Mac 向け Citrix Workspace アプリ

Contents

このリリースについて

June 10, 2022

> 注:
>
> - 2203.1 リリースでは、次のバグが修正されています：Citrix AppFlow が Citrix ADC で構成されている場合、Citrix Workspace アプリセッションが起動しないことがあります。[HDX-39496]
> - macOS Catalina 以降、Apple は管理者が構成する必要のあるルート CA 証明書と中間証明書について、追加の要件を適用しています。詳しくは、Apple のサポート記事HT210176を参照してください。

Apple シリコン（**M1** チップ）のネイティブサポート（**Technical Preview**）

macOS 向け Citrix Workspace アプリは、Apple シリコン（M1 チップ）を搭載した Mac をユニバーサルアーキテクチャによりネイティブサポートするようになりました。ユニバーサルアーキテクチャを使用すると、Citrix Workspace アプリは、Rosetta エミュレーションなしに、Apple シリコンと Intel ベース Mac コンピューターの両方でネイティブに実行されます。Technical Preview ビルドは Apple シリコンを搭載した Mac でネイティブに実行され、M1 チップを使用して Mac にインストールし、テストする必要があります。

> 注:
>
> Citrix は引き続き、Rosetta 2 ダイナミックバイナリトランスレーターを使用する Intel ベースの Mac をサポートします。ただし、Citrix は、Rosetta エミュレーションを使用する Mac 向け Citrix Workspace アプリを間もなく廃止します。「廃止」セクション記載のお知らせに注意してください。

ユニバーサルアーキテクチャビルドは、「Downloads」の「**Citrix Workspace App for macOS (Apple silicon) - Universal Architecture**」セクションからダウンロードできます。Apple シリコン（M1 チップ）を実行している Mac で Citrix Workspace アプリを使用している場合は、HDX RealTime Optimization Pack（RTOP）をアップグレードする必要があります。これにより、Microsoft Skype for Business のオーディオ/ビデオ会議やボイスオーバー IP の企業向け電話が最適化されます。Mac 用 HDX RealTime Media Engine 2.9.500 は、Citrix Web サイトの「Downloads」からインストールできます。

所属組織でサードパーティのプラグインまたは仮想チャネルを使用している場合は、これらのプラグインが Apple シリコンを実行する Mac と互換性があることを確認する必要があります。プラグインが社内で開発されたものである場合は、ユニバーサルアーキテクチャビルドをインストールする前に、これらのプラグインを再構築（リビルド）する必要があります。

ユニバーサルアーキテクチャビルドのアンインストールやカスタム仮想チャネル SDK（VCSDK）の使用などについて詳しくは、「Apple シリコンのネイティブサポート (Technical Preview)」を参照してください。

2204 の新機能

allowedWebStoreURLs の Global App Configuration Service の設定

管理者は、Global App Config Service を使用して、カスタム Web ストアの設定を構成できるようになりました。管理者は、allowedWebStoreURLsプロパティを使用してカスタム Web ストアを構成できます。Global App Configuration Service について詳しくは、「はじめに」を参照してください。

最大化モードで Citrix Workspace アプリを開くためのサポート

管理者は、Global App Configuration Service のmaximise workspace windowプロパティを構成して、Citrix Workspace アプリをデフォルトで最大化モードで開くようにできます。Global App Configuration Service について詳しくは、「はじめに」を参照してください。

高 DPI モニターのサポート［Technical Preview］

Mac 向け Citrix Workspace アプリは、4K を超える解像度の高 DPI モニターと互換性があります。デスクトップセッションでは、アプリ、テキスト、画像、およびその他のグラフィック要素が、これらの高解像度モニターで快適に表示できるサイズで表示されます。

この機能を有効にするには、macOS 端末で次のコマンドを実行します:

```
defaults write com.citrix.receiver.nomas EnableHighDPI -bool YES
```

管理者は、ディスプレイの解像度に合わせて、デスクトップセッションの最大ビデオバッファサイズをキロバイト単位で指定する表示メモリの制限ポリシーを編集できます。表示メモリ制限ポリシーのデフォルト値は 65536KB で、最大 2x4K モニター（2x32400KB）ではこれで十分です。管理者はこの機能を使用するために、［Citrix Studio］ > ［ポリシー］ > ［表示メモリの制限］に移動してこのデフォルト値を編集し、393216KB の値を使用する必要があります。

表示メモリの制限ポリシーについて詳しくは、「表示メモリの制限」を参照してください。

> 注:
>
> この機能は、最大 2 台の接続されているモニターで機能します。
>
> 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ケースは受け付けられませんが、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。ベータビルドは実稼働環境に展開しないことをお勧めします。

リモートデスクトップセッションの永久クライアントアクセスライセンス（CAL）の強化

このリリースでは、リモートデスクトップにアクセスするために環境で CAL を実行している場合、クライアント ID が 15 文字を超えると、恒久ライセンスを使用してリモートデスクトップセッションを起動できます。

この機能を有効にするには、管理者が以下を実行して**default.**icaファイルを構成する必要があります:

1. StoreFront サーバーで、*C:\inetpub\wwwroot\Citrix<StoreName>\App_Data* に移動し、任意のエディターで**default.**icaファイルを開きます。
2. **[WFClient]** セクションに、次の行を追加します:

```
isRDSLicensingEnabled=On
```

デフォルトのキーボード設定の復元

Citrix Workspace アプリでキーボード設定を変更していた場合、デフォルトのキーボード設定を復元できるようになりました。キーボード設定をデフォルト値に戻すには、Citrix Workspace アプリを開いて ［設定］ > ［キーボード］に移動し、［デフォルトに戻す］をクリックします。［はい］をクリックして確定します。

Microsoft Teams の **HDX** 最適化とアプリ保護との互換性

このリリースでは、デリバリーグループに対してアプリ保護が有効になっている場合、モニターやデスクトップの全面共有は無効になります。Microsoft Teams で［コンテンツを共有］をクリックすると、画面選択メニューから［デスクトップ］オプションが削除されます。VDA が 2109 以降である場合、開いているアプリを共有するために選択できるオプションは［ウィンドウ］だけです。2019 より古い VDA に接続している場合、コンテンツは選択できません。

Citrix Workspace Browser

このリリースには、Chromium バージョン 99 ベースの Citrix Workspace Browser バージョン 99.1.1.8 が含まれています。Citrix Workspace Browser について詳しくは、「Citrix Workspace Browser」のドキュメントを参照してください。

Citrix Workspace Browser をデフォルトのブラウザーにする

Citrix Workspace Browser をデフォルトのブラウザーにすることができるようになりました。Citrix Workspace Browser をデフォルトのブラウザーにすると、すべてのリンクと Web および SaaS アプリがデフォルトで Citrix Workspace Browser で開きます。
macOS で Citrix Workspace Browser をデフォルトのブラウザーにするには、以下を実行します:

1. Citrix Workspace Browser を開き、省略記号アイコンをクリックして ［設定］メニューを開きます。
2. 左側のペインで、［デフォルトのブラウザー］オプションをクリックします。
3. ［デフォルトのブラウザー］ページで、［デフォルトにする］をクリックします。プロンプトが表示されたら、［**Citrix Workspace Browser** を使用する］をクリックして選択内容を確認し、変更を適用します。

2204 で解決された問題

- Windows Server 2019 で Citrix Virtual Delivery Agent（VDA）2112 以降にアップグレードすると、セッションがランダムに切断されたり、応答しなくなることがあります。この問題は、Citrix Workspace アプリバージョン 2203 で発生します。[CVADHELP-19687]
- オフライン（イントラネット）モードで Citrix Workspace アプリを使用している場合、Citrix Broker Service および Citrix Director ではクライアント名がランダムな文字で表示されます。[RFMAC-10842]
- ブラウザーを使用してデスクトップまたはアプリのセッションを起動すると、セッションウィンドウがブラウザーウィンドウの背後のバックグラウンドで起動します。[RFMAC-11362]
- StoreFront にログインすると、Citrix Workspace アプリがクラッシュする場合があります。[RFMAC-11378]

2204 の既知の問題

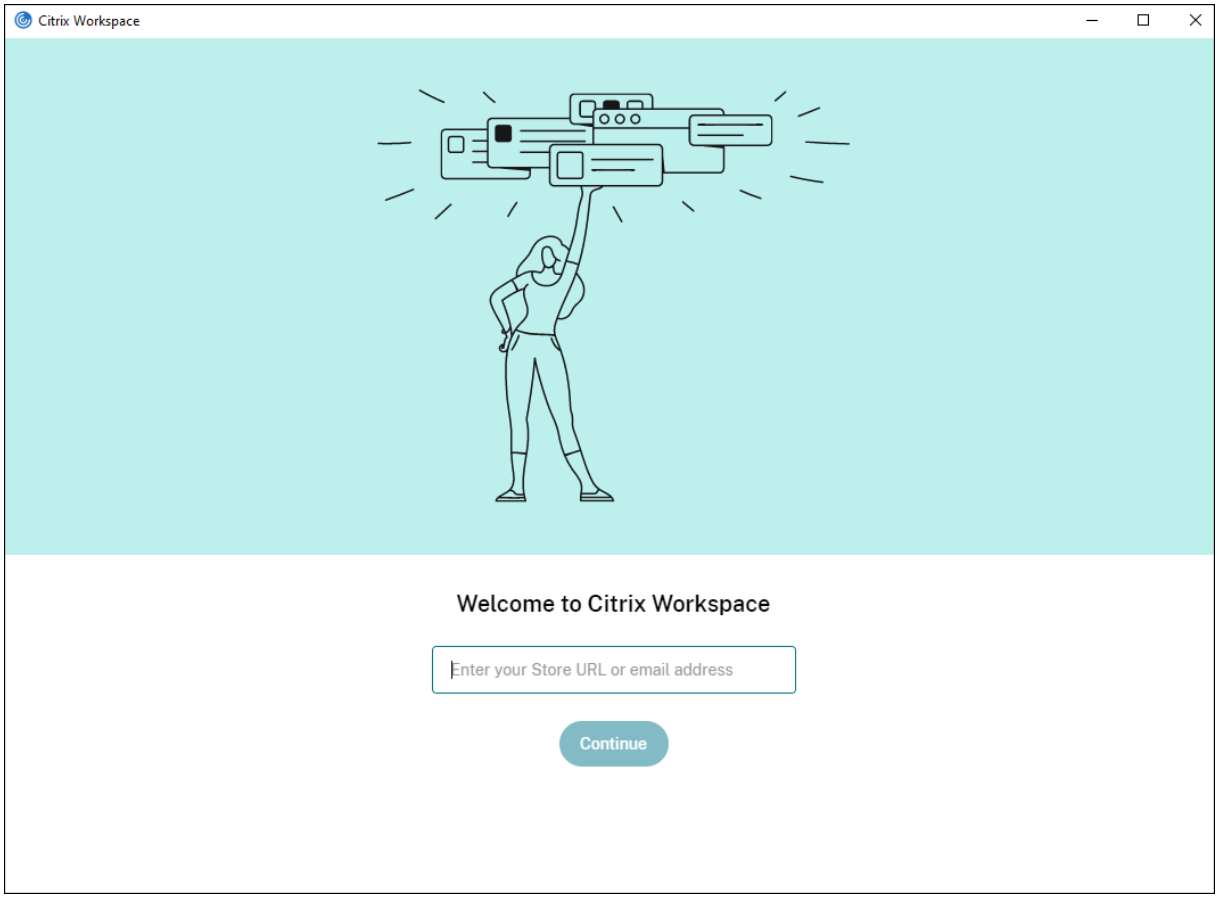
- スマートカードを使用して StoreFront にログインできない場合があります。[CVADHELP-19372]
- 最適化された Microsoft Teams では、別の仮想デスクトップまたはアプリのセッションを開始した場合、ビデオ機能が機能しない場合があります。[HDX-40451]

以前のリリース

このセクションでは、以前のリリースの機能と、解決された既知の問題を示します。リリースは、リリース日の 18 か月後に製品終了（EOL）になります。サポートされているバージョンのライフサイクル日程について詳しくは、「Lifecycle Milestones for Citrix Workspace app and Citrix Receiver」を参照してください。

2203.1

このリリースには、初めてのユーザー向けのシンプルかつ直感的なオンボーディング操作環境が導入されています。



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は 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（旧称 Citrix Virtual Apps and Desktops サービス）セッションまたは Citrix StoreFront ストアには影響しません。

詳しくは、「Citrix Workspace アプリの非アクティブタイムアウト」を参照してください。

PDF ユニバーサル印刷

Mac から印刷するときに PDF ユニバーサル印刷機能を使用できるようになりました。Citrix ユニバーサルプリンタードライバー（UPD）を使用して Mac でクライアントプリンターを自動作成する場合、HP Color LaserJet 2800 シリーズ PS ドライバーをインストールする必要がなくなりました。

この機能を使用する方法について詳しくは、「印刷」を参照してください。

Web および **SaaS** アプリ向けに強化されたシングルサインオン（**SSO**）エクスペリエンスのサポート **[Technical Preview]**

この機能により、サードパーティの ID プロバイダー（IdP）を使用しながら、内部 Web アプリおよび SaaS アプリ向けの SSO の構成を簡素化できます。強化された SSO エクスペリエンスにより、プロセス全体がいくつかのコマンドに集約されます。SSO をセットアップするために ID プロバイダーチェーンで Citrix Secure Private Access を構成するという、必須の前提条件がなくなります。また、Citrix Workspace アプリと起動中の特定の Web または SaaS アプリの両方の認証に同じ ID プロバイダーが使用される場合、ユーザーエクスペリエンスも向上します。

このPodio フォームを使用して、この Technical Preview に登録できます。

> 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ケースは受け付けられませんが、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。ベータビルドは実稼働環境に展開しないことをお勧めします。

Linux VDA における **TLS**（**Transport Layer Security**）プロトコルバージョン **1.3** のサポート（**Technical Preview**）

TLS バージョン 1.3 を実行している場合は、Linux オペレーティングシステムでホストされている仮想アプリと仮想デスクトップに接続できるようになりました。

> 注:
>
> TLS バージョン 1.3 を実行している場合、Windows 仮想アプリと仮想デスクトップに接続することはできません。

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ケースは受け付けられませんが、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「コンテンツの共有」機能を使用してアプリを共有

Microsoft Teams の画面共有機能を使用して、個別のアプリケーション、ウィンドウ、または全画面を共有できます。Citrix Virtual Delivery Agent 2109 は、この機能の前提条件です。
特定のアプリケーションを表示するには、会議コントロールの ［コンテンツの共有］をクリックして、目的のアプリケーションを選択します。選択したアプリの周囲に赤い境界線が表示された後、通話中のピアはアプリを見ることができます。アプリを最小化すると、Microsoft Teams は共有アプリの最後の画像を表示します。共有を再開するには、ウィンドウを最大化します。

Microsoft Teams のマルチウィンドウチャットと会議

Citrix Virtual Apps and Desktops および Citrix DaaS で HDX による最適化が行われると、Microsoft Teams（1.5.00.5967 以降）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。ユーザーは、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 Office 365 サイトの「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 VDA を使用している場合、Microsoft 社は将来シングルウィンドウコードを廃止する予定ですので注意してください。ただし、複数のウィンドウをサポートする VDA/CWA のバージョン（2203 以降）にアップグレードするまで、少なくとも 9 か月の猶予があります。

> 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。詳細については、Microsoft 365 のロードマップを参照してください。

Microsoft Teams の制御を渡すまたは取り戻す

［制御を渡す］ボタンを使用して、会議に参加している他のユーザーに共有画面への制御アクセス権を与えることができます。ほかの参加者は、キーボード、マウス、クリップボードの入力を使用して、共有画面を選択および変更できます。自分もほかのユーザーも共有画面を制御できるようになり、いつでも制御を取り戻すことができます。

画面共有セッション中に制御を獲得する場合、参加者は誰でも ［制御を要求する］ボタンを使用して制御アクセス権を要求できます。画面共有している人は、その要求を承認または拒否できます。制御権を持つと、共有画面でキーボードやマウスの入力を制御したり、制御を手放して共有制御を停止したりできます。

> 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。

StoreFront から **Workspace** への移行

組織がオンプレミスの StoreFront から Workspace に移行するとき、ユーザーは新しい Workspace URL を Citrix Workspace アプリに手動で追加する必要があります。この機能により、管理者は最小限のユーザー操作でユーザーを StoreFront ストアから Workspace ストアにシームレスに移行できます。

この機能について詳しくは、「StoreFront から Workspace への URL の移行」を参照してください。

Global App Config Service

Citrix Workspace 向けの新しい Citrix Global App Configuration Service を使用すると、シトリックス管理者は集中管理されたサービスによって Workspace サービスの URL と Citrix Workspace アプリの設定を配信できます。
詳しくは、「Global App Configuration Service」のドキュメントを参照してください。

フルスクリーンモードを複数のモニターで使用する

2 台以上のモニターで同時にフルスクリーンモードにすることができるようになりました。この機能を使用するには、次の手順を実行します:

1. Citrix Viewer を開きます。
2. 接続されている他のモニターでフルスクリーンモードを使用するには、ウィンドウをプライマリモニターからドラッグして、接続されているモニターに移動します。メニューバーから、[表示] > [フルスクリーンにする] を選択します。これらのモニターで、ウィンドウはフルスクリーンモードになります。

   > 注:
   >
   > 以前に [すべてのディスプレイをフルスクリーンで使用する] オプションを選択した場合は、これによって、接続されているすべてのモニターでフルスクリーンモードが選択されているため、必ず選択を解除してください。

プライマリモニターを含めて、使用は最大 3 台のモニターにすることをお勧めします。

Citrix Workspace Browser

このリリースには、Chromium バージョン 98 ベースの Citrix Workspace Browser バージョン 98.1.2.17 が含まれています。Citrix Workspace Browser の機能またはバグ修正については、Citrix Workspace Browser ドキュメントの「新機能」を参照してください。

解決された問題

- アクティブなセッション中、Citrix Workspace アプリのウォーターマークが透明になり、ウィンドウのコンテンツがバックグラウンドで表示されます。この問題は、シームレスモードでのみ発生します。[CVADHELP-19153]
- VDA（2112 以降）から Citrix ADC 経由でセッションを起動すると、セッション画面の保持が開始されているが再接続されていない状態で、セッションが中断される場合があります。[CVADHELP-19687]
- Mimecast プラグインからの [Large File Receive] ポップアップダイアログが Outlook に表示されません。[HDX-37137]
- Path MTU Discovery（PMTUD）の値が 1500（デフォルト）ではない場合、ユーザーは Azure クラウド環境で TCP にフォールバックできません。[HDX-37215]
- 最適化された Microsoft Teams ビデオ通話で Web カメラがオンになっていると、エンドポイントで CPU 使用率が高くなる場合があります。[HDX-37168]
- 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]

- Citrix AppFlow が Citrix ADC で構成されている場合、Citrix Workspace アプリセッションが起動しないことがあります。[HDX-39496]
- 自動更新が無効になっている場合に ［環境設定］ > ［詳細］に移動すると、Citrix Workspace アプリがクラッシュします。[RFMAC-10978]

2201

StoreFront から Workspace への移行 [Technical Preview]

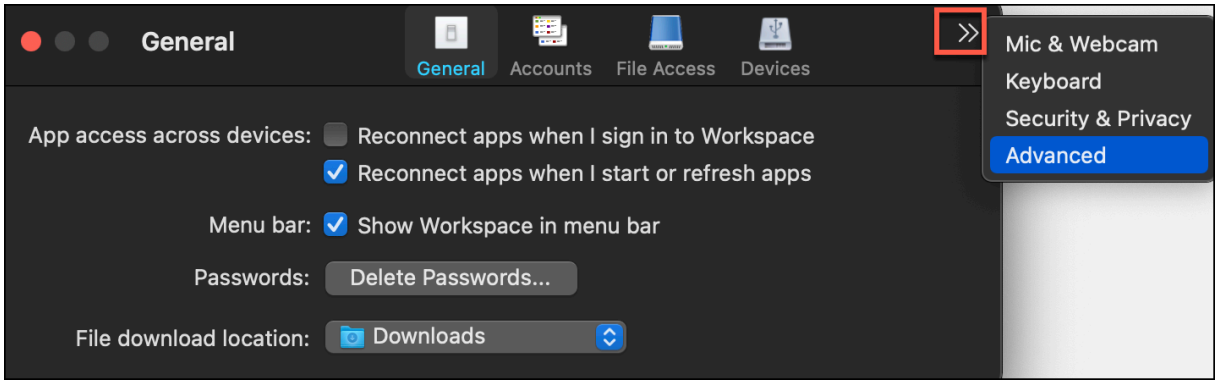
組織がオンプレミスの StoreFront から Workspace に移行するとき、ユーザーは新しい Workspace URL を Citrix Workspace アプリに手動で追加する必要があります。この機能により、管理者は最小限のユーザー操作でユーザーを StoreFront ストアから Workspace ストアにシームレスに移行できます。

> 注:
>
> Technical Preview は、お客様が非実稼働環境または制限のある実稼働環境でテストし、フィードバックを共有するためのものです。機能プレビューのサポートケースは受け付けられませんが、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。ベータビルドは実稼働環境に展開しないことをお勧めします。

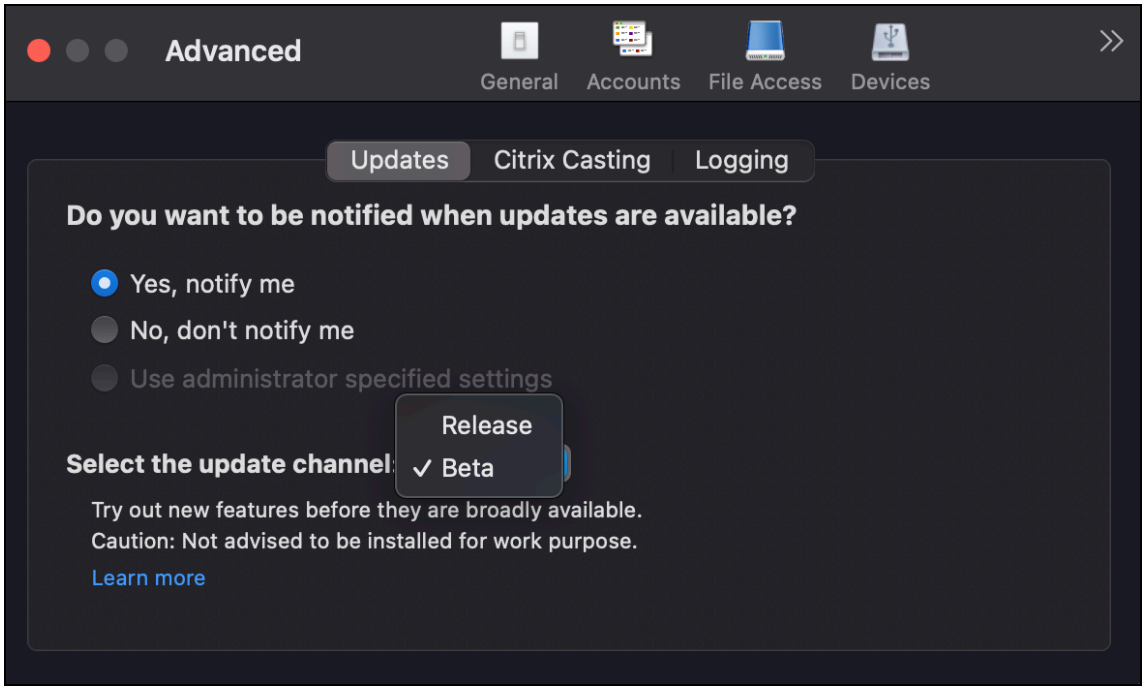
Citrix Workspace アプリのベータプログラム

このリリース以降、Citrix Workspace アプリの既存のインストールを最新のベータビルドに自動的に更新して、それらをテストすることができます。ベータビルドは、完全にサポートされている安定版リリースアップデートが一般提供される前にリリースされる、早期アクセスバージョンです。Citrix Workspace アプリが自動更新用に構成されている場合は、更新通知を受け取ります。

ベータビルドにアクセスするには、Citrix Workspace アプリを開き、ツールバーで Citrix Workspace を右クリックして ［環境設定］ > ［詳細］をクリックします。ベータビルドに更新するには、ドロップダウンリストから ［**Beta**］チャネルを選択します。



- **Beta** - 一般提供前に簡単にテストして問題を報告できる早期アクセスリリース。
- **Release** - 完全にサポートされている安定版リリースの更新プログラム。



この機能の使用について詳しくは、「アップデート」を参照してください。

フルスクリーンモードを複数のモニターで使用 **[Technical Preview]**

2 台以上のモニターで同時にフルスクリーンモードにすることができるようになりました。この機能を使用するには、次の手順を実行します:

1. Citrix Viewer を開きます。
2. 接続されている他のモニターでフルスクリーンモードを使用するには、ウィンドウをプライマリモニターからドラッグして、接続されているモニターに移動します。メニューバーから、[表示] > [フルスクリーンにする] を選択します。これらのモニターで、ウィンドウはフルスクリーンモードになります。

   > 注:
   >
   > 以前に ［すべてのディスプレイをフルスクリーンで使用する］オプションを選択した場合は、これによって、接続されているすべてのモニターでフルスクリーンモードが選択されているため、必ず選択を解除してください。

プライマリモニターを含めて、使用は最大 3 台のモニターにすることをお勧めします。

> 注:
>
> Technical Preview は、お客様が非実稼働環境または制限のある実稼働環境でテストし、フィードバックを共有するためのものです。機能プレビューのサポートケースは受け付けられませんが、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。ベータビルドは実稼働環境に展開しないことをお勧めします。

解決された問題

- キーボードの左矢印または右矢印を使用して入力システム作成ウィンドウから候補テキストを選択しても、入力カーソルがそれに応じて移動しません。この問題は、Citrix Workspace アプリの［設定］の［キーボード］ウィンドウで ［リモートサーバーのキーボードレイアウトではなくローカルのレイアウトを使用する］チェックボックスがオンになっているデスクトップを起動した場合に発生します。この問題は、日本語と中国語でのみ発生します。[HDX-34956]
- Workspace アプリのセッションでマウスポインターが断続的に消え、何もクリックできなくなります。[HDX-36820]
- Excel シートのピボットテーブルのセルをドラッグすると、デスクトップセッションが予期せず終了します。[HDX-37178]
- バージョン 2112 にアップグレードした後、無損失および全画面 H.264 コーデックのポリシーが適用されている場合、デスクトップセッションでグラフィックの問題が発生することがあります。[HDX-37272]
- Citrix Workspace アプリ 2010 からバージョン 2112 にアップグレードすると、デスクトップまたはアプリに接続できなくなります。[RFMAC-10811]

2112

新機能

カスタム **Web** ストアのサポート

Mac 向け 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るようになりました。以前は、ブラウザーからのみ、カスタマイズされたすべてのストアにアクセスできました。

Mac 向け Citrix Workspace アプリは、ブラウザーのようなエクスペリエンスのカスタム Web ストアを読み込み、アプリ保護機能をカスタム Web ストアに拡張します。ネイティブの Citrix Workspace アプリからカスタムポータルにアクセスできるようにすることで、この機能を完全に利用でき、同じユーザーエクスペリエンスが提供されます。Global App Configuration Service について詳しくは、「Getting Started」を参照してください。

カスタム Web ストアの構成について詳しくは、「カスタム Web ストア」を参照してください。

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。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:

［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。

動的緊急通報（**Dynamic e911**）

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 通話プラン、Operator Connect、ダイレクトルーティングで使用すると、以下を実行できます:

- 緊急電話の構成とルーティング
- セキュリティ担当者への通知

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送信されます。Ray Baum 法では、911 発信者の派遣可能位置情報を、適切な緊急通報受理機関（PSAP）に送信する必要があります。Windows 向け Citrix Workspace アプリ 2112.1 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。この機能について詳しくは、「**Microsoft** 電話システム」セクションの「ダイナミック e911 のサポート」を参照してください。

PDF ユニバーサル印刷（**Technical Preview**）

PDF ユニバーサル印刷機能は、Citrix Virtual Apps and Desktops 2112 リリースで使用できます。この機能はデフォルトでは無効になっています。この機能を使用するには、こちらのWeb フォームを使用してサインアップする必要があります。この機能は、シトリックス側がお客様の情報を受け取ると、有効になります。お客様も、機能の使用方法と、有効にする必要がある印刷ポリシーについての説明を受け取ります。

> 注:
>
> Technical Preview は、お客様が非実稼働環境または制限のある実稼働環境でテストし、フィードバックを共有するためのものです。機能プレビューのサポートケースは受け付けられませんが、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。ベータビルドは実稼働環境に展開しないことをお勧めします。

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、仮想アプリと仮想デスクトップを起動できます。Citrix Workspace Web 拡張機能は、Web ブラウザーでアプリやデスクトップにアクセスするユーザーにサービス継続性を提供します。

Citrix 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。

Citrix Workspace Browser

このリリースの Workspace Browser は、Chromium バージョン 95 が基になっています。Citrix Workspace Browser の機能またはバグ修正については、Citrix Workspace Browser ドキュメントの「新機能」を参照してください。

解決された問題

- トランスポートプロトコルが Enlightened Data Transport（EDT）から TCP に切り替わると、「サーバーに接続できません」エラーが表示されます。[CVADHELP-18310]
- 保護されている Progressive Web Apps（PWA）が macOS で開かれている場合、アプリ保護ポリシーが適用されていません。[RFMAC-10128]

2111

新機能

- このリリースでは、ユーザーは Mac 向け Citrix Workspace アプリをシステムにインストールされているバージョンよりも前のバージョンに手動でロールバックすることはできません。たとえば、Mac デバイスに Citrix Workspace アプリバージョン 2109 がインストールされている場合、アプリをバージョン 2108 以前に手動でロールバックすることはできません。
- クライアントアクセスライセンス（CAL）を実行してリモートデスクトップにアクセスしている場合は、恒久ライセンスを使用してリモートデスクトップセッションを起動します。クライアント ID が 15 文字を超える場合は、リモートデスクトップセッションを起動できます。
- Citrix Workspace アプリ 2111 を実行している Mac に Citrix 仮想チャネル SDK を読み込むには、カスタム仮想チャネルを再コンパイルする必要があります。詳しくは、Mac 向け Citrix Workspace アプリでのカスタム仮想チャネルの更新を参照してください。

カスタム **Web** ストアのサポート **[Technical Preview]**

このリリースでは、macOS 向け 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。管理者は、この機能を使用するために、Global App Configuration Service で許可されている URL の一覧にカスタム Web ストアを追加する必要があります。URL を追加したら、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 macOS 向け Citrix Workspace アプリウィンドウで開きます。

> 注:
>
> Technical Preview は、お客様が非実稼働環境または制限のある実稼働環境でテストし、フィードバックを共有するためのものです。機能プレビューのサポートケースは受け付けられませんが、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。

> ベータビルドは実稼働環境に展開しないことをお勧めします。

Citrix Workspace Browser - Citrix Workspace Browser の新機能またはバグ修正については、Citrix Workspace Browser ドキュメントの「新機能」を参照してください。

解決された問題

- macOS を実行しているデバイスでは、Advanced Audio Coding（AAC）はサポートされていません。[CTXBR-1844]
- `.cr`ファイルを使用して Citrix Workspace アプリを構成し、資格情報を使用してサインインした場合、ホームページはしばらくしてから表示されます。[RFMAC-9990]
- 保護された SaaS アプリを開き、新しいタブを開きます。新しいタブをタブバーからドラッグして新しいウィンドウに分離します。次に、2 つのウィンドウを並べて配置し、2 番目のウィンドウで新しいタブを開いてスクリーンショットを撮ります。そうすると、保護された SaaS アプリのスクリーンショットもキャプチャできます。[RFMAC-10060]
- あるストアから別のストアに切り替えると、最初のストアからサインアウトされる場合があります。[RFMAC-10137]
- Citrix Workspace アプリへのサインイン中に誤った資格情報を入力すると、「資格情報が正しくありません」というエラーメッセージは表示されず、認証プロンプトがもう一度表示されます。ドメイン\ユーザーがユーザー名の代わりに認証プロンプトに表示されることがあります。[RFMAC-10210]
- Mac 向け Citrix Workspace アプリ 2109 から Windows 向け Citrix Workspace アプリ 2109 に最適化された Microsoft Teams の P2P 呼び出しが行われると、呼び出しエラーが発生します。[HDX-35223]

2109.1

新機能

macOS Monterey のサポート

Mac 向け Citrix Workspace アプリは、macOS Monterey（12.0.1）でサポートされています。

解決された問題

- 保護されたアプリ、保護されていない SaaS アプリ、および保護されたデスクトップセッションを開いた場合、ブラウザーが予期せず終了します。この問題は、保護されたデスクトップセッションウィンドウから、保護されていない SaaS アプリに切り替えるときに発生します。[CTXBR-2087]
- 管理者が Google Chrome に外部拡張機能をインストールしている場合、Citrix Workspace Browser を開くとクラッシュします。[CTXBR-2135]

2109

新機能

> 注:
>
> サービス継続性が有効になっていて、バージョン 2109 にアップグレードすると、接続リースファイルが更新されます。機能拡張の一環として、既存のすべてのリースが削除され、新しいリースがフェッチされます。

macOS Monterey Beta 版の **Mac** 向け **Citrix Workspace** アプリ

Mac 向け Citrix Workspace アプリ 2109 は、macOS Monterey Beta 7 でテストされています。このセットアップをテスト環境で使用し、フィードバックを提供します。

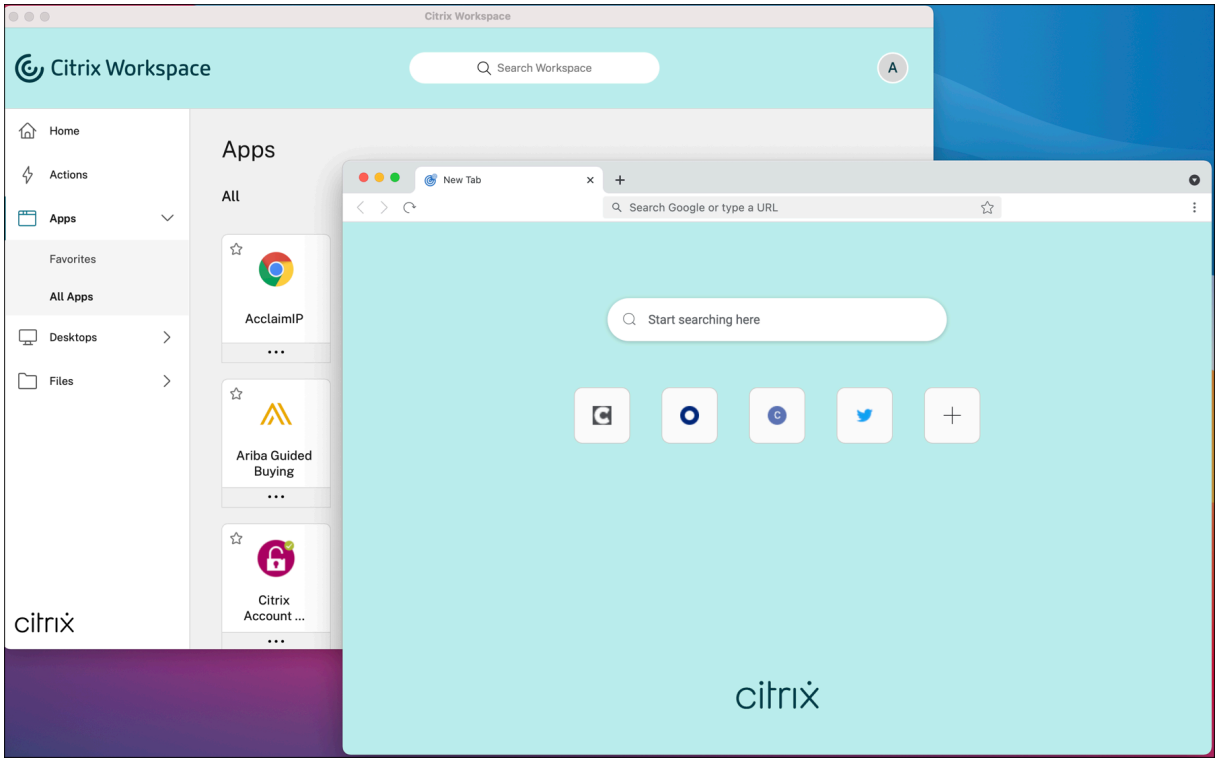
> 注意:
>
> 実稼働環境で macOS Monterey Beta 版の Mac 向け Citrix Workspace アプリを使用しないでください。

ストアのメールベースの自動検出

Mac 向け 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。

Citrix Workspace Browser

Citrix Workspace Browser は、クライアントマシンで実行されるネイティブブラウザーです。これにより、ユーザーは Citrix Workspace アプリから安全な方法で Web アプリまたは SaaS アプリを開くことができます。ブラウザーでは、さまざまな Web アプリまたは SaaS アプリへのアクセス時に、一貫性のあるユーザーインターフェイスが提供され、生産性の向上と、アプリのレンダリングでの優れたパフォーマンスが実現します。



新しい Workspace ブラウザーは、ユーザーエクスペリエンスの向上に引き続き重点を置いており、次の機能を備えた、強化された、よりネイティブブラウザーのようなエクスペリエンスを提供します:

- 内部 Web ページへの VPN レスアクセス
- マイクと Web カメラのサポート
- タブブラウジングエクスペリエンス
- マルチウィンドウビュー
- 編集可能なオムニボックス
- ブックマーク
- 新しいタブページのショートカット
- カスタマイズ可能な設定
- 分析

管理者は、URL ごとにさまざまな組み合わせで、キーロガー対策、スクリーンキャプチャ対策、ダウンロード、印刷、クリップボード制限、透かしなどの、Secure Private Access やアプリ保護ポリシーを有効にできます。

詳しくは、Citrix Workspace Browserのドキュメントを参照してください。

エンドポイント解析（**EPA**）の機能強化

このリリース以降、macOS 向け Citrix Workspace アプリはエンドポイント解析（EPA）をサポートします。高度なエンドポイント分析（EPA）がデバイスをスキャンして、Citrix Gateway で設定されているエンドポイントのセキュリティ要件を確認します。スキャンが正常に完了すると、ユーザーにアクセス権が付与されます。

> 中:
>
> この機能は、環境で nFactor 認証を構成した場合にのみ有効になります。

EPA スキャンについて詳しくは、「Advanced Endpoint Analysis スキャン」を参照してください。

アダプティブオーディオ

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

Microsoft Teams による **H.264 Advanced Video Coding**（**MPEG-4 AVC**）のサポート

このリリースには、ハードウェアアクセラレーションによる H.264 ビデオエンコーディング/デコーディングのサポートが含まれています。これにより、CPU 使用率の負荷が軽減され、ビデオ会議のエクスペリエンスが向上します。Citrix HDX 最適化された Microsoft Teams のマルチメディアエンジン（HdxRtcEngine.exe）は、エンコーディングとデコーディングに Apple の Video Toolbox フレームワークを使用するようになりました。このフレームワークは、ビデオをより高速かつリアルタイムで圧縮および解凍します。また、GPU へのエンコーディングとデコーディングのオフロードが最適化されます。デバイスがサポートしている場合は、ハードウェアアクセラレーションによるビデオのエンコーディングとデコーディングはデフォルトで有効になっています。この機能拡張により、Microsoft Teams が HDX で最適化されている場合、マルチメディアの使用中の CPU の負荷が軽減されます。

解決された問題

- Mac 向け Citrix Workspace アプリにサインインすると、数時間後に認証を求めるプロンプトが表示されます。[RFMAC-10032]
- Citrix Workspace アプリにストアを追加し、サーバーコンソールで認証ドメインを変更し、アプリを数分間アイドル状態にしてからアプリまたはデスクトップセッションを開くと、Citrix Workspace アプリがクラッシュする可能性があります。[RFMAC-10133]
- 仮想アプリまたはデスクトップが既に実行されていて、別の仮想アプリまたはデスクトップを起動すると、Citrix Viewer は表示されますが、仮想アプリは開きません。この問題は、macOS 11.6 を実行しているデバイスで発生します。[RFMAC-10134]

2108.1

新機能

このリリースではさまざまな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

仮想アプリまたはデスクトップが既に実行されていて、別の仮想アプリまたはデスクトップを起動すると、Citrix Viewer は表示されますが、仮想アプリは開きません。この問題は、macOS 11.6 を実行しているデバイスで発生します。[RFMAC-10134]

2108

新機能

Mac 向け Citrix Workspace アプリで、Enlightened Data Transport（EDT）で最大転送単位（MTU）検出がサポートされるようになりました。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。

> 注:
>
> EDT の MTU 検出は、macOS Big Sur 以降でサポートされています。

解決された問題

- Microsoft Teams での会議通話中に、ビデオに遅延が生じます。[HDX-32603]
- macOS Big Sur を実行している Mac クライアントで、HTTP 404 または HTTP/1.1 内部サーバーエラーが発生する場合があります。この問題は、セッションへの再接続時に発生します。[RFMAC-9448]

2107

新機能

このリリースではさまざまな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

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

2106

新機能

301 リダイレクトを使用したカスタマイズした **URL** のサポート

HTTP 301 リダイレクトを使用して StoreFront または Citrix Gateway から Citrix Workspace にリダイレクトする URL を追加できます。

StoreFront から Citrix Workspace に移行する場合は、HTTP 301 リダイレクトを使用して StoreFront URL を Citrix Workspace URL にリダイレクトできます。その結果、古い StoreFront URL を追加すると、Citrix Workspace に自動的にリダイレクトされます。

リダイレクトの例:

StoreFront URL の`https://< Citrix Storefront url>/Citrix/Roaming/Accounts`は、Citrix Workspace URL の`https://<Citrix Workspace url>/Citrix/Roaming/Accounts`にリダイレクトできます。

> 注:
>
> - Microsoft での変更内容が保留状態のため、Mac 向け Citrix Workspace アプリは、Microsoft Teams でのデュアルトーンマルチ周波数（DTMF）をサポートしていません。
> - このリリース以降、Citrix Viewer のバージョン番号と Citrix Workspace アプリのバージョン番号が一致しない場合があります。お客様がこの変更の影響を受けることはありません。

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、仮想アプリと仮想デスクトップを起動できます。

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

Microsoft Teams の機能強化

Desktop Viewer がフルスクリーンモードの場合、ユーザーは **Desktop Viewer** がカバーするすべての画面から 1 つを選択して共有できます。ウィンドウモードでは、ユーザーは ［**Desktop Viewer**］ウィンドウを共有できます。シームレスモードでは、ユーザーはエンドポイントデバイスに接続されている複数の画面から 1 つの画面を選択できます。
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。

ユーザーが画面を共有したい場合は、使用可能なすべての画面のプレビューが画面共有パネルに表示されるため、プレビューから適切な画面を直感的に選択できます。

解決された問題

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

2104

新機能

Mac 向け Citrix Workspace アプリは、組織がシングルサインオンを有効にしていない限り、ユーザーによるネットワーク共有への手動サインオンをサポートします。共有ネットワークの場所にアクセスするには、Citrix Workspace アプリを開き、［ファイル］ > ［ネットワーク共有］に移動し、資格情報を提供します。ネットワーク共有のセットアップについて詳しくは、「ストレージゾーンコネクタの作成と管理」を参照してください。

解決された問題

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

2102

新機能

このリリースではさまざまな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

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

2101

新機能

Apple Silicon（**M1** チップ）のサポート

Mac 向け Citrix Workspace アプリで、macOS Big Sur（11.0 以降）で動作し Rosetta 2 を使用する Apple Silicon デバイス（M1 チップ搭載）がサポートされるようになりました。その結果、すべてのサードパーティの仮想チャネルは Rosetta 2 を使用する必要があります。それ以外の場合、macOS Big Sur（11.0 以降）で動作する Mac 向け Citrix Workspace アプリで仮想チャネルが機能しない可能性があります。Rosetta について詳しくは、Apple のサポート記事を参照してください。

シームレスなアプリセッションのための **Microsoft Teams** 最適化のサポート

Mac 向け Citrix Workspace アプリで、シームレスなアプリセッションのための Microsoft Teams 最適化がサポートされるようになりました。その結果、Citrix Workspace アプリ内からアプリケーションとして Microsoft Teams を起動できます。詳しくは、次の記事を参照してください：

- Microsoft Teams の最適化
- Microsoft Teams リダイレクト

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

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

解決された問題

- OWA（Outlook Web App）を使用して Microsoft Teams のミーティングを開こうとすると失敗し、関連するすべてのウィンドウが予期せず終了する場合があります。[CTXBR-1175]
- ビデオ通話を開始するときに Microsoft Teams が応答しなくなり、「`Citrix HDX not connected`」エラーが表示されることがあります。[RFMAC-6727]
- macOS Big Sur（11.0.1）では、USB デバイスを接続しようとすると失敗し、セッションが予期せず終了する場合があります。[RFMAC-7079]
- 公開デスクトップでは、ローカル Mac デバイスに保存されたファイルの作成日が、現在の日付ではなく、1979 年 11 月 30 日として表示される場合があります。[CVADHELP-16309]
- 公開アプリのログオン画面が正しく表示されないことがあり、その結果、ウィンドウのサイズが小さくなり、背景色が赤になります。[CVADHELP-16027]
- オーディオデバイスを切断して接続すると、この操作を行った側で音声通話が切断される場合があります。[RFMAC-7371]
- クリップボード制限ポリシーが有効になっていても、Office 365 アプリ内からテキストをコピーできる場合があります。[CTXBR-1166]
- HDX RealTime Connector エンジンの問題が原因で、Microsoft Teams を起動しようとすると失敗する場合があり、次のエラーメッセージが表示されます:

  ```
  Sorry, we couldn't connect you
  ```

  [CVADHELP-16432]

2012

新機能

Apple Silicon（**M1** チップ）サポート **-** プレビュー

Mac 向け Citrix Workspace アプリは、プレビューベースで Apple Silicon デバイス（M1 チップ搭載）をサポートするようになりました。

Microsoft Teams での画面共有の最適化

Mac 向け Citrix Workspace アプリは、Microsoft Teams での画面共有の最適化をサポートします。詳しくは、以下を参照してください:

- Microsoft Teams の最適化
- Microsoft Teams リダイレクト

パフォーマンスの向上

このリリースではさまざまな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

- Mac 向け Citrix Workspace アプリ 2008 以降のを使用している場合、公開アプリケーションの複数のインスタンスを起動しようとすると失敗することがあります。[CVADHELP-16019]
- USB ドッキングステーションを使用している場合、汎用 USB リダイレクトを開始しようとすると失敗することがあります。[RFMAC-6687]
- 公開デスクトップで CTRL+O を使用してウィンドウを開こうとすると、2 つのウィンドウが開くことがあります。[CVADHELP-15747]
- macOS Big Sur Beta で Mac 向け Citrix Workspace アプリを使用すると、音声通話が切断される場合があります。この問題は、音声通話中にオーディオデバイスを切断して別のオーディオデバイスを接続すると発生します。[RFMAC-6112]
- Microsoft Teams でカメラをオンまたはオフにすると、HDX RealTime Connector エンジンが予期せず終了する場合があります。[RFMAC-6293]
- Mac 向け Citrix Workspace アプリ内から Citrix Files を起動しようとすると、シングルサインオンの問題で失敗する場合があります。[RFMAC-4477]

既知の問題

2203.1 の既知の問題

- ブラウザーウィンドウが最大化されていない限り、Jira アプリの ［**Create**］ボタンをクリックすることはできません。[CTXBR-1976]
- Web ソケット接続は、Citrix Secure Private Access 経由でトンネリングされません。[CTXBR-2439]
- Citrix Workspace アプリをバージョン 2203 にアップグレードすると、Citrix Workspace Browser アイコンに疑問符アイコンが表示されます。この問題は、アップグレード前に Workspace Browser がドックに固定されていた場合に発生します。[CTXBR-2864]
- Citrix Workspace Browser の ［**Advanced**］セクションで ［**Reset settings**］オプションをクリックしても、ログ設定はデフォルトにリセットされません。この問題を回避するには、［**Logs**］ページで ［**Reset to default log settings**］オプションをクリックします。[CTXBR-2929]

- Citrix Workspace Browser バージョン 2201 からバージョン 2203 にアップグレードすると、以前に保存したパスワードが失われ、新しいパスワードを保存できなくなります。[CTXBR-3063]
- フルスクリーンモードは、ノッチのある Mac では使用できません。[CVADHELP-19337]
- ブラウザーを使用してデスクトップまたはアプリのセッションを起動すると、セッションウィンドウがブラウザーウィンドウの背後のバックグラウンドで起動します。[RFMAC-11362]

2201 の既知の問題

- オフライン（イントラネット）モードで Citrix Workspace アプリを使用している場合、Citrix Broker Service および Citrix Director ではクライアント名がランダムな文字で表示されます。[RFMAC-10842]

2112 の既知の問題

- 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]

2111 の既知の問題

このリリースで確認されている新しい問題はありません。

2109.1 の既知の問題

このリリースで確認されている新しい問題はありません。

2109 の既知の問題

- `.cr`ファイルを使用して Citrix Workspace アプリを構成し、資格情報を使用してサインインした場合、ホームページはしばらくしてから表示されます。[RFMAC-9990]
- 保護されている Progressive Web Apps（PWA）が macOS で開かれている場合、アプリ保護ポリシーが適用されていません。[RFMAC-10128]
- Citrix Workspace アプリでストアを追加した後、[**Workspace** アプリの再認証期間］で ［現在の再認証期間］を変更し、数分後にオンプレミスからクラウドストアに切り替えると、クラウドストアからサインアウトされ、認証プロンプトが表示されます。Citrix Workspace アプリにサインインすると、スピナーがいつまでも表示され、サインインできなくなります。[RFMAC-10140]

2108.1 の既知の問題

このリリースで確認されている新しい問題はありません。

2108 の既知の問題

サーバーコンソールで認証ドメインを変更した後にサブスクライブ済みの SaaS アプリを起動すると、セッションが開始されず、次のエラーメッセージが表示されます:

「認証ドメインが変更されました。しばらくしてからもう一度サインインしてください。」[RFMAC-9616]

2107 の既知の問題

サーバーコンソールで認証ドメインを変更し、資格情報を使用してサインインした場合、次のエラーメッセージが表示されます:

「サーバーに接続できません」

[**OK**] をクリックすると、ストアにアクセスできます。[RFMAC-9494]

2106 の既知の問題

画面を共有すると、黒い画面が表示されます。[HDX-30083]

2104 の既知の問題

このリリースで確認されている新しい問題はありません。

2102 の既知の問題

このリリースで確認されている新しい問題はありません。

2101 の既知の問題

- Mac 向け Citrix Workspace アプリ内から［ネットワーク共有］のファイルにアクセスしようとすると、オプションが有効になっていても失敗する場合があります。[RFMAC-7272]
- macOS Big Sur では、Mac 向け Citrix Workspace アプリでシングルサインオンで利用できる SAML Web アプリを起動しようとすると失敗し、次のエラーメッセージが表示される場合があります。

  ```
  Page could not load. Please try again later or contact your administrator
   for assistance. Incident ID:-202
  ```

  [RFMAC-7282]

2012 の既知の問題

- ビデオ通話を開始するときに Microsoft Teams が応答しなくなり、「`Citrix HDX not connected`」エラーが表示されることがあります。この問題を回避するには、Microsoft Teams または VDA を再起動します。[RFMAC-6727]
- Microsoft Skype for Business のビデオ通話は、macOS Big Sur（11.0.1）ではサポートされていません。
- macOS Big Sur（11.0.1）では、USB デバイスを接続しようとすると失敗し、セッションが予期せず終了する場合があります。この問題を回避するには、USB デバイスを再接続します。[RFMAC-7079]

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。

Mac 向け Citrix Workspace アプリのサードパーティ製品についての通知

Apple シリコンのネイティブサポート（**Technical Preview**）

June 10, 2022

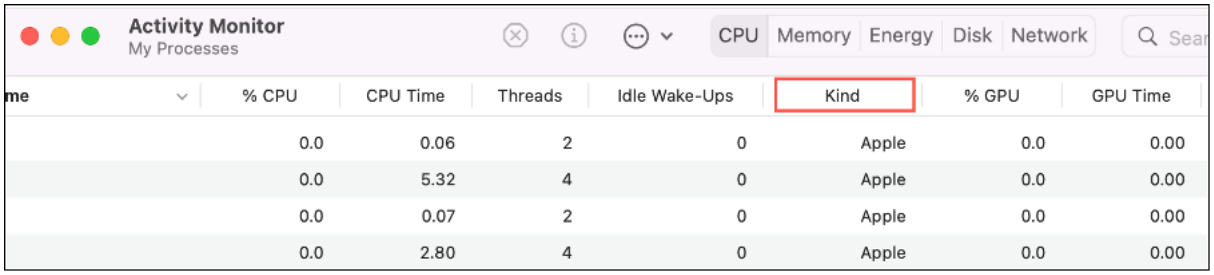
Apple シリコン（**M1** チップ）のネイティブサポート **-** ユニバーサルアーキテクチャ

macOS 向け Citrix Workspace アプリは、Apple シリコン（M1 チップ）を搭載した Mac をネイティブサポートするようになりました。デフォルトでは、Technical Preview ビルドは Apple シリコンを搭載した Mac でネイティブに実行され、M1 チップを使用して Mac にインストールし、テストする必要があります。ユニバーサルアーキテクチャビルドは、「Downloads」の「**Citrix Workspace App for macOS (Apple silicon) - Universal Architecture**」セクションからダウンロードできます。

> 注:
>
> Citrix は引き続き、Rosetta 2 ダイナミックバイナリトランスレーターを使用する Intel ベースの Mac をサポートします。ただし、Citrix は、Rosetta エミュレーションを使用する Mac 向け Citrix Workspace アプリを間もなく廃止します。「廃止」セクション記載のお知らせに注意してください。

Apple シリコン(M1 チップ)を実行している Mac で Citrix Workspace アプリを使用している場合は、「Downloads」の Citrix Web サイトから、Mac 用の HDX RealTime Media Engine 2.9.500 をインストールして、HDX RealTime Optimization Pack（RTOP）をアップグレードする必要があります。

Citrix Workspace アプリが Apple シリコンでネイティブに実行されているかどうかを確認するには、Mac でアクティビティモニタを開きます。［**CPU**］タブの ［**Kind**］列は、Workspace アプリが Apple Silicon または Intel プロセッサのどちらで実行されているかを示します。



ユニバーサルアーキテクチャビルドをアンインストールし、**Intel** ベースの **Mac** 向けの **Citrix Workspace** アプリをインストールする

ユニバーサルアーキテクチャビルドをアンインストールすることで、Intel ベースの Mac 向けの Citrix Workspace アプリに切り替えることができます。Citrix Workspace アプリをアンインストールするには、「アンインストール」セクションを参照してください。

アプリをアンインストールしたら、Intel ベース Mac 向け Citrix Workspace アプリの最新バージョンを Citrix のダウンロードページからダウンロードし、「手動インストール」セクションの手順に従います。

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（VCSDK）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 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（VDAPI）。VDAPI 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。
- 視覚的要素を強化し、ICA と統合されたサードパーティアプリケーションをサポートする Windows Monitoring API。
- プログラミングテクニックの実例となる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。

Apple シリコン（**M1** チップ）を搭載した **Mac** にカスタム仮想チャネルをロードする

エンドユーザーは、M1 チップセットを搭載した Mac にカスタム仮想チャネル SDK（VCSDK）を正常にロードできます。ユニバーサルアーキテクチャでは、M1 チップセットデバイス上の最新の VCSDK を使用してカスタム仮想チャネルを再コンパイルし、Apple シリコンを搭載した Mac に VCSDK をロードする必要があります。ユニバーサルアーキテクチャビルドは、「Downloads」の「**Virtual Channel SDK 2204 for macOS (Apple silicon) - Universal Architecture**」セクションからダウンロードできます。

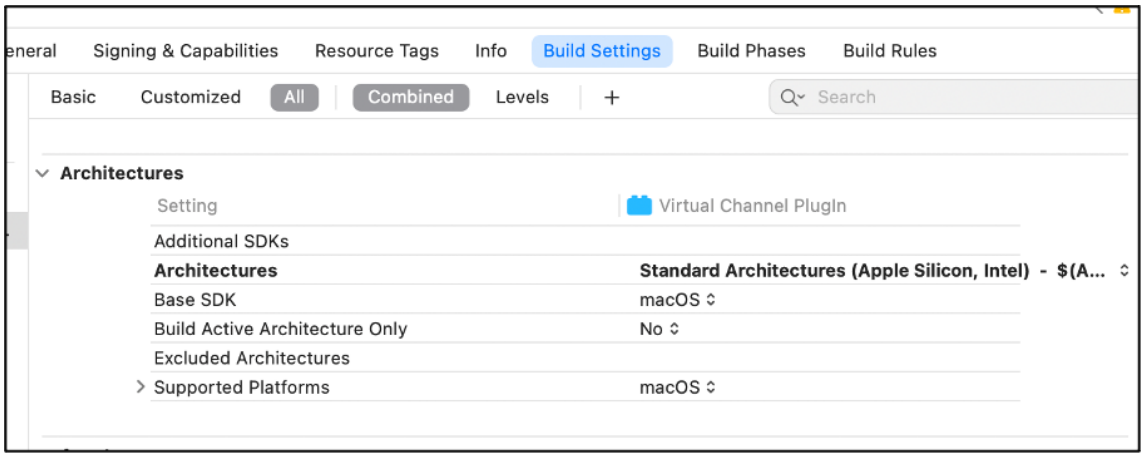
VCSDK をロードするには、次の手順を実行します:

1. 「Downloads」から macOS 用の Virtual Channel SDK 2204 をダウンロードします。
2. Xcode でカスタム仮想チャネルプロジェクトを開きます。
3. コードを変更します。
4. カスタム仮想チャネルをコンパイルして、仮想チャネルバンドルを生成します。

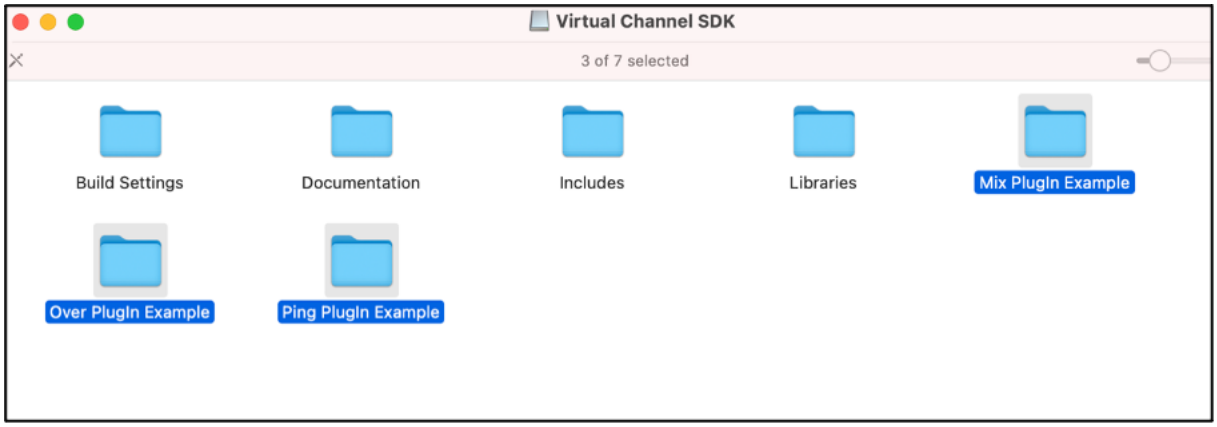
仮想チャネルソフトウェア開発キット（**VCSDK**）をテストする

Citrix 仮想チャネルソフトウェア開発キット（VCSDK）を使用している場合は、カスタマイズした仮想チャネルが正しく実行されるように、いくつかの変更を加える必要があります。VCSDK をテストするには、次の手順を実行します:

1. カスタマイズした仮想チャネルのリンクされたライブラリがすべてユニバーサルバイナリ用にコンパイルされていることを確認します。
2. ユニバーサルバイナリをサポートするようにプロジェクトファイルを変更します:
   - [**Project**] > [**Build Settings**] を開きます。
   - [**Architectures**] を [**Standard Architectures**] に設定します。



VCSDK の例は、*VCSDK.dmg* 内にあります。これらの例は、Apple シリコンと Intel ベース Mac コンピューターの両方でネイティブに実行される Apple のユニバーサル macOS バイナリをサポートしています。これは、両方のアーキテクチャの実行可能コードが含まれているためです。これらの例をリファレンスとして使用できます。



制限事項

この Technical Preview では、Web ブラウザーでのサービス継続性はサポートされていません。

> 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ケースは受け付けられませんが、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。ベータビルドは実稼働環境に展開しないことをお勧めします。

システム要件と互換性

May 14, 2022

サポートされるオペレーティングシステム

Mac 向け Citrix Workspace アプリは、以下のオペレーティングシステムをサポートします:

- macOS Monterey（12.3.1 まで）
- macOS Big Sur 11（マイナーおよびパッチバージョンを含む）
- macOS Catalina（10.15）

互換性のある **Citrix** 製品

Mac 向け Citrix Workspace アプリは、以下の 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詳しくは、Citrix 製品マトリクスを参照してください。

互換性のあるブラウザー

Mac 向け Citrix Workspace アプリは、次のブラウザーと互換性があります:

- Safari 7.0 以降
- Mozilla Firefox 22.x 以降
- Google Chrome 28.x 以降

ハードウェア要件

- 269MB 以上の空きディスク領域
- サーバーに接続するためのネットワークまたはインターネット接続

ソフトウェア要件

- Mac 向け Citrix Workspace アプリを展開するには:
  - Citrix Workspace for Web 2.1、2.5、および 2.6
- StoreFront:
  Mac 向け Citrix Workspace アプリまたは Web ブラウザーからアプリにアクセスする場合は、StoreFront 2.x 以降。

接続、証明書、認証

接続

Mac 向け Citrix Workspace アプリは、Citrix Virtual Apps and Desktops および Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）への以下の接続をサポートします:

- HTTPS
- ICA-over-TLS

Mac 向け Citrix Workspace アプリは以下の構成をサポートします:

LAN 接続	セキュリティ保護されたリモートまたはローカルの接続
StoreFront サービスサイトまたは Citrix Receiver for Web サイトを使用する StoreFront。	Citrix Gateway 10.5～12.0（VPX を含む）。Enterprise Edition 9.x～10.x（VPX を含む）。VPX。

証明書

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。その後、Mac 向け Citrix Workspace アプリを使用して Citrix リソースに正常にアクセスできます。

> 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、ローカルのキーストアにルート証明書が含まれていないため、信頼されていない機関からの証明書に関する警告が表示されます。ユーザーが警告に対してそのまま続行することを選択した場合、アプリケーションの一覧が表示されます。ただし、アプリケーションの起動は失敗します。

Mac 向け Citrix Workspace アプリデバイスへのルート証明書のインポート

証明書の発行者のルート証明書を取得して、デバイスに設定されているアカウントに電子メールで送信します。添付ファイルをクリックすると、ルート証明書をインポートするかどうかを確認するメッセージが表示されます。

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。Mac 向け Citrix Workspace アプリでは、ワイルドカード証明書がサポートされています。

中間証明書と Citrix Gateway

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関連付ける必要があります。このタスクについて詳しくは、Citrix Gatewayのドキュメントを参照してください。証明書のインストール、リンク、更新について詳しくは、「中間証明書を Citrix Gateway にインストールしてプライマリ CA とリンクする方法」を参照してください。

サーバー証明書検証ポリシー

Mac 向け 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 Mac 向け 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、接続できない可能性があります:
>
> - 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

Mac 向け Citrix Workspace アプリは、サーバー証明書を検証する時にサーバー（またはゲートウェイ）が提供するすべての証明書を使用するようになりました。以前の Mac 向け Citrix Workspace アプリリリース同様、証明書が信頼済みかについても確認します。すべての証明書が信頼済みでない場合、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、Mac 向け Citrix Workspace アプリの接続に失敗することがあります。

以下は、ゲートウェイがこのような有効な証明書で構成されていることを前提としています。この構成は、Mac 向け Citrix Workspace アプリで使用されるルート証明書を正確に確認するために、より厳格な検証が必要なユーザーにお勧めします：

- 「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」

次に、Mac 向け 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。Mac 向け Citrix Workspace アプリが「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。Mac 向け 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」を構成すると、これらのユーザーデバイスで Mac 向け 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。ルート証明書の有効期限についても注意してください。
>
> 注
>
> 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。

以下は、ゲートウェイがこのような有効な証明書で構成されていることを前提としています。通常は、このルート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」

Mac 向け 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。次に、ユーザーデバイスでルート証明書を検索します。「ルート証明書サンプル」など、正しく検証される信頼された機関からの証明書が見つかった場合、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、Mac 向け Citrix Workspace アプリが必要とする中間証明書が提供されますが、Mac 向け 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、Mac 向け 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、ゲートウェイは通常、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
>
> 一部の認証機関は、複数のルート証明書が存在する状況では、クロス署名の中間証明書を使用します 。以前のルート証明書は、新しいルート証明書と同時に使用されています。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。
>
> 注
>
> クロスルート用中間証明書およびルート証明書は、同じサブジェクト名（発行先）ですが、クロスルート中間証明書には異なる発行者名（発行元）があります。これによって、クロスルート用中間証明書と通常の中間証明書（「中間証明書サンプル 2」など）を区別できます。

通常は、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、Mac 向け 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。

認証

StoreFront への接続では、Mac 向け Citrix Workspace アプリで以下の認証方法がサポートされます:

	Workspace for Web（ブラウザー環境）	StoreFront サービスサイト（ネイティブ）	StoreFront XenApp Services サイト（ネイティブ）	Citrix Gateway から Workspace for Web（ブラウザー）	Citrix Gateway から StoreFront サービスサイト（ネイティブ）
匿名	はい	はい			
ドメイン	はい	はい		はい *	はい *
ドメインパススルー					
セキュリティトークン				はい *	はい *
2 要素認証（ドメイン + セキュリティトークン）				はい *	はい *
SMS				はい *	はい *
スマートカード	はい	はい		はい *	はい
ユーザー証明書				はい	はい（Citrix Gateway Plug-in）

* Citrix Gateway が動作する環境でのみ使用できます（デバイスへの関連プラグインのインストールは不要）。

インストール、アンインストール、およびアップグレード

June 10, 2022

Mac 向け Citrix Workspace アプリは単一のインストールパッケージで提供されており、Citrix Gateway および Secure Web Gateway を使用したリモートアクセスをサポートしています。

Mac 向け Citrix Workspace アプリを以下のいずれかの方法でインストールできます:

- Citrix の Web サイトからインストール
- Workspace for Web サイトからの自動インストール

- ESD（Electronic Software Delivery：電子ソフトウェア配信）ツールによるインストール

Citrix Workspace アプリが ［**Applications**］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。インストールパスは次のとおりです：

- フルインストール - ”/Applications/Citrix\ Workspace.app/”
- Mac 向け Citrix Workspace アプリ実行ファイル - ”/Applications/Citrix\ Workspace.app/Contents/MacOS/Citrix\ Workspace”

手動インストール

ユーザーによる **Citrix.com** からのインストール

初めて使用する場合、Mac 向け Citrix Workspace アプリを Citrix.com または社内のダウンロードサイトからダウンロードできます。アカウントをセットアップするときに、サーバーの URL の代わりにメールアドレスを入力できます。メールアドレスに関連付けられた Citrix Gateway や StoreFront サーバーが Mac 向け Citrix Workspace アプリにより識別され、ログオン用のメッセージが表示されてインストールを続行します。この機能は、メールアドレスによるアカウント検出と呼ばれます。

> 注：
>
> 初めて使用するユーザーとは、デバイスに Mac 向け Citrix Workspace アプリをインストールしていないユーザーを指します。

Citrix.com 以外の場所（Citrix Receiver for Web サイトなど）からダウンロードした場合は、メールアドレスによるアカウントセットアップを使用できません。

Mac 向け Citrix Workspace アプリの構成が必要な環境では、ほかの方法でアプリをユーザーに配布してください。

ESD（**Electronic Software Delivery**：電子ソフトウェア配信）ツールによるインストール

Mac 向け Citrix Workspace アプリを初めて使用するユーザーがアカウントをセットアップするには、サーバーの URL を入力する必要があります。

Citrix のダウンロードページ

管理者は、Mac 向け Citrix Workspace アプリをネットワーク共有を使用してインストールできます。または、直接ユーザーデバイスにインストールできます。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、アプリをインストールできます。

Mac 向け Citrix Workspace アプリをインストールするには：

1. シトリックス社の Web サイトから、適切なバージョンの Mac 向け Citrix Workspace アプリの DMG ファイルをダウンロードし、
2. ダウンロードしたファイルを開きます。
3. ［はじめに］ページで ［続ける］をクリックします。

4. ［使用許諾契約］ページで ［続ける］をクリックします。
5. 使用許諾契約の内容を確認して、［同意する］をクリックします。
6. ［インストールの種類］ページで、［インストール］をクリックします。
7. ［アカウントの追加］ページで、［アカウントの追加］を選択してから ［続行］をクリックします。
8. ローカルデバイスに管理者のユーザー名とパスワードを入力します。

アンインストール

Mac 向け Citrix Workspace アプリは.dmg ファイルを開いて手動でアンインストールできます。［**Citrix Workspace** アプリのアンインストール］を選択して、画面に表示される指示に従って操作します。DMG ファイルは、Mac 向け Citrix Workspace アプリを初めてインストールするときにシトリックスのサイトからダウンロードされるファイルです。ファイルがコンピューター上に見つからない場合は、Citrix のダウンロードから再度ダウンロードして、アプリケーションをアンインストールします。

アップグレード

Mac 向け Citrix Workspace アプリから、既存バージョンの更新または新しいバージョンへのアップグレードが利用可能になったときに通知が送信されます。

Mac 向け Citrix Workspace アプリは、以前のどのバージョンからもアップグレードできます。

Mac 向け Citrix Workspace アプリの新しいバージョンにアップグレードすると、以前のバージョンは自動的にアンインストールされます。マシンを再起動する必要はありません。

アップデート

February 21, 2022

手動更新

Mac 向け Citrix Workspace アプリを手動で更新するには、Citrix ダウンロードページから最新バージョンのアプリをダウンロードしてインストールします。

自動更新

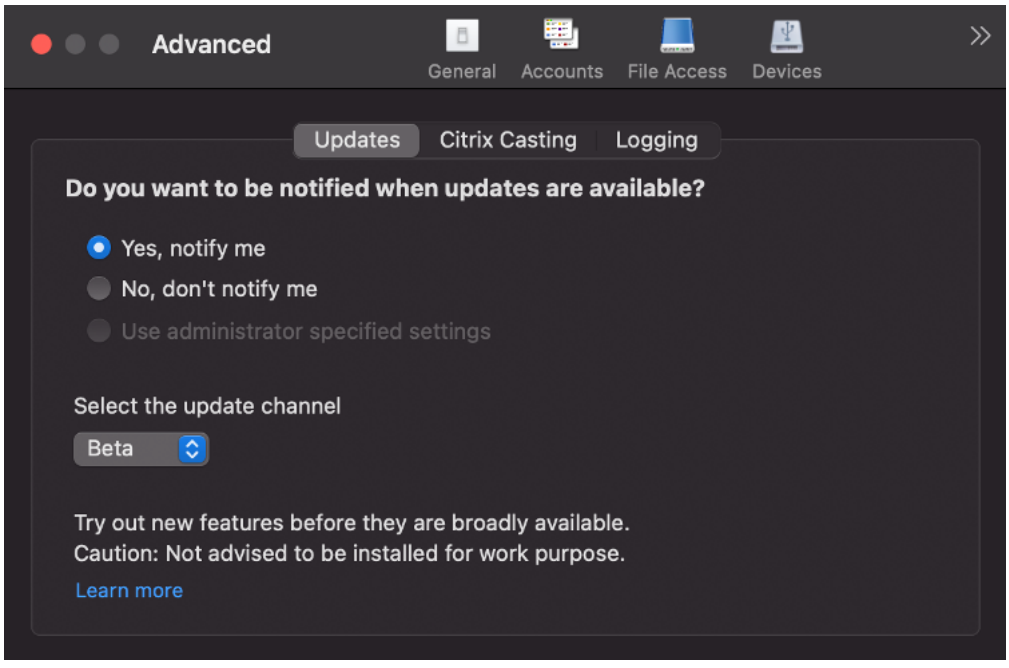
新しいバージョンの Citrix Workspace アプリがリリースされると、Citrix Workspace アプリがインストールされたシステムで更新がプッシュされます。利用可能な更新プログラムが通知されます。

> 注:
>
> - 送信プロキシをインターセプトするよう SSL を構成している場合、Workspace の自動更新署名サービス（https://citrixupdates.cloud.com/）およびダウンロード場所（https://downloadplugins.citrix.com/）に例外を追加して Citrix からの更新を受信します。
> - 更新を受信するには、システムがインターネットに接続している必要があります。
> - Web 向け Workspace のユーザーは、StoreFront ポリシーを自動的にダウンロードできません。
> - Citrix Workspace の更新に macOS 用の HDX RTME が含まれています。Citrix Workspace アプリで使用可能な HDX RTME の更新に関する通知を受け取ります。
> - バージョン 2111 から、Citrix Workspace の更新ログのパスが変更されています。Workspace の更新ログは /Library/Logs/Citrix Workspace Updaterにあります。ログの収集について詳しくは、「ログ収集」セクションを参照してください。

Citrix Workspace アプリのベータプログラムのインストール

Citrix Workspace アプリが自動更新用に構成されている場合は、更新通知を受け取ります。システムにベータビルドをインストールするには、次の手順を実行します:

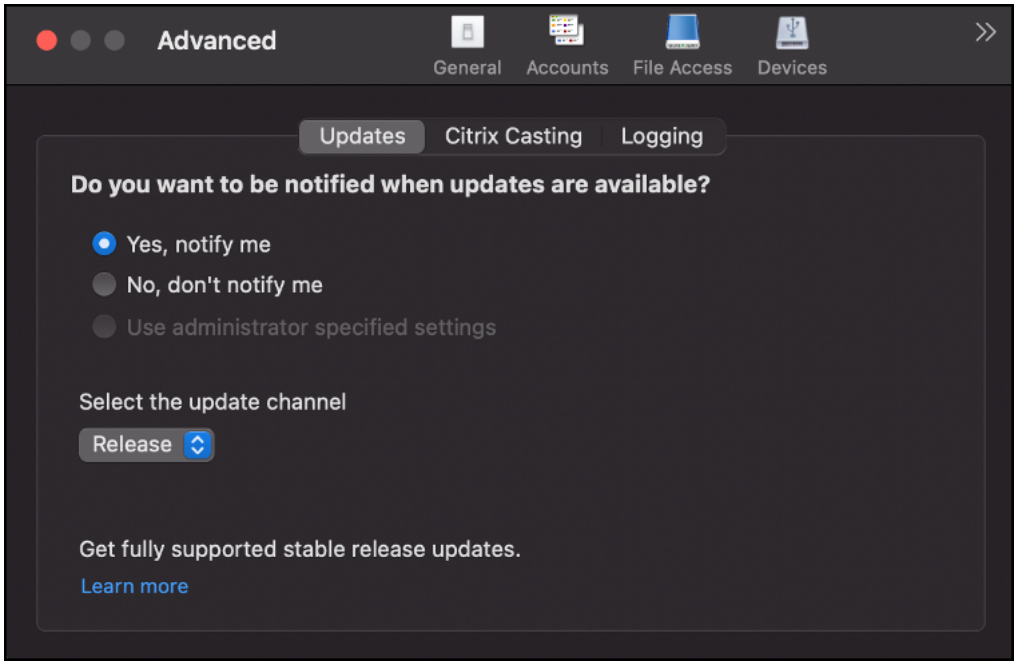
1. Citrix Workspace アプリを開きます。
2. システムトレイで Citrix Workspace を右クリックし、［環境設定］ > ［詳細］をクリックします。
3. ベータビルドが利用可能になったら、ドロップダウンリストから ［ベータ版］を選択します。



ベータビルドからリリースビルドに切り替えるには、次の手順を実行します:

1. Citrix Workspace アプリを開きます。
2. システムトレイで Citrix Workspace を右クリックし、［環境設定］ > ［詳細］をクリックします。

3. ［更新チャネルを選択します］ドロップダウンリストから ［リリース］を選択します。



> 注:
>
> ベータビルドは、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、フィードバックを共有するためのものです。ベータビルドのサポートケースは受け付けていませんが、機能向上のためのフィードバックは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。ベータビルドは実稼働環境に展開しないことをお勧めします。

自動更新の詳細設定（**Citrix Workspace** の更新）

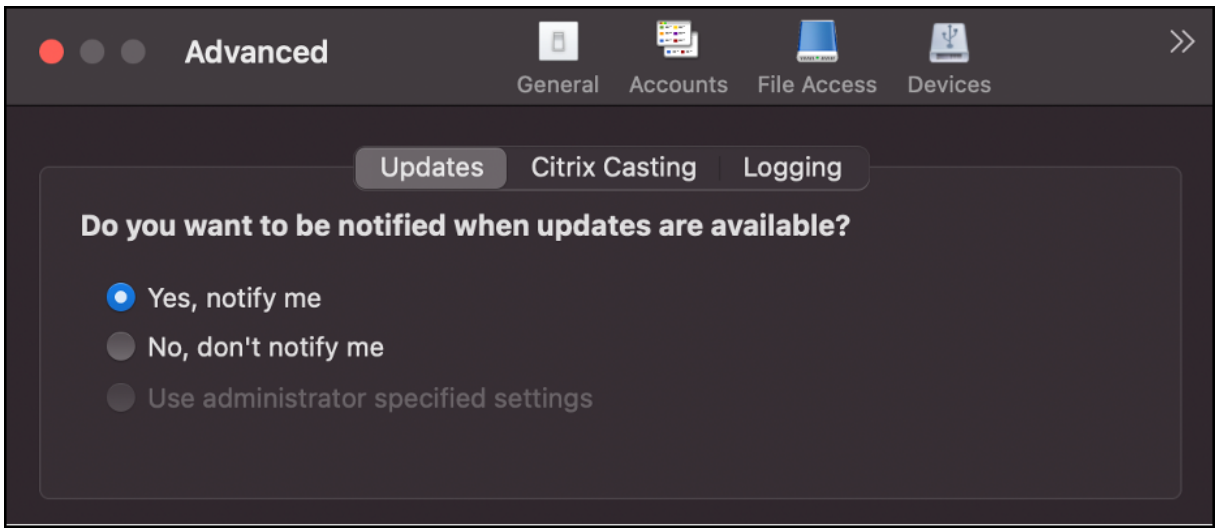
Citrix Workspace の更新は、次の方法で構成できます:

1. GUI
2. StoreFront

GUI を使用した **Citrix Workspace** の更新プログラムの構成

個々のユーザーは、［詳細］設定ダイアログボックスの Citrix Workspace の更新プログラム設定（ユーザーごとの構成で、現在のユーザーにのみ適用される設定）を上書きできます。GUI を使用して更新プログラムを構成するには、次の手順を実行します:

1. Mac で Citrix Workspace アプリヘルパーアイコンを選択します。
2. ドロップダウンリストから、［環境設定］ > ［詳細］を選択します。
3. 更新通知設定を選択し、ウィンドウを閉じます。



StoreFront を使用した **Citrix Workspace** 更新プログラムの構成

1. テキストエディターを使用して、web.configファイル（通常C:\inetpub\wwwroot\Citrix\Roaming directoryにある）を開きます。
2. このファイルで、ユーザーアカウント要素の場所を見つけます（「Store」は使用環境のアカウント名です）。

   たとえば、次のようになります：<account id=... name="Store">

   </account>タグの前に、ユーザーアカウントのプロパティに移動します：

```
<properties>
       <clear/>
 </properties>
 <!--NeedCopy-->
```

3. *<clear />* タグの後に、自動更新タグを追加します。

```
<account>

    <clear />

    <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
        F84Store"

      description="" published="true" updaterType="Citrix"
         remoteAccessType="None">

```



```
<annotatedServices>

  <clear />

  <annotatedServiceRecord serviceRef="1__Citrix_F84Store">

    <metadata>

      <plugins>

        <clear />

      </plugins>

      <trustSettings>

        <clear />

      </trustSettings>

      <properties>

        <property name="Auto-Update-Check" value="auto" />

        <property name="Auto-Update-DeferUpdate-Count" value
           ="1" />

        <property name="Auto-Update-Rollout-Priority" value=
           "fast" />

            </properties>

    </metadata>

  </annotatedServiceRecord>

</annotatedServices>

<metadata>

  <plugins>

    <clear />

  </plugins>
```



```
52
53          <trustSettings>
54
55            <clear />
56
57          </trustSettings>
58
59          <properties>
60
61            <clear />
62
63          </properties>
64
65        </metadata>
66
67      </account>
68
69  <!--NeedCopy-->
```

以下は、プロパティの意味と使用可能な値の詳細です:

- **Auto-update-Check**: Citrix Workspace アプリが、利用可能な更新を自動的に検出したことを示します。
- **Auto-update-Rollout-Priority**:: 更新を受信できる配信期間を示します。
- **Auto-update-DeferUpdate-Count**: リリースの更新通知を延期できる回数を示します。

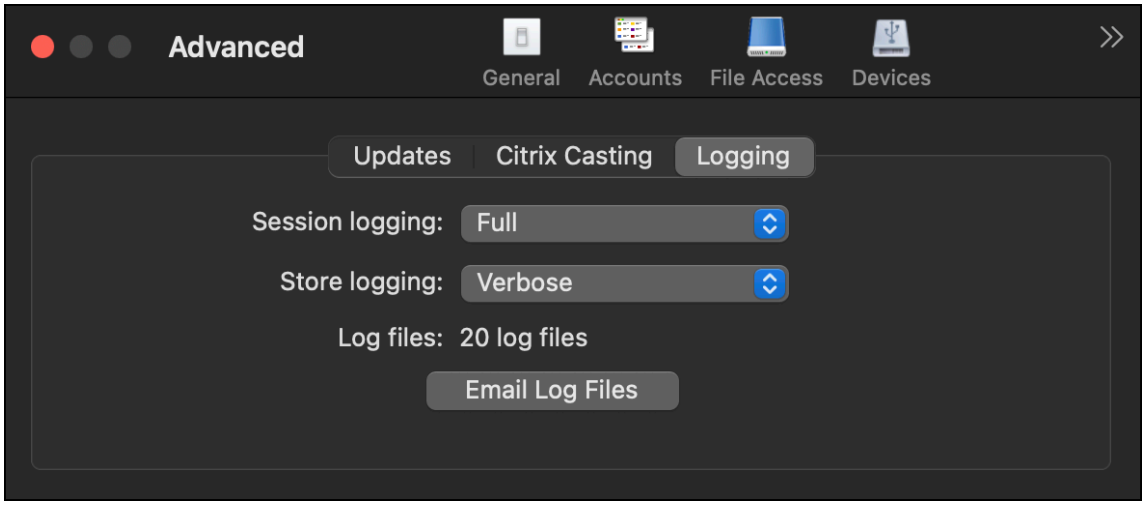
ログ収集

ログ収集では、Citrix Workspace アプリのログを収集するプロセスが簡素化されました。ログは、Citrix でのトラブルシューティングに役立ち、問題が複雑な場合はサポートを提供します。

GUI を使用してログを収集できます。

ログの収集:

1. Citrix Workspace アプリを開きます。
2. システムトレイで Citrix Workspace を右クリックし、［環境設定］ > ［詳細］をクリックします。
3. ［ログ］を選択します。



4. 次のセッションログレベルのいずれかを選択します:

   - 無効（デフォルト）: 基本的なトラブルシューティングのために、最小限のログが収集されます。
   - 接続診断: 接続中のエラーを識別します。セッションが成功したと見なされる時点まで、すべてのログが有効になります。
   - 完全: 接続診断を含むすべてをキャプチャします。有効にすると、Citrix Workspace アプリは最大 10 個のセッションログを保存し、その後、10 個のログを維持するために最も古いものから削除されます。

   > 注:
   >
   > ログのオプションとして ［完全］を選択すると、パフォーマンスに影響を与える可能性があります。データ量が多いため、問題のトラブルシューティング中にのみ使用します。通常の使用中はログで［完全］を有効にしないでください。このログレベルを有効にすると、警告ダイアログが表示されます。続行するには、このダイアログを確認する必要があります

5. 次のストアログレベルのいずれかを選択します:

   - 無効（デフォルト）: 基本的なトラブルシューティングのために、最小限のログが収集されます。
   - 標準: ストア通信ログのみが収集されます。
   - 詳細: 認証およびストア通信の詳細ログが収集されます。

6. ［ログファイルをメールで送信］クリックし、ログを収集して.zip ファイルとして共有します。

構成

June 13, 2022

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、Mac 向け Citrix Workspace アプリをインストールした後で、以下の構成を行う必要があります。

ユーザーは、インターネットまたはリモートの場所から接続します。こうしたユーザーは、Citrix Gateway を使用して認証を構成します。

管理者のタスクと注意事項

ここでは、Mac 向け Citrix Workspace アプリの管理者に関連するタスクと注意事項について説明します。

> 重要:
>
> macOS 10.15 を実行している場合は、システムが Apple 社のmacOS 10.15 での信頼された機関からの証明書の要件に準拠していることを確認してください。Mac 向け Citrix Workspace アプリバージョン 2106 にアップグレードする前に、この確認を行ってください。

フィーチャーフラグ管理

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

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

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

次の **URL** へのトラフィックを有効にする

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `Firehose.launchdarkly.com`
- `mobile.launchdarkly.com`

IP アドレスの許可リストを作成する

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

LaunchDarkly のシステム要件

Citrix ADC の分割トンネリングが以下のサービスに対して［オフ］に設定されている場合、アプリがこれらのサービスと通信できることを確認してください:

- LaunchDarkly サービス。
- APNs リスナーサービス

Sentry

Sentry は、アプリログを収集して問題やクラッシュを分析し、製品の品質を向上させるために使用されます。Citrix は、その他の個人ユーザー情報を収集または保存したり、機能分析データに Sentry を使用したりすることはありません。Sentry について詳しくは、「[https://sentry.io/welcome/]」を参照してください。

Content Collaboration サービスの統合

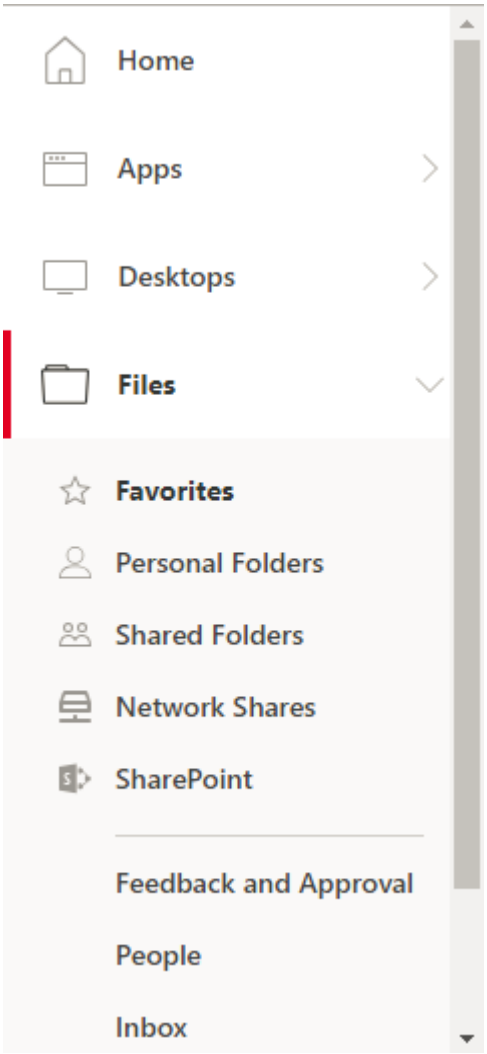
Citrix Content Collaboration を使用すると、ドキュメントを簡単かつセキュアに交換したり、メールで大容量のドキュメントを送信したり、サードパーティへのドキュメント転送をセキュアに処理したり、コラボレーションスペースにアクセスすることができます。

また、Web ベースのインターフェイス、モバイルクライアント、デスクトップアプリ、Microsoft Outlook や Gmail との統合など、Citrix Content Collaboration により、さまざまな方法で作業できます。

Citrix Content Collaboration 機能には、Citrix Workspace アプリの ［ファイル］タブからアクセスできます。この ［ファイル］タブは、Citrix Cloud コンソールのワークスペース構成で Content Collaboration サービスが有効になっている場合にのみ表示されます。

> 注:
>
> オペレーティングシステムでセキュリティオプションが設定されているため、Windows Server 2012 および Windows Server 2016 では、Citrix Content Collaboration の統合はサポートされていません。

次の図は、新しい Citrix Workspace アプリの ［ファイル］タブの例です:



制限事項

- Citrix Workspace アプリをリセットしても、Citrix Content Collaboration はログオフされません。
- Citrix Workspace アプリでストアを切り替えても、Citrix Content Collaboration はログオフされません。

USB リダイレクト

HDX USB デバイスリダイレクト機能を使用すると、USB デバイスのクライアント側へのリダイレクトおよびクライアント側からのリダイレクトが有効になります。ユーザーがデスクトップでホストされるアプリケーションや仮想デスクトップを使用しているときに、ローカルのユーザーデバイスに装着したフラッシュドライブにアクセスできるようになります。

セッション中、ユーザーは画像転送プロトコル（PTP）デバイスなどのデバイスを接続して使用できます。例:

- デジタルカメラ、デジタルオーディオプレーヤーやポータブルメディアプレーヤーなどのメディア転送プロトコル（MTP）デバイス。

- POS（Point-Of-Sale）デバイス、3D SpaceMouse、スキャナー、署名パッドなどのデバイス。

> 注:
>
> デスクトップでホストされるアプリケーションのセッションでは、ダブルホップ USB はサポートされません。

USB リダイレクトは、次のデバイスで使用できます:

- Windows
- Linux
- Mac

USB リダイレクトのデフォルトでは、特定のクラスの USB デバイスでのみ許可され、ほかのクラスのデバイスはリダイレクトされません。仮想デスクトップで使用可能な USB デバイスの種類を制限するには、リダイレクトがサポートされている USB デバイスの一覧を更新します。詳しくは、このセクションの後半で説明します。

> ヒント
>
> ユーザーデバイスとサーバーとの間でセキュリティを分離する必要がある場合は、避けるべき USB デバイスの種類についてユーザーに通知するようにしてください。

一般的な USB デバイスをリダイレクトするための仮想チャネルが最適化されており、WAN 接続でも良好なパフォーマンスが提供されます。低速な狭帯域幅接続では、最適化された仮想チャネルを使用することで最高のパフォーマンスが得られます。

> 注:
>
> Mac 向け Citrix Workspace アプリの USB リダイレクトで SMART ボードを使用する場合、マウスとして処理されます。

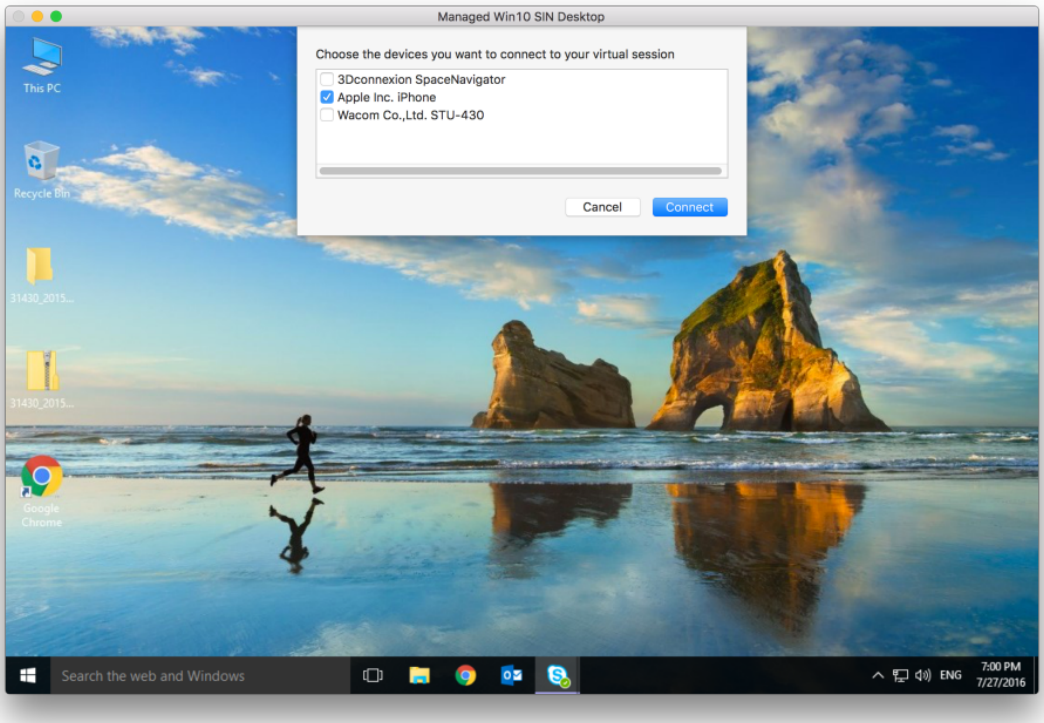
この製品は、USB 3.0 デバイスと USB 3.0 ポートを使用する最適化された仮想チャネルをサポートします。たとえば、CDM 仮想チャネルは、カメラ上でファイルを表示したり、ヘッドセットに音声を提供するために使用されます。USB 3.0 デバイスを USB 2.0 ポートに接続した場合も、汎用 USB リダイレクトがサポートされます。

Web カメラのヒューマンインターフェイスデバイス（HID）ボタンなど、一部のデバイス固有の機能は、最適化された仮想チャネルで正しく動作しない場合があります。代わりに、汎用 USB 仮想チャネルを使用してください。

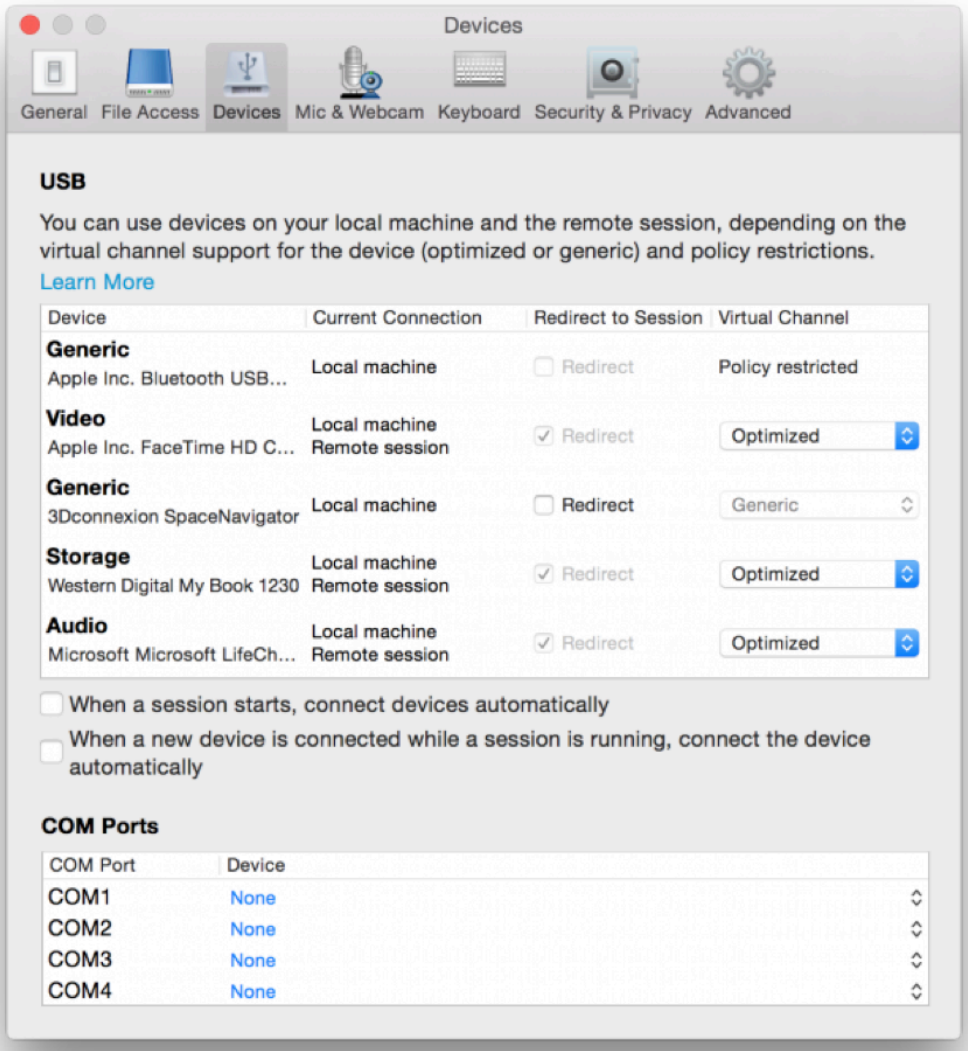
一部のデバイスはデフォルトではリダイレクトされず、ローカルセッションでのみ使用可能になります。たとえば、内部 USB で直接装着されたネットワークインターフェイスカード（NIC）は、リダイレクトには適しません。

USB リダイレクトを使用するには:

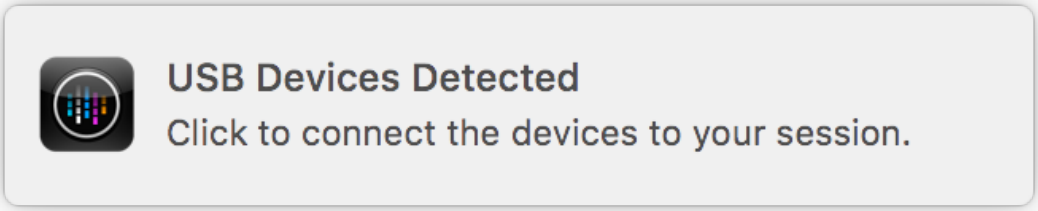
1. Mac 向け Citrix Workspace アプリがインストールされているデバイスに USB デバイスを接続します。
2. ローカルシステムで、使用できる USB デバイスを選択するメッセージが表示されます。



3. 接続するデバイスを選択して、［接続］をクリックします。接続できない場合は、エラーメッセージが表示されます。
4. ［環境設定］ウィンドウの ［デバイス］タブで、接続された USB デバイスが［USB］パネルに一覧表示されます：



5. USB デバイスの仮想チャネルの種類（汎用または最適化）を選択します。
6. メッセージが表示されます。クリックして USB デバイスをセッションに追加します:



USB デバイスの装着と取り外し

ユーザーは、仮想セッションの開始前および開始後に USB デバイスを装着できます。Mac 向け Citrix Workspace アプリでは、以下の点について考慮してください:

- セッションを開始した後で装着したデバイスは、Desktop Viewer の［USB］メニューに直ちに追加されます。
- USB デバイスが正しくリダイレクトされない場合、仮想セッションが開始されてからデバイスを装着することで問題が解決される場合があります。
- データの損失を避けるため、Windows で推奨される手順（［ハードウェアの安全な取り外し］メニューなど）に従って USB デバイスを取り外してください。

サポートされている **USB** デバイス

Apple がカーネル機能拡張（KEXT）の廃止を発表したことで、Mac 向け Citrix Workspace アプリは Apple が提供する新しいユーザーモードの USB フレームワーク`IOUSBHost`に移行しました。この記事では、サポートされている USB デバイスを一覧表示します。

USB リダイレクトと互換性がある **USB** デバイス

次の USB デバイスは、USB リダイレクトとシームレスに連携します:

- 3DConnexion SpaceMouse
- 大容量記憶装置デバイス
- Kingston DataTraveler USB フラッシュドライブ
- Seagate 外付け HDD
- Kingston/Transcend フラッシュドライブ 32GB/64GB
- NIST PIV スマートカード/リーダー
- YubiKey

USB リダイレクトで失敗する **USB** デバイス

次のデバイスは USB リダイレクトと互換性がありません:

- Transcend SSD 外付けハードディスク

未確認の **USB** デバイス

Mac 向け Citrix Workspace アプリで USB リダイレクトが成功するかを Citrix が検証していないデバイスはたくさんあります。これらのデバイスの一部を次に示します:

- その他のハードディスク
- カスタム HID プロトコルを使用するキーボードとヘッドセットの特殊キー

大容量記憶装置デバイスのサポート

一部のタイプの大容量記憶装置デバイスは、正常にリダイレクトできないことが報告されています。リダイレクトに失敗したデバイスには、クライアントドライブマッピングと呼ばれる最適化された仮想チャネルがあります。クライアントドライブマッピングを使用すると、大容量記憶装置デバイスへのアクセスは、Delivery Controller のポリシーで制御できます。

アイソクロナスデバイスのサポート

汎用 USB リダイレクトは、Mac 向け Citrix Workspace アプリのアイソクロナスクラスの USB デバイスをサポートしていません。USB 仕様におけるデータ転送のアイソクロナスモードとは、タイムスタンプ付きデータを一定の速度でストリーミングするデバイスのことです。例：Web カメラ、USB ヘッドホンなど

複合デバイスのサポート

USB 複合デバイスは、複数の機能を実行できる単一のガジェットです。例：マルチ機能プリンター、iPhone など。現在、Mac 向け Citrix Workspace アプリは、Citrix Virtual Apps and Desktops および Citrix DaaS セッションへの複合デバイスのリダイレクトをサポートしていません。

サポートされていない **USB** デバイス用の代替手段

汎用 USB リダイレクトでサポートされていないデバイスを処理できる最適化された仮想チャネルがあります。これらの仮想チャネルは、汎用 USB リダイレクトと比較すると速度が最適化されています。以下は、いくつかの例です：

- **Web** カメラリダイレクト：未処理の Web カメラトラフィックデータに最適化されています。Microsoft Teams Optimization Pack には、独自の Web カメラリダイレクト方法があります。この場合、Web カメラリダイレクト仮想チャネルは利用できません。
- オーディオリダイレクト：オーディオストリームを転送するように最適化されています。
- クライアントドライブマッピング：大容量記憶装置デバイスを Citrix Virtual Apps and Desktops および Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）セッションにリダイレクトするように最適化されています。例：フラッシュドライブ、ハードディスク、DVD ROM/RW など。

Enlightened Data Transport（EDT）

Mac 向け Citrix Workspace アプリでは、デフォルトで EDT が有効になっています。

Mac 向け Citrix Workspace アプリは、デフォルトの.ica ファイルに設定された **EDT** 設定を読み取り、適切に適用します。

EDT を無効にするには、ターミナルで次のコマンドを実行します：

```
defaults write com.citrix.receiver.nomas HDXOverUDPAllowed -bool NO
```


セッション画面の保持機能およびクライアントの自動再接続機能

セッション画面の保持機能は、ICA セッションをアクティブのまま保持し、ネットワークの接続が切断されても、セッションの画面を表示したままにできます。ユーザーは、接続が回復するまでセッション画面を見ることができます。

セッション画面の保持機能を有効にすると、データを損失することなく、サーバー上のセッションがアクティブのまま保持されます。ネットワークが中断されると、セッション画面が停止するため、ユーザーにもネットワークが切断されていることがわかります。また、セッションに再接続するときに再認証用のログオン画面が表示されないため、ユーザーは即座に作業を再開できます。

> 重要
>
> - Mac 向け Citrix Workspace アプリのユーザーは、サーバー側の設定を上書きできません。
> - 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。

セッション画面の保持機能とともに、TLS（Transport Layer Security）を使用できます。

> 注
>
> TLS は、ユーザーデバイスと Citrix Gateway 間で送信されるデータのみを暗号化します。

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許可または禁止します。

［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。この時間を長く設定することもできますが、この機能はユーザーに利便性を提供します。したがって、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
>
> セッション画面の保持のタイムアウトを延長すると、ユーザーの気が散ってデバイスから離れたときに、許可されていないユーザーがセッションにアクセスできるようになる可能性があります。

デフォルトでは、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。このポート番号はポリシーの［セッション画面の保持のポート番号］設定で変更できます。

［クライアントの自動再接続時の認証］ポリシー設定を構成して、中断されたセッションにユーザーが再接続するときに再認証を要求することができます。

セッション画面の保持機能とクライアントの自動再接続機能を一緒に使用する場合は、次のように処理されます。まず、ネットワークが切断されると、セッション画面の保持機能により、セッションがアクティブのままサーバー上に保持されます。［セッション画面の保持のタイムアウト］ポリシー設定で指定した時間が経過すると、サーバー上のセッションが終了または切断されます。この後でクライアントの自動再接続のポリシー設定が有効になり、切断セッションへの再接続が行われます。

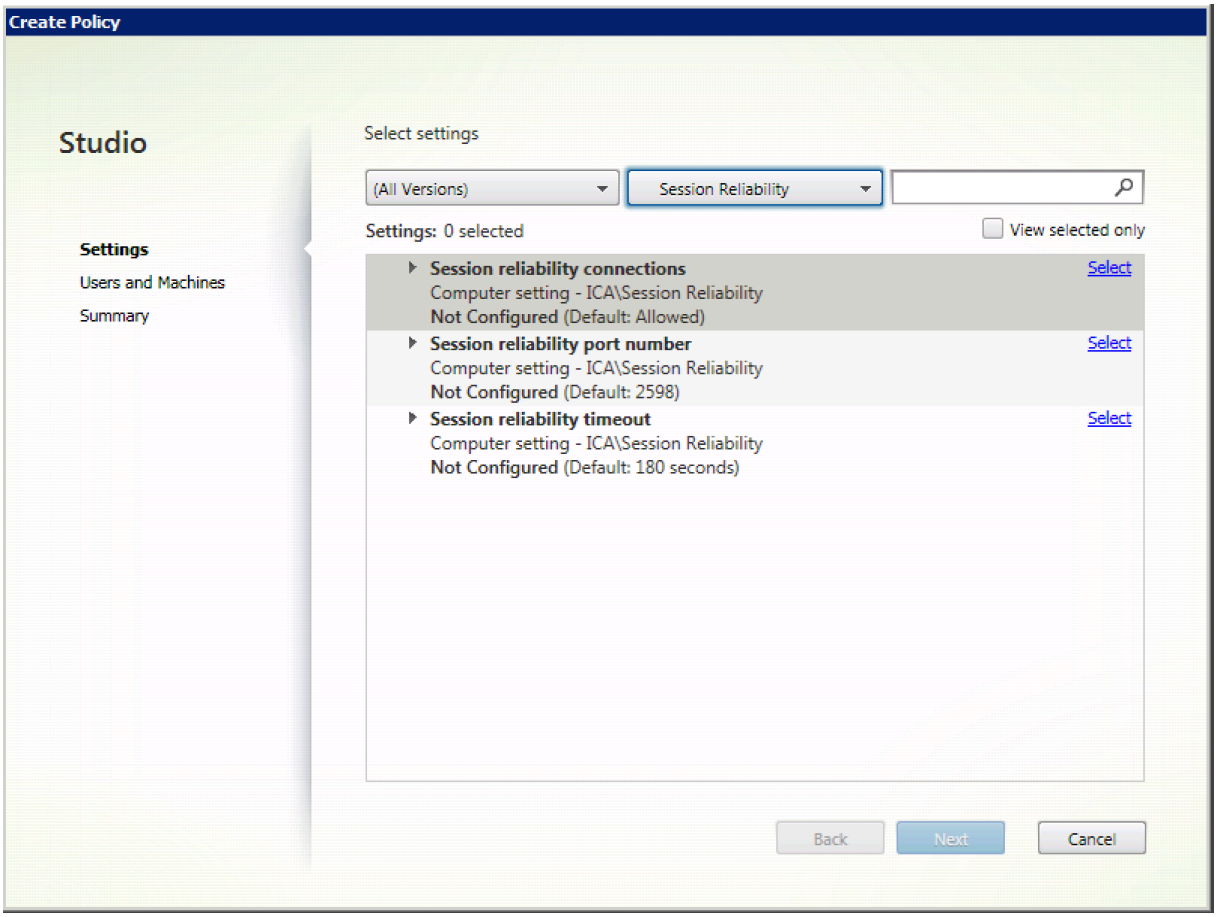
> 注
>
> セッション画面の保持は、サーバーでデフォルトで有効になっています。この機能を無効にするには、サーバーで管理するポリシーを構成します。

Citrix Studio からセッション画面の保持を設定する

デフォルトでは、セッション画面の保持機能は有効になっています。

セッション画面の保持を無効にするには:

1. Citrix Studio を起動します。
2. [セッション画面の保持] ポリシーを開きます。
3. ポリシーを [禁止] に設定します。



セッション画面の保持のタイムアウトを設定する

デフォルトでは、セッション画面の保持のタイムアウトは 180 秒に設定されています。

> 注:
>
> セッション画面の保持のタイムアウトポリシーは、XenApp および XenDesktop 7.11 以降でのみ構成できます。

セッション画面の保持のタイムアウトを変更するには:

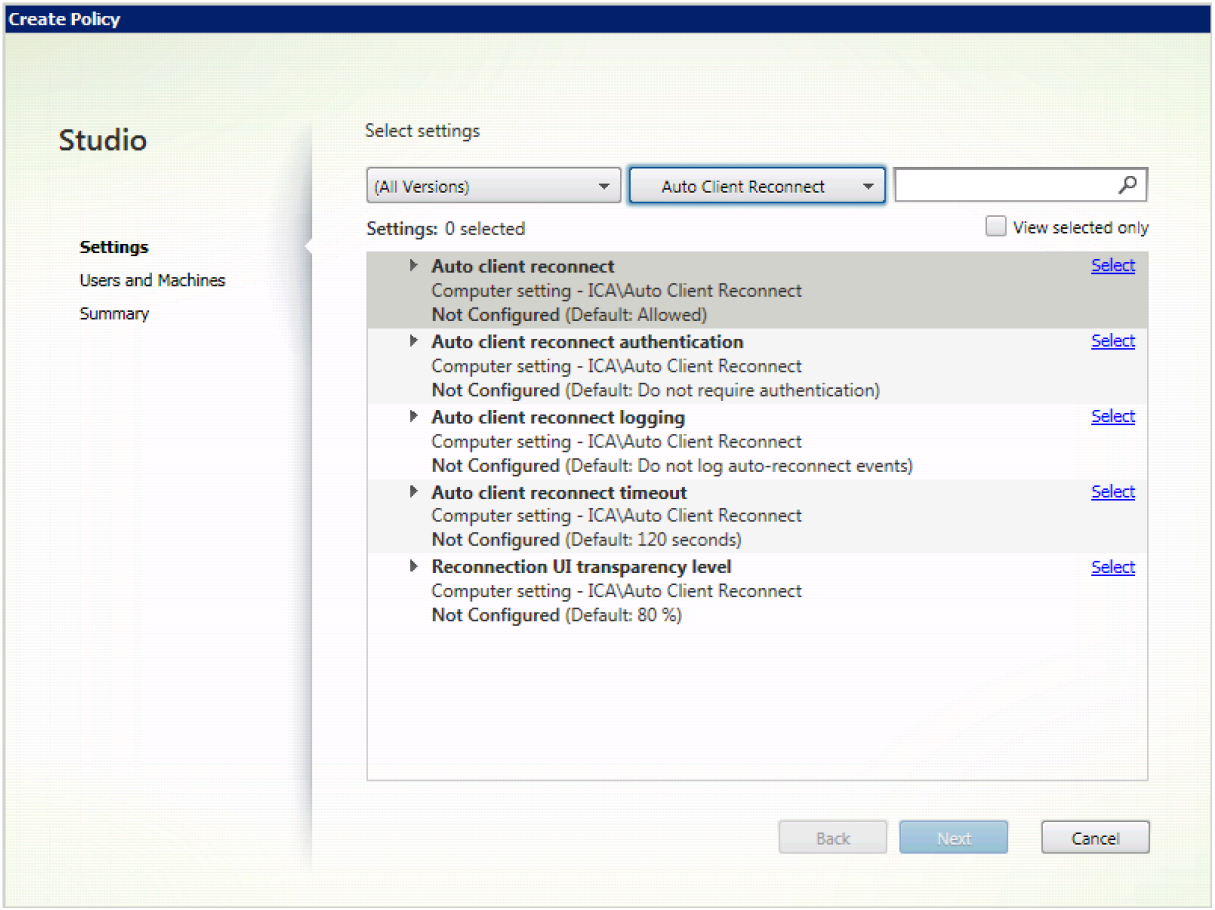
1. Citrix Studio を起動します。
2. [セッション画面の保持のタイムアウト] ポリシーを開きます。
3. タイムアウト値を編集します。
4. [**OK**] をクリックします。

Citrix Studio を使用してクライアントの自動再接続を設定する

デフォルトでは、自動再接続機能は有効になっています。

自動再接続を無効にするには:

1. Citrix Studio を起動します。
2. [クライアントの自動再接続] ポリシーを開きます。
3. ポリシーを [禁止] に設定します。



クライアントの自動再接続のタイムアウトを設定する

デフォルトでは、クライアントの自動再接続のタイムアウトは 120 秒に設定されています。

> 注:
>
> クライアントの自動再接続のタイムアウトポリシーは、XenApp および XenDesktop 7.11 以降でのみ構成できます。

クライアントの自動再接続のタイムアウトを変更するには:

1. Citrix Studio を起動します。
2. [クライアントの自動再接続] ポリシーを開きます。
3. タイムアウト値を編集します。
4. [**OK**] をクリックします。

> 制限事項:
>
> Mac 向け Citrix Workspace アプリは、ターミナルサーバーの VDA で、ユーザー設定に関係なくタイムアウト値に 120 秒を使用します。

再接続ユーザーインターフェイスの透明度を設定する

セッションのユーザーインターフェイスは、セッション画面の保持およびクライアントの自動再接続の試行中に表示されます。ユーザーインターフェイスの透明度は、Studio のポリシーを使用して変更できます。

デフォルトでは、再接続 UI の透明度は、80 に設定されています。

再接続ユーザーインターフェイスの透明度を変更するには:

1. Citrix Studio を起動します。
2. [再接続 **UI** の透過レベル] ポリシーを開きます。
3. 値を編集します。
4. [**OK**] をクリックします。

クライアントの自動再接続とセッション画面の保持の操作

さまざまなアクセスポイント間の切り替え、ネットワークの中断、遅延に関連したタイムアウトの表示など、モバイルには多数の課題があります。このため、Mac 向け Citrix Workspace アプリのアクティブなセッションでリンクの整合性を保持しようとすると問題が発生することがあります。Citrix の強化されたセッション画面の保持および自動再接続テクノロジーがこの問題を解決します。

この機能により、ユーザーはネットワークの中断から回復した後、セッションに自動的に再接続できます。これらの機能は、Citrix Studio のポリシーで有効にでき、ユーザーエクスペリエンスを向上します。

> 注:
>
> クライアントの自動再接続およびセッション画面の保持のタイムアウト値は、StoreFront の **default.ica** フ

> ァイルを使用して変更できます。

クライアントの自動再接続

クライアントの自動再接続は、Citrix Studio ポリシーで有効または無効にできます。この機能は、デフォルトで有効になります。このポリシーの変更について詳しくは、この記事で前述されたクライアントの自動再接続に関するセクションを参照してください。

StoreFront でデフォルトの.ica ファイルを使用して、AutoClienreconnect の接続タイムアウトを変更します。デフォルトでは、タイムアウトは 120 秒（2 分）に設定されています。

設定	例	デフォルト
TransportReconnectRetryMaxT:	TransportReconnectRetryMaxT:	120

セッション画面の保持

セッション画面の保持機能の有効または無効の設定は、Citrix Studio ポリシーで行います。この機能は、デフォルトで有効になります。

StoreFront の **default.ica** ファイルを使用して、セッション画面の保持の接続タイムアウトを変更します。デフォルトでは、このタイムアウトは 180 秒（3 分）に設定されています。

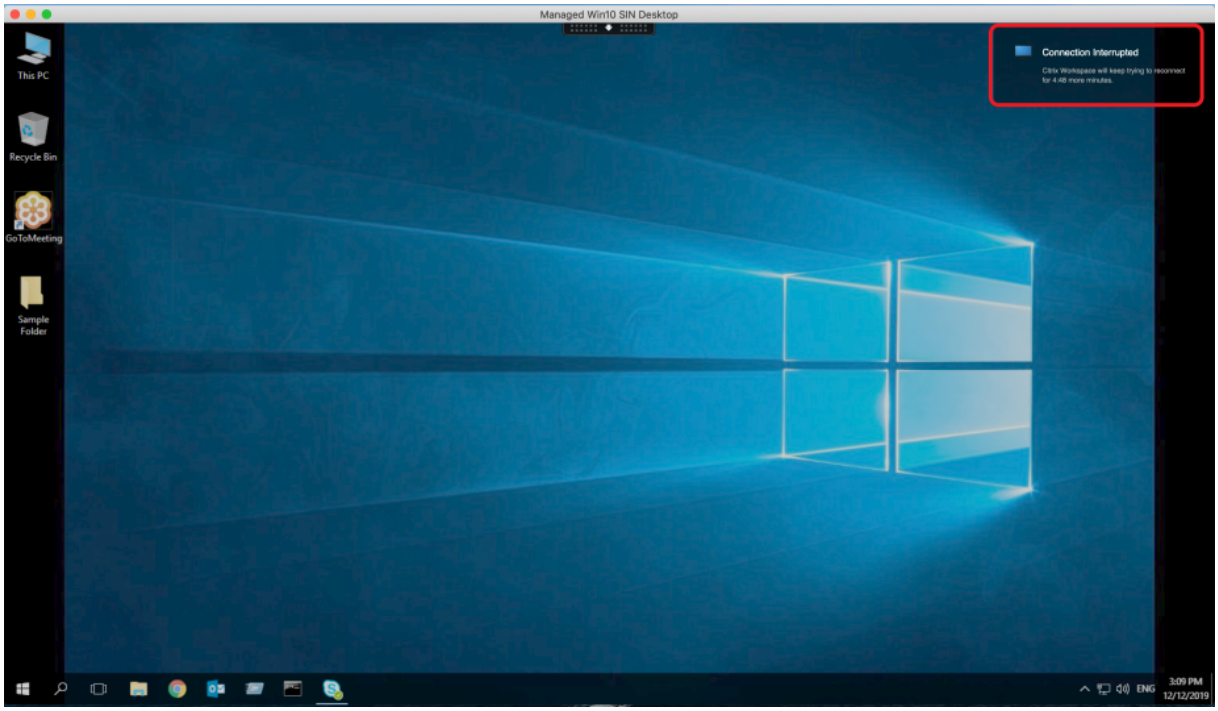
設定	例	デフォルト
SessionReliabilityTTL	SessionReliabilityTTL=120	180

クライアントの自動再接続およびセッション画面の保持の仕組み

Mac 向け Citrix Workspace アプリでクライアントの自動再接続機能およびセッション画面の保持機能を有効にする場合、以下に注意してください：

- 再接続中は、セッションウィンドウが灰色になります。セッションを再接続するまでの残り時間がカウントダウンタイマーで表示されます。セッションがタイムアウトになると、接続は切断されます。

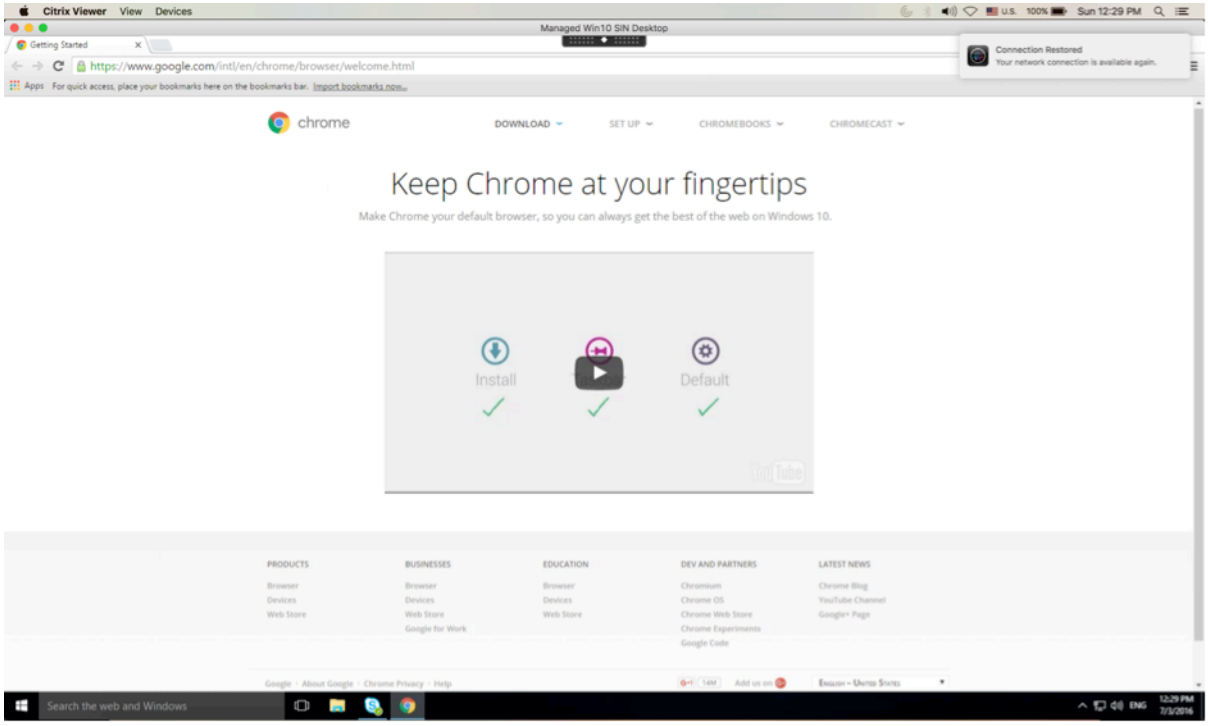
デフォルトでは、再接続のカウントダウン通知の最小値は 5 分です。このタイマー値は、自動再接続のデフォルトの値（2 分）およびセッション画面の保持のデフォルトの値（3 分）を組み合わせた値です。以下の画面は、セッションインターフェイスの右上に表示されるカウントダウン通知です：



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、コマンドプロンプトを使用して変更できます。たとえば、defaults write com.citrix.receiver.nomas NetDisruptBrightness 80 はデフォルト設定です。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。

- セッションの再接続が成功した場合（またはセッションが切断された場合）に通知が表示されます。この通知は、セッションインターフェイスの右上に表示されます：



- 自動再接続およびセッション画面の保持コントロールの下に表示されるセッション画面では、セッションの接続状態を知らせるメッセージが提供されます。アクティブなセッションに戻るには、[再接続のキャンセル] をクリックします。

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、Mac 向け Citrix Workspace アプリの構成および使用に関するデータが収集され、そのデータが Citrix と Google Analytics に自動的に送信されます。	このデータは、Citrix Workspace アプリの品質、信頼性、およびパフォーマンスを向上させる目的で使用させていただきます。

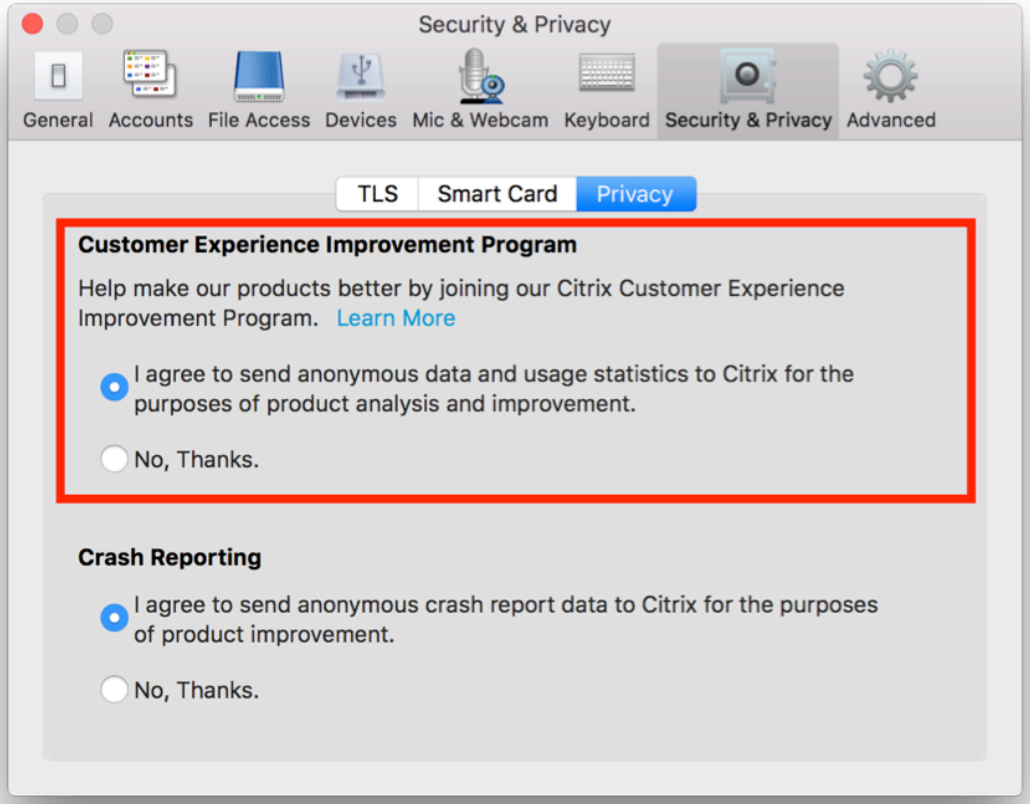
追加情報

Citrix は、お客様のデータを Citrix との契約条件に従って処理します。お客様のデータは、Citrix Trust Centerで入手できるCitrix Services Security Exhibitに従って保護されます。

Citrix は、CEIP の一環として、Google Analytics を使用して Citrix Workspace アプリから特定のデータを収集します。Google Analytics のために収集されたデータの Google での取り扱い方法について確認してください。

Citrix および Google Analytics への CEIP データの送信を無効にするには、次の手順を実行します:

1. ［環境設定］ウィンドウで ［セキュリティとプライバシー］を選択します。
2. ［プライバシー］タブを選択します。
3. ［いいえ］を選択して CEIP を無効にするか、参加を見送ります。
4. ［**OK**］をクリックします。



ターミナルで以下のコマンドを実行して CEIP を無効にすることもできます:

```
defaults write com.citrix.receiver.nomas ”CEIPEnabled”-bool NO
```

Google Analytics によって収集される特定の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	セッションの起動	汎用 USB リダイレクトの使用

アプリケーションの配信

Citrix Virtual Apps and Desktops および Citrix DaaS でアプリケーションをユーザーに配信するときは、アプリケーションにアクセスするユーザーのエクスペリエンスを向上させるために、次のオプションについて検討します:

Web アクセスモード

Mac 向け Citrix Workspace アプリでは、構成を必要とせずに、アプリケーションやデスクトップに対するブラウザーベースのアクセスである Web アクセスを実行できます。Workspace for Web を Web ブラウザーで開き、使用するアプリケーションを選択して実行するだけです。Web アクセスモードでは、ユーザーのデバイスのアプリフォルダーにアプリのショートカットが置かれます。

セルフサービスモード

StoreFront アカウントを Mac 向け Citrix Workspace アプリに追加するか、StoreFront サイトを参照してセルフサービスモードを使用するよう Mac 向け Citrix Workspace アプリを構成します。これによって、ユーザーに Mac 向け Citrix Workspace アプリ経由でアプリケーションにサブスクライブすることを許可するセルフサービスモードを構成できます。この拡張ユーザーエクスペリエンスはモバイルアプリケーションストアのものと同様です。セルフサービスモードでは、必要に応じて必須設定、自動プロビジョニング設定、お勧めのアプリキーワード設定を構成できます。いずれかのユーザーがアプリケーションを選択すると、そのアプリケーションに対するショートカットがユーザーデバイスのアプリフォルダーに置かれます。

StoreFront 3.0 サイトにアクセスすると、Mac 向け Citrix Workspace アプリのプレビューが表示されます。

Citrix Virtual Apps ファームでアプリケーションを公開する場合、StoreFront ストアを介したアプリケーションにユーザーがアクセスするときの利便性を高めるため、公開されたアプリのわかりやすい説明を含めるようにしてください。この説明は、Mac 向け Citrix Workspace アプリを介してユーザーに表示できます。

セルフサービスモードの構成

前述のように、StoreFront アカウントを Mac 向け Citrix Workspace アプリに追加するか、StoreFront サイトを参照してセルフサービスモードを使用するよう Mac 向け Citrix Workspace アプリを構成することができます。これによって、ユーザーに Mac 向け Citrix Workspace アプリのユーザーインターフェイスを使用してアプリケーションにサブスクライブすることを許可するセルフサービスモードを構成できます。この拡張ユーザーエクスペリエンスはモバイルアプリケーションストアのものと同様です。

セルフサービスモードでは、必要に応じて必須設定、自動プロビジョニング設定、お勧めのアプリキーワード設定を構成できます。

- Citrix Virtual Apps でアプリを公開しているときに、説明に文字列「`KEYWORDS:Auto`」を追加して、ストアのすべてのユーザーをアプリに自動的にサブスクライブします。ユーザーがストアにログインすると、アプリは自動的にプロビジョニングされ、手動でサブスクライブする必要はありません。

- ユーザーが特定のアプリケーションに簡単にアクセスできるようにするために、そのアプリケーションをユーザーの Mac 向け Citrix Workspace アプリの［おすすめ］一覧に表示できます。Mac のおすすめの一覧にアプリを表示するには、アプリの説明に文字列「**KEYWORDS:Featured**」を追加します。

詳しくは、StoreFrontのドキュメントを参照してください。

Citrix Workspace 更新プログラム

GUI を使用した構成

各ユーザーが ［環境設定］ダイアログボックスで ［**Citrix Workspace** 更新プログラム］設定を上書きできます。この処理により、ユーザーごとの構成および設定は、現在のユーザーにのみ適用されます。

1. Mac 向け Citrix Workspace アプリの ［環境設定］に移動します。
2. ［詳細］ペインで、［アップデート］を選択します。［Citrix Workspace 更新プログラム］ダイアログボックスが開きます。
3. 次のいずれかのオプションを選択します：
   - はい。通知します
   - いいえ。通知しません
   - 管理者指定の設定を使用する
4. 変更を保存するには、ダイアログボックスを閉じます。

StoreFront を使用した Citrix Workspace の更新の構成

管理者は、StoreFront を使用して Citrix Workspace 更新プログラムを構成できます。Mac 向け Citrix Workspace アプリは、「管理者が指定した設定を使用する」を選択したユーザーに対してのみ、この設定を使用します。この設定を手動で構成するには、以下の手順に従ってください。

1. テキストエディターで web.config ファイルを開きます。ファイルのデフォルトの場所は、次のとおりです：`C:\inetpub\wwwroot\Citrix\Roaming\web.config`
2. このファイルで、ユーザーアカウント要素の場所を見つけます（「Store」は使用環境のアカウント名です）。

   例：<account id=… name=”Store”>

   </account> タグの前に、ユーザーアカウントのプロパティに移動します：

   <properties>

   <clear />
   </properties>
3. *<clear />* タグの後に、自動更新タグを追加します。

auto-update-Check

この自動更新チェックにより、更新が利用可能かどうかを Mac 向け Citrix Workspace アプリで検出します。

有効な値は次のとおりです:

- Auto - 更新プログラムを利用できるときに、通知を受け取る場合に使用します。
- Manual - 更新プログラムを利用できるときに、通知を受け取らない場合に使用します。ユーザーは、［更新の確認］を選択して手動で更新を確認する必要があります。
- Disabled - ［Citrix Workspace 更新プログラム］を無効にする場合に使用します。

auto-update-DeferUpdate-Count

最新バージョンの Mac 向け Citrix Workspace アプリに強制的に更新される前に、ユーザーに送信される更新通知の回数を設定します。デフォルト値は、7 です。

有効な値は次のとおりです:

- -1 – 更新プログラムが利用できるようになったときに、ユーザーは後で通知を受け取ります。
- 0 - 更新プログラムが利用できるようになったときに、ユーザーは、最新バージョンの Mac 向け Citrix Workspace アプリに更新するよう強制されます。
- 正の整数 – ユーザーが更新を強制される前に更新通知を受信する回数を指定します。Citrix では、この値を 8 以上に設定しないことをお勧めします。

auto-update-Rollout-Priority

更新が利用可能であることがデバイスに表示されるタイミングを指定します。

有効な値は次のとおりです:

- Auto - 利用可能な更新をユーザーにロールアウトする時期を Citrix Workspace の更新システムが決定します。
- Fast - ユーザーへの自動更新のロールアウトが、Mac 向け Citrix Workspace アプリで高い優先度に設定されます。
- Medium - ユーザーへの自動更新のロールアウトが、Mac 向け Citrix Workspace アプリで中程度の優先度に設定されます。
- Slow - ユーザーへの自動更新のロールアウトが、Mac 向け Citrix Workspace アプリで低い優先度に設定されます。

キーボードレイアウトの同期

Windows VDA または Linux VDA の使用中は、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。

キーボードレイアウトの同期を有効にするには、［環境設定］**>**［キーボード］に移動し、「リモートサーバーのキーボードレイアウトではなくローカルのレイアウトを使用する」を選択します。

> 注:
>
> 1. ローカルキーボードレイアウトオプションで、クライアント IME（Input Method Editor）を有効にします。日本語、中国語、韓国語を使用しているユーザーは、サーバー IME を使用できます。その場合、[環境設定] > [キーボード] のチェックボックスをオフにして、ローカルキーボードレイアウトオプションを無効にする必要があります。次のセッションに接続すると、セッションは、リモートサーバーで指定されたキーボードレイアウトに戻します。
> 2. この機能は、クライアントでスイッチがオンになっていて、VDA で対応する機能が有効になっている場合にのみセッションで有効になります。[デバイス] > [キーボード] > [インターナショナル] に項目 [クライアントのキーボードレイアウトを使用する] が追加され、有効な状態であることが表示されます。

制限事項

- この機能を使用している間は、「**Mac** でサポートされているキーボードレイアウト」に記載されているキーボードレイアウトを使用できます。クライアントのキーボードレイアウトを互換性のないレイアウトに変更すると、VDA 側でレイアウトが同期される可能性はありますが、機能を使用できない場合があります。
- 管理者権限で実行しているリモートアプリは、クライアントのキーボードレイアウトと同期することはできません。この問題を解決するには、VDA でキーボードレイアウトを手動で変更するか、UAC を無効にします。
- ユーザーが RDP セッション内で作業している場合、RDP がアプリとして展開されていると、`Alt + Shift` ショートカットを使用してキーボードレイアウトを変更することはできません。回避策として、ユーザーは RDP セッションの言語バーを使用して、キーボードレイアウトを切り替えることができます。

Windows VDA でのキーボードレイアウトのサポート

Supported keyboard layouts on Mac

Language on Mac	Input source on Mac
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Right
	British
	British - PC
	Canadian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Bulgarian	Bulgarian
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish
Hungarian	Hungarian
Italian	Italian
Greek	Greek
Dutch	Belgian
	Dutch
Romanian	Romanian - Standard
Russian	Russian - PC
Croatian	Croatian - PC
Slovak	Slovak
	Slovak - QWERTY
Turkish	Turkish
	Turkish - QWERTY PC
Portuguese	Brazilian
	Brazilian - ABNT2
	Portuguese
Ukrainian	Ukrainian - PC
Belarusian	Belarusian
Slovenian	Slovenian
Estonian	Estonian
Latvian	Latvian
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	
Chinese, Traditional	

Linux VDA でのキーボードレイアウトのサポート

Language in MAC	Input Source in MAC
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Reft
	British
	British - PC
	Candian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish
Hungarian	Hungarian
Italian	Italian
Greek	Greek
Dutch	Belgian
	Dutch
Russian	Russian - PC
Croatian	Croatian - PC
Slovak	Slovak
	Slovak - QWERTY
Turkish	Turkish
	Turkish - QWERTY PC
Portuguese	Brazilian
	Brazilian - ABNT2
	Portuguese
Ukrainian	Ukrainian - PC
Belarusian	Belarusian
Slovenian	Slovenian
Estonian	Estonian
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	Pinyin -Simplified
Chinese, Traditional	Pinyin - Traditional

クライアントの拡張は、キーボードレイアウトの同期機能に依存します。デフォルトでは、キーボードレイアウトの同期機能が有効になっていると、拡張機能が有効になります。この機能のみを制御するには、**Config** ファイル（~/**Library**/**Application Support**/**Citrix Receiver**/フォルダー）を開いて、「**EnableIMEEnhancement**」設定で値を「true」（有効）または「false」（無効）にします。

> 注:
>
> セッションの再起動後に設定の変更が有効になります。

言語バー

GUI を使用して、アプリケーションセッションでリモート言語バーを表示または非表示にすることができます。言語バーには、セッションで優先される入力言語が表示されます。以前のリリースでは、VDA のレジストリキーを使用することによってのみ、この設定を変更できました。Mac 向け Citrix Workspace アプリのバージョン 1808 以降では、［環境設定］ダイアログを使用して変更できます。言語バーは、デフォルトでセッションに表示されます。

> 注:
>
> この機能は、VDA 7.17 以降で動作するセッションで使用できます。

リモート言語バーの表示または非表示を構成する

1. ［環境設定］を開きます。
2. ［キーボード］をクリックします。
3. ［公開アプリケーションのリモート言語バーを表示する］をオンまたはオフにします。

> 注:
>
> 設定の変更は直ちに有効になります。アクティブなセッションの設定を変更できます。入力言語が 1 つだけの場合、リモート言語バーはセッションに表示されません。

Citrix Casting

Citrix Casting は、近くの Citrix Ready ワークスペースハブデバイスに Mac の画面をキャストするために使用されます。Mac 向け Citrix Workspace アプリでは Citrix Casting がサポートされており、ワークスペースハブに接続されているモニターに Mac の画面をミラーリングできます。

詳しくは、Citrix Ready ワークスペースハブのドキュメントを参照してください。

前提条件

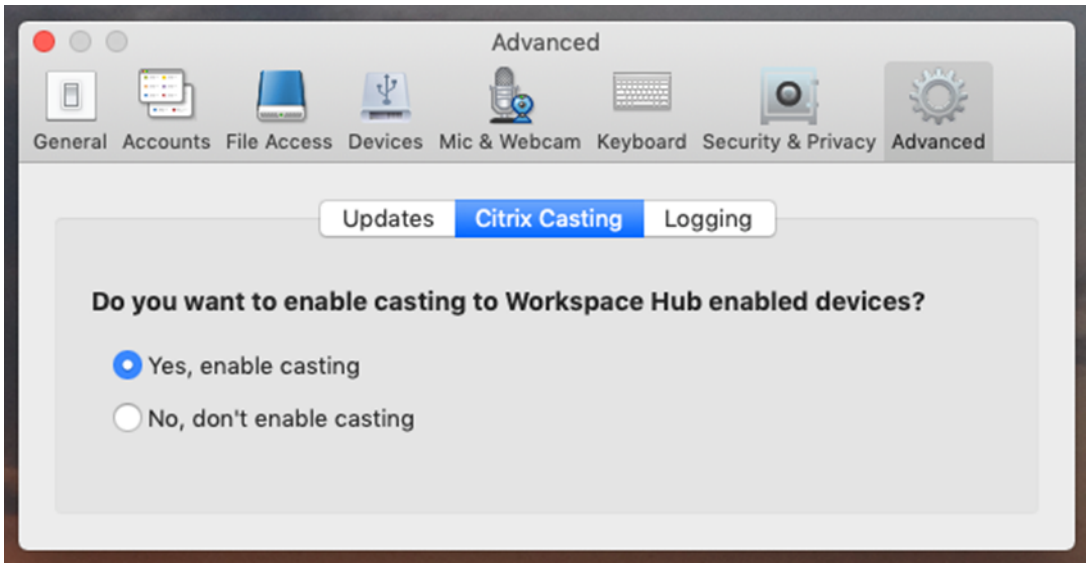
- Mac 向け Citrix Workspace アプリ 1812 以降。
- ハブ検出のためにデバイス上で Bluetooth が有効になっている。
- Citrix Ready ワークスペースハブと Citrix Workspace アプリが、同じネットワーク上に存在する。

- Citrix Workspace アプリが実行されているデバイスと Citrix Ready ワークスペースハブとの間でポート 55555 がブロックされていない。
- ポート 55556 は、モバイルデバイスと Citrix Ready ワークスペースハブの間の SSL 接続のデフォルトポートです。Raspberry Pi の設定ページで別の SSL ポートを構成できます。SSL ポートがブロックされている場合、ユーザーはワークスペースハブへの SSL 接続を確立できません。
- Citrix Casting の場合、ポート 1494 がブロックされていない必要があります。

Citrix Casting を有効にする

Citrix Casting は、デフォルトで無効になっています。Mac 向け Citrix Workspace アプリで Citrix Casting を有効にするには:

1. ［環境設定］に移動します。
2. パネルで ［詳細］、［**Citrix Casting**］の順に選択します。
3. ［はい。キャストを有効にします］を選択します。



Citrix Casting が起動すると通知が表示され、メニューバーに Citrix Casting のアイコンが表示されます。

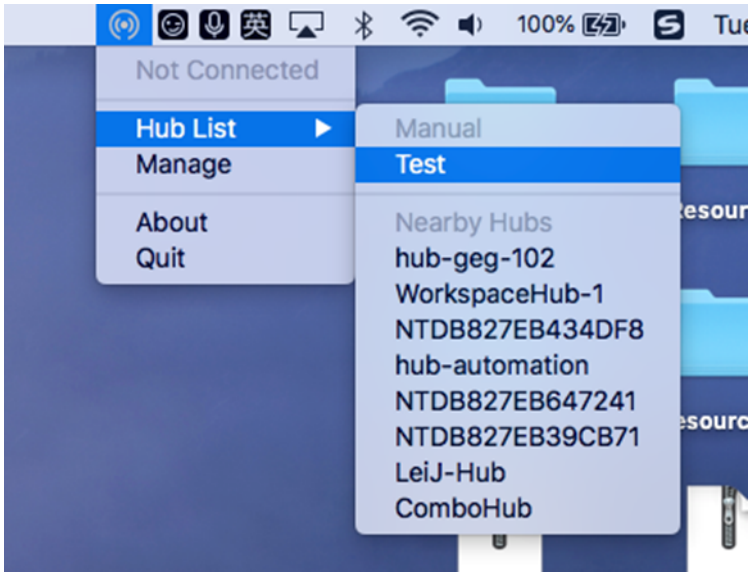
> 注:
>
> いったん有効にすると、［環境設定］**>**［詳細］**>**［**Citrix Casting**］で ［いいえ。キャストを有効にしません］を選択して無効にするまで、Mac 向け Citrix Workspace アプリの実行時に毎回、Citrix Casting が自動的に起動します。

ワークスペースハブデバイスを自動的に検出する

ワークスペースハブに自動的に接続するには:

1. Mac で Citrix Workspace アプリにサインインし、Bluetooth がオンになっていることを確認します。Bluetooth により、近くのワークスペースハブが検出されます。

2. メニューバーで、**Citrix Casting** のアイコンを選択します。このメニューを使って、Citrix Casting の全機能を操作します。
3. ［ハブ一覧］サブメニューに、同じネットワーク上の近くにあるすべてのワークスペースハブが表示されます。管理者の Mac に近いハブから降順に、ワークスペースハブの設定名で一覧表示されます。［近くのハブ］の下に、自動検出されたすべてのハブが表示されます。
4. 接続するハブの名前を選択します。



接続中にワークスペースハブの選択をキャンセルするには、［キャンセル］を選択します。ネットワーク接続状況が悪く接続に通常よりも時間がかかる場合にも、［キャンセル］を使ってキャンセルすることができます。

> 注:
>
> 選択したハブがメニューに表示されないことがあります。しばらくしてから、［ハブ一覧］メニューをもう一度確認するか、手動でハブを追加してください。Citrix Casting でワークスペースハブのブロードキャストを定期的に受信します。

ワークスペースハブデバイスを手動で検出する

［ハブ一覧］メニューに Citrix Ready ワークスペースハブデバイスが見つからない場合は、ワークスペースハブの IP アドレスを手動で追加してアクセスします。ワークスペースハブを追加するには:

1. Mac で Citrix Workspace アプリにサインインし、Bluetooth がオンになっていることを確認します。Bluetooth により、近くのワークスペースハブが検出されます。
2. メニューバーで、**Citrix Casting** のアイコンを選択します。
3. メニューで ［管理］を選択します。［ハブの管理］ウィンドウが開きます。
4. ［新規追加］をクリックして使用するハブの IP アドレスを入力します。
5. デバイスが追加された後、［ハブ名］列にハブのフレンドリ名が表示されます。この名前を、［ハブ一覧］サブメニューの ［手動］に表示されるハブの識別名として使用します。

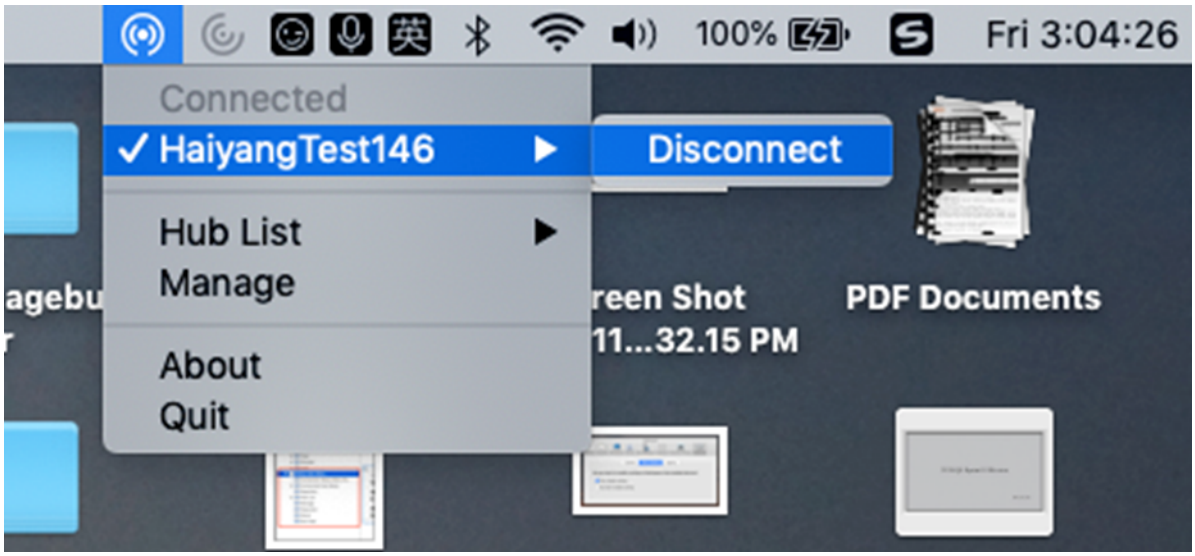
> 注:
>
> 現在、ミラーモードのみがサポートされています。［表示モード］列では、［ミラー］のみがオプションとして表示されます。

ワークスペースハブを切断する

現在のセッションを切断し、Citrix Ready ワークスペースハブを自動または手動で終了できます。

- 画面キャストのセッションを自動的に切断するには、ノートブックを閉じます。
- 画面キャストのセッションを手動で切断するには、以下を実行します:

1. **Citrix Casting** のアイコンを選択します。
2. ハブ一覧で、対象のワークスペースハブの名前を選択します。［切断］オプションが右側に表示されます。
3. ［切断］を選択してハブを切断します。



既知の問題

- ミラーリングされた画面を表示するときに、わずかな遅延が発生することがわかっています。ネットワーク接続状況が悪い場合、遅延時間が長くなることがあります。
- Citrix Ready ワークスペースハブで SSL が有効になっていて、このハブの証明書が信頼されていない場合、通知ウィンドウが表示されます。この問題を解決するには、キーチェーンツールを使用して、信頼された機関からの証明書の一覧に証明書を追加します。

クライアント側のマイク入力

Mac 向け Citrix Workspace アプリは、クライアント側の複数のマイク入力をサポートします。ユーザーは、ローカルのマイクを使用して以下の操作を実行できます。

- ソフトフォンでの通話や Web 会議などのライブイベント。
- ホストされている録音アプリケーション（ディクテーションプログラムなど）の使用。
- 録画と録音。

Mac 向け Citrix Workspace アプリでは、デジタルディクテーションがサポートされます。

ユーザーは、デバイスに接続されたマイクを使用できます。**Mac** 向け **Citrix Workspace** アプリの ［環境設定］の［マイクと **Web** カメラ］タブで、次のいずれかの設定を選択します：

- マイクと Web カメラを使用する
- マイクと Web カメラを使用しない
- 毎回確認する

［毎回確認する］を選択すると、接続するたびに、そのセッションでマイクを使用するかどうかを確認するダイアログボックスが開きます。

Windows 特殊キー

Mac 向け Citrix Workspace アプリには、Mac キーボードで Windows アプリケーションのファンクションキーなどの特殊キーを簡単に使用するためのオプションが多数用意されています。［キーボード］タブでは、必要に応じて以下のオプションを選択できます：

- Ctrl キー用のショートカット：セッション内で Ctrl キーと文字キーの組み合わせとして使用する Mac キーボードの組み合わせを指定します。ここで［⌘（command）または ⌃（control）］を選択すると、使い慣れた command+ 文字キーの Mac ショートカットを Windows の Ctrl+ 文字キーとして使用できます。［⌃（control）］を選択すると、control+ 文字キーを Ctrl+ 文字キーとして使用できます。
- Alt キー用のショートカット：セッション内で、Alt キーとして使用する Mac キーボードのキーを指定します。ここで［⌘⌥（command+option）］を選択すると、Mac キーボードの command+option+ 文字キーを、Windows の Alt+ 文字キーの組み合わせとして使用できます。［⌘（command）］を選択すると、command キーを Alt キーとして使用できます。
- Windows ロゴキーとして右側の ⌘（command）を使用する：Mac キーボードの右側にある command キーを Windows ロゴキーとして使用できます。このオプションが無効な場合、右側の command キーは左側の command キーと同じように動作します。この場合、Windows ロゴキーを使用するには、［キーボード］メニューを使用します（［キーボード］**>** ［**Windows** ショートカットを送信］**>** ［スタート］）。
- 特殊キーをそのまま送信する：チェックボックスをオンにすると、特殊キーの変換が無効になり、Mac キーボードの操作がそのままセッションに送信されます。たとえば、option キーとテンキーの 1 キーを一緒に押すと、セッションでは F1 キーに変換されます。この動作を変更し、セッションでは 1 キーとして処理されるように設定できます。そのためには、［特殊キーをそのまま送信する］チェックボックスをオンにします。このチェックボックスはデフォルトでオフになっており、option+1 キーは F1 キーに変換されます。

ファンクションキーやそのほかの特殊キーをセッション内で使用するときに、［キーボード］メニューを使用することもできます。

テンキーが付属しているキーボードでは、さらに以下のキー操作を使用できます：

PC キー	Mac キー操作
挿入	テンキーの 0（ゼロ）キー。Num Lock をオフにする必要があります。**clear** キーを使ってこれをオンまたはオフにすることができます。option+help
削除	テンキーの小数点キー。Num Lock をオフにする必要があります。**clear** キーを使ってこれをオンまたはオフにすることができます。clear
F1 から F9	option+1～9（テンキー）
F10	option+0（テンキー）
F11	option+ テンキーの負符号（-）キー
F12	option+ テンキーの正符号（+）キー

Windows のショートカットやキーの組み合わせ

Mac キーボードからのキーの組み合わせ（著作権記号「©」を入力する option+G キーなど）は、リモートセッションでも正しく処理されます。ただし、セッション中の一部のキー操作は、リモートのアプリケーションやデスクトップで処理されません。Mac オペレーティングシステム側で処理されます。この場合、そのキー操作により Mac オペレーティングシステムの機能がトリガーされます。

また、セッションで Ins など一部の Windows キーを使用しようと思っても、通常の Mac キーボードにこれらのキーはありません。Windows 8 では、チャームやアプリコマンドを表示したり、アプリのスナップや切り替えを行ったりするための専用のショートカットがあります。Mac キーボードでは、これらのショートカットを使用できません。ただし、［キーボード］メニューを使用してリモートデスクトップやアプリケーションに送信できます。

キーボードやキー操作の構成は、デバイスにより大きく異なることがあります。このため、Mac 向け Citrix Workspace アプリには、セッション内のアプリケーションやデスクトップにキー操作を正しく転送するためのオプションが用意されています。これらのキー操作については、下の表を参照してください。ここで示されているのは、デフォルトの動作です。Citrix Workspace アプリやそのほかの設定でデフォルト値を変更すると、異なるキー操作が送信されてリモート PC アクセスにおける動作が異なる場合があります。

> 重要
>
> 新しい Mac キーボードでは、下の表に示す一部のキーの組み合わせを使用できない場合があります。この場合、これらのキー操作をセッションで使用するには、［キーボード］メニューを使用します。

下の表について、以下の点に注意してください：

- Mac キーボードの特殊キーは小文字で示します（ファンクションキーを除く control、command、option など）。また、英字キーは大文字で表記されていますが、Shift キーを同時に押すという意味ではありません。
- キー名の間のプラス記号（+）は、それらのキーを同時に押すことを示します（control+C など）。

- 文字キーはテキスト入力を作成し、英数字と句読点のすべてを含みます。特殊キーは単独ではテキスト入力を作成せず、修飾キーや制御キーとして機能します。Ctrl（control）、Alt、Shift（shift）、command、option、方向キー、およびファンクションキーが含まれます。
- 使用するメニューは、そのセッションの Citrix Viewer メニューを指します。
- ユーザーデバイスの構成によっては、一部のキーの組み合わせが意図したとおりに機能しない場合があります。この場合、その代替操作を示します。
- fn キーは Mac キーボードの修飾キーのうちの 1 つで、F1～F12 キーは PC または Mac キーボードの各ファンクションキーに相当します。

Windows キー	Mac の場合
Alt+ 文字キー	command+option+ 文字キー（たとえば、セッションで Alt+C キー操作を使用するには、command+option+C を押します）
Alt+ 特殊キー	option+ 特殊キー（option+tab など）。command+option+ 特殊キー（command+option+tab など）
Ctrl+ 文字キー	command+ 文字キー（command+C など）。control+ 文字キー（control+C など）
Ctrl+ 特殊キー	control+ 特殊キー（control+F4 など）。command+ 特殊キー（command+F4 など）
Ctrl/Alt/Shift/Windows ロゴ + ファンクションキー	［キーボード］メニューの［ファンクションキーを送信］>（control/option/shift/command を押しながら）［F1～F12］
Ctrl+Alt	control+option+command
Ctrl+Alt+Del	control+option+fn+command+delete。［キーボード］メニューの［Ctrl+Alt+Del を送信］
Delete	Delete。［キーボード］メニューの［キーを送信］>［Del］。fn+backspace（一部の US キーボードでは fn+delete）
End	End。fn+ 右方向キー
Esc	Esc。［キーボード］メニューの［キーを送信］>［Esc］
F1 から F12	F1～F12。［キーボード］メニューの［ファンクションキーを送信］>［F1～F12］
Home	Home。fn+ 左方向キー
Ins	［キーボード］メニューの［キーを送信］>［Ins］
NumLock	Clear

Windows キー	Mac の場合
PgDn	PgDn。fn+ 下方向キー
PgUp	PgUp。fn+ 上方向キー
Space バー	［キーボード］メニューの［キーを送信］>［スペース］
タブ	［キーボード］メニューの［キーを送信］>［Tab］
Windows ロゴ	右側の command キー（デフォルトのキーボード設定）。［キーボード］メニューの［Windows ショートカットを送信］>［スタート］
チャームを表示するキー	［キーボード］メニューの［Windows ショートカットを送信］>［チャーム］
アプリコマンドを表示するキー	［キーボード］メニューの［Windows ショートカットを送信］>［アプリコマンド］
アプリをスナップするキー	［キーボード］メニューの［Windows ショートカットを送信］>［スナップ］
アプリを切り替えるキー	［キーボード］メニューの［Windows ショートカットを送信］>［アプリの切り替え］

IME（Input Method Editor）とインターナショナルキーボードレイアウトの使用

Mac 向け Citrix Workspace アプリでは、ユーザーデバイス（クライアント）側またはサーバー側の IME（Input Method Editor）を使用できます。

クライアント側 IME が有効な場合、ユーザーが入力する文字列は、別ウィンドウではなく入力ポイントに直接入力されます。

また、Mac 向け Citrix Workspace アプリで使用するキーボードレイアウトを選択することもできます。

クライアント側の **IME** を有効にするには

1. ［Citrix Viewer］メニューバーで、［キーボード］**>**［インターナショナル］**>**［クライアント **IME** を使用］を選択します。
2. サーバー側の IME が直接入力モードまたは半角英数モードになっていることを確認します。
3. Mac 側の IME（入力プログラム）を使用して文字列を入力します。

IME 入力時の確定前文字列の挿入ポイント（‘）を表示するには

- ［Citrix Viewer］メニューバーで、［キーボード］**>**［インターナショナル］**>**［変換中マークを使用］を選択します。

サーバー側の **IME** を使用するには

- クライアント側の IME が半角英数モードになっていることを確認します。

サーバー側 **IME** の入力モードキーの割り当て

Mac 向け Citrix Workspace アプリでは、サーバー側の Windows IME で入力モードを切り替えるときに使用するキーが、特定の Mac キーボードに割り当てられます。次の表は、サーバー側のシステムロケールの設定と、Mac キーボードの **option** キーに割り当てられる Windows IME の入力モードキーを示しています:

サーバー側システムロケール	サーバー側 IME の入力モードキー
日本語	漢字キー（日本語キーボードの Alt + 半角/全角）
韓国語	右 Alt キー（韓国語キーボードのハングル/英語切り替え）

インターナショナルキーボードレイアウトを使用するには

- クライアント側およびサーバー側で、サーバー側のデフォルトの入力言語と同じキーボードレイアウトが設定されていることを確認してください。

複数モニター

Mac 向け Citrix Workspace アプリでは、複数のモニターにまたがるフルスクリーンモードを実行できます。

1. Citrix Viewer を開きます。
2. 要件に基づいて、メニューバーで ［表示］をクリックして、次のオプションのいずれかを選択します:
   - フルスクリーンにする - プライマリモニターのみ全画面にします。
   - すべてのディスプレイをフルスクリーンで使用する - 接続されているすべてのモニターを全画面にします。
3. Citrix Virtual Desktops の画面を複数のモニターの間にドラッグします。

画面がすべてのモニターに拡張されます。

制限事項

- 単一モニターのフルスクリーンまたはすべてのモニターを使ったフルスクリーンモードのみがサポートされています。これはメニューアイテムを使って構成できます。
- Citrix では、最大でも 2 台のモニターを使用することをお勧めします。3 台以上のモニターを使用すると、セッションのパフォーマンスが低下したり、ユーザビリティの問題が発生する可能性があります。
- フルスクリーンモードは、ノッチのある Mac では使用できません。

デスクトップツールバー

ウィンドウモードおよびフルスクリーンモードのどちらでもデスクトップツーバーにアクセスできるようになりました。以前は、フルスクリーンモードでのみデスクトップツールバーが表示されていました。ツールバーには、ほかにも次のような変更が追加されています:

- ツールバーから ［ホーム］ボタンが削除されました。この機能は、次のコマンドを使って実行できます:
  - Cmd+Tab を押して、前のアクティブなアプリケーションに切り替えます。
  - Ctrl+ 左矢印を押して、前のスペースに切り替えます。
  - 内蔵のトラックパッドを使って、または Magic Mouse のジェスチャーにより別のスペースに切り替えます。
  - フルスクリーンモード時に画面の端にカーソルを動かすと、アクティブにするアプリケーションを選択できるドックが表示されます。
- ツールバーから ［ウィンドウ］ボタンが削除されました。次のいずれかの方法に従って、フルスクリーンモードからウィンドウモードに切り替えます:
  - OS X 10.10 で、ドロップダウンメニューバーにある緑色のウィンドウボタンをクリックします。
  - OS X 10.9 で、ドロップダウンメニューバーにある青色のメニューボタンをクリックします。
  - OS X のすべてのバージョンで、ドロップダウンメニューバーにある ［表示］メニューから ［フルスクリーンを解除］を選択します。
- 複数モニターを使った全画面のウィンドウ間でのドラッグがサポートされています。

ワークスペースコントロール

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのデスクトップやアプリケーションでの作業を継続できます。たとえば、病院で臨床医がほかのワークステーションに移動しても、移動先のデバイスでデスクトップやアプリケーションを起動し直す必要がなくなります。

ポリシーおよびクライアント側ドライブのマッピングの構成は、ユーザーがほかのデバイスに移動したときに、そのデバイスに適したものに自動的に切り替わります。ポリシーおよびマッピングの構成は、ユーザーがログオンするデバイスに応じて動的に適用されます。たとえば、医療従事者は救急処置室のユーザーデバイスからサインアウトし、レントゲン室のワークステーションにサインインできます。レントゲン室でのセッションに適したポリシー、プリンターマッピング、およびクライアント側ドライブのマッピング設定が、レントゲン室のセッションで有効になります。

ワークスペースコントロール設定を構成するには

1. Mac 向け Citrix Workspace アプリウィンドウで のアイコンをクリックして、［環境設定］を選択します。
2. ［一般設定］タブをクリックします。
3. 次のいずれかのオプションを選択します:
   - Citrix Workspace アプリの起動時にアプリに再接続します。ユーザーが Citrix Workspace を起動してログオンしたときに、切断セッションに再接続されます。

- アプリの起動時または更新時に再接続する：ユーザーがアプリを起動したとき、および Mac 向け Citrix Workspace アプリのメニューで［アプリケーション一覧の更新］を選択したときに、切断セッションに再接続されます。

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を有効にすると、セッション内でユーザーデバイス上のローカルドライブ（CD-ROM ドライブ、DVD ドライブ、USB メモリスティックなど）にアクセスできるようになります。サーバー構成でクライアント側ドライブのマッピングが許可されている場合、ユーザーはローカルに保存されているファイルにアクセスして、セッション中にそれらのファイルで作業を行うことができます。ユーザーは、ローカルドライブまたはサーバー上のドライブに、それらを保存することもできます。

Mac 向け Citrix Workspace アプリは、CD-ROM ドライブ、DVD ドライブ、USB メモリスティックなどのハードウェア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を監視して、セッション内で追加された新しいディレクトリを、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します。

ユーザーは、Mac 向け Citrix Workspace アプリの［環境設定］を使用して、マップされたドライブに対する読み取りと書き込みアクセスを制御できます。

マップされたドライブの読み取りと書き込みアクセスを制御するには

1. Mac 向け Citrix Workspace アプリのホームページで▼のアイコンをクリックし、［環境設定］を選択します。
2. ［ファイルアクセス］をクリックします。
3. 以下のいずれかのアクセスレベルを選択します：
   - 読み出し/書き込み
   - 読み取り専用
   - アクセスなし
   - 毎回確認する
4. 変更内容を適用するには、既存のセッションからログオフして、再接続します。

カスタム **Web** ストア

Mac 向け 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、管理者はカスタム Web ストアを Global App Configuration Service の`allowedWebStoreURLs`プロパティで許可されている URL の一覧に追加する必要があります。

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。

カスタム Web ストアの URL を追加するには、次の手順を実行します：

1. Citrix Workspace アプリを開き、［アカウント］に移動します。
2. ［アカウント］ウィンドウで、［**+**］アイコンをクリックして URL を入力します。

カスタム Web ストアの URL を削除するには、次の手順を実行します:

1. Citrix Workspace アプリを開き、［アカウント］に移動します。
2. ［アカウント］ウィンドウで、削除するアカウントを選択し、［-］アイコンをクリックします。

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は 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 Citrix 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、1 分から 1440 分まで設定できます。デフォルトでは、無操作状態による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。Citrix Workspace 構成のための PowerShell モジュールをダウンロードするには、こちらをクリックしてください。

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。Mac のシステム環境設定で Citrix Workspace アプリの通知を有効にした場合、通知が表示されます。
- この通知は、設定された非アクティブタイムアウト値が 5 分を超えた場合にのみ表示されます。たとえば、設定された値が 6 分である場合、3 分間の非アクティブが検出されると通知が表示されます。設定された非アクティブタイムアウト値が 5 分以下の場合、ユーザーは通知なしでサインアウトされます。
- 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。

StoreFront から Workspace への移行

StoreFront から Workspace への URL 移行により、最小限のユーザー操作でエンドユーザーを StoreFront ストアから Workspace ストアにシームレスに移行できます。

すべてのエンドユーザーが Workspace アプリに StoreFront ストア`storefront.com`を追加することを前提とします。管理者は、Global App Configuration Service で StoreFront URL から Workspace URL へのマッピング {‘storefront.com’:’xyz.cloud.com’} を構成できます。Global App Config Service は、StoreFront URL`storefront.com`が追加された、管理対象デバイスと非管理対象デバイスの両方で、すべての Citrix Workspace アプリインスタンスに設定をプッシュします。

設定が検出されると、Citrix Workspace アプリはマップされた Workspace URL`xyz.cloud.com`を別のストアとして追加します。エンドユーザーが Citrix Workspace アプリを起動すると、Citrix Workspace ストアが開きま

す。以前に追加された StoreFront ストアstorefront.comは、Citrix Workspace アプリに追加されたままです。ユーザーは、Citrix Workspace アプリの ［アカウントの切り替え］オプションを使用して、いつでも StoreFront ストアstorefront.comに戻すことができます。管理者は、ユーザーのエンドポイントの Citrix Workspace アプリから StoreFront ストアstorefront.comの削除を制御できます。削除は、Global App Config Service を介して行うことができます。

この機能を有効にするには、次の手順を実行します:

1. Global App Config Service を使用して、StoreFront から Workspace へのマッピングを構成します。Global App Config Service について詳しくは、「Global App Config Service」を参照してください。
2. App Config Service でペイロードを編集します。

```
{
  ”serviceURL”: Unknown macro: {
  ”url” }

,
”settings”:{

”name”:”Productivity Apps”, [New Store Name]
”description”:”Provides access StoreFront to Workspace Migration”,
”useForAppConfig”:true,
”appSettings”:
{
  ”macos”:[ Unknown macro: {
  ”category” }

]
 }

 }

 }

<!--NeedCopy-->
```

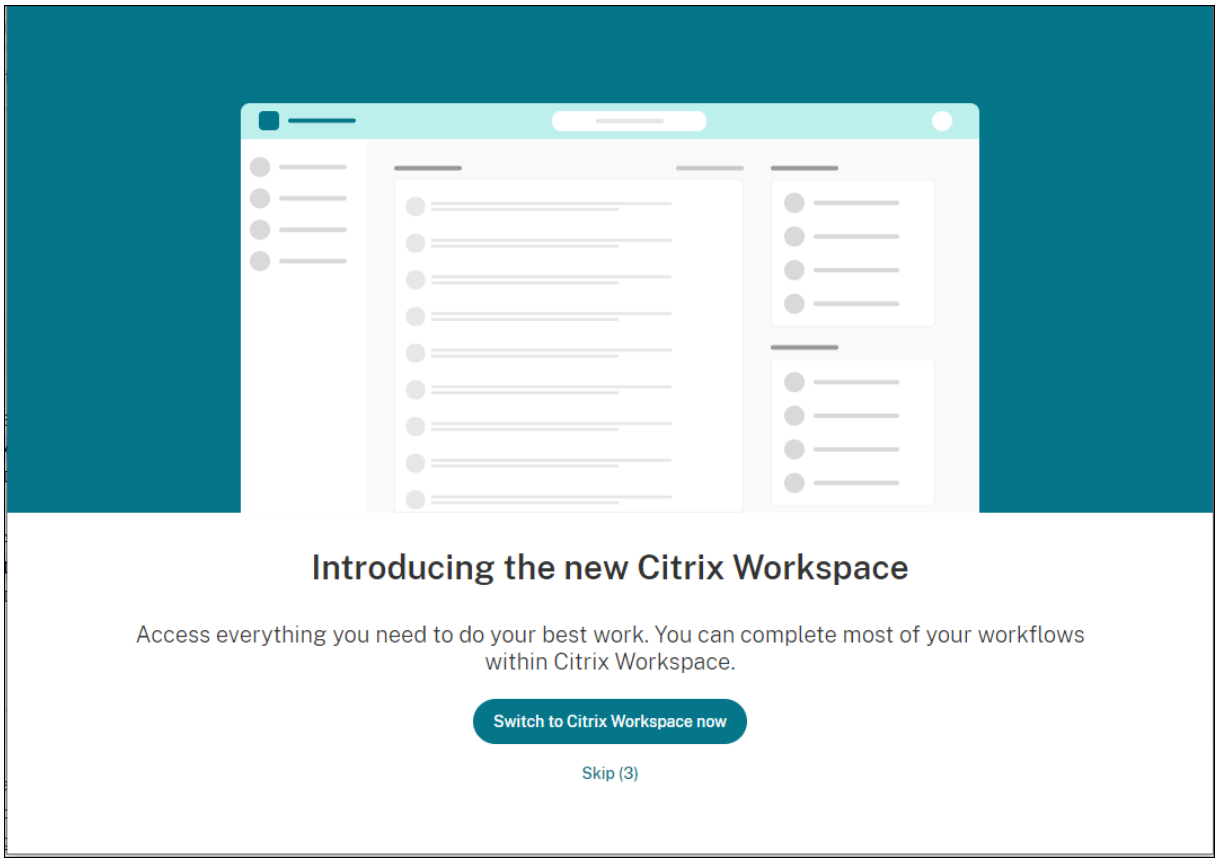
> 注:
>
> 初めてペイロードを構成する場合は、POSTを使用します。
> 既存のペイロード構成を編集する場合は、PUTを使用して、サポートされているすべての設定により構成されたペイロードがあることを確認してください。

3. StoreFront URLstorefront.comを **serviceURL** セクションの **URL** の値として指定します。

4. セクション **migrationUrl** 内で Workspace URL `xyz.cloud.com`を構成します。
5. **storeFrontValidUntil** を使用して、Citrix Workspace アプリから StoreFront ストアを削除するためのスケジュールを設定します。このフィールドはオプションです。要件に基づいて、次の値を設定できます。
    - YYYY-MM-DD 形式の有効な日付

    > 注:
    >
    > 過去の日付を指定した場合、StoreFront ストアは URL の移行と同時に削除されます。未来の日付を指定した場合、StoreFront ストアは設定された日付に削除されます。

App Config Service 設定がプッシュされると、次の画面が表示されます:



ユーザーが ［**Switch to Citrix Workspace now**］をクリックすると、Workspace URL が Citrix Workspace アプリに追加され、認証プロンプトが表示されます。ユーザーのオプションは制限されており、移行を最大 3 回遅らせることができます。

Microsoft Teams

エンコーダーのパフォーマンス見積もりツール

`HdxRtcEngine.exe`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、480p、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。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。

エンドポイントには次の 4 つのパフォーマンスカテゴリがあり、それぞれ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
Medium	720p（1280x720 16:9 @ 30fps）	2
Slow	360p（640x360 16:9 @ 30 fps または 640x480 4:3 @ 30 fps）	1
Very slow	240p（320x180 16:9 @ 30 fps または 320x240 4:3 @ 30 fps）	0

たとえば、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:

```
defaults write com.citrix.HdxRtcEngine OverridePerformance -int 1
```

Microsoft Teams の最適化について詳しくは、「Microsoft Teams の最適化」を参照してください。

印刷

Mac から印刷するときに PDF ユニバーサル印刷を使用できるようになりました。PDF ユニバーサル印刷を選択した場合、ユニバーサル印刷ドライバーを使用してプリンターを自動作成するときに、HP Color LaserJet 2800 シリーズ PS ドライバーをインストールする必要がなくなりました。

PostScript 印刷

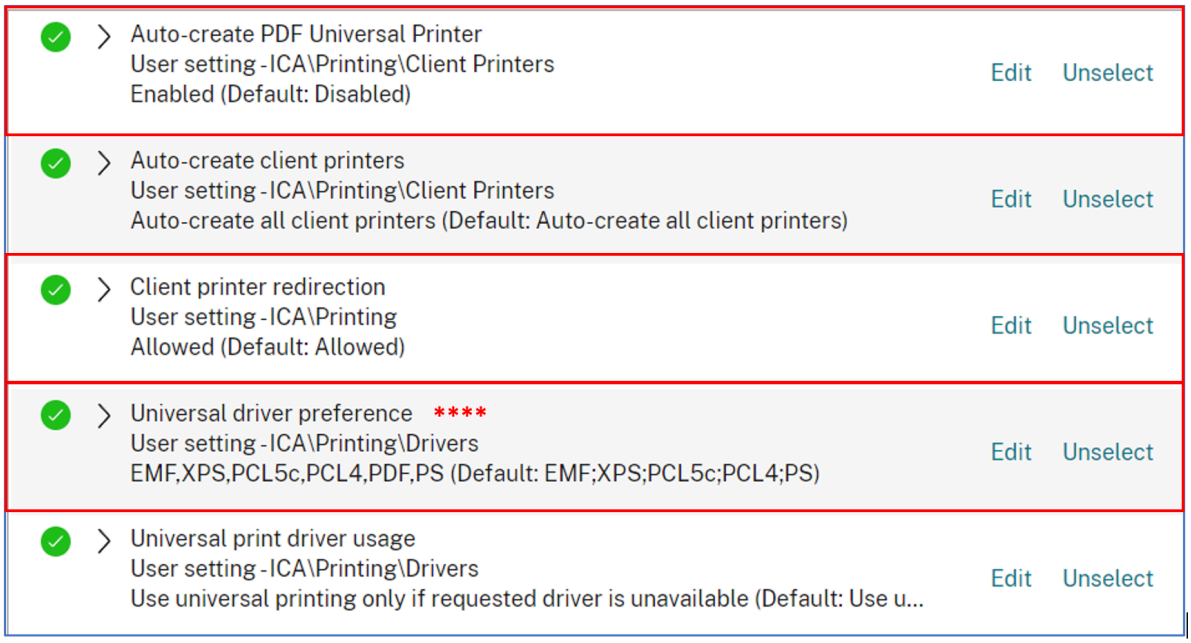
デフォルトでは、自動的にリダイレクトされたクライアントプリンターは、PostScript をサポートする Citrix UPD を使用して作成されます。
詳しくは、サポート記事CTX296662を参照してください。

クライアントプリンターのリダイレクト、ユニバーサル印刷の使用、およびユニバーサルプリントドライバーの優先度ポリシーがデフォルトに設定されていることを確認します。また、VDA に HP Color LaserJet 2800 シリーズ PS ドライバーがインストールされていることを確認してください。
ドライバーのインストールについて詳しくは、サポート記事CTX140208を参照してください。

PDF ユニバーサル印刷

前提条件:

- Mac 向け Citrix Workspace アプリバージョン 2112 以降 - Mac 向け Citrix Workspace アプリの PDF 印刷ストリームの使用を有効にします。
- Citrix Virtual Apps and Desktops バージョン 2112 以降 - 自動作成されたクライアントプリンターの PDF ユニバーサル印刷を有効にします。
- Citrix Studio または Web コンソールでクライアントプリンターのリダイレクトポリシーを有効にします。



**** "PDF" needs to be added manually if absent from the Universal Driver Preference policy

次のオプションのいずれかまたは両方を構成すると、PDF で印刷できます:

1. 各セッションで作成された単一の PDF ユニバーサルプリンターを提供します。
2. 通常の自動作成プリンターには UPD を使用します。

各セッションで作成された単一の **PDF** ユニバーサルプリンターを提供

Mac クライアントまたはその他の PDF 対応クライアントエンドポイントからのセッションで **PDF** ユニバーサルプリンターの作成を有効にするには、Citrix Studio または Web コンソールに移動し、**PDF** ユニバーサルプリンターを自動作成するポリシーを有効にします。
ポリシーを有効にすると、セッションで PDF ユニバーサルプリンターが作成されます。プリンターは **Citrix PDF** プリンターと呼ばれます。

このプリンターをセッションで使用すると、PDF 出力が生成され、クライアントに配信され、エンドポイント上のデフォルトの PDF 処理アプリケーションに渡されます。macOS クライアントの場合、これは通常、組み込みのプレビ

ューアプリケーションですが、Adobe Acrobat Reader などの登録済みの PDF 処理アプリケーションの場合もあります。

通常の自動作成プリンターに **UPD** を使用

Mac クライアントからのセッションでリダイレクトされたすべてのクライアントプリンターで PDF ユニバーサル印刷を有効にするには、Citrix Studio または Web コンソールにアクセスし、ユニバーサル印刷ドライバーの優先ポリシーを構成してPDFメタファイル形式を優先リスト内のPSの前に配置します。

この変更を行った後、PDF 対応の Mac クライアントでユニバーサルドライバーを使用する自動作成プリンターは、ホスト上の HP Color LaserJet 2800 シリーズ PS ドライバーの代わりに Citrix PDF ユニバーサルドライバーを使用します。
自動作成されたプリンターの 1 つをセッションで使用する場合、PDF が印刷ジョブの中間形式になります。ただし、印刷は、選択したクライアント接続プリンターから直接出力されます。

認証

June 10, 2022

スマートカード

Mac 向け Citrix Workspace アプリは次の構成においてスマートカード認証をサポートします:

- Workspace for Web または StoreFront 2.x 以降でのスマートカード認証
- Citrix Virtual Apps and Desktops 7 1808 以降
- XenDesktop 7.1 以降または XenApp 6.5 以降
- Microsoft Outlook や Microsoft Office などのスマートカード対応アプリケーションでは、仮想デスクトップやアプリケーションセッションでドキュメントにデジタル署名を追加したりファイルを暗号化したりできます。
- Mac 向け Citrix Workspace アプリは単一のスマートカードまたは複数のスマートカードでの複数の証明書の使用をサポートします。ユーザーがスマートカードをリーダーに挿入すると、ユーザーデバイス上で実行する、Mac 向け Citrix Workspace アプリを含むすべてのアプリケーションで複数の証明書を使用できるようになります。
- ダブルホップセッションでは、Mac 向け Citrix Workspace アプリとユーザーの仮想デスクトップとの間に追加の接続が確立されます。

Citrix Gateway へのスマートカード認証について

スマートカードを使用して接続を認証する場合、使用可能な証明書が複数あります。Mac 向け Citrix Workspace アプリでは、証明書を選択するように求められます。証明書を選択すると、Mac 向け Citrix Workspace アプリでスマートカードのパスワードを入力するようにプロンプトが表示されます。認証後、セッションが開始します。

スマートカードに適切な証明書が 1 つしかない場合、Mac 向け Citrix Workspace アプリはその証明書を使用し、選択を求めるプロンプトは表示されません。ただし、接続を認証してセッションを開始するために、スマートカードに割り当てられたパスワードを入力する必要はあります。

スマートカード認証用の **PKCS#11** モジュールの指定

> 注:
>
> PKCS#11 モジュールのインストールは必須ではありません。このセクションの記述は、ICA セッションにのみ適用されます。スマートカードが必要な Citrix Workspace から Citrix Gateway への、または StoreFront へのアクセスでは適用されません。

スマートカード認証用の PKCS#11 モジュールを指定するには:

1. Mac 向け Citrix Workspace アプリで ［環境設定］を選択します。
2. ［セキュリティとプライバシー］をクリックします。
3. ［セキュリティとプライバシー］セクションで、［スマートカード］をクリックします。
4. **PKCS#11** フィールドで適切なモジュールを選択します。一覧に必要なモジュールがない場合は、［その他］をクリックして PKCS#11 モジュールの場所を参照します。
5. 適切なモジュールを選択したら、［追加］をクリックします。

サポートされるリーダー、ミドルウェア、およびスマートカードプロファイル

Mac 向け Citrix Workspace アプリは多くの macOS 互換スマートカードリーダーおよび暗号化ミドルウェアをサポートします。Citrix では以下を使用して操作を検証済みです。

サポートされるスマートカードリーダー:

- 一般的な USB 接続スマートカードリーダー

サポートされるミドルウェア:

- Clarify
- ActivIdentity クライアントのバージョン
- Charismathics クライアントのバージョン

サポートされるスマートカード:

- PIV カード
- Common Access Card（CAC）
- Gemalto .NET カード

ユーザーデバイスを構成するため、ベンダーの macOS 互換スマートカードリーダーおよび暗号化ミドルウェアにより提供された指示に従います。

制限

- 証明書は、ユーザーデバイス上ではなくスマートカード上に格納されている必要があります。
- Mac 向け Citrix Workspace アプリでは、ユーザーの選択した証明書が保存されません。
- Mac 向け Citrix Workspace アプリでは、ユーザーのスマートカード PIN が格納または保存されません。PIN の取得はオペレーティングシステムにより処理され、独自のキャッシングメカニズムがある場合があります。
- Citrix Workspace アプリでは、スマートカードが挿入されたときに自動的には切断セッションに再接続されません。
- スマートカード認証で VPN トンネルを使用するには、ユーザーが Citrix Gateway Plug-in をインストールして Web ページ経由でログオンする必要があります。この場合、各手順でスマートカードと PIN を認証に使用します。スマートカードユーザーは、Citrix Gateway Plug-in を使用した StoreFront へのパススルー認証を使用できません。

Azure Active Directory での条件付きアクセス

この認証方法は現在、Mac 向け Citrix Workspace アプリではサポートされていません。

セキュリティで保護された通信

June 10, 2022

サイトと Mac 向け Citrix Workspace アプリ間の通信をセキュアに保護するには、Citrix Gateway など、以下の一連のセキュリティ技術を使用します。Citrix Gateway と Citrix StoreFront の構成について詳しくは、StoreFrontのドキュメントを参照してください。

> 注:
>
> StoreFront サーバーとユーザーデバイス間の通信を保護するには、Citrix Gateway を使用することをお勧めします。

- 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 とサーバー間の接続を制御できます。Mac 向け 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 Secure Web Gateway。Citrix Secure Web Gateway を使うことで、社内ネットワーク上のサーバーにインターネットを介して接続できる、暗号化された安全な単一のアクセスポイントをユーザーに提供できます。
- Transport Layer Security（TLS）プロトコルによる SSL Relay ソリューション

- 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 NAT（Network Address Translation：ネットワークアドレス変換）などの外部インターネットアドレスにマップするファイアウォールを使用する場合は、外部アドレスを構成します。

> 注：
>
> macOS Catalina 以降、Apple は管理者が構成する必要のあるルート CA 証明書と中間証明書について、追加の要件を適用しています。詳しくは、Apple のサポート記事HT210176を参照してください。

Citrix Gateway

リモートのユーザーが Citrix Gateway を介して XenMobile 展開に接続できるようにするには、StoreFront をサポートするように Citrix Gateway を構成します。このアクセスを有効にする方法は、XenMobile のエディションによって異なります。

ネットワークで XenMobile を展開する場合、Citrix Gateway と StoreFront を統合することで Citrix Gateway を経由して内部ユーザーやリモートユーザーが StoreFront に接続できます。ユーザーは、StoreFront に接続して XenApp の公開アプリケーションや XenDesktop の仮想デスクトップにアクセスします。ユーザーは、Mac 向け Citrix Workspace アプリを使用して接続を行います。

Citrix Secure Web Gateway による接続

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。リレーモードについて詳しくは、XenApp および Citrix Secure Web Gatewayのドキュメントを参照してください。

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、Mac 向け 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。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.example.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（example）、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（example.com）をドメイン名といいます。

プロキシサーバー経由の接続

プロキシサーバーは、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、Mac 向け Citrix Workspace アプリとサーバー間の接続を制御するために使います。Mac 向け 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の両方をサポートしています。

Mac 向け Citrix Workspace アプリで Web サーバーと通信する場合は、ユーザーデバイス上のデフォルトの Web ブラウザーで構成されているプロキシサーバー設定が使用されます。各ユーザーデバイス上のデフォルトの Web ブラウザーで、プロキシサーバー設定を構成します。

ファイアウォールを介した接続

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。Mac 向け Citrix Workspace アプリと Web サーバーおよび Citrix 製品のサーバーとの通信がファイアウォールでブロックされないように設定する必要があります。このためには、ユーザーデバイスと Web サーバー間の HTTP トラフィック（一般に標準 HTTP ポート 80、またはセキュアな Web サーバーを使用している場合はポート 443 での通信）がファイアウォールを通過できるように設定します。また、Citrix Workspace と Citrix 製品サーバー間の通信では、ポート 1494 とポート 2598 の受信 ICA トラフィックがファイアウォールを通過できるように設定します。

TLS

Transport Layer Security（TLS）は、SSL プロトコルの最新の標準化バージョンです。IETF（Internet Engineering TaskForce）が、TLS 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。

Mac 向け Citrix Workspace アプリは、ビット長 1024、2048 および、3072 の RSA キーをサポートします。さらに、ビット長 4096 の RSA キーを持つルート証明書がサポートされます。

> 注
>
> Mac 向け Citrix Workspace アプリは、プラットフォーム（OS X）の暗号化機能を Mac 向け Citrix Workspace アプリと StoreFront の接続に使用します。

次の暗号の組み合わせは、セキュリティを強化するために廃止されました：

- 接頭辞が「TLS_RSA_*」の暗号の組み合わせ
- 暗号の組み合わせ RC4 および 3DES
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

Mac 向け Citrix Workspace アプリは以下の暗号の組み合わせのみをサポートします:

- 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 1.0 ユーザーの場合、Mac 向け Citrix Workspace アプリ 1910 以降は以下の暗号の組み合わせのみをサポートします:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（0xc013）

DTLS 1.0 を使用する場合は、Citrix Gateway のバージョンを 12.1 以降にアップグレードすることをお勧めします。それ以外の場合は、DDC ポリシーに基づいて TLS にフォールバックします。

次のマトリックスは、内部および外部ネットワーク接続の詳細を提供します:

		Direct connections								
		TLS			DTLS v1.0			DTLS v1.2		
Client cipher set	VDA cipher set	Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			Y		
	COM	Y	X	X	Y			Y		
	GOV	Y	Y	Y	Y			Y		
COM	ANY	Y	X	X	Y					
	COM	Y	X	X	Y					
	GOV	Y	X	X	Y					
GOV	ANY	Y	Y	Y	X			Y		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			Y		

Client cipher set	VDA cipher set	External connections with Citrix Gateway								
		TLS			DTLS v1.0			DTLS v1.2		
		Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	Y	Y	Y			X		
COM	ANY	Y	X	X	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	X	X	Y			X		
GOV	ANY	Y	Y	Y	X			X		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			X		

> 注:
>
> - EDT を正しく機能させるために、Citrix Gateway 12.1 以降を使用します。以前のバージョンは、DTLS モードで ECDHE の暗号の組み合わせをサポートしていません。
> - Citrix Gateway は DTLS 1.2 をサポートしていません。そのため、`TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` と `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` はサポートされません。Citrix Gateway が DTLS 1.0 で正しく動作するためには、`TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA` を使用するように構成する必要があります。

Citrix Workspace アプリの **TLS** の構成と有効化

TLS のセットアップは、以下の 2 つの手順で行います:

1. Citrix Virtual Apps and Desktops および Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）のサーバー上で SSL Relay をセットアップし、必要なサーバー証明書を入手してインストールします。
2. ユーザーデバイス上で、ルート証明書をインストールします。

ユーザーデバイスへのルート証明書のインストール

TLS 機能が有効になっている Mac 向け Citrix Workspace アプリとサーバーファーム間の通信を TLS でセキュアに保護するには、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。このルート証明書は、サーバー証明書上の証明機関の署名を検証します。

macOS X には、約 100 の商用ルート証明書がインストール済みです。ただし、それ以外の証明書を使用する場合は、該当する証明機関からルート証明書を取得して、各ユーザーデバイスにインストールする必要があります。

ルート証明書をインストールするようユーザーに勧めるのではなく、組織のポリシーと手順に従って、各デバイスにルート証明書をインストールします。ルート証明書を簡単および確実にインストールするには、macOS X のキーチェーンにその証明書を追加します。

ルート証明書をキーチェーンに追加するには

1. 証明書を含んでいるファイルをダブルクリックします。この操作により、キーチェーンアクセスアプリケーションが自動的に起動します。
2. [証明書の追加] ダイアログボックスで、[キーチェーン] ポップアップメニューから以下のいずれかのオプションを選択します:
   - ログイン: 現在のログインユーザーにのみ証明書が適用されます。
   - システム: そのデバイスにログインするすべてのユーザーに証明書が適用されます。
3. [OK] をクリックします。
4. [認証] ダイアログボックスにパスワードを入力し、[OK] をクリックします。

ルート証明書がインストールされ、TLS が有効なクライアントおよび TLS を使用するすべてのアプリケーションで使用されるようになります。

TLS ポリシーについて

ここでは、TLS 経由の ICA セッションのセキュリティポリシーを構成するための情報について説明します。ICA 接続に使用される一部の TLS 設定を Mac 向け Citrix Workspace アプリで構成できます。これらの設定はユーザーインターフェイスに表示されません。変更するには Mac 向け Citrix Workspace アプリが動作するデバイス上でコマンドを実行する必要があります。

> 注
>
> TLS ポリシーは、OS X サーバーやほかのモバイルデバイス管理ソリューションで制御されているデバイスによって、ほかの方法で管理されます。

TLS ポリシーには以下の設定が含まれます:

SecurityComplianceMode。ポリシーのセキュリティコンプライアンスモードを設定します。SecurityComplianceMode を構成しない場合は、デフォルト値として FIPS が使用されます。この設定に適用できる値は以下のとおりです:

- なし。コンプライアンスモードは適用されません。
- **FIPS**。FIPS 暗号モジュールが使用されます。
- **SP800-52**。NIST SP800-52r1 コンプライアンスが適用されます。

```
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800-52
```

SecurityAllowedTLSVersions。プロトコルネゴシエーション中に受け入れられる TLS プロトコルのバージョンを指定します。この情報は配列として表され、指定可能な値のどの組み合わせもサポートされます。この設定を構成しない場合は、TLS10、TLS11、TLS12 がデフォルト値として使用されます。この設定に適用できる値は以下のとおりです:

- **TLS10**。TLS 1.0 プロトコルを許可することを指定します。
- **TLS11**。TLS 1.1 プロトコルを許可することを指定します。
- **TLS12**。TLS 1.2 プロトコルを許可することを指定します。


```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array
TLS11 TLS12
```

SSLCertificateRevocationCheckPolicy。Citrix サーバーの暗号化認証機能が強化され、クライアントとサーバーの間の SSL/TLS 接続の全体的なセキュリティが向上します。この設定は、OS X クライアントで SSL を介してリモートセッションを開く際の、信頼されたルート証明機関（CA）の処理を制御します。

この設定を有効にすると、サーバー証明書が失効していないかがクライアントによりチェックされます。証明書失効一覧のチェックには複数のレベルがあります。たとえば、クライアントはローカルの証明書一覧のみをチェックしたり、ローカルとネットワークの証明書一覧をチェックするように構成できます。さらに、すべての証明書失効一覧で証明書の有効性が検証された時のみユーザーがログオンできるように、証明書チェックを構成できます。

証明書失効一覧（CRL）チェックは、一部の証明書発行元によりサポートされる高度な機能です。これにより、証明書の秘密キーの暗号化が危うくなったり、DNS 名に予期しない変更があったりした場合に、管理者はセキュリティ証明書を失効させる、つまり失効日より前に無効にすることができます。

この設定に適用できる値は以下のとおりです：

- **NoCheck**。証明書失効一覧をチェックしません。
- **CheckWithNoNetworkAccess**。証明書失効一覧がチェックされます。ローカルの証明書失効一覧のストアのみが使用されます。すべての配布ポイントが無視されます。証明書失効一覧の検索は、対象の SSL Relay または Citrix Secure Web Gateway サーバーによって提示されるサーバー証明書の検証において重要ではありません。
- **FullAccessCheck**。証明書失効一覧がチェックされます。ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。証明書失効一覧の検索は、対象の SSL Relay または Citrix Secure Web Gateway サーバーによって提示されるサーバー証明書の検証において重要ではありません。
- **FullAccessCheckAndCRLRequired**。証明書失効一覧がチェックされますがルート証明機関は除外されます。ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。すべての必要な証明書失効一覧の検索が、検証において重大な意味を持ちます。
- **FullAccessCheckAndCRLRequiredAll**。ルート証明機関を含め、証明書失効一覧がチェックされます。ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。すべての必要な証明書失効一覧の検索が、検証において重大な意味を持ちます。

> 注
>
> SSLCertificateRevocationCheckPolicy を設定しない場合は、デフォルト値として FullAccessCheck が使用されます。
>
> ```
> defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy
>  FullAccessCheckAndCRLRequired
> ```

TLS ポリシーの構成

管理対象外のコンピューターで TLS 設定を構成するには、Terminal.app で **defaults** コマンドを実行します。

defaults はコマンドラインアプリケーションで、OS X の環境設定リストファイルにアプリ設定を追加、編集、および削除するために使用できます。

設定を変更するには:

1. [アプリケーション]、[ユーティリティ]、[ターミナル] の順に選択します。
2. ターミナルで以下のコマンドを実行します:

```
defaults write com.citrix.receiver.nomas <name> <type> <value>
```

場所:

<name>: 前述のように設定の名前です。

<type>: 設定の種類を指定するスイッチで、-string または-array のどちらかです。設定の種類が文字列である場合は、この設定を省略できます。

<value>: 設定の値。値が配列であり、複数の値を指定する必要がある場合は、値をスペースで区切ります。

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array
TLS11 TLS12
```

デフォルト構成へのリセット

設定をデフォルトに戻すには:

1. [アプリケーション]、[ユーティリティ]、[ターミナル] の順に選択します。
2. ターミナルで以下のコマンドを実行します:

```
defaults delete com.citrix.receiver.nomas <name>
```

場所:

<name>: 前述のように設定の名前です。

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```

セキュリティの設定

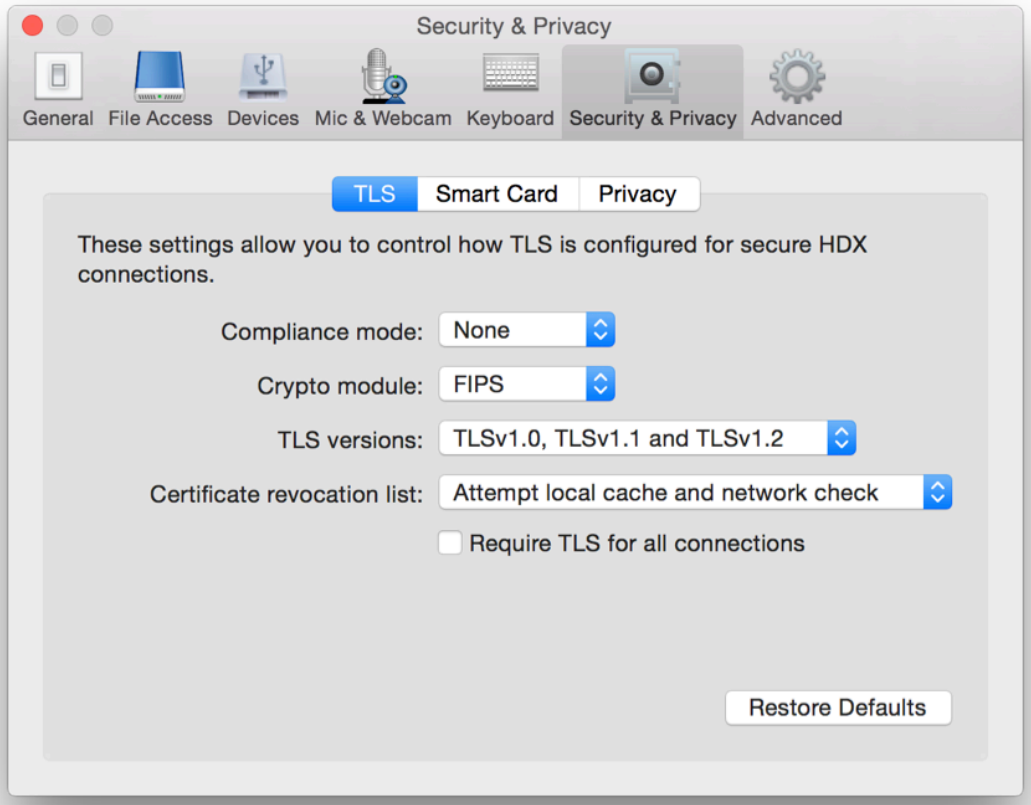
Citrix Receiver for Mac のバージョン 12.3 では、以下のようにセキュリティ機能が改善、強化されています:

- セキュリティ構成のユーザーインターフェイスが強化されました。以前のリリースでは、セキュリティ関連の変更を実施する場合、コマンドラインが優先される方法でしたが、セッションセキュリティに関連する構成設定がシンプルになり、UI からアクセスできるようになりました。この改善により、ユーザーエクスペリエンスが向上し、シームレスにセキュリティ関連の設定を採用するための方法が提供されます。
- TLS 接続の表示。特定の TLS バージョンを使用する接続、暗号化アルゴリズム、モード、キーサイズ、および SecureICA の状態を検証できます。また、TLS 接続のサーバー証明書も表示できます。

強化された [セキュリティとプライバシー] 画面の [**TLS**] タブには、以下の新しいオプションが含まれます:

- コンプライアンスモードの設定
- 暗号モジュールの構成
- 適切な TLS のバージョンの選択
- 証明書失効一覧の選択
- すべての TLS 接続の設定を有効にする

以下の図は、UI でアクセス可能な ［セキュリティとプライバシー］設定を示します:



Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States