Mac 向け Citrix Workspace アプリ

Contents

このリリースについて

June 29, 2021

> 重要
>
> 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。

2106 の新機能

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

Citrix Workspace アプリでは、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 を追加できるようになりました。

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。

2104 の新機能

Mac 向け Citrix Workspace アプリは、組織でシングルサインオンが有効になっていない限り、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ています。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。

2102 の新機能

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。

2101 の新機能

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 サポートの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、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。

2012 の新機能

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。

2010 の新機能

認証の強化

シームレスなエクスペリエンスを提供するために、Citrix Workspace アプリ内に認証ダイアログが表示されるようになりました。ストアの詳細がログオン画面に表示されます。認証トークンは暗号化され保存されるため、システムの再起動やセッションの再起動時に資格情報を再入力する必要はありません。

> 注:
>
> この認証機能強化は、クラウド展開でのみ適用されます。

macOS Big Sur のサポート

Mac 向け Citrix Workspace アプリは、macOS Big Sur（11.0.1）でサポートされています。

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。

2009 の新機能

Microsoft Teams の最適化（プレビュー）

Citrix Virtual Apps and Desktops および Citrix Workspace アプリを通じたデスクトップベースの Microsoft Teams の最適化です。Microsoft Teams の最適化は、Microsoft Skype for Business の HDX RealTime の最適化に似ています。両者の違いは、Microsoft Teams 最適化で必要となるすべてのコンポーネントは VDA と Mac 向け Workspace アプリに付属しているという点にあります。Mac 向け Citrix Workspace アプリは、Microsoft Teams 最適化でオーディオとビデオをサポートします。

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
- 既知の問題

Mac 向け **Citrix Workspace** アプリを **macOS Big Sur Beta** で使用

Mac 向け Citrix Workspace アプリ 2009 は、macOS Big Sur Beta 8 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てください。macOS Big Sur Beta に固有の問題については、「既知の問題」セクションを参照してください。

> 注意:

> 実稼働環境で macOS Big Sur Beta バージョンが使用されている場合、Mac 向け Citrix Workspace アプリを使用しないでください。

USB リダイレクトのカーネル拡張

Mac 向け Citrix Workspace アプリ 2009 は、USB リダイレクトのカーネル拡張（KEXT）に依存しなくなりました。

2008 の新機能

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。

macOS バージョンのサポート

Mac 向け Citrix Workspace アプリ 2008 は、macOS バージョンの High Sierra（10.13）と Mojave（10.14）をサポートする最新リリースです。

2007 の新機能

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。

2006 の新機能

Citrix Analytics Service の更新

Citrix Workspace アプリには、ブラウザーから起動した ICA セッションから Citrix Analytics Service にデータをセキュアに転送するための機能があります。Citrix Analytics がどのようにこの情報を使用するかについて詳しくは、「パフォーマンスでのセルフサービス」および「Virtual Apps and Desktops でのセルフサービス検索」を参照してください。

Web カメラリダイレクトでの H.264 サポート

Mac 向け Citrix Workspace アプリで、H.264（別名 MPEG-4 AVC）ビデオ圧縮規格がサポートされるようになりました。その結果、64 ビットの公開アプリで Web カメラリダイレクトを使用できるようになりました。

安定性の向上

このリリースは、さまざまな問題に対応しているため、安定性が総合的に向上しています。

2005 の新機能

言語サポート

Mac 向け Citrix Workspace アプリがイタリア語で利用できるようになりました。

パフォーマンスの向上

- このリリースでは問題に対応しているため、Citrix Workspace（クラウドストア）でのパフォーマンスや安定性が総合的に向上しています。
- このリリースでは、クラウドユーザーのログオン時間、アプリの列挙時間が短縮されます。

2002 の新機能

FIPS モードでの **4096** ビットキーサポート

Mac 向け Citrix Workspace アプリでは、FIPS 140 暗号化モードで長さ 4096 ビットの RSA キーをサポートするようになりました。

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。

2001 の新機能

アプリ保護

Mac 向け Citrix Workspace アプリで、アプリ保護をサポートするようになりました。アプリ保護は、Citrix Virtual Apps and Desktops の使用時にセキュリティを強化する機能です。この機能により、キーロガーや画面キャプチャマルウェアによりクライアントが侵害される可能性が制限されます。アプリ保護では、画面に表示されるユーザーの資格情報や個人情報などの機密情報の流出を防ぎます。この機能を使うと、ユーザーおよび攻撃者がスクリーンショットを撮る、またはキーロガーを使用することにより機密情報を収集、悪用することを防ぐことができます。Citrix Virtual Apps and Desktops でのアプリ保護の構成については、「アプリ保護」を参照してください。

既知の問題または制限事項:

この機能を適切に機能させるには、VDA でクライアントクリップボードリダイレクトポリシーを無効にします。

言語サポート

Mac 向け Citrix Workspace アプリがポルトガル語（ブラジル）で利用できるようになりました。

サードパーティの仮想チャネル読み込み機能強化

Mac 向け Citrix Workspace アプリで、サードパーティの仮想チャネルの読み込み機能が強化されました。そのため、ユーザーエクスペリエンスが次のように向上します:

- Citrix Workspace アプリをアンインストールしてから再インストールする場合に、サードパーティの仮想チャネル（RealTime Media Engine など）をインストールし直す必要はありません。
- 通常アカウント権限のユーザーでも、最適化された Real Time Optimization Pack の機能を利用できます。RealTime Media Engine が管理者によりインストールされている場合も同様です。

1912 の新機能

Workspace のインテリジェント機能

このバージョンの Mac 向け Citrix Workspace アプリは、今後リリースされるインテリジェント機能を使用するように最適化されています。詳しくは、「Workspace のインテリジェント機能 - マイクロアプリ」を参照してください。

1910.2 の新機能

このリリースで、Citrix Workspace 更新プログラムと macOS Catalina の問題が解決されます。

- Mac 向け Citrix Workspace アプリ 1910 および 1910.1 を使用中の顧客が Citrix Workspace 更新プログラムで将来のアップデートを受信するには、Mac 向け Citrix Workspace アプリ 1910.2 に手動でアップグレードする必要があります。
- Mac 向け Citrix Workspace アプリ 1906 以前を使用中の顧客は、Mac 向け Citrix Workspace アプリ 1910.2 を Citrix Workspace 更新プログラムで入手できます。

1910.1 の新機能

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。

1910 の新機能

macOS Catalina のサポート

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

> 注:
>
> Mac 向け Citrix Workspace アプリと Citrix Viewer を macOS Catalina で初めて開くと、OS が Citrix Viewer からの通知を許可するように要求します。［許可］をクリックして Mac 向け Citrix Workspace アプリ関連の通知を受信します。

暗号の組み合わせの更新

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 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 では NetScaler 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。詳しくは、Knowledge Center の記事CTX250104を参照してください。

Citrix Casting の更新

Citrix Casting は、ユーザーがノートパソコンのカバーを閉じたときに自動的に切断されるようになりました。

1906 の新機能

Citrix Casting の更新

周辺機器を使用して Citrix Ready ワークスペースハブでセッションを制御します。ハブとデバイスの両方でキーボードとマウスを使用してセッションを管理できるようになりました。詳しくは、「Citrix Ready ワークスペースハブ」を参照してください。

言語サポート

Mac 向け Citrix Workspace アプリがオランダ語で利用できるようになりました。

1903.1 の新機能

Citrix Casting の更新

Citrix Casting は、新機能および機能強化によって総合的に更新されました。Citrix Casting について詳しくは、「Citrix Casting」を参照してください。

1901 の新機能

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。

1812 の新機能

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。このリリースでは、Mac の画面をワークスペースハブに接続されたモニターにミラーリングするためのサポートが提供されています。

Citrix Casting について詳しくは、「Citrix Casting の構成」を参照してください。

キーボードレイアウトの同期

このリリース以降、Mac 向け Citrix Workspace アプリはセッションでクライアントから Linux VDA にキーボードレイアウトを動的に同期できます。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、たとえば、キーボードのレイアウトを英語からスペイン語に変更するときに、一貫したユーザーエクスペリエンスを提供します。

キーボードレイアウトの構成について詳しくは、「キーボードレイアウト」を参照してください。Linux VDA でのキーボードレイアウトの同期の構成について詳しくは、「動的なキーボードレイアウトの同期」を参照してください

クライアント IME 機能の拡張

このリリース以降、Mac 向け Citrix Workspace アプリはクライアント側の IME 入力および Linux VDA においてより優れたユーザーエクスペリエンスを提供します。この機能を使用すると、クライアントの IME 入力が以下の 2 つの点で向上します:

- 入力文字の候補一覧を表示するウィンドウは、以前のような左下隅ではなく常に挿入ポイントの横に表示されます。
- VDA に表示された入力文字には、確定文字と混同しないようにマークが付けられています。

クライアント IME 機能の拡張は、キーボードレイアウトの同期機能に依存します。

クライアント IME 機能の拡張を構成する方法について詳しくは、「拡張クライアント IME」を参照してください。Linux VDA でクライアント IME を構成する方法について詳しくは、「クライアント側 IME ユーザーインターフェイスの同期」を参照してください。

選択的 **H264**

選択的 H264 を使用すると、ビデオの再生時などに、画面の急激に変化する部分を H264 ストリームとして受信できます。選択的 H264 を有効にするには、［圧縮にビデオコーデックを使用する］ポリシーを ［領域をアクティブに変更］に設定します。

1809 の新機能

macOS Mojave のサポート

Mac 向け Citrix Workspace アプリは、ダークモードなどの macOS Mojave の機能を完全にサポートしています。

WebApp のサポート

Mac 向け Citrix Workspace アプリの Secure Browser が Cookie をサポートし、Citrix Gateway 使用時のリダイレクトをサポートするようになりました。

1808 の新機能

64 ビットのサポート

Mac 向け Citrix Workspace アプリは 64 ビット要件に完全準拠するようになりました。

> 注:
>
> Citrix Workspace アプリにアップグレードすると、ビット数が一致しないため最適化された Skype for Business（Lync）環境を利用できません。Mac 向け Citrix Workspace アプリは 64 ビット版ですが、現在インストールされているバージョンの RTME は 32 ビット版です。この問題を回避するために、RTME のプレビュー版の使用を検討してください。
>
> 注:
>
> 32 ビットのカスタム仮想チャネルは機能しなくなるため、64 ビットに更新する必要があります。

Federated 認証

Mac 向け Citrix Workspace アプリは、Azure Active Directory を使用した Federated 認証をサポートするようになりました。

リモート言語バーを表示または非表示にする

このリリースから、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。これ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す。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。

詳しくは、「構成」および Knowledge Center のCTX231913を参照してください。

> 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。

Citrix Analytics のサポート

Citrix Workspace アプリには、Citrix Analytics にログをセキュアに送信するための機能があります。有効になっている場合、ログは分析され、Citrix Analytics に保存されます。Citrix Analytics について詳しくは、Citrix Analyticsのドキュメントを参照してください。

解決された問題

2106 で解決された問題

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 で解決された問題

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 で解決された問題

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 で解決された問題

- 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 で解決された問題

- 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]

2010 で解決された問題

- 公開デスクトップまたはアプリケーションを起動しようとすると失敗し、エラーメッセージが表示されることがあります。この問題は、コンピューター名に特殊文字が含まれている場合に発生します。[CVADHELP-15492]
- 公開アプリケーションやデスクトップのセッションにサインインしようとすると失敗することがあります。この問題は、マウスを使用して［**OK**］をクリックしてサインインする場合に発生します。[CVADHELP-15300]

2009 で解決された問題

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。

2008 で解決された問題

VDA に EULA を追加した場合、公開デスクトップを起動しようとすると、灰色または黒色の画面が表示されることがあります。[CVADHELP-14986]

2007 で解決された問題

- ユーザーが Citrix Gateway で Enlightened Data Transport（EDT）を有効にすると、クライアントのオーディオ設定に問題がある場合に、Mac 向け Citrix Workspace アプリが予期せず終了することがあります。[CVADHELP-14686]
- Intel SDK が ［圧縮にビデオコーデックを使用する］ポリシーが有効になった VDA で使用されている場合、公開デスクトップを起動しようとすると緑の画面が表示されることがあります。[CVADHELP-13647]
- WMI（Windows Management Instrumentation）の遅延データを取得しようとすると、Mac 向け Citrix Workspace アプリバージョン 2002 および 2005 で失敗することがあります。[RFMAC-4325]

2006 で解決された問題

- Mac 向け Citrix Workspace アプリへのサインインに失敗し、無関係な UI が表示されることがあります。回避方法として、メニューで ［アプリケーション一覧の更新］をクリックしてストアを読み込みます。[RFMAC-4063]

2005 で解決された問題

- PIV スマートカードを使用して macOS Catalina で動作している Citrix Workspace アプリにサインインすると、失敗し、「指定のアカウントを検出できません」というエラーメッセージが表示されることがあります。[CVADHELP-14155]
- Microsoft Outlook の公開インスタンスのメインウィンドウがモーダルウィンドウにフォーカスがあるときに黒く表示される場合があります。[CVADHELP-14169]

2002 で解決された問題

- PIV スマートカードを使用して macOS Catalina（10.15.2）で動作している Citrix Workspace アプリ内でセッションを起動しようとすると、「1 つ以上のルート証明書が無効です」というエラーメッセージが表示されることがあります。[RFMAC-3365]
- 言語セットを中国語または日本語に設定している場合、公開アプリ（メモ帳など）での入力に失敗することがあります。[RFMAC-3556]

2001 で解決された問題

- MacBook で、最大表示色数ポリシーの値が 16 bpp に設定されている公開デスクトップを起動しようとすると、灰色の画面が表示され、応答しなくなることがあります。[CVADHELP-13605]
- DingTalk アプリで撮影したスクリーンショットを Microsoft Paint または Microsoft Word の公開インスタンスに貼り付けようとすると、失敗し、Microsoft Paint では空白の画面、Microsoft Word ではエラーメッセージが表示されることがあります。[CVADHELP-13938]

1912 で解決された問題

- Mac 向け Citrix Workspace アプリのバージョン 1812 または 1901 を使用している場合、公開アプリを画面上で移動しようとすると応答が遅くなります。[RFMAC-2300]
- PIV スマートカードを使用して macOS Catalina で動作している Citrix Workspace アプリにサインインしようとすると、失敗することがあります。[RFMAC-2788]
- Mac 向け Citrix Workspace アプリのバージョン 1909 を使用している場合、ファイル名が英語以外の ICA ファイルを開くと、Citrix Viewer が予期せず終了することがあります。[RFMAC-2986]
- Mac 向け Citrix Workspace アプリのアップグレード後に、公開されている Microsoft Outlook または PowerShell アプリを起動しようとすると、応答しないか、応答が遅くなります。[LD1192]
- 公開アプリのウィンドウを画面上で移動すると、更新されないか、更新が遅くなります。[LD1485]

1910.2 で解決された問題

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。

1910.1 で解決された問題

- MacBook Pro 2018 以降および FaceTime を使用している場合、ビデオプレビューの下部に緑色のバーが表示されることがあります。[RFMAC-2317]
- Citrix Gateway 経由でスマートカードを使用してセッションを起動すると失敗し、「リモート SSL の警告。ハンドシェイクに失敗しました」というエラーメッセージが表示されることがあります。[RFMAC-2727]
- SAML 認証が有効な場合、認証画面の動作が遅くなったり、応答しなくなったりすることがあります。この問題が発生した場合は、デバイスを再起動してください。[RFMAC-3047]
- サブスクライブ済みアプリの起動後にオートメーション権限を拒否すると、Mac 向け Citrix Workspace アプリが応答しなくなることがあります。[RFMAC-3048]

1910 で解決された問題

- Mac 向け Citrix Workspace アプリから別のアプリケーションにテキストをコピーすると、間違った文字が表示されることがあります。[RFMAC-2581]

- Mac 向け Citrix Workspace アプリへのサインインに通常より時間がかかる場合があります。[RFMAC-2608]
- プロキシを使用して接続すると、プロキシが予期せず終了することがあります。[RFMAC-2612]
- 複数のモニターを使用している場合、シームレスアプリでマウスの動きが同期しなくなることがあります。[RFMAC-2623]
- Mac 向け Citrix Workspace アプリに再度サインインすると、アプリが予期せず終了することがあります。[RFMAC-2679]
- Command+Tab ショートカットキーを使用してタブを切り替えると、仮想デスクトップが応答しなくなります。[RFMAC-2691]
- セキュリティ強化がオンになっていると、ShareFile アプリの起動に失敗します。[RFMAC-2724]
- Citrix Viewer が CPU を過剰に消費することがあります。[RFMAC-2777]

1906 で解決された問題

- スマートカードセッションがランダムに切断されることがあります。[RFMAC-1816, RFMAC-2313]
- セッションが切断されると、Mac 向け Citrix Workspace アプリが応答しなくなることがあります。[RFMAC-2137]
- Web ビューのウィンドウはすべてのアプリケーションの手前に表示されます。[RFMAC-2146]
- MacBook をスリープ状態から起動後、Mac 向け Citrix Workspace アプリが繰り返し認証を要求します。[RFMAC-2161]
- ログオン時に、サーバーが見つからないというエラーが表示されることがあります。[RFMAC-2192]
- シングルサインオンを構成せずに Web アプリを起動すると、資格情報が要求されずに 401 エラーが発生することがあります。[RFMAC-2194]
- セカンダリモニターに移動すると、シームレスアプリケーションのウィンドウが表示されなくなることがあります。[RFMAC-2314]
- 「ページを読み込めませんでした」というエラーページが表示されることがあります。[RFMAC-2322]
- 公開されている Microsoft Outlook の使用中に、ユーザーがメニューを選択できないことがあります。[RFMAC-2335]
- Web フォームを使用すると認証エラーが表示されることがあります。[RFMAC-2349]
- Citrix Gateway 経由で接続を試行しているときに仮想サーバーで署名済み中間証明書の使用が構成されている場合、Mac 向け Citrix Workspace アプリが SSL エラー 61 で予期せず終了します。[RFMAC-2393]
- 特定の Web サイトの資格情報が消去され、ユーザーがサインインできなくなることがあります。[RFMAC-2394]
- Outlook Web アプリを起動すると、空白のページが表示されます。[RFMAC-2395]
- シームレスアプリケーションを最小化して最大化すると、アプリが正しく再描画しなくなることがあります。[RFMAC-2411]
- 公開アプリとして起動すると、ユーザーが Jira にファイルをアップロードできない可能性があります。[RFMAC-2467]

1903.1 で解決された問題

- デスクトップセッションを起動すると、Mac 向け Citrix Workspace アプリが予期せず終了することがあります。
- 特定のカスタムアプリケーションが起動しないことがあります。[RFMAC-2081]
- メモ帳アプリを移動すると、2 つ以上のアプリがアクティブなときにアプリがバックグラウンドに移動することがあります。[RFMAC-2107]
- Citrix Workspace のストアを編集しようとすると、代わりに Citrix Files の UI が表示されます。[RFMAC-2111]
- シームレスアプリの起動後、アプリが完全に起動される前にドックアイコンをクリックすると、セッションはシームレスではなくなります。[RFMAC-2139]
- MacBook をスリープ状態から起動後、Citrix Workspace が繰り返し認証を要求します。[RFMAC-2161]
- シームレス VDA セッションに再接続すると、セッション内のグラフィックが歪んで表示されることがあります。[RFMAC-2176]
- ローカルキーボードレイアウトと日本語キーボードを使用している場合、確定していない入力文字を削除すると正しく動作しないことがあります。[RFMAC-2287]

1901 で解決された問題

- Mac 向け Citrix Workspace アプリをアップグレードした後に、アプリが起動しないことがあります。[RFMAC-2003]
- USB オーディオリダイレクトが正常に機能しないことがあります。[RFMAC-2043]
- シームレスバージョンの Microsoft Outlook では、ドロップダウンメニューを選択できません。[RFMAC-2079]
- シームレスアプリケーションを使用している場合、セッションが応答しなくなることがあります。[RFMAC-2083]
- 複数のモニターに表示されたウィンドウを最小化または最大化するときに、セッションが応答しなくなることがあります。[RFMAC-2103]

1812 で解決された問題

- Microsoft Office アプリケーション内でヒントを閉じた後、ヒントが表示されていた場所に黒い領域が残ります。[RFMAC-1793]
- Retina ディスプレイの場合、セッションがぼやけて表示されることがあります。[RFMAC-1944]
- 3 台のモニターで実行されているセッション中にトラックパッドで 3 本指でのスワイプジェスチャを使用すると、正しく動作しないことがあります。[RFMAC-1968]
- Citrix Viewer をバックグラウンドで実行している場合、App Nap 機能が働くことがあります。[RFMAC-1979]
- ネットワーク接続が切断された後、ネットワークに再接続すると、ログオンページが表示されるまでに通常より長い時間がかかることがあります。[RFMAC-2001]

- delete キーを押すと、複数の文字が削除されることがあります。[RFMAC-2011]
- YouTube の動画を 3 分以上再生すると、EDT が有効になっている VDA が応答しなくなることがあります。[RFMAC-2017]
- Citrix Receiver Launcher が Google Chrome に登録されている場合、Citrix Workspace アプリにアップグレードすると、セッションが Chrome から起動しなくなります。[RFMAC-2020]
- ［圧縮にビデオコーデックを使用する］ポリシーが正常に機能しない場合があります。[RFMAC-2021]

1809 で解決された問題

- 再接続したセッションが接続されていないことがあります。[RFMAC-1823]

1808 で解決された問題

- デュアル GPU の Mac デバイスで、クライアントがバッテリー電源で電力効率の高い統合 GPU ではなく単体 GPU を使用することがあります。[RFMAC-1439]
- JamF が同時にインストールされている場合、クライアントが正しくアップグレードされないことがあります。[RFMAC-1523]
- USB デバイスは、一般的な USB のリダイレクトに使用しようとするとセッションに表示されないことがあります。[RFMAC-1592]
- クライアントの更新プログラムを確認するときに、「更新の確認の問題」エラーが発生することがあります。[RFMAC-1589]
- 複数の公開アプリウィンドウが開いている場合、公開アプリケーションウィンドウをアクティブにすると、別の公開アプリウィンドウが最前面に表示されることがあります。[RFMAC-1696]

既知の問題

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]

2010 の既知の問題

- Skype for Business では、着信ビデオは macOS Big Sur（11.0.1）で表示されません。
- 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]
- MacBook Pro 2018 以降および FaceTime を使用している場合、ビデオプレビューの下部に緑色、黒、または歪んだ長方形のバーが表示されることがあります。[RFMAC-2829]

2009 の既知の問題

macOS Big Sur Beta

- クラウド展開では、公開デスクトップの起動時に、背景色が一致しない場合があります。この問題は、一部の macOS Big Sur Beta バージョンで断続的に発生します。[RFMAC-6343]
- **CitrixWorkspaceApp.dmg** ファイルを開いたときに、Mac 向け Citrix Workspace アプリのインストーラーアイコンが表示されない場合があります。この問題は、一部の macOS Big Sur Beta バージョンで断続的に発生します。[RFMAC-6378]

Microsoft Teams の最適化（プレビュー）

- Mac 向け Citrix Workspace アプリで Microsoft Teams の画面共有を使用する場合、共有できるのはサードパーティアプリケーション（Microsoft PowerPoint など）のみです。ただし、受信画面共有は完全にサポートされています。[RFMAC-3403]
- 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]
- Microsoft Teams での最適化されたビデオ通話でカメラデバイスを切り替えると、HDX RealTime Connector エンジンが予期せず終了する場合があります。[RFMAC-6157]
- Microsoft Teams でネットワークを切り替えると、音声通話とビデオ通話が切断される場合があります。[RFMAC-6292]
- 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]

2008 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。

2007 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。

2006 での既知の問題

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。

2005 の既知の問題

- Mac 向け Citrix Workspace アプリへのサインインに失敗し、無関係な UI が表示されることがあります。回避方法として、メニューで ［アプリケーション一覧の更新］をクリックしてストアを読み込みます。[RFMAC-4063]

2002 の既知の問題

- Mac 向け Citrix Workspace アプリでは、32 ビットの公開アプリでのみ Web カメラリダイレクトがサポートされます。そのため、64 ビットの公開アプリである Microsoft Teams アプリでは Web カメラのリダイレクトを利用できません。[RFMAC-2199]
- Mac 向け Citrix Workspace アプリでは、高 DPI（Retina）ディスプレイはサポートされていません。その結果、Retina ディスプレイ搭載デバイスで文字がぼやけて表示されることがあります。[RFMAC-650]

- PIV スマートカードを使用して macOS Catalina で動作している Citrix Workspace アプリにサインインすると、失敗し、「指定のアカウントを検出できません」というエラーメッセージが表示されることがあります。[CVADHELP-14155]

2001 の既知の問題

- PIV スマートカードを使用して macOS Catalina で動作している Citrix Workspace アプリにサインインすると、失敗し、「指定のアカウントを検出できません」というエラーメッセージが表示されることがあります。[CVADHELP-12609]
- PIV スマートカードを使用して macOS Catalina（10.15.2）で動作している Citrix Workspace アプリ内でセッションを起動しようとすると、「1 つ以上のルート証明書が無効です」というエラーメッセージが表示されることがあります。[RFMAC-3365]

1912 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。

1910.2 の既知の問題

- PIV スマートカードを使用して macOS Catalina で動作している Citrix Workspace アプリにサインインすると、失敗することがあります。[RFMAC-2788]

1910.1 の既知の問題

- PIV スマートカードを使用して macOS Catalina で動作している Citrix Workspace アプリにサインインすると、失敗することがあります。[RFMAC-2788]

1910 の既知の問題

- MacBook Pro 2018 以降および FaceTime を使用している場合、ビデオプレビューの下部に緑色のバーが表示されることがあります。[RFMAC-2317]
- Citrix Gateway 経由でスマートカードを使用してセッションを起動すると失敗し、「リモート SSL の警告。ハンドシェイクに失敗しました」というエラーメッセージが表示されることがあります。[RFMAC-2727]
- PIV スマートカードを使用して macOS Catalina で動作している Citrix Workspace アプリにサインインすると、失敗することがあります。[RFMAC-2788]
- SAML 認証が有効な場合、認証画面の動作が遅くなったり、応答しなくなったりすることがあります。この問題が発生した場合は、デバイスを再起動してください。[RFMAC-3047]
- サブスクライブ済みアプリの起動後にオートメーション権限を拒否すると、Mac 向け Citrix Workspace アプリが応答しなくなることがあります。この問題を回避するには、［システム環境設定］**>**［セキュリティ

とプライバシー］**>**［プライバシー］**>**［オートメーション］の順に選択し、Citrix Viewer アプリ、Citrix Workspace アプリ、およびすべてのサブスクライブ済みアプリに対する権限を許可します。[RFMAC-3048]

1906 の既知の問題

- MacBook Pro 2018 以降および FaceTime を使用している場合、ビデオプレビューの下部に緑色のバーが表示されることがあります。[RFMAC-2317]

1903.1 の既知の問題

- スマートカードセッションがランダムに切断されることがあります。[RFMAC-1816]
- ログオン時に、サーバーが見つからないというエラーが表示されることがあります。[RFMAC-2192]
- MacBook Pro 2018 以降および FaceTime を使用している場合、ビデオプレビューの下部に緑色のバーが表示されることがあります。[RFMAC-2317]

1901 の既知の問題

- スマートカードセッションがランダムに切断されることがあります。[RFMAC-1816]

1812 の既知の問題

- スマートカードセッションがランダムに切断されることがあります。[RFMAC-1816]
- USB オーディオリダイレクトが正常に機能しないことがあります。[RFMAC-2043]

1809 の既知の問題

- Safari バージョン 12 を使用している場合、アプリセッションやデスクトップセッションが起動しないことがあります。この問題を回避するには、Knowledge Center のCTX238286を参照してください。回避策の実行後は、ユーザーはセッションを開始するたびに Safari に権限を許可する必要があります。

1808 の既知の問題

- セキュアな SaaS アプリでエラーが発生すると、ブラウザーに表示されるエラーはローカライズされません。[RFMAC-1836]

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

システム要件と互換性

June 10, 2021

サポートされてい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 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、シトリックス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

- 257.7MB 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ケーション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 への以下の接続をサポートします:

- HTTP
- 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）、信頼されていない証明書の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。中間証明書を Citrix Gateway アプライアンスにインストールして、プライマリ CA とリンクする方法については、How to Install and Link Intermediate Certificate with Primary CA on Citrix Gateway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。例えば、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。また、ルート証明書の有効期限についても注意してください。
>
> 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。正しく検証される証明書が見つかり、信頼済みである場合（「ルート証明書サンプル」など）、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
>
> 証明機関によっては、クロスルート用中間証明書を使用します。これは、複数のルート証明書がある場合を想定しています。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 *

	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）
2 要素（セキュリティトークンがあるドメイン）*				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

April 10, 2021

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：

- シトリックスの 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

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。

シトリックス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。このためのファイルは、シトリックスの Web サイト（ダウンロード）からダウンロードできます。

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て開きます。
2. ［はじめに］ページで ［続ける］をクリックします。
3. ［使用許諾契約］ページで ［続ける］をクリックします。
4. 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。
5. ［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。
6. ［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 ［続行］をクリックします。
7. 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、シトリックス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。また、Citrix Workspace アプリアイコンを右クリックしてから ［更新の確認］をクリックして、更新またはアップグレードが利用可能かを確認することもできます。

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へのアップグレードを実行すると、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。

構成

July 7, 2021

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、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、システムが Apple 社のmacOS 10.15 での信頼された証明書の要件に準拠していることを確認してください。

機能フラグ管理

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、機能フラグと、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最新状態については、LaunchDarkly のステータス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

Content Collaboration サービスの統合

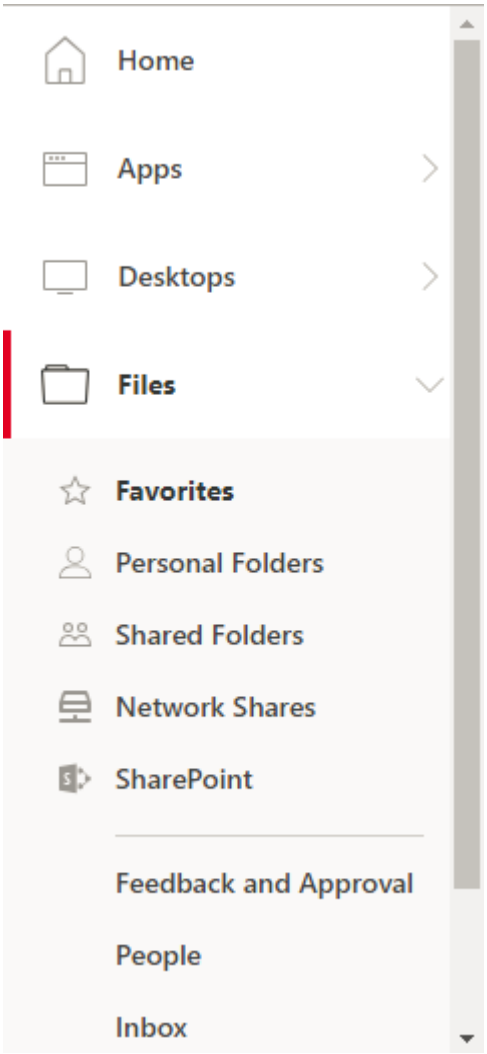
Citrix Content Collaboration を使用すると、ドキュメントを簡単かつセキュアに交換したり、メールで大容量のドキュメントを送信したり、サードパーティへのドキュメント転送をセキュアに処理したり、コラボレーションスペースにアクセスすることができます。

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。［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:
>
> Citrix Workspace アプリでの Citrix Content Collaboration の統合は、Windows Server 2012 および Windows Server 2016 ではサポートされていません。これは、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です。

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。たとえば、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。次に例を示します：

- 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。管理者は、リダイレクトする USB デバイスの一覧を変更して、仮想デスクトップで使用可能になる USB デバイスの種類を制限できます。詳しくは、このセクションの後半で説明します。

> ヒント
>
> Citrix では、ユーザーデバイスとサーバー間でセキュリティ境界による分離が必要な環境では、使用を禁止する USB デバイスの種類についてユーザーに通知することをお勧めします。

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。

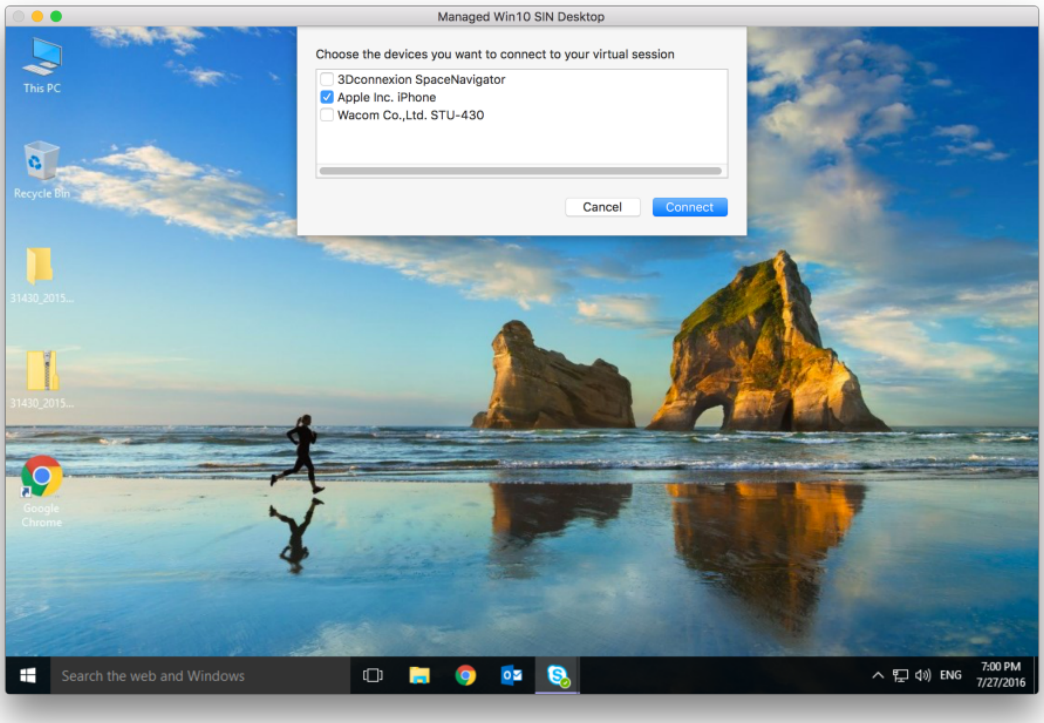
この製品は、USB 3.0 デバイスと USB 3.0 ポートを使用する最適化された仮想チャネルをサポートします。たとえば、CDM 仮想チャネルは、カメラ上でファイルを表示したり、ヘッドセットに音声を提供するために使用されます。USB 3.0 デバイスを USB 2.0 ポートに接続した場合も、汎用 USB リダイレクトがサポートされます。

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。問題が発生する場合は、汎用 USB 仮想チャネルを使用してください。

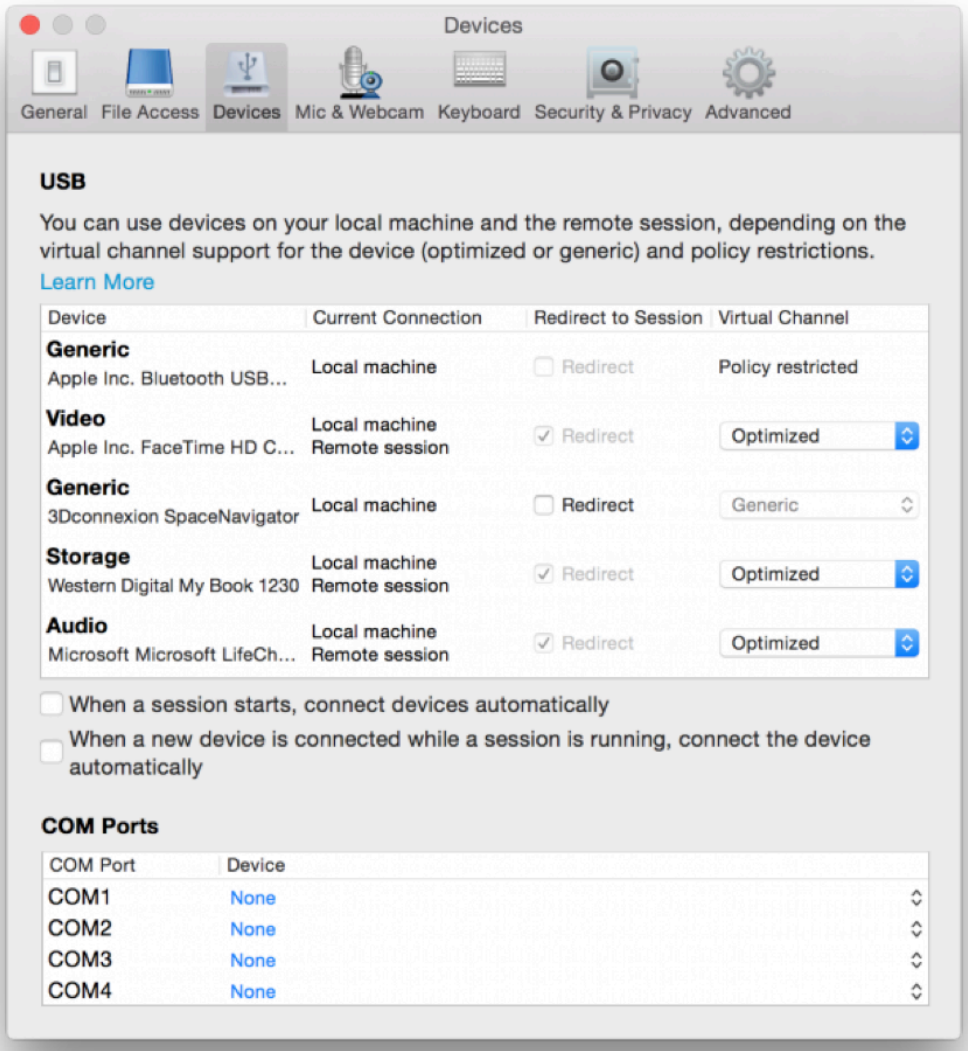
一部のデバイスはデフォルトではリダイレクトされず、ローカルセッションでのみ使用可能になります。たとえば、内部 USB で直接装着されたネットワークインターフェイスカード（NIC）は、リダイレクトには適しません。

USB リダイレクトを使用するには:

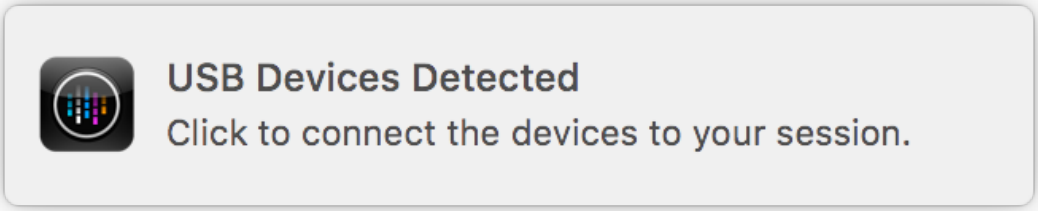
1. Mac 向け Citrix Workspace アプリがインストールされているデバイスに USB デバイスを接続します。
2. ローカルシステムで、使用できる USB デバイスを選択するメッセージが表示されます。



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。

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
```

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 リダイレクトで動作する 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 Data Traveller 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 リダイレクトで機能しません:

- 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シトリックスが検証していないデバイスはたくさんあります。以下は、これらのデバイスの一部です:

- 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 のポリシーで完全に制御できます。

アイソクロナスデバイスのサポート

USB デバイスのアイソクロナスクラスは、Mac 向け Citrix Workspace アプリの汎用 USB リダイレクトではまだサポートされていません。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 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るため、注意してください。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 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。

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。このとき、セッションウィンドウが閉じたりエラーメッセージが表示されたりする代わりに画面表示が保持され、バックグラウンドで再接続が試行されます。ネットワーク接続が回復すると、自動的にセッションでの作業を再開できるようになります。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
>
> 必要以上に長い時間を設定すると、接続の再開を待ちきれないユーザーが席を離れることがあります。その間に不正なユーザーがセッションにアクセスしてしまう危険性があります。

セッション画面の保持機能が有効な受信接続ではポート 2598 が使用されます。このポート番号は［セッション画面の保持のポート番号］ポリシー設定で変更できます。

切断したセッションに再接続するユーザーを再認証する場合は、クライアントの自動再接続機能を使用します。［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時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。

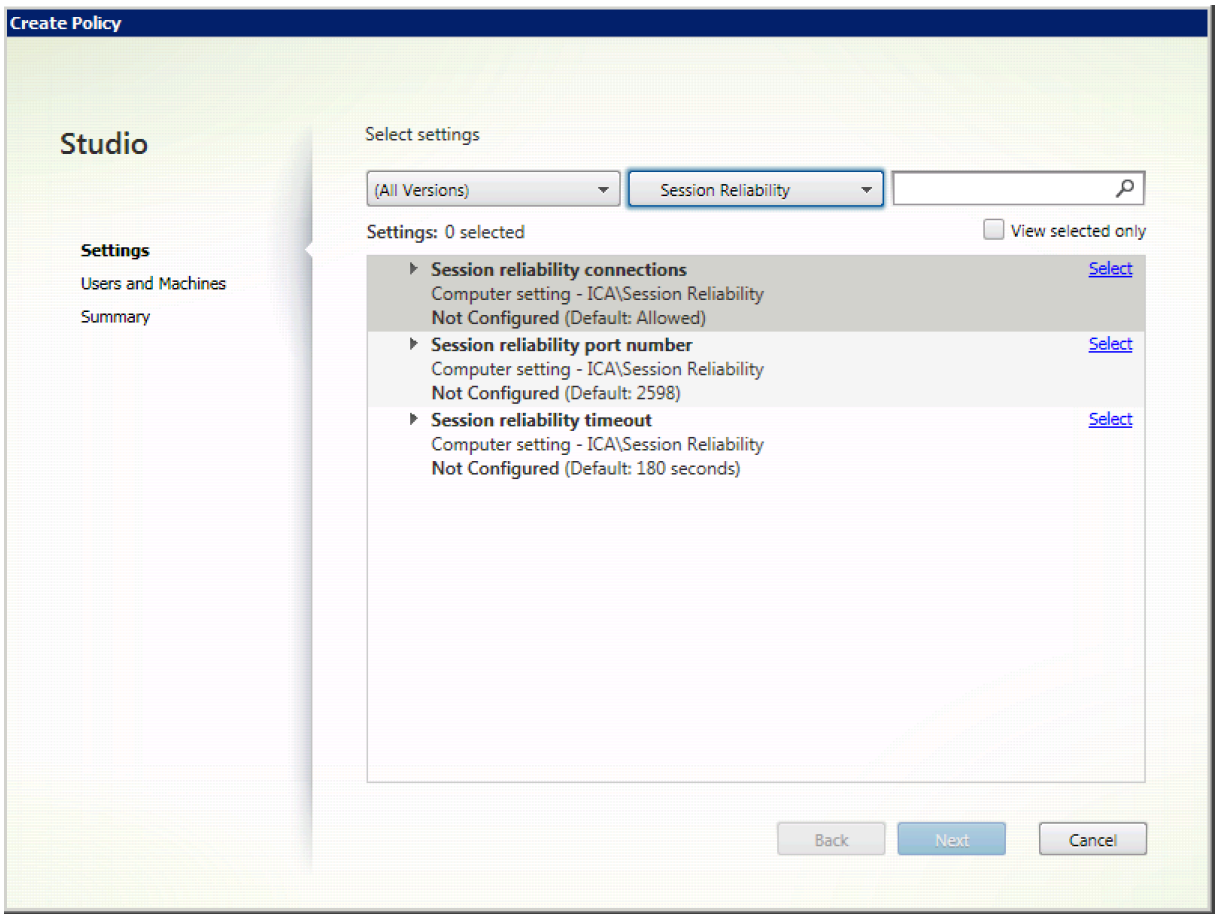
> 注
>
> セッション画面の保持は、サーバーでデフォルトで有効になっています。この機能を無効にするには、サーバーで管理するポリシーを構成します。

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:

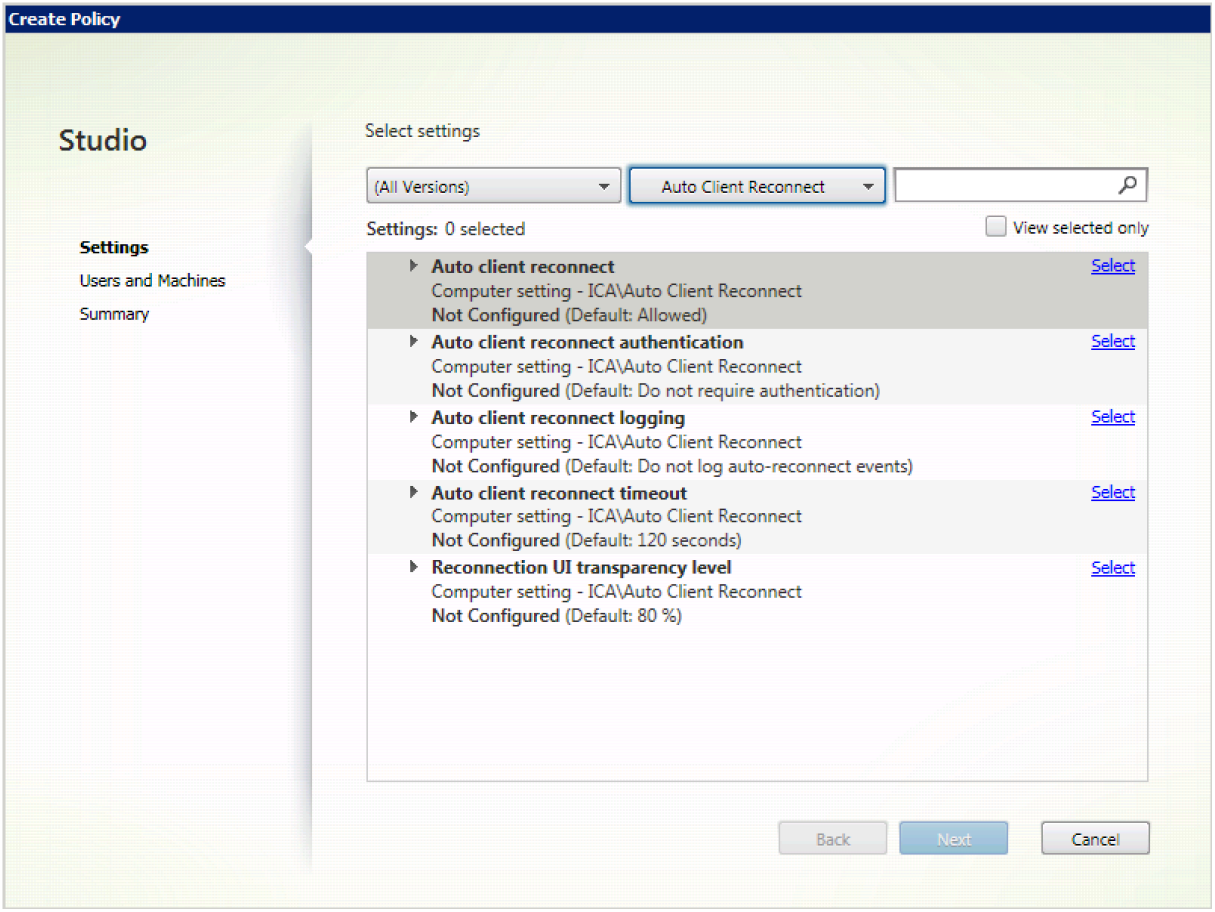
1. Citrix Studio を起動します。
2. [セッション画面の保持のタイムアウト] ポリシーを開きます。
3. タイムアウト値を編集します。
4. [**OK**] をクリックします。

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。この問題を解決するために、Mac 向け Citrix Workspace アプリのこのバージョンでは、セッション画面の保持および自動再接続テクノロジが強化されました。

自動再接続およびセッション画面の保持機能によって、ネットワークの中断からの回復後、Mac 向け Citrix Workspace アプリ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大幅に向上できます。

> 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。

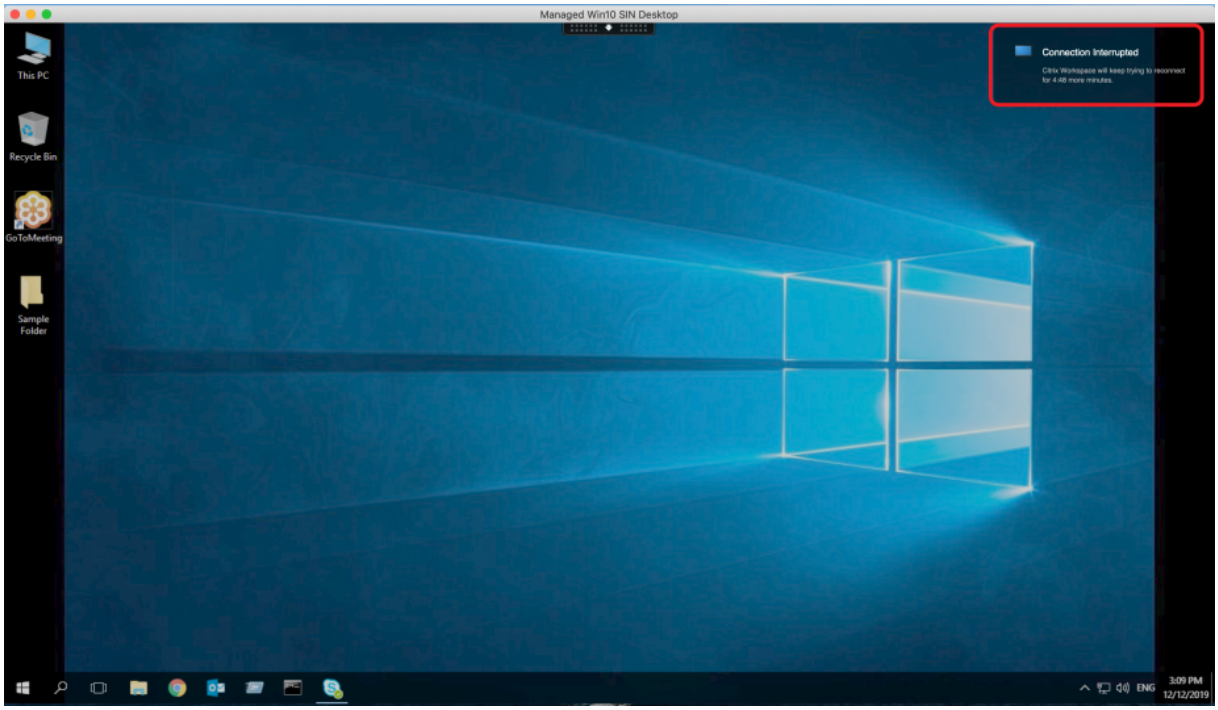
設定	例	デフォルト
SessionReliabilityTTL	SessionReliabilityTTL=120	180

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：

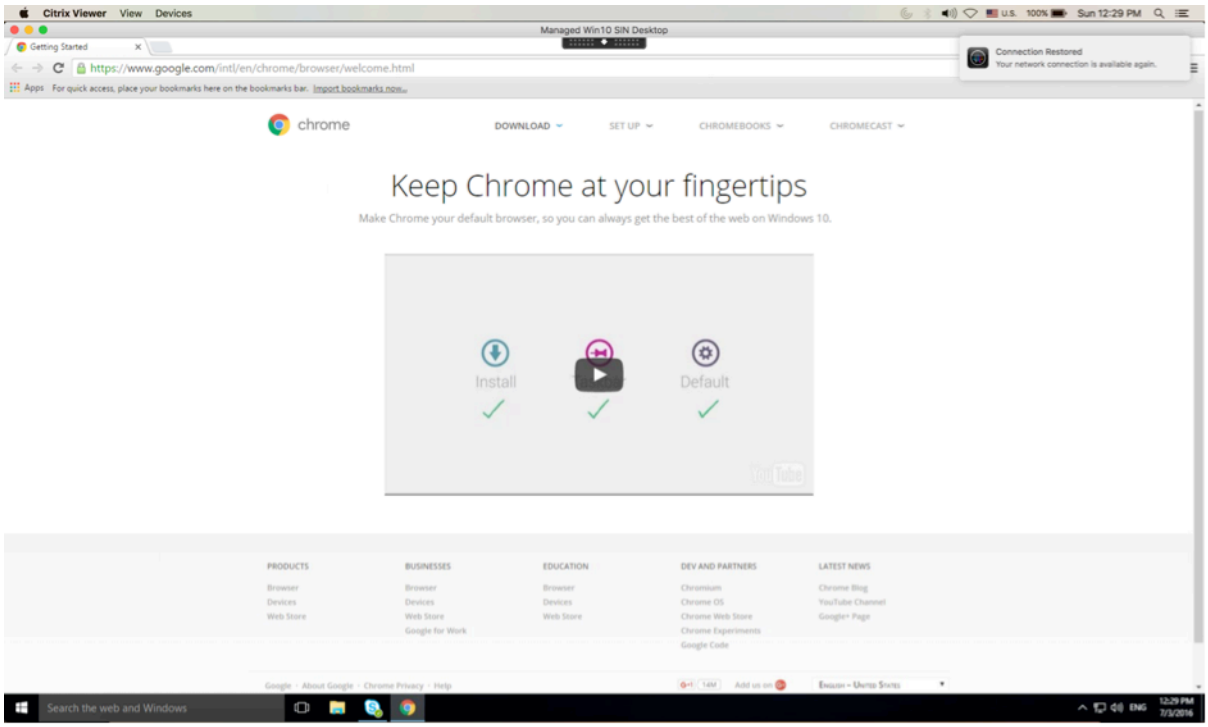
- 再接続中は、セッションウィンドウが灰色になります。セッションを再接続するまでの残り時間がカウントダウンタイマーで表示されます。セッションがタイムアウトになると、接続は切断されます。

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**）

収集されたデータ	説明	使用目的
構成および使用状況データ	Ctrix 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状況データが収集され、Citrix および Google Analytics に自動的に送信されます。	このデータは、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 Citrix によって使用させていただきます。

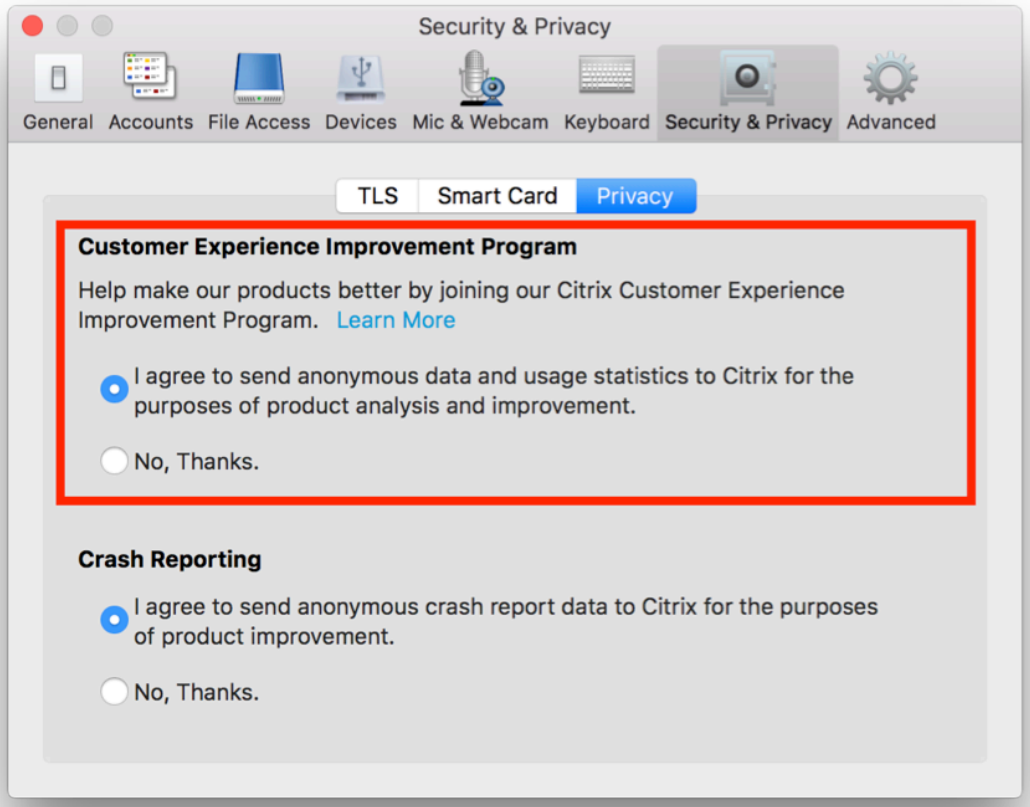
追加情報

Citrix は、お客様のデータを Citrix との契約条件に従って処理し、Citrix Trust CenterのCitrix Services Security Exhibitにおいて指定されているとおりにお客様のデータを保護します。

Citrix は、CEIP の一環として、Google Analytics を使用して Citrix Workspace アプリから特定のデータを収集します。Google でのGoogle Analytics のために収集されたデータ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 データの送信をオフにすることができます。これを行うには、次の操作を行います。

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 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、公開アプリケーションについてわかりやすい説明を付加してください。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、お勧めのアプリケーションキーワード設定を構成できます。

- アプリケーションがストアのユーザー全員に自動的にサブスクライブされるようにするには、Citrix Virtual Apps でそのアプリケーションを公開するときに、説明に「KEYWORDS:Auto」という文字列を追加します。ユーザーがストアにログオンすると、アプリケーション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。これを行うには、アプリケーションの説明として「KEYWORDS:Featured」という文字列を追加します。

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。このような、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

このコマンドにより、更新が利用可能かを 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 - このオプションは、更新が利用可能なときに通知します。

- Manual - このオプションは、更新が利用可能であっても通知しません。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 - このオプションは、［Citrix Workspace 更新プログラム］を無効にします。

auto-update-DeferUpdate-Count

このコマンドは、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 – ユーザーは、更新が利用可能になったときに、［後で通知する］オプションを選択できます。
- 0 - ユーザーは、更新が利用可能になった時に、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

このコマンドは、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は、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は、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は、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（管理者として実行している場合など）で実行しているリモートアプリケーションは、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。
- RDP がアプリケーションとして展開され、ユーザーが RDP セッションで作業をしていると、キーボードレイアウトを Alt + Shift ショートカットで変更することはできません。この問題を回避するには、RDP セッションの言語バーでキーボードレイアウトを切り替えます。

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 Workspace**/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

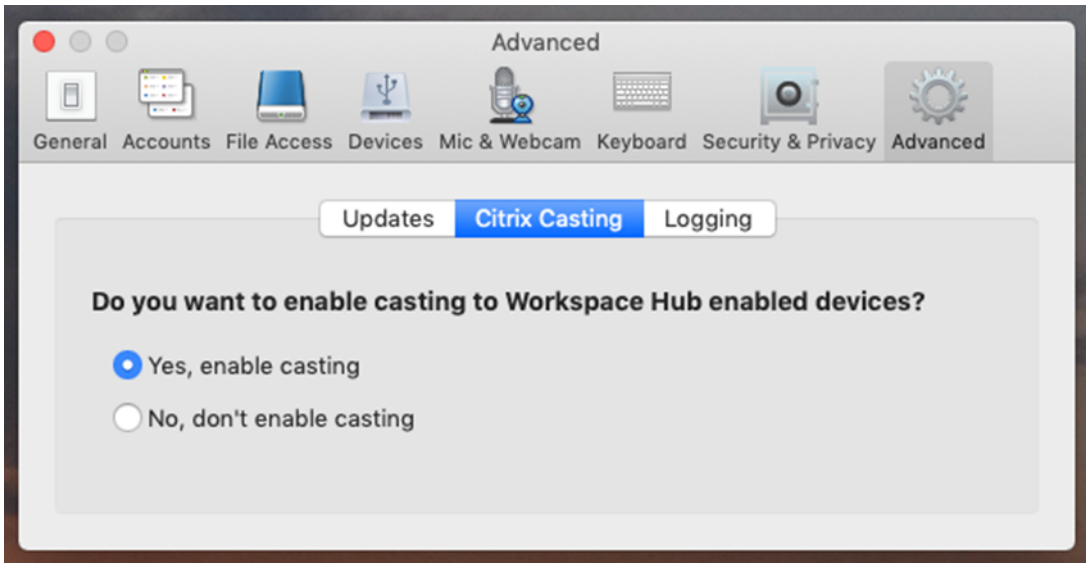
- Mac 向け Citrix Workspace アプリ 1812 以降。
- ハブ検出のためにデバイス上で Bluetooth が有効になっている。
- Citrix Ready ワークスペースハブと Citrix Workspace アプリが、同じネットワーク上に存在する。

- 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。

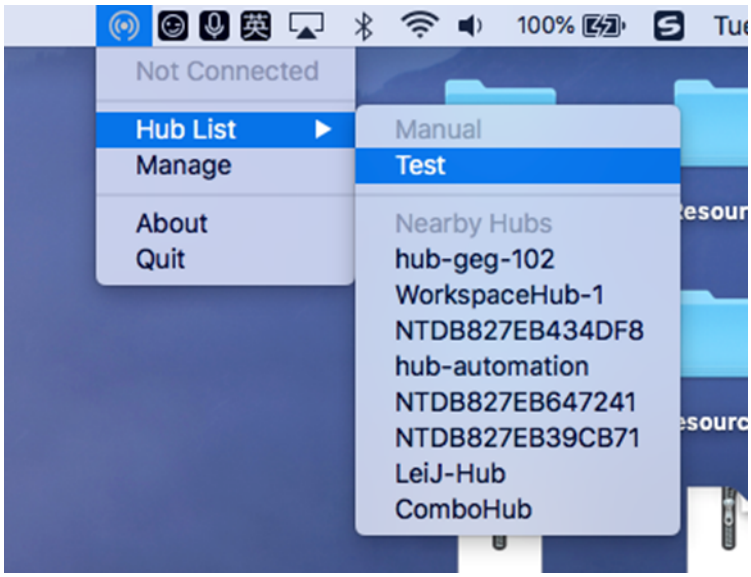
> 注:
>
> いったん有効にすると、［環境設定］**>**［詳細］**>**［**Citrix Casting**］で ［いいえ。キャストを有効にしません］を選択して無効にするまで、Mac 向け Citrix Workspace アプリの実行時に毎回、Citrix Casting が自動的に起動します。

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。

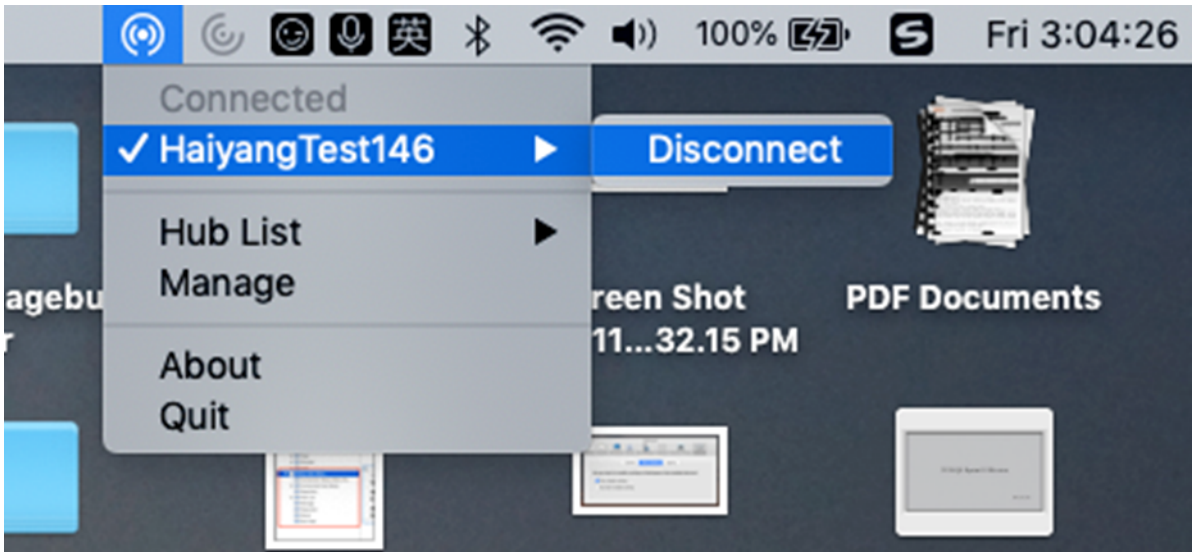
> 注:
>
> 現在、ミラーモードのみがサポートされています。［表示モード］列では、［ミラー］のみがオプションとして表示されます。

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、ユーザーデバイスに接続されたマイクをセッションで使用できます。**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、次のいずれかのオプションを選択します：

- 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。Mac 向け 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、英数字および句読点のキーを指します。特殊キーは単独では文字を入力しない修飾キーや制御キーを指し、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］
削除	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］
ホーム	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ーケルの設定と、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. Desktop Viewer を選択し、下向き矢印をクリックします。
2. ［ウィンドウ］を選択します。
3. Citrix Virtual Desktops の画面を複数のモニターの間にドラッグします。各モニターに画面の約半分が表示されていることを確認してください。
4. Citrix Virtual Desktops のツールバーで、［フルスクリーン］を選択します。

画面がすべてのモニターに拡張されます。

既知の制限事項

- 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。

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。フルスクリーンモードからウィンドウモードには次の方法により切り替えることができます:
  - OS X 10.10 の場合、ドロップダウンメニューバーで緑色のウィンドウボタンをクリックします。
  - OS X 10.9 の場合、ドロップダウンメニューバーで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の ［表示］メニューから ［フルスクリーンを解除］を選択します。
- ツールバードラッグの動作が更新され、複数モニターを使ったフルスクリーン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。これにより、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、医療従事者が病院の救急処置室のユーザーデバイスからログオフし、同じ病院のレントゲン室のワークステーションにログオンするとします。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、レントゲン室のユーザーデバイスにログオンするとセッション開始時に有効になります。

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下向き矢印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、ユーザーはセッション内で各自のローカルファイルを読み込んで、再びローカルドライブに保存したり、サーバーのドライブに保存したりできます。

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下向き矢印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。

認証

August 14, 2020

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、スマートカード対応のアプリケーション。これにより、仮想デスクトップまたは仮想アプリケーションのセッションで、ユーザーがドキュメントにデジタル署名を追加したり、ドキュメント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、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。シトリックスは次の操作について検証済みです。

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。

セキュリティで保護された通信

May 24, 2021

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 アドレスを外部インターネットアドレスにマップするネットワークファイアウォール（つまり NAT（Network Address Translation：ネットワークアドレス変換））を介して Mac 向け Citrix Workspace アプリを使用する場合は、外部アドレスを構成します。

> 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

例えば、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 社から引き継いだ時に、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：

Client cipher set	VDA cipher set	Direct connections								
		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			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 および TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 はサポートされていません。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 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。

企業の方針によっては、ルート証明書のインストールはエンドユーザーではなく管理者が行う場合があります。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。これにより、キーチェーンアクセスが起動します。
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可能になります。

TLS ポリシーについて

ここでは、Mac 向け Citrix Workspace アプリで 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
>
> デバイスが OS X サーバーなど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場合は、TLS ポリシーはほかの方法でも管理できます。

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。この設定により、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が指定されます。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。この機能により、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。この設定により、OS X クライアントで SSL 経由のリモートセッションを開く時に、所与の信頼されたルート証明機関を扱う方法を制御します。

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、単に 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 CA 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>
```

各項目の意味は次の通りです:

<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れを省略できます。

<value>: 設定の値です。値が配列で複数の値を設定する場合は、値をスペースで区切る必要があります。

```
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>
```

各項目の意味は次の通りです:

<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

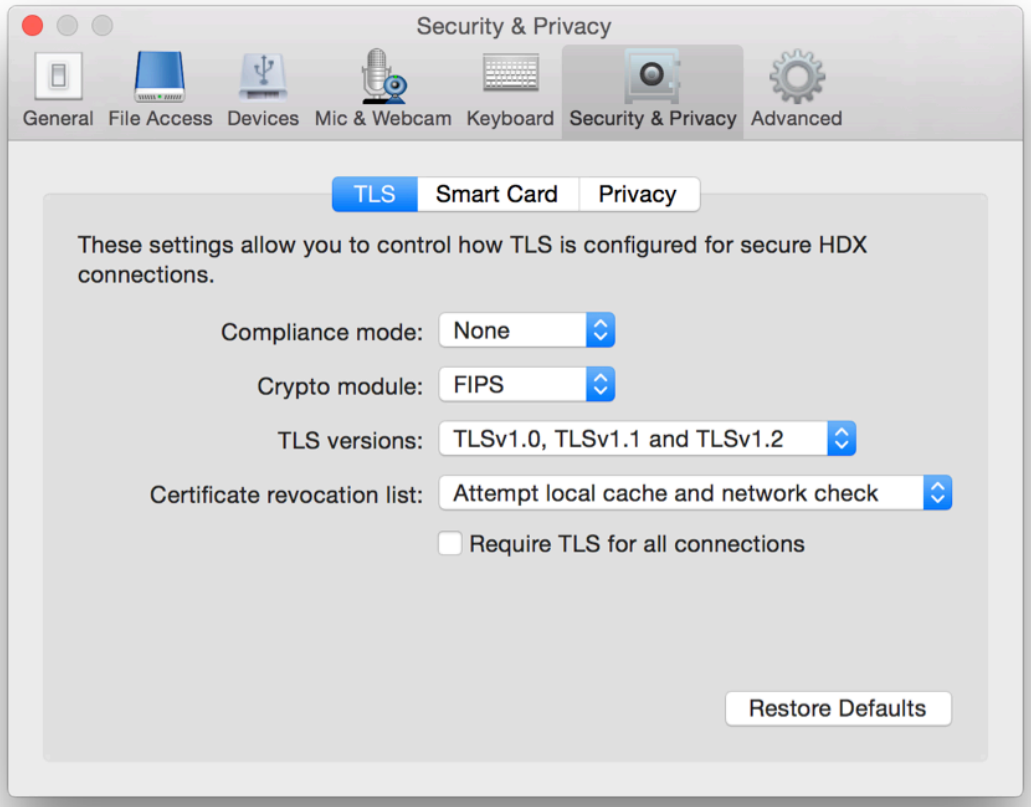
Citrix Receiver for Mac のバージョン 12.3 では、以下のようにさまざまなセキュリティ機能が強化されています:

- 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関連の構成設定は、UI から簡単にアクセスしやすくなりました。これによって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環境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 バージョンを使用したサーバーへの接続、接続に使用される暗号化アルゴリズム、モード、キーサイズ、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