aws

管理指南

Amazon 瀏 WorkSpaces 覽器

Amazon 瀏 WorkSpaces 覽器: 管理指南

Table of Contents

什麼是 Amazon WorkSpaces 安全瀏覽器？ 1
版本歷史記錄 1
使用 WorkSpaces 安全瀏覽器時須知的術語 2
相關服務 3
架構 4
存取 WorkSpaces 安全瀏覽器 4
設定 WorkSpaces 安全瀏覽器 5
註冊和建立使用者 5
註冊一個 AWS 帳戶 5
建立具有管理權限的使用者 5
授予程式設計存取權 7
網路和存取 8
VPC 要求 8
VPC 設定建議 18
支援的可用區域 19
VPC 連線 21
用戶端/使用者連線 21
開始使用 WorkSpaces 安全瀏覽器 24
步驟 1：建立 Web 入口網站 24
進行網路設定 25
進行入口網站設定 25
進行使用者設定 27
設定身分提供者 28
檢閱和啟動 36
步驟 2：測試您的 Web 入口網站 36
步驟 3：分發您的 Web 入口網站 37
後續步驟 37
管理您的 Web 入口網站 38
檢視 Web 入口網站詳細資訊 38
編輯 Web 入口網站 38
刪除 Web 入口網站 39
管理入口網站的服務配額 39
要求增加入口網站 40
要求最大並行工作階段增加 41

限制範例 41
管理服務配額 42
其他服務配額 42
控制重新驗證 SAML IdP 權杖的間隔 42
設定使用者存取日誌記錄 43
範例日誌 44
設定或編輯瀏覽器政策 45
設定自訂瀏覽器政策 (範例) 46
編輯基準瀏覽器政策 52
設定輸入法編輯器 (IME) 53
設定工作階段內本地化 54
設定 IP 存取控制 (選用) 57
建立 IP 存取控制群組 57
將 IP 存取設定與 Web 入口網站建立關聯 58
編輯 IP 存取控制群組 58
刪除 IP 存取控制群組 59
啟用單一登入擴充功能 (選用) 59
設定網址過濾 61
允許深層連結 (選擇性) 62
安全 64
資料保護 64
資料加密 65
網際網路流量隱私權 67
使用者存取日誌記錄 67
身分和存取權管理 67
物件 68
使用身分驗證 68
使用政策管理存取權 71
Amazon 安 WorkSpaces 全瀏覽器如何使用 IAM 73
身分型政策範例 78
AWS 受管理政策 81
故障診斷 89
使用服務連結角色 91
事件反應 94
法規遵循驗證 94
恢復能力 95

基礎架構安全 95
組態與漏洞分析 96
安全最佳實務 96
監控 98
使用監控 CloudWatch 98
CloudTrail 日誌 100
WorkSpaces 安全瀏覽器資訊 CloudTrail 100
瞭解 WorkSpaces 安全瀏覽器記錄檔項目 101
使用者存取日誌記錄 102
WorkSpaces 安全瀏覽器使用者指南 103
瀏覽器和裝置相容 103
存取 Web 入口網站 103
工作階段指引 104
啟動工作階段 104
使用工具列 105
使用瀏覽器 107
結束工作階段 107
故障診斷 108
單一登入擴充功能 109
相容性 109
安裝 109
故障診斷 110
文件歷史紀錄 111
..... cxiv

什麼是 Amazon WorkSpaces 安全瀏覽器？

> **Note**
>
> Amazon WorkSpaces 安全瀏覽器以前被稱為 Amazon WorkSpaces 網絡。

Amazon WorkSpaces Secure Browser 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，以及從拋棄式容器瀏覽網際網路。 WorkSpaces 安全瀏覽器可與使用者現有的網頁瀏覽器搭配使用，不會因管理設備、基礎架構、專用用戶端軟體或虛擬私人網路 (VPN) 連線而造成 IT 負擔。Web 內容會串流至使用者的 Web 瀏覽器，而實際的瀏覽器和網頁內容則隔離在中 AWS。透過使用支援 Amazon WorkSpaces 和 Amazon AppStream 2.0 等 AWS 終端使用者運算服務的相同基礎技術， WorkSpaces Secure Browser 比傳統虛擬桌面更具成本效益，相較於為公司擁有的裝置提供管理軟體，可降低複雜性。 WorkSpaces 安全瀏覽器通過流式傳輸 Web 內容降低數據洩露的風險。不會將 HTML、文件物件模型 (DOM) 或機密公司資料傳輸至本機電腦。透過將裝置、企業網路和網際網路彼此隔離，瀏覽器攻擊面幾乎消除了。

您可以在所有工作階段上強制執行企業瀏覽器原則 (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 安全瀏覽器易於設置和操作。每個工作階段都會啟動時，Chrome 瀏覽器的全新且完整修補版本，並套用公司政策和設定。

版本歷史記錄

2024 年 5 月 20 日，Amazon WorkSpaces 網站更名為 Amazon WorkSpaces 安全瀏覽器。對於現有客戶而言，他們使用服務管理使用者或資源的方式並沒有變更。下列清單說明此重新命名也會發生的適用更新。

為了向後兼容，工作區-Web API 命名空間保持不變。因此，以下資源仍然相同：

- CLI 指令。
- Amazon CloudWatch 指標。如需詳細資訊，請參閱 the section called “使用監控 CloudWatch”。
- 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。
- 包含工作區-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”。

- 包含工作區網頁的主控台 URL。
- 包含工作區網頁的文件 URL。如需詳細資訊，請參閱 Amazon WorkSpaces 安全瀏覽器文件。
- 現有的 ReadOnly 受管理角色。如需詳細資訊，請參閱 the section called “AWS 受管理政策”。
- KMS 授予名稱。
- UAL (使用者活動記錄) Kinesis 流前置詞。

此外，現有的入口網站 URL 會保持不變。2024 年 5 月 20 日之前建立之入口網站的網址使用的格式為 <UUID>.工作空間-web.com。 WorkSpaces 安全瀏覽器入口網站會繼續使用此格式和工作區-web.com 網域。

使用 WorkSpaces 安全瀏覽器時須知的術語

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。您可以將現有的 IdP 配置為使用 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。您還必須授予用戶訪問權限，才能在 IdP 中使用 WorkSpaces 安全瀏覽器。

身分提供者 (IdP) 中繼資料文件

WorkSpaces 安全瀏覽器需要來自身分識別提供者 (IdP) 的特定中繼資料才能建立信任。您可以上傳從 IdP 下載的中繼 WorkSpaces 資料交換檔案，將此中繼資料新增至安全瀏覽器。

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 安全瀏覽器充當服務提供者，已通過其 IdP 驗證的使用者。

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，將您的內容與安 WorkSpaces 全瀏覽器連結。

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 VPC、子網路和安全群組取自與安 WorkSpaces 全瀏覽器主控台相同的區域。

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_UNITED，該網站可能正在使用私有憑證授權單位 (PCA) 所簽署的憑證。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才能載入網站，您必須將該憑證新增至您的信任存放區，才能讓使用者在 WorkSpaces Secure Browser 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。

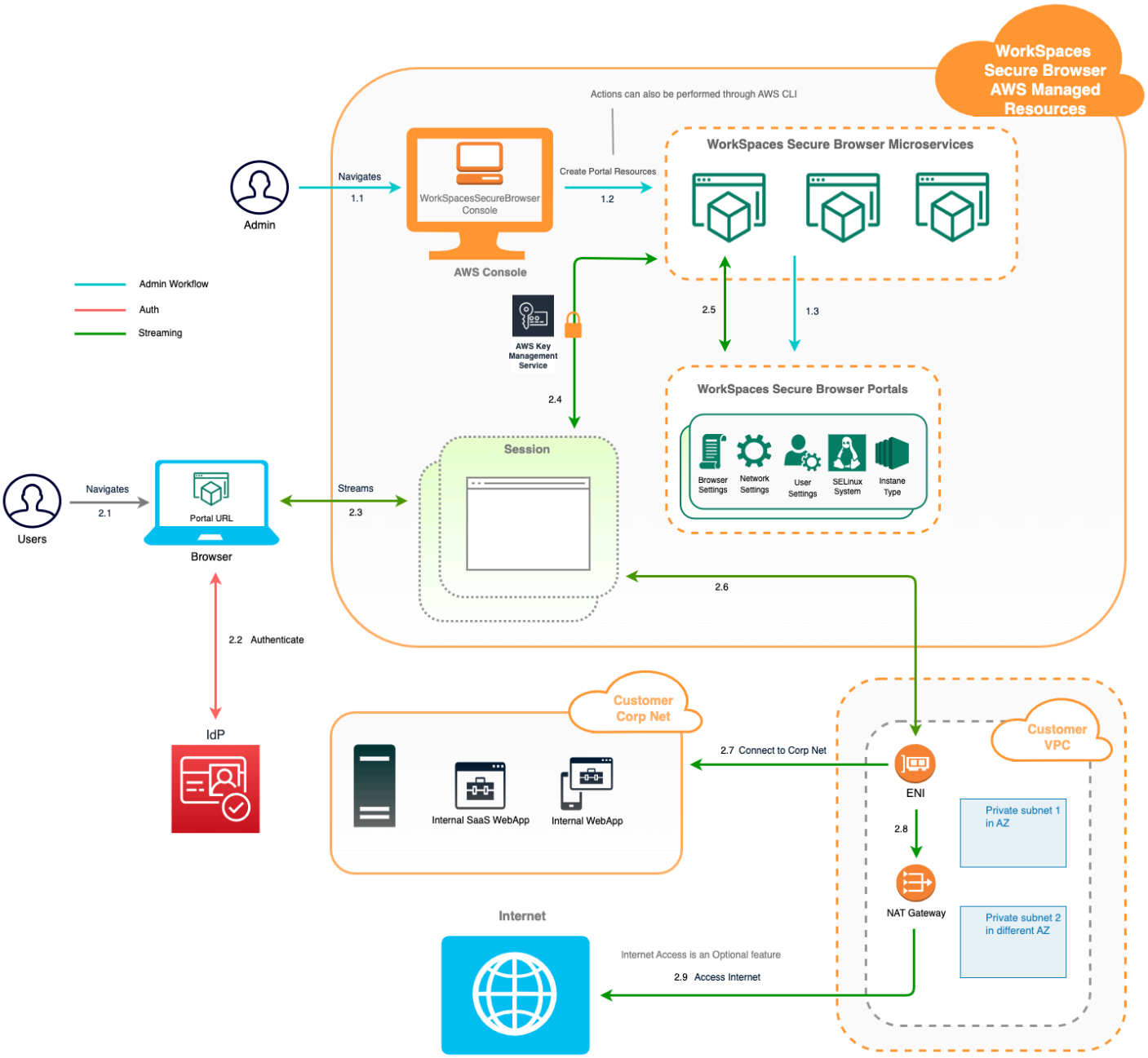
可在網際網路上公開使用端點，且可以嵌入您的網路。

相關服務

WorkSpaces 安全瀏覽器是 Amazon WorkSpaces 在 AWS 最終使用者運算產品組合中提供的一項功能。 WorkSpaces 與 AppStream 2.0 版相比， WorkSpaces 安全瀏覽器是專為促進安全、基於 Web 的工作負載而構建的。 WorkSpaces 安全瀏覽器會自動管理，並由 AWS 根據需求佈建和更新容量、擴展和映像。例如，您可以選擇為需要存取桌上型電腦資源的軟體開發人員提供永久性的 Workspace Desktop，以及為只需要存取少數內部和 SaaS 網站 (包括網路以外託管的網站) 在桌上型電腦上的客服中心使用者提供 WorkSpaces 安全瀏覽器。

架構

下圖顯示了 WorkSpaces 安全瀏覽器的體系結構。



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 WorkSpaces 安全瀏覽器

您必須先完成下列先決條件，才能設定 WorkSpaces 安全瀏覽器以存取內部網站和 SaaS 應用程式。

主題

- 註冊和建立使用者
- 授予程式設計存取權
- 網路和存取

註冊和建立使用者

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 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，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。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。

建立具有管理權限的使用者

註冊後，請保護 AWS 帳戶 AWS 帳戶根使用者、啟用和建立系統管理使用者 AWS IAM Identity Center，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。AWS Management Console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)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 (主控台)。

建立具有管理權限的使用者

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 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

- 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 身分中心使用者登入的說明，請參閱使用AWS 登入 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 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

授予程式設計存取權

如果使用者想要與 AWS 之外的 AWS Management Console. 授與程式設計存 AWS取權的方式取決於正在存取的使用者類型。

若要授與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	By
人力身分 (IAM Identity Center 中管理的使用者)	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需詳細資訊 AWS CLI，請參閱《使 AWS CLI 用AWS Command Line Interface者指南》 AWS IAM Identity Center中的〈配置使用〉。 • 如需 AWS SDK、工具和 AWS API，請參閱 AWS SDK 和工具參考指南中的 IAM 身分中心身分驗證。
IAM	使用臨時登入資料來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	遵循《IAM 使用者指南》中的〈將臨時登入資料搭配 AWS 資源使用〉中的指示
IAM	(不建議使用) 使用長期認證來簽署對 AWS CLI、 AWS SDK 或 AWS API 的程式設計要求。	請依照您要使用的介面所提供的指示操作。 • 如需相關資訊 AWS CLI，請參閱使用指南中的使用 IAM 使用者登入資料進行驗證。AWS Command Line Interface • 對於 AWS SDK 和工具，請參閱 AWS SDK 和工具參

哪個使用者需要程式設計存取權？	到	By
		考指南中的使用長期憑據進行身份驗證。 • 如需 AWS API，請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰。

網路和存取

下列主題說明如何設定 WorkSpaces 安全瀏覽器串流執行個體，讓使用者可以連線到這些執行個體。同時也說明如何讓您的 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

- VPC 要求
- VPC 設定建議
- 支援的可用區域
- VPC 連線
- 用戶端/使用者連線

VPC 要求

建立 WorkSpaces 安全瀏覽器入口網站期間，您會在帳戶中選取 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。您的子網路必須具有足夠的 IP 位址，才能支援預期的 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 建立和設定新的 VPC。
- 所有子網路必須與使用者透過 WorkSpaces 安全瀏覽器存取的任何內部內容 (位於內部部署 AWS 雲端 或內部部署) 建立穩定的連線。

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 建立和設定新的 VPC。

WorkSpaces 安全瀏覽器不會為串流執行個體指派任何公用 IP 位址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用網際網路內容和私人虛擬私人雲端內容，請完成中啟用不受限制的網際網路瀏覽 (建議)的步驟。

建立和設定新的 VPC

本節說明如何使用 VPC 精靈來建立具有公有子網路和一個私有子網路的 VPC。過程中，精靈會建立網際網路閘道和 NAT 閘道，它也會建立與公有子網路相關聯的自訂路由表。接著會更新與私有子網路相關聯的主路由表。會自動在您 VPC 的公有子網路中建立 NAT 閘道。

使用精靈建立 VPC 組態後，您必須新增第二個私有子網路。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。

步驟 1：配置彈性 IP 地址

在建立 VPC 之前，您必須在 WorkSpaces 安全瀏覽器區域中分配彈性 IP 位址。配置完成後，您可以將彈性 IP 地址與您的 NAT 閘道建立關聯。透過彈性 IP 地址，您可以快速地將地址重新映射至您 VPC 中的另一個串流執行個體，藉以遮罩串流執行個體的故障。如需詳細資訊，請參閱彈性 IP 地址。

> **Note**
>
> 您可能需要為使用的彈性 IP 地址付費。如需詳細資訊，請參閱彈性 IP 地址定價頁面。

如果您還沒有彈性 IP 地址，請完成以下步驟。若您要使用現有的彈性 IP 地址，您必須先確認它目前並未與其他執行個體或網路界面建立關聯。

配置彈性 IP 地址

1. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽窗格中，於 Network & Security (網路與安全) 下方，選擇 Elastic IPs (彈性 IP)。
3. 選擇 Allocate New Address (配置新地址)，然後選擇 Allocate (配置)。
4. 請記下主控台上顯示的彈性 IP 地址。
5. 在彈性 IP 窗格的右上角，按一下 × 圖示來關閉窗格。

步驟 2：建立新的 VPC

請完成下列步驟，以建立具有公有子網路和一個私有子網路的新 VPC。

建立新的 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 VPC dashboard (VPC 儀表板)。
3. 選擇 Launch VPC Wizard (啟動 VPC 精靈)。
4. 在 Step 1: Select a VPC Configuration (步驟 1：選取 VPC 組態) 中，選擇 VPC with Public and Private Subnets (含公有和私有子網路的 VPC)，然後選擇 Select (選取)。
5. 在 Step 2: VPC with Public and Private Subnets (步驟 2：含公有和私有子網路的 VPC)中，按照以下內容設定 VPC：
   - 針對 IPv4 CIDR block (IPv4 CIDR 區塊)，請指定 VPC 的 IPv4 CIDR 區塊。
   - 針對 IPv6 CIDR block (IPv6 CIDR 區塊)，請保留預設值 No IPv6 CIDR Block (無 IPv6 CIDR 區塊)。
   - 針對 VPC 名稱，請輸入 VPC 的專屬名稱。
   - 根據以下內容設定公有子網路：
     - 針對 Public subnet's IPv4 CIDR (公有子網路的 IPv4 CIDR)，請為子網路指定 CIDR 區塊。
     - 針對 Availability Zone (可用區域)，請保留預設值 No Preference (無偏好設定)。
     - 針對公有子網路名稱，輸入子網路的名稱。例如 **`WorkSpaces Secure Browser Public Subnet`**。
   - 根據以下內容設定第一個私有子網路：
     - 針對 Private subnet's IPv4 CIDR (私有子網路的 IPv4 CIDR)，請為子網路指定 CIDR 區塊。記下您指定的值。
     - 針對 Availability Zone (可用區域)，請選取特定區域並記下您選取的區域。
     - 針對私有子網路名稱中，輸入子網路名稱。例如 **`WorkSpaces Secure Browser Private Subnet1`**。
   - 如果適用，請保留其他欄位的預設值。
   - 針對彈性 IP 配置 ID，請輸入與您建立之彈性 IP 地址對應的值。這個地址會指派至 NAT 閘道。如果您沒有彈性 IP 地址，請在 https://console.aws.amazon.com/vpc/ 使用 Amazon VPC 主控台建立地址。
   - 針對服務端點，如果您的環境需要 Amazon S3 端點，請指定一個。

如果要指定 Amazon S3 端點，請按照以下步驟操作：

1. 選擇 Add Endpoint (新增端點)。
2. 對於「服務」，請選取相關網站。 **##** .s3 項目，其中「*##*」是 AWS 區域 您要在其中建立 VPC 的位置。
3. 針對 Subnet (子網路)，選擇 Private subnet (私有子網路)。
4. 針對 Policy (政策)，請保留預設值 Full Access (完整存取權)。

- 針對 Enable DNS hostnames (啟用 DNS 主機名稱)，請保留預設值 Yes (是)。
- 針對 Hardware tenancy (硬體租用)，請 保留預設值 Default (預設)。
- 選擇建立 VPC。
- 設定 VPC 需要幾分鐘的時間。建立 VPC 之後，選擇 OK (確定)。

步驟 3：新增第二個私有子網路

在上一個步驟中，您建立了具有一個公有子網路和一個私有子網路的 VPC。請完成以下步驟來新增您的 VPC 的第二個私有子網路。建議您在第一個私有子網路以外的可用區域新增第二個私有子網路。

新增第二個私有子網路

1. 在導覽窗格中，選擇 Subnets (子網)。
2. 選取您在上一個步驟中建立的第一個私有子網路。在 Description (描述) 標籤上 (位在子網路清單下方)，記下此子網路的可用區域。
3. 在子網路窗格的左上角選擇 Create Subnet (建立子網路)。
4. 針對名稱標籤，輸入私有子網路的名稱。例如 **WorkSpaces Secure Browser Private Subnet2**。
5. 針對 VPC，請選取您在前一個步驟建立的 VPC。
6. 針對可用區域，請選取您為第一個私有子網路使用之可用區域以外的可用區域。選取其他可用區域可提升容錯能力，並協助避免發生容量不足的錯誤。
7. 針對 IPv4 CIDR block (IPv4 CIDR 區塊)，請為新的子網路指定專屬的 CIDR 區塊範圍。舉例來說，如果您第一個私有子網路的 IPv4 CIDR 區塊範圍是 **10.0.1.0/24**，可以為第二個私有子網路指定 **10.0.2.0/24** 的 CIDR 區塊範圍。
8. 選擇建立。
9. 建立子網路之後，請選擇 Close (關閉)。

步驟 4：確認並為您的子網路路由表命名

在您建立並設定 VPC 後，請完成以下步驟來為您的路由表指定名稱：您需要驗證以下您的路由表詳細資訊是否正確：

- 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，並選取您建立的公有子網路。例如，WorkSpaces 安全瀏覽器 2.0 公共子網路。
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：

目的地	目標	描述
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，選取您建立的第一個私有子網路 (例如，**WorkSpaces Secure Browser Private Subnet1**)。
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 **workspacesweb-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：

目的地	目標	描述
公有子網路 IPv4 CIDR 區塊 (例如 10.0.0/20)	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。

啟用不受限制的網際網路瀏覽 (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 安全瀏覽器存取公用網際網路上的網站，以及託管在 VPC 中或與 VPC 連線的私人網站。

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用網際網路內容和私人虛擬私人雲端內容，請依照下列步驟執行：

> **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，請參閱建立和設定新的 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。如需如何建立第二個私有子網路的資訊，請參閱the section called "步驟 3：新增第二個私有子網路"。

   > **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到 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。

啟用受限制的網際網路瀏覽（使用輸出 HTTP 代理）

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用網際網路和私人內容。如需詳細資訊，請參閱 the section called "啟用不受限制的網際網路瀏覽 (建議)"。但是，您可能需要使用 Web Proxy 來控制從 WorkSpaces 安全瀏覽器入口網站到網際網路的輸出通訊。例如，如果您使用 Web Proxy 做為網際網路閘道，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 (例如本機網頁或軟體更新) 來減少頻寬使用量並改善網路效能。對於某些使用案例，您可能擁有只能透過 Web Proxy 存取的私人內容。

您可能已經熟悉在受管理設備上或虛擬環境的映像上設定 Proxy 設定。但是，如果您無法控制裝置 (例如，使用者使用的是非企業擁有或管理的裝置)，或者您需要管理虛擬環境的映像，這會帶來挑戰。透過 WorkSpaces 安全瀏覽器，您可以使用網頁瀏覽器內建的 Chrome 政策來設定代理伺服器設定。您可以通過為 WorkSpaces 安全瀏覽器設置 HTTP 出站代理來做到這一點。

此解決方案是以建議的輸出 VPC Proxy 設定為基礎。代理解決方案是以開放原始碼 HTTP 代理伺服器 Squid 為基礎。然後，它會使用 WorkSpaces 安全瀏覽器瀏覽器設定，將 WorkSpaces 安全瀏覽器入口網站設定為連線到 Proxy 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設定輸出 VPC Proxy。

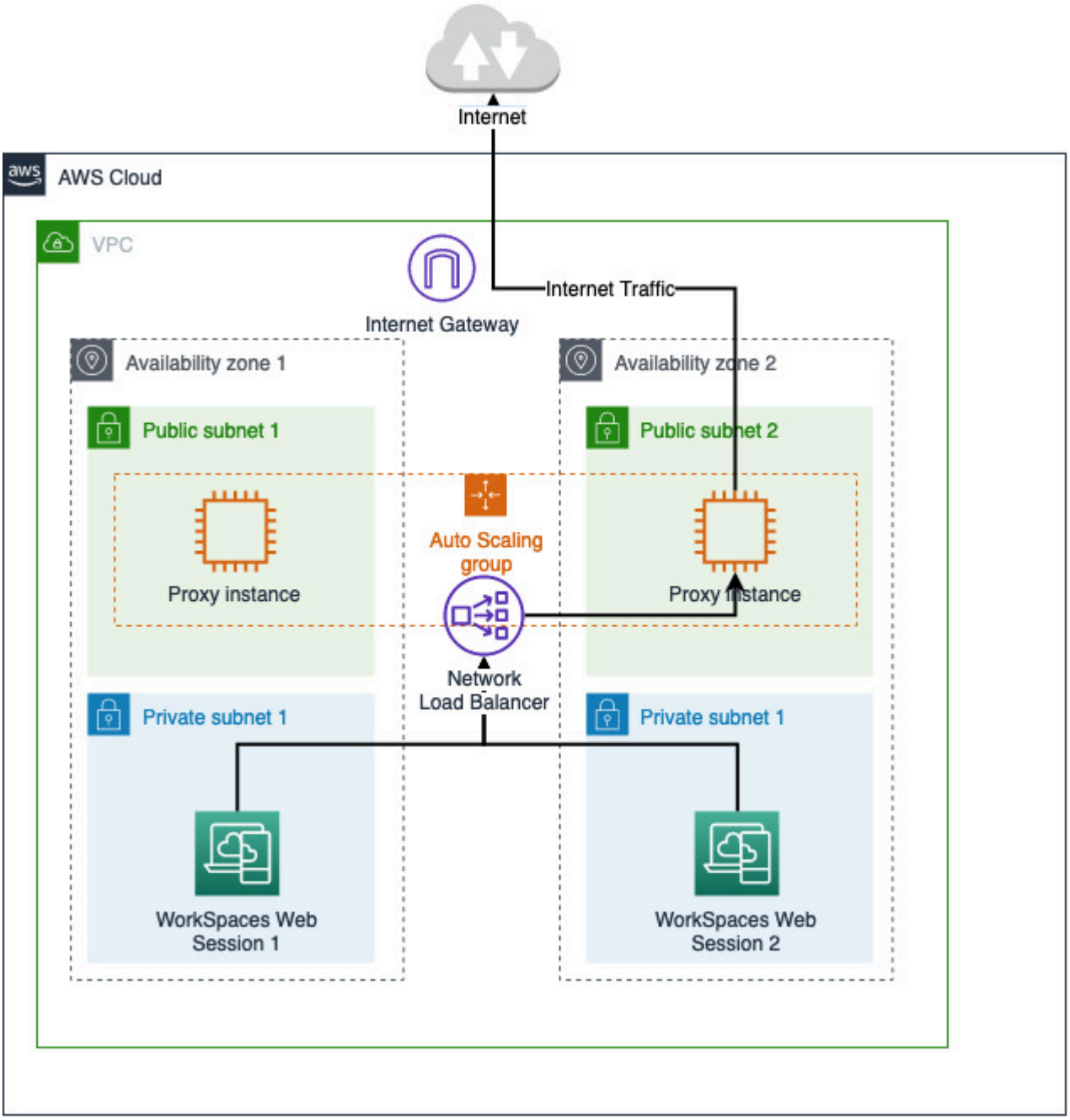
此解決方案為您提供以下優點：

- 輸出代理，其中包含由網路負載平衡器託管的一組 auto-scaling Amazon EC2 執行個體。代理實例位於公共子網中，每個實例都附有彈性 IP，因此可以訪問互聯網。

- 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 閘道即可啟用網際網路存取。相反地，您可以設定瀏覽器原則，以便所有網際網路流量都會經過輸出 Proxy。如果您想使用自己的代理伺服器， WorkSpaces 安全瀏覽器入口網站的設定將會類似。

架構

以下是 VPC 中典型 Proxy 設定的範例。代理 Amazon EC2 實例位於公共子網中，並與彈性 IP 相關聯，因此他們可以訪問互聯網。網路負載平衡器主控 Proxy 執行個體的 auto 調整資源調度群組。如此可確保 Proxy 執行個體能夠自動擴充，而網路負載平衡器是單一 Proxy 端點，可由 WorkSpaces Secure Browser 工作階段使用。



必要條件

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多個可用區域 (AZ)。如需如何設定 VPC 環境的詳細資訊，請參閱預設 V PC。

- 您需要一個可從私有子網路存取的單一 Proxy 端點，其中 WorkSpaces 安全瀏覽器工作階段存取 (例如，網路負載平衡器 DNS 名稱)。如果您想要使用現有的 Proxy，請確定它也有可從您的私有子網路存取的單一端點。

為 WorkSpaces 安全瀏覽器設定 HTTP 輸出代理

若要為 WorkSpaces 安全瀏覽器設定 HTTP 輸出 Proxy，請依照下列步驟執行。

1. 若要將範例輸出 Proxy 部署到您的 VPC，請遵循如何使用網域白名單和內容篩選設定輸出 VPC Proxy 中的步驟進行操作。
   a. 依照「安裝 (一次性設定)」中的步驟，將 CloudFormation範本部署到您的帳戶。請務必選擇正確的 VPC 和子網路做為 CloudFormation 範本參數。
   b. 部署後，找到 CloudFormation 輸出參數OutboundProxy域和OutboundProxy端口。這是代理伺服器的 DNS 名稱和連接埠。
   c. 如果您已經擁有自己的代理伺服器，請略過此步驟，並使用 Proxy 的 DNS 名稱和連接埠。
2. 在 WorkSpaces 安全瀏覽器的主控台中，選取您的入口網站，然後選擇 [編輯]。
   a. 在 [網路連線詳細資料] 中，選擇可存取 Proxy 的 VPC 和私人子網路。
   b. 在 [原則] 設定中，使用 JSON 編輯器新增下列 ProxySettings原則。此`ProxyServer`欄位應該是您代理伺服器的 DNS 名稱和連接埠。如需有關 ProxySettings 策略的詳細資訊，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 安全瀏覽器會話中，您將看到代理已應用於 Chrome 設置 Chrome 正在使用管理員的代理設置。

4. 前往 chrome://政策和 Chrome 政策索引標籤，以確認該政策已套用。
5. 確認您的 WorkSpaces 安全瀏覽器工作階段可以在沒有 NAT 閘道的情況下順利瀏覽網 在記錄 CloudWatch 檔中，確認是否已記錄 Squid 代理存取記錄檔。

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無法存取網際網路，請依照下列步驟嘗試解決問題：

- 確認 Proxy 端點可從 WorkSpaces 安全瀏覽器入口網站所在的私有子網路存取。為此，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 Proxy 端點的連線。
- 確認代理伺服器具有網際網路存取權。
- 確認 Chrome 政策是否正確無誤。
  - 確認策略`ProxyServer`欄位的下列格式：`<Proxy DNS name>:<Proxy port>`前綴`https://`中不應該有`http://`或。
  - 在「 WorkSpaces 安全瀏覽器」工作階段中，使用 Chrome 瀏覽至 chrome://政策，並確認 ProxySettings 政策已成功套用。

VPC 設定建議

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) 足以支援您預期的需求。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/。如需有關預設 WorkSpaces 安全瀏覽器配額的資訊，請參閱the section called “管理入口網站的服務配額”。
- 如果您打算提供串流工作階段可存取網際網路，建議您在公有子網路中使用 NAT 閘道來設定 VPC。

彈性網路界面

- 在串流期間，每個 WorkSpaces 安全瀏覽器工作階段都需要自己的 elastic network interface。WorkSpaces 安全瀏覽器會建立盡可能多的彈性網路介面 (ENI) 與您的叢集所需的最大容量一樣多。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

- 在制定擴充使用者規模的計劃時，請記住，每個 WorkSpaces 安全瀏覽器工作階段都需要來自您設定的子網路的唯一用戶端 IP 位址。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 安全瀏覽器支援的每個唯一可用區域中設定子網路，以便考量可用性和擴展性。如需詳細資訊，請參閱 the section called “建立和設定新的 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安 WorkSpaces 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。

支援的可用區域

當您建立虛擬私有雲 (VPC) 以搭配 WorkSpaces 安全瀏覽器使用時，您的 VPC 子網路必須位於您要啟動 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，每個 AWS 帳戶都有相同的位置。

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的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
亞太區域 (孟買)	ap-south-1	aps1-az1, aps1-az3
亞太區域 (首爾)	ap-northeast-2	apne2-az1 , apne2-az2 , apne2-az3
亞太區域 (新加坡)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
亞太區域 (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

如需有關可用區域和 AZ ID 的詳細資訊，請參閱 Amazon EC2 使用者指南中的區域、可用區域和 Local Zones。

VPC 連線

每個 WorkSpaces Secure Browser 串流執行個體都有一個客戶網路介面，可提供 VPC 內資源的連線能力，如果設定了具有 NAT 閘道的私有子網路，則可連線至網際網路。

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

用戶端/使用者連線

WorkSpaces 安全瀏覽器設定為透過公用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網路資產。若要允許此流量，您必須允許 允許的網域 中所列的網域。

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

主題

- IP 地址和連接埠需求
- 允許的網域

IP 地址和連接埠需求

若要存取 WorkSpaces 安全瀏覽器執行個體，使用者裝置需要下列連接埠的輸出存取權：

- 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 允許的網域 所列的必要網域。
- AWS 以 JSON 格式發佈其目前 IP 位址範圍，包括工作階段閘道和 CloudFront 網域可能解析為的範圍。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，如果您正在使用 AWS Tools for Windows PowerShell，則可以使用Get-AWSPublicIpAddressRange PowerShell指令存取相同的資訊。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。

允許的網域

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

在下表中，將 *{region}* 替換為操作門戶網站的區域的代碼。例如，s3。 對##########的門戶網站，應該是西部-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。

類別	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 *.shortbread.aws.dev
WorkSpaces 安全瀏覽器靜態資產	*.workspaces-web.com

類別	網域或 IP 地址
	二元四乙肝 4263. 雲前網
WorkSpaces 安全瀏覽器驗證	*.auth.*{region}*.amazoncognito.com cognito-identity.*{region}*.amazonaws.com cognito-idp.*{region}*.amazonaws.com *.cloudfront.net
WorkSpaces 安全的瀏覽器指標和報告	*.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。檢閱您的 IdP 文件，以確定您需要允許哪些網域清單， WorkSpaces 安全瀏覽器才能使用該提供者。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。

開始使用 WorkSpaces 安全瀏覽器

請依照下列步驟建立 WorkSpaces 安全瀏覽器入口網站，並讓使用者從現有瀏覽器存取內部和 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。

> **Note**
>
> 若要要求提高多個入口網站的限制，請連絡支援人員，並提供您的 AWS 帳戶 ID、要求的入口網站數量，以及 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定價，包括為積極使用該服務的用戶提供低廉的每月價格。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 WorkSpaces 安全瀏覽器。

主題

- 步驟 1：建立 Web 入口網站
- 步驟 2：測試您的 Web 入口網站
- 步驟 3：分發您的 Web 入口網站
- 後續步驟

步驟 1：建立 Web 入口網站

請執行下列步驟以建立 Web 入口網站：

主題

- 進行網路設定

- 進行入口網站設定
- 進行使用者設定
- 設定身分提供者
- 檢閱和啟動

進行網路設定

1. 開啟 WorkSpaces 安全瀏覽器主控台，網址為 https://console.aws.amazon.com/workspaces-web/home。
2. 選擇WorkSpaces 安全瀏覽器，然後選擇 Web 入口網站，然後選擇建立入口網站。
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. 如需網路詳細資訊，請選擇連線到您希望使用者透過 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 網路和存取。
        - 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。

進行入口網站設定

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 “管理入口網站的服務配額”。

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

3. 在使用者存取日誌記錄底下，針對 Kinesis 串流 ID，選取您要將資料傳送到哪個 Amazon Kinesis 資料串流。如需詳細資訊，請參閱 the section called “設定使用者存取日誌記錄”。
4. 在政策設定下，完成下列操作：
   - 針對選項，請選取視覺化編輯器或 JSON 檔案上傳。您可以使用其中一種方法來提供 Web 入口網站的政策組態詳細資訊。如需詳細資訊，請參閱 the section called “設定或編輯瀏覽器政策”。
     - WorkSpaces 安全瀏覽器包含 Chrome 企業政策的支援。您可以使用視覺化編輯器或手動上傳政策檔案，以新增和管理政策。您可隨時切換使用這兩個選項。
     - 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。
   - (選用) 針對啟動 URL – 選用，輸入當使用者啟動瀏覽器時當成首頁的網域。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 “設定使用者存取日誌記錄”。

   - 在 [URL 篩選] 底下，您可以設定使用者可以在工作階段期間造訪哪些 URL。如需詳細資訊，請參閱 the section called “設定網址過濾”。
   - (選用) 針對瀏覽器書籤 – 選用，針對您要使用者在其瀏覽器中看到的任何書籤，輸入顯示名稱、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。

   - (選用) 為您的入口網站新增標籤。您可以使用標籤來搜尋或篩選資 AWS 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。
5. 在 IP 存取控制 (選用) 底下，選擇是否要限制存取受信任的網路。如需詳細資訊，請參閱 the section called “設定 IP 存取控制 (選用)”。
6. 選擇 Next (下一步) 繼續。

進行使用者設定

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. 針對使用者許可，請選擇是否啟用單一登入擴充功能。如需詳細資訊，請參閱 the section called “啟用單一登入擴充功能 (選用)”。
2. 針對剪貼簿許可，請選擇停用或啟用。
3. 在檔案傳輸下，選擇停用或啟用。
4. 對於 [允許使用者從其 Web 入口網站列印至本機裝置]，請選擇 [允許] 或 [不允許]。
5. 對於 [允許使用者深入連結至其 Web 入口網站]，請選擇 [允許] 或 [不允許]。如需深層連結的詳細資訊，請參閱the section called “允許深層連結 (選擇性)”。
6. 針對使用者工作階段詳細資訊，指定以下內容：

   - 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。不然的話，他們會連線到含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。然後，使用者使用的執行個體就會終止。

   - 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。使用者會在由於未活動而導致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。不然的話，他們會連線到含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**
     >
     > 當使用者在其串流工作階段期間停止提供鍵盤或滑鼠輸入時，便會將其視為閒置。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。

設定身分提供者

請使用下列步驟來設定您的身分識別提供者 (IdP)。

主題

- 選擇身分識別提供者類型
- 設定標準驗證類型
- 設定 IAM 身分中心驗證類型
- 變更身分識別提供者類型

選擇身分識別提供者類型

WorkSpaces 安全瀏覽器提供兩種驗證類型：標準和 AWS IAM Identity Center. 您可以在 [設定身分識別提供者] 頁面上選擇要搭配入口網站使用的驗證類型。

- 對於標準 (預設選項)，請直接將您的第三方 SAML 2.0 身分識別提供者 (例如 Okta 或 Ping) 與入口網站聯合。如需詳細資訊，請參閱 the section called “設定標準驗證類型”。標準類型支援 SP 起始和 IDP 起始的驗證流程。
- 對於 IAM 身分中心 (進階選項)，請將 IAM 身分中心與入口網站聯合。若要使用此身分驗證類型，您的 IAM 身分中心和 WorkSpaces 安全瀏覽器入口網站必須位於同一個類型 AWS 區域。如需詳細資訊，請參閱 the section called “設定 IAM 身分中心驗證類型”。

設定標準驗證類型

對於標準 (預設)，請直接將您的第三方 SAML 2.0 身分識別提供者 (例如 Okta 或 Ping) 與入口網站聯盟。

標準身分識別類型可以透過符合 SAML 2.0 標準的 IdP 支援 service-provider-initiated identity-provider-initiated (SP 起始) 和 (IdP 起始) 登入流程。

步驟 1：開始在 WorkSpaces 安全瀏覽器上配置您的身份提供者

完成下列步驟來設定您的身分識別提供者：

1. 在建立精靈的設定身分提供者頁面上，選擇標準。
2. 選擇「繼續標準 IdP」。
3. 下載 SP 中繼資料檔案，並保持開啟個別中繼資料值的索引標籤。

- 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至您的 IdP。如果沒有此功能，使用者將無法登入。
- 如果您的供應商未上傳 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 宣告，或者僅限 SP 起始的 SAML 判斷提示。
   - SP 起始和 IDP 起始的 SAML 判斷提示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將 SAML 宣告呈現給服務身分識別聯合端點，而不需要使用者透過造訪入口網站 URL 啟動工作階段。
     - 選擇此選項以允許入口網站接受來路不明的 IDP 起始 SAML 宣告。
     - 此選項需要在 SAML 2.0 身分識別提供者中設定預設的轉送狀態。入口網站的轉送狀態參數位於 IdP 起始 SAML 登入下的主控台中，或者您可以從下的 SP 中繼資料檔案複製它。`<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=ExIdentity-Provider`。
       - 如果您複製並貼上 SP 中繼資料檔案中的值，請確定您將變更`&amp;` 為`&`。 `&amp;`是 XML 逸出字元。
   - 只針對入口網站選擇 SP 起始的 SAML 宣告，以僅支援 SP 起始的登入流程。此選項將拒絕來自 IDP 起始登入流程的來路不明的 SAML 宣告。

   > **Note**
   >
   > 某些協力廠商 IdPs 允許您建立自訂 SAML 應用程式，該應用程式可利用 SP 啟動的流程提供 IdP 起始的驗證體驗。例如，請參閱新增 Okta 書籤應用程式。

5. 選擇是否要對此提供者啟用「簽署 SAML 要求」。SP 啟動的驗證可讓您的 IdP 驗證驗證要求來自入口網站，以防止接受其他第三方要求。
   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 中啟用已簽署的要求。名稱可能會有所不同，具體取決於 IdP。

> **Note**
>
> RSA-SHA256 是唯一支援的要求和預設要求簽章演算法。

6. 選擇是否要啟用需要加密的 SAML 宣告。這可讓您加密來自 IdP 的 SAML 判斷提示。它可以防止在 IdP 和安全瀏覽器之間的 SAML 判斷提示中攔截資料。 WorkSpaces

> **Note**
>
> 此步驟無法使用加密憑證。它將在您的門戶網站啟動後創建。啟動入口網站之後，請下載加密憑證並將其上傳到您的 IdP。然後，在 IdP 中啟用斷言加密（名稱可能會有所不同，具體取決於 IdP。

7. 選擇是否要啟用「單一登出」。單一登出可讓您的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 安全瀏覽器下載簽名證書，並將其上傳到您的 IdP。這與上一個步驟中用於「要求簽署」的簽署憑證相同。
   b. 使用單一登出時，您必須在 SAML 2.0 身分識別提供者中設定單一登出 URL。您可以在服務提供者 (SP) 詳細資料下的主控台中找到入口網站的單一登出 URL-顯示個別中繼資料值，或從下`<md:SingleLogoutService>`的 SP 中繼資料檔案。
   c. 在 IdP 中啟用單一登出。名稱可能會有所不同，具體取決於 IdP。

步驟 2：在您自己的 IdP 上設定您的身分識別提供者

在瀏覽器中開啟新的分頁。然後使用您的 IdP 完成下列步驟：

1. 將入口網站中繼資料新增至您的 SAML IdP。

   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。某些供應商不允許檔案上傳。

   此過程的詳細信息可能因提供商而異。如the section called “具體的指導 IdPs”需如何將入口網站詳細資料新增至 IdP 組態的說明，請參閱中的提供者說明文件。

2. 確認您的 SAML 宣告的 NameID。

請確定您的 SAML IdP 使用使用者電子郵件欄位填入 SAML 宣告中的 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。使用永久性 SAML 名稱識別碼格式。

3. 可選：為 IDP 起始的驗證設定轉送狀態。

   如果您在上一個步驟中選擇了接受 SP 起始和 IdP 起始的 SAML 宣告，請依照步驟 2 中的步驟設定 IdP 應用程式的預設the section called “步驟 1：開始在 WorkSpaces 安全瀏覽器上配置您的身份提供者”轉送狀態。

4. 選用性：設定要求簽署。如果您在上一個步驟中選擇「將 SAML 要求簽署給此提供者」，請遵循步驟 3 中的步驟，將簽署憑證上傳the section called “步驟 1：開始在 WorkSpaces 安全瀏覽器上配置您的身份提供者”到您的 IdP 並啟用要求簽署。某些 IdPs 例如 Okta 可能要求您的 NameID 屬於「永久」類型才能使用請求簽名。請依照上述步驟確認您的 SAML 判斷提示的 NameID。

5. 選用性：設定宣告加密。如果您選擇需要來自此提供者的加密 SAML 宣告，請等到入口網站建立完成，然後遵循下面「上傳中繼資料」中的步驟 4，將加密憑證上傳至您的 IdP 並啟用宣告加密。

6. 選用性：設定單一登出。如果您選擇「單一登出」，請按照步驟 5 中的步驟將簽署憑證上傳the section called “步驟 1：開始在 WorkSpaces 安全瀏覽器上配置您的身份提供者”到 IdP，填寫「單一登出 URL」，然後啟用「單一登出」。

7. 授予 IdP 中的使用者使用 WorkSpaces 安全瀏覽器的存取權。

8. 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元數據上傳到 WorkSpaces 安全瀏覽器。

步驟 3：在 WorkSpaces 安全瀏覽器上完成身分提供者的設定

返回 WorkSpaces 安全瀏覽器主控台。在建立精靈的 [設定身分識別提供者] 頁面上，在 IdP 中繼資料下，上傳中繼資料檔案，或從您的 IdP 輸入中繼資料 URL。入口網站會使用 IdP 中繼資料來建立信任。

1. 若要上載中繼資料檔案，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。

2. 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。

3. 完成時請選擇 Next (下一步)。

4. 如果入口網站已啟用「需要來自此提供者的加密 SAML 宣告」選項，您必須從入口網站 IdP 詳細資料區段下載加密憑證，並將其上傳至您的 IdP。然後，您可以在此處啟用該選項。

Note

WorkSpaces 安全瀏覽器需要在 IdP 的設定中，在 SAML 宣告中對應並設定主旨或 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 安全瀏覽器需要在 SAML 回應中提供下列宣告。<Your SP Entity ID><Your SP ACS URL>您可以透過主控台或 CLI 尋找入口網站的服務提供者詳細資料或中繼資料文件，並從中找到。

- 具有將您的 SP 實體 ID 設定為回應目標的`Audience`值的`AudienceRestriction`宣告。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>">
```

- 具有您的 SP ACS 網址`Recipient`值的`SubjectConfirmationData`宣告，以及與原始 SAML 要求識別碼相符的`InResponseTo`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 判斷提示。對於 IdP 起始的 SAML 宣告，請求的詳細資訊必須格式化為 HTTP POST 要求主體中的`RelayState`參數。要求主體也必須包含您的 SAML 判斷提示做為`SAMLResponse`參數。如果您遵循上一個步驟，這兩者都應該存在。
以下是 IdP 起始之 SAML 提供者的範例`POST`主體。

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

具體的指導 IdPs

若要確保您正確設定入口網站的 SAML 聯盟，請參閱下列連結以取得常用 IdPs的說明文件。

IdP	SAML 應用程式設定	使用者管理	IDP 啟動的身份驗證	請求簽署	斷言加密	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
恩特拉	創建自己的應用程序	快速入門：建立並指派使用者帳戶	啟用企業應用程式的單一登入	SAML 要求簽名驗證	設定 Microsoft 中央 SAML 權杖加密	單一登出 SAML 通訊協定
Ping	新增 SAML 應用程式	使用者	啟用 IDP 起始的單一登入	PingOne 為企業配置身份驗證請求登錄	企業版是否 PingOne 支援加密？	單一登出
一次登入	SAML 客製化連接器 (進階) (4266907)	OneLogin 手動新增使用者	SAML 客製化連接器 (進階) (4266907)	SAML 客製化連接器 (進階) (4266907)	SAML 客製化連接器 (進階) (4266907)	SAML 客製化連接器 (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 IAM 身分中心驗證類型

對於 IAM 身分中心類型 (進階)，您可以將 IAM 身分中心與入口網站聯合。只有在下列情況適用於您時，才選取此選項：

- 您的 IAM 身分中心設定 AWS 區域 為 AWS 帳戶 與您的入口網站相同。

- 如果您使用 AWS Organizations的是管理帳戶。

使用 IAM 身分中心驗證類型建立入口網站之前，您必須將 IAM 身分中心設定為獨立提供者。如需詳細資訊，請參閱 IAM 身分識別中心中的一般工作入門。或者，您可以將 SAML 2.0 IdP 連線到身分識別中心。如需詳細資訊，請參閱 Connect 至外部身分識別提供者。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。

如果您已在使用 IAM 身分中心，則可以選擇 IAM 身分中心做為提供者類型，然後按照以下步驟從 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，您的 IAM 身分中心必須 AWS 帳戶 與 AWS 區域 您的 WorkSpaces 安全瀏覽器入口網站位於同一個位置。如果您的 IAM 身分中心位於單獨 AWS 區域， AWS 帳戶 或者請遵循標準身份驗證類型的說明進行操作。如需詳細資訊，請參閱 the section called "設定標準驗證類型"。
> 如果您使用的是 AWS Organizations，您只能使用管理帳戶建立與 IAM 身分中心整合的 WorkSpaces 安全瀏覽器入口網站。

使用 IAM Identity Center 來建立 Web 入口網站

1. 在步驟 4：設定身分識別提供者建立入口網站期間，請選擇AWS IAM Identity Center。
2. 選擇「繼續使用 IAM 身分中心」。
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. 核取您要新增至入口網站的使用者或群組旁邊的方塊。
5. 建立入口網站之後，您關聯的使用者可以使用他們的 IAM 身分中心使用者名稱和密碼登入 WorkSpaces 安全瀏覽器。

使用 IAM Identity Center 來管理 Web 入口網站

1. 建立入口網站之後，該入口網站會在 IAM 身分中心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現有的 Web 入口網站

1. 開啟 WorkSpaces 安全瀏覽器主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 [WorkSpaces 安全瀏覽器]、[入口網站]、選擇您的入口網站，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。

若要檢視或移除 Web 入口網站的使用者和群組

- 您可以使用「已指派的使用者」表格中的可用動作來檢視或移除使用者對此應用程式的存取權限。如需詳細資訊，請參閱管理應用程式的存取權。

> **Note**
>
> 您無法從 WorkSpaces 安全瀏覽器入口網站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。

變更身分識別提供者類型

請依照下列步驟隨時變更入口網站的驗證類型：

- 若要從 IAM 身分中心變更為標準，請遵循中的步驟the section called “設定標準驗證類型”。

- 若要從標準變更為 IAM 身分中心，請遵循中的步驟the section called “設定 IAM 身分中心驗證類型”。

身分識別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的工作階段。

您可以透 AWS CloudTrail 過檢查`UpdatePortal`事件來檢視入口網站的身分識別提供者類型變更。該類型在事件的請求和響應有效載荷中可見。

檢閱和啟動

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。

步驟 2：測試您的 Web 入口網站

建立入口網站後，您可以登入 WorkSpaces 安全瀏覽器端點，以使用者的方式瀏覽連線的網站。

如果您已在 the section called “設定身分提供者” 中完成這些步驟，可跳過本部分並且前往 步驟 3：分發您的 Web 入口網站。

1. 開啟 WorkSpaces 安全瀏覽器主控台，網址為 https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇WorkSpaces 安全瀏覽器，Web 門戶，選擇您的門戶，然後選擇查看詳細信息
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 認證。
5. 當您看到 [正在準備工作階段] 頁面時，表示您的 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。

步驟 3：分發您的 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散佈入口網站：

- 將入口網站新增至 SAML 應用程式閘道，讓使用者能夠直接從其 IdP 啟動工作階段。您可以透過 IdP 起始的登入流程，以及符合 SAML 2.0 標準的 IdP 來執行此操作。如需詳細資訊，請參閱中的 SP 起始和 IdP 起始的 SAML 宣告。the section called “設定標準驗證類型”或者，您也可以建立自訂 SAML 應用程式，透過使用 SP 起始的流程提供 IdP 起始的驗證體驗。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。

後續步驟

建立第一個 Web 入口網站後，您可以隨時檢視詳細資訊、編輯詳細資訊或刪除 Web 入口網站。如需詳細資訊，請參閱 管理您的 Web 入口網站。

您 AWS 帳戶 可以在每個可用 WorkSpaces 安全瀏覽器的 AWS 區域 地方創建一個門戶網站。每個 Web 入口網站可隨時支援多達 25 個使用者連線。若要增加可在區域中建立的入口網站數量，或為入口網站支援更多同時發生的工作階段，請參閱 the section called “管理入口網站的服務配額”。

管理您的 Web 入口網站

設定好 Web 入口網站後，您可以檢視或編輯其詳細資訊，也可以刪除不再需要使用的入口網站。

主題

- 檢視 Web 入口網站詳細資訊
- 編輯 Web 入口網站
- 刪除 Web 入口網站
- 管理入口網站的服務配額
- 控制重新驗證 SAML IdP 權杖的間隔
- 設定使用者存取日誌記錄
- 設定或編輯瀏覽器政策
- 設定輸入法編輯器 (IME)
- 設定工作階段內本地化
- 設定 IP 存取控制 (選用)
- 啟用單一登入擴充功能 (選用)
- 設定網址過濾
- 允許深層連結 (選擇性)

檢視 Web 入口網站詳細資訊

檢視 Web 入口網站詳細資訊

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

編輯 Web 入口網站

若要編輯 Web 入口網站

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

2. 選擇 [WorkSpaces 安全瀏覽器]、[入口網站]、選擇您的入口網站，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。

刪除 Web 入口網站

刪除 Web 入口網站

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

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。系統管理員必須注意兩個配額，這兩個配額可能需要增加才能支援其使用案例。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目。您可以從 AWS 主控台的 [Service Quotas] 頁面要求增加這些配額。

下表列出預設服務配額限制。

AWS 區域 依帳戶內的預設配額	Value
Web 入口網站	3
最大並行工作階段數-標準。一般	25
最大並行工作階段數-標準。大	10
同時工作階段數目上限-標準 .xlarge	5

> **Important**
>
> 服務配額一次只會影響一個 AWS 區域 配額。您必須在每個需要更多資源的 AWS 區域 地方申請增加服務配額。如需詳細資訊，請參閱 Amazon WorkSpaces 安全瀏覽器端點和配額。

請求增加服務配額

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。

要求增加入口網站

入口網站是服務的基本資源。每個入口網站都是您的 SAML 2.0 身分識別提供者與您與網際網路的網路連線以及任何私人網頁內容之間的關聯。每個入口網站都可以有個別的入口網站瀏覽器原則和使用者設定，因此管理員通常會在同一地區建立多個入口網站，以處理不同的使用案例 例如，您可以向 A 組提供具有限制性政策的特定網站的訪問權限（例如，禁用剪貼板和文件傳輸），而 B 組可以在沒有 URL 過濾的情況下訪問一般互聯網。您可以在任何支援的情況下建立入口網站 AWS 區域。若要檢視目前的服務可用性，請參閱 AWS 服務 (按區域)。

請求增加服務配額

1. 在您想要的地區開啟「Service Quotas」頁面。
2. 選擇入口網站的數目。

3. 選擇「在帳戶層級要求提高」。
4. 在 [增加配額值] 底下，輸入您希望配額設為的總金額。

要求最大並行工作階段增加

同時工作階段配額上限是可同時連線至入口網站的最高使用者數量。如果未正確設定最大並行工作階段的服務配額限制，使用者可能會發現工作階段在登入時無法使用。除了增加此服務配額之外，客戶還必須確保其 VPC 和子網路擁有足夠的 IP 空間，以支援最大的同時工作階段。

若要求最大並行階段作業增加

1. 在您想要的地區開啟「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同時工作階段數目上限。
3. 選擇「在帳戶層級要求提高」。
4. 在 [增加配額值] 底下，輸入您希望配額設為的總金額。

> **Note**
>
> 對於大量或緊急增加，請前往您的 Service Quotas 歷史記錄頁面，選取要求狀態欄中的連結，連結至您的支援案例，然後新增回覆，其中包含有關您使用案例和/或緊急程度的詳細資訊。這項資訊可協助服務團隊排定要求的優先順序，並確保為您的帳戶分配足夠的容量。

限制範例

例如，假設系統管理員在美國東部 (維吉尼亞北部) 為 125 位使用者設定兩個入口網站。在建立入口網站之前，系統管理員會識別第一個入口網站 (入口網站 A) 將支援 100 位使用者。在測試這些使用者的工作流程時，系統管理員會判斷他們需要 XL 執行個體類型，以支援工作階段期間的音訊和視訊串流。第二個入口網站 (入口網站 B) 最多可供 25 位使用者使用，才能支援存取客戶 VPC 中託管的單一靜態網頁。測試此使用案例時，系統管理員會判斷標準執行個體類型是否可支援此使用案例。

對於入口網站 A，系統管理員必須提交服務配額增加要求，將 XL 執行個體的限制從預設區域 (即 5) 提高到 100。完成後，系統管理員可以編輯入口網站來配置容量。對於入口網站 B，管理員可以在不要求增加配額的情況下繼續前進 (也就是說，標準執行個體類型的區域預設配額為 25)。

管理服務配額

若要隨時檢視每個區域分配給您帳戶的 Service Quotas，請參閱服務配額頁面。

其他服務配額

您可以檢視並要求增加「Service Quotas」頁面上列出的其他配額。實際上，大多數客戶會發現沒有必要要求提高這些限制。這些配額大致分為兩種類型：「數量」和「費率」。

針對數量配額，當您提交 Web 入口網站數目的服務配額增加時，您會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，如果您要求將入口網站從 3 增加到 5，瀏覽器和使用者設定的服務配額將自動從 3 增加到 5。您可以根據需要選擇重複使用或創建新的子資源。

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比率的使用案例。例如，系統管理員可能想要增加瀏覽器設定數目，以測試其他入口網站組態。這些服務配額請求將被審核並完成 case-by-case 基礎上。

對於費率配額，不論帳戶入口網站的限制為何，都不需要調整「Service Quotas」中公開的速率限制。

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。

如果使用者擁有有效的 SAML IdP 權杖，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。這些值可控制使用者上次互動與 WorkSpaces 安全瀏覽器工作階段因閒置而結束之間的時間長度。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 “步驟 1：建立 Web 入口網站” 中的步驟 5。

> **Note**
>
> 如果使用者的工作階段逾時，但使用者仍然擁有有效的 SAML IdP 權杖，則無需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。

設定使用者存取日誌記錄

您可以設定使用者存取日誌記錄，以記錄下列使用者事件：

- 工作階段開始-標記 WorkSpaces 安全瀏覽器工作階段的開始。
- 工作階段結束-標記 WorkSpaces 安全瀏覽器工作階段的結束。
- URL 導覽 – 記錄使用者載入的 URL。

> **Note**
>
> 從瀏覽器歷程記錄記錄 URL 導航日誌。未記錄在瀏覽器歷程記錄中的 URL (以無痕模式造訪或從瀏覽器歷程記錄中刪除) 不會記錄在日誌中。客戶可以決定是否使用瀏覽器政策關閉無痕模式或是刪除歷程記錄。

此外，每個事件還包括以下資訊：

- Event time (事件時間)
- 使用者名稱
- Web 入口網站 ARN

客戶有責任瞭解使用 WorkSpaces 安全瀏覽器時所產生的潛在法律問題，並確保其使用 WorkSpaces 安全瀏覽器符合所有適用的法律和法規。其中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。

在 WorkSpaces 安全瀏覽器入口網站上啟用使用者存取日誌可能會產生 Amazon Kinesis Data Streams 的費用。如需定價的詳細資訊，請參閱 Amazon Kinesis Data Streams 定價。

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 Stream 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？。

> **Note**
>
> 若要從 WorkSpaces 安全瀏覽器接收日誌，您必須擁有以「amazon-workspaces-web-*」開頭的 Amazon Kinesis 資料串流。您的 Amazon Kinesis 資料串流必須關閉伺服器端加密，或者必須用 AWS 受管金鑰 於伺服器端加密。
> 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？。

範例日誌

以下是每個可用事件的範例，包括驗證StartSessionVisitPage、、和EndSession。

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"
}
```

設定或編輯瀏覽器政策

透過 WorkSpaces 安全瀏覽器，您可以使用適用於最新穩定版本的 Chrome 政策，設定自訂瀏覽器政策。您可以在 Web 入口網站套用 300 多項政策。如需詳細資訊，請參閱 the section called “設定自訂瀏覽器政策 (範例)” 和 Chrome Enterprise 政策清單。

使用主控台檢視畫面來建立 Web 入口網站，您可以套用以下政策：

- StartURL
- 書籤和書籤資料夾
- 開啟和關閉隱私瀏覽
- 刪除歷程記錄
- 使用 AllowURL 和 BlockURL 篩選 URL

如需有關使用主控台來檢視政策的資訊，請參閱 開始使用 WorkSpaces 安全瀏覽器。

WorkSpaces Secure Browser 會將基準瀏覽器原則組態套用至所有入口網站，以及您指定的任何原則。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

- 設定自訂瀏覽器政策 (範例)
- 編輯基準瀏覽器政策

設定自訂瀏覽器政策 (範例)

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。

在下例中，您可以建立具有下列政策控制項目的 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
- 步驟 2：收集政策
- 步驟 3：建立自訂的 JSON 政策檔案
- 步驟 4：將政策加入範本
- 步驟 5：將您的政策 JSON 檔案上傳到您的 Web 入口網站

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 “步驟 1：建立 Web 入口網站”。

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— 在瀏覽器啟動時安裝擴充功能。
   - 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— 將書籤新增至網頁。
   - RestoreOnStartupURL — 設定每當啟動新的瀏覽器視窗時，要開啟哪些網頁。
   - AllowDeletingBrowserHistory— 配置用戶是否可以刪除其瀏覽歷史記錄。
   - IncognitoModeAvailability— 配置用戶是否可以訪問隱身模式。

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. 開啟 WorkSpaces 安全瀏覽器主控台，位於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。

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原則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。

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`。
- 可以使用主控台檢視 URL 篩選功能或 JSON 上傳來擴充 `URLAllowlist` 和 `URLBlocklist` 政策。不過無法覆寫基準線 URL。從您的 Web 入口網站下載的 JSON 檔案中看不到這些政策。不過，如果您在工作階段期間有造訪過「chrome://policy」，遠端瀏覽器會顯示套用的政策。

設定輸入法編輯器 (IME)

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 依預設，安全瀏覽器工作階段包含 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 IME
  - 若要向前循環 IME (或向右移動鍵盤配置)，請按 Shift+Control+Left Alt。
- 日文
  - 要選擇平假名，請按 F6。
  - 要選擇片假名，請按 F7。

- 若要選擇 Latin，請按 F10。
- 若要選擇 Wide Latin，請按 F9。
- 要選擇直接輸入，請按 ALT +、ALT + @、全寬半寬。

- 韓文
  - 若要選擇韓文，請按 Shift+Space。
  - 若要選擇漢字，請按 F9。

若要移除 IME 工具列和功能表，或從 WorkSpaces 安全瀏覽器工作階段關閉螢幕鍵盤，請連絡 AWS Support。

設定工作階段內本地化

當使用者啟動工作階段時， WorkSpaces Secure Browser 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。

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)
- Chinese
  - zh – 中文
  - zh-CN – 中文 (中國)
  - zh-HK – 中文 (香港)
  - zh-TW – 中文 (台灣)

按以下優先順序確定工作階段語言：

1. 入口網站瀏覽器設定中的ForcedLanguages原則。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

若要設定使用者的本機端瀏覽器設定，請執行下列其中一項操作：

- 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。

設定 IP 存取控制 (選用)

WorkSpaces 安全瀏覽器允許您控制您的門戶網站可以從哪些 IP 地址訪問。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。

默認情況下， WorkSpaces 安全瀏覽器允許用戶從任何地方訪問他們的門戶網站。IP 存取控制群組充當虛擬防火牆，篩選使用者可用來連線至 Web 入口網站的 IP 地址。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。一旦連接， WorkSpaces 安全瀏覽器會持續監控用戶的 IP 地址，以確保他們從受信任的網絡保持連接。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**
>
> 客戶有責任瞭解其使用 WorkSpaces 安全瀏覽器時所產生的潛在法律問題，並確保其使用 WorkSpaces 安全瀏覽器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。

建立 IP 存取控制群組

請按照下列步驟來建立 IP 存取控制群組。

1. 開啟 WorkSpaces 安全瀏覽器主控台，位於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 Web 入口網站建立關聯

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. 開啟 WorkSpaces 安全瀏覽器主控台，位於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 “進行入口網站設定” 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。

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. 開啟 WorkSpaces 安全瀏覽器主控台，位於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。

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. 開啟 WorkSpaces 安全瀏覽器主控台，位於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。

啟用單一登入擴充功能 (選用)

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。

當使用者登入入口網站時，系統會提示使用者安裝擴充功能。

預設情況下，Chrome 無痕式視窗或 Firefox 私密瀏覽視窗中的擴充功能不會啟用。使用者可以手動啟用它們。如需 Chrome 的詳細資訊，請參閱無痕模式下的擴充功能。如需 Firefox 的詳細資訊，請參閱隱私瀏覽中的擴充套件。

您可以更新入口網站現有的使用者設定組態，或是在第一次建立 Web 入口網站時更新。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。

您有責任測試和識別要同步的 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。

若要查看哪些網域搭配最常見的 IdP 使用，請參閱下表：

IdP 和網域

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

接下來，在主控台中造訪您的入口網站。然後允許擴充功能，並加入應同步哪些網域的 cookie。請依照下列步驟建立允許使用擴充功能的新入口網站，或是更新現有入口網站。

若要在建立新的 Web 入口網站時允許擴充功能，請依照下列步驟執行：

1. 請按照 the section called “步驟 1：建立 Web 入口網站” 中的步驟操作，直到到達 the section called “進行使用者設定” 為止。
2. 針對 the section called “進行使用者設定” 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 “進行使用者設定” 中的步驟和 the section called “步驟 1：建立 Web 入口網站” 的其餘部分，以建立您的 Web 入口網站。

請依照下列步驟執行，以將擴充功能加入現有的 Web 入口網站：

1. 開啟 WorkSpaces 安全瀏覽器主控台，網址為 https://console.aws.amazon.com/workspaces-web/home。
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。

請依照下列步驟編輯網域或移除擴充功能：

1. 開啟 WorkSpaces 安全瀏覽器主控台，網址為 https://console.aws.amazon.com/workspaces-web/home。
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. 一旦移除，工作階段將不再同步 Cookie，即使使用者在其瀏覽器中安裝了 WorkSpaces 安全瀏覽器延伸功能也是如此。

如需有關擴充功能使用者體驗的詳細資訊，請參閱 the section called “單一登入擴充功能”。

設定網址過濾

您可以使用 Chrome 政策來篩選使用者可從遠端瀏覽器存取哪些網址。Chrome 政策提供了兩種過濾網址的機制：URL 允許列表和網址阻止列表。您可以使用 WorkSpaces Secure Browser 主控台介面將 URL 篩選設定為入口網站設定，也可以將其新增為自訂 JSON 陳述式的一部分 (無論是在內嵌編輯器中，或作為 JSON 檔案上傳)。

使用主控台設定 URL 篩選

1. 開啟 WorkSpaces 安全瀏覽器主控台，位於https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 選擇 [WorkSpaces 安全瀏覽器]、[入口網站]、選擇您的入口網站，然後選擇 [檢視詳細資料
3. 對於 URL 篩選，請從下列選項中選擇：

   - 允許存取所有 URL：預設情況下，入口網站允許存取所有 URL。您可以將特定網站新增至 BlockURL 清單，以防止使用者在工作階段期間造訪這些網站。例如，將 www.anycorp.com 添加到塊 URL 列表將阻止用戶在其會話期間導航到 www.anycorp.com。
   - 封鎖對所有 URL 的存取：根據預設，入口網站會封鎖對所有 URL 的存取。您可以將特定網站新增至 URL 允許清單，以組織使用者可以造訪的網站清單，並封鎖任何其他網站的流量。請考慮將每個 URL 新增為書籤，以便在使用者工作階段期間啟用一鍵式存取權限。
   - 進階設定：選擇此選項可 parallel 時建立 AllowURL 和區塊 URL 清單。URL 允許清單的優先順序高於 URL 封鎖清單。此選項會依路徑啟用 URL 篩選。例如，您可以將 www.anycorp.com 新增至封鎖清單，然後將網站新增至允許清單。這允許用戶訪問我們的網址，但是他們將無法訪問其他網址路徑，例如網址。

如需使用封鎖和允許 URL 的詳細指引，請參閱允許或封鎖存取網站。按照 Chrome 的阻止列表過濾器格式將網址添加到這些列表中，以獲得最佳結果。如需詳細資訊，請參閱 URL 封鎖清單篩選格式。

使用 JSON 編輯器或檔案上傳設定 URL 篩選

1. 在 [原則設定] 模組中，選擇 [JSON 編輯器]，並略過 [編輯器] 或 [檔案上傳] 檢視的主控台 UI 模組。
   - 編輯器可讓客戶在主控台內嵌建立自訂政策陳述式。編輯器在策略創建期間突出顯示 JSON 語句中的錯誤。
   - 檔案上傳功能可讓客戶新增在主控台外建立的 JSON 檔案 (例如從現有的 Chrome 瀏覽器匯出)。
2. 請參閱 Chrome 政策詳細資料，瞭解 URL 允許清單和 URL 封鎖清單，以正確格式化入口網站的允許/拒絕 URL 清單。如需詳細資訊，請參閱 URL 允許清單和 URL 封鎖清單。

允許深層連結 (選擇性)

當使用者登入 WorkSpaces 安全瀏覽器時，他們會在系統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，以便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。連結會顯示在設定為工作階段開始的首頁旁邊，或者如果工作階段已在進行中，則會顯示該連結本身。此功能允許管理員使用 WorkSpaces 安全瀏覽器創建更加動態的用戶體驗。若要允許深層連結的權限，請在建立使用者設定時選擇「允許」。如需詳細資訊，請參閱 the section called “進行使用者設定”。

深層連結會在 WorkSpaces 安全瀏覽器工作階段中開啟頁面。如果會話已經在運行，它將在新選項卡中打開深層鏈接。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，而入口網站預設首頁則會在另一個索引標籤中開啟。如果深層連結包含一個以上的 URL，它將首先顯示在焦點中列出的深層連結 URL，每個後續 URL (包括預設首頁) 都會在不同的索引標籤中開啟。

深層連結必須符合下列要求：

- 入口網站的深層連結權限必須設定為 [允許]。如需詳細資訊，請參閱 the section called “進行使用者設定”。
- 您想要深層連結的網站必須經過 URL 編碼。例如，若要將某個使用者連結至「https://www.example.com/?query=true」，請將連結更新至網址。
- 以下列格式將 URL 附加至允許列出的入口網站 URL，其中 UUID 是入口網站識別碼：

  HTTP://<uuid>. 工作空間-網站深層連結 = 網址 %3A%2F%2FFF

- 深層連結最多可包含 10 個以逗號劃定的 URL。例如：

  HTTPS://<uuid>. 工作空間網站網站深層連結 = 網址 %3A%2F%2FFF 網站範例 .2F%3F 查詢 %3D 真實, 網站 %3A%2fFLE 範例 2fPLE 查詢 %3dtrue3, 網址 %3A%2F%2F%2fF% 3 查詢 %3Dtrue4

如果您可以從入口網站存取該網域，而不是在 URL 封鎖清單中存取該網域，則您與之共用此入口網站連結的任何使用者都可以操控深層連結值以造訪網站。若要建立限制允許清單或封鎖清單，以防止使用者透過您的入口網站造訪非預期的網域，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。如需詳細資訊，請參閱the section called “設定網址過濾”和允許或封鎖存取網站。

Amazon 安 WorkSpaces 全瀏覽器的安全

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。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 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。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 服務範圍內的合規計劃 。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 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。它說明如何設定 Amazon 安 WorkSpaces 全瀏覽器，以符合您的安全和合規目標。您也會學到如何使用其他可 AWS 協助您監控和保護 Amazon 安 WorkSpaces 全瀏覽器資源的服務。

目錄

- Amazon WorkSpaces 安全瀏覽器的數據保護
- Amazon WorkSpaces 安全瀏覽器的 Identity and Access Management
- Amazon WorkSpaces 安全瀏覽器中的事件回應
- Amazon WorkSpaces 安全瀏覽器的合規驗證
- Amazon WorkSpaces 安全瀏覽器的彈性
- Amazon 安 WorkSpaces 全瀏覽器的基礎設施安全
- Amazon WorkSpaces 安全瀏覽器中的配置和漏洞分析
- Amazon 安 WorkSpaces 全瀏覽器的安全最佳實踐

Amazon WorkSpaces 安全瀏覽器的數據保護

AWS 共同責任模型適用於 Amazon WorkSpaces 安全瀏覽器中的資料保護。如此模型中所述， AWS 負責保護執行所有 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。如需有關資料隱私權的詳細資訊，請參閱資料隱私權FAQ。 如需歐洲資料保護的相關資訊，請參閱AWS 安全性GDPR部落格上的AWS 共同責任模型和部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 認證並設定個別使用者。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：

- 對每個帳戶使用多重要素驗證 (MFA)。
- 使用SSL/TLS與 AWS 資源溝通。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 使用設定API和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 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 AWS 透過命令列介面或存取時需要 FIPS 140-3 驗證的密碼編譯模組API，請使用端點。FIPS 如需有關可用FIPS端點的詳細資訊，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 安全瀏覽器或其他 AWS 服務 使用主控台API、AWS CLI、或時 AWS SDKs。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URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

資料加密

Amazon WorkSpaces Secure Browser 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、身分識別提供者資訊、信任存放區資料和信任存放區憑證資料。 WorkSpaces Secure Browser 也會收集瀏覽器原則資料、使用者偏好設定 (針對瀏覽器設定) 和工作階段記錄。收集到的資料會存放在 Amazon DynamoDB 和 Amazon S3 中。 WorkSpaces 安全瀏覽器用 AWS Key Management Service 於加密。

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「完整存取權」角色或「唯讀」角色。如需詳細資訊，請參閱AWS WorkSpaces 安全瀏覽器的受管理政策。
- 透過提供客戶管理的金鑰來保護端對端資料，因此 WorkSpaces Secure Browser 可以使用您提供的金鑰來加密靜態資料。
- 請謹慎共享入口網域和使用者憑證：
  - 管理員必須登入 Amazon 主 WorkSpaces 控台，且使用者必須登入 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 安全瀏覽器默認情況下，通過加密所有敏感數據來保護內容和元數據。 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 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。

靜態加密

預設為靜態加密。 WorkSpaces 安全瀏覽器中使用的客戶特定數據使 AWS KMS用加密。 WorkSpaces 安全瀏覽器為您建立的資源提供靜態加密。此服務會在資源建立時接受 AWS KMS 客戶管理金鑰，如果未提供，則會使用 AWS 擁有的金鑰來加密靜態資源。此服務會加密您可以提供的瀏覽器政策文件，以自訂瀏覽器工作階段、身分提供者組態設定，以及入口網站的顯示名稱。這些資訊將使用客戶管理金鑰或 AWS 擁有的金鑰保持加密，同時儲存在我們的後端。

您可以決定建立 WorkSpaces 安全瀏覽器資源時要使用的金鑰。如果屬於該資源一部分的資料已加密，則 WorkSpaces 安全瀏覽器會接受該`customerManagedKeyArn`欄位做為的一部分`createAPI`。提供的金鑰必須是對稱 AWS KMS 金鑰，而使用此金鑰建立資源的管理員必須具有 `kms:Decrypt`、`kms:GenerateDataKey` 和 `kms:CreateGrant` 許可。使用金鑰建立資源之後，即無法移除或變更金鑰。如果您使用客戶自管金鑰，則存取資源的管理員必須具有 `kms:Decrypt` 和 `kms:GenerateDataKey` 許可。如果您在使用主控台時看到有關拒絕存取的錯誤訊息，請確定使用主控台的使用者具有所使用之金鑰的這些許可。

您可以透過檢查 AWS KMS 授權的狀態來疑難排解和稽核金鑰使用情況。如需詳細資訊，請參閱在管理授權。在入口網站建立期間， WorkSpaces 安全瀏覽器會建立授權，以允許服務以非同步方式存取金鑰。您可以檢查授權與使用授權時提供的加密內容來檢查金鑰使用狀態。加密內容一律包含有金鑰 `aws:workspaces-web:portal:id` 的項目，以及等於入口網站 ID 的值。對於其他資源，加密內容永遠包含格式 `aws:workspaces-web:`*`RESOURCE_TYPE`*`:id` 的項目和對應的資源 ID。

傳輸中加密

WorkSpaces 安全瀏覽器會加密傳輸中HTTPS和 TLS 1.2 的資料。您可以使用主控台或直接API呼叫傳送要求至 WorkSpaces 。傳輸的要求資料會透過HTTPS或TLS連線傳送所有資料來加密。請求數據可以從 AWS 控制台傳輸 AWS Command Line Interface，或傳輸 AWS SDK到 WorkSpaces 安全瀏覽器。

依預設會設定傳輸中的加密，並且預設會設定安全連線 (HTTPS、TLS)。

金鑰管理

您可以提供自己的客戶管理 AWS KMS 金鑰來加密您的客戶資訊。如果您沒有提供一個，WorkSpaces 安全瀏覽器將使用 AWS 擁有的密鑰。您可以使用設定金鑰 AWS SDK。

網際網路流量隱私權

若要保護安 WorkSpaces 全瀏覽器與內部部署應用程式之間的連線，您可以使用 WorkSpaces 安全瀏覽器在自己VPC的內部啟動瀏覽器工作階段 與內部部署應用程式的連線是由您自己設定的VPC，不受 WorkSpaces 安全瀏覽器控制。

為了保護帳戶之間的連接， WorkSpaces Secure Browser 使用服務鏈接角色安全地連接到客戶帳戶並代表客戶執行操作。如需詳細資訊，請參閱針對安全瀏覽器使用服務 WorkSpaces 連結角色。

使用者存取日誌記錄

系統管理員可以記錄 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。使用者存取記錄中的瀏覽資訊不會由儲存 AWS，也不會儲存在未設定記錄的工作階段中存取。URL使用者存取記錄不會記錄在無痕模式下的造訪，或URLs從瀏覽器歷程記錄中刪除的造訪。

Amazon WorkSpaces 安全瀏覽器的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM管理員控制誰可以驗證（登錄）和授權（有權限）使用 WorkSpaces 安全瀏覽器資源。IAM 是一種您 AWS 服務 可以使用，無需額外費用。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- Amazon 安 WorkSpaces 全瀏覽器如何使用 IAM
- Amazon WorkSpaces 安全瀏覽器的基於身份的政策示例
- AWS WorkSpaces 安全瀏覽器的受管理政策

- 疑難排解 Amazon WorkSpaces 安全瀏覽器身分和存取
- 針對安全瀏覽器使用服務 WorkSpaces 連結角色

物件

根據您在 WorkSpaces 安全瀏覽器中執行的工作，使用方式 AWS Identity and Access Management (IAM) 會有所不同。

服務使用者 — 如果您使用 WorkSpaces 安全瀏覽器服務來完成工作，則管理員會為您提供所需的認證和權限。當您使用更多 WorkSpaces 安全瀏覽器功能來完成工作時，您可能需要額外的權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法在 WorkSpaces 安全瀏覽器中存取某項功能，請參閱疑難排解 Amazon WorkSpaces 安全瀏覽器身分和存取。

服務管理員 — 如果您負責公司的 WorkSpaces 安全瀏覽器資源，您可能擁有 WorkSpaces 安全瀏覽器的完整存取權。決定您的服務使用者應存取哪些 WorkSpaces 安全瀏覽器功能和資源是您的工作。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要深入瞭解貴公司如何IAM搭配 WorkSpaces 安全瀏覽器使用，請參閱Amazon 安 WorkSpaces 全瀏覽器如何使用 IAM。

IAM系統管理員 — 如果您是IAM系統管理員，您可能想要瞭解如何撰寫原則以管理 WorkSpaces 安全瀏覽器存取權的詳細資訊。若要檢視可在中使用的 WorkSpaces 安全瀏覽器身分型原則範例IAM，請參閱。Amazon WorkSpaces 安全瀏覽器的基於身份的政策示例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以IAM使用者身分或假設IAM角色來驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以密碼編譯方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署要求的詳細資訊，請參閱使用IAM者指南中的簽署 AWS API要求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。若要深入瞭解，請參閱使用AWS IAM Identity Center 者指南中的多重要素驗證和使用多重要素驗證 (MFA) AWS的使用IAM者指南。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步至您自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需IAM身分識別中心的相關資訊，請參閱IAM識別中心是什麼？在《AWS IAM Identity Center 使用者指南》中。

IAM 使用者和群組

IAM使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為的群組，IAMAdmins並授與該群組管理IAM資源的權限。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM角色

IAM角色是您 AWS 帳戶 中具有特定權限的身份。它類似於用IAM戶，但不與特定人員相關聯。您可以 AWS Management Console 透過切換角色來暫時擔任中的角色。IAM您可以透過呼叫 AWS CLI 或 AWS API作業或使用自訂來擔任角色URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時IAM使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (受信任的主體) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或將物件存放在 Amazon S3 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色執行中的動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。
  - 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。
- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行的應用程式以及發出 AWS CLI 或 AWS API請求的臨時登入資料。這比在EC2執行個體中儲存存取金鑰更可

取。若要將 AWS 角色指派給EC2執行個體並讓其所有應用程式都能使用，請建立附加至執行個體的執行個體設定檔。執行個體設定檔包含角色，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以JSON文件的形式儲存在中。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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。

預設情況下，使用者和角色沒有許可。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或取得角色資訊 AWS API。

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。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。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的策略IAM中使用 AWS 受管政策。

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3 和 Amazon VPC 是支持服務的示例ACLs。 AWS WAF若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略 (SCPs) — SCPs 是指定中組織或組織單位 (OU) 最大權限的JSON策略 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個帳戶 AWS 帳戶根使用者。如需有關 Organizations 的詳細資訊SCPs，請參閱AWS Organizations 使用指南中的服務控制原則。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱《IAM使用指南》中的工作階段原則。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要瞭解如何在涉及多個原則類型時 AWS 決定是否允許要求，請參閱IAM使用指南中的原則評估邏輯。

Amazon 安 WorkSpaces 全瀏覽器如何使用 IAM

在您用IAM來管理 WorkSpaces 安全瀏覽器的存取權限之前，請先了解 WorkSpaces 安全瀏覽器可使用哪些IAM功能。

IAM您可以使用 Amazon WorkSpaces 安全瀏覽器的功能

IAM特徵	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
ACLs	否
ABAC(策略中的標籤)	部分
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	是

若要取得 WorkSpaces 安全瀏覽器和其他 AWS 服務如何搭配大部分IAM功能運作的高階檢視，請參閱IAM使用者指南IAM中的適用AWS 服務。

安全瀏覽器的基於身份的 WorkSpaces 策略

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。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。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

安全瀏覽器的基於身份的策略示例 WorkSpaces

若要檢視 WorkSpaces 安全瀏覽器以身分識別為基礎的原則範例，請參閱。Amazon WorkSpaces 安全瀏覽器的基於身份的政策示例

WorkSpaces 安全瀏覽器中的資源型政策

支援資源型政策：否

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者和資源不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。

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策略來指定誰可以存取什麼內容。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策略Action元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯的 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

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 安全瀏覽器動作清單，請參閱服務授權參考中由 Amazon WorkSpaces 安全瀏覽器定義的動作。

WorkSpaces 安全瀏覽器中的原則動作會在動作之前使用下列前置詞：

```
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 安全瀏覽器以身分識別為基礎的原則範例，請參閱。Amazon WorkSpaces 安全瀏覽器的基於身份的政策示例

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策略來指定誰可以存取什麼內容。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。

ResourceJSON原則元素會指定要套用動作的一個或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (ARN) 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示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清單ARNs，請參閱服務授權參考中由 Amazon WorkSpaces 安全瀏覽器定義的資源。若要了解您可以針對每個資源指定哪些動作，請參閱 Amazon WorkSpaces 安全瀏覽器定義ARN的動作。

若要檢視 WorkSpaces 安全瀏覽器以身分識別為基礎的原則範例，請參閱。Amazon WorkSpaces 安全瀏覽器的基於身份的政策示例

WorkSpaces 安全瀏覽器的政策條件金鑰

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。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。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》中的IAM政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

若要查看 WorkSpaces 安全瀏覽器條件金鑰清單，請參閱服務授權參考中的 Amazon WorkSpaces 安全瀏覽器的條件金鑰。若要了解可以使用條件金鑰的動作和資源，請參閱 Amazon WorkSpaces 安全瀏覽器定義的動作。

若要檢視 WorkSpaces 安全瀏覽器以身分識別為基礎的原則範例，請參閱。Amazon WorkSpaces 安全瀏覽器的基於身份的政策示例

WorkSpaces 安全瀏覽器中的存取控制清單 (ACLs)

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

基於屬性的訪問控制（ABAC）與 WorkSpaces 安全瀏覽器

支援 ABAC (策略中的標籤): 部分

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。在中 AWS，這些屬性稱為標籤。您可以將標籤附加至IAM實體 (使用者或角色) 和許多 AWS 資源。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤與他們嘗試存取的資源上的標籤相符時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則管理變得繁瑣的情況。

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。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

搭配 WorkSpaces 安全瀏覽器使用臨時憑證

支援臨時憑證：是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配使用 AWS 服務 ，請參閱《IAM使用指南》IAM中的使用方式。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立臨時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM使用者指南》中的〈切換到角色 (主控台)〉。

您可以使用 AWS CLI 或手動建立臨時認證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS。 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。

WorkSpaces 安全瀏覽器的跨服務主體權限

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色在中執行動作時 AWS，您會被視為主參與者。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS會使用主參與者呼叫的權限 AWS 服務，並結

合要求 AWS 服務 向下游服務發出要求。FAS只有當服務收到需要與其他 AWS 服務 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

WorkSpaces 安全瀏覽器的服務角色

支援服務角色：否

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色 IAM。如需詳細資訊，請參閱《IAM使用指南》 AWS 服務中的建立角色以將權限委派給

> **Warning**
>
> 變更服務角色的權限可能會中斷 WorkSpaces 安全瀏覽器的功能。只有當 WorkSpaces 安全瀏覽器提供指引時，才編輯服務角色。

安全瀏覽器的服務 WorkSpaces 連結角色

支援服務連結角色：是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需有關建立或管理服務連結角色的詳細資訊，請參閱使用IAM的AWS 服務。在表格中尋找服務，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 安全瀏覽器的基於身份的政策示例

根據預設，使用者和角色沒有建立或修改 WorkSpaces 安全瀏覽器資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或執行工作 AWS API。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

若要瞭解如何使用這些範例原則文件來建立以IAM身分識別為基礎的JSON策略，請參閱使用指南中的IAM建立IAM策略。

有關 WorkSpaces 安全瀏覽器定義的動作和資源類型的詳細資訊，包括每種資源類型的格式，請參閱服務授權參考中的 Amazon WorkSpaces Secure Browser 的動作、資源和條件金鑰。ARNs

主題

- 政策最佳實務
- 使用 WorkSpaces 安全瀏覽器主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

以身分識別為基礎的原則會決定使用者是否可以在您的帳戶中建立、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 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您的使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，請參閱AWS 《IAM使用指南》中針對工作職能的AWS 受管理策略或受管理的策略。
- 套用最低權限權限 — 當您使用原則設定權限時，IAM只授與執行工作所需的權限。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。如需有關使用套用權限IAM的詳細資訊，請參閱《使用指南》IAM中的IAM《策略與權限》。
- 使用IAM策略中的條件進一步限制存取 — 您可以在策略中新增條件，以限制對動作和資源的存取。例如，您可以撰寫政策條件，以指定必須使用傳送所有要求SSL。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱《IAM使用指南》中的IAMJSON策略元素：條件。
- 使用 IAM Access Analyzer 驗證您的原IAM則，以確保安全和功能性的權限 — IAM Access Analyzer會驗證新的和現有的原則，以便原則遵循IAM原則語言 (JSON) 和IAM最佳做法。IAMAccess Analyzer 提供超過 100 項原則檢查和可行的建議，協助您撰寫安全且功能正常的原則。如需詳細資訊，請參閱IAM使IAM用指南中的存取分析器原則驗證。
- 需要多因素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟以取得額外MFA的安全性。若要在呼叫API作業MFA時需要，請在原則中新增MFA條件。如需詳細資訊，請參閱《IAM使用指南》中的 < 設定MFA受保護的API存取 >。

如需有關中最佳作法的詳細資訊IAM，請參閱《IAM使用指南》IAM中的「安全性最佳作法」。

使用 WorkSpaces 安全瀏覽器主控台

若要存取 Amazon WorkSpaces 安全瀏覽器主控台，您必須擁有最少一組許可。這些權限必須允許您列出和檢視有關 AWS 帳戶. WorkSpaces 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。

您不需要為只對 AWS CLI 或撥打電話的使用者允許最低主控台權限 AWS API。相反地，只允許存取符合他們嘗試執行之API作業的動作。

若要確保使用者和角色仍可使用 WorkSpaces 安全瀏覽器主控台，請同時將 WorkSpaces 安全瀏覽器ConsoleAccess或ReadOnly AWS 受管理的原則附加至實體。如需詳細資訊，請參閱《使用指南》中的〈將權限新增至IAM使用者〉。

允許使用者檢視他們自己的許可

此範例顯示如何建立原則，讓使IAM用者檢視附加至其使用者身分識別的內嵌和受管理原則。此原則包含在主控台上或以程式設計方式使用或完成此動作的 AWS CLI 權限 AWS API。

```
{
    "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 安全瀏覽器的受管理政策

若要新增使用者、群組和角色的權限，使用 AWS 受管理的原則比自己撰寫原則更容易。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。這些政策涵蓋常見使用案例，並可在您的 AWS 帳戶中使用。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 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務有時可能會新增其他權限至受 AWS 管理的政策，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 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，`ReadOnlyAccess` AWS 受管理的策略提供對所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。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。

AWS 受管理的策略： AmazonWorkSpacesWebServiceRolePolicy

您無法將 `AmazonWorkSpacesWebServiceRolePolicy` 政策附加至 IAM 實體。此原則附加至服務連結角色，可讓 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”。

此原則授與允許存取 WorkSpaces 安全瀏覽器所使用或管理的 AWS 服務和資源的管理權限。

許可詳細資訊

此政策包含以下許可：

- workspaces-web— 允許訪問 WorkSpaces 安全瀏覽器使用或管理的 AWS 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 “設定使用者存取日誌記錄”。

```
{
    "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 受管理的策略： AmazonWorkSpacesSecureBrowserReadOnly

您可將 AmazonWorkSpacesSecureBrowserReadOnly 政策連接到 IAM 身分。

此原則會授與唯讀權限，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，提供對 WorkSpaces 安全瀏覽器及其相依性的唯讀存取。
- ec2：允許主體描述 VPC、子網路與安全群組。這會在安 WorkSpaces 全瀏覽器的 AWS 管理主控台中使用，以顯示可與服務搭配使用的 VPC、子網路和安全性群組。
- Kinesis – 允許主體取得 Kinesis 資料串流的清單。這會在 WorkSpaces 安全瀏覽器的 AWS 管理主控台中使用，以顯示可與服務搭配使用的 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 受管理的策略： AmazonWorkSpacesWebReadOnly

您可將 AmazonWorkSpacesWebReadOnly 政策連接到 IAM 身分。

此原則會授與唯讀權限，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原則，請切換至新AmazonWorkSpacesSecureBrowserReadOnly原則。

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，提供對 WorkSpaces 安全瀏覽器及其相依性的唯讀存取。
- ec2：允許主體描述 VPC、子網路與安全群組。這會在安 WorkSpaces 全瀏覽器的 AWS 管理主控台中使用，以顯示可與服務搭配使用的 VPC、子網路和安全性群組。
- Kinesis – 允許主體取得 Kinesis 資料串流的清單。這會在 WorkSpaces 安全瀏覽器的 AWS 管理主控台中使用，以顯示可與服務搭配使用的 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": "*"
        }
    ]
}
```

WorkSpaces AWS 受管理策略的安全瀏覽器更新

檢視有關 WorkSpaces 安全瀏覽器 AWS 受管理原則的詳細資料，因為此服務開始追蹤這些變更。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	日期
AmazonWorkSpacesSecureBrowserReadOnly – 新政策	WorkSpaces 安全瀏覽器新增了一項新政策，透過 AWS 管理主控台、開發套件和 CLI 提供對 WorkSpaces 安全瀏覽器及其相依性的唯讀存取。	2024年6月24日

變更	描述	日期
AmazonWorkSpacesWebServiceRolePolicy-更新的政策	WorkSpaces 安全瀏覽器更新了政策，限制 CreateNetworkInterface 使用 aws:RequestTag/WorkSpacesWebManaged: true 標記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 ENI。	2022 年 12 月 15 日
AmazonWorkSpacesWebReadOnly-更新的政策	WorkSpaces 安全瀏覽器已更新原則，以納入使用者存取記錄的讀取權限，並列出 Kinesis 資料串流。如需詳細資訊，請參閱 the section called “設定使用者存取日誌記錄”。	2022 年 11 月 2 日
AmazonWorkSpacesWebServiceRolePolicy-更新的政策	WorkSpaces 安全瀏覽器已更新政策，以說明 Kinesis 資料串流的摘要，並將記錄放入 Kinesis 資料串流中以供使用者存取記錄。如需詳細資訊，請參閱 the section called “設定使用者存取日誌記錄”。	2022 年 10 月 17 日
AmazonWorkSpacesWebServiceRolePolicy-更新的政策	WorkSpaces 安全瀏覽器更新了策略以在 ENI 創建期間創建標籤。	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/ 使用命名空間新增至 PutMetricData API 權限。	2022 年 4 月 6 日

變更	描述	日期
AmazonWorkSpacesWebReadOnly – 新政策	WorkSpaces 安全瀏覽器新增了一項新政策，透過 AWS 管理主控台、開發套件和 CLI 提供對 WorkSpaces 安全瀏覽器及其相依性的唯讀存取。	2021 年 11 月 30 日
AmazonWorkSpacesWebServiceRolePolicy – 新政策	WorkSpaces 安全瀏覽器新增了一項新政策，允許存取 WorkSpaces 安全瀏覽器所使用或管理的 AWS 服務和資源。	2021 年 11 月 30 日
WorkSpaces 安全瀏覽器開始追蹤變更	WorkSpaces 安全瀏覽器開始追蹤其 AWS 受管理政策的變更。	2021 年 11 月 30 日

疑難排解 Amazon WorkSpaces 安全瀏覽器身分和存取

使用下列資訊可協助您診斷及修正使用 WorkSpaces 安全瀏覽器和時可能會遇到的常見問題IAM。

主題

- 我沒有在 WorkSpaces 安全瀏覽器中執行操作的權限
- 我沒有授權執行 iam：PassRole
- 我想允許 AWS 帳戶以外的人員存取我的 WorkSpaces 安全瀏覽器資源

我沒有在 WorkSpaces 安全瀏覽器中執行操作的權限

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。

當使用mateojacksonIAM者嘗試使用主控台來檢視虛構*my-example-widget*資源的詳細資料，但沒有虛構的workspaces-web:*GetWidget*權限時，就會發生下列範例錯誤。

```
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 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到未授權執行iam:PassRole動作的錯誤訊息，您必須更新原則，才能讓您將角色傳遞給 WorkSpaces 安全瀏覽器。

有些 AWS 服務 允許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。

當名為的使用IAM者marymajor嘗試使用主控台在 WorkSpaces Secure Browser 中執行動作時，就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 沒有將角色傳遞至該服務的許可。

```
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 系統管理員。您的管理員提供您的簽署憑證。

我想允許 AWS 帳戶以外的人員存取我的 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。對於支援以資源為基礎的政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策授與人員存取您的資源。

如需進一步了解，請參閱以下內容：

- 若要瞭解 WorkSpaces 安全瀏覽器是否支援這些功能，請參閱Amazon 安 WorkSpaces 全瀏覽器如何使用 IAM。
- 若要瞭解如何提供您所擁有資 AWS 帳戶 源的存取權，請參閱《IAM使用指南》中的〈提供存取權給您 AWS 帳戶 所擁有的其他IAM使用者〉。
- 若要瞭解如何將您的資源存取權提供給第三方 AWS 帳戶，請參閱《IAM使用指南》中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要瞭解如何透過身分聯盟提供存取權，請參閱《使用指南》中的提供對外部驗證使用IAM者的存取權 (身分聯合)。

- 若要瞭解針對跨帳號存取使用角色與以資源為基礎的政策之間的差異，請參閱《使用IAM者指南》IAM中的〈跨帳號資源存取〉。

針對安全瀏覽器使用服務 WorkSpaces 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 Secure Browser 預先定義，並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您輕鬆設定 WorkSpaces 安全瀏覽器，因為您不需要手動新增必要的權限。WorkSpaces 安全瀏覽器會定義其服務連結角色的權限，除非另有定義，否則只有 WorkSpaces 安全瀏覽器可以擔任其角色。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。這樣可以保護您的 WorkSpaces 安全瀏覽器資源，因為您無法不小心移除存取資源的權限。

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。

WorkSpaces 安全瀏覽器的服務連結角色權限

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`

名為的角色權限原則`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。

建立安全瀏覽器的服務 WorkSpaces 連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或 AWS API 中建立第一個入口網站時 AWS CLI， 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workspaces-web.amazonaws.com服務名稱建立服務連結角色。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。

編輯安全瀏覽器的服務 WorkSpaces 連結角色

WorkSpaces 安全瀏覽器不允許您編輯AWSServiceRoleForAmazonWorkSpacesWeb服務鏈接的角色。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。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除安全瀏覽器的服務 WorkSpaces 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**
>
> 當您嘗試刪除資源時，如果 WorkSpaces 安全瀏覽器服務正在使用此角色，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。

若要刪除使用的 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 主控台或 AWS API 刪除 AWSServiceRoleForAmazonWorkSpacesWeb服務連結角色。AWS CLI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。

支援 WorkSpaces 安全瀏覽器服務連結角色的區域

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

您可以透過監控 `SessionFailure` Amazon CloudWatch 指標來偵測事件。若要接收事件警示，請使用`SessionFailure`測量結果的 CloudWatch 警示。如需更多詳細資訊，請參閱 Amazon 監控 Amazon WorkSpaces 安全瀏覽器 CloudWatch。

Amazon WorkSpaces 安全瀏覽器的合規驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()PCI) 中保護安全控制指引的最佳做法，並將其對應至安全性控制。ISO
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。

- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

Amazon WorkSpaces 安全瀏覽器的彈性

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。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 全域基礎結構。

WorkSpaces 安全瀏覽器目前不支持以下內容：

- 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 安 WorkSpaces 全瀏覽器的基礎設施安全

作為一項受管服務，Amazon 安 WorkSpaces 全瀏覽器受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的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：

- 傳輸層安全性 (TLS)。我們需要 TLS 1.2 並推薦 TLS 1.3。

- 具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與IAM主體相關聯的秘密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

WorkSpaces 安全瀏覽器通過對所有服務應用標準 AWS SIGv4 身份驗證和授權來隔離服務流量。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。

所有網際網路存取都可透過設定網路設定 (例如、子網路或安全性群組) 來控制。VPC目前不支援多租戶和VPC端點 (PrivateLink)。

Amazon WorkSpaces 安全瀏覽器中的配置和漏洞分析

WorkSpaces 安全瀏覽器更新和修補應用程式和平台需要代表您，包括 Chrome 和 Linux。您無需進行修補或重建。但是，您有責任根據規格和指南配置 WorkSpaces 安全瀏覽器，並監控用戶使用 WorkSpaces 安全瀏覽器的使用情況。所有與服務相關的配置和漏洞分析均由 WorkSpaces 安全瀏覽器負責。

您可以要求提高 WorkSpaces 安全瀏覽器資源的限制，例如入口網站的數量和使用者數量。WorkSpaces 安全瀏覽器可確保服務和 SLA 的可用性。

Amazon 安 WorkSpaces 全瀏覽器的安全最佳實踐

Amazon 安 WorkSpaces 全瀏覽器提供許多安全功能，您可以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：

- 若要偵測與您使用安 WorkSpaces 全瀏覽器相關的潛在安全事件，請使用 AWS CloudTrail 或 Amazon CloudWatch 偵測和追蹤存取歷史記錄和處理日誌。如需詳細資訊，請參閱 Amazon 監控 Amazon WorkSpaces 安全瀏覽器 CloudWatch 及 使用記錄 WorkSpaces 安全瀏覽器 API 呼叫 AWS CloudTrail。
- 要實施偵測控制並識別異常情況，請使用 CloudTrail 日誌和 CloudWatch指標。如需詳細資訊，請參閱 Amazon 監控 Amazon WorkSpaces 安全瀏覽器 CloudWatch 及 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 “設定使用者存取日誌記錄”。

為了防止與您使用安 WorkSpaces 全瀏覽器相關的潛在安全事件，請遵循以下最佳做法：

- 實作最低權限存取，並建立用於「 WorkSpaces 安全瀏覽器」動作的特定角色。使用 IAM 範本建立完整存取或唯讀角色。如需詳細資訊，請參閱 AWS WorkSpaces 安全瀏覽器的受管理政策。
- 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

監控是維持 Amazon WorkSpaces 安全瀏覽器和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。 AWS 提供下列監控工具來監視您的 WorkSpaces 安全瀏覽器入口網站及其資源、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 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 CloudWatch 追蹤 Amazon EC2 執行個體的 CPU 使用率或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- Amazon CloudWatch 日誌可讓您從 Amazon EC2 執行個體和其他來源監控 CloudTrail、存放和存取日誌檔。 CloudWatch 記錄檔可以監控記錄檔中的資訊，並在符合特定臨界值時通知您。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 日誌使用者指南。
- AWS CloudTrail擷取您帳戶或代表您 AWS 帳戶發出的 API 呼叫和相關事件，並將日誌檔傳送到您指定的 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 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

主題

- Amazon 監控 Amazon WorkSpaces 安全瀏覽器 CloudWatch
- 使用記錄 WorkSpaces 安全瀏覽器 API 呼叫 AWS CloudTrail
- 使用者存取日誌記錄

Amazon 監控 Amazon WorkSpaces 安全瀏覽器 CloudWatch

您可以使用監控 Amazon WorkSpaces 安全瀏覽器 CloudWatch，該瀏覽器會收集原始資料並將其處理為可讀且近乎即時的指標。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。

CloudWatch Amazon WorkSpaces 安全瀏覽器的指標

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	成功的 Amazon WorkSpaces 安全瀏覽器工作階段啟動次數。	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啟動次數。	PortalId	平均數、總和、上限、下限	計數
GlobalCpuPercent	Amazon WorkSpaces 安全瀏覽器工作階段執行個體的 CPU 使用率。	PortalId	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憶體 (RAM) 使用量。	PortalId	平均數、總和、上限、下限	百分比

> **Note**
>
> 您可以檢視GlobalCpuPercent或GlobalMemoryPercent判斷入口網站上作用中的並行階段作業數目的「SampleCount」測量結果統計資料。每個工作階段每分鐘會發出一次資料點。

使用記錄 WorkSpaces 安全瀏覽器 API 呼叫 AWS CloudTrail

WorkSpaces 安全瀏覽器與服務整合 AWS CloudTrail，該服務可提供使用者、角色或 AWS 服務在 Amazon WorkSpaces 安全瀏覽器中採取的動作記錄。 CloudTrail 將 Amazon WorkSpaces 安全瀏覽器的所有 API 呼叫擷取為事件。其中包括來自 Amazon WorkSpaces 安全瀏覽器主控台的呼叫，以及對 Amazon WorkSpaces 安全瀏覽器 API 作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Amazon WorkSpaces 安全瀏覽器的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以識別向 Amazon WorkSpaces 安全瀏覽器發出的請求、提出請求的來源 IP 地址、提出請求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

WorkSpaces 安全瀏覽器資訊 CloudTrail

CloudTrail 在您創建 AWS 帳戶時，您的帳戶已啟用。在 Amazon WorkSpaces Secure 瀏覽器中發生活動時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。在活動歷史記錄中，您可以查看，搜索和下載 AWS 帳戶中的最近事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需 AWS 帳戶中持續的事件記錄 (包括 Amazon WorkSpaces 安全瀏覽器的事件)，您可以建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 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。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

所有 Amazon WorkSpaces 安全瀏覽器動作都會記錄下來， CloudTrail 並記錄在 Amazon WorkSpaces API 參考中。例如，呼叫`DeleteUserSettings`和`ListBrowserSettings`動作會`CreatePortal`在 CloudTrail 記錄檔中產生項目。

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 使 userIdentity 元素。

瞭解 WorkSpaces 安全瀏覽器記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，操作的日期和時間，請求參數和其他詳細信息的信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範`ListBrowserSettings`動作的 CloudTrail 記錄項目。

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


使用者存取日誌記錄

Amazon WorkSpaces 安全瀏覽器可讓客戶記錄工作階段事件，包括開始、停止和 URL 造訪。這些日誌會傳送到您為 Web 入口網站指定的 Amazon Kinesis Data Stream。如需更多詳細資訊，請參閱 the section called “設定使用者存取日誌記錄”。

WorkSpaces 安全瀏覽器使用者指南

系統管理員使用 WorkSpaces 安全瀏覽器建立連線到公司網站的入口網站，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。

下列內容可協助引導想要深入瞭解如何存取 WorkSpaces 安全瀏覽器、啟動和設定工作階段，以及使用工具列和網頁瀏覽器的使用者。

主題

- 瀏覽器和裝置相容
- 存取 Web 入口網站
- 工作階段指引
- 故障診斷
- 單一登入擴充功能

瀏覽器和裝置相容

Amazon 安 WorkSpaces 全瀏覽器由 NICE DCV 網絡瀏覽器客戶端提供支持，該客戶端在 Web 瀏覽器中運行，因此無需安裝。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。

有關 Web 瀏覽器客戶端支持的最多 up-to-date 詳細信息，請參閱 Web 瀏覽器客戶端。

> **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。目前，蘋果 Safari 瀏覽器和 Mozilla FireFox 不支持網絡攝像頭。

存取 Web 入口網站

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。

工作階段指引

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

- 啟動工作階段
- 使用工具列
- 使用瀏覽器
- 結束工作階段

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。這表明 Amazon WorkSpaces 安全瀏覽器正在為您創建會話。在幕後，Amazon WorkSpaces Secure 瀏覽器正在建立執行個體、啟動受管網頁瀏覽器，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。

- 透過選取瀏覽器中的鎖定圖示，並選取 [永遠允許快顯視窗] 設定，讓 Amazon WorkSpaces Secure 瀏覽器啟動其他監視器視窗。

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。

使用工具列

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，請將游標暫留在工具列上，然後選取向上箭號按鈕，或連按兩下頂端區段中的打火機列。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拉近。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，請依照下列步驟執行：

1. 選取工具列或網頁內容。
2. 按住 Ctrl + 可以放大顯示，或按 Ctrl + - 來縮小顯示。

如要在 Mac 裝置上放大或縮小，請依照下列步驟操作：

1. 選取工具列或網頁內容。
2. 按下 Cmd + + 來放大顯示，或按下 Cmd + - 來縮小顯示。

若要將工具列固定在螢幕頂端，請在「工具列」模式下選擇「偏好設定」、「一般」和「停靠」。

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.
	**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。

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。

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 安全瀏覽器會刪除工作階段中的所有資料。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。

故障診斷

我的 Amazon WorkSpaces 安全瀏覽器門戶不允許我登錄。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 Secure Browser 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。

單一登入擴充功能

Amazon WorkSpaces 安全瀏覽器提供了一個擴展單一登錄與桌面計算機上的 Chrome 和 Firefox 瀏覽器。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 安全瀏覽器建置了擴充功能，以便在工作階段期間對網站進行單一登入。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)。

相容性

該擴展功能適用於以下裝置：

- 筆記型電腦
- 桌上型電腦

該擴展功能適用於以下瀏覽器：

- Chrome
- Firefox

安裝

當您登入入口網站時，請依照提示安裝適用於您的 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。

為確保擴充功能能如預期般運作，請在一般瀏覽視窗中使用擴充功能，而不是無痕模式 (Chrome) 或私密瀏覽 (Firefox)。

故障診斷

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. 確保您的瀏覽器上安裝了 Amazon 安 WorkSpaces 全瀏覽器擴展。如果您刪除了瀏覽器資料，則可能意外刪除了擴充功能。
2. 確保你不是隱身（鉻）或私人瀏覽（火狐瀏覽器）。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
允許深層連結	允許入口網站在工作階段期間接收將使用者連線至特定網站的深層連結。	2024年6月25 日
受管政策更新	新增 AmazonWorkSpacesSecureBrowserReadOnly 受管理政策	2024年6月24日
使用工具列縮放	您可以使用工具列增加顯示、圖示和文字的大小。	2024年5月1日
新的入口網站設定	您現在可以為入口網站指定執行個體類型和最大同時使用者限制。	2024年4月22 日
CloudWatch 度量	添加 GlobalCpuPercent 和 GlobalMemoryPercent 指標。	2024年2月26日
設定網址過濾	您可以使用 Chrome 政策來篩選使用者可從遠端瀏覽器存取哪些網址。	2024年2月21 日
IdP 驗證類型	您可以選擇標準或 IAM 身分中心驗證類型。	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 安全瀏覽器的用戶指南	新增內容可協助引導使用者、想要進一步了解如何存取 Amazon WorkSpaces Secure 瀏覽器、啟動和設定工作階	2023 年 7 月 17 日

	段，以及使用工具列和網頁瀏覽器的使用者。	
IP 存取控制	WorkSpaces 安全瀏覽器允許您控制您的門戶網站可以從哪些 IP 地址訪問。	2023 年 5 月 31 日
受管政策更新	更新的 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	更新的 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	更新的 AmazonWorkSpacesWebReadOnly 受管政策	2022 年 11 月 2 日
受管政策更新	更新的 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	更新的 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 受管理的政策，以將 AWS/ 使用命名空間新增至 API 權限 PutMetricData	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 受管理策略	2021 年 11 月 30 日
受管政策	新的 AmazonWorkSpacesWebServiceRolePolicy 受管理策略	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。