



# ChromeOS 向け Citrix Workspace アプリ

## Contents

<b>ChromeOS 向け Citrix Workspace アプリ</b>	<b>3</b>
このリリースについて	4
<b>Technical Preview の機能</b>	<b>27</b>
インストールの前提条件	37
インストール	39
開始	45
構成	51
カスタマーエクスペリエンス向上プログラム (CEIP)	57
クリップボード	61
ファイルの処理	63
ファイルタイプの関連付け	72
グラフィック	73
キーボード	80
ライセンス	91
マルチメディア	93
<b>Microsoft Teams の最適化</b>	<b>99</b>
<b>Zoom の最適化のサポート</b>	<b>109</b>
マルチモニター	113
周辺機器	118
電源設定	136
印刷	137
シームレスなエクスペリエンス	140
セッションエクスペリエンス	146

ストアエクスペリエンス	160
タッチとモビリティのサポート	172
<b>URL</b> のリダイレクト	174
仮想チャンネル	177
トラブルシューティング	180
構成ユーティリティツール	188
認証	196
<b>ID</b> プロバイダーとして <b>Okta</b> を使用した <b>Citrix Workspace</b> アプリのシングルサインオン	200
<b>ID</b> プロバイダーとして <b>Microsoft Azure</b> を使用した <b>Citrix Workspace</b> アプリのシングルサインオン	206
<b>SDK</b> および <b>API</b>	213
廃止	217

## ChromeOS 向け Citrix Workspace アプリ

June 18, 2024

ChromeOS 向け Citrix Workspace アプリはネイティブ Chrome パッケージアプリです。ユーザーはこれを使用して、Citrix によりホストされたワークスペースのアプリケーションおよび仮想デスクトップに Chrome デバイスからアクセスできます。アプリは Chrome ウェブストアから入手できます。

機能、解決された問題、既知の問題について詳しくは、「[このリリースについて](#)」ページを参照してください。

ChromeOS 向け Citrix Workspace アプリをインストールすると、Web ブラウザー内のデスクトップやアプリケーションにアクセスできます。StoreFront で追加の構成または展開オプションは必要ありません。

ChromeOS 向け Citrix Workspace アプリの機能について詳しくは、[Citrix Workspace アプリの機能マトリックス](#)を参照してください。

廃止済みの項目については、「[廃止済み](#)」ページを参照してください。

### 言語サポート

ChromeOS 向け Citrix Workspace アプリは、英語以外の言語での使用に適応しています。ChromeOS 向け Citrix Workspace アプリでサポートされている言語の一覧については、「[言語サポート](#)」を参照してください。

### ChromeOS LTS の互換性

より少ない更新を希望する場合、Google は ChromeOS で長期サポート (LTS) バージョンを提供しています。特定の時点で、1 つまたは複数のバージョンの Citrix Workspace アプリが、最新バージョンの ChromeOS LTS と互換性があります。

最新のバグ修正と新機能が有効になった Citrix Workspace アプリのバージョンをお探しの場合は、以下をお勧めします：

- 最新バージョンの Citrix Workspace アプリを使用する
- Stable チャンネルの最新の Google ChromeOS バージョンを使用する。

後方互換性、除外、および一般的な質問について詳しくは、「インストール」ページの「[ChromeOS LTS 互換性](#)」セクションを参照してください。

### 参考記事

- [Global App Configuration Service](#)
- [Microsoft Teams の最適化](#)



- [Citrix Virtual Apps and Desktops 環境での Microsoft Teams の最適化](#)
- [技術概要: Workspace のシングルサインオン](#)
- [技術論文: Citrix Workspace アプリクイックスタートガイド](#)
- [技術概要: Citrix Workspace](#)
- [開発者用のドキュメント - Citrix Workspace app for Chrome HDX SDK](#)
- [開発者用のドキュメント - Citrix Virtual Channel SDK](#)
- [Citrix Workspace アプリのリリーススケジュール](#)

### 関連製品の到着情報

- [Citrix DaaS](#)
- [Citrix Workspace](#)
- [StoreFront](#)
- [Windows 向け Citrix Workspace アプリ](#)
- [HTML5 向け Citrix Workspace アプリ](#)
- [ワークスペースユーザーインターフェイス \(user interface: UI\)](#)

### 古いドキュメント

保守終了 (EOL) に達した製品リリースについては、[古いドキュメント](#)を参照してください。

### このリリースについて

June 19, 2024

新機能、機能強化、解決された問題、既知の問題について説明します。

注:

Technical Preview の機能をお探しの場合は、1 か所で見つけられるように厳選した一覧を作成しました。「[Technical Preview の機能](#)」ページをご覧ください、記載されている Podio フォームリンクを使用してフィードバックを共有してください。

### 2405 の新機能

このリリースは ChromeOS バージョン 125 と互換性があります。このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

## Technical Preview

- [セッション内ツールバーの機能が向上しました。](#)

Technical Preview 機能の完全な一覧については、「[Technical Preview の機能](#)」ページを参照してください。

### 2405 で解決された問題

- マルチモニター環境では、公開されたアプリを開くと、アプリ画面の代わりに空白の画面が表示されます。この問題は、全画面 H.264 モードを使用するときに発生します。詳しくは、「[制限](#)」を参照してください。[CVADHELP-24883]
- 管理されていないデバイスでアプリまたはデスクトップセッションを開始すると、ChromeOS 向け Citrix Workspace アプリから送信されるクライアント名が HTML5-XX になります。修正後、クライアント名は CrOS-XX として表示されるようになりました。[RFHTMCRM-12155]
- サービス継続性機能を有効にしてセッションをオフラインで開始すると、Citrix Workspace からサインアウトして再度サインインした後、リースファイルのダウンロードが断続的に失敗します。[RFHTMCRM-12492]
- デスクトップセッションを開始し、テキストを入力するためにアプリを開き、入力を開始すると、テキストが消えて再び表示されます。テキストの表示がちらついて見えます。この問題は、全画面 H.264 モードを使用するときに発生します。詳しくは、「[制限](#)」を参照してください。[CVADHELP-24883]

### 2405 の既知の問題

新しい既知の問題はありません。

注:

- 以前のリリースの問題については、「[既知の問題](#)」セクションを参照してください。

### 以前のリリース

このセクションでは、[Citrix Workspace アプリのライフサイクルマイルストーン](#)に従ってサポートされている以前のリリースの新機能と解決された問題に関する情報を提供します。

#### 2402.1

##### 新機能

このリリースは ChromeOS バージョン 121 と互換性があります。このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

**Zoom** の最適化のサポート 2402.1 バージョン以降、ChromeOS 向け Citrix Workspace アプリは、セッション内から最適化されたオーディオおよびビデオ会議エクスペリエンスを実現する、Zoom 仮想デスクトップインフラストラクチャ (VDI) ソリューションとの統合をサポートします。

この機能に関連したサードパーティの依存関係に対処したため、すぐに構成して使用できるようになりました。ユーザーが最適化されたオーディオとビデオを活用できるほか、Citrix セッション内の Zoom 会議中、VDA リソースの消費量が減少することが確認されています。

この機能について詳しくは、「[Zoom の最適化のサポート](#)」を参照してください。

**サービス継続性** 2402.1 バージョン以降、サービス継続性機能は無効になっています。

注:

以前にサービス継続性機能を有効にしている場合、ChromeOS 向け Citrix Workspace アプリの古いバージョンを使用している場合は、サービス継続性機能を使用できない可能性があります。この機能を有効にするには、Citrix Workspace アプリを最新バージョン (2402.1 以降) に更新し、Knowledge Center の記事 [CTX632723](#) の手順を実行することをお勧めします。

構成について詳しくは、「[サービス継続性](#)」のドキュメントを参照してください。

**構成ユーティリティツール** このリリースでは、構成ユーティリティツールに関する安定性が総合的に向上するように対処しています。構成の設定 **allowEditStoreName** は、このツールに含まれています。

**ツールへのアクセス方法** 以前は、構成ユーティリティツールは [Knowledge Center](#) ページで入手できました。

2402 バージョン以降、[Citrix ダウンロード](#) ページから構成ユーティリティツールをダウンロードできます。

**仮想チャネル SDK** 2402 リリース以降、Citrix Virtual Channel SDK (VCSDK) for ChromeOS には、ChromeOS 向け Citrix Workspace アプリとサードパーティのプラグインとの互換性を促進する機能が追加されました。サードパーティのプラグインは VCSDK と統合する必要があります。この機能の処理により、すべてのバージョンと組み合わせにわたってシームレスな下位互換性と上位互換性が確保されます。これらの機能について詳しくは、[開発者ドキュメント](#) のページを参照してください。

さらに、マルチモニターシナリオをサポートする API が追加されています。

**Chromebook の HTTP プロキシ設定** Chromebook で HTTP プロキシ設定を行っている場合、セッションが開始されない可能性があります。

問題の解決方法について詳しくは、「[Chromebook の HTTP プロキシ設定](#)」の記事を参照してください。

ストア **URL** の短い名前 以前は、ストア URL を表示できましたが、ストア URL の短い名前を追加または変更する機能はありませんでした。これは、管理者やユーザーがストア URL を覚える妨げになっていました。

2402 リリース以降、管理対象ユーザーに対して、管理者は Google 管理コンソールからストア URL とともにカスタムストア名をプッシュできるようになりました。この機能により、ユーザーはさまざまなストアを簡単に識別できるようになります。

この機能について詳しくは、「[ストア URL の短い名前](#)」を参照してください。

### 解決された問題

- デリバリーグループ名にマルチバイト文字が含まれる仮想デスクトップがある場合、仮想デスクトップセッションを開始できません。[CVADHELP-24846]
- 最適化された Microsoft Teams 通話中に画面の共有を停止すると、ビデオセッションの代わりに空白の四角形が表示されることがあります。[RFHTMCRM-11689]
- キオスクモードでは、StoreFront で [デスクトップを自動的に起動する] 設定が有効になっている場合でも、セッションが自動的に開始されない場合があります。[CVADHELP-23698] [RFHTMCRM-11815]
- サービス継続性機能を有効にして [**Workspace** に再接続] をクリックすると、サインイン画面に [**Workspace** をオフラインで使用する] バナーが表示されません。[RFHTMCRM-11720]
- 実際のデスクトップセッションのアイコンではなく、Citrix Workspace アプリのアイコンが Chrome シェルフに表示されます。この問題は、サービス継続性機能を有効にし、クラウド環境の停止が発生した場合に発生します。[RFHTMCRM-11647]
- クライアントドライブマッピング機能を使用してローカルデバイスから VDA に 4KB を超えるファイルをコピーして貼り付けると、データが破損する可能性があります。[RFHTMCRM-12156]
- セッション中に、マウスのクリックが応答しなくなる場合があります。[RFHTMCRM-11841] [CVADHELP-24210]
- ユーザーが（意図的に、または非アクティブであることによって）ストアページからサインアウトし、同じストアページに再度サインインすると、ストアページが空白になるか、読み込み中アイコンがいつまでも表示されることがあります。この問題は、サービス継続性が有効なクラウド展開で発生します。[RFHTMCRM-12212]

## 2312

### 新機能

このリリースは ChromeOS バージョン 119 と互換性があります。このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

セカンダリ呼び出しのサポート セカンダリ呼び出し機能を使用して、Microsoft Teams が最適化されているときに受信通知を受け取るセカンダリデバイスを選択できます。

たとえば、スピーカーをセカンダリ呼び出し機器として設定し、エンドポイントがヘッドフォンに接続されているとします。この場合、Microsoft Teams は受信の呼び出し音をヘッドフォンとスピーカーの両方に送信します。次の場合、セカンダリ呼び出しを設定することはできません：

- 複数のオーディオデバイスが接続されていない場合
- 周辺機器（Bluetooth ヘッドセットなど）が利用できない場合

### 注

デフォルトでは、この機能は無効になっています。

### この機能の既知の制限事項

- この機能を有効にすると、セカンダリ呼び出し音がわずかに遅れて 2 回再生されることがあります。この問題は Microsoft Teams のバグであり、今後の Microsoft Teams リリースで修正される予定です。

構成について詳しくは、「[セカンダリ呼び出し音のサポート](#)」を参照してください。

最適化された **Microsoft Teams** ビデオ会議通話でサイマルキャストの実装 2312 リリース以降、最適化された Microsoft Teams ビデオ会議通話に対して、デフォルトでサイマルキャストサポートが有効になっています。このサポートにより、さまざまなエンドポイントでのビデオ会議通話の品質とエクスペリエンスが向上します。適切な解像度に適応することによってすべての発信者に最適な通話エクスペリエンスを提供できます。

この向上したエクスペリエンスにより、各ユーザーは、エンドポイントの機能、ネットワークの状態などのいくつかの要因に応じて、複数のビデオストリームを異なる解像度で配信できます。たとえば、720p、360p などです。次に、受信側のエンドポイントは、可能な範囲で最高品質の解像度を要求します。これにより、すべてのユーザーに最適なビデオ体験を提供できます。

**HTTPS** を使用せずに **URL** を保存する 2312 リリース以降、URL に <https://> を明示的に指定せずにストア URL を直接入力できるようになりました。

### 注:

まだ <http> ストアを使用している場合は、<https> ストアに移行することを強くお勧めします。それまでは、ストア URL の先頭に <http> を明示的に追加することで、<http> ストアにアクセスできます。

### 解決された問題

- クラウド環境の停止が発生すると、セッションの開始に失敗する可能性があります。サービス継続性の構成について詳しくは、「[サービス継続性](#)」を参照してください。[RFHTMCRM-11539]

- セッション中、Microsoft Excel アプリを開いて **Ctrl +** スペースキーの組み合わせを使用すると、キーの組み合わせが正常に機能しない可能性があります。[RFHTMCRM-11718]

## 2311

### 2311 の新機能

このリリースは ChromeOS バージョン 119 と互換性があります。このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

### Technical Preview

- アダプティブトランスポート

Technical Preview 機能の完全な一覧については、「[Technical Preview の機能](#)」ページを参照してください。

### 2311 で解決された問題

- Desktop Delivery Controller マシンの Citrix Studio に設定された Desktop Delivery Controller V1 ポリシーが有効になっていない場合、USB リダイレクトが成功しない可能性があります。この問題は、Desktop Delivery Controller V1 ポリシーが VDA レジストリ設定のキー `\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\GenericUSB` よりも優先度が高く設定されていない場合に発生します。[RFHTMCRM-11072]
- デスクトップセッションを開始して Citrix Director コンソールを確認すると、ICA 往復時間値がゼロと表示される場合があります。ICA 往復時間値は、セッションの開始直後に確認すると、正の値になることがあります。ただし、しばらくすると、ゼロとして表示される場合があります。[CVADHELP-23905]

## 2310

### 新機能

このリリースは ChromeOS バージョン 118 と互換性があります。このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

### 2310 で解決された問題

- Chromebook で ChromeOS 向け Citrix Workspace アプリのセッションを開始すると、Google ドライブのファイルが開かない場合があります。[RFHTMCRM-10540]

- ChromeOS 向け Citrix Workspace アプリを開いて [設定] > [一般] で [高 DPI スケール] オプションを選択すると、デスクトップセッションの開始時に重複したカーソルが表示される場合があります。[RFHTMCRM-10839]
- デスクトップセッションで Microsoft Teams を使用する場合、ディスプレイ解像度を [デバイスのピクセル縦横比でスケール] オプションに設定すると、参加者のビデオが正しく表示されない場合があります。[RFHTMCRM-5271]
- セッション中に、スピーカーとマイクの両方を含むオーディオデバイスが表示されない場合があります。この問題は、ローカルマシンにマイクデバイスがない場合、またはユーザーがすべてのマイクデバイスを無効にした場合に発生します。[RFHTMCRM-10900]

## 2309.5

### 新機能

このリリースは ChromeOS バージョン 117 と互換性があります。このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

### 解決された問題

このリリースでは、仮想チャネル SDK に関する Window Management API 関連の問題を解決しています。

## 2309

### 新機能

このリリースは ChromeOS バージョン 117 と互換性があります。このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

**[Scan code]** 入力モード Citrix Workspace アプリを使用すると、外部の物理キーボードを使用して、VDA のサーバー側のキーボードレイアウトと連携できます。管理者が [Scan code] モードを有効にすると、エンドユーザーはクライアントではなくサーバーのキーボードレイアウトを使用する可能性があります。

この機能により、特に東アジア言語の物理キーボードを使用する場合のユーザーエクスペリエンスが向上します。

#### メモ:

- デフォルトでは、この機能は無効になっています。
- タッチデバイスでは、[Scan code] が有効になっていると、Citrix Workspace アプリでスクリーンキーボードソフトウェアが機能しません。

構成について詳しくは、[Scan code input mode](#)を参照してください。

カスタムキーボードマッピング バージョン 2309 以降、VDA が Windows OS マシンで、ネイティブ入力デバイスが ChromeOS キーボードである場合、エンドユーザーは Windows 固有のショートカットとキーの組み合わせを使用できるようになります。カスタムマッピングを使用して、**Ctrl** キーと **Alt** キーを割り当てることができるようになりました。ユーザーは、右または左のコントロール (Ctrl) キーを選択して、Alt キーとして機能させることができます。

メモ:

- マッピングは全画面モードでのみ可能です。
- 設定を保存すると、マッピングはすべてのセッションで有効になります。
- この機能はデフォルトで有効にされています。

構成について詳しくは、[Custom keyboard mapping](#)を参照してください。

この機能の使用方法について詳しくは、[ヘルプ](#)を参照してください。

**VDA** への、全画面モードでのシステムショートカット ChromeOS デバイス向け Citrix Workspace アプリのバージョン 2309 以降で、VDA (リモートデスクトップセッション) への、全画面モードでのシステムショートカットを渡すことができるようになりました。ただし、クライアント OS では機能しません。

以前では、これらのキー組み合わせはローカルでは機能していました。この機能が全画面モードで有効の場合、これらのキー組み合わせは VDA に送信されますが、ローカルでは作用しません。たとえば、更新キーは Chromebook のシステムキーであり、**Ctrl + Shift + 更新キー**の組み合わせは画面を回転するための、ChromeOS のシステムショートカットです。しかし、Windows OS にはそのようなショートカットがないため、Windows VDA では何も起こりません。

別の例として、**Alt+ [** は ChromeOS ウィンドウを左側にドッキングするのに使用されますが、同じショートカットは Windows VDA では作用しません。一部のアプリケーションでは、特定の機能に対してこのようなショートカットを使用する場合があります。例えば、一部のバーコードスキャナーでは **Alt+ [** がプレフィックスとして使用されます。

注:

- この機能はデフォルトで有効になっています。

構成について詳しくは、[System shortcuts to VDA in full screen mode](#)を参照してください。

### 2309 で解決された問題

- マルチモニター設定のキオスクモードでは、2 番目のモニターを接続してセッションを開始すると、両方のモニターとも画面が黒くなる場合があります [RFHTMCRM-10905]。

バージョン 2308 を使用している場合は、2309 にアップグレードすることをお勧めします。

ただし、2308 での作業を続行する場合は、Google 管理コンソールで次の JSON データを追加します:



```

1  {
2
3  "settings": {
4
5      "Value": {
6
7          "settings_version": "1.0",
8          "engine_settings": {
9
10             "features": {
11
12                 "graphics": {
13
14                     "graphicsWebWorker": {
15
16                         "enabled":
17                             false
18                     }
19                 },
20                 "graphicsWasmRender": false
21             }
22         }
23     }
24 }
25
26 }
27
28 }
29
30 }
31
32 <!--NeedCopy-->

```

## 2308

### 2308 の新機能

このリリースは ChromeOS バージョン 115 と互換性があります。このリリースでは、グラフィックス関連のパフォーマンスが向上しています。

### 2308 で解決された問題

- 管理対象ゲストセッションモードでセッションを開始すると、USB の自動リダイレクト機能が予期したとおりに動作しない可能性があります。[RFHTMCRM-10625]
- サービス継続性機能が動作しません。つまり、停止中に DaaS のアプリとデスクトップに接続できません。[RFHTMCRM-9261]

## 2307

### 新機能

このリリースは ChromeOS バージョン 114 と互換性があります。また、このリリースではいくつかの問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

**Microsoft Teams** の機能強化 Microsoft Teams の最適化では、Microsoft Teams でライブキャプションが有効になっているときにスピーカーが話す内容のリアルタイムの文字起こしがサポートされています。

**USB** デバイスの自動リダイレクト USB デバイスを自動的にリダイレクトするには、USB デバイス規則に従う必要があります。

次の方法で USB デバイス規則を設定できます。

- [Google 管理ポリシー](#)
- [デバイス規則](#)
- [クライアント USB デバイスリダイレクト規則 \(バージョン 2\)](#)

**HDX** セッションのエクスペリエンスの強化 強化された圧縮技術により、ChromeOS 向け Citrix Workspace アプリではネットワークリソースの消費量が減少し、セッションの応答性が向上しています。

**DDC** ポリシーによる複合 **USB** リダイレクトの強化 バージョン 2307 以降では、特定の複合 USB インターフェイスまたはインターフェイスクラスがデフォルトで VDA にリダイレクトできるかどうかを判断できるようになりました。ChromeOS デバイ스에 複合 USB が接続されている場合、**enableDefaultAllowPolicy** 構成は、DDC ポリシーによる USB リダイレクトをデフォルトで許可できるかどうかを決定するのに役立ちます。この機能は、VDA バージョン 2212 以降でサポートされています。

詳しくは、「[DDC ポリシーによる複合 USB リダイレクトの強化](#)」ドキュメントを参照してください。

クライアントドライブマッピング 2307 バージョン以降、クライアントドライブマッピング (CDM) 機能によりローカルの ChromeOS デバイス上でフォルダーのマッピングがサポートされ、セッション内からアクセスできるようになります。ChromeOS デバイスから任意のフォルダーをマッピングできます。たとえば、フォルダーにシステムファイルが含まれていない場合、ダウンロード、Google ドライブ、USB ドライブのフォルダーなどをマッピングできます。

エンドユーザーは次の操作を実行できます：

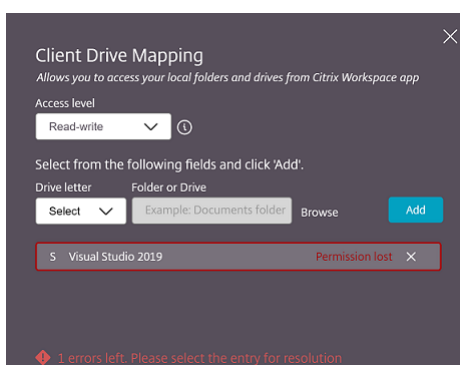
- ファイルとフォルダーをセッションからマップされたドライブに、および逆方向にコピーする。
- マップされたドライブでファイルとフォルダーの一覧を表示する。
- マップされたドライブでファイルの内容を開いて、読み取り、変更する。

- マップされたドライブでファイルのプロパティ（変更時刻とファイルサイズのみ）を表示する。

この機能を使用すると、HDX セッション内のファイルエクスプローラーで、仮想デスクトップドライブとローカルマシンドライブの両方に同時にアクセスできるという利点があります。

### 既知の制限事項

- マップされたドライブ内のファイルとフォルダーの名前を変更することはできません。
- マッピングには完全なパスではなく、フォルダーの名前が含まれます。
- ローカルフォルダーに非表示のファイルがあり、そのフォルダーをマップした場合、非表示のファイルは、マップされたドライブのセッション内で表示されます。
- マップされたドライブでファイルプロパティを読み取り専用アクセスに変更することはできません。
- [HDX SDK を使用してセッションが埋め込みモード](#)で開かれている場合、CDM はサポートされません。
- リムーバブルデバイスからフォルダーをマップし、アクティブなセッション中にそのデバイスを削除すると、マップされたドライブをセッション内で使用できなくなります。マッピングを手動で削除するには、特定のマッピングの **[X]** マークをクリックします。



詳しくは、「[クライアントドライブマッピング](#)」を参照してください。

## Technical Preview

- アクセシビリティと TalkBack

Technical Preview 機能の完全な一覧については、「[Technical Preview の機能](#)」ページを参照してください。

### 解決された問題

- エンドユーザーが公開アプリを開いて Citrix Workspace アプリを更新すると、公開アプリの重複したインスタンスが表示されます。構成設定を適用するには、「[ストアの更新](#)」セクションを参照してください。  
[CVADHELP-22229]

- マルチモニターモードでは、セカンダリモニターで公開アプリを開いたときに、マウスクリックが正常に動作しない場合があります。[CVADHELP-21916]
- セッションが開始されても、画面右下に表示されるセッション起動の進行状況通知ウィンドウが閉じない場合があります。この問題は、VDA バージョンが 7.15 の場合に発生します。[RFHTMCRM-10161]

## 2306

このリリースは、Google が長期サポート (LTS) バージョンとして選択した ChromeOS バージョン 114 と互換性があります。そのため、Citrix は、LTS ライフサイクルが終了するまでこのリリースのサポートを継続します。詳細と除外事項については、Citrix の [互換性に関するステートメント](#) を参照してください。

### 新機能

**DDC** ポリシーによる複合 **USB** リダイレクトの構成 以前は、管理者は Google 管理ポリシーを使用してクライアント側の USB リダイレクトを構成しました。

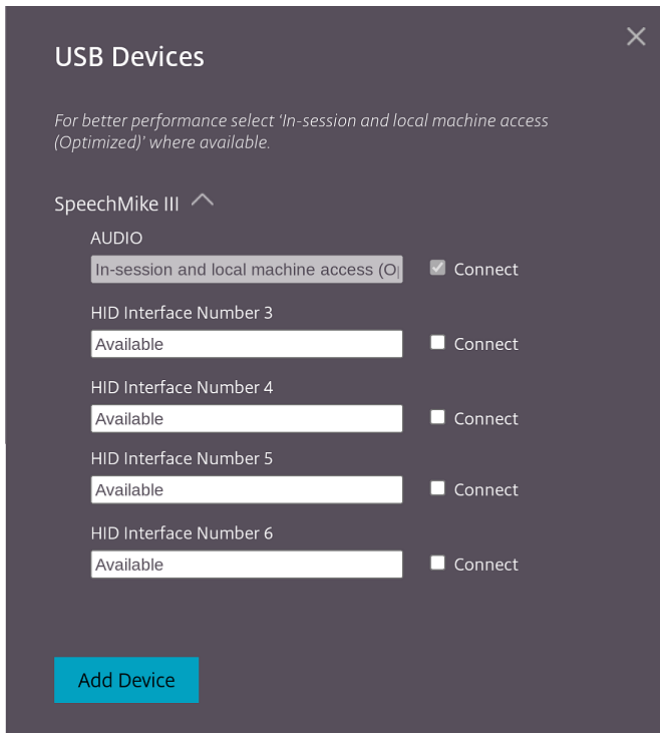
2306 リリース以降は、DDC ポリシーを通じて USB リダイレクトを構成することもできます。DDC ポリシーによる構成により、管理者がポリシーと動作を定義する場合に、統一かつ一元的な方法を使用できます。これらのポリシーは、オンプレミスおよびクラウド展開の管理対象デバイスおよびユーザーに適用できます。この機能は、VDA バージョン 2212 以降でサポートされています。

構成方法について詳しくは、「[DDC ポリシーによる複合 USB リダイレクトの構成](#)」のドキュメントを参照してください。

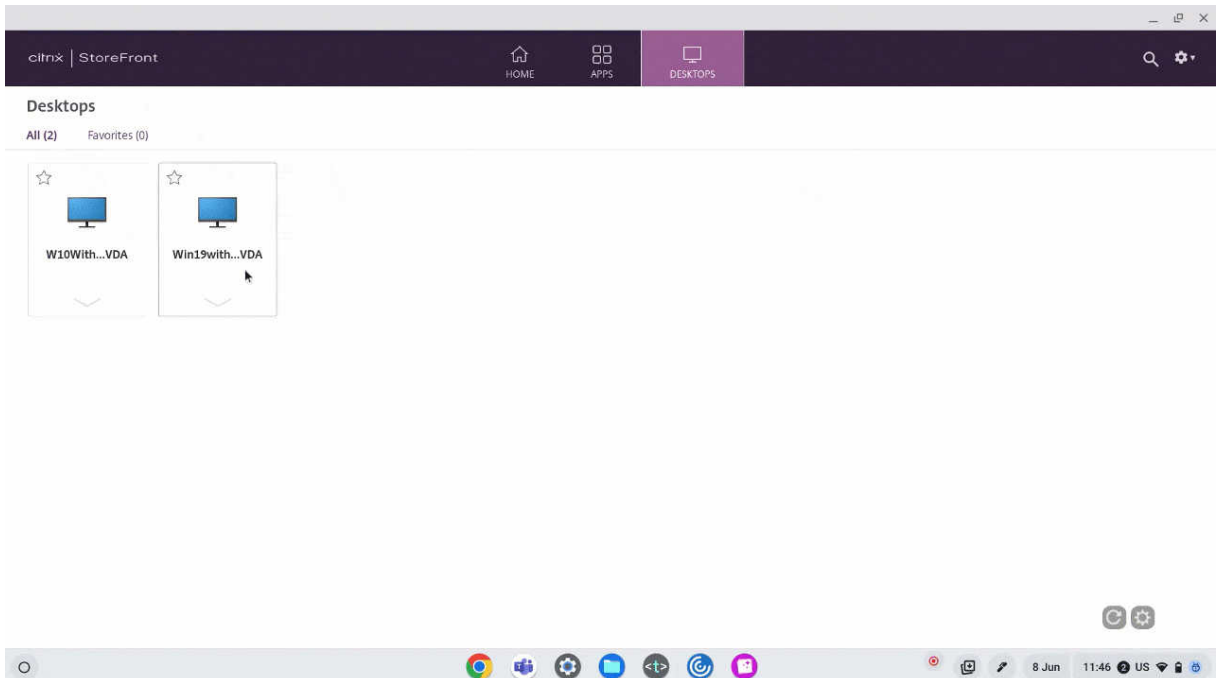
複合 **USB** デバイスの **UI** の機能強化 2306 リリース以降、複合 USB デバイスの構成の「split」が true に設定されている場合、**USB** デバイスの UI にはインターフェイスクラスではなくインターフェイス番号に基づいてコンポーネントが表示されます。

詳しくは、「[複合 USB リダイレクト](#)」の記事を参照してください。

ユーザーインターフェイス 以下はその例です：



仮想アプリとデスクトップの起動エクスペリエンスの向上 2306 リリース以降、アプリとデスクトップの起動エクスペリエンスが向上し、起動状態に関連した情報がタイムリーに提供されます。



### 解決された問題

- 既にセッションが開始されている USB デバイスを接続解除して再接続すると、デバイスのリダイレクトが再度失敗します。Citrix Workspace アプリを再起動するまで、読み込み中のアイコンが表示されます。[RFHTMCRM-9715]
- 最適化された Microsoft Teams 会議に参加していると、カメラのストリーミングが失敗します。ビデオがぼやけて見えたり、ビデオが応答しなくなることがあります。この問題は、画面共有機能が無効になっており、エンドユーザーが Microsoft Teams 会議でカメラを有効にしている場合に発生します。[RFHTMCRM-9968]
- Chromebook では、セッションがタブレットモードのときに、Chrome シェルフからアプリアイコン（メモ帳アイコンなど）を複数回タップして、シームレスアプリケーションにフォーカスを移動することが必要な場合があります。[RFHTMCRM-9803]
- セッションがタブレットモードの場合、Chromebook のスタイラスペンが機能しない可能性があります。[RFHTMCRM-9951]
- セッション中、エンドユーザーは断続的な音声の問題を経験することがあります。この問題は、ChromeOS 向け Citrix Workspace アプリ 2304 以降のバージョンにアップグレードすると発生します。[CVADHELP-22784]

## 2305

### 新機能

ネットワークプリンターのサポート 以前は、仮想デスクトップセッションから印刷する場合に Citrix PDF プリンターオプションが使用されていました。プリンタードライバーはファイルを PDF に変換し、その PDF をローカルデバイスに転送します。これによって、この PDF を新しいウィンドウで表示したり、印刷したりできました。

2305 リリース以降、ChromeOS 向け Citrix Workspace アプリはネットワーク印刷をサポートします。エンドユーザーは、セッション内で Chromebook に接続されているプリンターの一覧を表示できます。ユーザーは、ローカルデバイス上で中間 PDF ファイルを生成せずに、プリンターを直接選択できます。この機能は以下でサポートされています：

- VDA バージョン 2112 以降。
- ChromeOS バージョン 112 以降。

#### 注：

- デフォルトでは、この機能は有効になっており、PDF 形式の **メタファイル** の印刷のみがサポートされています。

構成方法について詳しくは、「[ネットワークプリンターのサポート](#)」のドキュメントを参照してください。

複数のストアをサポート 2305 リリース以降、IT 管理者はエンドユーザーに複数のストアを割り当てることができます。エンドユーザーは、正確なストア URL を覚えていなくても、複数のストアを簡単に切り替えることができるよ

うになりました。この機能により、複数のストアにアクセスするときのユーザー エクスペリエンスが向上します。

構成方法について詳しくは、「[複数のストアのサポート](#)」のドキュメントを参照してください。

**URL リダイレクトの機能強化** 以前は、[ホストからクライアントへのリダイレクト](#)を有効にすると、URL はサーバー VDA でインターセプトされてからユーザーデバイスに送信されていました。ChromeOS 向け Citrix Workspace アプリが、URL をセッション内で開くかローカルデバイスで開くかを選択するようにユーザーに求めるダイアログボックスを表示します。ダイアログボックスは、URL ごとに表示されていました。

2305 以降、管理者は、さらにダイアログボックスを表示することなく、ローカルデバイス内のリンクを開くように URL リダイレクトを構成できるようになりました。この機能強化により、ユーザーエクスペリエンスが向上します。

注:

- デフォルトでは、この機能は無効になっています。

構成方法については、「[URL リダイレクトの機能強化](#)」のドキュメントを参照してください。

**SDK の Manifest V3 サポート** 2305 リリース以降、ChromeOS 向け Citrix Workspace アプリは、[manifest version 3](#)を含む Chrome 拡張機能を使用する HDX SDK をサポートします。

詳しくは、開発者ガイドドキュメントの「[Citrix Workspace app for ChromeOS HDX SDK](#)」を参照してください。

**仮想チャネル SDK の機能強化** 2305 リリース以降、ChromeOS 向け Citrix Workspace アプリは、仮想チャネル SDK の Windows Management API をサポートします。Web API を使用すると、IT 管理者は対話型アプリケーションを作成し、エンドユーザー向けにカスタマイズできます。

### 解決された問題

- HDX SDK for ChromeOS を使用して仮想アプリまたはデスクトップセッションを切断しようとする、セッションは Desktop Delivery Controller でアクティブなままになります。ただし、セッションの状態は数分後に非アクティブに変わります。[RFHTMCRM-9181]
- セッションで 2 人の参加者が最適化された Microsoft Teams 会議に参加している場合、画面共有とオーディオが失敗することがあります。この問題は、通話中にカメラを数回有効または無効にすると発生します。[CVADHELP-22251]
- デバイスを ChromeOS バージョン 108 にアップグレードすると、公開デスクトップ上のテキストがぼやけて表示される場合があります。この問題は、グラフィック処理装置 (GPU) が中精度をサポートしていないデバイスで発生します。[CVADHELP-22362]

注:

- 一部のデバイスの表示設定は高精度をサポートしておらず、公開デスクトップ上のテキストが正しく表示される場合があります。ただし、この修正により表示がおかしくなる場合があります。これを修復するには、管理者が Google 管理ポリシーを通じて **webglHighPrecision** 属性を **false** に設定します。

このような JSON データの例を次に示します:

```

1  ``
2      "hardware" : {
3
4          "webglHighPrecision" : false
5      }
6  ,
7  <!--NeedCopy-->  ``

```

## 2304

### 新機能

タッチデバイスでのジェスチャの機能強化 2304 リリース以降、Citrix Workspace アプリは、ジェスチャ、マルチタッチ、およびソフトキーボード機能（タブレットモード）に関連したエンドユーザーエクスペリエンスを強化します。Citrix Workspace アプリセッションで、タップ、スワイプ、ドラッグなど、一般的なマルチタッチジェスチャを使用できます。

ジェスチャガイドは次のとおりです:

これを行うには、以下の手順に従います:	Citrix Workspace アプリで次の操作をする:
クリック	1 本指でタップ
右クリック	タッチしたまま押さえて離す
キーボードを表示する	3 本の指でタップ（またはツールバーのキーボードアイコンをタップ）
ドラッグ	タッチしてそのままドラッグする方向に指を動かす
カーソルを有効にする	2 本の指でタップ

### 2304 で解決された問題

- このリリースで解決された問題はありません。



## 2303

### 新機能

このリリースは ChromeOS バージョン 111 と互換性があります。また、このリリースではいくつかの問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

オーディオデバイスのプラグアンドプレイのサポート 以前は、単一のオーディオ再生および録音デバイスのみがサポートされ、実際のデバイス名に関係なく「**Citrix HDX Audio**」として表示されていました。

2303 リリース以降、複数のオーディオデバイスを接続し VDA にリダイレクトできます。USB オーディオデバイスをリダイレクトするときに、VDA の **[Sound] > [Playback]** と **[Sound] > [Recording]** でオーディオデバイスの実際の名前が表示されるようになりました。VDA 上のデバイス一覧は、オーディオデバイスをプラグインする、または取り外すたびに動的に更新されます。

#### 注:

この機能は、デフォルトで有効になります。

詳しくは、「[オーディオデバイスのプラグアンドプレイのサポート](#)」を参照してください。

**Microsoft Teams** の最適化における背景のぼかしと効果 2303 リリース以降、ChromeOS 向け Citrix Workspace アプリで、Microsoft Teams によるビデオ通話の最適化で背景のぼかしと効果が導入されました。これで、背景をぼかしたり、Microsoft Teams が提供する背景の効果に置き換えたりして、会話の最中シルエット（体と顔）に集中できるようにすることで、突然集中力が乱されることを回避できます。この機能は、P2P および電話会議で使用できます。

#### メモ:

- デフォルトでは、この機能は無効になっています。
- この機能は、Microsoft Teams の UI と統合されました。マルチウィンドウのサポートは、VDA を 2112 以降に更新するときに必要な前提条件です。詳しくは、「[マルチウィンドウ会議とチャット](#)」を参照してください。

詳しくは、「[Microsoft Teams の最適化における背景のぼかしと効果](#)」を参照してください。

### 2303 で解決された問題

- セッションで、2 人の参加者が最適化された Microsoft Teams 会議に参加している場合、カメラが無効になると画面が黒くなります。さらに、画面共有、チャット、ユーザーのアイコンをクリックすると、アイコンをクリック可能になります。ただし、その下のオプションは黒い画面の下に隠れてしまい、正常に表示されません。[CVADHELP-22173]

## 2301.1

### 新機能

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

### 解決された問題

- セッションでテキストをコピーまたは貼り付けると、セッションが応答しなくなります。この問題は、バージョン 2301 以降の ChromeOS 向け Citrix Workspace アプリを使用している場合に発生します。[CVADHELP-21951]
- Citrix Virtual Apps and Desktops セッションへのオーディオデバイスのリダイレクトが機能していません。システムトレイの音量操作アイコンに赤い「X」マークが表示されます。この問題は、ChromeOS 向け Citrix Workspace アプリを 2301 バージョンに更新した後に発生します。[RFHTMCRM-8799]

## 2301

### 新機能

このリリースは ChromeOS バージョン 109 と互換性があります。また、このリリースではいくつかの問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

**サービス継続性** サービス継続性により、接続プロセスに関与するコンポーネントの可用性に依存することがなくなるか、依存が削減されます。クラウドサービスのヘルス状態に関係なく、Citrix Virtual Apps and Desktops および Citrix DaaS を起動できます。つまり、サービス継続性により、停止中に DaaS アプリとデスクトップに接続できます。前提条件として、デバイスはリソースの場所へのネットワーク接続を維持する必要があります。

詳しくは、Citrix Workspace ドキュメントの「[サービス継続性](#)」セクションを参照してください。

**オーディオデバイスのプラグアンドプレイのサポート** 以前は、単一のオーディオ再生および録音デバイスのみがサポートされ、実際のデバイス名に関係なく「**Citrix HDX Audio**」として表示されていました。

バージョン 2301 以降、複数のオーディオデバイスがサポートされ、それらは VDA にリダイレクトされます。これで、オーディオデバイスをリダイレクトするときに、VDA の **[Sound] > [Playback]** と **[Sound] > [Recording]** でオーディオデバイスの実際の名前が表示されるようになりました。VDA 上のデバイス一覧は、オーディオデバイスを接続する、または取り外すたびに動的に更新されます。

### 既知の制限事項

- VDA では、内蔵オーディオデバイスの名前は英語のみで表示されます。この問題は、ChromeOS ベースのデバイスを使用している場合に発生します。[RFHTMCRM-8667]

詳しくは、「[オーディオデバイスのプラグアンドプレイのサポート](#)」セクションを参照してください。

**Microsoft Teams** のマルチウィンドウチャットと会議 バージョン 2301 以降では、Microsoft Teams でのチャットと会議に複数のウィンドウを使用できます。会話や会議をさまざまな方法でポップアウトできます。

ポップアウトウィンドウ機能について詳しくは、「[Pop out a chat in Teams](#)」を参照してください。

トラブルシューティングについては、[CTX253754](#)を参照してください。

Microsoft では、将来的に単一ウィンドウのサポートを廃止する予定です。古いバージョンの Citrix Workspace アプリまたは Virtual Delivery Agent (VDA) を実行している場合は、次のバージョンにアップグレードできます：

- Citrix Workspace アプリ 2301 以降  
および
- VDA 2203 以降

**ブラウザコンテンツリダイレクト** ブラウザーコンテンツリダイレクト (BCR) は、リモートブラウザのコンテンツをユーザーのコンピューターデスクトップにリダイレクトします。BCR は、リモートデスクトップウィンドウ内で実行されるフレームやフチのない Web ブラウザーであり、リモート (VDA) ブラウザーのコンテンツ領域に重なります (オーバーレイ)。

BCR はブラウザのコンテンツをクライアントデバイスにリダイレクトし、Citrix Workspace アプリに埋め込まれた対応する Web ブラウザーを作成します。この機能は、ネットワーク使用量、ページ処理、およびグラフィックレンダリングをエンドポイントにオフロードします。そうすることで、要求の多い Web ページ、特に HTML5 または WebRTC を組み込んだ Web ページを閲覧する際のユーザーエクスペリエンスが向上します。ビューポート (ユーザーの Web ページの表示領域) のみがエンドポイントにリダイレクトされます。ブラウザコンテンツリダイレクトは、VDA のブラウザのユーザーインターフェイス (アドレスバー、ツールバーなど) はリダイレクトしません。

つまり、BCR は、クライアント側の許可リストにある Web ページをレンダリングする機能を提供します。この機能は、Citrix Workspace アプリを使用してクライアント側の対応するレンダリングエンジンをインスタンス化し、URL から HTTP および HTTPS コンテンツを取得します。

注：

- BCR は、Citrix Virtual Apps and Desktops バージョン 2212 以降と互換性があります。

許可リストの設定方法について詳しくは、以下を参照してください：

- [Chrome 向けの Web ブラウザーコンテンツリダイレクト拡張機能](#)。
- [ブラウザコンテンツリダイレクトのポリシー設定](#)。

### この機能の既知の問題

- BCR 中、新しいタブで Web サイトのリンクを開くと、セッションブラウザではなくクライアントブラウザで開きます。[HDX-43206]

### この機能の既知の制限事項

- この機能は、以下をサポートしていません：
  - サーバー側でフェッチし、クライアント側でレンダリングするシナリオ。
  - 統合 Windows 認証 (IWA) Web サーバー。
  - マルチモニター機能。
- BCR でリダイレクトされた Web サイトにファイルをアップロードまたはダウンロードする場合、VDA セッションのファイルピッカーの代わりに ChromeOS のファイルピッカーが表示されます。[HDX-43207]
- BCR でリダイレクトされたページからの印刷はサポートされていません。

**ダブルホップ** 2301 バージョン以降、Citrix Workspace アプリはダブルホップシナリオをサポートします。この機能は、USB リダイレクトの拡張機能です。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[Citrix Virtual Apps and Desktops でのダブルホップ](#)」を参照してください。

**USB の自動リダイレクト設定** 以前は、USB の自動リダイレクト設定に関するエンドユーザーによる設定オプションがありませんでした。管理者がこれらのポリシーを制御するため、エンドユーザーはセッションを開始するたびに必要な USB デバイスを手動でリダイレクトする必要があります。

2301 バージョン以降、エンドユーザーは、仮想デスクトップセッション内の任意の USB デバイスの自動リダイレクトの設定を選択できます。Citrix Workspace アプリは、エンドユーザーが USB の自動リダイレクトを制御できるアプリレベルの設定を提供するようになりました。エンドユーザーは設定を実行することができ、起動されるセッション間でその設定を保持できます。

これには 2 つのオプションがあります。1 つはセッションの起動時、もう 1 つはセッションの進行中です。

All changes made will take effect after relaunching the sessions.

**Multi-monitor settings**

- Use all the monitors to span display

**Customer Experience Improvement Program**

- Send anonymous usage statistics to improve Citrix Workspace app  
(Relaunch the app to apply this setting)

**High DPI Scaling**

- Scale the session for monitors with high device pixel ratio

**Client cursor settings**

- Show assistive cursor when actual cursor is not visible

**USB Auto-Redirection Settings**

- When a session starts, connect devices automatically
- When a new device is connected while a session is running, connect the device automatically

Version 23.1.0.24

[Citrix Workspace app for Chrome Third Party Notices](#)[Send Feedback](#)**注:**

- この機能は、オンプレミスとクラウドの環境をサポートし、管理対象 Chrome ユーザーのみが利用できます。

**2301 で解決された問題**

- クラウド展開では、強化された PDF 印刷機能が正常に動作しません。印刷プレビューは、同じウィンドウではなく新しいウィンドウで開きます。[RFHTMCRM-8672]
- Citrix Virtual Apps and Desktops バージョン 2206 以降を使用すると、Web カメラのリダイレクトが機能しません。最新の修正プログラムにより、バージョン 2301 以降の ChromeOS 向け Citrix Workspace アプリから Web カメラのリダイレクトが正常に行われるようになりました。[RFHTMCRM-8580]
- Citrix Virtual Apps and Desktops バージョン 2203 以降を使用すると、VDA セッションが乱れて表示されることがあります。[RFHTMCRM-8657]
- Chromebook を使用して、最適化された Microsoft Teams から通話しようとする、通話が正常に機能しません。次のエラーメッセージが表示されます:

「Sorry, it wasn't possible to connect. (申し訳ありません。接続できませんでした。)」[CVADHELP-21670]  
[CVADHELP-21500]

## 既知の問題

### 2402.1 の既知の問題

- サービス継続性機能は、カスタムドメイン URL では機能しない可能性があります。[RFHTMCRM-12363]
- 一時ファイルに依存するアプリを使用してファイルをダウンロードしたり、VDA からマップされたドライブ内のファイルを変更したりしようとする、データが破損する可能性があります。たとえば、ブラウザ、Excel などの Microsoft Office アプリなどの場合です。[RFHTMCRM-12156] [RFHTMCRM-11474]
- セッション中に、音質が低下する場合があります。オーディオストリームのピッチが自動的に変更される場合があります。

この問題を回避するには、属性 **AudioRedirectionV4** を **false** に設定します。**AudioRedirectionV4** を無効にする方法の詳細な手順については、「[オーディオデバイスのプラグアンドプレイのサポート](#)」セクションを参照してください。[CVADHELP-24722]

### 2402 の既知の問題

- 一時ファイルに依存するアプリを使用してファイルをダウンロードしたり、VDA からマップされたドライブ内のファイルを変更したりしようとする、データが破損する可能性があります。たとえば、ブラウザ、Excel などの Microsoft Office アプリなどの場合です。[RFHTMCRM-12156] [RFHTMCRM-11474]
- ユーザーが（意図的に、または非アクティブであることによって）ストアページからサインアウトし、同じストアページに再度サインインすると、ストアページが空白になるか、読み込み中アイコンがいつまでも表示されることがあります。この問題は、サービス継続性機能が有効なクラウド展開で発生します。

回避策として、ストアページの再読み込みアイコンをクリックします。[RFHTMCRM-12212]

- セッション中に、音質が低下する場合があります。オーディオストリームのピッチが自動的に変更される場合があります。

この問題を回避するには、属性 **AudioRedirectionV4** を **false** に設定します。**AudioRedirectionV4** を無効にする方法の詳細な手順については、「[オーディオデバイスのプラグアンドプレイのサポート](#)」セクションを参照してください。[CVADHELP-24722]

### 2312 の既知の問題

- サービス継続性機能を有効にし、クラウド環境の停止が発生すると、実際のデスクトップアイコンまたはアプリセッションのアイコンではなく、Citrix Workspace アプリのアイコンが Chrome シェルフに表示されます。[RFHTMCRM-11647]

### 2310 の既知の問題

- Citrix Workspace アプリを使用してデスクトップセッションを開始すると、UI をブロックする緑色の領域が表示画面が現れます。この問題は、起動したデスクトップ内でアプリケーションウィンドウを移動すると発生する可能性があります。[CVADHELP-23377]
- キオスクモードでは、セッションが自動的に開始されない場合があります。[CVADHELP-23698]

### 2309 の既知の問題

- Chromebook デバイスでは、Citrix Workspace アプリはデュアルスタック Wi-Fi ネットワーク上で IPv6 から IPv4 にフォールバックしません。[CVADHELP-22537]

### 2203 の既知の問題

- 一部の Citrix Virtual Apps and Desktops または XenDesktop では、Web カメラのリダイレクトが機能しない場合があります。[HDX-39396]

### 制限事項

- ChromeOS 向け Citrix Workspace アプリは、複数のモニターでの全画面 H.264 モードをサポートしていません。
- Microsoft Teams 最適化を使用した画面共有中、共有ウィンドウの周囲の赤い枠線は表示されません。
- Citrix Studio で **[Use Hardware Encoding for Video Codec]** が **[Enabled]** に設定されている場合、Intel vGPU VDA を使用したセッション中に画面が緑色で表示されることがあります。[RFHTMCRM-5521]
- Microsoft Windows 7 VDA を介したマルチモニターセッションでは、拡張モニターが黒く表示されます。また、マウスカーソルが正しくレンダリングされない場合があります。幅と高さが 4800 ピクセル未満のディスプレイ解像度を組み合わせて選択することをお勧めします。[RFHTMCRM-5539]
- サーバーは、Graphics-Thinwire YUV444 設定が構成されている場合でも、YUV420 にフォールバックします。グラフィックが豊富なアプリケーションは、YUV420 の範囲によって制限を受けます。[RFHTMCRM-5520]
- Google ID プロバイダー (ID プロバイダー) でのシングルサインオン (SSO) はサポートされていません。
- Citrix Workspace アプリにサインインしようとする、サインインプロセス中に問題が発生する可能性があります。エラーメッセージ「ERR\_TOO\_MANY\_REDIRECTS」が表示されます。  
この問題は、Google ID プロバイダーを使用しているときに発生します。[CVADHELP-19362]
- 最適化された Microsoft Teams ビデオ通話で、3 番目の参加者を追加すると、最初の参加者 2 人のうちいずれかのビデオ画面で何も表示されなくなります。この問題は、最初の 2 人の参加者が ChromeOS を使用し、3 番目の参加者が別の OS を使用している場合に発生します。[RFHTMCRM-7408]

- セッション中に、複数のオーディオデバイスを接続すると、音声は 1 つのデバイスからしか聞こえません。他のオーディオデバイスに切り替えることができない場合があります。[HDX-49312]
- セッション中に、ツールバーから切断してから以前のセッションに再接続すると、音声は聞こえない場合があります。[HDX-49313]
- エンドユーザーが Imprivata を使用して ID プロバイダー (IdP) として構成されたストアにサインインすると、クライアント検出画面が表示されます。ただし、ユーザーが **[Citrix Workspace アプリを検出]** をクリックすると、次のエラーが表示されます：

「receiver links are blocked.」

回避策として、ChromeOS 向け Citrix Workspace アプリを再読み込みします。[CVADHELP-22026]

- ネットワークを切り替えたときに、Wi-Fi 接続の 1 つがインターネットに接続できない場合、セッション画面の保持機能は適切に機能しません。[RFHTMCRM-12349]
- Citrix Workspace アプリの再読み込みボタンをクリックするたびに、リースファイルの同期タイマーがリセットされます。このアクションは、エンドユーザーへのサービス継続性機能の提供に影響を与えます。[RFHTMCRM-12499]
- ChromeOS 向け Citrix Workspace アプリからサインオフして再度サインインした後、リースファイルのダウンロードに失敗します。[RFHTMCRM-12492]
- キオスクモードではサービス継続性機能はサポートされません。[RFHTMCRM-12518]

### 廃止

廃止済みの項目については、「[廃止済み](#)」ページを参照してください。

### 古いドキュメント

保守終了 (EOL) に達した製品リリースについては、[古いドキュメント](#)を参照してください。

## Technical Preview

Technical Preview の機能は、非実稼働環境または制限のある稼働環境で使用でき、お客様がフィードバックを共有する機会を提供します。Technical Preview の機能のサポートは行っていませんが、改善に関するフィードバックをお待ちしております。重要度と重大度により、フィードバックに対応する場合があります。

## Technical Preview の機能





June 18, 2024



Technical Preview の機能は、非実稼働環境または制限のある稼働環境で使用でき、お客様がフィードバックを共有する機会を提供します。Technical Preview の機能のサポートは行っていませんが、改善に関するフィードバックをお待ちしております。重要度と重大度により、フィードバックに対応する場合があります。

## Technical Preview の機能の一覧

次の表に、Technical Preview の機能を示します。これらの機能は、リクエストベースで提供される Preview 機能です。これらの機能についてフィードバックを提供する場合は、対応するフォームにご記入ください。

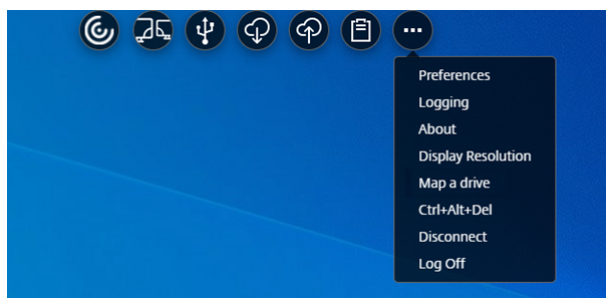
タイトル	利用できる最小バージョン	有効化フォーム（アイコンをクリック）	フィードバックフォーム（アイコンをクリック）
<a href="#">セッション内ツールバーの機能が向上しました</a>	2405	機能を構成することができません	
<a href="#">アダプティブトランスポート</a>	2311		
<a href="#">アクセシビリティと TalkBack</a>	2307	有効化は不要	

### セッション内ツールバーの機能が向上しました

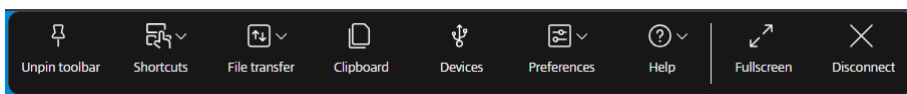
これは、**2405** リリース以降の **Technical Preview** 段階の機能です。

2405 バージョン以降では、デスクトップセッションを開始すると、強化されたツールバー UI が表示されます。セッション内ツールバー UI の外観と操作性が変更されました。ツールバー UI は、オプションをユーザーフレンドリーな方法で整理することで、エンドユーザーのエクスペリエンスを向上させるように特別に設計されています。

### 古いツールバー UI



### 新しいツールバー UI



#### 注:

この機能はデフォルトでは無効になっています。この機能を有効にするには、構成手順を実行してください。この機能に関するフィードバックを提供するには、[Podio のフォーム](#)をクリックします。

### 構成

Google 管理者ポリシーを使用して、新しいツールバー UI を有効にすることができます。

**Google 管理ポリシー** 管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用して機能を有効にできます:

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [**Chrome** 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を **engine\_settings** キーの下の **policy.txt** ファイルに追加します。

#### 注:

この構成は以下にも適用できます:

- [Device] > [Chrome] > [Apps and extensions] > [Users and browsers] から、拡張機能を検索して、拡張機能のポリシーを見つけます。
- [Device] > [Chrome] > [Apps and extensions] > [Kiosks] から、拡張機能を検索して、拡張機能のポリシーを見つけます。
- [Device] > [Chrome] > [Apps and extensions] > [Managed guest sessions] から、拡張機能を検索して、拡張機能のポリシーを見つけます。

このような JSON データの例を次に示します:

```
1 {
2
3     "engine_settings": {
4
5         "ui": {
6
7             "toolbar":
8                 {
9                 "switchToNewToolbar": true
10                }
11        }
```

```
12     }
13
14     }
15
16 }
17
18 <!--NeedCopy-->
```

#### 4. 変更を保存します。

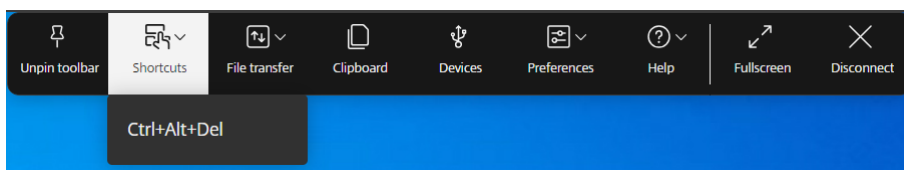
### アイコンと操作

エンドユーザーは次の操作を実行できます：

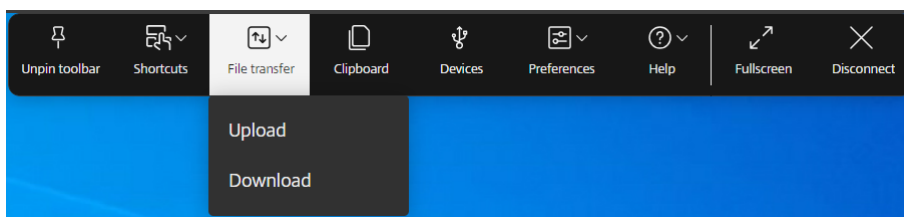
注：

アイコンは、組織の管理者がその機能を有効にしている場合にのみ、エンドユーザーに表示されます。

- ツールバーのノッチ - アプリまたはデスクトップセッションを開始すると、画面の上部にツールバーのノッチが表示されます。ノッチをクリックすると、ツールバーが固定されていない状態で表示されます。ツールバーのノッチを画面の任意の側にドラッグして再配置します。マウスを放すと、ノッチは自動的に最も近い端に配置されます。
- 固定-固定すると、ツールバーを画面の任意の側にドラッグして再配置できます。マウスを放すと、ノッチは自動的に最も近い端に配置されます。ツールバーを固定するメリットは、ツールバーアイコンに関連する操作を完了した後、ツールバーがノッチ内に最小化されないことです。
- 固定を解除-ツールバーの固定を解除すると、ツールバーアイコンに関連する操作を完了した後に、ツールバーがノッチ内に最小化されます。
- ショートカットキー-ボタンをクリックするだけで、**Ctrl + Alt + Del** キーの機能を実行できます。このオプションにより、ユーザーはサインアウト、ユーザーの切り替え、システムのロック、またはタスクマネージャーへのアクセスが容易になります。



- ファイル転送 - ユーザーのデバイスとセッション間でファイルをアップロードまたはダウンロードできます。詳しくは、「[ファイルの処理](#)」を参照してください。

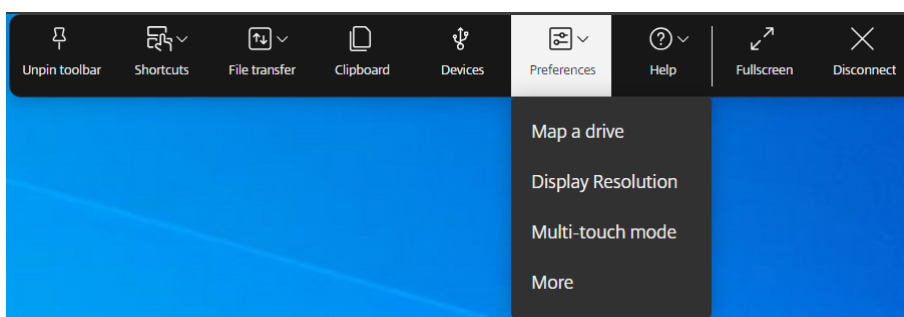


- クリップボード-クリップボードオプションを使用すると、プレーンテキストと HTML データを VDA からローカルデバイスにコピーして貼り付けたり、その逆方向の操作を実行したりできます。詳しくは、「[クリップボード](#)」を参照してください。
- デバイス-クリックすると **USB** デバイスダイアログボックスが開きます。ローカルデバイスに接続されている USB デバイスを表示するには、[追加] をクリックします。ダイアログボックスには、セッションにリダイレクトできるデバイスが一覧表示されます。USB デバイスをリダイレクトするには、適切なデバイスを選択して [接続] をクリックします。詳しくは、「[USB デバイスリダイレクト](#)」を参照してください。

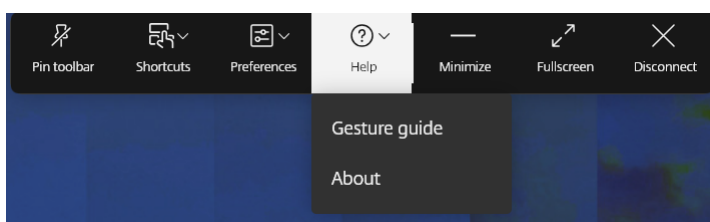
注:

IT 管理者がポリシー設定を介して USB デバイスに接続するためのアクセスを提供している場合にのみ、デバイスアイコンが表示されます。

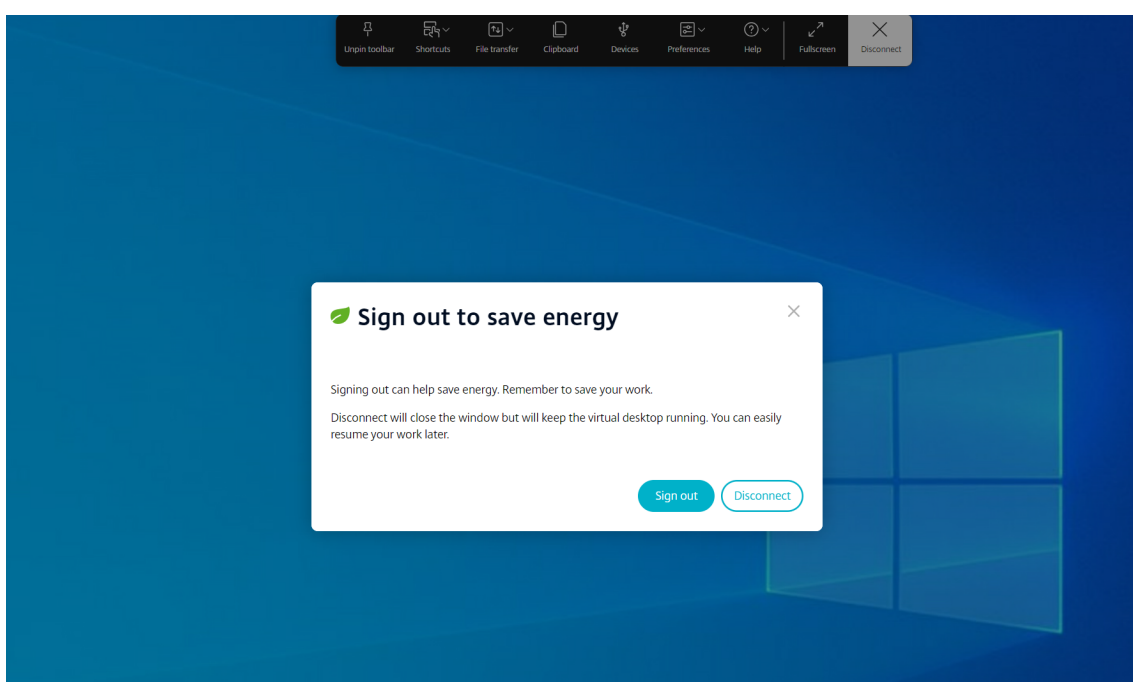
- 基本設定-次のように基本設定を設定できます。次の 4 つのオプションが表示されます:



- ドライブをマップする-クライアントドライブマッピング (CDM) 機能を使用すると、Citrix Workspace アプリからローカルフォルダーやドライブにアクセスできます。詳しくは、「[ファイルの処理](#)」を参照してください。
  - 画面解像度-セッション表示の解像度のサイズを選択します。デフォルトでは、画面の解像度は [全画面-自動] に設定されています。
  - マルチタッチモード-クリックするとマルチタッチモードが使用されます。パンモードとマルチタッチモードを切り替えることができます。このオプションはタッチスクリーンデバイスに適用できます。詳しくは、「[タッチとモビリティのサポート](#)」を参照してください。
  - 詳細-ソフトキーボードボタンと Citrix カスタマーエクスペリエンス向上プログラム (CEIP) に関する設定を表示します。
- ヘルプ-次の 3 つのオプションが表示されます:



- ジェスチャガイド-指のタップを使用する方法に関するジェスチャガイドが表示されます。このオプションはタッチスクリーンデバイスに適用できます。
- バージョン情報-使用している Citrix Workspace アプリの現在のバージョンを表示します。
- 最小化-セッションウィンドウを最小化できます。
- フルスクリーン --画面をウィンドウ表示からフルスクリーン表示に切り替えることができます。マルチモニターのセットアップを使用している場合、フルスクリーンボタンはセットアップ全体に画面を拡張し、マルチモニターボタンとしても機能します。
- 切断-切断操作により仮想デスクトップは実行を継続します。サインアウトして電力を節約する。詳しくは、「[Citrix Workspace アプリでのサステナビリティに関する取り組み](#)」を参照してください。



### アダプティブトランスポート

これは、**2311** リリース以降の **Technical Preview** 段階の機能です。

バージョン 2311 以降、ChromeOS 向け Citrix Workspace アプリはアダプティブトランスポート機能をサポートします。

アダプティブトランスポートは、サーバーのスケラビリティを維持しながら、要求の厳しい長距離接続で優れたユーザーエクスペリエンスを提供します。この機能は、Web ベースのプラットフォームで高品質の HDX エクスペリエンスを提供します。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[アダプティブトランスポート](#)」を参照してください。

### メモ:

- この機能はデフォルトでは無効になっています。
- これは、リクエストベースで提供されるプレビュー機能です。ご使用の環境でこれを有効にするには、[Podio フォーム](#)に記入してください。

### システム要件

アダプティブトランスポートと EDT を使用するための要件は次のとおりです:

- コントロールプレーン
  - ☒ Citrix DaaS (旧称: Citrix Virtual Apps and Desktops サービス)
  - ☒ Citrix Virtual Apps and Desktops 1912 以降
- Virtual Delivery Agent
  - ☒ バージョン 1912 以降 (2203 以降を推奨)
  - ☒ バージョン 2012 は、Citrix Gateway Service で EDT を使用するために必要な最小バージョンです
- StoreFront
  - ☒ バージョン 3.12.x
  - ☒ バージョン 1912.0.x
- Citrix Gateway (ADC)
  - ☒ 13.1.17.42 以降 (推奨)
  - ☒ 13.0.52.24 以降
  - ☒ 12.1.56.22 以降
- ファイアウォール (VDA の観点から)
  - ☒ UDP 1494 受信-セッション画面の保持が無効になっている場合
  - ☒ UDP 2598 受信-セッション画面の保持が有効になっている場合
  - ☒ UDP 443 受信-ICA 暗号化 (DTLS) で VDA SSL を有効にしている場合
  - ☒ UDP 443 送信-Citrix Gateway サービスを使用している場合。詳しくは、[Citrix Gateway サービスのドキュメント](#)を参照してください。

### 管理者の構成

- Citrix ポリシーで **HDX** アダプティブトランスポート設定を構成するには、Citrix Virtual Apps and Desktops ドキュメントの「[構成](#)」セクションを参照してください。

- アダプティブトランスポート機能は次の方法で構成できます：

### Google 管理ポリシー

管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用して機能を有効にできます：

1. Google 管理ポリシーにサインインします。
2. この構成は以下に適用できます：
  - [Device] > [Chrome] > [Apps and extensions] > [Users and browsers] から、拡張機能を検索して、拡張機能のポリシーを見つけます。
  - [Device] > [Chrome] > [Apps and extensions] > [Kiosks] から、拡張機能を検索して、拡張機能のポリシーを見つけます。
  - [Device] > [Chrome] > [Apps and extensions] > [Managed guest sessions] から、拡張機能を検索して、拡張機能のポリシーを見つけます。

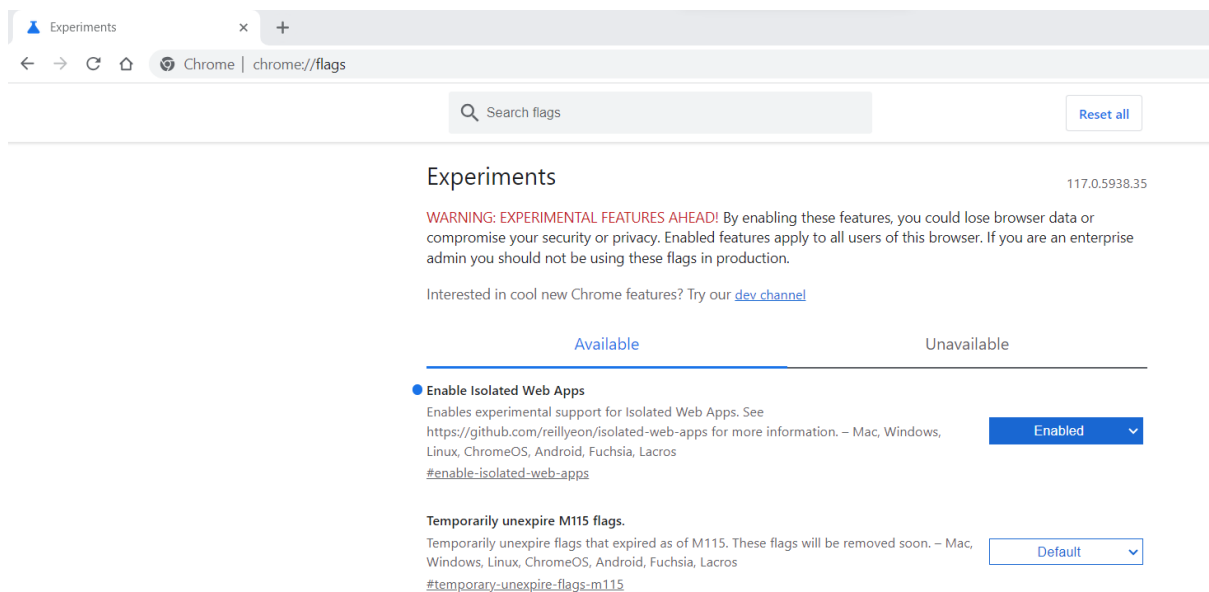
このような JSON データの例を次に示します：

```
1  {
2
3  "settings": {
4
5  "Value": {
6
7      "settings_version": "1.0",
8      "engine_settings": {
9
10         "features": {
11
12             "edt": {
13
14                 "enabled": true
15             }
16         }
17     }
18 }
19 }
20 }
21 }
22 }
23 }
24 }
25 }
26 }
27 <!--NeedCopy-->
```

3. 変更を保存します。

### エンドユーザー構成

アダプティブトランスポート機能を有効にするには、Google Chrome ブラウザーのアドレスバーに「**chrome://flags**」を入力します。次のスクリーンショットに示すように、**[Enable Isolated Web Apps]** オプションを有効にします：



### アクセシビリティと TalkBack

これは、**2307** リリース以降の **Technical Preview** 段階の機能です。

Citrix Workspace アプリは、TalkBack 機能により強化されたユーザーエクスペリエンスを提供します。TalkBack 機能は、画面を見ることが困難なエンドユーザーをサポートします。UI の使用時に、ナレーターが画面要素を読み上げます。

ChromeOS ナレーター (ChromeVox) を使用する場合、エンドユーザーはキーボードのショートカット (Ctrl + Alt + Z) でナレーターをオンにします。ナレーターをオフにするには、同じキーの組み合わせを使用します。

#### 注：

- デフォルトでは、この機能は無効になっています。

### 構成

アクセシビリティ機能は次のいずれかの方法で実行できます：

- Configuration.js
- Google 管理ポリシー



**Configuration.js configuration.js** ファイルを使用してアクセシビリティ機能を有効にするには、次の手順を実行します：

1. **configuration.js** ファイルを、**ChromeApp** ルートフォルダーで見つけます。

メモ：

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

2. **configuration.js** ファイルを編集し、**accessibility** 属性を追加します。**enable** 属性を **true** に設定します。

このような JSON データの例を次に示します：

```

1  'features' :
2  {
3
4      'accessibility': {
5
6          'enable': true
7      }
8  ,
9  }
10
11
12 <!--NeedCopy-->

```

3. 変更を保存します。

**Google 管理ポリシー** 管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用して機能を有効にできます：

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [**Chrome** 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を engine\_settings キーの下の policy.txt ファイルに追加します。

このような JSON データの例を次に示します：

```

1  'features' :
2  {
3
4      'accessibility': {
5
6          'enable': true

```

```
7      }  
8      ,  
9      }  
10  
11  
12 <!--NeedCopy-->
```

4. 変更を保存します。

## インストールの前提条件

May 16, 2024

### システム要件と互換性

#### 要件

すべてのデバイスは、オペレーティングシステムのハードウェア要件を満たしている必要があります。

ユーザーのデバイスが Citrix Workspace アプリを使用してデスクトップやアプリにアクセスするには、最新の Google Chrome オペレーティングシステム (OS) が必要です。Citrix は、Google ChromeOS の Stable チャンネルの最新 Citrix Workspace アプリを使用することをお勧めします。

ChromeOS 向け Citrix Workspace アプリは ChromeOS 上でのみサポートされます。Citrix Workspace アプリで、ChromeOS Flex オペレーティングシステムもサポートされるようになりました。

**Chrome** アプリを追加して開く ChromeOS 向け Citrix Workspace アプリは ChromeOS 上でのみサポートされます。Chromebook では、[Chrome ウェブストア](#)でアプリを追加して開くことができます。詳しくは、[Google のサポート](#)記事を参照してください。

#### メモ:

- Chrome ウェブストアの Chrome アプリは Chromebook でのみサポートされ、2022 年 12 月以降は Windows、Mac、Linux では動作しなくなっています。
- 製品終了 (EOL) した Chromebook デバイスは、Google ChromeOS の最新バージョンには更新されません。EOL デバイスは、ChromeOS 向け Citrix Workspace アプリのすべての更新をサポートしているわけではありません。Citrix は、Google Chrome オペレーティングシステムの最新バージョンを推奨しサポートします。

### サポートに関するマトリックス

ChromeOS 向け Citrix Workspace アプリは StoreFront の次のバージョンを介したデスクトップおよびアプリケーションへのアクセスをサポートします。ストアには、Citrix Receiver for Web サイトを介してアクセスする必要があります。ChromeOS 向け Citrix Workspace アプリは、ストア URL または XenApp Services URL のいずれかを使った StoreFront ストアへの直接アクセスはサポートしません。

- StoreFront 2.5 以降

ChromeOS 向け Citrix Workspace アプリを使って次の製品バージョンにより配信されるデスクトップやアプリケーションにアクセスできます：

- XenApp および XenDesktop 7.6 以降

### ユーザー接続の保護

実稼働環境では、Citrix Workspace for Web サイトとユーザーのデバイス間の通信を Citrix Gateway および HTTPS で保護することをお勧めします。ChromeOS 向け Citrix Workspace アプリが展開される環境においては、キーサイズが 1024 ビット以上の SSL 証明書を使用することを Citrix ではお勧めします。ChromeOS 向け Citrix Workspace アプリを次のバージョンの Citrix Gateway と組み合わせると、ユーザーはパブリックネットワークからデスクトップおよびアプリケーションにアクセスできます。

- NetScaler Gateway 10.5 以降

ChromeOS 向け Citrix Workspace アプリは、HDX Insight 分析を使って CloudBridge Insight Center で表示することに加えて、圧縮およびプリンター圧縮を無効にする CloudBridge をサポートするようになりました。

- CloudBridge 7.4 以降

#### 注：

ChromeOS 向け Citrix Workspace アプリで SSL 対応の VDA に接続できない場合は、「[VDA 上の TLS 設定](#)」を参照してください。最適な暗号の組み合わせを構成します。

## Microsoft Teams の最適化要件

### 最小バージョン：

- Microsoft Teams による音声通話、ビデオ通話、画面共有の最適化は、リリース 2105.5 以降で一般提供されます。

[最新バージョン](#)の ChromeOS 向け Citrix Workspace アプリを使用することをお勧めします。デフォルトでは、画面共有は無効になっています。画面共有を有効にする手順については、「[設定](#)」を参照してください。

- VDA バージョン 1906 以降。

ハードウェア:

ピアツーピアのビデオ会議通話または画面共有の場合、最小要件は次のとおりです:

- 720p HD 解像度をサポートする 2.4GHz クアッドコア CPU を搭載した Intel® Core™ i3 プロセッサ。

## インストール

May 16, 2024

エンドユーザーと IT 管理者の両方が ChromeOS 向け Citrix Workspace アプリをインストールできます。

### Chrome ウェブストアからインストールする

ユーザーは、次のように Chrome ウェブストアから ChromeOS 向け Citrix Workspace アプリをインストールできます:

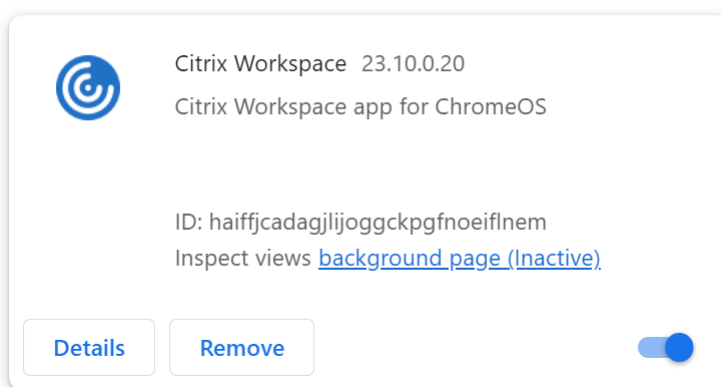
1. リンク「<https://chromewebstore.google.com/detail/citrix-workspace/haiffjcadaglijoggckpgfnoeiflnem>」をクリックします。

ChromeOS 向け Citrix Workspace アプリの Web ストアページが表示されます。

2. [**Chrome** に追加] をクリックします。

アプリがインストールされています。Chrome ブラウザーで `chrome://extensions` に移動して、Chrome アプリを表示します。

Chrome Apps



3. ChromeOS ランチャーで「Citrix Workspace アプリ」を検索して使用します。

### 注

アプリの使用を開始するには、エンドユーザーは有効なストア URL またはメールアドレスを入力します。通常、IT 管理者はストア URL アドレスを提供するか、関連するストア URL を使用してメールアドレスを設定します。組織のガイドラインに従ってください。

### 手動インストール

ChromeOS 向け Citrix Workspace アプリには多くの展開オプションがあります。

- Google App 管理コンソールでは、Google ポリシーを使用して Citrix Workspace を構成できます。ChromeOS の構成について詳しくは、Knowledge Center の[CTX141844](#)を参照してください。
- ChromeOS 向け Citrix Workspace アプリを再パッケージして、生成済みの Citrix Workspace 構成 (.cr) ファイルをパッケージ内に含めることができます。\*.cr ファイルには、ユーザーのデスクトップおよびアプリケーションを提供する Citrix Gateway および Citrix Receiver for Web サイトに関する接続の詳細が含まれています。ユーザーは `chrome://extensions` を参照してから、再パッケージしたアプリ (.crx) ファイルを Chrome ウィンドウにドラッグして ChromeOS 向け Citrix Workspace アプリをインストールします。アプリが事前構成されるため、ユーザーは Citrix Workspace アプリをインストールした後、追加構成をすることなく使用を開始できます。

次の方法で、管理者がエンドユーザーにカスタム ChromeOS 向け Citrix Workspace アプリを配信できます：

- Google 管理コンソールを使い、Google Apps for Business を介してユーザー用に再パッケージしたアプリケーションを公開します。
- メールなどそのほかの方法で、ユーザーに.crx ファイルを提供します。
- ユーザーは、Chrome ウェブストアから ChromeOS 向け Citrix Workspace アプリをインストールできます。詳しくは、「[Chrome ウェブストアからインストールする](#)」を参照してください。

インストールしたら、ユーザーのデスクトップおよびアプリを提供する Citrix Gateway および Citrix Receiver for Web サイトに関する接続の詳細を、Chrome 向け Citrix Workspace アプリで構成する必要があります。この機能は、2 とおりの方法で実行できます：

- 適切な接続の詳細を含む\*.cr ファイルを生成し、このファイルをユーザーに配布します。ChromeOS 向け Citrix Workspace アプリを構成するには、ユーザーが\*.cr ファイルをダブルクリックして、プロンプトが表示されたら [追加] をクリックします。StoreFront から.crx ファイルを生成する方法については、「[ユーザー用のストアプロビジョニングファイルのエクスポート](#)」を参照してください。
- ユーザーが初めて ChromeOS 向け Citrix Workspace アプリを起動するときに、手動で入力する URL を指示します。

### 再パッケージ

ユーザーに対する展開処理を簡素化するには、新しい **.cr** ファイルで ChromeOS 向け Citrix Workspace アプリを再パッケージして、ChromeOS 向け Citrix Workspace アプリで環境に適した接続の詳細を再構成できます。ユーザーは ChromeOS 向け Citrix Workspace アプリをインストールすると、追加構成を一切することなくすぐにその使用を開始できます。

1. ChromeOS 向け Citrix Workspace アプリのパッケージ化されていないバージョンを適切な場所にダウンロードします。
2. サンプルの構成ファイルをダウンロードして、環境に適合するようにそれをカスタマイズします。
3. 修正した構成ファイルの名前を `default.cr` と変更し、ChromeOS 向け Citrix Workspace アプリのルートディレクトリにコピーします。

ChromeOS 向け Citrix Workspace アプリを再パッケージする場合、別の名前または別の場所にある構成ファイルは含まれません。

4. デフォルトでは、セッション内でツールバーが有効になっています。セッション内ツールバーを無効にする場合は、次の手順を実行します。

注: `configuration.js` ファイルに変更を加える前に、バックアップを作成することをお勧めします。

- a) テキストエディターを使って Chrome 向け Citrix Workspace アプリルートディレクトリにある `configuration.js` ファイルを開きます。
- b) ファイル内で次のセクションを検索します。

```
pre codeblock 'appPrefs':{ 'chromeApp':{ 'ui': { 'toolbar': {  
  'menubar':true, 'clipboard': false <!--NeedCopy-->
```

- c) `menubar` 属性の設定を **false** に変更します。

注: 以前の構成を上書きするには、Google 管理コンソールを使用してポリシーをプッシュすることをお勧めします。

5. ChromeOS 向け Citrix Workspace アプリは、デフォルトで Chromebook のファイルアプリを使用してあらゆる拡張子のファイルを開くことができます。Chromebook では、Google ドライブでファイルを開くために VDA の `FileAccess` コンポーネントを使用できます。

管理者がこのオプションを無効にして Citrix Workspace アプリのパッケージ化されていないファイルをダウンロードする場合、`manifest.json` の "file handlers" セクションを次のように編集します:

```
1 "file handlers" : {  
2  
3   "text" :  
4     "extensions" : [  
5       "ica",  
6       "cr"  
7     ]
```

```

8         }
9
10    }
11
12 <!--NeedCopy-->

```

6. Chrome で `chrome://extensions` に移動し、ページ右上隅にある [デベロッパーモード] チェックボックスをオンにして [拡張機能をパッケージ化] ボタンをクリックします。

セキュリティ上の理由により、StoreFront は既知の ChromeOS 向け Citrix Workspace アプリインスタンスからの接続のみを受け入れます。再パッケージしたアプリケーションを許可リストに登録して、ユーザーが Citrix Receiver for Web サイトに接続できるようにする必要があります。

7. StoreFront サーバーで、テキストエディターを使って Citrix Receiver for Web サイトの `web.config` ファイルを開きます。このファイルは、Web ディレクトリ「**C:\inetpub\wwwroot\Citrix\storename**」にあります。ストア名はストアの作成時に指定した名前です。

8. ファイル内で次の要素を検索します。

```

pre codeblock <html5 ... chromeAppOrigins="chrome-extension://
haiffjcadagjlijoggckpgfnoeiflnem"... /> <!--NeedCopy-->

```

9. **chromeAppOrigins** 属性の値を `chrome-extension://packageid` に変更します。ここで **packageid** は、再パッケージしたアプリケーションに対して生成された ID です。

## バックアップビルドおよび早期アクセスリリースビルド

ChromeOS 向け Citrix Workspace アプリのバックアップビルドおよび早期アクセスリリースビルドを使用するオプションがあります。バックアップビルドオプションは、実稼働ビルドで進行中の問題がある場合にビジネスの継続性を提供します。先に進む前に、次のビルド ID について理解しておいてください。

- **haiffjcadagjlijoggckpgfnoeiflnem**: Chrome ウェブストアにある ChromeOS 向け Citrix Workspace アプリの公開バージョンの ID です。
- **lbfgjakkeeccemhonnolnmglmfmccaag**: ChromeOS 向け Citrix Workspace アプリの早期アクセスリリース (EAR) バージョンの ID です。
- **anjihnbmjbbpofafpmklejenkgnjfcdi**: ChromeOS 向け Citrix Workspace アプリのバックアップビルドの ID です。バックアップビルドには、現在の製品リリースより前の異なるバージョン ID のリリース内容が含まれています。

バックアップビルドにアクセスするには

バックアップビルドにアクセスするには、次の手順を実行します：

1. リンク<https://chrome.google.com/webstore/detail/citrix-workspace-backup/anjihnbmjbbpofafpmklejenkgnjfcdi>をクリックします。

Citrix Workspace アプリのバックアップ拡張機能ページが表示されます。

2. [**Chrome** に追加] をクリックします。

アプリがインストールされています。Chrome ブラウザーで `chrome://extensions` に移動して、拡張機能を表示します。

3. ChromeOS ランチャーで「Citrix Workspace アプリ」を検索して使用します。

### EAR ビルドにアクセスするには

EAR ビルドにアクセスするには、次の手順を実行します：

1. リンク「<https://chrome.google.com/webstore/detail/citrix-workspace-backup/lbfgjakkeecce mhonnolnmglmfmccaag>」をクリックします。

ChromeOS 向け Citrix Workspace アプリの拡張機能ページが表示されます。

2. [**Chrome** に追加] をクリックします。

アプリがインストールされています。Chrome ブラウザーで `chrome://extensions` に移動して、拡張機能を表示します。

3. ChromeOS ランチャーで「Citrix Workspace アプリ」を検索して使用します。

### ChromeOS LTS の互換性

より少ない更新を希望する場合、Google は ChromeOS で長期サポート (LTS) バージョンを提供しています。特定の時点で、1 つまたは複数のバージョンの Citrix Workspace アプリが、最新バージョンの ChromeOS LTS と互換性があります。

最新のバグ修正と新機能が有効になった Citrix Workspace アプリのバージョンをお探しの場合は、以下をお勧めします：

- 最新バージョンの Citrix Workspace アプリを使用する
- Stable チャンネルの最新の Google ChromeOS バージョンを使用する。

### 後方互換性

ChromeOS または Citrix Workspace アプリのバグ修正は、ChromeOS LTS バージョンと後方互換性がない場合があります。後方互換性を利用するには、ChromeOS の Stable チャンネルへの切り替えが必要な場合があります。

Citrix または Google が提供する新機能は、それぞれの新しいソフトウェアのバージョンによって異なる場合があります。新機能にアクセスするには、ChromeOS の Stable チャンネルと最新バージョンの Citrix Workspace アプリを使用してください。



### 除外

以下の機能は、ChromeOS LTS との互換性の対象外です：

- Microsoft Teams の最適化
- ブラウザーコンテンツリダイレクト

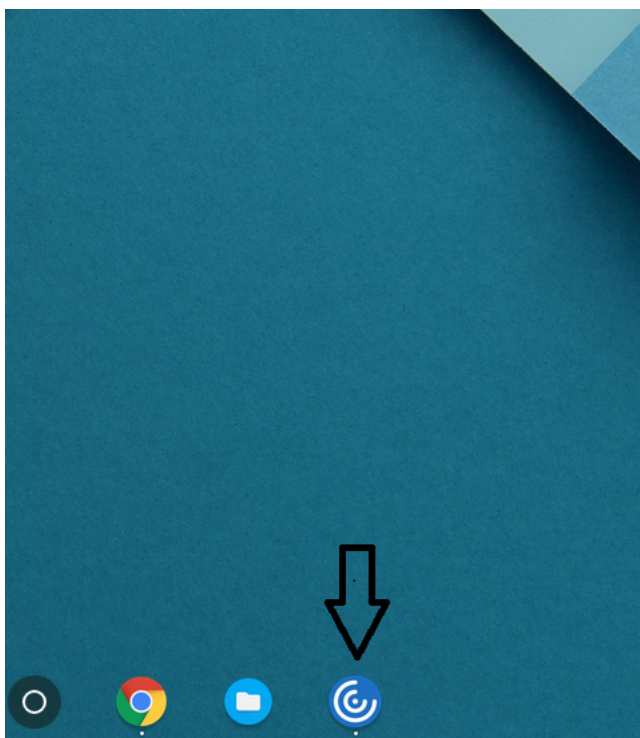
除外された機能の更新は、Stable チャンネルの最新バージョンの ChromeOS と最新バージョンの Citrix Workspace アプリの組み合わせで利用できます。

### 一般的な質問

- 最新の ChromeOS LTS リリースと互換性のある Citrix Workspace アプリのバージョンを確認するにはどうすればよいですか？
  - 最新バージョンは、「[このリリースについて](#)」ページで確認できます。
  - 最新バージョンのインストール可能なファイルは、[Citrix ダウンロードページ](#)で見つけることができます。
- 管理者が、ChromeOS LTS チャンネルでテストするにはどうすればよいですか？
  - 詳しくは、Google ChromeOS の Education ページで[Long-term support releases](#)を参照してください。
- Citrix Workspace アプリを使用する ChromeOS LTS で問題が発生した場合、管理者として何をする必要がありますか？
  - Stable チャンネルの最新バージョンの ChromeOS と最新バージョンの Citrix Workspace アプリの組み合わせで、同じ問題が発生しているかどうかを確認してください。発生している場合は、通常のサポートを利用して問題を報告します。発生していない場合は、問題がないバージョンに更新します。

### アンインストール

Citrix Workspace アプリをインストールして構成した後、Chrome アプリ一覧で Citrix Workspace アイコンを選択します。次の画像に示すように、ChromeOS 向け Citrix Workspace アプリが起動します。デバイスから ChromeOS 向け Citrix Workspace アプリを削除するには、Chrome アプリ一覧で Citrix Workspace アイコンを右クリックし、[アンインストール] を選択します。



## アップグレード

新しい Citrix Workspace アプリにアップグレードするには、次のいずれかの手順を実行します：

- [Citrix のダウンロードページ](#)から Citrix Workspace アプリをダウンロードしてインストールし、Citrix Receiver から Citrix Workspace アプリにアップグレードします。
- お使いの OS のアプリストアを使用して Citrix Workspace アプリをアップグレードします。
- Windows および macOS では、Citrix Receiver の更新プログラムを使用して Citrix Receiver から Citrix Workspace アプリに自動更新します。

Citrix Receiver for Chrome のドキュメントについては、[Citrix Receiver](#)を参照してください。

## 開始

May 16, 2024

## セットアップ

ログインすると、デスクトップおよびアプリケーションが表示されます。ユーザーはリソースを検索でき、アイコンをクリックして新しいウィンドウでデスクトップやアプリケーションを起動できます。

ユーザーが追加のアプリケーションを起動すると、セッションを作成する前に既存のセッション内でアプリケーションを起動できるかどうかを ChromeOS 向け Citrix Workspace アプリによりチェックされます。この機能によって、シングルセッションで多くのアプリケーションにアクセスできるようになります。

ChromeOS 向け Citrix Workspace アプリの機能は、次の方法で構成できます：

- Google 管理ポリシー
- StoreFront の Web.config
- default.ica
- configuration.js

注：

バージョン 1901 以降、スプラッシュスクリーンはユーザーに表示されません。スキーマ “**splashScreen**” : **false**” は、将来のリリースではサポートされなくなりました。このスキーマが存在する場合は、Google 管理ポリシーまたは configuration.js ファイルから削除する必要があります。

### Google 管理ポリシーを使用する

注：

ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、この方法を使用することをお勧めします。

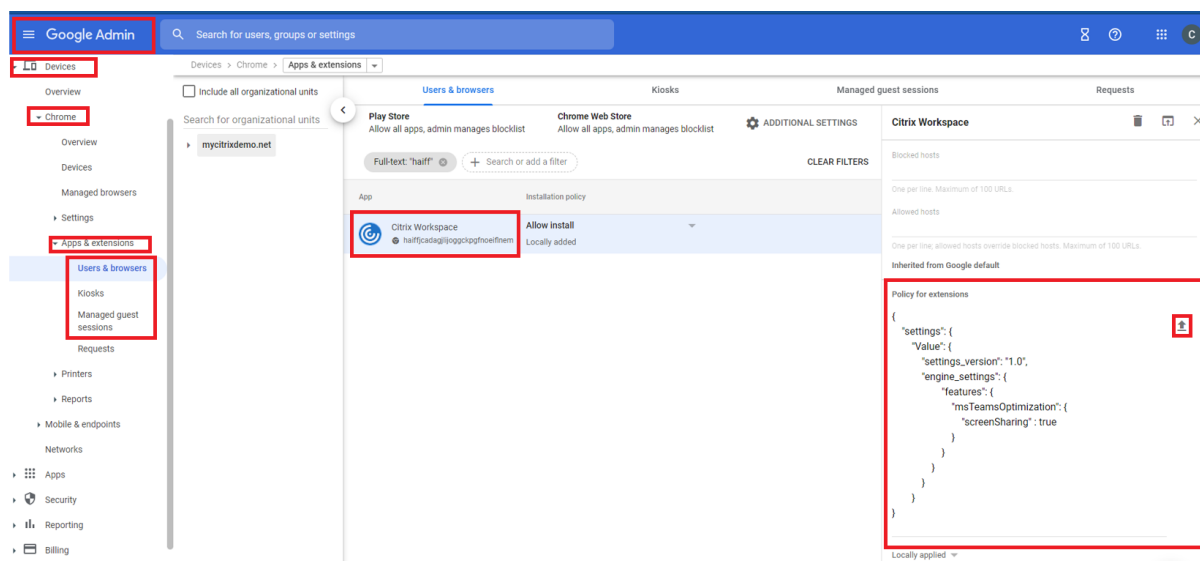
バージョン 2.1 より前は、Google 管理ポリシーを使ってストア/ビーコンに関連する構成のみをプッシュできました。このポリシーについて詳しくは、Knowledge Center の[CTX141844](#)と[CTX229141](#)を参照してください。

ChromeOS 向け Citrix Workspace アプリバージョン 2.1 では、他の Chrome 構成も Google 管理ポリシーからプッシュできます。

### Google 管理コンソールでポリシーをプッシュする方法

Google 管理コンソールでポリシーをプッシュするには、次の手順に従います：

1. **Google** 管理コンソールで、**[Devices]** > **[Chrome]** > **[Apps & extensions]** > **[Users & browsers]** を選択します。
2. Citrix Workspace アプリを検索します(Web ストアアプリ ID、たとえば `haifffjcadagjlijoggckpgfnoeiflne` などを入力します)。
3. Citrix Workspace アプリのアイコンをクリックします。
4. 拡張機能のポリシーが開きます。ポリシーをコピーして貼り付けるか、関連する JSON を含む policy.txt ファイルをアップロードします。
5. **[Save]** をクリックします。
6. 必要に応じて、キオスクおよび管理対象ゲストセッションに対してこの手順を繰り返します。



詳しくは、[Google サポートサイト](#)を参照してください。

### ポリシーの構成の確認

ポリシーが正しくプッシュされていることを確認するには、次の手順を実行します。

1. `chrome://policy/`にアクセスします。
2. `Reload policies`をクリックします。
3. ChromeOS 向け Citrix Workspace アプリのウェブストアID(`haiffjcadagjlijoggckpgfnoeiflnem`)を検索します。

- ポリシーが Google 管理コンソールから正常にプッシュされている場合、ウェブストア ID (`haiffjcadagjlijoggckpgfnoeiflnem`) の下に表示されます。表示されない場合は、ポリシーが正しく構成されていることを確認します。ポリシーを作成または編集するには、[Configuration Utility Tool](#)を使用してください。
- ポリシーがウェブストア ID の下に表示されていてもセッション中に有効にならない場合は、Citrix テクニカルサポートに問い合わせてください。

### web.config ファイルの使用

注:

ChromeOS 向け Citrix Workspace アプリのストアバージョンを使用している場合、**web.config** ファイルによる方法は構成目的でのみ使用することを Citrix ではお勧めします。

Web.config ファイルの方法を使用して構成を変更するには（オンプレミスの StoreFront を使用している場合のみ）:

1. Citrix Receiver for Web サイトの **web.config** ファイルを開きます。このファイルは、`**C:\inetpub\wwwroot\Citrix\<ストア名>Web**` フォルダにあります (\* ストア名 \* はストア作成時に指定したストア名です)。ストア名 >
2. **chromeAppPreferences** フィールドを見つけて、構成の値を JSON 文字列として設定します。

例:

```

1 chromeAppPreferences = {
2
3   "ui": {
4
5     "toolbar": {
6
7       "menubar": false
8     }
9
10    }
11  }
12 }
13
14 <!--NeedCopy-->

```

以下は別のサンプル例です。

```

43 <csrfProtection excludedUserAgents="CitrixReceiver;CitrixWebAPI-NoCSRFToken" />
44 </serverSettings>
45 <clientSettings>
46 <authManager getUsernameURL="Authentication/GetUserName" logoffURL="Authentication/Logoff"
47   changeCredentialsURL="ExplicitAuth/GetChangeCredentialForm"
48   loginFormTimeout="5" webviewReturnURL="ExplicitAuth/Bounce"
49   webviewResumeURL="ExplicitAuth/ResumeForms" allowSelfServiceAccountManagementURL="ExplicitAuth
50 <storeProxy keepAliveURL="Home/KeepAlive">
51 <resourcesProxy listURL="Resources/List" resourceDetails="default" />
52 <sessionsProxy listAvailableURL="Sessions/ListAvailable" disconnectURL="Sessions/Disconnect"
53   logoffURL="Sessions/Logoff" />
54 <clientAssistantProxy getDetectionTicketURL="ClientAssistant/GetDetectionTicket"
55   getDetectionStatusURL="ClientAssistant/GetDetectionStatus" />
56 </storeProxy>
57 <pluginAssistant enabled="true" upgradeAtLogin="false" showAfterLogin="false">
58 <win32 path="http://downloadplugins.citrix.com/Windows/CitrixReceiverWeb.exe" />
59 <macOS path="http://downloadplugins.citrix.com/Mac/CitrixReceiverWeb.dmg"
60   minimumSupportedOSVersion="10.6" />
61 <html5 enabled="Fallback" platforms="Firefox;Chrome;Version/([6-9])\d\d).*Safari;MSIE \d\d;Tri
62   launchURL="clients/HTML5Client/src/SessionWindow.html" preferences=""
63   singleTabLaunch="false" chromeAppOrigins="chrome-extension://haiffjcadaglijjogqckpgfnoeifne
64   chromeAppPreferences = '{\"ui\": {\"toolbar\": {\"menubar\": false, \"displayResolution\": false}}}' />
65 <protocolHandler enabled="true" platforms="(Macintosh|Windows NT).*{(Firefox/([5[2-9]]|[6789][0
66   skipDoubleHopCheckWhenDisabled="false" />
67 </pluginAssistant>

```

### default.ica ファイルの使用

注:

**default.ica** ファイルの方法は、Web Interface ユーザー向けに構成する場合のみ使用することを Citrix ではお勧めします。

ChromeOS 向け Citrix Workspace アプリでは、初期プログラム値なしでカスタム ICA ファイルを使用できません。

**default.ica** ファイルを使用して構成を変更するには:

1. default.ica ファイルを開きます。Web インターフェイスの顧客の場合、このファイルは、**\*\*C:\inetpub\wwwroot\Citrix\<>サイト名 >\conf\default.ica\*\*** ディレクトリにあります。ここで、**\*\*<サイト名 >\*\*** はストアの作成時に指定した名前です。  
StoreFront ユーザーの場合、**\*\*default.ica\*\*** ファイルは、**\*\*C:\inetpub\wwwroot\Citrix\\\\\<ストア名 >\App\_Data\default.ica\*\*** にあります。ここで、**\*\*<ストア名 >\*\*** はストアの作成時に指定した名前です。ストア名 > サイト名 > サイト名 >
2. ファイルの末尾にキー **chromeAppPreferences** を追加して、構成の値を JSON オブジェクトとして設定します。

例:

```
1 chromeAppPreferences={
2
3     "ui":{
4
5         "toolbar": {
6
7             "menubar": false
8         }
9
10        }
11
12        }
13
14 <!--NeedCopy-->
```

サンプル **default.ica** ファイルは、次のようになります:

```

web.config x default.ica x
19
20 [Application]
21 TransportDriver=TCP/IP
22 DoNotUseDefaultCSL=On
23 BrowserProtocol=HTTPOnTCP
24 LocHttpBrowserAddress=!
25 WinStationDriver=ICA 3.0
26 ProxyTimeout=30000
27 AutologonAllowed=ON
28 TWIMode=Off
29 FontSmoothingType=0
30
31 [EncRC5-0]
32 DriverNameWin16=fdc0w.dll
33 DriverNameWin32=fdc0n.dll
34
35 [EncRC5-40]
36 DriverNameWin16=fdc40w.dll
37 DriverNameWin32=fdc40n.dll
38
39 [EncRC5-56]
40 DriverNameWin16=fdc56w.dll
41 DriverNameWin32=fdc56n.dll
42
43 [EncRC5-128]
44 DriverNameWin16=fdc128w.dll
45 DriverNameWin32=fdc128n.dll
46
47 [Compress]
48 DriverNameWin16=fdcompw.dll
49 DriverNameWin32=fdcompn.dll
50
51 chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}'

```

## configuration.js ファイルを使用する

**configuration.js** ファイルは、**ChromeApp** ルートフォルダーにあります。ChromeOS 向け Citrix Workspace アプリを変更する場合は、直接このファイルにアクセスします。

注:

- Citrix では、configuration.js ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- configuration.js ファイルを編集するには、管理者レベルの資格情報が必要です。ファイルを編集した後、ツールバー要素の変更をさらに行うには、アプリを再パッケージしてください。
- キオスクモードでは、ツールバーはデフォルトで非表示になっています。configuration.js ファイルを編集してツールバーを有効にする場合、キオスクモードが無効になっていることを確認してください。ツールバーを有効にするそのほかの方法（default.ica ファイルなど）を使用することを Citrix ではお勧めします。

### ロゴとアイコンのカスタムブランド

必要に応じて、Citrix Workspace アプリのロゴとアプリおよびデスクトップのアイコンをカスタマイズできます。カスタマイズの手順は次のとおりです：

1. [Chrome ウェブストア](#)から ChromeOS 向け Citrix Workspace アプリをインストールします。
2. `/chromeAppUI/resources/images` フォルダに移動します。
3. 次の画像を、同じサイズの必要な画像に置き換えます：
  - icon\_16x16.png
  - icon\_32x32.png
  - icon\_48x48.png
  - icon\_128x128.png
  - icon\_256x256.png
4. **ChromeApp** ルートフォルダに移動し、**manifest.json** ファイルを開きます。
5. 名前と説明の値を必要な文字列に置き換えます。
6. 変更を保存します。
7. [拡張機能](#) ページからアプリを再読み込みします。

### 構成

May 16, 2024

#### フィーチャーフラグ管理

実稼働環境の Citrix Workspace アプリで問題が発生した場合、機能が出荷された後でも、影響を受ける機能を Citrix Workspace アプリで動的に無効にすることができます。無効化するには、フィーチャーフラグと、LaunchDarkly と呼ばれるサードパーティ製サービスを使用します。

#### 構成方法

ファイアウォールまたはプロキシが送信トラフィックをブロックしている場合を除いて、LaunchDarkly へのトラフィックを有効にするために構成する必要はありません。送信トラフィックがブロックされている場合、ポリシー要件に応じて、特定の URL または IP アドレス経由の LaunchDarkly へのトラフィックを有効にします。

LaunchDarkly へのトラフィックと通信は、次の方法で有効化できます：



次の **URL** へのトラフィックを有効にする

- events.launchdarkly.com
- app.launchdarkly.com

**IP** アドレスの許可リストを作成する IP アドレスの許可リストを作成する必要がある場合、現在のすべての IP アドレス範囲については、「[LaunchDarkly のパブリック IP 一覧](#)」を参照してください。この一覧を使用すると、インフラストラクチャの更新に合わせてファイアウォールの構成が自動的に更新されます。インフラストラクチャの変更の状態について詳しくは、[LaunchDarkly Status](#)のページを参照してください。

**LaunchDarkly** サービスを無効にするプロビジョニング オンプレミスストアとクラウドストアの両方で LaunchDarkly サービスを無効にすることができます。

クラウド環境では、管理者は Global App Configuration Service で **enableLaunchDarkly** 属性を **False** に設定することにより、LaunchDarkly サービスを無効にすることができます。

詳しくは、[Global App Configuration Service](#)のドキュメントを参照してください。

オンプレミス環境では、管理者は次のように Google 管理ポリシーを使用して LaunchDarkly サービスを無効にすることができます：

1. Google 管理コンソールにサインインします。
2. [端末管理] > [**Chrome** 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を **engine\_settings** キーの下の **policy.txt** ファイルに追加します。

```
1  "thirdPartyServices": {
2
3
4    "enableLaunchDarkly": false
5  }
6  ,
7
8
9  <!--NeedCopy-->
```

4. [**Save**] をクリックします。

注：

- デフォルトでは、**enableLaunchDarkly** 属性が存在しない場合、LaunchDarkly サービスが有効になります。

オンプレミス環境では、管理者は次のように configuration.js ファイルを使用して LaunchDarkly サービスを無効にすることができます：

注:

- configuration.js ファイルを編集するには、管理者レベルの資格情報が必要です。ファイルを編集した後、アプリを再パッケージして変更を保存してください。

1. **configuration.js** ファイルを開きます。
2. **enableLaunchDarkly** 属性を追加し、この属性を **false** に設定します。

```
1  "thirdPartyServices": {
2
3
4      "enableLaunchDarkly": false
5
6  }
7  ,
8  <!--NeedCopy-->
```

3. **[Save]** をクリックします。

注:

- デフォルトでは、**enableLaunchDarkly** 属性が存在しない場合、LaunchDarkly サービスが有効になります。

### JSON 構成に関する注意

バージョン 2202.1 (22.2.1.8) 以降、Citrix Workspace アプリは、構成をプッシュするために使用できるのは有効な JSON のみを優先します。JSON ファイルを検証するには、次の手順を実行します:

1. JSON データを確認します。リンク「<https://jsonlint.com/>」を使用して検証します。
2. 更新するには、「はじめに」ページに記載されている手順に従ってください:
  - Google ポリシー
  - web.config
  - default.ica
  - configuration.js

[構成ユーティリティツール](#)を使用して有効な JSON 設定を生成し、以下を使用する ChromeOS 向け Citrix Workspace アプリをカスタマイズすることをお勧めします:

- configuration.js
- web.config
- default.ica
- Google ポリシー

注:

JSON 構成が無効な場合、セッション起動に関する問題が発生する可能性があります。

## Chromebook の HTTP プロキシ設定

Chromebook で HTTP プロキシ設定を行っている場合、セッションが開始されない可能性があります。

この問題を解決するには、Google 管理コンソールで **nativeSocket** 設定を無効にし、Desktop Delivery Controller で **WebSocket** 接続ポリシーが有効になっていることを確認します。詳しくは、[WebSocket](#)に関する記事を参照してください。

このような JSON データの例を次に示します:

```
1 {
2
3     "settings": {
4
5         "Value": {
6
7             "settings_version": "1.0",
8             "engine_settings": {
9
10                "transport":
11                    {
12    "nativeSocket": false
13                    }
14                }
15            }
16        }
17    }
18
19 }
20
21 }
22
23 <!--NeedCopy-->
```

警告:

**nativeSocket** 属性を無効にすると WebSocket 接続が有効になり、ネイティブソケットを使用する場合と比較してパフォーマンスに影響を与える可能性があります。

## キオスクモード

ChromeOS 向け Citrix Workspace アプリは、キオスクモードで同じウィンドウ内にすべてのアプリを実行できます。この機能を使って、Citrix Workspace をキオスクモードで実行し、同じモードで任意の Windows アプリやデ

スクリーンを起動できます。さらにキオスクモードを使って、永続 URL を使用する専用 Chrome パッケージとしてリモートアプリやデスクトップを公開できます。

### 構成方法

Chrome 管理パネルでキオスク設定を調節して、この機能を制御できます。この設定は、管理対象の Chrome デバイスにのみ適用されます。

管理されているおよび管理されていない Chrome デバイスでキオスクモードを実行するために Citrix Workspace アプリを有効にする手順については、[Google サポートサイト](#)を参照してください。

Citrix Workspace アプリを展開中の場合は、[Public/unlisted](#)に設定した表示のオプションを使って公開し、キオスクモードとの相互運用性を確保する必要があります。[Chrome Web Store Developer Dashboard](#)にアクセスします。

キオスクモードがアクティブな場合、ストア URL は読み取り専用で、アカウント設定画面を使って編集できません。ただし、この設定は次のいずれかの方法で変更できます：

- `.cr`ファイルを使用してアプリを再パッケージ化する、または
- Google 管理コンソールを使用する。Google ポリシー管理を使用して Google 管理コンソールにアクセスします。

```
1 <Services version="1.0">
2 <Service>
3 <rfWeb>http://your_RfWebURL_or_persistenturl</rfWeb>
4 <Name>Mystore</Name>
5 <Gateways>
6 <Gateway>
7 <Location>https://yourcompany.gateway.com</Location>
8 </Gateway>
9 </Gateways>
10 <Beacons>
11 <Internal>
12 <Beacon>http://yourcompany.internalwebsite.net</Beacon>
13 </Internal>
14 <External>
15 <Beacon>http://www.yourcompany.externalwebsite.com</Beacon>
16 </External>
17 </Beacons>
18 </Service>
19 </Services>
20
21 <!--NeedCopy-->
```

Google 管理コンソールを使っている場合は、Citrix Workspace 構成を含む **policy.txt** ファイルを編集します。“rf\_web” の下の “url” の値を永続 URL と置き換えます。

```
1 {
2
```

```
3   "settings": {
4
5   "Value": {
6
7   "settings_version": "1.0",
8   "store_settings": {
9
10  "beacons": {
11
12  "external": [
13  {
14
15  "url": "http://www.yourcompany.externalwebsite.com"
16  }
17
18  ],
19  "internal": [
20  {
21
22  "url": "http://yourcompany.internalwebsite.net"
23  }
24
25  ]
26  }
27  ,
28  "gateways": [
29  {
30
31  "is_default": true,
32  "url": "https://yourcompany.gateway.com"
33  }
34
35  ],
36  "name": "mystore",
37  "rf_web": {
38
39  "url": " http://your_RfWebURL_or_persistenturl "
40  }
41
42  }
43
44  }
45
46  }
47
48  }
49
50 <!--NeedCopy-->
```

## Global App Configuration Service

このリリース以降、管理者は Global App Configuration Service を使用して次のことができるようになります：

- 一元的にアプリ設定を管理および構成し、デフォルトを設定する。
- 管理対象デバイスと非管理（BYOD）デバイスの両方に設定を適用する
- クラウドユーザー（ドメイン要求）とオンプレミスユーザー（URL 要求）の両方に設定を適用する。

詳しくは、[Global App Configuration Service](#)のドキュメントを参照してください。

メモ：

この機能は、ワークスペースおよび HTTPS ベースのストアでのみ使用できます。

Global App Configuration Service が機能するためには、ユーザーが URL 「<https://discovery.cem.cloud.us>」、 「<https://gacs-discovery.cloud.com>」、 および 「<https://gacs-config.cloud.com>」 にアクセスできることを確認してください。

## カスタマーエクスペリエンス向上プログラム（CEIP）

May 16, 2024

### 構成方法

収集データ	説明	使用目的
構成および使用状況データ	Citrix カスタマーエクスペリエンス向上プログラム（CEIP）では、Citrix Workspace アプリの構成および使用に関するデータが収集され、そのデータが Citrix と Google Analytics に自動的に送信されます。	このデータは、Citrix Workspace アプリの品質、信頼性、およびパフォーマンスを向上させる目的で使用させていただきます。

### 追加情報

Citrix は、お客様のデータを Citrix との契約条件に従って処理します。また、[Citrix Trust Center](#)で利用できる[Citrix Services Security Exhibit](#)で指定されているとおりにお客様のデータを保護します。

Citrix は、CEIP の一環として、Google Analytics を使用して Citrix Workspace アプリから特定のデータを収集します。CEIP データを無効にするかブロックすることができます。[Google Analytics のために収集されたデータの Google での取り扱い方法について確認してください。](#)

注:

欧州連合 (EU)、欧州経済領域 (EEA)、スイス、および英国 (UK) のユーザーのデータは収集されません。

## Citrix および Google Analytics への CEIP データの送信

バージョン 2203 から、エンドユーザーは次のことができるようになりました。

- 利用状況データを Citrix および Google Analytics に送信するかどうかを決定する
- GUI を使用して CEIP をブロックする

## CEIP の無効化

Citrix および Google Analytics への CEIP データの送信を無効にすることができます。これを行うには、次のいずれかの方法を使用します:

- Google Admin Policy を使用して CEIP を無効にする
- configuration.js を使用して CEIP を無効にする

注:

2203 以降のバージョンで CEIP を無効にすると、インストールされている Citrix Workspace アプリのバージョンを含む最小限の情報がアップロードされます。この最小限の情報は、顧客により使用されているさまざまなバージョンの分布状況を Citrix が把握する上で、大変に貴重です。

## Google Admin Policy を使用して CEIP を無効にするには

注:

この手順を実行するには管理者レベルの資格情報が必要です。

1. Google 管理コンソールにログオンします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 手順 4 の後ろに記載された文字列を、policy.txt ファイルの **engine\_settings** キーの下に追加します。
4. [Save] をクリックします。

Google ポリシーについて詳しくは、Knowledge Center の [CTX141844](#) を参照してください。

バージョン 1907 以前では、**ceip** の **enabled** 属性を **false** に設定します。

```
1 "ceip":{
2
3     "enabled":false,
4 }
5
6 <!--NeedCopy-->
```

バージョン 1908 以降では、**analytics** の `enabled` 属性を **false** に設定します。**analytics** キーは、**ceip** キーと後方互換性があります。

```
1 "analytics":{
2
3   "enabled":false,
4 }
5
6 <!--NeedCopy-->
```

**configuration.js** を使用して **CEIP** を無効にするには

**configuration.js** ファイルは、**ChromeApp** ルートフォルダーにあります。このファイルを編集して ChromeOS 向け Citrix Workspace アプリを構成します。

```
1 > **Notes:**
2 >
3 > - Citrix recommends that you back up the **configuration.js** file
  before making changes.
4 > - Citrix recommends editing the **configuration.js** file, only if
  the Citrix Workspace app for ChromeOS is repackaged for users.
5 > - Administrator-level credentials are required to edit the **
  configuration.js** file.
```

バージョン 1907 以前では、**configuration.js** ファイルの **ceip** の `enabled` 属性を **false** に設定します。

```
1 "ceip":{
2
3   "enabled":false,
4 }
5
6 <!--NeedCopy-->
```

バージョン 1908 以降では、**configuration.js** ファイルの **analytics** の `enabled` 属性を **false** に設定します。

```
1 "analytics":{
2
3   "enabled":false,
4 }
5
6
7 <!--NeedCopy-->
```

### CEIP のブロック

バージョン 2007 以降の場合、管理者は `configuration.js` ファイルおよび Google 管理ポリシーを使用して CEIP をブロックできます。

バージョン 2203 以降の場合、エンドユーザーは GUI を使用して CEIP をブロックできます。



この構成は、GUI および Google 管理ポリシーを使用して行われた構成よりも優先され、CEIP データは Citrix に送信されません。

### Google Admin Policy を使用して CEIP をブロックするには

注:

この手順を実行するには管理者レベルの資格情報が必要です。

1. Google 管理コンソールにログオンします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 手順 4 の後ろに記載された文字列を、policy.txt ファイルの **engine\_settings** キーの下に追加します。
4. [Save] をクリックします。

```
1 "analytics":{
2
3     "connectionEnabled":false,
4     }
5
6 <!--NeedCopy-->
```

### configuration.js を使用して CEIP をブロックするには

1. configuration.js ファイルを開きます。
2. **connectionEnabled** 属性を追加し、この属性を **false** に設定します:

```
1 "analytics":{
2
3     "connectionEnabled":false,
4     }
5
6
7 <!--NeedCopy-->
```

### GUI を使用して CEIP をブロックするには

注:

GUI を使用して CEIP 設定を変更できるのはエンドユーザーのみです。

1. ChromeOS 向け Citrix Workspace アプリを起動します。
2. [設定] > [一般] を選択します。
3. [匿名の使用統計情報を送信して **Citrix Workspace** の機能向上に協力する] オプションをオフにします。

Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

## 特定の CEIP データ

Google Analytics が収集する特定の CEIP データ要素は次のとおりです：

Citrix Workspace アプリのバージョン	セッションモード（キオスク、パブリック/全般）	セッションの種類（デスクトップ/アプリケーション）	XenDesktop 情報（Delivery Controller および VDA バージョン）
起動の種類（SDK/I-CAFile/FTA/Store など）	セッションのタイムゾーン	セッションの言語	クライアントのキーボードレイアウト
ネットワークソケットの種類（HTTPS/HTTP）	機能の使用状況（クリップボード、ファイル転送、アプリスイッチャー、印刷、USB、スマートカードなど）	デバイスのピクセル縦横比	Secure ICA（使用/未使用）
登録済みのエンタープライズ Chromebook のアセット ID	再接続のタイムアウト（!= 180 の場合）	マルチモニター	Global App Configuration Service

## クリップボード

May 16, 2024

### 画像クリップのコピーのサポート

標準のキーボードショートカットを使用して、ローカルデバイスと仮想デスクトップおよびアプリセッションの間で画像クリップをコピーして貼り付けることができます。コピーと貼り付けには、標準のキーボードショートカットを使用できます。例として、Microsoft Word、Microsoft Paint、Adobe Photoshop などのアプリを使用できます。以前は、この機能はテキストでのみ使用できました。

#### 注：

- ネットワーク帯域幅の制約により、2MB を超える画像クリップをコピーして貼り付けようとすると、セッションが応答しなくなる場合があります。
- 対象を選択してから Ctrl+C、Ctrl+V の順に押して、コピーして貼り付けることができます。右クリック

- によるコピーまたは貼り付けもサポートされています。
- この機能は、BMP、PNG、JPEG、および GIF 形式でテスト済みです。

### クリップボードを構成する

Chrome でリンクをコピーすると、HTML コンテンツをコピーし、形式を保持できます。<img> タグが HTML 形式で追加され、画像とテキストをコピーできます。これは、プレーンテキストよりも豊富なデータを提供します。

この機能を有効にするには、VDA に次のレジストリエントリを追加する必要があります：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\Virtual Clipboard\Additional Formats\HTML Format

**“Name” = “HTML Format”**

#### 警告

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows のインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

クリップボード機能に関しては、多くの問題が解決されました。詳しくは Knowledge Center の [CTX086028](#) を参照してください。

### HTML データ形式のサポート

バージョン 2207 以降、仮想デスクトップとエンドポイントデバイス間のクリップボード操作に、HTML 形式を使用できるようになりました。HTML データをコピーして貼り付けると、ソースコンテンツ形式がコピーされます。データを貼り付けると、貼り付け先のコンテンツにも書式設定が適用されます。また、HTML 形式は外観が良くなります。

ポリシーの設定方法について詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[クライアントクリップボードに書き込みを許可する形式](#)」を参照してください。

### クリップボードが HTML 形式をサポート

仮想デスクトップとエンドポイントデバイス間のクリップボード操作に、HTML 形式を使用できるようになりました。HTML データをコピーすると、ソースコンテンツの形式がコピーされ、データを貼り付けると、コピー先のコンテンツにその形式が適用されます。また、HTML 形式は外観が良くなります。

ポリシーの設定方法について詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[クライアントクリップボードに書き込みを許可する形式](#)」を参照してください。

## ファイルの処理

May 16, 2024

### ファイル転送

Chrome 向け Citrix Workspace アプリでは、ユーザーデバイスとセッション間で安全なファイル転送を実行できます。セッションの種類は、Citrix Virtual Apps and Desktops セッションおよび DaaS が対象になります。この機能は、クライアントドライブマッピングの代わりにファイル転送仮想チャネルを使用します。

デフォルトでは、ユーザーは次のことを実行できます：

- ローカルのダウンロードフォルダーまたは接続された周辺機器からファイルをアップロードし、
- Citrix Virtual Apps and Desktops セッションおよび Citrix DaaS セッションからのデータにシームレスにアクセスできます。
- Citrix Virtual Apps and Desktops セッションおよび Citrix DaaS セッションからファイルをダウンロードします。
- ユーザーデバイスのローカルフォルダーや周辺機器にファイルをダウンロードできます。

管理者は、Citrix Studio のポリシーを使用して、ファイルの転送、アップロード、またはダウンロードを有効または無効にできます。

#### 前提条件

- 以下を含む XenApp or XenDesktop 7.6 以降：
  - サーバー OS VDA(Windows 2008 R2 または Windows 2012 R2)上の Hotfix ICATS760WX64022.msp
  - クライアント OS VDA (Windows 7 または Windows 8.1) 上の Hotfix ICAWS760WX86022.msp または ICAWS760WX64022.msp
- ファイル転送ポリシーを変更するには：Citrix Studio を実行中のマシン上のグループポリシー管理 (GPM) Hotfix GPMx240WX64002.msi または GPMx240WX86002.msi

#### 機能の制限事項：

- ユーザーが一度にアップロードまたはダウンロードできるのは、最大 10 ファイルまでです。
- 最大ファイルサイズ：
  - アップロード：2147483647 バイト (2GB)
  - ダウンロード：262144000 バイト (250MB)
- デスクトップにファイルをアップロードまたはデスクトップからファイルをダウンロードポリシーのどちらかが [無効] に設定された場合でも、ツールバーは [アップロード] および [ダウンロード] アイコンを両方表示したままです。ただし、機能はポリシー設定に基づいて有効になります。両方のポリシーが [無効] に設定されると、[アップロード] および [ダウンロード] アイコンはツールバーに表示されません。

### ファイル転送ポリシーを構成する

Citrix Studio ポリシーを使ってファイル転送を構成するには

デフォルトでは、ファイル転送は有効になっています。

Citrix Studio を使って、[ユーザー設定] > [ICA] > [ファイルのリダイレクト] にあるこれらのポリシーを変更します。

---

Citrix Studio ポリシー	説明
デスクトップとクライアント間のファイル転送を許可する	ファイル転送機能を有効または無効にします
デスクトップにファイルをアップロード	セッションでファイルのアップロードを有効または無効にします。「デスクトップとクライアント間のファイル転送を許可する」ポリシーを true に設定する必要があります。
デスクトップからファイルのダウンロード	セッションでファイルのダウンロードを有効または無効にします。「デスクトップとクライアント間のファイル転送を許可する」ポリシーを true に設定する必要があります。

---

**configuration.js** ファイルを使用してファイル転送を構成するには

**configuration.js** ファイルは、**ChromeApp** ルートフォルダーにあります。このファイルを直接編集し、要件に応じて Citrix Workspace アプリを変更します。

メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。ファイルを編集した後、ツールバー要素にさらに変更を加え、アプリを再パッケージします。

**configuration.js** ファイルを使用してツールバーの構成を無効にするには

**configuration.js** ファイルを開き、以下のように設定します。

ファイル転送クライアントの設定	説明
AllowUpload	クライアント側からのアップロードを有効または無効にします。デフォルトでは、true（有効）に設定されています。
AllowDownload	クライアント側からのダウンロードを有効または無効にします。デフォルトでは、true（有効）に設定されています。
MaxUploadSize	アップロードできるファイルの最大サイズ（バイト）で設定します。デフォルトでは、2147483648 バイト（2GB）に設定されています。
MaxDownloadSize	ダウンロードできるファイルの最大サイズ（バイト）で設定します。デフォルトでは、2147483648 バイト（2GB）に設定されています。

Citrix Studio とクライアントで設定されたポリシーが異なる場合、次のように動作します。

Citrix Studio ポリシー	アップロード/ダウンロード	クライアント側の設定	アップロード/ダウンロード	動作
無効		有効		無効
無効		無効		無効
有効		無効		無効
有効		有効		有効

注:

レジストリおよびクライアント側の設定でアップロードまたはダウンロードの最大ファイルサイズに競合する値が設定されている場合、どちらか小さいサイズが適用されます。

**Google** 管理ポリシーを使ってファイル転送機能を構成するには

転送機能は、デフォルトで有効になっています。

無効にするには、enabled 属性を false に設定します。

```

1 {
2
3   "settings": {
4     "Value": {
5
6

```

```
7         "settings_version": "1.0",
8         "engine_settings": {
9
10            "ui": {
11
12               "features": {
13
14                  "filetransfer" : {
15
16                     "allowupload": true,
17                     "allowdownload": true,
18                     "maxuploadsize": 2147483647,
19                     "maxdownloadsize": 2147483647
20                  }
21            }
22          }
23        }
24      }
25    }
26  }
27 }
28 }
29 }
30 }
31 }
32 }
33 }
34 }
35 <!--NeedCopy-->
```

ファイル転送オプションと説明の一覧:

- **allowupload**: デバイスからリモートセッションにファイルをアップロードできます。
- **allowdownload**: デバイスからリモートセッションにファイルをダウンロードできます。
- **maxuploadsize**: これは、アップロードできる最大ファイルサイズ (バイト単位) です。デフォルトでは、2,147,483,648 バイト (2GB) に設定されています。
- **maxdownloadsize**: これは、ダウンロードできる最大ファイルサイズ (バイト単位) です。デフォルトでは、2,147,483,648 バイト (2GB) に設定されています。

### クライアントドライブマッピング

2307 バージョン以降、クライアントドライブマッピング (CDM) 機能によりローカルの ChromeOS デバイス上でフォルダーのマッピングがサポートされ、セッション内からアクセスできるようになります。このフォルダーにシステムファイルが含まれていない場合は、ChromeOS デバイスの任意のフォルダー (ダウンロード、Google ドライブ、USB ドライブのフォルダーなど) をマッピングできます。

エンドユーザーは次の操作を実行できます:

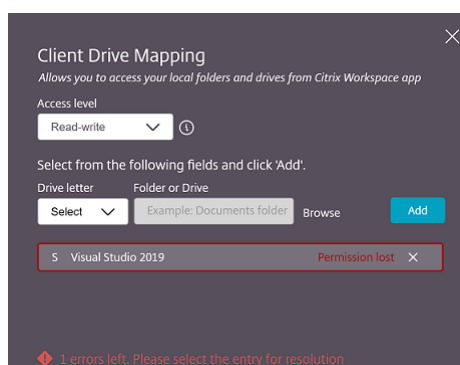
- ファイルとフォルダーを、セッションからマップされたドライブにコピーしたり、逆方向にコピーしたりする。

- マップされたドライブでファイルとフォルダーの一覧を表示する。
- マップされたドライブでファイルの内容を開いて、読み取り、変更する。
- マップされたドライブでファイルのプロパティ（変更時刻とファイルサイズのみ）を表示する。

この機能を使用すると、HDX セッション内のファイルエクスプローラーで、仮想デスクトップドライブとローカルマシンドライブの両方に同時にアクセスできるという利点があります。

### 既知の制限事項

- マップされたドライブ内のファイルとフォルダーの名前を変更することはできません。
- マッピングには完全なパスではなく、フォルダーの名前が含まれます。
- ローカルフォルダーに非表示のファイルがあり、そのフォルダーをマップした場合、非表示のファイルは、マップされたドライブのセッション内で表示されます。
- マップされたドライブでファイルプロパティを読み取り専用アクセスに変更することはできません。
- [HDX SDK](#) を使用してセッションが埋め込みモードで開かれている場合、CDM はサポートされません。
- リムーバブルデバイスからフォルダーをマップし、アクティブなセッション中にそのデバイスを削除すると、マップされたドライブをセッション内で使用できなくなります。マッピングを手動で削除するには、特定のマッピングの **[X]** マークをクリックします。



## CDM の構成

CDM 機能は次のいずれかの方法で構成できます：

- Configuration.js
- Google 管理ポリシー

### 注：

- 前提条件として、管理者は Delivery Controller (DDC) でクライアントドライブリダイレクトポリシーを有効にする必要があります。詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[クラ](#)



「[クライアントドライブリダイレクト](#)」を参照してください。

## Configuration.js

**configuration.js** ファイルを使用して CDM サポートを無効にするには、次の手順を実行します：

1. **configuration.js** ファイルを、**ChromeApp** ルートフォルダーで見つけます。
2. このファイルを編集して CDM 機能を構成します。

メモ：

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

3. **clientDriveMapping** の値を **false** に設定します。

このような JSON データの例を次に示します：

```
1  'features': {
2
3      'clientDriveMapping': {
4
5          'enabled': false,
6          'availableAccessLevels': ["Read-write", "Read-only, No-access
7          "],
8          'accessLevel': "Read-write"
9      }
10 }
11
12 <!--NeedCopy-->
```

4. 変更を保存します。

## Google 管理ポリシー

管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用して CDM 機能を無効にできます：

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を **engine\_settings** の下の **policy.txt** ファイルに追加します。

注:

この構成は以下にも適用できます:

- [Device] > [Chrome] > [Apps and extensions] > [Kiosks] から、拡張機能を検索して、拡張機能のポリシーを見つけます。
- [Device] > [Chrome] > [Apps and extensions] > [Managed guest sessions] から、拡張機能を検索して、拡張機能のポリシーを見つけます。

このような JSON データの例を次に示します:

```

1  {
2
3  "settings": {
4
5    "Value": {
6
7      "settings_version": "2.0",
8      "engine_settings": {
9
10     "features": {
11
12       "clientDriveMapping": {
13
14         "availableAccessLevels": ["Read-write", "Read-only", "No-access"],
15         "accessLevel": "Read-write"
16       }
17     }
18   }
19 }
20 }
21 }
22 }
23 }
24 }
25 }
26 }
27 }
28 <!--NeedCopy-->

```

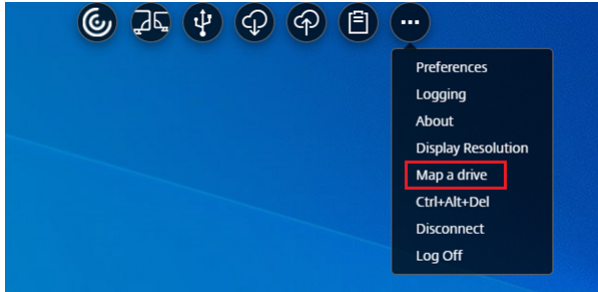
#### 4. 変更を保存します。

**アクセスレベル** この機能が有効な場合、フォルダーまたはドライブのアクセスレベルを設定できます。たとえば、管理者が **availableAccessLevels** を **[\*\* “No-Access” , “Read-only” \*\*]** に設定する場合、エンドユーザーは、ドロップダウンリストで **[読み取り専用アクセス]** オプションと **[アクセスなし]** オプションを表示できます。

## CDM 機能の使用方法

デスクトップセッションの場合:

1. [ツールバー] > その他 (...) > [ドライブをマップする] に移動します。

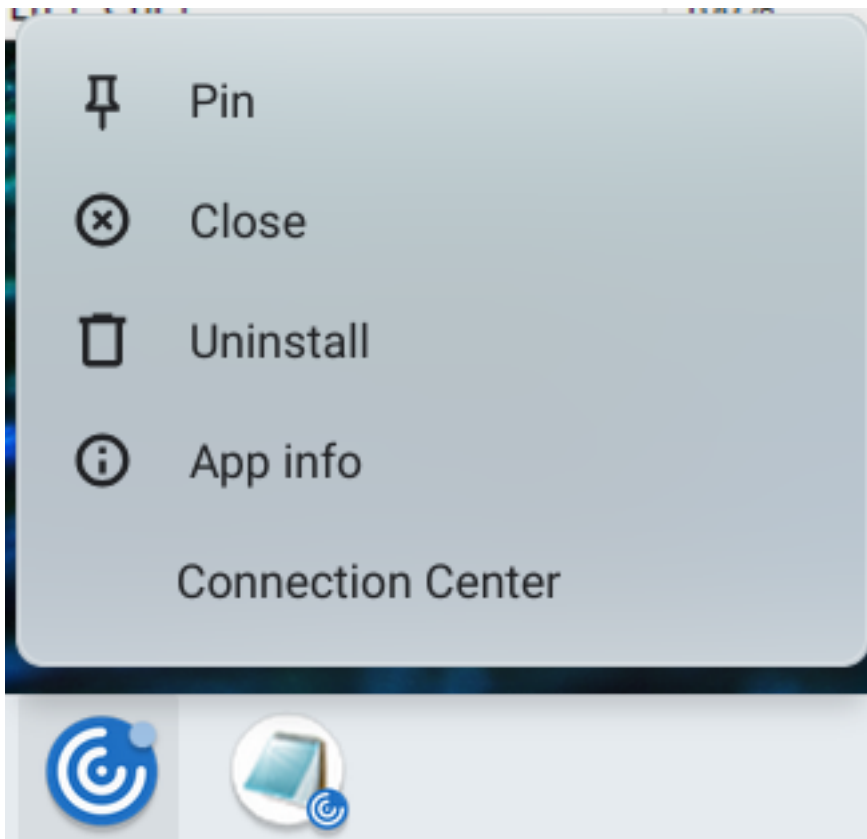


CDM ダイアログボックスが開きます。

2. 次の手順については、「[CDM UI の使用方法](#)」セクションを参照してください。

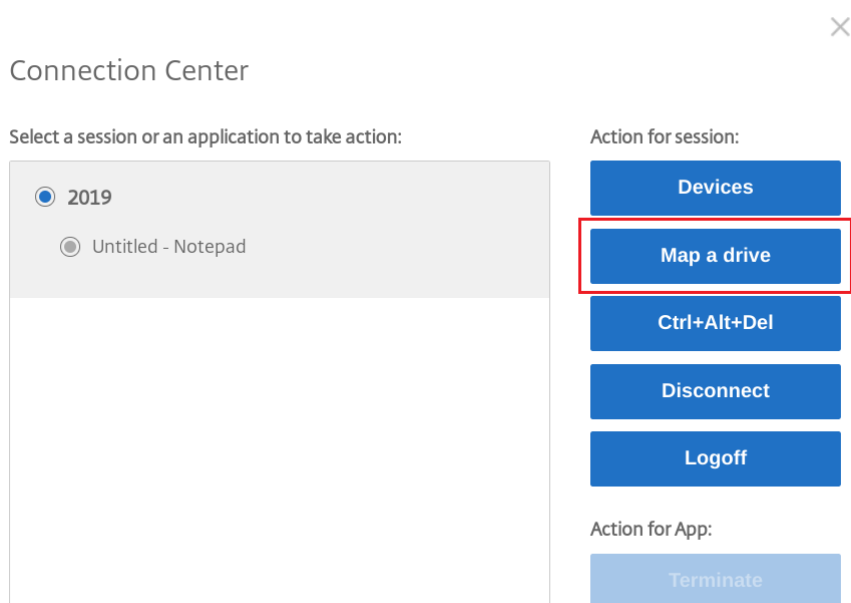
アプリとデスクトップのセッション: の場合:

1. Chrome シェルフで Citrix Workspace アイコンを右クリックして、[コネクションセンター] を選択します。



[コネクションセンター] 画面が開きます。

2. セッションとアプリを選択します。[ドライブをマップする] をクリックします。

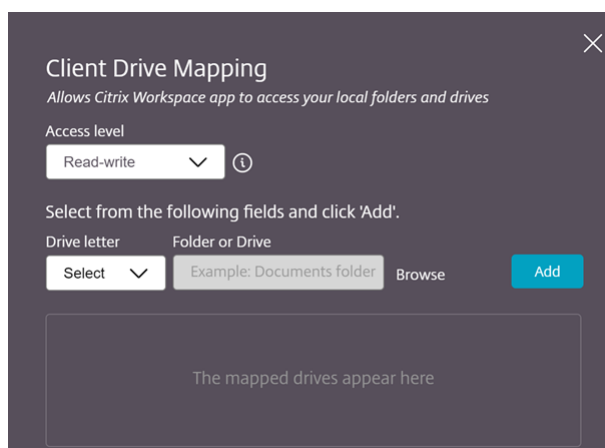


CDM ダイアログボックスが開きます。

3. 次の手順については、「[CDM UI の使用方法](#)」セクションを参照してください。

## CDM UI の使用方法

1. フォルダーまたはドライブの [アクセスレベル] を選択します。表示されるドロップダウンオプションは、組織の IT 管理者がプロファイルに対して設定したアクセスレベルによって異なります。



2. ドライブ文字を選択し、[参照] をクリックして、Chromebook のフォルダーまたはドライブに移動します。
3. [追加] をクリックします。
4. セッションを切断して再接続します。

セッションには、セッション内でマップされているドライブ文字が表示されます。

## ファイルタイプの関連付け

May 16, 2024

### Google ドライブへのアクセス

Google ドライブにより、ユーザーは Citrix Workspace を実行する Chrome デバイスから Windows のファイルタイプを開き、それを編集したり、保存したりできます。Google Chrome デバイスを実行中に、ユーザーは既存の Windows ベースのアプリケーション（Microsoft Word など）をシームレスに使用して、Google ドライブに置かれているファイルにアクセスできます。

ユーザーが Google ドライブでファイルを開いて編集し、ドライブに保存すると、Citrix Virtual Apps でホストされているアプリケーションを使用して同じファイルにアクセスできます。たとえば、Gmail からダウンロードされた .docx 添付ファイルなどです。そのファイルにアクセスして開き、編集して、Google ドライブに保存できます。

### 構成方法

#### 前提条件

Google ドライブへのアクセスを有効にするには、ユーザーの VDA 上に Citrix File Access コンポーネント (FileAccess.exe) をインストールして、Citrix Studio でファイルタイプの関連付けを有効にします。Citrix File Access は、[Citrix のダウンロードページ](#)からダウンロードします。

### Citrix Workspace から Google ドライブへのアクセスを有効にするには

1. 各 Citrix Virtual Apps または Citrix Virtual Apps and Desktops および Citrix DaaS の VDA に `FileAccess.exe` をインストールします。
2. Citrix Studio の公開アプリケーション用に適切な FTA を構成します。
3. Cookie を有効にして、サイト <https://accounts.google.com> と <https://ssl.gstatic.com> を信頼します。これは、Citrix Virtual Apps または Citrix Virtual Apps and Desktops および Citrix DaaS の VDA で実行できます。

Citrix Workspace を使って Google ドライブのファイルのみを開くことができます。Google ドライブからファイルを開くには、ファイルを右クリックして Citrix Workspace で開きます。

Citrix では 1 つのファイルタイプは 1 つの公開アプリケーションに対してのみ割り当てられることをお勧めします。

### プロキシ接続のサポート

ChromeOS 向け Citrix Workspace アプリは、認証されていないプロキシサーバー経由で、公開アプリケーションを使用して Google ドライブのドキュメントを開くことができます。

構成方法:

プロキシ接続を有効にするには、インターネットオプションでプロキシ設定を構成します。

**Citrix Workspace** から **Google** ドライブへのアクセスを無効にするには

manifest.json ファイルで、次のように置換を実行します:

```
1 "file_handlers" : {
2
3     "all-file-types" : {
4
5         "extensions" : [
6             "*"
7         ]
8     }
9
10 }
11 ,
12 <!--NeedCopy-->
```

以下と置き換えます:

```
1     "file_handlers" : {
2
3         "cr-file-type" : {
4
5             "extensions" : [
6                 "cr",
7                 "ica"
8             ]
9         }
10     }
11 ,
12 <!--NeedCopy-->
```

### グラフィック

June 18, 2024

## グラフィックと H.264

### 構成方法

グラフィックと H.264 プロトコルのサポートを構成するには、Google 管理ポリシーを編集して、以下を含めます：デフォルトでは、H.264 プロトコルのサポートは有効になっています。無効にするには、`enabled` 属性を `false` に設定します。

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "ui": {
11
12          "features": {
13
14            "graphics": {
15
16              "jpegSupport": true,
17              "h264Support" : {
18
19                "enabled": true,
20                "losslessOverlays": true,
21                "dirtyRegions": true,
22                "yuv444Support": false
23              }
24            }
25          }
26        }
27      }
28    }
29  }
30 }
31 }
32 }
33 }
34 }
35 }
36 }
37 }
38 }
39 }
40 <!--NeedCopy-->
```

グラフィックオプションと説明の一覧：

- “jpegSupport”：グラフィック (Thinwire) の JPEG 機能です。

- “h264Support”: H.264 プロトコルのサポートです。
- “enabled”: Thinwire の H.264 サポート機能です。
- “losslessOverlays”: Thinwire の無損失オーバーレイ機能です。
- “dirtyRegions”: Thinwire のダーティリージョン機能です。
- “yuv444Support”: Thinwire の Yuv444 サポート機能です。

注:

[従来のグラフィック モード] を [無効] に設定することをお勧めします。

### 機能の制限事項

- ChromeOS 向け Citrix Workspace アプリは、複数のモニターでの全画面 H.264 モードをサポートしていません。
- デスクトップセッションを開始し、テキストを入力するためにアプリを開き、入力を開始すると、テキストが消えて再び表示されます。テキストの表示がちらついて見えます。この問題は、全画面 H.264 モードを使用するときに発生します。
- マルチモニター環境では、公開されたアプリを開くと、アプリ画面の代わりに空白の画面が表示されます。この問題は、全画面 H.264 モードを使用するときに発生します。

### 選択的な H.264

#### 構成方法

**StoreFront** の **web.config** ファイルを使用して選択的な **H.264** を構成する **web.config** ファイルを使用して選択的な H.264 の構成を変更するには:

1. Citrix Receiver for Web サイトの **web.config** ファイルを開きます。  
このファイルは、通常 C:\inetpub\wwwroot\Citrix\Store-name はストア作成時に指定したストア名)。
2. **chromeAppPreferences** フィールドを見つけて、構成の値を JSON 文字列として設定します。例:  

```
chromeAppPreferences= { "graphics" : { "selectiveH264" :false}}
```

**configuration.js** ファイルを使用して選択的な **H.264** を構成する **configuration.js** ファイルは、**ChromeApp** ルートフォルダにあります。このファイルを編集し、要件に応じて Citrix Workspace アプリを変更します。

デフォルトでは、選択的 H.264 は true に設定されています。

**configuration.js** ファイルを使用して選択的な H.264 の構成を無効にするには:

1. **configuration.js** ファイルを開いて、**selectiveH264** 属性を **false** に設定します。



```
'graphics': {  
  'selectiveH264': false  
}
```

メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

## その他 (H.264)

### 構成方法

H.264 を構成するには、Google 管理ポリシーを編集して、以下を含めます: デフォルトでは、**other** セクションのオプションは無効になっています。有効にするには、無効になっている属性 `h264nonworker` を `true` に設定します。

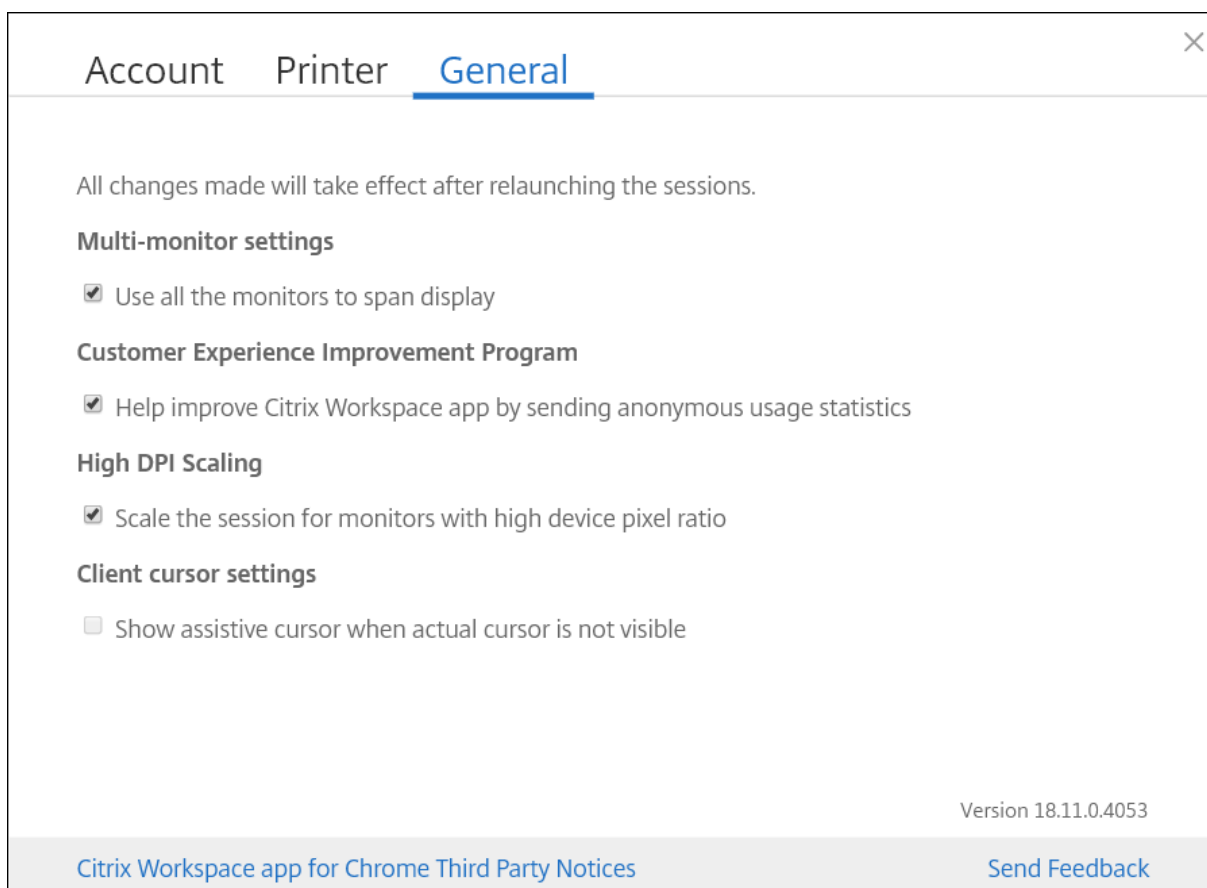
```
1 {  
2  
3   "settings": {  
4  
5     "Value": {  
6  
7       "settings_version": "1.0",  
8       "engine_settings": {  
9  
10        "other": {  
11  
12          "h264nonworker" : false  
13        }  
14      }  
15    }  
16  }  
17 }  
18  
19 }  
20  
21 }  
22  
23  
24 <!--NeedCopy-->
```

オプションと説明の一覧:

- “h264nonworker”：メインスレッドで H.264 フレームをデコードするオプションを有効にします。

## 補助カーソル

デスクトップセッション内でカーソルが表示されない場合は、補助カーソルを有効にすることができます。セッションの再起動が必要です。



## 構成方法

補助カーソル機能はデフォルトでは無効になっています。補助カーソル機能を有効にするには、Google 管理ポリシーを編集して、以下を含めます：

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
```

```

10         "ui": {
11
12             "assistiveCursor": true
13         }
14     }
15 }
16
17 }
18
19 }
20
21 }
22
23
24 <!--NeedCopy-->

```

注:

- 管理者が前述のように補助カーソルを有効にすると、クライアント側の設定で関連チェックボックスがデフォルトで選択されます。この機能を無効にするには、チェックボックスをオフにします。
- 管理者が前述のように補助カーソルを無効にすると、チェックボックスはオフになり、機能は無効になります。

## DPI スケール機能

### この機能について

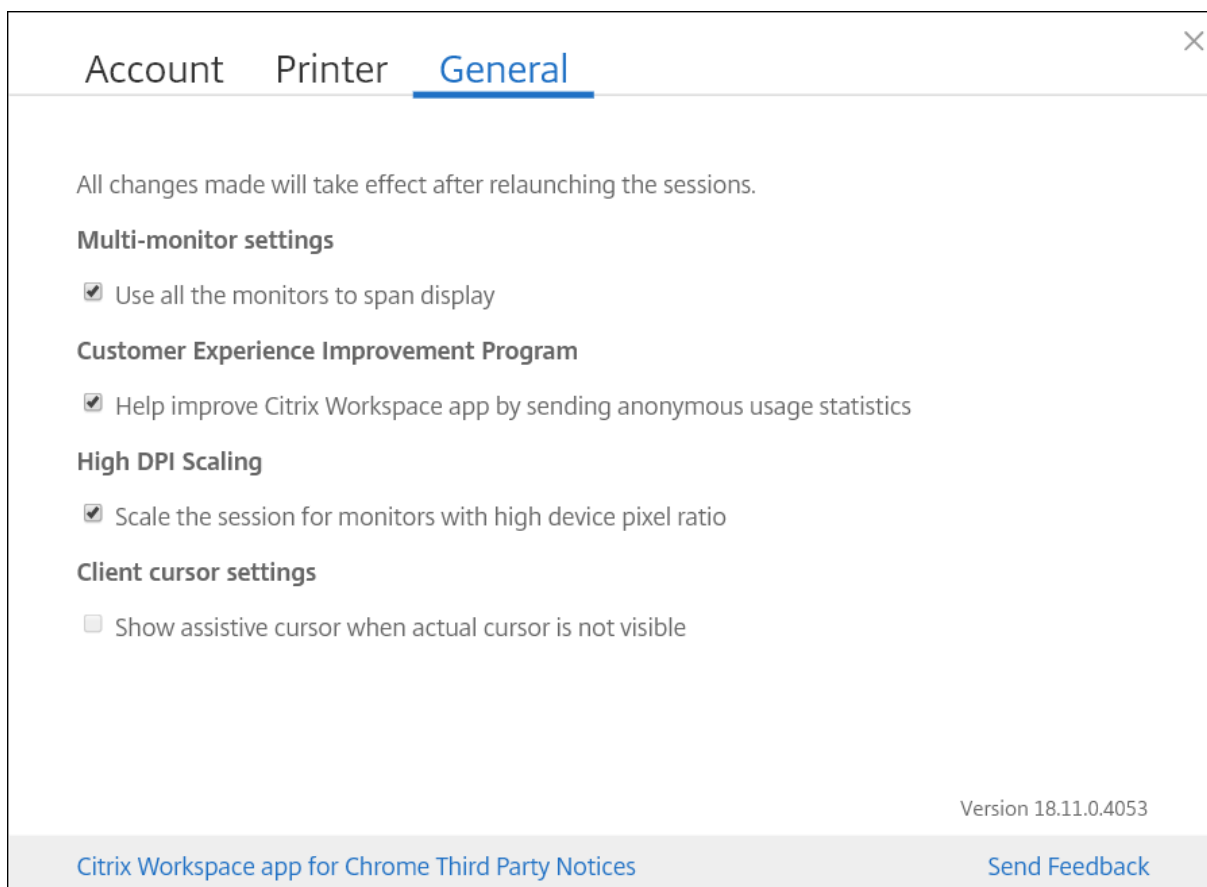
ChromeOS 向け Citrix Workspace アプリは、オペレーティングシステムでアプリセッションおよびデスクトップセッションの解像度を制御でき、単一モニター上のアプリセッションに対する DPI クライアントスケールをサポートします。

ChromeOS 向け Citrix Workspace アプリは、DPI スケールをサポートしているため、高いピクセル縦横比のモニター上で VDA の解像度を設定できます。

高 DPI スケール機能は、アプリおよびデスクトップセッションではデフォルトで無効になっています。高 DPI 対応デバイスの解像度を向上させるには、[設定] にアクセスして [高 DPI スケール] チェックボックスをオンにします。

### 構成方法

[高 DPI スケール] 設定は、Google Admin Policy のみで構成できます。



DPI スケール機能 [モニターのセッションを高いデバイスピクセル縦横比でスケール] は、デフォルトで有効になっています。

デスクトップセッションの解像度を設定するには、セッションツールバーにアクセスします。[基本設定] > [解像度を表示する] > [デバイスのピクセル縦横比を使用する] を選択して VDA で正しい解像度を設定します。VDA で解像度を適切に設定すると、ぼやけたテキストが鮮明に表示されます。

この機能を有効または無効にするには、**Google** 管理コンソールポリシーを編集し、**scaleToDPI** の値を **true** または **false** に設定します。

たとえば、機能を無効にするには、**scaleToDPI** プロパティを **false** に設定します。

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10      "features" : {
11
12      "graphics" : {
```

```
13
14     "dpiSetting": {
15
16         "scaleToDPI": false
17     }
18
19     }
20
21     }
22
23     }
24
25     }
26
27     }
28
29     }
30
31
32
33 <!--NeedCopy-->
```

## キーボード

May 16, 2024

### 東アジア言語の汎用クライアント **IME**

汎用クライアント IME 機能は、中国語、日本語、および韓国語（CJK）の文字の入力および表示エクスペリエンスを強化します。セッション中にこの機能を使用すると、カーソル位置に CJK 文字を入力できます。この機能は、Windows VDA および Linux VDA 環境で使用できます。

IME は通常、候補ウィンドウ、テキスト作成ウィンドウなどのユーザーインターフェイス（UI）コンポーネントを表示します。テキスト作成ウィンドウには、作成に使用する文字とテキスト作成 UI 要素が含まれます。テキスト作成 UI 要素には、下線、背景色などがあります。候補ウィンドウには、候補リストが表示されます。



テキスト作成ウィンドウでは、確定済みの文字と作成中の文字を選択できます。作成ウィンドウと候補ウィンドウは、入力カーソルに沿って移動します。結果として、この機能により、テキスト作成ウィンドウでのカーソル位置での文字入力機能が強化されています。また、テキスト作成ウィンドウと候補ウィンドウでの表示機能も改善されています。

前提条件:

- Linux VDA の場合、クライアントキーボードレイアウトの同期と **IME** の改善ポリシーを有効にします。
- Windows VDA の場合、**Unicode** キーボードレイアウトのマッピングポリシー、クライアントキーボードレイアウトの同期および **IME** の改善ポリシーを有効にします。
- Citrix Linux VDA バージョン 2012 以降を使用します。Citrix Windows VDA の場合は、現在利用可能なすべての Windows VDA バージョンが、汎用クライアント IME 機能をサポートしています。
- ブラウザーの言語は、日本語、中国語（簡体字）、中国語（繁体字）、または韓国語である必要があります。
- Google Chrome または Mozilla Firefox を使用してください。

機能の制限事項:

- Microsoft Excel のセル内での文字入力が失敗します。この問題は、マウスクリックを使用してセルを選択した場合に発生します。[RFHTMCRM-6086]
- 拡張画面を使用する場合に、汎用クライアント IME がサポートされるようになりました。ただし、マルチモニターセッションはまだサポート対象外であるため、代わりにサーバー **IME** を使用できます。

サーバー **IME** を有効にするには、次の操作を実行します:

1. 必要に応じて、VDA またはサーバーのキーボード言語を中国語、日本語、または韓国語（CJK）に変更します。
2. Chromebook のキーボード言語を英語に変更します。

この機能の既知の問題:

- Citrix IME が VDA デスクトップセッションに追加されていない場合、IME 文字を入力できない場合があります。この問題は、VDA バージョン 2202 以前で断続的に発生します。[HDX-36748]

構成:

バージョン 2209 以降、汎用クライアント IME 機能はデフォルトで有効になっています。

管理者は、StoreFront サーバー（通常、%ProgramFiles%\Citrix\Receiver StoreFront\HTML5Client）にある **configuration.js** ファイルを使用して機能を有無効にできます。この機能を無効にするには、**app-Prefs>chromeApp>feature>ime** に移動し、**genericIME** を **false** に設定します。

例:

```
1     "appPrefs":{
2
3         "chromeApp":{
4
5             "features" : {
6
7                 "ime" : {
8
9                     "genericIME": false
10                }
11            }
12        }
13    }
14 }
15 }
16 }
17 }
18 <!--NeedCopy-->
```

- 管理者は、**genericIME** を **false** に設定することにより、Google 管理ポリシーコンソールを使用してこの機能を無効にすることができます。

例:

```
1     {
2
3     "settings": {
4
5     "Value": {
6
7         "settings_version": "1.0",
8         "engine_settings": {
9
```

```
10     "features": {
11
12         "ime": {
13
14             "genericIME": false
15         }
16     }
17 }
18
19 }
20
21 }
22
23 }
24
25 }
26
27 <!--NeedCopy-->
```

## ショートカット

ユーザーは標準的な Windows ショートカットキーを使用して、ホストされるアプリケーション間で、文字、表、画像などのデータをコピーできます。このホストされるアプリケーションは次のとおりです：

- 同じセッション内
- 異なるセッション内

ホストされているアプリケーションとデバイスのローカルクリップボード間では、Unicode のプレーンテキストのみをコピーして貼り付けることができます。

ユーザーは、ChromeOS 向け Citrix Workspace アプリで標準の Windows キーボードを使うことができます。これは、ショートカットが ChromeOS からホストされるアプリケーションに渡されるためです。同様に、いずれの ChromeOS ショートカットとも競合することなく、特定のアプリケーションに特有のショートカットも使用することができます。

ただし、ファンクションキーを認識させるためには **Windows** キーも押す必要があります。そのため、外付けキーボードが必要です。ChromeOS での Windows キーボードの使用については、<https://support.google.com/chromebook/answer/1047364>を参照してください。セッションとウィンドウ間の切り替えに使用する Citrix 特定のショートカットについては、ChromeOS 向け Citrix Workspace アプリでは使用できません。

## Excel のショートカット

### 構成方法

キーボードショートカットは **sendAllKeys** 属性で構成されます：



すべてのショートカットが Excel で機能するようにするには、次のように構成します: **HTML5\_CONFIG > features > sendAllKeys**

**sendAllKeys** 属性は、デフォルトで **true** に設定されています。デフォルトを変更するには、**configuration.js** ファイルを開き、**sendAllKeys** 属性を追加して、その値を **false** に設定します。

詳しくは、「[Google 管理コンソールでポリシーをプッシュする方法](#)」を参照してください。

## Microsoft Windows ロゴキーとショートカットキーのサポート

注:

- Chromebook で、検索キーを使用して Microsoft Windows ロゴキーをマッピングします。

バージョン 2108 リリース以降、ChromeOS 向け Citrix Workspace アプリのセッションで、Microsoft Windows ロゴキーとショートカットキーがサポートされています。

次のキーの組み合わせのサポートが追加されました:

- Windows + R
- Windows + D
- Windows + E
- Windows + M
- Windows + S
- Windows + CTRL + S
- Windows + T
- Windows + U
- Windows + 数字
- Windows + X
- Windows + K

## 仮想キーボードの自動表示

バージョン 2211 以降、編集可能なフィールドにカーソルを置くと、仮想キーボードが自動的に表示されます。この機能は、仮想キーボードを表示するためにキーボードアイコンをクリックする必要があった以前の動作とは異なり、タッチスクリーンデバイスでのユーザーエクスペリエンスを向上させます。

## [Scan code] 入力モード

Citrix Workspace アプリを使用すると、外部の物理キーボードを使用して、VDA のサーバー側のキーボードレイアウトと連携できます。管理者が [Scan code] モードを有効にすると、エンドユーザーはクライアントではなくサーバーのキーボードレイアウトを使用する可能性があります。

この機能により、特に東アジア言語の物理キーボードを使用する場合のユーザーエクスペリエンスが向上します。

### メモ:

- デフォルトでは、この機能は無効になっています。
- タッチデバイスでは、[Scan code] が有効になっていると、Citrix Workspace アプリでスクリーンキーボードソフトウェアが機能しません。

### 構成

[Scan code] での入力方法は次のいずれかの手段で設定できます。

- Configuration.js
- Google 管理ポリシー

### Configuration.js

#### メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

**configuration.js** ファイルを使用して [Scan code] サポート機能を有効にするには、次の手順を実行します。

1. **configuration.js** ファイルを、ChromeApp ルートフォルダーで見つけます。
2. 同ファイルを編集し、**scancode** の値を **true** に設定します。

このような JSON データの例を次に示します:

```
1  "features" : {
2
3      "ime": {
4
5          "scancode": true,
6      }
7  }
8  }
9
10 <!--NeedCopy-->
```

3. 変更を保存します。

**Google 管理ポリシー** 管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用して [Scan code] サポート機能を有効にできます:

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を engine\_settings キーの下の **policy.txt** ファイルに追加します。

注:

この構成は以下にも適用できます:

- [Device] > [Chrome] > [Apps and extensions] > [Kiosks] から、拡張機能を検索して、拡張機能のポリシーを見つけます。
- [Device] > [Chrome] > [Apps and extensions] > [Managed guest sessions] から、拡張機能を検索して、拡張機能のポリシーを見つけます。

このような JSON データの例を次に示します:

```
1  "features" :  
2  {  
3  
4      "ime": {  
5  
6          "scancode": true  
7      }  
8  
9  }  
10  
11 <!--NeedCopy-->
```

4. 変更を保存します。

## カスタムキーボードマッピング

バージョン 2309 以降、VDA が Windows OS マシンで、ネイティブ入力デバイスが ChromeOS キーボードである場合、エンドユーザーは Windows 固有のショートカットとキーの組み合わせを使用できるようになります。カスタムマッピングを使用して、**Ctrl** キーと **Alt** キーを割り当てることができるようになりました。ユーザーは、右または左のコントロール (Ctrl) キーを選択して、Alt キーとして機能させることができます。

メモ:

- マッピングは全画面モードでのみ可能です。
- 設定を保存すると、マッピングはすべてのセッションで有効になります。
- この機能はデフォルトで有効にされています。

## 構成

カスタムキーボードマッピングは、次のいずれかの方法で構成できます。

- Configuration.js
- Google 管理ポリシー

## Configuration.js

メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

**configuration.js** ファイルを使用してこの機能を無効にするには、次の手順を実行します。

1. **configuration.js** ファイルを、ChromeApp ルートフォルダーで見つけます。
2. 同ファイルを編集し、**CustomKeyboardMapping** の値を **false** に設定します。

このような JSON データの例を次に示します:

```
1  "features" : {
2
3      "ime": {
4
5          "CustomKeyboardMapping": false,
6      }
7  }
8  }
9
10 <!--NeedCopy-->
```

3. 変更を保存します。

**Google 管理ポリシー** 管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用して機能を有効にできます:

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を engine\_settings キーの下の **policy.txt** ファイルに追加します。

メモ:

この構成は以下にも適用できます:

- [Device] > [Chrome] > [Apps and extensions] > [Kiosks] から、拡張機能を検索して、拡張機能のポリシーを見つけます。

- [Device > Chrome] > [Apps and extensions] > [Managed guest sessions] から、拡張機能を検索して、拡張機能のポリシーを見つけます。

このような JSON データの例を次に示します:

```
1  "features" :  
2  {  
3  
4      "ime": {  
5  
6          "CustomKeyboardMapping": false  
7      }  
8  
9  }  
10  
11 <!--NeedCopy-->
```

4. 変更を保存します。

この機能の使用方法について詳しくは、[ヘルプドキュメント](#)の記事を参照してください。

## VDA への、全画面モードでのシステムショートカット

ChromeOS デバイス向け Citrix Workspace アプリのバージョン 2309 以降で、VDA (リモートデスクトップセッション) への、全画面モードでのシステムショートカットを渡すことができるようになりました。ただし、クライアント OS では機能しません。

以前では、これらのキー組み合わせはローカルでは機能していました。この機能が全画面モードで有効の場合、これらのキー組み合わせは VDA に送信されますが、ローカルでは作用しません。たとえば、更新キーは Chromebook のシステムキーであり、**Ctrl + Shift + 更新キー**の組み合わせは画面を回転するための、ChromeOS のシステムショートカットです。しかし、Windows OS にはそのようなショートカットがないため、Windows VDA では何も起こりません。

別の例として、**Alt+[** は ChromeOS ウィンドウを左側にドッキングするのに使用されますが、同じショートカットは Windows VDA では作用しません。一部のアプリケーションでは、特定の機能に対してこのようなショートカットを使用する場合があります。例えば、一部のバーコードスキャナーでは **Alt+[** がプレフィックスとして使用されます。

注:

- この機能はデフォルトで有効になっています。

キーの組み合わせは次のとおりです。

ショートカットキーの組み合わせ	ChromeOS でのアクション
ChromeOS でのアクション	サインアウトする
Ctrl+Shift+ 更新	画面を 90 度回転する
Ctrl+Shift+L	Chromebook をロックする
Alt+ [	ウィンドウを左サイドにドッキングする
Alt+ ]	ウィンドウを右サイドにドッキングする。ウィンドウを右サイドにドッキングしたり、ウィンドウをスナップして復元したりするためのキー。
Alt+ ” - “	ウィンドウを最小化する
Alt+ ” +”	ウィンドウを最大化する

---

注:

- これらのキーの組み合わせは ChromeOS のシステムショートカットであるため、VDA では ChromeOS とは同じアクションを行わない場合があります。

### 構成

この機能は次のいずれかの手段で構成できます。

- Configuration.js
- Google 管理ポリシー

### Configuration.js

メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

**configuration.js** ファイルを使用してこの機能を無効にするには、次の手順を実行します。

1. **configuration.js** ファイルを、ChromeApp ルートフォルダーで見つけます。
2. 同ファイルを編集し、**sendSysShortcutForFullscreen** の値を **false** に設定します。

このような JSON データの例を次に示します:

```

1  "features" : {
2
3      "ime": {
4
5          "sendSysShortcutForFullscreen": false,
6      }
7  }
8  }
9
10 <!--NeedCopy-->

```

3. 変更を保存します。

**Google 管理ポリシー** 管理対象デバイスおよびユーザーに対し、管理者は、次のように Google 管理ポリシーを使用してこの機能を無効にできます。

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を engine\_settings キーの下の **policy.txt** ファイルに追加します。

メモ:

この構成は以下にも適用できます:

- [Device] > [Chrome] > [Apps and extensions] > [Kiosks] から、拡張機能を検索して、拡張機能のポリシーを見つけます。
- [Device] > [Chrome] > [Apps and extensions] > [Managed guest sessions] から、拡張機能を検索して、拡張機能のポリシーを見つけます。

このような JSON データの例を次に示します:

```

1  "features" :
2  {
3
4      "ime": {
5
6          "sendSysShortcutForFullscreen": false
7      }
8  }
9  }
10
11 <!--NeedCopy-->

```

4. 変更を保存します。

## ライセンス

May 16, 2024

### 資産 ID

この機能について

Citrix Workspace アプリは、登録された Chromebook から起動したセッションで管理者が Google 管理コンソールを使用して設定するクライアント名に、資産 ID を使用します。

### 構成方法

デフォルトでは以前のバージョンと同様、Citrix Workspace アプリは登録された Chromebook に固有のクライアント ID を生成します。この機能を使用するには、Citrix Workspace アプリのポリシーを設定する必要があります。

入力するデータ値は、15 文字以下にする必要があります。これを超えると、15 文字に省略されます。

### 資産 ID の設定

1. Google 管理コンソールにログオンします。
2. [Device Management] > [Chrome] > [Devices Console] に移動して、デバイスに Asset ID を入力します。
3. Google Admin Console ポリシーを編集して、`useAssetID` の値を **true** に設定します。デフォルトでは、`useAssetID` は **false** に設定されています。

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "uniqueID": {
11
12         "useAssetID": true
13        }
14      }
15    }
16  }
```



```

17     }
18
19   }
20
21 }
22
23
24 <!--NeedCopy-->

```

機能の制限事項:

- プッシュできる Google 管理ポリシーが必要です。これがない場合、現在使用している管理対象 Chromebook 固有のクライアント ID を生成する方法は変更されません。
- 入力する値は、15 文字以下にする必要があります。これを超えると、15 文字に省略されます。

### 一意の ID と資産 ID

一意の ID はクライアント名のプレフィックスとして適用されます。

Citrix Workspace アプリは、登録された Chromebook から起動したセッションで管理者が **Google** 管理コンソールを使用して設定するクライアント名に資産 ID を使用します。

構成方法

GUI を使用して資産 ID を構成するには、**[Device Management]** > **[Chrome]** > **[Devices Console]** に移動して **[Asset ID]** を追加します。

資産 ID と一意の ID を構成するには、Google 管理ポリシーを編集して、以下を含めます:

```

1  {
2
3    "settings": {
4
5      "Value": {
6
7        "settings_version": "1.0",
8        "engine_settings": {
9
10         "uniqueID" : {
11
12           "prefixKey" : "CR-",
13           "restrictNameLength" : true,
14           "useAssetID": false
15         }
16
17       }
18
19     }

```

```
20
21     }
22
23 }
24
25
26 <!--NeedCopy-->
```

uniqueID オプションと説明の一覧:

- “prefixKey”: クライアント名の前に使用されるプレフィックスです。デフォルト値は CR です。
- “restrictNameLength”: prefixKey の名前の長さを有効または無効にします。
- “useAssetID”: 登録済みの Chromebook から起動されるセッションのクライアント名として設定される資産 ID です。

機能の制限事項:

- プッシュできる Google 管理ポリシーが必要です。これがない場合、現在使用している管理対象 Chromebook 固有のクライアント ID を生成する方法は変更されません。
- 入力する値は、15 文字以下にする必要があります。これを超えると、15 文字に省略されます。

## マルチメディア

May 16, 2024

### オーディオ

セッション内で USB ヘッドセットを使用して、話したり聞いたりすることができます。USB ヘッドセットのボタンを使用することもできます（ミュートやスキップなど）。スムーズなオーディオ出力を提供することで、ユーザーエクスペリエンスが向上します。

### アダプティブオーディオ

アダプティブオーディオを使用すれば、VDA でオーディオ品質ポリシーを構成する必要はありません。アダプティブオーディオは環境の設定を最適化します。従来のオーディオ圧縮形式を置き換え、優れたユーザーエクスペリエンスを提供します。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[アダプティブオーディオ](#)」を参照してください。

### 機能の属性

次の 2 つの機能の属性があります：

- **EnableAdaptiveAudio**： 値を true に設定すると、アダプティブオーディオ機能が有効になります。この機能を無効にするには、値を false に設定します。
- **EnableStereoRecording**： ステレオ録音はオプションの機能です。デフォルトでは、この機能は無効になっています。 **EnableStereoRecording** 属性の値を **true** に設定してステレオ録音を有効にするか、値を **false** に設定してこの機能を無効にします。この機能は、アダプティブオーディオ機能が有効になっている場合のみサポートされます。 **EnableStereoRecording** 属性を true に設定すると、エコーキャンセルを無効にしたステレオ録音がサポートされます。

### 構成方法

アダプティブオーディオ機能は次の方法で構成できます：

- Configuration.js
- Google 管理ポリシー

**Configuration.js configuration.js** ファイルを使用してアダプティブオーディオを構成するには、次の手順を実行します：

1. **configuration.js** ファイルを、**ChromeApp** ルートフォルダーで見つけます。
2. このファイルを編集してアダプティブオーディオ機能を構成します。

メモ：

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

3. **EnableAdaptiveAudio** のデフォルト値を **true** に設定します。 **EnableStereoRecording** のデフォルト値を **false** に設定します。

このような JSON データの例を次に示します：

```
1  "features" : {
2
3      "audio" : {
4
5          "EnableAdaptiveAudio": true
6      }
}
```

```

7
8   }
9
10
11  "features" : {
12
13    "audio" : {
14
15      "EnableStereoRecording": false
16    }
17  }
18 }
19
20 <!--NeedCopy-->

```

4. 変更を保存します。

注:

- この機能を無効にするには、**EnableAdaptiveAudio** 属性を **false** に設定します。

**Google 管理ポリシー** オンプレミス環境では、管理者は次のように Google 管理ポリシーを使用してアダプティブオーディオ機能を有効にできます:

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を **engine\_settings** キーの下の **policy.txt** ファイルに追加します。

このような JSON データの例を次に示します:

```

1  "features" : {
2
3    "audio" : {
4
5      "EnableAdaptiveAudio": {
6
7        "type": "boolean" }
8
9      }
10
11    }
12
13  "features" : {
14
15    "audio" : {
16
17      "EnableStereoRecording": {
18
19        "type": "boolean" }
20

```

```
21
22         }
23
24     }
25
26 <!--NeedCopy-->
```

4. 変更を保存します。

### オーディオデバイスのプラグアンドプレイのサポート

以前は、単一のオーディオ再生および録音デバイスのみがサポートされ、実際のデバイス名に関係なく「**Citrix HDX Audio**」として表示されていました。

バージョン 2301 以降、複数のオーディオデバイスがサポートされ、それらは VDA にリダイレクトされます。これで、オーディオデバイスをリダイレクトするときに、VDA の **[Sound] > [Playback]** と **[Sound] > [Recording]** でオーディオデバイスの実際の名前が表示されるようになりました。VDA 上のデバイス一覧は、オーディオデバイスを接続する、または取り外すたびに動的に更新されます。

注:

この機能は、デフォルトで有効になります。

### 構成

この機能は次のいずれかの方法で実行できます：

- Configuration.js
- Google 管理ポリシー

**Configuration.js configuration.js** ファイルを使用してオーディオデバイスのプラグアンドプレイを無効にするには、次の手順を実行します：

1. **configuration.js** ファイルを、**ChromeApp** ルートフォルダーで見つけます。
2. ファイルを編集して、オーディオデバイスのプラグアンドプレイのサポート機能を構成します。

メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

3. **AudioRedirectionV4** の値を **false** に設定します。このような JSON データの例を次に示します:

```

1   "features" : {
2
3     "audio" : {
4
5       "AudioRedirectionV4": false
6     }
7
8   }
9
10 <!--NeedCopy-->
```

4. 変更を保存します。

**Google** 管理ポリシー オンプレミス環境では、管理者は次のように Google 管理ポリシーを使用してオーディオデバイスのプラグアンドプレイ機能を無効にできます:

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を **engine\_settings** キーの下の **.txt** ファイルに追加します。

このような JSON データの例を次に示します:

```

1   "features" : {
2
3     "audio" : {
4
5       "AudioRedirectionV4": false
6     }
7
8   }
9
10 <!--NeedCopy-->
```

4. 変更を保存します。

#### 既知の制限事項

- VDA では、内蔵オーディオデバイスの名前は英語のみで表示されます。この問題は、ChromeOS ベースのデバイスを使用している場合に発生します。[RFHTMCRM-8667]

#### Web カメラ

ChromeOS 向け Citrix Workspace アプリは、強化された Web カメラリダイレクト機能を提供します。Web カメラ入力の H.264 ハードウェアエンコードにより、CPU 負荷を減らし、Chromebook デバイスのバッテリーを長持

ちさせます。これらのデバイスの H.264 エンコーダーは、PPB\_VideoEncoder API を介して Intel 機能を使用します。

ChromeOS 向け Citrix Workspace アプリは、32 ビットと 64 ビットの両方のアプリケーションで Web カメラリダイレクトをサポートしています。

### Web カメラリダイレクト

Web カメラリダイレクトが 32 ビットと 64 ビットの両方のアプリケーションで利用できます。32 ビット版と 64 ビット版のアプリケーションの両方で Web カメラリダイレクトがサポートされているのは、内蔵 Web カメラのみです。

ChromeOS 向け Citrix Workspace アプリの仮想デスクトップおよびアプリで外部 Web カメラを使用できるようになりました。Citrix Workspace アプリは、新しく接続された外部 Web カメラを検出し、動的に使用可能にします。

#### 構成方法

64 ビットの Web カメラリダイレクトは、次のように構成します：

**configuration.js** ファイルと **Google** 管理コンソールを使用した **Web** カメラの構成 バージョン 2101 以降の場合：

次のパスを使用して Web カメラリダイレクトを構成します：**HTML5\_CONFIG > features > video**

注：

Web カメラリダイレクトを構成するには、**HTML5\_CONFIG > features > video** のパスを使用することをお勧めします。他方のパスは当面の間機能しますが、将来のリリースで削除される予定です。

#### Web カメラリダイレクトの推奨事項

- Citrix Delivery Controller の音質ポリシーを「低」または「中」に設定してください。低電力の Chromebook を使用している場合、音質ポリシーを設定しないとオーディオの遅延が発生する可能性があります。
- パフォーマンスを最適化するため、上位の Chromebook を使用し、帯域幅が十分に遅延が少ないネットワークに接続することをお勧めします。
- VDA で次のレジストリキーを設定します：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\HdxRealTime

名前: OfferH264ToApp

種類: REG\_DWORD

値: 1

### 注:

この設定は、現在のユーザー設定に適用されます。新しいユーザーの場合は、Windows グループポリシーオブジェクト (GPO) エディターを使用してレジストリキーを設定します。

**免責事項:** 注意。レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix は一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

## Microsoft Teams の最適化

May 16, 2024

仮想デスクトップセッションおよび仮想アプリセッションに Microsoft Teams の次の機能を使用できるようになりました。

- 最適化された音声通話
- 最適化されたビデオ通話
- 最適化された画面共有

VDA バージョン 1906 以降でのみサポートされます。

### メモ:

- デフォルトでは、画面共有により画面全体の共有が許可されます。ただし、画面共有を制限できるのは、Citrix Workspace アプリコンテンツのみです。詳しくは、「[Citrix Workspace アプリコンテンツの画面共有の制限](#)」を参照してください。Google 管理ポリシーで画面共有機能を有効にするには、「[Microsoft Teams の最適化設定](#)」を参照してください。
- トラブルシューティングを行い、クライアントセッション内で Microsoft Teams を非最適化から最適化に変更するには、「[Microsoft Teams 最適化のトラブルシューティング](#)」を参照してください。
- Microsoft Teams 最適化を使用した画面共有中、共有ウィンドウの周囲の赤い枠線は表示されません。
- アプリの共有はサポートされていません。
- Microsoft Teams による音声通話、ビデオ通話、画面共有の最適化は、リリース 2105.5 以降で一般提供されます。最新バージョンの ChromeOS 向け Citrix Workspace アプリに更新することをお勧めします。



### 外部モニターでのビデオ通話と画面共有

外部モニターで、通話中に Microsoft Teams の次の機能を使用できるようになりました。

- 最適化されたビデオ
- 最適化された画面共有

これらの機能は、仮想デスクトップ内の Microsoft Teams 通話で使用できます。また、Microsoft Teams ウィンドウを外部モニターに配置したときに、Microsoft Teams 仮想アプリ経由で行われた通話でも使用できます。

### メモ (ChromeOS バージョン 96 アップデート)

- ChromeOS バージョン 96 の更新プログラムが Microsoft Teams の機能に与える影響を回避するには、ChromeOS を更新する前に次の手順を実行してください:
- 再パッケージ化されたバージョンの Citrix Workspace アプリを使用しているユーザーの場合は、Knowledge Center の記事[CTX331648](#)を参照して、手順を実行してください。
- バージョン 2110 以前の ChromeOS 向け Citrix Workspace アプリの他のすべてのユーザーは、Knowledge Center の記事[CTX331653](#)を参照してください。

### Microsoft Teams の最適化設定

画面共有を有効にするには

Google 管理ポリシーを使用して画面共有を有効にするには、次のように **msTeamsOptimization** の画面共有の値を **true** に変更します。

詳しくは、「[Google 管理コンソールでポリシーをプッシュする方法](#)」の記事を参照してください。

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "features":{
11
12          "msTeamsOptimization":{
13
14            "screenSharing" : true
15          }
16
17        }
18      }
19    }
20  }
```

```
19     }
20
21     }
22
23     }
24
25     }
26
27
28 <!--NeedCopy-->
```

個人所有のデバイス（BYOD）のユーザーの画面共有を有効にするには（オンプレミスの StoreFront を使用している場合のみ）:

「[web.config ファイルの使用](#)」記事の手順に従い、次のように **chromeAppPreferences** 値を追加します:

例:

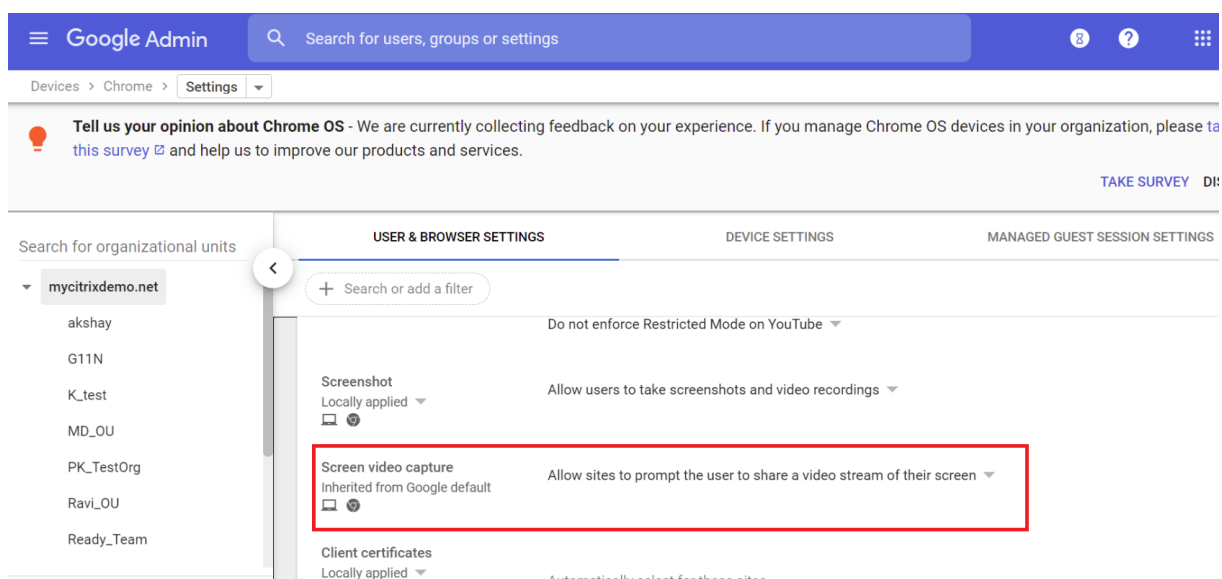
```
1 chromeAppPreferences = {
2
3     "features":{
4
5         "msTeamsOptimization":{
6
7             "screenSharing":true
8         }
9     }
10
11     }
12
13     }
14 <!--NeedCopy-->
```

### Google 管理コンソールの設定

画面共有の最適化が機能するように、**Google** 管理コンソールで次の設定が許可されていることを確認してください。

**Google** 管理コンソールで [デバイス] > [Chrome] > [設定] の3つのカテゴリすべてで [Screen Video Capture] から [Allow sites to prompt the user to share a video stream of their screen] を選択します:

- ユーザーとブラウザの設定
- デバイスの設定
- 管理対象ゲストセッションの設定（または適切なカテゴリ）。



### Citrix Workspace アプリコンテンツの画面共有の制限

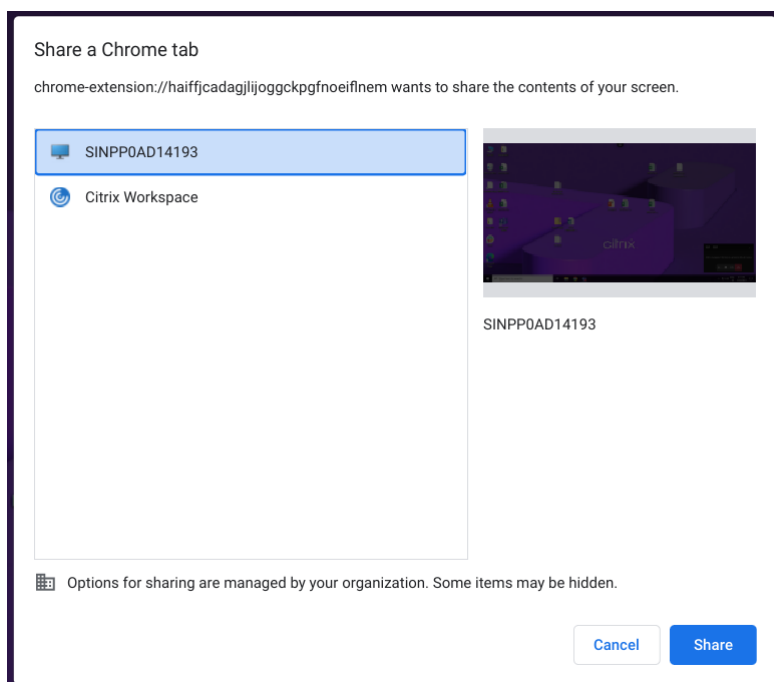
Microsoft Teams を最適化するために、管理者は、管理対象 Chrome デバイスの Citrix Workspace アプリでのみ開かれているアプリとデスクトップの画面共有を制限できます。

管理者がこの機能をオンにすると、エンドユーザーは Citrix Workspace アプリのみから開かれているリソースを共有できます。

この機能は、Chrome バージョン M98 以降で利用できます。

設定を構成するには、次のように Google ポリシーを使用します：

1. **Google** 管理コンソールから、[Settings] > [User & browser settings] に移動します。
2. [Screen video capture allowed by sites]>[Allow tab video capture (same site only) by these sites] に移動して、ChromeOS 向け Citrix Workspace アプリのアプリ ID (haiffjcadaglijjogckpgf-noeiflnem) を入力します。

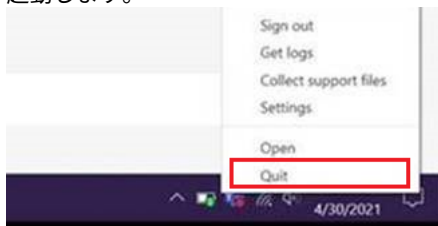


これで、エンドユーザーはタブを選択し、Citrix Workspace アプリでのみ表示されるコンテンツを共有できます。

### Microsoft Teams 最適化のトラブルシューティング

クライアントセッション内で Microsoft Teams を非最適化の状態から最適化に変更するには、以下を実行してください：

- Microsoft Teams アイコンを右クリックして [終了] をクリックし、終了します。Microsoft Teams を再起動します。



- 終了が機能しない場合は、セッションからログオフしてから再度ログオンします。
- ログオフして再ログオンが機能しない場合、VDA のディレクトリ **C:\Users\Administrator\AppData\Roaming\Micro** でキャッシュをクリアし、Microsoft Teams を再起動します。

詳しくは、「[トラブルシューティング](#)」を参照してください。

shim ライブラリバージョンのトラブルシューティングについては、「[Microsoft Teams の最適化ログ](#)」のセクションを参照してください。

### 動的緊急通報 (Dynamic e911) のサポート

Citrix Workspace アプリは、動的緊急通報をサポートしています。Microsoft Calling Plans、Operator Connect、および Direct Routing で使用すると、次の機能が提供されます：

- 緊急通報の構成とルーティング
- セキュリティ担当者に通知する

通知は、VDA 上の Microsoft Teams クライアントではなく、エンドポイントで実行されている Citrix Workspace アプリの現在の場所に基づいて送信されます。

Ray Baum 法では、緊急車両を派遣可能な 911 発信者の位置情報を、適切な公衆安全応答ポイント (PSAP) に送信する必要があります。ChromeOS 向け Citrix Workspace アプリ 2112 以降、HDX を使用した Microsoft Teams の最適化は Ray Baum 法に準拠しています。

### Microsoft Teams の最適化における背景のぼかしと効果

2303 リリース以降、ChromeOS 向け Citrix Workspace アプリで、Microsoft Teams によるビデオ通話の最適化で背景のぼかしと効果が導入されました。Microsoft Teams が提供する背景効果をぼかしたり置き換えたりできます。この機能は、話の最中シルエット (体と顔) に集中できるようにすることで、突然集中力が乱されることを回避できます。この機能は、P2P および電話会議で使用できます。

#### メモ：

- デフォルトでは、この機能は無効になっています。
- この機能は、Microsoft Teams の UI と統合されました。マルチウィンドウのサポートは、VDA を 2112 以降に更新するときに必要な前提条件です。詳しくは、「[マルチウィンドウ会議とチャット](#)」を参照してください。

#### 制限事項

- 管理者およびユーザーが定義したバックグラウンドの置換はサポートされていません。
- この機能を有効にすると、パフォーマンスの問題が発生する場合があります。
- ICA セッションが再接続された後、効果はオフになります。ただし、Microsoft Teams UI は、前の効果がまだオンになっていることをチェックマークで示しています。Citrix と Microsoft は、この問題を解決するために協力しています。

構成方法 背景の効果機能は、次のいずれかの方法で有効にできます：

- Configuration.js
- Google 管理ポリシー
- Global App Configuration Service

**Configuration.js configuration.js** ファイルを使用して背景のぼかしと効果を構成するには、次の手順を実行します。

1. **configuration.js** ファイルを、**ChromeApp** ルートフォルダーで見つけます。

メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

2. **configuration.js** ファイルを編集し、**backgroundEffects** のデフォルト値を **true** に設定します。

このような JSON データの例を次に示します:

```

1  "features" :
2  {
3
4      "msTeamsOptimization" : {
5
6          "backgroundEffects" : true
7      }
8
9  }
10
11 <!--NeedCopy-->

```

3. 変更を保存します。

**Google 管理ポリシー** オンプレミス環境では、管理者は次のように Google 管理ポリシーを使用して背景の効果機能を有効にできます:

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を **engine\_settings** キーの下の **policy.txt** ファイルに追加します。

このような JSON データの例を次に示します:

```

1  "features" :
2  {
3
4      "msTeamsOptimization" : {
5
6          "backgroundEffects" : true
7      }
8
9  }

```

```
10  
11 <!--NeedCopy-->
```

4. 変更を保存します。

**Global App Configuration Service** クラウド環境では、管理者は Global App Configuration Service で **backgroundEffects** 属性を **True** に設定することで、背景の効果機能を有効にできます。

詳しくは、[Global App Configuration Service](#)のドキュメントを参照してください。

### Microsoft Teams でのデュアルトーンマルチ周波数 (DTMF) のサポート

Citrix Workspace アプリで、テレフォニーシステム (PSTN など) および Microsoft Teams の電話会議でのデュアルトーンマルチ周波数 (DTMF) シグナリングの使用がサポートされるようになりました。この機能はデフォルトで有効になっています。

### Microsoft Teams のライブキャプション

Microsoft Teams の最適化では、Microsoft Teams でライブキャプションが有効になっているときにスピーカーが話す内容のリアルタイムの文字起こしがサポートされています。

### セカンダリ呼び出しのサポート

2312 リリース以降、セカンダリ呼び出し機能を使用して、受信通知を受け取るセカンダリデバイスを選択できます。この機能は、Microsoft Teams が最適化されている場合にのみ適用されます。

たとえば、スピーカーをセカンダリ呼び出し機器として設定し、エンドポイントがヘッドフォンに接続されているとします。この場合、Microsoft Teams は受信の呼び出し音をヘッドフォンとスピーカーの両方に送信します。次の場合、セカンダリ呼び出しを設定することはできません：

- 複数のオーディオデバイスが接続されていない場合
- 周辺機器 (Bluetooth ヘッドセットなど) が利用できない場合

#### 注

デフォルトでは、この機能は無効になっています。

### この機能の既知の制限事項

- この機能を有効にすると、セカンダリ呼び出し音がわずかに遅れて 2 回再生されることがあります。この問題は Microsoft Teams のバグであり、今後の Microsoft Teams リリースで修正される予定です。

## 構成

セカンダリ呼び出し音機能は次のいずれかの手段で構成できます：

- Configuration.js
- Google 管理ポリシー

### Configuration.js

メモ：

Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。

**configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

**configuration.js** ファイルを使用してこの機能を有効にするには、次の手順を実行します：

1. **configuration.js** ファイルを、ChromeApp ルートフォルダーで見つけます。
2. このファイルを編集し、**secondaryRingtone** の値を **true** に設定します。

このような JSON データの例を次に示します：

```
1 {
2
3     "features":{
4
5         "msTeamsOptimization":{
6
7             "secondaryRingtone" : true
8         }
9     }
10 }
11
12 }
13
14 <!--NeedCopy-->
```

3. 変更を保存します。

**Google 管理ポリシー** 管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用して機能を有効にできます：

1. Google 管理ポリシーにサインインします。
2. この構成は以下にも適用できます：
  - **[Device] > [Chrome] > [Apps and extensions] > [Users and browsers]** から、拡張機能を検索して、拡張機能のポリシーを見つけます。



- **[Device] > [Chrome] > [Apps and extensions] > [Kiosks]** から、拡張機能を検索して、拡張機能のポリシーを見つけます。
- **[Device] > [Chrome] > [Apps and extensions] > [Managed guest sessions]** から、拡張機能を検索して、拡張機能のポリシーを見つけます。

このような JSON データの例を次に示します：

```

1      {
2
3          "settings": {
4
5              "Value": {
6
7                  "settings_version": "1.0",
8                  "engine_settings": {
9
10                     "features": {
11
12                         "msTeamsOptimization": {
13
14                             "secondaryRingtone" :
15                                 true }
16
17
18
19
20
21
22
23
24
25
26 <!--NeedCopy-->
```

3. 変更を保存します。

### 最適化された **Microsoft Teams** ビデオ会議通話でサイマルキャストの実装

2312 リリース以降、最適化された Microsoft Teams ビデオ会議通話に対して、デフォルトでサイマルキャストサポートが有効になっています。このサポートにより、さまざまなエンドポイントでのビデオ会議通話の品質とエクスペリエンスが向上します。適切な解像度に適応することによってすべての発信者に最適な通話エクスペリエンスを提供できます。

この向上したエクスペリエンスにより、各ユーザーは、複数のビデオ ストリームを異なる解像度（720p、360p など）で配信できます。解像度は、エンドポイントの機能、ネットワークの状態などのいくつかの要因によって異なります。次に、受信側のエンドポイントは、可能な範囲で最高品質の解像度を要求します。これにより、すべてのユーザーに最適なビデオ体験を提供できます。

## Zoom の最適化のサポート

May 16, 2024

2402.1 バージョン以降、ChromeOS 向け Citrix Workspace アプリは、セッション内から最適化されたオーディオおよびビデオ会議エクスペリエンスを実現する、Zoom 仮想デスクトップインフラストラクチャ (VDI) ソリューションとの統合をサポートします。

注:

この機能はデフォルトで有効になっていますが、管理者が構成する必要があります。VDA バージョン 1906 以降でのみサポートされます。

### 前提条件

管理者は以下を構成する必要があります:

- Zoom 仮想チャネルを使用する DDC ポリシー **VirtualChannelWhiteList**。詳しくは、ドキュメントの「[仮想チャネルの許可リストポリシー設定](#)」を参照してください。
- [ChromeOS 用 Zoom VDI を構成する前提条件](#)。

### 機能の制限事項

- Zoom 会議の表示ウィンドウは、プライマリモニターのみに制限されます。
- HID デバイスはサポートされていません
- その他の制限については、「[Limitations of using Zoom VDI for ChromeOS](#)」を参照してください。

### 構成方法

この機能は次のいずれかの手段で構成できます:

- Configuration.js
- Google 管理ポリシー

### Configuration.js

メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configura-**

**tion.js** ファイルを編集することをお勧めします。

- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

**configuration.js** ファイルを使用してこの機能を構成するには、次の手順を実行します：

1. **configuration.js** ファイルを、ChromeApp ルートフォルダーで見つけます。
2. **configuration.js** ファイルを編集し、必要に応じて Zoom URL を追加します。

このような JSON データの例を次に示します：

```
1  "features" :
2  {
3
4      "customVC": [
5          {
6
7              "streamName": "ZOOMHDX",
8              "appId": "html=https://zoom.us/vdi/plugin"
9          }
10     ,
11     {
12
13         "streamName": "ZOOMHDC",
14         "appId": "html=https://zoom.us/vdi/plugin"
15     }
16     ,
17     {
18
19         "streamName": "ZOOMPHX",
20         "appId": "html=https://zoom.us/vdi/plugin"
21     }
22 ],
23 "customVCWhitelistURL": [
24     {
25
26         "url": "https://zoom.us/vdi/plugin",
27         "permissions": [
28             "media"
29         ]
30     }
31     ,
32     {
33
34         "url": "https://zoom.us/vdi/webview",
35         "permissions": [
36             "media"
37         ]
38     }
39 ]
40 ]
41 ]
42 ]
```

```
43 }
44
45 <!--NeedCopy-->
```

3. 変更を保存します。

## Google 管理ポリシー

管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用して機能を構成できます：

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を engine\_settings キーの下の **policy.txt** ファイルに追加します。

注：

この構成は以下にも適用できます：

- [Device] > [Chrome] > [Apps and extensions] > [Users and browsers] から、拡張機能を検索して、拡張機能のポリシーを見つけます。
- [Device] > [Chrome] > [Apps and extensions] > [Kiosks] から、拡張機能を検索して、拡張機能のポリシーを見つけます。
- [Device] > [Chrome] > [Apps and extensions] > [Managed guest sessions] から、拡張機能を検索して、拡張機能のポリシーを見つけます。

このような JSON データの例を次に示します：

```
1 {
2
3 "settings": {
4
5 "Value": {
6
7     "settings_version": "1.0",
8
9 "customVC": [
10    {
11
12        "streamName": "ZOOMHDX",
13        "appId": "html=https://zoom.us/vdi/plugin"
14    }
15    ,
16    {
17
18        "streamName": "ZOOMHDC",
19        "appId": "html=https://zoom.us/vdi/plugin"
20    }
21    ,
```

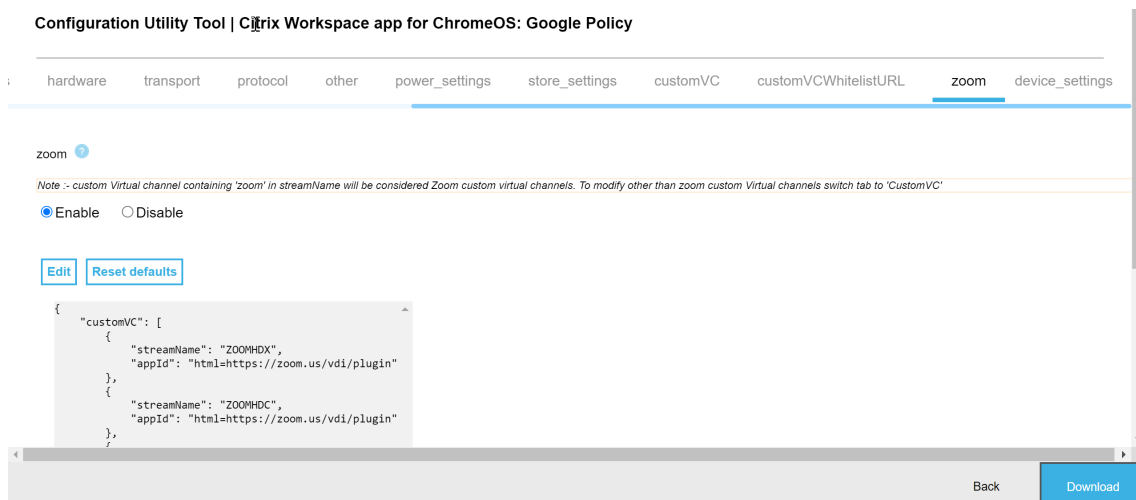
```
22     {
23
24         "streamName": "ZOOMPHX",
25         "appId": "html=https://zoom.us/vdi/plugin"
26     }
27
28 ],
29 "customVCWhitelistURL": [
30     {
31
32         "url": "https://zoom.us/vdi/plugin",
33         "permissions": [
34             "media"
35         ]
36     }
37     ,
38     {
39
40         "url": "https://zoom.us/vdi/webview",
41         "permissions": [
42             "media"
43         ]
44     }
45 ]
46 }
47 }
48 }
49 }
50 }
51 }
52 }
53 <!--NeedCopy-->
```

4. 変更を保存します。

#### 構成ユーティリティツール

機能をカスタマイズするには、以下の手順を実行します：

1. [\[Downloads\]](#) をクリックします。
2. 構成ユーティリティツールセクションまでスクロールし、要素を展開します。
3. ファイルをダウンロードして展開します。
4. [構成ユーティリティツール](#)のドキュメントリンクをクリックして、ツールの使用方法を確認します。
5. [Google ポリシー構成](#)を作成します。
6. 水平方向にスクロールして、**[Zoom]** タブを選択します。続行するには機能を有効にしてください。



7. **[Download]** をクリックして、**policy.txt** ファイルを生成して保存します。
8. 適切な URL を指定して、必要に応じてこの機能をカスタマイズします。
9. Google 管理コンソール内で Citrix Workspace アプリを開きます。
10. 生成された **policy.txt** ファイルをアップロードするか、内容をコピーして貼り付けます。

### ChromeOS 用 Zoom VDI の構成

詳しくは、Zoom のサポート記事「[ChromeOS 用 Zoom VDI の構成](#)」を参照してください。

### マルチモニター

May 16, 2024

#### マルチモニター表示

マルチモニター表示機能は、最大 2 台の外部モニターをサポートします（デバイスの内蔵モニター 1 台 + 外部モニター 2 台）。デフォルトでは、マルチモニター機能は [有効] に設定されています。

UI ダイアログとツールバーは、プライマリモニターでのみ表示されます。一方、USB およびスマートカード認証ダイアログはすべてのモニターに表示されます。

#### 構成方法

デフォルトでは、マルチモニター機能は [有効] に設定されています。

注:

- XenApp 6.5 で実行される Citrix Workspace アプリを使用する場合、マルチモニター機能を使用するにはシャドウポリシーを [無効] に設定します。
- デスクトップセッションで画面が全画面に設定されていると、設定の表示解像度オプションが非アクティブになります。
- UI ダイアログとツールバーは、プライマリモニターでのみ表示されます。一方、USB およびスマートカード認証ダイアログはすべてのモニターに表示されます。

キオスクモードで拡張マルチモニター表示を無効にするには

キオスクモードでの拡張マルチモニター表示は、デフォルトで有効になっています。

キオスクモードを無効にするには、**configuration.js** ファイルまたは **Google** 管理コンソールポリシーを編集し、**kioskMultimonitor** の値を **false** に設定します。

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "features": {
11
12          "graphics": {
13
14            "multiMonitor": true,
15            "kioskMultimonitor": true
16          }
17        }
18      }
19    }
20  }
21
22 }
23
24 }
25
26 }
27
28
29 <!--NeedCopy-->
```

### 注:

キオスクモードでセッションを起動するには、デスクトップ統合モードを有効にする必要があります。

1. Web ブラウザーを起動して次のコマンドを入力します: `chrome://flags`
2. フラガー一覧から `UnifiedDesktopMode` を検索して、これを [有効] に設定します。

統合デスクトップモードを構成するには

1. Google 管理コンソールにログオンします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 統合デスクトップポリシーを [Make Unified Desktop mode available to user] に設定します。
4. [Save] をクリックします。

マルチモニターのパフォーマンス

ChromeOS 向け Citrix Workspace アプリでは、マルチモニター環境でのセッションの全体的なパフォーマンスと安定性が改善されました。以前のバージョンでは、複数のモニターでセッションが実行されていると、パフォーマンスが低下しました。

構成方法

キオスクモードでのマルチモニター表示 キオスクモードでの拡張マルチモニター表示は、デフォルトで有効になっています。

キオスクモードを無効にするには、**configuration.js** ファイルまたは **Google** 管理コンソールポリシーを編集し、**kioskMultimonitor** の値を **false** に設定します。

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "features": {
11
12          "graphics": {
13
14            "kioskMultimonitor": false
15          }
16        }
17      }
18    }
19  }
```



```
18
19     }
20
21     }
22
23     }
24
25 }
26
27
28 <!--NeedCopy-->
```

注:

キオスクモードでセッションを起動するには、デスクトップ統合モードを有効にする必要があります。

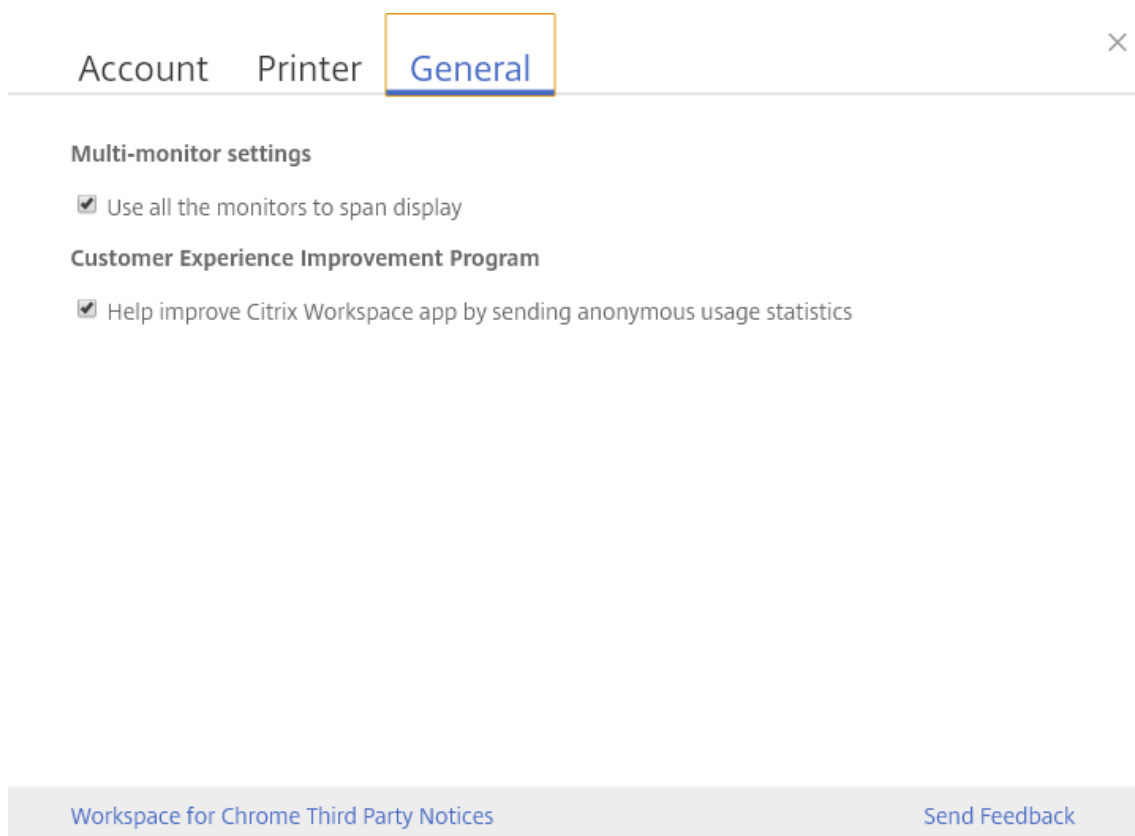
1. Web ブラウザーを起動して次のコマンドを入力します: `chrome://flags`
2. フラガー一覧から `UnifiedDesktopMode` を検索して、これを [有効] に設定します。

**Google** 管理ポリシーを使用して統合デスクトップモードを構成するには

1. Google 管理コンソールにログオンします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 統合デスクトップポリシーを [Make Unified Desktop mode available to user] に設定します。
4. [Save] をクリックします。

マルチモニター機能を無効にするには デフォルトでは、マルチモニター機能は [有効] に設定されています。

1. ChromeOS 向け Citrix Workspace アプリを起動します。
2. [設定] > [一般] を選択します。
3. [すべてのモニターにまたがって表示する] をオフにします。



デスクトップとアプリケーションの両方で、マルチモニター表示を使用できます。

マルチモニター表示を使用すると、デスクトップセッションは以下の 2 とおりの方法ですべてのモニターに表示されます：

4. ウィンドウモード：デスクトップセッションが単一モニターモードで表示されます。
5. 全画面モード：デスクトップセッションが全画面モードに切り替えられると、[すべてのモニターにまたがって表示する] が選択されている場合のみ、セッションはマルチモニターモードで表示されます。

2 台のモニターが接続されている場合、デスクトップセッションのモニターにまたがって表示するには、[すべてのモニターにまたがって表示する] オプションを選択して全画面モードを選択します。

アプリケーションセッションで、2 台のモニターが接続され、[すべてのモニターにまたがって表示する] オプションが選択されていると、セッションは自動的にマルチモニターモードで表示されます。

**Citrix Virtual Desktops** をデュアルモニターで使用する：

1. ツールバーで [マルチモニター] をクリックします。

画面が両方のモニターに拡張されます。

機能の制限事項：

- ChromeOS 向け Citrix Workspace アプリは、複数のモニターでの全画面 H.264 モードをサポートしていません。

- モニター数の制限はハードコードされていません。管理およびレンダリングされる合計解像度が制限数に影響します。
  - この機能は、最大 2 台の外部モニターをサポートします（デバイスの内蔵モニター 1 台 + 外部モニター 2 台）。画面の合計解像度が 2 x (1920x1080) ピクセルを超えるセッションを起動すると、画面の表示に遅延が発生することがあります。この遅延は、モニターの解像度の制限により発生する場合があります。
  - 最新の Chromebook の組み込み画面は、(1920x1080) ピクセルを超える解像度をサポートしています。この機能は、このようなデバイスではテストされていません。
- マルチモニターモードでは全画面 H264 は無効になっています。これは、テスト中に問題が発生したためです。
  - 大型の外部モニターを 1 台使用した場合には問題は発生せず、H264 は引き続き動作します。このシナリオでは、選択的 H264 も動作します。
- 解像度の異なる画面を使用すると、パフォーマンスの問題が発生する可能性があります。
- 高解像度の内蔵モニターと低解像度の外部モニターを一緒に使用すると、パフォーマンスの問題が発生する可能性があります。

### マルチモニター設定での仮想デスクトップのサポート

使用可能なモニターのサブセットすべてで、仮想デスクトップを全画面モードで使用できるようになりました。以前は、ツールバーからマルチモニターモードを選択すると、仮想デスクトップは使用可能なすべてのモニターにまたがっていました。これで、仮想デスクトップをドラッグして 2 台のモニター（3 台以上の場合）にまたがるようにしてから、マルチモニターモードを選択できます。このシナリオの一般的な使用例は、ネイティブデバイスのモニターでビデオ会議アプリを実行することを選択し、通話中に仮想デスクトップのコンテンツを他の 2 台のモニターにまたがって全画面で表示したい場合です。

#### 注:

- この機能を使用するには、[一般] 設定の [マルチモニター設定] で [すべてのモニターにまたがって表示する] オプションを選択します。

### 周辺機器

May 20, 2024

## USB デバイスリダイレクト

ChromeOS 向け Citrix Workspace アプリでは、より幅広い USB 周辺機器がサポートされています。この機能の追加により、Google ポリシーを作成して、Citrix Workspace での使用を有効にするデバイスの PID/VID を特定できます。これは新しい USB デバイスでもサポートされます。

### 構成方法

USB デバイスの構成については、Knowledge Center で[CTX200825](#)を参照してください。

### キオスクモードでの USB デバイスの自動リダイレクト

キオスクモードでは、USB デバイスは手動で操作することなくセッション内で自動的にリダイレクトされます。ユーザーモードとパブリックモードでは、最初にツールバーまたはコネクションセンターから USB デバイスをセッションに手動でリダイレクトする必要があります。この操作は、Chrome オペレーティングシステムに USB デバイスへのアクセスを許可するために必要です。その後 USB デバイスが挿入されると、自動的にセッションにリダイレクトされます。

#### 重要:

- 多くのセッションを実行しているときに USB デバイスを挿入すると、USB はフォーカスされているセッションにリダイレクトされます。
- セッションにフォーカスがない場合、USB デバイスはどのセッションにもリダイレクトされません。
- 1つのセッションが実行中で、USB デバイスを挿入したときにフォーカスされていない場合、USB デバイスがリダイレクトされないことがあります。

### USB デバイスを新しいセッションにリダイレクトするには

#### 注:

USB デバイスを新しいセッションにリダイレクトするには、前のセッションから USB デバイスを削除する必要があります。

1. Citrix Workspace アイコンを右クリックして、[コネクションセンター] を選択します。[コネクションセンター] ウィンドウが開きます。
2. セッションまたはアプリケーションを選択します。
3. [デバイス] をクリックします。
4. [USB] セクションに移動します。
5. [ユーザーを解放] をクリックします。

### ダブルホップ

2301 バージョン以降、Citrix Workspace アプリはダブルホップシナリオをサポートします。この機能は、USB リダイレクトの拡張機能です。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[Citrix Virtual Apps and Desktops でのダブルホップ](#)」を参照してください。

### 複合 **USB** リダイレクト

以前は、複合 USB デバイスがローカルデバイスに接続されていた場合、USB リダイレクトによって単一のデバイスとしてのみリダイレクトされていました。デメリットは、最適化されたチャネルがあるにもかかわらず、オーディオやビデオなどのインターフェイスも USB でリダイレクトされることでした。インターフェイスが分離されていないことが原因で、管理者は USB でリダイレクトするコンポーネントと、最適なパフォーマンスを得るために最適化された仮想チャネルでリダイレクトするコンポーネントを判別できませんでした。

2211 リリース以降、管理者は、デバイスの特定のインターフェイスが USB リダイレクトを介してセッションにリダイレクトされるかどうかを構成できます。エンドユーザーは複合 USB デバイスの特定の構成インターフェイスを Citrix Workspace アプリのセッションにリダイレクトする場合、USB リダイレクトを使用することを選択してからリダイレクトできます。

### 複合 **USB** リダイレクトについて

USB 2.1 以降は、多くの子デバイスが同じ USB バスで単一の接続を共有する USB 複合デバイスの概念をサポートしています。このようなデバイスは、単一の構成スペースと共有バス接続を採用しており、一意のインターフェイス番号 00-ff を使用して各子デバイスを識別します。また、このようなデバイスは USB ハブとは異なります。USB ハブは、ほかの個別にアドレス指定された USB デバイスが接続する USB バスの新しい起点を提供します。

クライアントエンドポイントで検出された複合デバイスは、次のいずれかとして仮想ホストに転送できます：

- 単一の複合 USB デバイス、または
- 独立した子デバイスのセット（分割デバイス）

複合 USB デバイスが転送されると、デバイス全体がローカルデバイスで使用できなくなります。転送により、Citrix Workspace アプリを含むローカルデバイス上のすべてのアプリケーションについて、デバイスのローカル使用が禁止されます。

オーディオデバイスとミュートとボリュームコントロール用の HID ボタンの両方を備えた USB ヘッドセットデバイスを検討してください。デバイス全体が汎用 USB チャネルを使用して転送される場合、デバイスは最適化された HDX オーディオチャネルを介したリダイレクトで使用できなくなります。ただし、汎用チャネルと比較すると、最適化された HDX オーディオチャネルでオーディオが送信される場合の方がパフォーマンスは向上します。

これらの問題を解決するために、複合デバイスを分割し、汎用 USB チャネルを使用する子インターフェイスのみを転送することを Citrix ではお勧めします。このようなメカニズムにより、最適化された HDX エクスペリエンスを提

提供する Citrix Workspace アプリなど、ローカルデバイス上のアプリケーションで他の子デバイスを使用できるようになります。この方法では、必要なデバイスを転送してリモートセッションで使用できます。

この機能を有効にする方法

この機能は、次の方法で有効にできます：

- Configuration.js
- Global App Configuration Service
- Google 管理ポリシー

**Configuration.js configuration.js** ファイルを使用して複合 USB リダイレクトを構成するには、次の手順を実行します：

1. **configuration.js** ファイルを、**ChromeApp** ルートフォルダーで見つけます。
2. **configuration.js** ファイルを編集して、複合 USB リダイレクト機能を構成します。

メモ：

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

3. **enableCompositeDeviceSplit** を **true** に設定します。

このような JSON データの例を次に示します：

```
1  `` `
2  {
3
4      "features": {
5
6          "usb": {
7
8              "enableCompositeDeviceSplit": true
9          }
10     }
11 }
12
13 }
14
15 <!--NeedCopy--> `` `
```

1. 変更を保存します。

注:

- この機能を無効にするには、**enableCompositeDeviceSplit** 属性を **false** に設定します。

**Global App Configuration Service** クラウド環境では、管理者は Global App Configuration Service で **enableCompositeDeviceSplit** 属性を True に設定することで、複合 USB リダイレクト機能を有効にできます。

詳しくは、[Global App Configuration Service](#)のドキュメントを参照してください。

**Google 管理ポリシー** オンプレミス環境では、管理者は次のように Google 管理ポリシーを使用して複合 USB リダイレクト機能を有効にできます:

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [**Chrome** 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を engine\_settings キーの下の **policy.txt** ファイルに追加します。このような JSON データの例を次に示します:

```
1 {
2
3     "features": {
4
5         "usb": {
6
7             "enableCompositeDeviceSplit": true
8         }
9     }
10 }
11
12 }
13
14 <!--NeedCopy-->
```

4. 変更を保存します。

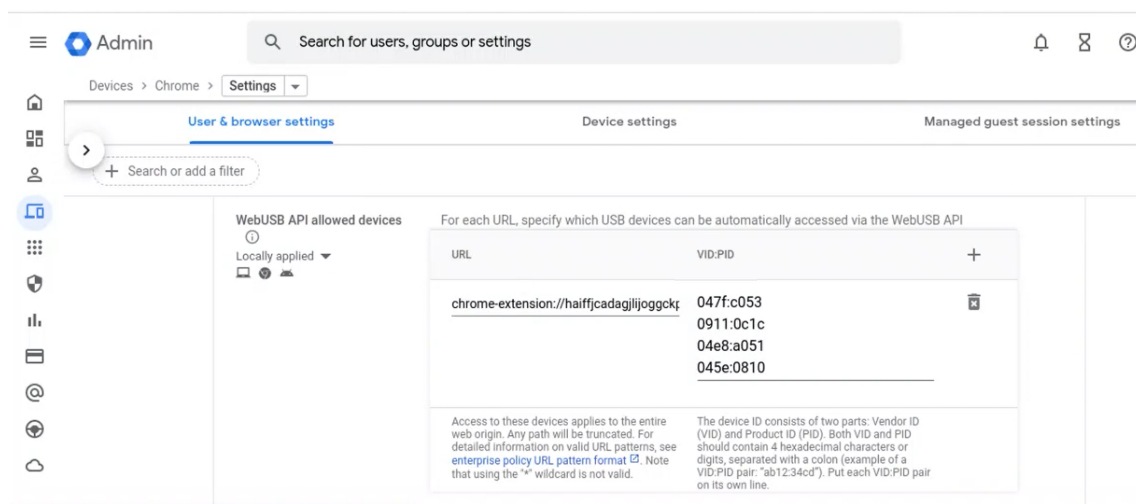
#### 構成

#### 前提条件:

- USB デバイスを VID:PID 値とともに許可リストに登録、および Delivery Controller での USB デバイスリダイレクトのポリシーを有効化。詳しくは、Knowledge Center の記事[CTX200825](#)を参照してください。
- この機能は、管理対象デバイスで機能し、BYOD では機能しません。

USB の自動検出を有効にするには:

1. Google Admin Policy 設定に移動します。
2. **[WebUSB API allowed devices]** オプションを選択します。
3. ChromeOS 拡張機能 ID に Citrix Workspace アプリを入力します。例: `chrome-extension://haiffjcadagjlijoggckpgfnoeiflnem`。
4. 次のように、デバイスの VID と PID を追加します:



VID および PID の値を追加すると、Citrix Workspace アプリがセッション内のデバイスを自動的に検出できるようになりました。

5. Google Admin Policy を適用します。デバイス規則とサンプル JSON データの詳細については、次のセクションを参照してください。
6. 変更を保存します。

### デバイス規則

Citrix Workspace アプリは、デバイスの規則を使用して、リモートセッションへの転送を許可または禁止する USB デバイスを決定します。

キーワードについては、以下を参照してください:

- **allow:** このセクションには、セッションにリダイレクトできるデバイスと、その子インターフェイスの一覧が含まれます。
- **deny:** このセクションには、セッションにリダイレクトできないデバイスと、その子インターフェイスの一覧が含まれます。
- **autoRedirect:** このセクションには、USB リダイレクトでセッションに自動リダイレクトできるデバイスと、その子インターフェイスの一覧が含まれます。



注:

- 各オブジェクトは、USB デバイスの必須の「vid」値と「pid」値を持つデバイスを表します。「split」値と「interfaceClass」の値は任意です。

- **vid, pid** (必須): USB デバイスのベンダー ID (VID) と製品 ID (PID) を表します。10 進数形式で値を入力します。
- **split** (任意): デバイスが子インターフェイスに分割されるかどうかを示すブール値を入力します。
- **interfaceClass** (任意): USB インターフェイスのクラスを表します。使用できる値は、audio (オーディオ)、video (ビデオ)、hid (ヒューマンインターフェイスデバイス)、printer (プリンター)、storage (ストレージ) などです。

このような JSON データの例を次に示します:

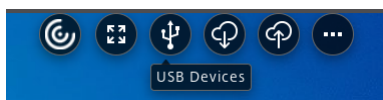
```
1 {
2
3 "settings": {
4
5 "value": {
6
7 "settings_version": "1.0",
8 "device_settings": {
9
10 "deviceRules": {
11
12
13 "allow": [
14 {
15 "vid": "11","pid": "22", "split":true, "interfaceClass":["audio","
16 video"] }
17 //split device and allow redirection of 'audio' & 'video' interfaces.
18 ],
19 "deny": [
20 {
21 "vid": "33","pid": "44" }
22 , //deny redirection of this whole device with vid= 33 & pid = 44,
23 including all of its interfaces.
24 {
25 "vid": "77","pid": "88","split":true,"interfaceClass":["audio"] }
26 //split device and deny the redirection of 'audio' interface only;
27 remaining interfaces(if any) are redirected through USB.
28 ],
29 "autoRedirect": [
30 {
31 "vid": "55","pid": "66" }
32 , //auto redirect the device when it's connected.
33 {
34 "vid": "55","pid": "66","split":true,"interfaceClass":["hid"] }
```

```
34 //split device and auto redirect only the 'hid' interface when the
    device is connected.
35 ]
36         }
37
38     }
39
40 }
41
42 }
43
44 }
45
46 <!--NeedCopy-->
```

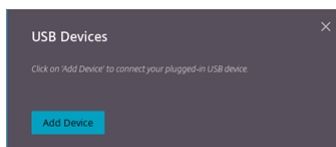
### この機能の使用方法

複合 USB リダイレクト機能を使用するには:

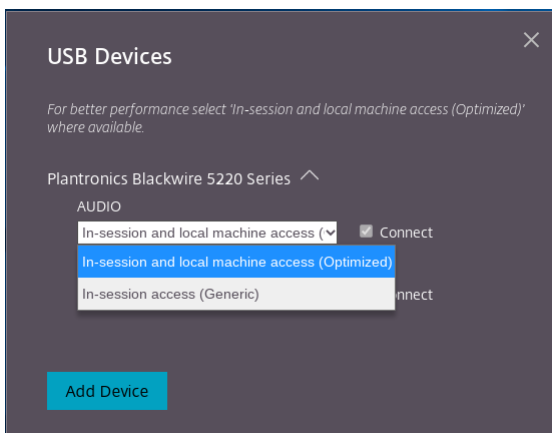
1. ツールバーの USB アイコンをクリックします。



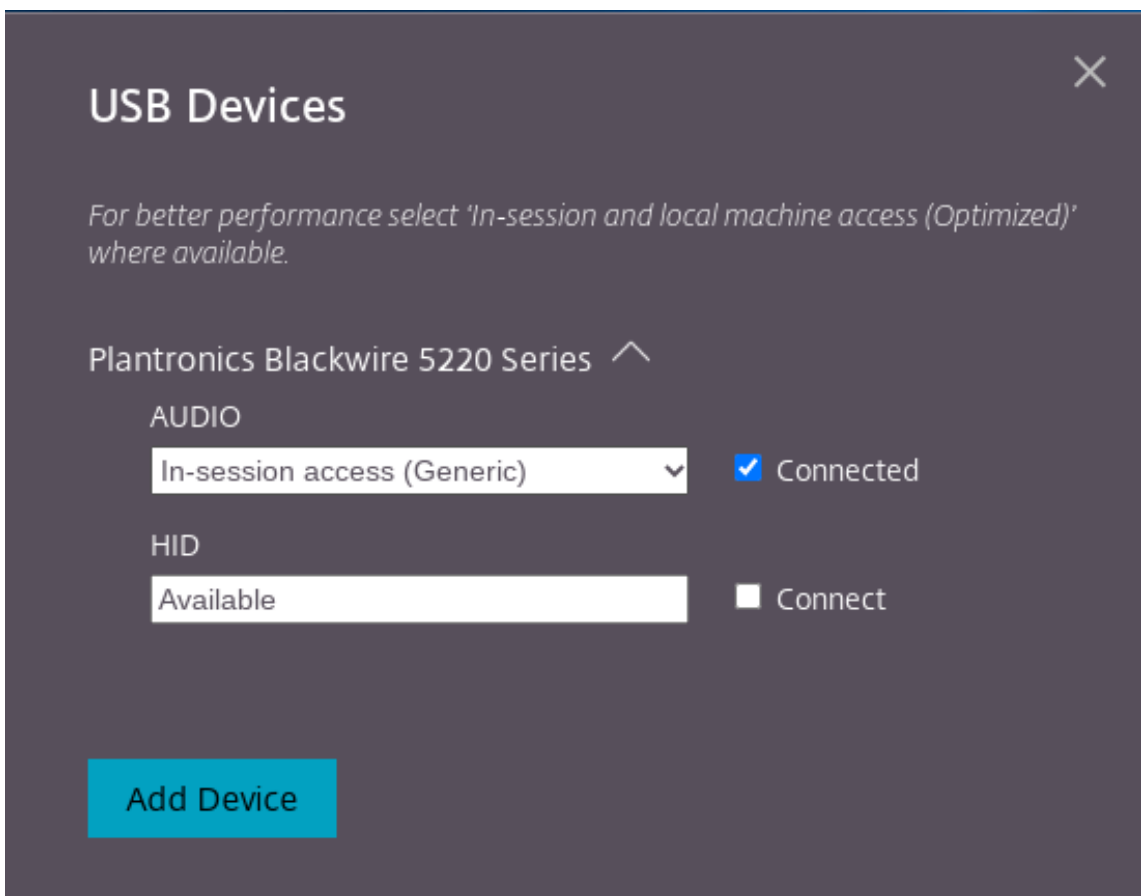
USB デバイスが接続されていない場合は、次のポップアップが表示されます:



2. USB デバイスをローカルマシンに接続します。  
次のポップアップが表示されることがあります:
3. **[USB デバイス]** をクリックして、USB 構成を表示してリダイレクトします。接続に成功すると、Citrix Workspace アプリが USB を検出します。各 USB 構成インターフェイスについて、ドロップダウンメニューが表示されます。2 つのオプションは次のとおりです:
  - セッション内およびローカルマシンアクセス (最適化): デバイス上およびセッション内の USB にアクセスする場合は、このオプションを選択します。
  - セッション内アクセス (一般): セッション内でのみ USB にアクセスする場合は、このオプションを選択します。より高いパフォーマンスを得るには、[セッション内およびローカルマシンアクセス (最適化)] オプションを選択します。



4. インターフェイスをリダイレクトするには、[接続] を選択します。



リダイレクトに成功すると、ステータスが [接続済み] に変わります。

メモ:

- USB デバイスを手動で追加するには、[デバイスの追加] をクリックします。USB デバイスの一覧が Chrome ピッカーダイアログボックスに表示されます。一覧からデバイスを選択できます。
- USB デバイスの接続が拒否される場合は、次のエラーメッセージが表示されます:

「新しく挿入されたデバイスを管理者がブロックしました。  
組織の管理者に問い合わせてください。」

### セッション間で **USB** インターフェイスを転送する方法

ツールバーの USB アイコンをクリックすると、セッションに接続している USB デバイスの一覧が表示されます。USB デバイスが別のセッションで既に使用されている場合は、USB 構成が [別のセッションに接続済み] と表示されていることを確認できます。

現在のセッションにリダイレクトするには、USB 構成の反対側にある [接続] を選択します。それに応じて状態が変化します。

### 複合 **USB** 自動リダイレクト設定

以前は、USB の自動リダイレクト設定に関するエンドユーザーによる設定オプションがありませんでした。管理者がこれらのポリシーを制御するため、エンドユーザーはセッションを開始するときに必要な USB デバイスを手動でリダイレクトする必要があります。

2301 バージョン以降、エンドユーザーは、仮想デスクトップセッション内の任意の USB デバイスの自動リダイレクトの設定を選択できます。Citrix Workspace アプリは、エンドユーザーが USB の自動リダイレクトを制御できるアプリレベルの設定を提供するようになりました。エンドユーザーは設定を実行することができ、起動されるセッション間でその設定を保持できます。

これには 2 つのオプションがあります。1 つはセッションの起動時、もう 1 つはセッションの進行中です。

Account

**General**

✕

All changes made will take effect after relaunching the sessions.

**Multi-monitor settings**

- Use all the monitors to span display

**Customer Experience Improvement Program**

- Send anonymous usage statistics to improve Citrix Workspace app  
(Relaunch the app to apply this setting)

**High DPI Scaling**

- Scale the session for monitors with high device pixel ratio

**Client cursor settings**

- Show assistive cursor when actual cursor is not visible

**USB Auto-Redirection Settings**

- When a session starts, connect devices automatically
- When a new device is connected while a session is running, connect the device automatically

Version 23.1.0.24

[Citrix Workspace app for Chrome Third Party Notices](#)[Send Feedback](#)

注:

- この機能は、オンプレミスとクラウドの環境をサポートし、管理対象 Chrome ユーザーのみが利用できます。

**DDC** ポリシーによる複合 **USB** リダイレクトの構成

以前は、管理者は Google 管理ポリシーを使用してクライアント側の USB リダイレクトを構成しました。

2306 リリース以降は、DDC ポリシーを通じて USB リダイレクトを構成することもできます。DDC ポリシーによる構成により、管理者がポリシーと動作を定義する場合に、統一かつ一元的な方法を使用できます。これらのポリシーは、オンプレミスおよびクラウド展開の管理対象デバイスおよびユーザーに適用できます。この機能は、VDA バージョン 2212 以降でサポートされています。

構成

この機能は次のいずれかの方法で実行できます：

- Configuration.js
- Google 管理ポリシー

注:

- ポリシー **enableDDCUSBPolicy** はデフォルトで **true** に設定されています。

**Configuration.js configuration.js** ファイルを使用してこの機能を無効にするには、次の手順を実行します:

1. **configuration.js** ファイルを、**ChromeApp** ルートフォルダーで見つけます。
2. ファイルを編集します。

メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

3. **enableDDCUSBPolicy** の値を **false** に設定します。このような JSON データの例を次に示します:

```
1  "features" : {
2
3  "usb" : {
4
5      "enableDDCUSBPolicy": false
6      }
7  }
8  }
9
10 <!--NeedCopy-->
```

4. 変更を保存します。

**Google 管理ポリシー** 管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用してこの機能を無効にできます:

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を engine\_settings キーの下の **policy.txt** ファイルに追加します。  
このような JSON データの例を次に示します:

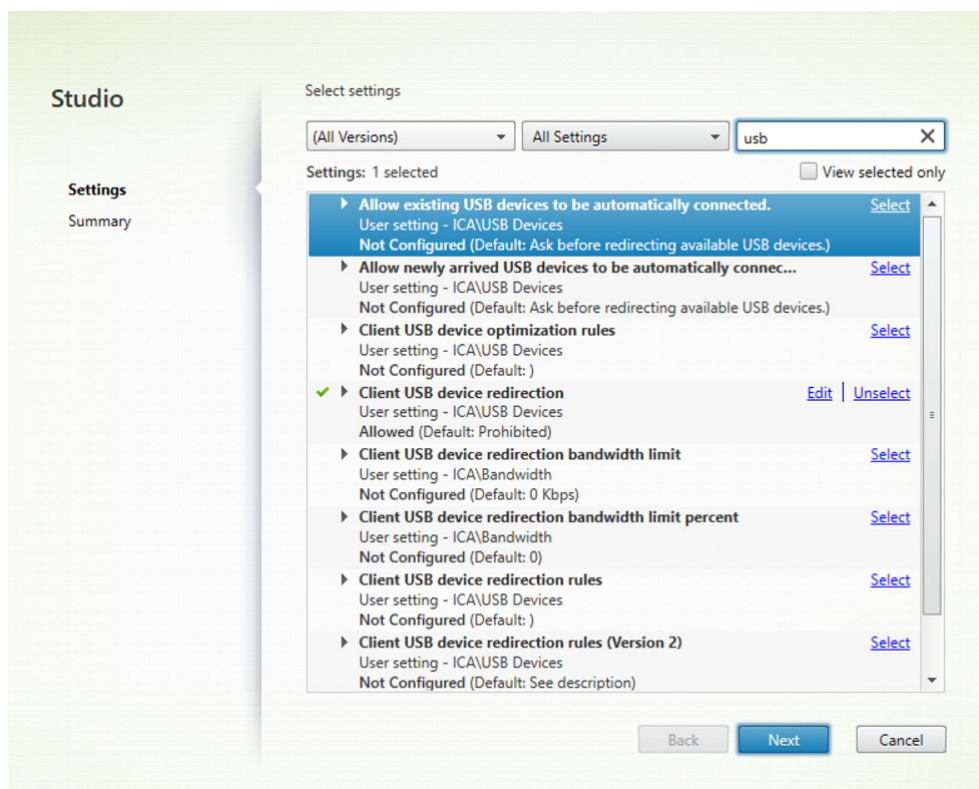
```

1   "features" : {
2
3   "usb" : {
4
5       "enableDDCUSBPolicy": false
6   }
7
8 }
9
10 <!--NeedCopy-->

```

4. 変更を保存します。

**DDC** ポリシー 以下のスクリーンショットは、USB リダイレクトに関連する DDC ポリシーです。この機能は、VDA バージョン 2212 以降でサポートされています。



USB リダイレクトに関連した DDC ポリシーについて詳しくは、Citrix Virtual Apps and Desktops ドキュメントの次の記事を参照してください:

- [クライアント USB デバイスリダイレクト規則](#)
- [既存の USB デバイスの自動接続を許可する](#)
- [新しく受信した USB デバイスの自動接続を許可する](#)
- [クライアント USB デバイスリダイレクト規則 \(バージョン 2\)](#)

## USB デバイスの自動リダイレクト

USB デバイスを自動的にリダイレクトするには、USB デバイス規則に従う必要があります。  
次の方法で USB デバイス規則を設定できます。

- [Google 管理ポリシー](#)
- [クライアント USB デバイスリダイレクト規則 \(バージョン 2\)](#)

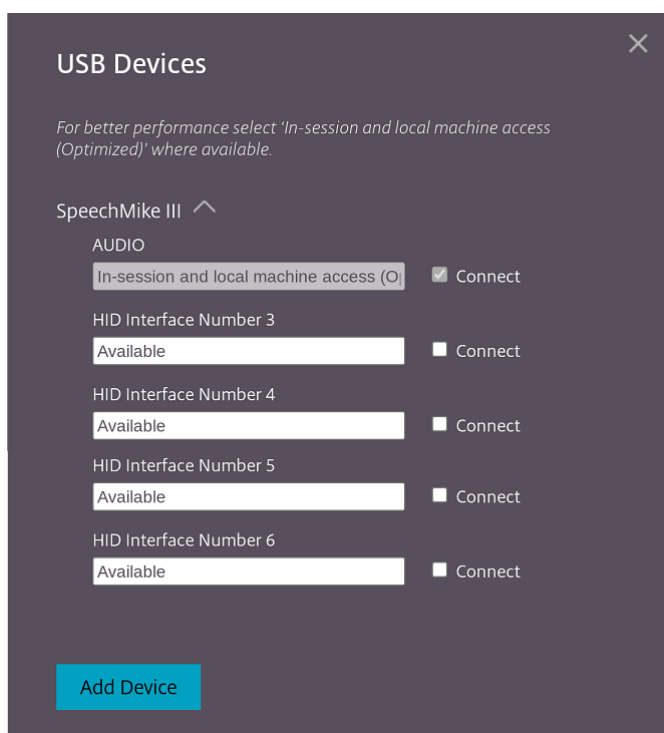
## 複合 USB デバイスの UI の機能強化

2306 リリース以降、複合 USB デバイスの構成の「split」が true に設定されている場合、**USB** デバイスの UI にはインターフェイスクラスではなくインターフェイス番号に基づいてコンポーネントが表示されます。

詳しくは、「[複合 USB リダイレクト](#)」の記事を参照してください。

## ユーザーインターフェイス

以下はその例です：



## DDC ポリシーによる複合 USB リダイレクトの強化

バージョン 2307 以降では、特定の複合 USB インターフェイスまたはインターフェイスクラスがデフォルトで VDA にリダイレクトできるかどうかを判断できるようになりました。ChromeOS デバイ스에複合 USB が接続されてい



る場合、**enableDefaultAllowPolicy** 構成は、DDC ポリシーによる USB リダイレクトをデフォルトで許可できるかどうかを決定するのに役立ちます。この機能は、VDA バージョン 2212 以降でサポートされています。

#### 使用方法

属性 **enableDefaultAllowPolicy** を **true** に設定し、特定のインターフェイスクラスまたはインターフェイス番号を VDA にリダイレクトする場合は、他のインターフェイスクラスまたは番号のリダイレクトを拒否するポリシー規則を追加する必要があります。この機能は、DDC ポリシーのクライアント **USB** デバイスリダイレクト規則（バージョン 2）を使用して構成できます。

詳しくは、「[クライアント USB デバイスリダイレクト規則（バージョン 2）](#)」を参照してください。さらに、Google 管理ポリシーを使用して拒否された部分を構成できますが、これはインターフェイスクラスレベルに対してのみです。

詳しくは、「[複合 USB デバイスの UI の機能強化](#)」を参照してください。

ここでは、DDC ポリシーのクライアント **USB** デバイスリダイレクト規則（バージョン 2）を使用した構成例を示します。この場合、インターフェイス番号 03 のリダイレクトを許可しています。

```
1  ````
2  "DENY: vid=1188 pid=A301 split=01 intf=00,01,02"
3  <!--NeedCopy-->  ````
```

ここでは、Google 管理ポリシー規則を使用した構成例を示します。この場合、HID インターフェイスによるリダイレクトを許可し audio インターフェイスクラスを拒否します。

```
1  ````
2  "deny": [
3    {
4      "vid":"05e9", "pid":"0428", "split":true, "interfaceClass":["audio"]
5    }
6  ]
7  ]
8  <!--NeedCopy-->  ````
```

構成 この機能は次のいずれかの方法で実行できます：

- Configuration.js
- Google 管理ポリシー

#### 注：

- デフォルトでは、ポリシー **enableDefaultAllowPolicy** は **true** に設定されています。

**Configuration.js configuration.js** ファイルを使用してこの機能を無効にするには、次の手順を実行します：

1. **configuration.js** ファイルを、**ChromeApp** ルートフォルダーで見つけます。
2. ファイルを編集します。

メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

3. **EnableDefaultAllowPolicy** の値を **false** に設定します。

このような JSON データの例を次に示します:

```

1  "features" : {
2
3    "usb" : {
4
5      "enableDefaultAllowPolicy": false
6    }
7  }
8  }
9
10 <!--NeedCopy-->
```

4. 変更を保存します。

**Google** 管理ポリシー 管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用してこの機能を無効にできます:

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を **engine\_settings** キーの下の **policy.txt** ファイルに追加します。

このような JSON データの例を次に示します:

```

1  'features' : {
2
3    'usb' : {
4
5      'enableDefaultAllowPolicy': {
6        "type": "false" }
7
8    }
9
10  }
11
```

```
12 <!--NeedCopy-->
```

4. 変更を保存します。

## シリアル COM ポートリダイレクト

デフォルトでは、ChromeOS 向け Citrix Workspace アプリは、COM5 をリダイレクトで優先するシリアル COM ポートとしてマッピングします。

### 構成方法

シリアル COM ポートリダイレクトを構成するには、Citrix Virtual Apps and Desktops および Citrix DaaS のポートリダイレクト設定を適用して、機能を有効にします。ポートリダイレクトについては、「[ポートリダイレクトのポリシー設定](#)」を参照してください。

注:

デフォルトでは、ChromeOS 向け Citrix Workspace アプリは、COM5 をリダイレクトで優先するシリアル COM ポートとしてマッピングします。

VDA でポリシーのシリアル COM ポートリダイレクト設定を有効にするには、次の方法のうちの 1 つを使用して ChromeOS 向け Citrix Workspace アプリを構成します:

- Google 管理ポリシー
- configuration.js ファイル
- アクティブな ICA セッションでコマンドを発行して、デフォルトのマッピングを変更する。

**Google 管理ポリシー**を使用して **COM** ポートリダイレクトを構成する この方法では、ポリシーファイルを編集してシリアル COM ポートをリダイレクトします。

ヒント:

ChromeOS 向け Citrix Workspace アプリが再パッケージされる時のみ、ポリシーファイルを使用して COM ポートを構成することをお勧めします。

Google 管理ポリシーを編集して、以下を含めます:

```
1  {
2
3      "settings": {
4
5          "Value": {
6
7              "settings_version": "1.0",
8              "store_settings": {
```

```
9
10     "rf_web": {
11
12         "url": "<http://YourStoreWebURL>"
13     }
14
15     }
16 ,
17     "engine_settings":{
18
19     "features" : {
20
21     "com" : {
22
23     "portname" : "<COM4>", where COM4 indicates the port number that
        is set by the administrator.
24
25     }
26
27     }
28
29     }
30
31     }
32
33     }
34
35
36 <!--NeedCopy-->
```

シリアル COM ポート名オプションと説明の一覧:

- “portname”: COM (シリアル) 仮想チャネルのポート番号です。デフォルトでは、値は COM5 です。

**configuration.js** ファイルを使用して、**COM** ポートリダイレクトを構成する この方法では、**configuration.js** ファイルを編集して、シリアル COM ポートをリダイレクトします。configuration.js ファイルで portname フィールドを見つけて、ポート番号を変更することで値を編集します。

例:

```
1  "com" :{
2
3
4  "portname" : "COM4"
5
6  }
7
8  <!--NeedCopy-->
```

### 注:

ChromeOS 向け Citrix Workspace アプリが再パッケージされ、StoreFront に再公開された場合のみ、configuration.js ファイルを使用した方法でシリアルポートリダイレクトを構成することをお勧めします。

**ICA** セッションでコマンドを発行して、**COM** ポートリダイレクトを構成する この方法を使用して、シリアル COM ポートをリダイレクトします。アクティブな ICA セッションで次のコマンドを実行します:

```
1 net use COM4 : \Client\COM5
2 <!--NeedCopy-->
```

### ヒント:

上記の例では、COM4 がリダイレクトで優先して使用されるシリアルポートです。

## 電源設定

May 16, 2024

### スリープしない設定

ChromeOS 向け Citrix Workspace アプリでは、ユーザーがアクティブ状態でない場合でも、管理対象の Chromebook デバイスはスリープ状態になりません。

スリープしない設定機能はデフォルトでは無効になっています。

### 構成方法

この機能を有効にするには、**Google** 管理コンソールでポリシーを編集し、**power\_settings** の **keep\_away\_level** プロパティを「**system**」または「**display**」に設定してから、セッションを再起動します。

「**system**」レベルに設定すると、システムはスリープ状態に入りませんが、画面が暗くなるか消えます。「**display**」レベルに設定すると、システムはスリープ状態に入らず、アクティブなままになります。

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
```

```
8     "power_settings": {
9
10        "keep_awake_level": " system" or "display"
11    }
12
13    }
14
15    }
16
17    }
18
19 <!--NeedCopy-->
```

電源設定オプションと説明の一覧:

- “keep\_away\_level”: ユーザーがアクティブでない場合でもデバイスをスリープにならない状態に保ちます。次の 2 つの値のいずれかを選択できます:
  - “system”: システムはスリープ状態になりませんが、画面が暗くなるか消えます。
  - “display”: システムはスリープ状態にならずアクティブなままです。

注:

キオスクモードの場合は、**Google** 管理コンソールの [Allow app to manage power] 設定が無効になっていることを確認します。

## 印刷

May 16, 2024

### PDF 印刷

Citrix PDF ユニバーサルプリンタードライバーによりユーザーは、XenDesktop 7.6 および XenApp 7.6 以降で配信された、ホストされているアプリケーション、または仮想デスクトップ上で実行しているアプリケーションで使用されているドキュメントを印刷できます。ユーザーが [Citrix PDF プリンター] オプションを選択すると、ドライバーがファイルを PDF に変換して、これをローカルデバイスに転送します。PDF は新しいウィンドウで表示したり、印刷したりできます。

ホストされるアプリケーションまたは仮想デスクトップで実行中のアプリケーションで開いているドキュメントを印刷する場合、そのドキュメントを PDF で印刷できます。PDF をローカルデバイス上に転送して、そこで表示したりローカルプリンターで印刷したりできます。ファイルは ChromeOS 向け Citrix Workspace アプリに保存されません。

### 重要

ローカル PDF 出力は、XenApp/XenDesktop 7.6 以降でのみサポートされています。

### 構成方法

**要件** ChromeOS 向け Citrix Workspace アプリのダウンロードページにアクセスするには、My Citrix アカウントが必要です。

ホストされたデスクトップおよびアプリケーションで開いたドキュメントをユーザーが印刷できるようにするには：

1. Citrix PDF プリンターをダウンロードして、Citrix Workspace アプリユーザーにデスクトップまたはアプリを配信する各 VDA マシンに Citrix PDF ユニバーサルプリンタードライバをインストールします。プリンタードライバをインストール後、マシンを再起動します。
2. Citrix Studio の左側のペインで [ポリシー] ノードを選択し、ポリシーを作成するか、既存のポリシーを編集します。  
Citrix Virtual Apps and Desktops ポリシーの構成について詳しくは、「[ポリシー](#)」を参照してください。
3. ポリシーの [PDF ユニバーサルプリンターを自動作成する] 設定を [有効] にします。

### ネットワークプリンターのサポート

以前は、仮想デスクトップセッションから印刷する場合に Citrix PDF プリンターオプションが使用されていました。プリンタードライバはファイルを PDF に変換し、その PDF をローカルデバイスに転送します。これによって、この PDF を新しいウィンドウで表示したり、印刷したりできました。

2305 リリース以降、ChromeOS 向け Citrix Workspace アプリはネットワーク印刷をサポートします。エンドユーザーは、セッション内で Chromebook に接続されているプリンターの一覧を表示できます。ユーザーは、ローカルデバイス上で中間 PDF ファイルを生成せずに、プリンターを直接選択できます。この機能は以下でサポートされています：

- VDA バージョン 2112 以降。
- ChromeOS バージョン 112 以降。

### 注：

- デフォルトでは、この機能は有効になっており、PDF 形式の [メタファイル](#) の印刷のみがサポートされています。

詳しくは、次の記事を参照してください：

- [Citrix Virtual Apps and Desktops ドキュメントの環境内のプリンターとプリンタードライバの管理。](#)

- Citrix ポリシーを使用してデフォルトのセッションプリンターを設定する方法についての Knowledge Center の記事 ([How to use Citrix Policy to Set a Default Session Printer - CTX232031](#))。
- Citrix の印刷に関するクイックスタートガイドとデフォルトの設定についての Knowledge Center の記事 ([Citrix Printing Quick Start Guide and Default configuration - CTX227534](#))。

### 構成

この機能は次のいずれかの方法で無効にできます：

- Configuration.js
- Google 管理ポリシー

#### 注：

- 前提条件として、IT 管理者は Delivery Controller (DDC) で [汎用ユニバーサルプリンターを自動作成する] を有効にする必要があります。詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[クライアントプリンターのポリシー設定](#)」を参照してください。

**Configuration.js configuration.js** ファイルを使用してこの機能を無効にするには、次の手順を実行します：

1. **configuration.js** ファイルを、ChromeApp ルートフォルダーで見つけます。

#### メモ：

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

2. **configuration.js** ファイルを編集し、**networkPrinting** のデフォルト値を `false` に設定します。このような JSON データの例を次に示します：

```
1  {
2
3    "features": {
4
5      " networkPrinting ": {
6
7        "enable": false
8      }
9    }
10 }
11
```



```
12 }
13
14 <!--NeedCopy-->
```

3. 変更を保存します。

**Google 管理ポリシー** IT 管理者は、次のように Google 管理ポリシーを使用してこの機能を無効にできます：

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を **engine\_settings** キーの下の **policy.txt** ファイルに追加します。このような JSON データの例を次に示します：

```
1 {
2
3   "features": {
4
5     " networkPrinting ": {
6
7       "enable": false
8     }
9
10  }
11 }
12 }
13
14 <!--NeedCopy-->
```

4. 変更を保存します。

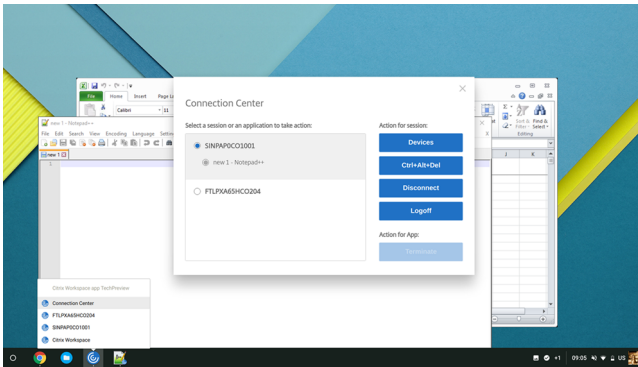
## シームレスなエクスペリエンス

May 16, 2024

### コネクションセンター

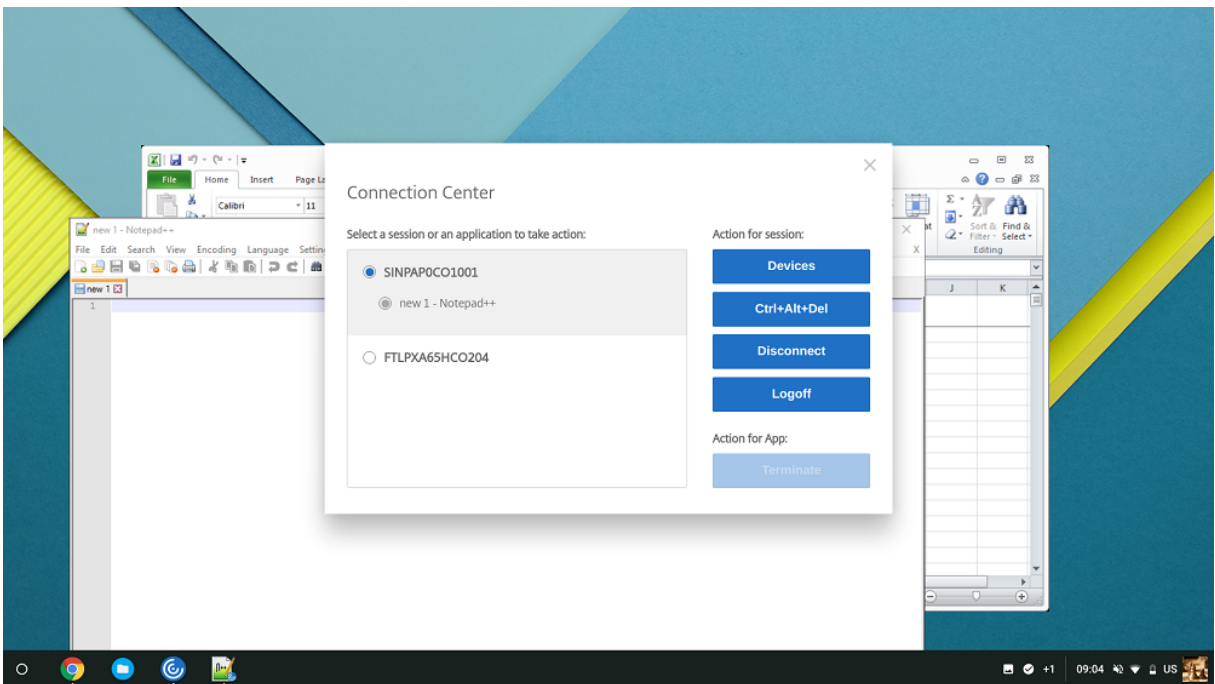
コネクションセンターは、開かれているすべてのアプリケーションを一覧表示するタスクバーを提供することにより、シームレスなセッションを使用するときのアプリケーション管理を行いやすくするものです。

コネクションセンターを起動するには、Citrix Workspace アイコンを右クリックして、[コネクションセンター] を選択します。



コネクションセンターでは、アプリケーションを選択してから、以下の操作を実行できます：

1. デバイスを表示します。
2. Ctrl+Alt+Del コマンドを送信します。
3. セッションから切断します。
4. セッションからログオフします。



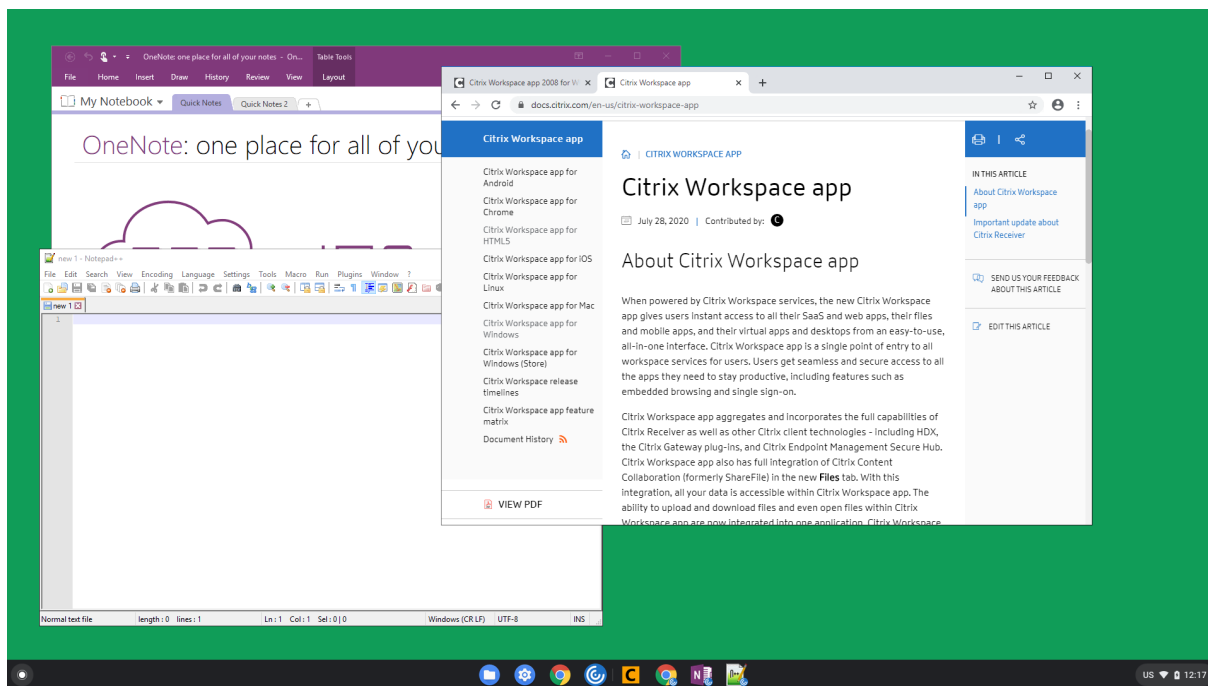
また、[コネクションセンター] ウィンドウで、対応するアプリケーションのラジオボタンを選択して [終了] をクリックすると、アプリを終了できます。

### シームレスウィンドウ統合

ChromeOS 向け Citrix Workspace アプリは、アクティブなセッション内で別のウィンドウでホストされている複数のアプリのシームレスな統合を追加することで、ユーザーエクスペリエンスを向上します。ChromeOS 向け

Citrix Workspace アプリのこの機能を使用すると、単一のウィンドウのセッションですべてのアプリを起動するのではなく、独立したユーザーインターフェイスでアプリを起動できます。

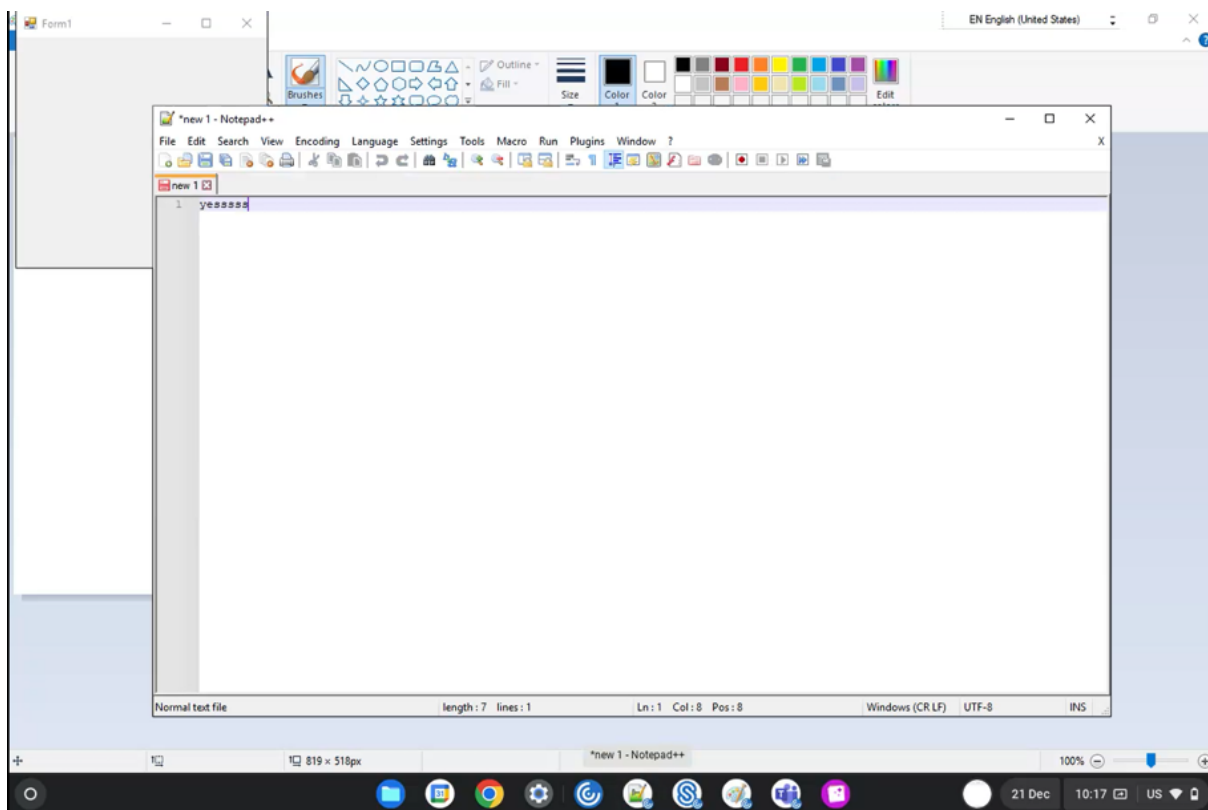
シームレスアプリケーションを個別のウィンドウでホストできます。この機能により、リモートアプリケーションはクライアントデバイス上でネイティブに実行されます。



### 機能の制限事項:

- Chrome タスクバーに追加の項目が表示されます。いずれかのエントリーをクリックすると、選択したセッションが前面に表示されます。
- アクティブなセッションで開いているすべてのアプリが単一のウィンドウで実行されます。アクティブなセッションの 1 つのアプリにフォーカスすると、そのセッションに含まれるほかのすべてのアプリとともに、そのウィンドウがフォーカスされます。

タスクバーのシームレスなアプリアイコンを使用して、アプリをすばやく切り替えることができます:



ヒント:

1つのセッションのすべてのアプリが単一のウィンドウで実行されます。アプリを第2のモニターへ移動すると、そのセッションに含まれるすべてのアプリが第2のモニターへ移動します。

### アプリの切り替え

セッション内で開かれているアプリを表示します。

注:

このオプションは、キオスクモード専用です。

アプリスイッチャーを使うと、ユーザーは同じセッションで実行中の複数のアプリ間で切り替えることができます。フォーカスのあるアプリが強調表示されます。

### 構成方法

構成するには、Google 管理ポリシーを編集して、以下を含めます:

```
1 {  
2  
3   "settings": {
```

```
4
5     "Value": {
6
7         "settings_version": "1.0",
8         "engine_settings": {
9
10            "ui": {
11
12                "appSwitcher": {
13
14                    "showTaskbar": true,
15                    "showIconsOnly": false,
16                    "autoHide": false
17                }
18            }
19        }
20    }
21 }
22
23 }
24
25 }
26
27 }
28
29
30 <!--NeedCopy-->
```

アプリの切り替えオプションと説明の一覧:

- **showTaskbar**: true に設定すると、タスクバーがセッションの下部に表示されます。タスクバーを非表示にするには、このオプションを false に設定します。
- **showIconsOnly**: true に設定すると、タスクバーアイコンが表示されます。このオプションのデフォルト値は false です。
- **autoHide**: true に設定すると、タスクバーは自動的に非表示になります。このオプションのデフォルト値は false です。

### タスクバーのアイコン

アクティブなセッションで Citrix Virtual Apps and Desktops および Citrix DaaS を使用して構成されたアプリケーションおよびデスクトップは、個別のアプリとして表示されます。これらのアプリは、ChromeOS デバイスのタスクバー（シェルフ）に表示されます。この機能は、公開アプリケーションおよびデスクトップに適用できます。これは、Windows オペレーティングシステムでのタスクバーと同様の機能と動作を提供します。

この機能は、デフォルトで有効になります。

### 構成方法

### Google Admin Policy を使ったタスクバーアイコンの構成

注:

ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、この方法を使用することをお勧めします。

1. Google 管理コンソールにログインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. `policy.txt`ファイルに以下の文字列を追加します。

```
//Preferences for chrome app
'appPrefs':{
  'chromeApp':{
    'seamless' : {
      'showInShelf' : false
    },
  },
}
```

4. [保存] をクリックして、ファイルを閉じます。

### StoreFront の `web.config` ファイルを使用したタスクバーアイコンの構成

注:

`web.config`ファイルの方法は、構成目的でのみ使用することを Citrix ではお勧めします。この方法を使用できるのは、ChromeOS 向け Citrix Workspace アプリのストアバージョンが使用されている場合です。

1. Citrix Receiver for Web サイトの`web.config`ファイルを開きます。このファイルは `C:\inetpub\wwwroot\Citrix\...\<Storename>Web` にあります。Storename は、ストアの作成時に指定した名前です。
2. `chromeAppPreferences` フィールドを見つけて、構成の値を JSON 文字列として設定します。

例:

```
1 chromeAppPreferences='{
2
3   "seamless":{
4
5     "showInShelf":false
6   }
7
8   }
9
10 <!--NeedCopy-->
```

`configuration.js` ファイルを使用したタスクバーアイコンの構成 `configuration.js` ファイルは、`ChromeApp` ルートフォルダーにあります。Citrix Workspace アプリを変更する場合は、直接このファイルにアクセスします。

注:

configuration.js ファイルを編集するには、管理者レベルの資格情報が必要です。ファイルを編集した後、アプリを再パッケージして変更を保存してください。

**configuration.js** ファイルを使用して **ChromeOS** タスクバーを変更するには、以下のようになります:

1. configuration.js ファイルを開いて、**showInShelf** 属性を true に設定します。

例:

```
//Preferences for chrome app
'appPrefs':{
  'chromeApp':{
    'seamless' : {
      'showInShelf' : false
    },
  },
}
```

機能の制限事項:

1. 同じアプリケーションの複数のインスタスが起動されると、アイコンでスタックが作成されることなく別々のアイコンとして表示されます。たとえば、メモ帳の 2 つのインスタスがあると、タスクバーに 2 つのメモ帳アイコンが表示されます。
2. アプリのピン留めはサポートされていません。

## セッションエクスペリエンス

June 18, 2024

全画面モード

構成方法

デスクトップセッションを常に全画面モードで開くように構成するには、Google 管理ポリシーを編集して以下を含めます:

注:

- デフォルトでは、" window state" の値は" maximized" に設定されているため、デスクトップセッションは最大化されたウィンドウで開きます。

```
1 {
2
3
4   "settings": {
5
6
7     "Value": {
8
9       "settings_version": "1.0",
10      "engine_settings": {
11
12        "ui": {
13
14          "sessionsize": {
15
16            "windowstate": "fullscreen"
17          }
18        }
19      }
20    }
21  }
22
23  }
24
25  }
26
27 }
28
29 <!--NeedCopy-->
```

## セッションサイズ

### 構成方法

セッションサイズ設定では、セッションの解像度をカスタマイズできます。Google 管理ポリシーを編集して、以下を含めます:

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "ui": {
11
12          "sessionsize" : {
13
```



```
14         "minwidth" : 240,  
15         "minheight" : 120,  
16         "available" : {  
17  
18             "default" : "Fit_To_Window",  
19             "values" : [  
20                 "Fit_To_Window",  
21                 "Use_Device_Pixel_Ratio",  
22                 "1280x800",  
23                 "1440x900",  
24                 "1600x1200"  
25             ]  
26         }  
27     }  
28 }  
29 }  
30 }  
31 }  
32 }  
33 }  
34 }  
35 }  
36 }  
37 }  
38 }  
39 }  
40 }  
41 <!--NeedCopy-->
```

さまざまな解像度オプションと説明の一覧:

- **minwidth:** 240: セッション幅の最小値です。
- **minheight:** 120: セッションの高さの最小値です。
- **available:** セッションの解像度を設定するオプションです。
  - **default:** 設定した値はデフォルトの解像度に適用されます。デフォルトでは、この値は“Fit\_To\_Window” に設定されています。次のように、デフォルト値を変更できます:
    - \* **values:** 以下は、他の解像度の値です:
      - **Fit\_To\_Window:** 利用可能なデフォルトの解像度の値です。ウィンドウサイズと一致するため、さまざまな画面解像度をエミュレートできます。
      - **Use\_Device\_Pixel\_Ratio:** デバイスの DPI に一致するようにセッションを拡大縮小します。
      - **1280x800:** セッションサイズを 1280\*800 ピクセルに設定します。
      - **1440x900:** セッションサイズを 1440\*900 ピクセルに設定します。
      - **1600x1200:** セッションサイズを 1600\*1200 ピクセルに設定します。

### ネットプロモータースコア

ChromeOS 向け Citrix Workspace アプリは、ネットプロモータースコア (NPS) フィードバックを定期的に表示します。表示されるのは、ChromeOS 向け Citrix Workspace アプリの使用体験を評価するよう求めるメッセージです。NPS フィードバックは、顧客満足度を測定することで、アプリの操作性をさらに向上させるためのツールとして導入されました。

1~5 の段階で使用体験を評価することができ、5 は満足していることを示します。

### 構成方法

NPS を構成するには、Google 管理ポリシーを編集して、以下を含めます：オプションが true に設定されている場合、ユーザーは評価を提供できます。

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "ui": {
11
12          "netPromoters": true
13        }
14      }
15    }
16  }
17 }
18
19 }
20
21 }
22
23
24 <!--NeedCopy-->
```

### ICA セッションの自動起動

ChromeOS 向け Citrix Workspace アプリは、Google の管理対象デバイスまたはユーザーで ICA (Independent computing architecture) セッションの自動起動をサポートします。

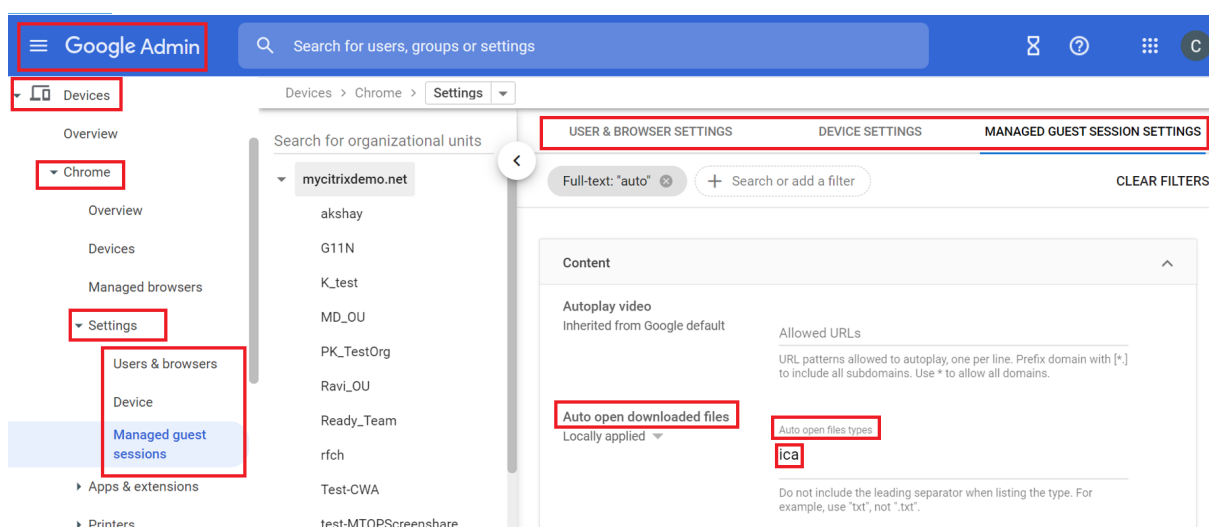
この機能を使用すると、Web の Citrix Workspace からリモートでリソースにアクセスできます。ダウンロードされた ICA ファイルは、デバイスにインストールされた場合、ChromeOS 向け Citrix Workspace アプリで自動的に起動します。以前は、リソースを開始するために、ICA ファイルをダウンロードして手動で開くことしかできません

でした。また、ICA ファイルは開かれても削除されず、デバイスに残り続けました。このリリースでは、ICA ファイルがセッションの自動起動に使用されると、デバイスから自動的に削除されるようになりました。

### 構成方法

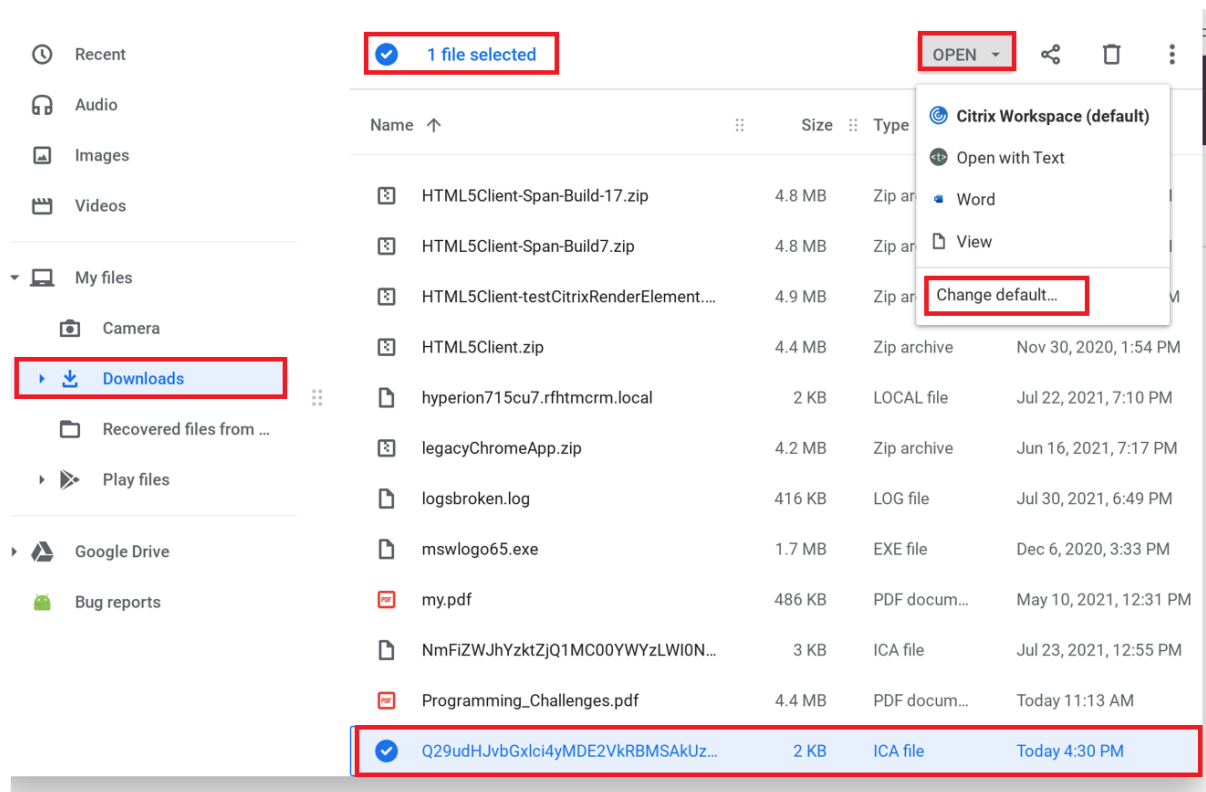
ICA セッションの自動起動を構成するには、管理者としてログインし、次の手順を実行します：

1. **Google** 管理コンソールにログオンします。
2. **Google** 管理コンソールで、[Devices] > [Chrome] > [Settings] を選択します。
3. [Settings] で (必要に応じて) [Users & Browsers]、[Device]、[Managed Guest Session Settings] を選択し、[Auto-open downloaded files] を設定し、**ica** を (管理対象ユーザーと管理対象デバイスの) 必要に応じて [User & Browser Settings]、[Device Settings]、[Managed Guest Session Settings] の [Auto-open file types] に追加します。



次にユーザーに、以下の手順で ICA ファイルを ChromeOS デバイス上で ChromeOS 向け Citrix Workspace アプリに関連付けるよう依頼します：

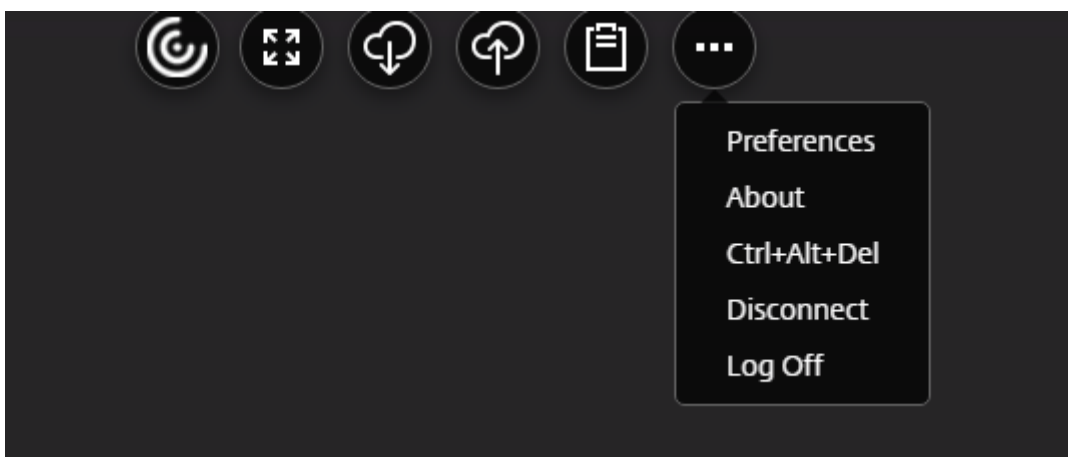
1. ファイルマネージャーを開き、以前にダウンロードした ICA ファイルに移動します。
2. ICA ファイルをクリックします。
3. ナビゲーションバーの右側にある [Open] をクリックして、その横にある矢印を選択します。
4. 次に、[Change default] を選択します。
5. 利用可能なアプリの一覧が表示されます。
6. **Citrix Workspace** を選択します。



### セッション内ツールバーとダイアログ

セッション内ツールバーは、画面上の任意の場所に移動できるフローティングツールバーです。ツールバーには、Citrix Workspace アプリのアイコンが埋め込まれています。カスタマイズされたツールバーにより、ユーザーエクスペリエンスが向上します。この強化により、ツールバーから新しいオプションにアクセスできるようになり、次のような一般的なタスクを実行しやすくなりました：

- 全画面モードへの切り替え
- ファイルのアップロードまたはダウンロード
- アクティブなセッションからクリップボードへのコンテンツのコピーによってセッション間の共有を実現
- より多くのオプションへのアクセス



注:

タッチ操作可能なデバイスでは、Citrix Workspace アプリアイコンが上部中央に表示され、デスクトップセッション中のフローティングツールバーを示します。カーソルを Citrix Workspace に移動すると、フローティングツールバーを示すメニューボタンがワークスペースアイコンに変わります。

構成方法

ツールバーはデフォルトで有効になっています。

個々のツールバー項目を非表示にまたはカスタマイズするには、**Google** 管理ポリシーを編集して、以下を含めます:

```

1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "ui" : {
11
12          "toolbar" : {
13
14            "menubar" :true,
15            "usb": true,
16            "fileTransfer":true,
17            "about":true,
18            "lock":true,
19            "disconnect":true,
20            "logoff":true,
21            "fullscreen":true,
22            "multitouch":true,
23            "preferences":true,

```

```
24         "gestureGuide": true
25     }
26
27     }
28
29     }
30
31     }
32
33     }
34
35 }
36
37
38 <!--NeedCopy-->
```

セッション内ツールバーのオプションと説明の一覧:

- **menubar:** **true** に設定するとツールバーが表示され、**false** に設定すると非表示になります。
- **usb:** USB デバイスダイアログボックスを開きます。セッションにリダイレクトできるデバイス一覧が含まれています。USB デバイスをリダイレクトするには、適切なデバイスを選択して [接続] クリックします。
- **fileTransfer:** ユーザーデバイスと Citrix Virtual Apps and Desktops セッションおよび Citrix DaaS セッション間でのセキュアなファイル転送機能です。セッションに対してファイルをアップロードおよびダウンロードし、データにシームレスにアクセスできます。
- **about:** サードパーティのライセンスページを表示し、バージョン番号を指定します。
- **lock:** 「Ctrl+Alt+Del」をセッションに送信します。
- **disconnect:** セッションを切断します。
- **logoff:** セッションからログオフします。
- **fullscreen:** セッションを全画面モードに調整します。セッションが複数のモニターに接続されている場合、全画面アイコンではなく、マルチモニターアイコンがメニューバーに表示されます。全画面モードのときは、メニューバーに [Restore] アイコンが表示されます。最大化モードを復元するには、ツールバーの UI で [Restore] をクリックします。
- **multitouch:** すべてのジェスチャを仮想セッションにリモート処理します。アプリはサポートされるジェスチャをベースにして動作します。
- **preferences:** CEIP およびディスプレイの解像度設定をカスタマイズするオプションを提供します。
- **gestureGuide:** タッチモードでのジェスチャのガイドを提供します。

**configuration.js** ファイルを使用してツールバーの構成を無効にするには、以下の手順を実行します:

**configuration.js** ファイルは、**ChromeApp** ルートフォルダーにあります。ChromeOS 向け Citrix Workspace アプリに変更を加える場合は、直接このファイルを編集します。

1. **configuration.js** ファイルを開いて、**menubar** 属性を **false** に設定します。

個別のアイコンを非表示にして、ツールバーに表示されないようにすることもできます。たとえば、ツールバーの [Ctrl+Alt+Del] ボタンを非表示にするには、次の手順に従います:

## 1. configuration.js ファイルを開いて、lock 属性を false に設定します。

メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

## セッション共有

このセッション共有機能を使用するには、アプリケーションが同じマシン上でホストされており、ウィンドウのサイズ、色深度、暗号化などのパラメーター設定が同じシームレスウィンドウモードで構成されている必要があります。ホストされているアプリケーションを使用できる場合は、デフォルトでセッション共有が有効になっています。

## バッテリー状態インジケータ

デバイスのバッテリー状態が、仮想デスクトップセッションのシステムトレイに表示されます。以前は、セッションでバッテリー状態インジケータが表示されなかったため、バッテリー残量がなくなった後にノートブックがシャットダウンし、生産性が低下することがありました。

この機能は、VDA バージョン 7.18 以降でのみサポートされています。

注:

- Microsoft Windows 10 VDA では、バッテリー状態インジケータが表示されるまでに約 1~2 分かかる場合があります。

## サービス継続性

サービス継続性により、接続プロセスに関与するコンポーネントの可用性に依存することがなくなるか、依存が削減されます。クラウドサービスのヘルス状態に関係なく、Citrix Virtual Apps and Desktops および Citrix DaaS を起動できます。つまり、サービス継続性により、停止中に DaaS アプリとデスクトップに接続できます。前提条件として、デバイスはリソースの場所へのネットワーク接続を維持する必要があります。

詳しくは、Citrix Workspace ドキュメントの「[サービス継続性](#)」セクションを参照してください。

メモ:

- サービス継続性機能は無効になっています。
- 以前にサービス継続性機能を有効にしていた、ChromeOS 向け Citrix Workspace アプリの古いバージョンを使用している場合は、サービス継続性機能を使用できない可能性があります。この機能を有効に

するには、Citrix Workspace アプリを最新バージョン（2402.1 以降）に更新し、Knowledge Center の記事 [CTX632723](#) の手順を実行することをお勧めします。

### 構成

次の方法でサービス継続性機能を有効にできます：

- Google 管理ポリシー

**Google 管理ポリシー** 管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用してサービス継続性機能を有効にできます：

1. Google 管理ポリシーにサインインします。

2. この構成は以下に適用できます：

- **[Device] > [Chrome] > [Apps and extensions] > [Users and browsers]** から、拡張機能を検索して、拡張機能のポリシーを見つけます。
- **[Device] > [Chrome] > [Apps and extensions] > [Kiosks]** から、拡張機能を検索して、拡張機能のポリシーを見つけます。
- **[Device] > [Chrome] > [Apps and extensions] > [Managed guest sessions]** から、拡張機能を検索して、拡張機能のポリシーを見つけます。

このような JSON データの例を次に示します：

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "features": {
11
12          "serviceContinuity": {
13
14            "enable": true
15          }
16        }
17      }
18    }
19  }
20
21  }
22
23 }
```



```
24
25   }
26
27
28 <!--NeedCopy-->
```

### ブラウザコンテンツリダイレクト

ブラウザコンテンツリダイレクト (BCR) は、リモートブラウザのコンテンツをクライアントのデバイスにリダイレクトします。BCR は、リモートデスクトップウィンドウ内で実行されるフレームやフチのない Web ブラウザーであり、リモート (VDA) ブラウザーのコンテンツ領域に重なります (オーバーレイ)。

BCR はブラウザのコンテンツをクライアントデバイスにリダイレクトし、Citrix Workspace アプリに埋め込まれた対応する Web ブラウザーを作成します。この機能は、ネットワーク使用量、ページ処理、およびグラフィックレンダリングをエンドポイントにオフロードします。そうすることで、要求の多い Web ページ、特に HTML5 または WebRTC を組み込んだ Web ページを閲覧する際のユーザーエクスペリエンスが向上します。ビューポート (ユーザーの Web ページの表示領域) のみがエンドポイントにリダイレクトされます。ブラウザコンテンツリダイレクトは、VDA のブラウザのユーザーインターフェイス (アドレスバー、ツールバーなど) はリダイレクトしません。

つまり、BCR は、クライアント側の許可リストにある Web ページをレンダリングする機能を提供します。この機能は、Citrix Workspace アプリを使用してクライアント側の対応するレンダリングエンジンをインスタンス化し、URL から HTTP および HTTPS コンテンツを取得します。

許可リストの設定方法について詳しくは、以下を参照してください:

- [Chrome 向けの Web ブラウザーコンテンツリダイレクト拡張機能](#)
- [ブラウザコンテンツリダイレクトのポリシー設定](#)

### この機能の既知の問題

- BCR オーバーレイの際、新しいタブで Web サイトのリンクを開くと、セッションブラウザではなくクライアントブラウザで開きます。[HDX-43206]

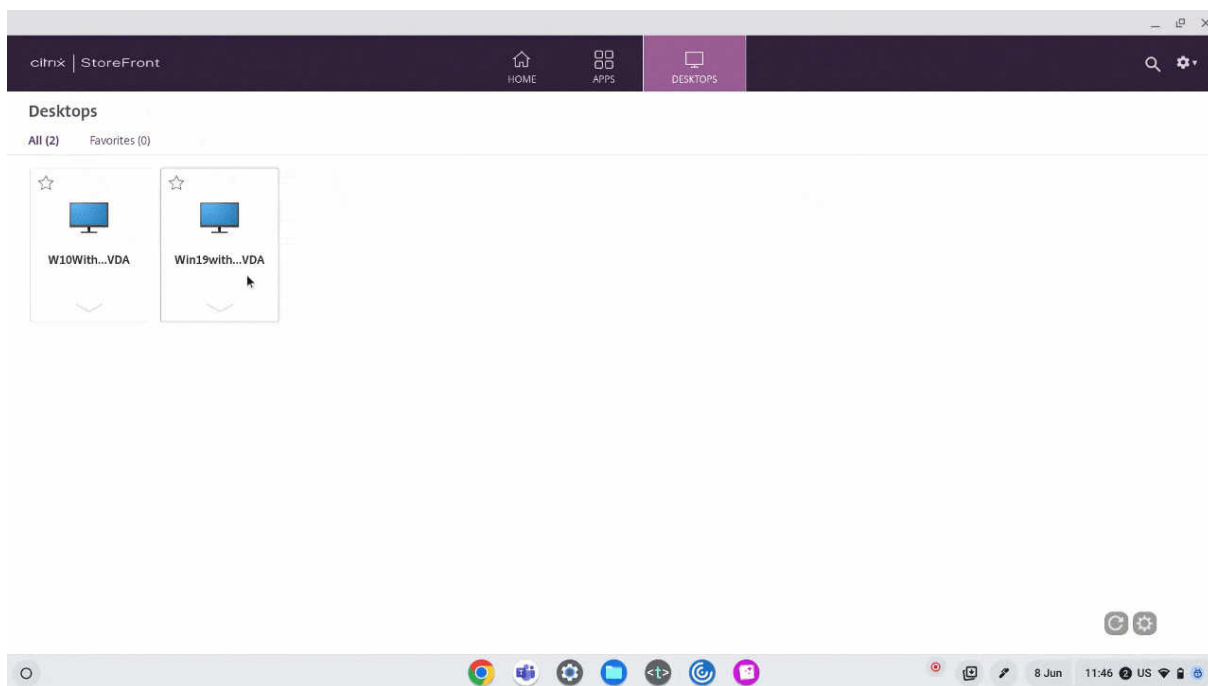
### この機能の既知の制限事項

- この機能は、以下をサポートしていません:
  - サーバー側でフェッチし、クライアント側でレンダリングするシナリオ。
  - 統合 Windows 認証 (IWA) Web サーバー。
  - マルチモニター機能。
- BCR でリダイレクトされた Web サイトにファイルをアップロードまたはダウンロードする場合、VDA セッションのファイルピッカーの代わりに ChromeOS のファイルピッカーが表示されます。[HDX-43207]

- BCR でリダイレクトされたページからの印刷はサポートされていません。

### 仮想アプリとデスクトップの起動エクスペリエンスの向上

2306 リリース以降、アプリとデスクトップの起動エクスペリエンスが向上し、起動状態に関連した情報がタイムリーに提供されます。



### セッション起動通知の表示を構成する

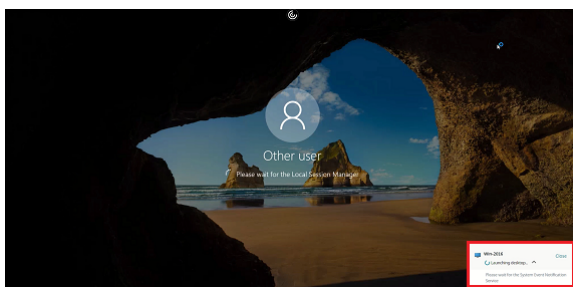
2307 以降、管理者は次の設定を使用して起動の進行状況通知の表示を有効または無効にできます。

この構成が有効になっている場合、画面の右下にセッション起動の進行状況通知が表示されます。この構成が無効になっている場合、セッション起動の進行状況通知は表示されません。

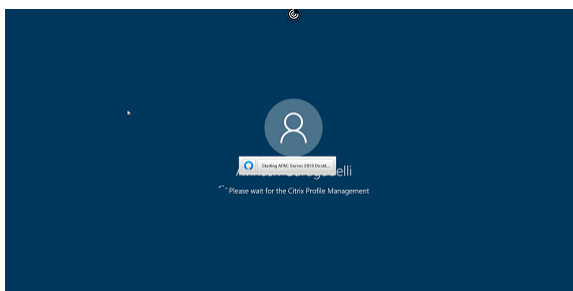
#### 注:

- デフォルトでは、この構成は有効になっています。

通知が無効になっていると、エンドユーザーは起動状態に関する関連情報をタイムリーに得ることができなくなります。



通知が有効になっている場合、エンドユーザーには画面の右下に起動の進行状況が表示されます。



構成 この機能は次のいずれかの方法で実行できます：

- Configuration.js
- Google 管理ポリシー

**Configuration.js configuration.js** ファイルを使用してこの機能を無効にするには、次の手順を実行します：

1. **configuration.js** ファイルを、**ChromeApp** ルートフォルダーで見つけます。
2. ファイルを編集します。

メモ：

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

3. 起動の進行状況通知の表示を無効にするには、**CTXTUI** の値を **false** に設定します。

このような JSON データの例を次に示します：

```
1 {
2
3   "vc_channel": {
4
```

```
5     "CTXTUI": false
6     }
7
8   }
9
10  <!--NeedCopy-->
```

4. 変更を保存します。

**Google 管理ポリシー** 管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用してこの機能を無効にできます：

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を **engine\_settings** キーの下の **policy.txt** ファイルに追加します。

このような JSON データの例を次に示します：

```
1  {
2
3     "settings": {
4
5         "Value": {
6
7             "settings_version": "1.0",
8             "engine_settings": {
9
10                "vc_channel":
11
12            {
13
14                "CTXTUI": false
15
16            }
17
18        }
19
20    }
21
22 }
23
24 <!--NeedCopy-->
```

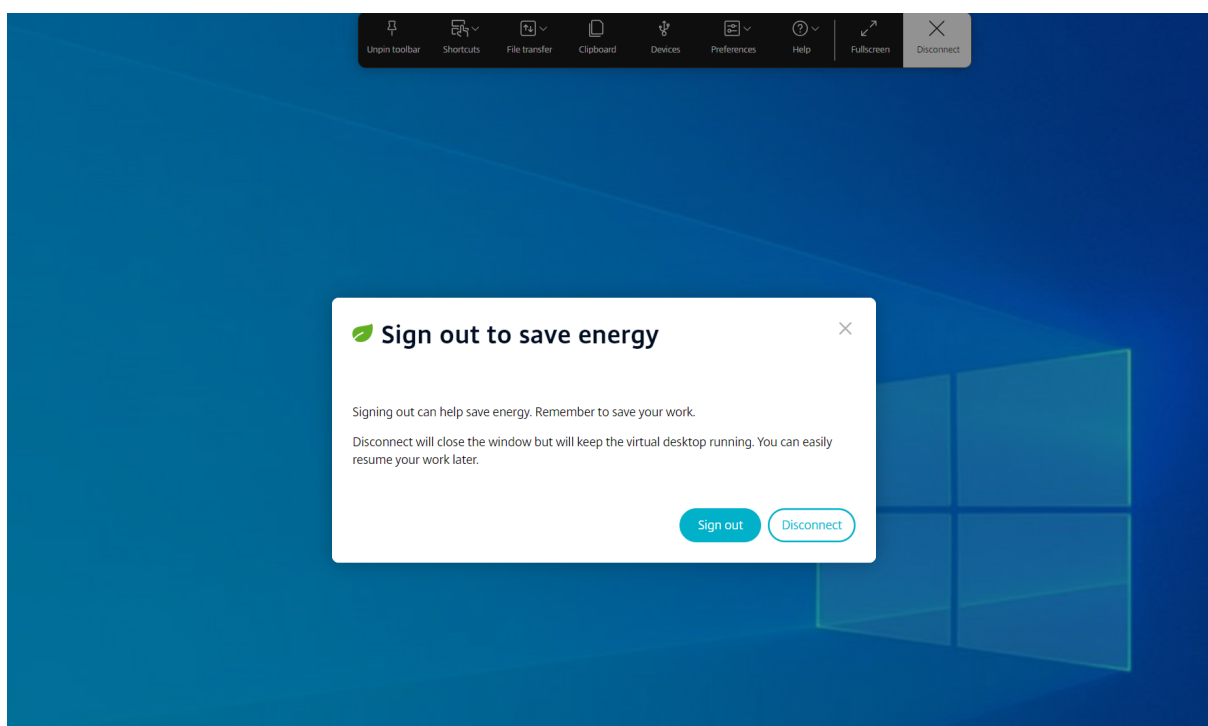
4. 変更を保存します。

## Citrix Workspace アプリでのサステナビリティに関する取り組み

以前は、ユーザーが「X」ボタンをタップして仮想デスクトップを閉じると、仮想デスクトップは切断された状態のままでした。これにより、不必要な電力とリソースが消費されていました。

バージョン 2405 以降、未使用の仮想デスクトップの実行によって使用される可能性のある電力を節約することをユーザーに奨励する、サステナビリティに関する取り組みが導入されました。

この機能を有効にすると、ユーザーが **X** アイコンをタップしてセッションを切断すると、デスクトップセッションからサインアウトするように求めるメッセージが表示されます。Windows OS ポリシーを使用して、ユーザーがログインしていないときに仮想マシンをシャットダウンしている企業の場合、この機能は電力の節約に役立つ可能性があります。



エンドユーザーは次の 2 つの方法でセッションを終了できます：

省エネのためにサインアウトする - このサステナビリティアクションにより、仮想マシンがシャットダウンされ、電力が節約されます。エンドユーザーは、サインアウトする前に作業内容を必ず保存してください。

切断して、仮想デスクトップセッションウィンドウを閉じる。ただし、仮想セッションは次回サインインするまでアクティブなままです。エンドユーザーは簡単に作業を再開できます。

## ストアエクスペリエンス

May 16, 2024

## ストアの設定

## 構成方法

ストアを作成するには、サーバーとの通信を特定して構成します。ストアで利用可能にするリソースを指定できます。次に、Citrix Gateway 経由でのストアへのリモートアクセスを設定します（任意）。ストア設定を構成するには、Google 管理ポリシーを編集して、以下を含めます：

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "store_settings": {
9
10        "name": "SampleStore",
11        "gateways": [{
12
13          "url": "https://yourcompany.gateway.com",
14          "is_default": true
15        }
16      ],
17      "beacons": {
18
19        "internal": [{
20
21          "url": "http://yourcompany.internalwebsite.net"
22        }
23      ],
24      "external": [{
25
26        "url": "http://www.yourcompany.externalwebsite.com"
27      }
28    ]
29  }
30 },
31 "rf_web": {
32
33   "url": "http://yourcompany.storefrontstoreweb.net"
34 }
35 }
36 }
37 }
38 }
39 }
40 }
41 }
42 }
```

```
43
44
45 <!--NeedCopy-->
```

ストア設定オプションと説明の一覧:

- “name”: ストア名を入力します。
- “gateways”: ゲートウェイ URL です。

ゲートウェイ URL を <https://gateway.domain.com> または <https://yourcompany.gateway.com> の形式で追加して、ユーティリティページで [追加] をクリックします。

2 つ以上のゲートウェイ URL が追加されている場合、デフォルトのゲートウェイを設定できます。

ゲートウェイをデフォルトにするには、“is\_default” フラグに true を設定します。デフォルトを指定しない場合は、フラグを false に設定します。

例:

```
1      {
2
3          "settings": {
4
5              "Value": {
6
7                  "settings_version": "1.0",
8                  "store_settings": {
9
10                     "name": "RTST",
11                     "gateways": [{
12
13                         "url": "https://yourcompany.gateway.com"
14
15                         "is_default": true
16                     }
17                 },
18                 {
19                     "url": "https://gateway2.domain.com",
20                     "is_default": false
21                 }
22             ]
23         }
24     }
25 }
26
27 }
28
29 }
30
31
32 <!--NeedCopy-->
```

- “internal”：Citrix Workspace アプリが StoreFront に直接接続するか、ゲートウェイ経由で接続するかを指定します。例: <https://storefront.domain.com>。
- “external”：指定されたネットワークインターフェイスが利用可能で、トラフィックを許可するかを指定します。例: <https://citrix.com>。
- “rf\_web”：ストア URL です。

### 複数のストアをサポート

2305 リリース以降、IT 管理者はエンドユーザーに複数のストアを割り当てることができます。エンドユーザーは、正確なストア URL を覚えていなくても、複数のストアを簡単に切り替えることができるようになりました。この機能により、複数のストアにアクセスするときのユーザー エクスペリエンスが向上します。

### 構成方法

複数のストアを構成するために、IT 管理者は Google 管理ポリシーを編集できます。このような JSON データの例を次に示します：

```
1 {
2
3     "settings_version": "1.0",
4     "store_settings": {
5
6         "name": "SampleStore",
7         "gateways": [{
8
9             "url": " https: //yourcompany.gateway.com",
10            "is_default": true
11        }
12    ],
13    "beacons": {
14
15        "internal": [{
16
17            "url": " http: //yourcompany.internalwebsite.
18        net"
19        }
20    ],
21    "external": [{
22
23        "url": " http: //www.yourcompany.externalwebsite.com"
24    }
25    ]
26    ,
27    "rf_web": {
28
29        "url": " http: //yourcompany.storefrontstoreweb.net"
```



```
30     }
31   ,
32     "secondary_stores": [{
33       "name": " SampleStore",
34       "gateways": [{
35         "url": " https: //yourcompany.gateway.com ",
36         "is_default": true
37       }
38     ],
39     "beacons": {
40       "internal": [{
41         "url": " http: //yourcompany.internalwebsite.
42         net "
43       }
44     ],
45     "external": [{
46       "url": " http: //www.yourcompany.externalwebsite.
47       com "
48     }
49   ]
50   , {
51     "rf_web": {
52       "url": " http: //yourcompany.storefrontstoreweb.net "
53     }
54   }
55   , {
56     "rf_web": {
57       "url": " http: //yourcompany.storefrontstoreweb.net "
58     }
59   }
60 ]
61 }
62 }
63 }
64 }
65 }
66 }
67 }
68 }
69 }
70 }
71 }
72 }
73 }
74 <!--NeedCopy-->
```

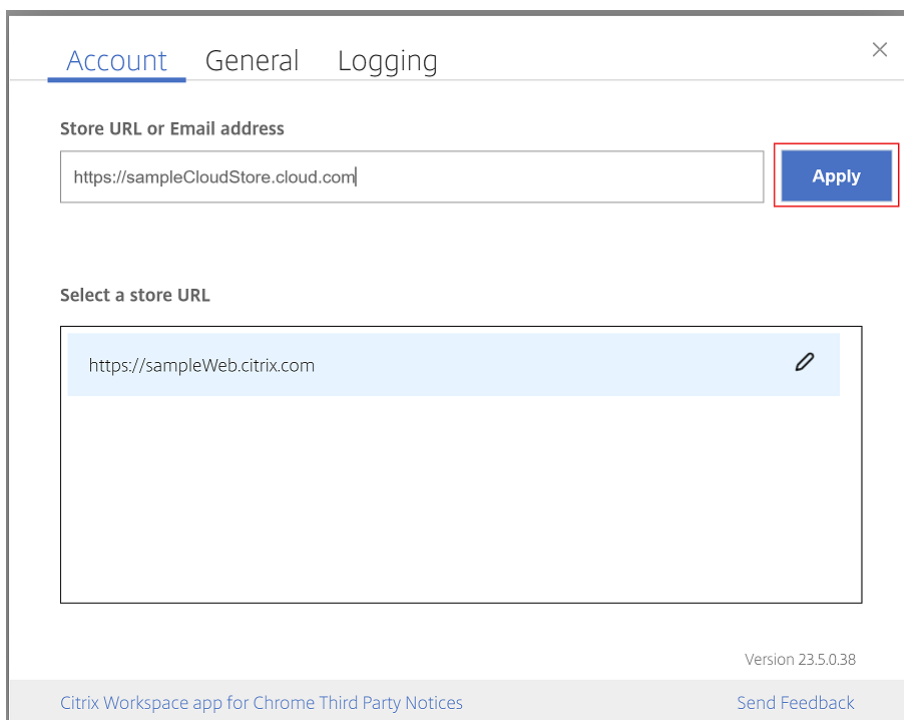
**secondary\_stores** 属性では、複数のストアを構成できます。管理者は JSON 構造を複数回使用できます。ChromeOS 向け Citrix Workspace アプリのカスタマイズ方法について詳しくは、「[構成ユーティリティツール](#)」を参照してください。

## 複数の **StoreFront**

Citrix Workspace を再起動せずにストアアドレスを変更できます。既存の Citrix Workspace セッションが実行中であれば、中断せずに続行します。

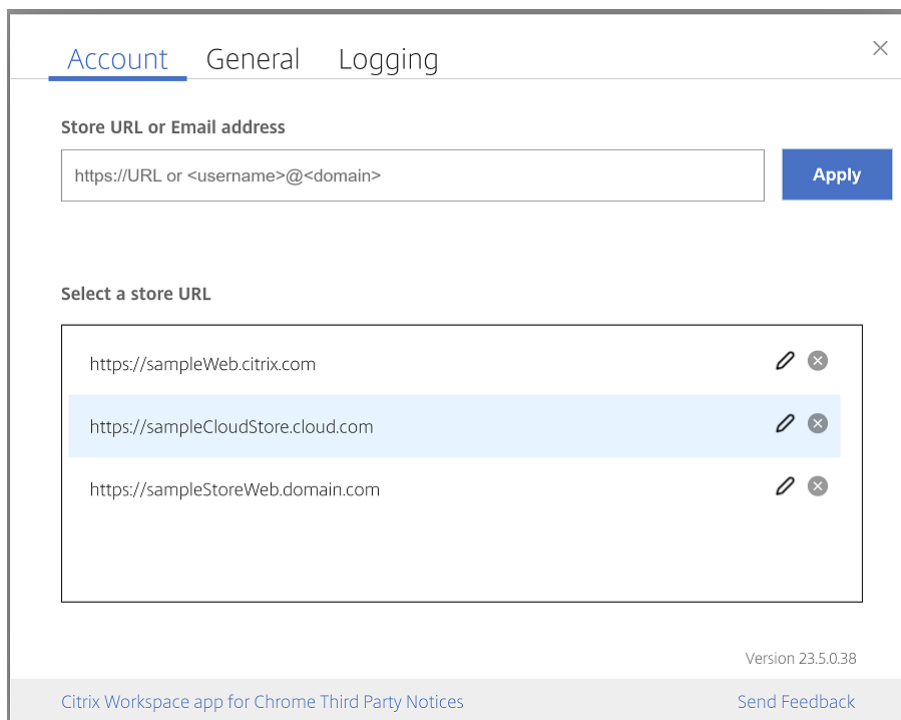
ストアを追加するには、以下の手順を実行します：

1. ChromeOS 向け Citrix Workspace アプリで [設定] をクリックし、[アカウント] タブをクリックします。
2. [ストア **URL** またはメールアドレス] フィールドに StoreFront URL またはメールアドレスを入力します。
3. [適用] をクリックして新しいストアを保存します。

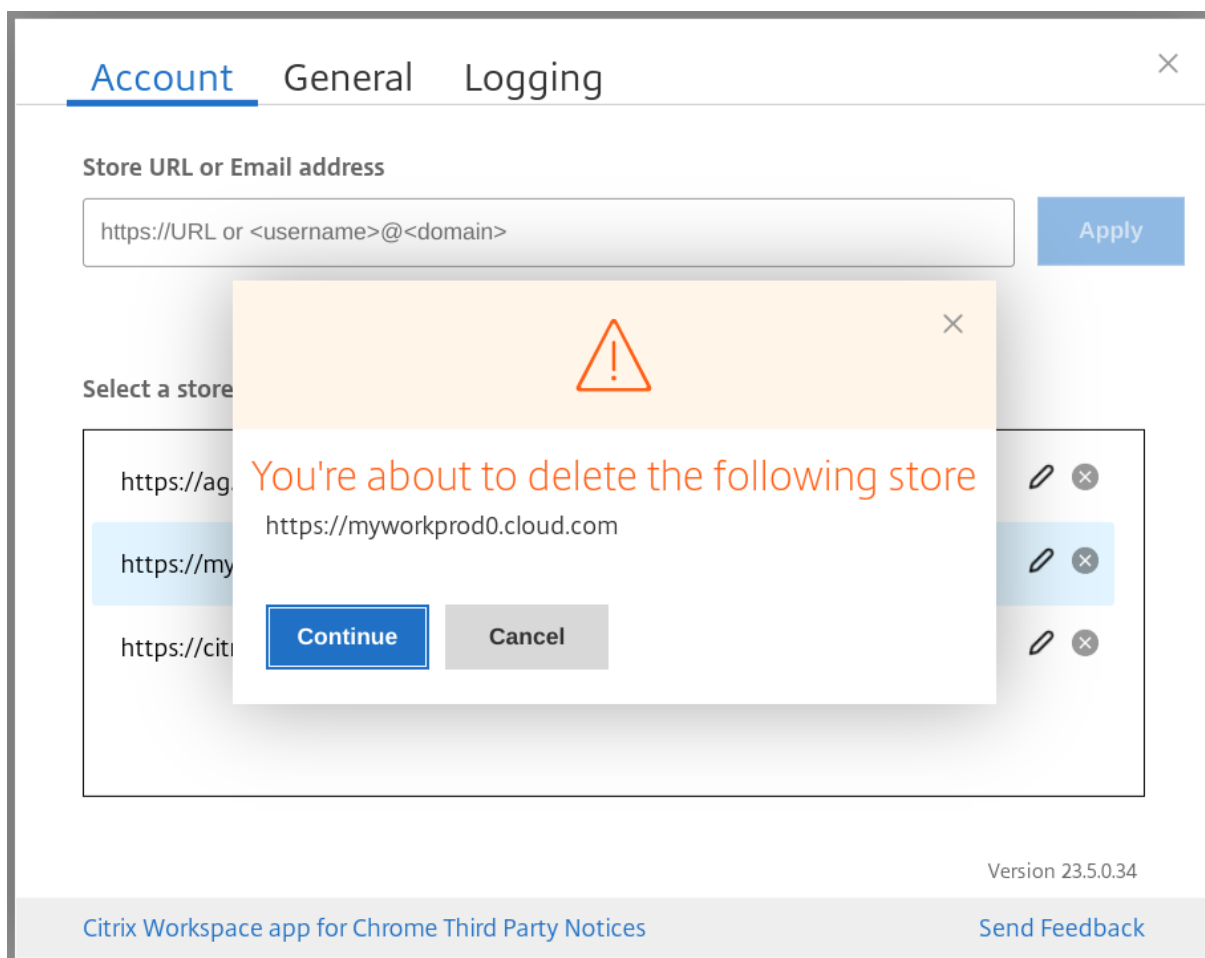


The screenshot shows the 'Account' settings page in the Citrix Workspace app. At the top, there are three tabs: 'Account' (selected), 'General', and 'Logging'. Below the tabs, there is a section titled 'Store URL or Email address' with a text input field containing 'https://sampleCloudStore.cloud.com'. To the right of the input field is a blue 'Apply' button, which is highlighted with a red rectangular box. Below this section is another section titled 'Select a store URL' with a list of store URLs. The first item in the list is 'https://sampleWeb.citrix.com', which is highlighted in light blue. At the bottom right of the list is a small edit icon. At the very bottom of the screen, there is a footer with 'Version 23.5.0.38', 'Citrix Workspace app for Chrome Third Party Notices', and 'Send Feedback'.

ストアを切り替えるには、[ストア **URL** を選択してください] 一覧からストアを選択します。



一覧からストアを削除するには、削除するストアアドレスの横の **削除 アイコン**をクリックし、削除を確定します。



## ストアを再読み込み

ChromeOS 向け Citrix Workspace アプリウィンドウでは、再読み込み操作のボタンが追加されました。ボタンをクリックすると、ストアの Cookie がクリアされ、ストアページが再度読み込まれます。

## Refresh store

2307 リリース以降、次の構成を適用することで、公開アプリのインスタンスの重複を回避できるようになりました。

注:

- デフォルトでは、この構成は無効になっています。この構成を有効にすると、公開されたアプリの重複したインスタンスが表示されなくなります。🔄アイコンをクリックしてストアを更新します。

この機能は次のいずれかの方法で実行できます:

- Configuration.js
- Google 管理ポリシー

## Configuration.js

**configuration.js** ファイルを使用してこの機能を有効にするには、次の手順を実行します：

1. **configuration.js** ファイルを、**ChromeApp** ルートフォルダーで見つけます。

メモ：

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

2. ファイルを編集し、**refreshStore** を **true** に設定します。

このような JSON データの例を次に示します：

```
1  'ui' :{  
2  
3    'refreshStore': true  
4  }  
5  
6  <!--NeedCopy-->
```

3. 変更を保存します。

## Google 管理ポリシー

管理対象デバイスとユーザーの場合、管理者は、次のように Google 管理ポリシーを使用してこの機能を有効にできます。

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [Chrome 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を **engine\_settings** の下の **policy.txt** ファイルに追加します。

注：

この構成は以下にも適用できます：

- [Device] > [Chrome] > [Apps and extensions] > [Kiosks] から、拡張機能を検索して、拡張機能のポリシーを見つけます。

- [Device] > [Chrome] > [Apps and extensions] > [Managed guest sessions] から、拡張機能を検索して、拡張機能のポリシーを見つけます。

このような JSON データの例を次に示します:

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "ui": {
11
12          "refreshStore": true
13        }
14      }
15    }
16  }
17 }
18
19 }
20
21 }
22
23 <!--NeedCopy-->
```

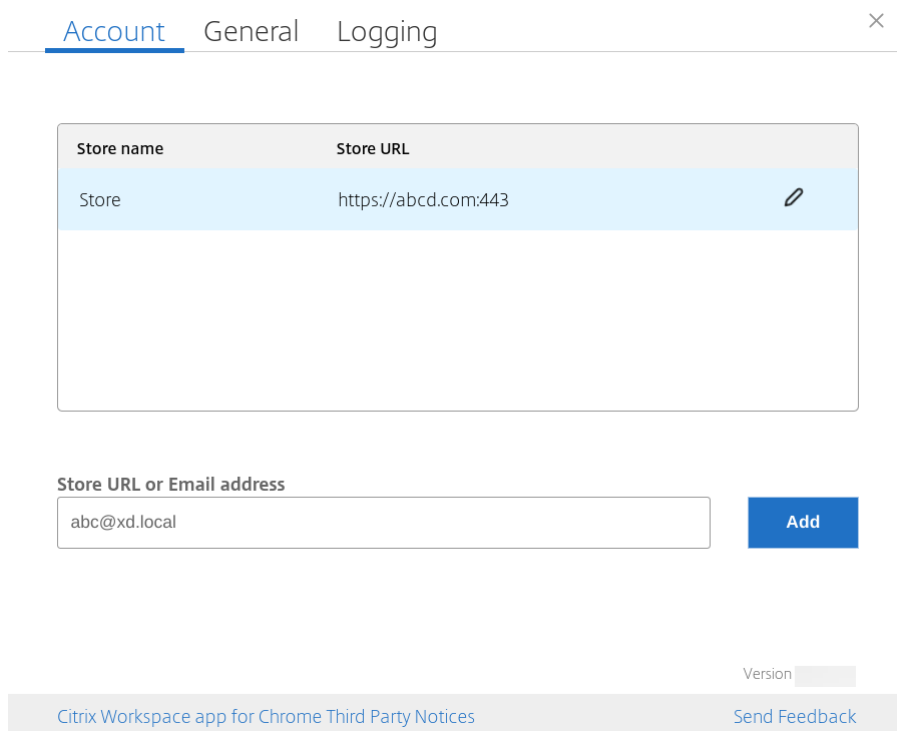
4. 変更を保存します。

#### メールアドレスによるストア検出

これで、ストアの URL を記憶しなくても、メール ID を使用して Citrix Workspace アプリにアクセスできます。アカウントに割り当てられたストアは自動的に入力されます。[アカウント] > [メールアドレスまたはストア URL] ドロップダウンメニューに移動して、メールに関連付けられているストアの一覧を表示します。

注:

ストア URL を使用してサインインすることもできます。



管理者として、ストアアカウントを維持および自動入力するには、前提条件として「[Citrix Cloud API の概要](#)」を参照してください。

詳しくは、「[Global App Configuration Service](#)」を参照してください。

### ストア URL の短い名前

以前は、ストア URL を表示できましたが、ストア URL の短い名前を追加または変更する機能はありませんでした。これは、管理者やユーザーがストア URL を覚える妨げになっていました。

2402 リリース以降、管理対象ユーザーに対して、管理者は Google 管理コンソールからストア URL とともにカスタムストア名をプッシュできるようになりました。この機能により、ユーザーはさまざまなストアを簡単に識別できるようになります。また、管理者は属性 **allowEditStoreName** を **true** または **false** に設定することで、ユーザーがストア名を編集できるかどうかを決定できます。詳しくは、後述の構成セクションを参照してください。

BYOD ユーザーの場合、ストア名は自動生成されます。たとえば、Store、Store 1、Store 2 などです。ストアは、[メールアドレスによるストア検出](#)機能を使用して設定されます。ユーザーは必要に応じてストア名を編集できます。

### 構成

デフォルトでは、BYOD ユーザーはストア名を編集できます。

管理対象デバイスとユーザーの場合、管理者は、属性 **allowEditStoreName** を **true** に設定することで、次のように Google 管理ポリシーを使用してこの機能を有効できます。

注:

- デフォルトでは、属性 **allowEditStoreName** は **false** に設定されています。

**Google 管理ポリシー** このポリシーを有効にするには、次の手順を実行します:

1. Google 管理コンソールにサインインします。
2. この構成は以下にも適用できます:
  - **[Device] > [Chrome] > [Apps and extensions] > [Users and browsers]** から、拡張機能を検索して、拡張機能のポリシーを見つけます。
  - **[Device] > [Chrome] > [Apps and extensions] > [Kiosks]** から、拡張機能を検索して、拡張機能のポリシーを見つけます。
  - **[Device] > [Chrome] > [Apps and extensions] > [Managed guest sessions]** から、拡張機能を検索して、拡張機能のポリシーを見つけます。

このような JSON データの例を次に示します:

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "store_settings": {
9
10        "name": "Citrix store",
11        "allowEditStoreName": true,
12        "rf_web":
13          {
14
15            "url": "https://xyz.cloud.com"
16          }
17        }
18      },
19    }
20  }
21 }
22
23 }
24
25 <!--NeedCopy-->
```

3. 変更を保存します。



### 注:

コードスニペットでは、属性 **name** はストアの短い名前を使用します。

**機能の使用方法** デフォルトでは、BYOD ユーザーはストア名を編集できます。管理対象ユーザーの場合は、組織の管理者がストア名を編集する権限を付与していると編集することができます。詳しくは、「[ストア URL の短い名前](#)」を参照してください。

## タッチとモビリティのサポート

May 16, 2024

### マルチタッチモード

ChromeOS 向け Citrix Workspace アプリでは、Google 管理コンソールからマルチタッチをデフォルトモードとして設定できます。マルチタッチモードでは、マルチタッチジェスチャを有効にするかどうかを制御します。

パンモードとマルチタッチモードを切り替えることができます。以前は、パンモードがデフォルトモードとして設定されていました。

タッチデバイスでセッションを起動すると、デフォルトでは、ジェスチャはパンモードで処理されます。ツールバーを使用してマルチタッチモードに切り替えることができます。この機能により、ユーザーエクスペリエンスが向上します。

### 構成方法

この機能をデフォルトとして設定するには、**Google** 管理コンソールでポリシーを編集し、**[defaultMode]** の値を「**multitouch**」に設定します。

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8         "engine_settings": {
9
10          "ui": {
11
12            "touch" : {
13
```

```

14         "defaultMode" : "multitouch"
15     }
16
17     }
18
19     }
20
21     }
22
23     }
24
25     }
26
27
28 <!--NeedCopy-->

```

## タッチのサポート

ChromeOS 向け Citrix Workspace アプリでは、タッチ対応の Chrome デバイスでタブレットモードでセッションを実行できるようになり、タッチのサポートが強化されました。現在、ジェスチャ、マルチタッチ、およびソフトキーボード機能がサポートされています。

Chrome デバイスがタブレットモードのときに、[キーボードを開く] アイコンがセッションツールバーに表示されるようになりました。この機能を使用するか、3 本指でタップすると、ソフトキーボードが表示されます。

## タッチデバイスでのジェスチャの機能強化

23.4.0 リリース以降、Citrix Workspace アプリは、ジェスチャ、マルチタッチ、およびソフトキーボード機能（タブレットモード）に関連したエンドユーザーエクスペリエンスを強化します。Citrix Workspace アプリセッションで、タップ、スワイプ、ドラッグなど、一般的なマルチタッチジェスチャを使用できます。

ジェスチャガイドは次のとおりです：

これを行うには、以下の手順に従います：	Citrix Workspace アプリで次の操作をする：
クリック	1 本指でタップ
右クリック	タッチしたまま押さえて離す
キーボードを表示する	3 本の指でタップ（またはツールバーのキーボードアイコンをタップ）
ドラッグ	タッチしてそのままドラッグする方向に指を動かす
カーソルを有効にする	2 本の指でタップ

### キーボードの自動表示

入力フィールドに表示されるフローティングキーボードボタンを使用して、サーバーでキーボードの自動表示を有効にできます。キーボードの自動表示機能を使用するには、サーバー側の設定が有効になっていることを確認します。

機能の制限事項:

- マルチタッチモードでは、3本の指でタップしてもソフトキーボードは取得できません。機能するのはパンモードのみです。
- ソフトキーボードが正しく機能するためには、常にシステムのソフトキーボードではなく、セッションツールのキーボードを開くアイコンを使用して、閉じてください。システムのソフトキーボードを使用してソフトキーボードを閉じると、ソフトキーボードが予期しない動作をする場合があります。

### 構成方法

サーバー側の設定を有効にするには、次の手順を実行します:

1. Delivery Controller で、Citrix Studio を開きます。
2. [ポリシー] を選択します。
3. [ポリシーの作成] をクリックします。
4. [キーボードの自動表示] を検索し、[許可] を選択します。

## URL のリダイレクト

May 16, 2024

### ホストからクライアントへのリダイレクト

コンテンツのリダイレクトを使用すると、ユーザーが次のいずれの方法で情報にアクセスするかを制御できます:

- サーバー上で公開されているアプリケーションを使用する、または
- ユーザーデバイス上でローカルにアプリケーションを実行する。

ホストからクライアントへのリダイレクトは、コンテンツのリダイレクト機能の一種です。これは、Citrix XenApp および XenDesktop バージョン 7.15 LTSR 以降を搭載したサーバー OS VDA (デスクトップ OS VDA ではない) のみサポートされます。

詳しくは、XenApp および XenDesktop ドキュメントの「[ホストからクライアントへのリダイレクト - XenApp および XenDesktop](#)」を参照してください。

ホストからクライアントへのリダイレクト機能を有効にすると、URL はサーバー VDA でインターセプトされてからユーザーデバイスに送信されます。ChromeOS 向け Citrix Workspace アプリが、URL をセッション内で開くかローカルデバイスで開くかを選択するようにユーザーに求めるダイアログボックスを表示します。このダイアログは、すべての URL に対して表示されます。

ホストからクライアントへのリダイレクト機能が無効な場合、URL はサーバー VDA 上の Web ブラウザーまたはマルチメディアプレーヤーで開きます。ホストからクライアントへのリダイレクト機能を有効な場合、ユーザーがこの機能を無効にすることはできません。

ホストからクライアントへのリダイレクトは、以前はサーバーからクライアントへのリダイレクトと呼ばれていました。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[一般コンテンツリダイレクト](#)」を参照してください。

### URL リダイレクトの機能強化

以前は、[ホストからクライアントへのリダイレクト](#)機能を有効にすると、URL はサーバー VDA でインターセプトされてからユーザーデバイスに送信されていました。ChromeOS 向け Citrix Workspace アプリが、URL をセッション内で開くかローカルデバイスで開くかを選択するようにユーザーに求めるダイアログボックスを表示します。ダイアログボックスは、URL ごとに表示されていました。

2305 以降、管理者は、さらにダイアログボックスを表示することなく、ローカルデバイス内のリンクを開くように URL リダイレクトを構成できるようになりました。この機能強化により、ユーザーエクスペリエンスが向上します。

#### 注:

- デフォルトでは、この機能は無効になっています。

### 構成方法

この機能は次のいずれかの方法で有効にできます:

- Configuration.js
- Google 管理ポリシー

**Configuration.js** **configuration.js** ファイルを使用してこの機能を有効にするには、次の手順を実行します:

1. **configuration.js** ファイルを、**ChromeApp** ルートフォルダーで見つけます。

メモ:

- Citrix では、**configuration.js** ファイルに変更を加える前に、バックアップを作成することをお勧めします。
- ChromeOS 向け Citrix Workspace アプリをユーザー向けに再パッケージする場合のみ、**configuration.js** ファイルを編集することをお勧めします。
- **configuration.js** ファイルを編集するには、管理者レベルの資格情報が必要です。

2. **configuration.js** ファイルを編集し、**forceOpenInClient** のデフォルト値を **true** に設定します。このような JSON データの例を次に示します:

```
1 {
2
3   "features": {
4
5     "UrlRedirection": {
6
7       "forceOpenInClient": true
8     }
9   }
10 }
11
12 }
13
14 <!--NeedCopy-->
```

3. 変更を保存します。

**Google 管理ポリシー** オンプレミス環境では、管理者は次のように Google 管理ポリシーを使用してこの機能を有効にできます:

1. Google 管理ポリシーにサインインします。
2. [端末管理] > [**Chrome** 搭載端末] > [ユーザー設定] の順に移動します。
3. 次の文字列を **engine\_settings** キーの下の **policy.txt** ファイルに追加します。このような JSON データの例を次に示します:

```
1 {
2
3   "features": {
4
5     "UrlRedirection": {
6
7       "forceOpenInClient": true
8     }
9   }
10 }
11
```

```
12 }  
13  
14 <!--NeedCopy-->
```

4. 変更を保存します。

## 仮想チャネル

May 16, 2024

### 仮想チャネルについて

仮想チャネルは、サーバー側のアプリケーションと通信するクライアント側の仮想ドライバーで構成されます。仮想チャネルは Citrix Virtual Apps and Desktops サーバーを使用したリモートコンピューティング環境に不可欠な要素です。

仮想チャネルは次の用途に使用されます：

- 印刷
- シリアルポートマッピング
- クリップボード
- オーディオ
- マルチメディア
- コントロールチャネル
- EUEM
- USB
- ファイル転送
- モビリティ
- マルチタッチ
- スマートカード
- モバイル デバイス上の Receiver
- Microsoft Teams
- Input Method Editor
- ブラウザーコンテンツリダイレクト
- クライアントドライブマッピング
- 透過的なユーザーインターフェイス

## 構成方法

すべての仮想チャネルはデフォルトで有効になっています。特定の仮想チャネルを無効にするには、Google 管理ポリシーを編集して、以下を含めます:” vc\_channel” の下の機能名を選択して、ユーティリティページで [追加] をクリックします。例:

```

1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "vc_channel": {
11
12          "<vc_name1>": false,
13          "<vc_name2>": false,
14          "<vc_name3>": false,
15          "<vc_namen>": false
16        }
17      }
18    }
19  }
20 }
21
22 }
23
24 }
25
26
27 <!--NeedCopy-->

```

特定の” vc\_channel” を有効にするには、機能を選択し、ユーティリティページで [削除] をクリックします。

### 注:

名前は 1~n の範囲で指定できます。最後の name 「n」に true または false を設定した後は、コンマを使用することはできません。

```

1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "vc_channel": {
11

```

```

12         "CTXCPM " : false,
13         "CTXCAM " : false,
14         "CTXGUSB" : false
15     }
16
17     }
18
19     }
20
21     }
22
23 }
24
25
26 <!--NeedCopy-->

```

仮想チャンネルオプションと説明の一覧:

- “CTXCPM” : PDF 印刷です。
- “CTXCCM” : クライアントのシリアルポートのマッピングです。
- “CTXCLIP” : セッションから VDA へ、および VDA からセッションへのクリップボード操作です。
- “CTXCAM” : クライアントオーディオマッピングです。
- “CTXMM” : Citrix マルチメディアリダイレクトです。
- “CTXCTL” : Citrix コントロール仮想チャンネルです。
- “CTXEUEM” : EUEM (End User Experience Monitoring: エンドユーザー状況監視) です。
- “CTXGUSB” : USB デバイスをセッションにリダイレクトします。
- “CTXFILE” : ユーザーデバイスと Citrix Virtual Apps and Desktops セッションおよび Citrix DaaS (Citrix Virtual Apps and Desktops サービスの新名称) セッション間での、セキュアなファイル転送機能です。セッションに対してファイルをアップロードおよびダウンロードし、データにシームレスにアクセスできます。
- “CTXMTCH” : マルチタッチは、仮想セッションへのすべてのジェスチャをリモート処理します。アプリは、サポートするジェスチャに基づいて動作します。
- “CTXSCRD” : スマートカードのサポートです。
- 「CTXMOB」: モバイルデバイス上の Receiver の仮想チャンネル。
- 「CTXMTOP」: Microsoft Teams の仮想チャンネル。
- 「CTXIME」: Input Method Editor (IME)。
- 「CTXCSB」: ブラウザーコンテンツリダイレクト。
- 「CTXCDM」: クライアントドライブマッピング。
- 「CTXTUI」: 透過的なユーザーインターフェイス。

### カスタム仮想チャンネル

Chrome の仮想チャンネル SDK を使用すると、サードパーティの Chrome アプリでカスタム仮想チャンネルを作成できます。これらのチャンネルは、Citrix Workspace アプリまたは HDX SDK for Chrome を使用して起動されたアプリおよびデスクトップセッションで初期化されます。



さらに、仮想チャンネル SDK を使用すると、サードパーティの Chrome アプリ、アプリおよびデスクトップからデータを簡単に書き込み、受信できます。

### 構成方法

カスタム仮想チャンネルを構成するには、Google 管理ポリシーを編集して、以下を含めます：

```
1 {
2
3   "settings": {
4
5     "Value": {
6
7       "settings_version": "1.0",
8       "engine_settings": {
9
10        "customVC": [
11          {
12
13            "appId": "xyz",
14            "streamName": "abc"
15          }
16        ]
17      }
18    }
19  }
20 }
21
22 }
23
24 }
25
26
27 <!--NeedCopy-->
```

CustomVC オプションと説明の一覧：

- “appId”：カスタム仮想チャンネルを実装している Chrome アプリの ID です。
- “streamName”：仮想チャンネル名です。

### トラブルシューティング

May 16, 2024

### ログを収集する方法

ChromeOS 向け Citrix Workspace アプリは、ユーザーデバイスが生成したログにタイムスタンプを付けます。Citrix Workspace アプリは、進行中の仮想デスクトップおよび仮想アプリのセッションのログ収集をサポートしません。

エンドユーザーは、トラブルシューティングに役立つログを収集できます。ログはユーザーデバイスとマシンの両方で生成できます。デスクトップのログとアプリケーションのログを生成できます。

以前は、進行中のセッションで [ログの開始] を選択した後に起動されたセッションのログのみを収集できました。これによって、[ログの停止] を選択するまで、進行中およびその後のセッションのログが収集されます。

ユーザーデバイスでログ機能を有効にするには

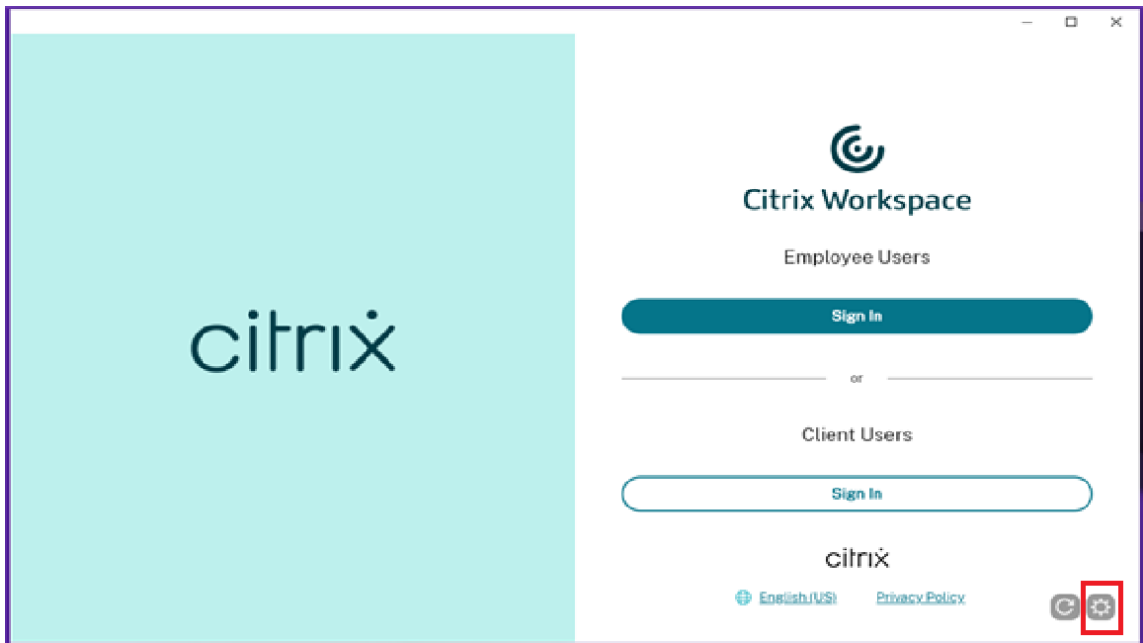
1. ユーザーデバイスで、Citrix Workspace アプリを起動し、ログインページに移動します。
2. 右下隅にある設定の画像ボタンを選択します。
3. [設定] ダイアログボックスで [ログの開始] を選択します。  
[設定] ダイアログボックスに、収集されたログファイルの詳細が一覧で表示されます。
4. [ログの停止] を選択してユーザーデバイス上でのログの収集を終了します。

### クライアントログ

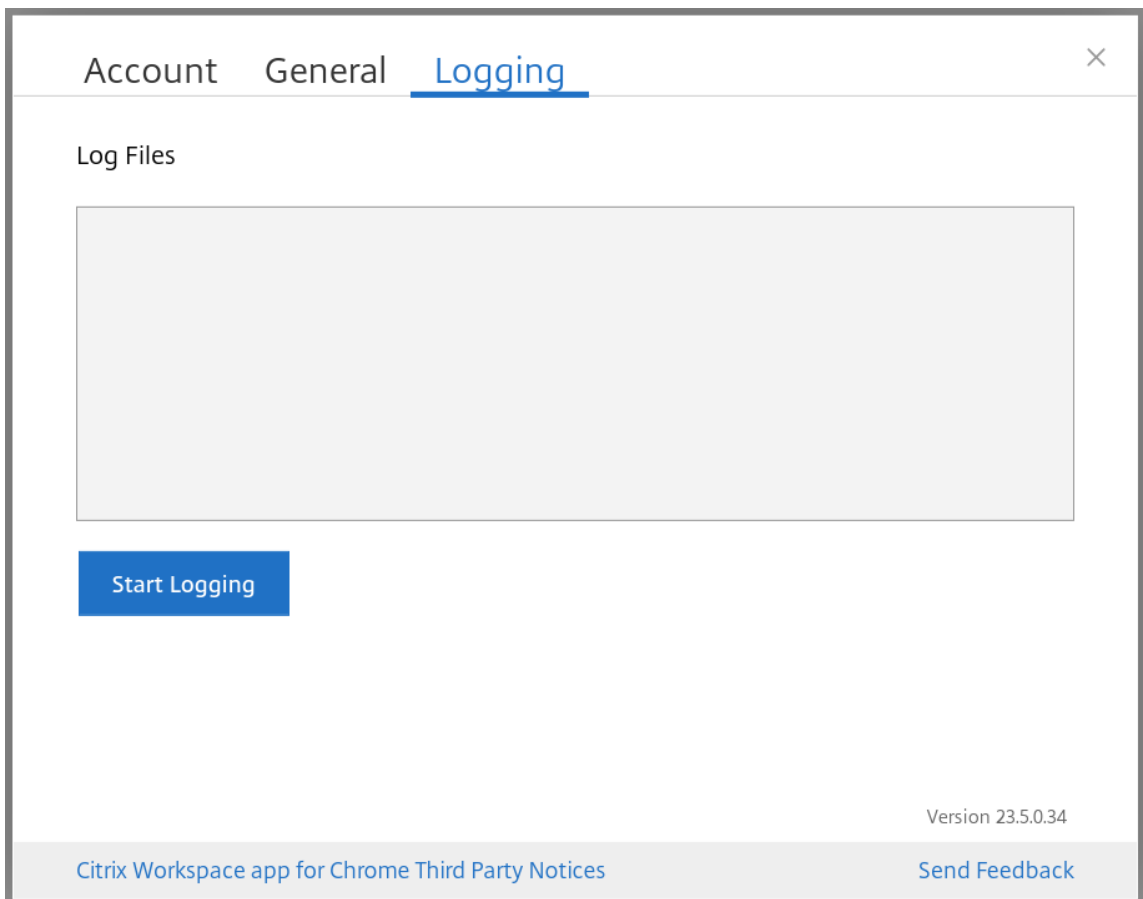
注:

- リリース 2207 以降、コンソールログはクライアントログの一部になります。

1. Citrix Workspace アプリのサインイン画面の右下にある設定ボタンをクリックします。



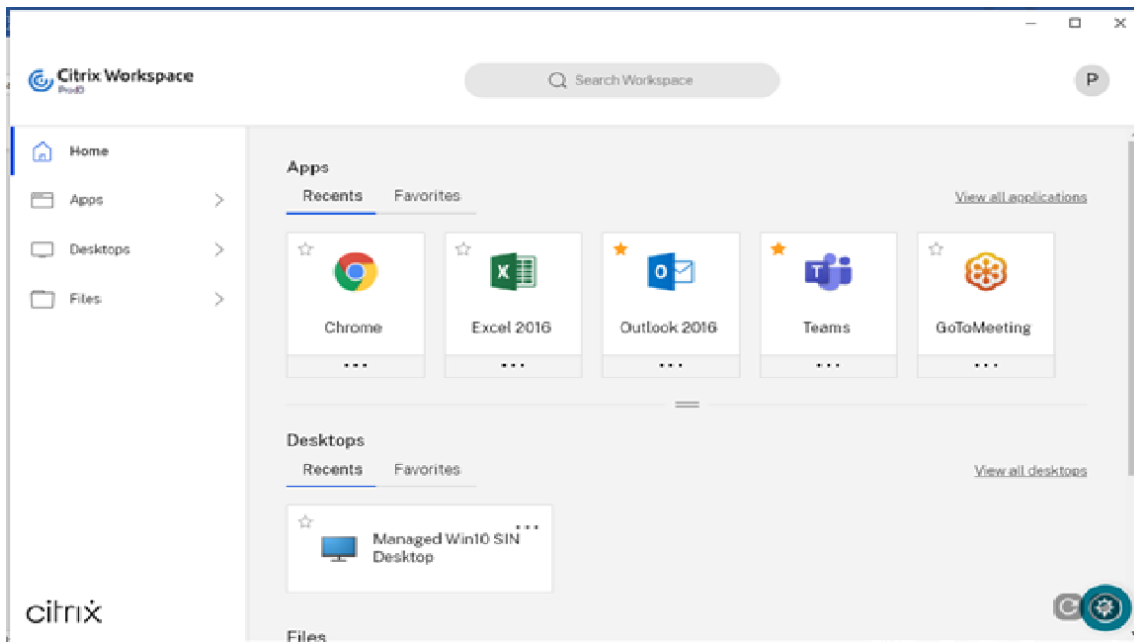
2. [ログ] の下の [ログの開始] ボタンをクリックして、ログの収集を有効にします。



3. [ログの開始] ボタンが [ログの停止] に変わります。この変更は、ログの収集が有効になっていることを示します。

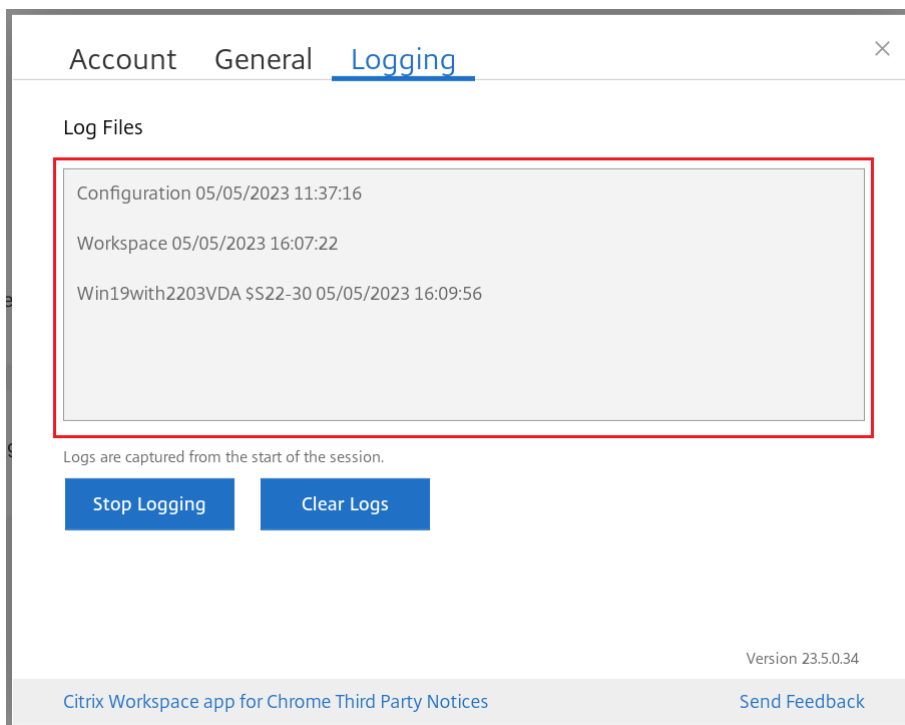
[アカウント] ダイアログボックスを閉じます。

4. Citrix Workspace アプリ仮想デスクトップにサインインして仮想アプリセッションを起動し、問題を再現してログを収集します。



問題を再現するために、セッションで作業を続けます。

5. 問題が再現されたら、セッションを閉じます。
6. 設定ボタンをもう一度クリックして、[アカウント] ダイアログボックスを開きます。
7. [ログ] タブをクリックします。
8. [ログ] ダイアログボックスには、キャプチャされたログファイルの一覧が表示されます。



9. ログファイルの上にマウスを移動すると、右側に小さな矢印が表示されます。



10. 矢印ボタンをクリックして、ログファイルをダウンロードして保存します。
11. [ログファイル] の下に一覧表示されているすべてのログファイルを保存し、管理者または Citrix サポートエンジニアと共有します。
12. [ログの停止] をクリックします。

注:

キオスクモードの場合、ファイルは USB リムーバブルデバイスに保存できます。

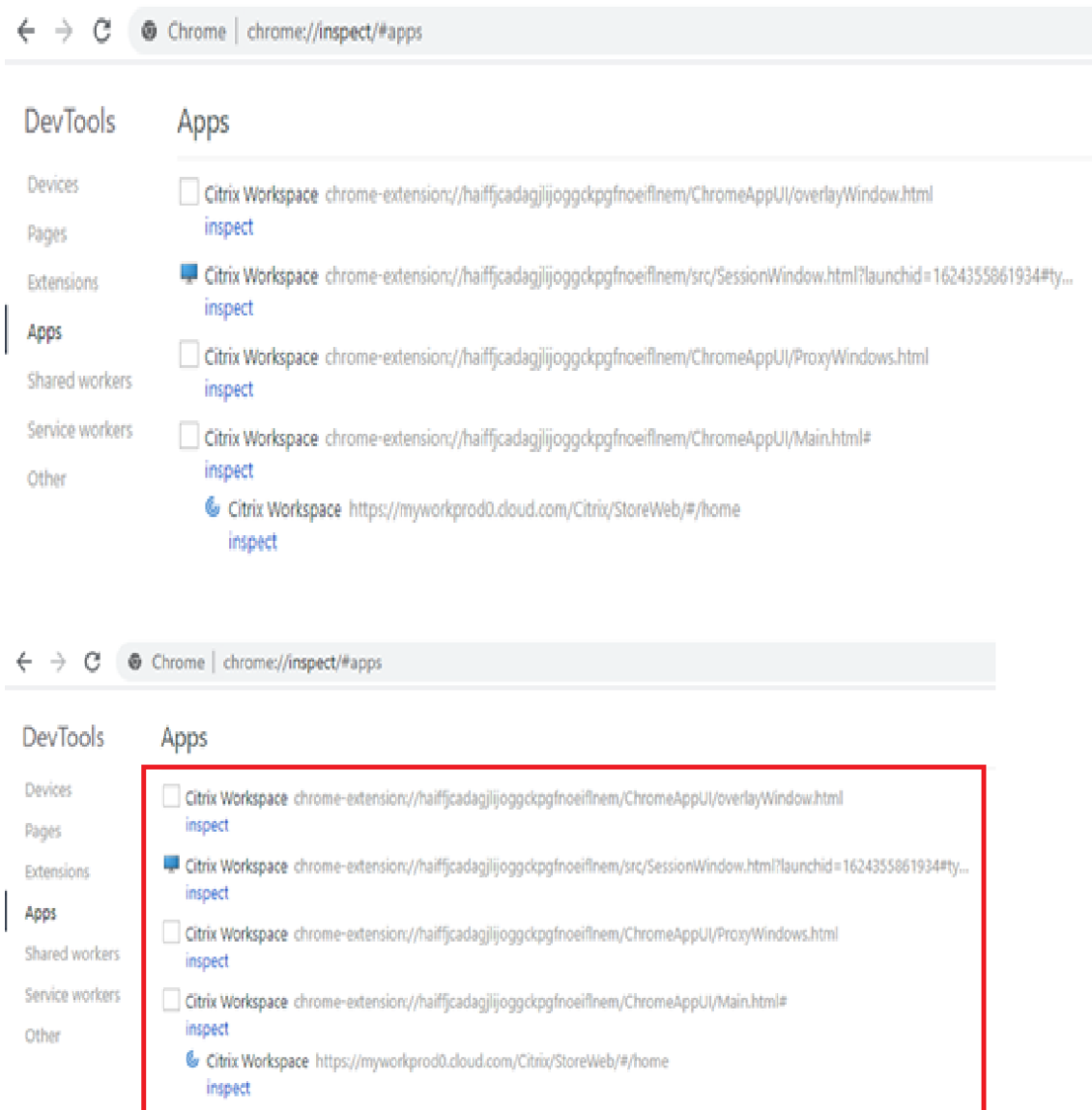
### コンソールログ

注:

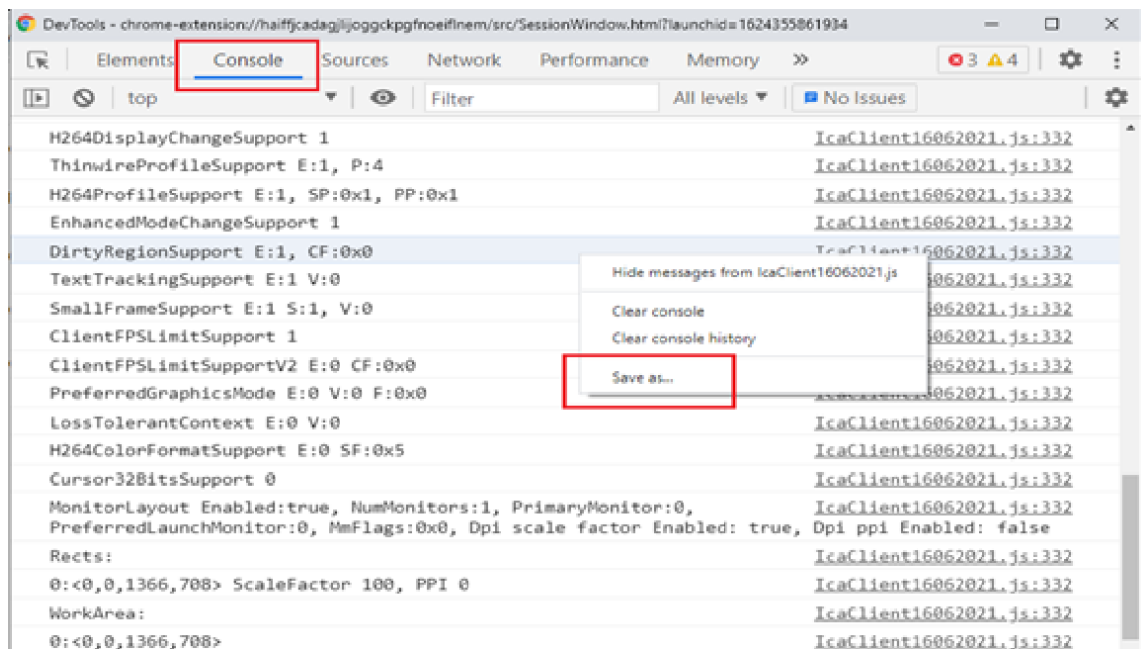
- バージョン 2207 以降、コンソールログはクライアントログの一部になります。したがって、クライアント

トログを収集するだけで十分です。

1. Citrix Workspace アプリの Google Chrome ブラウザーで **chrome://inspect/#apps** ページを開きます。
2. **[Apps]** タブで、Citrix Workspace 関連のすべてのウィンドウ (SessionWindow.html、Main.html、およびその子ノード) で **[inspect]** をクリックします。



3. 開かれた開発者ツールウィンドウごとに、**[Console]** をクリックします。次に、右クリックして **[Save as]** オプションを選択し、ログ全体を保存します。

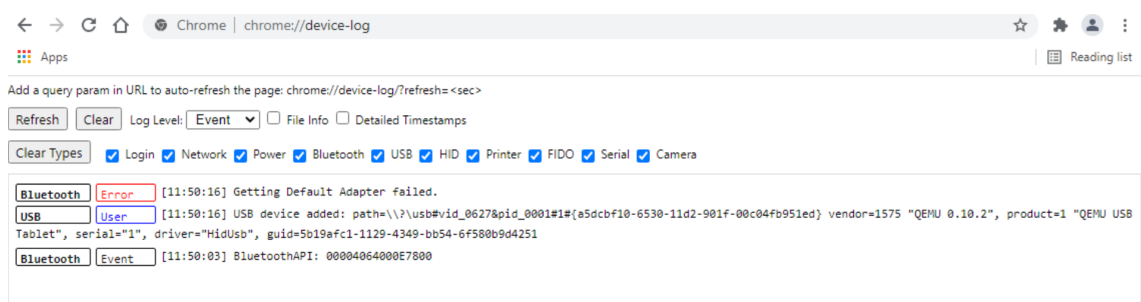


## USB リダイレクトログ

1. ChromeOS の「[Web.config の使用](#)」の手順に従い、次の方法で USB の moreLogs を有効にします:

StoreFront の web.config ファイルで chromeAppPreferences に moreLogs 構成値を追加します:  
`chromeAppPreferences = '{ "moreLogs":{ "usb":true } }'`

2. 次に、Google Chrome ブラウザーで新しいタブを開き、**chrome://device-log** を入力して ログを共有します。



## ファイル転送ログ

ファイル転送ログは、クライアントおよびサーバーの両方から取得できます。

クライアントからファイル転送ログを取得するには:

1. ブラウザーを起動します。

2. 次の URL でログ取得を開始します。

<storefronturl>/clients/html5client/src/viewlog.html

ここで、<storefronturl> は、ストアが構成された StoreFront サーバー FQDN または IP アドレスです。

詳しくは、[HTML5 および Chrome ファイル転送に関するブログ](#)を参照してください。

## Microsoft Teams の最適化ログ

Microsoft Teams の最適化は、最新の shim ライブラリバージョン 1.8.0.12 をサポートします。

使用している現在の shim バージョンを確認するには:

1. Microsoft Teams アプリケーションを起動し、ユーザーの 1 人との通話を開始します。
2. 通話が確立されたら、Microsoft Teams ウィンドウを最大化します。
3. セッション内の スクリーンキーボード を開き、**Ctrl + Alt + Shift + 1** キーをクリックします。  
これで、ダウンロードフォルダーにあるログファイルを表示できます。
4. `MSTeams Diagnostics Log <date><time>_vdi partner.txt` ファイルを開いて、**type\_script** で shim バージョンを検索します。  
shim バージョンが 1.8.0.12 かを確認します。
5. (オプション) shim のバージョンが 1.8.0.12 でない場合は、管理者に連絡して最新バージョンにアップグレードしてください。

## キオスクモードのクライアントログ

キオスクモードでログを収集するには:

1. リムーバブル USB デバイスを Chromebook に接続します。
2. ログファイルをダウンロードします。
3. 接続されている USB デバイスにログファイルを保存します。  
ログファイルが USB デバイスに転送されます。

## ショートカット

- キーボードのショートカット Ctrl+Alt+Shift+1 は、仮想デスクトップ内の最適化された Microsoft Teams では機能しない可能性があります。回避策として、スクリーンキーボードを開き、ショートカットを使用します。[RFHTMCRM-5441]



## 構成ユーティリティツール

May 16, 2024

ChromeOS 向け Citrix Workspace アプリをカスタマイズするには、4つのオプションがあります：

- configuration.js
- web.config
- default.ica
- Google ポリシー

4つのオプションは、UI ベースの構成 Web ページである構成ユーティリティで使用できます。

[ダウンロード](#) ページから構成ユーティリティツールをダウンロードします。

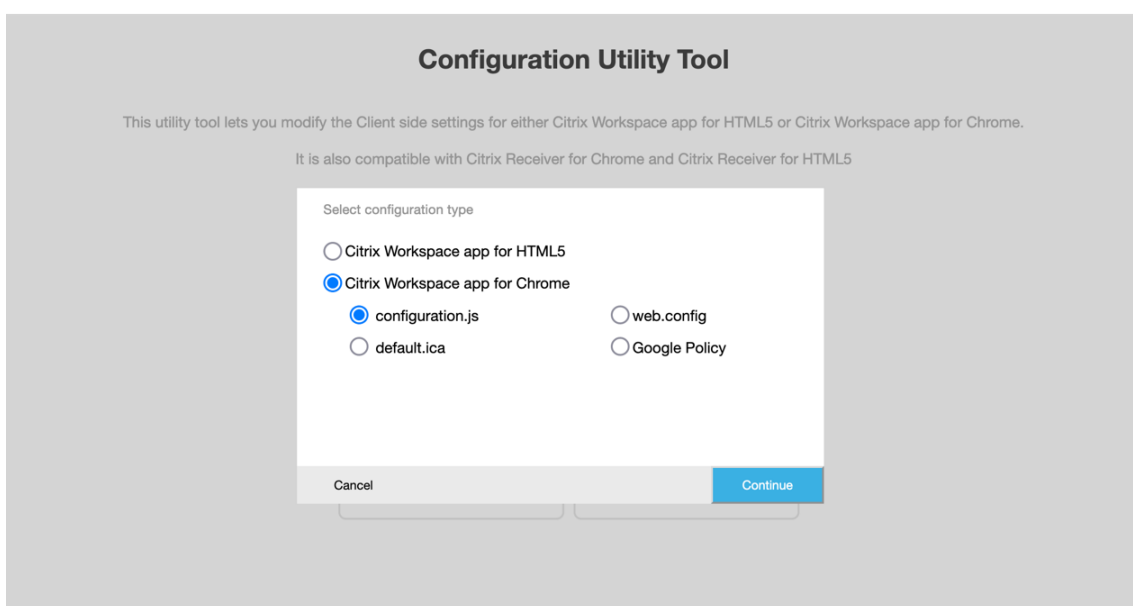
### 構成ユーティリティツールの使用方法

1. **[Creat New]** をクリックします。
2. **Chrome** 向け **Citrix Workspace** アプリを選択し、4つの構成オプションのいずれかを選択します。次に **[Continue]** をクリックして続行するか、**[Cancel]** をクリックしてホームページに戻ります。

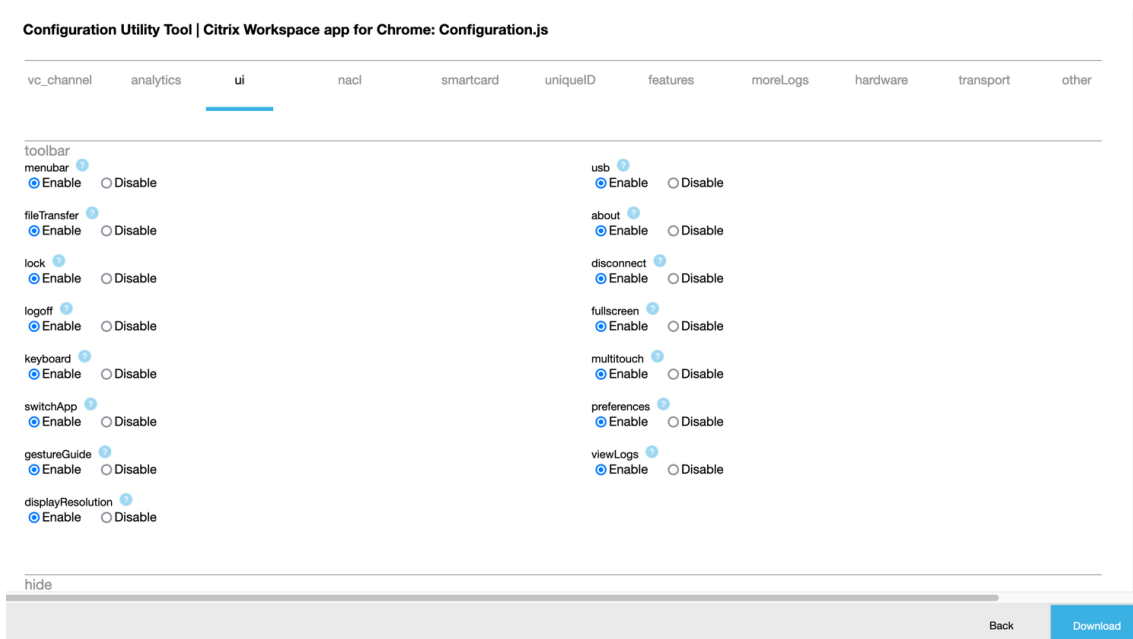
### configuration.js の場合

構成を作成するには、以下を実行します。

1. **configuration.js** を選択してから **[Continue]** をクリックして構成するか、**[Cancel]** をクリックしてホームページに戻ります。



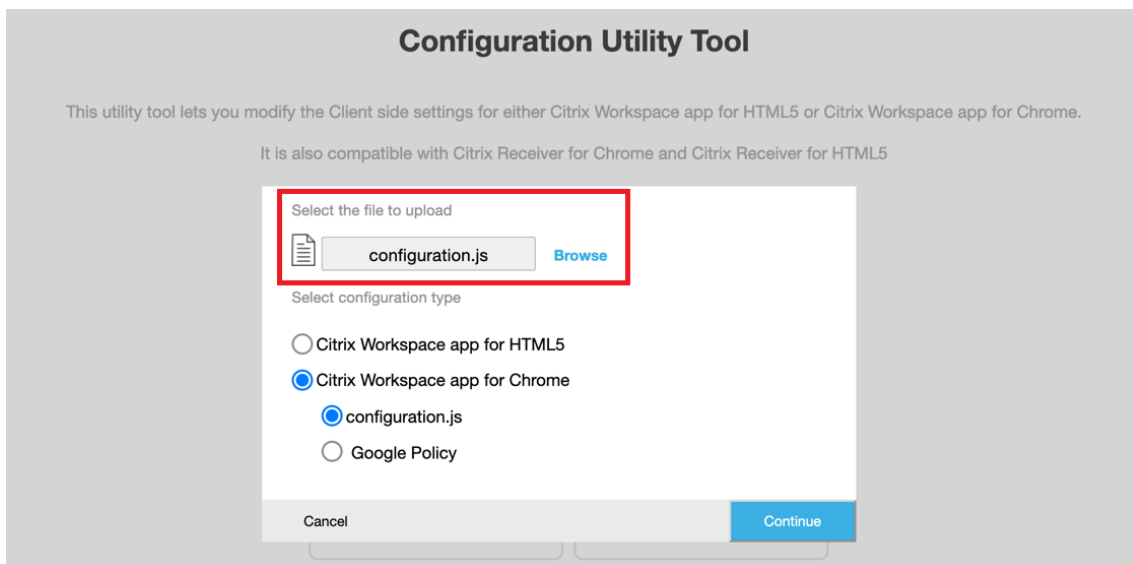
2. 構成ユーティリティツールで、目的の機能を選択し適切な値を設定します。



3. **[Download]** をクリックして configuration.js ファイルをダウンロードします。

構成を編集するには、以下を実行します。

1. **[Upload existing file]** をクリックします。
2. **Chrome** 向け **Citrix Workspace** アプリを選択し、**configuration.js** を選択します。
3. **[Browse]** をクリックし、configuration.js ファイルの場所に移動し、ファイルを選択してアップロードします。

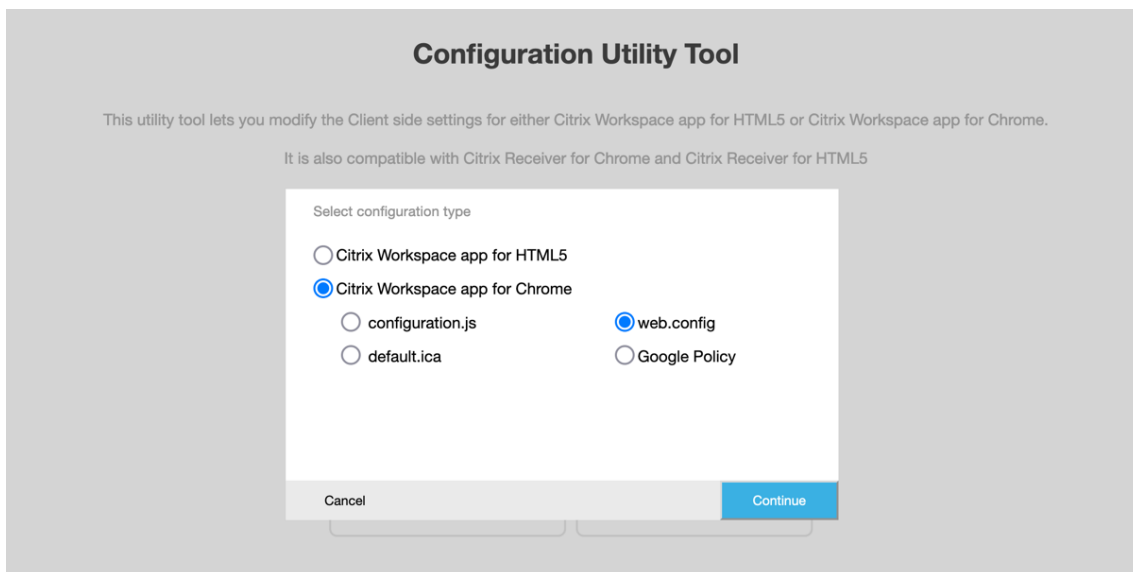


4. **[Continue]** をクリックして構成するか、**[Cancel]** をクリックしてホームページに戻ります。

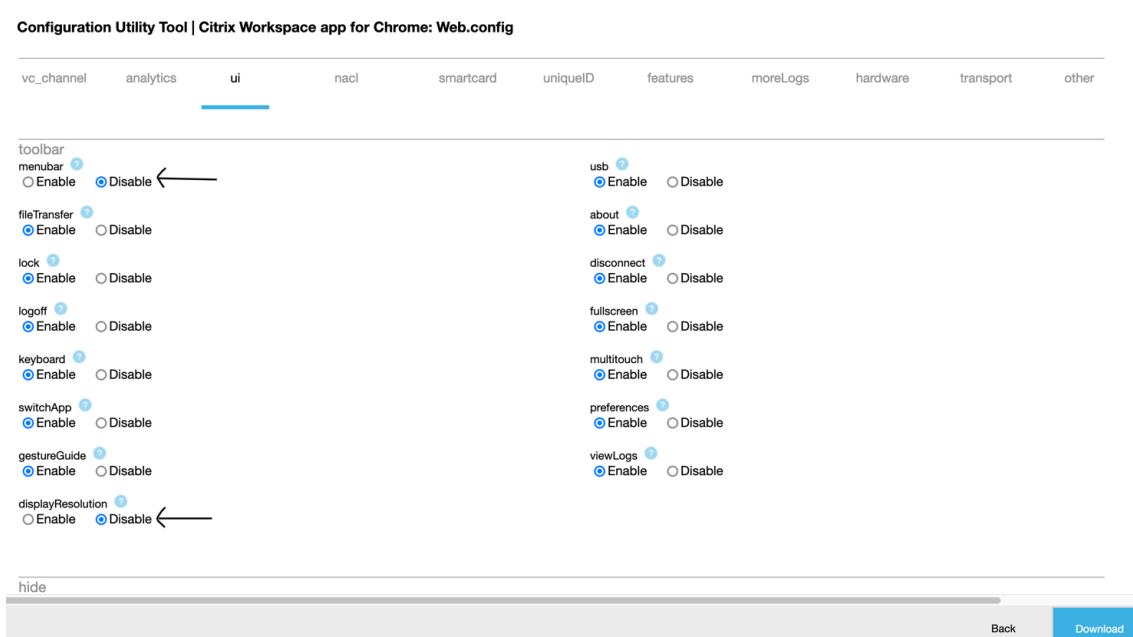
5. 目的の機能を選択し、適切な値を設定します。
6. **[Download]** をクリックして configuration.js ファイルをダウンロードします。

## web.config の場合 (StoreFront)

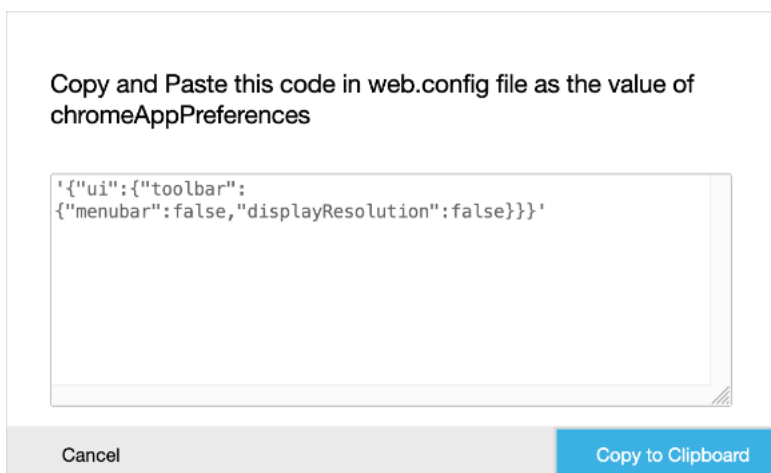
1. **web.config** を選択してから **[Continue]** をクリックして構成するか、**[Cancel]** をクリックしてホームページに戻ります。



2. 目的の機能と適切な値を選択し **[Download]** をクリックします (たとえば、menubar: disable、displayResolution: disable などを選択)



3. ダイアログボックスのコンテンツをコピーします。



4. Citrix Receiver for Web サイトの web.config ファイルを開きます。このファイルは通常、**C:\inetpub\wwwroot\Citrix\ストア名 Web** フォルダにあります。ここでストア名は、ストア作成時に指定したストアの名前です。
5. ファイル内の chromeAppPreferences フィールドを見つけ、ダイアログボックスからコピーした JSON 文字列を使用してその値を設定します。

```

1     chromeAppPreferences = '{
2
3         "ui":{
4
5             "toolbar":{
6
7                 "menubar":false,"displayResolution":false
8             }
9
10            }
11
12            }
13    '
14    <!--NeedCopy-->

```

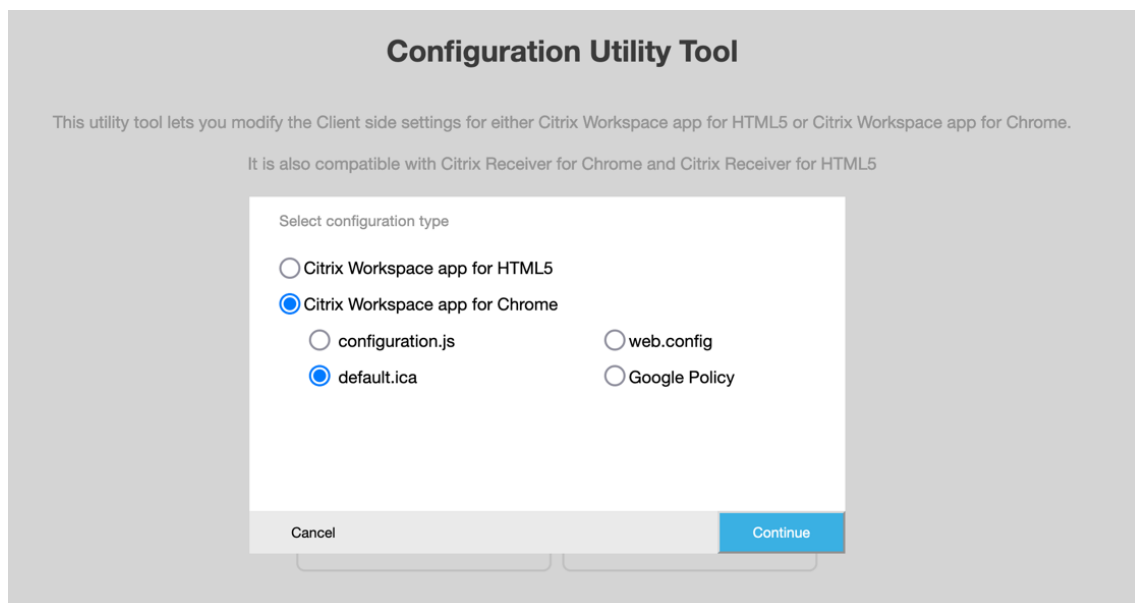
```

43 <csrfProtection excludedUserAgents="CitrixReceiver;CitrixWebAPI-NoCSRFToken" />
44 </serverSettings>
45 <clientSettings>
46 <authManager getUsernameURL="Authentication/GetUserName" logoffURL="Authentication/Logoff"
47   changeCredentialsURL="ExplicitAuth/GetChangeCredentialForm"
48   loginFormTimeout="5" webviewReturnURL="ExplicitAuth/Bounce"
49   webviewResumeURL="ExplicitAuth/ResumeForms" allowSelfServiceAccountManagementURL="ExplicitAuth
50 <storeProxy keepAliveURL="Home/KeepAlive">
51 <resourcesProxy listURL="Resources/List" resourceDetails="default" />
52 <sessionsProxy listAvailableURL="Sessions/ListAvailable" disconnectURL="Sessions/Disconnect"
53   logoffURL="Sessions/Logoff" />
54 <clientAssistantProxy getDetectionTicketURL="ClientAssistant/GetDetectionTicket"
55   getDetectionStatusURL="ClientAssistant/GetDetectionStatus" />
56 </storeProxy>
57 <pluginAssistant enabled="true" upgradeAtLogin="false" showAfterLogin="false">
58 <win32 path="http://downloadplugins.citrix.com/Windows/CitrixReceiverWeb.exe" />
59 <macOS path="http://downloadplugins.citrix.com/Mac/CitrixReceiverWeb.dmg"
60   minimumSupportedOSVersion="10.6" />
61 <html5 enabled="Fallback" platforms="Firefox;Chrome;Version/([6-9])\d\d).*Safari;MSIE \d\d;Tri
62   launchURL="clients/HTML5Client/src/SessionWindow.html" preferences=""
63   singleTabLaunch="false" chromeAppOrigins="chrome-extension://haiffjadagjlijoggkpgfnoeiflne
64   chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}' />
65 <protocolHandler enabled="true" platforms="(Macintosh|Windows NT).*((Firefox/[5[2-9]][6789][
66   skipDoubleHopCheckWhenDisabled="false" />
67 </pluginAssistant>

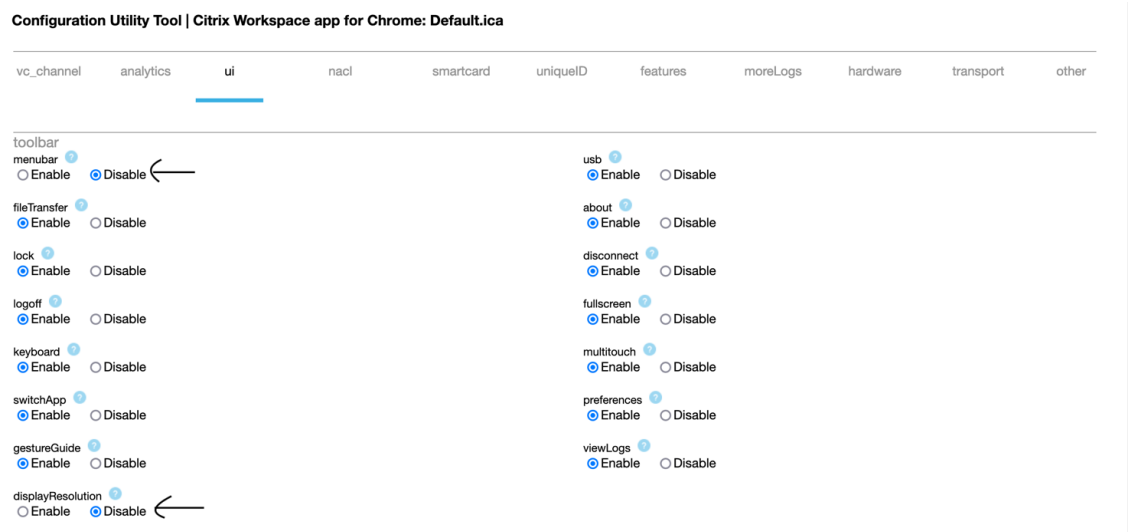
```

## default.ica の場合

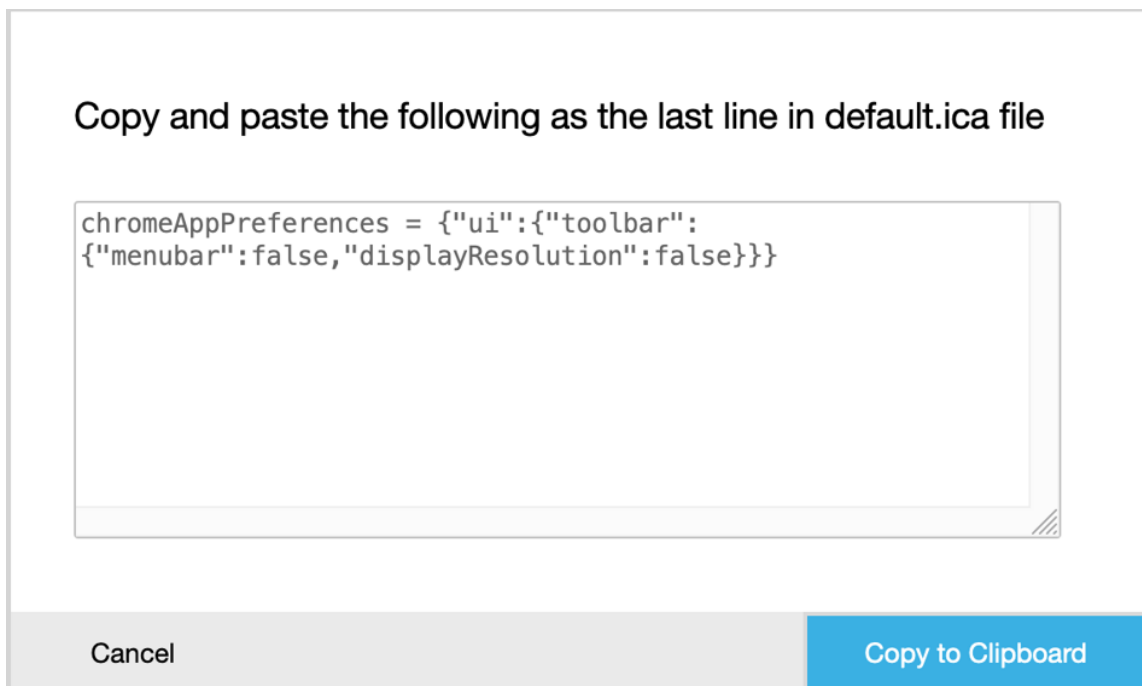
1. **default.ica** を選択してから **[Continue]** をクリックして構成するか、**[Cancel]** をクリックしてホームページに戻ります。



2. 目的の機能と適切な値を選択し **[Download]** をクリックします（たとえば、**menubar > disable** や **displayResolution > disable** などを選択）。



3. ダイアログボックスのコンテンツをコピーします。



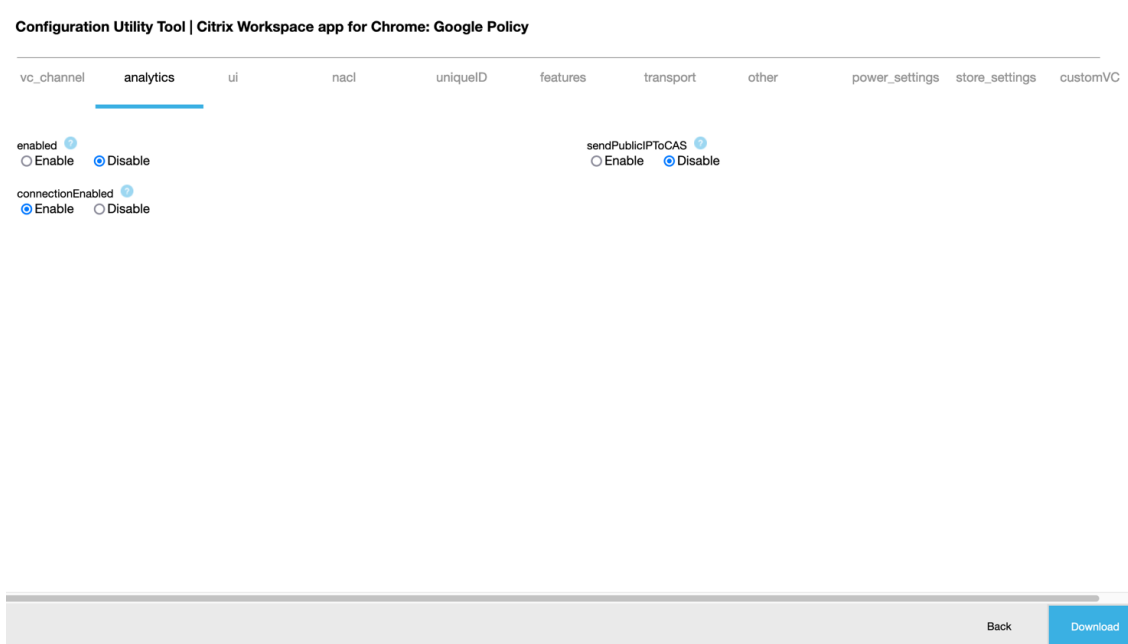
4. default.ica ファイルを開きます。Web インターフェイスの顧客の場合、このファイルは通常、**\*\*C:\inetpub\wwwroot\Citrix\<>サイト名>\conf\default.ica\*\*** ディレクトリにあります。ここで、<サイト名> はストアの作成時に指定した名前です。StoreFront ユーザーの場合、default.ica ファイルは、**\*\*C:\inetpub\wwwroot\Citrix\\>ストア名>\App\_Data\default.ica\*\*** にあります。ここで、<ストア名> はストアの作成時に指定した名前です。ストア名>ストア名>サイト名>サイト名>
5. 以下のように、default.ica ファイルの最後の行にコンテンツを追加します。

```
web.config x default.ica x
19
20 [Application]
21 TransportDriver=TCP/IP
22 DoNotUseDefaultCSL=On
23 BrowserProtocol=HTTPOnTCP
24 LocHttpBrowserAddress=!
25 WinStationDriver=ICA 3.0
26 ProxyTimeout=30000
27 AutologonAllowed=ON
28 TWIMode=Off
29 FontSmoothingType=0
30
31 [EncRC5-0]
32 DriverNameWin16=fdc0w.dll
33 DriverNameWin32=fdc0n.dll
34
35 [EncRC5-40]
36 DriverNameWin16=fdc40w.dll
37 DriverNameWin32=fdc40n.dll
38
39 [EncRC5-56]
40 DriverNameWin16=fdc56w.dll
41 DriverNameWin32=fdc56n.dll
42
43 [EncRC5-128]
44 DriverNameWin16=fdc128w.dll
45 DriverNameWin32=fdc128n.dll
46
47 [Compress]
48 DriverNameWin16=fdccompw.dll
49 DriverNameWin32=fdccompn.dll
50
51 chromeAppPreferences = '{"ui":{"toolbar":{"menubar":false,"displayResolution":false}}}'
```

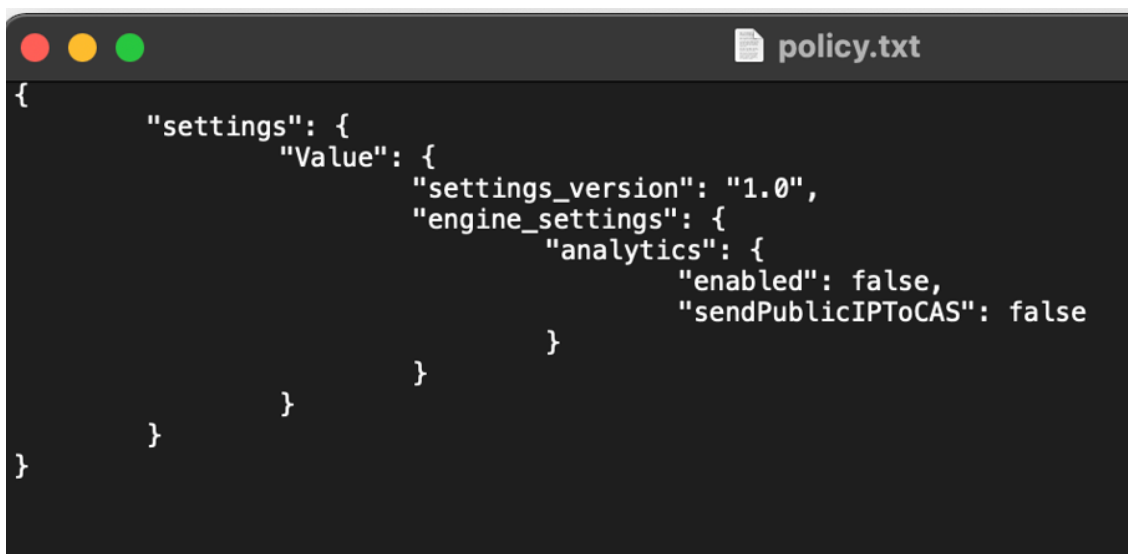
## Google ポリシーの場合

構成を作成する方法

1. **Google** ポリシーを選択してから **[Continue]** をクリックして構成するか、**[Cancel]** をクリックしてホームページに戻ります。
2. 目的の機能と適切な値を選択し、**[Download]** をクリックします（たとえば、sendPublicIPToCas: disabled を選択します）



3. [Download] をクリックすると、**policy.txt** ファイルが作成されます。



## 構成を編集する方法

機能の制限事項:

編集できるのは、アップロードファイル (**policy.txt**) にある設定と値のみです。他のポリシーを編集する必要がある場合は、ポリシーファイルを作成して設定を含めます。詳しくは、「[構成を作成する方法](#)」を参照してください。

1. [Upload existing file] をクリックします。
2. **Chrome** 向け **Citrix Workspace** アプリを選択し、**policy.txt** を選択します。



Select the file to upload

[Browse](#)

Select configuration type

Citrix Workspace app for HTML5

Citrix Workspace app for Chrome

configuration.js

Google Policy

[Cancel](#) [Continue](#)

3. [**Browse**] をクリックし、**policy.txt** ファイルの場所に移動し、ファイルを選択してアップロードします。
4. [**Continue**] をクリックして編集するか、[**Cancel**] をクリックしてホームページに戻ります。
5. 適切な値を選択して設定を編集します。
6. [**Download**] をクリックして、更新された **policy.txt** ファイルをダウンロードします。

## 認証

June 18, 2024

### スマートカード

ChromeOS 向け Citrix Workspace アプリは、StoreFront で USB スマートカードリーダーをサポートしています。スマートカードは、以下の目的で利用できます：

- Citrix Workspace アプリへのスマートカードによるサインイン認証。
- スマートカード対応の公開アプリを使った、ローカルのスマートカードリーダーへのアクセス。
- 文書や電子メールに署名するためのスマートカード。たとえば、ICA セッションで起動される Microsoft Word と Outlook。

サポートされているスマートカード（USB スマートカードリーダー付き）には、次のものがあります：

- Personal Identity Verification (PIV)
- Common Access Card (CAC)

### 前提条件

- StoreFront バージョン 3.6 以降
- XenDesktop 7.6 以降
- XenApp 6.5 以降
- Citrix Virtual Apps and Desktops 1808 以降
- Citrix Workspace アプリ 1808 以降

#### 重要:

- StoreFront 3.5 以前でのスマートカード認証でスマートカード認証を有効にするには、カスタムスクリプトが必要です。[Citrix サポート](#)に連絡してください。
- サポートされているバージョンの最新情報にアクセスするには、[Citrix Workspace アプリ](#)および[Citrix Virtual Apps and Desktops](#)のライフサイクルマイルストーンを参照してください。

### デバイス構成の前提条件

- Google Smart Card Connector は、デバイスの USB スマートカードリーダーと通信する[アプリ](#)です。コネクタアプリは、Personal Computer Smart Card (PCSC) Lite API を Citrix Workspace アプリを含む他のアプリに公開します。
- 証明書プロバイダーは、ベンダーによって作成された Smart Card Connector と通信するミドルウェアアプリです。ミドルウェアアプリは、スマートカードリーダーにアクセスし、証明書を読み取り、ChromeOS にスマートカード証明書を提供します。

ミドルウェアアプリは、PIN の入力を使用した署名機能も実装しています。  
たとえば、CACKey です。

詳しくは、「[ChromeOS でスマートカードを利用する](#)」を参照してください。

- StoreFront でスマートカード認証を構成すると、Citrix Workspace アプリは ChromeOS にスマートカードでのクライアント証明書を提供するように要求します。ChromeOS は、プロバイダーから受け取った証明書を提示します。PIN の入力画面は認証を示します。

Citrix Workspace アプリには、スマートカード認証で許可されているオペレーティングシステムの承認済み一覧があります。StoreFront 3.6 以降では、ChromeOS も承認されています。StoreFront の以前のバージョンでは、カスタムスクリプトを使用した ChromeOS でのスマートカード認証を許可できます。カスタムスクリプトについては、Citrix サポートにお問い合わせください。

- StoreFront を使用したスマートカード認証ワークフローは、Citrix Workspace アプリでは制御していません。ただし、場合によっては、StoreFront がブラウザを閉じて Cookie を消去するように要求することがあります。

すべての Cookie を消去し、ストア URL を再度読み込むには、ChromeOS 向け Citrix Workspace アプリで再読み込みボタンをクリックします。

また、ChromeOS デバイスからサインアウトすることで、Cookie をさらに消去することができます。

- アプリセッションまたはデスクトップセッションを起動しようとする場合、Citrix Workspace アプリはスマートカードリダイレクトを使用しません。代わりに、PC/SC Lite API のスマートカードコネクタアプリと通信します。

Windows サインインに必要な PIN 入力画面はセッション内に表示されます。ここでは、証明書プロバイダーに出番はありません。Citrix Workspace アプリは、ダブルポップやメールへの署名などのセッション中のアクティビティを管理します。

### スマートカードの制限事項

- スマートカードを ChromeOS デバイスから削除すると、スマートカード証明書はキャッシュされます。この動作は Google Chrome での既知の問題です。ChromeOS デバイスを再起動してキャッシュをクリアします。
- ChromeOS 向け Citrix Workspace アプリが再パッケージ化された場合、管理者は Google から appId の承認を受けてください。そうすることで、スマートカードコネクタアプリケーションがパススルーできることを確認します。
- 同時にサポートできるスマートカードリーダーは 1 つのみです。
- 仮想スマートカードと高速スマートカードはサポートされていません。
- スマートカードは Citrix Workspace (クラウド) ではサポートされていません。

### ChromeOS デバイス上でスマートカードのサポートを構成するには

1. スマートカードコネクタアプリケーションをインストールします。ChromeOS デバイスで Personal Computer Smart Card (PCSC) をサポートするには、スマートカードアプリケーションが必要です。このアプリケーションは、USB インターフェイスを使用して、スマートカードを読み取ります。このアプリケーションは、[Chrome の Web サイト](#)からインストールできます。
2. ミドルウェアアプリケーションをインストールします。ミドルウェアアプリケーションは、スマートカードや他のクライアント証明書と通信するインターフェイスとして必要です。たとえば、Charismathics または CACKey などです：
  - Charismathics スマートカード拡張機能または CACKey をインストールするには、[Chrome の Web サイト](#)を参照してください。
  - ミドルウェアアプリケーションおよびスマートカード認証について詳しくは、[Google サポートサイト](#)を参照してください。
3. 以下を使用したスマートカード認証の構成：
  - Citrix Gateway
  - StoreFront 管理コンソール

詳しくは、Citrix Gateway ドキュメントの「[スマートカード認証の構成](#)」および「[認証サービスの構成](#)」を参照してください。

## SAML 認証

シングルサインオンを構成するには:

1. SAML 認証の ID プロバイダー (IdP) が既に設定されていない場合、サードパーティの IdP をセットアップします。たとえば、ADFS 2.0 などです。

詳しくは、Knowledge Center の[CTX133919](#)を参照してください。

2. SAML ID プロバイダーを使用して Google Apps でシングルサインオンをセットアップします。これによって、Google Enterprise アカウントの代わりに Google Apps を使用して、サードパーティの ID を適用できるようになります。

詳しくは、Google サポートの[サードパーティの ID プロバイダーを使用した管理対象 Google アカウントへのシングルサインオンの設定](#)を参照してください。

3. SAML ID プロバイダー経由でサインインするように Chrome デバイスを構成します。これによって、ユーザーはサードパーティの ID プロバイダーを使用して Chrome デバイ스에サインインできます。

詳しくは、Google サポートの[Chrome 搭載デバイスに SAML シングルサインオンを設定する](#)を参照してください。

4. SAML ID プロバイダー経由でサインインするように Citrix Gateway を構成します。これによって、ユーザーはサードパーティの ID プロバイダーを使用して Citrix Gateway にサインインできます。

詳しくは、「[SAML 認証の構成](#)」を参照してください。

5. Citrix Virtual Apps and Desktops でフェデレーション認証を構成して、動的に生成された証明書で Citrix Virtual Apps and Desktops にサインインします。ユーザー名とパスワードの組み合わせでサインインせずに、SAML サインインプロセス後に実行できます。

詳しくは、「[フェデレーション認証サービス](#)」を参照してください。

仮想アプリと仮想デスクトップへの SSO を可能にするために、フェデレーション認証サービス (FAS) を展開する必要があります。

注:

FAS がない場合は、Active Directory のユーザー名とパスワードの入力を求められます。詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

6. Chrome デバイス上で、Chrome アプリの SAML SSO 拡張機能をインストールして構成します。詳しくは、Google の Web サイトを参照してください。この拡張機能は、SAML Cookie をブラウザから取得して、

Citrix Workspace に提供します。Citrix Workspace が SAML Cookie を取得できるようにするには、次のポリシーを構成する必要があります。

ChromeOS 向け Citrix Workspace アプリを再パッケージする場合、appId を正しく変更する必要があります。また、ドメインを組織の SAML IdP ドメインに変更する必要があります。

```
1 {
2
3     "whitelist" : {
4
5         "Value" : [
6             {
7
8                 "appId" : "haiffjcadagjlijoggckpgfnoeiflnem",
9                 "domain" : "saml.yourcompany.com"
10            }
11        ]
12    }
13 }
14
15 }
16
17 <!--NeedCopy-->
```

7. SAML サインイン用に構成された Citrix Gateway を使用するように、Citrix Workspace を構成します。これによって、SAML サインイン用に構成された Citrix Gateway を使用できるようになります。ChromeOS の構成について詳しくは、Knowledge Center の [CTX141844](#) を参照してください。

## ID プロバイダーとして **Okta** を使用した **Citrix Workspace** アプリのシングルサインオン

May 16, 2024

Okta を ID プロバイダー (ID プロバイダー) として使用して、Citrix Workspace アプリへのシングルサインオン (SSO) を構成できます。

### 前提条件

次の前提条件には管理者特権が必要です：

- Citrix Cloud
- Cloud Connector

注:

Citrix Cloud を初めて使用する場合は、リソースの場所を定義し、コネクタを構成します。実稼働環境には、少なくとも 2 つのクラウドコネクタを展開することをお勧めします。Citrix Cloud Connector のインストール方法については、「[Cloud Connector のインストール](#)」を参照してください。

- Citrix Workspace アプリ
- フェデレーション認証サービス (オプション)。詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。
- Citrix DaaS (旧称: Citrix Virtual Apps and Desktops サービス)
- AD ドメイン参加済み VDA、または物理 AD 参加済みデバイス
- Okta テナント
- Okta 統合 Windows 認証 (IWA) エージェント
- Okta Verify (Okta Verify はアプリストアからダウンロードできます) (オプション)
- Active Directory (AD)

### SSO の構成方法

Okta を ID プロバイダーとして使用して Citrix Workspace アプリの SSO を構成する手順は次のとおりです:

1. [Okta AD エージェントのインストール](#)
2. [Okta OIDC Web アプリケーション統合の作成](#)
3. [Okta OIDC Web アプリケーションの構成](#)
4. [Okta API トークンの作成](#)
5. [Citrix Cloud を Okta 組織に接続](#)
6. [ワークスペースの Okta 認証を有効にする](#)
7. [Okta 多要素認証 \(MFA\) バイパスの構成](#)
8. [Okta IWA エージェントのセットアップ](#)
9. [ID プロバイダーのルーティング規則の構成](#)
10. [Google 管理コンソールでの Okta ID プロバイダーの構成](#)
11. [SAML SSO Chrome 拡張機能を使用した ChromeOS 向け Citrix Workspace アプリの SSO の構成](#)

### Okta AD エージェントのインストール

前提条件:

エージェントをインストールする前に、「[Active Directory integration prerequisites](#)」リンクに記載されている前提条件が満たされていることを確認してください。

Okta AD エージェントをインストールするには:

1. Okta 管理ポータルで、**[Directory]** > **[Directory Integrations]** をクリックします。
2. **[Add Directory]** > **[Add Active Directory]** をクリックします。
3. Agent Architecture および Installation Requirements を含むワークフローに従い、インストール要件を確認します。
4. **[Set Up Active Directory]** ボタンをクリックしてから、**[Download Agent]** をクリックします。
5. 「[Install the Okta AD agent](#)」に記載されている手順に従って、Okta AD Agent を Windows Server にインストールします。

### Okta OIDC Web アプリケーション統合の作成

Okta を ID プロバイダーとして使用するには、ユーザーの資格情報を Citrix Cloud で使用できるように、Okta **OIDC - OpenID Connect Web** アプリケーションを作成する必要があります。このアプリは、サインインシーケンスを開始し、サインアウトした場合の Citrix Workspace URL へのリダイレクトも処理します。

詳しくは、「[Okta OIDC Web アプリケーション統合の作成](#)」を参照してください。

### Okta OIDC Web アプリケーションの構成

Okta OIDC アプリを作成したら、Citrix Cloud に必要な設定で構成します。これらの設定は、利用者が Okta を使用して Citrix Workspace にサインインするときの認証のために必要です。

詳しくは、「[Okta OIDC Web アプリケーションの構成](#)」リンクを参照してください。

### Okta API トークンの作成

Okta API トークンの作成方法について詳しくは、「[Okta API トークンの作成](#)」を参照してください。

### Citrix Cloud を Okta 組織に接続

Citrix Cloud に接続する方法について詳しくは、「[Citrix Cloud を Okta 組織に接続](#)」を参照してください。

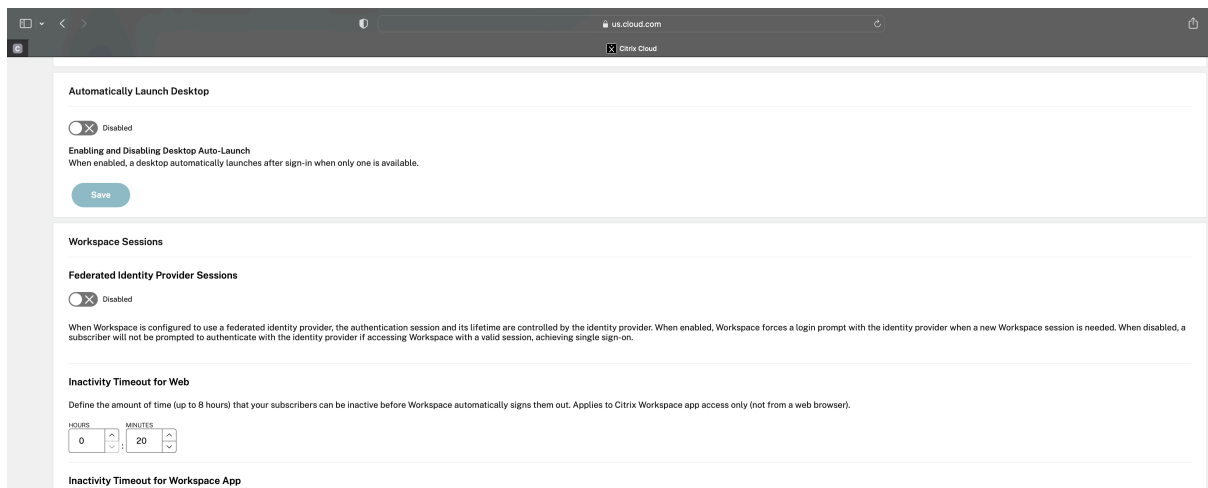
### ワークスペースの Okta 認証を有効にする

Okta 認証を有効にする方法について詳しくは、「[ワークスペースの Okta 認証を有効にする](#)」を参照してください。

### Okta 多要素認証 (MFA) バイパスの構成

ネットワークゾーンを作成して、環境にアクセスするために許可リストに登録する必要がある一連の IP アドレスを定義します。詳しくは、「[Create zones for IP addresses](#)」を参照してください。

[フェデレーション ID プロバイダーセッション] オプションを必ず無効にしてください。[ワークスペースの構成] > [カスタマイズ] > [環境設定] で Cloud コンソールに移動し、[フェデレーション ID プロバイダーセッション] を無効にします。



### Okta IWA エージェントのセットアップ

Okta IWA エージェントは、Okta サービスでデスクトップシングルサインオン (DSSO) を有効にする軽量のインターネットインフォメーションサービス (IIS) Web エージェントです。

DSSO は、ドメイン参加のコンピューターが Citrix Cloud にアクセスしている場合に使用されます。このドメイン参加のコンピューターでは、認証のプロンプトは必要ありません。

1. 次の前提条件の一覧が満たされていることを確認してください。

Okta IWA Web エージェントをインストールするための前提条件の一覧については、「[Okta IWA Web agent installation prerequisites](#)」を参照してください。

2. Okta IWA エージェントをインストールします。

Okta IWA Web エージェントをインストールするには、「[Install the Okta IWA Web agent](#)」を参照してください。

3. Windows ブラウザーを SSO 用に構成します。

Windows ブラウザーを SSO 用に構成するには、「[Configure Windows browsers for SSO](#)」を参照してください。

4. Okta IWA Web エージェントをテストします。

Okta IWA Web エージェントをダウンロードしてインストールした後、IWA サーバーがクライアントマシンから動作しているかどうかを確認します。

Okta エージェントが正しく構成されている場合は、**UserPrincipalName** と **SecurityIdentifier** に関連する詳細が表示されます。



確認方法について詳しくは、「[Test the Okta IWA Web agent](#)」を参照してください。

#### ID プロバイダーのルーティング規則の構成

ID プロバイダーのルーティング規則を構成するには、「[ID プロバイダーのルーティング規則の構成](#)」を参照してください。

注:

[ID プロバイダー] フィールドで、必ず [OnPremDSSO] を選択してください。

#### Google 管理コンソールでの Okta ID プロバイダーの構成

1. セキュリティアサッションマークアップランゲージ (SAML) アプリケーションを作成するには、「[Create SAML app integrations](#)」を参照してください。

[**Single sign-on URL**] フィールドと [**Audience URI (SP Entity ID)**] フィールドに必ず URL を入力してください。例: <https://admin.google.com>。

注:

Google 管理コンソールで SAML プロファイルを作成した後、サンプル URL の変更が必要になる場合があります。詳細については、次の手順を参照してください。

2. Google 管理コンソールでサードパーティの ID プロバイダーを使用して SAML を構成します。  
組織の SSO プロファイルを作成してユーザーを割り当てるには、「[Create a SAML SSO profile](#)」に記載されている手順に従います。  
SAML プロファイルの Okta サインイン、サインアウト、発行者、およびその他の ID プロバイダー情報を取得するには、「[SAML ID プロバイダーの追加](#)」に記載されている手順に従います。
3. SAML プロファイルを構成するには、「[How to Configure SAML 2.0 for Google Workspace link](#)」をご覧ください。
4. Google SAML プロファイルの詳細を使用して OKTA で SAML プロファイルを構成し、プロファイルを同期します:
  - a) [セキュリティ] > [認証] > [組織向けのサードパーティの **SSO** プロファイル] > [サードパーティの **SSO** プロファイル] に移動して、SAML プロファイルを開きます。
  - b) Okta ダッシュボードページ (ID プロバイダー) で、Google (サービスプロバイダー) SAML プロファイルの詳細を追加します。
    - [シングルサインオン URL] > [**ACS URL**] に移動し、[これを宛先 URL およびターゲット URL に使用する] オプションを選択します。

- **[Audience URI (SP Entity ID)]** > **[Entity ID]** に移動します。

ID プロバイダーと SP (サービスプロバイダー) SAML プロファイルが同期されると、管理対象ユーザーのサインインページが Chromebook の Okta サインインページに表示されます。

#### 5. OKTA SAML アプリケーションにユーザーを割り当てます。

ユーザーを割り当てる方法について詳しくは、「[Assign an app integration to a user](#)」を参照してください。

#### 検証チェックポイント

- ユーザーが Chromebook でエンタープライズ Google アカウントを追加すると、Okta 資格情報を使用してサインインできるようになります。
- Chromebook にサインインした後、ユーザーは Google Chrome ブラウザーを開いて Citrix Workspace URL を入力できる必要があります。
- ユーザーは Citrix Workspace アプリの UI を表示できる必要があります。ユーザーは、資格情報を要求されずに仮想アプリとデスクトップに移動できる必要があります。

#### 注:

SSO が失敗した場合は、「[Google 管理コンソールでの Okta ID プロバイダーの構成](#)」の手順を修正してください。

### SAML SSO Chrome 拡張機能を使用した ChromeOS 向け Citrix Workspace アプリの SSO の構成

SAML 拡張機能を使用して SSO を構成するには、次の手順を実行します:

1. Chrome デバイス上で、Chrome アプリの SAML SSO 拡張機能をインストールして構成します。  
拡張機能をインストールするには、[SAML SSO for Chrome Apps](#)をクリックします。
2. この拡張機能は、SAML Cookie をブラウザから取得して、ChromeOS 向け Citrix Workspace に提供します。
3. Citrix Workspace が SAML Cookie を取得できるようにするには、次のポリシーを構成します。ドメインを会社の Okta ID プロバイダードメインに置き換えます。

```
1 {
2
3     "whitelist" : {
4
5         "Value" : [
6             {
7
8                 "appId" : "haiffjcadagjlijoggckpgfnoeiflnem",
```

```
9         "domain" : "<domain.okta.com>"
10         }
11     ]
12     }
13 }
14
15 }
16
17 <!--NeedCopy-->
```

注:

ChromeOS 向け Citrix Workspace アプリを再パッケージする場合は、[haiffjcadagjlijoggckpgfnoeifl](#) を再パッケージされた AppID に置き換えます。

#### 4. FAS を展開して、仮想アプリとデスクトップへの SSO を実現します。

仮想アプリと仮想デスクトップへの SSO を可能にするには、フェデレーション認証サービス (FAS) を展開するか、Citrix Workspace アプリを構成します。

注:

- FAS がない場合は、Active Directory のユーザー名とパスワードの入力を求められます。詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

## ID プロバイダーとして **Microsoft Azure** を使用した **Citrix Workspace** アプリのシングルサインオン

May 16, 2024

ChromeOS デバイスの Security Assertion Markup Language (SAML) シングルサインオン (SSO) を構成できます。Microsoft Entra ID (旧称 Azure Active Directory) を SAML ID プロバイダーとして使用し、Google Admin をサービスプロバイダー (SP) として使用します。

この機能は、管理対象ユーザーに対してのみ設定できます。ユースケースとして、Azure 上に作成されたローカル Active Directory (AD) に Citrix VM を追加しました。Azure 上にオンプレミスの AD ベースの VM があり、Microsoft Entra ID ユーザーがいる場合は、この記事の説明に従ってください。

### 前提条件

次の前提条件には管理者特権が必要です:

- Active Directory (AD)

環境でアクティブなドメインコントローラーをインストールして構成します。詳しくは、「[サーバーマネージャーを使用して AD DS をインストールする](#)」を参照してください。サーバーマネージャーを使用して Active Directory ドメインサービスをインストールするには、[手順 1~19](#)を実行します。

- 証明機関 (CA)

CA をインストールします。詳しくは、「[証明機関をインストールします](#)」を参照してください。

証明機関は、次のいずれかのマシンにインストールして構成できます：

- 新しい専用マシン
- 既存の CA マシン
- Citrix Cloud Connector へのこの証明機関コンポーネントのインストール
- Active Directory マシン

- Citrix Cloud および Citrix Cloud Connector

Citrix Cloud を初めて使用する場合は、リソースの場所を定義し、コネクタを構成します。実稼働環境には、少なくとも 2 つの Cloud Connector を展開することをお勧めします。Citrix Cloud Connector のインストール方法については、「[Cloud Connector のインストール](#)」を参照してください。

- Azure Portal のグローバル管理者アカウント

Microsoft Entra ID のグローバル管理者である必要があります。この権限は、Entra ID を ID プロバイダーとして使用するよう Citrix Cloud を構成するのに役立ちます。接続して Entra ID を使用するとき Citrix Cloud が要求する権限について詳しくは、「[Citrix Cloud 用の Azure Active Directory の権限](#)」を参照してください。

- フェデレーション認証サービス (オプション)。

詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

- Google 管理コンソールのグローバル管理者アカウント

- Citrix Workspace アプリ

### 開始

開始するには、次の手順を実行します：

- インストールされているソフトウェアまたは役割を構成する前に、すべてのマシンをドメインに参加させます。
- それぞれのマシンに Citrix Cloud Connector ソフトウェアをインストールしますが、まだ何も設定しないでください。
- それぞれのマシンに Citrix FAS をインストールしますが、まだ何も構成しないでください。

## Azure AD を ID プロバイダーとして使用するように Citrix Cloud を構成する方法

注:

すべての前提条件を満たしていることを確認してください。

1. Entra ID を Citrix Cloud に接続するには、「[Azure Active Directory を Citrix Cloud に接続する](#)」を参照してください。
2. 管理者を Entra ID から Citrix Cloud に追加するには、「[Azure AD から Citrix Cloud に管理者を追加する](#)」を参照してください。
3. Entra ID を使用して Citrix Cloud にサインインするには、「[Azure AD を使用して Citrix Cloud にサインインする](#)」を参照してください。
4. 高度な Entra ID 機能を有効にするには、「[高度な Azure AD 機能を有効にする](#)」を参照してください。
5. 更新されたアプリの Entra ID に再接続するには、「[アプリのアップデートに対応するため Azure AD に再接続する](#)」を参照してください。
6. Entra ID に再接続するには、「[アプリのアップデートに対応するため Azure AD に再接続する](#)」を参照してください。
7. Entra ID Connect とアカウントを同期するには、「[アカウントを同期する](#)」を参照してください。

オンプレミスの AD アカウントを Entra ID と同期することをお勧めします。

注:

Citrix Workspace 構成でフェデレーション ID プロバイダーセッションのログインプロンプトを無効にします。

### Workspace Sessions

#### Federated Identity Provider Sessions

Disabled

When Workspace is configured to use a federated identity provider, the authentication session and its lifetime are controlled by the identity provider. When enabled, Workspace forces a login prompt with the identity provider when a new Workspace session is needed. When disabled, a subscriber will not be prompted to authenticate with the identity provider if accessing Workspace with a valid session, achieving single sign-on.

## Azure Portal で Microsoft Azure と ChromeOS の間に SSO とユーザープロビジョニングをセットアップ

Microsoft Entra ID テナントと Google for ChromeOS の間で SSO のプロビジョニングを設定すると、エンドユーザーは ChromeOS デバイスの Google サインイン画面ではなく、Azure 認証ページにサインインできるようになります。

詳しくは、次のトピックを参照してください:

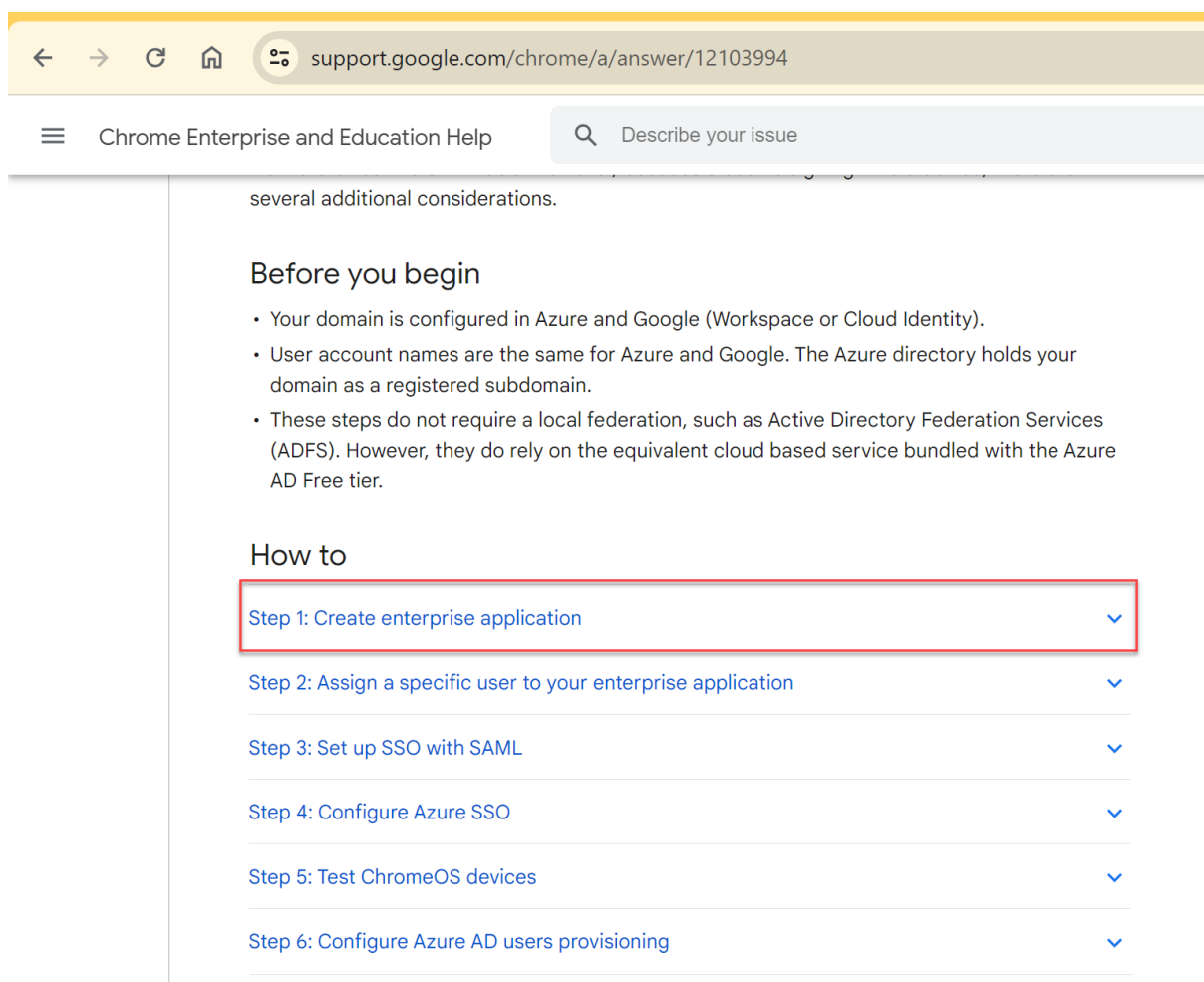
- Google の記事「[Microsoft Azure と ChromeOS 間の SSO およびユーザープロビジョニングを設定する](#)」。

および

- Microsoft チュートリアル「[チュートリアル: Microsoft Entra SSO と Google Cloud/G Suite Connector by Microsoft の統合](#)」。

Azure Portal で SSO を設定するには、以下の手順を実行します：

1. Microsoft Entra ID ポータルでエンタープライズアプリケーションを作成します。詳しくは、Google の記事「[Microsoft Azure と ChromeOS 間の SSO およびユーザープロビジョニングを設定する](#)」で手順 1 を参照してください。



The screenshot shows a browser window with the URL `support.google.com/chrome/a/answer/12103994`. The page title is "Chrome Enterprise and Education Help" and the search bar contains "Describe your issue". The main content area shows the text "several additional considerations." followed by a section titled "Before you begin" with three bullet points. Below this is a section titled "How to" with a list of six steps, each with a dropdown arrow. The first step, "Step 1: Create enterprise application", is highlighted with a red border.

1. 手順 1 で作成したエンタープライズアプリケーションに 1 人または複数のユーザーを割り当てます。詳しくは、Google の記事「[Microsoft Azure と ChromeOS 間の SSO およびユーザープロビジョニングを設定する](#)」で手順 2 を参照してください。
2. SAML を使用して SSO を設定します。詳しくは、Google の記事「[Microsoft Azure と ChromeOS 間の SSO およびユーザープロビジョニングを設定する](#)」で手順 3 を参照してください。

注:

Google 管理ポリシーで SAML ポリシーを作成した後、基本 SAML 構成を変更することをお勧めします。

SAML ベースのシングルサインオン用に Azure Portal で URL を設定すると、アプリケーションの表示は次のようになります。

[↑ Upload metadata file](#)
[↩ Change single sign-on mode](#)
[☰ Test this application](#)
[🗨 Got feedback?](#)

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Google Cloud / G Suite Connector by Microsoft.

- 1** Highly recommended: Install the Azure AD browser extension

The My Apps Secure Sign-in browser extension is already installed. Please continue with configuration.
- 2** Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	https://accounts.google.com/samlr/metadata?rpId=03vsmsh1tw5vcw
Reply URL (Assertion Consumer Service URL)	https://accounts.google.com/samlr/acs?rpId=03vsmsh1tw5vcw
Sign on URL	https://citrixcrvgso.cloud.com
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- 3** Attributes & Claims [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- 4** SAML Certificates

<b>Token signing certificate</b> <span style="float: right;"><a href="#">Edit</a></span>	
Status	Active
Thumbprint	9D5C836884D96D2FB1850ED88643633D9162D650
Expiration	12/27/2025, 11:51:11 AM
Notification Email	mgali@crvg.org
App Federation Metadata Url	<a href="https://login.microsoftonline.com/03b60c09-da29-...">https://login.microsoftonline.com/03b60c09-da29-...</a>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

---

<b>Verification certificates (optional) (Preview)</b> <span style="float: right;"><a href="#">Edit</a></span>	
Required	No
Active	0
Expired	0
- 5** Set up Google Cloud / G Suite Connector by Microsoft

You'll need to configure the application to link with Azure AD.

✔ My apps Secure Sign-in browser extension is installed. Click the button below to download the SAML Certificate and setup the application.

[Set up Google Cloud / G Suite Connector by Microsoft](#)

^ Configuration URLs

Login URL	<a href="https://login.microsoftonline.com/03b60c09-d-...">https://login.microsoftonline.com/03b60c09-d-...</a>
Azure AD Identifier	<a href="https://sts.windows.net/03b60c09-da29-4563-...">https://sts.windows.net/03b60c09-da29-4563-...</a>
Logout URL	<a href="https://login.microsoftonline.com/03b60c09-d-...">https://login.microsoftonline.com/03b60c09-d-...</a>
- 6** Test single sign-on with Google Cloud / G Suite Connector by Microsoft

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

[Test](#)



### 検証チェックポイント

ストア URL を入力すると、Azure ID プロバイダーのサインインページが表示されます。表示されなかった場合は、「Azure Portal で Microsoft Azure と ChromeOS の間に SSO とユーザープロビジョニングをセットアップする」の手順を再度確認してください。

## Google 管理コンソールで SAML SSO プロファイルを構成する

- ドメインとユーザーを追加し、OU を作成します。詳しくは、「[A complete guide to Google Organizational Units](#)」を参照してください。
- ID プロバイダーとして Microsoft Entra ID を使用して SAML SSO プロファイルを作成します。詳しくは、「[Configuring SAML single sign-on \(SSO\) for Azure AD Users](#)」を参照してください。

### 検証チェックポイント

Chromebook を使用する場合は、Azure 認証情報を使用して Citrix Workspace アプリにサインインできる必要があります。ブラウザーにストア URL を入力する場合は、サインインできる必要があります。

## SAML SSO Chrome 拡張機能を使用した ChromeOS 向け Citrix Workspace アプリの SSO の構成

SAML 拡張機能を使用して SSO を構成するには、次の手順を実行します：

1. Chrome デバイス上で、Chrome アプリの SAML SSO 拡張機能をインストールして構成します。  
拡張機能をインストールするには、[SAML SSO for Chrome Apps](#)をクリックします。
2. この拡張機能は、SAML Cookie をブラウザーから取得して、ChromeOS 向け Citrix Workspace に提供します。
3. Citrix Workspace アプリが SAML Cookie を取得できるようにするには、次のポリシーを構成します。以下は JSON データです：

```
1  {
2
3  "allowlist": {
4
5    "Value": [
6      {
7
8        "appId": "hai f f j c a d a g j l i j o g g c k p g f n o e i f l n e m",
9        "domain": "login.microsoftonline.com"
10     }
11   ]
12 }
13 }
14
15 }
```

```
16  
17 <!--NeedCopy-->
```

### 検証チェックポイント

Azure ID プロバイダストアと SSO 拡張機能を使用して Citrix Workspace アプリを起動する場合、Citrix Workspace アプリへのサインインが成功する必要があります。

## FAS を展開して仮想アプリとデスクトップへの SSO を可能にする

仮想アプリと仮想デスクトップへの SSO を可能にするために、フェデレーション認証サービス (FAS) を展開できません。

### 注:

FAS がない場合は、Active Directory のユーザー名とパスワードの入力を求められます。詳しくは、「[Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化](#)」を参照してください。

## SDK および API

May 16, 2024

### HDX SDK

ChromeOS 向け Citrix Workspace アプリでは、サードパーティ製 Chrome アプリをロックおよびロック解除したり、以下のセッションから切断したりできる Chrome API (実験的な API) を導入しました:

- Citrix Virtual Apps and Desktops
- Citrix DaaS (旧称 Citrix Virtual Apps and Desktops サービス) セッション

この API によって、埋め込みモードおよびキオスクモードの両方で ChromeOS 向け Citrix Workspace アプリを起動できます。埋め込みモードで起動されたセッションは、キオスクモードで起動されたセッションと同様に機能します。

SDK について詳しくは、[HDX SDK for Citrix Workspace app for ChromeOS](#)を参照してください。

HDX SDK の例については、[Citrixダウンロードページ](#)を参照してください。

## Citrix 仮想チャンネル SDK

Citrix 仮想チャンネルソフトウェア開発キット (SDK) は、ICA プロトコルを使用する追加の仮想チャンネルのための、サーバー側アプリケーションやクライアント側ドライバーの作成をサポートします。

サーバー側仮想チャンネルアプリケーションは、Citrix Virtual Apps または Citrix Virtual Apps and Desktops サーバー上にあります。このバージョンの SDK は、ChromeOS 向け Citrix Workspace アプリ用の新しい仮想チャンネルの作成をサポートします。他のクライアントプラットフォーム用の仮想ドライバーの作成については、Citrix にお問い合わせください。

仮想チャンネル SDK には、以下のものが用意されています。

- Citrix Server API SDK (WFAPI SDK) の仮想チャンネルとともに使用して、新しい仮想チャンネルを容易に作成できるインターフェイス。
- プログラミングテクニックの実例となるいくつかの仮想チャンネルサンプルプログラムの、実際に機能するソースコード。
- 仮想チャンネル SDK では、WFAPI SDK で仮想チャンネルのサーバー側を作成する必要があります。

仮想チャンネル (VC) SDK について詳しくは、[Citrix Virtual Channel SDK for Citrix Workspace app for ChromeOS](#)を参照してください。

## 仮想チャンネル SDK の機能強化

2305 リリース以降、ChromeOS 向け Citrix Workspace アプリは、仮想チャンネル SDK の Windows Management API をサポートします。Web API を使用すると、IT 管理者は対話型アプリケーションを作成し、エンドユーザー向けにカスタマイズできます。

## サードパーティ Chrome アプリで API を使用する手順

1. 最新バージョンの ChromeOS 向け Citrix Workspace アプリをインストールします。詳しくは、[Citrix ダウンロードページ](#)を参照してください。
2. ChromeOS 向け Citrix Workspace アプリのポリシーファイルを追加して、サードパーティの Chrome アプリを許可リストに追加します。Chrome の管理設定を使用して、ポリシーを追加します。

詳しくは、Google サポートの[組織部門単位での Chrome アプリの管理](#)を参照してください。

以下は、サードパーティの Chrome アプリを許可リストに追加する場合の、サンプルの `policy.txt` JSON データです：

```
1 {  
2  
3     "settings": {  
4
```

```
5         "Value": {
6
7             "settings_version": "1.0",
8             "store_settings": {
9
10                "externalApps": [ "<3rdParty_App1_ExtID>" , "<3
rdParty_App2_ExtID>" ]
11            }
12        }
13    }
14 }
15 }
16 }
17 }
18 }
19 <!--NeedCopy-->
```

注:

<3rdParty\_App1\_ExtID>は、externalApps の名前の例として使用され、ChromeOS 向け Citrix Workspace アプリにメッセージを送信できます。chrome://extensions サイトから **appid** を取得します。

3. 以下の手順に従って、ChromeOS 向け Citrix Workspace アプリでアプリケーションまたはデスクトップセッションを起動します:

- workspaceappID を取得します。

```
var workspaceappID = "haiffjcadagjlijoggckpgfnoeiflnem ";
```

注:

この例で、**workspaceappID** は ChromeOS 向け Citrix Workspace アプリのストアバージョンです。ChromeOS 向け Citrix Workspace アプリの再パッケージされたバージョンを使用する場合、適切な workspaceappID を使用してください。

- ICA データを INI から JSON 形式に変換します。

注:

通常、ICA ファイルは INI ファイルとして StoreFront から取得されます。以下のヘルパー機能で ICA INI ファイルを JSON に変換します。

```
1 //Helper function to convert ica in INI format to JSON
2 function convertICA_INI_TO_JSON(data){
3
4     var keyVals = {
5     }
6     ;
7     if (data) {
```

```
8
9  var dataArr;
10 if(data.indexOf('\r')== -1){
11
12  dataArr = data.split('\n');
13  }
14  else{
15
16  dataArr = data.split('\r\n');
17  }
18
19  for (var i = 0; i < dataArr.length; i++) {
20
21  var nameValue = dataArr[i].split('=', 2);
22  if (nameValue.length === 2) {
23
24  keyVals[nameValue[0]] = nameValue[1];
25  }
26
27  // This is required as LaunchReference contains '=' as well. The
28  // above split('=',2) will not provide
29  // the complete LaunchReference. Ideally, something like the
30  // following should be used generically as well
31  // because there can be other variables that use the '='
32  // character as part of the value.
33  if (nameValue[0] === "LaunchReference") {
34
35  var index = dataArr[i].indexOf('=');
36  var value = dataArr[i].substr(index + 1);
37  keyVals[nameValue[0]] = value;
38  }
39
40  }
41
42  return keyVals;
43  }
44
45  return null;
46  }
47  <!--NeedCopy-->
```

- サードパーティの Chrome アプリから ChromeOS 向け Citrix Workspace アプリに ICA メッセージを送信しません。

```
1  var icaFileJson = {
2  ... }
3  ; // ICA file passed as JSON key value pairs.
4  var message = {
5
6  "method" : "\launchSession",
```

```
7  "icaData" : icaJSON
8  }
9  ;
10 chrome.runtime.sendMessage(workspaceappID, message,
11   function(launchStatus) {
12
13     if (launchStatus.success) {
14
15       // handle success.
16       console.log("Session launch was attempted successfully");
17     }
18     else {
19
20       // handle errors.
21       console.log("error during session launch: ", launchStatus.message
22         );
23     }
24   }
25 );
26
27 <!--NeedCopy-->
```

**sendMessage** API コマンドについて詳しくは、以下のリンクを参照してください:

<https://developer.chrome.com/extensions/runtime#event-onMessageExternal>

<https://developer.chrome.com/extensions/runtime#method-sendMessage>

### SDK の Manifest V3 サポート

2305 リリース以降、ChromeOS 向け Citrix Workspace アプリは、[manifest version 3](#) を含む Chrome 拡張機能を使用する HDX SDK をサポートします。

詳しくは、開発者ガイドドキュメントの「[Citrix Workspace app for ChromeOS HDX SDK](#)」を参照してください。

### 廃止

May 16, 2024

この記事の告知は、段階的に廃止されるプラットフォーム、Citrix 製品、機能について前もってお知らせするためのものです。これらの告知を基にして、お客様は適宜ビジネス上の決定を下すことができます。

Citrix ではお客様の使用状況とフィードバックをチェックして、各プラットフォーム、Citrix 製品、機能を撤廃するかどうかを判断しています。お知らせする内容は以降のリリースで変わることがあり、廃止される機能がすべて含まれるわけではありません。

廃止となったアイテムはすぐには削除されません。このリリースでは引き続きサポートされますが、今後削除される予定です。

アイテム	廃止が発表されたリリース	削除されたリリース	代替手段
現時点ではありません	-	-	-



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).