



# Linux 向け Citrix Workspace アプリ

## Contents

このリリースについて	3
<b>Technical Preview</b>	<b>32</b>
システム要件と互換性	42
インストール、アンインストール、更新	53
開始	63
構成	76
認証	178
セキュリティで保護された通信	183
<b>Storebrowse</b>	<b>192</b>
トラブルシューティング	202
<b>SDK および API</b>	<b>227</b>
<b>ICA 設定リファレンス</b>	<b>228</b>

## このリリースについて

September 15, 2023

Linux 向け Citrix Workspace アプリの新機能、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 をお探しですか? 機能の一覧を [Technical Preview](#) に管理しているので、1 か所でさまざまな機能を見つけることができます。Preview 機能をご使用後、添付の 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。

### 2308 の新機能

#### プロキシサーバーの **HTTPS** プロトコルのサポート

以前は、SOCKS プロトコルを使用してのみプロキシサーバーに接続できました。Linux 向け Citrix Workspace アプリ 2308 以降では、HTTPS プロトコルを使用してプロキシサーバーに接続することもできます。

HTTPS プロトコルを使用してデスクトップを開く方法について詳しくは、「[プロキシサーバーの HTTPS プロトコルのサポート](#)」を参照してください。

#### **MJPEG Web** カメラのサポート

このリリースでは、MJPEG Web カメラは H264 ストリームでサポートされます。Web カメラは内部で MJPEG 圧縮を実行し、より良い画質とより高いフレームレートを実現します。この機能はデフォルトで有効になっています。ただし、Web カメラが MJPEG をサポートしていない場合、この機能は無効になります。

#### **SSL** 接続用のシステム証明書パスのサポート

このリリースの Citrix Workspace アプリは、SSL 接続用のシステム証明書パスをサポートします。この機能により、クライアント側の証明書管理プロセスがシンプルになり、ユーザーエクスペリエンスが向上します。この機能を使用すると、Citrix Workspace はシステム証明書パス内の証明書を使用して TLS 接続を作成できます。この機能はデフォルトで有効になっています。

#### 強化された仮想チャネル **SDK**

Linux 向け Citrix Workspace アプリの仮想チャネル SDK は、I/O 機能とウィンドウの位置に関する新しい API の追加により強化されています。詳しくは、以下を参照してください:

- [クライアント側メディアプレーヤー \(CSMP\)](#)
- [仮想ドライバーのフィーチャーフラグ機能](#)
- [仮想ドライバーのビューポート機能](#)

- [プログラミングのリファレンス](#)

全画面モードとウィンドウモードを切り替えるためのキーボードショートカットのサポート

以前は、Desktop Viewer の [ウィンドウ] ボタンまたは [全画面] ボタンを使用して、全画面モードとウィンドウモードを切り替えることができました。

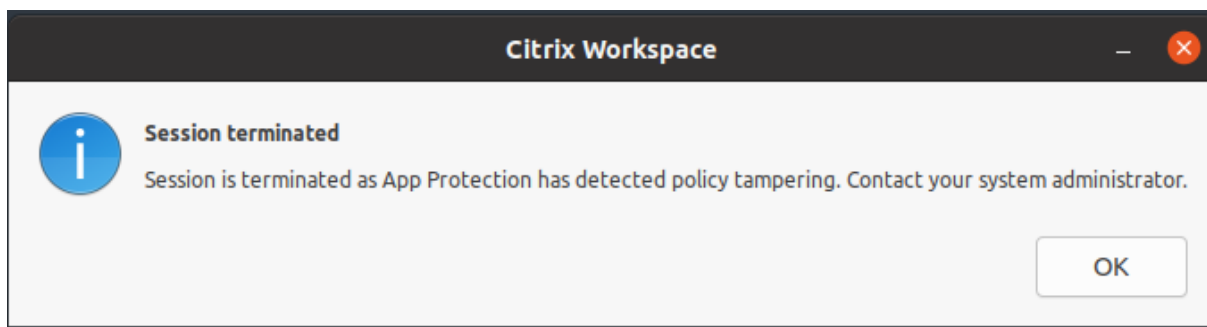
このリリース以降、キーボードショートカット Ctrl + F2 を使用して全画面モードとウィンドウモードを切り替えることができるようになりました。たとえば、デスクトップセッションが全画面モードのときに「Ctrl + F2」を押すと、デスクトップセッションが全画面モードを終了します。

この機能はデフォルトでは無効になっています。

詳しくは、「[全画面モードとウィンドウモードを切り替えるためのキーボードショートカットのサポート](#)」を参照してください。

ポリシーの改ざんの検出

ポリシーの改ざん検出機能は、App Protection の画面キャプチャ対策ポリシーとキーロガー対策ポリシーが改ざんされている場合、ユーザーが仮想アプリまたはデスクトップセッションにアクセスできないようにします。ポリシーの改ざんが検出された場合、仮想アプリまたはデスクトップセッションは次のエラーメッセージが表示されて終了します：



ポリシーの改ざんの検出機能について詳しくは、「[ポリシーの改ざんの検出](#)」を参照してください。

### Technical Preview

- ARM64 デバイスの Web カメラリダイレクトとサービス継続性のサポート
- パケット損失補間を有効にしてオーディオパフォーマンスを向上
- マルチタッチのサポート

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

## 2308 で解決された問題

- 2 番目のホップのシナリオでは、Topaz USB Signature Pad またはその他の USB デバイスを使用するアプリケーションから切断される可能性があります。この問題は、両方のホップで汎用 USB リダイレクト機能を使用する場合に発生します。[CVADHELP-23053]
- Linux 向け Citrix Workspace アプリを 2206 以降のバージョンにアップグレードした後、Citrix Workspace アプリへのサインインに失敗する場合があります。この問題は、共有ユーザーモードで 2 回目以降にサインインするときのみ発生します。[CVADHELP-22775]
- ブラウザーコンテンツリダイレクト (BCR) 機能が有効になっている場合、シンクライアントでディスク容量の問題が発生する可能性があります。この問題は、リダイレクトされた Web ページのローカルキャッシュがローカルに保存されるために発生します。[CVADHELP-21764]
- セッション内で誤った HDMI オーディオデバイスが検出される場合があります。[CVADHELP-18849]
- Linux 向け Citrix Workspace アプリの 64 ビット rpm パッケージをインストールする場合、32 ビットに必要なライブラリパッケージをインストールするための別の要件が発生することがあります。[CVADHELP-23347]
- 全画面モードでアクセスすると、YouTube の Web サイトでリダイレクトされたブラウザーコンテンツの検索ボックスにテキストを入力できない場合があります。この問題は、2106 以降の Linux 向け Citrix Workspace アプリで発生します。[CVADHELP-20339]
- Storebrowse -E または -S コマンドを使用して PNA ストアに接続する場合、2 回の認証が必要になる場合があります。この問題は、2205 以降の Linux 向け Citrix Workspace アプリで発生します。[CVADHELP-22917]
- ショートカットキー「Ctrl + Alt + Enter」を使用する場合、Enter キーを押すとキーボードが反応しなくなる場合があります。この問題は、Linux 向け Citrix Workspace アプリから開始された Linux VDA デスクトップセッションでのみ発生します。[CVADHELP-22930]
- 白いカーソルは、濃い青または黒の背景では明確に表示されません。この問題は、Linux 向け Citrix Workspace アプリバージョン 2307 で発生します。[HDX-52458]
- セッションの開始後にセカンダリモニターが接続された場合、両方のモニターで全画面モードでセッションを使用できない場合があります。[HDX-52816]
- ダブルホップセッションでは、USB ストレージデバイスをアプリまたはデスクトップにリダイレクトできない場合があります。[HDX-52155]
- Chrome のブラウザーコンテンツリダイレクト機能を使用してリダイレクトされたコンテンツについては、空白のページが表示される場合があります。この問題は、Linux 向け Citrix Workspace アプリ 2305 を使用して許可されたサイトにアクセスすると発生します。[HDX-50561]

## 2308 の既知の問題

- ブラウザーコンテンツリダイレクト先のサイトにアクセスした後、ユーザーセッションからサインアウトすると、エラーメッセージが表示される場合があります。回避策として、エラーメッセージを無視してください。[HDX-55087]

注:

以前のリリースの問題については、「[既知の問題](#)」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。

## 2307

### 新機能

#### Windows Media Player リダイレクトのシステム要件を検証するスクリプト

このリリースでは、Linux 向け Citrix Workspace アプリの Windows Media Player リダイレクト機能に必要な構成を検証するための新しい bash スクリプトが導入されました。この機能は、Windows Media Player リダイレクト機能のトラブルシューティングの時間を短縮するのに役立ちます。構成を検証するには、次の場所から入手できる同じ `rave_troubleshooting.sh` を使用できます。「[RAVE のシステム診断スクリプト](#)」。

#### 最適化された Microsoft Teams で短いトーンを再生するサポートを追加

以前は、セカンダリ呼び出し機能が有効になっていると、ビープ音や通知などの短いトーンが繰り返し再生されていました。たとえば、ゲストが Microsoft Teams 会議に参加するときのトーンが繰り返し再生されました。これを回避する唯一の方法は、Microsoft Teams を終了して再起動することでした。この問題により、エンドユーザーエクスペリエンスが低下していました。

このリリースでは、Citrix Workspace アプリが必要性に応じた短いトーンの再生をサポートします。このサポートでは、セカンダリ呼び出し機能も有効にすることができます。

前提条件:

Microsoft Teams を最新バージョンに更新してください。

注:

この機能は、Microsoft Teams から以降の更新がロールアウトされた後にのみ使用できます。Microsoft によって更新プログラムがロールアウトされたら、ドキュメントのアップデートおよび発表について、[CTX253754](#)で確認できます。

### Technical Preview

- プロキシサーバーの HTTPS プロトコルのサポート
- DTLS を使用した IPv6 UDT のサポート
- ARM64 デバイスでの App Protection のサポート

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

### 解決された問題

- `AllowMultistream`値が Ubuntu 22.04 で True に設定されている場合、Citrix Workspace アプリバージョン 2303 でセッションを開始できないことがあります。[HDX-49916]
- CAS データ収集に対する DNS ポーリングが、ICA の直接起動および CAS が無効なストアに対して発生する場合があります。[CVADHELP-20018], [CVADHELP-12344]
- Avaya WorkPlace を開くと、仮想アプリまたはデスクトップ画面に黒い枠線が残ります。[CVADHELP-21558]
- Snipping Tool などのツールを使用すると、仮想アプリやデスクトップにカーソルの影が表示されることがあります。[CVADHELP-22336]

## 2305

### 新機能

#### **GNOME 42** のキーボードレイアウト同期をサポートするための機能強化

このリリースより、Linux 向け Citrix Workspace アプリは、GNOME 42 以降のデスクトップ環境を使用する Ubuntu 22.04 などのデスクトップのキーボードレイアウトの同期をサポートします。

詳しくは、「[キーボードレイアウトの同期](#)」セクションを参照してください。

### 東アジア言語のクライアント **IME**

Linux 用 Citrix Workspace アプリでのクライアント入力システム (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。次の場合にクライアント IME を使用することを選択できます:

- Linux クライアントに必要な IME がある、または、
- IME がリモートサーバーから利用できない。

詳しくは、「[東アジア言語用のクライアント IME](#)」を参照してください。

### クライアント側のジッターバッファメカニズムの追加

この機能によって、ネットワーク遅延が変動する場合でもオーディオは確実にクリアになります。この機能は、デフォルトで有効になります。

この機能を無効にするには、`/opt/Citrix/ICAClient/config/module.ini`構成ファイルに移動し、`JitterBufferEnabled=FALSE`を編集します。

## 64 ビットの **Web** カメラリダイレクト

このリリースより、Web カメラリダイレクトは 64 ビット版アプリケーションに対応しています。詳しくは、「[Web カメラ](#)」を参照してください。

## **Azure Active Directory** で **200** を超えるグループをサポート

このリリースでは、200 を超えるグループに属している Azure Active Directory ユーザーは、そのユーザーに割り当てられているアプリとデスクトップを表示できるようになります。以前は、同じユーザーがこれらのアプリとデスクトップを表示することはできませんでした。

注:

この機能を有効にするには、ユーザーは Citrix Workspace アプリからサインアウトし、再度サインインする必要があります。

## **Ubuntu 22.04** での **App Protection** のサポート

Linux 向け Citrix Workspace アプリのバージョン 2305 より、Ubuntu 22.04 上の Citrix Workspace アプリから保護された仮想アプリおよびデスクトップを起動できるようになりました。

## 最適化された **Microsoft Teams** 通話のスリープモードの機能強化

以前は、最適化された Microsoft Teams 会議に参加しているときに、マウスまたはキーボードの操作がない場合、Citrix Workspace アプリまたは最適化された Microsoft Teams 画面がスリープモードになることがありました。

このリリースより、最適化された Microsoft Teams 会議中にマウスやキーボードの操作がない場合でも、Citrix Workspace アプリまたは最適化された Microsoft Teams の画面はスリープモードにならなくなりました。

## 最適化された **Microsoft Teams** ビデオ会議通話のエクスペリエンスの向上

このリリース以降、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。この機能強化では、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（720p、360p など）で配信できます。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。

注:

この機能は、Microsoft Teams からの更新のロールアウト後にのみ使用できます。ETA については、にアクセスして、Microsoft 365 ロードマップを検索してください。Microsoft によって更新プログラムがロールアウト



トされたら、ドキュメントのアップデートおよび発表について、[CTX253754](#)で確認できます。

### Technical Preview

- 2つの仮想デスクトップ間でファイルとフォルダーをコピーして貼り付ける
- ARM64 アーキテクチャのサポート
- TLS を使用した IPv6 TCP のサポート
- 32 ビットカーソルのサポートの機能強化
- オンプレミスストアへの接続で FIDO2 を使用した認証のサポート [Technical Preview]
- 最適化された Microsoft Teams でのハードウェアアクセラレーションへの対応

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

### 解決された問題

- 録音用アプリが Microsoft Windows API MME (Multimedia Extension) を使用している場合、録音されたオーディオが高速で再生されることがあります。たとえば、20 秒間録音したオーディオが、15 秒間で再生される可能性があります。[CVADHELP-22162]
- `.ICAClient` フォルダー内の `.NSAP_Data` ファイルのサイズが最大サイズを超えてしまい、シンクライアントの動作に影響を与える可能性があります。この問題は、NetScaler で HDX Insight が有効になっているときに発生します。[CVADHELP-22616]
- ハイブリッド起動を使用している場合、IGEL ディストリビューションで Mozilla Firefox から保護されたセッションを開くと失敗します。[CVADHELP-22436]
- Linux 向け Citrix Workspace アプリのバージョン 2209 からアプリまたはデスクトップを開くと、SSL エラーが発生する場合があります。[HDX-49324]
- VDI 内のユニバーサル Windows プラットフォーム (UWP) アプリが FIDO2 を使用して認証を試みると、Linux 向け Citrix Workspace アプリが応答を停止することがあります。[HDX-48942]
- 最適化された Microsoft Teams で画像アイコンを選択すると、gzip ファイルが自動的にダウンロードされず、最適化された Microsoft Teams では、画像を背景画像として適用できない場合があります。[HDX-51694]
- スマートカードを使用すると、Linux 向け Citrix Workspace アプリバージョン 2303 への認証に失敗することがあります。この問題は、Red Hat、Ubuntu 22.04、および Debian 11 Linux ディストリビューションで発生します。[RFLNX-9620]
- アプリインジケータから Citrix Workspace アプリを終了すると、アプリが応答を停止し、次のエラーメッセージが表示されることがあります：  
「Glib (gthread-posix.c): Unexpected error from C library during 'pthread\_setspecific': Invalid argument.」 [RFLNX-9445]
- `libAnalyticsInterface.so` で未定義のエラーが発生し、Citrix Workspace アプリからの Google Analytics データの共有に失敗する場合があります。[RFLNX-9705]

## 2303

### 新機能

#### 永続ログイン

永続ログイン機能を使用すると、管理者が設定した期間（2～365 日）、ログインしたままにすることができます。この機能が有効になっている場合、設定された期間中に Citrix Workspace アプリのログイン資格情報を入力する必要はありません。

この機能により、Citrix DaaS セッションへの SSO は、最大 365 日まで間延長されます。この拡張機能は、長期有効トークンの有効期間に基づいています。資格情報は、デフォルトで 4 日間または有効期間のいずれか短い方の期間、キャッシュされます。その後、Citrix Workspace アプリへの接続で 4 日以内にアクティブになったときに延長されます。

詳しくは、「[永続ログイン](#)」を参照してください。

#### HDX セッションで FIDO2 を使用した認証のサポート

このリリースでは、パスワードなしの FIDO2 セキュリティキーを使用して HDX セッション内で認証できます。FIDO2 セキュリティキーは、企業の従業員がユーザー名やパスワードを入力せずに FIDO2 をサポートするアプリやデスクトップに認証するためのシームレスな方法を提供します。FIDO2 について詳しくは、「[FIDO2 認証](#)」を参照してください。

##### 注:

USB リダイレクト経由で FIDO2 デバイスを使用している場合は、FIDO2 デバイスの USB リダイレクト規則を `$ICAR00T/` フォルダの `usb.conf` ファイルから削除します。この更新により、FIDO2 仮想チャンネルに切り替えることができます。

デフォルトでは、FIDO2 認証は無効になっています。

詳しくは、「[FIDO2 を使用した認証のサポート](#)」を参照してください。

#### オーディオエコーキャンセルのサポートの改善

このリリース以降、Citrix Workspace アプリではエコーキャンセルがサポートされます。この機能はリアルタイムのユーザーケース向けに設計されており、ユーザーエクスペリエンスを向上させます。エコーキャンセル機能は、低品質、中品質、およびアダプティブオーディオをサポートします。パフォーマンスを向上させるために、アダプティブオーディオを使用することを Citrix ではお勧めします。

詳しくは、「[オーディオエコーキャンセルのサポートの改善](#)」を参照してください。

#### Citrix Workspace アプリの非アクティブタイムアウト

非アクティブタイムアウト機能では、管理者が設定した値に基づいてユーザーが Citrix Workspace アプリからサインアウトされます。管理者は、ユーザーが Citrix Workspace アプリから自動的にサインアウトされるまでのアイドル

ル時間を指定できます。Citrix Workspace アプリウィンドウ内で、指定された時間内にマウス、キーボード、またはタッチによるアクティビティが発生しなくなると、自動的にサインアウトされます。無操作状態によるタイムアウトは、既に実行中の Citrix Virtual Apps and Desktops および Citrix DaaS セッションまたは StoreFront ストアには影響しません。

非アクティブタイムアウト値は、10 分から 1440 分まで設定できます。このタイムアウト値を変更する場合の間隔は、5 の倍数にする必要があります。例: 10、15、20、または 25 分。デフォルトでは、非アクティブタイムアウトは構成されていません。

注:

この機能は、クラウド展開でのみ適用できます。

InactivityTimeoutInMinutes を構成する方法について詳しくは、「[Citrix Workspace アプリの非アクティブタイムアウト](#)」セクションを参照してください。

### Web カメラリダイレクトの背景のぼかし

Linux 向け Citrix Workspace アプリが、Web カメラリダイレクトの背景のぼかしをサポートするようになりました。

詳しくは、「[Web カメラリダイレクトの背景のぼかし](#)」を参照してください。

### ブラウザコンテンツリダイレクトオーバーレイのブラウザの一時データストレージパスを構成する

Citrix Workspace アプリ 2303 バージョン以降では、CEF ベースのブラウザの一時データストレージパスを構成するように求められます。

詳しくは、「[ブラウザコンテンツリダイレクトオーバーレイのブラウザの一時データストレージパスを構成する](#)」を参照してください。

### 新しい PIV カードのサポート

このリリースでは、Citrix Workspace アプリは次の新しい Personal Identification Verification (PIV) カードをサポートします:

- IDEMIA の次世代スマートカード
- DELL TicTok スマートカード

### スマートカードドライバーのパフォーマンスの最適化

Citrix Workspace アプリ 2303 バージョンには、VDSCARDV2.DLL スマートカードドライバーのパフォーマンス関連の修正と最適化が含まれています。これらの機能強化は、バージョン 1 VDSCARD.DLL よりも優れたパフォーマンスを発揮するのに役立ちます。

## Microsoft Teams の機能強化

### 優先ネットワークインターフェースの構成

Citrix Workspace アプリ 2303 バージョン以降、メディアトラフィックの優先ネットワークインターフェースを構成できるようになりました。この機能強化により、複数のネットワーク接続があり、デフォルトのネットワークのパフォーマンスが弱い場合、別のネットワークに変更できます。

詳しくは、「[優先ネットワークインターフェースの構成](#)」を参照してください。

### 解決された問題

- Citrix Virtual Apps 経由で Hyperspace にアクセスすると、Hyperspace 専用のサインインページが、既に開始されているアプリの上に表示されることがあります。[CVADHELP-20368]
- 2 番目のアプリケーションにアクセスすると、現在のセッションが終了し、セッションが再開される場合があります。場合によっては前のセッションのデータが消えて、2 番目のアプリケーションが起動したときにセッションが開始されたかのようにデータが更新されます。この問題は、セッションで最初のアプリケーションを開始するときには発生しません。[CVADHELP-21914]
- [Selfservice] > [プロファイル] > [アカウント設定] > [地域の設定] > [時間形式] セクションで 24 時間形式を更新できない場合があります。この問題は、クラウドストアでのみ発生します。[CVADHELP-20866]
- 複数のファイルを VDA セッションから USB デバイスにドラッグしているときに USB デバイスを取り外すと、セッションが突然終了することがあります。この問題は、Ubuntu でのみ発生します。[HDX-30219]
- VDSCARDV2.DLL ドライバーバージョンのスマートカードを使用して Citrix Workspace アプリにサインインすると、パフォーマンスの問題が発生する場合があります。この問題は、eLux ディストリビューションでのみ発生します。[HDX-44314]

## 2302

### 新機能

#### Citrix Workspace アプリの非アクティブタイムアウト [Technical Preview]

非アクティブタイムアウト機能では、管理者が設定した値に基づいてユーザーが Citrix Workspace アプリからサインアウトされます。管理者は、ユーザーが Citrix Workspace アプリから自動的にサインアウトされるまでのアイドル時間を指定できます。Citrix Workspace アプリウィンドウ内で、指定された時間内にマウス、キーボード、またはタッチによるアクティビティが発生しなくなると、自動的にサインアウトされます。無操作状態によるタイムアウトは、既に実行中の Citrix Virtual Apps and Desktops および Citrix DaaS セッションまたは StoreFront ストアには影響しません。

非アクティブタイムアウト値は、10 分から 1440 分まで設定できます。このタイムアウト値を変更する場合の間隔は、5 の倍数にする必要があります。例: 10、15、20、または 25 分。デフォルトでは、非アクティブタイムアウトは構成されていません。管理者は、PowerShell モジュールを使用して `inactivityTimeoutInMinutes` プロパティを構成できます。

InactivityTimeoutInMinutes を構成する方法について詳しくは、「[Citrix Workspace アプリの非アクティブタイムアウト](#)」セクションを参照してください。

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

注:

Technical Preview は、顧客が非実稼働環境または制限のある稼働環境でテストし、フィードバックを共有する機会を提供するためのものです。機能プレビュー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としない場合があります。ベータ版のビルドは実稼働環境に展開しないことをお勧めします。

### 韓国語のサポート

Linux 向け Citrix Workspace アプリが韓国語で利用できるようになりました。

### Citrix Workspace アプリのパフォーマンスの最適化

このリリース以降、AuthManLite を使用した認証時の Linux 向け Citrix Workspace アプリのパフォーマンスが向上しました。

### Technical Preview

- カスタム Web ストアでの画面の固定

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

### 解決された問題

- Linux 向け Citrix Workspace アプリの ctxlogd.service と Linux VDA の ctxlogd.service で競合が発生する場合があります。[HDX-44569]
- 最適化された Microsoft Teams の会議で背景画像を正常に適用できない場合があります。この問題は、HP ThinPro OS などの特定のオペレーティングシステムで発生します。[HDX-47166]

## 2212

### 新機能

#### クライアント側のジッターバッファメカニズムの追加 **[Technical Preview]**

この機能によって、ネットワーク遅延が変動する場合でもオーディオは確実にスムーズになります。デフォルトでは、この機能は無効になっています。

この機能を有効にするには、次の手順を実行します:

1. 構成ファイル/opt/Citrix/ICAClient/config/module.iniに移動して編集します。
2. 次のように、オーディオ遅延の制御を無効にします:

```
1 `AudioLatencyControlEnabled = FALSE`
```

3. 次のようにジッターバッファを有効にします:

```
1 `JitterBufferEnabled = TRUE`
```

注:

Technical Preview は、顧客が非実稼働環境または制限のある稼働環境でテストし、フィードバックを共有する機会を提供するためのものです。機能プレビュー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としない場合があります。ベータ版のビルドは実稼働環境に展開しないことをお勧めします。

#### 複数のオーディオデバイスのサポート

このリリース以降の Citrix Workspace アプリは、セッションで使用可能なすべてのローカルオーディオデバイスを名前付きで表示します。また、プラグアンドプレイにも対応しています。

複数のオーディオデバイスのリダイレクト機能は、デフォルトで有効になっています。この機能を無効にするには、module.ini ファイルでAudioRedirectionV4の値を False に設定します。

#### オーディオ録音のサポート

このリリース以降、オーディオ録音機能はデフォルトで有効になっています。セッションが開始されると、オーディオを録音するデバイスが表示されます。

この機能を無効にするには、wfclient.ini ファイルでAllowAudioInputの値を False に設定します。

### Technical Preview

- 32 ビットカーソルのサポート
- Citrix Optimized Microsoft Teams での背景のぼかしと置き換え

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

#### 解決された問題

- スマートカードを取り外して再度挿入すると、有効なスマートカード証明書が見つからない場合があります。  
[CVADHELP-20787]
- TikTok スマートカードを使用して Citrix Workspace アプリにサインインできない場合があります。  
[CVADHELP-20578]

- IDEMIA のスマートカードを使用して Citrix Workspace アプリにサインインできない場合があります。[CVADHELP-20652]
- 複数のオーディオデバイスを有効にして Speex コーデックをオーディオリダイレクトで使用すると、Citrix Workspace アプリが応答しなくなることがあります。[CVADHELP-21212]
- Citrix Workspace アプリからサインアウトして再度サインインすると、サインイン資格情報を入力せずに Citrix Workspace アプリが起動します。この問題は、クラウド環境で `longLivedTokenSupport` パラメーター値が `True` に設定されている場合にのみ発生します。[RFLNX-9160]
- セッションを開始すると、トランザクション ID エラーメッセージが表示されることがあります。例: 「The option “-transactionid” is invalid」(オプション「-transactionid」は無効です)。[HDX-45618]
- Citrix Workspace アプリをインストールし、root 権限でセッションを開始すると、セッションが終了することがあります。[HDX-46967]
- Citrix Workspace アプリをインストールして起動すると、次のエラーメッセージが表示される場合があります:  
「The X request 130.1 caused error:”10: BadAccess(Attempt to access private resource denied)」(X リクエスト 130.1 が原因でエラー: ”10: 不正アクセス (プライベートリソースへのアクセス試行が拒否されました))。[HDX-44416]

## 2211

### 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

- デバイスの Audio インターフェイスをリダイレクトした後、VDA がクラッシュすることがあります。この問題は、Desktop Delivery Controller で「クライアント USB デバイスのリダイレクト」ポリシーを有効にし、複合 USB デバイス (USB ヘッドセットなど) をエンドポイントに接続すると発生します。[HDX-44117]
- USB リダイレクトを使用した後、Bloomberg 4 の QWERTY キーボードがセッションに対してロックされることがあります。[HDX-44555]
- Citrix Workspace アプリで、PIN コードを使用して YubiKey デバイスを登録して使用することができない場合があります。[HDX-44951]
- Snap Store のプロセスがバックグラウンドで実行されると、保護されたアプリとデスクトップを起動できないことがあります。[APPP-110]

## 2209

### 新機能

#### FIDO2 を使用した認証のサポート [Technical Preview]

このリリースでは、パスワードなしの FIDO2 セキュリティキーを使用して HDX セッション内で認証できます。FIDO2 セキュリティキーは、企業の従業員がユーザー名やパスワードを入力せずに FIDO2 をサポートするアプリやデスクトップに認証するためのシームレスな方法を提供します。FIDO2 について詳しくは、「[FIDO2 認証](#)」を参照してください。

注:

USB リダイレクト経由で FIDO2 デバイスを使用している場合は、FIDO2 デバイスの USB リダイレクト規則を `$ICAROOT/フォルダーのusb.conf` ファイルから削除します。この更新により、FIDO2 仮想チャネルに切り替えることができます。

デフォルトでは、FIDO2 認証は無効になっています。FIDO2 認証を有効にするには、次の手順を実行します:

1. `<ICAROOT>/config/module.ini` ファイルに移動します。
2. ICA 3.0 セクションに移動します。
3. `FIDO2= On` を設定します。

この機能は現在、PIN コードとタッチ機能を使用するローミング認証 (USB のみ) をサポートしています。FIDO2 セキュリティキーベースの認証を構成できます。前提条件とこの機能の使用については、「[FIDO2 を使用したローカル認証と仮想認証](#)」を参照してください。

FIDO2 をサポートするアプリまたは Web サイトにアクセスすると、プロンプトが表示され、セキュリティキーへのアクセスが要求されます。以前にセキュリティキーを PIN (最小 4 文字、最大 64 文字) で登録したことがある場合は、サインイン時に PIN を入力する必要があります。

以前に PIN なしでセキュリティキーを登録したことがある場合は、セキュリティキーをタッチするだけでサインインできます。

制限事項:

FIDO2 認証を使用して、2 台目のデバイスを同じアカウントに登録できない場合があります。

注:

Technical Preview は、お客様が非実稼働環境または制限のある稼働環境でテストし、フィードバックをご提供いただく機会を作るためのものです。機能プレビュー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としない場合があります。ベータ版のビルドは実稼働環境に展開しないことをお勧めします。

#### Microsoft Teams の機能強化

- アプリ共有の有効化: Linux 向け Citrix Workspace アプリ 2209 および Citrix Virtual Apps and Desktops 2109 より、Microsoft Teams の画面共有機能を使用してアプリを共有できます。



- **高 DPI サポートの機能強化**: 高 DPI 機能が有効になっており、4K モニターを使用している場合、Microsoft Teams ビデオのオーバーレイは目的の位置に適切なサイズで表示されます。単一モニターまたはマルチモニターの配置などのディスプレイ設定に関係なく、オーバーレイは常に正しく表示され、拡大されたり、目的の位置以外に表示されたりすることはありません。この強化機能を有効にするには、`wfclient.ini` 構成ファイルの `DPIMatchingEnabled` パラメーターが **True** に設定されていることを確認してください。詳しくは、「[DPI マッチングのサポート](#)」を参照してください。
- **WebRTC SDK のアップグレード**: 最適化された Microsoft Teams で使用される WebRTC SDK のバージョンは、バージョン M98 にアップグレードされます。

### 互換性ライブラリのアップグレード版

このリリース以降、Linux 向け Citrix Workspace アプリは次のライブラリと互換性があります:

- `glibc` 2.27 以降
- `glibcxx` 3.4.25 以降

### App Protection の更新

注:

App Protection は、Citrix Workspace アプリバージョン 2305 より前の Ubuntu 22.04 ではサポートされていません。その結果、App Protection モジュールを Ubuntu 22.04 にインストールすると、Citrix Workspace アプリで仮想アプリとデスクトップを起動できない場合があります。App Protection については、「[App Protection](#)」を参照してください。

### Technical Preview

- キーボード入力モードの機能強化
- 拡張キーボードレイアウトのサポート

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

### 解決された問題

- App Protection 機能を有効にすると、別ウィンドウの、Web ページを読み込む Authentication Manager インターフェイスで、キーロガー対策機能が動作しないことがあります。[RFLNX-9004]
- Linux 向け Citrix Workspace アプリ 2007 にアップグレードした後、Storebrowse を使用してストアを追加すると時間がかかる場合があります。この問題は、ストアがアクセスできないアプリ構成サービスに接続しようとするため発生します。[CVADHELP-20618]
- セルフサービスユーザーインターフェイスからクラウドストアに接続すると、サインインページで読み込み中アイコンが表示されることがあります。[CVADHELP-20039]

- 2つの異なるデリバリーグループから2つのアプリを開始すると、2つ目のアプリの開始に遅延が生じる場合があります。[CVADHELP-18198]

## 2207

### 新機能

#### オーディオ品質の強化

これまでは、Citrix Workspace アプリでオーディオをスムーズに再生するための最大出力バッファリング値は 200 ミリ秒でした。この値により、再生時には 200 ミリ秒の遅延が追加されていました。この最大出力バッファリング値は、インタラクティブオーディオアプリケーションにも影響を与えていました。

この機能拡張により、Citrix Workspace アプリの最大出力バッファリング値が 50 ミリ秒に低減され、インタラクティブオーディオアプリケーションのユーザーエクスペリエンスが向上しました。また、ラウンドトリップ時間 (RTT) が 150 ミリ秒短縮されました。

このリリース以降、適切な再生しきい値とパルスオーディオプリバッファを選択して、オーディオ品質を向上させることができるようになります。この機能拡張向けに、次のパラメーターが `module.ini` ファイルの [ClientAudio] セクションに追加されています：

- `PlaybackDelayThreshV4` – 出力バッファリングの初期レベルをミリ秒単位で指定します。Citrix Workspace アプリは、セッション継続中、このレベルのバッファリングを維持しようと努めます。`PlaybackDelayThreshV4` のデフォルト値は 50 ミリ秒です。このパラメーターは、`AudioRedirectionV4` が **True** に設定されている場合にのみ有効です。
- `AudioTempLatencyBoostV4` – オーディオスループットが急上昇した場合、または不安定なネットワークに対して十分でない場合、この値によって出力バッファリング値を増加させます。出力バッファリング値の増加により、スムーズなオーディオが提供されます。ただし、音声が若干遅れる場合があります。`AudioTempLatencyBoostV4` のデフォルト値は 100 ミリ秒に設定されています。このパラメーターは、`AudioRedirectionV4` が **True** に設定され、`AudioLatencyControlEnabled` が **True** に設定されている場合にのみ有効です。デフォルトでは、`AudioLatencyControlEnabled` の値は True に設定されています。

この拡張機能を有効にする方法については、「[オーディオ](#)」ドキュメントの「オーディオ品質の強化」セクションを参照してください。

#### 複合 USB デバイスリダイレクト

このリリース以降、Citrix Workspace アプリでは複合 USB デバイスを分割できるようになります。複合 USB デバイスは、複数の機能を実行できます。これらの機能は、各機能が異なるインターフェイスを使用することで可能となっています。複合 USB デバイスには、オーディオおよびビデオの入力および出力で構成されるヒューマンインターフェイスデバイス (HID) などが含まれます。

現在のところ、複合 USB デバイスリダイレクトは、デスクトップセッションでのみ利用できます。分割されたデバイスはデスクトップビューアに表示されます。

以前は、セッション中にデバイスのプラグを抜き差しすると、デバイスは自動的にリダイレクトされ、VDA に自動的に接続されていました。このリリース以降、構成ファイルの設定を介して手動で自動リダイレクトを有効にする必要があります。複合 USB デバイスの自動リダイレクトは、デフォルトでは無効になっています。

複合 USB デバイスのリダイレクトを構成する方法については、「[USB](#)」ドキュメントの「複合 **USB** デバイスリダイレクト」セクションを参照してください。

### オーディオエコーキャンセルのサポートの改善 **[Technical Preview]**

このリリース以降、Citrix Workspace アプリではエコーキャンセルがサポートされます。この機能はリアルタイムのユーザーケース向けに設計されており、ユーザーエクスペリエンスを向上させます。エコーキャンセル機能は、低品質、中品質、およびアダプティブオーディオをサポートします。パフォーマンスを向上させるために、アダプティブオーディオを使用することを Citrix ではお勧めします。

デフォルトでは、エコーキャンセル機能は無効になっています。リアルタイムのユーザーケースで、ヘッドセットの代わりにスピーカーを使用する場合は、エコーキャンセルをオンにすることをお勧めします。

#### 制限事項:

設計上、高品質のオーディオではエコーキャンセル機能は無効になっています。

詳しくは、「[オーディオ](#)」ドキュメントの「オーディオエコーキャンセルのサポートの改善」セクションを参照してください。

#### 注:

Technical Preview は、お客様が非実稼働環境または制限のある稼働環境でテストし、フィードバックをご提供いただく機会を作るためのものです。機能プレビュー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としない場合があります。ベータ版のビルドは実稼働環境に展開しないことをお勧めします。

### 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（「About/Version」で最適化された Citrix HDX）。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、ヘッドフォンが音声通話自体のプライマリの周辺機器であっても、Microsoft Teams は受信信号をスピーカーに送信します。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:

この機能は、Microsoft Teams から以降の更新がロールアウトされた後のみ使用できます。Microsoft の更新プログラムの公開予定日については、「[Microsoft 365 のロードマップ](#)」を参照してください。ドキュメント

の更新と発表については、[CTX253754](#)でも確認できます。

### Technical Preview

- DPI マッチングのサポート

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

### 解決された問題

- Lightweight X11 デスクトップ環境 (LXDE) を使用してデスクトップをフルスクリーンモードで起動した状態でネットワークから切断すると、ダイアログボックスの [終了] オプションで「<XXX>への接続が失われました」というエラーメッセージが表示されます。このメッセージは、自動クライアント再接続 (ACR) またはセッション信頼性 (SR) ポリシーの有効期限が切れている場合に表示されます。[終了] をクリックすると、ユーザーデスクトップが非表示になります。ただし、画面上の他の場所をクリックすると、いつまでたってもダイアログボックスに [終了] ボタンが表示されない場合があります。**Esc** キーまたは **Enter** キーを押して、ユーザーデスクトップを手動で終了する必要があります。[CVADHELP-17478]
- Linux 向け Citrix Workspace アプリで、オンプレミスの URL が「**cloud**」という文字列を含む場合 (たとえば、<xxx-yyy-cloud.com>)、クラウドドメインの URL として解釈される場合があります。[CVADHELP-19480]
- HDX Web カメラを使用しようとする、セッションが切断される場合があります。この問題は、VDA バージョン 2203 でのみ発生します。[CVADHELP-20223]
- 公開アプリケーション間、VDI セッション間、または VDI セッションと公開アプリケーション間でのコンテンツのコピーと貼り付けに失敗する場合があります。セッションまたはアプリケーションがしばらくの間応答しなくなることがあります。[CVADHELP-19899]
- Linux 向け Citrix Workspace アプリ 2205 バージョンのエンドポイントを介して接続すると、セッションの切断の問題が発生する場合があります。この問題は、特定のデフォルトのロック画面イメージを強制するポリシー設定を使用して特定の種類の JPEG ファイルタイプでロック画面を構成し、Citrix VDA 2203 に適用する場合に発生します。[CVADHELP-21572]
- Skype で Web カメラを使用してビデオをプレビューすると、プレビューに黒い画面が表示される場合があります。[HDX-37860]
- HDX RealTime Webcam ビデオ圧縮は、Citrix Workspace アプリでの MJPEG ビデオ形式のカメラをサポートしていません。[HDX-40352]
- Microsoft Teams の通話中に画面またはアプリを共有しているとき、他の参加者に視覚的なアーティファクトが表示される場合があります。この問題は、不適切なビデオ再生 (フリーズまたは一時的な黒い枠) などの不安定なフレームレートが原因で発生します。このリリースには、視覚的なアーティファクトを減らすのに役立つ改善されたフレームレートまたはサンプリングレートが含まれています。[HDX-38032]
- Citrix Workspace アプリのビデオまたは画像が正しくレンダリングされないことがあります。この問題は、Citrix Workspace アプリを VDA バージョン 2109 以降と一緒に使用した場合に発生します。[HDX-40287]
- `-span o` コマンドを使用して `wfica` を起動すると、セッションの起動に失敗し、使用可能なすべてのモニターにまたがる表示がされない場合があります。同様に、`-span h` コマンドを使用して `wfica` を起動すると、

ユーザーデバイスに現在接続されているモニターのリストが印刷されない場合があります。[HDX-32519]

- `-span o` コマンドを使用して `wfica` を起動すると、セッションの起動に失敗し、使用可能なすべてのモニターにまたがる表示がされない場合があります。同様に、`-span h` コマンドを使用して `wfica` を起動すると、ユーザーデバイスに現在接続されているモニターのリストが印刷されない場合があります。詳しくは、[コマンドリファレンス](#)を参照してください。[HDX-32519]
- TCP と EDT/UDP の接続試行中に 1 つのプロトコルで SSL エラーが発生した場合、競合状態が原因で両方の接続が失敗することがあります。この SSL エラーは、TLS 構成がプロトコル間で異なり、クライアントが 1 つのプロトコルを介して接続できない場合に発生する可能性があります。[RFLNX-8747]
- App Protection がインストールされた Citrix Workspace アプリがインストールされているマシンにリモートで接続しようとする、x11vnc サーバーがクラッシュし、接続が失敗します。その結果、x11vnc サーバーを介してマシンにリモートで接続できない場合があります。[RFLNX-8933]
- デフォルト設定でストアを追加すると、Storebrowse 列挙が失敗することがあります。この問題は、Debian 32 ビット OS でのみ発生します。[RFLNX-8743]
- 32 ビット Linux マシンで App Protection 機能を有効にして Citrix Workspace アプリをインストールすると、エラーメッセージが表示される場合があります。[RFLNX-8809]
- `storebrowse -a` コマンドを使用してストアを追加し、`storebrowse -E` コマンドを使用して列挙すると、Storebrowse 列挙が失敗することがあります。この問題は、Raspberry Pi OS でのみ発生します。[RFLNX-8803]

## 2205

### 新機能

#### Storebrowse の認証の強化

このリリース以降、Citrix Workspace アプリ内に認証ダイアログを配置し、ログオン画面にストアの詳細を表示するようになりました。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。認証トークンは暗号化され保存されるため、システムやセッションの再起動時に資格情報を再入力する必要はありません。

`AuthmanConfig.xml` ファイルの `StorebrowseIPC` キーを使用して、Storebrowse 機能の認証拡張機能のオフとオンを切り替えることもできます。デフォルトでは、トグル機能はオフになっています。

認証拡張機能は次の操作で Storebrowse をサポートします：

- Storebrowse -E：利用可能なリソースを一覧表示します。
- Storebrowse -L：公開リソースへの接続を開始します。
- Storebrowse -S：サブスクライブされたリソースを一覧表示します。
- Storebrowse -T：指定されたストアのすべてのセッションを終了します。
- Storebrowse -Wr：指定されたストアの、切断されてもアクティブなセッションを再接続します。[r] オプションは、切断されたすべてのセッションを再接続します。
- storebrowse -WR：指定されたストアの、切断されてもアクティブなセッションを再接続します。[R] オプションは、すべてのアクティブなセッションと切断されたセッションを再接続します。
- Storebrowse -s：指定したストアのリソースをサブスクライブします。

- Storebrowse -u: 指定したストアのリソースのサブスクリプションを解除します。
- Storebrowse -q: 直接 URL を使用してアプリケーションを起動します。このコマンドは、StoreFront ストアでのみ機能します。

注:

- 前に使用したとおり (AuthMangerDaemon を使用して) 引き続き残りの Storebrowse コマンドを使用できます。
- この認証拡張機能は、クラウド展開でのみ適用されます。
- この機能強化により、永続ログイン機能がサポートされます。

詳しくは、「[認証の強化](#)」を参照してください。

### 永続ログイン (Technical Preview)

永続ログイン機能を使用すると、管理者が設定した期間 (2~365 日)、ログインしたままにすることができます。この機能が有効になっている場合、設定された期間中に Citrix Workspace アプリのログイン資格情報を入力する必要はありません。

この機能により、Citrix DaaS セッションへの SSO は、最大 365 日まで間延長されます。この拡張機能は、長期有効トークンの有効期間に基づいています。資格情報は、デフォルトで 4 日間または有効期間のいずれか短い方の期間、キャッシュされます。その後、Citrix Workspace アプリへの接続で 4 日以内にアクティブになったときに延長されます。

注:

Technical Preview は、お客様が非実稼働環境または制限のある稼働環境でテストし、フィードバックをご提供いただく機会を作るためのものです。機能プレビュー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としない場合があります。ベータ版のビルドは実稼働環境に展開しないことをお勧めします。

詳しくは、「[永続ログイン](#)」を参照してください。

### ストアのメールアドレスの自動検出

Citrix Workspace アプリでメールアドレスを指定することで、メールアドレスに関連付けられているストアを自動的に検出できるようになりました。ドメインに複数のストアが関連付けられている場合、デフォルトでは、Global App Configuration Service によって返される最初のストアが、最適なストアとして追加されます。ユーザーは必要に応じていつでも別のストアに切り替えることができます。

詳しくは、「[Citrix Workspace アプリへのストア URL の追加](#)」の「ストアのメールアドレスの自動検出」セクションを参照してください。

### 解決された問題

- インターネットアクセスが制限されている顧客環境の DNS サーバーでは、URL 「[clientstream.launchdarkly.com](#)」 が解決されない可能性があります。その結果、Citrix Workspace アプリは多数の DNS クエリをこの URL に送信します（1 日あたり 3 秒以内に 1000 超）。[CVADHELP-19559]
- App Protection 機能を有効にすると、`UIDialogLibWebKit3.so` ライブラリを使用する Authentication Manager インターフェイスで、キーロガー対策機能が動作しないことがあります。この問題は、GNOME および KDE デスクトップ環境では解決されています。[RFLNX-8027]
- Raspberry Pi ARMHF クライアントバージョン 3 または 4 で実行されている VDA セッションから印刷しようとする、セッションが応答しなくなることがあります。[CVADHELP-18506]
- デフォルト設定でセルフサービスユーザーインターフェイスを起動すると、次のエラーメッセージが表示されることがあります：

「Response for Secondary Token request is not 200/400/404 42」

この問題は、Fedora 35 で発生します。[RFLNX-8603]

## 2203

### 新機能

#### EDT IPv6 のサポート

このリリース以降、Citrix Workspace アプリでは EDT IPv6 がサポートされます。

#### TLS プロトコルバージョン 1.3 のサポート

このリリース以降、Citrix Workspace アプリは TLS (Transport Layer Security) プロトコルバージョン 1.3 をサポートします。

詳しくは、「[TLS](#)」を参照してください。

#### カスタム Web ストア

2203 より、Citrix Workspace アプリから組織のカスタム Web ストアにアクセスできます。

注：

マルチモニター画面レイアウト機能の固定は、カスタム Web ストアではサポートされていません。

詳しくは、「[カスタム Web ストア](#)」を参照してください。

#### 認証拡張機能 [試験段階の機能](#)

このリリース以降、認証拡張機能は次の操作で Storebrowse をサポートします：

- Storebrowse -E は利用可能なリソースを一覧表示します。
- Storebrowse -L は、公開リソースへの接続を開始します。
- Storebrowse -S は、サブスクライブされたリソースを一覧表示します。

注:

AuthMangerDaemonで残りの storebrowse コマンドを引き続き使用でき、将来のリリースで認証拡張機能がサポートされる予定です。

詳しくは、「[Storebrowse の認証拡張機能](#)」を参照してください。

### キーボードレイアウトの同期の強化

キーボードレイアウトの同期によって、クライアントデバイスの優先キーボードレイアウトを切り替えることができます。この機能はデフォルトでは無効になっています。有効にすると、クライアントのキーボードレイアウトが Citrix Virtual Apps and Desktops および Citrix DaaS (Citrix Virtual Apps and Desktops サービスの新名称) セッションに自動的に同期されます。

バージョン 2203 以降、Citrix Workspace アプリは次の 3 つの異なるキーボードレイアウトの同期モードをサポートします:

- セッション起動時に **1** 回だけ同期する - `wfclient.ini` ファイルの `KeyboardLayout` 値に応じて、セッション起動時にクライアントのキーボードレイアウトをサーバーに同期します。 `KeyboardLayout` 値が 0 に設定されている場合、システムキーボードは VDA に同期されます。 `KeyboardLayout` 値が特定の言語に設定されている場合、その言語固有のキーボードは VDA に同期されます。セッション中にクライアントのキーボードレイアウトに加えた変更は、すぐに有効になりません。変更を適用するには、アプリからサインアウトしてサインインし直します。 [セッション起動時に **1** 回だけ同期する] モードは、Citrix Workspace アプリ用に選択されたデフォルトのキーボードレイアウトです。
- 動的な同期を許可する - このオプションは、クライアントのキーボードレイアウトを変更したときに、クライアントのキーボードレイアウトをサーバーに同期します。
- 同期させない - クライアントがサーバーのキーボードレイアウトを使用することを示します。

詳しくは、「[キーボードレイアウトの同期](#)」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

Citrix Virtual Apps and Desktops 2112 以降で HDX による最適化が行われた場合、Microsoft Teams で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、「[Microsoft Teams Pop-Out Windows for Chats and Meetings](#)」を参照してください。

古いバージョンの Citrix Workspace アプリまたは Virtual Delivery Agent (VDA) を使用している場合は、シングルウィンドウモードが今後 Microsoft によって廃止されることに注意してください。ただし、複数のウィンドウをサポートするバージョンの VDA または Citrix Workspace アプリ (2203 以降) にアップグレードすることができます。より高いバージョンにアップグレードするには、この機能が一般提供されてから最低 9 か月かかります。



### 注:

この機能は、Microsoft Teams から以降の更新がロールアウトされた後にのみ使用できます。Microsoft によって更新プログラムがロールアウトされたら、ドキュメントのアップデートおよび発表について、[CTX253754](#)で確認できます。

### USB デバイスの自動リダイレクト機能の強化

以前は、セッション中にデバイスのプラグを抜き差しすると、デバイスは自動リダイレクトされ、VDA に自動的に接続されていました。このリリース以降、構成ファイルの設定を介して手動で自動リダイレクトを有効にする必要があります。USB デバイスの自動リダイレクトは、デフォルトでは無効になっています。詳しくは、「[USB](#)」セクションを参照してください。

### 解決された問題

- ストアを追加してそれを Citrix Workspace アプリで認証すると、認証が成功した後も、2 回目の認証ウィンドウが読み込まれます。この問題は、`AuthManLiteEnabled`を **True** に設定した後、Citrix Workspace アプリに最初にサインインしたときに発生します。[RFLNX-8694]
- `glibc` 2.34以降を使用する OS に App Protection 機能を有効にした Citrix Workspace アプリをインストールした後、システムの再起動時に OS の起動に失敗することがあります。[RFLNX-8358]
- Microsoft Teams を使用して P2P 呼び出しを行ったり、会議に参加したりしてしばらく待機すると、ソケットエラーのために 1 つの CPU コアの負荷が 100% に増加する場合があります。[HDX-38974]
- Citrix Workspace アプリは、Debian bullseye ベースの新しいバージョンの Raspberry Pi OS をサポートしません。[HDX-37000]
- ICA ファイルを使用してセッションを開始し、セッションからサインオフすると、`wfica`コマンドラインから受け取る戻り値は通常 0 です。しかし、この値を受け取る代わりに 2 を受け取ります。この問題は、Citrix Workspace アプリバージョン 2106 以降で発生します。[HDX-38916]
- Citrix Workspace アプリでは、Microsoft Teams で通話を送受信するときに、断続的に障害が発生する場合があります。次のエラーメッセージが表示されます:

「通話を確立できませんでした。」

[HDX-38819]

### 既知の問題

#### 2307 の既知の問題

- Ubuntu バージョン 22.04 で Debian パッケージマネージャーを使用して Linux 向け Citrix Workspace アプリをインストールすると、次のエラーが発生します:

**A dependency job for AppProtectionService-install.service failed. See 'journalctl -xe' for details.** (AppProtectionService-install.service の依存関係ジョブが失敗しました。詳しくは、'journalctl -xe' を参照してください。)

App Protection が正常にインストールされている場合でも、このエラーが発生します。[RFLNX-9995]

### 2305 の既知の問題

- Snipping Tool などのツールを使用すると、仮想アプリやデスクトップにカーソルの影が表示されることがあります。[CVADHELP-22336]
- Avaya WorkPlace を開くと、仮想アプリまたはデスクトップ画面に黒い枠線が残ります。[CVADHELP-21558]

### 2303 の既知の問題

- UI を使用して Citrix Workspace アプリをインストールすると、Ubuntu 20.04 および 22.04 に App Protection 機能をインストールできない場合があります。この問題を回避するには、コマンドラインインターフェイスを使用してアプリをインストールします。[APPP-1067]
- AllowMultistream値が Ubuntu 22.04 で **True** に設定されている場合、Citrix Workspace アプリバージョン 2303 でセッションを開始できないことがあります。[HDX-49916]
- スマートカードを使用すると、Linux 向け Citrix Workspace アプリバージョン 2303 への認証に失敗することがあります。この問題は、Red Hat、Ubuntu 22.04、および Debian 11 Linux ディストリビューションで発生します。[RFLNX-9620]
- アプリインジケータから Citrix Workspace アプリを終了すると、アプリが応答を停止し、次のエラーメッセージが表示されることがあります：

「GLib (gthread-posix.c): Unexpected error from C library during 'pthread\_setspecific': Invalid argument.」

この問題を回避するには、glib バージョン 2.76 以降を使用していることを確認してください。[RFLNX-9445]

### 2211 の既知の問題

- セッションを開始すると、トランザクション ID エラーメッセージが表示されることがあります。例：「The option “-transactionid” is invalid」(オプション「-transactionid」は無効です)。この問題を回避するには、**[OK]** をクリックしてメッセージボックスを閉じ、次に進みます。[HDX-45618]
  - Citrix Workspace アプリをインストールして起動すると、次のエラーメッセージが表示される場合があります：
- 「The X request 130.1 caused error:”10: BadAccess(Attempt to access private resource denied)」(X リクエスト 130.1 が原因でエラー: ”10: 不正アクセス (プライベートリソースへのアクセス試行が拒否されました))

[キャンセル] をクリックして、セッションを続行します。

この問題を回避するには、構成ファイル `$HOME/.ICAClient/wfclient.ini` に移動し、`IgnoreErrors=9,15` を `IgnoreErrors=9,15,32` に置き換えます。[HDX-44416]

- Citrix Workspace アプリからサインアウトして再度サインインすると、サインイン資格情報を入力せずに Citrix Workspace アプリが起動します。この問題は、クラウド環境で `longLivedTokenSupport` パラメーター値が `True` に設定されている場合にのみ発生します。この問題を回避するには、次のいずれかを実行します：

1. `/config/AuthManConfig.xml` ファイルに移動します。
2. [AuthManLite] セクションに移動し、次のエントリを更新します：

```
<longLivedTokenSupport>false</longLivedTokenSupport>
```

[RFLNX-9160]

## 2209 の既知の問題

- Microsoft Edge アプリセッションを開始すると、Microsoft Edge アイコンがさまざまなスケールでランダムに表示されます。このエラーは、次の設定を適用した場合に発生します：

- `DPIMatchingEnabled` 値が **True** に設定されている
- ディスプレイのクライアントスケールが 100% に設定されていない

[HDX-39764]

- スマートカード認証を使用してサーバー VDA セッションを開始しようとする、複数のユーザーが使用するスマートカードが失敗する場合があります。この問題が発生した場合は、カードを再挿入します。[HDX-44255]
- デバイスのインターフェイスをリダイレクトした後、VDA がクラッシュすることがあります。この問題は、Desktop Delivery Controller で「クライアント USB デバイスのリダイレクト」ポリシーを有効にし、複合 USB デバイス (USB ヘッドセットなど) をエンドポイントに接続すると発生します。また、`usb.conf` ファイルで入力値を `vid=** pid=** split=01 and intf=00,01` として追加します。その後、Citrix Workspace アプリからセッションを開始し、デバイスのインターフェイスをリダイレクトするように設定します。[HDX-44117]
- Debian 11 ベースの Raspberry Pi ARMHF OS では、セッションの起動に失敗する場合があります。Citrix では、Debian 11 ベースの Raspberry Pi ARM64 OS または Debian 10 ベースのそれ以前の Raspberry Pi ARMHF OS を使用することをお勧めします。[HDX-41729]
- プライマリアカウントを削除すると、サインイン資格情報がセルフサービスキャッシュから削除されない場合があります。その結果、資格情報を提供せずにストアにサインインできる場合があります。この問題を回避するには、セルフサービスを終了して資格情報を削除します。[RFLNX-9051]
- サインイン資格情報を提供してセルフサービスを開始すると、白い画面が表示されることがあります。この問題を回避するには、セルフサービスを終了して再起動します。[RFLNX-8951]

- OpenSUSE SLES 15 では、クラウドストアに接続すると画面上で歯車アイコンが回転し続ける場合があります。[RFLNX-9109]
- RHEL9 および Fedora 36 でセルフサービスの開始に失敗する場合があります。この問題を回避するには、`$ICAROOT/config/AuthManConfig.xml` ファイルで `AuthManLiteEnabled` の値が `False` に設定されていることを確認してください。[RFLNX-9128]

#### 2207 の既知の問題

- CAS データ収集に対する DNS ポーリングが、ICA の直接起動および CAS が無効なストアに対して発生する場合があります。[CVADHELP-20018]
- `storebrowse` コマンドを使用しているとき、2 番目のストアを追加して列挙すると、アプリまたはデスクトップを最初のストアから起動できない場合があります。この問題を回避するには、アプリやデスクトップを起動する前に、特定のストアを再度列挙する必要があります。[RFLNX-8953]
- デスクトップセッションで Windows Media Player を使用してビデオを再生すると、Rave ビデオ上でマウスカーソルが消える場合があります。この問題は、DDC でポリシーを次のように設定した場合にのみ発生します：
  - 「圧縮にビデオコーデックを使用する」が「領域をアクティブに変更」になっている
  - 「Windows メディアリダイレクト」が「許可」になっている（デフォルト設定）
  - 「ブラウザーコンテンツのリダイレクト」が「許可」になっている（デフォルト設定）
  - 「InvertCursorEnabled」が「BOTH」になっていて、次の値が `~/.ICAClient/wfclient.ini` ファイルに追加されている：
    - \* `InvertCursorEnabled=True`
    - \* `InvertCursorRefreshRate=60`
    - \* `InvertCursorMode=1`

[HDX-37259]

#### 2205 の既知の問題

- Linux 向け Citrix Workspace アプリ 2205 バージョンのエンドポイントを介して接続すると、セッションの切断の問題が発生する場合があります。この問題は、特定のデフォルトのロック画面イメージを強制するポリシー設定を使用して特定の種類の JPEG ファイルタイプでロック画面を構成し、Citrix VDA 2203 に適用する場合に発生します。この問題を回避するには、Citrix Workspace アプリのバージョン 2207 以降にアップグレードしてください。[CVADHELP-21572]
- TCP と EDT/UDP の接続試行中に 1 つのプロトコルで SSL エラーが発生した場合、競合状態が原因で両方の接続が失敗することがあります。この SSL エラーは、TLS 構成がプロトコル間で異なり、クライアントが 1 つのプロトコルを介して接続できない場合に発生する可能性があります。この問題を回避するには、ICA ファイルで `HDXoverUDP` 属性をオンまたはオフに設定します。[RFLNX-8747]

- HDX RealTime Webcam ビデオ圧縮は、Citrix Workspace アプリでの MJPEG ビデオ形式のカメラをサポートしていません。[HDX-40352]
- Citrix Workspace アプリのビデオまたは画像が正しくレンダリングされないことがあります。この問題は、Citrix Workspace アプリを VDA バージョン 2109 以降と一緒に使用した場合に発生します。この問題を回避するには、次のいずれかを実行します。
  1. Citrix Studio にサインインします。
  2. [圧縮にビデオコーデックを使用する] のポリシー設定を編集します。
  3. [値] ドロップダウンリストから [画面全体に使用] オプションを選択します。[HDX-40287]
- `storebrowse -a` コマンドを使用してストアを追加し、`storebrowse -E` コマンドを使用して列挙すると、Storebrowse 列挙が失敗することがあります。この問題は、Raspberry Pi OS でのみ発生します。この問題を回避するには、次のいずれかを実行します：
  1. 「/opt/Citrix/ICAClient/config/AuthmanConfig.xml」に移動します。
  2. 次のエントリを追加します：

```
1 <StorebrowseIPCDisabled> true</StorebrowseIPCDisabled>
2 <!--NeedCopy-->
```

### [RFLNX-8803]

- デフォルト設定でストアを追加すると、Storebrowse 列挙が失敗することがあります。この問題は、Debian 32 ビット OS でのみ発生します。この問題を回避するには、次のいずれかを実行します：
  1. 「/opt/Citrix/ICAClient/config/AuthmanConfig.xml」に移動します。
  2. 次のエントリを追加します：

```
1 <GnomeKeyringDisabled>true</GnomeKeyringDisabled>
2 <!--NeedCopy-->
```

### [RFLNX-8743]

- Citrix Workspace アプリの Debian パッケージを Ubuntu 22.04 LTS にインストールできないことがあります。この失敗は、ICAClient に必要な `libidn11` パッケージが Ubuntu 22.04 LTS に存在しないことが原因です。この問題を回避するには、Citrix Workspace アプリの Debian パッケージをインストールする前に、`libidn11` を Ubuntu 22.04 LTS に個別にインストールしてください。[RFLNX-8839]

## 2203 の既知の問題

- Ubuntu エンドポイントで公開された RDP (リモートデスクトッププロトコル) アプリケーションを複数のモニターを使用して起動すると、クライアントマシンに複数のモニターがある場合でも、1 つのモニターのみがコンテンツを表示します。RDP 経由でリモートデスクトップに接続する前に、RDP アプリケーションの表示オプションの [リモートセッションですべてのモニターを使用する] チェックボックスが選択されています。この問題は、シームレスモードおよびマルチモニター環境で発生します。[CVADHELP-16768]

- Citrix Workspace アプリは、リソースの列挙中に `Clientname` および `clientaddress` パラメーターを DDC に渡しません。その結果、クライアント名またはクライアント IP でフィルターされた `Set-BrokerAccessPolicyRule` が正しく機能しない可能性があります。[CVADHELP-17667]
- Skype で Web カメラを使用してビデオをプレビューすると、プレビューに黒い画面が表示される場合があります。[HDX-37860]

#### 2112 の既知の問題

- テキストを入力しようとする、カーソルが白く表示されます。この問題は、Linux エンドポイントマシンから接続された場合のダブルホップシナリオで発生します。[CVADHELP-16170]

#### 2111 の既知の問題

- クラウドストアにログオンすると、画面が白く表示される場合があります。[RFLNX-8337]
- Citrix Workspace アプリを起動しようとする、セルフサービスユーザーインターフェイスが開かず、次のエラーメッセージが表示されることがあります:

「User-defined signal 2」

この問題は、デバッグビルドと Azure VM Debian 10 で発生します。[RFLNX-8336]

#### 2109 の既知の問題

- Citrix Workspace アプリをアンインストールすると、`$HOME/.local/share/webkitgtk` にある古いキャッシュファイルが自動的に削除されない場合があります。この問題を回避するには、キャッシュファイルを手動で削除します。  
[HDX-28187]
- マルチポートポリシーが DDC で有効になっている場合、Citrix Workspace アプリを使用してデスクトップまたはアプリケーションを起動しようとする、失敗することがあります。[HDX-31016]
- スマートカード認証を使用してセッションを起動しようとする、失敗する場合があります。この問題は、Linux 向け Citrix Workspace アプリのバージョン 2104 以降で発生します。この問題を回避するには、スマートカードの資格情報を手動で入力します。[CVADHELP-18402]
- 自動クライアントの再接続中、セッションへの再接続の試行が 1 回しか行われない場合があります。その結果、クライアントの自動再接続ポリシーが正常に機能しない可能性があります。[HDX-34114]
- アプリケーションの起動の進行状況を表示する進行状況バーを閉じると、`wfica` プロセスが失敗する場合があります。その結果、アプリケーションが起動して画面から消えることがあります。[HDX-34701]

#### 2108 の既知の問題

- グローバルサーバー負荷分散 (GSLB) を使用している場合、ドメインネームシステム (DNS) の応答は、有効期間 (TTL) の間キャッシュされないことがあります。その結果、WebView を使用した認証が失敗する可能性があります。[RFLNX-3673]

#### 2106 の既知の問題

- デスクトップセッションでは、CEF-BCR を使用してページがリダイレクトされた後、キーボードのフォーカスが現在のマウスの位置に移動します。この問題は、オープンソース CEF に対するサードパーティの制限が原因で発生します。[RFLNX-7724]
- フォアグラウンドで別のアプリケーションを使用して BCR オーバーレイ (YouTube 検索など) をクリックしようとする、ブラウザページがフォアグラウンドに表示されません。[RFLNX-7730]
- CEF-BCR を使用してページがリダイレクトされた後、リダイレクトされた Web ページを閉じると、セグメンテーションエラーがエラーログに記録されます。[RFLNX-7667]

#### 2103 の既知の問題

- ビデオ通話または画面共有中に、Microsoft Teams が応答なくなり、通話が突然終了することがあります。[CVADHELP-16918]

#### 2101 の既知の問題

- Citrix Workspace アプリが Microsoft Teams で受信ビデオをレンダリングできない場合があります。[RFLNX-6662]

#### 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。

#### サードパーティ製品についての通知

Citrix Workspace アプリには、次のドキュメントで定義された条件の下でライセンスが有効になったサードパーティのソフトウェアが含まれている可能性があります。

[Linux 向け Citrix Workspace アプリのサードパーティ製品についての通知 \(PDF のダウンロード\)](#)

#### 試験段階の機能

Citrix では、新しいテクノロジーおよび機能が潜在的にどのくらい求められているか顧客のフィードバックを求めるとのメカニズムとして、試験段階の機能をリリースすることがあります。試験段階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います。重要度と重大度により、フィードバックに対応する場合としない場合があります。Citrix が試験段階な機能を製品化するとは限らず、理由の如何を問わず、いつでもこれらの機能を撤回する可能性があります。

## Technical Preview

September 15, 2023

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。

### 2308

#### ARM64 デバイスの **Web** カメラリダイレクトとサービス継続性のサポート

このリリース以降、Linux 向け Citrix Workspace アプリを実行する ARM64 アーキテクチャベースのエンドポイントデバイスで次の機能がサポートされます：

- Web カメラリダイレクト
- サービス継続性

詳しくは、「[ARM64 アーキテクチャのサポート](#)」を参照してください。

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

#### パケット損失補間を有効にしてオーディオパフォーマンスを向上 **[Technical Preview]**

このリリースでは、ジッターバッファメカニズムが向上し、Speex コーデックと Opus コーデックの両方にパケット損失補間 (PLC) が追加されました。強化されたジッターバッファメカニズムにより、順序が乱れたデータパッカーを検出し、それらを正しく並べ替えることができます。PLC は、失われたデータパケットの再構築に役立ちます。この機能強化により、パケット損失耐性とジッター耐性が向上し、EDT Lossy プロトコルと UDP でのオーディオパフォーマンスが向上します。デフォルトでは、この拡張機能は無効になっています。

この拡張機能を有効にするには、次の手順を実行します：

1. `/opt/Citrix/ICAClient/config/module.ini` 構成ファイルに移動して編集します。
2. 次のようにジッターバッファを有効にします：

```
1 JitterBufferEnabled = TRUE
2 <!--NeedCopy-->
```

3. 次のように PLC を有効にします：

```
1 PacketLossConcealmentEnabled=TRUE
2 <!--NeedCopy-->
```

4. **EDT Lossy プロトコル [Technical Preview]**機能または**UDP オーディオ**機能のサポートを有効にします。

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。



### マルチタッチのサポート **[Technical Preview]**

このリリース以降、Linux 向け Citrix Workspace アプリは、マルチタッチデバイスをサポートします。この機能により、デバイスはタッチスクリーンから入力を受信できるようになります。入力には、タッチジェスチャとペンまたはスタイラスデバイスを使用した操作が含まれます。HDX セッションでアプリまたはデスクトップを使用しているときに、マルチタッチスクリーンを操作できます。

タッチスクリーン上でサポートされている操作と対応するジェスチャは次のとおりです：

- 項目を **1** つ選択：タッチパッドをタップします。
- スクロール：2本の指をタッチパッド上に置き、水平または垂直にスライドさせます。
- ズームインまたはズームアウト：タッチパッドに2本の指を置き、ピンチインまたはピンチアウトします。
- さらにコマンドを表示（右クリックに相当）：タッチパッドを2本の指でタップするか、右下隅を押します。

既知の制限事項：

- セッション画面の保持はサポートされていません。つまり、タッチイベントのキャッシュは保存されません。
- Linux VDA ではサポートされません

既知の問題：

- マルチタッチは、表示モードが **Join Displays**（拡張モード）に設定されているマルチモニターではサポートされていません。[HDX-52394]
- ASUS タッチスクリーンでは、画面を指で押したままにすることができない場合があります。[HDX-52521]

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

### オンプレミスストアへの接続で **FIDO2** を使用した認証のサポート **[Technical Preview]**

このリリースでは、ユーザーは Linux 向け Citrix Workspace アプリを通じてオンプレミスストアにサインインするときに、パスワードなしの FIDO2 セキュリティキーを使用して認証できるようになります。このセキュリティキーは、セキュリティ PIN、生体認証、カード読み取り、スマートカード、公開キー証明書など、さまざまな形式のセキュリティ入力をサポートします。FIDO2 について詳しくは、「[FIDO2 認証](#)」を参照してください。

Citrix Workspace アプリは、FIDO2 認証にデフォルトのブラウザーとして Citrix Enterprise Browser を使用します。管理者は、Citrix Workspace アプリに対する認証を行うブラウザーの種類を構成できます。

この機能を有効にするには、`$ICAROOT/config/AuthManConfig.xml` に移動して次のエントリを追加します：

```
1 <key>FIDO2Enabled</key>
2 <value>true</value>
3 <!--NeedCopy-->
```

デフォルトのブラウザーを変更するには、`$ICAROOT/config/AuthManConfig.xml` に移動してブラウザーの設定を必要に応じて変更します。使用できる値は CEB、chromium、firefox、および chromium-browser です。

```
1 <FID02AuthBrowser>CEB</FID02AuthBrowser>
2 <!--NeedCopy-->
```

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

## 2307

### DTLS を使用した IPv6 UDT のサポート

以前は、Linux 向け Citrix Workspace アプリと仮想配信エージェント（VDA）の間の DTLS 接続は、IPv4 ネットワーク経由でのみサポートされていました。

このリリースでは、Citrix Workspace アプリは IPv4 と IPv6 の両方での DTLS 接続をサポートします。

この機能はデフォルトで有効になっています。

Linux 向け Citrix Workspace アプリで VDA との IPv6 DTLS 直接接続を使用する場合、追加の構成は不要です。

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

### ARM64 デバイスでの App Protection のサポート

App Protection は、Linux 向け Citrix Workspace アプリを実行している ARM64 アーキテクチャベースのデバイスでサポートされています。詳しくは、「ARM64 アーキテクチャのサポート」を参照してください。

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

## 2305

### TLS を使用した IPv6 TCP のサポート

以前は、Linux 向け Citrix Workspace アプリと仮想配信エージェント（VDA）の間の TLS 接続は、IPv4 ネットワーク経由でのみサポートされていました。

このリリースでは、Citrix Workspace アプリは IPv4 と IPv6 の両方での TLS 接続をサポートします。

この機能はデフォルトで有効になっています。

Linux 向け Citrix Workspace アプリで VDA との IPv6 TLS 直接接続を使用する場合、追加の構成は不要です。

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

### 32 ビットカーソルのサポートの機能強化

Linux 向け Citrix Workspace アプリのバージョン 2212 より、32 ビットカーソルへの対応がデフォルトで有効になりました。

このリリースより、32 ビットカーソルへの対応を無効にできるようになりました。この拡張により、`Cursor32bitSupport`という名前の新しいパラメーターが`wfclient.ini`ファイルに追加されます。

32 ビットカーソルのサポートを無効にするには、「32 ビットカーソルのサポート」のドキュメントを参照してください

この Technical Preview のフィードバックは、[Podio](#)フォームからお送りいただけます。

### オンプレミスストアへの接続で **FIDO2** を使用した認証のサポート [Technical Preview]

このリリースでは、ユーザーは Linux 向け Citrix Workspace アプリを通じてオンプレミスストアにサインインするときに、パスワードなしの FIDO2 セキュリティキーを使用して認証できるようになります。このセキュリティキーは、セキュリティ PIN、生体認証、カード読み取り、スマートカード、公開キー証明書など、さまざまな形式のセキュリティ入力をサポートします。FIDO2 について詳しくは、「[FIDO2 認証](#)」を参照してください。

Citrix Workspace アプリは、FIDO2 認証にデフォルトのブラウザとして Citrix Enterprise Browser を使用します。管理者は、Citrix Workspace アプリに対する認証を行うブラウザの種類を構成できます。

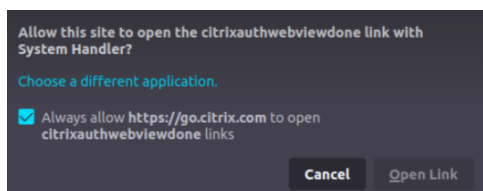
この機能を有効にするには、`$ICAROOT/config/AuthManConfig.xml`に移動して次のエントリを追加します:

```
1  `` `
2  <key>FIDO2Enabled</key>
3  <value>true</value>
4  <!--NeedCopy-->  `` `
```

デフォルトのブラウザを変更するには、`$ICAROOT/config/AuthManConfig.xml`に移動してブラウザの設定を必要に応じて変更します。使用できる値はCEB、`chromium`、`firefox`、および`chromium-browser`です。

```
1  `` `
2  <FIDO2AuthBrowser>CEB</FIDO2AuthBrowser>
3  <!--NeedCopy-->  `` `
```

ユーザー権限については、FIDO2 認証後に初めてブラウザを開いたときに、次のダイアログボックスが表示されます:



[**Always allow <https://go.citrix.com> to open citrixauthwebviewdone links**] チェックボックスをオンにし、[リンクを開く] をクリックします。

この Technical Preview のフィードバックは、[Podio](#)フォームからお送りいただけます。

### 2 つの仮想デスクトップ間でファイルとフォルダーをコピーして貼り付ける

以前は、2 つの仮想デスクトップ間でコピーできるのはテキストのみでした。このリリースでは、2 つの仮想デスクトップ間でファイルとフォルダーをコピーして貼り付けることができます。Linux Virtual Delivery Agent では、1 回のコピー/貼り付け操作でのデータの最大転送量は 200MB です。詳しくは、「[ファイルのコピーと貼り付け](#)」のドキュメントを参照してください。

この機能はデフォルトで有効になっています。

注:

2 つの仮想デスクトップ間でのファイルとフォルダーのコピーと貼り付けは、Linux 向け Citrix Workspace アプリを実行している x64 Linux ディストリビューションおよび ARM64 アーキテクチャベースのデバイスでのみサポートされます。

詳細については、「[2 つの仮想デスクトップ間でファイルとフォルダーをコピーして貼り付ける](#)」を参照してください。

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

### ARM64 アーキテクチャのサポート

このリリースより、Linux 向け Citrix Workspace アプリは、ARM64 アーキテクチャベースのデバイスをサポートします。この機能のために、インストーラーパッケージには、ARM64 ベースのデバイスに Citrix Workspace アプリをインストールできるようにするバイナリが含まれています。このインストーラーパッケージは、リソースの列挙、ICA の起動、およびオーディオリダイレクトのみをサポートします。前提条件とシステム要件は、他のアーキテクチャにアプリをインストールする場合と同じです。

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

### 最適化された **Microsoft Teams** でのハードウェアアクセラレーションへの対応

Linux 向け Citrix Workspace アプリは、Microsoft Teams ビデオ通話のパフォーマンスエクスペリエンスを改善します。

以前は、CPU はエンコーディングの目的のみで使用されていました。このリリースでは、GPU を使用して送信ビデオフレームをエンコードすることもできるため、CPU 使用率が削減されます。この機能は、限られた CPU リソースと予備の GPU を持つシンクライアントを使用する場合に役立ちます。

前提条件:

最新の GPU ドライバーの使用していない場合は、次のコマンドを使用して最新の GPU ドライバーをインストールします:

```
1  ````
2  sudo apt install va-driver-all
3  <!--NeedCopy-->  ````
```

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、次の手順を実行します：

1. `/var/.config/citrix/hdx_rtc_engine/config.json`ファイルに移動します。
2. 次の構成を設定します：

```
1  ````  
2  {  
3    "VideoHwEncode": 1,  }  
4  
5  <!--NeedCopy-->  ````
```

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

### 2302

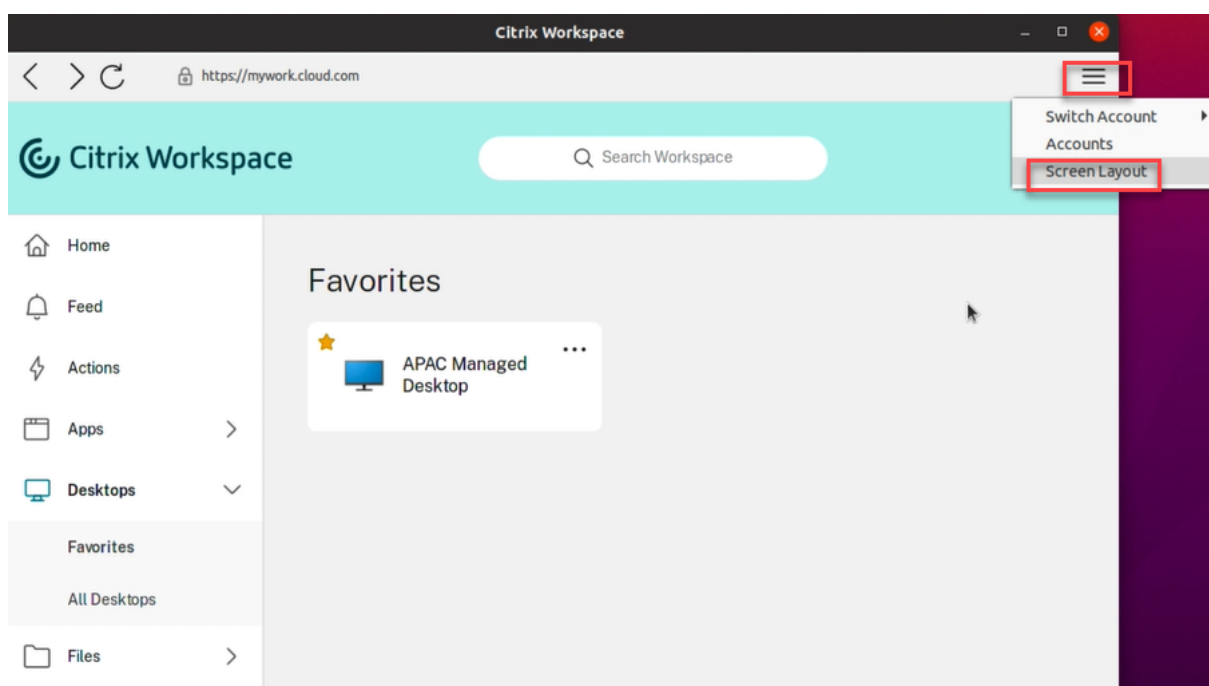
カスタム **Web** ストアでの画面の固定

バージョン 2302 以降、カスタム Web ストアでマルチモニター画面レイアウトの選択を保存できます。

前提条件として、`AuthManConfig.xml`ファイルでこの機能を有効にする必要があります。`$(ICAROOT)/config/AuthManConfig.xml`に移動し、次のエントリを追加します：

```
1 <key>ScreenPinEnabled</key>  
2 <value> true </value>  
3 <!--NeedCopy-->
```

上記のキーを追加して初めて、Citrix Workspace アプリメニューに [画面レイアウト] オプションが表示されます。



画面レイアウトを選択するには、Citrix Workspace アプリメニューで [画面レイアウト] を選択します。[画面レイアウト] ダイアログボックスが開きます。

ドロップダウンメニューから仮想デスクトップを選択します。レイアウトの選択は、選択したデスクトップにのみ適用されます。

1 つまたは複数のタイルを選択して、長方形のレイアウトを形成します。レイアウトの選択に従って、セッションが表示されます。

制限事項:

- 画面の固定を有効にすると、セッションのレイアウト保存機能が無効になります。
- この機能は、お気に入りのマークが付けられているデスクトップにのみ適用できます。

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

## 2212

### 32 ビットカーソルのサポート

以前は、カスタムの 32 ビットカーソルを使用していると、カーソルの周りに黒いボックスが表示されることがありました。

Linux 向け Citrix Workspace アプリのバージョン 2212 より、32 ビットカーソルへの対応がデフォルトで有効になりました。その結果、カーソルの周りの黒いボックスの問題が解決されました。

バージョン 2305 より、32 ビットカーソルへのサポートを無効にすることができます。この拡張により、`Cursor32bitSupport` という名前の新しいパラメーターが `wfclient.ini` ファイルに追加されます。

32 ビットカーソルへのサポートを無効にするには、次の手順を実行します:

1. 構成ファイル `$HOME/.ICAClient/wfclient.ini` に移動します。
2. [Thinwire3.0] セクションに移動し、次のエントリを設定します:

```
1 Cursor32bitSupport = False
2 <!--NeedCopy-->
```

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

### Citrix Optimized Microsoft Teams での背景のぼかしと置き換え

前提条件:

wget がインストールされていることを確認します。

Citrix Workspace アプリのバージョン 2212 以降、Linux 向け Citrix Workspace アプリの Citrix Optimized Microsoft Teams で、背景のぼかしと背景の置き換えがサポートされるようになりました。この機能を使用するには、会議中または P2P 呼び出し中に [More] > [Apply Background Effects] を選択します。

## 2209

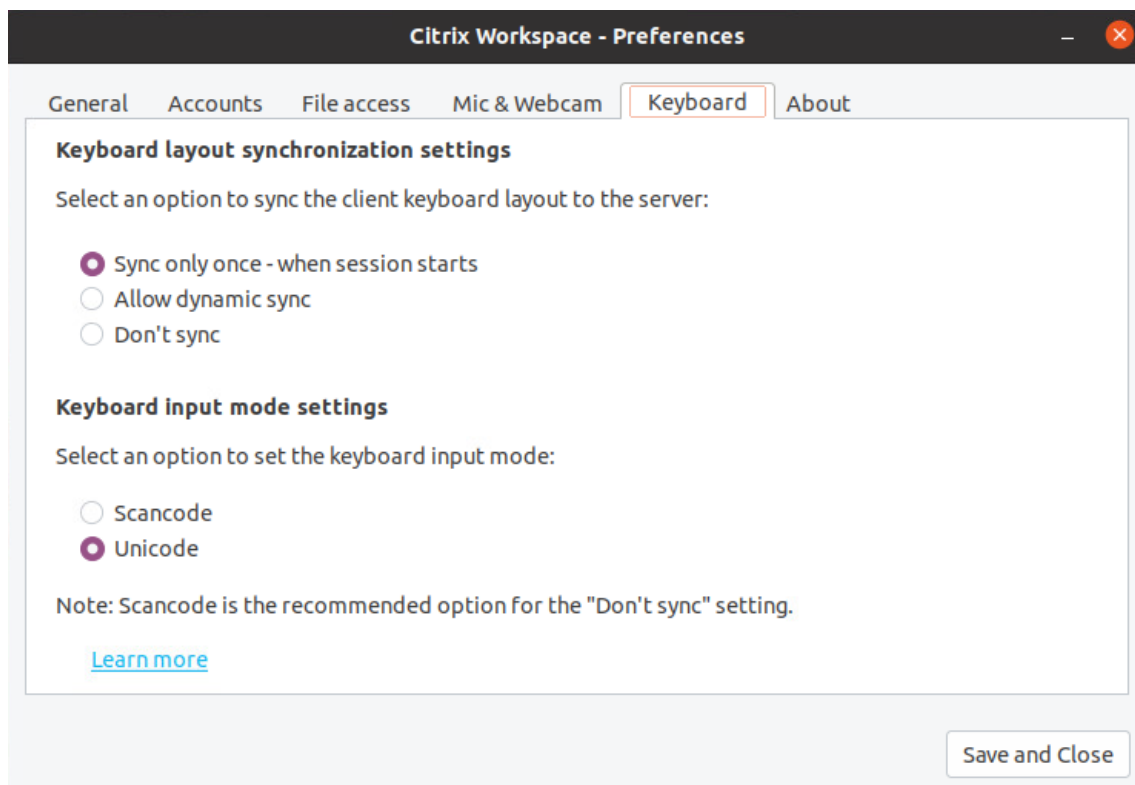
### キーボード入力モードの機能強化

以前は、構成ファイルの `KeyboardEventMode` の値を更新することによってのみ、さまざまなキーボード入力モードを有効にすることができました。キーボード入力モードを選択する UI オプションはありませんでした。

Citrix Workspace アプリ 2209 以降では、新しく導入された [キーボード入力モードの設定] セクションからさまざまなキーボード入力モードを構成できます。キーボード入力モードとして [スキャンコード] または [Unicode] を選択できます。

GUI を使用してキーボード入力モードを構成するには、次の手順を実行します：

1. システムトレイの Citrix Workspace アプリアイコンから [基本設定] を選択します。  
[Citrix Workspace - 基本設定] ダイアログボックスが開きます。
2. [キーボード] をクリックします。  
[キーボード入力モードの設定] セクションを確認できます。



3. 次のいずれかのオプションを選択します：

- [スキャンコード] - クライアント側のキーボードから VDA にキー位置を送信し、VDA が対応する文字を生成します。サーバー側のキーボードレイアウトを適用します。
- [Unicode] - クライアント側のキーボードから VDA にキーを送信し、VDA は同じ文字を生成します。クライアント側のキーボードレイアウトを適用します。

デフォルトでは、[キーボード入力モードの設定] は **[Unicode]** が選択されています。キーボード入力モードについて詳しくは、「[キーボードレイアウトの同期](#)」に関するドキュメントの「キーボードレイアウトの構成」セクションを参照してください。

4. [保存して閉じる] をクリックします。

注:

アプリケーションに再接続すると、キーボード構成の変更が有効になります。UI でキーボード入力モードを変更すると、`wfclient.ini` ファイル内の `KeyboardEventMode` のパラメーター値も自動的に更新されません。

たとえば、US インターナショナルキーボードレイアウトを使用しているときに、VDA がロシア語のキーボードレイアウトを使用しているシナリオを想定してみます。

[スキャンコード] を選択して Caps Lock の隣のキーを入力すると、スキャンコード `1E` が VDA に送信されます。次に、VDA は `1E` を使用して文字 `Ѡ` を表示します。

[Unicode] を選択して Caps Lock の隣のキーを入力すると、文字 `a` が VDA に送信されます。そのため、VDA がロシア語のキーボードレイアウトを使用している場合でも、文字 `a` が画面に表示されます。

### 拡張キーボードレイアウトのサポート

Citrix Workspace アプリバージョン 2209 以降、スキャンコードキーボード入力モードは、次の拡張キーボードレイアウトでサポートされます:

- 日本語 106 キーボード
- ポルトガル語 ABNT/ABNT2 キーボード
- マルチメディアキーボード

スキャンコードキーボード入力モードは、拡張キーボードレイアウトとすべてのキーボードレイアウト同期モードをサポートします。

このサポートはデフォルトでは有効になっています。

## 2207

### DPI マッチングのサポート

バージョン 2207 以降、Citrix Workspace アプリで設定された表示解像度と DPI スケール値は、仮想アプリとデスクトップセッションの対応する値と一致するようになります。Linux クライアントで必要なスケール値を設定でき、VDA セッションのスケールリングが自動的に更新されます。

DPI スケールリングは、主に大型で高解像度のモニターで使用されます。この機能によって、以下を快適なサイズで表示することができます:

- アプリケーション



- テキスト
- イメージ
- その他のグラフィック要素

注:

DPI マッチング機能は、GNOME、KDE、および Xfce デスクトップ環境のみをサポートします。

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、次の手順を実行します:

1. 構成ファイル `$HOME/.ICAClient/wfclient.ini` に移動します。
2. [WFClient] セクションに移動し、次のエントリを設定します:

```
DPIMatchingEnabled=TRUE
```

制限事項:

現在、DPI マッチング機能では、クライアント側での小数スケールリングはサポートされていません。

DPI スケール値が高い場合、Microsoft Teams の最適化が正常にサポートされない可能性があります。

## 2211

### カスタム Web ストアのサポート

このリリースでは、Citrix Workspace アプリから組織のカスタム Web ストアにアクセスできます。

この機能を使用するには、管理者はドメインまたはカスタム Web ストアを Global App Configuration Service で許可されている URL の一覧に追加する必要があります。URL の追加後、Citrix Workspace アプリの [アカウントの追加] 画面でカスタム Web ストアの URL を指定できます。カスタム Web ストアはネイティブの Workspace アプリウィンドウで開きます。

エンドユーザー向けの Web ストア URL の構成については、「[Global App Configuration Service](#)」を参照してください。

カスタム Web ストアを削除するには、[アカウント] > [アカウントの追加または削除] に移動して、カスタム Web ストアの URL を選択し、[削除] をクリックします。

前提条件として、`AuthManConfig.xml` ファイルでカスタム Web ストアを有効にする必要があります。詳しくは、「[カスタム Web ストア](#)」を参照してください。

注:

- カスタム Web ストアの `AuthManConfig.xml` ファイルで指定されている URL のみを使用できます。カスタム Web ストアで考慮する `AuthManConfig.xml` ファイルには、複数の URL を追加できます。
- Technical Preview は、お客様が非実稼働環境または制限のある稼働環境でテストし、フィードバックをご提供いただく機会を作るためのものです。機能プレビュー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としない場合があります。ベータ版のビルドは実稼働環境に展開しないことをお勧めします。

## 2109

### Google Chrome 用の Citrix Workspace Web 拡張機能によるサービス継続性のサポート

Google Chrome 用の Citrix Workspace Web 拡張機能によるサービス継続性のサポートは、Public Technical Preview 段階です。Google Chrome 用の Workspace Web 拡張機能は、Linux 向け Citrix Workspace アプリ 2109 で使用できます。この拡張機能は、[Google Chrome ウェブストア](#)で入手できます。Workspace アプリは、Web ブラウザー拡張機能用のネイティブメッセージングホストプロトコルを使用して、Citrix Workspace Web 拡張機能と通信します。Workspace アプリと Workspace Web 拡張機能は、Workspace 接続リースを使用して、停止中に Web ブラウザーユーザーがアプリとデスクトップにアクセスできるようにします。詳しくは、「[サービス継続性](#)」を参照してください。

### Global App Config Service

Citrix Workspace 向けの新しい Global App Configuration Service を使用すると、Citrix 管理者は、一元管理されたサービスによって Workspace Service の URL を配信できます。

前提条件として、AuthManConfig.xml ファイルでこの機能を有効にする必要があります。`$ICAROOT/config/AuthManConfig.xml`に移動し、次のエントリを追加します：

```
1 <key>AppConfigEnabled</key>
2 <value> true </value>
3 <!--NeedCopy-->
```

Workspace Service の URL の設定について詳しくは、「[Global App Configuration Service](#)」のドキュメントを参照してください。

注：

- Linux 向け Citrix Workspace アプリは、Global App Configuration Service のみを使用して Workspace Service の URL を配信します。

### Technical Preview から一般提供 (GA)

| 移行日 | サービスまたは機能 | 追加情報

|---|

システム要件と互換性

September 15, 2023

## 要件

### ハードウェア要件

#### **Linux** カーネル:

- バージョン 2.6.29 以降

#### ディスク領域:

- 55MB 以上
- ディスク上でインストールパッケージを展開/抽出する場合はさらに 110MB が必要
- HDX MediaStream Flash リダイレクトを使用する SoC (system-on-a-chip) デバイスでは、1GB 以上の RAM が必要

#### カラービデオディスプレイ:

- 256 色以上のビデオディスプレイ

### ライブラリとコーデック

#### ライブラリ:

- `glibcxx` 3.4.25 以降
- `glibc` 2.27 以降
- `gtk` 2 (2.20.1 以降)
- `libcap1` または `libcap2`
- `libjson-c` (計測用)
- X11 または X.Org (Wayland はサポートされていません)
- `udev` がサポートされている
- Advanced Linux Sound Architecture (ALSA) `libasound2`
- PulseAudio

#### セルフサービスユーザーインターフェイス:

- `webkit2gtk` 2.16.6 以降
- `libxml2` 2.7.8
- `libxerces-c` 3.1

#### コーデックライブラリ:

- Speex
- Vorbis コーデックライブラリ

#### **Red Hat Package Manager (RPM)** ベースの配布要件:

- `chkconfig`

ネットワークの要件

ネットワークプロトコル:

- TCP/IP

#### **H.264** 要件

**x86** デバイスの場合:

- プロセッサの速度 1.6GHz 以上

**HDX 3D Pro** 機能の場合:

- プロセッサの速度 2GHz 以上
- 高速グラフィックスドライバーを備えたネイティブハードウェア

**ARM** デバイスの場合:

- 通常の H.264 サポート機能および HDX 3D Pro 機能を使用する場合は、ハードウェア H.264 デコーダーが必要です。

#### **HDX MediaStream Flash** リダイレクト

HDX MediaStream Flash リダイレクトの要件については、Knowledge Center の[CTX134786](#)を参照してください。

最新機能およびセキュリティ上の修正を活用するには、新しいバージョンを展開する前に、この記事参照して最新のプラグインをテストすることをお勧めします。

認証の要件

クラウド認証用の、OpenSSL を使用した cURL 7.68 以降。

カスタマーエクスペリエンス向上プログラム (**CEIP**) の統合の要件

- [zlib](#) 1.2.3.3
- [libtar](#) 1.2 以降
- [libjson](#) 7.6.1 以降

#### **HDX RealTime Web** カメラビデオ圧縮の要件

- Video4Linux 互換 Web カメラ
- ディストリビューションの「plugins-good」パッケージを含む[GStreamer](#) 0.10.25 (または 0.10.x 以降)  
または

- ディストリビューションの「plugins-base」、「plugins-good」、「plugins-bad」、「plugins-ugly」、「gststreamer-libav」パッケージを含むGStreamer 1.0（または 1.x 以降）

#### **HDX MediaStream Windows Media** リダイレクトの要件

- ディストリビューションの「plugins-good」パッケージを含むGStreamer 0.10.25（または 0.10.x 以降）。通常は、HDX MediaStream Windows Media リダイレクトにはバージョン 0.10.15 以降で十分です。

または

- ディストリビューションの「plugins-base」、「plugins-good」、「plugins-bad」、「plugins-ugly」、「gststreamer-libav」パッケージを含むGStreamer 1.0（または 1.x 以降）

注:

- GStreamerが Linux ディストリビューションに含まれていない場合、[GStreamer](#) ページからダウンロードできます。
- 特定のコード（「plugins-ugly」のコードなど）の使用には、その製造元からのライセンスが必要な場合があります。詳しくは、システム管理者に問い合わせてください。

#### **Web** ブラウザーコンテンツのリダイレクトの要件

- webkit2gtk バージョン 2.16.6

#### **Philips SpeechMike** の要件

- Philips の Web サイトにアクセスして、関連するドライバーをインストールする

#### **App Protection** の要件

App Protection は、Gnome Display Manager と併せて、次のオペレーティングシステムで最適に機能します:

- 64 ビット Ubuntu 18.04、Ubuntu 20.04、および Ubuntu 22.04
- 64 ビット Debian 9 および Debian 10
- 64 ビット CentOS 7
- 64 ビット RHEL 7
- ARMHF 32 ビット Raspberry Pi OS (Debian 10 (buster) ベース)
- ARM64 Raspberry Pi OS (Debian 11 (bullseye) ベース)

注:

- バージョン 2204 より前の Citrix Workspace アプリを使用している場合、App Protection 機能はglibc 2.34 以降を使用するオペレーティングシステムをサポートしません。
- Ubuntu 20.04.5 以降では、.debパッケージファイルをダブルクリックすると、Snap Store インスト

ラーが開きます。このインストーラーは、ユーザープロンプトに対応していません。そのため、ターミナルでコマンドラインを使用するか、`gnome-software`、`gdebi`、`synaptics`などの他のソフトウェアインストーラーを使用して、Citrix Workspace アプリをインストールする必要があります。

### Microsoft Teams の最適化要件

最小バージョン:

- Citrix Workspace アプリ 2006

ソフトウェア:

- `GStreamer` 1.0 以降および `Cairo` 2
- `libc++-9.0` 以降
- `libgdk` 3.22 以降
- `OpenSSL` 1.1.1d
- x64 Linux ディストリビューション

ハードウェア:

- 1.8GHz 以上のデュアルコア CPU を搭載し、ピアツーピアのビデオ会議通話で 720p HD の解像度に対応している
- デュアルまたはクアッドコア CPU、基本速度 1.8GHz で、2.9GHz 以上の高速 Intel Turbo Boost を搭載している

認証の強化:

- `Libsecret` ライブラリ
- `libunwind-12` ライブラリ

サービス継続性の要件

バージョン 2106 以降、Citrix Workspace アプリの Debian バージョンにサービス継続性をインストールできます。

Citrix Workspace アプリをインストールする前に、ターミナルから次のコマンドを実行します:

```
sudo apt-get update -y
```

必須の事前インストールライブラリ:

- `libwebkit2gtk-4.0-37` バージョン 2.30.1 以降
  - Debian を使用している場合は、次のコマンドを実行します:

```
1 sudo apt-get install libwebkit2gtk-4.0-37
2 <!--NeedCopy-->
```

- RPM を使用している場合は、次のコマンドを実行します:

```
1 sudo yum install libwebkit2gtk-4*
2 <!--NeedCopy-->
```

- Ubuntu、RHEL、SUSE、Fedora、または Debian の場合、最新の libwebkit2gtk-4.0-37 バージョン 2.30.1 以降をインストールすることを Citrix ではお勧めします。
- Buster OS を搭載した Raspberry Pi の場合、libwebkit2gtk-4.0-37 バージョン 2.30.1 をインストールすることを Citrix ではお勧めします。

- gnome-keyring バージョン 3.18.3 以降

- Debian を使用している場合は、次のコマンドを実行します：

```
1 sudo apt-get install gnome-keyring
2 <!--NeedCopy-->
```

- RPM を使用している場合は、次のコマンドを実行します：

```
1 sudo yum install gnome-keyring
2 <!--NeedCopy-->
```

- Libsecret

- Debian を使用している場合は、次のコマンドを実行します：

```
1 sudo apt-get install libsecret-1-0
2 <!--NeedCopy-->
```

- RPM を使用している場合は、次のコマンドを実行します：

```
1 sudo yum install libsecret-1*
2 <!--NeedCopy-->
```

注：

1910 バージョン以降、オペレーティングシステムが次の GCC バージョン基準を満たしている場合にのみ、Citrix Workspace アプリが正常に動作します：

- x64 アーキテクチャ用の GCC バージョン： 4.8 以降
- ARMHF アーキテクチャ用の GCC バージョン： 4.9 以降

2101 バージョン以降、オペレーティングシステムが次の要件を満たしていない場合、Citrix Workspace アプリが正常に動作しないことがあります：

- GCC バージョン 4.9 以降
- glibcxx 3.4.20 以降

2209 バージョン以降、オペレーティングシステムが次の要件を満たしていない場合、Citrix Workspace アプリが正常に動作しないことがあります：

`glibcxx 3.4.25` 以降

### 互換性マトリックス

Citrix Workspace アプリは、Citrix 製品の現在サポートされているバージョンと互換性があります。

Citrix 製品のライフサイクル、および製品のバージョンごとのサポートが停止される時期については、[Citrix 製品マトリックス](#)を参照してください。

### サーバーの要件

#### StoreFront

- 現在サポートされているすべてのバージョンの Citrix Workspace アプリで、内部ネットワーク接続と Citrix Gateway の両方から StoreFront ストアにアクセスできます：
  - StoreFront 1811 以降。
  - StoreFront 3.12。
- StoreFront では、Web 向け Workspace を構成することができます。Web 向け Workspace が、Web ブラウザーから StoreFront ストアへのアクセスを提供します。この展開方法での制限事項については、StoreFront ドキュメントの「[重要な注意事項](#)」を参照してください。

### 接続と証明書

#### 接続

Linux 向け Citrix Workspace アプリでは、以下の構成のいずれかを介して、HTTP、HTTPS、および ICA-over-TLS 接続を確立できます。

- LAN 接続の場合：
  - StoreFront サービスまたは Web 向け Workspace を使用する StoreFront
- セキュアなリモート接続またはローカル接続の場合：
  - Citrix Gateway 12.0 以降
  - NetScaler Gateway 10.1 以降
  - NetScaler Access Gateway Enterprise エディション 10
  - NetScaler Access Gateway Enterprise エディション 9.x
  - NetScaler Access Gateway VPX

StoreFront でサポートされる Citrix Gateway のバージョンについては、StoreFront ドキュメントの「[システム要件](#)」を参照してください。



### 証明書

クライアントとサーバー間のトランザクションのセキュリティを保護するために、次の証明書を使用します：

#### プライベート（自己署名）証明書

リモートゲートウェイにプライベート証明書がインストールされている場合、ユーザーデバイスに組織の証明機関のルート証明書がインストールされている必要があります。このインストールは、Citrix Workspace アプリを使用して Citrix リソースにアクセスするのに役立ちます。

#### 注：

接続時にリモートゲートウェイの証明書を検証できない場合、信頼されていない証明書の警告が表示されます。ルート証明書がローカルのキーストアに含まれていないため、この検証は失敗する可能性があります。警告に対してそのまま続行することを選択した場合、アプリの一覧が表示されますが、アプリの起動に失敗することがあります。ルート証明書をクライアントの証明書ストアにインストールする必要があります。

#### ルート証明書

ドメイン参加マシンでは、グループポリシーオブジェクト管理用テンプレートを使用して CA 証明書を配布および信頼できます。

ドメイン非参加マシンでは、カスタムインストールパッケージを作成して、CA 証明書を配布およびインストールできます。詳しくは、システム管理者にお問い合わせください。

#### ユーザーデバイスへのルート証明書のインストール

TLS を使うには、サーバー証明書の証明機関の署名を確認するためのルート証明書がユーザーデバイスにインストールされている必要があります。Citrix Workspace アプリでは、デフォルトで以下の証明書がサポートされます。

証明書	証明機関
Class4PCA_G2_v2.pem	Verisign Trust Network
Class3PCA_G2_v2.pem	Verisign Trust Network
BTCTRoot.pem	Baltimore Cyber Trust Root
GTECTGlobalRoot.pem	GTE Cyber Trust Global Root
Pcs3ss_v4.pem	Class 3 Public Primary Certification Authority
GeoTrust_Global_CA.pem	GeoTrust
DigiCertGlobalRootCA.pem	DigiCert Global Root CA

### ワイルドカード証明書

ワイルドカード証明書は、同一ドメイン内の任意のサーバーで個別のサーバー証明書の代わりに使用します。Citrix Workspace アプリはワイルドカード証明書をサポートしますが、組織のセキュリティポリシーに従って使用する必要があります。

サブジェクトの別名 (SAN) 拡張内のサーバー名の一覧に含まれている証明書などのワイルドカード証明書に代わるものを考慮する必要がある場合があります。このような証明書は、私的証明機関および公的証明機関の両方が発行します。

### Citrix Gateway への中間証明書の追加

証明書チェーンに中間証明書が含まれる場合は、中間証明書を Citrix Gateway のサーバー証明書に追加する必要があります。詳しくは、Citrix Gateway ドキュメントの「[中間証明書の構成](#)」を参照してください。

お使いの StoreFront サーバーが使用している証明書と一致する中間証明書を提供できない場合、または中間証明書をインストールしてスマートカードユーザーをサポートする場合、StoreFront ストアを追加する前に次の手順を実行します：

- 1 つまたは複数の PEM 形式の中間証明書を別途入手します。

ヒント：

拡張子が.pem のファイルで証明書が見つからない場合は、`openssl`ユーティリティを使用して、証明書を拡張子が.pem のファイルに変換します。

2. パッケージ (通常は root) をインストールする場合：

- a) 1 つまたは複数のファイルを `$ICAROOT/keystore/intcerts` にコピーします。

- b) パッケージをインストールした後、次のコマンドを実行します：

```
$ICAROOT/util/ctx_rehash
```

### 共同サーバー証明書検証ポリシー

Citrix Workspace アプリには、サーバー証明書に関する厳格な検証ポリシーがあります。

重要：

このバージョンの Citrix Workspace アプリをインストールする前に、サーバーまたはゲートウェイの証明書が、ここで説明されているように正しく構成されていることを確認してください。以下の場合、接続できないことがあります：

- サーバーまたはゲートウェイの構成に間違ったルート証明書が含まれている
- サーバーまたはゲートウェイ構成にすべての中間証明書が含まれていない
- サーバーまたはゲートウェイ構成に期限切れまたは無効な中間証明書が含まれている
- サーバーまたはゲートウェイ構成にクロスルート用中間証明書が含まれていない

Citrix Workspace アプリは、サーバー証明書を検証するときにサーバー（またはゲートウェイ）が提供するすべての証明書を使用します。以前の Citrix Workspace アプリのバージョンと同様、証明書が信頼済みかについて確認します。信頼済みでない証明書がある場合、接続に失敗します。

このポリシーは、Web ブラウザーの証明書ポリシーより厳格です。多くの Web ブラウザーには、多数の信頼済みのルート証明書セットが含まれます。

サーバー（またはゲートウェイ）は、正しい証明書セットで構成する必要があります。不正な証明書のセットを使用すると、Citrix Workspace アプリの接続に失敗することがあります。

ゲートウェイがこれらの有効な証明書で構成されている場合は、次の構成を使用してより厳密な検証を行います。この構成により、Citrix Workspace アプリがどのルート証明書を使用するかが正確に決定します：

- サーバー証明書サンプル
- 中間証明書サンプル
- ルート証明書サンプル

Citrix Workspace アプリは、これらすべての証明書が有効であることを確認します。また、ルート証明書サンプルを信頼済みであることも確認します。Citrix Workspace アプリがルート証明書サンプルを信頼していない場合、接続に失敗します。

**重要：**

- 証明機関によっては、複数のルート証明書があります。このような、より厳格な検証が必要であれば、構成で適切なルート証明書が使用されていることを確認してください。たとえば、現在同じサーバー証明書を検証できる 2 つの証明書（DigiCert/GTE CyberTrust Global Root および DigiCert Baltimore Root/Baltimore CyberTrust Root）があるとします。ユーザーデバイスによっては、両方のルート証明書が使用できます。その他のデバイスでは、1 つの証明書のみを使用できます（DigiCert Baltimore Root/Baltimore CyberTrust Root）。
- ゲートウェイで GTE CyberTrust Global Root 証明書を構成すると、これらのユーザーデバイスで Citrix Workspace アプリの接続に失敗します。どのルート証明書を使用すべきかについては、証明機関のドキュメントを参照してください。また、ルート証明書の有効期限についても注意してください。
- サーバーやゲートウェイによっては、ルート証明書が構成されていても、送信しないことがあります。この場合、より厳格な検証は機能しません。

ゲートウェイがこれらの有効な証明書で構成されている場合、ルート証明書を省略して次の構成を使用できます：

- サーバー証明書サンプル
- 中間証明書サンプル

Citrix Workspace アプリはこれら 2 つの証明書を使用します。ユーザーデバイスでルート証明書を検索します。Citrix Workspace アプリが、正しく検証された信頼済みのルート証明書（ルート証明書サンプルなど）を見つけた場合、接続は成功します。信頼済みの証明書が見つからない場合は、失敗します。この構成では、Citrix Workspace アプリが必要とする中間証明書が提供されますが、Citrix Workspace アプリは任意の有効な、信頼済みのルート証明書を選択できます。

以下は、ゲートウェイがこのような証明書で構成されていることを前提としています：

- サーバー証明書サンプル
- 中間証明書サンプル
- 間違ったルート証明書

Web ブラウザーは、不正なルート証明書を無視することがありますが、Citrix Workspace アプリは不正なルート証明書を無視しないため、接続は失敗します。

証明機関によっては、複数の中間証明書を使用します。この場合ゲートウェイは、以下のようにすべて中間証明書（ルート証明書ではない）で構成されます：

- サーバー証明書サンプル
- 中間証明書サンプル 1
- 中間証明書サンプル 2

**重要：**

- 証明機関によっては、クロスルート用中間証明書を使用します。この証明書は、複数のルート証明書があり、以前のルート証明書が最新のルート証明書と同時に使用中の状況を想定しています。この場合、少なくとも 2 つの中間証明書が存在します。たとえば、以前のルート証明書 *Class 3 Public Primary Certification Authority* には、関連するクロスルート用中間証明書 *Verisign Class 3 Public Primary Certification Authority - G5* があります。ただし、ルート証明書 *Verisign Class 3 Public Primary Certification Authority - G5* も利用可能であり、*Class 3 Public Primary Certification Authority* に置き換わります。最新のルート証明書はクロスルート用中間証明書を使用しません。
- クロスルート用中間証明書とルート証明書は、同じサブジェクト名（発行先）です。ただし、クロスルート用中間証明書は、発行者名（発行元）が異なります。この違いによって、クロスルート用中間証明書と通常の間接証明書（中間証明書サンプル 2 など）を区別できます。

このルート証明書およびクロスルート用中間証明書を省略した構成が推奨されます：

- サーバー証明書サンプル
- 中間証明書サンプル

クロスルート用中間証明書をゲートウェイで構成しないでください。これは、ゲートウェイで以前のルート証明書が選択されるようになるのを避けるためです：

- サーバー証明書サンプル
- 中間証明書サンプル
- クロスルート用中間証明書サンプル（非推奨）

ゲートウェイでサーバー証明書のみを構成しないでください：

- サーバー証明書サンプル

この場合、Citrix Workspace アプリはすべての中間証明書を検出できないため、接続に失敗します。

### SSL 接続用のシステム証明書パスのサポート

Citrix Workspace アプリバージョン 2308 は、SSL 接続用のシステム証明書パスをサポートします。この機能により、クライアント側の証明書管理プロセスがシンプルになり、ユーザーエクスペリエンスが向上します。この機能を使用すると、Citrix Workspace はシステム証明書パス内の証明書を使用して TLS 接続を作成できます。この機能はデフォルトで有効になっています。

### Workspacecheck

Citrix Workspace アプリインストールパッケージの一部として `workspacecheck.sh` スクリプトが提供されています。このスクリプトは Citrix Workspace アプリの機能をサポートするすべてのシステム要件をデバイスが満たしているかどうかをチェックします。スクリプトはインストールパッケージの `Utilities` ディレクトリにあります。

#### Workspacecheck.sh スクリプトを実行するには

1. Linux マシンでターミナルを開きます。
2. `cd $ICAROOT/util` と入力して **Enter** キーを押し、インストールパッケージの `Utilities` ディレクトリに移動します。
3. `./workspacecheck.sh` と入力してスクリプトを実行します。

#### サポート外のアプリケーションとオペレーティングシステム

Citrix は、ベンダーによってサポートされなくなったアプリケーションおよびオペレーティングシステムについてはサポートを提供しません。

報告された問題の対処と解決を試みている間、Citrix は問題がサポート対象外のアプリケーションやオペレーティングシステムに直接関連しているかどうかを評価します。その判断に役立つため、サポートされているバージョンのアプリケーションおよびオペレーティングシステムを使用して問題を再現できるかどうか試していただくよう、Citrix からお願いをすることがあります。問題がサポート対象外のアプリケーションやオペレーティングシステムに関連していると思われる場合、Citrix が問題をさらに調査することはありません。

#### インストール、アンインストール、更新

September 15, 2023

Citrix Web サイトの [\[ダウンロード\]](#) からファイルをダウンロードすることで、Citrix Workspace アプリをインストールできます。

## Citrix Workspace アプリのバージョン確認

システムにインストールされている Citrix Workspace アプリの現在のバージョンを確認するには、次の手順を実行します：

1. ターミナルウィンドウを開きます。
2. 次のコマンドを実行します：

Debian パッケージの場合：

```
1 dpkg --get-architecture | grep -i icaclient
2 <!--NeedCopy-->
```

または

```
1 cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
2 <!--NeedCopy-->
```

Red Hat パッケージの場合：

```
1 rpm -qa | grep -i icaclient
2
3 <!--NeedCopy-->
```

または

```
1 cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
2 <!--NeedCopy-->
```

Tarball パッケージの場合：

```
1 cat /opt/Citrix/ICAClient/pkginf/Ver.core.linuxx64
2 <!--NeedCopy-->
```

## 手動インストール

[Citrix のダウンロード](#) ページから次のパッケージをダウンロードします。

### Debian パッケージ

使用マシンの OS アーキテクチャに応じて、`Icaclient` パッケージをインストールします。

汎用 USB リダイレクトを使用するには、使用マシンの OS アーキテクチャに適したいずれかの `ctxusb` パッケージをインストールします。

注:

互換性の問題を回避するには、必ず同じバージョンの `Icaclient` と `ctxusb` パッケージをインストールしてください。

パッケージ名	コンテンツ
<b>Debian</b> パッケージ ( <b>Ubuntu</b> 、 <b>Debian</b> 、 <b>Linux Mint</b> など)	
<code>icaclient_&lt;version&gt;_amd64.deb</code>	セルフサービスサポート、64 ビット x86_64
<code>icaclient_&lt;version&gt;_i386.deb</code>	セルフサービスサポート、32 ビット x86
<code>icaclient_&lt;version&gt;_armhf.deb</code>	セルフサービスサポート、ARM HF
<code>ctxusb_&lt;version&gt;_amd64.deb</code>	USB パッケージ、64 ビット x86_64
<code>ctxusb_&lt;version&gt;_i386.deb</code>	USB パッケージ、32 ビット x86
<code>ctxusb_&lt;version&gt;_armhf.deb</code>	USB パッケージ、ARM HF

#### Debian パッケージを使用したインストール

前提条件:

[システム要件](#)に関するセクションに記載されているように、必要なシステム要件をすべてインストールしたことを確認します。

Ubuntu 上に Citrix Workspace アプリを Debian パッケージでインストールする場合は、Ubuntu ソフトウェアセンターでパッケージを開きます。

以下の手順で、

**`packagename`** にインストールするパッケージの名前を指定します。

このプロシージャではコマンドラインと Ubuntu、Debian、または Mint 用のネイティブパッケージマネージャーを使用します。また、ファイルブラウザでダウンロードした `.deb` パッケージをダブルクリックしてパッケージをインストールすることもできます。通常、これによりパッケージマネージャーが起動して、必要なソフトウェアが自動的にダウンロードされます。パッケージマネージャーを使用できない場合は、コマンドラインツール **`gdebi`** を使用することを Citrix ではお勧めします。

注:

Ubuntu 20.04.5 以降では、`.deb` パッケージファイルをダブルクリックすると、Snap Store インストーラーが開きます。このインストーラーは、ユーザープロンプトに対応していません。そのため、ターミナルでコマンドラインを使用するか、`gnome-software`、`gdebi`、`synaptics`などの他のソフトウェアインストーラーを使用して、Citrix Workspace アプリをインストールする必要があります。

コマンドラインを使ってパッケージをインストールするには:

1. スーパーユーザー (root) としてログオンします。
2. ターミナルウィンドウを開きます。
3. 次のいずれかのコマンドを使用してインストールを実行します:

- **apt** - 次のコマンドを使用して、Citrix Workspace アプリと依存関係をインストールします:

```
1 sudo apt install -f ./icaclient_<version>._amd64.deb
2 <!--NeedCopy-->
```

USB パッケージをインストールするには、次のコマンドを実行します:

```
1 sudo apt install -f ctxusb_<version>._amd64.deb
2 <!--NeedCopy-->
```

- **dpkg -i** - 次のコマンドを使用して、Citrix Workspace アプリをインストールします:

```
1 sudo dpkg -i icaclient_<version>_amd64.deb
2 sudo apt-get -f install
3 <!--NeedCopy-->
```

USB パッケージをインストールするには、次のコマンドを実行します:

```
1 sudo dpkg -i ctxusb_<version>_amd64.deb
2 sudo apt-get -f install
3 <!--NeedCopy-->
```

- **gdebi** - 次のコマンドを使用して、Citrix Workspace アプリをインストールします:

```
1 gdebi icaclient_<version>_amd64.deb
2 <!--NeedCopy-->
```

USB パッケージをインストールするには、次のコマンドを実行します:

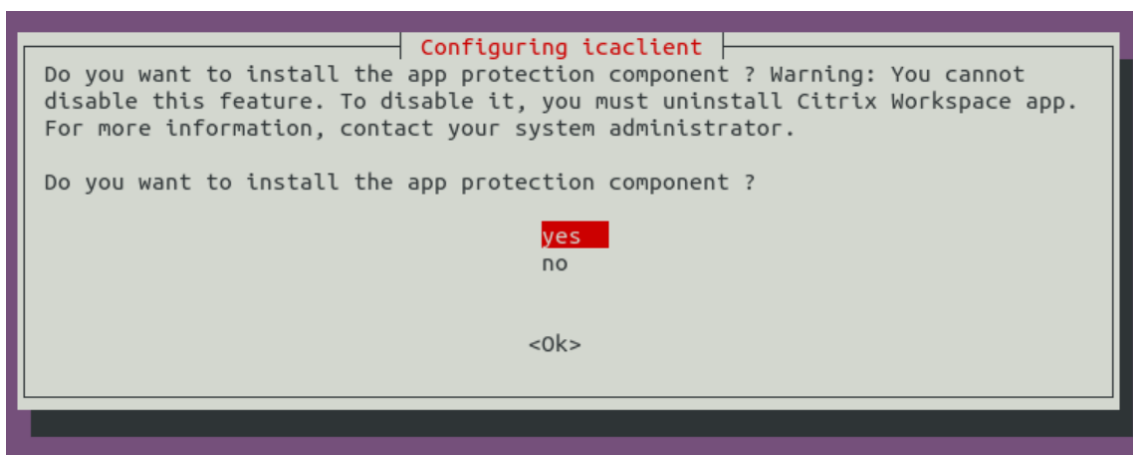
```
1 gdebi ctxusb_<version>_amd64.deb
2 <!--NeedCopy-->
```

注:

必要に応じて、**ctxusb**パッケージで汎用 USB リダイレクト機能をサポートします。

4. バージョン 2101 以降、App Protection をインストールするように求める次のインタラクティブなプロンプトが表示されます:





5. [はい] を選択して、App Protection コンポーネントのインストールを続行します。

### Debian パッケージへの App Protection コンポーネントのサイレントインストール

バージョン 2102 以降、Citrix Workspace アプリの Debian バージョンで App Protection がサポートされています。

App Protection コンポーネントをサイレントインストールするには、Citrix Workspace アプリをインストールする前に、ターミナルから次のコマンドを実行します：

```
1 export DEBIAN_FRONTEND="noninteractive"
2 <!--NeedCopy-->
```

```
1 sudo debconf-set-selections <<< "icaclient app_protection/
install_app_protection select yes"
2 <!--NeedCopy-->
```

```
1 sudo debconf-show icaclient
2 <!--NeedCopy-->
```

```
1 sudo apt install -f ./icaclient_<version>._amd64.deb`
2
3 <!--NeedCopy-->
```

### Red Hat パッケージ

使用マシンの OS アーキテクチャに応じて、ICAClient パッケージをインストールします。

汎用 USB リダイレクトを使用するには、使用マシンの OS アーキテクチャに適したいずれかの ctxusb パッケージをインストールします。

注:

互換性の問題を回避するには、必ず同じバージョンの `Icaclient` と `ctxusb` パッケージをインストールしてください。

パッケージ名	コンテンツ
<b>Redhat</b> パッケージ ( <b>Redhat</b> 、 <b>SUSE</b> 、 <b>Fedora</b> など)	
<code>ICAClient-rhel-&lt;version&gt;.x86_64.rpm</code>	セルフサービスサポート、Red Hat (Linux VDA を含む) ベース、64 ビット x86_64
<code>ICAClient-rhel-&lt;version&gt;.i386.rpm</code>	セルフサービスサポート、Red Hat ベース、32 ビット x86
<code>ICAClient-suse-&lt;version&gt;.x86_64.rpm</code>	セルフサービスサポート、SUSE ベース、64 ビット x86_64
<code>ICAClient-suse-&lt;version&gt;.i386.rpm</code>	セルフサービスサポート、SUSE ベース、32 ビット x86
<code>ctxusb-&lt;version&gt;.x86_64.rpm</code>	USB パッケージ、64 ビット x86_64
<code>ctxusb-&lt;version&gt;.i386.rpm</code>	USB パッケージ、32 ビット x86

注:

SuSE 11 SP3 Full Package (Self-Service Support) RPM パッケージは廃止されました。

### RPM パッケージを使用したインストール

Citrix Workspace アプリを SUSE の RPM パッケージからインストールしている場合は、YaST または Zypper コーティリティを使用します。RPM コーティリティは、`.rpm` パッケージをインストールします。必要な従属ソフトウェアが見つからない場合、エラーが発生します。

ヒント:

RPM Package Manager では、必要なソフトウェアが自動的にダウンロードされません。

- SUSE を使用している顧客の場合、OpenSUSE のコマンドラインで `zypper install <filename>` を使用してソフトウェアをダウンロードしてインストールします。
- Red Hat を使用している顧客の場合、Fedora/Red Hat で `yum localinstall <filename>` を使用してソフトウェアをダウンロードし、インストールします。

### RPM パッケージからインストールするには

前提条件:

システム要件に関するセクションに記載されているように、必要なシステム要件をすべてインストールしたことを確認します。

1. EPEL リポジトリを設定します。

注:

RHEL および CentOS の場合、Linux VDA を正常にインストールする前に、EPEL リポジトリをインストールします。EPEL のインストール方法については、[手順](#)を参照してください。

2. スーパーユーザー (root) としてログオンします。
3. ターミナルウィンドウを開きます。
4. に「Zypper」と入力して、次の3つのパッケージのインストールを実行します。

```
> ** 注: **
```

```
>
```

```
> - 'ctxusb' パッケージはオプションです。汎用 USB リダイレクト機能をサポートするには、このパッケージをインストールしてください。
```

```
> - 'ctxappprotection' パッケージはオプションです。App Protection コンポーネントをインストールする場合にのみ、このパッケージをインストールしてください。
```

```
**SUSE のインストールの場合: **
```

```
- 'zypper in ICAClient-suse-.x86_64.rpm'
```

```
- 'zypper in ctxusb-.x86_64.rpm'
```

```
- 'zypper in ctxappprotection-.x86_64.rpm'
```

```
**Red Hat のインストールの場合: **
```

```
- 'yum localinstall ICAClient-rhel-.x86_64.rpm'
```

```
- 'yum localinstall ctxusb-.x86_64.rpm'
```

```
- 'yum localinstall ctxappprotection-.x86_64.rpm'
```

不足しているパッケージをインストールするには

Red Hat ベースのディストリビューション (RHEL、CentOS、Fedora など) で、次のエラーメッセージが表示される場合、EPEL リポジトリを追加します (詳細は<https://docs.fedoraproject.org/en-US/epel/>を参照してください):

```
1  “... requires libwebkitgtk-1.0.so.0”
```

## Tarball パッケージ

使用マシンの OS アーキテクチャに応じて、次のいずれかのパッケージをインストールします。

パッケージ名	コンテンツ
<b>Tarball</b> (任意のディストリビューション用のスク립トインストール)	
<code>linuxx64-&lt;version&gt;.tar.gz</code>	64 ビット Intel
<code>linuxx86-&lt;version&gt;.tar.gz</code>	32 ビット Intel
<code>linuxarmhf-&lt;version&gt;.tar.gz</code>	ARM HF

## 注:

- Citrix Workspace アプリをインストールするディレクトリをカスタマイズする場合は、Tarball パッケージを使用します。必要なパッケージを自動的にインストールする場合は、Debian パッケージまたは RPM パッケージから Citrix Workspace アプリをインストールします。
- 同じマシンで 2 種類のインストール方法を使用しないでください。使用した場合、エラーメッセージが表示され問題が発生する可能性があります。

**Tarball** パッケージを使用したインストール

## 注:

Tarball パッケージは依存関係のチェックまたは依存関係のインストールを実行しません。すべてのシステムの依存関係は、別個に解決される必要があります。

1. ターミナルウィンドウを開きます。
2. `.tar.gz` ファイルの内容を抽出して、その内容を空のディレクトリに保存します。たとえば、次のように入力します: `tar xvfz packagename.tar.gz`。
3. 「`./setupwfc`」と入力して Enter キーを押し、セットアッププログラムを実行します。
4. デフォルトの 1 (Citrix Workspace アプリのインストール) を選択して **Enter** キーを押します。
5. 必要なインストールディレクトリのパスおよび名前を入力して Enter キーを押します。または、Enter キーを押して Citrix Workspace アプリをデフォルトの場所にインストールします。

スーパーユーザー (root) のデフォルトのインストールディレクトリは、`/opt/Citrix/ICAClient` です。

非スーパーユーザーのデフォルトのインストールディレクトリは、`$HOME/ICAClient/platform` です。platform は、システムにより生成されるオペレーティングシステム ID で、たとえば Linux/x86 の場合は `$HOME/ICAClient/linuxx86` のようになります。

## 注:

デフォルトのインストール先以外のディレクトリにインストールする場合は、`$HOME/.profile` また

は `$HOME/.bash\_\_profile` の `$ICAROOT` にそのディレクトリを設定します。

6. インストールを続行するには、「y」を入力し、Enter キーを押します。
7. Citrix Workspace アプリをデスクトップ環境に統合するかどうかを選択できます。これにより、Citrix Workspace アプリを起動するためのメニューオプションがデスクトップ環境に作成されます。「y」と入力すると、デスクトップ統合が有効になります。
8. GStreamer がインストール済みの場合は、GStreamer を Citrix Workspace アプリに統合するかどうかを選択でき、HDX MediaStream マルチメディアアクセラレーションをサポートできます。Citrix Workspace アプリを GStreamer に統合する場合は、「y」と入力します。

注:

一部のプラットフォームでは、tarball パッケージからクライアントをインストールすると、KDE および GNOME への統合を求めるプロンプトが表示された後でシステムが応答しなくなることがあります。この問題は、gststreamer-0.10 を初めて初期化する場合に発生します。この問題が発生した場合、(Ctrl+C を用いて) インストール処理を中断し、コマンド `gst-inspect-0.10 -- gst-disable-registry-fork --version` を実行します。コマンドの実行後、問題が発生することなく tarball パッケージを再実行できます。

9. スーパーユーザー (root) としてログオンしている場合、Citrix Virtual Apps and Desktops または Citrix DaaS (Citrix Virtual Apps and Desktops サービスの新名称) の公開 VDI アプリケーションで USB サポートのインストールを選択できます。「y」と入力すると、USB サポートがインストールされます。

注:

スーパーユーザー (root) としてログオンしていない場合、次の警告が表示されます:

「USB support cannot be installed by non-root users. Run the installer as root to access this install option. (root 以外のユーザーは USB サポートをインストールできません。この機能を使用する場合は、スーパーユーザーとしてインストーラーを実行してください。)」

10. インストールが完了すると、メインのインストールメニューに戻ります。セットアッププログラムを終了するには、「3」を入力して Enter キーを押します。

## アンインストール

環境変数 `ICAROOT` はクライアントのインストールディレクトリに設定する必要があります。非スーパーユーザーのデフォルトのインストールディレクトリは、`$HOME/ICAClient/platform` です。platform は、システムにより生成されるオペレーティングシステム ID で、たとえば Linux/x86 の場合は `$HOME/ICAClient/linuxx86` のようになります。権限を持つユーザーのインストールでは、デフォルトが `/opt/Citrix/ICAClient` です。

注:

- Citrix Workspace アプリをアンインストールするには、インストール時と同じユーザーアカウントでシステムにログオンする必要があります。

- Citrix Workspace アプリをアンインストールすると、`$HOME/.local/share/webkitgtk`にある古いキャッシュファイルが自動的に削除されない場合があります。回避策としては、キャッシュファイルを手動で削除します。

**Tarball** パッケージで **Citrix Workspace** アプリをアンインストールするには

1. `$ICAROOT/setupwfc`と入力して Enter キーを押し、セットアップを実行します。
2. クライアントを削除するには、2と入力して **Enter** キーを押しします。

**Debian/Ubuntu** オペレーティングシステムで **Citrix Workspace** アプリをアンインストールするには

1. ターミナルウィンドウを開きます。
2. 次のいずれかのコマンドを使用してインストールを実行します:

```
1 sudo apt remove icaclient -y
2 <!--NeedCopy-->
```

```
1 sudo apt autoremove -y
2 <!--NeedCopy-->
```

または

```
1 sudo apt remove icaclient -y
2 <!--NeedCopy-->
```

```
1 sudo apt purge icaclient -y
2 <!--NeedCopy-->
```

注:

オペレーティングシステム側の標準的なツールを使用して Debian パッケージを削除することもできます。

**Fedora/RHEL/CentOS** オペレーティングシステムで **Citrix Workspace** アプリをアンインストールするには

1. ターミナルウィンドウを開きます。
2. 次のコマンドを使用してインストールを実行します:

```
1 yum remove icaclient -y
2 <!--NeedCopy-->
```

### 注:

オペレーティングシステム側の標準的なツールを使用して RPM パッケージを削除することもできます。

Citrix Workspace アプリが正常にアンインストールされたかどうかを確認します。詳しくは、「[Citrix Workspace アプリのバージョン確認](#)」セクションを参照してください。

### アップデート

Citrix Workspace アプリを更新する前に、システムにインストールされている Citrix Workspace アプリの現在のバージョンを確認します。詳しくは、「[Citrix Workspace アプリのバージョン確認](#)」セクションを参照してください。

新しいバージョンの Citrix Workspace アプリに更新するには、[Citrix ダウンロードページ](#)から最新の Citrix Workspace アプリをダウンロードしてインストールします。インストール手順については、次の各セクションに記載されている手順に従ってください:

- [Debian パッケージ](#)
- [Red Hat パッケージ](#)
- [Tarball パッケージ](#)

システムに Citrix Workspace アプリがインストールされている場合、システムは既存のアプリを検出し、新しいバージョンに更新します。ただし、Tarball パッケージの場合は、以前のバージョンのアプリを 1 つのフォルダーにインストールし、新しいバージョンのアプリを別のフォルダーにインストールしたシナリオを想定してください。このシナリオでは、アプリの両方のバージョンがシステムに存在する可能性があります。

アプリの更新時、アンインストールおよび再インストール時に **Citrix Workspace** の画面オーバーレイがアプリを最初に起動すると表示されます。[OK] をクリックして Citrix Workspace アプリを引き続き使用するか、[詳細情報を表示する] をクリックして詳細を表示します。

### 開始

September 15, 2023

このドキュメントは、Linux 向け Citrix Workspace アプリの使用を開始する場合に参照できます。

システムにインストールされている Citrix Workspace アプリの現在のバージョンを確認します。詳しくは、「[Citrix Workspace アプリのバージョン確認](#)」(//ja-jp/citrix-workspace-app-for-linux/install.html#verify-the-version-of-the-citrix-workspace-app) セクションを参照してください。

### ストア

ストアは、ユーザーが使用できるアプリケーションとデスクトップを 1 つの場所に集約します。ユーザーは複数のストアを持ち、必要に応じてストアを切り替えることができます。管理者は、リソースと設定が事前に構成されたストア URL を配信します。ストアには、Citrix Workspace アプリからアクセスできます。

詳しくは、[StoreFront](#)のドキュメントを参照してください。

### ストアの種類

Citrix Workspace アプリでは、次の種類のストアを追加できます：

- [Workspace](#)
- [StoreFront](#)
- [Citrix Gateway Store](#)
- [カスタム Web ストア](#)

### Workspace

Citrix Workspace は、場所とデバイスを選ばず、アプリ、デスクトップ、およびコンテンツ（リソース）へのセキュアで統合されたアクセスを提供する、クラウドベースのエンタープライズアプリストアです。これらのリソースには、Citrix DaaS、コンテンツアプリ、ローカルアプリとモバイルアプリ、SaaS アプリと Web アプリ、ブラウザアプリなどがあります。詳しくは、「[Citrix Workspace の概要](#)」を参照してください。

### StoreFront

StoreFront は、Citrix Virtual Apps and Desktops サイトからアプリケーションとデスクトップを集約して、使いやすい単一のストアとして機能するオンプレミスのエンタープライズアプリストアです。

詳しくは、[StoreFront](#)のドキュメントを参照してください。

### Citrix Gateway Store

ユーザーが内部ネットワークの外から接続できるように Citrix Gateway を構成します。たとえば、インターネットやリモートの場所から接続するユーザーです。

### カスタム **Web** ストア

2203 より、Citrix Workspace アプリから組織のカスタム Web ストアにアクセスできます。

グローバルアプリ構成サービスが利用可能な場合に、この機能を使用するには：

管理者はドメインまたはカスタム Web ストアを Global App Configuration Service で許可されている URL の一覧に追加する必要があります。ドメインまたは Web ストアの追加後、Citrix Workspace アプリの [アカウントの追加] 画面でカスタム Web ストアの URL を指定します。カスタム Web ストアはネイティブの Workspace アプリウィンドウで開きます。

エンドユーザー向けの Web ストア URL の構成について詳しくは、「[Global App Configuration Service](#)」を参照してください。



注:

マルチモニター画面レイアウト機能の固定は、カスタム Web ストアではサポートされていません。

カスタム Web ストアを削除するには、[アカウント] > [アカウントの追加または削除] に移動して、カスタム Web ストアの URL を選択し、[削除] をクリックします。

前提条件として、AuthManConfig.xml ファイルでカスタム Web ストアを有効にする必要があります。有効にするには次の手順に従います:

1. 構成ファイル \$ICAROOT/config/AuthManConfig.xml に移動します。
2. 次のエントリを追加します:

```
1 <key>AppConfigEnabled</key>
2 <value>true</value>
3 <!--NeedCopy-->
```

グローバルアプリ構成サービスが利用できない場合に、この機能を使用するには:

次の構成の変更を実行します:

1. 構成ファイル \$ICAROOT/config/AuthManConfig.xml に移動します。
2. 次のエントリを追加します:

```
1 <key>AppConfigEnabled</key>
2 <value>>false</value>
3 <!--NeedCopy-->
```

3. カスタム Web ストアで考慮する必要のある URL の一覧を次のように追加します。

```
1 <AllowedWebStoreCache>
2 <value><URL1></value>
3 <value><URL2></value>
4 ..
5 <value>....</value>
6 </AllowedWebStoreCache>
7 <!--NeedCopy-->
```

注:

カスタム Web ストアの AuthManConfig.xml ファイルで指定されている URL のみを使用できます。カスタム Web ストアで考慮する AuthManConfig.xml ファイルには、さらに URL を追加できます。

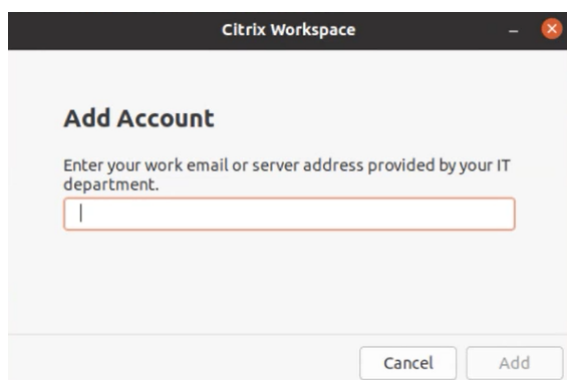
### Citrix Workspace アプリへのストア URL の追加

以下により仮想デスクトップおよびアプリケーションにアクセスするために必要なアカウント情報をユーザーに提供できます:

- アカウント情報をユーザーに手入力させる
- メールベースの自動検出の構成
- CLI を使用したストアの追加

アカウント情報をユーザーに手入力させる

Citrix Workspace アプリを正常にインストールした後、アプリを初めて起動すると、次の画面が表示されます。ユーザーは、アプリやデスクトップにアクセスするためにメールアドレスまたはサーバーアドレスを入力する必要があります。ユーザーが新しいアカウントの詳細を入力すると、Citrix Workspace アプリにより接続が検証されます。検証に成功すると、Citrix Workspace アプリでそのアカウントにログオンするための画面が開きます。



ユーザーが手動でアカウントをセットアップできるようにするには、ユーザーが仮想デスクトップとアプリケーションに接続するために必要な情報を提供します。

- Workspace ストアに接続するには、Workspace URL を指定します。
- StoreFront ストアに接続する場合は、そのサーバーの URL を提供します。例: <https://servername.company.com>。
- Citrix Gateway 経由で接続するには、Citrix Gateway の完全修飾ドメイン名をユーザーに提供します。

ストアのメールベースの自動検出

Citrix Workspace アプリでメールアドレスを指定することで、メールアドレスに関連付けられているストアを自動的に検出できるようになりました。ドメインに複数のストアが関連付けられている場合、デフォルトでは、Global App Configuration Service によって返される最初のストアが、最適なストアとして追加されます。ユーザーは必要に応じていつでも別のストアに切り替えることができます。

この機能を無効にするには、次の手順を実行します：

1. `$ICAROOT/config/AuthManConfig.xml`ファイルに移動します。
2. 次のエントリを `false` に設定します。

```
1 <key>AppConfigEnabled</key>
2 <value>false</value>
3 <!--NeedCopy-->
```

### CLI を使用したストアの追加

管理者として、コマンドラインインターフェイスを使用して Linux 向け Citrix Workspace アプリをインストールします。

詳しくは、「[Storebrowse](#)」セクションを参照してください。

### セットアップ

インストールパッケージをダウンロードし、構成をカスタマイズしてから、Citrix Workspace アプリをインストールできます。

Citrix Workspace アプリのパッケージの内容を変更後、ファイルを再パッケージ化できます。

### インストールのカスタマイズ

1. Citrix Workspace アプリパッケージファイルを空のディレクトリに展開します。パッケージファイルの名前は、`platform.major.minor.release.build.tar.gz` (Linux/x86 プラットフォームなら `linuxx86-<version>.tar.gz` など) です。
2. Citrix Workspace アプリパッケージに必要な変更を加えます。たとえば、標準の Citrix Workspace アプリのインストールには含まれていない証明機関からの証明書を使用する場合は、TLS ルート証明書をパッケージに追加できます。
3. `PkgID` ファイルを開きます。
4. パッケージを変更したことを示すために次の行を追加します：

```
MODIFIED=traceinfo
```

ここで `traceinfo` は、パッケージの変更者と変更日時を示します。

5. ファイルを保存して閉じます。
6. パッケージファイルの一覧 `platform/platform.psf` (たとえば Linux/x86 プラットフォームの場合なら `linuxx86/linuxx86.psf`) を開きます。
7. パッケージファイルの一覧を更新して、パッケージに対する変更を適用します。更新しない場合、新しいパッケージのインストール時にエラーが発生する可能性があります。変更には、修正したファイルのサイズの更新、またはパッケージに追加したファイルに対する新しい行の追加などを含めることができます。パッケージファイルの一覧に含まれている列には次のようなものがあります：

- ファイルタイプ
- 相対パス
- サブパッケージ (常に `cor` に設定)
- アクセス権
- 所有者

- グループ
  - サイズ
8. ファイルを保存して閉じます。
  9. `tar` コマンドを使用して、Citrix Workspace アプリパッケージファイルを再構築します。たとえば `tar czf ../newpackage.tar.gz *` のようなコマンドで、`newpackagez` は新しい Citrix Workspace アプリパッケージファイルの名前です。

### 最新の **Webkit** サポート

Linux 向け Citrix Workspace アプリでは `libwebkit2gtk` (2.16.6 以降) が必要となります。

`libwebkit2gtk` には以下の利点があります：

- UI エクスペリエンスの向上。`webkit2gtk` は、ブラウザーコンテンツのリダイレクト機能と互換性があります。YouTube の視聴をさらに快適にするには、`webkit2gtk` バージョン 2.24 以降を使用してください。
- `webkit2gtk` バージョン 2.16.6 以降では、サインイン操作が改善され、サインインにかかる時間も短くなっています。
- このアプリは、新しい Linux ディストリビューションで適切に機能し、最新の WebKit セキュリティ修正に対応しています。

注：

`webkit2gtk` は一部の Linux ディストリビューションでは利用できません。問題を回避するには、以下のオプションを検討してください：

- Citrix Workspace アプリ 1906 をインストールする前に、ソースから `webkit2gtk` をビルドします。
- `webkit2gtk` 2.16.6 以降をサポートする新しい Linux ディストリビューションに移行します。

### 起動

Citrix Workspace アプリは、コマンドウィンドウ、またはサポートされているデスクトップ環境を使って起動できます。

環境変数 `ICAROOT` に実際のインストール先ディレクトリを指定しておく必要があります。

ヒント：

以下の手順は、Web パッケージによるインストールで `Tarball` が使用されている場合は適用されません。この手順は、セルフサービス要件が満たされなかった場合に適用可能です。

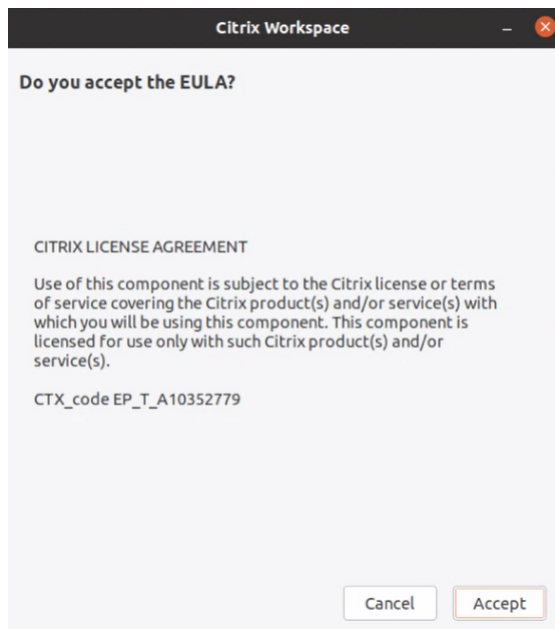
### コマンドウィンドウ

コマンドウィンドウで Citrix Workspace アプリを起動するには：

1. `/opt/Citrix/ICAClient/selfservice` を入力します

2. Enter キーを押します (/opt/Citrix/ICAClient は Citrix Workspace アプリをインストールしたディレクトリです)。

[EULA に同意しますか?] ダイアログボックスが開きます。



3. [同意] をクリックして、ストアの追加に進みます。

注:

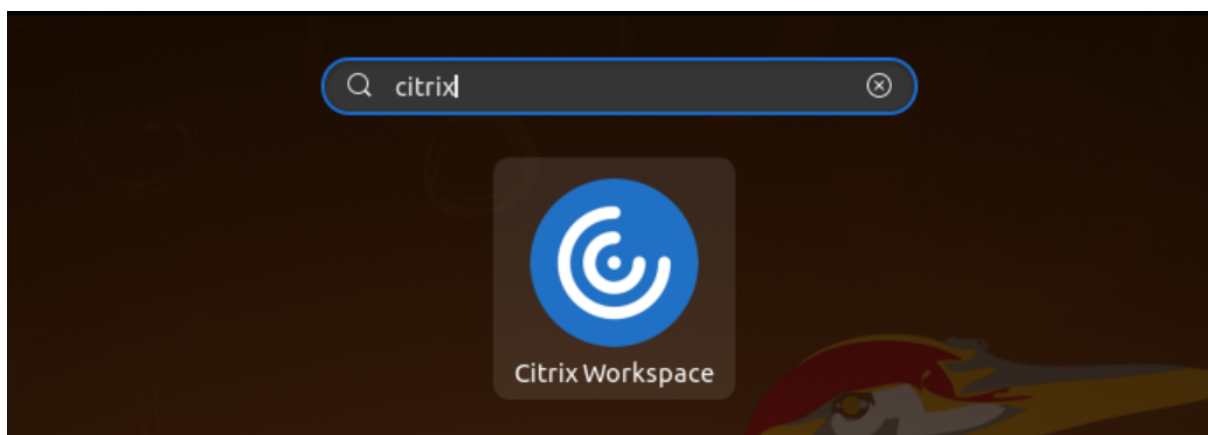
[EULA に同意しますか?] ダイアログボックスは、インストール後に初めて Linux 向け Citrix Workspace アプリにアクセスした場合にのみ表示されます。

## Linux デスクトップ

ファイルマネージャーを使ってデスクトップ環境から Citrix Workspace アプリを起動できます。

一部のデスクトップでは、メニューから Citrix Workspace アプリを起動することもできます。Linux のディストリビューションによって、Citrix Workspace アプリを起動するためのメニューが異なる場合があります。

Ubuntu では、Citrix Workspace アプリのアイコンは次のように表示されます:



## 基本設定

各種設定を行うには、Citrix Workspace アプリメニューの [環境設定] を選択します。以下を制御できます：

- デスクトップの表示方法
- さまざまなアプリケーションやデスクトップへの接続
- ファイルとデバイスへのアクセスの管理

## アカウントの管理

デスクトップおよびアプリケーションにアクセスするには、アカウントに Citrix Virtual Apps and Desktops または Citrix DaaS (Citrix Virtual Apps and Desktops サービスの新名称) が必要です。IT ヘルプデスクは、このために Citrix Workspace にアカウントを追加するよう依頼したり、既存のアカウントで異なる Citrix Gateway または Access Gateway サーバーを使用するよう依頼することがあります。また、Citrix Workspace からアカウントを削除することもできます。

1. [環境設定] ダイアログボックスの [アカウント] ページで、次のいずれかを実行します。
  - アカウントを追加するには、[追加] をクリックします。詳しくは、システム管理者に問い合わせてください。
  - アカウントで接続するストアの詳細 (デフォルトのゲートウェイなど) を変更するには、[編集] をクリックします。
  - アカウントを一覧から削除するには、[削除] をクリックします。
2. 画面の指示に従って操作します。プロンプトが表示されたら、サーバーに認証します。

## デスクトップの表示

デスクトップを全画面で表示 (全画面モード。デフォルト) したり、ウィンドウ内に表示 (ウィンドウモード) したりできます。

- [環境設定] ダイアログボックスの [全般] ページを開き、[デスクトップの表示] オプションを使用して表示モードを選択します。

**[You can enable Desktop Viewer]** ツールバー機能を有効にして、リモートセッションのウィンドウ構成を動的に変更できます。

## Desktop Viewer

ユーザーが仮想デスクトップにアクセスする方法の要件は、ユーザーによって、そして企業ニーズが展開するにつれて変化する可能性があります。

ユーザーが仮想デスクトップを操作する場合は、Desktop Viewer を使用します。ユーザーの仮想デスクトップには公開仮想デスクトップを使用でき、共有または専用デスクトップのいずれでも可能です。このアクセスシナリオでは、**Desktop Viewer** ツールバー機能により、モニターを横断したマルチモニターサポートなど、ウィンドウモードと全画面モードのセッションの切り替えることができます。ユーザーは、同じユーザーデバイス上で複数の Citrix Virtual Apps and Desktops または Citrix DaaS の接続を確立して、デスクトップセッションを切り替え、複数のデスクトップを使用できます。すべてのデスクトップセッションを最小化し、Ctrl+Alt+Del シーケンスを送信し、接続を切断し、セッションをログオフするボタンが提供されるため、簡単にユーザーのセッションを管理できます。

**Ctrl+Alt+Break** キーを押すと、ポップアップウィンドウで **Desktop Viewer** ツールバーが開きます。

### セッションの自動再接続

Citrix Workspace アプリは、切断されたデスクトップおよびアプリケーションに再接続できます。(ネットワークインフラストラクチャの問題など。)

- [環境設定] ダイアログボックスの [全般] ページを開き、[アプリやデスクトップへの再接続] でオプションを選択します。

### ローカルファイルへのアクセス

仮想デスクトップやアプリケーションからローカルコンピューター上のファイルにアクセスする場合は、そのアクセス方法を制御することができます。

1. [環境設定] ダイアログボックスの [ファイルアクセス] ページを開き、マップするドライブを選択してから適切なオプションを選択します。
  - 読み取り/書き込み: デスクトップやアプリケーションでのローカルファイルの読み取りおよび書き込みを許可します。
  - 読み取りのみ: デスクトップやアプリケーションでのローカルファイルの読み取りのみを許可し、書き込みを禁止します。
  - アクセスなし: デスクトップやアプリケーションでのローカルファイルへのアクセスを禁止します。
  - 毎回確認する: デスクトップやアプリケーションでのローカルファイルにアクセスするときに、毎回確認メッセージを表示します。
2. [追加] をクリックして場所を指定し、それに割り当てるドライブ文字を選択します。

## マイクと **Web** カメラ

マイクまたは Web カメラを設定するには、仮想デスクトップまたはアプリケーションからローカルのマイクまたは Web カメラへのアクセス方法を変更します。

[環境設定] ダイアログボックスの [マイクと **Web** カメラ] ページでは、次のオプションを選択できます：

- マイクと **Web** カメラを使用する：デスクトップやアプリケーションでのマイクや Web カメラの使用を許可します。
- マイクと **Web** カメラを使用しない：デスクトップやアプリケーションでのマイクや Web カメラの使用を禁止します。

## Flash Player

Flash コンテンツの表示方法を選択できます。通常、これらのコンテンツにはビデオ、アニメーション、およびアプリケーションが含まれ、**Flash Player** を使って表示します。

[環境設定] ダイアログボックスの [**Flash**] ページでは、次のオプションを選択できます：

- コンテンツを最適化する：コンテンツの再生品質を向上させます。ただし、セキュリティが低下する可能性があります。
- 最適化しない：セキュリティを犠牲にすることなく、標準的な再生品質が提供されます。
- 毎回確認する：Flash コンテンツを表示するときに、毎回確認メッセージを表示します。

## 接続

Citrix Workspace アプリにより、仮想デスクトップやアプリケーションへの安全なセルフサービスアクセスと、Windows、Web、および SaaS (Software as a Service) アプリケーションへのオンデマンドアクセスが提供されます。ユーザーのアクセスは、Citrix StoreFront や従来の Web Interface の Web ページにより管理されます。

**Citrix Workspace** のユーザーインターフェイスを使用してリソースに接続するには

Citrix Workspace アプリのホームページには、ユーザーのアカウント設定（つまり接続先のサーバー）と Citrix Virtual Apps and Desktops または Citrix DaaS の管理者による構成に基づいて、そのユーザーに提供されている仮想デスクトップやアプリケーションが表示されます。ユーザーは、[環境設定] ダイアログボックスの [アカウント] ページに StoreFront サーバーの URL や自分のメールアドレス（メールアドレスによるアカウント検出が有効な場合）を入力してアカウントの構成を行います。

### ヒント：

StoreFront サーバーの複数のストアに同じ名前を使用する場合、数字を追加することで重複を防ぐことができます。このようなストアの名前は追加する順番に従います。Citrix Workspace アプリの場合、ストアの URL が表示され、ストアを確実に識別します。



ストアへの接続後、セルフサービスで次のタブが表示されます：お気に入り、デスクトップ、アプリ。セッションを起動するには、適切なアイコンをクリックします。アイコンを [お気に入り] に追加するには、アイコンの横の [詳細] リンクをクリックして [お気に入りに追加] を選択します。

### コネクション設定の構成

Citrix Workspace アプリと、Citrix Virtual Apps and Desktops または Citrix DaaS サーバー間の接続に対する複数のデフォルト設定を構成できます。必要に応じて、個々の接続に関する設定を変更することもできます。

管理者とユーザーの作業と責任範囲は重複することがありますが、一般的にユーザーが行う操作について「ユーザー」という用語を使用して区別します。

### コマンドラインまたは **Web** ブラウザーからリソースに接続する

Citrix Workspace アプリのホームページでデスクトップやアプリケーションのアイコンをクリックすると、サーバーへの接続が作成されます。また、コマンドラインや Web ブラウザーからコネクションを開くこともできます。

コマンドラインで **Program Neighborhood** または **StoreFront** サーバーへのコネクションを作成するには

前提条件：

Citrix Workspace アプリがストアを認識できるようにします。必要に応じて、次のコマンドを実行してストアを追加します：

```
1  `` `
2  ./util/storebrowse --addstore \<store URL\>
3  <!--NeedCopy--> `` `
```

1. 接続するデスクトップまたはアプリケーションの固有の ID を取得します。この ID は、以下のコマンドによる出力の最初の引用文字列です。

- サーバー上のすべてのデスクトップおよびアプリケーションの一覧を取得するには、次のコマンドを実行します。

```
1  ./util/storebrowse -E <store URL>
2  <!--NeedCopy-->
```

- サブスクリプション済みのデスクトップおよびアプリケーションの一覧を取得するには、次のコマンドを実行します。

```
1  ./util/storebrowse -S <store URL>
2  <!--NeedCopy-->
```

2. 次のコマンドを実行して、デスクトップまたはアプリケーションを起動します。

```
1 ./util/storebrowse -L <desktop or application ID> <store URL>
2 <!--NeedCopy-->
```

サーバーに接続できない場合は、管理者に対してサーバーの場所または SOCKS プロキシに関する問題の確認が必要な場合があります。詳しくは、「[プロキシサーバー](#)」を参照してください。

**Web** ブラウザーで接続を作成するには

通常、Web ブラウザーからセッションを開始するための構成はインストール中に自動で構成されます。さまざまなブラウザおよびオペレーティングシステムがあるため、手動の構成が必要な場合もあります。

Firefox、Mozilla、または Chrome 用に `.mailcap` および `MIME` ファイルを手動で設定する場合は、次の手順に従ってファイルを変更します。これらの変更を使用して、`.ICA` ファイルにより Citrix Workspace アプリの実行可能ファイル (`wfica`) が起動するようにします。ほかのブラウザを使用するには、必要に合わせてブラウザ構成を変更します。

1. 管理者以外の環境に Citrix Workspace アプリをインストールするには、以下のコマンドを実行します。デフォルト以外の場所にインストールされている場合、`ICAROOT` の設定が異なることがあります。次のコマンドで結果をテストできます：

```
xdg-mime query default application/x-ica。このコマンドを実行すると、「wfica.desktop」が返されるはずですが。
```

```
export ICAROOT=/opt/Citrix/ICAClient
```

```
xdg-icon-resource install --size 64 $ICAROOT/icons/000_Receiver_64.png
Citrix Workspace app
```

```
xdg-mime default wfica.desktop application/x-ica
```

```
xdg-mime default new_store.desktop application/vnd.citrix.receiver.
configure
```

2. ファイル「`/etc/xdg/mimeapps.list`」（管理者のインストールの場合）または「`$(HOME)/.local/share/applications/mimeapps.list`（`mimeapps.list`）」を作成または拡張します。ファイルは [Default Applications] で開始し、最後に以下が追加されている必要があります：

```
application/x-ica=wfica.desktop;
```

```
application/vnd.citrix.receiver.configure=new_store.desktop;
```

Firefox の場合、環境設定/アプリケーション設定ページの構成が必要なことがあります。

「Citrix ICA settings file content」の場合、次を選択します：

- ドロップダウンメニューから [Citrix Workspace app Engine (default)]

または

- [Use other ...] からファイル「/usr/share/applications/wfica.desktop」（管理者の Citrix Workspace アプリのインストールの場合）

または

- 「\$HOME/.local/share/applications/wfica.desktop」（管理者以外のインストールの場合）

### コネクションセンター

ユーザーがアクティブなコネクションを管理するには、コネクションセンターを使用します。セッションの動作が遅い、またはコネクションに問題がある場合、ユーザーや管理者はコネクションセンターを使用してトラブルシューティングを行えます。ユーザーは、コネクションセンターで以下の操作を行えます。

- アプリケーションを終了する。
- セッションからログオフする。これによりセッションが終了し、実行中のアプリケーションが終了します。
- セッションから切断する。これにより、アプリケーションを実行したまま（切断時にアプリケーションを閉じるようにサーバーを構成していない場合）、選択したコネクションのサーバー接続が切断されます。
- コネクションの転送統計値を参照する。

### 接続の管理

コネクションセンターを使用して接続を管理するには：

1. Citrix Workspace アプリメニューで [コネクションセンター] をクリックします。

接続先のサーバーと、アクティブなセッションが表示されます。

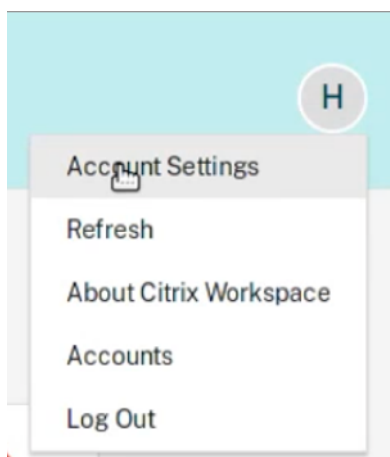
2. 次のいずれかを行います：

- サーバーを選択するか、切断またはログオフするか、サーバーのプロパティを表示します。
- アプリケーションを選択し、ウィンドウを閉じます。

### ユーザーインターフェイスの機能強化

以前は、設定メニューは Desktop Viewer の [基本設定] オプションから利用できました。

バージョン 2106 以降、設定メニューは Self-Service plug-in のインラインに表示されます。メニューオプションは、ネイティブの Citrix Workspace の外観に合わせて向上しました。この機能強化により、シームレスかつ優れたユーザーエクスペリエンスが実現します。



注:

この拡張機能は、クラウド展開の Citrix Workspace アプリバージョン 2106 でデフォルトで利用できます。

ネイティブのスタイルと古いスタイルの外観を切り替えるには、次の手順を実行します:

`$ICAROOT/config/AuthManConfig.xml`に移動し、`WebUISettings`の値を **False** に設定します。

### 構成

September 15, 2023

Linux 向け Citrix Workspace アプリを使用する場合、ホストされているアプリケーションやデスクトップにユーザーがアクセスできるようにするには、以下の構成を行う必要があります。

### 設定

#### 構成ファイル

Citrix Workspace アプリの構成ファイルを編集すると、高度な設定や一般的ではない設定を変更できます。これらの構成ファイルは、`wfica`の起動時に毎回読み取られます。変更する内容により、さまざまな構成ファイルを編集できます。

セッション共有が有効な場合は、更新した構成ファイルに基づくセッションが作成される代わりに既存のセッションが使用されることがあります。この場合、更新した構成ファイルの設定はセッションに反映されません。

#### デフォルト設定

Citrix Workspace アプリのすべてのユーザーに変更されたデフォルト設定を適用する場合は、`$ICAROOT/config`ディレクトリ内の`module.ini`構成ファイルを編集します。

注:

All\\\_Regions.iniでエントリが特定の値に設定されていると、module.iniでのそのエントリに対する値は使用されません。All\\\_Regions.iniの値は、module.iniの値よりも優先されます。

### テンプレートファイル

\$HOME/.ICAClient/wfclient.iniファイルが存在しない場合、wficaが\$ICAROOT/config/wfclient.templateをコピーして作成します。このテンプレートファイルに変更を加えると、すべての Citrix Workspace アプリユーザーに適用されます。

### ユーザー設定

ユーザーの構成変更を適用するには、ユーザーの\$HOME/.ICAClientディレクトリにあるwfclient.iniファイルを変更します。この構成ファイルによる設定は、そのユーザーの新しいコネクションに適用されます。

### 構成ファイルエントリを検証する

wfclient.iniのエントリの値を制限するには、設定可能な値またはその範囲をAll\\\_Regions.iniで指定します。

値を1つだけ指定すると、その値が使用されます。\$HOME/.ICAClient/All\\\_Regions.iniファイルは、\$ICAROOT/config/All\\\_Regions.iniファイルに設定されている可能な値と一致させる、または値を減らすことができますが、制限を取り除くことはできません。

注:

wfclient.iniで設定された値は、module.iniの値よりも優先されます。

### パラメーター

各構成ファイルのパラメーターは、セクションでグループ化されています。各セクションの冒頭には、かっこで囲まれたセクション名（クライアント側ドライブのマッピングに関するパラメーターの\[ClientDrive\]など）が記述されています。

特に注記がある場合を除き、記述されていないパラメーターには自動的にデフォルト値が適用されます。パラメーターに値が設定されていない場合も、自動的にデフォルト値が適用されます。たとえば、InitialProgramパラメーターの後に等号(=)が続き、値が記述されていない場合、デフォルト値（ログオン後にプログラムを実行しない）が適用されます。

### 優先順位

All\\\_Regions.iniファイルにより、ほかの構成ファイルに設定可能なパラメーターが指定されます。設定可能な値の範囲を指定したり、特定の値を指定したりできます。

構成ファイルは以下の順序でチェックされます：

1. `All\\_Regions.ini` - この構成ファイルの値は、以下のファイルの値よりも優先されます。
  - コネクションの `.ICA` ファイル
  - `wfclient.ini`
2. `module.ini` - この構成ファイルの値は、`All\\_Regions.ini`、コネクションの `.ICA` ファイル、または `wfclient.ini` で設定されていない場合に適用されます。ただし、これらの値は `All\\_Regions.ini` で制限されません。

いずれの構成ファイルでも設定されていない場合は、Citrix Workspace アプリのデフォルト設定が適用されます。

注：

上記の優先順位には例外があります。たとえば、セキュリティ上の理由から、一部の値が `wfclient.ini` から読み取られる場合があります。

### Citrix Workspace アプリの非アクティブタイムアウト

非アクティブタイムアウト機能では、管理者が設定した値に基づいてユーザーが Citrix Workspace アプリからサインアウトされます。2303 バージョンより、管理者は、ユーザーが Citrix Workspace アプリから自動的にサインアウトされるまでのアイドル時間を指定できます。Citrix Workspace アプリウィンドウ内で、指定された時間内にマウス、キーボード、またはタッチによるアクティビティが発生しなくなると、自動的にサインアウトされます。無操作状態によるタイムアウトは、既に実行中の Citrix Virtual Apps and Desktops および Citrix DaaS セッションまたは StoreFront ストアには影響しません。

非アクティブタイムアウト値は、10 分から 1440 分まで設定できます。このタイムアウト値を変更する場合の間隔は、5 の倍数にする必要があります。例：10、15、20、または 25 分。デフォルトでは、非アクティブタイムアウトは構成されていません。

注：

この機能は、クラウド展開でのみ適用できます。

前提条件として、`AuthManConfig.xml` ファイルでこの機能を有効にする必要があります。`$ICAROOT/config/AuthManConfig.xml` に移動し、次のエントリを追加します：

```
1 <key>IT0Enabled</key>
2 <value>true</value>
3 <!--NeedCopy-->
```

管理者は、PowerShell モジュールを使用して `inactivityTimeoutInMinutes` プロパティを構成できます。

クライアントマシンで **InactivityTimeoutInMinutes** を構成する手順：

1. PowerShell モジュールを使用した Citrix Workspace の構成をダウンロードします。

2. このモジュールを使用するには、API のクライアント ID とシークレットを生成する必要があります。資格情報の取得と Citrix Cloud API の使用開始について詳しくは、「[Get started with Citrix Cloud APIs \(Citrix Cloud API の使用を開始する\)](#)」を参照してください。
3. このモジュールをインポートするには、Citrix.Workspace.StoreConfigs へのパスを Import-Module コマンドレットに渡します。つまり、このファイルを含むディレクトリから `Import-Module ./Citrix.Workspace.StoreConfigs` を実行します。
4. モジュールがインポートされたら、`Get-Help -Full` を実行して特定のコマンドレットのヘルプを取得します。例: `Get-Help Set-WorkspaceCustomConfigurations -Full`
5. たとえば、次のコマンドを実行して `inactivityTimeoutInMinutes` を 1 時間に設定します。

```
1 Set-WorkspaceCustomConfigurations -WorkspaceUrl -ClientId -  
   ClientSecret -InactivityTimeoutInMinutes "60"  
2 <!--NeedCopy-->
```

すべてのクライアントで上記のコマンドを実行する必要はありません。一度だけ実行してテストする必要があります。

エンドユーザーエクスペリエンスは次のとおりです:

- サインアウトの 3 分前に通知が表示され、サインインしたままにするか、サインアウトするかを選択できます。
- ユーザーは [サインイン状態を維持] をクリックして通知を閉じ、アプリの使用を続行できます。その場合、無通信タイマーは構成された値にリセットされます。[サインアウト] をクリックして、現在のストアのセッションを終了することもできます。

注:

非アクティブタイムアウト機能は、Wayland をデフォルトのグラフィックプロトコルとして使用するディストリビューションをサポートしていません。Wayland を使用しているディストリビューションでは、次のいずれかのコメントを解除します: `/etc/gdm/custom.conf` または `/etc/gdm3/custom.conf` の `WaylandEnable=false`。

### 永続ログイン

2303 バージョンより、永続ログイン機能を使用すると、管理者が設定した期間 (2~365 日)、ログインしたままにすることができます。この機能が有効になっている場合、設定された期間中に Citrix Workspace アプリのログイン資格情報を入力する必要はありません。

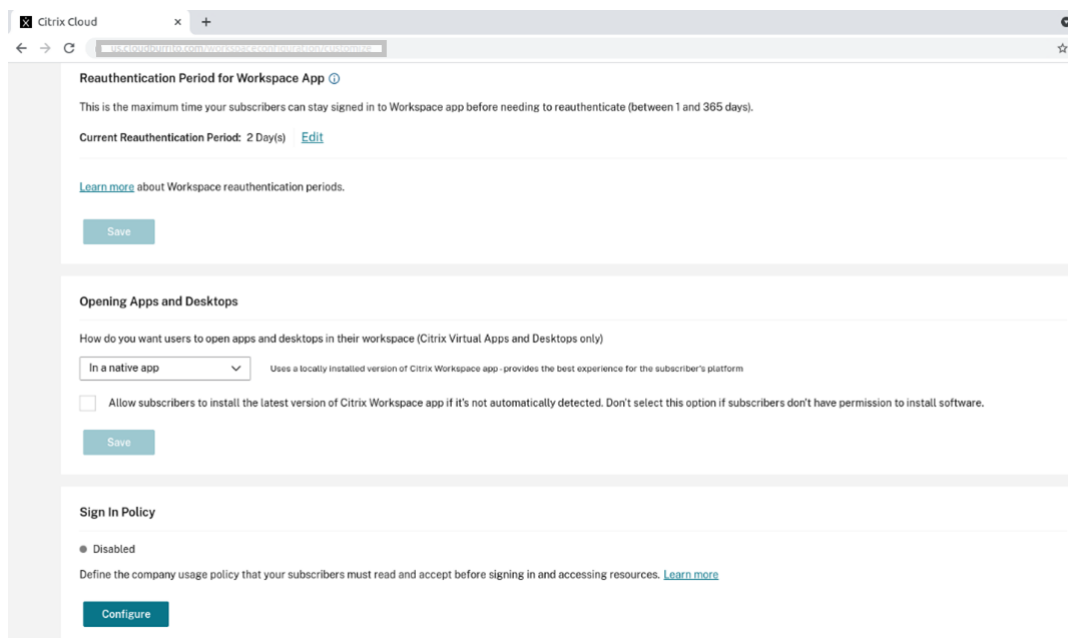
この機能により、Citrix DaaS セッションへの SSO は、最大 365 日まで間延長されます。この拡張機能は、長期有効トークンの有効期間に基づいています。資格情報は、デフォルトで 4 日間または有効期間のいずれか短い方の期間、キャッシュされます。その後、Citrix Workspace アプリへの接続で 4 日以内にアクティブになったときに延長されます。

### 永続ログイン機能の構成

管理者は、次の手順を実行して、Workspace 環境で永続ログインを構成する必要があります：

1. Citrix Cloud にサインインします。
2. Citrix Cloud コンソールで、画面の左上隅にあるメニューをクリックします。
3. [ワークスペース構成] > [カスタマイズ] > [基本設定] を選択します。
4. [Workspace アプリの再認証期間] まで下にスクロールします。
5. [現在の再認証期間] フィールドの横にある [編集] をクリックします。
6. [現在の再認証期間] フィールドに必要な日数を入力します。
7. [現在の再認証期間] フィールドには 2 日以上を入力する必要があります。

詳しくは、次の画像の [Reauthentication Period for Workspace App] (Workspace アプリの再認証期間) セクションの指示を参照してください：

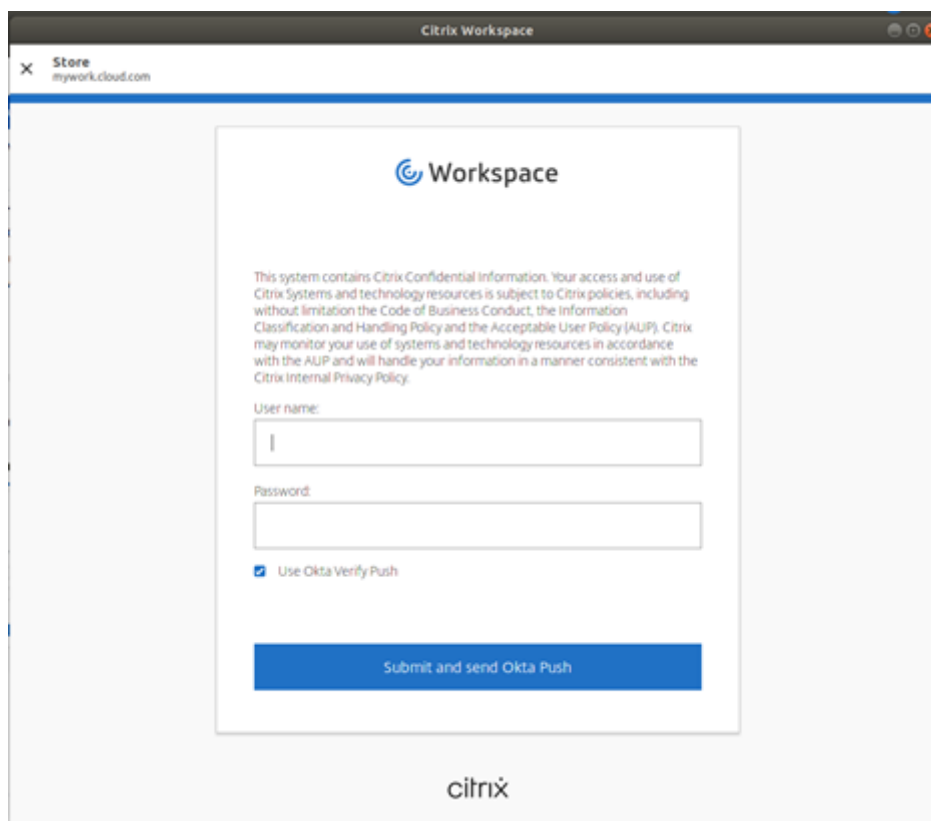


### 強化された認証のエクスペリエンス

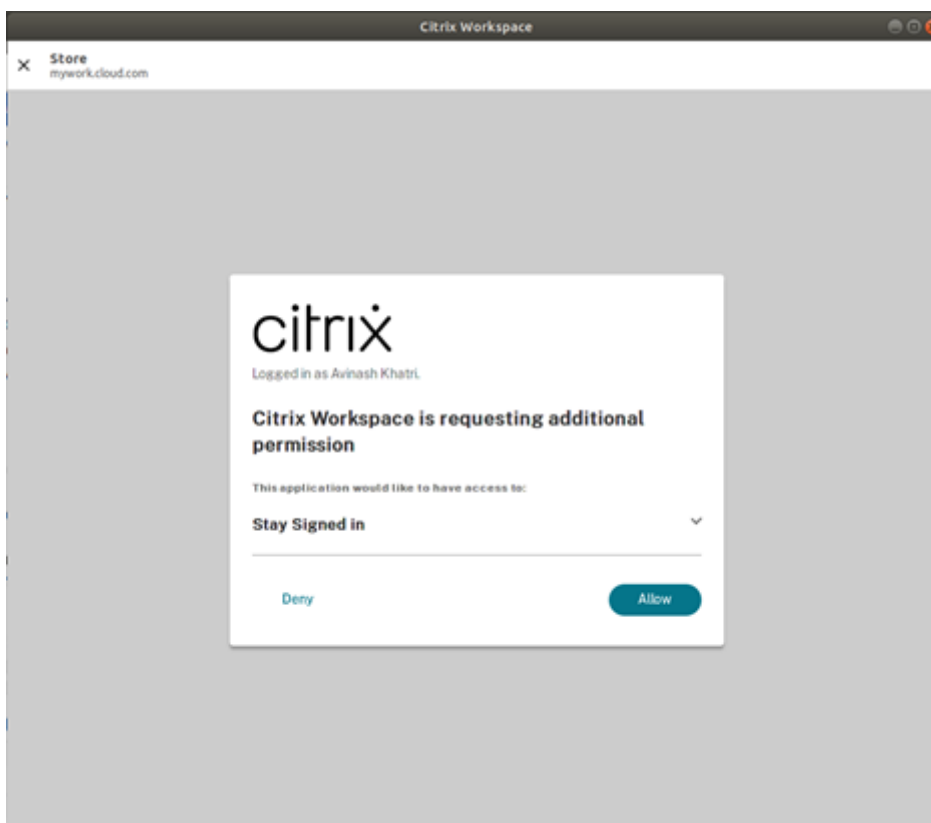
永続ログインウィンドウは、セルフサービスウィンドウ内に組み込まれています。

1. Citrix Workspace アプリにアクセスします。  
認証ウィンドウが表示されます。





2. 資格情報を入力してサインインします。  
受け入れのための [許可] プロンプトにリダイレクトされます。



3. [許可] をクリックします。

注:

同意に対して [拒否] を選択すると、ログインプロンプトが再度表示され、24 時間ごとに Citrix Workspace アプリにサインインする必要があります。

#### 永続ログイン機能の無効化

管理者は、Citrix Cloud UI または `AuthManConfig.xml` ファイル内で、永続ログイン機能を無効にできます。ただし、`AuthManConfig.xml` ファイルに設定した値は、Citrix Cloud UI に設定した値を上書きします。

#### Citrix Cloud UI の使用

1. Citrix Cloud にサインインします。
2. Citrix Cloud コンソールで、画面の左上隅にあるメニューをクリックします。
3. [ワークスペース構成] > [カスタマイズ] > [基本設定] を選択します。
4. [Workspace アプリの再認証期間] まで下にスクロールします。
5. [現在の再認証期間] フィールドの横にある [編集] をクリックします。
6. [現在の再認証期間] フィールドに 1 日を入力します。

## AuthManConfig.xml ファイルの使用

永続ログイン機能を無効にするには、次の手順を実行します

1. <ICAROOT>/config/AuthManConfig.xml ファイルに移動します。
2. 値を次のように設定します：

```
1 <AuthManLite>
2
3 <primaryTokenLifeTime>1.00:00:00</primaryTokenLifeTime>
4
5 <secondaryTokenLifeTime>0.01:00:00</secondaryTokenLifeTime>
6
7 <longLivedTokenSupport>false</longLivedTokenSupport>
8
9 <nativeLoggingEnabled>>true</nativeLoggingEnabled>
10
11 <platform>linux</platform>
12
13 <saveTokens>true</saveTokens>
14
15 </AuthManLite>
16 <!--NeedCopy-->
```

## ネットワーク要求でのカスタムユーザーエージェント文字列の作成

2109 バージョン以降では、ネットワーク要求にユーザーエージェント文字列を追加し、ネットワーク要求の送信元を特定するオプションが、Citrix Workspace アプリに導入されました。このユーザーエージェント文字列の要求に基づいて、ネットワーク要求の管理方法を決定できます。この機能を使用すると、信頼できるデバイスからのネットワーク要求のみを受け入れることができます。

注：

- この機能は、Citrix Workspace アプリのクラウド展開でサポートされています。また、x86、x64、および ARMHF がサポートされているパッケージです。

ユーザーエージェント文字列をカスタマイズするには、次の手順を実行します：

1. 構成ファイル \$ICAROOT/config/AuthManConfig.xml を見つけます。
2. 次のエントリに値を追加します：

```
<UserAgentSuffix> </UserAgentSuffix>
```

カスタマイズされたテキストにアプリとバージョンを含む例：

```
<UserAgentSuffix>App/AppVersion </UserAgentSuffix>
```

App と AppVersion を追加する場合は、スラッシュ（「/」）で区切ります。

- ネットワーク要求が UI ベースの Citrix Workspace アプリからのものである場合、次のユーザーエージェントがネットワーク要求に表示されます:

`CWAWEBVIEW/CWAVersion App/AppVersion`

- ネットワーク要求が UI ベースの Citrix Workspace アプリからのものである場合、次のユーザーエージェントがネットワーク要求に表示されます:

`CWA/CWAVersion App/AppVersion`

注:

- UserAgentSuffix 文字列の最後に AppVersion を付加しない場合、Citrix Workspace アプリのバージョンがネットワーク要求に追加されます。
- 変更を保存するには、AuthManagerDaemonとServiceRecordを再起動します。

### 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、最小限に抑えられます。ユーザーは、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 (Citrix Virtual Apps and Desktops サービスの新名称) を起動できます。

Citrix Workspace アプリでサービス継続性をサポートする要件については、「[システム要件](#)」を参照してください。

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。

### マルチモニター画面レイアウトの固定

バージョン 2103 以降、マルチモニター画面レイアウトの選択を保存できます。このレイアウトは、デスクトップセッションの表示方法です。固定すると、選択したレイアウトでセッションを再開できるため、ユーザーエクスペリエンスが最適化されます。

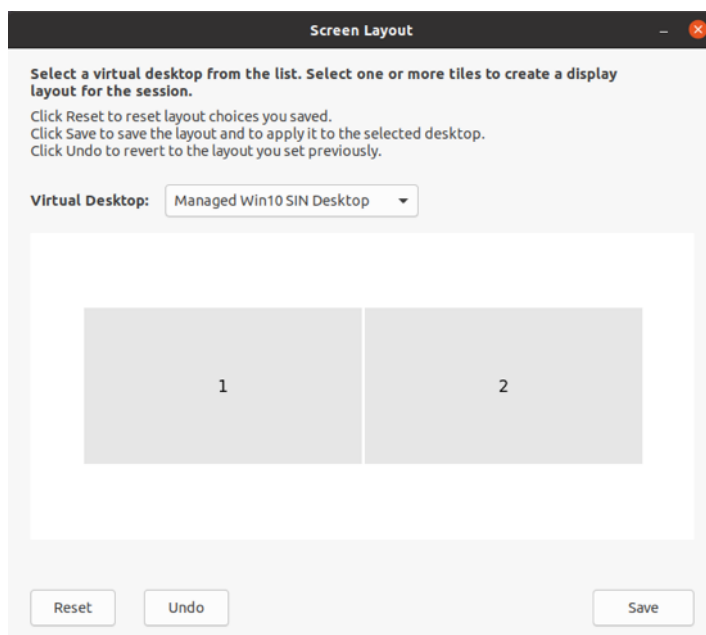
前提条件として、AuthManConfig.xml ファイルでこの機能を有効にする必要があります。`$ICAROOT/config/AuthManConfig.xml` に移動し、次のエントリを追加します:

```
1 <key>ScreenPinEnabled</key>
2 <value> true </value>
3 <!--NeedCopy-->
```

上記のキーを追加して初めて、アプリインジケータアイコンに [画面レイアウト] オプションが表示されます。アプリインジケータアイコンについて詳しくは、「[アプリインジケータアイコン](#)」を参照してください。

画面レイアウトを選択するには、タスクバーのアプリインジケータアイコンをクリックし、[画面レイアウト] を選択します。[画面レイアウト] ダイアログボックスが開きます。

または、Self-Service ウィンドウで **Ctrl+m** キーを押して [画面レイアウト] を起動できます。



ドロップダウンメニューから仮想デスクトップを選択します。レイアウトの選択は、選択したデスクトップにのみ適用されます。

1 つまたは複数のタイルを選択して、長方形のレイアウトを形成します。レイアウトの選択に従って、セッションが表示されます。

制限事項:

- 画面の固定を有効にすると、セッションのレイアウト保存機能が無効になります。
- この機能は、お気に入りのマークが付けられているデスクトップにのみ適用できます。

### アプリケーションカテゴリ

アプリケーションカテゴリを使用すると、ユーザーは Citrix Workspace アプリ内のアプリケーションのコレクションを管理できます。次のアプリケーショングループを作成できます:

- 異なるデリバリーグループ間で共有されているアプリケーション
- デリバリーグループ内のユーザーのサブセットが使用するアプリケーション

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[デリバリーグループの作成](#)」セクションを参照してください。

## App Protection

### 免責事項

App Protection ポリシーはオペレーティングシステムの必要な機能へのアクセスをフィルタリングできます。画面のキャプチャまたはキーボードの操作には、特定の API 呼び出しが必要です。つまりこの機能は、App

Protection ポリシーがカスタムの目的別に構築されたハッカーツールに対しても保護を提供できることを意味します。ただし、オペレーティングシステムの進化によって、画面のキャプチャやキーのログ記録には新しい方法が出てきます。引き続きこうした方法に対応していきませんが、特定の構成や展開では完全な保護を保証することはできません。

App Protection は、Citrix Virtual Apps and Desktops の使用時にセキュリティを強化する機能です。この機能により、キーロガーや画面キャプチャマルウェアによりクライアントが侵害される可能性が制限されます。App Protection では、画面に表示されるユーザーの資格情報や個人情報などの機密情報の流出を防ぎます。この機能を使うと、ユーザーおよび攻撃者がスクリーンショットを撮る、またはキーロガーを使用することにより機密情報を収集、悪用することを防ぐことができます。

注:

- この機能は、tarball、Debian、Red Hat Package Manager (RPM) パッケージを使用して Citrix Workspace アプリがインストールされている場合にサポートされます。また、サポートされているアーキテクチャは x64 と ARMHF の 2 つだけです。
- この機能は、オンプレミスの Citrix Virtual Apps and Desktops 環境でサポートされます。また、StoreFront で Citrix Virtual Apps and Desktops サービスを使用する環境でもサポートされます。

App Protection では、ライセンスサーバーにアドオンライセンスをインストールする必要があります。Citrix Virtual Desktops ライセンスも必要です。ライセンスについて詳しくは、[Citrix Virtual Apps and Desktops](#)の「構成」セクションを参照してください。

バージョン 2108 以降、App Protection 機能の全機能が使用可能になりました。App Protection 機能はアプリとデスクトップセッションをサポートし、デフォルトで有効になっています。ただし、`AuthManConfig.xml` ファイルで App Protection 機能を構成して、認証マネージャーと Self-service Plug-in インターフェイスで有効にする必要があります。

このバージョン以降、Mozilla Firefox の実行中に、保護されたリソースを Citrix Workspace アプリから起動できません。

バージョン 2012 以降、App Protection 機能は、[試験段階の機能](#)です。

前提条件:

App Protection は、Gnome Display Manager と併せて、次のオペレーティングシステムで最適に機能します:

- 64 ビット Ubuntu 18.04、Ubuntu 20.04、および Ubuntu 22.04
- 64 ビット Debian 9 および Debian 10
- 64 ビット CentOS 7
- 64 ビット RHEL 7
- ARMHF 32 ビット Raspberry Pi OS (Debian 10 (buster) ベース)
- ARM64 Raspberry Pi OS (Debian 11 (bullseye) ベース)

注:

バージョン 2204 より前の Citrix Workspace アプリを使用している場合、App Protection 機能は `glibc`

2.34 以降を使用するオペレーティングシステムをサポートしません。

`glibc` 2.34 以降を使用する OS に App Protection 機能を有効にした Citrix Workspace アプリをインストールした場合、システムの再起動時に OS の起動に失敗することがあります。OS の起動エラーから回復するには、次のいずれかを実行します：

- OS を再インストールします。ただし、`glibc` 2.34 以降を使用する OS では App Protection 機能はサポートされていません。
- OS のリカバリモードに移動し、ターミナルを使用して Citrix Workspace アプリをアンインストールします。
- ライブ OS から起動し、既存の OS から `rm -rf /etc/ld.so.preload` ファイルを削除します。

### **App Protection** コンポーネントのアンインストール：

`tarball` パッケージを使用して Citrix Workspace アプリをインストールすると、次のメッセージが表示されます。

「App Protection コンポーネントをインストールしますか？ 警告： この機能を無効にすることはできません。無効にするには、Citrix Workspace アプリをアンインストールする必要があります。詳しくは、システム管理者に問い合わせてください。[default \$INSTALLER\_N]:」

**Y** を入力して、App Protection コンポーネントをインストールします。

デフォルトでは、App Protection コンポーネントはインストールされていません。

変更を保存するには、マシンを再起動します。App Protection は、マシンを再起動した後にのみ正常に機能します。

### **RPM** パッケージへの **App Protection** コンポーネントのインストール：

バージョン 2104 以降、Citrix Workspace アプリの RPM バージョンで App Protection がサポートされています。

App Protection をインストールするには、次の手順を実行します：

1. Citrix Workspace アプリをインストールします。
2. Citrix Workspace アプリインストーラーから `App Protectionctxappprotection<version>.rpm` パッケージをインストールします。
3. 変更を保存するには、システムを再起動します。

### **Debian** パッケージへの **App Protection** コンポーネントのインストール：

バージョン 2101 以降、Citrix Workspace アプリの Debian バージョンで App Protection がサポートされています。

App Protection コンポーネントをサイレントインストールするには、Citrix Workspace アプリをインストールする前に、ターミナルから次のコマンドを実行します：

```
1 export DEBIAN_FRONTEND="noninteractive"
2 sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select yes"
3
4 sudo debconf-show icaclient
```

```
5 * app_protection/install_app_protection: yes
6
7 sudo apt install -f ./icaclient_<version>._amd64.deb
8 <!--NeedCopy-->
```

Citrix Workspace アプリではバージョン 2106 以降、Authentication Manager インターフェイスと Self-service Plug-in インターフェイスの両方で、キーロガー対策および画面キャプチャ対策機能を個別に構成できるオプションが導入されます。

#### Authentication Manager の App Protection の構成:

\$ICAROOT/config/AuthManConfig.xml に移動し、次のようにファイルを編集します:

```
1 /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
  authmananti -A 1
2   <key>AuthManAntiScreenCaptureEnabled</key>
3   <value>true</value>
4   <key>AuthManAntiKeyLoggingEnabled</key>
5   <value>true </value>
6
7 <!--NeedCopy-->
```

#### Self-service Plug-in インターフェイスの App Protection の構成:

\$ICAROOT/config/AuthManConfig.xml に移動し、次のようにファイルを編集します:

```
1 /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
  protection -A 4
2 <!-- Selfservice App Protection configuration -->
3   <Selfservice>
4     <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
5     <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
6   </Selfservice>
7
8 <!--NeedCopy-->
```

#### 既知の問題:

- 保護された画面を最小化すると、App Protection は引き続きバックグラウンドで実行されます。

#### 制限事項:

- Snap Store からインストールされたアプリケーションの実行中に、保護されたリソースを起動できない場合があります。回避策としては、Citrix Workspace アプリのログファイルから問題の原因となっているアプリケーションを特定し、そのアプリケーションを終了します。
- 保護されたウィンドウのスクリーンショットを撮影しようとする、バックグラウンドの保護されていないアプリを含む画面全体が灰色に表示されていました。



### 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、Citrix Desktop セッションのシステムトレイに表示されるようになりました。

注:

2111 バージョン以降、サーバー VDA のバッテリー状態インジケータも表示されます。

バッテリー状態インジケータはデフォルトで有効になっています。

バッテリー状態インジケータを無効にするには:

1. <ICAROOT>/config/module.ini フォルダに移動します。
2. ICA 3.0 セクションに移動します。
3. MobileReceiver= Off を設定します。

### カスタマーエクスペリエンス向上プログラム (CEIP)

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、Linux 向け Citrix Workspace アプリの構成および使用状況データが収集され、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。

また、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。[Google Analytics のために収集されたデータ](#) の Google の取り扱い方法についてもご確認ください。

Citrix および Google Analytics への CEIP データの送信をオフにします。このアクティビティでは、Google Analytics 用に収集されたデータで、次のセクションの 2 番目の表に \* 付きで表示されているものは例外となります。Citrix および Google Analytics への CEIP データの送信をオフにするには次の手順を実行します:

1. <ICAROOT>/config/module.ini フォルダの CEIP セクションに移動します。
2. エントリ EnableCeip を選択して Disable に設定します。

注:

EnableCeip キーを Disable に設定すると、Google Analytics によって収集された最後の 2 つの CEIP データ要素の送信を無効にできます。これらのデータ要素は、オペレーティングシステムのバージョンと

Workspace アプリのバージョンです。このアクションでは、次のセクションに移動し、推奨されている値を設定します：

場所: <ICAROOT>/config/module.ini

セクション: `GoogleAnalytics`

エントリ: `DisableHeartBeat`

値: **True**

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。

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

オペレーティングシステムバージョン *	Workspace アプリバージョン *	アプリ名	Workspace アプリの言語
セッションの起動方法	コンパイラバージョン	ハードウェアプラットフォーム	ストア構成
Citrix Virtual Apps and Desktops のセッション起動状態	認証構成	接続プロトコル	ブラウザコンテンツのリダイレクト機能の使用状況
接続リソースの詳細	App Protection の構成		

### アプリインジケータアイコン

Citrix Workspace アプリを起動すると、アプリインジケータが起動します。システムトレイに表示されるアイコンです。アプリインジケータの導入により、Linux 向け Citrix Workspace アプリのログオンパフォーマンスが向上しました。

パフォーマンスの向上は、以下の動作で確認できます：

- Citrix Workspace アプリの最初の起動
- アプリを閉じて再起動
- アプリの終了と再起動

注:

アプリインジケータを表示するには、`libappindicator` パッケージが必要です。使用する Linux ディストリビューションに適した `libappindicator` パッケージを Web サイトからインストールします。

## ICA-to-X プロキシ

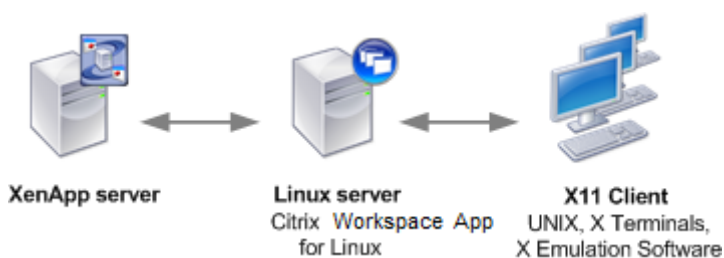
Citrix Workspace アプリを実行しているワークステーションをサーバーとして使用し、出力を別の X11 対応デバイスに転送できます。Citrix Workspace アプリを使用できない X 端末または UNIX ワークステーションに Microsoft Windows 用アプリケーションを配信する場合などに、このタスクを実行できます。

注:

Citrix Workspace アプリは多くの X デバイスで使用できるので、このデバイスへのソフトウェアのインストールはこの方法を使用することをお勧めします。Citrix Workspace アプリを ICA-to-X プロキシとして実行することを、サーバー側 ICA と呼びます。

この方法では、実行する Citrix Workspace アプリを ICA から X11 へのコンバーターとして使うことで、X11 の出力をローカルの Linux デスクトップ画面に転送します。また、その出力をさらに別の X11 コンピューターの画面に転送できます。1 つのシステムで Citrix Workspace アプリの追加コピーを同時に実行できます。この場合、各 Citrix Workspace アプリはその出力を異なるデバイスに送信します。

この図は、Linux 向け Citrix Workspace アプリが ICA-to-X プロキシとして動作するシステムを示しています。



この方法を使うようにシステムを設定するには、Linux サーバーを ICA から X11 へのプロキシサーバーとして機能させる必要があります。

- X 端末が既にある場合は、X アプリケーションを X 端末に供給する Linux サーバーで Citrix Workspace アプリを実行できます。
- Citrix Workspace アプリを使用できない UNIX ワークステーションにアプリケーションを配布する場合は、プロキシサーバーとして機能するサーバーが 1 台必要です。たとえば、Linux を実行している PC をサーバーとして使用できます。

アプリケーションは、ICA プロトコルの機能を使用して、X11 の最終デバイスに提供されます。デフォルトで、プロキシサーバー上のドライブにアクセスするには、ドライブマッピング機能を使う方法しかありません。(通常はローカルドライブがない) X 端末を使用している場合は、この設定で問題ありません。ほかの UNIX ワークステーションにアプリケーションを配布する場合は、次のいずれか実行できます:

- ローカルの UNIX ワークステーションを NFS を使ってプロキシサーバーにマウントし、プロキシサーバー上の NFS マウントポイントをクライアントドライブとしてマップしてアクセスする。
- SAMBA などの NFS から SMB へのプロキシサーバー、または Microsoft Services for UNIX などのサーバー上の NFS クライアントを使用する。

次の機能は、最終デバイスに提供されません:

- USB リダイレクト
- スマートカードリダイレクト
- COM ポートリダイレクト
- プロキシとして機能するサーバーがオーディオをサポートしている場合でも、X11 デバイスではオーディオを使用できません。
- クライアントプリンターは、X11 デバイスでは使用できません。LPD 印刷機能を使ってサーバーから UNIX プリンターに手でアクセスするか、ネットワークプリンターを使用します。
- マルチメディア入力のリダイレクトはサポートしていません。これは、Citrix Workspace アプリを実行しているマシン上でサーバーがプロキシとして機能するためには Web カメラが必要なためです。GStreamer がインストールされたサーバーがプロキシとして機能する場合、マルチメディア出力のリダイレクトをサポートします（未テスト）。

X 端末または UNIX ワークステーションから Citrix Workspace アプリをサーバー側 ICA として起動するには：

1. ssh または telnet を使って、プロキシとして動作しているデバイスに接続します。
2. プロキシデバイスのシェルで、**DISPLAY** 環境変数をローカルデバイスに設定します。たとえば、C シェルでは、次のように入力します：

```
setenv DISPLAY <local:0>
```

注：

コマンド `ssh -X` を使ってプロキシとして動作するデバイスに接続する場合は、**DISPLAY** 環境変数を設定する必要はありません。

3. ローカルデバイスのコマンドプロンプトで、次のように入力します： `xhost <proxy server name>`
4. Citrix Workspace アプリがデフォルトのインストールディレクトリにインストールされているかどうかを確認します。インストールされていない場合、環境変数 `ICAROOT` に実際のインストール先ディレクトリが指定されているか確認します。
5. Citrix Workspace アプリがインストールされているディレクトリを探します。コマンドプロンプトで「`selfservice &`」と入力します。

### サーバーからクライアントへのコンテンツリダイレクト

公開アプリケーションで使用しているファイル内に埋め込まれている特定の URL を、ローカルアプリケーションで開くように指定できます。たとえば、セッションで実行する Microsoft Outlook で Web ページへのリンクをクリックすると、その Web ページがユーザーデバイス上の Web ブラウザーで開きます。

管理者は、この機能を使ってサーバーの Citrix リソースをより効率よく配分し、ユーザー側のパフォーマンスを向上させることができます。次の種類の URL をクライアントにリダイレクトできます。

- HTTP
- HTTPS
- RTSP (Real Player)

- RTSPU (Real Player)
- PNM (従来の Real Players)

URL は、次の場合にサーバーアプリケーションを使用して開かれます：

- Citrix Workspace アプリに適切なアプリケーションがない
- Citrix Workspace アプリがコンテンツに直接アクセスできない

サーバーからクライアントへのコンテンツのリダイレクトはサーバー上で構成されています。この機能は、パスに以下が含まれている場合、Citrix Workspace アプリでデフォルトで有効になっています：

- RealPlayer
- Firefox、Mozilla、または Netscape のいずれか。

RealPlayer と Web ブラウザーがパスにない場合に、サーバーからクライアントへのコンテンツリダイレクト機能を有効にするには：

1. 構成ファイル `wfclient.ini` を開きます。
2. [Browser] セクションで、次の設定を変更します。

Path=<path>

Command=<command>

ここで <path> は、Web ブラウザーの実行ファイルのディレクトリです。また、<command> はリダイレクトされる URL を処理する実行ファイルの名前で、サーバーから送信される URL に追加されます。例：

`$ICAROOT/ns\launch Netscape, Firefox, Mozilla`

このコマンドにより、以下が実行されます：

- 既存の Web ブラウザーウィンドウに URL を渡す `ns\launch` ユーティリティが起動します。
- リストで指定された各 Web ブラウザーを順番に試行して、コンテンツを表示します。

3. [Player] セクションで、次の設定を変更します：

Path=<path>

Command=<command>

ここで <path> は、RealPlayer の実行ファイルのディレクトリです。また、<command> はリダイレクトされるマルチメディア URL を処理する実行ファイルの名前で、サーバーから送信される URL に追加されます。

4. ファイルを保存して閉じます。

注：

どちらのパス設定においても、Web ブラウザーおよび RealPlayer 実行ファイルが利用可能なディレクトリを指定する必要があります。実行ファイルのフルパスは必要ありません。たとえば、[Browser] セクションではパスの値は `/usr/X11R6/bin/netscape` ではなく、`/usr/X11R6/bin` となります。また、追加のディレクトリ名をコロンで区切って指定できます。この値を指定しない場合、`$PATH` が使用されます。

Citrix Workspace で、サーバーからクライアントへのコンテンツリダイレクト機能を無効にするには:

1. 構成ファイル `module.ini` を開きます。
2. `CREnabled` 設定を `Off` に変更します。
3. ファイルを保存して閉じます。

### 接続

#### 接続の構成

デバイスのプロセッサの処理能力や接続に使用する帯域幅が限られている場合は、使用する機能とパフォーマンスのバランスを考慮する必要があります。ユーザーおよび管理者は、パフォーマンスを低下させずに多くの機能を利用できるように、構成を変更することができます。サーバーまたはユーザーデバイスで次の変更を行うと、接続に必要な帯域幅を減らしてパフォーマンスを向上させることができます。

- **SpeedScreen** の有効化 - SpeedScreen を有効にすると、遅延時間の長いネットワーク接続のパフォーマンスが向上し、ユーザーの入力やマウスのクリックに対する反応時間が短くなります。この構成は、サーバー上で SpeedScreen 管理ツールを使用して行います。デフォルトでは、Citrix Workspace アプリでは、この機能はキーボードに対して無効になっています。この機能は、高遅延接続のマウスでのみ有効になります。詳しくは、『[Citrix Workspace app for Linux OEM's Reference Guide](#)』を参照してください。
- データ圧縮の有効化 - データを圧縮すると、接続を介して転送されるデータ量が減少します。この構成にはデータの圧縮と展開を行うためのプロセッサリソースがさらに必要になりますが、低帯域幅接続でのパフォーマンスを向上させることができます。この機能を有効にするには、**Citrix** ポリシーの [音質] および [イメージ圧縮] 設定を使用します。
- ウィンドウサイズの縮小 - ウィンドウサイズを必要最小限に抑えます。ファームでセッションオプションを設定します。
- 表示色数の変更 - 表示色数を 256 色に変更します。Citrix Virtual Apps and Desktops または Citrix DaaS サイトで、[セッションオプション] を設定します。
- 音質の変更 - サウンドのサポート機能を使用する場合は、Citrix ポリシーの [音質] 設定で音質を下げます。

トラブルシューティングについて詳しくは、トラブルシューティングのセクションの「[接続](#)」を参照してください。

### フォント

#### ClearType フォントスムージング

ClearType フォントスムージングにより、次の方法で表示フォントの質が向上します:

- 従来のフォントスムージングまたは、
- アンチエイリアス。

ClearType フォントスムージングは、サブピクセルフォントレンダリングとも呼ばれます。この機能は、有効または無効にできます。

次の手順に従い、スムージングのタイプを指定することもできます:

1. 適切な構成ファイルの [WFClient] セクションに移動します。
2. 次の設定を編集します:

FontSmoothingType = <number>

<number> に以下のいずれかの値を設定します:

値	動作
0	デバイス側の設定が適用されます。この値は、 <b>FontSmoothingTypePref</b> で定義します。
1	スムージング処理なし
2	標準のスムージング
3	ClearType (水平サブピクセル) スムージング

標準スムージングまたは ClearType スムージングを使用すると、Citrix Workspace アプリで消費される帯域幅が増加することがあります。

**重要:**

サーバー側の設定は、ICAファイルのFontSmoothingTypeで定義できます。この値は、[WFClient] の設定よりも優先されます。

サーバーがこの値を 0 に設定する場合、[WFClient] の次の設定によりローカルの動作が決定されます:

FontSmoothingTypePref = number

<number> に以下のいずれかの値を設定します:

値	動作
0	スムージング処理なし
1	スムージング処理なし
2	標準のスムージング
3	ClearType (水平サブピクセル) スムージング (デフォルト)

### フォルダー

#### ユーザーフォルダーのリダイレクトの構成

この機能では、ユーザーごとに個別に設定される以下の 2 つのユーザーフォルダー（特殊フォルダー）が対象になります。

- ユーザーのデスクトップフォルダー
- ユーザーのドキュメントフォルダー（Windows XP ではマイドキュメント）

ユーザーフォルダーのリダイレクトを使用すると、ユーザーの特殊フォルダーの場所を指定できます。その結果、サーバーの種類やファーム構成が異なってもこれらのフォルダーに一貫してアクセスできるようになります。たとえば、異なるサーバーファームのサーバーにログオンする必要があるモバイルユーザーなどにとって便利な機能です。常に同じサーバーファーム内のサーバーにログオンする静的な社内ワークステーションの場合、この機能はあまり必要ではありません。

ユーザーフォルダーのリダイレクトを構成するには：

module.ini ファイルにエントリを追加してユーザーフォルダーのリダイレクトを設定し、次のようにフォルダーの場所を指定します：

1. 次の文字列を module.ini（\$ICAROOT/config/module.ini など）に追加します。

```
[ClientDrive]
```

```
SFRAllowed = True
```

```
DocumentsFolder = <documents>
```

```
DesktopFolder = <desktop>
```

ここで <documents> と <desktop> は、それぞれユーザーの Documents フォルダーおよび Desktop フォルダーとして使用するディレクトリの UNIX ファイル名（フルパス）です。例：

```
DesktopFolder = $HOME/.ICAClient/desktop
```

- \$HOME などの環境変数として、パスで任意のコンポーネントを指定できます。
- 両方のパラメーターの値を指定します。
- 指定するディレクトリは、クライアントデバイスのマッピングで使用可能なディレクトリです。つまり、マップされたクライアントデバイスのサブツリーに存在する必要があります。
- ドライブ文字として、C またはそれ以降を使用します。

#### クライアント側ドライブのマッピング

クライアント側ドライブのマッピング機能により、Citrix Virtual Apps and Desktops サーバーおよび Citrix DaaS サーバーのドライブ文字をローカルユーザーデバイスにあるディレクトリにリダイレクトできます。たとえば、Citrix ユーザーセッション内で表示される H ドライブにアクセスしたときに、Workspace アプリを実行するローカルユーザーデバイスの特定のディレクトリにリダイレクトされるように設定できます。



クライアントドライブマッピングは、ローカルユーザーデバイスに任意のディレクトリをマウントできます。ローカルユーザーデバイスには、セッション中にユーザーが使用できる CD-ROM、DVD、または USB メモリスティックが含まれます。また、ローカルユーザーには、ローカルユーザーデバイスにアクセスする権限があります。サーバーがクライアントドライブマッピングを許可するように構成されている場合：

- ユーザーはローカルに保存されたファイルにアクセスできます
- セッション中にファイルを使用します
- 次に、それらをローカルドライブまたはサーバー上のドライブに再度保存します。

Citrix Workspace アプリは、Citrix Virtual Apps and Desktops サーバーおよび Citrix DaaS サーバーへの接続に対してクライアントデバイスのマッピングをサポートします。この機能によって、サーバー上で実行しているリモートアプリケーションから、ローカルのユーザーデバイスに接続しているデバイスにアクセスできるようになります。ユーザーデバイスのユーザーには、アプリケーションやシステムなどのリソースがローカルで実行されているように表示されます。クライアントデバイスのマッピングを実行する前に、サーバーでこの機能をサポートしていることを確認します。

注：

SELinux (Security-Enhanced Linux) のセキュリティモジュールにより、クライアント側ドライブのマッピング機能と USB リダイレクト機能が正しく動作しなくなることがあります。このモデルは、Citrix Virtual Apps and Desktops と Citrix DaaS の両方に適用されます。これらの機能を使用する場合は、サーバー上でこれらの機能を構成する前に SELinux を無効にしてください。

2 種類のドライブマッピングを実行できます。

- 静的なクライアントドライブマッピング - ログオン時にユーザーデバイスの任意のファイルシステムがサーバー上の特定のドライブにマップされるように設定できます。たとえば、ユーザーのホームディレクトリの全部または一部または /tmp をマップするために使用できます。また、CD-ROM、DVD、USB メモリスティックなどの大容量記憶装置デバイスのマウントポイントをマップします。
- 動的なクライアントドライブマッピングでは、CD-ROM ドライブ、DVD ドライブ、USB メモリスティックなどの大容量記憶装置デバイスがマウントされるユーザーデバイス上のディレクトリが監視されます。セッション内で追加した新しいデバイスが、サーバーで使用可能な最初のドライブ文字に自動的にマップされます。

クライアント側デバイスのマッピングを無効にしない限り、Citrix Workspace アプリが Citrix Virtual Apps and Desktops または Citrix DaaS に再接続したときに、マッピングが再度確立されます。ポリシーを使用すると、クライアント側デバイスのマッピングを詳細に制御できます。詳しくは、[Citrix Virtual Apps and Desktops](#) のドキュメントを参照してください。

ユーザーがドライブマッピングを設定するときは、[環境設定] ダイアログボックスを使用します。

注：

デフォルトでは、静的なクライアントドライブマッピングを有効にすると自動的に動的なクライアントドライブマッピングも有効になります。後者を無効にして前者を有効にするには、`wfclient.ini` で `DynamicCDM` を **False** に設定します。

バージョン 2101 以降、マップされたドライブへのアクセスに追加のセキュリティ機能が提供されています。

セッション内のすべてのストアのマップされたドライブについて、アクセスレベルを選択できるようになりました。

アクセスレベルのダイアログが毎回表示されないようにするには、[今後は確認しない] オプションを選択します。設定はその特定のストアに適用されます。

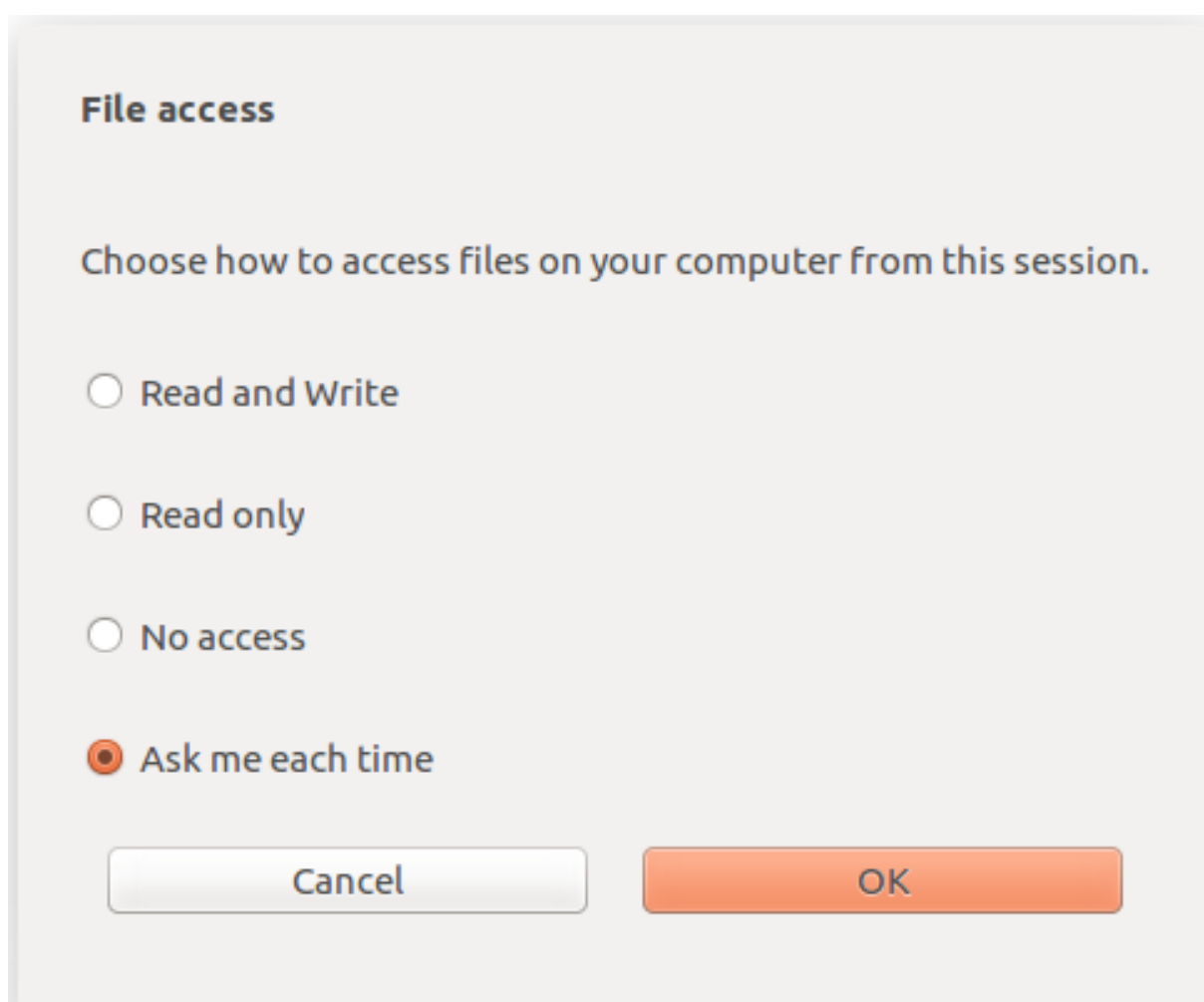
それ以外の場合は、セッションが開始されるたびに表示されるアクセスレベルを設定できます。

以前は、CDM によるファイルアクセスの設定は、すべての構成済みストアに適用されていました。

バージョン 2012 以降の Citrix Workspace アプリでは、ストアごとに CDM ファイルアクセスを構成できます。

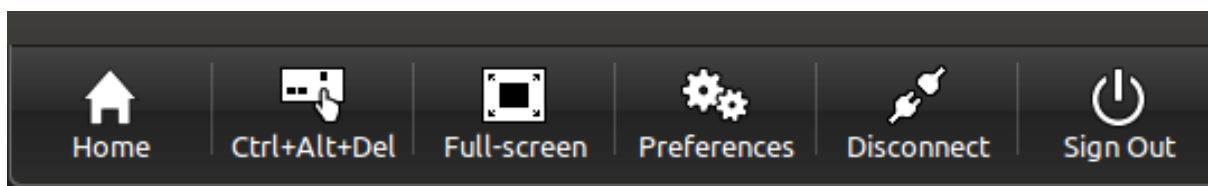
注:

Web 向け Workspace を使用する場合、ファイルアクセス設定はセッション間で永続的ではありません。デフォルトのオプションは、[毎回確認する] です。

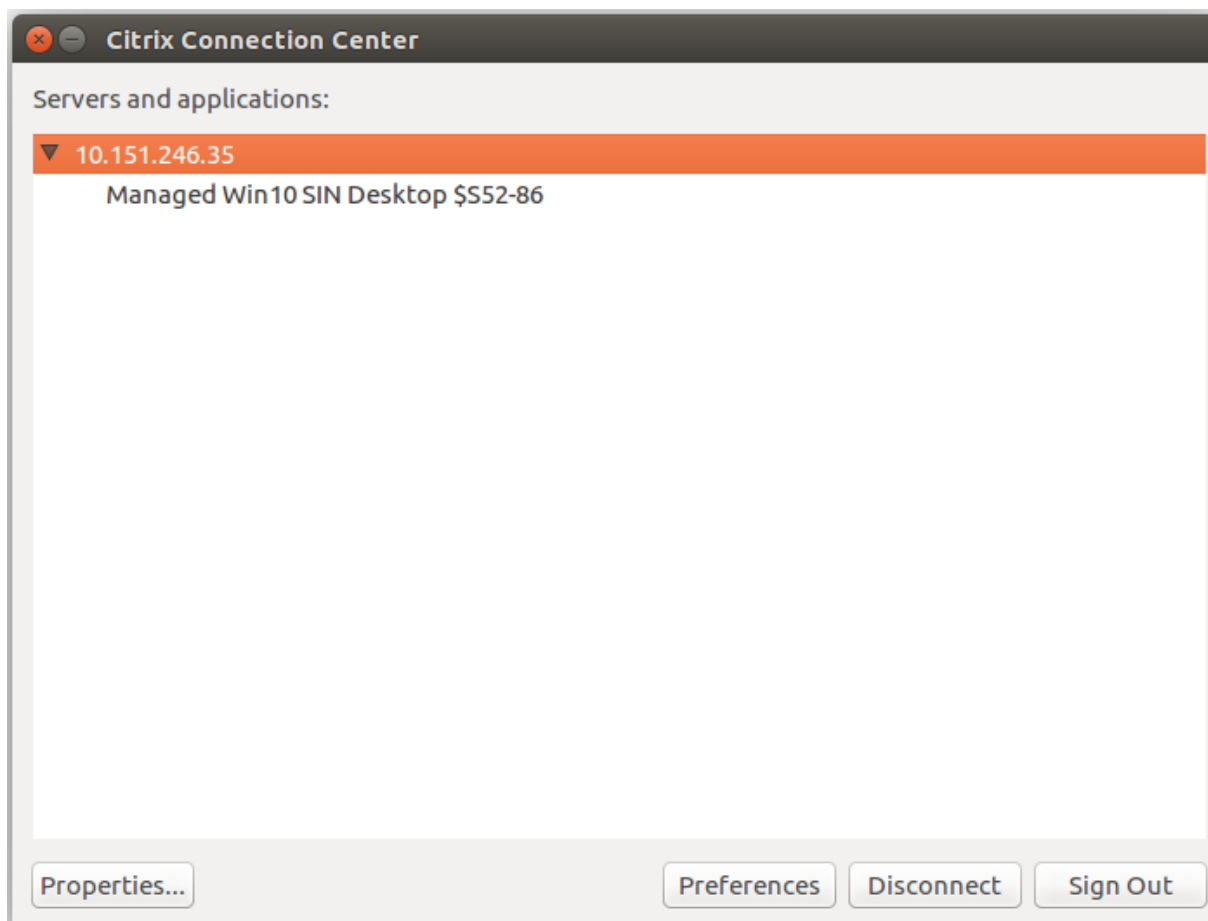


wfclient.iniファイルを使用して、マップされたパスとファイル名の属性を構成できます。上のスクリーンキャプチャに示されているように、GUI でファイルアクセスレベルを設定します。

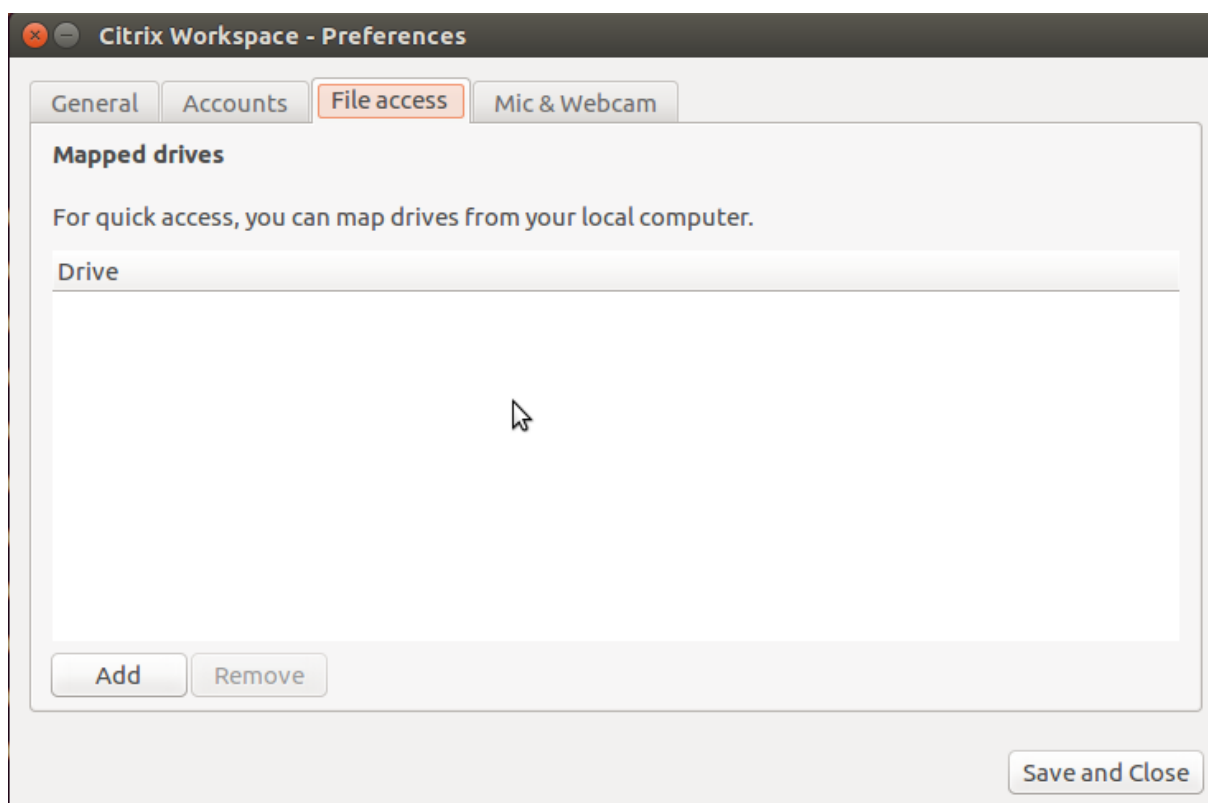
デスクトップセッションでは、Desktop Viewer で [基本設定] > [ファイルアクセス] ダイアログに移動して、ファイルアクセスレベルを設定できます。



アプリセッションでは、**Citrix Connection Center** から [ファイルアクセス] ダイアログを起動して、ファイルアクセスレベルを設定できます。



[ファイルアクセス] ダイアログには、マップされたフォルダー名とそのパスが含まれています。



アクセスレベルフラグは、`wfclient.ini` ファイルではサポートされなくなりました。

#### クライアントプリンターのマッピング

Citrix Workspace アプリは、ネットワークプリンターおよびユーザーデバイスにローカルで接続されているプリンターへの出力をサポートします。デフォルトでは、ポリシーを作成して変更しない限り、Citrix Virtual Apps and Desktops または Citrix DaaS により次のことを実行できます：

- ユーザーデバイスからアクセス可能なすべての印刷デバイスに出力する
- プリンターを追加する

ただし、これらの設定は、すべての環境で完全に対応しているとは限りません。たとえば、ユーザーデバイスからアクセスできるすべてのプリンターへの出力が可能なデフォルトの設定は、最も管理しやすい設定です。ただし、この設定は一部の環境ではログオンに時間がかかる要因となる可能性があります。このような状況では、ユーザーデバイス上で構成されたプリンターの一覧に制限するようにします。

このように、組織のセキュリティポリシーによってはローカルプリンターポートのマッピングをやめる必要があります。その場合は、サーバーの ICA ポリシーで [クライアント **COM** ポートを自動接続する] 設定を [無効] に設定します。

ユーザーデバイス上で構成されたプリンターの一覧を制限するには：

1. 次のいずれかの場所にある構成ファイル (`wfclient.ini`) を開きます。
  - `$HOME/.ICAClient` (1人のユーザーに対してプリンターを制限する場合)

- \$ICAROOT/config (すべての Workspace アプリユーザーに対してプリンターを制限する場合)。この場合の「すべてのユーザー」は、変更後に self-service プログラムを最初に使用したユーザーです。

2. [WFClient] セクションに、次のパラメーターを入力します。

```
ClientPrinterList=printer1:printer2:printer3
```

ここで printer1、printer2 などは、選択したプリンターの名前です。各プリンターをコロン (:) で区切って指定します。

3. ファイルを保存して閉じます。

### ローカルプリンターのマッピング

Linux 向け Citrix Workspace アプリは Citrix PS ユニバーサルプリンタードライバをサポートします。そのため、通常ネットワークプリンターまたはユーザーデバイスにローカルで接続されているプリンターへの出力をユーザーがローカルで構成する必要はありません。ユーザーデバイスのプリントソフトウェアがユニバーサルプリンタードライバをサポートしていない場合などは、Citrix Virtual Apps and Desktops または Citrix DaaS for Windows 上でクライアントプリンターを手動でマップすることがあります。

サーバーにローカルプリンターを割り当てるには：

1. Citrix Workspace アプリでサーバーへのセッションを開始して起動し、Citrix Virtual Apps and Desktops または Citrix DaaS サーバーにログオンします。
2. [スタート] ボタンをクリックし、[設定] > [プリンター] の順に選択します。
3. [ファイル] メニューから [プリンターの追加] を選択します。

プリンターの追加ウィザードが開きます。

4. ウィザードを使って、クライアントネットワークやクライアントドメインからネットワークプリンターを追加します。通常、この値が標準のプリンター名です。標準のプリンター名とは、ネイティブのリモートデスクトップサービスで使用される「セッション 3 の (クライアント名からの) HP LaserJet 4」などです。

プリンターの追加について詳しくは、Windows オペレーティングシステムのドキュメントを参照してください。

### オーディオ

バージョン 2112 以降、`module.ini` ファイルの `VdcamVersion4Support` 属性の名前が `AudioRedirectionV4` に変更されました。バージョン 2212 以降、`AudioRedirectionV4` のデフォルト値は **True** に設定されています。次のような結果になります：

- PulseAudio ライブラリはオーディオデバイスへのアクセスに使用され、追加のデバイスがサポートされています。
- 一度に複数のアプリがオーディオデバイスを使用できます。

- Citrix Workspace アプリは、セッションで使用可能なすべてのローカルオーディオデバイスを表示します。Citrix HDX Audio の代わりに、それぞれのデバイス名で表示されるようになりました。セッションでは、使用可能な任意のデバイスに動的に切り替えることができます。
- オーディオデバイスを接続または削除すると、セッションは動的に更新されます。

AudioRedirectionV4の値を **False** に設定した場合:

- ALSA ライブラリはオーディオデバイスへのアクセスに使用され、単一のデバイスのみがサポートされます。
- Citrix HDX Audio という名前のデフォルトのオーディオデバイスのみがセッションに表示されます。
- Citrix HDX Audio デバイスを一度に使用できるアプリは 1 つだけです。

AudioRedirectionV4を **False** に設定するには、次の手順を実行します:

1. <ICAROOT>/configフォルダーに移動し、module.iniファイルを開きます。

2. [ClientAudio] セクションに移動し、次のエントリを追加します:

```
AudioRedirectionV4=False
```

3. 変更を保存するには、セッションを再起動します。

### オーディオ録音のサポート

バージョン 2212 以降、オーディオ録音機能はデフォルトで有効になっています。セッションが開始されると、オーディオを録音するデバイスが表示されます。

この機能を無効にするには、wfclient.iniファイルでAllowAudioInputの値を *False* に設定します。

注:

- [設定] ダイアログボックスの [マイクと **Web** カメラ] オプションは、デフォルトでは無効です。マイクと Web カメラを有効にする方法については、「[基本設定](#)」を参照してください。
- Citrix Workspace アプリバージョン 2010 では、マルチストリーム ICA 機能改善に関する問題は解決されています。

既知の制限事項:

デフォルトでは、AudioRedirectionV4の値は **True** に設定されています。AudioRedirectionV4の値が **True** に設定されている場合、次の既知の制限が存在します:

- root 権限でコマンドラインインターフェイスからセッションを起動する場合、PulseAudio サーバーに接続しようとする、接続が拒否されることがあります。この場合、オーディオデバイスは、単一のデバイスのみをサポートする ALSA ライブラリの使用を開始する可能性があります。

AudioRedirectionV4の値を **False** に設定している場合、次の既知の制限があります:

- Windows Server 2016 で実行されている VDA では、セッションでオーディオデバイスの選択を変更することはできません。選択は、デフォルトのオーディオ入力および出力のみに設定されます。この制限は、AudioRedirectionV4の値を **True** に設定すると解消されます。

- オーディオデバイスのリダイレクトは、Bluetooth オーディオデバイスではサポートされていません。この制限は、`AudioRedirectionV4`の値を **True** に設定すると解消されます。
- デフォルトのオーディオデバイスは、Windows 10、Windows 7、および Windows 8 オペレーティングシステムでのみ変更できます。Windows Server 2012、2016、2019 などの Windows Server オペレーティングシステムでは、デフォルトのオーディオデバイスを変更することはできません。この問題は、Microsoft リモートデスクトップセッションの制限によるものです。
- オーディオデバイスのリダイレクトは、HDMI オーディオデバイスではサポートされていません。この制限は、`AudioRedirectionV4`の値を **True** に設定すると解消されます。ただし、Citrix Workspace アプリは、セッションで接続されていない HDMI オーディオデバイスを表示する場合があります。

`AudioRedirectionV4`の値が **False** の場合、デフォルトのオーディオデバイスは、一般的にはシステムに対して構成されているデフォルトの ALSA デバイスです。次の方法を使って、別のデバイスを指定します。

1. 変更を適用するユーザーの構成ファイルを選択して開きます。ほかのユーザーに適用される特定の設定ファイルを更新する方法については、「[デフォルト設定](#)」を参照してください。
2. 次のオプションを追加して、必要に応じてセクションを作成します：

```
1 [ClientAudio]
2
3 AudioDevice = \<device\>
4 <!--NeedCopy-->
```

このセクションで、デバイス情報は、オペレーティングシステム上の ALSA 構成ファイルにあります。

### 注：

この情報の場所は、すべての Linux オペレーティングシステムでの標準ではありません。Citrix ではこの情報の場所について、使用されているオペレーティングシステムのドキュメントを確認することをお勧めします。

### オーディオ品質の強化

これまで、Citrix Workspace アプリでオーディオをスムーズに再生するための最大出力バッファリング値は 200 ミリ秒でした。この値により、再生時には 200 ミリ秒の遅延が追加されていました。この最大出力バッファリング値は、インタラクティブオーディオアプリケーションにも影響を与えていました。

この機能拡張により、Citrix Workspace アプリの最大出力バッファリング値が 50 ミリ秒に低減され、インタラクティブオーディオアプリケーションのユーザーエクスペリエンスが向上しました。また、ラウンドトリップ時間 (RTT) が 150 ミリ秒短縮されました。

バージョン 2207 以降、適切な再生しきい値とパルスオーディオプリバッファを選択して、オーディオ品質を向上させることができます。この機能拡張向けに、次のパラメーターが `module.ini` ファイルの `[ClientAudio]` セクションに追加されています：

- `PlaybackDelayThreshV4` – 出力バッファリングの初期レベルをミリ秒単位で指定します。Citrix Workspace アプリは、セッション継続中、このレベルのバッファリングを維持しようと

努めます。`PlaybackDelayThreshV4`のデフォルト値は 50 ミリ秒です。このパラメーターは、`AudioRedirectionV4`が **True** に設定されている場合にのみ有効です。

- `AudioTempLatencyBoostV4` – オーディオスループットが急上昇した場合、または不安定なネットワークに対して十分でない場合、この値によって出力バッファリング値を増加させます。出力バッファリング値の増加により、スムーズなオーディオが提供されます。ただし、音声が若干遅れる場合があります。`AudioTempLatencyBoostV4`のデフォルト値は 100 ミリ秒に設定されています。このパラメーターは、`AudioRedirectionV4`が **True** に設定され、`AudioLatencyControlEnabled`が **True** に設定されている場合にのみ有効です。デフォルトでは、`AudioLatencyControlEnabled`の値は True に設定されています。

デフォルトでは、`AudioRedirectionV4`の値は True に設定されています。この機能を無効にするには、次の手順を実行します：

1. `<ICAROOT>/config`フォルダーに移動し、`module.ini` ファイルを開きます。
2. `[ClientAudio]` セクションに移動し、次のエントリを追加します：  
`AudioRedirectionV4=False`
3. 変更を保存するには、セッションを再起動します。

#### オーディオエコーキャンセルのサポートの改善

バージョン 2303 以降、Citrix Workspace アプリではエコーキャンセルがサポートされます。この機能はリアルタイムのユーザーケース向けに設計されており、ユーザーエクスペリエンスを向上させます。エコーキャンセル機能は、低品質、中品質、およびアダプティブオーディオをサポートします。パフォーマンスを向上させるために、アダプティブオーディオを使用することを Citrix ではお勧めします。

デフォルトでは、エコーキャンセル機能は無効になっています。リアルタイムのユーザーケースで、ヘッドセットの代わりにスピーカーを使用する場合は、エコーキャンセルをオンにすることをお勧めします。

この機能を有効にするには、次の手順を実行します：

1. `<ICAROOT>/config`フォルダーに移動し、`module.ini`ファイルを開きます。
2. `[ClientAudio]` セクションに移動して、`EnableEchoCancellation`パラメーターの値を次のように更新します：

```
EnableEchoCancellation =TRUE
```

#### 制限事項：

設計上、高品質のオーディオではエコーキャンセル機能は無効になっています。

#### クライアント側のジッターバッファメカニズムの追加

バージョン 2305 より、Citrix Workspace アプリでは、ネットワーク遅延が変動してもクリアなオーディオが保証されます。この機能は、デフォルトで有効になります。



この機能を無効にするには、`/opt/Citrix/ICAClient/config/module.ini`構成ファイルに移動し、`JitterBufferEnabled=FALSE`を編集します。

### クライアントオーディオのマッピング

クライアントオーディオマッピングにより、Citrix Virtual Apps and Desktops サーバーまたは Citrix DaaS サーバー上で実行しているアプリケーションのサウンドを、ユーザーデバイスにインストールされているサウンドデバイスで再生できます。管理者はサーバーで接続ごとに音質レベルを設定できますが、ユーザーもユーザーデバイスで音質レベルを設定できます。ユーザーデバイスとサーバーの音質レベルの設定が異なる場合は、低い方の音質レベルが使用されます。

クライアントオーディオマッピングを使用すると、サーバーとネットワークに大きな負荷がかかります。音質を高くすると、オーディオデータの伝送により多くの帯域幅が必要になります。また高音質にするとサーバーの CPU もより多く使用します。

クライアントオーディオマッピングは、ポリシーを使用して構成できます。詳しくは、[Citrix Virtual Apps and Desktops](#)のドキュメントを参照してください。

### アダプティブオーディオ

バージョン 2109 以降、Citrix Workspace アプリではアダプティブオーディオがサポートされます。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手動で構成する必要がありません。アダプティブオーディオは環境の設定を最適化し、古いオーディオ圧縮形式を置き換えることで、優れたユーザーエクスペリエンスを提供します。アダプティブオーディオはデフォルトで有効になっています。詳しくは、「[アダプティブオーディオ](#)」を参照してください。

バージョン 2112 以降、ユーザーデータグラムプロトコル (UDP) オーディオ配信の使用時に、アダプティブオーディオが機能するようになります。

既知の制限事項：

- アダプティブオーディオには、Streaming SIMD Extensions (SSE) 4.x がサポートされている CPU プロセッサが必要です。SSE 4.x がサポートされていない CPU プロセッサでアダプティブオーディオを使用すると、Citrix Workspace アプリが終了する場合があります。

### UDP オーディオの有効化

UDP オーディオ機能を有効にすると、インターネット接続を介した通話品質が向上します。TCP の代わりに UDP を使用します。

バージョン 2112 以降、UDP オーディオ配信の使用時にアダプティブオーディオが機能するようになります。また、このバージョンから、Citrix Workspace アプリでは、UDP オーディオのデータグラムトランスポート層セキュリティ (DTLS) プロトコルがサポートされます。その結果、Citrix Gateway を介して UDP オーディオにアクセスできます。デフォルトでは、この機能は無効になっています。

バージョン 2202 より、Citrix Workspace アプリでは、Citrix Gateway を介した UDP オーディオをサポートします。

UDP オーディオを有効にするには：

1. `module.ini` ファイルの `[ClientAudio]` セクションで、以下のオプションを設定します：
  - `EnableUDPAudio` を **True** に設定します。デフォルトでは、この値は **False** に設定されており、UDP オーディオは無効になっています。
  - `UDPAudioPortLow` および `UDPAudioPortHigh` に、UDP オーディオで使用されるポート番号の最小値および最大値をそれぞれ指定します。デフォルトでは、ポート 16500～16509 が使用されます。
2. デフォルトでは、アダプティブオーディオは VDA で有効になっており、UDP オーディオをサポートしています。アダプティブオーディオが無効になっている場合、UDP オーディオをサポートするには、クライアント側およびサーバー側のオーディオ設定を以下のように構成します。その場合、結果として得られるオーディオの品質は中レベルの音質です（つまり、高品質でも低品質でもありません）。

		クライアント側の音質レベル	クライアント側の音質レベル	クライアント側の音質レベル
		高	中	低
サーバー側の音質レベル	高	高	中	低
サーバー側の音質レベル	中	中	中	低
サーバー側の音質レベル	低	低	低	低

Citrix Gateway を介して UDP オーディオを有効にするには：

1. `<ICAROOT>/config` フォルダーに移動し、`module.ini` ファイルを開きます。
2. `[WFClient]` セクションに移動し、次のエントリを設定します：
 

```
EnableUDPThroughGateway=True
```
3. `[ClientAudio]` セクションに移動し、次のエントリを設定します：
 

```
EnableUDPAudio=True
```

注：

StoreFront default.ica 構成を使用する場合、`[Application]` セクションで設定された `EnableUDPThroughGateway` の値は、`module.ini` ファイルで設定された値よりも優先されます。ただし、`module.ini` ファイルのみを使用して `[ClientAudio]` セクションの `EnableUDPAudio` 値を設定できます。また、この値が StoreFront default.ica 構成で設定された値よりも優先されることはありません。

制限事項：

- 暗号化されたセッション（TLS または ICA 暗号化を使用するセッション）では、UDP オーディオを使用できません。このようなセッションでは、TCP 上でオーディオデータが転送されます。
- ICA チャンネルの優先度により、UDP オーディオの動作が異なります。

#### クライアント上の **UDP**

1. `$ICAROOT/config/module.ini`ファイルに移動します。

2. [ClientAudio] セクションで次のように設定します：

```
EnableUDPAudio=True
```

```
UDPAudioPortLow=int
```

```
UDPAudioPortHigh=int
```

3. [WFClient] セクションで次のように設定します：

```
EnableUDPThroughGateway=True
```

4. `$HOME/.ICAClient/wfclient.ini`ファイルに移動します。

5. [WFClient] セクションで次のように設定します：

```
AllowAudioInput=True
```

```
EnableAudioInput=true
```

```
AudioBandWidthLimit=1
```

注：

- [WFClient] セクションの `AllowAudioInput`、`EnableAudioInput` および `AudioBandWidthLimit` 属性に設定された値は、UDP オーディオと TCP オーディオの両方に適用できます。
- `.ICAClient` フォルダがない場合は（初回インストール後の起動のみ）、Citrix Workspace アプリを開始して、終了します。この操作により、`.ICAClient` フォルダが作成されます。
- `AudioBandWidthLimit` が 1 に設定されている場合、クライアント側の音質は Medium です。

6. Domain Delivery Controller (DDC) で次のポリシーを設定します：

- 「Windows Media redirection」に「Prohibited」を設定します。
- 「Audio over UDP」に「Allowed」を設定します。
- 「Audio over UDP real time transport」に「Enabled」を設定します。
- 「Audio quality」に「Medium」を設定します。

#### **Citrix Workspace** アプリの使用方法の変更

ICA 技術は高度に最適化されているため、通常、処理能力の高い CPU を搭載したクライアントデバイスや広い帯域幅を必要としません。ただし、接続の帯域幅が非常に狭い接続では、適切なパフォーマンスを得るために、次のことを考慮してください：

- クライアント側ドライブ上のサイズの大きいファイルにはアクセスしない。クライアントドライブマッピングを使ってファイルにアクセスすると、サーバーとの接続でそのファイルのデータが転送されることになります。低速接続では、このファイル転送に時間がかかることがあります。
- クライアント側のローカルプリンターで大きな文書を印刷しない。クライアント側のローカルプリンターで文書を印刷すると、サーバーとの接続でそのファイルのデータが転送されることになります。低速接続では、このファイル転送に時間がかかることがあります。
- マルチメディアコンテンツを再生しない。マルチメディアファイルを再生するには、広い帯域幅が必要です。そのため、パフォーマンスが低下する可能性があります。

## USB

USB サポート機能により、ユーザーが仮想デスクトップ上で作業しているときにさまざまな種類の USB デバイスを使用できるようになります。構成ファイル設定で自動リダイレクトを手動で有効にした後、ユーザーがコンピューターに USB デバイスを接続すると、仮想デスクトップ内でそのデバイスを操作できるようになります。USB デバイスの自動リダイレクトは、デフォルトでは無効になっています。リモートに使用できる USB デバイスには次のものがあります：

- フラッシュドライブ
- スマートフォン
- PDA
- プリンター
- スキャナー
- MP3 プレーヤー
- セキュリティデバイス
- タブレット

USB リダイレクトには、Citrix Virtual Apps and Desktops 7.6 またはそれ以降が必要です。

Web カメラ、マイク、スピーカー、およびヘッドセットなどの USB デバイスのアイソクロナス機能は、一般的な低遅延または高速 LAN 環境でサポートされます。ただし通常は、標準のオーディオや Web カメラのリダイレクトの方が適しています。

以下の種類のデバイスは直接サポートされるため、仮想アプリと仮想デスクトップのセッションで USB サポート機能は使用されません：

- キーボード
- マウス
- スマートカード
- ヘッドセット
- Web カメラ

注：

特殊用途の USB デバイス（Bloomberg キーボードや 3D マウスなど）では、USB サポート機能が使用され

るよう構成できます。そのほかの特殊用途の USB デバイスのポリシー規則の構成について詳しくは、[CTX119722](#)を参照してください。

デフォルトでは、特定の種類の USB デバイスが Citrix Virtual Apps and Desktops または Citrix DaaS で動作しないように設定されています。たとえば、内部 USB でシステムボードに装着された NIC は、リモートで動作する仮想デスクトップで NIC の使用には適しません。次の種類の USB デバイスは、仮想アプリおよび仮想デスクトップでの使用をデフォルトでサポートしていません：

- Bluetooth ドングル
- 統合された NIC
- USB ハブ

リモート操作可能な USB デバイスのデフォルトの一覧を更新するには、`$ICAROOT/`フォルダーにある `usb.conf` ファイルを編集します。詳しくは、「リモートで実行できる USB デバイスの一覧の更新」を参照してください。

エンドポイント側の USB デバイスを仮想デスクトップ内で使用できるようにするには、USB ポリシー規則を有効にする必要があります。詳しくは、[Citrix Virtual Apps and Desktops](#)のドキュメントを参照してください。

### USB サポートのしくみ

ユーザーが USB デバイスを接続すると、USB ポリシーに照らしてチェックされます。許可されている場合は、仮想デスクトップにリダイレクトされます。デフォルトのポリシーで拒否されるデバイスは、ローカルのデスクトップ上でのみ使用可能になります。

デスクトップアプライアンスモードを介してアクセスされるデスクトップにユーザーが USB デバイスを接続している場合、そのデバイスは、構成ファイル設定で自動リダイレクトを手動で有効にした後、仮想デスクトップに自動でリダイレクトされるようになります。USB デバイスの自動リダイレクトは、デフォルトでは無効になっています。USB デバイスの自動リダイレクトを構成するには、次の手順を実行します：

1. 構成ファイル `$Home/.ICAClient/wfclient.ini` に移動します。

2. 次のエントリを追加します：

```
DesktopApplianceMode=True
```

3. 構成ファイル `/opt/Citrix/ICAClient/usb.conf` に移動します。

4. 次のデバイスルールのいずれかを設定します：

- **CONNECT** – 「CONNECT」キーワードを設定すると、セッション開始時のデバイスの自動リダイレクトが有効になります。
- **ALLOW** – 「ALLOW」キーワードを設定すると、セッション開始後のみデバイスの自動リダイレクトが許可されます。  
ただし、「CONNECT」キーワードまたは「ALLOW」キーワードが設定されている場合、セッション中にデバイスのプラグを抜き差しすると、デバイスは自動リダイレクトされます。

サンプルデバイスルール:

CONNECT: vid=046D pid=0002 # vid/pid により特定のデバイスを許可する

ALLOW: vid=046D pid=0102 # vid/pid により特定のデバイスを許可する

デスクトップアプライアンスモードが使用中でない限り、ユーザーがリダイレクトを実行するためユーザーデバイスに接続するとき、セッションウィンドウにフォーカスがある必要があります。

既知の制限事項:

USB リダイレクトについて、`usb.conf`ファイルで定義されたポリシーが機能せず、USB デバイスがセッションにリダイレクトされないことがあります。この問題は、`usb.conf`ファイルの文字数が 2000 文字を超えている場合に発生します。回避策として、ポリシーへの既存のコメントを削除して、`usb.conf`ファイルの文字数を減らします。

### 大容量記憶装置デバイス

USB 大容量記憶装置デバイスがローカルデスクトップに接続されたままユーザーが仮想デスクトップを切断した場合、再接続しても、デバイスは仮想デスクトップにリダイレクトされません。大容量記憶装置デバイスが仮想デスクトップに接続されるようにするには、仮想デスクトップへの再接続後にデバイスを一度取り外してから再接続する必要があります。

注:

USB 大容量記憶装置デバイスのリモートサポートを拒否するように構成されている Linux ワークステーションに大容量記憶装置デバイスを接続すると、Citrix Workspace アプリはデバイスを受け入れず、別の Linux ファイルブラウザが開くことがあります。そのためユーザーデバイス上では、事前にリムーバブルストレージの [メディアが挿入されたら参照する] 設定を無効にしておくことを Citrix ではお勧めします。Debian ベースのデバイスでは、Debian メニューバーで [Desktop] > [Preferences] > [Removable Drives and Media] を選択します。[Storage] タブの [Removable Storage] で [Browse removable media when inserted] のチェックを外します。

クライアント USB デバイスのリダイレクトについては、次の点に注意してください。

注:

クライアント USB デバイスリダイレクトサーバーポリシーを有効にすると、クライアントドライブマッピングが有効な場合でも、大容量記憶装置デバイスは USB デバイスとして送信されます。

### USB のクラス

次の USB デバイスのクラスは、デフォルトの USB ポリシー規則により許可されます:

- オーディオ (クラス 01)
  - マイク、スピーカー、ヘッドセット、および MIDI コントローラーがあります。
- 物理的インターフェイス (クラス 05)

このデバイスは HID に似ていますが、一般的にはリアルタイムの入力またはフィードバックを提供します。また、フォースフィードバックジョイスティック、モーションプラットフォーム、およびフォースフィードバックエクソスケルトンなども含まれます。

- 静止画 (クラス 06)

このクラスのデバイスとして、デジタルカメラおよびスキャナーがあります。デジタルカメラは、画像転送プロトコル (PTP) またはメディア転送プロトコル (MTP) を使ってコンピューターやほかの周辺機器にイメージを転送する静止画クラスをサポートします。カメラは大容量記憶装置としても機能する場合があります。また、カメラ自体のメニューを使っていずれかのクラスを使用するように構成できます。

カメラが大容量記憶装置デバイスとして機能する場合はクライアントドライブマッピングが使用され、USB サポートは必要ありません。

- プリンター (クラス 07)

一部のプリンターではベンダー固有のプロトコル (クラス ff) が使用されますが、一般的にはこのクラスにほとんどのプリンターが含まれます。マルチ機能プリンターの場合は、USB ハブが内蔵されていたり、混合デバイスであったりする場合があります。いずれの場合も、印刷機能では一般的にプリンタークラスが使用され、スキャナーや FAX 機能では静止画などの別のクラスが使用されます。

プリンターは通常、USB サポートなしで適切に動作します。

- マスストレージデバイス (クラス 08)

最も一般的なマスストレージデバイス (大容量記憶装置) として、USB フラッシュドライブがあります。そのほかには、USB 接続のハードドライブ、CD/DVD ドライブ、および SD/MMC カードリーダーがあります。また、内部ストレージを持つさまざまな種類のデバイスが大容量記憶装置インターフェイスを使用します。これらのデバイスには、メディアプレーヤー、デジタルカメラ、スマートフォンなどが含まれます。既知のサブクラスには次のものが含まれます:

- 01 制限付きフラッシュデバイス
- 02 一般的な CD/DVD デバイス (ATAPI/MMC-2)
- 03 一般的なテープデバイス (QIC-157)
- 04 一般的なフロッピーディスクドライブ (UFI)
- 05 一般的なフロッピーディスクドライブ (SFF-8070i)
- 06 ほとんどの大容量記憶装置デバイスはこの SCSI のバリエーションを使用します

大容量記憶装置デバイスには、クライアントドライブマッピングを介して頻繁にアクセスすることができ、USB サポートは必要ありません。

重要: ウィルスプログラムの中には、あらゆる種類の大容量記憶装置デバイスを媒体にして活発に増殖するものがあります。クライアントドライブマッピングまたは USB サポートのいずれかを介した大容量記憶装置デバイスの使用を許可する業務上の必要性があるか、慎重に検討してください。このリスクを減らすため、クラ

イアントドライブマッピングによりファイルが実行されるのを防ぐようにサーバーを構成することができます。

注:

現在、ユーザーが汎用 USB リダイレクトを使用して USB 3.0 ドライバーを Linux VDA にリダイレクトする必要がある場合は、USB フラッシュドライブを USB 3.0 スロットに差し込んでください。

- コンテンツセキュリティ (クラス 0d)

通常、ライセンスまたはデジタル権利の管理のためのコンテンツ保護を実行します。このクラスのデバイスとして、ドングルがあります。

- パーソナルヘルスケア (クラス 0f)

これらのデバイスには、次のような個人用健康器具が含まれます:

- 血圧センサー
- 心拍数モニター
- 万歩計
- 薬剤モニター
- 肺活量計

- アプリケーションおよびベンダー固有 (クラス fe および ff)

多くのデバイスがベンダー独自のプロトコルまたは USB コンソーシアムで標準化されていないプロトコルを使用しており、これらのデバイスは通常はベンダー固有 (クラス ff) として分類されます。

### USB デバイスのクラス

次の USB デバイスのクラスは、デフォルトの USB ポリシー規則により拒否されます:

- 通信および CDC コントロール (クラス 02 および 0a)

モデム、ISDN アダプター、ネットワークアダプター、一部の電話および FAX 機器があります。

仮想デスクトップ自体への接続にこれらのデバイスのいずれかが使用される場合があるため、デフォルトの USB ポリシーではこれらのデバイスのリモートでの実行は許可されていません。

- ヒューマンインターフェイスデバイス (クラス 03)

さまざまな種類の入出力デバイスを含みます。一般的なヒューマンインターフェイスデバイス (HID) には、次が含まれます:

- キーボード
- マウス
- ポインティングデバイス
- グラフィックタブレット
- センサー



- ゲームコントローラー
- ボタン
- コントロール機能

Subclass 01 は起動インターフェイスクラスと呼ばれ、キーボードおよびマウスで使用されます。

デフォルトの USB ポリシーは USB キーボード (クラス 03、サブクラス 01、プロトコル 1) または USB マウス (クラス 03、サブクラス 01、プロトコル 2) を許可しません。この設定は、ほとんどのキーボードとマウスが USB のサポートを必要とすることなく適切に処理できるためです。通常、こうしたデバイスは仮想デスクトップ内だけでなくローカルでも使用する必要があります。

- USB ハブ (クラス 09)

USB ハブにより、追加のデバイスをローカルコンピューターに接続できます。これらのデバイスにリモートでアクセスする必要はありません。

- スマートカード (クラス 0b)

スマートカードリーダーには、非接触式および接触式のスマートカードリーダーがあり、また埋め込みスマートカード同等チップがある USB トークンもあります。

スマートカードリーダーは、スマートカードサポート機能によりアクセスできるため、USB サポートは必要ありません。

- ビデオ (クラス 0e)

ビデオクラスは、ビデオまたはビデオ関連の素材を操作するために使用される次のようなデバイスをカバーします:

- Web カメラ
- デジタルカムコーダー
- アナログビデオ変換機
- 一部のテレビチューナー
- ビデオストリーミングをサポートする一部のデジタルカメラ

デフォルトでは、HDX RealTime Web カメラビデオ圧縮機能により Web カメラのパフォーマンスが最適化されます。

- ワイヤレスコントローラー (クラス e0)

このクラスのデバイスとして、ウルトラワイドバンドコントローラーや Bluetooth など、さまざまなワイヤレスコントローラーがあります。

これらのデバイスの中には、重要なネットワークアクセスを提供していたり、Bluetooth キーボードやマウスなどの基幹周辺装置を接続していたりするものがあります。

デフォルトの USB ポリシーはこれらのデバイスを許可していません。ただし、USB サポートを使ったアクセスに適したデバイスもあります。

**USB** デバイスの一覧

仮想デスクトップセッション内で使用できる USB デバイスの範囲を更新できます。範囲を更新するには、`$ICAROOT/`のユーザーデバイスにある`usb.conf`ファイルでデフォルト規則の一覧を編集します。

新しいポリシー規則を追加して一覧を更新し、デフォルト範囲に含まれない USB デバイスを許可または拒否できます。この方法により管理者が作成した規則は、どのデバイスがサーバーに提供されるかを制御します。次にサーバー上で規則が、どのデバイスを許可するかを制御します。

デバイスのリモートでの実行を許可しないためのデフォルトポリシー構成は次のとおりです：

DENY: class=09 # Hub デバイス

DENY: class=03 subclass=01 # HID 起動デバイス (キーボードとマウス)

DENY: class=0b # スマートカード

DENY: class=e0 # ワイヤレスコントローラー

DENY: class=02 # 通信および CDC 制御

DENY: class=03 # UVC (Web カメラ)

DENY: class=0a # CDC データ

ALLOW: # 完全なフォールバック: すべてを許可

**USB** ポリシー規則

ヒント：ポリシー規則を作成する場合、次の USB Web サイトで USB クラスコードを参照してください：

<http://www.usb.org/>. ユーザーデバイス上の`usb.conf`ファイルで指定するポリシー規則は、「`{ALLOW:|DENY:}`」に次のタグの値をベースとした式セットが付いた形式にします：

タグ	説明
VID	デバイス記述子のベンダー ID
REL	デバイス記述子のリリース ID
PID	デバイス記述子の製品 ID
クラス	デバイス記述子またはインターフェイス記述子のクラス
SubClass	デバイス記述子またはインターフェイス記述子のサブクラス
Prot	デバイス記述子またはインターフェイス記述子のプロトコル

ポリシー規則を作成する場合、以下の点に注意してください：

- 大文字と小文字は区別されません。
- 規則の末尾に、「#」で始まる任意のコメントを追加できます。区切り文字は不要で、コメントは無視されます。
- 空白行およびコメントのみの行は無視されます。
- 区切りとして使用されるスペースは無視されますが、番号または識別子の間にスペースを入れることはできません。たとえば、Deny: Class=08 SubClass=05 は有効な規則ですが、Deny: Class=0 8 Sub Class=05 は無効です。
- タグには等号 (=) を使用する必要があります。たとえば、VID=1230 とします。

例

次の例は、ユーザーデバイス上の `usb.conf` ファイルのセクションを示しています。これらの規則を実装するには、サーバー上に同じ規則のセットがある必要があります。

```
ALLOW: VID=1230 PID=0007 \## ANOther Industries, ANOther Flash Drive
```

```
DENY: Class=08 SubClass=05 \## Mass Storage Devices
```

```
DENY: Class=0D \## All Security Devices
```

開始時のモード

デスクトップアプライアンスモードを使って、仮想デスクトップを開始したときに既に接続されているクライアント側の USB デバイスを有効にしたり無効にしたりできます。各ユーザーデバイスにある `$ICAROOT/config/module.ini` ファイルの **WfClient** セクションで、`DesktopApplianceMode = Boolean` を次のように設定します。

---

TRUE	すべての接続済みの USB デバイスは開始時に使用できます。デバイスが開始時に使用可能となるのは、サーバー（レジストリエントリ）またはユーザーデバイス（ポリシールール構成ファイル）の USB ポリシーでデバイスが拒否されていない場合のみです。
FALSE	開始時に使用できる USB デバイスはありません。

---

注：

「CONNECT」キーワードを設定すると、セッション開始時のデバイスの自動リダイレクトが有効になります。また、「ALLOW」キーワードを設定すると、セッション開始後にのみデバイスの自動リダイレクトが許可されます。ただし、「CONNECT」キーワードまたは「ALLOW」キーワードが設定されている場合、セッション中にデバイスのプラグを抜き差しすると、デバイスは自動リダイレクトされます。

## USB デバイスの自動リダイレクトの構成

以前は、セッション中にデバイスのプラグを抜き差しすると、デバイスは自動的にリダイレクトされ、VDA に自動的に接続されていました。Citrix Workspace アプリ 2207 リリース以降、構成ファイルの設定を介して手動で自動リダイレクトを有効にする必要があります。USB デバイスの自動リダイレクトは、デフォルトでは無効になっています。

USB デバイス（通常および複合デバイス）の自動リダイレクトを構成するには、次の手順を実行します：

1. 構成ファイル `$Home/.ICAClient/wfclient.ini` に移動します。
2. 次のエントリを追加します：  
`DesktopApplianceMode=True`
3. 構成ファイル `/opt/Citrix/ICAClient/usb.conf` に移動します。
4. 次のデバイスルールのいずれかを設定します：
  - **CONNECT** – 「CONNECT」キーワードを設定すると、セッション開始時のデバイスの自動リダイレクトが有効になります。
  - **ALLOW** – 「ALLOW」キーワードを設定すると、セッション開始後にはのみデバイスの自動リダイレクトが許可されます。

ただし、「CONNECT」キーワードまたは「ALLOW」キーワードが設定されている場合、セッション中にデバイスのプラグを抜き差しすると、デバイスは自動リダイレクトされます。

サンプルデバイス規則：

`CONNECT: vid=046D pid=0002 # vid/pid により特定のデバイスを許可する`

`ALLOW: vid=046D pid=0102 # vid/pid により特定のデバイスを許可する`

## 複合 USB デバイスリダイレクト

バージョン 2207 以降、Citrix Workspace アプリでは複合 USB デバイスを分割できるようになります。複合 USB デバイスは、複数の機能を実行できます。これらの機能は、各機能が異なるインターフェイスを使用することで可能となっています。複合 USB デバイスには、オーディオおよびビデオの入力および出力で構成されるヒューマンインターフェイスデバイス (HID) などが含まれます。

現在のところ、複合 USB デバイスリダイレクトは、デスクトップセッションでのみ利用できます。分割されたデバイスはデスクトップビューアに表示されます。

以前は、セッション中にデバイスのプラグを抜き差しすると、デバイスは自動リダイレクトされ、VDA に自動的に接続されていました。このリリース以降、構成ファイルの設定を介して手動で自動リダイレクトを有効にする必要があります。複合 USB デバイスの自動リダイレクトは、デフォルトでは無効になっています。

USB 2.1 以降は、複数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。この設定は USB ハブのものとは異なります。USB ハブでは、個別にアドレス指定された別の 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、デバイス全体がエンドポイントで使用できなくなります。この動作により、最適化された HDX リモートエクスペリエンスに必要な Citrix Workspace クライアントを含む、エンドポイント上のすべてのアプリケーションでのデバイスのローカル使用がブロックされます。

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 チャン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 オーディオチャン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 USB リモート処理経由でホスト側のオーディオドライバを使用して送信されるオーディオとは異なり、最適化された HDX オーディオチャンネル経由で送信されるオーディオでは、最高のエクスペリエンスを実現できます。これは、USB オーディオプロトコルの性質がノイズが多いためです。

また、システムキーボードまたはポインティングデバイスが、リモートセッションのサポートに必要な他の統合機能を備えた複合デバイスの一部である場合にも問題が発生します。完全な複合デバイスが転送されると、システムのキーボードまたはマウスは、リモートデスクトップセッションまたはアプリケーション内を除いて、エンドポイントで操作できなくなります。

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 チャン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。この設定により、最適化された HDX エクスペリエンスを提供する Citrix Workspace アプリなど、クライアントエンドポイント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、必要なデバイスのみを転送してリモートセッションで使用できるようになります。

デバイス規則：

通常の USB デバイスと同様に、転送する複合デバイスは、Citrix Workspace アプリの構成で設定されたデバイスルールに基づいて選択されます。Citrix Workspace アプリは、これらの規則を使用して、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。

それぞれの規則には、アクションキーワード（ALLOW、CONNECT、または DENY）、コロン（:）、エンドポイント USB サブシステムの実際のデバイスと一致する 0 個以上のフィルターパラメーターが含まれます。これらのフィルターパラメーターは、すべての USB デバイスが自身を識別するために使用する USB デバイスの記述子メタデータに対応します。

デバイス規則はクリアテキストであり、各規則は 1 行に表示され、オプションのコメントは # 文字の後に記載されています。規則はトップダウンで照合されます（優先度の降順）。デバイスまたは子インターフェイスに一致する最初の規則が適用されます。同じデバイスまたはインターフェイスを選択する後続の規則は無視されます。

デバイスルールを変更するには、次の手順を実行します：

1. /opt/Citrix/ICAClient/usb.conf ファイルに移動します。

2. 必要に応じてデバイスルールを更新します。

サンプルデバイス規則:

```
ALLOW: vid=046D pid=0102 ## Allow a specific device by vid/pid
```

```
ALLOW: vid=0505 class=03 subclass=01 ## Allow any pid for vendor 0505 w/  
subclass=01
```

```
DENY: vid=0850 pid=040C ## deny a specific device (including all child  
devices)
```

```
DENY: class=03 subclass=01 prot=01 ## deny any device that matches all  
filters
```

```
CONNECT: vid=0911 pid=0C1C ## Allow and auto-connect a specific device
```

```
ALLOW: vid=0286 pid=0101 split=01 ## Split this device and allow all  
interfaces
```

```
ALLOW: vid=1050 pid=0407 split=01 intf=00,01 ## Split and allow only 2  
interfaces
```

```
CONNECT: vid=1050 pid=0407 split=01 intf=02 ## Split and auto-connect  
interface 2
```

```
DENY: vid=1050 pid=0407 split=1 intf=03 ## Prevent interface 03 from being  
remoted
```

次のフィルターパラメーターのいずれかを使用して、検出されたデバイスに規則を適用できます:

フィルターパラメーター	説明
vid=xxxx	USB デバイスのベンダー ID (4 桁の 16 進コード)
pid=xxxx	USB デバイスの製品 ID (4 桁の 16 進コード)
rel=xxxx	USB デバイスのリリース ID (4 桁の 16 進コード)
class=xx	USB デバイスのクラスコード (2 桁の 16 進コード)
subclass=xx	USB デバイスのサブクラスコード (2 桁の 16 進コード)
prot=xx	USB デバイスのプロトコルコード (2 桁の 16 進コード)
split=1 (または split=0)	分割する (または分割しない) 複合デバイスを選択します

フィルターパラメーター	説明
intf=xx[,xx,xx,...]	複合デバイスの子インターフェイスの特定のセットを選択します (2 桁の 16 進コードのコンマで区切られた一覧)

最初の 6 つのパラメーターは、規則を適用する必要がある USB デバイスを選択します。パラメーターが指定されていない場合、規則はそのパラメーターが ANY の値を持つデバイスと一致します。

USB Implementors Forum (USB-IF) は、Defined Class Code のクラス、サブクラス、およびプロトコル値の定義済み一覧を維持管理しています。USB-IF は、登録されたベンダー ID の一覧も所有しています。特定のデバイスのベンダー、製品、リリース、およびインターフェイス ID は、lsusb などの無料ツールを使用して確認できます：

```

1  <username@username>-ThinkPad-T470:/var/log$ lsusb
2
3  Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
4
5  Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
6
7  Bus 002 Device 002: ID 0bda:0316 Realtek Semiconductor Corp. USB3.0-CRW
8
9  Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
10
11 Bus 001 Device 005: ID 138a:0097 Validity Sensors, Inc.
12
13 Bus 001 Device 004: ID 5986:111c Acer, Inc Integrated Camera
14
15 Bus 001 Device 003: ID 8087:0a2b Intel Corp.
16
17 Bus 001 Device 006: ID 17ef:609b Lenovo Lenovo USB Receiver
18
19 Bus 001 Device 045: ID 1188:a001 Bloomberg L.P. Lenovo USB Receiver
20
21 Bus 001 Device 044: ID 1188:a301 Bloomberg L.P.
22
23 Bus 001 Device 043: ID 1188:a901 Bloomberg L.P. Keyboard Hub
24
25 Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
26
27 <!--NeedCopy-->

```

```

1  | <username@username>-ThinkPad-T470:/var/log$ lsusb -t
2

```

```
3   /: Bus 04.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 10000
   M
4
5   /: Bus 03.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 480M
6
7   /: Bus 02.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/6p, 5000M
8
9   |__ Port 3: Dev 2, If 0, Class=Mass Storage, Driver=usb-storage,
   5000M
10
11  /: Bus 01.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/12p, 480M
12
13  |__ Port 1: Dev 43, If 0, Class=Hub, Driver=hub/4p, 480M
14
15      |__ Port 1: Dev 46, If 0, Class=Human Interface Device, Driver=
         usbhid, 12M
16
17      |__ Port 4: Dev 45, If 0, Class=Human Interface Device, Driver=
         usbhid, 12M
18
19      |__ Port 4: Dev 45, If 1, Class=Human Interface Device, Driver=
         usbhid, 12M
20
21      |__ Port 2: Dev 44, If 3, Class=Audio, Driver=snd-usb-audio, 12
         M
22
23      |__ Port 2: Dev 44, If 1, Class=Vendor Specific Class, Driver=,
         12M
24
25      |__ Port 2: Dev 44, If 4, Class=Audio, Driver=snd-usb-audio, 12
         M
26
27      |__ Port 2: Dev 44, If 2, Class=Audio, Driver=snd-usb-audio, 12
         M
28
29      |__ Port 2: Dev 44, If 0, Class=Human Interface Device, Driver=
         usbhid, 12M
30
31      |__ Port 4: Dev 6, If 1, Class=Human Interface Device, Driver=
         usbhid, 12M
32
33      |__ Port 4: Dev 6, If 2, Class=Human Interface Device, Driver=
         usbhid, 12M
34
35      |__ Port 4: Dev 6, If 0, Class=Human Interface Device, Driver=
```



```
usbhid, 12M
36
37 |__ Port 7: Dev 3, If 0, Class=Wireless, Driver=btusb, 12M
38
39 |__ Port 7: Dev 3, If 1, Class=Wireless, Driver=btusb, 12M
40
41 |__ Port 8: Dev 4, If 1, Class=Video, Driver=uvcvideo, 480M
42
43 |__ Port 8: Dev 4, If 0, Class=Video, Driver=uvcvideo, 480M
44
45 |__ Port 9: Dev 5, If 0, Class=Vendor Specific Class, Driver=, 12M
46 |
47 <!--NeedCopy-->
```

最後の2つのパラメーター（存在する場合）はUSB複合デバイスにのみ適用されます。splitパラメーターは、複合デバイスを分割デバイスとして転送するか、単一の複合デバイスとして転送する必要があるかを決定します。

Split=1は、複合デバイスの選択された子インターフェイスは分割デバイスとして転送する必要があることを示します。

Split=0は、複合デバイスを分割するべきではないことを示します。

注:

splitパラメーターを省略した場合、Split=0と見なされます。

intfパラメーターでは、アクションを適用する必要がある複合デバイスの特定の子インターフェイスを選択します。省略した場合、アクションは複合デバイスのすべてのインターフェイスに適用されます。

6つのインターフェイスを備えた複合USBデバイス（たとえば、Bloomberg 4 キーボード）について考えてみます:

- インターフェイス 0 - Bloomberg 4 キーボード HID
- インターフェイス 1 - Bloomberg 4 キーボード HID
- インターフェイス 2 - Bloomberg 4 HID
- インターフェイス 3 - Bloomberg 4 キーボードオーディオチャンネル
- インターフェイス 4 - Bloomberg 4 キーボードオーディオチャンネル
- インターフェイス 5 - Bloomberg 4 キーボードオーディオチャンネル
- この種類のデバイスに推奨される規則は次のとおりです:

```
CONNECT: vid=1188 pid=9545 split=01 intf=00 ## Bloomberg 4 Keyboard HID
```

```
CONNECT: vid=1188 pid=9545 split=01 intf=01 ## Bloomberg 4 Keyboard HID
```

```
CONNECT: vid=1188 pid=9545 split=01 intf=02 ## Bloomberg 4 HID
```

```
DENY: vid=1188 pid=9545 split=01 intf=03 ## Bloomberg 4 Keyboard Audio Channel
```

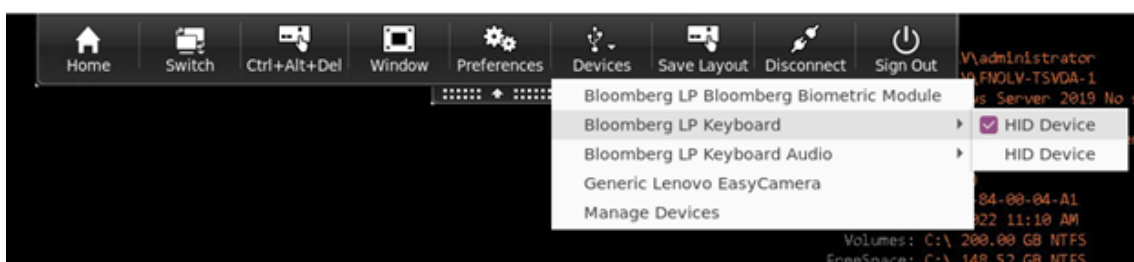
```
DENY: vid=1188 pid=9545 split=01 intf=04 ## Bloomberg 4 Keyboard Audio Channel
```

```
DENY: vid=1188 pid=9545 split=01 intf=05 ## Bloomberg 4 Keyboard Audio Channel
```

### Citrix Viewer を使用した複合 USB デバイスリダイレクト

[デバイス] セクションから USB デバイスを接続するには、次の手順を実行します：

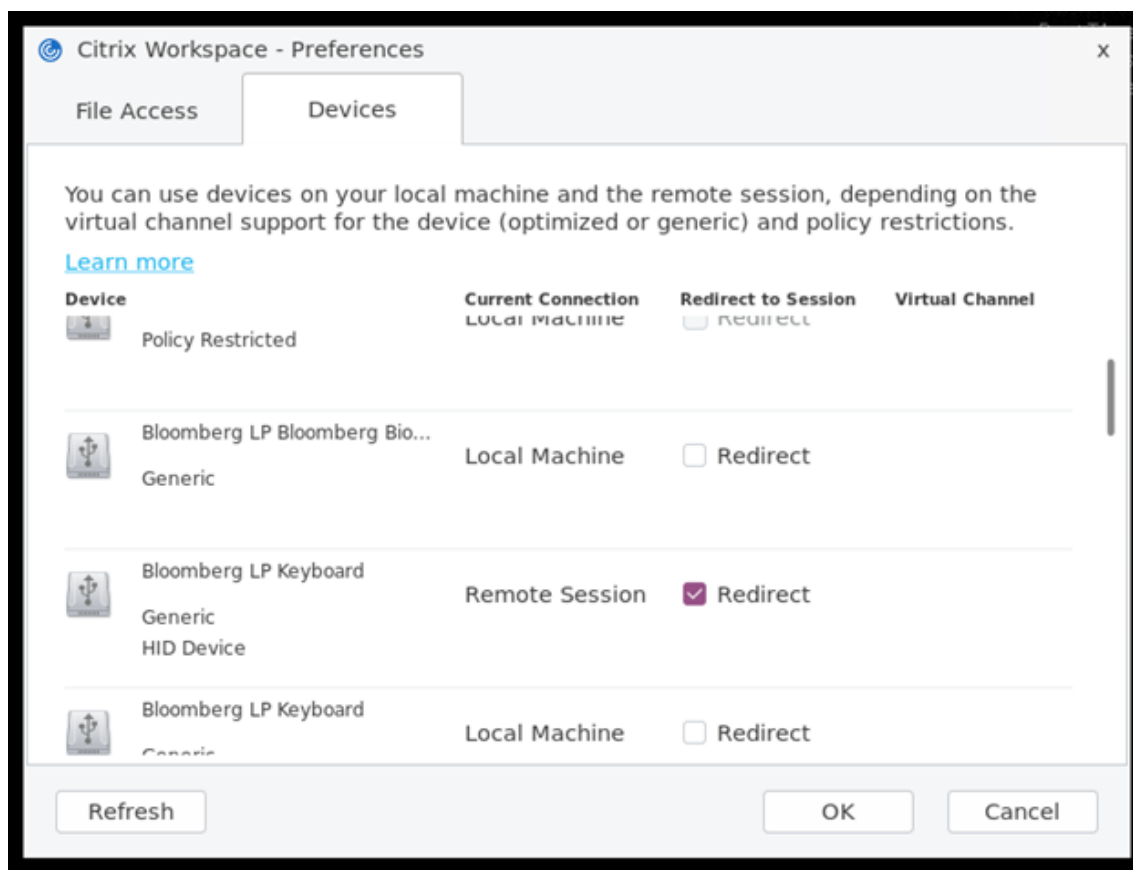
1. デスクトップセッションで、[デバイス] の下の [デスクトップビューア] に移動します。  
分割された USB デバイスが表示されます。



2. デバイスを接続するには、必要なメニュー項目を選択します。

[設定] セクションから USB デバイスを接続するには、次の手順を実行します：

1. [環境設定] > [デバイス] セクションの順に移動します。  
分割された USB デバイスが表示されます。



2. 必要に応じて、デバイスの横にあるチェックボックスをオンにします。

3. **[OK]** をクリックします。

選択した構成がデバイス接続に適用されます。

注:

デバイスを切断するには、デバイスの横にある必要なメニュー項目またはチェックボックスをオフにします。

## Web カメラ

デフォルトでは、HDX RealTime Web カメラビデオ圧縮機能により Web カメラのパフォーマンスが最適化されます。ただし一部の環境では、ユーザーが USB サポート機能を使って Web カメラを接続しなければならない場合があります。USB サポートを使用して Web カメラを接続するには、HDX RealTime Web カメラビデオ圧縮を無効にします。

## Web カメラリダイレクト

Web カメラのリダイレクトについて、次の点に注意してください:

- Web カメラリダイレクトは、RTME の有無にかかわらず利用できます。

- Web カメラリダイレクトは、32 ビット版および 64 ビット版のアプリケーションで機能します。(例: Skype、GoToMeeting) Web カメラリダイレクトをオンラインで確認するには、32 ビット版および 64 ビット版の Web ブラウザーを使ってください。例: <https://webcamtests.com/>。
- Web カメラの使用は、1 つのアプリケーションに限定されます。たとえば、Skype で Web カメラを使用中に GoToMeeting を起動した場合、GoToMeeting で Web カメラを使用するには Skype を終了します。

## 64 ビットアプリの Web カメラリダイレクト

2305 リリースより、Web カメラリダイレクトは 64 ビット版アプリケーションに対応しています。

### システム要件

- システムにインストールされている現在のバージョンに応じて、GStreamer フレームワークバージョン 0.1.x または 1.x。
- GStreamer 1.x を使用している場合は、ICAClient は 2106 より後のバージョン。
- Gstreamer のバージョンとプラグイン:
  - `gststreamer1.0-plugins-base`
  - `gststreamer1.0-plugins-bad`
  - `gststreamer1.0-plugins-good`
  - `gststreamer1.0-plugins-ugly`
  - `gststreamer1.0-vaapi plugin` および `libva` ライブラリ
  - x264 ライブラリ

#### 注:

GStreamer プラグインのバージョンは、GStreamer フレームワークのバージョンと一致している必要があります。たとえば、Gstreamer 1.2.4 をインストールする場合、Gstreamer 1.x プラグインのすべてのバージョンが 1.2.4 である必要があります。

## Web カメラリダイレクトの構成

Linux 向け Citrix Workspace アプリで 64 ビットアプリの Web カメラリダイレクト機能をアクティブ化および構成するには、次の手順を実行します。

### 手順 1: ICAClient の構成を確認

`AllowAudioInput` 値を **True** に設定して、Web カメラリダイレクト機能を有効にします。デフォルトでは、この値は ICAClient のインストールの際に **True** に設定されます。

`AllowAudioInput` 値が **False** に設定されている場合は、次を実行して Web カメラリダイレクト機能を有効にします:

1. 構成ファイル `~/ .ICAClient/wfclient.ini` に移動して編集します。

2. `AllowAudioInput`値を **True** に設定します。

```
AllowAudioInput=True
```

#### 手順 2: Theora エンコーダーの構成を確認

`ICAClient`を正常にインストールし、`AllowAudioInput`値を **True** に設定すると、デフォルトで Theora エンコーダーが構成されます。このエンコーダーは、許容可能なパフォーマンスが設定されたソフトウェアベースのエンコーダーです。ただし、このエンコーダーは VDA で 32 ビットアプリのみをサポートします。

Theora エンコーダーが 32 ビットアプリをサポートしていることを確認するには、次の手順を実行します:

1. Firefox 32 ビットを VDA にインストールします。
2. Web カメラテストサイト (<https://webcamtests.com/>) にアクセスします。

Theora エンコーダーは、VDA 上の 64 ビットアプリの Web カメラリダイレクト機能をサポートしていません。VDA 上の 64 ビットアプリの Web カメラリダイレクト機能をサポートするように H264 エンコーダーオプションを構成します。

#### 手順 3: H264 エンコーダーの構成

H264 エンコーダーは、VDA 上の 64 ビットアプリの Web カメラリダイレクト機能をサポートします。H264 エンコーダーを有効にするには、次の手順を実行する必要があります:

1. 構成ファイル `~/.ICAClient/wfclient.ini` に移動して編集します。
2. `HDXH264InputEnabled`値を **True** に設定します。

```
HDXH264InputEnabled=True
```

次の手順を実行して、H264 エンコーダーが 64 ビットアプリをサポートしていることを確認します:

1. Firefox 64 ビットを VDA にインストールします。
2. Web カメラテストサイト (<https://webcamtests.com/>) にアクセスします。

#### 手順 4: システムの依存関係を確認

H264 エンコーダーを構成した後、Web カメラリダイレクト機能が VDA で 64 ビットアプリをサポートしていない場合は、システムの依存関係を確認してください。

64 ビットアプリの Web カメラリダイレクト機能は、`GStreamer` フレームワークに基づいています。`ICAClient` は、システムにインストールされている現在のバージョンに応じて、`GStreamer` フレームワークバージョン 0.1.x または 1.x を使用します。

**手順 4.1: ICAClient** のバージョンの確認

GStreamer 1.x を使用している場合は、ICAClient が 2106 より後のバージョンであることを確認します。以前のバージョンの ICAClient は失敗する可能性があります。


次の手順を実行して、ICAClient のバージョンがシステムにインストールされている GStreamer フレームワークに基づいていることを確認します：

1. コマンドラインに次のコマンドを入力します：

```
1 cd /opt/Citrix/ICAClient/util
2 <!--NeedCopy-->
```

```
1 ls -alh
2 <!--NeedCopy-->
```

2. 次の図に示すように、gst\_read symlink が gst\_read1.0 または gst\_read0.1.1 にリンクされているかどうかを確認します。



```
28K Jan 26 2021 ctxlogd
.3M Jan 26 2021 ctx_rehash
.8M Jan 26 2021 ctxwebhelper
.0K Jan 26 2021 deploy-AppProtectionService.sh
26K Jan 26 2021 echo_cmd
30K Jan 26 2021 gst_aud_play
30K Jan 26 2021 gst_aud_read
 38 Feb 19 14:55 gst_play -> /opt/Citrix/ICAClient/util/gst_play1.0
55K Jan 26 2021 gst_play0.10
55K Jan 26 2021 gst_play1.0
 38 Feb 19 14:55 gst_read -> /opt/Citrix/ICAClient/util/gst_read1.0
51K Jan 26 2021 gst_read0.10
55K Jan 26 2021 gst_read1.0
32K Jan 26 2021 hdxcheck.sh
.1M Feb 22 10:50 HdxRtcEngine
32K Jan 26 2021 HdxRtcEngine.org
```

util ディレクトリで workspaceappcheck.sh スクリプトを実行し、GStreamer 依存関係を参照するセクションの出力を確認することもできます。

ICAClient 2106 以降のバージョンと GStreamer 1.x を使用することを Citrix ではお勧めします。

**手順 4.2: Gstreamer** のバージョンとプラグインの確認

GStreamer 1.x フレームワークとは別に、次の必要なプラグインをインストールする必要があります：

- Gstreamer1.0-plugins-base
- Gstreamer1.0-plugins-bad
- Gstreamer1.0-plugins-good
- Gstreamer1.0-plugins-ugly
- Gstreamer1.0-vaapi plugin

- [ibva library](#)
- [x264 library](#)

上記のpluginsのインストールについて詳しくは、[GStreamerインストールガイド](#)を参照してください。

注:

GStreamerプラグインのバージョンは、GStreamerフレームワークのバージョンと一致している必要があります。たとえば、Gstreamer1.2.4をインストールする場合、Gstreamer1.xプラグインのすべてのバージョンが1.2.4である必要があります。

次のコマンドを実行して、GStreamerフレームワークの現在のバージョンを確認します:

```
1 gst-inspect-1.0 --gst-version
2 <!--NeedCopy-->
```

トラブルシューティングについて詳しくは、トラブルシューティングのセクションの「[Web カメラ](#)」を参照してください。

### Web カメラリダイレクトの背景のぼかし

Linux 向け Citrix Workspace アプリが、Web カメラリダイレクトで背景のぼかしをサポートするようになりました。この機能を有効にするには、次の手順を実行します:

1. 構成ファイル~/[.ICAClient/wfclient.ini](#)に移動します。
2. [wfclient.ini](#) ファイルに次のエントリを追加します:

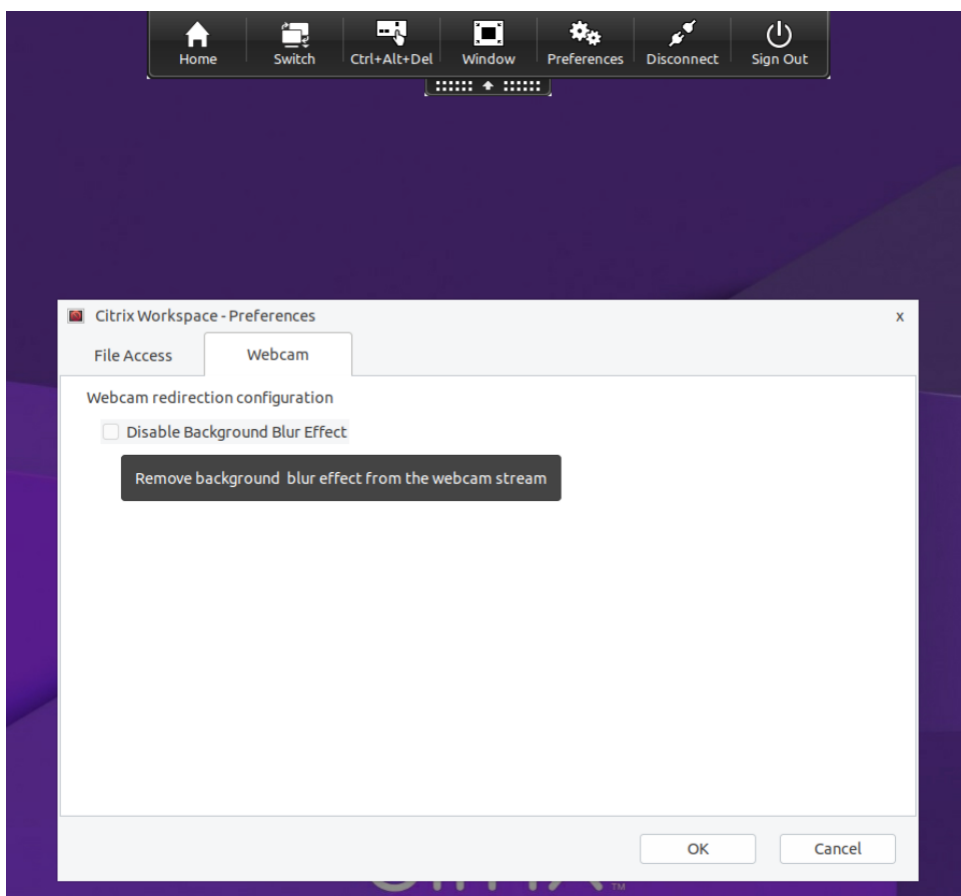
```
1 HDXWebCamEnableBackgndEffect=True
2 <!--NeedCopy-->
```

注:

この設定は、UIの有無にかかわらずクライアントでWebカメラリダイレクト機能の背景のぼかしを有効にします。

グラフィカルユーザーインターフェイスを使用して、**Web** カメラリダイレクトのセッション内で背景のぼかしを無効にするには:

1. **[Desktop Viewer]** で **[環境設定]** をクリックします。**[Citrix Workspace - 基本設定]** ダイアログボックスが開きます。
2. **[Web カメラ]** タブをクリックします。次のダイアログボックスが表示されます。



3. [背景のぼかし効果を無効にする] チェックボックスをオンにして、Web カメラリダイレクトの背景のぼかしを無効にします。
4. [OK] をクリックします。

### **MJPEG Web** カメラのサポート

2308 バージョン以降、MJPEG Web カメラは H264 ストリームでサポートされます。Web カメラは内部で MJPEG 圧縮を実行し、より良い画質とより高いフレームレートを実現します。この機能はデフォルトで有効になっています。ただし、Web カメラが MJPEG をサポートしていない場合、この機能は無効になります。

### **Xcapture**

Citrix Workspace アプリパッケージには、ヘルパーアプリケーション xcapture が含まれています。このアプリケーションによって、サーバーのクリップボードと、X デスクトップ上の ICCCM に準拠していない X Window アプリケーション間で画像をコピーおよび貼り付けできるようになります。xcapture を使って、次の操作を実行できます。

- ダイアログボックスや画面領域をキャプチャし、コネクションウィンドウ内で実行中のアプリケーションと、ユーザーデバイスデスクトップ (ICCCM に準拠していない X Window アプリケーションを含む) 間でコピーする。



- コネクションウィンドウと、グラフィックを編集する X Window アプリケーションである xmag または xv 間で、画像をコピーする。

コマンドラインから xcapture を起動するには、以下を実行します：

コマンドプロンプトで、`/opt/Citrix/ICAClient/util/xcapture` と入力し、Enter キーを押します（ここで `/opt/Citrix/ICAClient` は、Citrix Workspace アプリをインストールしたディレクトリ）。

ユーザーデバイスのデスクトップからコピーするには：

1. [xcapture] ダイアログボックスで、[画面から] をクリックします。カーソルが十字型に変わります。
2. 次のいずれかを選択します。
  - ウィンドウの選択。コピーするウィンドウの上にカーソルを移動し、マウスの中央ボタンをクリックします。
  - 領域の選択。マウスの左ボタンを押したままカーソルをドラッグして、コピーする領域を選択します。
  - 選択の取り消し。マウスの右ボタンをクリックします。ドラッグしているときに中央ボタンまたは左ボタンを押したままマウスの右ボタンをクリックすると、選択が解除されます。
3. [xcapture] ダイアログボックスで、[ICA へ] をクリックします。ボタンの色が変わり、情報を処理していることが示されます。
4. 転送が完了したら、コネクションウィンドウから起動したアプリケーションで適切なコマンドを使用して、情報を貼り付けます。

xv から、ICA セッション内のアプリケーションにコピーするには：

1. xv で情報をコピーします。
2. [xcapture] ダイアログボックスで、[xv から]、[ICA へ] の順にクリックします。ボタンの色が変わり、情報を処理していることが示されます。
3. 転送が完了したら、コネクションウィンドウから起動したアプリケーションで適切なコマンドを使用して、情報を貼り付けます。

ICA セッション内のアプリケーションから xv にコピーするには：

1. ICA セッション内のアプリケーションで、情報をコピーします。
2. [xcapture] ダイアログボックスで、[ICA から]、[xv へ] の順にクリックします。ボタンの色が変わり、情報を処理していることが示されます。
3. 転送が完了したら、コピーした情報を xv 内に貼り付けます。

## カーソル

### カーソルの色反転のサポート

以前は、Citrix Workspace アプリは、テキストの白黒の背景と同じ色を使用した点線のカーソルを表示していました。その結果、カーソルの位置を特定することが困難でした。

バージョン 2112 以降、カーソルの色はテキストの背景色に基づいて反転します。その結果、テキスト内のカーソルの位置を簡単に見つけることができます。デフォルトでは、この機能は無効になっています。

前提条件:

- `.ICAClient`が既に現在のユーザーのホームフォルダーに存在する場合:

`All_Regions.ini`ファイルを削除します

または

`All_Regions.ini`ファイルを保持するには、[Virtual Channels\Thinwire Graphics] セクションの最後に次の行を追加します:

`InvertCursorEnabled=`

`InvertCursorRefreshRate=`

`InvertCursorMode=`

`.ICAClient`フォルダーが存在しない場合は、Citrix Workspace アプリの新規インストールです。この場合、機能のデフォルト設定は保持されます。

この機能を有効にするには、次の手順を実行します:

1. 構成ファイル`$HOME/.ICAClient/wfclient.ini`に移動します。
2. [Thinwire3.0] セクションに移動し、次のエントリを設定します:

`InvertCursorEnabled=True`

注:

Citrix Studio の [圧縮にビデオコーデックを使用する] の値が `Do not use video codec` に設定されている場合、カーソルは反転しません。

## マウス

### 相対マウス

相対マウスのサポートでは、マウスの絶対位置ではなく相対位置を読み取るオプションを提供します。この機能は、マウスの絶対位置ではなく相対位置の入力を必要とするアプリケーションに必要です。

注:

この機能は、Citrix Virtual Apps and Desktops 7.8 以降または Citrix DaaS で実行されているセッションでのみ使用できます。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:

ファイル`$HOME/.ICAClient/wfclient.ini`の [WFClient] セクションにエントリ `RelativeMouse=1` を追加します。

この手順で有効にするまでは、機能は無効になっています。相対マウス機能を有効にする方法について詳しくは、「相対マウスのその他の値」のセクションを参照してください。

この機能を有効にするには:

「Ctrl/F12」と入力します。

機能が有効になったら、Ctrl/F12 を再度入力して、サーバーポインターの位置をクライアントと同期させます。相対マウスを使用すると、サーバーとクライアントのポインターの位置が同期しません。

この機能を無効にするには:

「Ctrl-Shift/F12」と入力します。

この機能は、セッションウィンドウからフォーカスが失われた場合もオフになります。

### 相対マウスのその他の値

別の方法として、相対マウスで次の値も使用できます:

- **RelativeMouse=2**。機能を有効にし、セッションウィンドウがフォーカスを取り戻すとアクティブになります。
- **RelativeMouse=3**。機能を有効にし、アクティブにし、常時アクティブ状態に維持します。
- **RelativeMouse=4**。クライアント側のマウスポインターが非表示または表示のときに、機能を有効または無効にします。このモードは、ファーストパーソンゲーム形式のアプリケーションインターフェイスで相対マウスを自動的に有効または無効にする場合に適しています。

キーボードコマンドを変更するには、以下のような設定を追加します。

- **RelativemouseOnChar=F11**
- **RelativemouseOnShift=Shift**
- **RelativemouseOffChar=F11**
- **RelativemouseOffShift=Shift**

**RelativemouseOnChar** および **RelativemouseOffChar** でサポートされる値は、Citrix Workspace アプリインストールツリーの config/module.ini ファイルの [Hotkey Keys] に一覧があります。**RelativeMouseOnShift** および **RelativeMouseOffShift** の値は、使用される識別子キーを設定し、[Hotkey Shift States] 見出しの下に一覧があります。

### キーボード

#### キーボードの動作

Ctrl+Alt+Del キーを送信するためのキーを設定するには:

1. Ctrl+Alt+Del キー操作を送信するために使用するキーの組み合わせを決定します。
2. 適切な構成ファイルを開き、[WFClient] セクションの UseCtrlAltEnd で、以下の値を設定します:
  - **True** を指定すると、Ctrl+Alt+End キーを押すことでリモートのデスクトップに Ctrl+Alt+Del キー操作が送信されます。

- False (デフォルト) を指定すると、Ctrl+Alt+Enter キーを押すことでリモートのデスクトップに Ctrl+Alt+Del キー操作が送信されます。

#### 汎用リダイレクト

クライアント側で汎用 USB リダイレクトを使用して Bloomberg v4 キーボードを構成します:

前提条件として、Domain Delivery Controller (DDC) でポリシーが有効になっている必要があります。

1. Bloomberg キーボードの vid および pid を見つけます。たとえば、Debian と Ubuntu では次のコマンドを実行します:

```
lsusb
```

2. \$ICAROOT に移動し、usb.conf ファイルを編集します。
3. usb.conf ファイルで以下のエントリを追加し、Bloomberg キーボードの USB リダイレクトを許可してから、ファイルを保存します。

```
ALLOW: vid=1188 pid=9545
```

4. クライアント上で `ctxusbd` デモンを再起動します。たとえば、Debian と Ubuntu では次のコマンドを実行します:

```
systemctl restart ctxusbd
```

5. クライアントセッションを起動します。リダイレクトを実行するために Bloomberg v4 キーボードに接続するとき、セッションにフォーカスがあることを確認します。

注:

次の構成を追加して、`selectconfiguration` コマンドを無効にすることができます:

```
ALLOW: vid=1100 pid=0101 disableselectconfig=1。
```

`selectconfiguration` は、USB デバイスを構成するために VDA で使用されるコマンドです。

#### 選択的なリダイレクト

この機能を使用することで、複数のセッションで Bloomberg キーボード v4 および v5 インターフェイスを使えるようになります。これにより、フィンガープリントおよびオーディオインターフェイスを除くすべてのリモートセッションでキーボードを柔軟に使用できます。フィンガープリントおよびオーディオインターフェイスは、以前と同様に単一のセッションにリダイレクトされます。

この機能を有効にするには:

1. `$HOME/.ICAClient/wfclient.ini` ファイルの `BloombergRedirection` セクションを次のように編集します。

```
1 BloombergRedirection=true
2 <!--NeedCopy-->
```

2. 「[汎用リダイレクト](#)」に記載されているすべての手順を実行します。

この機能を無効にするには：

1. `$HOME/.ICAClient/wfclient.ini` ファイルの `BloombergRedirection` セクションを次のように編集します。

```
1 BloombergRedirection=false
2 <!--NeedCopy-->
```

2. 「[汎用リダイレクト](#)」に記載されているすべての手順を実行します。

注：

値を `false` に設定すると、機能が旧バージョンの動作に戻って、すべてのインターフェイスが 1 つのセッションにリダイレクトされるようになります。

全画面モードとウィンドウモードを切り替えるためのキーボードショートカットのサポート

以前は、Desktop Viewer の [ウィンドウ] ボタンまたは [全画面] ボタンを使用して、全画面モードとウィンドウモードを切り替えることができました。

Citrix Workspace アプリ 2308 リリース以降、キーボードショートカット `Ctrl + F2` を使用して全画面モードとウィンドウモードを切り替えることができるようになりました。たとえば、デスクトップセッションが全画面モードのときに「`Ctrl + F2`」を押すと、デスクトップセッションが全画面モードを終了します。

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：

1. 新しい Linux 向け Citrix Workspace アプリがインストールされているときに、現在のユーザーのホームフォルダーに `.ICAClient` が既に存在する場合：

`All_Regions.ini` ファイルを削除します

または、

`AllRegions.ini` ファイルを保持する場合、`[Client Engine\Application Launching]` セクションの最後に次の行を追加します：

```
1 FullScreenShortcutSupport=*
2 <!--NeedCopy-->
```

2. `/opt/Citrix/ICAClient/config/All_Regions.ini` ファイルに移動して、`FullScreenShortcutSupport` の値を次のように変更します：

```

1 FullScreenShortcutSupport=true
2 <!--NeedCopy-->

```

デフォルトでは、キーボードのショートカットは Ctrl+F2 です。

ショートカットキーをカスタマイズすることもできます。ショートカットは、`All_Regions.ini` ファイル内の **KeyPassthroughEscapeShift** と **KeyPassthroughEscapeChar** などの 2 つの異なる部分で構成されます。

使用する 2 つのキーは、次の一覧にあるものにする必要があります：

名前	セクション	値
KeyPassthroughEscapeShift	All_Regions.ini ファイルの [Virtual Channels\Keyboard]	[Alt、Ctrl、Shift、Alt+Ctrl、 Alt+Shift、Ctrl+Shift、 Alt+Ctrl+Shift]、デフォルト値： Ctrl
KeyPassthroughEscapeChar	All_Regions.ini ファイルの [Virtual Channels\Keyboard]	[F1、F2、F3、F4、F5、F6、F7、 F8、F9、F10、F11、F12、マイナ ス (-)、プラス (+)、Tab、Pause]、 デフォルト値：F2、注：マイナス とプラスはテンキーのキーです。

たとえば、「Ctrl+Shift+F3」をキーボードのショートカットとして使用したい場合は、次のように項目を設定する必要があります：

- KeyPassthroughEscapeShift=Ctrl+Shift
- KeyPassthroughEscapeChar=F3

制限事項：

- クライアント OS のショートカットと競合するキーの組み合わせを使用する場合、またはシステムショートカットが含まれるキーの組み合わせを使用する場合は、クライアント OS がこのショートカットの使用を優先するため、全画面の切り替えが機能しない可能性があります。たとえば、「Ctrl+F3」を Linux OS のシステムショートカットとして使用していると、「Ctrl+F3」または「Shift+Ctrl+F3」を Citrix Workspace アプリの全画面の切り替えで使用できません。
- Ctrl+Alt+F<sup>n</sup>または Alt+Ctrl+F<sup>n</sup>（F<sup>n</sup>は F1～F12 を指します）は、Linux で仮想ターミナルを切り替えるために使用されるキーボードショートカットです。これらのショートカットを全画面の切り替えに使用しないでください。
- Alt+Ctrl+ プラスまたは Alt+Ctrl+ マイナス（プラスとマイナスは数字キーボードのキー）は Linux システムの記号「XF86Next\_VMode」や「XF86Prev\_VMode」にマッピングされ、ショートカットとして使用できません。そのため、これらの組み合わせを全画面の切り替えに使用しないでください。

## ブラウザコンテンツリダイレクト

### ブラウザコンテンツのリダイレクトの **Chromium** 埋め込みフレームワーク (CEF)

バージョン 1912 より前のリリースでは、BCR は WebkitGTK+ ベースのオーバーレイを使用してコンテンツをレンダリングしました。ただし、シンクライアントでは、パフォーマンスの問題がありました。バージョン 1912 以降、BCR は CEF ベースのオーバーレイを使用します。これにより、BCR のユーザーエクスペリエンスが向上し、ネットワーク使用量、ページ処理、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できます。

バージョン 2106 以降、CEF ベースのブラウザコンテンツリダイレクトは完全に機能します。この機能はデフォルトで有効にされています。

必要な場合は、Workspace アプリパッケージで提供された `libffmpeg.so` ファイルを、`$ICAROOT/bcr/libffmpeg.so` パスの必要なコーデックが使用された適切な `libffmpeg.so` ファイルと置き換えることができます。

#### 注:

この機能は、ARMHF プラットフォームではサポートされていません。

### CEF ベースの BCR の有効化

CEF ベースの BCR を有効にするには、次の手順を実行します:

1. `$ICAROOT/config/All_Regions.ini` ファイルに移動します。`$ICAROOT` は Citrix Workspace アプリのデフォルトのインストールディレクトリです。
2. `[Client Engine\WebPageRedirection]` セクションに移動し、次のエントリを設定します:  
`UseCefBrowser=True`

#### 制限事項:

- BCR が使用されると、ポップアップを使用する Web アプリが機能しない可能性があります。

#### 既知の問題:

- `~/.ICAClient/All_Regions.ini` の `UseCefBrowser` オプションを **True** に設定すると、日本語、中国語 (簡体字)、韓国語の IME で入力フィールドが機能しないことがあります。Linux 向け Citrix Workspace アプリは、Citrix 埋め込みブラウザでセキュアな SaaS アプリを使用する場合、日本語、中国語 (簡体字)、韓国語の IME をサポートしません。
- CEF ベースの BCR を使用して Web ページのリダイレクトを開始しようとすると、不明な証明書エラーが発生する場合があります。この問題は、Citrix Workspace アプリバージョン 2106 以降で発生します。この問題を回避するには、ターミナルで次のコマンドを使用して、自己署名証明書を `nssdb` にインポートします:

```
1 certutil -A -n "badssl.cer" -t "C,," -d ~/.pki/nssdb -i ~/
  Downloads/badssl.cer
2 <!--NeedCopy-->
```

コマンドの引数は次のとおりです：

- `-A` - データベースに証明書を追加します。
- `-n` - 証明書の名前。この引数はオプションであり、ニックネームを追加するために使用できます。
- `"badssl.cer"` - `badssl.com` サイトからエクスポートされた証明書の名前。
- `-t "C,,"` - `-t` は TRUSTARGS 用で、`C` は CA 証明書用です。詳しくは、[Google のドキュメント](#)を参照してください。
- `-d ~/ .pki/nssdb` - データベースの場所。
- `-i` - 入力ファイルを示します。この引数は、証明書ファイルの場所と名前を追加するためのものです。

BCR について詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[Web ブラウザーコンテンツのリダイレクト](#)」を参照してください。

ブラウザコンテンツリダイレクトオーバーレイのブラウザの一時データストレージパスを構成する

Citrix Workspace アプリ 2303 バージョン以降では、CEF ベースのブラウザの一時データストレージパスを構成するように求められます。パスを構成するには、次の手順を実行します：

1. `$(ICAROOT)/config/All_Regions.ini`ファイルに移動します。`$(ICAROOT)` は Citrix Workspace アプリのデフォルトのインストールディレクトリです。
2. `[Client Engline\WebPageRedirection]`セクションに移動し、次のエントリを追加します：

```
1 CefCachePath = <folder for CEF based BCR tmp files>
2 <!--NeedCopy-->
```

### 自動再接続

このトピックでは、HDX Broadcast のクライアント自動再接続機能について説明します。この機能は、HDX Broadcast セッション画面の保持機能と組み合わせて使用することを Citrix ではお勧めします。

ネットワークの状態が不安定であったり、待ち時間が非常に変わりやすかったりする場合、また、無線デバイスの伝送距離に制限がある場合に、セッションが切断されてしまうことがあります。HDX Broadcast のクライアント自動再接続機能では、ネットワークの問題などによって切断されたセッションを Linux 向け Citrix Workspace アプリが検出すると、そのセッションに自動的に再接続します。

この機能がサーバーで有効になっていると、ユーザーは作業を続けるために手動で再接続する必要がありません。Citrix Workspace は、セッションへの接続に成功するかユーザーがキャンセルするまで設定した回数再接続を試行します。サーバー側でユーザー認証を要求する設定になっている場合、再接続時にユーザーの資格情報を入力するためのダイアログボックスが開きます。ユーザーがセッションからログオフしないでアプリケーションを終了してセッションを切断した場合、自動再接続は行われません。自動再接続は、ユーザーによる切断以外の理由で切断されたセッションに対してのみ行われます。

デフォルトでは、Linux 向け Citrix Workspace アプリは 30 秒間待機してから切断したセッションに再接続を実行し、またこれを 3 回試行します。



AccessGateway を介して接続すると、ACR は使用できません。ネットワークの障害から保護するため、セッション画面の保持をサーバーとクライアントで有効にし、Access Gateway 上で構成しておきます。

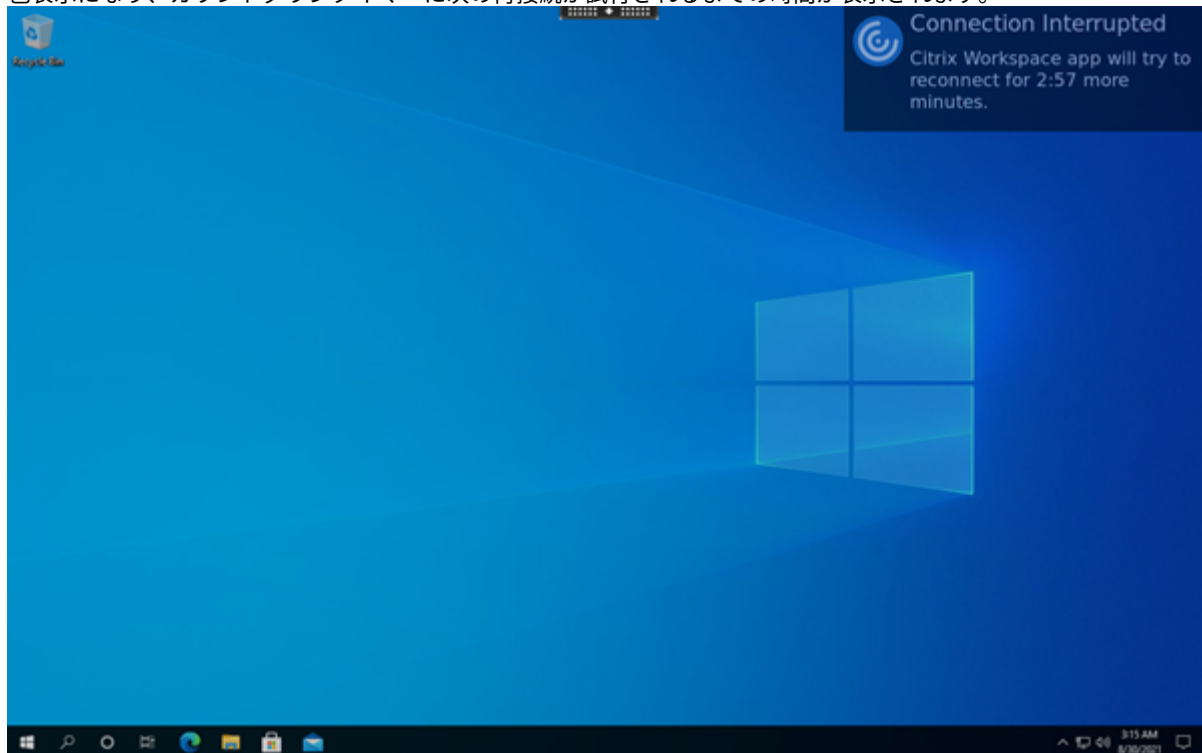
HDX Broadcast のクライアント自動再接続の構成手順については、Citrix Virtual Apps and Desktops のドキュメントを参照してください。

### セッション画面の保持

このトピックは、デフォルトで有効になっている HDX Broadcast セッション画面の保持機能について説明します。

HDX Broadcast セッション画面の保持を有効にすると、公開アプリケーションへの接続が中断しても、ユーザーのセッション画面には作業中の画面が保持され、表示されたままになります。たとえば、ワイヤレス接続でのセッション中にトンネルや障害物などの影響で接続に障害が生じた場合、ユーザーデバイス上の画面表示が停止します。トンネルから出るなどして再接続されると、ユーザーはそのまま作業を続行できます。接続が切断している間、ユーザーのデータのすべて、キー入力、およびその他の操作は記憶され、アプリケーションは応答しないまま表示されます。接続が再度確立されると、これらすべての操作がアプリケーション内に反映されます。

これで、セッション画面の保持が開始されると画面が変わります。この機能拡張により、セッションウィンドウが灰色表示になり、カウントダウンタイマーに次の再接続が試行されるまでの時間が表示されます。



#### ヒント

非アクティブなセッションに使用されるグレースケールの明るさは、[再接続 UI の透過レベル] ポリシーを使用して変更できます。デフォルト値は、80 に設定されています。最大値は 100（半透明の画面）より上に設定できません。最小値は 0（完全に黒くなった画面）に設定できます。

セッションが正常に再接続されると、カウントダウンのための通知メッセージが消えます。通常どおりデスクトップを操作できます。

2109 バージョン以降、セッション画面の保持通知はデフォルトで有効になっています。

この拡張機能を無効にするには:

1. 構成ファイル/opt/Citrix/ICAClient/config/module.iniに移動します。
2. [WFClient] セクションで、次の設定を変更します:

`SRNotification=False`

注:

この機能は、Citrix Virtual Desktops でのみサポートされています。

クライアント自動再接続とセッション画面の保持が構成されている場合、接続の問題がある場合にはセッションの画面保持が優先して実行されます。セッション画面の保持は既存のセッションへの接続を再度確立しようとします。接続の問題を検出するまでに最大で 25 秒かかることがあります。また、再接続を試みるための構成可能な期間（デフォルトは 180 秒）も必要です。セッション画面の保持が再接続に失敗すると、クライアント自動再接続が再接続を試みます。

HDX Broadcast セッション画面の保持を有効にすると、セッションの通信に使用されるデフォルトのポートは、1494 から 2598 に変更されます。

Citrix Workspace のユーザーには、サーバー側の設定が自動的に適用されます。

重要:

HDX Broadcast セッション画面の保持では、サーバー上で（ポリシー設定を使って）Common Gateway Protocol を有効にする必要があります。Common Gateway Protocol を無効にすると、HDX Broadcast セッション画面の保持も無効になります。

セッション画面の保持ポリシーを使用する

[セッション画面の保持] ポリシー設定により、セッション画面の保持を有効にします。

[セッション画面の保持のタイムアウト] ポリシー設定には、デフォルトで 180 秒（3 分）が設定されています。必要に応じて、セッション画面の保持によってセッションを開いたままにしておく時間を延長できます。その間、ユーザーに再認証を求めるプロンプトは表示されません。

ヒント

必要以上に長い時間を設定すると、接続の再開を待ちきれないユーザーが席を離れることがあります。その間に不正なユーザーがセッションにアクセスしてしまう危険性があります。

セッション画面の保持機能が有効な受信接続ではポート 2598 が使用されます。このポート番号は [セッション画面の保持のポート番号] ポリシー設定で変更できます。

[セッション画面の保持] ポリシーの設定について詳しくは、「[セッション画面の保持のポリシー設定](#)」を参照してください。

注:

セッション画面の保持は、サーバーでデフォルトで有効になっています。この機能を無効にするには、サーバーで管理するポリシーを構成します。

### マルチメディアのパフォーマンス

Citrix Workspace アプリには、メディアリッチな今日のユーザー環境に高品位なユーザーエクスペリエンスを提供する幅広い技術セットが含まれています。これらの技術により、ホストされるアプリケーションやデスクトップでのユーザーエクスペリエンスが向上します。

- [HDX MediaStream Windows Media リダイレクト](#)
- [HDX MediaStream Flash リダイレクト](#)
- [HDX RealTime Web カメラビデオ圧縮](#)
- [H.264](#)

注:

Linux バージョン 1901 以降(GStreamer 0.1)で HDX RealTime Optimization Pack と Citrix Workspace アプリを併用できます。

### **HDX MediaStream Windows Media** リダイレクト

HDX MediaStream Windows Media リダイレクトを実行すると、Linux ユーザーデバイスでアクセスする仮想 Windows デスクトップでマルチメディア再生時の帯域幅が軽減されます。Windows Media リダイレクトは、サーバーではなくユーザーデバイスでメディアランタイムファイルを再生するメカニズムを提供します。その結果、マルチメディアファイルの再生に必要な帯域幅が削減されます。

Windows Media リダイレクトは、仮想 Windows デスクトップで実行中の Windows Media Player および互換プレーヤーのパフォーマンスを向上させます。次の形式を含む、さまざまなファイル形式をサポートしています:

- Advanced Systems Format (ASF)
- Motion Picture Experts Group (MPEG)
- Audio-Video Interleaved (AVI)
- MPEG Audio Layer-3 (MP3)
- WAV サウンドファイル

Citrix Workspace アプリには、Windows 用のメディア形式である GUID をGStreamer用の MIME タイプに変換するためのテキストベースの変換テーブルである MediaStreamingConfig.tbl が含まれています。この変換テーブルは、以下の目的で編集できます:

- 不明またはサポートされないメディアフィルター/ファイル形式を変換テーブルに追加する。
- 問題が生じる GUID をブロックして、強制的にサーバー側でレンダリングされるようにする。
- GStreamerパラメーターの変更により問題のある形式をトラブルシューティングできるようにするため、パラメーターを既存の MIME 文字列に追加する。

- ユーザーデバイス上のGStreamerによりサポートされているメディアファイルの種類に応じて、カスタムの構成を管理および展開する。

クライアント側でのコンテンツ取得機能を使用すると、<http://>、<mms://>、または<rtsp://>形式の URL からのストリーム配信メディアを、Citrix サーバーを介さずにユーザーデバイスで直接取得できます。サーバーは、ユーザーデバイスをメディアに接続して、再生、一時停止、停止、音量、シークなどの制御コマンドを送信します。メディアデータの処理は行いません。この機能を使用するには、ユーザーデバイス上に高度なマルチメディアGStreamerライブラリをインストールする必要があります。

HDX MediaStream Windows メディアリダイレクトを実装するには:

1. オープンソースのマルチメディアフレームワークであるGStreamer 0.10 を各ユーザーデバイス上にインストールします。通常、Citrix Workspace アプリをインストールする前にGStreamerをインストールして、Citrix Workspace アプリがインストールプロセスで GStreamer の使用を構成できるようにします。

ほとんどの Linux ディストリビューションにはGStreamerが含まれています。または、<http://gstreamer.freedesktop.org>からGStreamerをダウンロードできます。

2. クライアント側でのコンテンツ取得機能を有効にするには、再生するメディアのファイルタイプに対応するGStreamerのプロトコルソースプラグインをインストールします。このプラグインのインストールおよび動作を確認するには、`gst-launch`ユーティリティを使用します。このプラグインが正しくインストールされている場合、`gst-launch`で URL のマルチメディアを再生できます。たとえば、`gst-launch-0.10 playbin2 uri=<http://example-source/file.wmv>`を実行してビデオが正しく再生されるかチェックします。
3. デバイス上で Citrix Workspace アプリをインストールするときに、Tarball スクリプトを使用している場合、GStreamer オプションを選択します（この手順は、`.deb`および`.rpm`パッケージでは自動で実行されます）。

クライアント側でのコンテンツ取得機能を使用する場合は、次のことに注意してください:

- この機能は、デフォルトで有効になります。無効にするには、`All-Regions.ini` ファイルの `Multimedia` セクションにある `SpeedScreenMMACSFEnabled` オプションを使用します。ここで「False」を指定すると、Windows Media リダイレクト機能が使用されます。
- デフォルトでは、すべての MediaStream 機能でGStreamerの `playbin2` プロトコルが使用されます。クライアント側でのコンテンツ取得機能を除くすべての MediaStream 機能を従来の`playbin`プロトコルに戻すことができます。クライアント側でのコンテンツ取得機能では、`All-Regions.ini`ファイルの `Multimedia` セクションにある`SpeedScreenMMAEnablePlaybin2`オプションを使用して、常に `playbin2` プロトコルを使用します。
- Citrix Workspace アプリでは、`.asx`や`.nsc`などのストリーム構成情報ファイルや再生リストファイルを認識できません。可能な場合は、これらのファイルを参照しない標準的な URL をユーザーが指定する必要があります。URL が有効かどうかは、`gst-launch`を使用して確認できます。

GStreamer 1.0 については、以下のことに注意してください:

- デフォルトでは、GStreamer 0.10 が HDX MediaStream Windows Media リダイレクトに使用されます。GStreamer 1.0 は、GStreamer 0.10 が使用できない場合にのみ使用されます。

- **GStreamer 1.0** を使用する場合は、次の手順を使用してください:
1. **GStreamer** プラグインのインストール先ディレクトリを検出します。プラグインのインストール先は、ディストリビューション、OS アーキテクチャ、**GStreamer** のインストール方法によって異なります。一般的なインストールパスは、`/usr/lib/x86_64-linux-gnu/gstreamer-1.0` または `$HOME/.local/share/gstreamer-1.0` です。
  2. Linux 向け Citrix Workspace アプリのインストールディレクトリを検出します。スーパーユーザー (root) のデフォルトのインストールディレクトリは、`/opt/Citrix/ICAclient` です。非スーパーユーザーのデフォルトのインストールディレクトリは、`$HOME/ICAclient/platform` (プラットフォームは `linuxx64` など) です。詳しくは、「[インストールとセットアップ](#)」を参照してください。
  3. **GStreamer** プラグインディレクトリでシンボリックリンクを作成することで、`libgstflatstm1.0.so` をインストールします:`-sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so`。この手順には、権限の昇格 (sudo 権限など) が必要な場合があります。
  4. `gst_play1.0` をプレーヤーとして使用する:`-sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play` この手順には、権限の昇格 (sudo 権限など) が必要な場合があります。
- HDX RealTime Web カメラビデオ圧縮で **GStreamer 1.0** を使用する場合、`gst_read1.0` をリーダーとして使用します。`sf $ICACLIENT_DIR/util/gst_read1.0 $ICACLIENT_DIR/util/gst_read`。

### **GStreamer 1.x** の有効化

1912 より前のリリースでは、**GStreamer 0.10** がマルチメディアリダイレクトでサポートされるデフォルトのバージョンでした。1912 リリース以降、**GStreamer 1.x** をデフォルトのバージョンとして構成することができます。

制限事項:

- ビデオを再生すると、早送りおよび巻き戻しオプションが正常に機能しないことがあります。
- ARMHF デバイスで Citrix Workspace アプリを起動すると、**GStreamer 1.x** が正常に機能しないことがあります。

### **GStreamer 1.x** をインストールするには

**GStreamer 1.x** フレームワークと以下のプラグインを <https://gstreamer.freedesktop.org/documentation/installing/on-linux.html> からインストールします:

- `Gstreamer-plugins-base`
- `Gstreamer-plugins-bad`
- `Gstreamer-plugins-good`
- `Gstreamer-plugins-ugly`
- `Gstreamer-libav`

バイナリをローカルにビルドするには

SUSE や openSUSE などの一部の Linux OS ディストリビューションでは、デフォルトのソースリストにGStreamerパッケージが見つからないことがあります。この場合、ソースコードをダウンロードし、すべてのバイナリをローカルにビルドします。

1. <https://gstreamer.freedesktop.org/src/>からソースコードをダウンロードします。
2. コンテンツを抽出します。
3. 解凍されたパッケージがあるディレクトリに移動します。
4. 次のコマンドを実行します:

```
1 $sudo ./configure
2 $sudo make
3 $sudo make install
4 <!--NeedCopy-->
```

デフォルトでは、生成されたバイナリは/usr/local/lib/gstreamer-1.0/で利用可能です。

トラブルシューティングについて詳しくは、Knowledge Center の記事[CTX224988](#)を参照してください。

**GStreamer 1.x** を構成するには

GStreamer 1.x を Citrix Workspace アプリで使用できるように構成するには、シェルプロンプトを使用して以下の構成を適用します:

- `$ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so`
- `$ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play`

各項目の意味は次のとおりです。

- ICACLIENT\_DIR - Linux 向け Citrix Workspace アプリのインストールパスです。
- GST\_PLUGINS\_PATH - GStreamer のプラグインパスです。たとえば、64 ビット Debian マシンでは、`/usr/lib/x86_64-linux-gnu/gstreamer-1.0/`です。

制限事項:

- バージョン 2106 より前のリリースでは、GStreamer バージョン 1.15.1 以降を使用する際に、Web カメラのリダイレクトが失敗し、セッションが切断されることがあります。

**HDX MediaStream Flash** リダイレクト

HDX MediaStream Flash リダイレクトにより、Adobe Flash コンテンツがユーザーデバイス上でローカルに再生され、帯域幅要件を増やすことなく高品位な音声やビデオの再生機能が提供されます。

1. この機能に必要な要件をユーザーデバイスが満たしていることを確認します。詳しくは、「[システム要件](#)」を参照してください。

2. `wfclient.ini` の [WFClient] セクション（特定ユーザーのすべての接続に適用する場合）または `All\_Regions.ini` の [Client Engine\Application Launching] セクション（環境内のすべてのユーザーに適用する場合）に、以下のパラメーターを追加します：

- **HDXFlashUseFlashRemoting=Ask: Never; Always**

ユーザーデバイス上で HDX MediaStream for Flash を有効にします。デフォルトでは、この値は **Never** に設定されています。また、この Flash コンテンツを含む Web ページに接続したときに、コンテンツを最適化するかどうかを確認するダイアログボックスがユーザーに表示されます。

- **HDXFlashEnableServerSideContentFetching=Disabled; Enabled**

Citrix Workspace アプリのサーバー側でのコンテンツ取得機能を有効または無効にします。デフォルトでは、この値は **Disabled** に設定されています。

- **HDXFlashUseServerHttpCookie=Disabled; Enabled**

HTTP Cookie のリダイレクトを有効または無効にします。デフォルト値は、**Disabled** に設定されています。

- **HDXFlashEnableClientSideCaching=Disabled; Enabled**

Citrix Workspace アプリにより取得された Web コンテンツのクライアント側キャッシュを有効または無効にします。デフォルト値は、**Enabled** に設定されています。

- **HDXFlashClientCacheSize= [25-250]**

クライアント側でのキャッシュのサイズを、MB 単位で定義します。この値は、25MB～250MB の間で定義できます。サイズが制限値に到達すると、キャッシュ内の既存のコンテンツが削除され、新しいコンテンツが保存されます。デフォルト値は、**100** に設定されています。

- **HDXFlashServerSideContentCacheType=Persistent: Temporary; NoCaching**

サーバー側でのコンテンツ取得機能により取得されたコンテンツの Citrix Workspace アプリでのキャッシュの種類を定義します。デフォルト値は、**Persistent** に設定されています。

注：このパラメーターは、

**HDXFlashEnableServerSideContentFetching** を **Enabled** に設定した場合にのみ必要です。

3. Flash リダイレクトはデフォルトで無効になっています。/config/module.ini ファイルで、FlashV2=Off を FlashV2=On に変更して、この機能を有効にします。

## HDX RealTime Web カメラビデオ圧縮

HDX RealTime 機能の Web カメラビデオ圧縮オプションを使用すると、ビデオ会議で消費される帯域幅を効率化できます。このオプションにより、GoToMeeting HDFaces、Skype for Business などのアプリケーションを使用するときに最適なパフォーマンスが提供されます。

1. この機能に必要な要件をユーザーデバイスが満たしていることを確認します。
2. **Multimedia**仮想チャネルが有効になっていることを確認します。これを有効にするには、`$ICAROOT/config/module.ini` ファイルを開き、[ICA3.0] セクションの **MultiMedia** が **On** に設定されていることを確認します。
3. オーディオ入力を有効にするには、[環境設定] ダイアログボックスの [マイクと **Web** カメラ] ページで、[マイクと **Web** カメラを使用する] をクリックします。

### HDX RealTime Web カメラビデオ圧縮の無効化

デフォルトでは、HDX RealTime Web カメラビデオ圧縮機能により Web カメラのパフォーマンスが最適化されます。ただし一部の環境では、ユーザーが USB サポート機能を使って Web カメラを接続しなければならない場合があります。この接続を行うには、次のことを実行する必要があります：

- HDX RealTime Web カメラビデオ圧縮を無効にする
- Web カメラの USB サポートを有効にする

1. 次のパラメーターを適切な INI ファイルの [WFClient] セクションに追加する：

```
AllowAudioInput=False
```

詳しくは、「[デフォルト設定](#)」を参照してください。

2. `usb.conf` ファイルを開きます。通常このファイルは、`$ICAROOT/usb.conf` にあります。
3. 次の行を削除するか、コメントアウトします：

```
DENY: class=0e # UVC (HDX RealTime Web カメラビデオ圧縮経由のデフォルト)
```

4. ファイルを保存して閉じます。

### Citrix 埋め込み **Web** ブラウザーでのセキュアな **SaaS** アプリ [試験段階の機能](#)

SaaS アプリへのセキュリティ保護されたアクセス機能によって、統合されたユーザーエクスペリエンスで公開 SaaS アプリをユーザーに提供できます。SaaS アプリはシングルサインオンで利用できます。管理者は、マルウェアやデータ漏えいから組織のネットワークやエンドユーザーデバイスを保護できるようになりました。この保護のために、特定の Web サイトや Web サイトカテゴリへのアクセスをフィルター処理できます。

Linux 向け Citrix Workspace アプリは、アクセス制御サービスを使用した SaaS アプリの使用をサポートします。このサービスにより、管理者は一貫したエクスペリエンスを提供し、シングルサインオンを統合し、コンテンツ検査を利用することができます。

前提条件：

`libgtkglext1` パッケージが利用可能であることを確認します。

SaaS アプリをクラウドで提供する利点は次のとおりです：

- シンプルな構成 - 操作、更新、使用が簡単です。



- シングルサインオン - シングルサインオンで簡単にログオンできます。
- さまざまなアプリの標準テンプレート - 一般的なアプリをテンプレートを使用して構成できます。

注:

Citrix Browser エンジンを使用した SaaS は、x64 および x86 プラットフォームでのみサポートされており、ArmHardFloatPort (ARMHF) ハードウェアではサポートされていません。

アクセス制御サービスを使用して SaaS アプリを構成する方法については、[アクセス制御に関するドキュメント](#)を参照してください。

SaaS アプリと Citrix Workspace アプリについて詳しくは、Windows 向け Citrix Workspace アプリのドキュメントで「[Workspace 構成](#)」を参照してください。

### H.264

Citrix Workspace アプリでは、Citrix Virtual Apps and Desktops 7 で配信される HDX 3D Pro グラフィックを含む H.264 グラフィックがサポートされます。この機能では、デフォルトで有効になっている深圧縮コーデックが使用されます。これにより、専門的なグラフィック処理アプリケーションを WAN ネットワークを介して使用する場合でも、既存の JPEG フォーマットよりも高いパフォーマンスが提供されます。

注:

H.264 では、Linux 向け Citrix Workspace アプリは YUV 420 形式のみをサポートし、YUV 444 形式はサポートしていません。

この機能を無効にする（つまりグラフィックを JPEG コーデックで処理する）には、このトピックの手順に従ってください。深圧縮コーデックを有効にしたまま、テキストトラッキングを無効にすることもできます。グラフィックに含まれるテキストが多くないまたは重要でない場合は、テキストトラッキングを無効にすることにより、複雑なグラフィック処理時の CPU 負荷を軽減できます。

重要:

この機能を構成する場合は、Citrix Virtual Apps and Desktops または Citrix DaaS の [表示品質] 設定で無損失品質を指定しないでください。無損失品質を指定するとサーバー側の H.264 エンコーディングが無効になり、Citrix Workspace アプリでこの機能が動作しなくなります。

深圧縮コーデックのサポートを無効にするには:

`wfclient.ini`ファイルで、**H264Enabled** を **False** に設定します。これにより、テキストトラッキングも無効になります。

テキストトラッキングのみを無効にするには:

深圧縮コーデックのサポートを有効にしたまま、`wfclient.ini`ファイルで **TextTrackingEnabled** を **False** に設定します。

## 画面タイル

Direct-to-Screen ビットマップデコード、バッチタイルデコード、および XSync の待機機能を使用すると、JPEG エンコードの画面タイルの処理パフォーマンスを最適化できます。

1. JPEG ライブラリがこれらの機能をサポートすることを確認します。
2. `wfclient.ini` の `Thinwire3.0` セクションで、`DirectDecode` および `BatchDecode` に「True」を指定します。

注: バッチタイルデコード機能を有効にすると、XSync の待機機能が自動的に有効になります。

## ログ

以前のバージョンでは、`debug.ini` および `module.ini` ファイルがログの構成に使用されました。

バージョン 2009 以降、次のいずれかの方法を使用してログを構成できます:

- コマンドラインインターフェイス
- GUI

また、バージョン 2009 の時点で、`debug.ini` 構成ファイルは Citrix Workspace アプリインストーラーパッケージから削除されています。

ログは、Citrix Workspace アプリ展開の詳細、構成の変更、および管理アクティビティをログデータベースにキャプチャします。サードパーティの開発者は、Citrix Workspace アプリの Platform Optimization SDK の一部としてバンドルされているログ SDK を使用して、このログメカニズムを適用できます。

ログ情報を使用して、以下を実行できます:

- 変更後に発生する問題を診断してトラブルシューティングする。ログではブレッドクラムが示されます。
- 変更管理の補助および構成の追跡を行う。
- 管理アクティビティのレポートを生成する。

Citrix Workspace アプリがルートユーザー権限でインストールされている場合、ログは `/var/log/citrix/ICAClient.log` に保存されます。それ以外の場合、ログは `${ HOME } /.ICAClient/logs/ICAClient.log` に保存されます。

Citrix Workspace アプリをインストールすると、ログ機能を処理するために `citrixlog` というユーザーが作成されます。

## コマンドラインインターフェイス

1. コマンドプロンプトで `/opt/Citrix/ICAClient/util` パスに移動します。
2. 次のコマンドを実行して、ログの環境設定を指定します。

```
./setlog help
```

使用可能なすべてのコマンドが表示されます。

次の表は、さまざまなモジュールと関連するトレースクラス値です。特定のコマンドラインログ値セットについては、次の表を使用してください：

モジュール	ログクラス
アサーション	LOG_ASSERT
オーディオモニター	TC_CM
CEF を使用した BCR	TC_CEFBCR
クライアントオーディオマッピング	TC_CAM
コネクションセンター	TC_CONNCENTER
クライアント通信ポート	TC_CCM
クライアント側ドライブのマッピング	TC_CDM
クリップ	TC_CLIP
クライアント側プリンターのマッピング	TC_CPM
クライアント側プリンターのマッピング	TC_CPM
フォント	TC_FONT
フレーム	TC_FRAME
グラフィックの抽象化	TC_GA
Input Method Editor	TC_IME
IPC	TC_IPC
キーボードマッピング	TC_KEY
ライセンスドライバー	TC_VDLIC
マルチメディア	TC_MMVD'
マウスマッピング	TC_MOU
MS Teams	TC_MTOP
その他のライブラリ	TC_LIB
プロトコルドライバー	TC_PD
PNA ストア	TC_PN
標準イベントログ	LOG_CLASS
SRCC	TC_SRCC
SSPI ログイン	TC_CSM

---

モジュール	ログクラス
スマートカード	TC_SCARDVD
セルフサービス	TC_SS
セルフサービスの拡張	TC_SSEXT
StorefrontLib	TC_STF
Transport Driver	TC_TD
Thinwire	TC_TW
透過的なウィンドウインターフェイス	TC_TUI
仮想チャンネル	TC_VD
PAL	TC_VP
UI	TC_UI
UIDialogLibWebKit3	TC_UIDW3
UIDialogLibWebKit3_ext	TC_UIDW3E
USB デーモン	TC_CTXUSB
ビデオフレームドライバー	TC_VFM
Web キット	TC_WEBKIT
WinStation ドライバー	TC_WD
Wfica	TC_NCS
Wficaエンジン	TC_WENG
Wfica Shell	TC_WFSHELL
Web ヘルパー	TC_WH
ゼロ遅延	TC_ZLC

---

## GUI

[Menu] > [Preferences] に移動します。[Citrix Workspace-Preferences] ダイアログボックスが開きます。

トレースの詳細レベルを上げると、次の値を使用できます：

- 無効
- エラーのみ
- Normal (標準)

- 詳細

[ログ:] オプションのデフォルト値は [エラーのみ] です。

大量のデータが生成され、トレースが Citrix Workspace アプリのパフォーマンスに大きな影響を与える可能性があります。このため、トラブルシューティングの場合を除き、[**Verbose**] を指定しないことをお勧めします。

必要なログレベルを選択したら、[**Save and Close**] をクリックします。変更はセッションに動的に適用されます。

[**Logging**] オプションドロップダウンメニューの横にある設定アイコンをクリックします。[**Citrix Log Preferences**] ダイアログボックスが開きます。

注:

ICAClient.log ファイルを削除した場合は、ログサービス `ctxlogd` を再起動する必要があります。

たとえば、systemd 対応のセットアップを使用している場合は、次のコマンドを実行します:

```
systemctl restart ctxlogd
```

バージョン **2006** 以前でのログの有効化:

バージョン 2006 以前を使用している場合は、以下の手順を使用してログを有効にします:

1. Linux マシンに Citrix Workspace アプリをダウンロードしてインストールします。
2. ICAROOT 環境変数をインストール場所に設定します。

例: `/opt/Citrix/ICAClient`。

デフォルトでは、TC\_ALL トレースクラスが有効であり、すべてのトレースが提供されます。

3. 特定のモジュールのログを収集するには、`$ICAROOT` の `debug.ini` ファイルを開き、[`wfica`] セクションに必要なトレースパラメーターを追加します。

トレースクラスは「+」記号で追加します。例: `+TC_LIB`。

パイプ記号で区切って複数のクラスを追加できます。

例: `+TC_LIB|+TC_MMVD`。

次の表は、`wfica` モジュールと関連するトレースクラス値です:

モジュール	TraceClasses 値
グラフィック	TC_TW
EUEM	TC_EUEM
WFICA (セッションの起動)	TC_NCS
印刷	TC_CPM
接続シーケンス - WD	TC_WD

モジュール	TraceClasses 値
接続シーケンス - PD	TC_PD
接続シーケンス - TD	TC_TD
プロキシ関連ファイル	TC_PROXY
マルチメディア仮想ドライバー/Web カメラ	TC_MMVD
仮想ドライバー	TC_VD
クライアント側ドライブのマッピング	TC_CDM
オーディオ	TC_CAM
COM (通信ポート)	TC_CCM
シームレス	TC_TWI
スマートカード	TC_SCARDVD

次の表に、コネクションセンターモジュールと関連するトレースクラス値を示します：

モジュール	TraceClasses 値
コネクションセンター	TC_CSM

次の表に、setWebHelper のトレースクラス値を示します：

TraceClasses 値
logSwitch を 1 (有効) または 0 (無効) に設定
例: logSwitch = 1

トラブルシューティング：

ctxlogd が応答しなくなった場合、ログは syslog でトレースされます。

起動のたびに新しいログおよび更新されたログを取得する方法については、「[syslog 構成](#)」を参照してください。

### syslog 構成

デフォルトでは、すべての syslog ログは /var/log/syslog に保存されます。/etc/rsyslog.conf ファイルの [RULES] セクションで以下の行を編集し、ログファイルのパスと名前を構成できます。例：

```
1 user.* -/var/log/logfile_name.log
```

変更を保存し、次のコマンドを使用して syslog サービスを再起動します：

```
sudo service rsyslog restart
```

確認事項：

- 新しい syslog が使用可能であることを確認するには、syslog を削除して、次のコマンドを実行します：  
`sudo service rsyslog restart`。
- メッセージが重複しないようにするには、`rsyslog.conf` ファイルの最初に **\$RepeatedMsgReduction on** を追加します。
- ログを受信するには、`rsyslog.conf` ファイルの最初の **\$ModLoad imuxsock.so** 行がコメント解除されていることを確認します。

リモートログ機能

リモートログ機能を有効にするには：

- サーバー側の構成： syslog サーバーの `rsyslog.conf` ファイルで次の行をコメント解除します：  
`$ModLoad imtcp`  
`$InputTCPServerRun 10514`
- クライアント側の構成： localhost をリモートサーバーの IP アドレスに置き換えて、`rsyslog.conf` ファイルに次の行を追加します：  
`*.* @@localhost:10514`

ログファイルの収集

以前は、Citrix Workspace アプリでログファイルを収集するために使用できるツールはなく、ログファイルは別のフォルダーにありました。さまざまなフォルダーからログファイルを手動で収集する必要があったのです。

2109 バージョン以降、Citrix Workspace アプリでは、さまざまなフォルダーからログファイルを収集するための `collectlog.py` ツールが導入されています。コマンドラインを使用してツールを実行できます。ログファイルは、圧縮されたログファイルとして生成され、ローカルサーバーからダウンロードできます。

前提条件

- Python 3
- ログを保存するために追加の容量が必要

バージョン 2109 以降、`collectlog.py` ツールを使用してログファイルを収集する、次の 2 つの新しいファイルが追加されています：

- `logcollector.ini`ファイル – ログファイルの名前とパスを保存します。
- `collectlog.py`ファイル – ログファイルを収集し、`cwalog_{ timestamp }.tar.gz`圧縮ファイルとして保存します。

デフォルトでは、`[hdxteams]`コンポーネントが`logcollector.ini`ファイルに追加され、Microsoft Teams のログファイルを収集します。ただし、次の手順を使用して、`logcollector.ini`ファイルに他のコンポーネントを追加することもできます：

1. `${ HOME } /.ICAClient/logs/ICAClient.log/logcollector.ini`ファイルに移動します。
2. 次の例に従って、ログファイルを収集するために必要なコンポーネントを追加します：

```
[component_name]
```

```
log_name1 = "log_path1"
```

```
log_name2 = "log_path2"
```

バージョン 2109 を使用している場合は、次の手順を使用してログファイルを収集します：

1. Linux マシンに Citrix Workspace アプリをダウンロードしてインストールします。
2. コマンドラインで`/opt/Citrix/ICAClient/util`パスに移動します。
3. 次のコマンドを実行します：

```
./collectlog.py -h
```

コマンドの使用方法についての情報が次のように表示されます：

```
usage: collect_log [-h] [-c CONFIG] [-a ARCHIVE] optional arguments: -h,
--help show this help message and exit -c CONFIG, --config CONFIG The
logcollector.ini path & file -a ARCHIVE, --archive ARCHIVE The archive
path & file
```

4. 必要に応じて、次のコマンドを実行します：

- `./collectlog.py` – デフォルトパスから構成ファイルを使用してログファイルを収集し、それらを圧縮ログファイルとしてデフォルトパスに保存します。
- `./collectlog.py -c /user_specified_path/logcollector.ini` – ユーザー指定のパスから構成ファイルを使用してログファイルを収集し、それらを圧縮ログファイルとしてデフォルトのパスに保存します。
- `./collectlog.py -c /user_specified_path/logcollector.ini -a/another_user_specified_path` / – ユーザー指定のパスから構成ファイルを使用してログファイルを収集し、それらをユーザー定義のパスに圧縮ログファイルとして保存します。

注：



構成ファイル `logcollector.ini` のデフォルトパスは `/opt/Citrix/ICAClient/config/logcollector.ini` です。圧縮ログファイルのデフォルトパスは `/tmp` です。

5. `/tmp` フォルダに移動し、`cwalog_{ timestamp }.tar.gz` 圧縮ファイルを収集します。

注:

ログファイルは、`cwalog_{ timestamp }.tar.gz` というファイル名で `/tmp` フォルダに保存されます。

## Microsoft Teams の最適化

Citrix Virtual Apps and Desktops または Citrix DaaS、および Citrix Workspace アプリを通じたデスクトップベースの Microsoft Teams の最適化です。Microsoft Teams の最適化は、Microsoft Skype for Business の HDX RealTime の最適化に似ています。両者の違いは、Microsoft Teams 最適化で必要となるすべてのコンポーネントは VDA と Linux 向け Workspace アプリに付属しているという点にあります。

Linux 向け Citrix Workspace アプリは、Microsoft Teams 最適化でオーディオ、ビデオ、画面共有機能をサポートします。

注:

- Microsoft Teams 最適化は、x64 Linux ディストリビューションでのみサポートされます。
- Microsoft の最適化は、Citrix Virtual Apps and Desktops と Citrix DaaS の両方でサポートされています。
- Dell Wyse を使用するシンクライアントの場合、**Citrix** 構成エディターを使用して `/var/.config/citrix/hdx_rtc_engine/config.json` ファイルのパラメーターを編集します。詳しくは、[Dell](#) のドキュメントを参照してください。

ログを有効にする方法については、「[Microsoft Teams のログ](#)」に記載されている手順に従ってください。

システム要件については、「[Microsoft Teams の最適化](#)」を参照してください。

詳しくは、「[Microsoft Teams の最適化](#)」と「[Microsoft Teams リダイレクト](#)」を参照してください。

### オーディオ構成の機能強化

Microsoft Teams が自動利得制御とノイズ抑制のオプションを構成する場合、Citrix リダイレクトの Microsoft Teams は構成された値を優先します。それ以外の場合、これらのオプションはデフォルトで有効になっています。ただし、Citrix Workspace アプリ 2104 以降、デフォルトではエコーキャンセルオプションは無効になっています。Citrix Workspace アプリ 2112 以降、管理者は以下を実行してデフォルト設定を変更し、オーディオの問題（ロボットのような音声、高い CPU 使用率によって音声途切れるなど）のトラブルシューティングを行うことができます:

1. `/var/.config/citrix/hdx_rtc_engine/config.json` ファイルに移動します。
2. 次のオプションを設定します。
  - `EnableAEC` の値を 1 に設定してエコーキャンセルを有効にする、または 0 に設定して無効にする

- `EnableAGC`の値を 1 に設定して自動利得制御を有効にする、または 0 に設定して無効にする
- `EnableNS`の値を 1 に設定してノイズ抑制を有効にする、または 0 に設定して無効にする

```
1 mkdir -p /var/.config/citrix/hdx_rtc_engine
2
3 vim /var/.config/citrix/hdx_rtc_engine/config.json
4
5 {
6
7
8     "EnableAEC":1,"EnableAGC":1,"EnableNS":1
9
10 }
11
12 <!--NeedCopy-->
```

通話が確立されたら、`webrpc`ログ(`/tmp/webrpc/<current date>/`)で次のエントリを監視して、変更が有効になったことを確認します:

```
1 /tmp/webrpc/Wed_Feb__2_14_56_33_2022/webrpc.log:[040.025] Feb 02
   14:57:13.220 webrtcapi.NavigatorUserMedia Info: getUserMedia. audio
   constraints, aec=1, agc=1, ns=1
2 <!--NeedCopy-->
```

### Microsoft Teams でのエンコーダーのパフォーマンス見積もりツール

`HdxRtcEngine`は Microsoft Teams のリダイレクトを処理する Citrix Workspace アプリに組み込まれた WebRTC メディアエンジンです。`HdxRtcEngine.exe`は、エンドポイントの CPU が過負荷状態になることなく維持できる最適な送信ビデオ（エンコーディング）の解像度を見積もることができます。使用できる値は、240p、360p、720p、1080p です。

パフォーマンス見積もりプロセスでは、特定のエンドポイントで達成できる最適な解像度を決定するためにマクロブロックコードを利用します。通話のセットアップ中のコーデックネゴシエーションには、可能な限り高い解像度が使用されます。コーデックネゴシエーションは、ピア間、またはピアと会議サーバー間で行われることがあります。

次の表に、エンドポイントの 4 つのパフォーマンスカテゴリを示します。各カテゴリに使用可能な最大解像度が指定されています:

エンドポイントのパフォーマンス	最大解像度	レジストリキー値
Fast	1080p (1920x1080 16:9 @ 30fps)	3
中	720p (1280x720 16:9 @ 30fps)	2

エンドポイントのパフォーマンス	最大解像度	レジストリキー値
低速	360p (640x360 16:9 @ 30fps または 640x480 4:3 @ 30fps の いずれか)	1
Very slow	240p (320x180 16:9 @ 30fps または 320x240 4:3 @ 30fps の いずれか)	0

たとえば、発信ビデオ（エンコーディング）の解像度値を 360p に設定するには、ターミナルから次のコマンドを実行します：

```
1 mkdir -p /var/.config/citrix/hdx_rtc_engine
2
3 vim /var/.config/citrix/hdx_rtc_engine/config.json
4
5 {
6
7
8     "OverridePerformance":1
9
10 }
11
12 <!--NeedCopy-->
```

### Microsoft Teams のログ

Microsoft Teams のログを有効にするには：

1. /opt/Citrix/ICAClient/debug.ini ファイルに移動します。
2. 以下のように、[HDXTeams] セクションを変更します：

```
1 [HDXTeams]
2 ; Retail logging for HDXTeams 0/1 = disabled/enabled
3 HDXTeamsLogSwitch = 1
4 ; Debug logging; , It is in decreasing order
5 ; LS_NONE = 4, LS_ERROR = 3, LS_WARNING = 2, LS_INFO = 1,
6     LS_VERBOSE = 0
7 WebrtcLogLevel = 0
8 ; None = 5, Info = 4, Warning = 3, Error = 2, Debug = 1, Trace = 0
9 WebrpcLogLevel = 0
```

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

config.json ファイルに次の行を追加してログを有効にすることもできます:

```
1 {
2
3   "WebrpcLogLevel": 0, "WebrtcLogLevel": 0
4 }
5
6 <!--NeedCopy-->
```

### llvm-12 に libunwind-12 ライブラリの依存関係を追加

2111 リリース以降、llvm-12 に libunwind-12 ライブラリと呼ばれる新しい依存関係が追加されました。ただしこれは、デフォルトでは本来のリポジトリに存在しません。次の手順で、libunwind-12 ライブラリをリポジトリに手動でインストールします:

1. ターミナルを開きます。
2. 次の行を入力して、llvmリポジトリキーファイルをインストールします:

```
1 wget -O - https://apt.llvm.org/llvm-snapshot.gpg.key | sudo apt-key
  add
2 <!--NeedCopy-->
```

3. 次の行を入力して、llvmリポジトリのソース一覧を構成します:

```
1 sudo vim /etc/apt/sources.list
2 <!--NeedCopy-->
```

4. 次の行を追加します:

```
1 deb http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
2 deb-src http://apt.llvm.org/bionic/ llvm-toolchain-bionic-12 main
3 <!--NeedCopy-->
```

5. 次のコマンドを実行して、libunwind-12 ライブラリをインストールします:

```
1 sudo apt-get update -y
2 sudo apt-get install libunwind-12
3 <!--NeedCopy-->
```

### 優先ネットワークインターフェースの構成

Citrix Workspace アプリ 2303 バージョン以降、メディアトラフィックの優先ネットワークインターフェースを構成できるようになりました。この機能強化により、複数のネットワーク接続があり、デフォルトのネットワークのパフォーマンスが弱い場合、別のネットワークに変更できます。この拡張機能を有効にするには：

1. `/var/.config/citrix/hdx_rtc_engine/config.json`ファイルに移動します。
2. 以下のセクションに移動します：

```
1      mkdir -p /var/.config/citrix/hdx_rtc_engine
2
3      vim /var/.config/citrix/hdx_rtc_engine/config.json
4
5      {
6
7          "NetworkPreference" :1
8
9      }
10
11
12 <!--NeedCopy-->
```

3. “NetworkPreference:” の値を、必要に応じて以下のいずれかの値に更新します：

- 1: イーサネット
- 2: Wi-Fi
- 3: 携帯ネットワーク
- 4: VPN
- 5: ループバック
- 6: 任意

デフォルトかつ値が設定されていない場合、WebRTC メディアエンジンは利用可能な最適なルートを選択します。

### Microsoft Teams 最適化の機能強化

- Citrix Workspace アプリのバージョン 2101 以降：
  - Citrix Workspace アプリのインストーラーは、Microsoft Teams の着信音をパッケージ化していません。
  - オーディオ出力は、新しく接続されたオーディオデバイスに自動的に切り替わり、適切な音量が設定されます。
  - HTTP プロキシで匿名認証をサポート。
- Citrix Workspace アプリのバージョン 2103 以降、VP9 ビデオコーデックはデフォルトで無効になっています。

- Citrix Workspace アプリのバージョン 2104 以降、エコーキャンセル機能はデフォルトで無効になっています。内蔵スピーカーやマイクを通話に使用しないことをお勧めします。代わりにヘッドフォンを使用してください。この修正は、シンクライアントで音声が届かない問題に対処することを目的としています。
- Citrix Workspace アプリのバージョン 2106 以降：
  - 以前は、[画面共有] をクリックすると、デフォルトまたはメインモニターのプレビューは画面共有でのみ使用できました。

このバージョンでは、すべての画面のプレビューが画面選択メニューに表示されます。VDA 環境で画面を共有するために任意の画面を選択できます。選択したモニターに赤い四角が表示され、選択した画面のコンテンツの小さな画像が画面選択メニューに表示されます。

シームレスモードでは、すべての画面から 1 つを選択して共有できます。Desktop Viewer がウィンドウモードを変更（最大化、復元、または最小化）すると、画面共有が停止します。
- Citrix Workspace アプリのバージョン 2112 以降：

注：

次の機能は、Microsoft Teams から今後の更新がロールアウトされてからのみ使用できます。Microsoft によって更新プログラムがロールアウトされたら、ドキュメントのアップデートおよび発表について、[CTX253754](#)で確認できます。

#### - Microsoft Teams での制御の要求

このリリースでは、参加者が画面を共有している場合、Microsoft Teams の通話中に制御を要求できます。制御できるようになると、共有画面に対して選択、編集、またはその他の変更を実行できます。

画面が共有されているときに制御を取得するには、Microsoft Teams 画面の上部にある [制御を要求] をクリックします。画面を共有している会議参加者は、要求を許可または拒否できます。

制御中は、共有画面に対して選択、編集、その他の変更を実行できます。入力が完了したら、[制御を停止] をクリックします。

制限事項：

- \* Linux クライアントのユーザーは、他のユーザーに制御を渡すことはできません。つまり、Linux クライアントのユーザーがコンテンツの共有を開始した後、[制御を渡す] オプションは共有ツールバーに表示されません。これは Microsoft の制限です。
- \* [制御を要求] オプションは、最適化ユーザーと、エンドポイントで実行されているネイティブの Microsoft Teams デスクトップクライアントのユーザーとの間のピアツーピア通話では使用できません。この問題を回避するために、ユーザーは会議に参加して [制御を要求] オプションを使用することができます。

#### - 動的な e911 のサポート

このリリースの 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 で実行されている 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、提供されます。

レイバウム法では、911 通報者の発信可能な位置を適切な緊急通報受付センター（PSAP）に送信することが義務付けられています。Linux 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。この機能をサポートするには、LLDP ライブラリがシンクライアントのオペレーティングシステムディストリビューションに含まれている必要があります。

- Citrix Workspace アプリのバージョン 2203 以降:

#### **Microsoft Teams** のマルチウィンドウチャットと会議

このリリースでは、Citrix Virtual Apps and Desktops 2112 以降で HDX による最適化が行われた場合、Microsoft Teams でチャットと会議に複数のウィンドウを使用できるようになりました。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、「[Microsoft Teams Pop-Out Windows for Chats and Meetings](#)」を参照してください。

古いバージョンの Citrix Workspace アプリまたは Virtual Delivery Agent (VDA) を使用している場合は、シングルウィンドウコードが今後 Microsoft によって廃止されることに注意してください。ただし、この機能が GA（一般提供）されてから、複数のウィンドウをサポートするバージョンの VDA または Citrix Workspace アプリ（2203 以降）にアップグレードされるまでに、最低 9 か月かかります。

注:

この機能は、Microsoft Teams から以降の更新がロールアウトされた後のみ使用できます。Microsoft によって更新プログラムがロールアウトされたら、ドキュメントのアップデートおよび発表について、[CTX253754](#)で確認できます。

- Citrix Workspace アプリのバージョン 2207 以降:

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（「About/Version」で最適化された Citrix HDX）。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、ヘッドフォンが音声通話自体のプライマリの周辺機器であっても、Microsoft Teams は受信信号をスピーカーに送信します。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:

この機能は、Microsoft Teams から以降の更新がロールアウトされた後のみ使用できます。Microsoft の更新プログラムの公開予定日については、「[Microsoft 365 のロードマップ](#)」を参照してください。ド

キュメントの更新と発表については、[CTX253754](#)でも確認できます。

- Citrix Workspace アプリのバージョン 2207 以降：
  - アプリ共有の有効化: Linux 向け Citrix Workspace アプリ 2209 および Citrix Virtual Apps and Desktops 2109 より、Microsoft Teams の画面共有機能を使用してアプリを共有できます。
  - 高 DPI サポートの機能強化: 高 DPI 機能が有効になっており、4K モニターを使用している場合、Microsoft Teams ビデオのオーバーレイは目的の位置に適切なサイズで表示されます。単一モニターまたはマルチモニターの配置などのディスプレイ設定に関係なく、オーバーレイは常に正しく表示され、拡大されたり、目的の位置以外に表示されたりすることはありません。この強化機能を有効にするには、`wfclient.ini`構成ファイルの `DPIMatchingEnabled` パラメーターが **True** に設定されていることを確認してください。詳しくは、「[DPI マッチングのサポート](#)」を参照してください。
  - **WebRTC SDK** のアップグレード: 最適化された Microsoft Teams で使用される WebRTC SDK のバージョンは、バージョン M98 にアップグレードされます。

- Citrix Workspace アプリのバージョン 2305 以降:

- 最適化された **Microsoft Teams** 通話のスリープモードの機能強化

以前は、最適化された Microsoft Teams 会議に参加しているときに、マウスまたはキーボードの操作がない場合、Citrix Workspace アプリまたは最適化された Microsoft Teams 画面がスリープモードになることがありました。

2305 リリース以降、最適化された Microsoft Teams 会議中にマウスやキーボードの操作がない場合でも、Citrix Workspace アプリまたは最適化された Microsoft Teams 画面はスリープモードになりません。

- 最適化された **Microsoft Teams** ビデオ会議通話のエクスペリエンスの向上

2305 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、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る適切な解像度に適応するため、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。

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（720p、360p など）で配信できます。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。

注:

この機能は、Microsoft Teams からの更新のロールアウト後のみ使用できます。ETA について詳しくは、にアクセスして、Microsoft 365 ロードマップを検索してください。Microsoft によって更新プログラムがロールアウトされたら、ドキュメントのアップデートおよび発表について、[CTX253754](#)で確認できます。

- 最適化された **Microsoft Teams** で短いトーンを再生するサポートを追加

以前は、セカンダリ呼び出し機能が有効になっていると、ビープ音や通知などの短いメロディやトーンが繰り返し再生されていました。たとえば、ゲストが Microsoft Teams 会議に参加するときのトーンが繰り返し再



生されました。これを回避する唯一の方法は、Microsoft Teams を終了して再起動することでした。この問題により、エンドユーザーエクスペリエンスが低下していました。

2307 リリースでは、Citrix Workspace アプリが必要性に応じた短いトーンの再生をサポートします。このサポートでは、セカンダリ呼び出し機能も有効にすることができます。

前提条件:

Microsoft Teams を最新バージョンに更新してください。

注:

上記の機能は、Microsoft Teams から以降の更新がロールアウトされた後のみ使用できます。Microsoft によって更新プログラムがロールアウトされたら、ドキュメントのアップデートおよび発表について、[CTX253754](#)で確認できます。

### NetScaler App Experience (NSAP) 仮想チャネルのサポート

以前は試験段階の機能であった NSAP 仮想チャネル機能が、バージョン 2006 以降完全にサポートされるようになりました。すべての HDX Insight データは、NSAP 仮想チャネルからのみ圧縮されずに送信されます。このアプローチにより、セッションのスケラビリティとパフォーマンスが向上します。NSAP 仮想チャネルはデフォルトでは有効になっています。無効にするには、`module.ini` ファイルで、VDNSAP フラグ `NSAP=Off` を切り替えます。

詳しくは、Linux Virtual Delivery Agent のドキュメントの「[HDX Insight](#)」および Citrix Application Delivery Management サービスのドキュメントの「[HDX Insight](#)」を参照してください。

### マルチモニターレイアウト永続性

この機能は、エンドポイント間でセッションモニターのレイアウト情報を保持します。セッションは、構成済みの同じモニターに表示されます。

前提条件:

この機能には、以下が必要です:

- StoreFront v3.15 以降。
- `.ICAClient` が既に現在のユーザーのホームフォルダーに存在する場合:

`All_Regions.ini` ファイルを削除します

または

`All_Regions.ini` ファイルを保持するには、`[Client Engine\Application Launching]` セクションの最後に次の行を追加します:

`SubscriptionUrl=`

`PreferredWindowsBounds=`

PreferredMonitors=

PreferredWindowState=

SaveMultiMonitorPref=

.ICAClient フォルダが存在しない場合は、Citrix Workspace アプリの新規インストールです。この場合、機能のデフォルト設定は保持されます。

#### 使用例

- 任意のモニターをウィンドウモードで起動し、設定を保存します。  
セッションを再起動すると、同じモードで、同じモニター上の同じ位置に表示されます。
- 任意のモニターを全画面モードで起動し、設定を保存します。  
セッションを再起動すると、同じモニター上に全画面モードで表示されます。
- 複数のモニターにまたがってウィンドウモードでセッションを表示させた後、全画面モードに切り替えると、セッションは、すべてのモニターで全画面表示を続けます。セッションを再起動すると、すべてのモニターにまたがって全画面モードで表示されます。

#### 注:

- レイアウトはすべての保存で上書きされ、レイアウトはアクティブな StoreFront にのみ保存されます。
- 別のモニターで同じ StoreFront から追加のデスクトップセッションを起動する場合、1 つのセッションにレイアウトを保存すると、すべてのセッションのレイアウト情報が保存されます。

#### レイアウトの保存

この機能を有効にするには、以下の手順に従います:

1. StoreFront 3.15 以降のバージョン (v3.15.0.12 以上) を互換性のある Delivery Controller (DDC) にインストールします。
2. [ダウンロード](#) ページから Linux 向け Citrix Workspace アプリ 1808 のビルドをダウンロードし、Linux マシンにインストールします。
3. ICAROOT 環境変数をインストール場所に設定します。
4. **All\_Regions.ini** ファイルが **.ICAClient** フォルダに存在するかを確認します。存在する場合は削除してください。
5. **\$ICAROOT/config/All\_Regions.ini** ファイルで、**SaveMultiMonitorPref** フィールドを見つけます。デフォルトでは、このフィールドの値は「true」です (この機能がオンになっていることを意味します)。オフに切り替えるには、このフィールドを「false」に設定します。  
**SaveMultiMonitorPref** の値を更新する場合は、**.ICAClient** フォルダにある **All\_Regions.ini** ファイルを削除して、値の不一致とプロファイルのロックダウンを防止する必要があります。セッションを開始する前に **SaveMultiMonitorPref** フラグを設定または解除します。

6. 新しいデスクトップセッションを開始します。
7. Desktop Viewer ツールバーの [レイアウトを保存] をクリックして現在のセッションレイアウトを保存します。画面の右下に成功を示す通知が表示されます。  
[レイアウトを保存] をクリックすると、アイコンが灰色表示になります。これは、保存が進行中であることを示します。レイアウトが保存されると、アイコンは正常な状態に戻ります。
8. セッションを切断またはログオフします。  
セッションを再起動すると、同じモードで、同じモニター上の同じ位置に表示されます。

制限事項とサポートされていないシナリオ:

- Linux Display Manager の制限によって、ウィンドウモードセッションのレイアウトを複数のモニターに保存することはできません。
- このリリースでは、さまざまな解像度でセッション情報をモニターに保存することはサポートされていないため、予期しない動作が発生する可能性があります。
- 追加の StoreFront を持つ顧客の展開環境

### **Citrix Virtual Desktops** をデュアルモニターで使用

1. Desktop Viewer を選択し、下向き矢印をクリックします。
2. [ウィンドウ] を選択します。
3. Citrix Virtual Desktops の画面を 2 つのモニターの間にドラッグします。各モニターに画面の約半分が表示されていることを確認します。
4. Citrix Virtual Desktops のツールバーで、[フルスクリーン] を選択します。  
画面が両方のモニターに拡張されます。

### **Workspace Launcher**

公開デスクトップおよび公開アプリケーションを起動するための Workspace Launcher (WebHelper) が Citrix で導入されました。

以前は、Linux 向け Citrix Workspace アプリとともに提供されていたブラウザーのプラグインを使用して、NPAPI ベースの公開デスクトップおよびアプリケーションを起動できました。

解決策として、Workspace Launcher (WebHelper) が Citrix に導入されました。この機能を有効にするには、Citrix Workspace アプリのインストールを検出する要求を Workspace Launcher に送信するように StoreFront を構成します。

バージョン 1901 以降、Citrix Workspace Launcher は StoreFront および Citrix Gateway との直接接続で使用できます。これによって、ICA ファイルを自動的に起動したり、Citrix Workspace アプリがインストールされているか検出することができます。

StoreFront の構成について詳しくは、Knowledge Center の [CTX237727](#) で **Solution – 2 の a) Administrator configuration** を参照してください。

注:

Citrix Workspace Launcher は現在、StoreFront への直接接続でのみ機能します。Citrix Gateway 経由の接続など、その他の場合はサポートされていません。

#### 新しいワークスペース **Web UI** モードの無効化

サードパーティのシンクライアントベンダーによるセルフサービス実行可能ファイルを使用して Linux 向け Citrix Workspace アプリを起動すると、CPU 使用率が 100% になるため、アプリケーションが応答しなくなることがあります。

この問題を回避するために、古い UI モードに戻すには:

1. 次のコマンドを使用して、キャッシュされたファイルを削除します:  

```
rm -r ~/.ICAClient
```
2. `$ICAROOT/config/AuthManconfig.xml` ファイルに移動します。
3. `CWACapableEnabled` キー値を「false」に変更します。
4. Linux 向け Citrix Workspace アプリを起動します。セルフサービス実行可能ファイルが古い UI を読み込みます。

#### キーボードレイアウトの同期

キーボードレイアウトの同期によって、クライアントデバイスの優先キーボードレイアウトを切り替えることができます。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と、クライアントのキーボードレイアウトが仮想アプリおよび仮想デスクトップのセッションに自動的に同期されます。

バージョン 2203 以降、Citrix Workspace アプリは次の 3 つの異なるキーボードレイアウトの同期モードをサポートします:

- セッション起動時に **1** 回だけ同期する - `wfclient.ini` ファイルの `KeyboardLayout` 値に応じて、セッション起動時にクライアントのキーボードレイアウトをサーバーに同期します。`KeyboardLayout` 値が 0 に設定されている場合、システムキーボードは VDA に同期されます。`KeyboardLayout` 値が特定の言語に設定されている場合、その言語固有のキーボードは VDA に同期されます。セッション中にクライアントのキーボードレイアウトに加えた変更は、すぐに有効になりません。変更を適用するには、アプリからサインアウトしてサインインし直します。[セッション起動時に **1** 回だけ同期する] モードは、Citrix Workspace アプリ用に選択されたデフォルトのキーボードレイアウトです。
- 動的な同期を許可する - このオプションは、クライアントのキーボードレイアウトを変更したときに、クライアントのキーボードレイアウトをサーバーに同期します。
- 同期させない - クライアントがサーバーのキーボードレイアウトを使用することを示します。

前提条件:

- Windows VDA の Unicode キーボードレイアウトマッピング機能を有効にします。詳しくは、Knowledge Center の[CTX226335](#)を参照してください。
- Linux VDA の動的なキーボードレイアウトの同期機能を有効にします。詳しくは、「[動的なキーボードレイアウトの同期](#)」を参照してください。
- キーボードレイアウトの同期は XKB lib に依存しています。
- Windows Server 2016 または Windows Server 2019 を使用している場合、`HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme`レジストリパスに移動し、キー名`DisableKeyboardSync`で `DWORD` 値を追加して値を0に設定します。
- `.ICAClient`が既に現在のユーザーのホームフォルダーに存在する場合：

All\_Regions.ini ファイルを削除します

または

All\_Regions.ini ファイルを保持するには、[Virtual Channels\Keyboard] セクションの最後に次の行を追加します：

```
KeyboardSyncMode=
```

```
KeyboardEventMode=
```

### キーボードレイアウトの構成

Citrix Workspace アプリは、3 つの異なるキーボードレイアウト同期モードを有効にするために、UI と構成の両方の設定を提供します。

グラフィカルユーザーインターフェイスを使用してキーボードレイアウトの同期を構成するには：

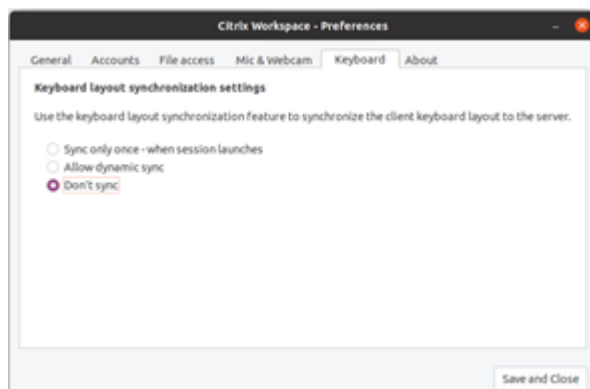
1. システムトレイの Citrix Workspace アプリアイコンから [基本設定] を選択します。

または

ターミナルを開き、インストールパスに移動して、次のコマンドを実行します：

```
util/configmgr
```

[**Citrix Workspace - 基本設定**] ダイアログが開きます。



2. [キーボード] タブをクリックします。

[キーボードレイアウトの同期設定] ページが開きます。

3. 次のいずれかのオプションを選択します：

- セッション起動時に **1** 回だけ同期する - セッション起動時に **1** 度のみキーボードレイアウトが VDA に同期されます。Unicode キーボード入力モードは、[セッション起動時に **1** 回だけ同期する] モードを起動するときに推奨されるオプションです。
- 動的な同期を許可する - セッション内でクライアントキーボードが変更されると、キーボードレイアウトは VDA に動的に同期されます。Unicode キーボード入力モードは、[動的な同期を許可する] モードで推奨されるオプションです。
- 同期しない - クライアントで選択されているキーボードレイアウトに関係なく、クライアントがサーバー上に存在するキーボードレイアウトを使用することを示します。スキャンコードキーボード入力モードは、[同期しない] モードで推奨されるオプションです。[同期しない] のオプションを Unicode に設定する場合は、クライアントのキーボードレイアウトが VDA 側のキーボードレイアウトと同じであることを確認する必要があります。

4. [保存して閉じる] をクリックします。

構成ファイル設定を使用してキーボードレイアウトの同期を構成するには：

構成ファイル `wfclient.ini` を変更して、必要なキーボードレイアウトを有効にします。

セッション起動時に **1** 回だけ同期する：

この機能を有効にした場合、セッションを起動すると、クライアントデバイスのアクティブなキーボードレイアウトが VDA に同期されます。 `wfclient.ini` ファイルの `KeyboardLayout` 値に応じて、セッション起動時にクライアントのキーボードレイアウトをサーバーに同期します。 `KeyboardLayout` 値が `0` に設定されている場合、システムキーボードは VDA に同期されます。 `KeyboardLayout` 値が特定の言語に設定されている場合、その言語固有のキーボードは VDA に同期されます。

このモードを選択するには、次の手順を実行します：

1. 構成ファイル `$HOME/.ICAClient/wfclient.ini` に移動します。
2. 次のエントリを追加します：

```
1 KeyboardSyncMode=Once
2 KeyboardEventMode=Unicode/Scancode
3 <!--NeedCopy-->
```

Unicode キーボード入力モードは、[セッション起動時に **1** 回だけ同期する] モードを起動するときに推奨されるオプションです。

動的な同期を許可する：

この機能を有効にすると、セッション中にクライアントデバイス上でキーボードレイアウトが変更された場合、セッションのキーボードレイアウトも正しく変更されます。

このモードを選択するには、次の手順を実行します：

1. 構成ファイル `$HOME/.ICAClient/wfclient.ini` に移動します。
2. 次のエントリを追加します：

```
1 KeyboardSyncMode=Dynamic
2 KeyboardEventMode=Unicode (or KeyboardEventMode= Scancode)
3 <!--NeedCopy-->
```

Unicode キーボード入力モードは、[動的な同期を許可する] モードで推奨されるオプションです。

同期させない：

この機能を有効にすると、クライアントデバイスで選択されているキーボードレイアウトに関係なく、VDA 側のキーボードレイアウトが使用されます。

このモードを選択するには、次の手順を実行します：

1. 構成ファイル `$HOME/.ICAClient/wfclient.ini` に移動します。
2. 次のエントリを追加します：

```
1 KeyboardSyncMode=No
2 KeyboardEventMode= Scancode (or KeyboardEventMode= Unicode)
3 <!--NeedCopy-->
```

スキャンコードキーボード入力モードは、[同期しない] モードで推奨されるオプションです。[同期させない] オプションを Unicode に設定する場合は、クライアントのキーボードレイアウトが VDA 側のキーボードレイアウトと同じであることを確認する必要があります。

注：

`wfclient.ini` ファイルで `KeyboardSyncMode=""` (空) を設定すると、モードは以前の動作に戻ります。以前の動作では、セッションの起動時にキーボードレイアウトが `$HOME/.ICAClient/wfclient.ini` ファイルから読み取られ、他のクライアント情報とともに VDA に送信されていました。

### キーボード入力モード

さまざまなキーボードレイアウト同期オプションについて、Citrix では、次のキーボード入力モードをお勧めします。

- [同期しない] オプションの場合、スキャンコードモード。
- [動的な同期を許可する] および [セッション起動時に 1 回だけ同期する] の場合、Unicode モード。

`wfclient.ini` ファイルで `KeyboardEventMode` の設定を変更できます。ただし、最高のパフォーマンスを得るには、さまざまなシナリオ、物理キーボード、およびクライアントデバイスに Citrix の推奨モードを使用してください。

## 東アジア言語のクライアント IME

Linux 用 Citrix Workspace アプリでのクライアント入力システム (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。Linux クライアントにお気に入りの IME があるときや、リモートサーバーから IME が利用できないときは、クライアント IME を使用することを選択できます。

この機能を有効にするには、次の手順を実行します：

1. 構成ファイル `$HOME/.ICAClient/wfclient.ini` に移動します。
2. 次のエントリを追加します：

```
1 KeyboardEventMode = Unicode
2 UseLocalIM = True
3 <!--NeedCopy-->
```

クライアントの Linux ディストリビューションに動作する iBus がない場合は、次のように `wfclient.ini` 構成ファイルで IME の言語に従って `KeyboardLayout` 値を明示的に設定する必要があります：

- 中国語 IME の場合 - `KeyboardLayout = Chinese (PRC)`
- 日本語 IME の場合 - `KeyboardLayout = Japanese (JIS)`
- 韓国語 IME の場合 - `KeyboardLayout = Korean`

## GNOME 42 のキーボードレイアウト同期をサポートするための機能強化

2305 バージョンより、Linux 向け Citrix Workspace アプリは、GNOME 42 以降のデスクトップ環境を使用する Ubuntu 22.04 などのデスクトップのキーボードレイアウトの同期をサポートします。

## Windows VDA および Linux VDA でのキーボードレイアウトのサポート

	Linux クライアント			Windows VDA			
Linux クライアントのキーボードの説明	Linux クライアントのキーボードのレイアウト	Linux クライアントのキーボードのバリエーション	同期先	Windows VDA キーボードのレイアウト (ID)	Linux VDA キーボードのレイアウト (ID)	Linux VDA キーボードのバリエーション	Linux VDA キーボードのバリエーション
アラビア語	ara	-	→	ar-SA	00000401	ara	-
アラビア語 (AZERTY)	ara	azerty	→	ar-DZ	00020401	ara	azerty
ドイツ語 (オーストリア)	at	-	→	de-AT	00000407	at	-



	Linux ク ライアント キーボード の説明	Linux ク ライアント キーボード のレイア ウト	Linux ク ライアント キーボード のバリアン ト	同期先	Windows ローケル ID	Windows VDA キー ボードのレ イアウト (ID)	Linux VDA キー ボードのレ イアウト	Linux VDA キー ボードのバ リアント
ベルギー言 語 (alt. ISO)	be	iso-	alternate	→	fr-BE	0000080 c	be	iso- alternate
ベルギー言 語	be	-	-	→	n1-BE	00000813	be	-
ブルガリア 語	bg	-	-	→	bg-BG	00030402	bg	-
ブルガリア 語 (Phonetic Tradi- tional)	bg	phonetic	-	→	bg-BG	00040402	bg	phonetic
ブルガリア 語 (New Phonetic)	bg	bas_phonetic	c	-	bg-BG	00020402	bg	bas_phonetic
ポルトガル 語 (ブラジ ル)	br	-	-	→	pt-BR	00000416	br	-
ベラルーシ 語	by	-	-	→	be-BY	00000423	by	-
英語 (カナ ダ)	ca	eng	-	→	en-CA	00000409	ca	eng
カナダマル チリンガル	ca	multix	-	→	fr-CA	00011009	ca	multix
フランス語 (カナダ、レ ガシー)	ca	fr-	legacy	→	fr-CA	00000c0c	ca	fr- legacy
フランス語 (カナダ)	ca	-	-	→	fr-CA	00001009	ca	-

	Linux ク クライアント キーボード の説明	Linux ク クライアント キーボード のレイア ウト	Linux ク クライアント キーボード のバリアン ト	同期先	Windows ローケル ID	Windows VDA キー ボードのレ イアウト (ID)	Linux VDA キー ボードのレ イアウト	Linux VDA キー ボードのバ リアント
フランス語 (スイス)	ch	fr	→	fr-CH	0000100c	ch	fr	
ドイツ語 (スイス)	ch	-	→	de-CH	00000807	ch	-	
中国語 (簡 体字)	cn	-	→	en-US	00000409	us	-	
チェコ語	cz	-	→	cs-CZ	00000405	cz	-	
チェコ語 (QWERTY)	cz	qwerty	→	cs-CZ	00010405	cz	qwerty	
ドイツ語	de	-	→	de-DE	00000407	de	-	
ドイツ語 (Macin- tosh)	de	mac	→	de-DE	00000407	de	mac	
デンマーク 語	dk	-	→	da-DK	00000406	dk	-	
エストニア 語	ee	-	→	et-EE	00000425	ee	-	
スペイン語 (ラテンア メリカ)	es	-	→	es-ES	0000040a	es	-	
スペイン語 (Macin- tosh)	es	mac	→	es-ES	0000040a	es	mac	
フィンラン ド語	fi	-	→	fi-FI	0000040b	fi	-	
フランス語	fr	-	→	fr-FR	0000040c	fr	-	
フランス語 (Macin- tosh)	fr	mac	→	fr-FR	0000040c	fr	mac	

	Linux ク	Linux ク		Windows	Windows	Linux	Linux
Linux ク	クライアント	クライアント		VDA キー	Linux	Linux	
クライアント	のキーボー	クライアント		ボードのレ	VDA キー	VDA キー	
キーボード	ドのレイア	キーボード		イアウト	ボードのレ	ボードのレ	
の説明	ウト	のバリアン	同期先	ID	イアウト	ボードのバ	
		ト		(ID)	リアント	リアント	
英語 (英国)	gb	-	→	en-GB	00000809	gb	-
英語 (Mac- intosh)	gb	mac	→	en-GB	00000809	gb	mac
英語 (英国、 拡張、Win キー付き)	gb	extd	→	en-GB	00000452	gb	extd
ギリシャ語	gr	-	→	el-GR	00000408	gr	-
クロアチア 語	hr	-	→	hr-HR	0000041a	hr	-
ハンガリー 語	hu	-	→	hu-HU	0000040e	hu	-
アイルラン ド語	ie	-	→	en-IE	00001809	ie	-
ヘブライ語	il	-	→	he-IL	0002040d	il	-
英語 (イン ド、ルピー)	in	eng	→	en-IN	00004009	in	eng
イラク語	iq	-	→	ar-IQ	00000401	iq	-
アイスラン ド語	is	-	→	is-IS	0000040f	is	-
イタリア語	it	-	→	it-IT	00000410	it	-
日本語	jp	-	→	en-US	00000409	us	-
日本語 (Macin- tosh)	jp	mac	→	en-US	00000409	us	mac
韓国語	kr	-	→	en-US	00000409	us	-
スペイン語 (ラテンア メリカ)	latam	-	→	es-MX	0000080a	latam	-

	Linux ク クライアント キーボード の説明	Linux ク クライアント キーボード のレイア ウト	Linux ク クライアント キーボード のバリアン ト	同期先	Windows ローカル ID	Windows VDA キー ボードのレ イアウト (ID)	Linux VDA キー ボードのレ イアウト	Linux VDA キー ボードのバ リアント
リトアニア 語	lt	-	-	→	lt-LT	00010427	lt	-
リトアニア 語 (IBM LST 1205-92)	lt	ibm	-	→	lt-LT	00000427	lt	ibm
リトアニア 語 (標準)	lt	std	-	→	lt-LT	00020427	lt	std
ラトビア語	lv	-	-	→	lv-LV	00020426	lv	-
ノルウェー 語	no	-	-	→	nb-NO	00000414	no	-
ポーランド 語	pl	-	-	→	pl-PL	00000415	pl	-
ポーランド 語 (QWERTZ)	pl	qwertz	-	→	pl-PL	00010415	pl	qwertz
ポルトガル 語	pt	-	-	→	pt-PT	00000816	pt	-
ポルトガル 語 (Macin- tosh)	pt	mac	-	→	pt-PT	00000816	pt	mac
ルーマニア 語 (標準)	ro	std	-	→	ro-RO	00010418	ro	std
セルビア語	rs	-	-	→	sr-Cyrī -RS	00000c1a	rs	-
セルビア語 (ラテン)	rs	latin	-	→	sr-Latn -RS	0000081a	rs	latin
ロシア語	ru	-	-	→	ru-RU	00000419	ru	-

	Linux ク	Linux ク		Windows	Windows	Linux	Linux
Linux ク	クライアント	クライアント		VDA キー	Linux	Linux	
クライアント	のキーボー	クライアント		ボードのレ	VDA キー	VDA キー	
キーボード	ドのレイア	キーボード		イアウト	ボードのレ	ボードのレ	
の説明	ウト	のバリアン	同期先	ID	イアウト	イアウト	リアント
		ト		(ID)			
ロシア語 (タイプライター)	ru	typewriter→		ru-RU	00010419	ru	typewriter
ロシア語 (Macintosh)	ru	mac	→	ru-RU	00000419	ru	mac
スウェーデン語	se	-	→	sv-SE	0000041d	se	-
スウェーデン語 (Macintosh)	se	mac	→	sv-SE	0000041d	se	mac
スロベニア語	si	-	→	sl-SI	00000424	si	-
スロバキア語	sk	-	→	sk-SK	0000041b	sk	-
スロバキア語 (QWERTY)	sk	qwerty	→	sk-SK	0001041b	sk	qwerty
タイ語	th	-	→	th-TH	0000041e	th	-
タイ語 (Pattachote)	th	pat	→	th-TH	0001041e	th	pat
タジク語	tj	-	→	tg-Cyrl-TJ	00000428	tj	-
トルコ語	tr	-	→	tr-TR	0000041f	tr	-
トルコ語 (F)	tr	f	→	tr-TR	0001041f	tr	f
繁体字中国語	tw	-	→	en-US	00000409	us	-

	Linux ク クライアント キーボード の説明	Linux ク クライアント のキーボー ドのレイア ウト	Linux ク クライアント キーボード のバリアン ト	同期先	Windows ローケル ID	Windows VDA キー ボードのレ イアウト (ID)	Linux VDA キー ボードのレ イアウト	Linux VDA キー ボードのバ リアント
ウクライナ 語	ua	-	-	→	uk-UA	00000422	ua	-
英語 (米国)	us	-	-	→	en-US	00000409	us	-
英語 (Mac- intosh)	us	mac	-	→	en-US	00000409	us	mac
英語 (Dvorak)	us	dvorak	-	→	en-US	00010409	us	dvorak
英語 (Dvorak、 左利き)	us	dvorak- l	-	→	en-US	00030409	us	dvorak- l
英語 (Dvorak、 右利き)	us	dvorak- r	-	→	en-US	00040409	us	dvorak- r
英語 (米国、 国際、デッ ドキー付き)	us	intl	-	→	n1-NL	00020409	us	intl
ベトナム語	vn	-	-	→	vi-VN	0000042a	vn	-

### VDA キーボードレイアウト

VDA キーボードレイアウト機能では、クライアントのキーボードレイアウトに関係なく VDA キーボードレイアウトを使用できます。次のキーボードをサポートしています：PC/XT 101、102、104、105、106。

サーバー側のキーボードレイアウトを使用するには、以下の手順を実行します：

1. wfclient.ini ファイルを開きます。
2. KeyboardLayout 属性の値を次のように変更します：

```
KeyboardLayout=(Server Default)
```

KeyboardLayout 属性のデフォルト値は（ユーザープロファイル）です。

3. 変更を保存するには、セッションを再起動します。

## 2 つの仮想デスクトップ間でファイルとフォルダーをコピーして貼り付ける **[Technical Preview]**

以前は、2 つの仮想デスクトップ間でコピーできるのはテキストのみでした。このリリースでは、2 つの仮想デスクトップ間でファイルとフォルダーをコピーして貼り付けることができます。Linux Virtual Delivery Agent では、1 回のコピー/貼り付け操作でのデータの最大転送量は 200MB です。詳細については、「[ファイルのコピーと貼り付け](#)」のドキュメントを参照してください。

この機能はデフォルトで有効になっています。

注:

2 つの仮想デスクトップ間でのファイルとフォルダーのコピーと貼り付けは、Linux 向け Citrix Workspace アプリを実行している x64 Linux ディストリビューションおよび ARM64 アーキテクチャベースのデバイスでのみサポートされます。

この機能を無効にするには、次の手順を実行します:

1. 構成ファイル `/opt/Citrix/ICAClient/config/module.ini` に移動します。
2. `VDGDT` の値を `Off` に編集します。

この Technical Preview のフィードバックは、[Podio](#) フォームからお送りいただけます。

注:

Technical Preview は、顧客が非実稼働環境または制限のある稼働環境でテストし、フィードバックを共有する機会を提供するためのものです。機能プレビュー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としない場合があります。ベータ版のビルドは実稼働環境に展開しないことをお勧めします。

### ファイルタイプの関連付け

Citrix Virtual Apps サービスも、アプリケーションやデスクトップではなくファイルを公開します。この処理は、コンテンツの公開と称され、`pnbrowse` により公開ファイルを開くことができます。

Citrix Workspace アプリが認識するファイルのタイプには制限があります。公開されたアプリケーションが公開されたファイルのファイルタイプに関連付けられている場合のみ:

- システムは、公開されたコンテンツのファイルタイプを認識します
- ユーザーは Citrix Workspace アプリからファイルを表示できます

たとえば、公開された Adobe PDF ファイルを Citrix Workspace アプリで表示するには、Adobe PDF ビューアなどのアプリケーションが公開されている必要があります。適切なアプリケーションが公開されていない場合、ユーザーは公開コンテンツを表示できません。

クライアント側で FTA を有効にするには、次の手順を実行します。

1. 関連付けるアプリがお気に入りまたはサブスクライブ済みのアプリケーションであることを確認します。
2. 公開アプリケーションとサーバー URL の一覧を取得するには、次のコマンドを実行します:

```
1 ./util/storebrowse -l
2
3 ./util/storebrowse -S <StoreFront URL>
4 <!--NeedCopy-->
```

3. 次の構文を使用して、./util/ctx\_app\_bind コマンドを実行します：

```
./util/ctx_app_bind [-p] example_file|MIME-type published-application [
server|server-URI]
```

例：

```
./util/ctx_app_bind a.txt BVT_DB.Notepad_AWTSVDA-0001 https://awddc1.
bvt.local/citrix/store/discovery
```

4. 開こうとしているファイルで、クライアントドライブマッピング (CDM) が有効になっていることを確認します。
5. ファイルをダブルクリックして、関連付けられたアプリケーションで開きます。

#### 公開アプリケーションのファイルタイプの関連付け

Citrix Workspace アプリは、管理者が Citrix Studio で構成した設定を読み取り、適用します。

前提条件：

FTA が構成されているストアサーバーに接続されていることを確認します。

ファイル名の拡張子を Linux 向け Citrix Workspace アプリに関連付けるには、次の手順を実行します：

1. アプリケーションを公開します。
2. Citrix Studio にログオンします。
3. アプリケーションを右クリックしてから、[プロパティ] を選択します。
4. [場所] を選択します。
5. [コマンドライン引数 (オプション)] フィールドに "%\*" (二重引用符で囲んだパーセントと 2 個のアスタリスク記号) を追加してコマンドラインの検証を省略し、[OK] をクリックします。
6. アプリケーションを右クリックし、[プロパティ] を選択します。
7. [ファイルタイプの関連付け] を選択します。
8. Citrix Workspace アプリに関連付けるアプリケーションの拡張子をすべて選択します。
9. [適用]、[ファイルタイプの更新] の順に選択します。
10. 「[ファイルタイプの関連付け](#)」に記載されている手順に従って、クライアント側で FTA を有効にします。



注:

StoreFront のファイルタイプの関連付けが有効になっている必要があります。デフォルトでは有効になっています。

### Citrix Analytics のサポート

バージョン 2006 以降の Citrix Workspace アプリは、ブラウザから起動した ICA セッションから Citrix Analytics Service にデータを転送できるよう更新されています。

Citrix Analytics がこの情報を使用する方法については、「[パフォーマンスでの検索セルフサービス](#)」および「[Virtual Apps and Desktops での検索セルフサービス](#)」を参照してください。

特定のイベントがトリガーされた場合、Linux 向け Citrix Workspace アプリには、Citrix Analytics にログをセキュアに送信するための機能があります。この機能が有効になっていると、ログは分析され、Citrix Analytics サーバーに保存されます。Citrix Analytics について詳しくは、[Citrix Analytics](#) ドキュメントを参照してください。

### 透過的なユーザーインターフェイス

Citrix ICA プロトコルは、透過的なユーザーインターフェイス仮想チャネル (TUI VC) プロトコルを使用して、Citrix Virtual Apps and Desktops または Citrix DaaS のクライアントとホストサーバー間でデータを送信します。TUI プロトコルは、リモート接続用のユーザーインターフェイス [UI] コンポーネントメッセージを送信します。

Linux 向け Citrix Workspace アプリは TUI VC 機能をサポートしています。このため、クライアントはサーバーから送信された TUI パケットを受信でき、クライアントは UI 関連のコンポーネントにアクセスできるようになりました。この機能は、デフォルトのオーバーレイ画面の表示を制御するのに役立ちます。`module.ini` ファイルで `VDTUI` フラグを切り替えることができます: `VDTUI - On/Off`

バージョン 1912 以降、`VDTUI` フラグはデフォルトで **On** に設定されています。その結果、アプリを起動したときに「\<アプリケーション\>の起動中」ダイアログボックスが表示されなくなりました。代わりに、「\<アプリケーション\>の接続中」ダイアログボックスが進行状況バーとともに表示されます。ダイアログには、アプリの起動の進行状況も表示されます。ただし、フラグを **Off** に設定すると、「\<アプリケーション\>の起動中」ダイアログボックスは、他のアプリケーションウィンドウの前面にレンダリングされ、ログインプロンプトを隠します。

仮想チャネルについて詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[Citrix ICA 仮想チャネル](#)」を参照してください。

### サポートされる仮想チャネル数の増加

以前のバージョンのクライアントでは、セッションは最大 32 個の仮想チャネルをサポートしていました。

2103 バージョン以降では、セッションで最大 64 個の仮想チャネルを使用できます。

## 認証

September 15, 2023

Citrix Workspace アプリ 2012 以降、Citrix Workspace アプリ内に認証ダイアログを表示でき、サインイン画面にストアの詳細を表示できます。これにより、優れたユーザーエクスペリエンスが実現します。

認証トークンは暗号化され保存されるため、システムやセッションの再起動時に資格情報を再入力する必要はありません。

注:

この強化された認証機能は、クラウド展開でのみ利用できます。

前提条件:

`libsecret` ライブラリをインストールします。

この機能はデフォルトで有効になっています。

### Storebrowse の認証の機能強化

バージョン 2205 以降では、より快適なユーザーエクスペリエンスを提供するために、Citrix Workspace アプリ内に認証ダイアログを配置し、ログオン画面にストアの詳細を表示するようになりました。認証トークンは暗号化され保存されるため、システムやセッションの再起動時に資格情報を再入力する必要はありません。

認証拡張機能は次の操作で Storebrowse をサポートします:

- `Storebrowse -E`: 使用可能なリソースを一覧表示します。
- `Storebrowse -L`: 公開リソースへの接続が起動します。
- `Storebrowse -S`: サブスクリプションするリソースを一覧表示します。
- `Storebrowse -T`: 指定されたストアのすべてのセッションを終了します。
- `Storebrowse -Wr`: 指定されたストアの、切断されてもアクティブなセッションを再接続します。[r] オプションは、切断されたすべてのセッションを再接続します。
- `storebrowse -WR`: 指定されたストアの、切断されてもアクティブなセッションを再接続します。[R] オプションは、すべてのアクティブなセッションと切断されたセッションを再接続します。
- `Storebrowse -s`: 指定したストアのリソースをサブスクライブします。
- `Storebrowse -u`: 指定したストアのリソースのサブスクリプションを解除します。
- `Storebrowse -q`: 直接 URL を使用してアプリケーションを起動します。このコマンドは、StoreFront ストアでのみ機能します。

注:

- 前に使用したとおり (AuthMangerDaemon を使用して) 引き続き残りの Storebrowse コマンドを使用できます。
- この認証拡張機能は、クラウド展開でのみ適用されます。

- この機能強化により、永続ログイン機能がサポートされます。

### Azure Active Directory で 200 を超えるグループをサポート

2305 リリースより、200 を超えるグループに属している Azure Active Directory ユーザーは、そのユーザーに割り当てられているアプリとデスクトップを表示できるようになります。以前は、同じユーザーがこれらのアプリとデスクトップを表示することはできませんでした。

注:

この機能を有効にするには、ユーザーは Citrix Workspace アプリからサインアウトし、再度サインインする必要があります。

### Storebrowse の認証拡張機能の構成

デフォルトでは、この認証拡張機能は無効になっています。

gnome-keyring が使用できない場合、トークンはセルフサービスプロセスメモリに保存されます。

トークンをメモリに強制的に保存するには、次の手順を使用して gnome-keyring を無効にします:

1. `/opt/Citrix/ICAClient/config/AuthmanConfig.xml` にアクセスします。
2. 次のエントリを追加します:

```
1 <GnomeKeyringDisabled>true</GnomeKeyringDisabled>
2 <!--NeedCopy-->
```

### スマートカード

Linux 向け Citrix Workspace アプリでスマートカードのサポートを構成するには、StoreFront コンソール経由で StoreFront サーバーを構成する必要があります。

Citrix Workspace アプリは、PCSC-Lite および PKCS#11 ドライバーと互換性があるスマートカードリーダーをサポートします。Citrix Workspace アプリはデフォルトで、標準の場所のいずれかで `opensc-pkcs11.so` を見つけることができるようになりました。

Citrix Workspace アプリは、標準以外の場所または別の PKCS\##11 ドライバーで `opensc-pkcs11.so` を見つけることができます。以下の手順で、それぞれの場所を保存できます:

1. 構成ファイルを見つけます: `$ICAROOT/config/AuthManConfig.xml`。
2. 行「`<key>PKCS11module</key>`」に移動し、この行のすぐ後でドライバーの場所を `<value>` エlement に追加します。

注:

ドライバーの場所のファイル名を入力すると、Citrix Workspace アプリは`$ICAROOT/PKCS\##11`ディレクトリ内のそのファイルに移動します。「/」から始まる絶対パスを使用することもできます。

スマートカードを取り出した場合の Citrix Workspace アプリの動作を構成するには、次の手順に従って `SmartCardRemovalAction` を更新します:

1. 構成ファイルを見つけます: `$ICAROOT/config/AuthManConfig.xml`
2. 行「`<key>SmartCardRemovalAction</key>`」に移動し、この行のすぐ後で `noaction` または `forcelogoff` を `<value>` エレメントに追加します。

デフォルトの動作は `noaction` です。スマートカード上で削除を実行するときに、保存されている資格情報や生成されるトークンはクリアされません。

`forcelogoff` を追加すると、スマートカードの削除時にすべての資格情報および StoreFront 内のトークンがクリアされます。

### スマートカードサポートの有効化

サーバーと Citrix Workspace アプリの両方でスマートカードが有効になっている場合、Citrix Workspace アプリはさまざまなスマートカードリーダーをサポートします。

スマートカードは、以下の目的で利用できます:

- スマートカードログオン認証 - Citrix Virtual Apps and Desktops または Citrix DaaS (Citrix Virtual Apps and Desktops サービスの新名称) サーバーに対してユーザーを認証します。
- スマートカードアプリケーションのサポート - スマートカード対応の公開アプリケーションを使用して、ローカルスマートカードデバイスにアクセスできるようにします。

スマートカードのデータは機密性の高い情報であるため、TLS などの信頼された証明機関から認証されたセキュリティアーキテクチャを経由して転送する必要があります。

次に、スマートカードサポートを使用するための条件を示します。

- スマートカードリーダーと公開アプリケーションが、業界標準の PC/SC 規格に準拠している必要があります。
- 使用するスマートカードに適切なドライバーをインストールします。
- PC/SC Lite パッケージをインストールします。
- ミドルウェアが PC/SC を使ってスマートカードにアクセスするための `pcscd` デーモンをインストールして実行します。
- 64 ビットシステムには、64 ビットと 32 ビットの両バージョンの `libpcsc-lite1` パッケージがある必要があります。

サーバー上でのスマートカードサポートの構成について詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[スマートカード](#)」を参照してください。

### スマートカードサポートの機能強化

バージョン 2112 以降、Citrix Workspace アプリはスマートカードリーダーのプラグアンドプレイ機能をサポートします。

スマートカードを挿入すると、スマートカードリーダーがサーバーとクライアントでスマートカードを検出します。

異なるカードを同時にプラグアンドプレイでき、これらすべてのカードが検出されます。

前提条件:

Linux クライアントに `libpcscd` ライブラリをインストールします。

注:

このライブラリは、ほとんどの Linux ディストリビューションの最近のバージョンにデフォルトでインストールされている可能性があります。ただし、Ubuntu 1604 などの一部の Linux ディストリビューションの以前のバージョンでは、`libpcscd` ライブラリのインストールが必要な場合があります。

この拡張機能を無効にするには:

1. `<ICAROOT>/config/module.ini` フォルダに移動します。
2. `SmartCard` セクションに移動します。
3. `DriverName=VDSCARD.DLL` を設定します。

### 新しい **PIV** カードのサポート

バージョン 2303 以降、Citrix Workspace アプリは次の新しい Personal Identification Verification (PIV) カードをサポートします:

- IDEMIA の次世代スマートカード
- DELL TicTok スマートカード

### スマートカードドライバーのパフォーマンスの最適化

Citrix Workspace アプリ 2303 バージョンには、`VDSCARDV2.DLL` スマートカードドライバーのパフォーマンス関連の修正と最適化が含まれています。これらの機能強化は、バージョン 1 `VDSCARD.DLL` よりも優れたパフォーマンスを発揮するのに役立ちます。

### 多要素 (**nFactor**) 認証のサポート

多要素認証は、アクセス権を付与するために追加の ID をユーザーに要求することで、アプリケーションのセキュリティを強化します。

多要素認証により、管理者が認証手順および関連する資格情報コレクションフォームを構成できます。

ネイティブの Citrix Workspace アプリは、既に StoreFront に実装されているフォームによるサインインのサポートを構築することで、このプロトコルをサポートします。Citrix Gateway および Traffic Manager 仮想サーバーの Web サインインページでも、このプロトコルを使用します。

詳しくは、Citrix ADC ドキュメントの「[SAML 認証](#)」および「[nFactor 認証](#)」を参照してください。

### HDX セッションで FIDO2 を使用した認証のサポート

2303 バージョン以降、パスワードなしの FIDO2 セキュリティキーを使用して HDX セッション内で認証できます。FIDO2 セキュリティキーは、企業の従業員がユーザー名やパスワードを入力せずに FIDO2 をサポートするアプリやデスクトップに認証するためのシームレスな方法を提供します。FIDO2 について詳しくは、「[FIDO2 認証](#)」を参照してください。

注:

USB リダイレクト経由で FIDO2 デバイスを使用している場合は、FIDO2 デバイスの USB リダイレクト規則を `$ICAROOT/` フォルダーの `usb.conf` ファイルから削除します。この更新により、FIDO2 仮想チャネルに切り替えることができます。

デフォルトでは、FIDO2 認証は無効になっています。FIDO2 認証を有効にするには、次の手順を実行します:

1. `<ICAROOT>/config/module.ini` ファイルに移動します。
2. `ICA 3.0` セクションに移動します。
3. `FIDO2= On` を設定します。

この機能は現在、PIN コードとタッチ機能を使用するローミング認証 (USB のみ) をサポートしています。FIDO2 セキュリティキーベースの認証を構成できます。前提条件とこの機能の使用については、「[FIDO2 を使用したローカル認証と仮想認証](#)」を参照してください。

FIDO2 をサポートするアプリまたは Web サイトにアクセスすると、プロンプトが表示され、セキュリティキーへのアクセスが要求されます。以前にセキュリティキーを PIN (最小 4 文字、最大 64 文字) で登録したことがある場合は、サインイン時に PIN を入力する必要があります。

以前に PIN なしでセキュリティキーを登録したことがある場合は、セキュリティキーをタッチするだけでサインインできます。

制限事項:

FIDO2 認証を使用して、2 台目のデバイスを同じアカウントに登録できない場合があります。

### カスタムの認証

次の表では、Citrix Workspace アプリで利用可能なカスタムの認証について説明します:

コマンド	SDK	認証の種類	使用するライブラリ		認証の種類を検出
			ラリ	バイナリ	
Fast Connect	<a href="#">Credential Insertion SDK</a>	ユーザー名/パスワード/スマートカード/ドメインパススルー	libCredInject.sc	cis	パラメーター - サードパーティ認証システムの統合で使用されます
Custom Dialog	<a href="#">プラットフォーム最適化 SDK</a>	ユーザー名/パスワード	UIDialogLib.so and UIDialogLib-WebKit3.so	いいえ	自動検出 - シンクライアントパートナーによって使用されます
Storebrowse	<a href="#">Citrix Workspace アプリ</a>	ユーザー名/パスワード	いいえ	Storebrowse	パラメーター

## セキュリティで保護された通信

September 15, 2023

サイトと Citrix Workspace アプリ間の通信を保護するために、Citrix Gateway などのセキュリティ保護技術と統合できます。

注:

StoreFront サーバーとユーザーデバイス間の通信に Citrix Gateway を使用することをお勧めします。

- ファイアウォール: ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。サーバーの内部 IP アドレスを外部インターネットアドレスにマップするネットワークファイアウォール（つまり NAT (Network Address Translation: ネットワークアドレス変換)）を介して Citrix Workspace アプリを使用する場合は、外部アドレスを構成します。
- 信頼されたサーバー。
- Citrix Virtual Apps and Desktops または Citrix DaaS (Citrix Virtual Apps and Desktops サービスの新名称) 展開環境の場合のみ (XenDesktop 7 には適用されません): SOCKS プロキシサーバーまたはセキュアプロキシサーバー (セキュリティプロキシサーバー、HTTPS プロキシサーバー、または Transport Layer Security (TLS) トンネリングプロキシサーバーとも呼ばれます)。プロキシサーバーでネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、Citrix Workspace アプリとサーバー間の接続を制御できます。Citrix Workspace アプリは、SOCKS プロトコルとセキュアプロキシプロトコルをサポートしています。

- Citrix Virtual Apps and Desktops または Citrix DaaS 展開環境の場合のみ: Citrix Secure Web Gateway または TLS プロトコルによる SSL Relay ソリューション。TLS Version 1.0 から 1.2 がサポートされます。

## Citrix Gateway

Citrix Gateway (旧称「Access Gateway」) を使用すると、StoreFront ストアへの接続をセキュアに保護します。また、管理者がデスクトップやアプリケーションへのユーザーアクセスを詳細に管理できます。

Citrix Gateway 経由でデスクトップやアプリケーションに接続するには:

1. 以下のいずれかの方法で、管理者により提供された Citrix Gateway の URL を指定します:
  - セルフサービスユーザーインターフェースの初回使用時に、[アカウントの追加] ダイアログボックスで URL を入力します。
  - セルフサービスユーザーインターフェースの初回使用時以降は、[環境設定] > [アカウント] > [追加] の順に選択します。
  - storebrowse コマンドで接続する場合は、コマンドラインに URL を入力します。

URL により、ゲートウェイと、必要に応じて特定のストアが指定されます。

- Citrix Workspace アプリで検出された最初のストアに接続されるようにするには、URL を「<https://gateway.company.com>」の形式で指定します。
  - 特定のストアに接続する場合は、URL を「<https://gateway.company.com?<storename>>」の形式で指定します。この URL には等号 (=) を含めないでください。storebrowse コマンドで特定のストアに接続する場合は、URL を引用符で囲んで指定します。
2. 資格情報の入力を確認するメッセージが表示されたら、ユーザー名、パスワード、およびセキュリティトークンを入力します。手順について詳しくは、Citrix Gateway のドキュメントを参照してください。
- 認証処理が完了すると、デスクトップまたはアプリケーションが表示されます。

## プロキシサーバー

プロキシサーバーは、ネットワーク内部から外部への、および外部から内部へのアクセスを制限して、Citrix Workspace アプリと Citrix Virtual Apps and Desktops または Citrix DaaS 展開環境との間の接続を制御するために使います。

Citrix Workspace アプリは、以下に加えて、SOCKS および HTTPS プロトコル (Technical Preview) をサポートします:

- Citrix Secure Web Gateway および Citrix SSL Relay、セキュアプロキシプロトコル
- Windows NT チャレンジ/レスポンス (NTLM) 認証。

SOCKS プロトコルを使用してデスクトップを起動するようにプロキシを構成するには、次の手順を実行します:

1. `~/ .ICAClient/All_Regions.ini` 構成ファイルに移動します。
2. 次の属性を更新します:



- a) ProxyTypeを更新します。ProxyTypeとしてSocksV5を使用できます。
- b) ProxyHostを更新します。ProxyHostは、次の形式で追加できます：

<IP>:<PORT>. 例: 「10.122.122.122:1080」

注:

- プロキシを使用するには、EDT を無効にします。EDT を無効にするには、`~/.ICAClient/All_Regions.ini` 構成ファイルの `[Network\UDT]` セクションで `HDXoverUDP` 属性を `off` に設定します。
- 確実にセキュアな接続を実行するには、TLS を有効にします。

#### プロキシサーバーの HTTPS プロトコルのサポート

以前は、SOCKS プロトコルを使用してのみプロキシサーバーに接続できました。Citrix Workspace アプリ 2308 以降では、HTTPS プロトコルを使用してプロキシサーバーに接続することもできます。

HTTPS プロトコルを使用してデスクトップを開くには、次の手順を実行します：

1. 構成ファイル `~/.ICAClient/All_Regions.ini` に移動します。
2. `[Network\UDT]` セクションに移動します。
3. 以下を設定します：

```
1 HDXoverUDP=Off
2 <!--NeedCopy-->
```

4. `[Network\Proxy]` セクションに移動します。

5. 次の属性を更新します：

- ProxyType を更新します。Secure を ProxyType として使用できます。
- ProxyHost を更新します。ProxyHost は、次の形式で追加できます：

<IP>:<PORT>. 例: 「192.168.101.37:6153」。

#### セキュアプロキシサーバー

セキュアプロキシプロトコルを使用する接続を構成して、Windows NT チャレンジ/レスポンス (NTLM) 認証のサポートを有効にできます。このプロトコルを使用できる場合は、追加構成なしで実行時にこれが検出され使用されます。

重要:

NTLM をサポートするには、OpenSSL 1.1.1d ライブラリと libcrypto.so ライブラリが必要です。ユーザー

デバイスにこれらのライブラリをインストールします。ライブラリは Linux ディストリビューションに含まれていることがよくあります。これらは、<http://www.openssl.org/>からダウンロードすることもできます。

### Secure Web Gateway と SSL

Citrix Workspace アプリを Citrix Secure Web Gateway または Citrix SSL (Secure Sockets Layer) Relay と共に使うことができます。Citrix Workspace アプリでは、TLS プロトコルがサポートされます。TLS (Transport Layer Security) は、標準化された SSL プロトコルの最新版です。IETF (Internet Engineering Task Force) が、SSL の公開標準規格の開発を Netscape Communications 社から引き継いだときに、SSL という名前を TLS に変更しました。TLS は、サーバーの認証、データの暗号化、メッセージの整合性の確認を行って、データ通信をセキュアに保護します。米国政府機関をはじめとする組織の中には、データ通信を保護するために TLS の使用を義務付けているところもあります。このような組織では、さらに FIPS 140 (Federal Information Processing Standard) などのテスト済み暗号化基準の使用を義務付けられる場合があります。FIPS 140 は、暗号化の情報処理規格です。

### Secure Web Gateway

Citrix Secure Web Gateway を通常モードまたはリレーモードで使用すると、Citrix Workspace アプリとサーバー間の通信チャネルをセキュリティで保護することができます。Secure Web Gateway を通常モードで使用している場合は、Citrix Workspace アプリ側での構成は不要です。

Citrix Secure Web Gateway Proxy がセキュリティで保護されたネットワーク内のサーバーにインストールされている場合は、Citrix Secure Web Gateway Proxy をリレーモードで使用できます。ただし、リレーモードで使用する場合、Citrix Secure Web Gateway サーバーはプロキシサーバーとして機能するため、Citrix Workspace アプリで次の項目を構成する必要があります：

- Citrix Secure Web Gateway サーバーの完全修飾ドメイン名。
- Citrix Secure Web Gateway サーバーのポート番号。

注：

Citrix Secure Web Gateway バージョン 2.0 では、リレーモードはサポートされていません。

完全修飾ドメイン名には、以下の 3 つの要素を順に指定する必要があります：

- ホスト名
- サブドメイン名
- 最上位ドメイン名

たとえば、my\_computer.my\_company.com は完全修飾ドメイン名です。ホスト名 (my\_computer)、サブドメイン名 (my\_company)、最上位ドメイン名 (com) が順に指定されています。サブドメイン名と最上位ドメイン名の組み合わせ (my\_company.com) をドメイン名といいます。

## SSL Relay

Citrix SSL Relay によるセキュアな TLS 通信では、デフォルトで Citrix Virtual Apps and Desktops または Citrix DaaS サーバーの TCP ポート 443 が使用されます。SSL Relay は、SSL/TLS 接続要求を受信すると、その要求を解読してからサーバーに転送します。

443 以外のリスナーポートを SSL Relay で構成する場合、Citrix Workspace アプリに対して非標準のリスナーポート番号を指定する必要があります。

Citrix SSL Relay を使用すると、次の通信をセキュアに保護できます：

- TLS が有効なユーザーデバイスとサーバー間の通信。

SSL Relay によるセキュリティ機能については、Citrix Virtual Apps のドキュメントを参照してください。

## TLS

以前は、サポートされる最小 TLS バージョンは 1.0 で、最大 TLS バージョンは 1.2 でした。バージョン 2203 以降、サポートされる最大 TLS バージョンは 1.3 です。

[WFClient] セクションに次の構成オプションを追加することでネゴシエートできる TLS プロトコルのバージョンを制御できます。

- MinimumTLS=1.1
- MaximumTLS=1.3

これらはデフォルト値で、コードで設定されています。必要に応じてこれを変更します。

注：

- これらの値は、プログラムの開始時に必ず読み取られます。self-service または storebrowse を開始した後でこれらの値を変更する場合、**killall AuthManagerDaemon ServiceRecord selfservice storebrowse** と入力します。
- Linux 向け Citrix Workspace アプリでは SSLv3 プロトコルは使用できません。
- TLS 1.0/1.1 は、それらをサポートする古い VDI または Citrix Gateway でのみ動作します。

暗号の組み合わせセットを選択するには、[WFClient] セクションで次の構成オプションを追加します。

- SSLCiphers=GOV

これがデフォルト値です。その他の認識される値は、COM および ALL です。

注：

TLS バージョン構成のように、self-service または storebrowse を開始した後にこの構成を変更する場合、**killall AuthManagerDaemon ServiceRecord selfservice storebrowse** と入力する必要があります。

## CryptoKit の更新

CryptoKit バージョン 14.2 は、OpenSSL 1.1.1d バージョンと統合されています。

### 暗号化の更新

この機能は、安全な通信プロトコルにとって重要な変更です。接頭辞が TLS\_RSA\_ の暗号の組み合わせは、Forward Secrecy を提供せず、強度が低いと見なされています。

TLS\_RSA\_ 暗号の組み合わせは完全に削除されました：代わりに、より高度な TLS\_ECDHE\_RSA\_ 暗号の組み合わせがサポートされています。

環境が TLS\_ECDHE\_RSA\_ 暗号の組み合わせで構成されていない場合、暗号化の強度が低いため、クライアントの起動はサポートされません。クライアント認証用に 1536 ビットの RSA キーがサポートされています：

次の高度な暗号の組み合わせがサポートされます：

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)

DTLS v1.0 では、次の暗号の組み合わせがサポートされています：

- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV

DTLS v1.2 では、次の暗号の組み合わせがサポートされています：

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV

TLS v1.3 では、次の暗号の組み合わせがサポートされています：

- TLS\_AES\_128\_GCM\_SHA256 (0x1301)
- TLS\_AES\_256\_GCM\_SHA384 (0x1302)

#### 注：

バージョン 1903 以降では、DTLS は Citrix Gateway 12.1 以降でサポートされています。Citrix Gateway で DTLS がサポートする暗号の組み合わせについては、「[DTLS プロトコルのサポート](#)」を参照してください。

### 暗号の組み合わせ

異なる暗号の組み合わせを有効にするには、パラメーター `SSLCiphers` の値を、`ALL`、`COM` または `GOV` に変更します。このオプションは `$ICAROOT/config` ディレクトリにある `All_Regions.ini` ファイルに含まれ、デフォルト値は `ALL` です。

以下は、ALL、GOV、COM それぞれによって提供される暗号の組み合わせセットです：

- ALL
  - 3つの暗号の組み合わせすべてがサポートされています。
- GOV
  - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)
  - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028)
- COM
  - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)

トラブルシューティング情報については、「[暗号の組み合わせ](#)」を参照してください。

接頭辞が TLS\_RSA\_ の暗号の組み合わせは、Forward Secrecy を提供しません。これらの暗号の組み合わせは現在業界では推奨されていません。ただし、以前のバージョンの Citrix Virtual Apps and Desktops または Citrix DaaS との後方互換性をサポートするために、Citrix Workspace アプリではこれらの暗号の組み合わせを有効にすることもできます。

セキュリティを強化するには、`Enable\\_TLS\\_RSA\\_` フラグを **False** に設定します。

以下は、非推奨の暗号の組み合わせの一覧です。

- TLS\_RSA\_AES256\_GCM\_SHA384
- TLS\_RSA\_AES128\_GCM\_SHA256
- TLS\_RSA\_AES256\_CBC\_SHA256
- TLS\_RSA\_AES256\_CBC\_SHA
- TLS\_RSA\_AES128\_CBC\_SHA
- TLS\_RSA\_3DES\_CBC\_EDE\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_MD5
- TLS\_RSA\_WITH\_RC4\_128\_SHA

注：

最後の2つの暗号の組み合わせは RC4 アルゴリズムを使用しており、セキュアではないため推奨されません。また、TLS\_RSA\_3DES\_CBC\_EDE\_SHA 暗号の組み合わせを非推奨にすることも検討してください。フラグを使用して、これらすべての非推奨を適用することができます。

DTLS v1.2 の構成について詳しくは、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](#)」セクションを参照してください。

前提条件：

バージョン 1901 以前を使用している場合、次の手順を実行します：

・ICAClientが既に現在のユーザーのホームディレクトリに存在する場合：

- `All\\_Regions.ini` ファイルを削除します

または

- `AllRegions.ini` ファイルを保持するには、`[Network\SSL]` セクションの最後に次の行を追加します：
  - `Enable_RC4-MD5=`
  - `Enable_RC4_128_SHA=`
  - `Enable_TLS_RSA=`

.`ICAClient` フォルダが現在のユーザーのホームフォルダに存在しない場合は、Citrix Workspace アプリの新規インストールです。この場合、機能のデフォルト設定は保持されます。

次の表は、各セットの暗号の組み合わせを示しています：

表 1 - 暗号の組み合わせのサポートマトリックス

注：

上記のすべての暗号の組み合わせは、FIPS および SP800-52 に準拠しています。最初の 2 つでのみ (D)TLS1.2 接続が許可されています。暗号の組み合わせのサポートに関する包括的な一覧については、表 1 - 暗号の組み合わせのサポートマトリックスを参照してください。

## 証明書

ストアを SAML 認証 (AUTHv3 プロトコルを使用) で使用すると、次のエラーメッセージが表示されます：「Unacceptable TLS Certificate。」

この問題は、Citrix Workspace アプリ 1906 以降を使用する場合に発生します。トラブルシューティングの手順については、次の Knowledge Center の記事を参照してください：

- [CTX260336](#)
- [CTX231524](#)
- [CTX203362](#)

お使いの StoreFront サーバーが使用している証明書と一致する中間証明書を提供できない場合、または中間証明書をインストールしてスマートカードユーザーをサポートする場合、StoreFront ストアを追加する前に次の手順を実行します：

1. 1 つまたは複数の PEM 形式の中間証明書を別途入手します。

ヒント：

PEM 形式の証明書が見つからない場合は、`openssl` ユーティリティを使用して CRT 形式の証明書を PEM ファイルに変換できます。

2. ユーザー（通常はルート）がパッケージのインストール時に、以下の手順を実行します：

- a) 1 つまたは複数のファイルを `$ICAROOT/keystore/intcerts` にコピーします。
- b) パッケージをインストールしたユーザーとして次のコマンドを実行します。

```
$ICAROOT/util/ctx_rehash
```

証明機関により発行され、ユーザーデバイスに信頼されていないサーバー証明書を認証するには、StoreFront ストアを追加する前に以下の手順を行ってください：

1. PEM 形式のルート証明書入手します。

ヒント: PEM 形式の証明書が見つからない場合は、`openssl`ユーティリティを使用して CRT 形式の証明書を PEM ファイルに変換できます。

2. パッケージをインストールしたユーザー（通常はルート）が、以下の手順を実行します。

- a) ルート証明書を `$ICAROOT/keystore/cacerts` にコピーします。

- b) 次のコマンドを実行します:

```
$ICAROOT/util/ctx_rehash
```

## HDX Enlightened Data Transport Protocol (EDT) の機能強化

以前のリリースでは、`HDXoverUDP`を`Preferred`に設定すると、EDT 経由のデータ転送が、TCP へのフォールバックのプライマリとして使用されます。

Citrix Workspace アプリのバージョン 2103 以降では、セッション画面の保持を有効にすると、EDT と TCP が次のタイミングで並行して試行されます:

- 初期接続
- セッション画面の保持による再接続
- クライアントの自動再接続

この機能強化により、EDT が優先される場合の接続時間が短縮されます。ただし、必要なベースの UDP トランスポートは利用できず、TCP を使用する必要があります。

デフォルトでは、TCP にフォールバックした後、アダプティブトランスポートは 5 分ごとに EDT を検索し続けます。

## Enlightened Data Transport (EDT) MTU 検出

Citrix Workspace アプリのバージョン 2109 では、Enlightened Data Transport (EDT) で最大転送単位 (MTU) 検出がサポートされます。その結果、EDT プロトコルの信頼性と互換性が向上し、ユーザーエクスペリエンスが向上します。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[EDT MTU Discovery](#)」セクションを参照してください。

## EDT IPv6 のサポート

Citrix Workspace アプリのバージョン 2203 以降では、EDT IPv6 がサポートされています。

注:

IPv6 は、TCP と EDT の両方でサポートされています。ただし、IPv6 は TCP over TLS および EDT over DTLS ではサポートされていません。

## Storebrowse

September 15, 2023

Storebrowse は、クライアントとサーバー間の相互通信に使用される軽量のコマンドラインユーティリティです。Storebrowse ユーティリティを使用すると、管理者は以下のような日常的な操作を自動化できます。

- ストアを追加します。
- 構成済みのストアから公開アプリと公開デスクトップを一覧表示します。
- 構成済みのストアからアプリとデスクトップをサブスクリブおよびサブスクリブ解除します。
- 公開アプリと公開デスクトップのショートカットを有効または無効にします。
- 公開アプリケーションを起動します。
- 切断されたセッションに再接続します。

通常、Storebrowse ユーティリティは `/util` フォルダにあります。インストール場所で見つけることができます。  
例: `/opt/Citrix/ICAClient/util`。

### 前提条件

Storebrowse ユーティリティには **libxml2** ライブラリパッケージが必要です。

### 公開デスクトップおよび公開アプリケーションの起動

リソースを起動するには、次の 2 つの方法があります：

- コマンドラインまたは Storebrowse コマンドを使用できます。
- UI を使用してリソースを起動できます。

ここでは、Storebrowse コマンドについて説明します。

### サービス継続性のための **Storebrowse** の強化

以前は、ワークスペース接続リースファイルは、セルフサービスプラグインを使用して接続した場合にのみ、リモートサーバーで使用可能なファイルと同期されていました。その結果、Storebrowse を使用してアプリまたはデスクトップセッションを起動したときに、サービス継続性機能がサポートされていませんでした。ほとんどのサードパーティのシンクライアントベンダーは、Storebrowse を使用して Workspace プラットフォームに接続しており、サービス継続性機能が有効になっていませんでした。

Citrix Workspace アプリのバージョン 2109 以降、Workspace 接続リースファイルは、Storebrowse を使用して接続するときに、リモートサーバーで使用可能なファイルと同期します。この機能により、サードパーティのシンクライアントベンダーはオフラインでも Workspace にアクセスできます。



### 注:

- この拡張機能は、クラウド展開でサービス継続性が有効になっている場合にのみ使用できます。詳しくは、Citrix Workspace ドキュメントの「[サービス継続性を構成する](#)」セクションを参照してください。

### コマンドの使用法

以下のセクションでは、Storebrowse ユーティリティで利用できる Storebrowse コマンドについて詳しく説明します。

#### ストアの追加

`-a, --addstore`

#### 説明

ストアをゲートウェイおよびピーコンの情報とともに ServiceRecord デモンプロセスに追加します。このコマンドは、ストアの完全な URL を返します。ストアの追加に失敗すると、エラーが表示されます。

StoreFront のコマンド例:

コマンド:

```
./storebrowse -a *URL of StoreFront or a PNAStore*
```

例:

```
./storebrowse -a https://my.firstexamplestore.net
```

### 注:

Storebrowse ユーティリティを使用して複数のストアを追加できます。

#### ヘルプ

`-, -h, --help`

#### 説明

Storebrowse ユーティリティの使用法の詳細を提供します。

#### ストアの一覧表示

`-l --liststore`

#### 説明

追加したストアの一覧が表示されます。

StoreFront のコマンド例:

```
./storebrowse -l
```

列挙

`-E --enumerate`

説明

使用可能なリソースの一覧が表示されます。デフォルトでは、次の値が表示されます:

- リソース名
- 表示名
- リソースフォルダー

詳細を表示するには、`-M --details` コマンドを `-E` コマンドに追加します。

注:

`-E` コマンドを実行すると、まだ資格情報を指定していない場合に認証ウィンドウが表示されます。

`-liststore` で表示されたストア URL 全体を入力します。

StoreFront のコマンド例:

- `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -E -M https://my.firstexamplestore.net/Citrix/Store/discovery`

サブスクライブ済み

`-S --subscribed`

説明

サブスクリプションするリソースを一覧表示します。デフォルトでは、次の値が表示されます:

- リソース名
- 表示名
- リソースフォルダー

詳細を表示するには、`-M --details` コマンドを `-E` コマンドに追加します。

StoreFront のコマンド例:

- `./storebrowse.exe -S https://my.firstexamplestore.net/Citrix/Store/discovery`

- `./storebrowse.exe -S -M https://my.firstexamplestore.net/Citrix/Store/discovery`

#### 詳細

`-M --details`

#### 説明

このコマンドは、公開アプリケーションのさまざまな属性を返します。通常は**-E** および**-S** コマンドとともに使用されます。このコマンドでは、必要な詳細に対応する数値の合計を引数として指定します。

- Publisher(0x1)
- VideoType(0x2)
- SoundType(0x4)
- AppInStartMenu(0x8)
- AppOnDesktop(0x10)
- AppIsDesktop(0x20)
- AppIsDisabled(0x40)
- WindowType(0x80)
- WindowScale(0x100)
- DisplayName(0x200)
- AppIsMandatory(0x10000)
- CreateShortcuts(0x100000)
- RemoveShortcuts(0x200000)

#### 注:

- サブスクライブしたアプリケーションのメニュー項目を作成するには、**-S**、**-s**、および**-u** コマンドで `CreateShortcuts (0x100000)` 引数を指定します。
- すべてのメニュー項目を削除するには、**-S** コマンドで `RemoveShortcuts (0x200000)` を使用します。

#### StoreFront のコマンド例:

```
./storebrowse.exe -S -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery
```

上記のコマンド例では、0x264 は、`DisplayName(0x200)`、`AppIsDisabled(0x40)`、`AppIsDesktop(0x20)`、`SoundType(0x4)` の組み合わせです。これによって、サブスクライブされたリソース一覧が詳細とともに表示されます。

**-M** コマンドを使用して、リソース一覧を必要な詳細とともに表示できます:

```
./storebrowse.exe -E -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery
```

### 注:

- 値は 10 進数または 16 進数形式で指定できます。たとえば、0x200 の場合は 512 です。
- これらの情報の一部が storebrowse では使用できない場合、出力値は 0 になります。

### サブスクライブ

`-s --subscribe`

#### 説明

指定したストアのリソースをサブスクライブします。

StoreFront のコマンド例:

```
./storebrowse -s <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

### サブスクリプション解除

`-u --unsubscribe`

#### 説明

指定したストアのリソースのサブスクリプションを解除します。

StoreFront のコマンド例:

```
./storebrowse -u <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

### 起動

`-L --launch`

#### 説明

公開リソースへの接続が起動します。セッションは接続されたまま、コマンドが自動的に終了します。

StoreFront のコマンド例:

```
./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

### アイコン

`-i --icons`

#### 説明

このコマンドは、デスクトップおよびアプリケーションのアイコンを PNG 形式で取得します。このコマンドは**-E** または**-S** コマンドとともに使用されます。

必要なサイズと深度のアイコンを取得するには、**best** 引数メソッドまたは**サイズ**引数メソッドを使用します。

### best 引数

**best** 引数メソッドを使用すると、サーバー上で利用可能な最適なサイズのアイコンを取得できます。後でアイコンを必要なサイズに変換できます。格納、帯域幅の適用、スクリプティングの簡素化には **best** 引数メソッドが最も効率的です。ファイルは `<resource name>.png` 形式で保存されます。

### サイズ引数

指定したサイズと深度のアイコンを取得するには、**サイズ**引数メソッドを使用します。サーバーが特定のサイズまたは深度のアイコンを取得できない場合、エラーが表示されます。

サイズ引数は **WxB** 形式です。各項目の意味は次のとおりです：

- **W** はアイコンの幅です。すべてのアイコンは正方形であるため、サイズの指定に必要な値は 1 つだけです。
- **B** は色の深度です。つまり、ピクセルあたりのビット数です。

注：

値 **W** は必須です。値 **B** はオプションです。

値を指定しない場合、使用可能なすべての解像度のアイコンが表示されます。ファイルは `<resource name>_WxWxB.png` 形式で保存されます。

どちらのメソッドも、**-E** コマンドまたは**-S** コマンドが返すリソースごとに、アイコンを **.png** 形式で保存します。

アイコンは、**.ICAClient/cache/icons** フォルダに保存されます。

StoreFront のコマンド例：

- `./storebrowse -E -i best https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -S -i 16x16 https://my.firstexamplestore.net/Citrix/Store/discovery`

### セッションの再接続

`-W [r|R] --reconnect [r|R]`

#### 説明

指定されたストアの、切断されてもアクティブなセッションを再接続します。[r] オプションは、切断されたすべてのセッションを再接続します。[R] オプションは、すべてのアクティブなセッションと切断されたセッションを再接続します。

StoreFront のコマンド例:

- `./storebrowse -Wr https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -WR https://my.firstexamplestore.net/Citrix/Store/discovery`

セッションの切断

`-WD --disconnect`

説明

指定したストアのすべてのセッションを切断します。

StoreFront のコマンド例:

`./storebrowse -WD https://my.firstexamplestore.net/Citrix/Store/discovery`

セッションの終了

`-WT --terminate`

説明

指定されたストアのすべてのセッションを終了します。

StoreFront のコマンド例:

`./storebrowse -WT https://my.firstexamplestore.net/Citrix/Store/discovery`

バージョン

`-v --version`

説明

storebrowse ユーティリティのバージョンを表示します。

StoreFront のコマンド例:

`./storebrowse -v`

ルートディレクトリ

`-r --icaroot`

説明

Linux 向け Citrix Workspace アプリがインストールされているルートディレクトリを指定します。ディレクトリを指定しない場合は、実行時にルートディレクトリが特定されます。

StoreFront のコマンド例:

```
./storebrowse -r /opt/Citrix/ICAClient
```

ユーザー名、パスワード、ドメイン

```
-U --username, -P --password, -D --domain
```

説明

ユーザー名、パスワード、ドメインの詳細をサーバーに渡します。このメソッドは、PNA ストアでのみ機能します。StoreFront ストアでは、このコマンドは無視されます。詳細情報はキャッシュされません。すべてのコマンドで詳細を入力します。

StoreFront のコマンド例:

```
./storebrowse -E https://my.firstexamplestore.net/Citrix/Store/discovery -U  
user1 -P password -D domain-name
```

ストアの削除

```
-d --deletestore
```

説明

ストアの ServiceRecord デモンへの登録を解除します。

StoreFront のコマンド例:

```
./storebrowse -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

セルフサービスの構成

```
-c --configselfservice
```

説明

セルフサービスユーザーインターフェイスの設定を取得および構成します。この設定は、StoreCache.ctx に格納されます。引数は、<entry[=value]> の形式で指定します。「entry」のみを指定すると、現在の設定値が出力されます。「value」を指定する場合、その値がセルフサービスユーザーインターフェイスに設定されます。

StoreFront のコマンド例:

```
./storebrowse -c SharedUserMode=True
```

### CR ファイルの追加

`-C --addcr`

#### 説明

Citrix Receiver (CR) ファイルを読み取って、各ストアの追加を確認するメッセージを表示します。-a コマンドと同じ出力が得られますが、複数のストアが含まれます (各行に 1 つのストア)。

StoreFront のコマンド例:

```
./storebrowse -C <path to CR file>
```

### 接続リースファイルの同期

`-o --synclease`

#### 説明

ワークスペース接続リースファイルと、指定されたストアのリモートサーバーで使用可能なファイルとの同期を開始します。このコマンドは、デフォルトストアを更新し、リースファイルの同期をトリガーするのに役立ちます。サービス継続性が無効になっている場合、エラーが表示されます。

コマンド:

```
./storebrowse -o *URL of Store *
```

StoreFront のコマンド例:

```
./storebrowse -o https://my.firstexamplestore.net
```

### storebrowse デーモンの終了

`-K --killdaemon`

#### 説明

storebrowse デーモンを強制終了します。その結果、すべての資格情報およびトークンがパーズされます。

StoreFront のコマンド例:

```
./storebrowse -K
```

### エラーコードの一覧表示

`-e --listerrorcodes`

#### 説明

登録されているエラーコード一覧を表示します。



StoreFront のコマンド例:

```
./storebrowse -e
```

ストアのゲートウェイ

```
-g --storegateway
```

説明

ServiceRecord デーモンに登録済みのストアのデフォルトのゲートウェイを設定します。

StoreFront のコマンド例:

```
./storebrowse -g “<unique gateway name>” https://my.firstexamplestore.net/  
Citrix/Store/discovery
```

注:

ストアのゲートウェイの一覧で、同じゲートウェイ名を使用することはできません。

クイック起動

```
-q, --quicklaunch
```

説明

直接 URL を使用してアプリケーションを起動します。このコマンドは、StoreFront ストアでのみ機能します。

StoreFront のコマンド例:

```
.\storebrowse.exe -q <https://my.firstexamplestore.net/Citrix/Store/resources  
/v2/Q2hJk0lmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix  
/Store/discovery>
```

デーモン化

```
-n --nosingleshot
```

説明

常に storebrowse プロセスをデーモン化します。

StoreFront のコマンド例:

```
./storebrowse -n
```

ファイルのパラメーター

`-F --fileparam`

説明

指定されたファイルパスとリソースでファイルを起動します。

StoreFront のコマンド例:

```
./storebrowse -F "<path to file>" -L <Resource Name> <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

ワークフロー

ここでは、storebrowse コマンドを使用してアプリを起動する簡単なワークフローを紹介します:

1. `./storebrowse -a https://my.firstexamplestore.net`

ストアを追加し、ストアの完全な URL を指定します。完全な URL は、後のコマンドで使用されるため、メモしておきます。

2. `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`

すべての公開アプリとデスクトップを一覧表示します。登録済みストアに表示されるポップアップを使用して、認証情報を入力します。

3. `./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery`

リソースを起動します。前のコマンドの出力から取り出したリソース名 (Resource\_Name) を使用します。

4. `./storebrowse -K`

このコマンドは、前段階で入力した資格情報を削除し、storebrowse デーモンを終了します。このコマンドを明示的に使用しない場合、storebrowse プロセスは 1 時間後に終了します。

## トラブルシューティング

September 15, 2023

ここでは、管理者による Citrix Workspace アプリのトラブルシューティングに役立つ情報を提供します。

接続

次の接続の問題が発生する可能性があります。

## Fedora 29/30 での ICA 起動

ICA 起動が Fedora 29/30 で失敗することがあります。この問題を回避するには、次の手順を実行します：

1. コマンドを使用して `compat-openssl10` をインストールします。

```
sudo yum install compat-openssl10.x86_64
```

2. `~/.bashrc` で環境変数を設定して、セッションごとに読み込みます。この操作は、古い `libcrypto` ライブラリを参照します。

```
export LD_PRELOAD=/lib64/libcrypto.so.1.0.2o
```

注：

Citrix Workspace アプリは Wayland Compositor よりも X.Org Server で適切に機能します。Wayland をデフォルトのグラフィックプロトコルとして使用しているディストリビューションでは、次のどちらかのコメントを解除します：

```
/etc/gdm/custom.conf または /etc/gdm3/custom.conf
```

```
の WaylandEnable=false
```

サインアウトしてからサインインして、X.Org サーバーを参照します。

## 公開リソースまたはデスクトップセッション

Windows サーバーへの接続を確立しているときに、ダイアログボックスに「サーバー xxx に接続しています」というメッセージが表示されて接続画面が開かない場合は、サーバーのクライアントアクセスライセンス (CAL) の構成を確認する必要があります。ライセンスについて詳しくは、「[ライセンス](#)」を参照してください。

## セッション再接続

Citrix Workspace アプリが必要とするものより多いウィンドウの色数でセッションを再接続しようとする、接続に失敗する場合があります。この障害は、サーバーで使用可能なメモリが不足している場合に発生します。

再接続に失敗した場合、Citrix Workspace アプリはセッションで元の色数を使おうとします。再接続した場合は、サーバーは新しいセッションを要求した色数で開始しようとし、元のセッションは切断されたままになります。ただし、サーバーのメモリが依然不足している場合は 2 つ目のセッションも失敗する可能性があります。

## 完全なインターネット名

Citrix では、ネットワークで DNS (ドメインネームサーバー) を構成することをお勧めします。この構成により、接続するサーバーの名前を解決できます。構成された DNS がない場合は、サーバー名を IP アドレスに解決することができません。また、サーバーを名前ではなく IP アドレスで指定することもできます。TLS 接続には、IP アドレスではなく、完全修飾ドメイン名が必要です。

### セッション開始の遅延

マウスを動かすまでセッションが開始されないことがあります。Linux カーネルでの乱数生成に問題があると、この問題が発生します。この問題を回避するには、`rngd`（ハードウェアベース）または `haveged`（Magic Software）などのエントロピー生成デーモンを実行してください。

### 暗号の組み合わせ

新しい暗号のサポートで接続が失敗した場合は、次の手順を実行します：

1. 以下のようなさまざまなツールを使用して、サーバーがサポートする暗号の組み合わせを確認できます：
  - `Ssllabs.com`（サーバーがインターネットにアクセスできるようにする必要があります）
  - `sslyze` (<https://github.com/nabla-c0d3/sslyze>)
2. Linux クライアントで、`WireShark` がパケット（Client Hello、Server Hello）を検出し、フィルター（`ip.addr == VDAIPAddress`）を使用して SSL セクションを検出します。結果には、クライアントによって送信され、サーバーによって受け入れられた暗号の組み合わせが表示されます。

### 不正な **Citrix Optimization SDK**

Citrix Optimization SDK パッケージに含まれている `UIDialogLibWebKit.so` のバージョンが正しくありません。この問題を回避するには、次のいずれかを実行します：

1. [ダウンロード](#) ページから Citrix Optimization SDK パッケージのバージョン 18.10 をダウンロードします。
  - a) パス「`CitrixPluginSDK/UIDialogLib/GTK`」を指定します：

```
cd CitrixPluginSDK/UIDialogLib/GTK
```
  - b) すべてのオブジェクトファイルを削除します：

```
rm -rf *.o
```
  - c) `WebKit` フォルダーに移動します：

```
cd ../WebKit
```
  - d) 既存の `UIDialogLibWebKit.so` を削除します：

```
rm -rf UIDialogLibWebKit.so
```
  - e) `WebKit` ディレクトリで次のコマンドを使用します：

```
make all
```

新しい `UIDialogLibWebKit.so` が生成されます：
  - f) 新しいライブラリを `$ICAROOT/lib` ディレクトリにコピーします。

### SSL 接続の暗号の組み合わせが弱い

TLS 接続を確立すると、Citrix Workspace アプリではより高度な、制限された暗号の組み合わせセットがデフォルトで提供されます。

古い暗号の組み合わせを必要とするサーバーに接続する場合、[WFClient] セクションで構成オプションを `SSLCiphers=ALL` に設定します。

次の高度な暗号の組み合わせがサポートされます：

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)、ALL、GOV
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028)、ALL、GOV
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)、ALL、COM

### 接続の切断

EDT プロトコルを使用すると、次のエラーメッセージが表示されることがあります：“...” への接続が失われました。この問題は、EDT の最大転送単位がデフォルトの 1,500 バイトより小さいルーター経由の接続が原因で発生することがあります。以下を実行します：

- 構成ファイルで `edtMSS=1000` を設定します。

### 接続エラー

接続エラーでは、さまざまな異なるエラーダイアログが表示されます。以下はその例です。

- 接続エラー：認証サービスとの通信中にプロトコルエラーが発生しました
- 認証サービスにアクセスできません
- このサーバーアドレスでアカウントを追加することはできません

こうしたエラーの原因は、以下のようにさまざまです：

- ローカルコンピューターとリモートコンピューターが共通の TLS プロトコルをネゴシエートできないとき。詳しくは、「[TLS](#)」を参照してください。
- リモートコンピューターの TLS 接続に古い暗号の組み合わせが必要な場合。この場合、接続の再開前に、構成ファイルの `[WFClient\]` セクションで構成オプションを `SSLCiphers=ALL` に設定し `killall AuthManagerDaemon ServiceRecord selfservice storebrowse` を実行します。
- リモートコンピューターが不適切にクライアント証明書を要求する場合。IIS は Citrix、Authentication、および Certificate の証明書のみを「許可」または「要求」する必要があります。
- そのほかの問題。

### 狭帯域幅接続

サーバー上では Citrix Virtual Apps and Desktops または Citrix DaaS (Citrix Virtual Apps and Desktops サービスの新名称) の最新バージョンを使用することを推奨します。また、ユーザーデバイスで最新の Citrix Workspace

アプリを使用することもお勧めします。

帯域幅の狭い接続を使用する場合は、Citrix Workspace アプリの構成や使い方を変えてパフォーマンスを向上させることができます。

- **Citrix Workspace** アプリの接続構成 - Citrix Workspace アプリの接続構成を変更することで、ICA で消費される帯域幅を減らしてパフォーマンスを改善できます。
- **Citrix Workspace** アプリの使用方法 - Citrix Workspace アプリの使用方法を変更することで、高いパフォーマンスが求められる接続での消費帯域幅を抑えることができます。
- **UDP** オーディオの有効化 - この機能を有効にすると、ネットワークトラフィック負荷の高い VoIP (Voice over IP) 接続での遅延レベルが安定します。
- 最新バージョンの **Linux** 向け **Citrix Workspace** アプリおよび **Citrix Virtual Apps and Desktops** または **Citrix DaaS** の使用 - Citrix 製品では、パフォーマンスを向上させて機能を拡張するためのバージョンアップが常に行われています。また、多くのパフォーマンス機能を使用するには、最新の Citrix Workspace アプリおよびサーバーソフトウェアが必要である場合もあります。

### 表示

#### スクリーンティアリング

スクリーンティアリングは、横ブロックに画面上で複数の異なるフレームが同時に積み重なって表示されるときに発生します。この問題は、画面上のコンテンツを迅速に大幅に変更する場合に多発します。

データが VDA でキャプチャされると、ティアリングは回避されます。データがクライアントに渡されるときに、ティアリングは発生しません。ただし、X11 (Linux/Unix グラフィックサブシステム) では、ティアリングを防ぐ一貫した方法で画面に描画することはできません。

スクリーンティアリングを防ぐには、Citrix ではアプリケーションの描画と画面の描画を同期化する標準的なアプローチをお勧めします。つまり、`vsvnc`による次のフレームの描画開始を待機します。クライアントのグラフィックハードウェアと使用しているウィンドウマネージャーに応じて、スクリーンティアリングを防ぐために次の 2 つのソリューショングループを利用できます：

- X11 GPU 設定
- コンポジションマネージャーを使用する

#### X11 GPU 構成

Intel HD グラフィックスについては、以下の内容で `xorg.conf.d` に

**20-intel.conf** というファイルを作成します：

```
1 Section "Device"
2
3 Identifier      "Intel Graphics"
4 Driver          "intel"
```

```
5 Option      "AccelMethod" "sna"  
6 Option      "TearFree" "true"  
7  
8 EndSection
```

NVIDIA グラフィックスについては、お使いの構成に対応する”MetaModes” オプションを含む、xorg.conf.d フォルダでファイルを見つけます。コンマ区切りの使用される MetaMode ごとに、以下を追加します：

```
{ForceFullCompositionPipeline = On}
```

例：

```
Option "MetaModes" "DFP-0: 1920x1200 +0+0 {ForceFullCompositionPipeline = On}"
```

注：

異なる Linux ディストリビューションは xorg.conf.d に対して異なるパスを使用します。たとえば、`/etc/X11/xorg.conf.d`、または、`/user/share/X11/xorg.conf.d`。

#### コンポジションマネージャー

以下を使用します：

- **Compiz** (Ubuntu Unity に組み込み)。CompizConfig Settings Manager をインストールします。CompizConfig Settings Manager を実行します。

**General>Composition** で **Undirect Fullscreen Windows** をクリアします。

注：

CompizConfig Settings Manager は注意して使用してください。誤って値を変更するとシステムが起動しなくなる可能性があります。

- **Compton** (アドオンユーティリティ)。詳しくは、Compton のメインページ/ドキュメントを参照してください。たとえば、次のコマンドを実行します：

```
compton --vsync opengl --vsync -aggressive
```

#### 不正なキーストローク

英語以外のキーボードを使用している場合、画面表示がキーボード入力と一致しないことがあります。この場合、使用しているキーボードの種類とレイアウトを指定する必要があります。キーボードの指定については、「[キーボードの構成](#)」を参照してください。

### 過剰な再描画

ウィンドウマネージャーの種類によっては、シームレスウィンドウを移動すると新しいウィンドウ位置が常にサーバーにレポートされるため、再描画が過度に発生することがあります。ウィンドウを移動したときにウィンドウ枠のみを描画するモードに切り替えると、この問題は解決します。

### アイコンの互換性

Citrix Workspace アプリは、ほとんどのウィンドウマネージャーと互換性のあるウィンドウアイコンを作成します。ただし、これらのアイコンは X Inter-Client Communication Convention と完全には互換性がありません。

### アイコンの完全な互換性

ICCCM に完全に準拠するには:

1. 構成ファイル `wfclient.ini` を開きます。
2. `[WFClient]` セクションで次のように行を編集します: `UseIconWindow=True`
3. ファイルを保存して閉じます。

### カーソルの色

カーソルの色が背景色と同じまたは似ている場合には、見分けるのが難しくなることがあります。この問題は、カーソルを黒または白にすることで解決できます。

カーソルの色を変更するには

1. 構成ファイル `wfclient.ini` を開きます。
2. 次のいずれかの行を `[WFClient]` セクションに追加します:  
`CursorStipple=ffff,ffff` (カーソルを黒で表示)  
`CursorStipple=0,0` (カーソルを白で表示)
3. ファイルを保存して閉じます。

### 色のちらつき

接続ウィンドウの内/外にマウスを移動させると、フォーカスのないウィンドウの色がちらつきます。これは、`PseudoColor` 表示で X Windows System を使用する場合の制限事項として知られています。可能な場合、問題のある接続ではより色数の多いウィンドウを使用してください。



## TrueColor 表示での色の変更

サーバーに接続するとき、ウィンドウの色数として 256 色を選択できます。256 色を選択する場合は、ビデオカードがパレットをサポートしていて、アプリケーションでパレットの色を変更し、アニメーション表示が可能であることが前提になります。

TrueColor 表示では、パレットを高速変更してアニメーションを生成する機能はエミュレートできません。ソフトウェアでのこの機能のエミュレーションは時間がかかり、多くのネットワークトラフィックが費やされます。この問題を解決するために、Citrix Workspace アプリは高速パレット変更をバッファに格納し、数秒ごとに実際のパレットを更新するように設定されています。

## 不正確な表示

Citrix Workspace アプリでは、日本語文字に EUC-JP または UTF-8 文字エンコードが使用されます。一方、サーバー側では Shift-JIS 文字エンコードが使用されます。Citrix Workspace アプリでは、これらの文字セット間でのエンコーディングが実行されません。この問題により、次の表示で問題が発生する可能性があります：

- サーバーに保存され、ローカルで表示されるファイル
- ローカルに保存され、サーバーで表示されるファイル

この問題は、拡張パラメーターパス機能で使用されるパラメーターの日本語でも発生します。

## セッションの表示モニター

全画面モードのセッションは、すべてのモニターの表示領域全体に表示されます。また、コマンドラインオプションとして `-span` を使用することもできます。これにより全画面セッションを追加モニターにまたがって表示できます。

Desktop Viewer ツールバーの機能によって、モニターを横断したマルチモニターのサポートなど、ウィンドウモードと全画面モードのセッションの切り替えることができます。

### 重要：

`-span` は、シームレスセッションや標準のウィンドウセッション（最大化されたウィンドウのセッションを含む）には適用されません。

`-span` オプションは、以下のように指定します：

```
-span [h][o][a|mon1[,mon2[,mon3, mon4]]]
```

`h` を指定すると、モニターの一覧が `stdout` に出力されます。`h` のみを指定した場合、`wfica` が終了します。

`o` を指定すると、セッションウィンドウの属性が `override-redirect` になります。

### 注意：

- このオプションの使用は推奨されません。これは、非協調性のウィンドウマネージャーで使用するための最後のオプションです。
- セッションウィンドウはウィンドウマネージャーで非表示となり、アイコンもなく、再スタックできません

ん。

- セッションを終了することによってのみウィンドウを削除できます。

`a`を指定すると、Citrix Workspace アプリはすべてのモニターを使用してセッションを表示します。

`-span` オプションの残りの値は、Citrix Workspace アプリではモニター番号の一覧として処理されます:

- 単一の値では特定のモニターを選択します。
- 2つの値は、表示領域の左上隅と右下隅にあるモニターを選択します。
- 4つの値は、この領域の上端、下端、左端、および右端のモニターを指定します。

`wfica` コマンドでは、(`o`を指定しない場合) `_NET_WM_FULLSCREEN_MONITORS` メッセージによりウィンドウマネージャーから適切なウィンドウレイアウトが取得されます (サポートされる場合)。それ以外の場合は、サイズおよび位置に関するヒントを使用して必要なレイアウトを要求します。

ウィンドウマネージャーがこのクライアントメッセージをサポートするかどうかを確認するには、次のコマンドを実行します:

```
xprop -root | grep \_NET\_WM\_FULLSCREEN\_MONITORS
```

出力がない場合、サポートされません。サポートされないウィンドウマネージャーでは、ウィンドウリダイレクトの上書き (`override-redirect`) が必要な場合があります。`-span o`を使って、`override-redirect` ウィンドウをセットアップできます。

コマンドラインからセッションを追加モニターにまたがって実行するには:

1. コマンドプロンプトで以下を入力します:

```
/opt/Citrix/ICAClient/wfica -span h
```

ユーザーデバイスに現在接続しているモニターの番号の一覧が `stdout` に出力され、`wfica` が終了します。

2. これらのモニターの番号をメモしておきます。

3. コマンドプロンプトで以下を入力します:

```
/opt/Citrix/ICAClient/wfica -span \[w\[,x\[,y,z\]\]\]
```

`w`、`x`、`y`、および `z` の値は、前の手順 1 のモニター番号です。単一の値 `w` は、特定のモニターを指定します。また、2つの値 `w` と `x` は、表示領域の左上隅と右下隅のモニターを指定します。4つの値 `w`、`x`、`y`、`z` は、領域の上端、下端、左端、および右端のモニターを指定します。

**重要:**

- ブラウザーで `self-service` を起動する前に、`WFICA_OPTS` 変数を定義します。この変数を定義するには、プロファイルファイル (通常は、`$HOME/.bash_profile` または `$HOME/.profile`) を編集して、`WFICA_OPTS` 変数を定義する行を追加します。例:

```
export WFICA_OPTS="--span a"
```

- この変更は、仮想アプリおよび仮想デスクトップの両方のセッションに影響を及ぼします。
- `self-service` または `storebrowse` を開始している場合は、新しい環境変数を適用するために開始

されたプロセスを削除します。次のコマンドで削除します：

```
killall AuthManagerDaemon ServiceRecord storebrowse
```

### ローカルアプリケーション

全画面セッションからローカルアプリケーションまたはほかのセッションに切り替えることができないことがあります。この問題は、クライアント側のシステム UI が非表示になっていて、キーボード透過機能が通常のキーボードコマンド (Alt+Tab など) を無効にし、代わりにサーバーにコマンドを送るために発生します。

この問題を回避するには、フォーカスがセッションウィンドウに移るまで Ctrl+F2 キーを押してキーボード透過機能を一時的にオフにします。また代替策として、\$ICAROOT/config/module.ini で TransparentKeyPassthrough を No に設定します。この回避策により、キーボード透過機能が無効になります。ただし、All\_regions.ini ファイルにこの設定を追加して **ICA** ファイルを上書きすることが必要な場合があります。

## Web カメラ

### デフォルトの Web カメラの更新

現在、Linux 向け Citrix Workspace アプリでの Web カメラリダイレクトは、一度に 1 つの Web カメラのみをサポートしています。選択されたデフォルトの Web カメラは、デバイスパス /dev/video0 にマップされます。これは、通常、ラップトップに組み込まれている Web カメラです。

システム内のビデオ機能を持つすべてのデバイスを一覧表示するには、次のコマンドを使用して v4l ツールをインストールする必要があります：

```
1 sudo apt-get install v4l-util
2 <!--NeedCopy-->
```

次のコマンドを使用して、ビデオデバイスを一覧表示します：

```
1 v4l2-ctl --list-devices
2 <!--NeedCopy-->
```

次のような出力が表示されます：

```
1 user@user-pc:~ $ v4l2-ctl --list-devices
2 UVC Camera (046d:09a6) (usb-0000:00:14.0-1):
3     /dev/video2
4     /dev/video3
5     /dev/media1
6 Integrated Camera: Integrated C (usb-0000:00:14.0-8):
7     /dev/video0
8     /dev/video1
9     /dev/media0
```

10 <!--NeedCopy-->

上記の例では、2つの Web カメラがあります。そのどちらでも使用できます。1つ目のインデックスを使用することを Citrix ではお勧めします。Ubuntu には既知の問題があり、1つの Web カメラに対して複数のインデックスが表示されることがあります。この例では、「/dev/video0」と「/dev/video2」を使用できます。

別のビデオの取り込みをデフォルトとして設定するには、次の手順を実行します：

1. 構成ファイル~/`.ICAClient/wfclient.ini`に移動して編集します。
2. [WFClient] セクションに、次の設定を追加します。

```
HDXWebCamDevice=<device path>
```

たとえば、`HDXWebCamDevice=/dev/video2` を追加すると、システムの `/dev/video2` にマップされた Web カメラが設定されます。

#### テスト機能

クライアントでは、Web カメラリダイレクトモジュールをさまざまなモードで使用して、顧客環境条件下で独立したコンポーネントをテストできます。

#### 実稼働モードとデバッグモード

このモードでは、VDA 側で表示されるビデオと、エンコーダーがクライアント側で生成する実際のバッファを比較します。パイプライン全体をテストできます。

このモードを有効にするには：

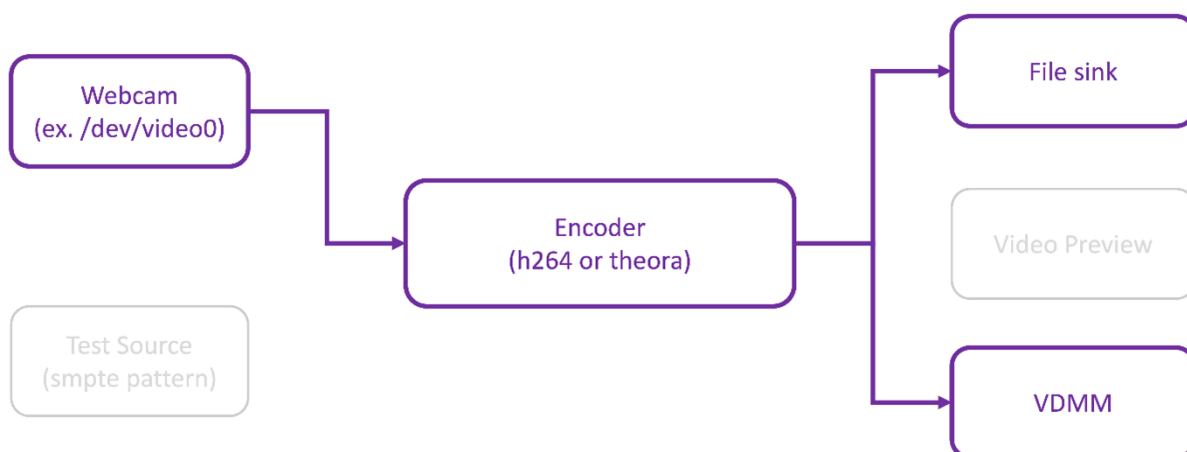
1. 構成ファイル~/`.ICAClient/wfclient.ini`に移動して編集します。
2. `HDXWebcamDebug`値を **True** に設定します。

```
HDXWebcamDebug = True
```

このモードを有効にすると、使用するエンコーダーごとにバッファを使用して次のファイルを生成します。

- H264 エンコーダーの場合：/tmp/file\_mode\_buffers.h264
- Theora エンコーダーの場合：/tmp/file\_mode\_buffers.theora

次の図は、実稼働モードとデバッグモードを示しています：



### Web カメラテスターモード

このモードでは、他のパイプライン要素から Web カメラを分離してテストできます。

```

1 ./gst_read --buffers | -b BUFFERS_AMOUNT [ --input_device | -i
  WEBCAM_DEVICE; default=/dev/video0]
2 <!--NeedCopy-->

```

Web カメラテスターモードを有効にするには、コマンドラインから次のコマンドを実行します：

```

1 cd /opt/Citrix/ICAClient/util
2 <!--NeedCopy-->

```

```

1 `$. ./gst_read -b 100 /dev/video0
2 <!--NeedCopy-->

```

このモードを有効にすると、ビデオプレビューが表示され、Web カメラからの raw バッファを使用して次のファイルが作成されます：

/tmp/wewbcam\_buffers.buf

Web カメラテスターモードに必要な唯一のスイッチは `--buffers` (`-b`) オプションです。テストする Web カメラデバイスを指定することもできます。たとえば、次を参照してください：

- `./gst_read -buffers 150`
- `./gst_read -buffers 100 -input_device /dev/video2`

次の図は、Web カメラテスターモードを示しています：



## エンコーダーテスターモード

このモードでは、パイプラインからエンコーダーを分離してテストできます。

```

1 ./gst_read --output_file | -o FILE_NAME [ --buffers | -b BUFFER_AMOUNT;
   default=10 0 ] [ --enableH264 | -e ]
2 <!--NeedCopy-->
  
```

エンコーダーテスターモードを有効にするには、コマンドラインから次のコマンドを実行します：

```

1 cd /opt/Citrix/ICAClient/util
2 <!--NeedCopy-->
  
```

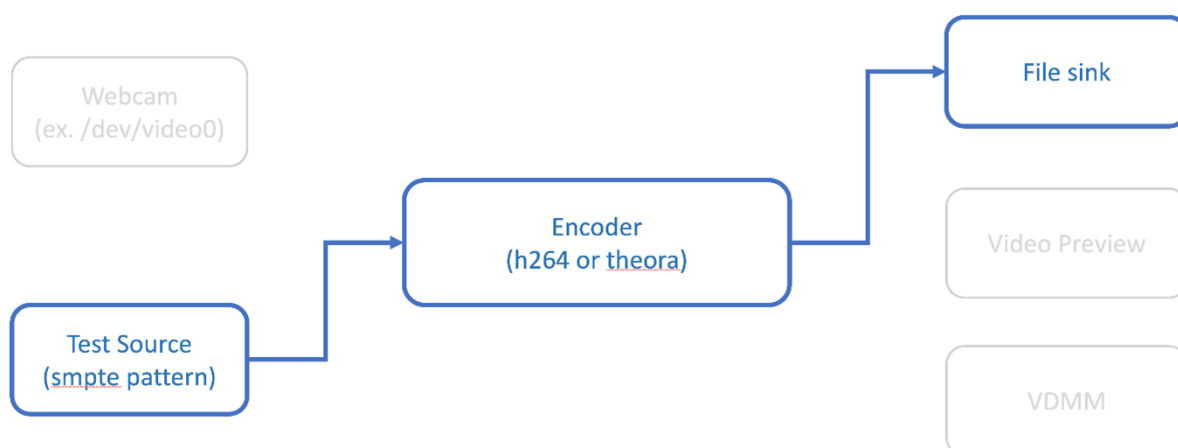
```

1 ./gst_read -o ~/file_buffers.h264 -e
2 <!--NeedCopy-->
  
```

このモードに必要な唯一のスイッチは `--output_file` (`-o`) オプションです。Theora または H264 エンコーダーと生成するバッファの量をテストすることもできます。たとえば、次を参照してください：

- H264 の場合： `./gst_read -output_file ~/file_buffers.h264 -buffers 200 -enableH264`
- Theora の場合： `./gst_read -o ~/file_buffers.theora -b 100`

次の図は、エンコーダーテスターモードを示しています：



## H264 ソフトウェアエンコーダー

ソフトウェアベースの H264 エンコーダーが正しく機能しない場合は、次の手順を使用して依存関係を確認する必要があります：

1. x264 GStreamer プラグインが `gststreamer-plugins-ugly` の一部としてシステムにあるかどうかを確認します。 `libgstx264.so` ライブラリで使用できる場合は、次のコマンドを実行して確認します：

```
1 gst-inspect-1.0 x264
2 <!--NeedCopy-->
```

```
.....:/opt/Citrix/ICAClient$ gst-inspect-1.0 x264
Plugin Details:
Name                x264
Description          libx264-based H264 plugins
Filename             /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
Version              1.14.5
License              GPL
Source module        gst-plugins-ugly
Source release date  2019-05-29
Binary package       GStreamer Ugly Plugins (Ubuntu)
Origin URL           https://launchpad.net/distros/ubuntu/+source/gst-plugins-ugly1.0

x264enc: x264enc

1 features:
+-- 1 elements
```

2. 次のコマンドを実行して、 `libgstx264.so` ライブラリの依存関係を確認します：

```
1 ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
2 <!--NeedCopy-->
```

```

/opt/Citrix/ICAClient$ ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstx264.so
linux-vdso.so.1 (0x00007ffc723c5000)
/usr/local/lib/AppProtection/libAppProtection.so (0x00007fde6482f000)
libgstvideo-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0 (0x00007fde64596000)
libgstpbutils-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstpbutils-1.0.so.0 (0x00007fde6425e000)
libgstreamer-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstreamer-1.0.so.0 (0x00007fde64023000)
libgobject-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0 (0x00007fde63dcf000)
libx264.so.152 => /usr/lib/x86_64-linux-gnu/libx264.so.152 (0x00007fde63a2a000)
libgmodule-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgmodule-2.0.so.0 (0x00007fde63826000)
libglib-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0 (0x00007fde6350f000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007fde6311e000)
libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007fde62eff000)
libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007fde62cfb000)
libX11.so.6 => /usr/lib/x86_64-linux-gnu/libX11.so.6 (0x00007fde629c3000)
libxcb.so.1 => /usr/lib/x86_64-linux-gnu/libxcb.so.1 (0x00007fde6279b000)
libstdc++.so.6 => /usr/lib/x86_64-linux-gnu/libstdc++.so.6 (0x00007fde62412000)
libXi.so.6 => /usr/lib/x86_64-linux-gnu/libXi.so.6 (0x00007fde62202000)
libgstbase-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstbase-1.0.so.0 (0x00007fde61f8d000)
liborc-0.4.so.0 => /usr/lib/x86_64-linux-gnu/liborc-0.4.so.0 (0x00007fde61d11000)
libm.so.6 => /lib/x86_64-linux-gnu/libm.so.6 (0x00007fde61973000)
libgstaudio-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstaudio-1.0.so.0 (0x00007fde616fe000)
libgstag-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstag-1.0.so.0 (0x00007fde614c3000)
librt.so.1 => /lib/x86_64-linux-gnu/librt.so.1 (0x00007fde612bb000)
libffi.so.6 => /usr/lib/x86_64-linux-gnu/libffi.so.6 (0x00007fde610b3000)
libpcre.so.3 => /lib/x86_64-linux-gnu/libpcre.so.3 (0x00007fde60e41000)
/lib64/ld-linux-x86-64.so.2 (0x00007fde64c64000)
libXau.so.6 => /usr/lib/x86_64-linux-gnu/libXau.so.6 (0x00007fde60c3d000)
libXdmp.so.6 => /usr/lib/x86_64-linux-gnu/libXdmp.so.6 (0x00007fde60a37000)
libgcc_s.so.1 => /lib/x86_64-linux-gnu/libgcc_s.so.1 (0x00007fde6081f000)
libXext.so.6 => /usr/lib/x86_64-linux-gnu/libXext.so.6 (0x00007fde6060d000)
libz.so.1 => /lib/x86_64-linux-gnu/libz.so.1 (0x00007fde603f0000)
libbsd.so.0 => /lib/x86_64-linux-gnu/libbsd.so.0 (0x00007fde601db000)

```

libgstx264.soファイルが存在しない場合は、次のコマンドを使用してGStreamerプラグイン (ugly) をインストールする必要があります:

- 1 sudo apt-get install gstreamer1
- 2 0-plugins-ugly
- 3 <!--NeedCopy-->

## H264 ハードウェアエンコーダー

1. vaapi GStreamerプラグインがgstreamer1.0-vaapiの一部としてシステムにあるかどうかを確認します。libgstvaapi.soライブラリで使用できる場合は、次のコマンドを実行して確認します:

- 1 gst-inspect-1.0 vaapi
- 2 <!--NeedCopy-->

```

/opt/Citrix/ICAClient$ gst-inspect-1.0 vaapi
Plugin Details:
Name: vaapi
Description: VA-API based elements
Filename: /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
Version: 1.14.5
License: LGPL
Source module: gstreamer-vaapi
Source release date: 2019-05-29
Binary package: gstreamer-vaapi
Origin URL: http://bugzilla.gnome.org/enter_bug.cgi?product=GStreamer

0 features:

```

2. 次のコマンドを実行して、libgstvaapi.so ライブラリの依存関係を確認します:

- 1 ldd /usr/lib/x86\_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
- 2 <!--NeedCopy-->



```

/opt/Citrix/ICAClient$ ldd /usr/lib/x86_64-linux-gnu/gstreamer-1.0/libgstvaapi.so
linux-vdso.so.1 (0x00007ffd635fe000)
/usr/local/lib/AppProtection/libAppProtection.so (0x00007f5eb1d5e000)
libgstcodecparsers-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstcodecparsers-1.0.so.0 (0x00007f5eb1b000)
libdrm.so.2 => /usr/lib/x86_64-linux-gnu/libdrm.so.2 (0x00007f5eb190a000)
libudev.so.1 => /lib/x86_64-linux-gnu/libudev.so.1 (0x00007f5eb16ec000)
libva-drm.so.2 => /usr/lib/x86_64-linux-gnu/libva-drm.so.2 (0x00007f5eb14e9000)
libXrandr.so.2 => /usr/lib/x86_64-linux-gnu/libXrandr.so.2 (0x00007f5eb12de000)
libXrender.so.1 => /usr/lib/x86_64-linux-gnu/libXrender.so.1 (0x00007f5eb10d4000)
libX11.so.6 => /usr/lib/x86_64-linux-gnu/libX11.so.6 (0x00007f5eb0d9c000)
libGL.so.1 => /usr/lib/x86_64-linux-gnu/libGL.so.1 (0x00007f5eb0b10000)
libva-x11.so.2 => /usr/lib/x86_64-linux-gnu/libva-x11.so.2 (0x00007f5eb090a000)
libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007f5eb0706000)
libEGL.so.1 => /usr/lib/x86_64-linux-gnu/libEGL.so.1 (0x00007f5eb04f2000)
libgmodule-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgmodule-2.0.so.0 (0x00007f5eb02ee000)
libva-wayland.so.2 => /usr/lib/x86_64-linux-gnu/libva-wayland.so.2 (0x00007f5eb00e9000)
libva.so.2 => /usr/lib/x86_64-linux-gnu/libva.so.2 (0x00007f5eafec8000)
libwayland-client.so.0 => /usr/lib/x86_64-linux-gnu/libwayland-client.so.0 (0x00007f5eafcb9000)
libgstgl-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstgl-1.0.so.0 (0x00007f5eafa53000)
libgstpbutils-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstpbutils-1.0.so.0 (0x00007f5eaf81b000)
libgstvideo-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstvideo-1.0.so.0 (0x00007f5eaf582000)
libgstbase-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstbase-1.0.so.0 (0x00007f5eaf30d000)
libgstallocators-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstallocators-1.0.so.0 (0x00007f5eaf109000)
libgstreamer-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstreamer-1.0.so.0 (0x00007f5eae9dce000)
libgobject-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0 (0x00007f5eae7a0000)
libglib-2.0.so.0 => /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0 (0x00007f5eae630000)
libm.so.6 => /lib/x86_64-linux-gnu/libm.so.6 (0x00007f5eae4c5000)
libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007f5eae2a6000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f5eadeb5000)
libxcb.so.1 => /usr/lib/x86_64-linux-gnu/libxcb.so.1 (0x00007f5eadc8d000)
libstdc++.so.6 => /usr/lib/x86_64-linux-gnu/libstdc++.so.6 (0x00007f5ead904000)
libXt.so.6 => /usr/lib/x86_64-linux-gnu/libXt.so.6 (0x00007f5ead6f4000)
librt.so.1 => /lib/x86_64-linux-gnu/librt.so.1 (0x00007f5ead4ec000)
/lib64/ld-linux-x86-64.so.2 (0x00007f5eb2261000)
libXext.so.6 => /usr/lib/x86_64-linux-gnu/libXext.so.6 (0x00007f5ead2da000)
libGLX.so.0 => /usr/lib/x86_64-linux-gnu/libGLX.so.0 (0x00007f5ead0a9000)
libGLdispatch.so.0 => /usr/lib/x86_64-linux-gnu/libGLdispatch.so.0 (0x00007f5eacdf3000)
libXfixes.so.3 => /usr/lib/x86_64-linux-gnu/libXfixes.so.3 (0x00007f5eacbed000)
libffi.so.6 => /usr/lib/x86_64-linux-gnu/libffi.so.6 (0x00007f5eac9e5000)
libX11-xcb.so.1 => /usr/lib/x86_64-linux-gnu/libX11-xcb.so.1 (0x00007f5eac7e3000)
libwayland-egl.so.1 => /usr/lib/x86_64-linux-gnu/libwayland-egl.so.1 (0x00007f5eac5e1000)
libgbm.so.1 => /usr/lib/x86_64-linux-gnu/libgbm.so.1 (0x00007f5eac3d2000)
libgudev-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgudev-1.0.so.0 (0x00007f5eac1c8000)
libgstreamer-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgstreamer-1.0.so.0 (0x00007f5eabf53000)
libgsttag-1.0.so.0 => /usr/lib/x86_64-linux-gnu/libgsttag-1.0.so.0 (0x00007f5eabd18000)
liborc-0.4.so.0 => /usr/lib/x86_64-linux-gnu/liborc-0.4.so.0 (0x00007f5eaba9c000)
libpcre.so.3 => /lib/x86_64-linux-gnu/libpcre.so.3 (0x00007f5eab82a000)
libXau.so.6 => /usr/lib/x86_64-linux-gnu/libXau.so.6 (0x00007f5eab626000)
libXdmp.so.6 => /usr/lib/x86_64-linux-gnu/libXdmp.so.6 (0x00007f5eab420000)
libgcc_s.so.1 => /lib/x86_64-linux-gnu/libgcc_s.so.1 (0x00007f5eab208000)
libwayland-server.so.0 => /usr/lib/x86_64-linux-gnu/libwayland-server.so.0 (0x00007f5eaff5000)
libexpat.so.1 => /lib/x86_64-linux-gnu/libexpat.so.1 (0x00007f5eaaadc3000)
libz.so.1 => /lib/x86_64-linux-gnu/libz.so.1 (0x00007f5eaaaba6000)
libbsd.so.0 => /lib/x86_64-linux-gnu/libbsd.so.0 (0x00007f5eaa991000)

```

3. 不足している依存関係を解決します。

vaapiをインストールして構成するには、GStreamer vappiインストールガイドに従ってください。

内部 **GStreamer** フレームワークと **gst\_read** ログの収集

通常のICAClientログの代わりに、gst\_readモジュールからログを収集する必要があります。

ログを収集するには、次の手順を実行します：

1. ターミナルを開き、次のコマンドを実行します：

```

1 export GST_DEBUG=2, gst_read_debug:6
2 <!--NeedCopy-->

```

```

1 export GST_DEBUG_FILE=~/.gst_read.log
2 <!--NeedCopy-->

```

注:

この変数は、ログのレベルとそれらを保存するファイルを設定します。この場合、GStreamerフレームワークにレベル 2 を設定し、gst\_read モジュールにレベル 7 を設定しています。詳しくは、[ドキュメント](#)を参照してください。内部GStreamerフレームワークおよびgst\_readのログレベルでエラーレベルと警告レベルのみを設定することをお勧めします。

2. 有効な VDA の ICA ファイルをダウンロードします。
3. 同じターミナルで、次のコマンドを実行して VDA セッションを開始します。

```
1 cd /opt/Citrix/ICAClient
2 <!--NeedCopy-->
```

```
1 ./wfica <ICA file path>/vda.ica
2 <!--NeedCopy-->
```

gst\_read.log ファイルは、内部GStreamerフレームワークとgst\_readログを使用して生成されます。

## GStreamer パイプライン検査

GStreamer フレームワークが作成している実際のパイプラインを確認するには、次の手順を実行します:

1. dot ファイルを保存するフォルダーを作成します (例: gstIntPipes)。
2. ターミナルを開き、GST\_DEBUG\_DUMP\_DOT\_DIR=<Absolute path>/gstIntPipes をエクスポートします。この変数は、dot ファイルを保存する場所をGStreamerに示します。
3. 有効な VDA の ICA ファイルをダウンロードします。
4. 同じターミナルで、次のコマンドを実行して VDA セッションを開始します:

```
1 cd /opt/Citrix/ICAClient/
2 <!--NeedCopy-->
```

```
1 ./wfica <ICA file path>/vda.ica
2 <!--NeedCopy-->
```

5. ディレクトリgstIntPipesには dot ファイルが含まれています。GStreamerは、パイプラインの状態が変化することに dot ファイルを生成します。その結果、パイプライン作成のすべてのプロセスを検査できます。以下は、dot ファイルのセットの例です。

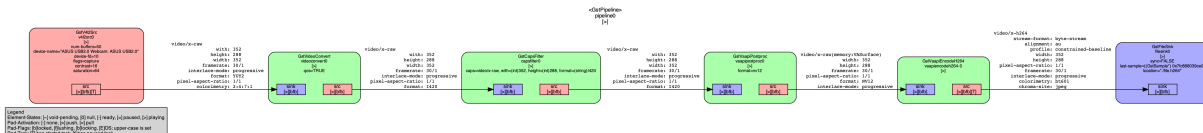
```

0.000000 336544413-gst_read_NULL_READY.dot 0.000000 378956105-gst_read_NULL_READY.dot 0.000000 583790518-gst_read_PAUSED_PLAYING.dot
0.000000 336544447-gst_read_NULL_READY.dot 0.000000 378956972-gst_read_NULL_READY.dot 0.000000 587545446-gst_read_PAUSED_PLAYING.dot
0.000000 344272726-gst_read_NULL_READY.dot 0.000000 381124838-gst_read_READY_PAUSED.dot 0.000000 685438888-gst_read_PAUSED_PLAYING.dot
0.000000 347927487-gst_read_NULL_READY.dot 0.000000 385383422-gst_read_READY_PAUSED.dot 0.000000 624393998-gst_read_PAUSED_PLAYING.dot
0.000000 368336488-gst_read_NULL_READY.dot 0.000000 424472654-gst_read_READY_PAUSED.dot 0.000000 658595228-gst_read_PAUSED_PLAYING.dot
0.000000 361899797-gst_read_NULL_READY.dot 0.000000 457465732-gst_read_READY_PAUSED.dot 0.000000 602781899-gst_read_PAUSED_PLAYING.dot
0.000000 363292312-gst_read_NULL_READY.dot 0.000000 471523885-gst_read_READY_PAUSED.dot 0.000000 665778884-gst_read_PAUSED_PLAYING.dot
0.000000 364805184-gst_read_NULL_READY.dot 0.000000 472899531-gst_read_READY_PAUSED.dot 0.000000 602316179-gst_read_PAUSED_PLAYING.dot
0.000000 365886731-gst_read_NULL_READY.dot 0.000000 478452388-gst_read_READY_PAUSED.dot 0.000000 672898814-gst_read_PAUSED_PLAYING.dot
0.000000 367843429-gst_read_NULL_READY.dot 0.000000 481289294-gst_read_READY_PAUSED.dot 0.000000 617414148-gst_read_PAUSED_PLAYING.dot
0.000000 368188649-gst_read_NULL_READY.dot 0.000000 483844671-gst_read_READY_PAUSED.dot 0.000000 608444153-gst_read_PAUSED_PLAYING.dot
0.000000 368345744-gst_read_NULL_READY.dot 0.000000 485177124-gst_read_READY_PAUSED.dot 0.000000 683898874-gst_read_PAUSED_PLAYING.dot
0.000000 378767591-gst_read_NULL_READY.dot 0.000000 492764612-gst_read_NULL_READY.dot 0.000000 686483326-gst_read_PAUSED_PLAYING.dot
0.000000 371911488-gst_read_NULL_READY.dot 0.000000 521888851-gst_read_READY_PAUSED.dot 0.000000 688238168-gst_read_PAUSED_PLAYING.dot
0.000000 372083836-gst_read_NULL_READY.dot 0.000000 565325791-gst_read_READY_PAUSED.dot 0.000000 641923719-gst_read_PAUSED_PLAYING.dot
0.000000 374383375-gst_read_NULL_READY.dot 0.000000 569828528-gst_read_READY_PAUSED.dot 0.000000 725784419-gst_read_READY_PAUSED.dot
0.000000 375518168-gst_read_NULL_READY.dot 0.000000 572117882-gst_read_READY_PAUSED.dot 0.000000 765829255-gst_read_PAUSED_PLAYING.dot
0.000000 376542299-gst_read_NULL_READY.dot 0.000000 576843667-gst_read_READY_PAUSED.dot 0.000000 776336614-gst_read_PAUSED_PLAYING.dot
0.000000 377604672-gst_read_NULL_READY.dot 0.000000 577692784-gst_read_READY_PAUSED.dot

```

6. パイプラインを視覚的に確認するには、dot ファイルユーティリティをインストールします。たとえば、[Graphviz](#)などです。次の画像は、パイプラインの作成の良い例と悪い例です：

正常に作成されたパイプライン：



リンクできないパイプライン：



注：

前の画像またはその他の画像を拡大するには、画像を右クリックして [画像を新しいタブで開く] を選択し、必要に応じてブラウザで拡大してください。

上の画像に示されているように、2 番目のパイプラインでは `GstCapsFilter` 要素と `GstVaapiEncodeH264` 要素をリンクできません。機能が完全にネゴシエートされることはありません。詳しくは、[ドキュメント](#)を参照してください。

### RAVE 用システム診断スクリプト

システム構成と依存関係が Remote Audio Video Extensions (RAVE) をサポートするのに適しているかどうかを確認するスクリプト `rave_troubleshooting.sh` が用意されています。

注：

RAVE は、Citrix VDA 向けに最適化された Web カメラリダイレクトと Windows Media Player リダイレクトをサポートする HDX 機能です。

スクリプトを実行するには、次の手順を実行します：

1. `rave_troubleshooting.sh` をクリックして、スクリプトをダウンロードします。
2. Linux マシンでターミナルを開きます。
3. `rave_troubleshooting.sh --help` または `rave_troubleshooting.sh -h` と入力して、サポートされているコマンドライン引数を表示します。
4. 次のいずれかを入力します：
  - `rave_troubleshooting.sh -w` または `rave_troubleshooting.sh --webcam` - このコマンドを使用して、Web カメラのリダイレクトのチェックを実行します。これはデフォルトのコマンドです。

- `rave_troubleshooting.sh -r`または`rave_troubleshooting.sh --rave`-このコマンドを使用して、RAVE のチェックを実行します。h264 テストビデオを再生するポップアップウィンドウが開きます。

システム構成と依存関係が表示されます。

### ブラウザ

#### ローカルブラウザ

Windows セッション内のリンクをクリックすると、コンテンツがクライアントコンピューターの Web ブラウザーで表示されます。サーバーからクライアントへのコンテンツリダイレクトは、`wfclient.ini` で有効になっています。このリダイレクトによって、ローカルのアプリケーションが実行されます。サーバーからクライアントへのコンテンツリダイレクト機能を無効にするは、「[サーバーからクライアントへのコンテンツリダイレクト](#)」を参照してください。

#### 公開リソースへのアクセス

公開リソースにアクセスする場合、Web ブラウザーにファイルの保存ダイアログボックスが表示されます。Firefox や Chrome 以外の Web ブラウザーでは、公開リソースに接続するための設定が必要な場合があります。公開されているリソースの一覧からアイコンをクリックしてリソースにアクセスしようとする、ICA ファイルの保存を確認するメッセージが表示されることがあります。

#### 特定のブラウザ

特定の Web ブラウザーで問題が生じる場合、`setupwfc`を実行する前に環境変数 `BROWSER` を設定して必要な Web ブラウザーのローカルパスや名前を指定してください。

### Firefox ブラウザー

Firefox でデスクトップまたはアプリケーションを起動するときにページが応答しない場合は、ICA プラグインを有効にすることを検討してください。

#### Firefox の ICA プラグイン

Firefox で ICA プラグインが有効になっている場合、デスクトップおよびアプリケーションセッションが開始されないことがあります。この場合、ICA プラグインを無効にしてください。

#### 構成エラー

このエラーは、接続エントリが適切に構成されていない場合に発生します。

**E\_MISSING\_INI\_SECTION** - 構成ファイルを検証してください: ”...” 構成ファイルでセクション”...”が見つかりません。

構成ファイルが直接編集されたか、壊れています。

**E\_MISSING\_INI\_ENTRY** - 構成ファイルを検証してください: ”...” セクション”...”にはエントリ”...”が含まれている必要があります。

構成ファイルが直接編集されたか、壊れています。

**E\_INI\_VENDOR\_RANGE** - 構成ファイルを検証してください: ”...” 構成ファイルの **X** サーバーベンダーの範囲”...”が無効です。

構成ファイル内の X サーバーのベンダー情報が壊れています。Citrix に連絡してください。

### **wfclient.ini** 構成エラー

これらのエラーは、wfclient.ini の構成が正しくない場合に発生します。

**E\_CANNOT\_WRITE\_FILE** - ファイルを書き込めません: ”...”

接続データベースに保存するときに、空きディスク容量が不足するなどのエラーが発生しました。

**E\_CANNOT\_CREATE\_FILE** - ファイルを作成できません: ”...”

接続データベースの作成時にエラーが発生しました。

**E\_PNAGENT\_FILE\_UNREADABLE - Citrix Virtual Apps** ファイル”...”を読み取れません: そのようなファイルまたはディレクトリはありません。

— または —

**Citrix Virtual Apps** ファイル”...”を読み取れません: アクセスは拒否されました。

デスクトップアイテムまたはメニューからリソースにアクセスしようとしていますが、そのリソースの Citrix Virtual Apps and Desktops または Citrix DaaS ファイルを使用できません。[ビュー] メニューの [アプリケーションの更新] を選択して公開リソースの一覧を更新し、もう一度リソースにアクセスしてみてください。問題が解決されない場合:

- デスクトップアイコンまたはメニューのプロパティを確認します。
- アイコンまたはメニューが参照している Citrix Virtual Apps and Desktops または Citrix DaaS ファイルを確認します。

その他

接続の問題

また、次の問題が発生する可能性があります。

### セッションを閉じる

サーバーが Citrix Workspace アプリにセッションを閉じる指示をしたかどうかを確認するには、*wfica* プログラムを使用します。このプログラムは、セッションを中断するコマンドをサーバーからいつ受信したのか、ログを記録します。

Syslog システムを介してこの情報を記録するには、値を 6 に設定した *SyslogThreshold* を構成ファイルの [WFClient] セクションに追加します。この設定により、LOG\_INFO 以上の優先度のメッセージのログが記録されます。*SyslogThreshold* のデフォルト値は 4 (LOG\_WARNING) です。

同様に、*wfica* が情報を標準のエラーに送信するようにするには、値を 6 に設定した *PrintLogThreshold* を [WFClient] セクションに追加します。*PrintLogThreshold* のデフォルト値は 0 (LOG\_EMERG) です。

ログについて詳しくは、「[ログ](#)」、syslog の構成について詳しくは、「[syslog 構成](#)」を参照してください。

### 構成ファイルの設定

設定を適用するには、*wfclient.ini* の各エントリに対応するエントリが *All\_Regions.ini* 内に存在している必要があります。また、*wfclient.ini* の [Thinwire3.0]、[ClientDrive]、および [TCP/IP] セクションについて、実行する設定に対して *canonicalization.ini* 内に対応するエントリが必要です。詳しくは、*\$ICAROOT/config* ディレクトリ内の *All\_Regions.ini* および *canonicalization.ini* ファイルを参照してください。

### 公開アプリケーション

シリアルポートにアクセスする公開アプリケーションの実行で問題が発生した場合、ポートがほかのアプリケーションによりロックされていると元のアプリケーションを実行できないことがあります（エラーメッセージの表示または非表示はアプリケーションにより異なる）。このような環境では、シリアルポートを一時的にロックしたり、シリアルポートをロックしたまま解除せずに終了したりしているアプリケーションがないかをチェックします。

この問題を解決するには、シリアルポートをブロックしているアプリケーションを停止します。UUCP スタイルのロックの場合は、アプリケーションが終了した後にロックファイルが残っている可能性があります。このロックファイルの場所は、使用しているオペレーティングシステムにより異なります。

### Citrix Workspace アプリの起動

Citrix Workspace アプリを起動できず、「Application default file could not be found or is out of date」というメッセージが表示される場合は、環境変数 *ICAROOT* が正しく定義されていない可能性があります。デフォルト以外の場所に Citrix Workspace アプリをインストールした場合は、環境変数 *ICAROOT* を定義する必要があります。この問題を解決するには、次のいずれかを実行することを Citrix ではお勧めします。

- *ICAROOT* をインストールディレクトリとして定義する。

*ICAROOT* 環境変数が正しく定義されているかをチェックするには、Citrix Workspace アプリをターミナルセッションから起動します。エラーメッセージが表示される場合は、*ICAROOT* 環境変数が正しく定義されていません。

- Citrix Workspace アプリをデフォルトの場所に再インストールします。Citrix Workspace アプリのインストール方法については、「[インストールとセットアップ](#)」を参照してください。

以前デフォルトの場所に Citrix Workspace アプリをインストールしていた場合は、再インストールする前に `/opt/Citrix/ICAClient` または `$HOME/ICAClient/platform` ディレクトリを削除する必要があります。

### Citrix CryptoKit (SSLSDK の新名称)

実行中の Citrix CryptoKit (SSLSDK の新名称) または OpenSSL のバージョン番号を確認するには、次のコマンドを使用できます：

```
strings libctxssl.so | grep "Citrix SSLSDK"
```

また、AuthManagerDaemon または PrimaryAuthManager 上でもこのコマンドを実行できます。

### キーボードショートカット

ウィンドウマネージャーで同じキーボードショートカットが定義されている場合、セッションでのキーボードショートカットが正しく機能しない場合があります。たとえば、KDE ウィンドウマネージャーでデスクトップ 13~16 に切り替えるためのキーの組み合わせである、`Ctrl+Shift+F1~F4` キーがこれに該当します。この問題を解決するには、以下の方法を使用します：

- ローカルのキーの組み合わせをサーバー側のキーの組み合わせにマップするトランスレートモードを使用します。たとえば、デフォルトのトランスレートモードでは、`Ctrl+Shift+F1` がサーバー側の `Alt+F1` にマップされています。これを変更してほかのローカルキーの組み合わせを使用するには、`$HOME/.ICAClient/wfclient.ini` の `[WFClient]` セクションを編集します。たとえば、次の変更によりローカルの `Alt+Ctrl+F1` がサーバー側の `Alt+F1` にマップされます。
  - `Hotkey1Shift=Ctrl+Shift` を `Hotkey1Shift=Alt+Ctrl` に変更する。
- キーの組み合わせをすべてサーバー側に直接送信するダイレクトモードを使用します。この場合、キーの組み合わせはローカルでは処理されません。ダイレクトモードを構成するには、`$HOME/.ICAClient/wfclient.ini` の `[WFClient]` セクションで、`TransparentKeyPassthrough` を `Remote` に設定します。
- ウィンドウマネージャー側のキーボードショートカットを再構成して競合を解消します。

### リモートでのクローチア語のキーボード

クローチア語キーボードレイアウトでリモートの仮想デスクトップに ASCII 文字が正しく送信されるようにするには、以下の手順に従います。

1. 適切な構成ファイルを開き、`[WFClient]` セクションの `UseEUKSforASCII` で `True` を指定します。
2. `UseEUKS` で `2` を指定します。

#### 日本語キーボード

日本語キーボードの使用を構成するには、wfclient.ini 構成ファイルで次のエントリを更新します。

KeyboardLayout=Japanese (JIS)

#### ABNT2 キーボード

ABNT2 キーボードの使用を構成するには、wfclient.ini 構成ファイルで次のエントリを更新します。

KeyboardLayout=Brazilian (ABNT2)

#### ローカルキーボード

ローカルキーボードの一部のキーが正常に機能しない場合、\$ICAROOT/config/module.ini の一覧で最適なサーバーレイアウトを選択します。

### Windows Media Player

要求されたフォーマットを処理するための GStreamer プラグインが Citrix Workspace アプリにないことがあります。通常この問題によって、サーバーに別のフォーマットが要求されます。まれに、適正プラグインの初期チェックにおいて間違っ必要プラグインが存在すると表示されることがあります。通常、この問題は検出され、ファイルの再生中 Windows Media Player で問題が起こったことを示すエラーダイアログがサーバーに表示されます。Citrix Workspace アプリによってフォーマットが拒否されることが原因であるため、通常はセッション内でファイルを再試行すると機能します。その結果、サーバーは別のフォーマットを要求するか、メディア自体を提供します。

まれに、進行状況インジケーターが Windows Media Player で正常に動作しているにもかかわらず、適正なプラグインが検出されずにファイルが正常に再生されないことがあります。

以降のセッションで、このエラーダイアログや再生の失敗を避けるには：

1. たとえば、構成オプション”SpeedScreenMMAVerbose=On”を \$Home/.ICAClient/wfclient.ini の [WF-Client] セクションに一時的に追加します。
2. ターミナルから開始されたセルフサービスの wfica を再開します。
3. このエラーを生成するビデオを再生します。
4. 見つからないプラグイントレースに関連付けられた MIME の種類、またはサポート対象であるが再生されない MIME の種類 (“video/x-h264.” など) を (トレースアウトプットなどに) メモします。
5. \$ICAROOT/config/MediaStreamingConfig.tbl を編集します。メモした MIME の種類がある行で、「:」とその MIME の種類の間「?」を挿入します。この設定によりフォーマットが無効となります。
6. このエラー状態の原因となるそのほかのメディアフォーマットに対して、(上記の) 手順 2~5 を繰り返します。
7. GStreamer プラグインのほかのセットがあるそのほかのマシンに、この変更した MediaStreamingConfig.tbl を配信します。



注:

または、MIME の種類を識別した後、それをデコードするために GStreamer プラグインをインストールすることができます。

### Windows Media Player リダイレクトのシステム要件を検証するスクリプト

2307 リリースでは、Linux 向け Citrix Workspace アプリの Windows Media Player リダイレクト機能に必要な構成を検証するための新しい bash スクリプトが導入されました。この機能は、Windows Media Player リダイレクト機能のトラブルシューティングの時間を短縮するのに役立ちます。構成を検証するには、次の場所から入手できる同じ `rave_troubleshooting.sh` を使用できます。[RAVE 用システム診断スクリプト]/ja-jp/citrix-workspace-app-for-linux/troubleshooting.html#system-diagnostic-script-for-rave)。

#### シリアルポート設定

単一のシリアルポートを構成するには、`$ICAROOT/config/module.ini` 構成ファイルに次のエントリを追加します:

```
LastComPortNum=1
```

```
ComPort1=device
```

複数のシリアルポートを構成するには、`$ICAROOT/config/module.ini` 構成ファイルに次のエントリを追加します:

```
LastComPortNum=2
```

```
ComPort1=device1
```

```
ComPort2=device2
```

#### エラー

ここでは、Citrix Workspace アプリの使用中に発生する可能性がある一般的なエラーを示します。

エラーが発生しました。エラーコードは **11 (E\_MISSING\_INI\_SECTION)** です。ドキュメントを参照してください。終了しています。

Citrix Workspace アプリをコマンドラインから実行するときにこのメッセージが表示される場合は、通常コマンドラインに指定した名前が `appsrv.ini` がないことを意味します。

**E\_BAD\_OPTION - オプション”...”は無効です。**

オプション「...」の引数が指定されていません。

**E\_BAD\_ARG - オプション”...”に無効な引数があります: ”...”。**

オプション「...」に無効な引数が指定されています。

**E\_INI\_KEY\_SYNTAX** - 構成ファイル”...“のキー”...“が無効です。

構成ファイル内の X サーバーのベンダー情報が壊れています。構成ファイルを作成してください。

**E\_INI\_VALUE\_SYNTAX** - 構成ファイル”...“の値”...“が無効です。

構成ファイル内の X サーバーのベンダー情報が壊れています。構成ファイルを作成してください。

**E\_SERVER\_NAMELOOKUP\_FAILURE** - サーバー”...“に接続できません。

サーバー名を解決できません。

**1** つまたは複数のファイルに書き込めません: ”...“。ディスクの空き容量の問題または権限の問題を解決して、もう一度実行してください。

ディスクの空き容量または権限をチェックします。問題が見つかった場合は、これを修正し、エラーのあった操作をもう一度試してください。

サーバー接続がなくなりました。再接続してもう一度実行します。これらのファイルにはデータがない可能性があります: ”...“。

再接続し、エラーのあった操作をもう一度試してください。

## 診断情報

Citrix Workspace アプリの実行時に問題が発生した場合、Citrix テクニカルサポートに診断情報の提出を求められる場合があります。この情報は、Citrix テクニカルサポートで問題を調査して修正する目的で使用されます。

Citrix Workspace アプリに関する診断情報を取得するには:

1. インストール先のディレクトリで、util/lurdump を実行します。セッションが開かれていて、可能なら問題が発生している間にこの修正を実行することをお勧めします。

Citrix Workspace アプリのバージョン、構成ファイルの内容、およびさまざまなシステム変数値などの詳細な診断情報を提供するファイルが作成されます。

2. テクニカルサポートにこのファイルを送信する前に、ファイルに機密情報が含まれていないことを確認してください。

## リソース接続のトラブルシューティング

ユーザーがアクティブなコネクションを管理するには、コネクションセンターを使用します。セッションの動作が遅い、またはコネクションに問題がある場合、ユーザーや管理者はコネクションセンターを使用してトラブルシューティングを行えます。ユーザーは、コネクションセンターで以下の操作を行えます。

- アプリケーションを終了する。
- セッションからログオフする。これによりセッションが終了し、実行中のアプリケーションが終了します。
- セッションから切断する。これにより、アプリケーションを実行したまま（切断時にアプリケーションを閉じるようにサーバーを構成していない場合）、選択したコネクションのサーバー接続が切断されます。

- コネクションの転送統計値を参照する。

## SDK および API

June 19, 2023

### Citrix 仮想チャネル SDK

Citrix 仮想チャ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ネルアプリケーションは、Citrix Virtual Apps and Desktops または Citrix DaaS (Citrix Virtual Apps and Desktops サービスの新名称) サーバー上にあります。

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 テクニカルサポートにお問い合わせください。

仮想チャネル SDK には、以下のものが用意されています。

- Citrix Server API SDK (WFAPI SDK) の仮想チャネル機能とともに使用して新しい仮想チャネルを作成する、Citrix Virtual Driver Application Programming Interface (VD-API)。VD-API によって提供される仮想チャネルサポートは、独自の仮想チャネルを容易に作成できるように設計されています。
- 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。
- 仮想チャネル SDK では、WFAPI SDK で仮想チャネルのサーバー側を作成する必要があります。

詳しくは、[Citrix Virtual Channel SDK for Citrix Workspace app for Linux](#)を参照してください。

### コマンドラインのリファレンス

コマンドラインのリファレンスとパラメーターについて詳しくは、[Citrix Workspace app for Linux Command Reference](#)を参照してください。

### プラットフォーム最適化 SDK

Linux 向け Citrix Workspace アプリの HDX SoC 計画の一環として「プラットフォーム最適化 SDK」を導入しました。

この SDK は、低コスト、省電力、高パフォーマンスのデバイスに画期的なフォームファクタを組み合わせたエコシステムを実現しました。

開発者は、Platform Optimization SDK を使用して、Linux ベースのデバイスのパフォーマンスを向上させることができます。この SDK を使用すると、開発者は Citrix Workspace アプリの ICA エンジンコンポーネント (`wfica`)

の拡張プラグインを作成できます。プラグインは共有可能なライブラリとして構築され、`wfica`はこれらのライブラリを動的に読み込みます。

プラグインによって、Linux デバイスのパフォーマンスを最適化して、以下の機能を実現できます。

- セッション画面の描画に使用される JPEG および H.264 データのデコーディングをアクセラレート
- セッション画面の描画に使用されるメモリの割り当てを制御
- セッション画面の低レベル描画を制御してパフォーマンスを向上
- X11 をサポートしない OS 環境で、画像の出力およびユーザーの入力サービスを提供

詳しくは、[Citrix Workspace app for Linux - Platform Optimization SDK](#)を参照してください。

## ICA 設定リファレンス

June 19, 2023

ICA 設定リファレンスファイルは、レジストリ設定および ICA ファイル設定のリストを提供し、管理者は環境に対して Citrix Workspace アプリの動作を高度にカスタマイズできます。また、ICA 設定リファレンスを使用して、予期しない Citrix Workspace アプリの動作をトラブルシューティングできます。

[ICA 設定リファレンス \(PDF のダウンロード\)](#)





© 2023 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).