議。非 Chromium 架構的瀏覽器目前不支援網路攝影機。

如需如何設定 Google Chrome 瀏覽器的詳細資訊，請參閱使用攝影機和麥克風。

我的 Web 入口網站不會啟動額外的監視器。

如果您嘗試啟動雙監視器，並在頂端瀏覽器的網址列末端看到彈出視窗已封鎖圖示，請選取永遠允許彈出視窗和重新導向旁邊的圖示和圓形按鈕。在允許彈出視窗的情況下，選擇工具欄上的雙監視器圖示以啟動新視窗，重新定位監視器上的視窗，然後將瀏覽器分頁拖到視窗中。

我試著從檔案窗格下載檔案時，沒有任何反應。

如果您嘗試從檔案窗格下載檔案，並在頂端瀏覽器的網址列末端看到彈出視窗已封鎖圖示，請選取永遠允許彈出視窗和重新導向旁邊的圖示和圓形按鈕。在允許彈出視窗的情況下，請嘗試再次下載檔案。

如何得知正在使用哪個麥克風和/或網路攝影機，以及如何變更？

按一下麥克風或攝影機旁的向下箭頭圖示。選單會顯示可用的裝置，並帶有一個核取記號，指出您目前的裝置。選取不同的裝置，以變更您要用於工作階段的裝置。

直接從公司的自訂網域存取時，我的 Web 入口網站不會啟動

如果您嘗試使用像是 的非 workspaces-web.com 網域名稱來啟動工作階段`acme.secureportal.mycompany.com`，請確定您的瀏覽器已為您存取的公司網域啟用第三方 Cookie。

Amazon WorkSpaces 安全瀏覽器的單一登入延伸模組

Amazon WorkSpaces 安全瀏覽器提供在桌上型電腦上使用 Chrome 和 Firefox 瀏覽器的單一登入擴充功能。如果您的管理員有啟用擴充功能，Web 入口網站會在您登入時要求您安裝擴充功能。

Amazon WorkSpaces 安全瀏覽器建置 擴充功能，以在工作階段期間啟用網站單一登入。例如，如果您使用 Okta 或 Ping 等 SAML 2.0 身分提供者登入 Web 入口網站，並且您在工作階段期間使用相同的身分提供者造訪網站，則該擴充功能可移除其他登入提示讓您更輕鬆地存取網站。

您無需安裝擴展程序即可存取 Web 入口網站，但它可以減少要求您輸入使用者名稱和密碼的次數，讓您有更好的使用體驗。

當您登入時，擴充功能會尋找您的管理員為您的工作階段列出的 cookie。擴充功能找到的所有資料都會在靜態和傳輸期間進行加密。這些資料都不會存在您的本機端瀏覽器中。當您結束工作階段時，會刪除所有工作階段資料 (例如，開啟的分頁、下載的檔案，以及在工作階段期間傳送或建立的 cookie)。

主題

Amazon WorkSpaces 安全瀏覽器的單一登入延伸模組相容性

單一登入延伸模組適用於下列裝置和瀏覽器：

- Devices
  - 筆記型電腦
  - 桌上型電腦
- 瀏覽器

- Google Chrome
- Mozilla Firefox

安裝 Amazon WorkSpaces 安全瀏覽器的單一登入擴充功能

若要安裝單一登入擴充功能，請遵循下列步驟。

當您登入入口網站時，請依照提示安裝 Chrome 或 Firefox 瀏覽器的擴充功能。您只需為每個網頁瀏覽器執行此操作一次。

如果您切換裝置、在同一部裝置上切換使用其他瀏覽器，或從本機端瀏覽器刪除擴充功能，則在您開始下一個工作階段時會看到安裝擴充功能的提示。

為了確保擴充功能如預期運作，請在正常瀏覽視窗中使用擴充功能，而不是 Incognito (Chrome) 或 Private Browsing (Firefox)。

Amazon WorkSpaces 安全瀏覽器的單一登入延伸模組故障診斷

使用單一登入擴充功能時，您可能會遇到下列問題。

如果您已安裝擴充功能，但仍要求您在工作階段期間登入，請依照下列步驟執行：

1. 請確定您的瀏覽器已安裝 Amazon WorkSpaces 安全瀏覽器延伸模組。如果您刪除了瀏覽器資料，則可能意外刪除了擴充功能。
2. 請確定您不是 Incognito (Chrome) 或 Private Browsing (Firefox)。這些模式可能會造成擴充功能發生問題。
3. 如果問題仍然存在，請聯絡入口網站管理員以取得其他協助。

Amazon WorkSpaces 安全瀏覽器管理指南的文件歷史記錄

下表說明 Amazon WorkSpaces 安全瀏覽器的文件版本。

變更	描述	日期
工作階段記錄器	設定工作階段記錄器以擷取各種工作階段事件。	2025 年 8 月 1 日
CloudWatch 指標	已更新 CloudWatch 指標。	2025 年 7 月 21 日
工具列控制項	使用工具列控制項，您可以為最終使用者工作階段設定工具列呈現。	2025 年 2 月 21 日
使用界面 VPC 端點存取 APIs (AWS PrivateLink)	從私有雲端 (VPC) 直接呼叫 Amazon WorkSpaces 安全瀏覽器 API 端點，而不是透過網際網路連線。	2025 年 1 月 10 日
資料保護設定	新增資料保護設定，以協助保護資料免於在工作階段期間共用。	2024 年 11 月 20 日
FIPS 端點	使用 FIPS 端點保護傳輸中的資料。	2024 年 10 月 7 日
工作階段管理儀表板	使用工作階段管理儀表板來監控和管理作用中和完整的工作階段。	2024 年 9 月 19 日
允許深層連結	允許入口網站接收深層連結，以在工作階段期間將使用者連線至特定網站。	2024 年 6 月 25 日
受管政策更新	新增 AmazonWorkSpacesSecureBrowserReadOnly 受管政策	2024 年 6 月 24 日

使用工具列縮放	您可以使用工具列來增加顯示、圖示和文字的大小。	2024 年 5 月 1 日
新的 Web 入口網站設定	您現在可以為您的 Web 入口網站指定執行個體類型和最大並行使用者限制。	2024 年 4 月 22 日
CloudWatch 指標	新增 GlobalCpuPercent 和 GlobalMemoryPercent 指標。	2024 年 2 月 26 日
設定 URL 篩選	您可以使用 Chrome 政策來篩選使用者可以從遠端瀏覽器存取URLs。	2024 年 2 月 21 日
IdP 身分驗證類型	您可以選擇標準或 IAM Identity Center 身分驗證類型。	2024 年 2 月 5 日
啟用單一登入的擴充功能	您可以為終端使用者啟用擴充功能，以獲得更好的入口網站登入體驗。	2023 年 8 月 28 日
Amazon WorkSpaces 安全瀏覽器的使用者指南	新增內容以協助引導想要進一步了解如何存取 Amazon WorkSpaces 安全瀏覽器、啟動和設定工作階段，以及使用工具列和 Web 瀏覽器的最終使用者。	2023 年 7 月 17 日
IP 存取控制	WorkSpaces 安全瀏覽器可讓您控制可從哪些 IP 地址存取 Web 入口網站。	2023 年 5 月 31 日
受管政策更新	更新 AmazonWorkSpacesWebReadOnly 受管政策	2023 年 5 月 15 日
設定身分提供者更新	WorkSpaces 安全瀏覽器提供兩種身分驗證類型：標準和 AWS IAM Identity Center	2023 年 3 月 15 日

瀏覽器政策更新	更新和重組的瀏覽器政策部分	2023 年 1 月 31 日
受管政策更新	更新 AmazonWorkSpacesWebServiceRolePolicy 受管政策	2022 年 12 月 15 日
允許清單和封鎖清單	指定允許清單和封鎖清單，以指定您的使用者可以存取或無法存取的網域清單。	2022 年 11 月 14 日
受管政策更新	更新 AmazonWorkSpacesWebReadOnly 受管政策	2022 年 11 月 2 日
受管政策更新	更新 AmazonWorkSpacesWebServiceRolePolicy 受管政策	2022 年 10 月 24 日
使用者存取日誌記錄	設定使用者存取日誌記錄以記錄使用者事件	2022 年 10 月 17 日
網路更新	「網路和存取」部分的各種更新	2022 年 9 月 22 日
受管政策更新	更新 AmazonWorkSpacesWebServiceRolePolicy 受管政策	2022 年 9 月 6 日
設定使用者工作階段	設定輸入法編輯器 (IME) 和工作階段內本地化	2022 年 7 月 28 日
網路更新	「網路和存取」部分的各種更新	2022 年 7 月 7 日
連線逾時值	指定中斷連線逾時 (以分鐘為單位) 和閒置中斷連線逾時 (以分鐘為單位)	2022 年 5 月 16 日
已更新受管政策	更新 AmazonWorkSpacesWebServiceRolePolicy 受管政策，以新增 AWS/Usage 命名空間到 PutMetricData API 許可	2022 年 4 月 6 日

服務連結角色	新的 AWSServiceRoleForAmazonWorkSpacesWeb 服務連結角色	2021 年 11 月 30 日
受管政策	新的 AmazonWorkSpacesWebReadOnly 受管政策	2021 年 11 月 30 日
受管政策	新的 AmazonWorkSpacesWebServiceRolePolicy 受管政策	2021 年 11 月 30 日
初始版本	WorkSpaces 安全瀏覽器管理指南的初始版本	2021 年 11 月 30 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。