Windows 向け Citrix Workspace アプリ 1912 LTSR

Contents

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

このリリースについて

September 25, 2023

1912 の新機能

累積更新プログラム 7（CU7）は、1912 LTSR の最新の更新プログラムです。

Microsoft Teams の機能強化

次の Microsoft Teams の機能強化は、CU6 以降のリリースでサポートされています：

Desktop Viewer が全画面モードの場合、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、ユーザーはすべての画面から 1 つを選択して共有できます。Desktop Viewer がウィンドウモードを変更（最大化、復元、または最小化）すると、画面共有が停止します。

次の Microsoft Teams の機能強化は、CU5 以降のリリースでサポートされています：

- 画面共有機能の向上 - 画面共有を行うと、Desktop Viewer 画面のみがネイティブビットマップ形式でキャプチャされるようになりました。
- ピアに、画面共有セッションで発表者のマウスポインターが表示されるようになりました。
- ビデオレンダリングの強化。
- パフォーマンスと信頼性の向上。
- WebRTC メディアエンジンは、クライアントデバイスで構成されたプロキシサーバーを優先するようになりました。
- エコーキャンセル、自動利得制御、ノイズ抑制構成の機能強化：Microsoft Teams がこれらのオプションを構成する場合、Citrix リダイレクトの Microsoft Teams は構成された値を優先します。それ以外の場合、これらのオプションはデフォルトで True に設定されています。
- メディアトラフィックの優先ネットワークインターフェイスを構成できるようになりました。

  `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`に移動し、`NetworkPreference`（REG_DWORD）という名前でキーを作成します。

  必要に応じて、次のいずれかの値を選択します：

  - 1：イーサネット
  - 2：Wi-Fi
  - 3：携帯ネットワーク

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 5：ループバック
  - 6：任意

  デフォルトかつ値が設定されていない場合、WebRTC メディアエンジンは利用可能な最適なルートを選択します。

- オーディオデバイスモジュール 2（ADM2）を無効にして、従来のオーディオデバイスモジュール（ADM）をクアッドチャネルマイクに使用できるようになりました。これは、通話中のマイクに関連する問題の解決に役立ちます。

  ADM2 を無効にするには、\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream に移動してDisableADM2という名前（REG_DWORD）でキーを作成し値を1に設定します。

- DirectWShowは現在デフォルトのレンダラーです。

  デフォルトのレンダラーを変更するには、次の手順を実行します：

  - レジストリエディターを起動します。
  - 次のキーの場所に移動します：HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream。
  - 次の値を更新します："UseDirectShowRendererAsPrimary"=dword:00000000

    その他の設定可能な値：

    * 0：メディアファンデーション
    * 1：DirectShow（デフォルト）
  - Citrix Workspace アプリを再起動します。

> 注：
>
> - 拡張機能は、Microsoft Windows 10 デスクトップオペレーティングシステムのエンドポイントでのみサポートされます。
> - 拡張機能は、Microsoft Windows 7 および 8 オペレーティングシステムのエンドポイントではサポートされていません。
> - 拡張サポートは、Citrix Workspace アプリパッケージのインストール時に決定されます。オペレーティングシステムを Microsoft Windows バージョン 7 からバージョン 10 にアップグレードするときは、Citrix Workspace アプリをアンインストールすることをお勧めします。

App Protection

> 免責事項
>
> App Protection ポリシーはオペレーティングシステムの必要な機能へのアクセスをフィルタリングすることで有効になります（画面のキャプチャまたはキーボードの操作が必要な特定の API 呼び出し）。つまり、この App Protection ポリシーは、カスタムの目的別に構築されたハッカーツールに対しても保護を提供できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ただし、オペレーティングシステムの進化によって、画面のキャプチャやキーのログ記録には新しい方法が出てきます。引き続きこうした方法に対応していきますが、特定の構成や展開では完全な保護を保証することはできません。

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

> 注:
>
> 保護されたセッションの起動には、ネイティブの Citrix Workspace アプリのみを使用することをお勧めします。

App Protection は、StoreFront と Controller の間で構成されます。Controller での App Protection の構成については、App Protectionのドキュメントを参照してください。この構成は、次のいずれかの方法で App Protection コンポーネントを含めることで、Citrix Workspace アプリに適用されます:

- グラフィカルユーザーインターフェイス
- コマンドラインインターフェイス

Citrix Workspace アプリのインストール時またはオンデマンドインストール時に、App Protection コンポーネントを含めることができます。

> 注:
>
> - この機能は、Windows 10、Windows 8.1、および Windows 7 などの Microsoft Windows デスクトップオペレーティングシステムでのみサポートされます。
> - この機能は、リモートデスクトッププロトコル（RDP）ではサポートされません。

Citrix Workspace アプリでの App Protection の構成について詳しくは、「App Protection」を参照してください。

App Protection の機能強化　以前は、保護されたウィンドウのスクリーンショットを撮影しようとすると、バックグラウンドの保護されていないアプリを含む画面全体が黒く表示されていました。

Snipping Tool を使ってスクリーンショットを撮ると、保護されたウィンドウだけが黒く表示される、または非表示になります。保護されたウィンドウの外側の領域のスクリーンショットを撮ることができます（Aero モードが無効で画面全体が黒く塗りつぶされる場合を除く）。

ただし、**PrtScr** キーを使用してスクリーンショットをキャプチャしている場合は、Citrix Workspace アプリを終了する必要があります。

さらに、このリリースでは、App Protection 機能を向上させるために問題に対応しています。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

インストーラーの強化

以前のリリースでは、ユーザーがインストールしたアプリのインスタンスを含むシステムに管理者が Citrix Workspace アプリをインストールしようとすると、インストールがブロックされていました。

このリリースでは、Citrix Workspace アプリのユーザーがインストールしたインスタンスを管理者が上書きし、インストールを正常に続行できるようになりました。

Citrix Workspace 更新プログラム の強化

以前のリリースでは、管理者が Citrix Workspace アプリをインストールした場合、管理者以外のユーザーはそのアプリを更新できませんでした。

このリリースでは、管理者以外のユーザーが、管理者がインストールしたインスタンスの Citrix Workspace アプリを更新できます。この処理を行うには、システムトレイ内の Citrix Workspace アプリアイコンを右クリックし、[更新の確認] を選択します。

> 注:
>
> Citrix Workspace アプリのユーザーがインストールしたインスタンスと管理者がインストールしたインスタンスの両方で、[更新の確認] オプションが使用できるようになりました。

送信プロキシのサポート

スマートコントロールを使用すると、管理者は詳細なポリシーを定義して、Citrix Gateway を使用して仮想アプリと仮想デスクトップのユーザー環境属性を構成および適用できます。たとえば、ユーザーがドライブをリモートデスクトップにマップできないようにしたい場合があります。Citrix Gateway のスマートコントロール機能を使用してこれを実現できます。

ただし、Citrix Workspace アプリと Citrix Gateway が別々のエンタープライズアカウントに属している場合には、シナリオは変わります。このようなシナリオでは、クライアントドメインに Gateway が存在しないため、クライアントドメインはスマートコントロール機能を適用できません。代わりに、送信 ICA プロキシを利用できます。送信 ICA プロキシを使用すると、Citrix Workspace アプリと Citrix Gateway が異なる組織に展開されている場合でも、スマートコントロール機能を使用できます。

Citrix Workspace アプリは、Citrix ADC LAN プロキシを使用したセッションの起動をサポートします。単一の静的プロキシを設定することも、送信プロキシプラグインを使用して実行時にプロキシサーバーを選択することもできます。

送信プロキシは、次の方法を使用して構成できます:

- 静的プロキシ: プロキシのホスト名とポート番号を指定してプロキシサーバーを構成します。
- 動的プロキシ: プロキシプラグイン DLL を使用して、1 つ以上のプロキシサーバーから 1 つのプロキシサーバーを選択できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

グループポリシーオブジェクト管理用テンプレートとレジストリエディターを使用して、送信プロキシを構成できます。

送信プロキシについて詳しくは、Citrix Gateway のドキュメントの「送信 ICA プロキシのサポート」を参照してください。

Citrix Workspace アプリでの送信プロキシの構成について詳しくは、「送信プロキシ」を参照してください。

Citrix 組み込みブラウザーバイナリ

このリリースでは、Citrix 組み込みブラウザーはインストールされなくなりました。バージョン 1912 にアップグレードすると、Citrix 組み込みブラウザーは削除されます。

Citrix 組み込みブラウザーがない場合、次の機能が変わります:

- ブラウザーコンテンツのリダイレクトは機能しません。
- SaaS アプリと Web アプリは、Citrix 組み込みブラウザーを使用して起動されません。代わりに、Citrix Secure Browser サービスで起動されます。

Microsoft Teams とのデスクトップ共有の強化

Microsoft Teams を使用してワークスペースを共有する場合、Citrix Workspace アプリは、現在共有されているモニターの領域を囲む赤い枠線を表示します。Desktop Viewer ウィンドウのみを共有することも、その上に重ねられたローカルウィンドウを共有することもできます。Desktop Viewer ウィンドウを最小化すると、画面共有が一時停止します。

Microsoft Teams でのエンドポイントエンコーダーのパフォーマンス見積もりツール

HdxTeams.exe プロセス（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）を開始すると、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ります。使用できる値は、240p、360p、720p、1080p です。

HdxTeams.exe が初期化されると、パフォーマンスの見積プロセス(`webrtcapi.EndpointPerformance` とも呼ばれます）が実行されます。マクロブロックコードは、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します。ピア間、またはピアと会議サーバー間のコーデックネゴシエーション中に、可能な限り高い解像度が使用されます。

エンドポイントエンコーダーの構成については、「Microsoft Teams でのエンドポイントエンコーダーパフォーマンス見積もりツール」を参照してください。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「Microsoft Teams の最適化」を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Analytics Service の機能強化

このリリースの Citrix Workspace アプリには、最新のネットワークホップのパブリック IP アドレスを Citrix Analytics Service にセキュアに送信するための機能があります。このデータは、セッションの起動ごとに収集されます。Citrix Analytics Service は、パフォーマンスの低下に関する問題が特定の地域に関連しているかどうかを分析するのに役立ちます。デフォルトでは、IP アドレスログは Citrix Analytics Service に送信されます。ただし、レジストリエディターを使用して Citrix Workspace アプリでこのオプションを無効にすることができます。

IP アドレスログの送信を無効にするには、次のレジストリパスに移動し、`SendPublicIPAddress`キーを **Off** に設定します。

- 64 ビット Windows マシンの場合、次のパスです: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`。
- 32 ビット Windows マシンの場合、次のパスです: `HKEY_LOCAL_MACHINE\SOFTWARE \Citrix\Dazzle`。

> 注:
>
> - Citrix Workspace アプリは起動に使用されるすべての IP アドレスを送信しますが、IP アドレスの送信はベストエフォートで行われます。一部のアドレスは正確ではない可能性があります。
> - エンドポイントがイントラネット内で動作している閉じられた顧客環境では、URL`https://locus.analytics.cloud.com/api/locateip`がエンドポイントのホワイトリストに登録されていることを確認してください。

パフォーマンス分析がこの情報を使用する方法については、「パフォーマンスでのセルフサービス」を参照してください。

解決された問題

November 3, 2023

Windows 向け **Citrix Workspace** アプリ **1912 LTSR CU7**

Citrix Workspace アプリ 1912 LTSR CU6 との比較

コンテンツリダイレクト

- Desktop Viewer が全画面モードに設定されており、エンドポイントデバイスでデフォルトのブラウザーが最大化されている場合、コンテンツの双方向リダイレクト機能によってローカルのデフォルトのブラウザーウィ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ンドウが前面に表示されない場合があります。この問題は、ローカルのデフォルトのブラウザーが Internet Explorer 以外の場合に発生します。[CVADHELP-19041]

ログオン/認証

- Citrix Gateway URL を追加しようとすると、次のエラーメッセージが表示されて断続的に失敗する場合があります:

  認証サービスにアクセスできません。

  [CVADHELP-19415]

セッション/接続

- Storebrowse ユーティリティを使用して Citrix Gateway URL のリソースを列挙すると、構成された Delivery Controller の少なくとも 1 つに到達できない場合に失敗する可能性があります。[CVADHELP-15416]
- Citrix IME が有効になっていると、特定のサードパーティアプリケーションが応答せず、ユーザーセッションでのアプリケーションの起動が失敗する場合があります。この問題は、CtxIme モジュールに障害がある場合に発生します。[CVADHELP-18511]
- アプリを更新または起動しようとすると、「ストアにアクセスできません」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、特定のサブスクライブ済みアプリのショートカットの説明の取得に失敗した場合に発生します。

  現在アプリケーションを使用できません。しばらく待ってから再試行するか、ヘルプデスクに次の情報を知らせてください: ストアにアクセスできません。

  [CVADHELP-18736]
- **selfservice.exe** -**init** -**ipoll** -**exit** コマンドを使用した後、ユーザーセッションを起動しようとすると失敗する場合があります。[CVADHELP-19095]
- この修正により、**TWITaskbarGroupingMode** をまたはHKEY_LOCAL_MACHINEで **GroupNone** にHKEY_CURRENT_USER設定できます。**TWITaskbarGroupingMode** キーは、HKEY_LOCAL_MACHINE\SOFTWA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows などにあります。[CVADHELP-19106]

ユーザーエクスペリエンス

- マルチモニター環境で［操作時は低品質］ポリシーが有効になっている場合、ノートブックと外部モニターにまたがった画面が歪む可能性があります。[CVADHELP-19065]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Windows 向け Citrix Workspace アプリ 1912 LTSR CU6

Citrix Workspace アプリ 1912 LTSR CU5 との比較

クライアントデバイスの問題

- Citrix Workspace アプリセッションで、YouTube ビデオまたは Microsoft Teams 呼び出しを開始してからヘッドセットを切断すると、セッションが応答しなくなることがあります。[CVADHELP-17629]

インストール、アンインストール、アップグレード

- セルフサービスをインストールせずに Windows 向け Citrix Workspace アプリをバージョン CU4 からバージョン CU5 にアップグレードすると、次のプロンプトが表示されることがあります:

  サポートされていないバージョンからのアップグレード

  Citrix Workspace は、古いバージョンを自動的にアンインストールし、すべての設定を削除します。これらの設定は後で復元できます。それ以外は、すべてを手動で削除する必要があります。［**OK**］をクリックして続行します。

  [CVADHELP-18790]

ログオン/認証

- 間違ったパスワードを使用して Citrix Gateway にログオンすると、ユーザーアカウントをロックアウトしてしまう可能性のある複数回の認証を Storebrowse が試行します。[CVADHELP-17467]
- Citrix Gateway を介してスマートカードを使用しようとすると、初期化後に Citrix Workspace アプリの認証が失敗することがあります。15 分後に認証プロセスを更新すると、Citrix Workspace 内の組み込みブラウザーに 404 エラーメッセージが表示されることがあります。これにより、アプリを閉じて再度開くまで、アプリが認証ループで停止します。[CVADHELP-18305]

セッション/接続

- フォルダーリダイレクト共有がオフラインのときにフォルダーリダイレクトを使用して公開アプリケーションを開くと、次のエラーメッセージが表示されて失敗することがあります。

  「**Unable to launch application**」（アプリケーションを起動できません）

  [CVADHELP-16387]

- ［ユーザーごとに **1** つのインスタンスに制限］オプションと ［**vPrefer**］オプションを有効にして、ショートカットを使用してアプリケーションを開こうとすると、Citrix Director に接続失敗エラーが表示されることがあります。[CVADHELP-17372]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 電話会議中に、HDX 最適化モードで Microsoft Teams を使用 すると、着信のビデオ部分がちらつく場合があります。[CVADHELP-17398]
- Citrix Workspace アプリが、内部ストアの外部ビーコンをポーリングすることがあります。この修正により、ストアがゲートウェイなしで使用された場合は外部ビーコンはポーリングされません。[CVADHELP-18275]
- Citrix Workspace アプリを介して公開されたアプリケーションのショートカットは、適切な権限がないと作成できません。その結果、更新のたびにアイコンがユーザープロファイルにダウンロードされ、エンドポイントのキャッシュサイズが増加し、StoreFront 側の CPU 消費量が増加することがあります。[CVADHELP-18609]
- Mac 向け Citrix Workspace アプリから Windows 向け Citrix Workspace アプリへの、最適化された Microsoft Teams ピアツーピア呼び出しが、切断されることがあります。[CVADHELP-18696]
- クライアントに複数の NIC がある場合、クライアント IP アドレスを指定するアクセスポリシー規則を使用してデリバリーグループからセッションを起動すると、失敗することがあります。

  ```
  Rule: Set-BrokerAccessPolicyRule -Name <rulename> -includedClientIPs
   <Client ip address>
  ```

  [CVADHELP-18783]

システムの例外

- Citrix Authentication Manager（AuthManSvr.exe）は、ログオン中に予期せず終了することがあります。[CVADHELP-17233]

ユーザーエクスペリエンス

- マルチモニター環境でウィンドウモードでデスクトップウィンドウを開くと、次の動作が見られることがあります。

  モニター 1 で開いてモニター 2 にドラッグしたウィンドウが、モニター 2 ではなくモニター 1 で最大化されて表示されることがあります。

  [CVADHELP-17373]

ユーザーインターフェイス

- この修正により、複数のアカウントと現在のアカウントレジストリが構成されている場合に、必要なアカウントに切り替えることができます。[CVADHELP-17718]
- グループポリシーオブジェクトを使用して有効なストアと無効なストアを一緒に構成すると、有効なストアで最初に X1 ユーザーインターフェイスではなく、非 X1 または緑色の泡のユーザーインターフェイスが表示されることがあります。[CVADHELP-17942]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Workspace アプリでストアアカウントを無効にしても、［スタート］メニューまたはデスクトップから、アプリのショートカットが削除されないことがあります。[CVADHELP-18260]

Windows 向け Citrix Workspace アプリ 1912 LTSR CU5

Citrix Workspace アプリ 1912 LTSR CU4 以降の修正

クライアントデバイスの問題

- Citrix Workspace アプリ 1912 LTSR CU4 を使用している場合、COM ポートに接続されているデバイスが 9 台を超える場合、セッション内でのマッピングに失敗する可能性があります。[CVADHELP-17734]

インストール、アンインストール、アップグレード

- Windows 向け Citrix Workspace アプリを**/forceinstall** パラメーターを使用してアップグレードしようとすると、失敗することがあります。この問題は、Receiver クリーンアップユーティリティがクリーンアッププロセスの開始に失敗した場合に発生します。[CVADHELP-17656]

ログオン/認証

- Citrix Gateway セッションがタイムアウトになった場合、アプリケーションの起動時に Citrix Workspace が認証を要求しないことがあります。[CVADHELP-17187]

シームレスウィンドウ

- 一部のサードパーティアプリケーションは前面に残り、起動された他のアプリケーションがバックグラウンドに保持される場合があります。[CVADHELP-16897]

セキュリティの問題

- USB .cat ファイルが SHA-1 証明書で署名されている場合、Windows 向け Citrix Workspace アプリ 1912 LTSR をインストールしようとすると失敗する可能性があります。[CVADHELP-17679]

セッション/接続

- GPU シンクライアント上で HTML またはアニメーションを使用する一部のブラウザーで Web ページを参照すると、Windows 向け Citrix Workspace アプリが応答しなくなることがあります。この問題は、wfica32 プロセスが大量のメモリを消費する場合に発生します。[CVADHELP-16172]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Windows 向け Citrix Workspace アプリをバージョン 1912 LTSR CU1 または CU2 にアップグレードした後、セッション画面の保持に失敗する可能性があります。この問題は、Enlightened Data Transport（EDT）プロトコルが有効になっていて、接続が Citrix Gateway を経由している場合に発生します。[CVADHELP-16694]
- エンドポイントで CGP ポート（2598）がブロックされている場合、Windows 向け Citrix Workspace アプリを介してセッションを起動しようとすると失敗する可能性があります。[CVADHELP-17632]

ユーザーエクスペリエンス

- この修正では、新しいグループポリシーオブジェクト設定（**Trusted Store Accounts List**）を利用して信頼アカウントのポップアップが表示されないようにします。[CVADHELP-16597]
- VDA で一部のサードパーティアプリケーションを使用すると、マウスの動きに遅延が発生する場合があります。[CVADHELP-16737]

ユーザーインターフェイス

- Windows 向け Citrix Workspace アプリ 1912 LTSR CU2 を使用している場合、［スタート］メニューのショートカットが自動的に更新されないことがあります。この問題は、新しいアプリケーションが追加されたとき、またはバックエンドで変更が加えられたときに発生します。[CVADHELP-17122]
- レジストリ HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle の **CurrentAccount** 値を **AllAccount** に設定すると、有効にならない場合があります。この問題は、1 つまたは複数のストアアカウントが存在する場合に発生します。[CVADHELP-17229]
- Windows 向け Citrix Workspace アプリを使用して Wyse シンクライアントデバイスにログオンしようとすると、認証プロンプトが **Desktop Lock** 画面の背後に表示される場合があります。その結果、認証プロンプトウィンドウを前面に表示するまでログオンできません。[CVADHELP-17880]

Windows 向け **Citrix Workspace** アプリ **1912 LTSR CU4**

Citrix Workspace アプリ 1912 LTSR CU3 との比較

クライアントデバイスの問題

- クライアント **COM** ポートリダイレクトポリシーを有効にすると、Bluetooth デバイスの COM ポートにアクセスできないことがあります。[CVADHELP-14939]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ログオン/認証

- ユーザー名にウムラウト記号が含まれている場合、Windows 向け Citrix Workspace アプリのバージョン 1912 LTSR CU3 にログオンしようとすると失敗することがあります。[CVADHELP-17267]

セキュリティの問題

- 制御フローガードのバイナリ保護が、バイナリから欠落している可能性があります。[CVADHELP-16531]

セッション/接続

- ピアツーピア通話中に Microsoft Teams の画面共有機能を使用すると、黒い画面が表示されることがあります。[CVADHELP-15605]
- **HDX** アダプティブトランスポートポリシーが優先に設定され、**EDT MTU** 検出が有効になっている場合、アプリケーションまたはデスクトップを起動しようとしたときに、警告メッセージとともに灰色または黒色の画面が表示されることがあります。[CVADHELP-15805]
- アプリケーションを無効にしたり、ショートカットのパスを変更したりした後も、そのアプリケーション用に作成したショートカットが削除されない場合があります。[[CVADHELP-16448]
- Citrix Gateway を経由して VPN 接続を接続または切断すると、Windows 向け Citrix Workspace アプリを使用してアプリケーションを起動できないことがあります。[CVADHELP-16714]
- ダブルホップシナリオでは、エンドポイントクライアント名が Delivery Controller または Director に渡されないことがあります。この問題は、VDA バージョン 2003 以降で発生します。[CVADHELP-16783]
- Windows 向け Citrix Workspace アプリをバージョン 1912 LTSR CU1 または CU2 にアップグレードした後、セッション画面の保持に失敗する可能性があります。この問題は、Enlightened Data Transport（EDT）プロトコルが有効になっていて、接続が Citrix Gateway を経由している場合に発生します。[CVADHELP-16694]

ユーザーエクスペリエンス

- Windows 向け Citrix Workspace アプリのバージョン 1912 LTSR CU2 を使用している場合、セッションで画面の内容を不鮮明にするグラフィックアーティファクトが表示されることがあります。[CVADHELP-16451]
- Citrix Receiver for Windows 4.9.6 を Citrix Workspace アプリのバージョン 1912 LTSR CU2 または CU3 にアップグレードした後、アプリケーションのショートカットを起動しようとすると、一部のデスクトップでショートカットアイコンが点滅することがあります。[CVADHELP-16967]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ユーザーインターフェイス

- セッションの実行中に ［ログアウト］を選択すると、操作が正しいかどうかを確認する ［サインアウト］プロンプトが表示されます。［キャンセル］をクリックするとエラーが発生します。[CVADHELP-15516]
- Citrix Receiver for Windows 4.9 LTSR CU7 を、Windows 向け Citrix Workspace アプリのバージョン CU2 または CU3 にアップグレードして、デフォルトのストアアカウントを設定しようとすると、整合性のない動作が発生することがあります。たとえば、デフォルトのストアアカウントは、常にデフォルトの「すべてのアカウント」になります。この変更により、Citrix Workspace アプリを終了して再起動した後でも、プライマリストアアカウントは別のストア名に設定されたままになります。[CVADHELP-16903]

Windows 向け Citrix Workspace アプリ 1912 LTSR CU3

Citrix Workspace アプリ 1912 LTSR CU2 以降の修正

インストール、アンインストール、アップグレード

- 手動で作成したショートカットを使用して Citrix Workspace アプリを更新しようとすると、ショートカットが削除されてから再作成される場合があります。[CVADHELP-15397]

キーボード

- 日本語キーボードを使用する場合、ローカルアプリアクセスを介して起動された Microsoft Excel では、全角入力モードが機能しないことがあります。この問題は、アプリ保護機能が有効になっている Windows 向け Citrix Workspace アプリで発生します。[CVADHELP-15410]

ログオン/認証

- ［サインインしたままにする］および ［今後 **60** 日間はこのメッセージを表示しない］ポリシーを有効にした場合でも、Microsoft Azure 多要素認証が認証を要求することがあります。

  > 注:
  >
  > ユーザーは、ストアからログオフするのではなく、ストアを終了することをお勧めします。ユーザーが Web ビュー認証を使用してストアからログオフすると、Internet Explorer の Cookie がクリアされるため、再度認証を求められる場合があります。デフォルトでは、修正が有効になっています（Cookie が保存されます）。［**Citrix** コンポーネント］**>** ［**Citrix Workspace**］**>** ［ユーザー認証］で ［永続的な **Cookie** が保存されないようにします］ GPO ポリシーを有効にすることで、この修正を無効にできます。修正を無効にすると、Cookie は保存されずログオフ中にクリアされます。修正を無効にすると、Cookie は保存されずログオフ中にクリアされます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

[CVADHELP-14814]

- Azure Active Directory（AD）に参加しているデバイスで、Citrix Workspace アプリがストアにアクセスしようとしてエンドポイントのログオン資格情報を渡すと、ユーザーにログオンが許可されない場合があります。また、別のユーザーアカウントでログオンするオプションはありません。[CVADHELP-14844]

印刷

- 生データ形式で印刷キューに送信すると、印刷されないことがあります。この問題は、XPS プリンタードライバーを使用すると発生します。[CVADHELP-14497]

セッション/接続

- 特定のシナリオでは、Citrix Studio に表示されるシトリックス製品のライセンスの使用状況が、Citrix License Manager に表示されるライセンス使用状況と一致しません。[CVADHELP-14950]
- **vPrefer** オプションを有効にすると、App-V アプリケーションがローカルサーバーではなくリモートサーバーで起動する場合があります。[CVADHELP-15356]
- ネイティブの Windows 向け Citrix Workspace アプリ経由で公開デスクトップを起動すると、ネイティブの Citrix Workspace アプリがデスクトップのフォアグラウンドで自動的に実行されます。この問題は、ローカルアプリアクセス機能が有効になっている場合に発生します。[CVADHELP-15654]
- Selfservice.exe プロセスが応答しなくなり、**.NET-BroadcastEventWindow.4.0.0.0.1** プロンプトが表示されることがあります。この問題は、Windows 10 バージョン 1909 を実行しているシステムからログオフしようとすると発生します。[CVADHELP-15700]
- セッションの確立時にすべてのストアアカウントに接続するように Windows 向け Citrix Workspace アプリを構成します。Citrix Workspace アプリからログオフして再度ログオンすると、ストアアカウント設定が、デフォルトですべてのアカウントに設定されず、1 つのストアアカウントに変更されます。[CVADHELP-15728]
- 双方向コンテンツリダイレクトポリシーを有効にすると、URL をクライアントから VDA にリダイレクトしようとして失敗する場合があります。[CVADHELP-15739]
- プロキシサーバーがポート 8080 を使用しないシナリオでは、Citrix Workspace アプリが公開アプリケーションおよびデスクトップに接続できないことがあります。この問題は、Windows 向け Citrix Workspace アプリがプロキシポートの使用に失敗し、代わりにデフォルトポートの 8080 を使用する可能性があるために発生します。[CVADHELP-15977]
- Windows 向け Citrix Workspace アプリは、プロキシの種類の設定を無視することがあります。この問題は、英語版以外の Microsoft Windows オペレーティングシステムで発生します。[CVADHELP-16017]
- **EnableFactoryReset** レジストリ設定が **False** に設定されている場合、Citrix Workspace アプリをアンインストールしようとすると、次のエラーメッセージが表示されて失敗することがあります:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

この機能は無効になりました。

[CVADHELP-16114]

- Microsoft Teams が最適化モードになっている場合に電話会議に参加すると、音声が乱れる可能性があります。[CVADHELP-16232]

システムの例外

- **EchoCancellation** ポリシーを有効にして音質を中に設定すると、wfica32.exe プロセスが断続的に終了し、セッションが最終的に切断される場合があります。[CVADHELP-14568]
- Receiver.exe プロセスが、予期せずに終了する場合があります。[CVADHELP-15669]

Windows 向け Citrix Workspace アプリ 1912 LTSR CU2

Citrix Workspace アプリ 1912 LTSR CU1 以降の修正

インストール、アンインストール、アップグレード

- Windows 向け Citrix Workspace アプリをバージョン 190*x* からバージョン 1912 にアップグレードしようとして、失敗することがあります。この問題は、問題のあるファイルが実行可能フォルダーのパスのいずれかに存在する場合に発生します。[CVADHELP-15277]
- Citrix Workspace アプリをバージョン 1912 からバージョン 1912 CU1 または 2006 に更新しようとすると、Citrix Workspace アプリの更新機能が英語以外の言語のオペレーティングシステムで機能しない場合があります。[CVADHELP-15357]

キーボード

- 中国語の入力システム（IME）Wuxiami を使用すると、Shift キーが押されたままになる場合があります。この問題は、一般的なローカル時間が **ON** に設定されている場合に発生します。[CVADHELP-15243]

セキュリティの問題

- この修正により、セキュリティ上の問題が 1 件解決されます。詳しくは、Knowledge Center のCTX277662を参照してください。[CVADHELP-15613]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

セッション/接続

- レジストリ編集ツールを無効にすると、アップグレードを実行した後、以前インストールされたレジストリキーが保持されない場合があります。その結果、デスクトップを起動しようとすると失敗します。[CVADHELP-15104]
- Citrix Workspace アプリでは、1911 より前のバージョンでスクリプトエラーが表示され、バージョン 1911 以降で空白のページが表示される場合があります。この問題は、Microsoft セキュリティベースライン GPO ポリシーが適用されている場合に、Internet Explorer WebBrowser コントロールを使用してログインページを表示するストアで発生します。[CVADHELP-15475]
- ダブルホップシナリオでは、［スタート］メニューのショートカットを使用してアプリケーションを起動しようとすると、失敗する場合があります。この問題は、1 ユーザーにつき 1 つのインスタンスのアプリケーション制限を有効にした場合に発生します。[CVADHELP-15576]
- Citrix Workspace アプリバージョン 1912 以降でストアにログオンすると、アプリケーションの列挙に失敗する場合があります。[CVADHELP-15597]

ユーザーエクスペリエンス

- VPN 経由で Self-service Plug-in（SSP）に接続する場合、SSP の更新に失敗する可能性があります。[CVADHELP-14418]
- **SelfService.exe -init -ipoll-exit** コマンドを使用して SelfService.exe プロセスを閉じようとすると失敗する場合があります。[CVADHELP-15126]
- HP Active Stylus ペンを使用して公開アプリケーションに書き込む場合、書き込み機能に 3〜4 秒の遅延が発生する場合があります。[CVADHELP-15203]
- Windows 向け Citrix Workspace アプリを新規インストールした後、または既存のインストールを最新のものにアップグレードした後、セッションを起動しようとすると失敗する場合があります。セッションの起動がデスクトップの準備画面でスタックします。この問題は、Citrix Gateway URL を使用して Desktop Lock を構成するときに発生します。

  > 注:
  >
  > Citrix Gateway URL と Desktop Lock を使用して Windows 向け Citrix Workspace アプリを初めて構成するときに、Desktop Lock が表示されるまでしばらくの間黒い画面が表示されます。黒い画面が長時間続く場合、物理マシンの場合は **Ctrl+Alt+Delete** キーを使用して、仮想マシンの場合は **Ctrl+Alt+End** キーを使用してサインアウトします。

  [CVADHELP-15334]
- Citrix Workspace アプリをバージョン 1912 からバージョン 1912 CU1 にアップグレードした後、アプリケーションの列挙が遅くなり、完了までに約 10 分かかる場合があります。[CVADHELP-15766]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Workspace アプリ 1912 LTSR CU1 Hotfix 1 for Windows（19.12.1001）

Windows 向け Citrix Workspace アプリ 1912 LTSR CU1 との比較

セキュリティの問題

- この修正により、セキュリティ上の問題が 1 件解決されます。詳しくは、Knowledge Center のCTX277662を参照してください。[CVADHELP-15613]

Windows 向け Citrix Workspace アプリ 1912 LTSR CU1

Citrix Workspace アプリ 1912 LTSR 以降の修正

コンテンツリダイレクト

- 長い URL をリダイレクトしようとすると、URL が VDA にリダイレクトされず、Redirector.exe プロセスが次の例外で予期せず終了することがあります。

  INVALID_CRUNTIME_PARAMETER

  [CVADHELP-13197]

インストール、アンインストール、アップグレード

- Windows 10 を実行している VDA に対して Citrix Workspace アプリをインストールまたはアップグレードしようとすると失敗することがあります。この問題は、次の手順の実行時に発生します:

  1. Citrix Workspace アプリをインストールします。
  2. VDA をインストールします。
  3. Citrix Workspace アプリを新しいバージョンにアップグレードします。

  この問題は、アップグレードまたはインストールによって Citrix ディスプレイアダプターが削除されるために発生します。[CVADHELP-13764]

- 自動更新機能を使用して、HDX RealTime Media Engine（RTME）と Citrix Workspace アプリを自動的に更新しようとすると失敗する場合があります。RTME を最新バージョンにアップグレードできません。[CVADHELP-15047]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ログオン/認証

- 2 つの異なるアカウントを使用して Windows 向け Citrix Workspace アプリに 2 つのストアを追加すると、プライマリストアを削除した後、セカンダリストアでサインインボタンが機能しないことがあります。[CVADHELP-13805]
- 多要素認証が有効で、Windows セキュリティダイアログを使用してログインする場合、ストアへの認証時に Active Directory フェデレーションサービス（ADFS）ダイアログは表示されません。[CVADHELP-14316]
- Citrix Workspace アプリを介してシングルサインオン（SSO）をサポートするように Citrix Gateway を構成すると、SSO が失敗する場合があります。この問題は、ユーザー名またはパスワードに**%**、**=**、**&** などの特殊文字が含まれている場合に発生します。[CVADHELP-14564]

SDK

- この修正により、従来の秘密キーハンドルのサポートが強化されます。[CVADHELP-14530]

セッション/接続

- ローカルアプリアクセスと Desktop Lock を有効にした場合、Ctrl+Alt+Del キーを押した後にユーザーの切り替え機能を実行すると、ローカルユーザーセッションが再接続されることがあります。ただし、サーバーセッションが再接続しようとすると、VDA が白い画面で表示され、デスクトップに接続されたことを示すメッセージが表示されます。デスクトップは表示されません。[CVADHELP-13046]
- マルチモニター環境では、ユーザーセッションを最大化しようとすると失敗する場合があります。この問題は、ノートブックを再接続すると発生します。[CVADHELP-13614]
- ダブルホップシナリオでは、セッションを起動しようとすると、Citrix HDX Engine が予期せず終了することがあります。[CVADHELP-13915]
- Citrix Workspace アプリで **vPrefer** オプションを有効にすると、App-V アプリケーションの起動に失敗して、次のエラーメッセージが表示されることがあります:

  起動できません

  [CVADHELP-14039]
- 公開アプリケーションを ［お気に入り］に追加すると、開くことができるアプリケーションが 1 つだけになります。この問題は、公開アプリケーションが **KEYWORDS:prefer=”** **<application_name>** と同じ実行可能ファイルの名前を使用すると発生します。[CVADHELP-14098]
- Citrix Workspace アプリのアップグレード後、廃止される機能である **HDX MediaStream for Flash** に関連したレジストリ値(Flash および Flash2 など)が､レジストリ設定(HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432No Client\Engine\Configuration\Advanced\Modules\ICA 3.0\VirtualDriver）から削除されない場合があります。この問題は、接続エラーを引き起こす可能性があります。[CVADHELP-14850]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

システムの例外

- セッションへ接続しようとすると、wfica32.exe プロセスが予期せずに終了する場合があります。この問題は、Windows 向け Citrix Workspace アプリのバージョン 1904.1 で発生します。[CVADHELP-12807]
- ローカルアプリアクセスを有効にすると、セッションが応答しなくなり、次のエラーメッセージが表示される場合があります:

  Citrix HDX Engine is not responding

  [CVADHELP-14058]
- セルフサービスモードを構成せずに Citrix Workspace アプリをインストールしようとすると、例外が発生する場合があります。この問題は、［高度な設定］シートから ［ショートカットと再接続］メニューを開いたときに発生します。この問題は、Citrix Workspace アプリのバージョン 1907～2002 で発生します。[CVADHELP-14940]

TWAIN

- TWAIN デバイスを使用してスキャンを実行しようとすると失敗する場合があります。Windows タスクマネージャーの ［アプリケーション］タブの ［状態］列に、Citrix HDX Engine が「応答なし」と表示されます。[CVADHELP-14782]

ユーザーエクスペリエンス

- マルチセッション OS 対応 VDA が最初のホップで実行され、公開アプリケーションが 2 番目のホップで実行されるダブルホップシナリオでは、Citrix Workspace アプリのアカウントメニューの［アプリ一覧の更新］オプションが機能しない場合があります。[CVADHELP-13230]
- Windows 向け Citrix Workspace アプリでストア URL を使用してアカウントを追加すると、完了までに時間がかかる場合があります。この問題は、URL にポート番号が含まれている場合に発生します。[CVADHELP-14051]
- システムトレイに 2 つの Citrix Workspace アプリアイコンが表示されます。この問題は、Citrix Workspace アプリバージョン 1912 で発生します。[CVADHELP-14577]
- VDA 環境でシングルサインオンを使用すると、スプラッシュスクリーンが表示される場合があります。この問題は、Windows 向け Citrix Workspace アプリをバージョン 1911 以降にアップグレードすると発生します。[CVADHELP-14590]

ユーザーインターフェイス

- アプリケーションが、現在のアプリケーションに代わって前面に移動しようと断続的に試みることがあります。タスクバーのアイコンが点滅し、アプリケーションが前面への移動を試みていることをユーザーに通知する場

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

合があります。[CVADHELP-13071]

Windows 向け Citrix Workspace アプリ 1912 LTSR

> 注:
>
> 現在、Citrix Workspace アプリ 1911 の最新リリースを使用していて、LTSR トラックに移行しようとしている場合:
>
> このリリースには、Citrix Workspace アプリ 1911 と比較して、以下の修正が含まれています。
>
> 現在、Citrix Receiver for Windows 4.9 を使用していて、LTSR トラックのまま使用する場合:
>
> このリリースでは、Citrix Receiver for Windows 4.9（CU を含む）から 4.12 までに含まれるすべての修正と、Citrix Workspace アプリ 1808 から 1911 までに含まれるすべての修正に加えて、Citrix Workspace アプリ 2002 に含まれる、次の一覧に示す修正（Citrix Workspace アプリ 1911 と比較した）が含まれています: バージョン 1912 には、Citrix Receiver for Windows 4.9 LTSR CU9と Citrix Workspace アプリバージョン 1911 の間のすべての修正に加えて、次の修正が含まれています:

HDX MediaStream Windows Media リダイレクト

- マルチモニター環境では、ユーザーセッションで Windows Media Player を使用して MP4 ビデオを再生すると、ビデオがプライマリモニターで正しく再生されます。ただし、プレーヤーを別の画面に移動すると、ドッキングステーションを使用して DisplayLink 経由で接続されたセカンダリモニターまたは拡張モニターに黒い画面が表示される場合があります。[CVADHELP-11848]

セッション/接続

- 高速スマートカードを使用して HDX RealTime Media Engine からセッションに再接続しようとすると、HDX RealTime Media Engine が予期せず終了する場合があります。[CVADHELP-12605]
- 公開アプリケーションが短時間に短い音を再生するための要求を多数受信すると、wfica32.exe プロセスが予期せず終了する場合があります。[CVADHELP-12855]
- セッションがタイムアウトになると、自動的にログオフする場合があります。セッションを再度起動しようとすると、セッションの起動に通常より時間がかかります。この問題は、ネットワークが中断したときに発生します。[CVADHELP-13017]
- シームレスアプリケーションウィンドウは、部分的に欠けた状態になり、手動でウィンドウのサイズを変更するまで欠けたままになることがあります。[CVADHELP-13108]
- Citrix Workspace アプリが、更新または起動するたびに、ショートカットアイコンの有無をチェックするようになりました。アイコンがない場合、Citrix Workspace アプリは再びアイコンを取得します。これにより、ショートカットが適切に表示されます。[RFWIN-15501]
- コンテンツの双方向リダイレクトポリシー（[コンピューターの構成] > [管理用テンプレート] > [従来の管理用テンプレート（**ADM**）] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [ユーザーエクスペリエン

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ス]）を有効にしようとすると、URL 固有のアプリケーションまたはデスクトップの上書きを有効にしていなくても、URL 固有のエントリの入力を求められます。[RFWIN-15867]

システムの例外

- CDF トレースのキャプチャ中に、Receiver.exe プロセスが予期せず終了することがあります。[CVADHELP-13077]

既知の問題

June 16, 2023

Windows 向け **Citrix Workspace** アプリ **1912 LTSR CU7** 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。

Windows 向け **Citrix Workspace** アプリ **1912 LTSR CU6** の既知の問題

- Microsoft Teams で公開アプリケーションとして画面を共有すると、共有画面の下部にある赤い境界線が表示されません。[LCMRFWIN-4194]

Windows 向け **Citrix Workspace** アプリ **1912 LTSR CU5** の既知の問題

- mRemoteNG などの特定のサードパーティのリモートアプリケーションをエンドポイントに接続し、公開アプリケーションのアプリケーションツールバーを側面にドッキングすると、システムの CPU 使用率が 100% になり応答しなくなる場合があります。[LCMRFWIN-4164]
- Microsoft Teams の最適化された通話中に画面共有を停止しようとすると、セッションが断続的に応答しなくなる場合があります。[LCMRFWIN-4184]

Windows 向け **Citrix Workspace** アプリ **1912 LTSR CU4** の既知の問題

- セッション中に ［更新をチェック］をクリックすると、更新が正常にダウンロードされ、現在のセッションが［ダウンロードが完了しました］ダイアログボックスの一覧に表示されません。[RFWIN-23152]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Windows 向け Citrix Workspace アプリ 1912 LTSR CU3 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。

Windows 向け Citrix Workspace アプリ 1912 LTSR CU2 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。

Windows 向け Citrix Workspace アプリ 1912 LTSR CU1 の既知の問題

- WebEx 会議で Web カメラを使用しようとすると、Citrix Workspace アプリが応答しなくなることがあります。この問題は、UDP オーディオを ［中］に設定すると発生します。

  この問題を回避するには、レジストリエディターで次のパスに移動し、次の設定を行います:

  パス:HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced

  値の名前：EchoCancellation

  種類：REG_SZ

  値：FALSE

  [DOCFB-3805]

Windows 向け Citrix Workspace アプリ 1912 LTSR の既知の問題

- **Print Screen** キーを使用して画面をキャプチャしようとすると、失敗することがあります。この問題は、保護された Citrix Workspace アプリのセッションを最小化すると発生します。[RFWIN-15155]
- 公開セッションとローカルデバイスの両方で Microsoft Word を起動し、アカウントからストアを削除すると、ローカルデバイスでアプリを起動したときに次のエラーメッセージが表示されます:

  このファイルを開くためのアプリケーションを **Citrix Workspace** で選択しますか**?**

  [RFWIN-15884]
- SSL が有効な VDA でセッションを起動しようとすると、失敗することがあります。[RFWIN-16129]
- 保護されたデスクトップセッションで、保護されていないセッションのスクリーンショットを撮ろうとすると失敗することがあります。[RFWIN-16704]
- グループポリシーオブジェクト（GPO）管理用テンプレートを使用して追加されたストアの詳細を、グラフィカルユーザーインターフェイスを使用して削除できない場合があります。[RFWIN-16754]
- 保護されたセッションで表示を変更しようとすると、セッションが終了します。[RFWIN-16784]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

サードパーティ製品についての通知

June 16, 2023

Windows 向け Citrix Workspace アプリ 1912 LTSR 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:

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

システム要件と互換性

April 22, 2024

要件

- 1GB の RAM。
- .NET Framework の要件
  - Self-Service plug-in には、NET 4.6.2 が必要です。これにより、Windows 向け Citrix Workspace アプリのユーザーインターフェイスまたはコマンドラインからアプリとデスクトップにサブスクライブして起動することができます。詳しくは、「コマンドラインパラメーターの使用」を参照してください。
- Microsoft Visual C++ 再頒布可能パッケージの最新バージョン。

  > 注:
  >
  > Citrix では Microsoft Visual C ++ 再頒布可能パッケージの最新バージョンを使用することをお勧めします。そうしないと、アップグレード中に再起動のプロンプトが表示されることがあります。

  バージョン 1904 以降、Citrix Workspace アプリのインストーラーには、Microsoft Visual C++ 再頒布可能パッケージのバイナリが個別に含まれるのではなく、Microsoft Visual C++ 再頒布可能パッケージのインストーラーが含まれています。Citrix Workspace アプリのインストーラーが Microsoft Visual C++ 再頒布可能パッケージがシステム上に存在するかどうかをインストール時に確認し、必要に応じてインストールします。Citrix Workspace アプリのバージョン 1912 以降では、Microsoft Visual C++ 再頒布可能パッケージバージョン 14.24.28127.4 以降が必要です。

  > 注:
  >
  > Microsoft Visual C++ 再頒布可能パッケージがインストールされていないシステムに管理者以外の権限で Citrix Workspace アプリをインストールしようとすると、失敗することがあります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Microsoft Visual C++ 再頒布可能パッケージをインストールできるのは、管理者のみです。

.NET Framework または Microsoft Visual C++ 再頒布可能パッケージのインストールに関する問題のトラブルシューティングについては、Knowledge Center の記事CTX250044を参照してください。

互換性マトリックス

Citrix Workspace アプリは、現在サポートされているすべてのバージョンの Citrix Virtual Apps and Desktops と Citrix DaaS（Citrix Virtual Apps and Desktops サービスの新名称）およびシトリックス製品マトリックスの一覧にある Citrix Gateway のバージョンと互換性があります。

Citrix Workspace アプリは、以下の Windows オペレーティングシステムと互換性があります。

> 注:
>
> Citrix Gateway End-Point Analysis Plugin（EPA）は Citrix Workspace でサポートされています。ネイティブの Citrix Workspace アプリでは、nFactor 認証を使用する場合にのみサポートされます。詳しくは、Citrix ADC ドキュメントの「nFactor 認証の要素として認証前および認証後の EPA スキャンを構成」を参照してください。

オペレーティングシステム
Windows 10 32 ビット版および 64 ビット版の Enterprise Edition。互換性のある Windows 10 オペレーティングシステムについて詳しくは、「Windows 10 と Windows 向け Citrix Workspace アプリとの互換性」を参照してください。
Windows 10 32 ビット版および 64 ビット版の Pro エディション（Windows 向け Citrix Workspace アプリ 1912 LTSR CU5 以降でサポート）
Windows 8.1 32 ビット版および 64 ビット版（Embedded エディションを含む）
Windows 7 の 32 ビットエディションと 64 ビットエディション（拡張セキュリティ更新プログラム - ESU）
Windows 7 Embedded Standard（拡張セキュリティ更新プログラム - ESU）
Windows Thin PC
Windows Server 2016
Windows Server 2012 R2、Standard および Datacenter エディション
Windows Server 2019
Windows Server 2008 R2
Windows 10 Enterprise LTSC 2019
Windows 10 Enterprise 2016 LTSB 1607

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Windows 10 と Windows 向け Citrix Workspace アプリとの互換性

> 注:
>
> - 半期チャネルバージョンより前にリリースされた Citrix ソフトウェアバージョンのインストールは推奨されません。これを実行するお客様は、Citrix ソフトウェアの新しいバージョンで、サポートコールを生成する問題がまだ対応されていないことを検証する必要があります（ある場合）。また、Citrix ソフトウェアの新しいバージョンへのアップグレードが必要な場合もあります。
> - Windows 10 バージョンがサービス終了になると、Microsoft からバージョンのサービスやサポートが提供されなくなります。シトリックスでは、製造元がサポートするオペレーティングシステムで実行する場合のみ Citrix ソフトウェアをサポートします。Windows 10 のサービス終了について詳しくは、Microsoft の Windows ライフサイクルファクトシートを参照してください。

Citrix Workspace アプリのバージョン	Windows 10 Enterprise エディションのバージョン番号	ビルド番号
1912 CU7 以降	LTSC 2021	19044
1912 CU6 以降	21H2	19044
1912 CU6 以降	21H2	19044
1912 CU5 以降	21H1	19043.1165
1912 CU2 以降	20H2	19042.685
1912 CU1 以降	2004	19041.329
1911 以降	1909	18363.418
1909 以降	1903	18362.116
1812 以降	1809	17763.107
1808 以降	10 1803	17134.376

サポートされているブラウザー

サポートされているブラウザーの一覧は、「Citrix Receiver for Web サイト経由でストアにアクセスする」を参照してください。

オペレーティングシステムマトリックス

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

タッチデバイスでサポートされるオペレーティングシステム
Windows 10
Windows 8
Windows 7

VDA でサポートされるオペレーティングシステム
Windows 10
Windows 8
Windows 7
Windows 2012 R2
Windows Server 2016
Windows 2008 R2

空きディスクスペースの検証

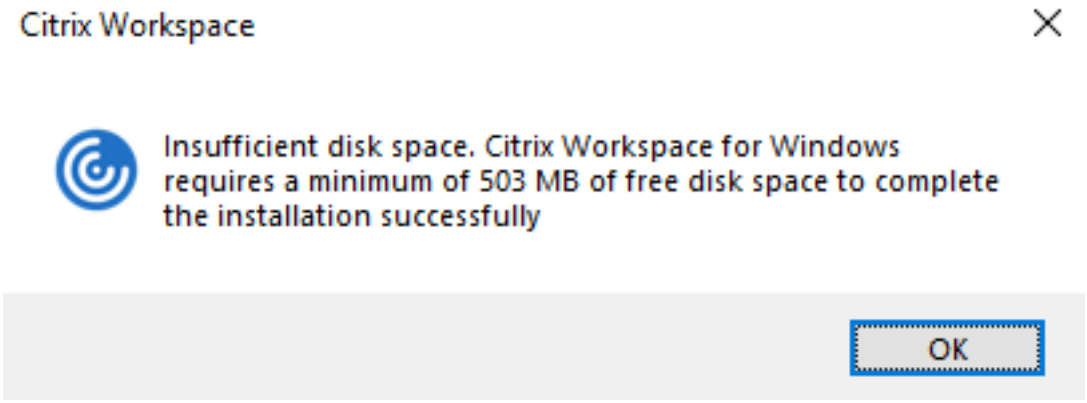
次の表に、Windows 向け Citrix Workspace アプリをインストールする場合の必要ディスクスペースの詳細を示します:

インストールの種類	必須ディスクスペース
新規インストール	572MB
アップグレード	350MB

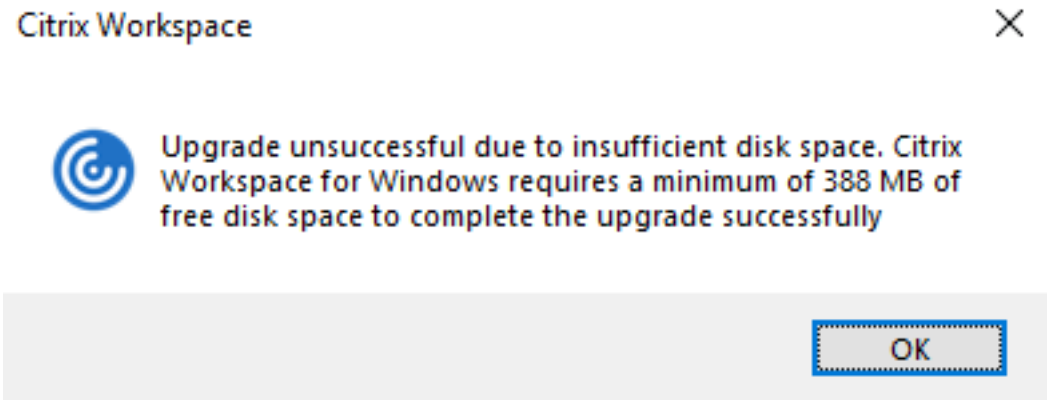
Citrix Workspace アプリは、インストールを完了するために必要なディスクスペースがあるかどうかのチェックを実行します。この検証は、新規インストールとアップグレードのどちらの場合にも実行されます。

新規インストール時にディスクスペースが不十分な場合は、インストールが停止し、次のダイアログが表示されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



アップグレード時にディスクスペースが不十分な場合は、インストールが終了し、次のダイアログが表示されます。



> 注:
>
> - インストーラーがディスクスペースのチェックを実行するのは、インストールパッケージの抽出後のみです。
> - サイレントインストール時にシステムのディスクスペースが少ない場合、ダイアログは表示されませんが、エラーメッセージが`CTXInstall\\_TrolleyExpress-\*.log`に記録されます。

接続、証明書、認証

接続

- HTTP ストア
- HTTPS ストア
- Citrix Gateway 10.5 以降
- Web Interface 5.4

証明書

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> Windows 向け Citrix Workspace アプリはデジタル署名されています。デジタル署名にはタイムスタンプが付けられています。したがって、証明書は有効期限が切れても有効です。

- プライベート（自己署名）証明書
- ルート証明書
- ワイルドカード証明書
- 中間証明書

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、Citrix リソースにアクセスする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。

> 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、アプリの一覧が表示されますが、アプリの起動に失敗することがあります。

ルート証明書

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

ドメイン非参加コンピューターでは、カスタムインストールパッケージを作成して、CA 証明書を配布およびインストールできます。詳しくは、システム管理者に問い合わせてください。

ワイルドカード証明書

ワイルドカード証明書は、同一ドメイン内のサーバーで使用されます。

Citrix Workspace アプリはワイルドカード証明書をサポートしますが、組織のセキュリティポリシーに従って使用する必要があります。実際には、サブジェクトの別名（SAN）拡張領域内のサーバー名一覧に含まれている証明書など、ワイルドカード証明書に代わるものです。このような証明書は、私的証明機関および公的証明機関が発行します。

中間証明書

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

認証

StoreFront への認証

	Web 向け **Workspace**（ブラウザー）	**StoreFront** サービスサイト（ネイティブ）	**StoreFront**、**Citrix Virtual Apps and Desktops**（ネイティブ）、**Citrix DaaS**	**Citrix Gateway** から **Web** 向け **Workspace**（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 *	はい *
ドメインパススルー	はい	はい	はい		
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（Citrix Gateway Plug-in）	はい（Citrix Gateway Plug-in）

* デバイスに Citrix Gateway Plug-in をインストールしている場合としない場合。

> 注:
>
> Citrix Workspace アプリは、Citrix Gateway から StoreFront ネイティブサービスを通じて 2 要素認証（ドメイン + セキュリティトークン）をサポートします。

Web Interface での認証　Citrix Workspace アプリは次の認証方法をサポートします（Web Interface ではドメインおよびセキュリティトークン認証に明示的という用語を使用します）:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

	Web Interface（ブラウザー）	**Web Interface Citrix Gateway** サイト	**Citrix Gateway** から **Web Interface**（ブラウザー）	**Citrix Gateway** から **Web Interface Citrix Gateway** サイト
匿名	はい			
ドメイン	はい	はい	はい *	
ドメインパススルー	はい	はい		
セキュリティトークン			はい *	
2 要素認証（ドメイン + セキュリティトークン）			はい *	
SMS			はい *	
スマートカード	はい	はい		
ユーザー証明書			はい（Citrix Gateway Plug-in）	

* Citrix Gateway が動作する環境でのみ使用できます（デバイスへのゲートウェイプラグインソフトウェアのインストールは不要）。

認証について詳しくは、次を参照してください:

- Citrix Gateway ドキュメントの「認証と承認」
- StoreFront ドキュメントの「認証と委任の構成」

証明書失効一覧

証明書失効一覧（CRL）のチェック機能を有効にすると、サーバー証明書が失効していないかどうかが Citrix Workspace アプリによってチェックされます。このチェックを行うことにより、TLS サーバーの暗号化認証機能が強化され、ユーザーデバイスとサーバー間の TLS 接続のセキュリティが向上します。

証明書失効一覧のチェック機能はさまざまな設定レベルで有効にできます。たとえば、ローカルの証明書失効一覧だけがチェックされるように Citrix Workspace アプリを構成したり、ローカルとネットワーク上の両方の証明書失効一覧がチェックされるように構成したりできます。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ときのみログオンするように構成できます。

Citrix Workspace アプリを終了し、コネクションセンターなどの Citrix Workspace コンポーネントをすべて終了します。

詳しくは、「TLS」セクションを参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

インストールとアンインストール

May 23, 2024

Windows 向け Citrix Workspace アプリ 1912 LTSR をインストールする前の管理者への注意事項

- Windows 向け Citrix Workspace アプリ 1912 LTSR には、.NET フレームワークバージョン 4.6.2 以降が必要です。システムに.NET Framework が導入されていない場合は、Citrix Workspace アプリインストーラーがダウンロードしてインストールします。ただし、Citrix Workspace アプリをインストールまたは更新する前に、必要な.NET Framework を手動でインストールすることをお勧めします。
- 無人インストールを行う場合は、Knowledge Center のCTX257546を参照してください。
- サポートされている暗号とサポートされていない暗号に関する最新情報については、Knowledge Center のCTX250104を参照してください。

所属する組織のダウンロードページまたは所属する組織のダウンロードページ（存在する場合）からCitrixWorkspaceApp.exeインストールパッケージをダウンロードして、Citrix Workspace アプリをインストールできます。パッケージは次の方法でインストールできます:

- Windows ベースのインタラクティブなインストールウィザードを実行する。
- コマンドラインインターフェイスを使用して、インストーラーのファイル名、インストールコマンド、インストールプロパティを入力する。コマンドラインインターフェイスを使用した Citrix Workspace アプリのインストールについて詳しくは、「コマンドラインパラメーターの使用」を参照してください。

管理者権限と非管理者権限によるインストール:

ユーザーと管理者の両方が Citrix Workspace アプリをインストールできます。Windows 向け Citrix Workspace アプリで パススルー認証およびCitrix Ready ワークスペースハブを使用する場合にのみ、管理者権限が必要です。

次の表では、Citrix Workspace アプリを管理者またはユーザーとしてインストールした場合の違いについて説明します:

	インストールフォルダー	インストールの種類
管理者	C:\Program Files (x86)\Citrix\ICA Client	システムごとのインストール
ユーザー	%USERPROFILE%\AppData\Local\Citrix\ICA Client	ユーザーごとのインストール

> 注:
>
> ユーザーがインストールした Windows 向け Citrix Workspace アプリインスタンスがシステム上に存在し、管理者が Windows 向け Citrix Workspace アプリを同じシステムにインストールすると、競合が発生します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Windows 向け Citrix Workspace アプリを管理者としてインストールする前に、ユーザーがインストールしたすべての Windows 向け Citrix Workspace アプリインスタンスをアンインストールすることをお勧めします。

Windows 向けインストーラーの使用

インストールメディア、ネットワーク共有、Windows エクスプローラー、またはコマンドラインで`CitrixWorkspaceApp.exe`インストーラーパッケージを手動で実行して Windows 向け Citrix Workspace アプリをインストールできます。

デフォルトでは、インストーラーのログは`%temp%\CTXReceiverInstallLogs*.logs`にあります。

1. `CitrixWorkspaceApp.exe`ファイルを起動して ［開始］をクリックします。
2. ライセンス契約書を読んで同意してから、インストールを続行します。
3. 管理者権限でドメイン参加のマシンにインストールしようとすると、シングルサインオンを有効または無効にするダイアログボックスが開きます。詳しくは、「[ドメインパススルー認証]」(/en-us/citrix-workspace-app-for-windows/authentication.html#domain-pass-through-authentication) を参照してください。
4. Windows 向けインストーラーの手順に従ってインストールを完了します。

コマンドラインパラメーターの使用

コマンドラインインターフェイスでインストーラーのファイル名、インストールコマンド、インストールプロパティを入力して、Citrix Workspace アプリをインストールできます。コマンドラインオプションを指定して、Citrix Workspace アプリのインストーラーをカスタマイズできます。インストーラーパッケージは自己展開型であり、セットアップが起動する前にシステムの一時フォルダーに展開されます。領域要件には、プログラムファイル、ユーザーデータ、およびいくつかのアプリケーションを起動した後の一時フォルダーが含まれます。

Windows コマンドラインを使用して Citrix Workspace アプリをインストールするには、コマンドプロンプトを起動してインストーラーのファイル名、インストールコマンド、インストールプロパティを 1 行に入力します。以下は、使用可能なインストールコマンドとプロパティです:

```
CitrixWorkspaceApp.exe [commands] [properties]
```

コマンドラインパラメーター一覧

パラメーターは大まかに次のように分類されます:

- 一般的なパラメーター
- インストールパラメーター
- HDX 機能のパラメーター
- 基本設定とユーザーインターフェイスのパラメーター

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 認証パラメーター

一般的なパラメーター

- /?または/help - すべてのインストールコマンドとプロパティを一覧表示します。
- /silent - インストール中のインストールダイアログとプロンプトを無効にします。
- /noreboot - インストール中に再起動ダイアログのプロンプトを表示しません。再起動プロンプトを表示しない場合、一時停止状態だった USB デバイスは、ユーザーデバイスを再起動するまで Citrix Workspace アプリで認識できません。
- /includeSSON - 管理者としてインストールする必要があります。Citrix Workspace アプリはシングルサインオンコンポーネントとともにインストールされます。詳しくは、「[ドメインパススルー認証]」(/en-us/citrix-workspace-app-for-windows/authentication.html#domain-pass-through-authentication) を参照してください。
- /rcu - このスイッチは、サポートされていないバージョンのソフトウェアからアップグレードする場合のみ有効です。既存のバージョンをアンインストールして、Citrix Workspace アプリをインストールまたはアップグレードします。これにより、既存の設定も消去されます。

  > 注:
  >
  > /rcuスイッチは、バージョン 1909 で廃止されます。詳しくは、「廃止」を参照してください。

- /forceinstall - このスイッチは、以下のシナリオで Citrix Workspace アプリの既存の構成またはエントリをシステム上でクリーンアップするときに役立ちます:
  - Citrix Workspace アプリのサポートされていないバージョンからアップグレードする。
  - インストールまたはアップグレードに失敗した。

インストールパラメーター

/AutoUpdateCheck

Citrix Workspace アプリが、利用可能な更新を検出することを示します。

- Auto（デフォルト）- 更新が利用可能になると通知します。例: CitrixWorkspaceApp.exe /AutoUpdateCheck=auto。
- Manual - 更新が利用可能になっても通知されません。手動で更新をチェックします。例: CitrixWorkspaceApp.exe /AutoUpdateCheck=manual。
- Disabled - 自動更新を無効にします。例: CitrixWorkspaceApp.exe /AutoUpdateCheck=disabled。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

/AutoUpdateStream

自動更新を有効にすると、更新先のリリーストラックを選択できます。詳しくは、「ライフサイクルマイルストーン」を参照してください。

- LTSR - 長期サービスリリース（LTSR）累積更新プログラム（CU）にのみ自動更新します。例: `CitrixWorkspaceApp.exe /AutoUpdateStream=LTSR`。
- Current - Citrix Workspace アプリの最新バージョンにのみ自動更新します。例: `CitrixWorkspaceApp.exe /AutoUpdateStream=Current`。

/DeferUpdateCount

更新が利用可能な場合に更新通知を延期できる回数を示します。詳しくは、「[Citrix Workspace 更新プログラム]」(/en-us/citrix-workspace-app-for-windows/update.html#advanced-configuration-for-automatic-updates-citrix-workspace-updates) を参照してください。

- -1（デフォルト）- 通知を何度でも延期できます。例: `CitrixWorkspaceApp.exe /DeferUpdateCount=-1`。
- 0 - 利用可能な更新ごとに 1 回（のみ）通知を受信します。更新について再度通知されることはありません。例: `CitrixWorkspaceApp.exe /DeferUpdateCount=0`。
- 任意の数の「n」- 更新通知を「n」回延期できます。[後で通知する] オプションは、「n」回表示されます。例: `CitrixWorkspaceApp.exe /DeferUpdateCount=<n>`。

/AURolloutPriority

新しいバージョンのアプリがリリースされると、特定の配信期間に更新プログラムが Citrix からロールアウトされます。このパラメーターを使用すると、配信期間中に更新プログラムを受信するタイミングを制御できます。

- Auto(デフォルト)—配信期間中に Citrix での構成に従って更新を受信します。例: `CitrixWorkspaceApp.exe /AURolloutPriority=Auto`。
- Fast — 配信期間の開始時に更新を受信します。例: `CitrixWorkspaceApp.exe /AURolloutPriority=Fast`。
- Medium — 配信期間の中頃に更新を受信します。例: `CitrixWorkspaceApp.exe /AURolloutPriority=Medium`。
- Slow - 配信期間の最後に更新を受信します。例: `CitrixWorkspaceApp.exe /AURolloutPriority=Slow`。

/includeappprotection

Citrix Virtual Apps and Desktops および Citrix DaaS（Citrix Virtual Apps and Desktops サービスの新名称）を使用する場合のセキュリティを強化し、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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

可能性を抑制します。

- `CitrixWorkspaceApp.exe /includeappprotection`

詳しくは、「App Protection」を参照してください。

INSTALLDIR

Citrix Workspace アプリをインストールするためのカスタムインストールディレクトリを指定します。デフォルトのパスは`C:\Program Files\Citrix`です。例: `CitrixWorkspaceApp.exe INSTALLDIR =C:\Program Files\Citrix`。

ADDLOCAL

1 つまたは複数の指定したコンポーネントをインストールします。例: `CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopViewer,Flash ,Vd3d,WebHelper,BrowserEngine,WorkspaceHub,USB`。

HDX 機能のパラメーター

ALLOW_BIDIRCONTENTREDIRECTION

「クライアントからホスト」と「ホストからクライアント」の間でのコンテンツの双方向リダイレクトを有効化します。詳しくは、Citrix Virtual Apps and Desktops のドキュメントで「双方向のコンテンツリダイレクトのポリシー設定」を参照してください。

- 0（デフォルト）- 双方向のコンテンツリダイレクトが無効なことを示します。例: `CitrixWorkspaceApp .exe ALLOW_BIDIRCONTENTREDIRECTION=0`。
- 1 - 双方向のコンテンツリダイレクトが有効なことを示します。例: `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=1`。

FORCE_LAA

Citrix Workspace アプリはクライアント側ローカルアプリアクセスのコンポーネントとともにインストールされます。このコンポーネントを動作させるには、管理者権限で Citrix Workspace アプリをインストールする必要があります。詳しくは、Citrix Virtual Apps and Desktops のドキュメントで「[ローカルアプリアクセス]」(/en-us/citrix-virtual-apps-desktops/general-content-redirection/laa-url-redirect.html) を参照してください。

- 0（デフォルト）- ローカルアプリアクセスのコンポーネントがインストールされていないことを示します。例: `CitrixWorkspaceApp.exe FORCE_LAA=0`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 1 - クライアント側ローカルアプリアクセスのコンポーネントがインストールされていることを示します。例: `CitrixWorkspaceApp.exe FORCE_LAA=1`。

LEGACYFTAICONS

サブスクライブするアプリケーションに関連付けられているファイルタイプのドキュメントまたはファイルに、そのアプリケーションアイコンを表示するかどうかを指定します。

- False（デフォルト）- サブスクライブするアプリケーションに関連付けられているファイルタイプのドキュメントまたはファイルに、そのアプリケーションアイコンが表示されることを示します。False に設定すると、特定のアイコンが割り当てられていないドキュメントのアイコンがオペレーションシステムで生成されます。生成されたアイコンでは、標準的なアイコン上にアプリケーションの小さいアイコンが重なって表示されます。例: `CitrixWorkspaceApp.exe LEGACYFTAICONS=False`。
- True - サブスクライブするアプリケーションに関連付けられているファイルタイプのドキュメントまたはファイルに、そのアプリケーションアイコンが表示されないことを示します。例: `CitrixWorkspaceApp.exe LEGACYFTAICONS=True`。

ALLOW_CLIENTHOSTEDAPPSURL

ユーザーデバイスの URL リダイレクト機能を有効にします。詳しくは、Citrix Virtual Apps and Desktops のドキュメントで「[ローカルアプリアクセス]」(/en-us/citrix-virtual-apps-desktops/general-content-redirection/laa-url-redirect.html) を参照してください。

- 0(デフォルト)- ユーザーデバイスの URL リダイレクト機能を無効にします。例: `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0`。
- 1- ユーザーデバイスの URL リダイレクト機能を有効にします。例: `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=1`。

基本設定とユーザーインターフェイスのパラメーター

ALLOWADDSTORE

指定されたパラメーターを基にしてストア（http または https）の構成を許可します。

- S（デフォルト）- （HTTPS で構成された）セキュアなストアのみ追加や削除を許可します。例: `CitrixWorkspaceApp.exe ALLOWADDSTORE=S`。
- A - ストアの追加や削除を許可します（HTTPS または HTTP で構成されたストア）。Citrix Workspace アプリがユーザー単位でインストールされている場合は使用できません。例: `CitrixWorkspaceApp.exe ALLOWADDSTORE=A`。
- N - ユーザーによるストアの追加や削除を許可しません。例: `CitrixWorkspaceApp.exe ALLOWADDSTORE=N`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ALLOWSAVEPWD

ストア認証情報をローカルに保存できます。このパラメーターは、PNAgent プロトコルを使用するストアにのみ適用されます。

- S（デフォルト）- （HTTPS で構成された）セキュアなストアのみパスワードの保存を許可します。例: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=S`。
- N - パスワードの保存を許可しません。例: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=N`。
- A - セキュアなストア（HTTPS）およびセキュアではないストア（HTTP）の両方にパスワードの保存を許可します。例: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=A`。

STARTMENUDIR

[スタート] メニューのショートカットのフォルダーを指定します。

- <`Directory Name`> - デフォルトでは、[スタート] > [すべてのプログラム] の下にアプリケーションのショートカットが追加されます。ショートカットを配置するフォルダーを`\Programs`からの相対パスで指定します。たとえば、[スタート] > [すべてのプログラム] > [Workspace] にショートカットを配置するには、`STARTMENUDIR=\Workspace`と指定します。

DESKTOPDIR

デスクトップ上のショートカットのフォルダーを指定します。

> 注:
>
> DESKTOPDIR オプションを使用するときは、`PutShortcutsOnDesktop`キーを`True`に設定します。

- <`Directory Name`> - ショートカットは相対パスで指定できます。たとえば、[スタート] > [すべてのプログラム] > [Workspace] にショートカットを配置するには、`DESKTOPDIR=\Workspace`と指定します。

SELFSERVICEMODE

セルフサービスの Citrix Workspace アプリのユーザーインターフェイスに対するアクセスを制御します。

- True - ユーザーはセルフサービスのユーザーインターフェイスにアクセスできます。例: `CitrixWorkspaceApp.exe SELFSERVICEMODE=True`。
- False - ユーザーはセルフサービスのユーザーインターフェイスにアクセスできません。例: `CitrixWorkspaceApp.exe SELFSERVICEMODE=False`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ENABLEPRELAUNCH

セッションの事前起動を制御します。詳しくは、「[アプリケーションの起動時間]」(/en-us/citrix-workspace-app-for-windows/configure.html#application-launch-time) を参照してください。

- True - セッションの事前起動が有効です。例: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True`。
- False - セッションの事前起動が無効です。例: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False`。

DisableSetting

[高度な設定] シートで [ショートカット] と [再接続] オプションが表示されないようにします。詳しくは、「[高度な設定] シートから特定の設定を非表示にする」を参照してください。

- 0（デフォルト）- [高度な設定] シートで [ショートカット] と [再接続] の両方のオプションを表示します。例: `CitrixWorkspaceApp.exe DisableSetting=0`。
- 1 - [高度な設定] シートで [再接続] オプションを表示します。例: `CitrixWorkspaceApp.exe DisableSetting=1`。
- 2 - [高度な設定] シートで [ショートカット] オプションを表示します。例: `CitrixWorkspaceApp.exe DisableSetting=2`。
- 3 - [高度な設定] シートで [ショートカット] と [再接続] の両方のオプションを非表示にします。例: `CitrixWorkspaceApp.exe DisableSetting=3`。

EnableCEIP

カスタマーエクスペリエンス向上プログラム（CEIP）に参加することを示します。詳しくは、「CEIP」を参照してください。

- True（デフォルト）- CEIP にオプトインします。例: `CitrixWorkspaceApp.exe EnableCEIP=True`。
- False - CEIP からオプトアウトします。例: `CitrixWorkspaceApp.exe EnableCEIP=False`。

EnableTracing

常時トレース機能を制御します。

- True（デフォルト）- 常時トレース機能を有効にします。例: `CitrixWorkspaceApp.exe EnableTracing=true`。
- False - 常時トレース機能を無効にします。例: `CitrixWorkspaceApp.exe EnableTracing=false`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

CLIENT_NAME

サーバーでユーザーデバイスを識別するために使用される名前です。

- <ClientName> - サーバーでユーザーデバイスを識別するために使用される名前です。デフォルト名は%COMPUTERNAME%です。例: CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%。

ENABLE_DYNAMIC_CLIENT_NAME

クライアント名をコンピューター名と同じ名前にすることができます。この場合、ユーザーがコンピューター名を変更すると、クライアント名もそれに応じて変更されます。

- Yes(デフォルト)- クライアント名をコンピューター名と同じ名前にできます。例:CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes。
- No - クライアント名をコンピューター名と同じ名前にできません。CLIENT_NAMEプロパティの値を指定する必要があります。例: CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No。

認証パラメーター

ENABLE_SSON

Citrix Workspace アプリが/includeSSONコマンドでインストールされた場合、シングルサインオンを有効にします。詳しくは、「[ドメインパススルー認証]」(/en-us/citrix-workspace-app-for-windows/authentication.html#domain-pass-through-authentication) を参照してください。

- Yes（デフォルト）- シングルサインオンが有効になっています。例: CitrixWorkspaceApp.exe /ENABLE_SSON=Yes。
- No - シングルサインオンが無効になっています。例: CitrixWorkspaceApp.exe /ENABLE_SSON=No。

ENABLE_KERBEROS

HDX エンジンが Kerberos 認証を使用する必要があるかどうかを指定します。これは、シングルサインオン認証が有効な場合にのみ適用されます。詳しくは、「Kerberos を使用したドメインパススルー認証」を参照してください。

- Yes - HDX エンジンが Kerberos 認証を使用します。例: CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes。
- No - HDX エンジンが Kerberos 認証を使用しません。例: CitrixWorkspaceApp.exe ENABLE_KERBEROS=No。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

上記のプロパティに加えて、Citrix Workspace アプリで使用するストア URL も指定できます。10 ストアまで追加できます。このためには、以下のプロパティを使用します:

```
STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On, Off]; [storedescription]"
```

値:

- x - ストアを識別するために使用される整数 0～9。
- storename - ストアの名前。これは、StoreFront サーバーで構成される名前と同じである必要があります。
- servername.domain - ストアをホストするサーバーの完全修飾ドメイン名。
- IISLocation - IIS 内のストアへのパス。このストア URL は、StoreFront プロビジョニングファイルに記述されている URL と同じである必要があります。ストア URL は「/Citrix/store/discovery」の形式です。URL を取得するには、StoreFront からプロビジョニングファイルをエクスポートしてそれをメモ帳などのテキストエディターで開き、**Address** エレメントから URL をコピーします。
- [On、Off] - **Off** オプションを指定すると、無効なストアを配信できるようになります。これにより、そのストアにアクセスするかどうかをユーザーが選択できるようになります。このオプションを指定しない場合、デフォルトの設定は **On** になります。
- storedescription - ストアの説明（「HR App Store」など）。

コマンドラインを使用したインストールの例

Citrix Gateway のストア **URL** を指定するには:

```
CitrixWorkspaceApp.exe STORE0=HRStore;https://ag.mycompany.com#Storename;On;Store
```

ここで *Storename* は、構成する必要があるストアの名前です。

> 注:
>
> - Citrix Gateway のストア URL を上記の方法で構成した場合、Citrix Gateway を使用している PNA サービスサイトはサポートされません。
> - 複数のストアを構成する場合、Citrix Gateway のストア URL は一覧の最初に表示されます。Citrix Gateway ストアの URL は、1 つだけ構成できます。

以下のコマンドでは、すべてのコンポーネントをサイレントインストールして **2** つのアプリケーションストアを指定します。

```
CitrixWorkspaceApp.exe /silent
STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR App Store"
STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/discovery;on;Backup HR App Store"
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> - パススルー認証を成功させるには、ストア URL に/discoveryを含める必要があります。
> - Citrix Gateway のストア URL は、構成済みのストア URL 一覧で最初のエントリにする必要があります。

アンインストール

Windows 向けインストーラーの使用:

コントロールパネルの［プログラムと機能］（または［プログラムの追加と削除］）を使って Windows 向け Citrix Workspace アプリをアンインストールできます。

> 注:
>
> Windows 向け Citrix Workspace アプリのインストールを続行する前に、Citrix HDX RTME パッケージのアンインストールを求めるメッセージが表示されます。［OK］をクリックしてアンインストールを続行します。

コマンドラインインターフェイスの使用:

ユーザーは、コマンドラインから以下のコマンドを実行して Windows 向け Citrix Workspace アプリをアンインストールすることもできます。

```
CitrixWorkspaceApp.exe /uninstall
```

Windows 向け Citrix Workspace アプリをサイレントアンインストールするには、次のスイッチを実行します:

```
CitrixWorkspaceApp.exe /silent /uninstall
```

> 注:
>
> - reiver.adm/receiver.adml または receiver.admx によって作成されたレジストリキーは、アンインストール後も残ります。
> - アンインストール後、レジストリエディターにエントリが残っている場合、手動で削除してください。

展開

November 3, 2023

次のいずれかの方法で Citrix Workspace アプリを展開できます:

- Active Directory およびサンプルスタートアップスクリプトを使用して Windows 向け Citrix Workspace アプリを展開します。Active Directory については詳しくは、「Active Directory とサンプルスクリプトの使用」を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Web 向け Workspace を使用すると、ブラウザーからアプリケーションを起動する前に、Windows 向け Citrix Workspace アプリを確実にインストールできます。詳しくは、「Web 向け Workspace の使用」を参照してください。
- Microsoft System Center Configuration Manager 2012 R2 などの電子ソフトウェア配信（ESD）ツールを使用します。詳しくは、「System Center 2012 R2 Configuration Manager の使用」を参照してください。

Active Directory とサンプルスクリプトの使用

Active Directory のグループポリシースクリプトを使用して、Active Directory の組織構造に基づいてシステムに Windows 向け Citrix Workspace アプリを展開することができます。Citrix では.msi ファイルの展開ではなくスクリプトの使用をお勧めします。スタートアップスクリプトの概要については、Microsoft 社のドキュメントを参照してください。

Active Directory でスクリプトを使用するには:

1. 各スクリプトの組織単位を作成します。
2. 新しく作成した組織単位のグループポリシーオブジェクトを作成します。

スクリプトの編集

各ファイルのヘッダーセクションにあるスクリプトの次のパラメーターを編集します:

- **CURRENT VERSION OF PACKAGE**（パッケージの現在のバージョン）- ここに指定するバージョン番号が検証され、そのバージョンが存在しない場合は展開（インストール）が開始されます。たとえば、DesiredVersion= 3.3.0.XXXX に、展開するバージョンの番号を指定します。バージョンの一部（たとえば 3.3.0）を指定すると、その接頭辞を持つすべてのバージョン（3.3.0.1111、3.3.0.7777 など）に一致します。
- **PACKAGE LOCATION/DEPLOYMENT DIRECTORY**（パッケージの場所/展開ディレクトリ）- パッケージを格納するネットワーク共有を指定します。この共有にアクセスするための認証はスクリプトで実行しません。共有フォルダーで読み取りアクセス許可を EVERYONE に設定する必要があります。
- **SCRIPT LOGGING DIRECTORY**（スクリプトのログディレクトリ）- インストールログをコピーするネットワーク共有を指定します。この共有にアクセスするための認証はスクリプトで実行しません。共有フォルダーに Everyone の読み取り/書き込みアクセス許可を設定する必要があります。
- **PACKAGE INSTALLER COMMAND LINE OPTIONS**（パッケージインストーラーのコマンドラインオプション）- インストーラーに渡すコマンドラインオプションを指定します。コマンドライン構文については、「コマンドラインパラメーターの使用」を参照してください。

スクリプト

Citrix Workspace アプリインストーラーには、Citrix Workspace アプリのインストールおよびアンインストール用のコンピューター単位およびユーザー単位でのサンプルスクリプトが含まれています。スクリプトは、Windows

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

向け Citrix Workspace アプリの ［ダウンロード］ ページからダウンロードできます。

展開の種類	展開する	削除する
コンピューター単位	CheckAndDeployWorkspacePerMachineStartupScript.bat	CheckAndRemoveWorkspacePerMachineSta
ユーザー単位	CheckAndDeployWorkspacePerUserLogonScript.bat	CheckAndRemoveWorkspacePerUserLogonS

スタートアップスクリプトを追加するには:

1. グループポリシー管理コンソールを開きます。
2. ［コンピューターの構成］または ［ユーザーの構成］> ［ポリシー］> ［**Windows** の設定］> ［スクリプト］の順に選択します。
3. グループポリシー管理コンソールの右ペインで ［ログオン］を選択します。
4. ［ファイルの表示］を選択して適切なスクリプトを表示されたフォルダーにコピーします。
5. ダイアログを閉じます。
6. ［スタートアップのプロパティ］ダイアログボックスで ［追加］をクリックし、［参照］をクリックして新しく作成したスクリプトを検索し追加します。

Windows 向け **Citrix Workspace** アプリを展開するには:

1. 作成した組織単位に展開対象のユーザーデバイスを移動します。
2. ユーザーデバイスを再起動してログオンします。
3. 新しくインストールしたパッケージが ［プログラムと機能］に表示されることを確認します。

Windows 向け **Citrix Workspace** アプリを削除するには:

1. 作成した組織単位に削除対象のユーザーデバイスを移動します。
2. ユーザーデバイスを再起動してログオンします。
3. 新しくインストールしたパッケージが［プログラムと機能］に表示されないことを確認します。

Web 向け **Workspace** の使用

Windows 向け Citrix Workspace アプリを Web 向け Workspace から展開すると、ブラウザーからアプリケーションに接続する前に、Windows 向け Citrix Workspace アプリのインストールが済んでいることが保証されます。Web 向け Workspace のサイトを使用すると、ユーザーは Web ページを経由して StoreFront ストアにアクセスできます。Web 向け Workspace で適切なバージョンの Windows 向け Citrix Workspace アプリがインストールされていないことが検出されると、Windows 向け Citrix Workspace アプリをダウンロードしてインストールするためのページが表示されます。

Web 向け Workspace を使用して展開された Windows 向け Citrix Workspace アプリでは、メールアドレスによるアカウント検出機能はサポートされていませんメールアドレスによるアカウント検出機能が構成された環境では、初めて使用するユーザーが Windows 向け Citrix Workspace アプリを Citrix.com からインストールすると、メー

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ルアドレスまたはサーバーアドレスの入力が求められます。ここでユーザーがメールアドレスを入力すると、メールアドレスを使ってアカウントを追加できないという内容のエラーメッセージが表示されます。

ユーザーの混乱を避けるため、サーバーアドレスの入力のみが求められるようにします。

1. `CitrixWorkspaceApp.exe`をローカルコンピューターにダウンロードします。
2. `CitrixWorkspaceApp.exe`を`CitrixWorkspaceAppWeb.exe`という名前に変更します。
3. 名前を変更した実行可能ファイルを通常の方法で展開します。StoreFront を使用している場合は、StoreFront のドキュメントの「構成ファイルによる Web 向け Workspace サイトの構成」を参照してください。

Microsoft System Center 2012 R2 Configuration Manager の使用

Microsoft System Center Configuration Manager（SCCM）を使用して、Citrix Workspace アプリを展開できます。

> 注:
>
> Citrix Receiver for Windows バージョン 4.5 以降のみが SCCM 展開環境をサポートします。

SCCM を使用して Windows 向け Citrix Workspace アプリを展開する方法は 4 段階に分けられます:

1. Citrix Workspace アプリを SCCM 展開環境に追加する
2. 配布ポイントを追加する
3. Citrix Workspace アプリをソフトウェアセンターに展開する
4. デバイスコレクションを作成する

Citrix Workspace アプリを SCCM 展開環境に追加する

1. ダウンロードした Citrix Workspace アプリのインストールフォルダーを Configuration Manager サーバー上のフォルダーにコピーして、Configuration Manager コンソールを起動します。
2. ［ソフトウェアライブラリ］、［アプリケーション管理］の順に選択します。［アプリケーション］を右クリックして、［アプリケーションの作成］を選択します。
   アプリケーションの作成ウィザードが開きます。
3. ［全般］ページで ［アプリケーションの情報を手動で指定する］をクリックし、［次へ］をクリックします。
4. ［一般情報］ペインで、アプリケーションの情報（名前、製造元、ソフトウェアバージョンなど）を指定します。
5. ［アプリケーションカタログ］ウィザードで、追加の情報（言語、アプリケーション名、ユーザーカテゴリなど）を指定して、［次へ］をクリックします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> ユーザーはここで指定した情報を表示できます。

6. ［展開の種類］ペインで、［追加］を選択して Windows 向け Citrix Workspace アプリのセットアップで展開の種類を構成します。

   展開の種類の作成ウィザードが開きます。

7. ［全般］ペイン：展開の種類を Windows インストーラー（*.msi ファイル）に設定し、［展開の種類の情報を手動で指定する］を選択して、［次へ］をクリックします。

8. ［一般情報］ペイン：展開の種類の詳細（例：Workspace の展開）を指定して、［次へ］をクリックします。

9. ［コンテンツ］ペイン：

   a) Citrix Workspace アプリセットアップファイルのある場所へのパスを指定します。例：SCCM サーバー上のツール。

   b) ［インストールプログラム］に次のいずれかを指定します：

   - `CitrixWorkspaceApp.exe /silent`を指定して、サイレントインストールする。
   - `CitrixWorkspaceApp.exe /silent /includeSSON`を指定して、ドメインパススルーを有効にする。
   - `CitrixWorkspaceApp.exe /silent SELFSERVICEMODE=false`を指定して、セルフサービスモード以外で Citrix Workspace アプリをインストールします。

   c) ［アンインストールプログラム］に`CitrixWorkspaceApp.exe /uninstall`を指定します（SCCM でのアンインストールを有効にする）。

10. ［検出方法］ペイン：［この展開の種類のプレゼンスを検出する規則を構成する］を選択して ［句の追加］をクリックします。
    ［検出方法］ダイアログボックスが開きます。

    - ［設定の種類］をファイルシステムに設定します。
    - ［このアプリケーションを検出するためのファイルまたはフォルダーを指定してください］で、次のように設定します：
      - 種類 - ドロップダウンメニューから、［ファイル］を選択します。
      - パス - `%ProgramFiles(x86)%\\Citrix\\ICA Client\\Receiver\`
      - ファイル名またはフォルダー名 - `receiver.exe`
      - プロパティ - ドロップダウンリストから ［バージョン］を選択します
      - 演算子 - ドロップダウンメニューで ［次のもの以上］を選択します
      - 値 - 展開する Citrix Workspace アプリのバージョン番号を入力します。

> 注:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> この規則の組み合わせは、Windows 向け Citrix Workspace アプリのアップグレードにも適用されます。

11. ［ユーザー側の表示と操作］ペインで、次の値を設定します：

    - ［インストールの動作］ - ［システム用にインストールする］
    - ［必要なログオン状態］ - ［ユーザーのログオン状態に関係なし］
    - ［インストールプログラムの表示］ - ［通常］

    ［次へ］をクリックします。

    > 注：
    >
    > この展開の種類には、要件や依存関係を指定しないでください。

12. ［概要］ペインで、この展開の種類の設定を確認します。［次へ］をクリックします。

    成功メッセージが表示されます。

13. ［完了］ペインの［展開の種類］一覧に新しい展開の種類（Workspace の展開）が表示されます。
14. ［次へ］をクリックして、［閉じる］をクリックします。

配布ポイントを追加する

1. ［Configuration Manager］コンソールで Citrix Workspace アプリを右クリックして、［コンテンツの配布］を選択します。

   コンテンツの配布ウィザードが開きます。

2. ［コンテンツの配布］ペインで、［追加］**>**［配布ポイント］を選択します。

   ［配布ポイントの追加］ダイアログボックスが開きます。

3. コンテンツが利用可能な SCCM サーバーに移動して、［**OK**］をクリックします。

   ［完了］ペインで、成功メッセージが表示されます。

4. ［閉じる］をクリックします。

Citrix Workspace アプリをソフトウェアセンターに展開する

1. Configuration Manager コンソールで Citrix Workspace アプリを右クリックして、［展開］を選択します。

   ソフトウェアの展開ウィザードが開きます。

2. アプリケーションを展開するコレクション（デバイスコレクションまたはユーザーコレクション）を検索して、［次へ］をクリックします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. ［展開設定］ペインで ［アクション］を［インストール］に ［目的］を［必須］に設定します（無人インストールを有効にする）。［次へ］をクリックします。
4. ［スケジュール］ペインで、対象のデバイスでソフトウェアを展開するスケジュールを指定します。
5. ［ユーザー側の表示と操作］ペインで、［ユーザーへの通知］動作を設定します。［メンテナンスの期限または期間中の変更を確定する（再起動が必要）］を選択し、［次へ］をクリックしてソフトウェアの展開ウィザードを終了します。

［完了］ペインで、成功メッセージが表示されます。

対象のエンドポイントデバイスを再起動します（すぐにインストールを開始する場合のみ必要）。

エンドポイントデバイスの Citrix Workspace アプリは、利用可能なソフトウェアのソフトウェアセンターに表示されます。構成したスケジュールに基づいて、自動的にインストールが開始します。また、オンデマンドでスケジュール設定したり、インストールしたりできます。インストールの状態は、インストールの開始後、ソフトウェアセンターに表示されます。

デバイスコレクションを作成する

1. Configuration Manager コンソールを起動して、［資産とコンプライアンス］、［概要］、［デバイス］の順に選択します。
2. ［デバイスコレクション］を右クリックして、［デバイスコレクションの作成］を選択します。

   デバイスコレクションの作成ウィザードが開きます。
3. ［全般］ペインでデバイスの ［名前］を入力して、［参照］をクリックして制限するコレクションを検索します。

   これによって、デバイスの対象が決定されます。SCCM で作成されるデフォルトのデバイスコレクションの場合もあります。
   ［次へ］をクリックします。
4. ［メンバーシップの規則］ペインで、［規則の追加］を選択してデバイスを絞り込みます。

   ダイレクトメンバーシップの規則の作成ウィザードが開きます。

   - ［リソースの検索］ペインで、絞り込みたいデバイスに基づいて ［属性名］を選択し、属性名を入力して、デバイスを選択します。
5. ［次へ］をクリックします。［リソースの選択］ペインで、デバイスコレクションの一部にする必要があるデバイスを選択します。

   ［完了］ペインで、成功メッセージが表示されます。
6. ［閉じる］をクリックします。
7. ［メンバーシップの規則］ペインで、新しい規則の一覧が［次へ］をクリックの下に表示されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. ［完了］ペインで、成功メッセージが表示されます。［閉じる］をクリックして、デバイスコレクションの作成ウィザードを完了します。

   ［デバイスコレクション］の一覧に新しいデバイスコレクションが表示されます。新しいデバイスコレクションは、ソフトウェアの展開ウィザードの参照中のデバイスコレクションの一部です。

> 注:
>
> **MSIRESTARTMANAGERCONTROL** 属性を **False** に設定すると、SCCM を使用した Windows 向け Citrix Workspace アプリの展開が失敗することがあります。
> 分析によると、Windows 向け Citrix Workspace アプリはこのエラーの原因ではありません。再試行で展開が成功することがあります。

アップデート

April 22, 2024

手動更新

既に Windows 向け Citrix Workspace アプリをインストールしている場合は、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

バージョン 1912 の累積更新プログラム 4（CU4）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、マシン全体の更新の場合、C:\Program Files (x86)\Citrix\Logs にあります。ユーザー全体の更新の場合は、ユーザーの一時フォルダーにあります。

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。

> 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バー`https://downloadplugins.citrix.com/`に例外を追加して Citrix からの更新を受信します。
> - 自動更新は、Citrix Workspace アプリ 2104 および Citrix Workspace アプリ 1912 LTSR CU4 より前のバージョンでは利用できません。
> - 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`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **:**//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。
> - デフォルトでは、VDA で Citrix Workspace の更新が無効になっています。リモートデスクトップのマルチユーザーサーバーマシン、VDI、リモート PC アクセスマシンでも同様です。
> - Citrix Workspace の更新は、Desktop Lock がインストールされたマシンでは無効になっています。
> - 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 の更新は、LTSR 更新のみに限定されます。
> - Citrix Workspace の更新に Windows 用の HDX RTME が含まれています。Citrix Workspace アプリの LTSR と最新リリースの両方で使用可能な HDX RTME の更新が通知されます。

自動更新の詳細設定（**Citrix Workspace** の更新）

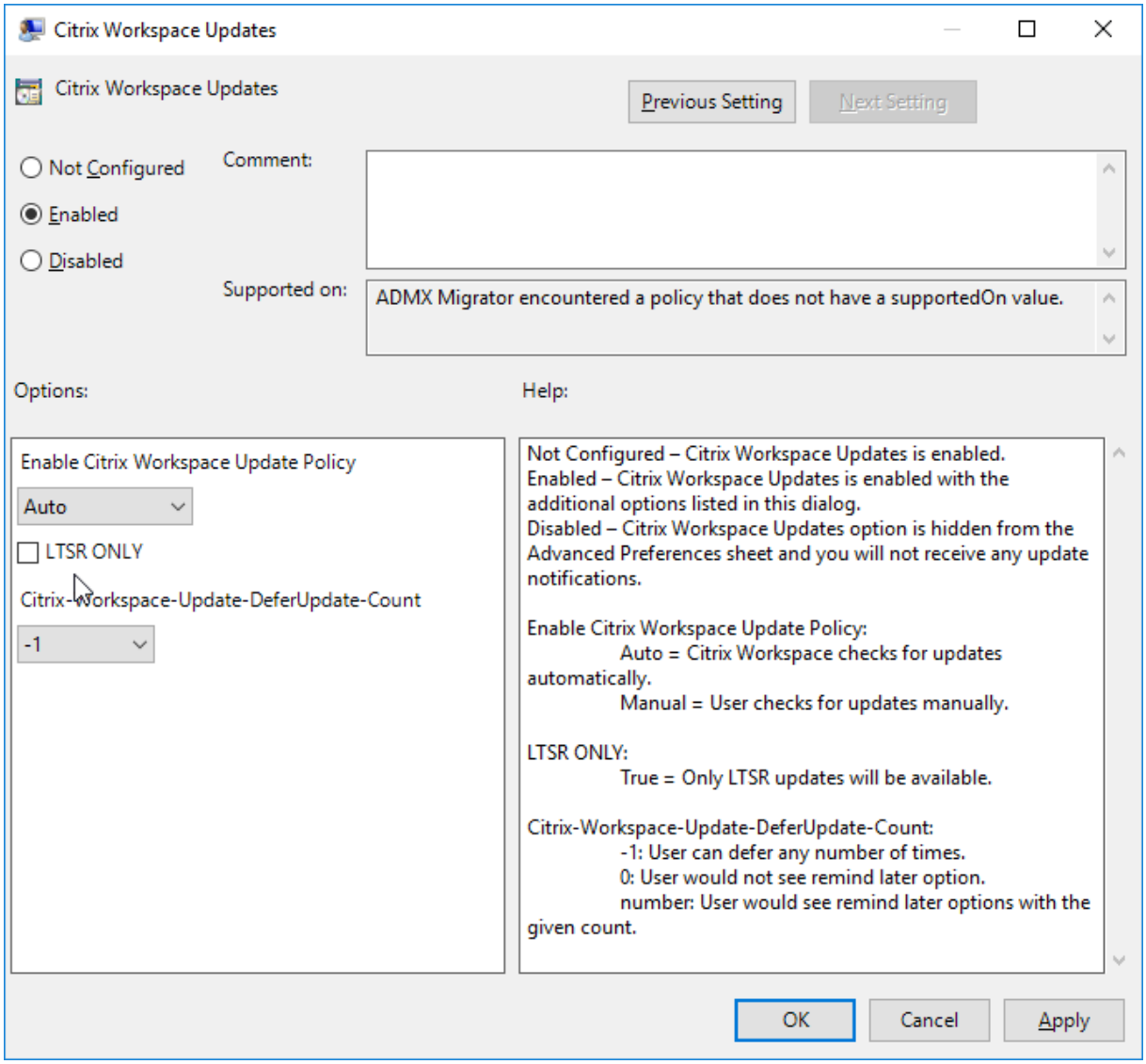
Citrix Workspace の更新は、次の方法で構成できます：

1. グループポリシーオブジェクト（GPO）管理用テンプレート
2. コマンドラインインターフェイス
3. グラフィカルユーザーインターフェイス
4. StoreFront

グループポリシーオブジェクト管理用テンプレートを使用した **Citrix Workspace** 更新プログラムの構成

gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開き、［コンピューターの構成］ノードで、［管理用テンプレート］>［**Citrix** コンポーネント］>［**Citrix Workspace**］>［**Citrix Workspace** の更新］の順に移動します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. 更新を有効または無効にする—［有効］または ［無効］を選択して、Workspace の更新を有効または無効にします。

   > 注:
   >
   > ［無効］を選択すると、新しい更新が通知されません。これにより、［高度な設定］シートの［Workspace の更新］オプションも非表示になります。

2. 更新通知—更新が利用可能になったときに、自動的に通知を受信するか、手動で確認するかを選択できます。Workspace の更新を有効にした後、［**Citrix Workspace** の更新ポリシーを有効にする］ドロップダウンリストの次のオプションから選択します:

   - Auto - 更新が利用可能になると通知します（デフォルト）。
   - Manual - 更新が利用可能になっても通知されません。手動で更新をチェックします。

3. ［**LTSR** のみ］を選択して LTSR の更新のみを取得します。

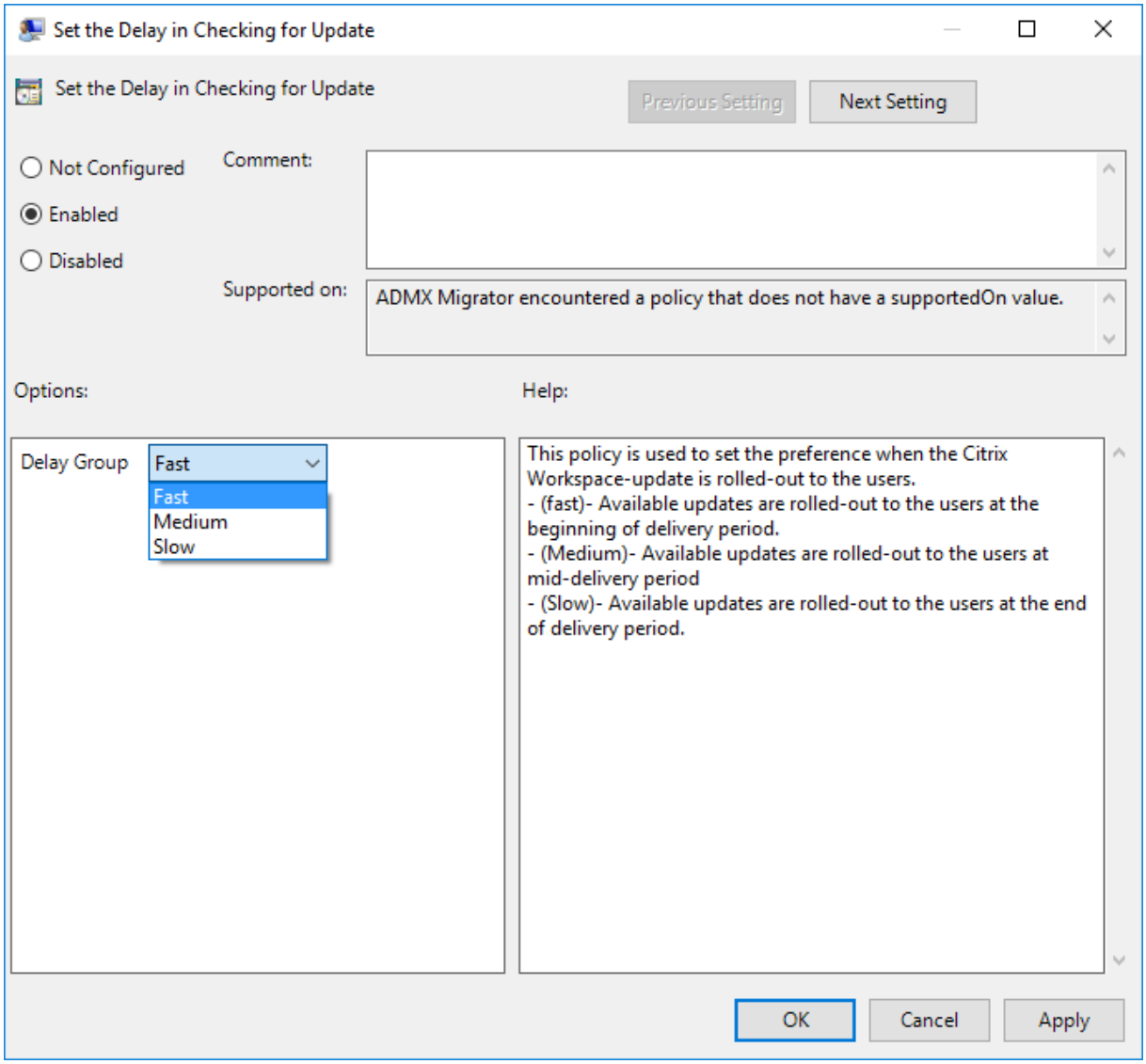
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. [**Citrix-Workspace-Update-DeferUpdate-Count**] ドロップダウンリストから、-1～30 の値を選択します:

   - -1 - 何度でも通知を延期できます（デフォルト）。
   - 0 - 更新の通知を一度のみ受信します。

更新のチェックで遅延を構成　新しいバージョンの Citrix Workspace アプリがリリースされると、特定の配信期間に更新プログラムがロールアウトされます。このプロパティを使用すると、配信期間中に更新を受信するタイミングを制御できます。

配信期間を構成するには、`gpedit.msc`を実行してグループポリシーオブジェクト管理用テンプレートを起動します。[コンピューターの構成] ノードで、[管理用テンプレート] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [更新のチェックで遅延を設定] の順に移動します。



[有効] を選択し、[遅延グループ] ドロップダウンリストの次のオプションから選択します:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Fast - 配信期間の最初に更新がロールアウトされます。
- Medium - 配信期間の中頃に更新がロールアウトされます。
- Slow - 配信期間の最後に更新がロールアウトされます。

> 注:
>
> ［無効］を選択すると、利用可能な更新が通知されません。これにより、［高度な設定］シートの［Workspace の更新］オプションも非表示になります。

コマンドラインインターフェイスを使用した **Citrix Workspace** 更新プログラムの構成

Citrix Workspace アプリのインストール中にコマンドラインパラメーターを指定する:

Citrix Workspace アプリのインストール中にコマンドラインパラメーターを指定することで、Workspace の更新を構成できます。詳しくは、「パラメーターのインストール」を参照してください。

Citrix Workspace アプリのインストール後にコマンドラインパラメーターを使用する:

Citrix Workspace の更新は、Windows 向け Citrix Workspace アプリのインストール後にも構成できます。Windows コマンドラインを使用して、CitrixReceiverUpdater.exe の場所に移動します。

通 常、CitrixWorkspaceUpdater.exe はCitrixWorkspaceInstallLocation\Citrix\Ica Client\Receiverにあります。このバイナリは、「パラメーターのインストール」セクションに記載されているコマンドラインパラメーターとともに実行できます。

例:

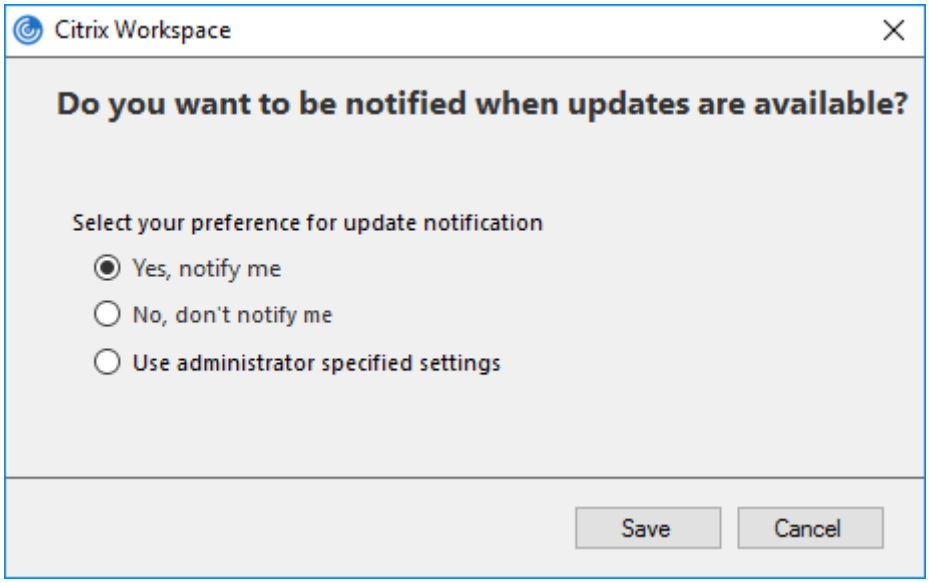
```
CitrixReceiverUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=
Current /DeferUpdateCount=-1 /AURolloutPriority=fast
```

> 注:
>
> /AutoUpdateCheckは、/AutoUpdateStream、/DeferUpdateCount、/AURolloutPriority などの他のパラメーターを構成するために設定する必要がある必須パラメーターです。

グラフィカルユーザーインターフェイスを使用した **Citrix Workspace** 更新プログラムの構成

各ユーザーが［高度な設定］ダイアログボックスで［Citrix Workspace の更新］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。システムトレイの Citrix Workspace アプリアイコンを右クリックします。［高度な設定］> ［**Workspace** の更新］を選択します。通知設定を選択し、［保存］をクリックします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> 注:
>
> システムトレイの Citrix Workspace アプリアイコンから表示できる［高度な設定］シートの一部または全部を非表示にすることができます。詳しくは、「高度な設定シート」セクションを参照してください。

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ってストアの`web.config`ファイルを開きます。このファイルは通常、`C:\inetpub\wwwroot\Citrix\Roaming directory`にあります。
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">

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<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-LTSR-Only" value
                 ="FALSE" />

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

            </properties>

    </metadata>

  </annotatedServiceRecord>

</annotatedServices>

<metadata>

  <plugins>

    <clear />

  </plugins>

  <trustSettings>

    <clear />

```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
70
71  <!--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することを示します。
- **Auto-update-LTSR-Only**: リリースの更新が LTSR のみであることを示します。
- **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。

開始

April 22, 2024

このドキュメントは、Citrix Workspace アプリのインストール後、環境をセットアップする場合に参照できます。

前提条件:

「システム要件」セクションに記載されたすべてのシステム要件を確認してください。

Citrix Workspace アプリを使用する前に、次の構成を完了する必要があります:

- グループポリシーオブジェクト管理用テンプレート
- StoreFront
- Citrix Gateway Store
- Citrix Workspace アプリへのストア URL の追加
- クライアントドライブマッピング
- DNS 名前解決

グループポリシーオブジェクト管理用テンプレート

ネットワークのルーティング、プロキシサーバー、信頼されるサーバーの設定、ユーザーのルーティング、リモートユーザーデバイス、およびユーザーエクスペリエンスに関する規則の構成では、グループポリシーオブジェクト管理

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

用テンプレートを使うことをお勧めします。
ドメインポリシーおよびローカルコンピューターのポリシーで receiver.admx/receiver.adml テンプレートファイルを使用することができます。ドメインポリシーの場合、グループポリシー管理コンソールを使ってテンプレートファイルをインポートします。これは組織全体に存在する多くの異なるユーザーデバイスに Citrix Workspace アプリの設定を適用するのに非常に有用です。単一ユーザーデバイスの場合は、デバイス上のローカルのグループポリシーエディターを使ってテンプレートをインポートします。

Windows グループポリシーオブジェクト（GPO）管理用テンプレートを使用して Citrix Workspace アプリを構成することをお勧めします。

Citrix Receiver for Windows バージョン 4.6 以降、インストールディレクトリに`CitrixBase.admx`、`CitrixBase.adml`、および管理用テンプレートファイル（receiver.adm または receiver.admx\receiver.adml - オペレーティングシステムによって異なります）が含まれています。

> 注:
>
> .adm ファイルは、Windows XP Embedded プラットフォームでのみ使用されます。.admx/.adml ファイルは、Windows Vista/Windows Server 2008、および以降のすべての Windows バージョンで使用されます。

Citrix Workspace アプリを VDA とともにインストールする場合、admx/adml ファイルはインストールディレクトリにあります。たとえば、\< インストールディレクトリ\>\\Online Plugin\\Configuration です。

Citrix Workspace アプリを VDA なしでインストールする場合、admx/adml ファイルは通常`C:\Program Files\Citrix\ICA Client\Configuration`ディレクトリにあります。

Citrix Workspace アプリの各テンプレートファイルとその配置場所については以下の表を参照してください。

> 注:
>
> 最新バージョンの Citrix Workspace アプリと共に提供される GPO テンプレートファイルを使用することをお勧めします。

ファイルタイプ	ファイルの場所
receiver.adm	\ICA Client\Configuration
receiver.admx	\ICA Client\Configuration
receiver.adml	\ICA Client\Configuration\[MUIculture]
CitrixBase.admx	\ICA Client\Configuration
CitrixBase.adml	\ICA Client\Configuration\[MUIculture]

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> - CitrixBase.admx\adml がローカル GPO に追加されないと、[**ICA** ファイルの署名を有効にします] ポリシーが失われることがあります。
> - Citrix Workspace アプリをアップグレードする場合、以下の手順に従って最新のテンプレートをローカル GPO に追加します。最新のファイルをインポートしても、以前の設定は保持されます。

ローカル **GPO** に **receiver.adm** テンプレートファイルを追加するには（**Windows XP Embedded** オペレーティングシステムの場合）:

グループポリシーオブジェクトエディターでオプションが正しく整理され、表示されるようにするには、CitrixBase.admx/CitrixBase.adml ファイルの使用をお勧めします。

adm テンプレートファイルを使用して、ローカル GPO やドメインベースの GPO のどちらか、または両方を構成できます。

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. グループポリシーエディターで ［管理用テンプレート］を選択します。
3. ［操作］メニューの ［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、テンプレートファイルの場所\<Installation Directory>\ICA Client\Configuration\receiver.admを参照します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。

   ローカル GPO ディレクトリ［管理用テンプレート］**>** ［従来の管理用テンプレート（**ADM**）］**>** ［**Citrix** コンポーネント］**>** ［**Citrix Workspace**］に、Citrix Workspace アプリのテンプレートファイルが追加されます。

ローカル GPO に.adm テンプレートファイルが追加されると、次のメッセージが表示されます:

「The following entry in the [strings] section is too long and has been truncated:
Click **OK** to ignore the message.」

ローカル **GPO** に**.admx/adml** テンプレートファイルを追加するには（最近のバージョンの **Windows** オペレーティングシステムの場合）:

adm テンプレートファイルを使用して、ローカル GPO やドメインベースの GPO のどちらか、または両方を構成できます。ADMX ファイルの管理については、こちらの Microsoft MSDN の記事を参照してください。

Citrix Workspace アプリをインストールしてから、以下の表のテンプレートファイルをコピーします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ファイルタイプ	コピー元	コピー先
receiver.admx	インストールディレクトリ\ICA Client\Configuration\receiver.admx	%systemroot%\policyDefinitions
CitrixBase.admx	インストールディレクトリ\ICA Client\Configuration\CitrixBase.admx	%systemroot%\policyDefinitions
receiver.adml	インストールディレクトリ\ICA Client\Configuration[MUIculture]receiver.adml	%systemroot%\policyDefinitions[MUIculture
CitrixBase.adml	インストールディレクトリ\ICA Client\Configuration[MUIculture]\CitrixBase.adml	%systemroot%\policyDefinitions[MUIculture

> 注:
>
> Citrix Workspace アプリのテンプレートファイルは、[管理用テンプレート]>[**Citrix** コンポーネント]>[**Citrix Workspace**] フォルダーのローカル GPO にあります（ユーザーが CitrixBase.admx/CitrixBase.adml を`\PolicyDefinitions`フォルダーに追加する場合のみ）。

StoreFront

Citrix StoreFront は、Citrix Virtual Apps and Desktops、Citrix DaaS（Citrix Virtual Apps and Desktops サービスの新名称）、VDI-in-a-Box への接続を認証し、使用可能なデスクトップおよびアプリケーションを Citrix Workspace アプリでアクセスできるストアに集約します。

ここで説明する構成手順に加えて、リモートユーザー（インターネットを介して接続するユーザーや遠隔地のユーザーなど）が内部ネットワークにアクセスできるように Citrix Gateway を構成する必要もあります。

> 注:
>
> すべてのストアを表示するオプションを選択すると、古い StoreFront ユーザーインターフェイスが表示されることがあります。

StoreFront を構成するには:

StoreFrontのドキュメントを参照して、StoreFront をインストールして構成します。Citrix Workspace アプリを使用するには、HTTPS 接続が必要です。StoreFront サーバーで HTTP が構成されている場合は、ユーザーデバイス上のレジストリキーを設定する必要があります。詳しくは、「コマンドラインパラメーターの使用」の **ALLOWADDSTORE** プロパティに関する説明を参照してください。

> 注:
>
> 独自の Windows 向け Citrix Workspace アプリダウンロードサイトを作成する管理者用に、テンプレートが提供されています。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Gateway Store

グループポリシーオブジェクト管理用テンプレートを使用して **Citrix Gateway** を追加または指定するには:

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. [コンピューターの構成] ノードで、[管理用テンプレート] > [従来の管理用テンプレート (**ADM**)] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [**StoreFront**] の順に移動します。
3. [**Citrix Gateway URL\StoreFront** アカウント一覧] を選択します。
4. 設定を編集します。
    - [ストア名] - ストアの表示名を指定します。
    - [ストア URL] - ストアの URL を指定します。
    - [#Store name]–Citrix Gateway の背後にあるストアの名前を指定します。
    - [ストアの有効/無効] - ストアの状態を On または Off で指定します。
    - [ストアの説明] - ストアの説明を入力します。
5. Citrix Gateway URL を追加または指定します。URL 名をセミコロンで区切って入力します:

例: `CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com#Storename;On;Store`
#Storename は Citrix Gateway の背後にあるストアの名前です。

以前のリリースでは、GPO の **Citrix Gateway URL/StoreFront Account List** ポリシーを使用してアカウントを追加または削除する場合、変更を有効にするには Citrix Receiver をリセットする必要がありました。

バージョン 1808 以降、**Citrix Gateway URL/StoreFront Account List** ポリシーに加えられた変更は、Citrix Workspace アプリを再起動するとセッションに適用されます。リセットは必要ありません。

> 注:
>
> Citrix Workspace アプリのバージョン 1808 以降を新たにインストールした場合、Citrix Workspace アプリのリセットは必要ありません。バージョン 1808 以降にアップグレードする場合は、変更を有効にするために Citrix Workspace アプリをリセットする必要があります。

制限事項:

- Citrix Gateway URL は先頭に入力し、その後に StoreFront の URL を続ける必要があります。
- 複数の Citrix Gateway URL はサポートされていません。
- Citrix Gateway の URL を上記の方法で構成した場合、Citrix Gateway の後ろにある PNA サービスはサポートされません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ワークスペースコントロール再接続の管理

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アプリケーションを起動し直す必要がなくなります。Citrix Workspace アプリの場合、クライアントデバイスのワークスペースコントロールの管理はレジストリを変更して行います。これはまた、グループポリシーを使用するドメイン参加クライアントデバイスに対しても実行できます。

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

WSCReconnectModeUser を作成し、既存のレジストリキー **WSCReconnectMode** を Master Desktop Image または Citrix Virtual Apps サーバーで変更します。公開デスクトップでは Citrix Workspace アプリの動作を変更できます。

Citrix Workspace アプリの WSCReconnectMode キー設定は次のとおりです:

- 0 = いずれに既存のセッションにも再接続しない
- 1 = アプリケーションの起動時に再接続する
- 2 = アプリケーションの更新時に再接続する
- 3 = アプリケーションの起動または更新時に再接続する
- 4 = Citrix Workspace インターフェイスを開いたときに再接続する
- 8 = Windows ログオン時に再接続する
- 11 = 3 と 8 の組み合わせ

Citrix Workspace アプリのワークスペースコントロールの無効化　ワークスペースコントロールを無効にするには、次のキーを作成します:

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`（64 ビット）

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\\Dazzle`（32 ビット版）

名前：**WSCReconnectModeUser**

種類：REG_SZ

値のデータ：0

次のキーをデフォルト値の 3 から 0 に変更

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\\Dazzle`（64 ビット）

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\\Dazzle`（32 ビット）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名前：**WSCReconnectMode**

種類：REG_SZ

値のデータ：0

> 注：
>
> キーを作成しない代わりに、REG_SZ 値の WSCReconnectAll を false に設定することができます。

状態インジケータータイムアウトの変更

ユーザーがセッションを起動しているときに状態インジケーターが表示される時間を変更できます。タイムアウト期間を変更するには、REG_DWORD 値の SI INACTIVE MS を HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\で作成します。状態インジケーターをすぐに非表示したい場合は、REG_DWORD 値を 4 に設定します。

コマンドラインを使用したアプリケーションショートカットの場所のカスタマイズ

［スタート］メニュー統合およびデスクトップショートカットのみのモードにより、公開アプリケーションのショートカットを **Windows** の［スタート］メニューやデスクトップ上に配置できます。ユーザーが Citrix Workspace のユーザーインターフェイスからアプリケーションをサブスクライブする必要はありません。これらの機能により、ユーザーのグループにシームレスなデスクトップエクスペリエンスを提供して、ユーザーは頻繁に使用するアプリケーションに一貫した方法でアクセスできるようになります。

Citrix Workspace アプリ管理者として、コマンドラインインストールフラグ、GPO、アカウントサービス、またはレジストリ設定を使って、通常の「セルフサービス」Citrix Workspace アプリインターフェイスを無効にし、事前定義した［スタート］メニューと置き換えることができます。このフラグは **SelfServiceMode** と呼ばれ、デフォルトで true に設定されています。管理者が **SelfServiceMode** フラグを false に設定すると、ユーザーはセルフサービスの Citrix Workspace アプリユーザーインターフェイスにアクセスできなくなります。その代わり、［スタート］メニューやデスクトップのショートカットを使って、サブスクライブ済みのアプリにアクセスします。これをショートカットのみのモードと呼びます。

ユーザーおよび管理者は、いくつかのレジストリ設定を使用してアプリのショートカットをカスタマイズできます。

ショートカットの操作

- ユーザーはアプリを削除できません。**SelfServiceMode** フラグを false に設定（ショートカットのみのモード）すると、すべてのアプリが必須アプリになります。ユーザーがデスクトップからショートカットアイコンを削除しても、システムトレイの Citrix Workspace アプリアイコンで［更新］を選択するとこれらのアイコンが再表示されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- ユーザーはストアを 1 つだけ構成できます。アカウントおよび基本設定オプションは使用できません。このため、ユーザーが追加のストアを構成できません。管理者はユーザーに特別な権限を付与し、これによりユーザーはグループポリシーオブジェクトテンプレートを使用して、またはクライアントマシンでレジストリキー（HideEditStoresDialog）を手動で追加して 1 つまたは複数のアカウントを追加できます。管理者がユーザーにこの権限を付与すると、ユーザーのシステムトレイの Receiver アイコンに［基本設定］オプションが表示され、アカウントを追加および削除できるようになります。
- ユーザーは **Windows** のコントロールパネルを介してアプリを削除することはできません。
- カスタマイズ可能なレジストリ設定を介してデスクトップショートカットを追加できます。デスクトップショートカットはデフォルトでは追加できません。レジストリ設定を変更したら、Citrix Workspace アプリを再起動する必要があります。
- ショートカットは、［スタート］メニューにデフォルトのカテゴリパス UseCategoryAsStartMenuPath で作成されます。

> 注：
>
> Windows 8、Windows 8.1、Windows 10 では、［スタート］メニュー内には階層分けされたフォルダーを作成できません。アプリケーションは個々に、または Citrix Virtual Apps で定義されたカテゴリサブフォルダー内ではないルートフォルダーの下に表示されます。

- インストール時にフラグ [/DESKTOPDIR=”Dir_name”] を指定すると、すべてのショートカットを単一のフォルダー内に配置できます。デスクトップショートカットのため CategoryPath がサポートされます。
- 変更アプリの自動再インストールは、レジストリキー AutoReInstallModifiedApps を介して有効にできる機能です。AutoReInstallModifiedApps が有効な場合、管理者がサーバー上の公開アプリおよび公開デスクトップの属性を変更すると、その変更がすべてクライアントマシンに反映されます。AutoReInstallModifiedApps が無効な場合、アプリとデスクトップの属性は更新されず、クライアント上で削除されたショートカットも更新時に復元されません。デフォルトでは、この AutoReInstallModifiedApps は有効です。「アプリケーションショートカットをカスタマイズするためのレジストリキーの使用」を参照してください。

レジストリエディターを使用したアプリケーションショートカットの場所のカスタマイズ

> 注：
>
> - デフォルトでは、レジストリキーは文字列形式を使用します。
> - ストアを構成する前にレジストリキーに変更を加える必要があります。レジストリキーをカスタマイズする場合には管理者かユーザーかに関わらず、Citrix Workspace アプリをリセットしてからレジストリキーを構成し、その後でストアを再構成する必要があります。

32 ビットマシンのレジストリキー：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Registry key	Value	Key path
WSCSupported	True	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\ SR\Store\" + primaryStoreID +\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Citrix \Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\Dazzle
WSCReconnectAll	True	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID + \Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies \Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID +\Properties • HKLM\SOFTWARE\Policies\Citrix \Dazzle • HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	Registry is not created during installation	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID+\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies \Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE \Citrix\Dazzle

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

64 ビットマシンのレジストリキー:

Registry key	Value	Key path
WSCSupported	True	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Dazzle • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\D
WSCReconnectAll	True	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Citrix\D
WSCreconnectMode	3	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\SR \Store\"+ primaryStoreID +"\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node \Policies\Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node \Citrix\Dazzle
WSCReconnectModeUser	Registry is not created during installation.	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\SR \Store\"+ primaryStoreID+\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node \Citrix\Dazzle

ユーザーアカウント

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

- メールアドレスによるアカウント検出の構成
- プロビジョニングファイル
- アカウント情報をユーザーに手入力させる

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要
>
> インストール後に Citrix Workspace アプリを再起動することをお勧めします。これは、ユーザーがアカウントを追加し、Citrix Workspace アプリがインストール時に一時停止状態だった USB デバイスを検出できるようにするためです。

インストールに成功したことを示すダイアログボックスが表示され、［アカウントの追加］ダイアログボックスが開きます。初めて使用するユーザーは、［アカウントの追加］ダイアログボックスにメールまたはサーバーアドレスを入力してアカウントをセットアップする必要があります。

［アカウントの追加］ダイアログボックスを非表示にする

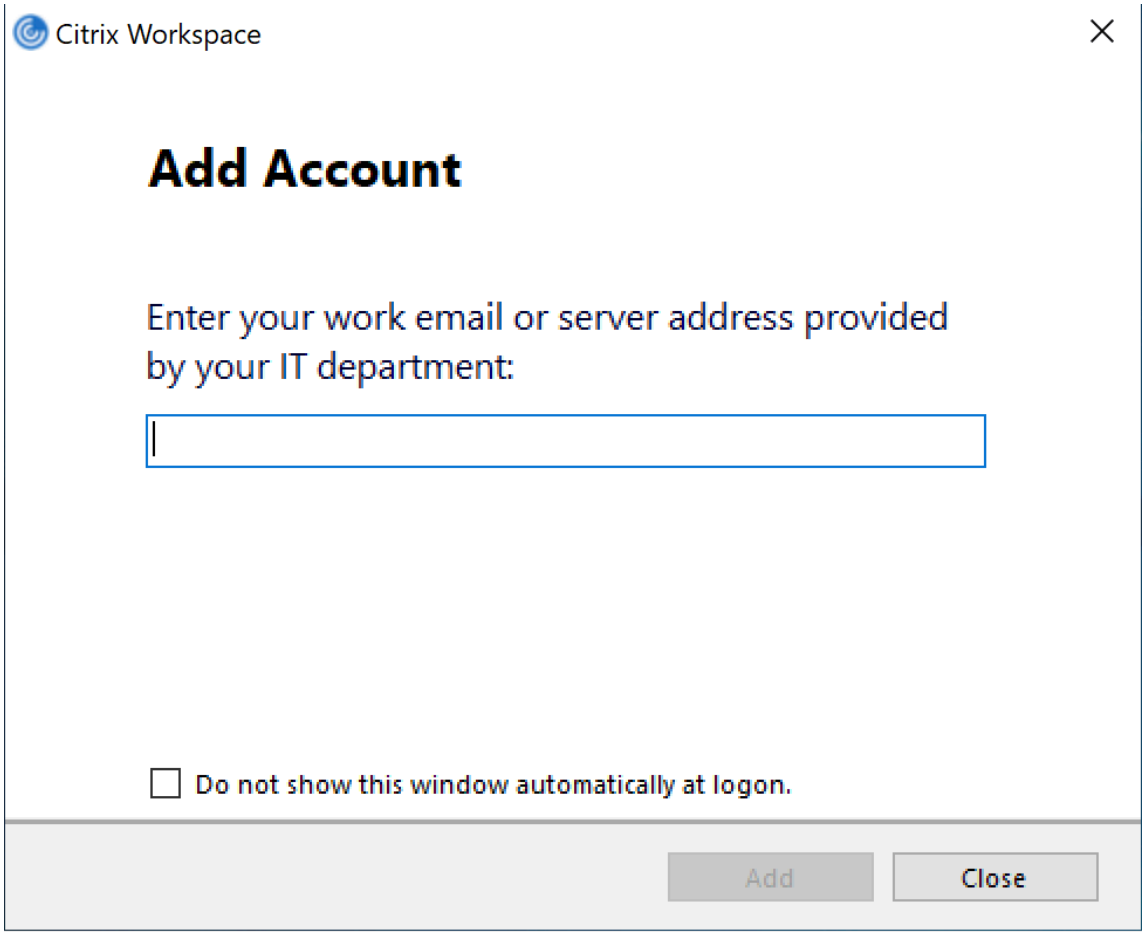
ストアが構成されていない場合、［アカウントの追加］ダイアログボックスが表示されます。［アカウントの追加］ダイアログボックスを使って、メールアドレスまたはサーバー URL を入力して Citrix Workspace アプリアカウントをセットアップすることができます。

Citrix Workspace アプリにより、入力したメールアドレスに関連付けられている Citrix Gateway、StoreFront サーバー、または App Controller 仮想アプライアンスが識別され、表示のためにログオンするようメッセージが表示されます。

［アカウントの追加］ダイアログボックスは次の方法で非表示にできます:

1. システムログオン時

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



次回以降のログオン時に ［アカウントの追加］ダイアログボックスがポップアップ表示されないようにするには、［ログオン時に自動的にこのウィンドウを表示しない］チェックボックスをオンにします。
これはユーザーごとの設定で、Windows 向け Citrix Workspace アプリのリセット時にリセットされます。

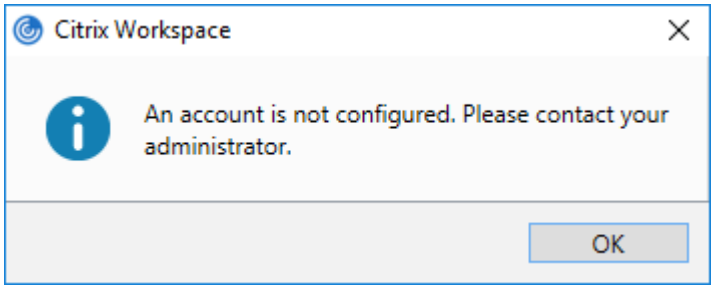
2. コマンドラインを使用したインストール

   管理者として、次のスイッチを指定して Windows 向け Citrix Workspace アプリをインストールします。

   ```
   CitrixWorkspaceApp.exe /ALLOWADDSTORE=N
   ```

   この設定はマシンごとであるため、動作の設定はすべてのユーザーに適用されます。

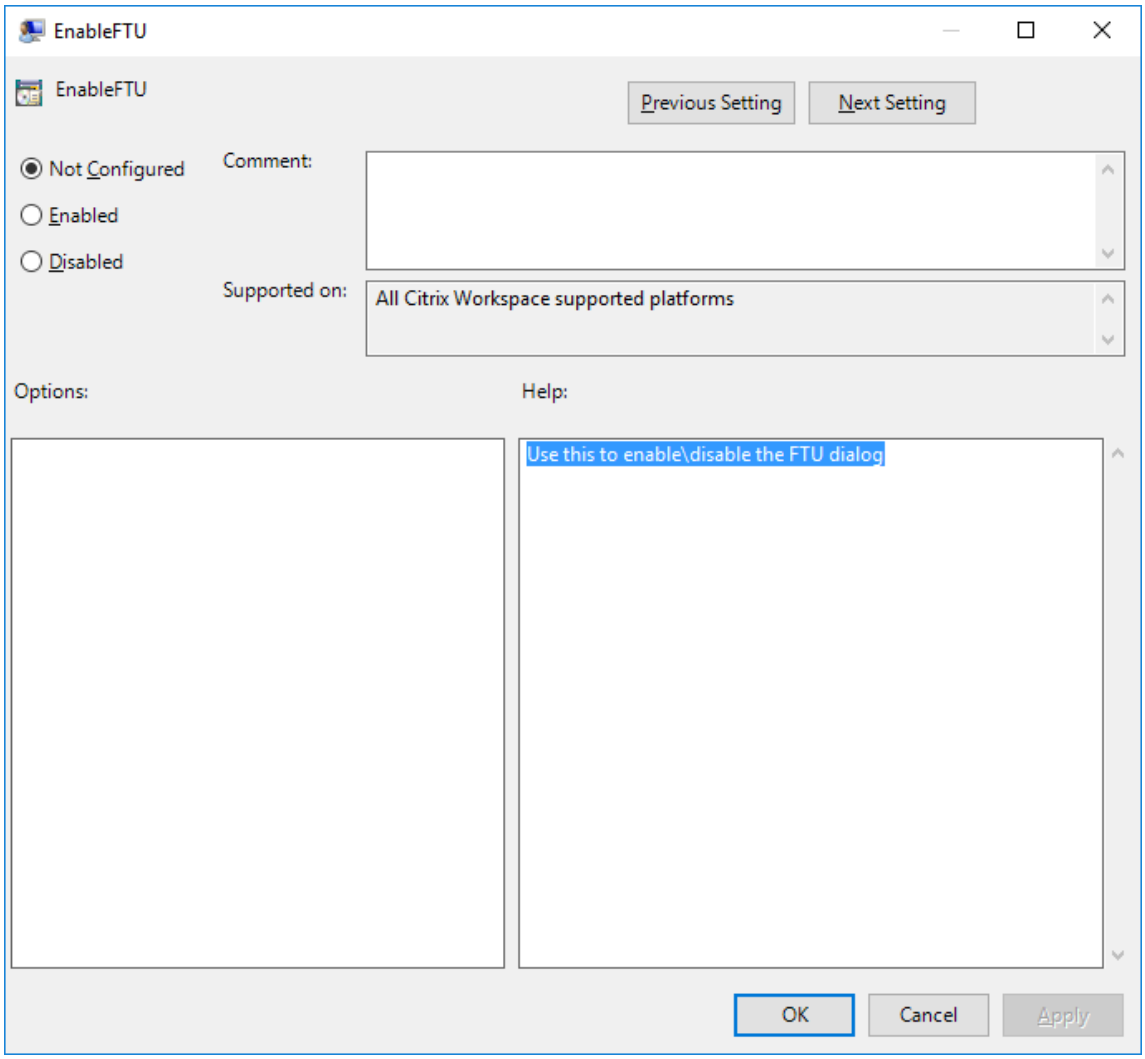
   ストアが構成されていない場合は、次のメッセージが表示されます。



［アカウントの追加］ダイアログボックスは次の方法で非表示にできます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **Citrix** 実行ファイルの名前を変更する:
  ファイルの名前を **CitrixWorkspaceApp.exe** から **CitrixWorkspaceAppWeb.exe** に変えて、［アカウントの追加］ダイアログボックスの動作を変更します。名前を変更することにより、［アカウントの追加］ダイアログボックスが［スタート］メニューに表示されなくなります。
- グループポリシーオブジェクト管理用テンプレート:
  Citrix Workspace アプリインストールウィザードで ［アカウントの追加］オプションが表示されないようにするには、以下のとおりにローカルグループポリシーオブジェクト管理用テンプレートで Self-Service ノードにある **EnableFTUpolicy** を無効にします。
  この設定はマシンごとであるため、動作の設定はすべてのユーザーに適用されます。



メールアドレスによるアカウント検出を構成する

管理者がメールアドレスによるアカウント検出機能を有効にした場合、ユーザーは Citrix Workspace アプリの初期設定時にサーバーの URL の代わりに自分のメールアドレスを入力できます。Citrix Workspace アプリで、DNS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

(Domain Name System) サービス (SRV) レコードによりメールアドレスに関連付けられている Citrix Gateway または StoreFront サーバーが検出され、仮想デスクトップやアプリケーションにアクセスするためのログオンを求めるメッセージが表示されます。

> 注:
>
> メールアドレスによるアカウント検出は、Web Interface 環境では使用できません。

メールアドレスによるアカウント検出の構成について詳しくは、「Global App Configuration Service」を参照してください。

ユーザーにプロビジョニングファイルを提供する

StoreFront により提供されるプロビジョニングファイルを使用して、ユーザーはストアに接続できます。

管理者は、StoreFront を使用して、接続の詳細情報を定義したプロビジョニングファイルを作成できます。作成したプロビジョニングファイルをユーザーに提供して、Citrix Workspace アプリを自動的に構成できるようにします。Citrix Workspace アプリのインストール後、ファイルを開いて Citrix Workspace アプリを構成するだけです。Web 向け Workspace サイトを構成すると、ユーザーはそれらのサイトから Citrix Workspace アプリのプロビジョニングファイルを取得することもできます。

詳しくは、StoreFront のドキュメントの「ユーザーに配布するストアプロビジョニングファイルをエクスポートするには」を参照してください。

アカウント情報をユーザーに手入力させる

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

- StoreFront ストアへの接続の場合は、そのサーバーの URL を提供します。例: `https://servername.company.com`。

  Web インターフェイスの展開の場合は、Citrix DaaS サイトの URL を指定します。

- Citrix Gateway を介する接続の場合は、ユーザーがすべての構成済みストアを表示する必要があるのか、または特定の Citrix Gateway に対するリモートアクセスが有効になった単一のストアだけにアクセスする必要があるのかを最初に判断します。

  - 構成済みストアをすべて表示させる場合は、ユーザーに Citrix Gateway の完全修飾ドメイン名を提供します。
  - 特定のストアへのアクセスに限定する場合は、ユーザーに Citrix Gateway の完全修飾ドメイン名とストア名を次の形式で提供します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

CitrixGatewayFQDN?MyStoreName:

たとえば、「SalesApps」という名前のストアで server1.com へのリモートアクセスが有効で、「HRApps」という名前のストアで server2.com へのリモートアクセスが有効な場合、ユーザーが SalesApps にアクセスするには <server1.com?SalesApps>、HRApps にアクセスするには <server2.com?HRApps> と入力する必要があります。この機能では、新規ユーザーは URL を入力してアカウントを作成する必要があり、電子メールベースの検出は使用できません。

ユーザーが新しいアカウントの詳細を入力すると、Citrix Workspace アプリにより接続が検証されます。検証に成功すると、Citrix Workspace アプリでそのアカウントにログオンするための画面が開きます。

アカウントを管理するには、Citrix Workspace アプリのホームページを開き、、［アカウント］の順にクリックします。

複数のストアアカウントの自動的共有

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

複数のストアアカウントがある場合は、セッションの確立時に Windows 向け Citrix Workspace アプリを構成してすべてのアカウントに自動的に接続できます。Citrix Workspace アプリを開くときにすべてのアカウントを自動的に表示するには、次の操作を実行します：

32 ビットシステムの場合、「**CurrentAccount**」というキーを作成します：

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

キーの名前：CurrentAccount

値：AllAccount

種類：REG_SZ

64 ビットシステムの場合、「**CurrentAccount**」というキーを作成します：

場所：HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle

キーの名前：CurrentAccount

値：AllAccount

種類：REG_SZ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

クライアントドライブマッピング

Windows 向け Citrix Workspace アプリではクライアント側デバイスのマッピング（割り当て）機能がサポートされており、ユーザーはセッション内でこれらのデバイスを使用できます。次のことを実行できます:

- ローカルのディスクドライブ、プリンター、および COM ポートにセッションから透過的にアクセスする。
- セッションとローカルの Windows クリップボードの間で、データをコピーして貼り付ける。
- セッション内で、サーバー上のサウンドを再生する。

Citrix Workspace アプリでサーバーにログオンすると、使用できるクライアントドライブ、COM ポート、LPT ポートなどがサーバーに通知されます。デフォルトでは、クライアントドライブがサーバーのドライブ文字にマップされ、クライアントプリンターの印刷キューがサーバー上に作成されます。このため、これらのデバイスがサーバーに直接接続されているかのように見えます。マップされたクライアント側デバイスは、そのセッションを実行中のユーザーだけが使用できます。ユーザーがログオフするとマッピングが削除され、そのユーザーが次にログオンしたときに再び作成されます。

ログオン時に特定のデバイスが自動的にマップされないように設定するには、ポリシーのリダイレクト設定を使用します。詳しくは、Citrix Virtual Apps and Desktops のドキュメントを参照してください。

デバイスマッピングを無効にする

Windows のサーバーマネージャーを使用して、ユーザーデバイスマッピング（ドライブ、プリンター、ポートなどのオプション）を構成できます。指定できるオプションについて詳しくは、リモートデスクトップサービスのドキュメントを参照してください。

クライアントフォルダーのリダイレクト

クライアントフォルダーのリダイレクトは、クライアント側のファイルがホスト側のセッションのへアクセスする方法を変更します。サーバー上でクライアント側ドライブのマッピングのみを有効にすると、クライアントの側の全ボリュームが UNC（Universal Naming Convention）リンクとしてセッションに自動的にマップされます。管理者がサーバー上でクライアントフォルダーのリダイレクトを有効にして、ユーザーがそれをユーザーデバイス上で構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

セッション内では、ユーザーデバイス上のすべてのファイルシステムの代わりにユーザー指定のフォルダーのみが UNC リンクとして表示されます。レジストリで UNC リンクを無効にすると、クライアントフォルダーはマップされたドライブとしてセッション内で表示されます。構成方法など、クライアントフォルダーのリダイレクトについて詳しくは Citrix Virtual Apps and Desktops のドキュメントを参照してください。

クライアントドライブをホスト側のドライブ文字にマップする

クライアント側ドライブのマッピング機能により、ホスト側のドライブ文字をユーザーデバイス上のドライブとしてリダイレクトできます。たとえば、Citrix ユーザーセッション内で表示される H ドライブにアクセスしたときに、

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Windows 向け Citrix Workspace アプリを実行するユーザーデバイスの C ドライブにリダイレクトされるように設定できます。

クライアントドライブマッピングは、Citrix の標準デバイスリダイレクト機能に透過的に組み込まれています。この方法でマップされたドライブ文字は、通常のネットワークドライブのマッピングの場合と同様に、ファイルマネージャー、エクスプローラー、およびアプリケーションで使用することができます。

仮想デスクトップやアプリケーションをホストするサーバーにインストールするときに、クライアントドライブが自動的にマップされるサーバーのドライブ文字のセットを設定できます。デフォルトでは、インストール時に、個々のハードディスクおよび CD ドライブに 1 文字ずつ、V からのアルファベットで未使用のドライブ文字がマップされます（クライアントのフロッピーディスクドライブには、元のドライブ文字がそのままマップされます）。この場合、セッションでのドライブマッピングは、次のようになります：

クライアントドライブ文字	セッション内でアクセスするときのドライブ文字
A	A
B	B
C	V
D	U

サーバーの既存のドライブ文字をアルファベットの後ろの方の文字に変更しておくと、サーバー側のドライブ文字がクライアント側のものと競合しなくなるため、ユーザーはローカルドライブと同じドライブ文字をセッション内で使用できます。たとえば、サーバーの C ドライブを M に変更し、D を N に変更しておくと、クライアントデバイスの既存の C ドライブや D ドライブにそのままアクセスできます。この場合、セッションでのドライブマッピングは、次のようになります：

クライアントドライブ文字	セッション内でアクセスするときのドライブ文字
A	A
B	B
C	C
D	D

サーバーの C ドライブを置き換えるために使用するドライブ文字は、インストール時に定義できます。そのほかの固定ドライブおよび CD/DVD ドライブのドライブ文字は、連続するドライブ文字に置き換えられます。たとえば、C ドライブは M、D は N、E は O に置き換えられます。これらのドライブ文字が、既存のネットワークドライブのマッピングと競合しないようにしてください。ネットワークドライブにマップされたドライブ文字がサーバーのドライブ文字と競合する場合、ネットワークドライブのマッピングが無効になります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

クライアント側デバイスの自動マッピングを無効にしない限り、ユーザーデバイスでサーバーに再接続すると、マッピングが再確立されます。デフォルトでは、クライアントドライブマッピングが有効になっています。設定を変更するには、リモートデスクトップ（ターミナルサービス）構成ツールを使用します。また、ポリシーを使用して、クライアントデバイスマッピングを詳細に制御できます。ポリシーについて詳しくは、Citrix Virtual Apps and Desktops ドキュメントを参照してください。

HDX Plug-n-Play USB デバイスリダイレクト

HDX Plug-n-Play の USB デバイスリダイレクトにより、カメラ、スキャナー、メディアプレーヤー、および POS 端末など、ユーザー側のさまざまなデバイスをサーバーに動的にリダイレクトできます。管理者やユーザーは、すべてまたは一部のデバイスのリダイレクトを制限できます。サーバー上でポリシーを編集するかユーザーデバイス上でグループポリシーを適用して、リダイレクト設定を構成します。詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「USB とクライアント側ドライブの考慮事項」を参照してください。

> 重要
>
> サーバーポリシーでこの USB デバイスリダイレクトを禁止すると、ユーザー側でこの機能を有効にすることはできなくなります。

ユーザーは、デバイスのリダイレクトを常に許可または拒否するか、またはデバイスの接続時に毎回確認のメッセージを表示するように設定できます。この設定は、Citrix Workspace アプリで行います。この設定は新しく接続するデバイスにのみ適用され、接続済みのデバイスには適用されません。

クライアントの **COM** ポートをサーバーの **COM** ポートにマップするには：

クライアント側 COM ポートのマッピングを有効にすると、セッション内でローカルマシンの COM ポート上のデバイスにアクセスできるようになります。マップされたクライアントの COM ポートは、ほかのネットワークドライブのマッピングと同様の方法で使用できます。

コマンドプロンプトからクライアント COM ポートをマップできます。また、Windows の管理ツールのリモートデスクトップ（ターミナルサービス）構成ツールまたはポリシーを使用して、クライアント COM ポートのマッピングを制御することもできます。ポリシーについて詳しくは、Citrix Virtual Apps and Desktops ドキュメントを参照してください。

> 重要
>
> COM ポートマッピングは TAPI 対応ではありません。

1. Citrix Virtual Apps and Desktops の展開では、クライアント COM ポートリダイレクトポリシー設定を有効にします。
2. Citrix Workspace アプリにログオンします。
3. コマンドプロンプトで以下を入力します：

```
net use comx: \\\\client\\comz:
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ここで、<x> にはサーバー上の COM ポート番号（ポート 1〜9）を指定し、<z> にはクライアントデバイス上の COM ポート番号を指定します。

4. 操作を確認するには、

   ```
   net use
   ```

   と入力し Enter キーを押します。マップされているドライブ、LPT ポート、およびマップされている COM ポートの一覧が表示されます。

この COM ポートを仮想デスクトップやアプリケーションのセッションで使用するには、割り当てられている COM ポートにデバイスをインストールします。たとえば、クライアントの COM1 をサーバーの COM5 にマップするには、セッション内で、COM5 に COM ポートデバイスをインストールします。この方法でマップした COM ポートは、ユーザーデバイスの COM ポートと同じように使用できます。

DNS 名前解決

Citrix XML Service を使用してサーバーファームに接続するときに IP アドレスの代わりにサーバーの DNS（ドメインネームサービス）名を要求するように Windows 向け Citrix Workspace アプリを構成できます。

> 重要:
>
> この機能を使用するために DNS 環境を設定していない場合は、Citrix ではサーバーファームで DNS アドレス解決を有効にしないことをお勧めします。

Web Interface を使用してリモートアプリケーションに接続する Citrix Workspace アプリも、接続に Citrix XML Service を使用します。この場合、Citrix Workspace アプリの代わりに Web Interface サーバーが DNS 名を解決します。

デフォルトで、DNS 名前解決はサーバーで無効、Citrix Workspace アプリで有効になっています。サーバーで DNS 名前解決が無効になっている場合、Citrix Workspace アプリが DNS 名を要求すると IP アドレスが返されます。Citrix Workspace アプリで DNS アドレス解決を無効にする必要はありません。

特定のユーザーデバイスの **DNS** 名前解決を無効にするには:

DNS 名前解決が使用されるサーバー展開環境で特定のユーザーデバイスに問題が発生した場合、そのデバイスの DNS 名前解決を無効にすることができます。

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

1. レジストリキー`HKEY\\_LOCAL\\_MACHINE\Software\\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing`に文字列値 **xmlAddressResolutionType** を追加します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 値を **IPv4-Port** に設定します。
3. ユーザーデバイスの各ユーザーでこれを繰り返します。

構成

May 23, 2024

App Protection

> 免責事項
>
> App Protection ポリシーはオペレーティングシステムの必要な機能へのアクセスをフィルタリングすることで有効になります（画面のキャプチャまたはキーボードの操作が必要な特定の API 呼び出し）。つまり、この App Protection ポリシーは、カスタムの目的別に構築されたハッカーツールに対しても保護を提供できます。ただし、オペレーティングシステムの進化によって、画面のキャプチャやキーのログ記録には新しい方法が出てきます。引き続きこうした方法に対応していきますが、特定の構成や展開では完全な保護を保証することはできません。

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

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

要件:

- Citrix Virtual Apps and Desktops バージョン 1912 以降。
- StoreFront バージョン 1912。
- Citrix Workspace アプリバージョン 1912 以降。

前提条件:

- Controller で App Protection 機能を有効にする必要があります。詳しくは、「App Protection」のドキュメントを参照してください。

以下のいずれかの方法で、Citrix Workspace アプリに App Protection コンポーネントを追加できます:

- Citrix Workspace アプリインストール中にコマンドラインインターフェイスまたはグラフィカルユーザーインターフェイスを使用する。または

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- アプリの起動中（オンデマンドインストール）。

> 注：
>
> - この機能は、Windows 10、Windows 8.1、および Windows 7 などの Microsoft Windows デスクトップオペレーティングシステムでのみサポートされます。
> - この機能は、リモートデスクトッププロトコル（RDP）ではサポートされません。

オンプレミスの **HDX** セッション保護：

2 つのポリシーがセッションでのキーロガー対策および画面キャプチャ対策機能を提供します。これらのポリシーは、PowerShell を使用して構成する必要があります。グラフィカルユーザーインターフェイスをこの目的に利用することはできません。

> 注：
>
> Citrix DaaS では、App Protection 機能はサポートされません。

Citrix Virtual Apps and Desktops での App Protection の構成については、App Protectionのドキュメントを参照してください。

App Protection - Citrix Workspace アプリの構成

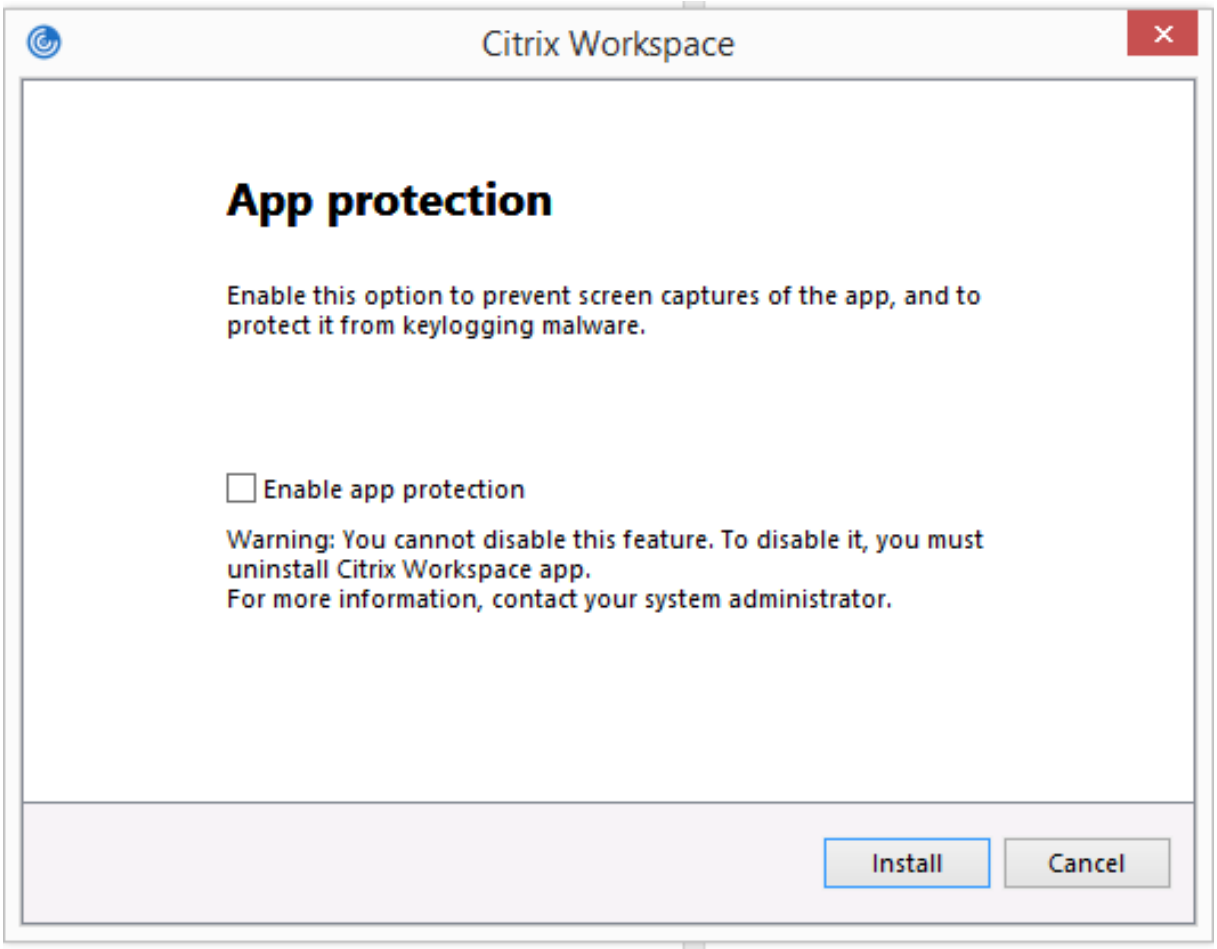
> 注：
>
> - 管理者から指示があった場合にのみ、Citrix Workspace アプリに App Protection コンポーネントを含めます。
> - App Protection コンポーネントによって、デバイスの画面キャプチャ機能が影響を受ける場合があります。

Citrix Workspace アプリのインストール中に、次のいずれかの方法で App Protection を追加できます：

- グラフィカルユーザーインターフェイス
- コマンドラインインターフェイス

グラフィカルユーザーインターフェイス　Citrix Workspace アプリのインストール中に、次のダイアログボックスを使用して App Protection コンポーネントを追加します。［**App Protection** を有効にする］を選択し、［インストール］をクリックしてインストールを続行します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> 注:
>
> インストール中にアプリの保護を有効にしないと、保護されたアプリを起動するときにプロンプトが表示されます。その場合、プロンプトに従って App Protection コンポーネントをインストールします。

コマンドラインインターフェイス　Citrix Workspace アプリのインストール中にコマンドラインスイッチ/`includeappprotection`を使用して、App Protection コンポーネントを追加します。

次の表に、展開に応じて保護される画面に関する情報を示します:

App Protection の展開	保護される画面	保護されない画面
Citrix Workspace アプリに含まれる	Self-service Plug-in と Auth Manager/［ユーザー認証情報］ダイアログボックス	コネクションセンター、デバイス、Citrix Workspace アプリのエラーメッセージ、クライアントの自動再接続、アカウントの追加

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

App Protection の展開	保護される画面	保護されない画面
Controller で構成	ICA セッション画面（アプリとデスクトップの両方）	コネクションセンター、デバイス、Citrix Workspace アプリのエラーメッセージ、クライアントの自動再接続、アカウントの追加

想定される動作:

想定される動作は、保護されたリソースが含まれる StoreFront ストアにアクセスする方法によって異なります。

> 注:
>
> - 保護されたセッションの起動には、ネイティブの Citrix Workspace アプリのみを使用することをお勧めします。

- **Web** 向け **Workspace** での動作:

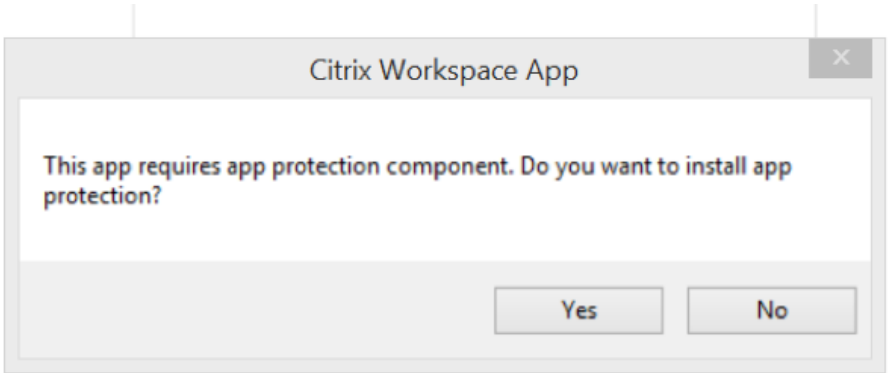
  App Protection コンポーネントは、Web 向け Workspace の構成ではサポートされません。App Protection ポリシーで保護されているアプリケーションは列挙されません。割り当てられるリソースについて詳しくは、システム管理者にお問い合わせください。

- **App Protection** をサポートしない **Citrix Workspace** アプリバージョンでの動作:

  Citrix Workspace アプリのバージョン 1911 以前では、App Protection ポリシーで保護されているアプリケーションは StoreFront で列挙されません。

- **Controller** に **App Protection** 機能が構成されているアプリの動作:

  Controller に App Protection 機能が構成されている場合に、保護されているアプリケーションを起動しようとすると、App Protection はオンデマンドでインストールされます。次のダイアログボックスが開きます:



［はい］をクリックすると、App Protection コンポーネントがインストールされ、ユーザーは保護されたアプリを起動できるようになります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- リモートデスクトッププロトコル（**RDP**）で保護されたセッションの動作
  - リモートデスクトッププロトコル（RDP）セッションを起動すると、アクティブな保護されたセッションが切断されます。
  - リモートデスクトッププロトコル（RDP）セッションでは、保護されたセッションを起動できません。

App Protection のエラーログ:

App Protection コンポーネントのログはデバッグ出力に登録されます。これらのログを収集するには、次の手順を実行します:

1. Microsoft の Web サイトからDebugViewアプリをダウンロードしてインストールします。
2. コマンドプロンプトを起動して、次のコマンドを実行します:

   ```
   Dbgview.exe /t /k /v /l C:\logs.txt
   ```

   上記の例から、log.txt ファイル内のログを表示することができます。

このコマンドでは以下が表示されます:

- /t —DebugView アプリが、システムトレイで最小化されて開始されます。
- /k —カーネルキャプチャを有効にします。
- /v —詳細カーネルキャプチャを有効にします。
- /l —出力を特定のファイルに記録します。

App Protection コンポーネントのアンインストール:

App Protection コンポーネントをアンインストールするには、システムから Citrix Workspace アプリをアンインストールする必要があります。変更を保存するには、システムを再起動します。

> 注:
>
> App Protection は、バージョン 1912 以降のアップグレードでのみサポートされます。

既知の問題または制限事項:

- この機能は、Windows Server 2012 R2 や Windows Server 2016 などの Microsoft サーバーのオペレーティングシステムではサポートされません。
- ローカルデバイスのスクリーンショットを取得するには、Citrix Workspace アプリ関連のウィンドウを最小化する必要があります。そうしないと、ローカルデバイスのスクリーンショットを取得できません。
- ダブルホップシナリオでは、この機能はサポートされません。
- 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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Microsoft Teams でのエンドポイントエンコーダーのパフォーマンス見積もりツール

HdxTeams.exe プロセス（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）を開始すると、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ります。使用できる値は、240p、360p、720p、1080p です。

HdxTeams.exe が初期化されると、パフォーマンスの見積プロセス(`webrtcapi.EndpointPerformance` とも呼ばれます）が実行されます。マクロブロックコードは、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します。ピア間、またはピアと会議サーバー間のコーデックネゴシエーション中に、可能な限り高い解像度が使用されます。

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	3
medium	720p	2
slow	360p	1
very slow	240p	0

VP9 または H264 コーデックを無効にする構成フラグがあります。
H264 は CPU 上で使用する CPU は比較的少ない量ですが、より多くの帯域幅を消費します。逆に、VP9 はより多くの CPU リソースを消費しますが、消費する帯域幅は少なくなります。

Citrix Workspace アプリのレジストリパス:

レジストリパス HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream に移動し、次のキーを作成します: \

名前	種類	値	説明
DisableVP9	DWORD	1; 0	1 - VP9 コーデックを無効にする。0 - 有効にする
DisableH264	DWORD	1;0	1 - H.264 コーデックを無効にする。0 - 有効にする
OverridePerformance	DWORD	0;1;2;3	目的のパフォーマンスを適用する。値は 0〜3 の範囲にする必要があります。0 は非常に遅く、3 は非常に高速であることを示します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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。

アダプティブトランスポート

アダプティブトランスポートは、Citrix Virtual Apps and Desktops および Citrix DaaS のデータ転送メカニズムです。高速で拡張性が高く、アプリケーションの対話機能が向上し、厳しい長距離の WAN とインターネット接続でのインタラクティブ性を高めます。アダプティブトランスポートでは、サーバーの高スケーラビリティと帯域幅の使用効率が維持されます。アダプティブトランスポートを使用すると、ICA 仮想チャネルはネットワーク状況の変化に自動的に対応します。Enlightened Data Transport（EDT）と呼ばれる Citrix プロトコルと TCP との間で、基になるプロトコルをインテリジェントに切り替えて、最適なパフォーマンスを実現します。これにより、Thinwire ディスプレイリモート、ファイル転送（クライアントドライブマッピング）、印刷、マルチメディアリダイレクトなど、すべての ICA 仮想チャネルのデータスループットが向上します。同じ設定を LAN と WAN の両方の条件に適用できます。

以前のリリースでは、**HDXoverUDP** を ［優先する］に設定すると、可能な場合、EDT 上のデータ転送が使用され、TCP にフォールバックします。

セッション画面の保持を有効にすると、セッション画面の保持による再接続、自動クライアント再接続中に EDT と TCP が同時に試行されます。この機能強化により、EDT が優先される状態で必要なベースの UDP トランスポートが利用できず、TCP を使用する必要がある場合、接続時間が短縮されます。

デフォルトでは、TCP にフォールバックした後、アダプティブトランスポートは 5 分ごとに EDT を検索し続けます。

要件:

- Citrix Virtual Apps and Desktops 7.12 以降。
- StoreFront 3.8。
- IPv4 VDA のみ。IPv6 および IPv6 と IPv4 の混在構成はサポートされません。
- VDA の UDP ポート 1494 および 2598 での受信トラフィックを許可するファイアウォール規則を追加します。

> 注:
>
> TCP ポート 1494 および 2598 は必須で、VDA をインストールするときに自動的に開かれます。ただし、UDP ポート 1494 および 2598 は自動的に開かれません。これらを有効に設定します。

Citrix Workspace アプリでは、デフォルトでアダプティブトランスポートが許可されます。また、同じくデフォルトで、クライアントがアダプティブトランスポートの使用を試みるのは、Delivery Controller で VDA が ［優先する］に構成され、その VDA に設定が適用されている場合だけです。

HDX アダプティブトランスポートポリシー設定を使用してアダプティブトランスポートを有効化できます。可能な場合、アダプティブトランスポートを使用し、TCP にフォールバックするには、新しいポリシーを ［優先する］に設定します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

グループポリシーオブジェクト（GPO）管理テンプレートを使用して、クライアントでアダプティブトランスポートを無効にします。

Citrix Workspace アプリグループポリシーオブジェクト（**GPO**）管理用テンプレートを使用してアダプティブトランスポートを構成するには

以下に、環境をカスタマイズするオプションの構成手順を示します。たとえば、セキュリティ上の理由で特定のクライアントに対して機能を無効にすることを選択する場合があります。

> 注:
>
> デフォルトでは、アダプティブトランスポートは無効（[オフ]）になっており、常に TCP が使用されます。

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］> ［**Citrix Workspace**］> ［ネットワークルーティング］の順に移動します。
3. ［**Citrix Workspace** のトランスポートプロトコル］ポリシーを ［有効］に設定します。
4. 必要な場合は、**Citrix Workspace** の通信プロトコルを選択します。
   - ［オフ］ - データ転送に TCP を使用することを示します。
   - ［優先］ - クライアントが最初に UDP を使用してサーバーに接続しようとすることを示します。UDP が使用できない場合、接続はフォールバックして TCP に切り替わります。
   - ［オン］ - Windows 向け Citrix Workspace アプリが、UDP のみを使用してサーバーに接続することを示します。このオプションでは、TCP にフォールバックしません。
5. ［適用］、［**OK**］の順にクリックします。
6. コマンドラインから`gpupdate /force`コマンドを実行します。

また、アダプティブトランスポート構成を使用するには、Citrix Workspace アプリテンプレートファイルをポリシー定義フォルダーに追加します。テンプレートファイルをローカル GPO に追加する方法については、「グループポリシーオブジェクトテンプレート」セクションを参照してください。

ポリシー設定の有効化を確認するには:

`HKEY\\_LOCAL\\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT`に移動して **HDXOverUDP** キーがあるかを確認します。

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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

高度な設定シート

システムトレイの Citrix Workspace アプリアイコンの右クリックメニューにある ［高度な設定］シートの使用およびシートの内容をカスタマイズできます。これによって、ユーザーはシステムで管理者が指定した設定のみを適用できるようになります。具体的には、次の操作が可能になります。

- ［高度な設定］シートをすべて非表示にする
- シートから以下の特定の設定を非表示にする
  - データ収集
  - コネクションセンター
  - 構成チェッカー
  - キーボードと言語バー
  - 高 DPI
  - サポート情報
  - ショートカットと再接続
  - Citrix Casting

右クリックメニューの［高度な設定］オプションを非表示にする

Citrix Workspace アプリグループポリシーオブジェクト（GPO）管理用テンプレートを使用して、［高度な設定］シートを非表示にすることができます:

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］> ［**Citrix Workspace**］> ［**Self Service**］> ［高度な設定］オプションの順に移動します。
3. ［高度な設定を無効にする］ポリシーを選択します。
4. システムトレイの Citrix Workspace アプリアイコンを右クリックし ［有効］を選択して、［高度な設定］オプションを非表示にします。

> 注:
>
> デフォルトでは、［未構成］オプションが選択されています。

グループポリシーオブジェクト（**GPO**）管理用テンプレートを使用して、［高度な設定］シートから特定の設定を非表示にする

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］> ［**Citrix Workspace**］> ［**Self Service**］> ［高度な設定］オプションの順に移動します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 非表示にする設定のポリシーを選択します。

以下の表は、選択できるオプションとそれぞれの効果です。

オプション	操作
未構成	設定を表示します
有効	設定を非表示にします
無効	設定を表示します

［高度な設定］シートでは、以下の設定を非表示にできます。

- 構成チェッカー
- コネクションセンター
- 高 DPI
- データ収集
- 保存したパスワードの削除
- キーボードと言語バー
- ショートカットと再接続
- サポート情報
- Citrix Casting

レジストリエディターを使用して［高度な設定］シートから［**Workspace** をリセット］オプションを非表示にする

レジストリエディターを使用して［高度な設定］シートから ［**Workspace** をリセット］オプションを非表示にすることができます。

1. レジストリエディターを起動します。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`にアクセスします。
3. 文字列値キー **EnableFactoryReset** を作成し、次のいずれかのオプションに設定します。
    - True - ［高度な設定］シートで［Workspace をリセット］オプションが表示されます
    - False - ［高度な設定］シートで［Workspace をリセット］オプションが非表示になります

［高度な設定］シートから［**Citrix Workspace** 更新プログラム］オプションを非表示にする

> 注:
>
> ［Citrix Workspace 更新プログラム］オプションのポリシーパスは、［高度な設定］シートにある他のオプションのポリシーパスとは異なります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. [コンピューターの構成] ノードで、[管理用テンプレート] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [**Citrix Workspace** の更新] の順に移動します。
3. [**Citrix Workspace** の更新] ポリシーを選択します。
4. [高度な設定] シートで [Workspace の更新] 設定を非表示にするには、[無効] を選択します。

アプリケーションの配信

Citrix Virtual Apps and Desktops および Citrix DaaS を使用してアプリケーションを配信する場合は、次のオプションを検討してユーザーエクスペリエンスを強化してください:

- Web アクセスモード - いずれの構成も行わない場合、Citrix Workspace アプリではアプリケーションおよびデスクトップへのブラウザーベースのアクセスが提供されます。Web 向け Workspace または Web Interface サイトで、使用するアプリケーションを選択して実行できます。このモードでは、ユーザーのデスクトップにショートカットは置かれません。
- セルフサービスモード - StoreFront アカウントを Citrix Workspace アプリに追加するか、StoreFront サイトをポイントするように Citrix Workspace アプリを構成して、「セルフサービスモード」を構成できます。このモードでは、Citrix Workspace アプリのユーザーインターフェイスを介してアプリケーションをサブスクライブできます。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。

> 注:
>
> Citrix Workspace アプリのデフォルトでは、[スタート] メニューに表示するアプリケーションを選択できます。

- アプリケーションショートカットのみのモード - Citrix Workspace アプリを構成してアプリケーションおよびデスクトップショートカットを [スタート] メニュー内に直接またはデスクトップ上に自動的に配置できます。新しい「ショートカットのみ」のモードにより、使い慣れた Windows のナビゲーションスキーマ内で公開アプリケーションを見つけることができます。

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

セルフサービスモードの構成

StoreFront アカウントを 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 Citrix Workspace アプリを構成します。セルフサービスによって、ユーザーが Citrix Workspace のユーザーインターフェイスからアプリケーションをサブスクライブできます。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。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> Citrix Workspace アプリのデフォルトでは、ユーザーは［スタート］メニューに表示するアプリケーションを選択できます。

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。

デリバリーグループアプリケーションの説明に、適切なキーワードを追加します:

- 個々のアプリを必須にして Citrix Workspace アプリから削除できないようにするには、アプリケーションの説明に「KEYWORDS: Mandatory」という文字列を追加します。ユーザーが必須アプリをサブスクリプション解除するための削除オプションはありません。
- 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、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、そのアプリケーションを手動でサブスクライブしなくても自動的にプロビジョニングされます。
- 説明に「KEYWORDS: Featured」という文字列を追加すると、そのアプリケーションが Citrix Workspace の［おすすめ］一覧に表示され、ユーザーがそのアプリケーションを見つけやすくなります。

グループポリシーオブジェクトテンプレートを使用したアプリショートカットの場所のカスタマイズ

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］> [**Citrix** コンポーネント] > [**Citrix Workspace**] > ［**Self Service**］の順に移動します。
3. [**SelfServiceMode** を管理します］ポリシーを選択します。
    a) Self Service ユーザーインターフェイスを表示するには、［有効］を選択します。
    b) アプリを手動でサブスクライブするには、［無効］を選択します。このオプションは、Self Service ユーザーインターフェイスを非表示にします。
4. ［アプリのショートカットを管理します］ポリシーを選択します。
5. 必要に応じてオプションを選択します。
6. ［適用］、［**OK**］の順にクリックします。
7. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

アプリショートカットをカスタマイズするための **StoreFront** アカウント設定の使用

［スタート］メニュー内およびデスクトップ上のショートカットを StoreFront サイトからセットアップできます。`C:\inetpub\wwwroot\Citrix\Roaming`にある web.config ファイルの **<annotatedServices>** セクションに次の設定を追加できます:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- デスクトップ上にショートカットを置くには、PutShortcutsOnDesktop を使用します。設定:”true”または”false”（デフォルトは false）。
- ［スタート］メニュー内にショートカットを置くには、PutShortcutsInStartMenu を使用します。設定:”true”または”false”（デフォルトは true）。
- ［スタート］メニュー内のカテゴリパスを使用するには、UseCategoryAsStartMenuPath を使用します。設定:”true”または”false”（デフォルトは true）。

> 注:
>
> Windows 8、Windows 8.1、Windows 10 では、［スタート］メニュー内には階層分けされたフォルダーを作成できません。アプリケーションは個々に、または Citrix Virtual Apps and Desktops で定義されたカテゴリサブフォルダー内ではないルートフォルダーの下に表示されます。

- ［スタート］メニュー内のすべてのショートカットを単一のフォルダー内に置くには、StartMenuDir を使用します。設定：文字列値、ショートカットが書き込まれるフォルダーの名前になります。
- 管理者により変更されたアプリが再インストールされるようにする（変更アプリの自動再インストール機能）には、AutoReinstallModifiedApps を使用します。設定:”true”または”false”（デフォルトは true）。
- デスクトップ上のすべてのショートカットを単一のフォルダー内に置くには、DesktopDir を使用します。設定：文字列値、ショートカットが書き込まれるフォルダーの名前になります。
- クライアントの’add/remove programs’でエントリを作成しないようにするには、DontCreateAddRemoveEntry を使用します。設定:”true”または”false”（デフォルトは false）。
- 以前にはストアから実行できたけど今はもう実行できないアプリケーションのショートカットや Citrix Workspace アイコンを削除するには、SilentlyUninstallRemovedResources を使用します。設定:” true”または”false”（デフォルトは false）。

web.config ファイルで、アカウントの **XML** セクションに変更を追加します。次の開始タグを検索し、このセクションに移動します。

```
<account id=... name="Store"
```

このセクションは、</account> タグで終わります。

このタグ内にある、次のような最初のプロパティセクションに移動します。

```
<properties> <clear> <properties>
```

このセクションの <clear /> タグの後ろにプロパティを追加できます。1 行ごとに名前と値を記述します。例:

```
<property name="PutShortcutsOnDesktop"value="True"/>
```

> 注:
>
> <clear /> タグの前に追加されたプロパティの要素により、それが無効になることがあります。プロパティ名と値の追加が任意の場合は、<clear /> タグを削除します。

プロパティの追加例:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
<properties <property name="PutShortcutsOnDesktop"value="True"<
property name="DesktopDir"value="Citrix Applications">
```

> 重要
>
> 複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上で Citrix StoreFront 管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。詳しくは、StoreFrontのドキュメントを参照してください。

Citrix Virtual Apps and Desktops 7.x のアプリごとの設定を使ったアプリショートカットの場所のカスタマイズ

アプリケーションおよびデスクトップショートカットを［スタート］メニュー内に直接またはデスクトップ上に自動的に配置するよう、Citrix Workspace アプリを構成できます。この機能は、以前にリリースされたバージョンの Windows 向け Workspace の機能と似ていますが、バージョン 4.2.100 では Citrix Virtual Apps を使ってアプリケーション設定ごとにアプリケーションショートカットの配置を制御できる機能が導入されています。この機能は、終始一貫した場所に表示する必要がある一部のアプリケーションが存在する環境で有用です。

ショートカットの場所を指定して、すべてのユーザーが同じ場所でそれにアクセスできるようにするには、Citrix Virtual Apps のアプリケーションごとの設定を使用します。

セルフサービスモードか、または［スタート］メニューモードかには関係なく、アプリごとの設定によりアプリケーションを配置する場所を決定する場合は。	Windows 向け Citrix Workspace アプリで **PutShortcutsInStartMenu=false** を構成して、アプリケーションごとの設定を有効にします。注：この設定は、Web Interface サイトにのみ適用されます。

> 注:
>
> **PutShortcutsInStartMenu=false** 設定は、XenApp 6.5 と XenDesktop 7.x の両方に適用されます。

XenApp 6.5 でのアプリケーションごとの設定の構成

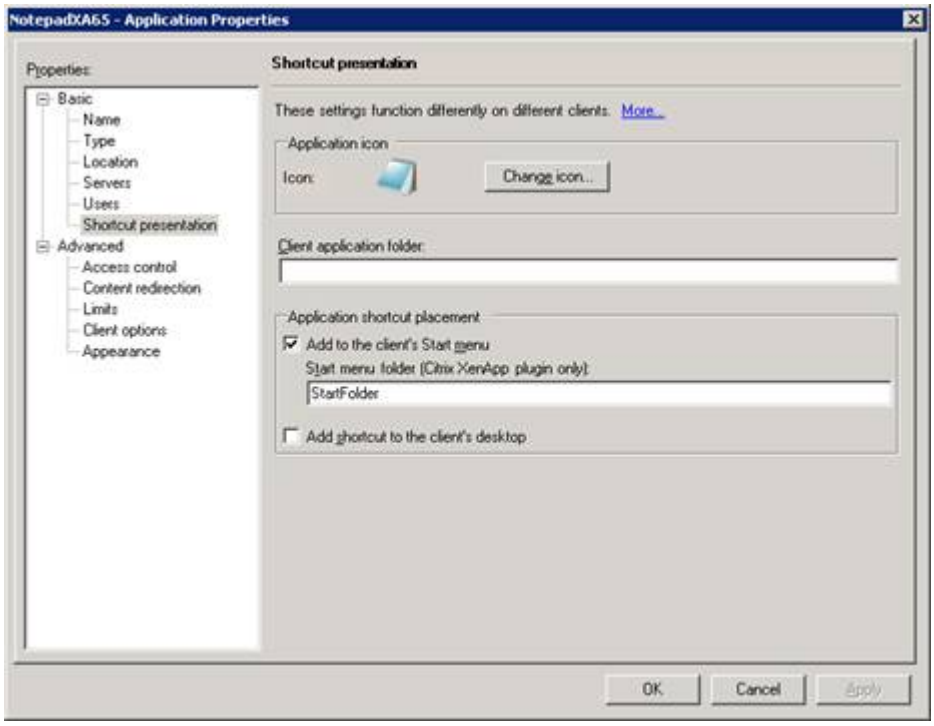
XenApp 6.5 でアプリケーションごとの公開ショートカットを構成するには

1. XenApp の ［アプリケーションのプロパティ］画面で、［基本設定］プロパティを展開します。
2. ［ショートカットの表示］オプションを選択します。
3. ［ショートカットの表示］画面の［アプリケーションのショートカットの追加先］で、［クライアントのスタートメニューに追加する］チェックボックスをオンにします。チェックボックスをオンにした後、ショートカッ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

トを置くフォルダーの名前を入力します。フォルダー名を指定しない場合は、XenApp により［スタート］メニューにフォルダーに入っていないショートカットが置かれます。

4. ［ショートカットをクライアントのデスクトップに追加するかどうかを示します］を選択して、クライアントマシンのデスクトップにショートカットを含めます。
5. ［適用］をクリックします。
6. ［**OK**］をクリックします。



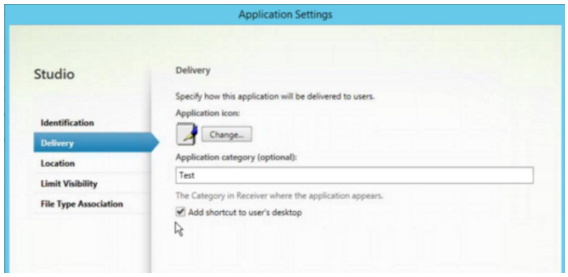
XenApp 7.6 のアプリごとの設定を使った、アプリショートカットの場所のカスタマイズ

XenApp 7.6 でアプリごとの公開ショートカットを構成するには

1. Citrix Studio で、［アプリケーション設定］画面を開きます。
2. ［アプリケーション設定］画面で ［配信］を選択します。この画面を使って、アプリケーションがユーザーにどのように配信されるかを指定できます。
3. アプリケーションの適切なアイコンを選択します。［変更］をクリックして、必要なアイコンの場所を参照します。
4. ［アプリケーションカテゴリ］に、アプリケーションが表示される Citrix Workspace アプリのカテゴリを指定します。たとえば、ショートカットを Microsoft Office アプリケーションに追加している場合は、「Microsoft Office」と入力します。
5. ［ユーザーのデスクトップにショートカットを追加する］チェックボックスをオンにします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. [OK] をクリックします。



列挙遅延またはアプリケーションスタブデジタル署名の削減

ユーザーのログオン時にアプリケーションの列挙に遅延が生じる場合、またはアプリケーションスタブにデジタル署名が必要な場合、ネットワーク共有から.EXE スタブをコピーする機能が Citrix Workspace アプリにより提供されます。

この機能を実行するには、次の複数の手順を実行します:

1. クライアントマシンにアプリケーションスタブを作成します。
2. アプリケーションスタブをネットワーク共有からアクセスできる場所にコピーします。
3. 必要な場合は、ホワイトリストを作成します（または、エンタープライズ証明書でスタブに署名します）。
4. レジストリキーを追加し、ネットワーク共有からスタブをコピーして Windows 向け Workspace がスタブを作成できるようにします。

RemoveappsOnLogoff および **RemoveAppsonExit** が有効で、ユーザーのログオン時にアプリ列挙に遅延が生じる場合、次の解決策により遅延を削減させます。

1. Regedit を使って、HKEY_CURRENT_USER\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d “true” を追加します。
2. Regedit を使って、HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d “true” を追加します。HKEY_CURRENT_USER は、HKEY_LOCAL_MACHINE よりも優先されます。

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

ネットワーク共有に格納されている事前作成のスタブ実行可能ファイルをマシンが使用できるようにします:

1. クライアントマシン上で、すべてのアプリケーションに対するスタブ実行可能ファイルを作成します。これを実行するには、Citrix Workspace アプリを使ってすべてのアプリケーションをマシンに追加します。Citrix Workspace アプリは実行可能ファイルを生成します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. %APPDATA%\Citrix\SelfService からスタブ実行可能ファイルを取得します。必要なのは.exe ファイルだけです。
3. 実行可能ファイルをネットワーク共有にコピーします。
4. ロックダウンされる各クライアントマシンに対して次のレジストリキーを設定します。

    a) Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d “\\ShareOne\WorkspaceStubs”
    b) Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v
    c) CopyStubsFromCommonStubDirectory /t REG_SZ /d “true” 。また、必要な場合は HKEY_CURRENT_USER でこれらの設定を構成することもできます。HKEY_CURRENT_USER は、HKEY_LOCAL_MACHINE よりも優先されます。
    d) Citrix Workspace アプリを終了して再起動し、設定をテストします。

ユースケースの例:

このトピックでは、アプリショートカットのユースケースについて紹介します。

［スタート］メニューに何を置くか、ユーザーが選べるようにする（**Self-servic**）

数十（または数百の）アプリがある場合は、ユーザーがお気に入りのアプリケーションを選択して、［スタート］メニューに追加できるようにするのが最も便利です:

［スタート］メニューに置くアプリケーションをユーザーが選べるようにするには、	Citrix Workspace アプリをセルフサービスモードに構成します。このモードでは、「自動プロビジョニング」設定および「必須」アプリキーワード設定も構成できます。
ユーザーが［スタート］メニューに置くアプリケーションを選べるようにして、また特定のアプリケーションショートカットをデスクトップに置くには、	Citrix Workspace アプリをオプション設定なしで構成して、デスクトップに置くアプリについてアプリごとの設定を使用します。必要に応じて、「自動プロビジョニング」および「必須」アプリを使用します。

［スタート］メニュー内にアプリショートカットなし

コンピューターを家族で共有して使用していて、アプリショートカットを一切置きたくないとします。このような場合、最も簡単なのはブラウザーアクセスです。いずれの構成も行わずに Citrix Workspace アプリをインストールし、Web 向け Workspace および Web interface をブラウズします。また、ショートカットをどこにも配置しないでセルフサービスアクセス用に Citrix Workspace アプリを構成することもできます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Workspace アプリが［スタート］メニューに自動的にアプリショートカットを配置しないようにするには。	Citrix Workspace アプリで PutShortcutsInStartMenu=False と構成します。アプリケーションごとの設定を使ってショートカットを置かない限り、セルフサービスモードであっても Citrix Workspace アプリにより［スタート］メニュー内にアプリケーションは配置されません。

［スタート］メニュー内、またはデスクトップ上にすべてにアプリショートカットを置く

ユーザーが所有するアプリケーションが少ない場合は、そのすべてを［スタート］メニュー内やデスクトップ上に、あるいはデスクトップ上のフォルダー内に置くことができます。

Citrix Workspace アプリによって［スタート］メニューにすべてのアプリケーションショートカットを自動的に配置するには	Citrix Workspace アプリで SelfServiceMode =False と構成します。使用可能なすべてのアプリが［スタート］メニュー内に表示されます。
すべてのアプリケーションショートカットをデスクトップ上に置く場合は、	Citrix Workspace アプリで PutShortcutsOnDesktop = true と構成します。使用可能なすべてのアプリがデスクトップに表示されます。
すべてのショートカットをデスクトップ上のフォルダー内に置く場合は、	Citrix Workspace アプリで DesktopDir=Name アプリケーションショートカットを置くデスクトップフォルダーの名前と構成します。

XenApp 6.5 または **7.x** でのアプリごとの設定

ショートカットの場所を指定して、すべてのユーザーが同じ場所でそれにアクセスできるようにするには、XenApp のアプリごとの設定を使用します：

セルフサービスモードか、または［スタート］メニューモードかには関係なく、アプリケーションごとの設定によりアプリケーションを配置する場所を決定する場合は、	Citrix Workspace アプリで PutShortcutsInStartMenu=false と構成して、アプリごとの設定を有効にします。

カテゴリフォルダーまたは特定のフォルダーのアプリ

特定のフォルダー内にアプリケーションを表示する場合は、次のオプションを使用します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Workspace アプリにより［スタート］メニューに置かれたアプリケーションショートカットを関連カテゴリ（フォルダー）内に表示するには	Citrix Workspace アプリで UseCategoryAsStartMenuPath=True と構成します。
Citrix Workspace アプリにより［スタート］メニューに置かれたアプリケーションを特定のフォルダー内に配置するには	Citrix Workspace アプリで StartMenuDir=［スタート］メニューフォルダーの名前と構成します。

ログオフまたは終了時にアプリを削除

エンドポイントをほかのユーザーと共有していて、自分のアプリケーションがそのユーザーには表示されないようにしたい場合は、ログオフまた終了時にアプリケーションが削除されるようにすることができます。

ログオフ時に Citrix Workspace アプリによりすべてのアプリケーションが削除されるようにするには	Citrix Workspace アプリで RemoveAppsOnLogoff=True と構成します。
終了時に Citrix Workspace アプリによりアプリが削除されるようにするには	Citrix Workspace アプリで RemoveAppsOnExit=True と構成します。

ローカルアプリアクセスのアプリケーションの構成

ローカルアプリアクセスのアプリケーションを構成する場合は次のようにします。

- 説明に「KEYWORDS:prefer=”<pattern>”」という文字列を追加すると、Citrix Workspace アプリでアクセスされるアプリケーションの代わりにローカルのアプリケーションが使用されるようになります。この機能は、「ローカルアプリアクセス」と呼ばれます。

  Citrix Workspace アプリは、ユーザーのコンピューターにアプリケーションをインストールする前に pattern で指定されたパターンを検索し、そのアプリケーションがローカルにインストールされているかどうかをチェックします。アプリケーションがローカルにインストールされている場合、Citrix Workspace アプリはそのアプリケーションをサブスクライブして、ショートカットは作成しません。ユーザーが Citrix Workspace アプリからそのアプリケーションを起動すると、ローカルにインストールされたアプリケーション（ここでは「優先アプリケーション」と呼びます）が起動します。

  ユーザーが Citrix Workspace アプリを使用せずに優先アプリケーションをアンインストールすると、Citrix Workspace アプリの次回更新時にそのアプリケーションのサブスクリプションが解除されます。ユーザーが Citrix Workspace アプリを使用して優先アプリケーションをアンインストールすると、Citrix Workspace アプリはそのアプリケーションのサブスクリプションを解除しますが、アンインストールはしません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> Citrix Workspace アプリでアプリケーションをサブスクライブすると、キーワード prefer が適用されます。アプリケーションをサブスクライブした後でこの文字列を追加しても、そのアプリケーションには適用されません。

同じアプリケーションに対して複数回 prefer キーワードを指定できます。この場合、指定したパターンの 1 つが一致すると、そのアプリケーションに設定が適用されます。以下のパターンを任意に組み合わせて指定できます:

- 説明に「KEYWORDS:prefer=”<pattern>”」という文字列を追加すると、Citrix Workspace アプリでアクセスされるアプリケーションの代わりにローカルのアプリケーションが使用されるようになります。この機能は、「ローカルアプリアクセス」と呼ばれます。

  Citrix Workspace アプリは、ユーザーのコンピューターにアプリケーションをインストールする前に pattern で指定されたパターンを検索し、そのアプリケーションがローカルにインストールされているかどうかをチェックします。アプリケーションがローカルにインストールされている場合、Citrix Workspace アプリはそのアプリケーションをサブスクライブして、ショートカットは作成しません。ユーザーが Citrix Workspace アプリからそのアプリケーションを起動すると、ローカルにインストールされたアプリケーション（ここでは「優先アプリケーション」と呼びます）が起動します。

  ユーザーが Citrix Workspace アプリを使用せずに優先アプリケーションをアンインストールすると、Citrix Workspace アプリの次回更新時にそのアプリケーションのサブスクリプションが解除されます。ユーザーが Citrix Workspace アプリを使用して優先アプリケーションをアンインストールすると、Citrix Workspace アプリはそのアプリケーションのサブスクリプションを解除しますが、アンインストールはしません。

1912 以降、Citrix Workspace アプリで、レジストリエディターを使用して自動更新動作を構成できるようになりました。

以前のリリースでは、Citrix Workspace アプリを再起動すると、キャッシュデータが利用可能な場合も自動更新が発生していました。

> 注:
>
> このオプションは、X1 ストア以外のアカウントでは構成できません。

レジストリエディターを使用して自動更新を構成するには、次の手順を実行します:

1. レジストリエディターを起動し、HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle パスに移動します。
2. 次の文字列値キーを作成します:

レジストリキー	値
InitialRefreshMinMs	10000（10 秒）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

レジストリキー	値
InitialRefreshMaxMs	15000（15 秒）
SuppressRefreshMs	1000（1 秒）

3. エディターを保存して閉じます。

> 注:
>
> Citrix Workspace アプリでアプリケーションをサブスクライブすると、キーワード prefer が適用されます。アプリケーションをサブスクライブした後でこの文字列を追加しても、そのアプリケーションには適用されません。

同じアプリケーションに対して複数回 prefer キーワードを指定できます。この場合、指定したパターンの 1 つが一致すると、そのアプリケーションに設定が適用されます。以下のパターンを任意に組み合わせて指定できます:

- prefer=”<ApplicationName>”

  ショートカットファイルに指定されているアプリケーション名にマッチします。単語または語句を指定できますが、語句の場合は引用句を使用する必要があります。単語やファイルパスの一部がマッチしても無視され、大文字/小文字も区別されません。アプリケーション名によるマッチは、管理者が手作業で設定する場合に便利です。

KEYWORDS:prefer=	Programs 配下のショートカット	マッチする?
Word	\Microsoft Office\Microsoft Word 2010	はい
Microsoft Word	\Microsoft Office\Microsoft Word 2010	はい
Console	McAfee\VirusScan Console	はい
Virus	McAfee\VirusScan Console	いいえ
Console	McAfee\VirusScan Console	はい

- prefer=”\\Folder1\Folder2\…\ApplicationName”

  ［スタート］メニューのショートカットファイルの絶対パスおよびアプリケーション名にマッチします。Programs フォルダーは、［スタート］メニューディレクトリのサブフォルダーであるため、フォルダーのアプリケーションを対象にするには絶対パスに Programs フォルダーを含む必要があります。パスにスペースが含まれている場合は、引用符を使用する必要があります。また、大文字と小文字は区別されます。絶対パスによるマッチは、Citrix Virtual Apps and Desktops でプログラム的に優先アプリケーションを設定する場合に便利です。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

KEYWORDS:prefer=	Programs 配下のショートカット	マッチする?
\Programs\Microsoft Office\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	はい
\Microsoft Office	\Programs\Microsoft Office\Microsoft Word 2010	いいえ
\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	いいえ
\Programs\Microsoft Word 2010	\Programs\Microsoft Word 2010	はい

- prefer=”\Folder1\Folder2\…\ApplicationName”

  ［スタート］メニューのショートカットファイルの相対パスにマッチします。相対パスにはアプリケーション名を含める必要があり、そのショートカットの親フォルダー名を含めることもできます。ショートカットのファイルパスの末尾が、指定したパターンに一致すると、そのアプリケーションに設定が適用されます。パスにスペースが含まれている場合は、引用符を使用する必要があります。また、大文字と小文字は区別されます。相対パスによるマッチは、プログラム的に優先アプリケーションを設定する場合に便利です。

KEYWORDS:prefer=	Programs 配下のショートカット	マッチする?
\Microsoft Office\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	はい
\Microsoft Office	\Microsoft Office\Microsoft Word 2010	いいえ
\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	はい
\Microsoft Word	\Microsoft Word 2010	いいえ

ほかのキーワードについては、StoreFront のドキュメントの「ユーザーエクスペリエンスの最適化」セクションを参照してください。

アプリケーションの起動時間

セッションの事前起動機能を使用すると、通常時および高トラフィック負荷時のアプリケーションの起動時間が短縮され、ユーザーエクスペリエンスが向上します。事前起動機能により、ユーザーが Citrix Workspace アプリにログオンするとき、またはログオン済みの場合は予定された時間に事前起動セッションを作成できます。

この事前起動セッションにより、最初のアプリケーションの起動時間が短縮されます。ユーザーが Windows 向け Citrix Workspace アプリで新しいアカウント接続を追加した後、次回のセッションまで事前起動セッションは適用

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

されません。このセッションでは、デフォルトのアプリケーション ctxprelaunch.exe が実行されます。ただし、このアプリケーションはユーザーには表示されません。

セッションの事前起動機能は、StoreFront 展開でサポートされます。Web Interface 環境では、ログオン用の画面が表示されるのを防ぐため、Web Interface の［パスワードを保存］オプションを有効にする必要があります。セッションの事前起動機能は、Citrix Virtual Apps and Desktops 環境ではサポートされません。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「デリバリーグループのセッションの事前起動およびセッション残留」を参照してください。

セッションの事前起動機能はデフォルトでは無効になっています。この機能を有効にするには、Workspace のコマンドラインで`ENABLEPRELAUNCH=true`パラメーターを指定するか、レジストリキー`EnablePreLaunch`に true を設定します。デフォルト値（null）は、事前起動が無効であることを示します。

> 注:
>
> ドメインパススルー（SSON）認証をサポートするようにクライアントマシンが構成されている場合、事前起動機能が自動的に有効になります。事前起動なしでドメインパススルー（SSON）を使用する場合は、**EnablePreLaunch** レジストリキーの値を
> false に設定します。

レジストリの場所は以下のとおりです。

- HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Dazzle

事前起動には 2 つの種類があります。

- 即時事前起動-トラフィック量にかかわらず、ユーザーの資格情報が認証されるとすぐに事前起動が開始されます。この設定は、通常のトラフィック負荷時に使用します。ユーザーは、Citrix Workspace アプリを再起動することで事前起動セッションを起動できます。
- 予定事前起動-予定した時間に事前起動が開始されます。予定事前起動は、ユーザーデバイスが実行中で認証済みの場合にのみ開始されます。これら 2 つの条件が満たされない場合は、予定された事前起動時間になってもセッションが起動しません。ネットワークとサーバーの負荷を分散するため、セッションは予定された時刻を含む一定期間内に起動します。たとえば、事前起動を午後 1 時 45 分に設定すると、午後 1 時 15 分から午後 1 時 45 分の間にセッションが起動されます。この設定は、高トラフィック負荷時に使用します。

Citrix Virtual Apps サーバーでの事前起動の構成には、事前起動アプリケーションの作成、変更、または削除と、事前起動アプリケーションを制御するユーザーポリシー設定の更新が含まれます。

receiver.admx ファイルで事前起動機能をカスタマイズすることはできません。ただし、Windows 向け Citrix Workspace アプリのインストール時またはインストール後にレジストリ値を変更することで、事前起動構成を変更することができます。

- HKEY_LOCAL_MACHINE 値は、Workspace のインストール時に追加されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- HKEY_CURRENT_USER 値では、同一マシン上の特定ユーザーに異なる値を設定できます。ユーザーは、管理者権限がなくても HKEY_CURRENT_USER 値を変更できます。管理者は、この機能を設定するためのスクリプトをユーザーに提供できます。

HKEY_LOCAL_MACHINE レジストリ値:

Windows オペレーティングシステム(64 ビット)の場合:HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

Windows オペレーティングシステム（32 ビット）の場合：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch

値の名前：**UserOverride**

値:

0 - HKEY_CURRENT_USER の値が存在しても、HKEY_LOCAL_MACHINE の値を使用します。

1 - 存在する場合は HKEY_CURRENT_USER の値を使用します。そうでない場合は、HKEY_LOCAL_MACHINE の値を使用します。

値の名前：**State**

値:

0 - 事前起動を無効にします。

1 - 即時事前起動を有効にします（ユーザーの資格情報が認証されると事前起動が開始されます）。

2 - 予定事前起動を有効にします（Schedule 値に指定した時刻に事前起動が開始されます）。

値の名前：**Schedule**

値:

予定事前起動を開始する、24 時間形式の時刻と曜日です。入力形式は次のとおりです:

HH:MM|M:T:W:TH:F:S:SU - ここで、HHとMMは時間と分、M:T:W:TH:F:S:SUは曜日です。月曜日、水曜日、および金曜日の午後 1 時 45 分に予定事前起動を有効にするには、Schedule=13:45 と設定します。	1:0:1:0:1:0:0。セッションが起動するのは午後 1 時 15 分から午後 1 時 45 分の間です。

HKEY_CURRENT_USER レジストリ値:

HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

値については、HKEY_LOCAL_MACHINE と同じ State および Schedule 値を使用します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

コンテンツの双方向リダイレクト

双方向のコンテンツリダイレクトポリシーによって、クライアントからホスト（およびホストからクライアント）への URL リダイレクトを有効にするか無効にできます。サーバーポリシーは Citrix Studio で設定し、クライアントポリシーは、Citrix Workspace アプリのグループポリシーオブジェクト管理用テンプレートで設定します。

URL リダイレクトに関しては、Citrix ではホストからクライアントへのリダイレクトおよびクライアント用のローカルアプリケーションアクセスが利用可能ですが、ドメインに参加している Windows クライアントに関しては、双方向のコンテンツリダイレクトを使用することをお勧めします。

次のいずれかの方法を使用して、コンテンツの双方向リダイレクトを有効にできます：

1. グループポリシーオブジェクト（GPO）管理用テンプレート
2. レジストリエディター

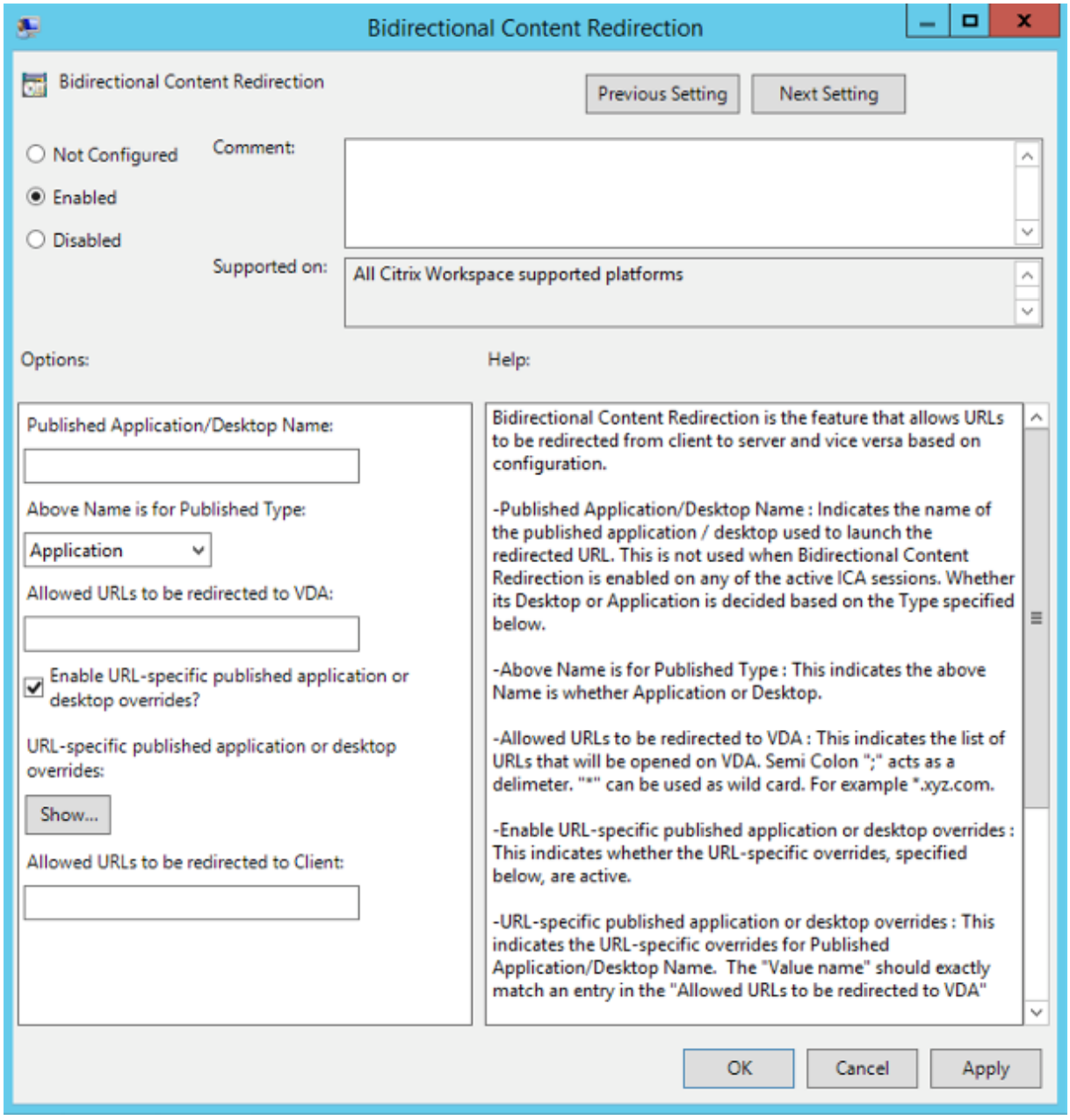
> 注：
>
> - ローカルアプリアクセスが有効であるセッション上では、コンテンツの双方向リダイレクトは機能しません。
> - コンテンツの双方向リダイレクトは、サーバーとクライアントの両方で有効である必要があります。サーバーとクライアントのいずれかで無効になると、機能が無効になります。
> - URL が複数ある場合、URL を 1 つずつ指定することもできますが、セミコロンで区切った URL の一覧で指定しても構いません。ワイルドカード文字としてアスタリスク（*）を使用できます。

GPO 管理用テンプレートを使用してコンテンツの双方向リダイレクトを有効化するには：

Windows 向け Citrix Workspace アプリを初めてインストールした場合のみ、グループポリシーオブジェクト管理用テンプレート構成を使用します。

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. ［ユーザー構成］ノードで、［管理用テンプレート］>［従来の管理用テンプレート（**ADM**）］>［**Citrix** コンポーネント］>［**Citrix Workspace**］>［ユーザーエクスペリエンス］の順に移動します。
3. ［コンテンツの双方向リダイレクト］ポリシーを選択します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



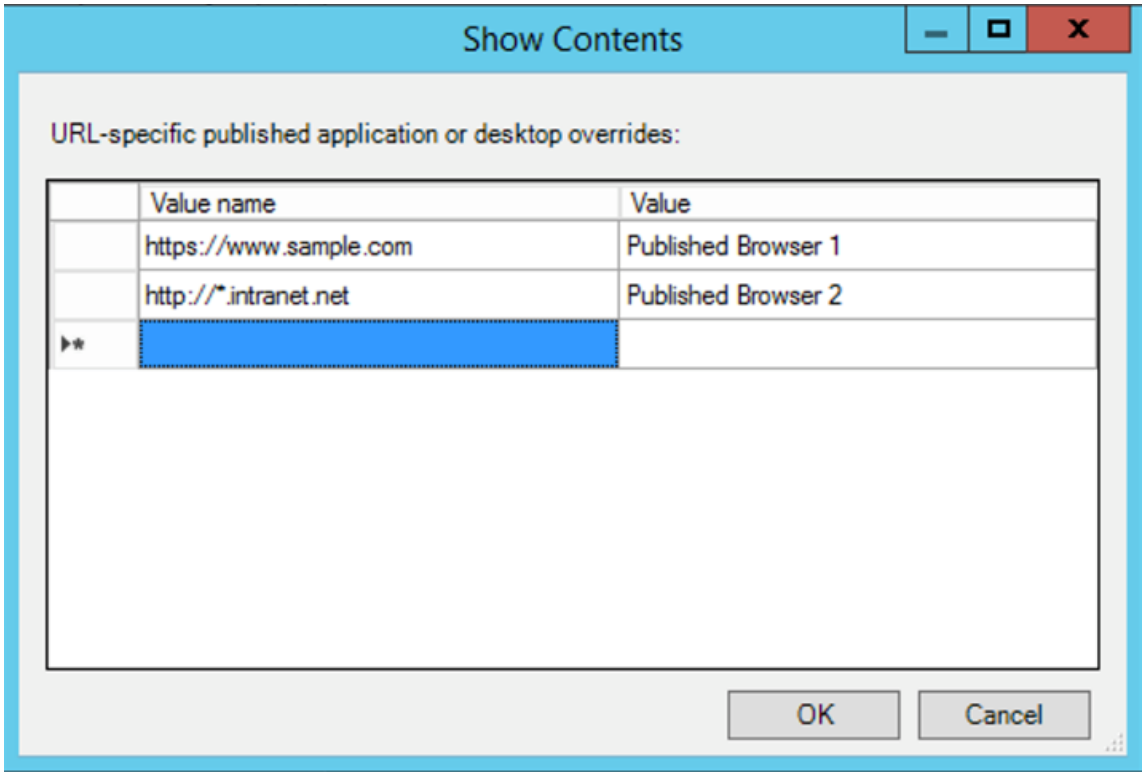
1. ［公開アプリケーション名/デスクトップ名］フィールドに、リダイレクトされた URL の起動に使用するリソースの名前を入力します。

   > 注:
   >
   > URL が複数ある場合、URL を 1 つずつ指定するか、セミコロンで区切った URL の一覧で指定します。ワイルドカード文字としてアスタリスク（*）を使用できます。

2. ［上記の名前の種類］で、必要に応じてリソースの［アプリケーション］または［デスクトップ］を選択します。
3. ［**VDA** へのリダイレクトを許可する **URL**］フィールドに、リダイレクトする必要がある URL を入力します。一覧はセミコロンで区切ります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. [**URL** 固有の公開アプリケーションまたはデスクトップの上書きを有効にしますか**?**] オプションを選択して URL を上書きします。
5. [表示] をクリックして、[**VDA** へのリダイレクトを許可する **URL**] フィールドのいずれかと一致する必要がある値の名前の一覧を表示します。値は公開アプリケーション名と一致する必要があります。



6. [クライアントへのリダイレクトを許可する **URL**:] フィールドに、サーバーからクライアントにリダイレクトする必要がある URL を入力します。一覧はセミコロンで区切ります。

> 注:
>
> URL が複数ある場合、URL を 1 つずつ指定するか、セミコロンで区切った URL の一覧で指定します。ワイルドカード文字としてアスタリスク（*）を使用できます。

7. [適用]、[**OK**] の順にクリックします。
8. コマンドラインから`gpupdate /force`コマンドを実行します。

レジストリを使用してコンテンツの双方向リダイレクトを有効化するには:

コンテンツの双方向リダイレクトを有効化するには、Citrix Workspace アプリインストールフォルダー（`C:\Program Files (x86)\Citrix\ICA Client`）から、`redirector.exe /RegIE`コマンドを実行します。

> 重要:
>
> - リダイレクト規則がループした構成になっていないことを確認してください。VDA 規則が、たとえば 1

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

つの URL、`https://www.my\\_company.com`がクライアントにリダイレクトされるように構成され、同じ URL が VDA にリダイレクトされるように構成されている場合、ループ構成になります。
- 明示的な URL リダイレクトのみがサポートされます。つまり、Web ブラウザーのアドレスバーに表示される URL や、ブラウザー内ナビゲーションによる URL だけが正しくリダイレクトされます。
- 同じ表示名を持つ 2 つのアプリケーションが複数の StoreFront アカウントを使用するように構成されている場合、プライマリ StoreFront アカウントの表示名を使用して、アプリケーションまたはデスクトップのセッションが起動されます。
- 新しいブラウザーウィンドウが開くのは、URL がクライアントにリダイレクトされた場合だけです。URL が VDA にリダイレクトされたときにブラウザーが既に開いていた場合、リダイレクトされた URL は新しいタブで開かれます。
- ドキュメント、メール、PDF などの、ファイルに埋め込まれたリンクがサポートされます。
- 同じマシンで、サーバーファイルタイプの関連付けとホストコンテンツのリダイレクトポリシーのいずれか 1 つだけが［有効］に設定されていることを確認します。URL リダイレクトが正しく機能するように、Citrix ではサーバーファイルタイプの関連付け機能またはホストコンテンツ（URL）リダイレクト機能を無効にすることをお勧めします。

制限事項:

セッションの起動に関する問題のため、リダイレクトが失敗してもフォールバックメカニズムは存在しません。

Bloomberg キーボード

Citrix Workspace アプリは、仮想アプリと仮想デスクトップのセッションで Bloomberg キーボードの使用をサポートします。必要なコンポーネントはプラグインとともにインストールされます。Bloomberg キーボード機能は、Windows 向け Citrix Workspace アプリのインストール時またはレジストリエディターで有効にできます。

複数のセッションで Bloomberg キーボードを使用しないでください。このキーボードはシングルセッション環境でのみ動作します。

Bloomberg キーボードの構成:

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

1. レジストリで次のキーを検索します:

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

2. 次のいずれかを行います:

   - この機能を有効にするには、種類が DWORD で名前が **EnableBloombergHID** の値のデータを 1 に設定します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- この機能を無効にするには、値のデータを 0 に設定します。

Bloomberg キーボードの構成について詳しくは、Knowledge Center でCTX122615を参照してください。

非アクティブな **Desktop Viewer** ウィンドウの減光を無効にするには:

Desktop Viewer の複数のウィンドウを使用する場合、デフォルトではアクティブでないウィンドウが減光されます。この機能により、複数のデスクトップを同時に表示する必要がある場合は、非アクティブなデスクトップ上の情報が読みづらくなる可能性があります。レジストリエディターを編集してデフォルトの設定を無効にし、Desktop Viewer ウィンドウの減光を防ぐことができます。

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

- ユーザーデバイスで、デバイスの現在のユーザーまたはデバイス自体で減光を防止するかどうかによって、**DisableDimming** という REG_DWORD エントリを次のいずれかのキーで作成します。デバイスで Desktop Viewer を使用したことがある場合は、エントリが既に存在します:
  - `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`
  - `HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer`

または、減光を制御する代わりに、同じ REG_WORD エントリを次のキーのどちらかに作成することによって、ローカルポリシーを定義できます。

- `HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer`
- `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer`

これらのキーを使用する前に、Citrix Virtual Apps and Desktops および Citrix DaaS の管理者がこの機能のポリシーを設定しているかどうか確認してください。

エントリを 1 または true のような 0 以外の値に設定します。

エントリが未指定、または 0 に設定されている場合は、Desktop Viewer ウィンドウが減光します。複数のエントリが指定されている場合、次の方法が使用されます。次の一覧の上位のエントリの値によって、ウィンドウを減光するかどうかが決まります。

1. HKEY_CURRENT_USER\Software\Policies\Citrix\…
2. HKEY_LOCAL_MACHINE\Software\Policies\Citrix\…
3. HKEY_CURRENT_USER\Software\Citrix\…
4. HKEY_LOCAL_MACHINE\Software\Citrix\…

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Casting

Citrix Ready ワークスペースハブは、デジタル環境と物理環境を組み合わせて、セキュアなスマートスペース内にアプリやデータを配信します。このシステム全体が、モバイルアプリやセンサーなどのデバイス（「モノ」）を接続して、インテリジェントで応答性の高い環境を作ります。

Citrix Ready ワークスペースハブは Raspberry Pi 3 プラットフォーム上に構築されます。Citrix Workspace アプリを実行しているデバイスは Citrix Ready ワークスペースハブに接続し、デスクトップまたはアプリをより大きなディスプレイにキャストします。Citrix Casting は、Microsoft Windows 10 バージョン 1607 以降、または Windows Server 2016 でのみサポートされます。

Citrix Casting は、モバイルデバイスから簡単かつセキュアに任意のアプリにアクセスして、大きな画面に表示できるようにする機能です。

> 注:
>
> - Citrix Casting for Windows は、Citrix Ready ワークスペースハブバージョン 2.40.3839 以降をサポートしています。以前のバージョンのワークスペースハブが検出されないか、キャストエラーが発生することがあります。
> - Citrix Casting 機能は、Windows（ストア）向け Citrix Workspace アプリではサポートされていません。

前提条件:

- 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 をブロックしないでください。
- Citrix Casting の場合、ポート 1494 をブロックしないでください。
- 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 は、Microsoft Windows 10 バージョン 1607 以降、または Windows Server 2016 でのみサポートされます。

Citrix Casting の起動の構成

> 注:
>
> システムトレイの Citrix Workspace アプリアイコンから表示できる［高度な設定］シートの一部または全部を非表示にすることができます。詳しくは、「高度な設定シート」を参照してください。

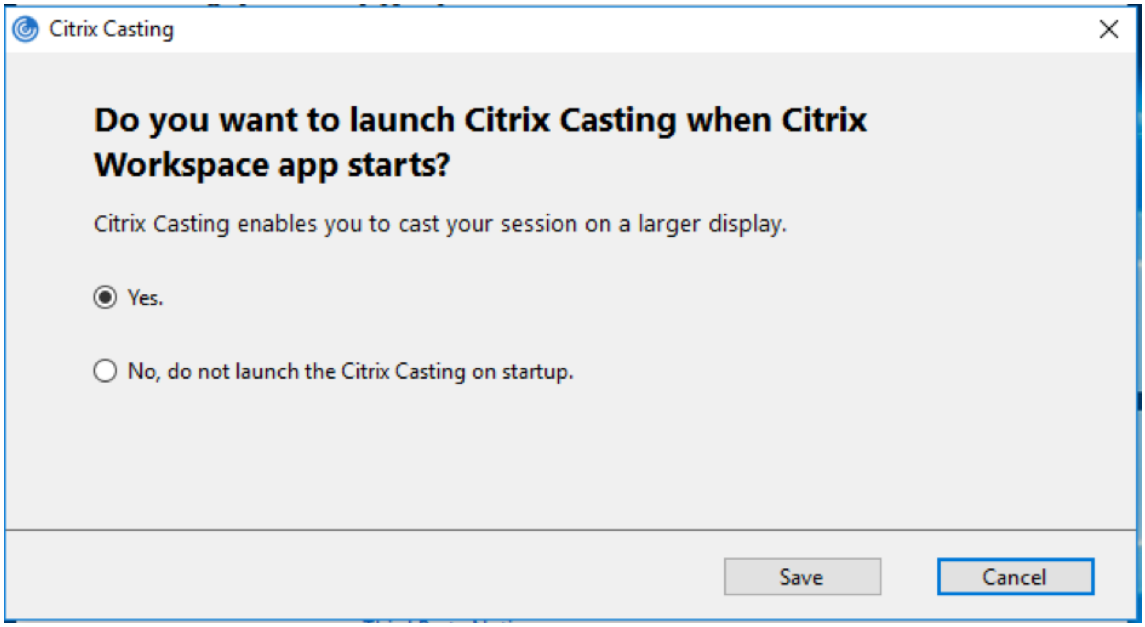
1. 通知領域で Citrix Workspace アプリアイコンを右クリックし、［高度な設定］をクリックします。

   ［高度な設定］ダイアログボックスが開きます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. [**Citrix Casting**] を選択します。

   [**Citrix Casting**] ダイアログボックスが表示されます。



3. 次のいずれかのオプションを選択します:

   - はい–Citrix Workspace アプリの起動時に Citrix Casting が起動されます。
   - いいえ。スタートアップ時に Citrix Casting を起動しません–Citrix Workspace アプリの起動時に Citrix Casting は起動されません。

   > 注:
   >
   > いいえを選択しても、現在の画面キャストのセッションは終了しません。この設定は、次回の Citrix Workspace アプリの起動時にのみ適用されます。

4. [保存] をクリックして変更を適用します。

Citrix Workspace アプリで **Citrix Casting** を使用する方法

1. Citrix Workspace アプリにログオンし、デバイス上で Bluetooth を有効にします。

   使用可能なハブの一覧が表示されます。一覧は、Citrix Ready ワークスペースハブビーコンパッケージの RSSI 値を基準として並べ替えられます。

2. 画面をキャストするワークスペースハブを選択し、次のいずれかを選択します。

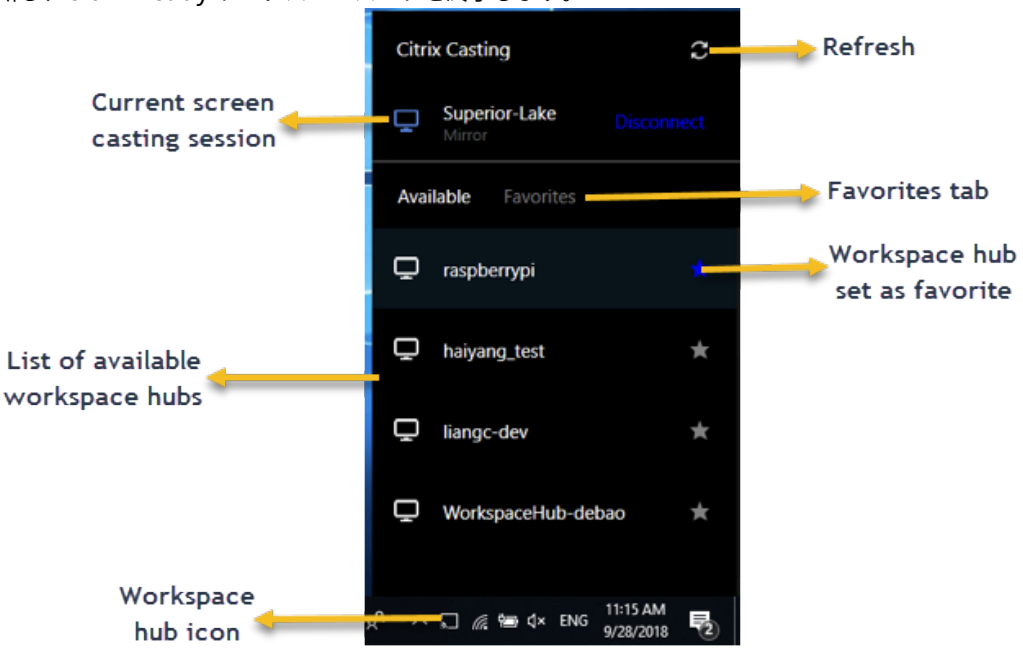
   - ミラーリング: プライマリ画面を複製し、接続されたワークスペースハブデバイスに表示をキャストします。
   - 拡張: ワークスペースハブデバイス画面をセカンダリ画面として使用します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> Citrix Workspace アプリを終了しても、Citrix Casting は終了しません。

［**Citrix Casting** の通知］ダイアログボックスには、次のオプションがあります:

1. 現在の画面キャストのセッションが上部に表示されます。
2. アイコンを ［更新］します。
3. ［切断］を選択して、現在の画面キャストのセッションを停止します。
4. 星アイコンをクリックして、ワークスペースハブを ［お気に入り］に追加します。
5. システムトレイのワークスペースハブアイコンを右クリックし、終了を選択して画面キャストのセッションを切断し、Citrix Ready ワークスペースハブを終了します。



セルフチェック一覧

Citrix Workspace アプリが範囲内の使用可能なワークスペースハブを検出して通信することができない場合は、セルフチェックの一環として以下を確認してください:

1. Citrix Workspace アプリと Citrix Ready ワークスペースハブが同じネットワークに接続している。
2. Citrix Workspace アプリが起動されたデバイスで Bluetooth が有効になり、正常に動作している。
3. Citrix Workspace アプリが起動されたデバイスが、Citrix Ready ワークスペースハブの範囲内（10 メートル未満。壁などの障害物がない）にある。
4. Citrix Workspace アプリでブラウザーを起動して、`http://<hub_ip>:55555/device-details.xml`を入力し、ワークスペースハブデバイスの詳細が表示されるかを確認します。
5. Citrix Ready ワークスペースハブで 更新 をクリックして、ワークスペースハブへの再接続を試みる。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

既知の問題と制限事項

1. デバイスが Citrix Ready ワークスペースハブと同じネットワークに接続されていないと、Citrix Casting は機能しません。
2. ネットワークに問題がある場合、ワークスペースハブデバイスでの表示に時間差が発生する可能性があります。
3. [拡張] を選択すると、Citrix Ready Workspace アプリが起動されるプライマリ画面が数回点滅します。
4. [拡張] モードでは、セカンダリディスプレイをプライマリディスプレイとして設定することはできません。
5. デバイスのディスプレイ設定が変更された場合、画面キャストのセッションは自動的に切断されます。たとえば、画面の解像度を変更されたり、画面の方向が変更されたりした場合などです。
6. 画面キャストのセッション中に、Citrix Workspace アプリを実行しているデバイスがロック、スリープまたは休止状態になると、ログイン時にエラーが表示されます。
7. 複数の画面キャストのセッションはサポートされていません。
8. Citrix Casting でサポートされている画面の最大解像度は 1920 x 1440 です。
9. Citrix Casting は、Citrix Ready ワークスペースハブバージョン 2.40.3839 以降をサポートしています。以前のバージョンのワークスペースハブが検出されないか、キャストエラーが発生することがあります。
10. この機能は、Windows（ストア）向け Citrix Workspace アプリではサポートされていません。
11. Windows 10 ビルド 1607 では、[拡張] モードの Citrix Casting が正しく配置されないことがあります。

複合 **USB** デバイスリダイレクト

複合 **USB** リダイレクトの構成:

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. [コンピューターの構成] ノードで、[管理用テンプレート] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [クライアントデバイスをリモート処理します] > [一般的な **USB** のリモート処理] の順に移動します。
3. **SplitDevices** ポリシーを選択します。
4. [有効] をクリックします。
5. [適用] および [**OK**] をクリックしてポリシーを保存します。

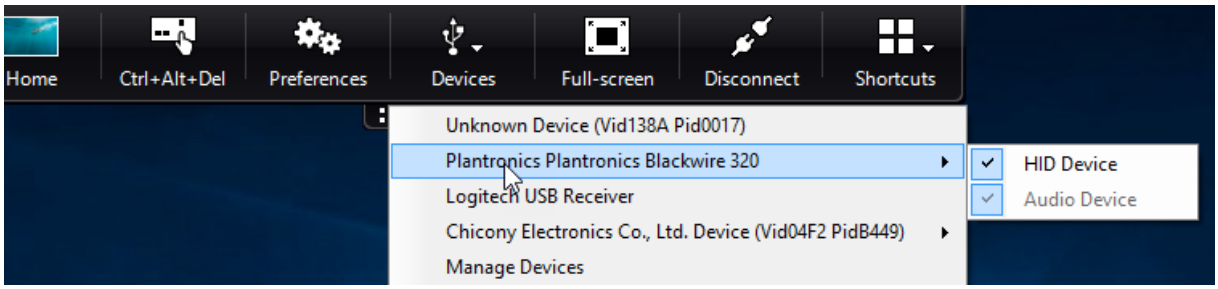
インターフェイスを許可または拒否するには:

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. [ユーザー構成] ノード配下で、[管理用テンプレート] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [クライアントデバイスをリモート処理します] > [一般的な **USB** のリモート処理] の順に移動します。
3. **USB** デバイス規則ポリシーを選択します。
4. [有効] をクリックします。
5. [**USB** デバイス規則] テキストボックスで、許可または拒否する USB デバイスを追加します。
   例: `ALLOW: vid=047F pid= C039 split=01 intf=00,03` - 00 および 03 インターフェイスを許可して、それ以外を禁止します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

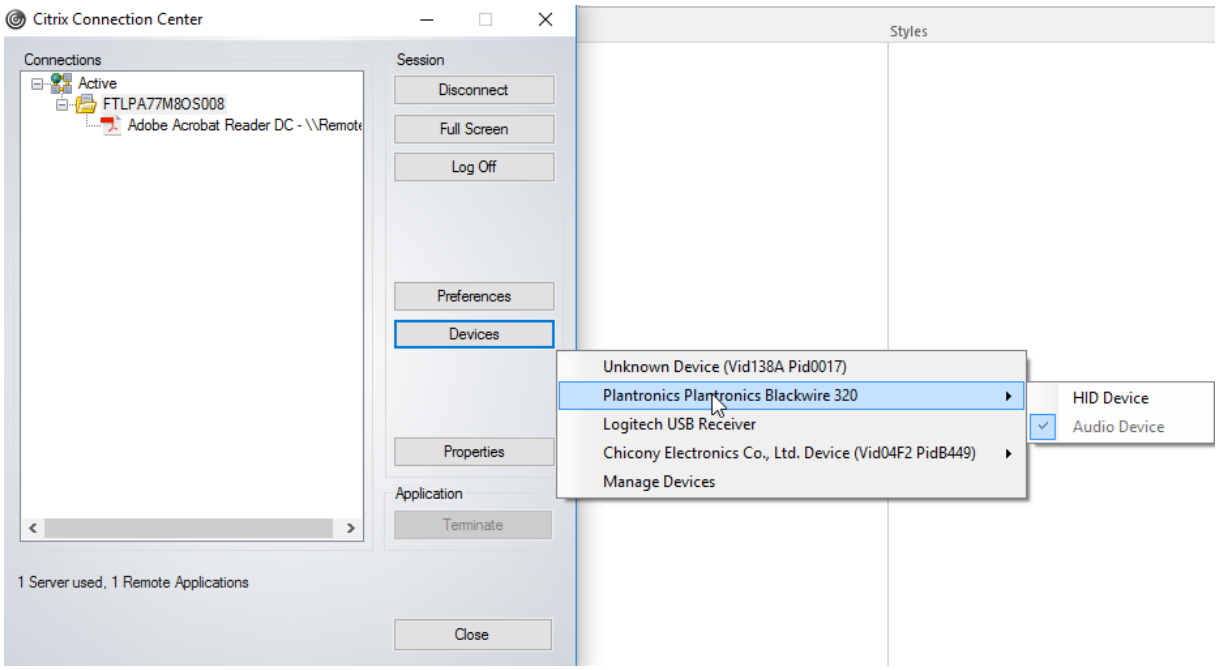
6. ［適用］、［**OK**］の順にクリックします。

デスクトップセッションでは、分割された USB デバイスは ［デバイス］の Desktop Viewer で表示されます。また、［基本設定］ > ［デバイス］から分割された USB デバイスを表示できます。



> 注:
>
> 汎用 USB リダイレクト用にコンポジット USB デバイスを分割する場合、デバイスをリダイレクトするには、Desktop Viewer またはコネクションセンターからデバイスを選択する必要があります。

アプリケーションセッションでは、分割デバイスはコネクションセンターで表示されます。



以下の表は、USB インターフェイスが許可または禁止される場合の動作に関する詳細です。

インターフェイスを許可する場合:

Split	インターフェイス	操作
TRUE	有効な数字 0 -n	指定のインターフェイスを許可する

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Split	インターフェイス	操作
TRUE	無効な数	すべてのインターフェイスを許可する
FALSE	任意の値	親デバイスの汎用 USB を許可する
指定なし	任意の値	親デバイスの汎用 USB を許可する

たとえば、SplitDevices- *true* は、すべてのデバイスが分割されることを示します。

インターフェイスを拒否する場合**:**

Split	インターフェイス	操作
TRUE	有効な数字 0 -n	指定のインターフェイスを拒否する
TRUE	無効な数	すべてのインターフェイスを拒否する
FALSE	任意の値	親デバイスの汎用 USB を拒否する
指定なし	任意の値	親デバイスの汎用 USB を拒否する

たとえば、SplitDevices- *false* は、デバイスが指定されたインターフェイス番号で分割されないことを示します。

例: *MyPlantronics* headset

インターフェイス番号:

- オーディオインターフェイスクラス -0
- HID インターフェイスクラス -3

MyPlantronics headset で使用される規則例:

- 許　　可: `vid=047F pid= C039 split=01 intf=00,03 /Allowed 00 and 03 interface, restrict others`
- 拒否: `vid=047F pid= C039 split=01 intf=00,03 / deny 00 and 03`

制限事項:

Citrix では Web カメラのインターフェイスは分割しないことをお勧めします。代わりに、汎用 USB リダイレクトを使用してデバイスを単一のデバイスにリダイレクトします。パフォーマンスを向上させるには、最適化された仮想チャネルを使用してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

DPI スケール機能

Windows 向け Citrix Workspace アプリでは、オペレーティングシステムがセッションの解像度を制御できます。

セッションに高 DPI を適用できますが、この機能はデフォルトでは無効になっています。つまり、セッションの表示サイズはオペレーティングシステムの解像度に従います。

次のオプションを使用して、DPI スケールを構成できます。

1. グループポリシーオブジェクト（GPO）管理用テンプレート（マシンごと）
2. 高度な設定（ユーザーごと）

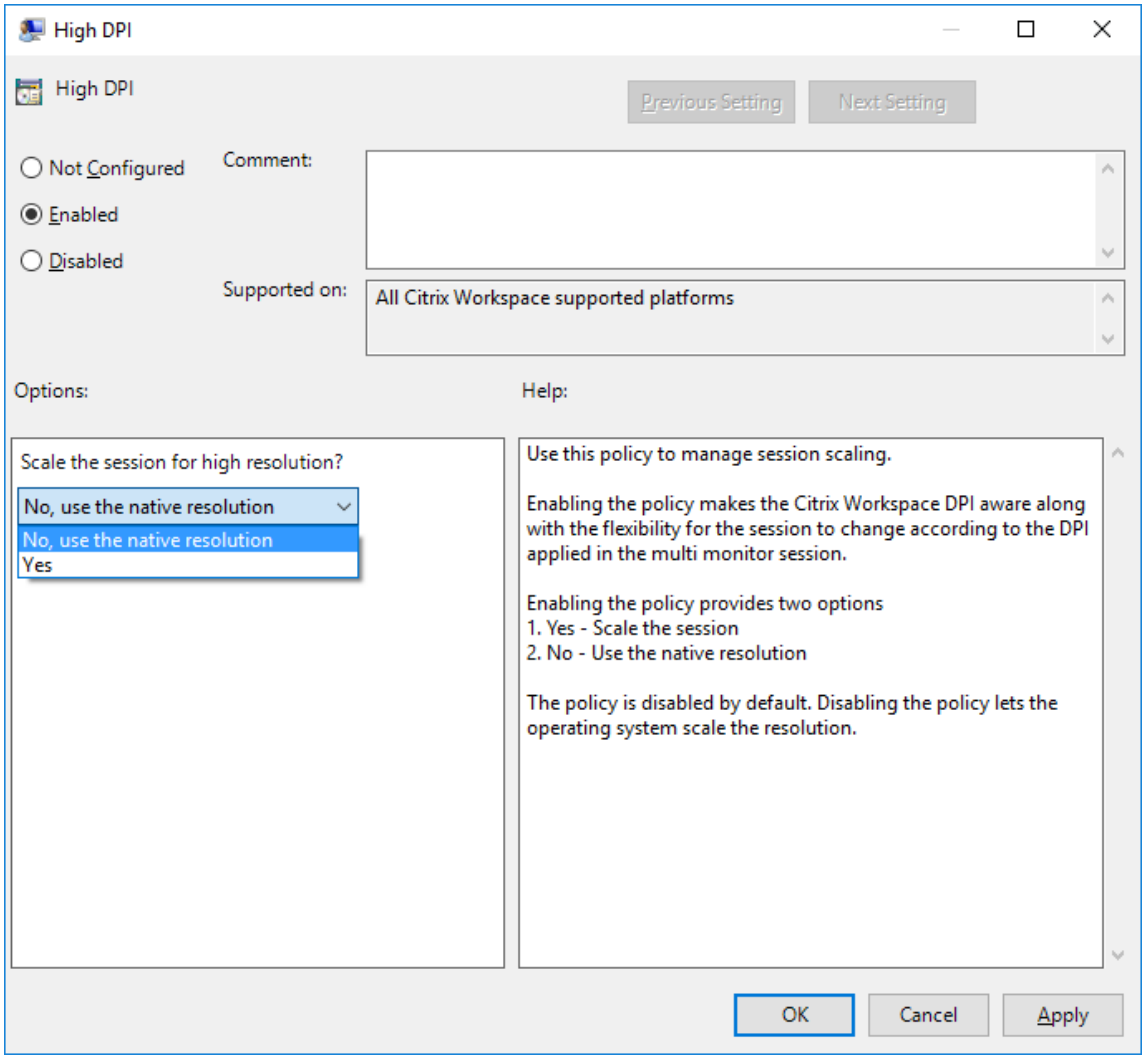
制限事項:

- この機能を有効にしても、Desktop Viewer の表示がわずかにぼやけます。
- セッションで、DPI 設定を変更して再起動すると、適切なセッションウィンドウのサイズにならないことがあります。この問題を解決するには、セッションウィンドウのサイズを変更します。

GPO 管理用テンプレートを使用して **DPI** スケールを構成するには:

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. [コンピューターの構成] ノードで、[管理用テンプレート] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [**DPI**] の順に移動します。
3. 高 **DPI** ポリシーを選択します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. 次のいずれかのオプションを選択します:

   a) はい - セッションに高 DPI が適用されます。
   b) いいえ、ネイティブ解像度を使用します - オペレーティングシステムによって設定されている解像度を使用します。

5. [適用]、[**OK**] の順にクリックします。
6. コマンドラインから`gpupdate /force`コマンドを実行して変更を適用します。

グラフィカルユーザーインターフェイスを使用した **DPI** スケールの構成:

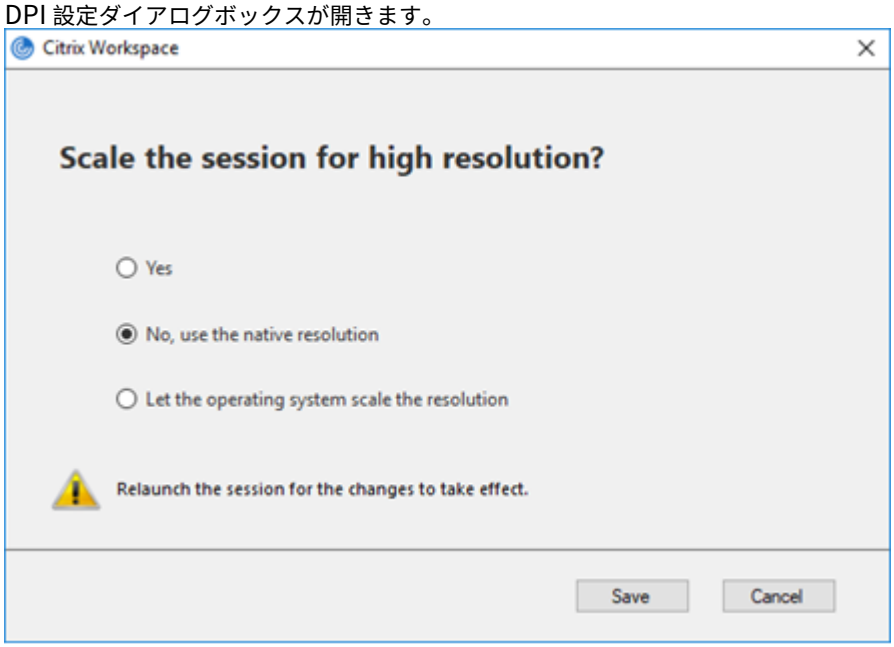
> 注:
>
> システムトレイの Windows 向け Citrix Workspace アプリアイコンで［高度な設定］シートの一部または全部を非表示にすることができます。詳しくは、「高度な設定シート」を参照してください。

1. システムトレイの Citrix Workspace アプリアイコンを右クリックします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. ［高度な設定］を選択して ［**DPI** 設定］をクリックします。

   DPI 設定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：

   a) はい - セッションに高 DPI が適用されます。
   b) いいえ、ネイティブ解像度を使用します - Citrix Workspace アプリは、VDA の DPI を検出して適用します。
   c) オペレーティングシステムの解像度スケールを適用します - デフォルトではこのオプションが選択されています。これにより、Windows は DPI スケールを処理できます。また、高 DPI ポリシーは無効に設定されます。

4. ［**Save**］をクリックします。
5. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

DPI スケールオプション

Citrix Workspace アプリの DPI スケールでは 3 種類の設定が可能です：Scaled、Unscaled、Operating system scaling。以下は、それぞれの使用例です。

Scaled:

Scaled 設定は、Operating system scaling と同様に VDA で解像度を変更しますが、異なる DPI が混在するシナリオもサポートします。これは、UI 設定の［はい］、または GPO ポリシーで高 DPI ポリシーを［有効］に設定した場合に相当します。この設定は、最新の VDA に接続するときの異なる DPI が混在するシナリオに適しています。シームレスセッションをスケール設定する唯一の方法です。スケールによって、特にテキスト画面の場合、画像がぼやける可能性があります。古い VDA（6.5、または従来のグラフィック用に構成）に接続すると、パフォーマンスが低下する

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

可能性があります。ローカルアプリアクセス、RTOP、画面の位置 API を使用するその他のプラグインはスケールで機能しません。設計上、シームレスアプリはこのモードでモニター間を移動して、正しいスケール設定を維持します。この設定は、最新の VDA に接続している Windows 10 のユーザーにお勧めします。サーバーのリソースに影響を与えることなく、異なる DPI の混在をサポートします。

Unscaled:

Unscaled 設定は、セッション内のすべてのモニターの高解像度を送信します。これらの解像度はスケールが解除されているため、アプリとデスクトップで小さなテキストやアイコンが表示されることがあります。これは、UI 設定の［いいえ］、または、GPO ポリシーで高 DPI ポリシーを［有効］に設定した場合に相当します。この設定ではスケールによって画面がぼやけることはありませんが、テキストやアイコンは小さくなることがあります。デスクトップセッションに接続するときは、DPI を VDA 内で設定して、目的のスケール設定を行うことができます。これは、RDS デスクトップやシームレスアプリケーションでは機能しません。この設定を有効にすると、セッションの解像度が高くなり、サーバーのパフォーマンスとスケーラビリティに影響を与えることがあります。
この設定は、追加のサーバーリソースが使用できる場合の、最高画質を必要とするデスクトップセッションにお勧めします。小さなテキストやアイコンがユーザーにとって問題にならない場合にも使用できます。

Operating system scaling:

Operating system scaling はデフォルトの設定であり、UI 設定の［オペレーティングシステムの解像度スケールを適用します］に相当します。このシナリオでは、高 DPI ポリシーが［無効］に設定されています。これにより、Windows オペレーティングシステムはセッションの DPI スケールを処理します。VDA の解像度は、DPI を基にしてスケール設定され、クライアントデバイスより小さな解像度になります。これは、単一のモニターセッションで適切に動作し、6.5 VDA または従来のグラフィック用に構成された VDA に接続するときに最適です。この方法では、異なる DPI の混在はサポートされません。すべてのモニターが同じ DPI ではない場合、セッションが機能しません。スケールによって、特にテキスト画面の場合、画像がぼやける可能性があります。Windows 10 オペレーティングシステムでカーソルサイズに問題が発生することもあります。
この設定は、最新の VDA に接続している Windows 7 エンドポイントのユーザー、または従来の VDA への接続時にお勧めします。異なる DPI が混在していない場合、Windows 10 でも使用できます。

仮想ディスプレイレイアウト

この機能では、リモートデスクトップに適用する仮想モニターレイアウトを定義し、1 つのクライアントモニターをリモートデスクトップ上の最大 8 つのモニターに仮想分割できます。仮想モニターは、Desktop Viewer の［モニターレイアウト］タブで設定できます。ここでは、垂直または水平の線で画面を仮想モニターに分けることができます。画面は、クライアントのモニター解像度で指定されたパーセンテージに従って分割されます。

DPI スケーリングまたは DPI マッチングに使用される仮想モニター用 DPI を設定できます。仮想モニターレイアウトを適用した後、セッションのサイズを変更するか、再接続します。

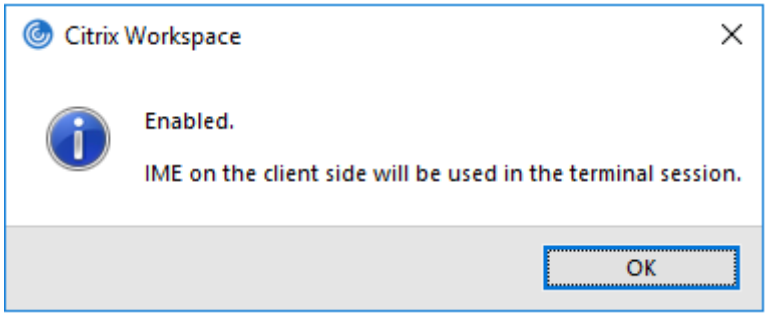
この構成は、全画面セッション、単一モニターのデスクトップセッションにのみ適用され、公開アプリケーションには影響しません。この構成は、以降のこのクライアントからのすべての接続に適用されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

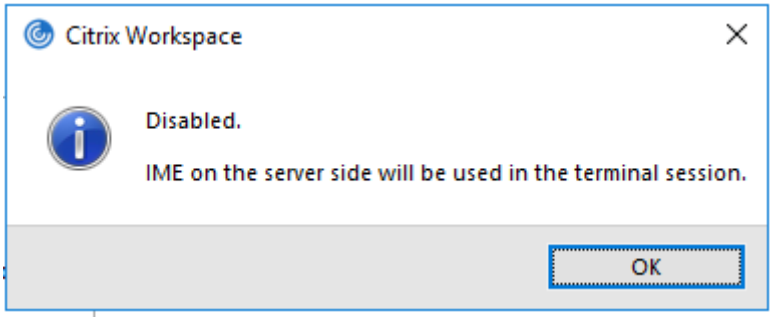
汎用クライアント入力システム（**IME**）

コマンドラインインターフェイスを使用した汎用クライアント **IME** の構成：

- 汎用クライアント IME を有効にするには、Citrix Workspace アプリインストールフォルダー（`C:\Program Files (x86)\Citrix\ICA Client`）から`wfica32.exe /localime:on`コマンドを実行します。



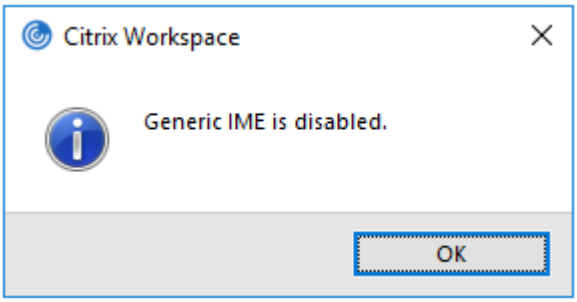
- 汎用クライアント IME を無効にするには、Citrix Workspace アプリインストールフォルダー（`C:\Program Files (x86)\Citrix\ICA Client`)から`wfica32.exe /localime:off`コマンドを実行します。



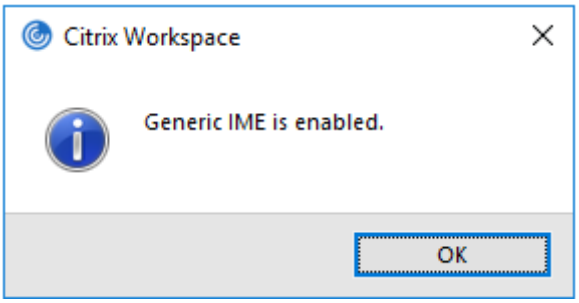
> 注：
>
> コマンドラインスイッチ`wfica32.exe /localime:on`を使用して、汎用クライアント IME とキーボードレイアウトの同期の両方を有効にすることができます。

- 汎用クライアント IME を無効にするには、Citrix Workspace アプリインストールフォルダー（`C:\Program Files (x86)\Citrix\ICA Client`）から`wfica32.exe /localgenericime:off`コマンドを実行します。このコマンドは、キーボードレイアウトの同期設定に影響を及ぼしません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



コマンドラインインターフェイスを使用して汎用クライアント IME を無効にした場合、`wfica32.exe /localgenericime:on`コマンドを実行することによって、再び機能を有効化できます。



トグル:

Citrix Workspace アプリは、この機能に対するトグルスイッチ機能をサポートしています。`wfica32.exe /localgenericime:on`コマンドを実行して、機能を有効/無効にできます。ただし、キーボードレイアウトの同期設定は、トグルスイッチより優先されます。キーボードレイアウトの同期がオフに設定されている場合、トグルしても汎用クライアント IME は有効になりません。

グラフィカルユーザーインターフェイスを使用した汎用クライアント **IME** の構成:

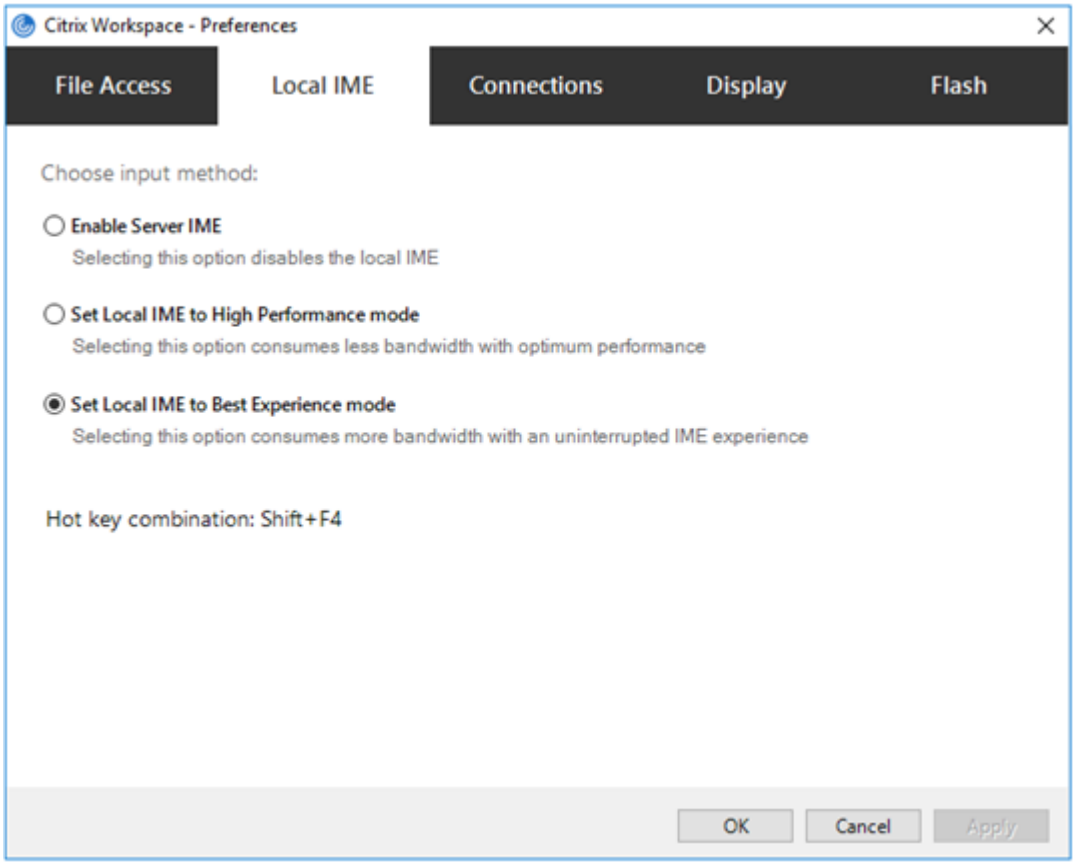
汎用クライアント IME には VDA Version 7.13 以降が必要です。

キーボードレイアウトの同期を有効化することにより、汎用クライアント IME 機能を有効化できます。詳しくは、「キーボードレイアウトの同期」を参照してください。

Citrix Workspace アプリを使用すると、汎用クライアント IME を使用するためのさまざまなオプションを構成できます。要件および使用状況に基づいて、これらのオプションのいずれかから選択できます。

1. アクティブなアプリケーションセッションで、システムトレイの Citrix Workspace アプリアイコンを右クリックして、［コネクションセンター］を選択します。
2. ［基本設定］、［ローカル **IME**］を選択します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



さまざまな IME モードをサポートするために以下のオプションを利用できます。

1. サーバー **IME** を有効にする - ローカル IME を無効にするため、サーバーの言語セットのみが利用できます。
2. ローカル **IME** を高パフォーマンスモードに設定する - ローカル IME を限られた帯域幅で使用できます。このオプションは、候補ウィンドウの機能を制限します。
3. ローカル **IME** を最適なエクスペリエンスモードに設定する - ローカル IME を最適なユーザーエクスペリエンスで使用できます。このオプションは、高帯域を消費します。デフォルトで、汎用クライアント IME が有効の場合、このオプションが選択されます。

設定変更は、現在のセッションにのみ適用されます。

レジストリエディターを使用したホットキー構成の有効化:

汎用クライアント IME が有効の場合、異なる IME モードを選択するには、**Shift+F4** ホットキーを使用できます。IME モードのさまざまなオプションがセッションの右上隅に表示されます。

デフォルトで、汎用クライアント IME のホットキーは無効です。

レジストリエディターで、`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys`に移動します。

AllowHotKey を選択して、デフォルト値を 1 に変更します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

制限事項:

- 汎用クライアント IME は、Search UI などの UWP（ユニバーサル Windows プラットフォーム）アプリや、Windows 10 オペレーティングシステムの Edge ブラウザーをサポートしません。回避策として、代わりにサーバー IME を使用します。
- 汎用クライアント IME は、保護モードの Internet Explorer バージョン 11 ではサポートされません。回避策として、インターネットオプションを使用して保護モードを無効にできます。そうする場合は、［セキュリティ］をクリックして、［保護モードを有効にする］をオフにします。

H.265 ビデオエンコーディング

Citrix Workspace アプリは、リモートグラフィックやビデオのハードウェアアクセラレーションで H.265 ビデオコーデックの使用をサポートしています。この機能を活用するには、VDA および Citrix Workspace アプリの両方でサポートされ、有効にする必要があります。エンドポイントの GPU が DXVA インターフェイスを使用する H.265 デコードをサポートしていない場合、グラフィックポリシー設定の H.265 デコードは無視され、セッションは H.264 ビデオコーデックの使用に戻ります。

前提条件:

1. VDA 7.16 以降。
2. VDA で **3D** 画像ワークロードの最適化ポリシーが有効になっている。
3. VDA でビデオコーデックにハードウェアエンコーディングを使用しますポリシーが有効になっている。

> 注:
>
> H.265 エンコーディングは、NVIDIA 社の GPU でのみサポートされます。

Windows 向け Citrix Workspace アプリでは、この機能がデフォルトで無効になっています。

グループポリシーオブジェクト（**GPO**）の管理用テンプレートを使用して **Citrix Workspace** アプリで **H.265** ビデオエンコーディングを構成する:

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. ［コンピューターの構成］ノードで、［管理用テンプレート］、［**Citrix Workspace**］、［ユーザーエクスペリエンス］の順に移動します。
3. グラフィックの **H.265** デコードポリシーを選択します。
4. ［有効］をクリックします。
5. ［適用］、［**OK**］の順にクリックします。

レジストリエディターを使用して **H.265** ビデオエンコーディングを構成する：

32 ビットオペレーティングシステムのドメイン不参加のネットワークで **H.265** ビデオエンコーディングを有効にする：

1. ［ファイル名を指定して実行］コマンドで regedit を使用してレジストリエディターを起動します。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine`にアクセスします。
3. **EnableH265** という名前で DWORD キーを作成し、キーの値を 1 に設定します。

64 ビットオペレーティングシステムのドメイン不参加のネットワークで **H.265** ビデオエンコーディングを有効にする：

1. ［ファイル名を指定して実行］コマンドで regedit を使用してレジストリエディターを起動します。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine`にアクセスします。
3. EnableH265 という名前で DWORD キーを作成し、キーの値を 1 に設定します。

変更を保存するには、セッションを再起動します。

> 注：
>
> - Windows 向け Citrix Workspace アプリのグループポリシーオブジェクト管理用テンプレートで ［グラフィックのハードウェアアクセラレーション］ポリシーが無効になっている場合、［グラフィックの **H.265** デコード］ポリシー設定は無視され、この機能は動作しません。
> - HDX Monitor 3.x ツールを実行して、セッション内で H.265 ビデオエンコーダーが有効になっているかを確認します。HDX Monitor 3.x ツールについて詳しくは、Knowledge Center のCTX135817を参照してください。

キーボードレイアウトと言語バー

キーボードレイアウト

> 注：
>
> システムトレイの Citrix Workspace アプリアイコンから表示できる［高度な設定］シートの一部または全部を非表示にすることができます。詳しくは、「高度な設定シート」を参照してください。

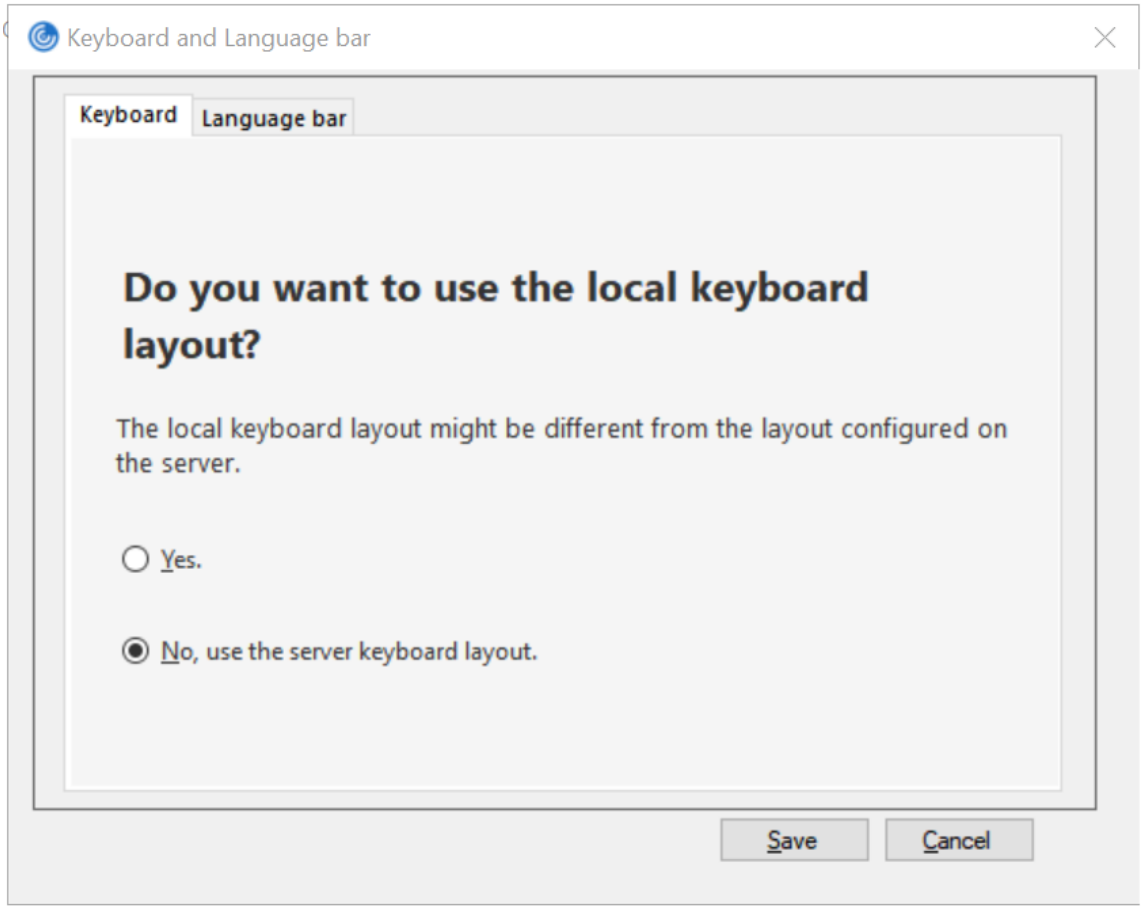
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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:

1. システムトレイの Citrix Workspace アプリアイコンから ［高度な設定］>［キーボードと言語バー］の順に選択します。

   キーボードと言語バーのダイアログが開きます。



2. 次のいずれかのオプションを選択します:

   - はい - セッションでローカルのキーボードレイアウトが使用されます。
   - いいえ、サーバーのキーボードレイアウトを使用します - VDA で使用されているキーボードレイアウトがセッションに適用されます。このオプションでは、ローカルキーボードレイアウト機能は無効に設定されます。

3. ［**Save**］をクリックします。

Windows インストールフォルダー（`C:\Program files (x86)\Citrix\ICA Client`）の Citrix Workspace アプリからコマンドラインを使用して`wfica32:exe /localime:on`または`wfica32:exe /localime:off`を実行することで、キーボードレイアウトの同期を有効または無効にすることもできま

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

す。

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）をアクティブにします。日本語、中国語、または韓国語を使用しているユーザーがサーバー IME を使用する場合、［いいえ］を選択するか、`wfica32:exe /localime:off`を実行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。

クライアントのキーボードレイアウトの切り替えがアクティブなセッションで有効にならないことがあります。この問題を解決するには、いったん Citrix Workspace アプリからログオフしてから、再度ログインしてください。

キーボードレイアウトの切り替え通知ダイアログを非表示にする：

キーボードレイアウトの変更通知ダイアログでは、VDA セッションがキーボードレイアウトを切り替えるときに通知します。キーボードレイアウトの切り替えには、約 2 秒かかります。通知ダイアログを非表示にする場合、間違った文字入力を避けるために、しばらく待ってから入力を開始してください。

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

レジストリエディターを使用してキーボードレイアウトの切り替え通知ダイアログを非表示にする：

1. レジストリエディターを起動して、`HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`に移動します。
2. **HideNotificationWindow** という名前で文字列値キーを作成します。
3. DWORD 値を **1** に設定します。
4. ［**OK**］をクリックします。
5. 変更を保存するには、セッションを再起動します。

制限事項：

- 管理者権限で実行しているリモートアプリケーション（例：アプリケーションアイコンを右クリックして、［管理者として実行］）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、サーバー側（VDA）で手動でキーボードレイアウトを変更するか、UAC を無効にします。
- ユーザーがクライアントのキーボードレイアウトをサーバーでサポートされていないレイアウトに変更すると、キーボードレイアウトの同期機能は、セキュリティ上の理由で無効になります。認識されないキーボードレイアウトは、潜在的なセキュリティ上の脅威として扱われるためです。キーボードレイアウト同期機能を復元するには、ログオフしてセッションに再ログインします。
- RDP セッションでは、Alt+Shift のショートカットキーでキーボードレイアウトを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を使用してキーボードレイアウトを切り替えます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- この機能は、パフォーマンス上のリスクの可能性があるサードパーティ製品の問題によって、Windows Server 2016 で無効になっています。これは、VDA のレジストリ設定で有効にできます：HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaImeで、**DisableKeyboardSync** という名称の新しいキーを追加し、値を 0 に設定します。

言語バー

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。Citrix Receiver for Windows バージョン 4.11 以降では、［高度な設定］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。

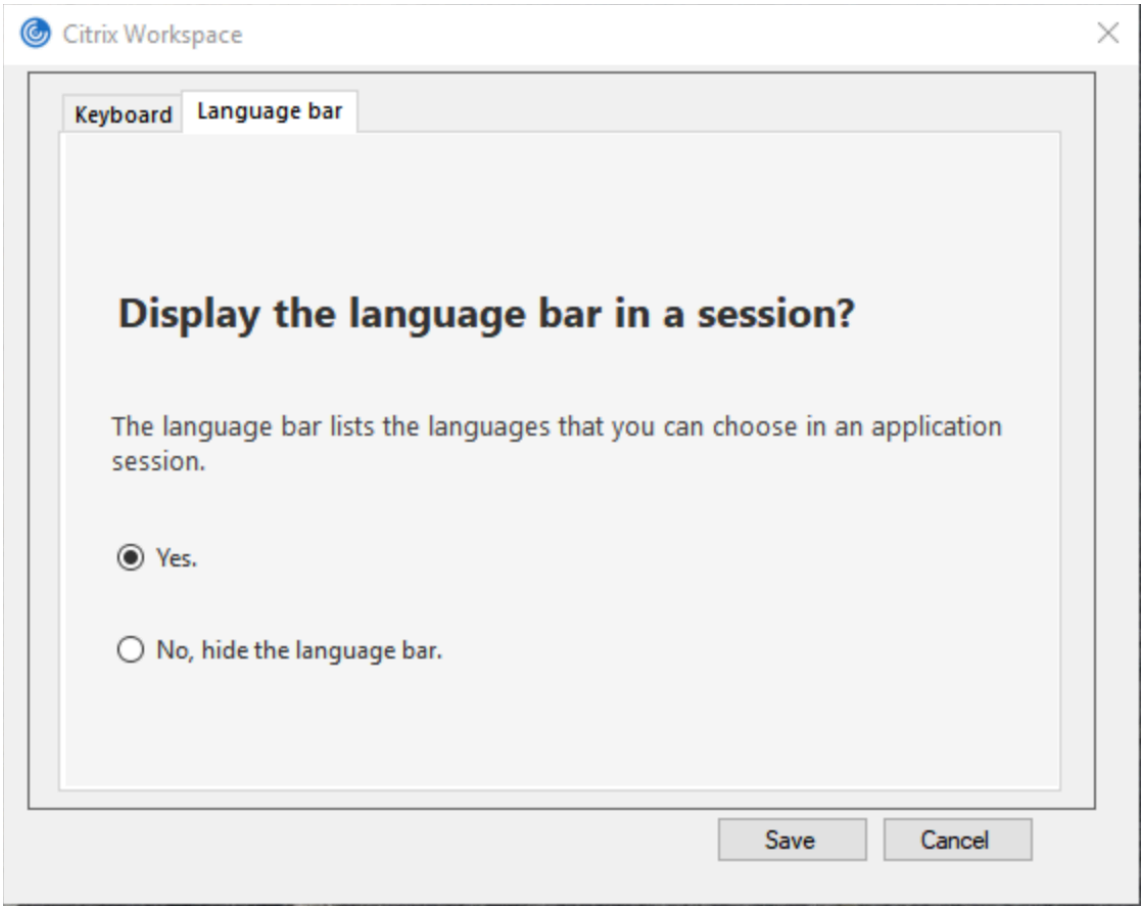
> 注：
>
> この機能は、VDA 7.17 以降で動作するセッションで使用できます。

リモート言語バーの表示または非表示を構成する：

1. 通知領域で Citrix Workspace アプリアイコンを右クリックし、［高度な設定］をクリックします。
2. ［キーボードと言語バー］を選択します。
3. ［言語バー］タブを選択します。
4. 次のいずれかのオプションを選択します：
   a) はい - セッションで言語バーが表示されます。
   b) いいえ。言語バーを非表示にします - セッションで言語バーが非表示になります。
5. ［**Save**］をクリックします。

   設定の変更は直ちに有効になります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> 注:
>
> - 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。

高度な設定シートで言語バータブを非表示にする:

レジストリを使用して、[高度な設定] シートから言語バータブを非表示にすることができます。

1. レジストリエディターを起動します。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME`にアクセスします。
3. DWORD 値キー **ToggleOffLanguageBarFeature** を作成し、**1** に設定すると、[高度な設定] シートで言語バーオプションが非表示になります。

USB サポート

USB サポート機能により、Citrix Virtual Apps and Desktops および Citrix DaaS 上で作業しているときにさまざまな種類の USB デバイスを使用できるようになります。コンピューターに USB デバイスを接続すると、仮想デスクトップ内でそのデバイスを操作できるようになります。この機能では、フラッシュドライブ、スマートフォン、

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

PDA、プリンター、スキャナー、MP3 プレーヤー、セキュリティデバイス、およびタブレットなどの USB デバイスがサポートされます。Desktop Viewer のユーザーは、ツールバーの基本設定を使用して、Citrix Virtual Apps and Desktops および Citrix DaaS で USB デバイスを使用できるようにするかどうかを制御できます。

Web カメラ、マイク、スピーカー、ヘッドセットなどの USB デバイスのアイソクロナス機能は、一般的な低遅延/高速 LAN 環境でサポートされます。これにより、Microsoft Office Communicator や Skype などのパッケージでこれらのデバイスを使用できるようになります。

以下の種類のデバイスは直接サポートされるため、仮想アプリと仮想デスクトップのセッションで USB サポート機能は使用されません。

- キーボード
- マウス
- スマートカード

特殊用途の USB デバイス（Bloomberg キーボードや 3D マウスなど）では、USB サポート機能が使用されるように構成できます。Bloomberg キーボードの構成について詳しくは、「Bloomberg キーボードの構成」を参照してください。

そのほかの特殊用途の USB デバイスのポリシー規則の構成について詳しくは、Knowledge Center の CTX122615を参照してください。

デフォルトでは、特定の種類の USB デバイスが Citrix Virtual Apps and Desktops および Citrix DaaS で動作しないように設定されています。たとえば、内部 USB でシステムボードに装着されたネットワークインターフェイスカードの場合、このデバイスのリモート操作は適しません。次の種類の USB デバイスは、仮想アプリと仮想デスクトップのセッションでの使用をデフォルトでサポートされていません。

- Bluetooth ドングル
- 統合ネットワークインターフェイスカード
- USB ハブ
- USB グラフィックアダプター

USB ハブに接続されたデバイスは仮想デスクトップで使用できますが、USB ハブ自体はリモート処理できません。

次の種類の USB デバイスは、Citrix Virtual Apps セッションでの使用をデフォルトでサポートしていません。

- Bluetooth ドングル
- 統合ネットワークインターフェイスカード
- USB ハブ
- USB グラフィックアダプター
- オーディオデバイス
- 大容量記憶装置デバイス

USB サポートのしくみ:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ユーザーがエンドポイントに USB デバイスを接続すると、USB ポリシーが照合され、許可されているデバイスであることが認識されると、仮想デスクトップ上で使用可能になります。USB ポリシーで拒否されるデバイスは、ローカルのデスクトップ上でのみ使用可能になります。

USB デバイスを接続すると、新しいデバイスについて知らせる通知が表示されます。ユーザーは、USB デバイスを接続するたびに、そのデバイスを仮想デスクトップで使用するかどうかを選択できます。ユーザーは、仮想デスクトップセッションの開始前、またはセッション実行中に接続した USB デバイスが、フォーカスのある仮想デスクトップで自動的に使用可能になるように設定することもできます。

大容量記憶装置デバイス

マスストレージデバイス（大容量記憶装置）の場合は、USB サポートに加え、クライアント側ドライブのマッピング機能によるリモートアクセスも可能で、これは Windows 向け Citrix Workspace アプリポリシーの ［クライアントデバイスをリモート処理します］>［クライアントドライブマッピング］で設定します。このポリシーを適用すると、ユーザーのログオン時にユーザーデバイス上のドライブが自動的に仮想デスクトップ上のドライブ文字にマップされます。これらのドライブは、マップされたドライブ文字を持つ共有フォルダーとして表示されます。

クライアント側リムーバブルドライブマッピングと USB サポートの 2 つの設定の主な違いは以下のとおりです。

機能	クライアントドライブマッピング	USB サポート
デフォルトで有効	はい	いいえ
読み取り専用アクセスの構成が可能	はい	いいえ
セッション中にデバイスを安全に取り外せる	いいえ	はい（ユーザーがシステムトレイの［ハードウェアの安全な取り外し］をクリックする場合）

［汎用 USB］と［クライアントドライブマッピング］の両方のポリシーが有効で、マスストレージデバイスがセッションの開始前に装着された場合は、USB サポート機能によるリダイレクトの前にクライアント側ドライブのマッピングによるリダイレクトが実行されます。マスストレージデバイスがセッションの開始後に装着された場合は、クライアントドライブマッピングの前に USB サポートによるリダイレクトが実行されます。

デフォルトで許可される **USB** デバイスのクラス：

以下のクラスの USB デバイスは、デフォルトの USB ポリシー規則により仮想デスクトップでの使用が許可されます。

この一覧に記載されていても、一部のクラスは構成を追加しなければ仮想アプリと仮想デスクトップのセッションでリモート処理ができません。それらのクラスについては以下に記述します。

- オーディオ（クラス **01**）- このクラスのデバイスとして、オーディオ入力デバイス（マイク）、オーディオ出力デバイス、および MIDI コントローラーがあります。最近のオーディオデバイスでは一般的にアイソクロナス転送が使用されますが、この機能は XenDesktop 4 以降でサポートされます。USB サポートを使用する

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Virtual Apps でオーディオデバイスをリモート操作できないため、オーディオ（クラス 01）は Citrix Virtual Apps に適用できません。

> 注:
>
> VoIP 電話などの一部の特殊デバイスには追加の構成が必要です。詳しくは、Knowledge Center のCTX123015を参照してください。

- 物理インターフェイスデバイス（クラス **05**）- このデバイスはヒューマンインターフェイスデバイス（HID）と似ていますが、一般的に「リアルタイム」の入力またはフィードバックを提供し、フォースフィードバックジョイスティック、モーションプラットフォーム、およびフォースフィードバックエクソスケルトンなどがあります。
- 静止画（クラス **06**）- このクラスのデバイスとして、デジタルカメラおよびスキャナーがあります。ほとんどのデジタルカメラは、画像転送プロトコル（PTP）またはメディア転送プロトコル（MTP）を使ってコンピューターやほかの周辺機器にイメージを転送する静止画クラスをサポートします。また、デジタルカメラはマスストレージデバイスとして機能する場合もあり、カメラ自体のメニューを使っていずれかのクラスを使用するように構成できます。

> 注:
>
> カメラがマスストレージデバイスとして機能する場合はクライアントドライブマッピングが使用され、USB サポートは必要ありません。

- プリンター（クラス **07**）- 一部のプリンターではベンダー固有のプロトコル（クラス ff）が使用されますが、一般的にはこのクラスにほとんどのプリンターが含まれます。マルチ機能プリンターの場合は、USB ハブが内蔵されていたり、混合デバイスであったりする場合があります。いずれの場合も、印刷機能では一般的にプリンタークラスが使用され、スキャナーや FAX 機能では静止画などの別のクラスが使用されます。

  プリンターは通常、USB サポートなしで適切に動作します。

  > 注
  >
  > このクラスのデバイス（特にスキャナー機能を持つプリンター）には追加の構成が必要です。構成手順については、Knowledge Center のCTX123015を参照してください。

- マスストレージデバイス（クラス **08**）- 最も一般的なマスストレージデバイス（大容量記憶装置）として、USB フラッシュドライブがあります。そのほかには、USB 接続のハードドライブ、CD/DVD ドライブ、および SD/MMC カードリーダーがあります。また、内部ストレージを持つさまざまなデバイスがあり、これらもこのクラスのインターフェイスを提供します。たとえば、メディアプレーヤー、デジタルカメラ、携帯電話などがあります。USB サポートを使用する Citrix Virtual Apps でマスストレージデバイスをリモート操作できないため、マスストレージ（クラス 08）は Citrix Virtual Apps に適用できません。既知のサブクラスには次のものが含まれます:

  - 01 制限付きフラッシュデバイス
  - 02 一般的な CD/DVD デバイス（ATAPI/MMC-2）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 03 一般的なテープデバイス（QIC-157）
- 04 一般的なフロッピーディスクドライブ（UFI）
- 05 一般的なフロッピーディスクドライブ（SFF-8070i）
- 06 ほとんどの大容量記憶装置デバイスはこの SCSI のバリアントを使用します

マスストレージデバイスには、クライアントドライブマッピングを介して頻繁にアクセスすることができ、USB サポートは必要ありません。

- コンテンツセキュリティ（クラス **0d**）- 通常、ライセンスまたはデジタル権利の管理のためのコンテンツ保護を実行します。このクラスのデバイスとして、ドングルがあります。
- ビデオ（クラス **0e**）- このクラスのデバイスとして、ビデオ、Web カメラ、デジタルカムコーダー、アナログビデオ変換機、一部のテレビチューナー、およびビデオストリーミングをサポートする一部のデジタルカメラなど、ビデオ関連の機器があります。

> 重要
>
> ほとんどのビデオストリーミングデバイスではアイソクロナス転送が使用されますが、この機能は XenDesktop 4 以降でサポートされます。動作検知機能付きの Web カメラなど、一部のビデオデバイスには追加の構成が必要です。構成手順については、Knowledge Center のCTX123015を参照してください。

- パーソナルヘルスケア（クラス **0f**）- このデバイスには、血圧センサー、心拍数モニター、万歩計、薬剤モニター、肺活量計などの個人用健康器具があります。
- アプリケーションおよびベンダー固有（クラス **fe** および **ff**）- 多くのデバイスがベンダー独自のプロトコルまたは USB コンソーシアムで標準化されていないプロトコルを使用しており、これらは通常はベンダー固有（クラス ff）として分類されます。

デフォルトで拒否される **USB** デバイスのクラス

次の USB デバイスの異なるクラスは、デフォルトの USB ポリシー規則により拒否されます。

- 通信および CDC コントロール（クラス 02 および 0a）。仮想デスクトップ自体への接続にこれらのデバイスのいずれかが使用される場合があるため、デフォルトの USB ポリシーではこれらのデバイスのリモートでの実行は許可されていません。
- ヒューマンインターフェイスデバイス（クラス 03）。さまざまな種類の入出力デバイスを含みます。一般的なヒューマンインターフェイスデバイス（HID）として、キーボード、マウス、ポインティングデバイス、グラフィックタブレット、センサー、およびゲームのコントローラー、ボタン、およびコントロール機能などがあります。

  サブクラス 01 は「起動インターフェイス」クラスとして知られ、キーボードおよびマウスで使用されます。

  デフォルトの USB ポリシーは USB キーボード（クラス 03、サブクラス 01、プロトコル 1）または USB マウス（クラス 03、サブクラス 01、プロトコル 2）を許可しません。これは、ほとんどのキーボードおよびマウ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

スは USB サポートなしでも適切に処理され、一般に仮想デスクトップ内だけでなくローカルでも使用されるためです。

- USB ハブ（クラス 09）。USB ハブを使用すると、より多くのデバイスをローカルのコンピューターに接続できます。これらのデバイスにリモートでアクセスする必要はありません。
- スマートカード（クラス 0b）。スマートカードリーダーには、非接触型および接触型のスマートカードリーダーと、スマートカードと同等のチップを埋め込んだ USB トークンがあります。

  スマートカードリーダーは、スマートカードサポート機能によりアクセスできるため、USB サポートは必要ありません。
- ワイヤレスコントローラー（クラス e0）。これらのデバイスの中には、重要なネットワークアクセスを提供していたり、Bluetooth キーボードやマウスなどの基幹周辺装置を接続していたりするものがある場合があります。

  デフォルトの USB ポリシーはこれらのデバイスを許可していません。ただし、USB サポートを使ったアクセスに適したデバイスもあります。
- その他のネットワークデバイス（クラス **ef**、サブクラス **04**）- これらのデバイスの一部は、重要なネットワークアクセスを提供している可能性があります。デフォルトの USB ポリシーはこれらのデバイスを許可していません。ただし、USB サポートを使ったアクセスに適したデバイスもあります。

仮想デスクトップで使用できる **USB** デバイスの一覧の変更

Windows 向け Citrix Workspace のテンプレートファイルを編集して、仮想デスクトップセッション内で使用できる USB デバイスの範囲を更新できます。これにより、グループポリシーを使用して Windows 向け Citrix Workspace に変更を加えることができます。このファイルは、次のインストールフォルダーにあります:

```
\C:\Program Files\Citrix\ICA Client\Configuration\en。
```

または、各ユーザーデバイスのレジストリに次のレジストリキーを追加できます:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB
Type=String Name="DeviceRules"Value=
```

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

製品のデフォルトの規則は、次の場所に保存されています:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB 種類 =MultiSz 名前 =” DeviceRules” 値 =

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

これらのデフォルトの規則は変更しないでください。

USB デバイスのポリシー設定について詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「USB デバイスのポリシー設定」を参照してください。

USB オーディオの構成

> 注:
>
> - Windows 向け Citrix Workspace アプリを初めてアップグレードまたはインストールする場合、最新のテンプレートファイルをローカル GPO に追加します。テンプレートファイルをローカル GPO に追加する方法について詳しくは、「グループポリシーオブジェクト管理用テンプレート」を参照してください。アップグレードの場合、最新のファイルをインポートするときに既存の設定が保持されます。
> - この機能は、Citrix Virtual Apps サーバーでのみ使用できます。

USB オーディオデバイスを構成するには:

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. [コンピューターの構成] ノードで、[管理用テンプレート] **>** [従来の管理用テンプレート (**ADM**)] **>** [**Citrix** コンポーネント] **>** [**Citrix Workspace**] **>** [ユーザーエクスペリエンス] の順に移動し、[一般的な **USB** リダイレクトによるオーディオ] をクリックします。
3. 設定を編集します。
4. [適用]、[**OK**] の順にクリックします。
5. コマンドプロンプトを管理者モードで開きます。
6. 次のコマンドを実行します。

```
gpupdate /force
```

vPrefer 起動

以前のリリースでは、**Citrix Studio** の KEYWORDS:prefer=”application”属性を設定することで、VDA にインストールされたアプリケーションのインスタンス（このドキュメントではローカルインスタンスと呼びます）を公開アプリケーションよりも優先して起動するよう指定できました。

バージョン 4.11 から、ダブルホップシナリオ（セッションをホストしている VDA で Citrix Workspace アプリが実行されている）では、VDA にインストールされたアプリケーションのローカルインスタンス（ローカルアプリとして使用できる場合）を、Citrix Workspace アプリがアプリケーションのホストされたインスタンスよりも優先して起動するかを制御できるようになりました。

vPrefer は、StoreFront バージョン 3.14 および Citrix Virtual Desktops 7.17 以降で使用できます。

アプリケーションを起動すると、Citrix Workspace アプリは StoreFront サーバー上のリソースデータを読み取り、列挙時に **vprefer** フラグに基づいてこの設定を適用します。Citrix Workspace アプリは、VDA の Windows レジ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、アプリケーションのホストされたインスタンスを起動します。
VDA にインストールされていないアプリケーションを起動すると、ホストされているアプリケーションが起動します。StoreFront でローカル起動を処理する方法について詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「公開デスクトップ上のアプリケーションのローカル起動を制御する」を参照してください。

アプリケーションのローカルインスタンスを VDA で起動しない場合は、Delivery Controller で PowerShell を使用して **LocalLaunchDisabled** を **True** に設定します。詳しくは、Citrix Virtual Apps and Desktopsのドキュメントを参照してください。

この機能によって、アプリケーションをよりすばやく起動できるため、より良いユーザーエクスペリエンスを実現できます。この機能は、グループポリシーオブジェクト（GPO）管理用テンプレートで構成できます。デフォルトでは、vPrefer はダブルホップシナリオでのみ有効です。

> 注:
>
> Citrix Workspace アプリを初めてアップグレードまたはインストールする場合、最新のテンプレートファイルをローカル GPO に追加します。テンプレートファイルをローカル GPO に追加する方法について詳しくは、「グループポリシーオブジェクト管理用テンプレート」を参照してください。アップグレードの場合、最新のファイルをインポートするときに既存の設定が保持されます。

1. gpedit.msc を実行して、Citrix Workspace アプリの GPO 管理用テンプレートを開きます。
2. [コンピューターの構成] ノードで、[管理用テンプレート] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [**SelfService**] の順に移動します。
3. **vPrefer** ポリシーを選択します。
4. [有効] を選択し、[アプリを許可] ドロップダウンリストの次のオプションから選択します。
    - [すべてのアプリを許可]: このオプションは、VDA 上のすべてのアプリのローカルインスタンスを起動します。Citrix Workspace アプリは、インストールされているアプリケーション（メモ帳、電卓、ワードパッド、コマンドプロンプトなどのネイティブ Windows アプリを含む）を検索し、ホストされているアプリの代わりに VDA で起動します。
    - インストール済みアプリを許可: このオプションは、VDA 上のインストール済みアプリのローカルインスタンスを起動します。アプリが VDA にインストールされていない場合は、ホストされているアプリを起動します。**vPrefer** ポリシーが [有効] に設定されている場合、デフォルトで [インストール済みアプリを許可] が選択されます。このオプションは、メモ帳、電卓などのネイティブ Windows オペレーティングシステムアプリケーションを除外します。
    - ネットワークアプリを許可: このオプションは、共有ネットワークに公開されているアプリのインスタンスを起動します。
5. [適用]、[**OK**] の順にクリックします。
6. 変更を保存するには、セッションを再起動します。

制限事項:

- Web 向け Workspace はこの機能をサポートしていません。

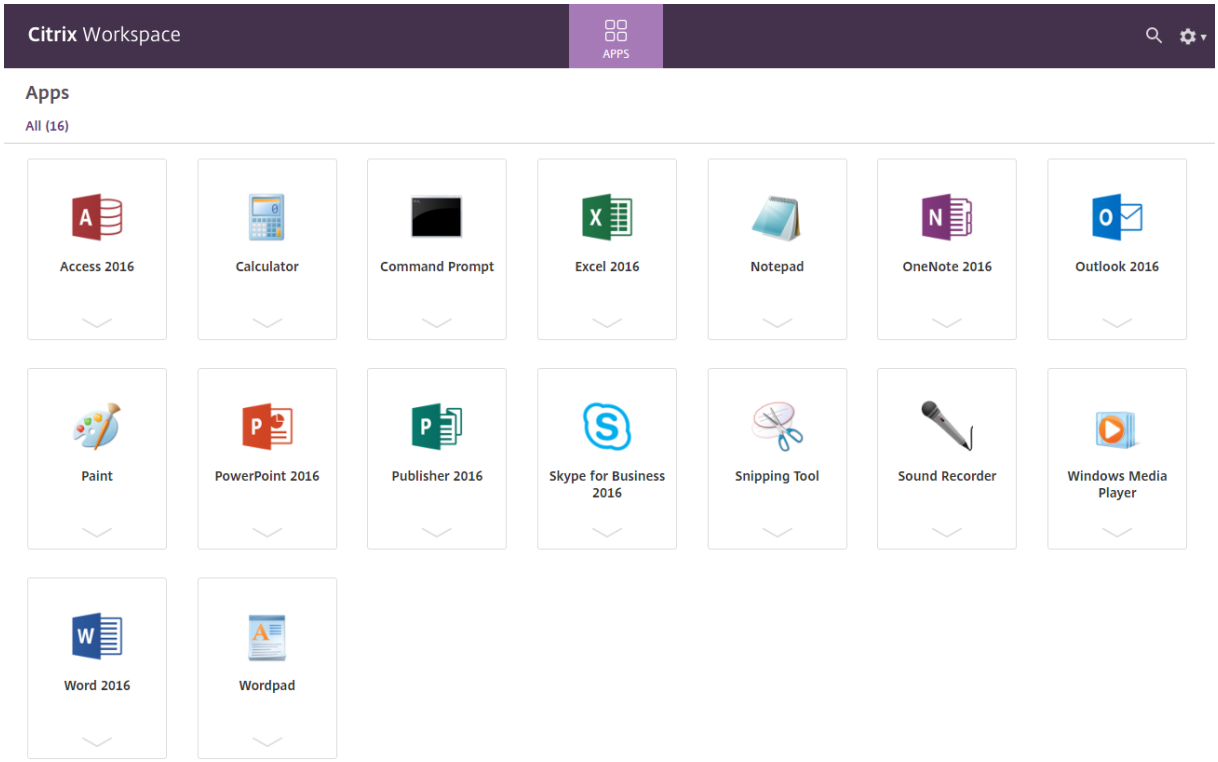
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ワークスペース構成

Windows 向け Citrix Workspace アプリでは、Citrix Cloud から提供されている 1 つまたは複数のサービスを使用している利用者のためのワークスペースを構成できるようになりました。

Citrix Workspace アプリには、ユーザーが権限を持つ特定のワークスペースリソースのみがインテリジェントに表示されます。Citrix Workspace アプリで使用可能なデジタルワークスペースリソースの提供はすべて、Citrix Cloud のワークスペース環境サービスが行います。

ワークスペースはデジタルワークスペースソリューションの一部で、これによって IT 部門は、任意のデバイスからアプリへの安全なアクセスを提供できます。
このスクリーンショットは、利用者に表示されるワークスペースの例です。インターフェイスは進化しているため、現在利用者に表示される内容とは異なる場合があります。たとえば、ページ上部に「Workspace」ではなく、「StoreFront」と表示されるようになっています。



SaaS アプリ

SaaS アプリへのセキュリティ保護されたアクセス機能によって、統合されたユーザーエクスペリエンスで公開 SaaS アプリをユーザーに提供できます。SaaS アプリはシングルサインオンで利用できます。管理者は、特定の Web サイトや Web サイトカテゴリへのアクセスをフィルター処理することで、マルウェアやデータ漏えいから組織のネットワークやエンドユーザーデバイスを保護できるようになりました。

Windows 向け Citrix Workspace アプリは、アクセス制御サービスを使用した SaaS アプリの使用をサポートしま

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

す。このサービスにより、管理者は一貫したエクスペリエンスを提供し、シングルサインオンを統合し、コンテンツ検査を利用することができます。

SaaS アプリをクラウドで提供する利点は次のとおりです:

- シンプルな構成 - 操作、更新、使用が簡単です。
- シングルサインオン - シングルサインオンで簡単にログオンできます。
- さまざまなアプリの標準テンプレート - 一般的なアプリをテンプレートを使用して構成できます。

前提条件:

- シングルサインオン機能を適用するには、SaaS アプリが SAML 2.0 認証をサポートしている必要があります。
- Citrix Enterprise Browser（旧称 Citrix Workspace Browser）が SaaS アプリケーションのレンダリングで使用されるように、アクセス制御サービスで ［セキュリティ強化を有効にする］オプションを有効にする必要があります。このオプションが有効になっていない場合、SaaS アプリはクライアントに設定されたデフォルトのブラウザーを使用して起動されます。

> 注:
>
> Citrix Workspace アプリは、オンプレミス環境とクラウド環境の両方から公開されたアプリおよびデスクトップを集約して、ユーザーエクスペリエンスを統合します。

Citrix Workspace アプリには、SaaS アプリを起動するための Citrix Secure Browser が組み込まれています。Citrix Secure Browser が組み込まれた Chromium 埋め込みフレームワークはバージョン 70 です。これによって、セキュアな SaaS アプリにアクセスするときに、より快適なユーザーエクスペリエンスを実現できます。

> 注:
>
> - Web 向け Workspace の場合、SaaS アプリは、Citrix Secure Browser ではなく、クライアントで設定されたデフォルトのブラウザーでのみ起動されます。
> - ICA セッションアプリとセキュリティ保護された SaaS アプリのユーザーエクスペリエンスが異なる場合があります。

Citrix Secure Browser ではツールバー、クリップボード、印刷、ダウンロード、透かしなどの操作を使用できます。これらの操作は、アクセス制御サービスのポリシー構成で定義されている Citrix Workspace アプリに適用されます。

Citrix Secure Browser を使用して実行できる操作:

ツールバー - アプリでツールバーオプションを有効にすると、起動したアプリで「戻る」、「進む」、「更新」オプションを表示できます。ツールバーには、クリップボード操作を含む省略記号も表示されます。

クリップボード - アプリでクリップボードアクセスを有効にすると、起動したアプリのツールバーに表示される切り取り、コピー、貼り付けのオプションを使用できます。このオプションを無効にすると、カット、コピー、貼り付けのオプションが灰色表示になります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

印刷 - 起動したアプリで印刷オプションを有効にすると、印刷コマンドを実行できます。無効にすると、起動したアプリに印刷オプションは表示されません。

ナビゲーション - ナビゲーションオプションを有効にすると、起動されたアプリのツールバーに「次へ」および「戻る」アイコンが表示されます。

ダウンロード - ダウンロードオプションを有効にすると、起動したアプリからファイルをダウンロードできます。起動したアプリを右クリックし、［名前を付けて保存］を選択します。保存先を選択して、［ダウンロード］をクリックします。

> 注:
>
> ファイルをダウンロードすると、ダウンロード状況を示す進行状況バーは表示されませんが、ダウンロードは正常に完了します。

透かし - 透かしオプションを有効にすると、起動したアプリに、クライアントマシンのユーザー名と IP アドレスを含む透かしが表示されます。透かしは半透明で、他の情報を表示するために編集することはできません。

GPO を使用したキャッシュの構成:

複数のユーザーが同じデバイスを使用してセキュアな SaaS アプリにログインすると、1 ユーザーのキャッシュが次のユーザーに適用され、ユーザー間で閲覧情報を共有することになります。

この問題を回避するため、Citrix Workspace アプリに新しいグループポリシーオブジェクト（GPO）管理ポリシーが導入されました。このポリシーを使用すると、ローカルデバイスにブラウザーのキャッシュを保存することはできません。

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］> ［**Citrix Workspace**］> ［**Citrix Secure Browser**］の順に移動します。
3. ［キャッシュ］ポリシーを選択します。
   注：デフォルトでは、このポリシーは ［有効］に設定されています。
4. 無効にするには、［無効］を選択して ［適用］、［**OK**］をクリックします。
5. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

制限事項:

1. 印刷オプションを有効にしてダウンロードを無効にした公開アプリを起動し、起動したアプリで印刷コマンドを発行すると、ダウンロード機能が制限されている場合でも PDF を保存できることがあります。ダウンロード機能を厳密に無効にするには、印刷オプションを無効にします。
2. アプリに埋め込まれた動画が機能しないことがあります。

ワークスペース構成について詳しくは、Citrix Cloud の「ワークスペース構成」を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

PDF 印刷

前提条件:

- Citrix Workspace アプリバージョン 1808 以降。
- Citrix Virtual Apps and Desktops バージョン 7 1808 以降。
- 少なくとも 1 つの PDF ビューアがコンピューターにインストールされている。

PDF 印刷を有効にするには:

1. Delivery Controller で Citrix Studio を使用して、左ペインの ［ポリシー］ノードを選択します。ポリシーを作成するか、既存のポリシーを編集することができます。
2. ［**PDF** ユニバーサルプリンターの自動作成］ポリシーを ［有効］にします。

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

制限事項:

- PDF の表示と印刷は、Microsoft Edge ブラウザーではサポートされていません。

Windows Continuum を使用して Windows 10 のタブレットモードを拡張

Windows Continuum は、クライアントデバイスの使用方法に対応する Windows 10 の機能です。Windows 向け Citrix Workspace アプリバージョン 4.10 以降では、モードの動的変更を含む Windows Continuum がサポートされています。

タッチ操作可能なデバイスの場合、キーボードまたはマウスが接続されていないと、Windows 10 VDA はタブレットモードで起動します。キーボード、マウス、またはその両方が接続されている場合は、デスクトップモードで起動します。Surface Pro のような 2 in 1 デバイスの画面やクライアントデバイスでキーボードを接続したり、接続解除したりすると、タブレットモードとデスクトップモードが切り替わります。詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「タッチスクリーンデバイス用タブレットモード」を参照してください。

Windows 10 VDA は、セッションに接続または再接続されると、タッチ操作可能なクライアントデバイス上でキーボードまたはマウスを検出します。また、セッション中にキーボードやマウスの接続や接続解除も検出します。この機能は VDA 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、Citrix Studio を使用して ［タブレットモードの切り替え］ポリシーを変更します。

タブレットモードでは、タッチスクリーンにより適した以下のユーザーインターフェイスが提供されます。

- やや大きめのボタン
- スタート画面や開始したすべてのアプリケーションを全画面で開く
- タスクバーに［戻る］ボタンを表示
- タスクバーからアイコンを削除

デスクトップモードでは、PC でキーボードとマウスを使用するのと同じように操作できる従来のユーザーインターフェイスが提供されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> Web 向け Workspace は Windows Continuum の機能をサポートしていません。

相対マウス

相対マウスのサポートでは、マウスの絶対位置ではなく相対位置を読み取るオプションを提供します。この機能は、マウスの絶対位置ではなく相対位置の入力を必要とするアプリケーションに必要です。

> 注
>
> この機能を適用できるのは、公開デスクトップセッションのみです。

レジストリエディターまたは default.ica ファイルを使用してこの機能を構成すると、セッションが終了した後も設定は保持されます。

以下のように、レジストリを使用してユーザー単位およびマシン単位でこの機能の可用性を制御できます:

レジストリエディターを使用した相対マウスの構成

この機能を構成するには、次のレジストリキーが適用されるよう設定し、セッションを再起動して変更を有効にします:

この機能をセッション単位で使用できるようにする場合:
`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse`

この機能をユーザー単位で使用できるようにする場合:
`HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse`

```
1 - Name: Mouse
2 - Type: REG_SZ
3 - Value: True
```

> 注:
>
> - レジストリエディターで設定した値は、ICA ファイルの設定よりも優先されます。
> - HKEY_LOCAL_MACHINE と HKEY_CURRENT_USER は同じ値を設定する必要があります。これらの値が異なると、競合が発生する可能性があります。

デフォルトの**.ica** ファイルを使用した相対マウスの構成

1. default.ica ファイルを開きます。このファイルは通常`C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica`にあります。ここで、sitename はストアの作成時に指定した名前で

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

す。StoreFront ユーザーの場合、default.ica ファイルは通常、C:\inetpub\wwwroot\Citrix\<Storename>\App_Data**default.ica**にあります。ここで、storename はストアの作成時に指定した名前です。

2. WFClient セクションに「RelativeMouse」という名前で新しいキーを追加し、そのデータ値を JSON オブジェクトとして同じ構成に設定します。
3. 必要に応じて値を設定します。
   - true –相対マウスを有効にする
   - false –相対マウスを無効にする
4. 変更を保存するには、セッションを再起動します。

> 注:
>
> レジストリエディターで設定した値は、ICA ファイルの設定よりも優先されます。

Desktop Viewer から相対マウスを有効にする

1. Citrix Workspace アプリにログオンします。
2. 公開デスクトップセッションを開始します。
3. Desktop Viewer のツールバーで ［基本設定］をクリックします。

   ［Citrix Workspace - 基本設定］ウィンドウが開きます。
4. ［接続］をクリックします。
5. ［相対マウスの設定］で ［相対マウスを使用する］をオンにします。
6. ［適用］、［**OK**］の順にクリックします。

> 注:
>
> Desktop Viewer から相対マウスを構成すると、セッション単位のみで適用されます。

ハードウェアのデコード

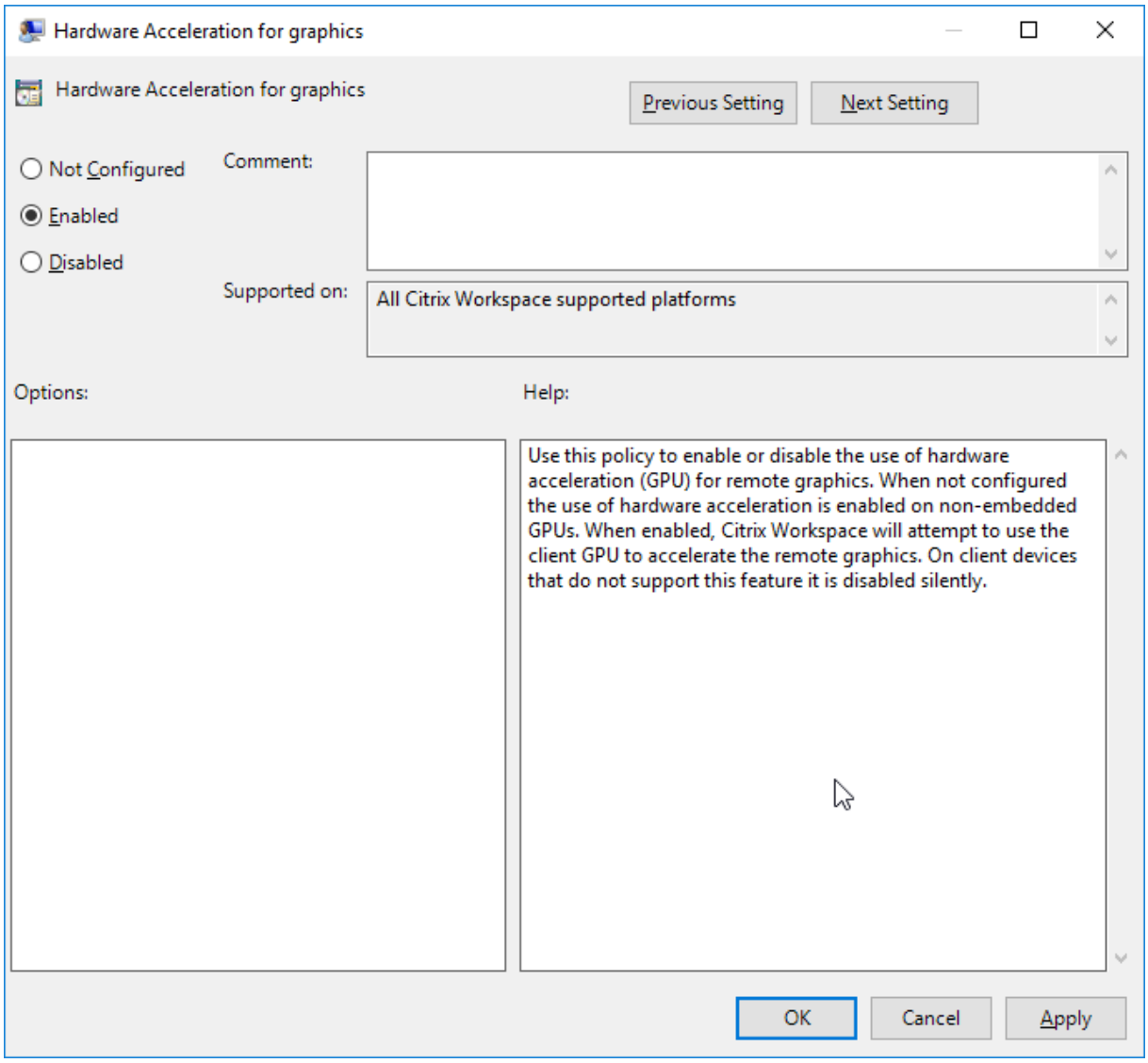
Citrix Workspace アプリ（HDX Engine 14.4 を含む）を使用する場合、クライアントで利用できる場合にはいつでも H.264 デコードに GPU を使用できます。GPU デコードで使用される API レイヤーは DirectX Video Acceleration です。

Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを使用してハードウェアのデコードを有効にするには:

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. ［コンピューターの構成］ノードで、［管理用テンプレート］、［**Citrix Workspace**］、［ユーザーエクスペリエンス］の順に移動します。
3. ［グラフィックのハードウェアアクセラレーション］を選択します。
4. ［有効］を選択して、［適用］および ［**OK**］をクリックします。



ポリシーが適用され、ハードウェアアクセラレーションがアクティブな ICA セッションで使用されているかを確認するには、次のレジストリキーを確認します。

レジストリのパス: `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender`

> ヒント
>
> **Graphics_GfxRender_Decoder** および **Graphics_GfxRender_Renderer** は 2 である必要があります。値が 1 の場合、CPU ベースのデコードが使用されています。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ハードウェアデコード機能が使用されている場合、次の制限事項を考慮してください。

- クライアントに GPU が 2 つあり、モニターの 1 つが 2 つ目の GPU でアクティブな場合、CPU デコードが使用されます。
- Windows Server 2008 R2 が動作する Citrix Virtual Apps 7.x サーバーに接続する場合、ユーザーの Windows デバイスではハードウェアデコードを使用しないことをお勧めします。これが有効な場合、文字列を強調表示する場合のパフォーマンスの低下やちらつきの問題が発生します。

マイク入力

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 会議などのリアルタイムのアクティビティ。
- 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。

Citrix Workspace アプリのユーザーは、コネクションセンターを使用して、デバイスに付属しているマイクを使用するかどうか選択することができます。Citrix Virtual Apps and Desktops および Citrix DaaS ユーザーも、ビューアの［基本設定］ダイアログボックスを使用してマイクおよび Web カメラを無効にできます。

マルチモニターサポート

Windows 向け Citrix Workspace アプリで最大 8 台のモニターを使用できます。

マルチモニター環境では、各モニターの製造元により解像度が異なる場合があります。また、セッション中にモニターの解像度や向きが変更されることもあります。

セッションを複数のモニター上に表示する場合、以下の 2 つのモードがあります。

- 全画面モード。セッションはマルチモニター全体に表示されます。ローカルでの場合と同様に、アプリケーションウィンドウが表示領域全体に最大化されます。

  Citrix Virtual Apps and Desktops および **Citrix DaaS**： Desktop Viewer ウィンドウをマルチモニターのいずれかの矩形表示領域内に表示するには、隣接するモニターにかかるようにウィンドウのサイズを変更して ［最大化］をクリックします。

- ウィンドウモード。単一のモニターがセッション用に使用されます。アプリケーションウィンドウは個々のモニター上に最大表示されません。

Citrix Virtual Apps and Desktops および **Citrix DaaS**：同じ割り当て（デスクトップグループ）に含まれるデスクトップを続けて起動すると、ウィンドウ設定が保持され、デスクトップが同じモニターに表示されます。矩形配置構成のマルチモニター環境では、複数の仮想デスクトップを 1 つのデバイス上で表示できます。デバイスのプライマリモニターを仮想アプリと仮想デスクトップのセッションで使用する場合は、セッションでもそのモニターがプラ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

イマリモニターになります。そうでない場合は、セッション内の最も小さい番号のモニターがプライマリモニターになります。

マルチモニター環境をサポートするには、次の条件を満たしている必要があります。

- ユーザーデバイスの構成でマルチモニターがサポートされている。
- オペレーティングシステムが各モニターを検出できる。Windows プラットフォームでモニターを検出できるかどうかは、［設定］ > ［システム］に移動し、［ディスプレイ］をクリックして、各モニターが別々に表示されていることを確認します。
- モニターが検出された後は、次の作業を行います。
  - **Citrix Virtual Desktops**： **Citrix** マシンポリシーの［表示メモリの制限］設定を使用して、グラフィックメモリの制限を構成します。
  - **Citrix Virtual Apps**：インストールした Citrix Virtual Apps サーバーのバージョンに応じて、以下の操作を行います：
    - **Citrix** ポリシーの［表示メモリの制限］設定を使用して、グラフィックメモリの制限を構成します。
    - Citrix Virtual Apps サーバー用 Citrix 管理コンソールの左ペインでサーバーファームを選択し、タスクペインで ［サーバーファームのプロパティの変更］、［すべてのプロパティの変更］、［サーバーのデフォルト設定］、［HDX Broadcast］、［表示設定］の順に選択します（または［サーバーファームのプロパティの変更］、［すべてのプロパティの変更］、［サーバーのデフォルト設定］、［ICA］、［表示設定］の順に選択します）。そして、［各セッションのグラフィックで使用する最大メモリ］を設定します。

この値を、グラフィックメモリを提供するのに十分なサイズに設定します（単位はキロバイト）。このボックスの値が必要なサイズに満たないと、公開リソースが一部のモニター上でしか表示されません。

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

1. Desktop Viewer を選択し、下向き矢印をクリックします。
2. ［ウィンドウ］を選択します。
3. Citrix Virtual Desktops の画面を 2 つのモニターの間にドラッグします。各モニターに画面の約半分が表示されていることを確認してください。
4. Citrix Virtual Desktops のツールバーで、［フルスクリーン］を選択します。

   画面が両方のモニターに拡張されます。

Citrix Virtual Apps and Desktops および Citrix DaaS のセッションのグラフィックメモリ要件の計算については、Knowledge Center のCTX115637を参照してください。

プリンター

ユーザーがプリンター設定を上書きするには

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. ユーザーデバイス上で、アプリケーションの ［印刷］ダイアログボックスを開き、［プロパティ］をクリックします。
2. ［クライアント設定］タブで ［高度な最適化］をクリックし、［イメージ圧縮］および［イメージおよびフォントキャッシュ］オプションの設定を変更します。

スクリーンキーボードの制御

Windows タブレットから仮想アプリケーションおよびデスクトップへのタッチ操作によるアクセスを有効にするため、テキスト入力フィールドがアクティブになったり、デバイスがテントまたはタブレットモードになったりすると、Citrix Workspace アプリによって自動的にスクリーンキーボードが表示されます。

一部のデバイスおよび一部の環境下では、Citrix Workspace アプリがデバイスのモードを正確に検出できず、必要時にスクリーンキーボードが表示されないことがあります。

コンバーチブルデバイスを使用しているときにスクリーンキーボードが表示されないようにするには、`HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver` で REG_DWORD の値 `DisableKeyboardPopup` を作成し、値を 1 に設定します。

> 注:
>
> x64 マシンで、`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver` に値を作成します。

キーは以下のような異なる 3 種のモードに設定できます。

- 自動: AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0
- 常にポップアップ（スクリーンキーボード）: AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0
- ポップアップしない（スクリーンキーボード）: AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1

キーボードショートカット

Citrix Workspace アプリで特定の機能を実行するキーの組み合わせを構成できます。キーボードショートカットのポリシーが有効な場合、Citrix ショートカットキーのマッピング、Windows ショートカットキーの動作、およびセッションでのキーボードの種類を指定できます。

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］> ［**Citrix** コンポーネント］> ［**Citrix Workspace**］> ［ユーザーエクスペリエンス］の順に移動します。
3. キーボードショートカットポリシーを選択します。
4. ［有効］と目的のオプションを選択します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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

32 ビットカラーアイコンのサポート:

Citrix Workspace アプリでは 32 ビット High Color アイコンがサポートされ、**Citrix** コネクションセンターに表示されるアプリケーションのアイコンに適した色数が自動的に選択されます。シームレスアプリケーションを実行しているときに［スタート］メニューとタスクバーに表示されるアプリケーションのアイコンも、同様に処理されます。

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

優先する深さを設定するには、`TWIDesiredIconColor`という文字列レジストリキーを`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences`に追加して、必要な値に設定します。定義できるアイコンの色数は、4、8、16、24、および 32 ビット/ピクセルです。ネットワーク接続が低速な場合は、ユーザーはより少ない色数を選択できます。

Desktop Viewer

企業組織にはそれぞれ異なるニーズがあります。ユーザーが仮想デスクトップにアクセスする方法の要件は、ユーザーによって、そして企業ニーズが展開するにつれて変化する可能性があります。ユーザーが仮想デスクトップに接続したり接続を構成したりするときの手順は、管理者による Windows 向け Citrix Workspace アプリのセットアップ方法によって異なります。

ユーザーが仮想デスクトップを操作する必要がある場合は、**Desktop Viewer** を使用します。ユーザーの仮想デスクトップには公開仮想デスクトップを使用でき、共有または専用デスクトップのいずれでも可能です。このアクセスシナリオでは、Desktop Viewer ツールバー機能により、ユーザーが仮想デスクトップをローカルデスクトップ上のウィンドウ内に開いて、必要に応じて仮想デスクトップの表示領域や表示サイズを変更できます。ユーザーは必要に応じて設定を変更でき、同じユーザーデバイス上で複数の Citrix Virtual Apps and Desktops および Citrix DaaS 接続を使用して複数の仮想デスクトップを実行できます。

> 注:
>
> 仮想デスクトップの解像度を変更する場合は、Citrix Workspace アプリを使用します。Windows コントロールパネルで解像度を変更することはできません。

Desktop Viewer でのキーボード入力

Desktop Viewer セッションでは、**Windows** ロゴ + L キーはローカルコンピューターに送信されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ctrl+Alt+Del キーは、ローカルコンピューターに送信されます。

通常、Microsoft 社のユーザー補助機能である固定キー、フィルターキー、および切り替えキー機能を有効にするキーはローカルコンピューターに送信されます。

Desktop Viewer のユーザー補助機能として、Ctrl + Alt + Break キーを押すと、ポップアップウィンドウで Desktop Viewer ツールバーが開きます。

Ctrl + Esc キーは、リモートの仮想デスクトップに送信されます。

> 注:
>
> デフォルトでは、Desktop Viewer を最大化した場合は Alt + Tab キーを押すとセッション内のウィンドウ間でフォーカスが切り替わります。Desktop Viewer をウィンドウ内に表示している場合は、Alt + Tab キーを押すとセッション外のウィンドウ間でフォーカスが切り替わります。

ホットキーシーケンスは、Citrix により設計されたキーの組み合わせです。たとえば、Ctrl + F1 シーケンスは Ctrl + Alt + Del キーを再現し、Shift + F2 はアプリケーションの全画面モードとウィンドウモードを切り替えます。Desktop Viewer で表示されている仮想デスクトップ（つまり、仮想アプリと仮想デスクトップのセッション）ではホットキーシーケンスを使用できませんが、公開アプリケーション（つまり、Citrix Virtual Apps セッション）ではこれを使用できます。

仮想デスクトップ

仮想デスクトップセッション内から同じ仮想デスクトップに接続することはできません。これを行うと、既存のデスクトップセッションが切断されます。そのため、Citrix では次のことをお勧めします:

- 管理者は、仮想デスクトップ上のクライアントが、同じデスクトップを公開しているサイトに接続するように構成しない。
- ユーザーは、同じデスクトップをホストしているサイトを参照しない（自動的に既存のセッションに再接続するようサイトが構成されている場合）。
- ユーザーは、同じデスクトップをホストしているサイトを参照したりそのデスクトップを起動したりしない。

仮想デスクトップとして動作するコンピューターにローカルでログオンするユーザーは、そのデスクトップへの接続がブロックされます。

ユーザーが仮想デスクトップ内から（Citrix Virtual Apps で公開された）仮想アプリケーションに接続し、別の管理者が Citrix Virtual Apps を管理している環境では、ローカルのデバイスが仮想デスクトップセッションおよび公開アプリケーションセッションで同様にマップされるように、Citrix Virtual Apps 管理者と共同してデバイスマッピングを定義することをお勧めします。仮想デスクトップセッションではローカルドライブがネットワークドライブとして表示されるため、Citrix Virtual Apps 管理者がドライブマッピングポリシーでネットワークドライブ（リモートドライブ）のマッピングを許可する必要があります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

状態インジケーターのタイムアウト

ユーザーがセッションを起動しているときに状態インジケーターが表示される時間を変更できます。タイムアウト期間を変更するには、REG_DWORD 値の SI INACTIVE MS を HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\で作成します。状態インジケーターをすぐに非表示したい場合は、REG_DWORD 値を 4 に設定します。

カスタマーエクスペリエンス向上プログラム（**CEIP**）

収集データ	説明	データの利用目的
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、Windows 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取り扱い、Citrix Trust Centerで利用できる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。

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

次の方法で、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（ただし、以下の 2 番目の表で * が付けられた 2 つデータ要素は除きます）:

1. システムトレイの Citrix Workspace アプリアイコンを右クリックします。
2. ［高度な設定］を選択します。
   ［高度な設定］ダイアログボックスが開きます。
3. ［データ収集］を選択します。
4. ［いいえ］を選択して CEIP を無効にするか、参加を見送ります。
5. ［**Save**］をクリックします。

または、次のレジストリエントリに移動し、推奨されている値を設定します:

パス: `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

キー: `Enable_CEIP`

値: `False`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> データ収集ダイアログで ［**No Thanks**］を選択するか、`Enable_CEIP`キーを`False`に設定したあと、Google Analytics によって収集された最後の 2 つの CEIP データ要素（オペレーティングシステムのバージョンと Citrix Workspace アプリのバージョン）の送信を無効にする場合は、次のレジストリエントリに移動し、推奨されている値を設定します:

パス: `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

キー: `DisableHeartbeat`

値: `True`

Citrix が収集する特定の CEIP データ要素は次のとおりです:

オペレーティングシステムバージョン	Citrix Workspace アプリのバージョン	接続されている外部デバイス	画面解像度
Flash のバージョン	Desktop Lock 構成	タッチ対応	認証構成
セッションの起動方法	グラフィック構成	Desktop Viewer 構成	印刷
接続エラー	起動時間	Citrix Workspace アプリの言語	VDA 情報
SSON の状態	インストーラーの状態	インストール時間	接続プロトコル
Internet Explorer バージョン			

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

オペレーティングシステムバージョン *	Citrix Workspace アプリのバージョン *	認証構成	Citrix Workspace アプリの言語
セッションの起動方法	接続エラー	接続プロトコル	VDA 情報
インストーラー構成	インストーラーの状態	クライアントのキーボードレイアウト	ストア構成
自動更新の設定	コネクションセンターの使用状況	App Protection 構成	

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

認証

November 3, 2023

セキュリティを最大限に高めるには、Citrix Workspace アプリと公開リソースの間の接続を保護します。次のタイプの認証を構成できます:

- ドメインパススルー
- スマートカード
- Kerberos パススルー

ドメインパススルー認証

シングルサインオンを使用すると、認証することで、仮想アプリと仮想デスクトップを再認証する必要なく使用できます。

Citrix Workspace アプリにログインすると、資格情報と列挙されたリソースを StoreFront に渡すことができます。

以前のリリースでは、Google Chrome、Microsoft Edge、または Mozilla FireFox を使用中、機能を有効にしていなくても、シングルサインオンセッションを開始することができました。

バージョン 1905 以降、すべての Web ブラウザーで、グループポリシーオブジェクト管理用テンプレートを使用してシングルサインオンを構成する必要があります。グループポリシーオブジェクト管理用テンプレートを使用したシングルサインオンの構成について詳しくは、「Citrix Gateway でのシングルサインオンの構成」を参照してください。

新規インストールまたはアップグレードの両方で次のいずれかのオプションを使用して、シングルサインオンを構成できます:

- コマンドラインインターフェイス
- グラフィカルユーザーインターフェイス（GUI）

新規インストール中のシングルサインオンの構成

新規インストール中のシングルサインオンの構成:

1. StoreFront または Web Interface で構成します。
2. Delivery Controller で XML 信頼サービスを構成します。
3. Internet Explorer の設定を変更します。
4. Citrix Workspace アプリのインストールでシングルサインオンを構成します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

StoreFront または **Web Interface** でのシングルサインオンの構成

Citrix Virtual Apps and Desktops の展開の種類により、StoreFront または Web Interface で管理コンソールを使用してシングルサインオンを構成できます。

以下の表で異なる使用例とそれぞれの構成を参照します:

使用例	構成の詳細	追加情報
StoreFront または Web Interface での構成	Citrix Studio を起動して、［ストア］>［認証方法の管理］に移動して ［ドメインパススルー］を有効にします。	シングルサインオンが構成されていない場合、Citrix Workspace アプリでは、認証方法が自動的に ［ドメインパススルー］から ［ユーザー名とパスワード］に切り替えられます（利用可能な場合）。
Web 向け Workspace が必要な場合	［ストア］>［**Workspace for Websites**］>［認証方法の管理］で［ドメインパススルー］を有効にします。	シングルサインオンが構成されていない場合、Citrix Workspace アプリでは、認証方法が自動的に ［ドメインパススルー］から ［ユーザー名とパスワード］に切り替えられます（利用可能な場合）。
StoreFront が構成されていない場合	Web Interface が VDA で構成されている場合、[XenApp Services Sites］>［**Authentication Methods**］>［**Pass-through**］を有効にします。	Citrix Workspace アプリでシングルサインオンが構成されていない場合、認証方法は自動的に **Pass-through** から **Explicit** に切り替えられます（利用可能な場合）。

Citrix Gateway でのシングルサインオンの構成

グループポリシーオブジェクト管理用テンプレートを使用して Citrix Gateway でシングルサインオンを有効にします。

1. gpedit.msc を実行して、Citrix Workspace アプリの GPO 管理用テンプレートを開きます。
2. ［コンピューターの構成］ノードで、[管理用テンプレート] > [**Citrix** コンポーネント] > [**Citrix Workspace**] >［ユーザー認証］の順に移動します。
3. **Citrix Gateway** のシングルサインオンポリシーを選択します。
4. ［有効］をクリックします。
5. ［適用］、［**OK**］の順にクリックします。
6. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Delivery Controller で **XML** 信頼サービスを構成

Citrix Virtual Apps and Desktops および Citrix DaaS（Citrix Virtual Apps and Desktops サービスの新名称）の Delivery Controller で管理者として次の PowerShell コマンドを実行します:

```
asnp Citrix* Set-BrokerSite -TrustRequestsSentToTheXmlServicePort
$True
```

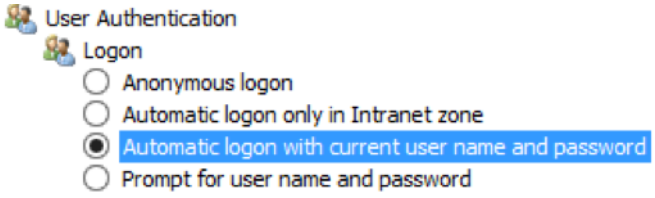
Internet Explorer 設定の変更

1. Internet Explorer を使用して信頼済みサイトの一覧に StoreFront サーバーを追加します。これを行うには、以下の手順に従います。

   a) ［コントロール］パネルで ［インターネットオプション］を起動します。
   b) ［セキュリティ］>［ローカルイントラネット］を選択し、［サイト］をクリックします。［ローカルイントラネット］ウィンドウが開きます。
   c) ［詳細設定］を選択します。
   d) 適切な HTTP または HTTPS プロトコルを使用して、StoreFront または Web Interface の FQDN の URL を追加します。
   e) ［適用］、［**OK**］の順にクリックします。

2. **Internet Explorer** で ［ユーザー認証］の設定を変更します。これを行うには、以下の手順に従います。

   a) ［コントロール］パネルで ［インターネットオプション］を起動します。
   b) ［セキュリティ］タブ >［信頼済みサイト］を選択します。
   c) ［レベルのカスタマイズ］をクリックします。［セキュリティ設定 - 信頼されたゾーン］ウィンドウが開きます。
   d) ［ユーザー認証］ウィンドウで、［現在のユーザー名とパスワードで自動的にログオンする］を選択します。



   a) ［適用］、［**OK**］の順にクリックします。

コマンドラインインターフェイスを使用したシングルサインオンの構成

/`includeSSON`スイッチを使用して Windows 向け Citrix Workspace アプリをインストールし、再起動して変更を有効にします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> Windows 向け Citrix Workspace アプリがシングルサインオンコンポーネントなしでインストールされている場合、/includeSSONスイッチを使用して最新バージョンにアップグレードすることはできません。

グラフィカルユーザーインターフェイスを使用したシングルサインオンの構成

1. Citrix Workspace アプリインストールファイル（CitrixWorkspaceApp.exe）を検索します。
2. CitrixWorkspaceApp.exeをダブルクリックしてインストーラーを起動します。
3. [シングルサインオンを有効化] ウィザードで、[シングルサインオンを有効化] オプションを選択します。
4. [次へ] をクリックし、ウィザードの指示に従ってインストールを完了します。

Citrix Workspace アプリを使用して、ユーザー資格情報を指定することなくログオンできるようになりました。

Citrix Workspace for Web でのシングルサインオンの構成

グループポリシーオブジェクト管理用テンプレートを使用して、Web 向け Workspace のシングルサインオンを構成できます。

1. gpedit.msc を実行して、Web 向け Workspace の GPO 管理用テンプレートを開きます。
2. [コンピューターの構成] ノードで、[管理用テンプレート] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [ユーザー認証] の順に移動します。
3. [ローカルユーザー名とパスワード] ポリシーを選択して [有効] に設定します。
4. [パススルー認証を有効にします] をクリックします。このオプションを使用すると、Web 向け Workspace はリモートサーバーでの認証にログイン資格情報を使用できます。
5. [すべての **ICA** 接続にパススルー認証を許可します] をクリックします。このオプションは、すべての認証制限を省略し、すべての接続で資格情報のパススルーを許可します。
6. [適用]、[**OK**] の順にクリックします。
7. Web 向け Workspace のセッションを再起動して、この変更を適用します。

シングルサインオンが有効になっていることを確認するには、タスクマネージャーを起動し、ssonsvr.exeプロセスが実行中であることを確認します。

Active Directory を使用したシングルサインオンの構成

Active Directory を使用してシングルサインオン認証を構成できます。この場合、Microsoft System Center Configuration Manager などの展開ツールを使用する必要はありません。

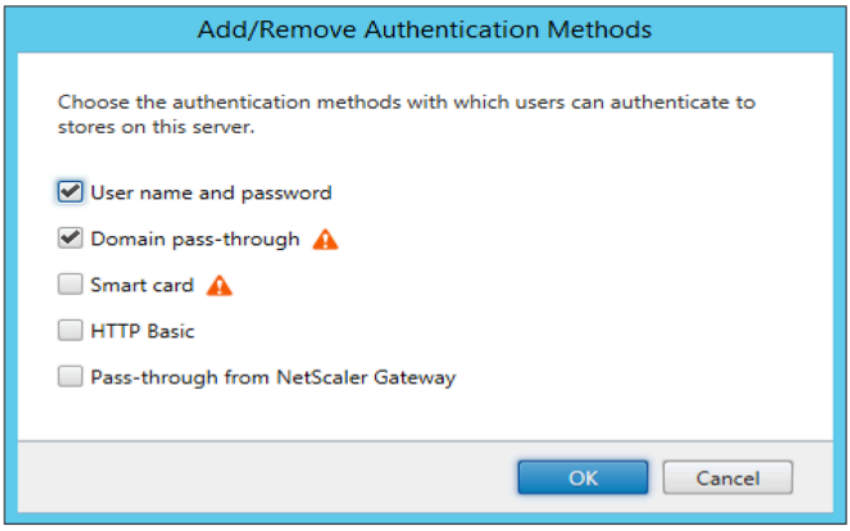
1. Citrix Workspace アプリインストールファイル（CitrixWorkspaceApp.exe）をダウンロードして適切なネットワーク共有に配置します。Citrix Workspace アプリをインストールする対象マシンからアクセス可能であることが必要です。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Windows 向け Citrix Workspace アプリのダウンロードページからCheckAndDeployWorkspacePerMachine.batテンプレートを入手します。
3. CitrixWorkspaceApp.exeの場所とバージョンを編集します。
4. **Active Directory** のグループポリシー管理コンソールでCheckAndDeployWorkspacePerMachineStartup.batをスタートアップスクリプトとして入力します。スタートアップスクリプトの展開について詳しくは、「Active Directory」のセクションを参照してください。
5. ［コンピューターの構成］ノードで ［管理用テンプレート］**>** ［テンプレートの追加と削除］に移動してicaclient.admファイルを追加します。
6. icaclient.admテンプレートの追加後、［コンピューターの構成］> ［管理用テンプレート］> [**Citrix** コンポーネント］> [**Citrix Workspace**］> ［ユーザー認証］に移動します。
7. ［ローカルユーザー名とパスワード］ポリシーを選択して ［有効］に設定します。
8. ［パススルー認証を有効にします］チェックボックスをオンにして ［適用］を選択します。
9. 変更を保存するには、マシンを再起動します。

StoreFront および **Web Interface** でのシングルサインオンの構成

StoreFront の構成　**Citrix Studio** を StoreFront サーバーで開いて ［認証］**>** ［認証方法の追加と削除］の順に選択します。［ドメインパススルー］を選択します。

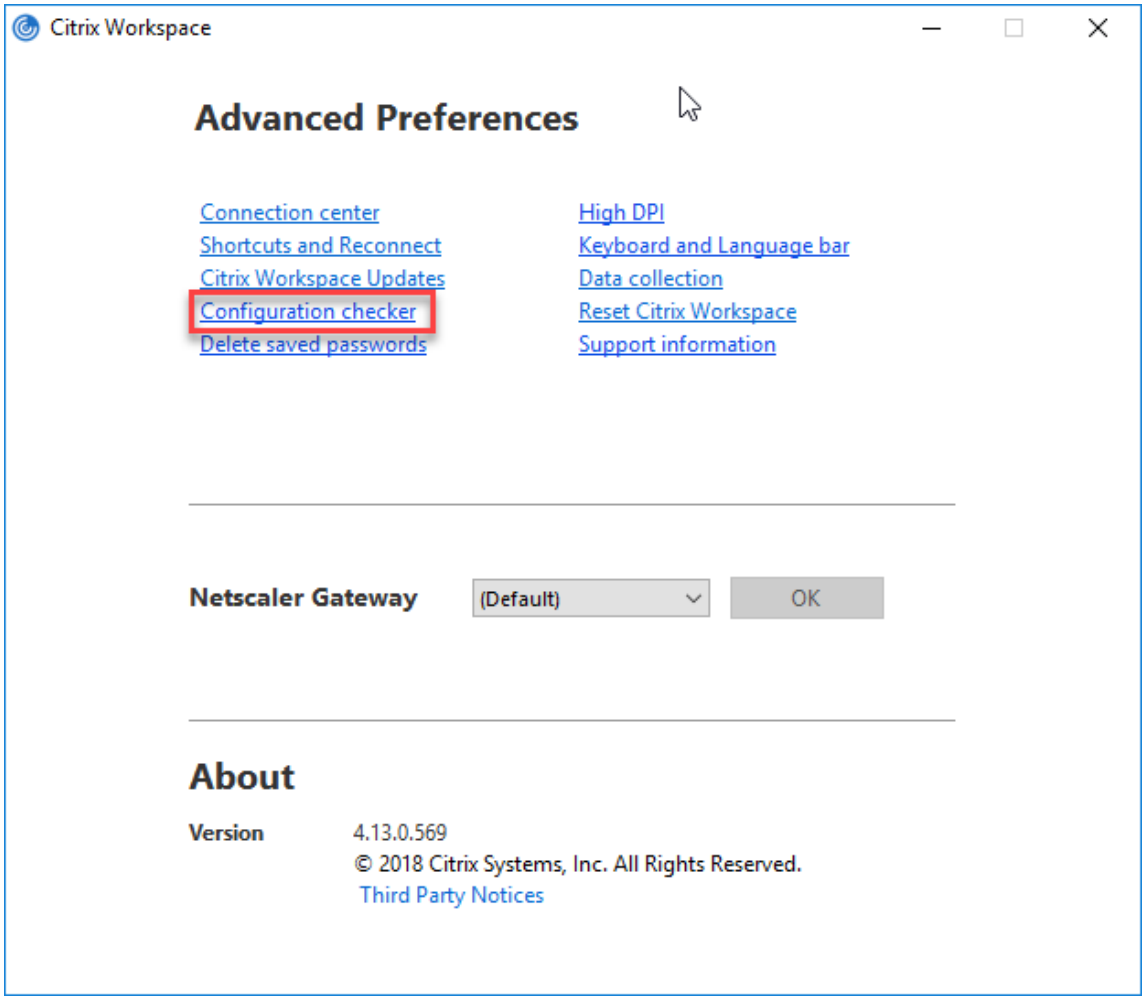


構成チェッカー

構成チェッカーで、シングルサインオンが正しく構成されていることを確認するためのテストを実行できます。テストはシングルサインオン構成の各チェックポイントに対して実行され、構成結果を表示します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 通知領域で Citrix Workspace アプリアイコンを右クリックし、［高度な設定］をクリックします。
   ［高度な設定］ダイアログボックスが開きます。
2. ［構成チェッカー］をクリックします。
   ［**Citrix** 構成チェッカー］ウィンドウが開きます。



3. ［選択］ペインで ［**SSONChecker**］チェックボックスをオンにします。
4. ［実行］をクリックします。テストの状態を示す進捗状況バーが表示されます。

［構成チェッカー］ウィンドウには次の列があります：

1. 状態：特定のチェックポイントでのテスト結果が表示されます。
   - 緑色のチェックマークは、チェックポイントが適切に構成されていることを示します。
   - 青色の I は、チェックポイントに関する情報を示します。
   - 赤色の X は、チェックポイントが適切に構成されていないことを示します。
2. プロバイダー：テストが実行されているモジュールの名前が表示されます。この場合は、シングルサインオンになります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. スイート：テストのカテゴリを示します。例：「インストール」。
4. テスト：実行中のテストの名前を示します。
5. 詳細：テストに関する詳細情報を提供します。

各チェックポイントおよび対応する結果の詳細を確認することができます。

以下のテストが実施されます：

1. シングルサインオンとともにインストール済み。
2. ログオン資格情報のキャプチャ。
3. ネットワークプロバイダーの登録：ネットワークプロバイダーの登録のテスト結果で緑色のチェックマークが表示されるのは、ネットワークプロバイダーの一覧で「Citrix Single Sign-on」が先頭に設定されている場合のみです。「Citrix Single Sign-On」が一覧の先頭以外の場所に表示されている場合、ネットワークプロバイダーの登録のテスト結果では青色の I と詳細情報が表示されます。
4. シングルサインオンプロセスが実行されている。
5. グループポリシー：デフォルトでは、このポリシーはクライアントで構成されます。
6. Internet Explorer のセキュリティゾーンの設定：［インターネットオプション］のセキュリティゾーンの一覧に Store/XenApp サービスの URL を追加していることを確認してください。
   セキュリティゾーンをグループポリシー経由で構成しており、そのポリシーを変更した場合、変更を有効にしてテストの正確な状態が表示されるようにするために、［高度な設定］ウィンドウを開き直す必要があります。
7. Web Interface/StoreFront の認証方法

> 注：
>
> - テスト結果は、Web 向け Workspace では適用されません。
> - 複数ストア設定の場合、認証方法のテストは構成済みのすべてのストアで実行されます。
> - テスト結果はレポートとして保存できます。デフォルトのレポート形式は.txt です。

［高度な設定］ウィンドウの［構成チェッカー］オプションを非表示にする

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. グループポリシーエディターで、［**Citrix** コンポーネント］>［**Citrix Workspace**］>［**Self Service**］>［**DisableConfigChecker**］の順に開きます。
3. ［有効］を選択すると、［高度な設定］ウィンドウで［構成チェッカー］オプションが表示されなくなります。
4. ［適用］、［**OK**］の順にクリックします。
5. `gpupdate /force`コマンドを実行します。

制限事項：

構成チェッカーの対象チェックポイントに、VDA 上の［Citrix XML Service への要求を信頼する］の構成は含まれません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ビーコンテスト　ビーコンチェッカーは、構成チェックユーティリティの一部です。これにより、ビーコンテストを実行して、ビーコン（ping.citrix.com）が到達可能かどうかを確認できます。このテストは、リソースの列挙が遅くなる理由として考えられる原因から、ビーコンが使用できないという可能性を排除するのに役立ちます。テストを実行するには、システムトレイの Citrix Workspace アプリを右クリックし、［高度な設定］>［構成チェッカー］を選択します。テスト一覧からビーコンチェッカーを選択して ［実行］をクリックします。

テスト結果は、次のいずれかになります:

- Reachable - Citrix Workspace アプリが正常にビーコンに通信できます。
- Not reachable - Citrix Workspace アプリはビーコンに通信できません。
- Partially reachable - Citrix Workspace アプリは、断続的にビーコンに通信できます。

Kerberos を使用したドメインパススルー認証

このトピックの内容は、Windows 向け Citrix Workspace アプリと StoreFront、Citrix Virtual Apps and Desktops および Citrix DaaS と間の接続にのみ適用されます。

Citrix Workspace アプリでは、スマートカードを使用する展開環境での Kerberos によるドメインパススルー認証がサポートされます。Kerberos とは、統合 Windows 認証（IWA）に含まれる認証方法の 1 つです。

Kerberos では、認証時に Citrix Workspace アプリのパスワードが使用されません。このため、トロイの木馬型の攻撃でユーザーデバイス上のパスワードが漏えいすることを避けることができます。ユーザーは、任意の認証方法を使用してログオンし、公開リソースにアクセスできます。たとえば、指紋リーダーなどの生体認証システムなどです。

スマートカード認証が構成された Citrix Workspace アプリ、StoreFront、Citrix Virtual Apps and Desktops、Citrix DaaS でスマートカードを使用してログオンすると、Citrix Workspace アプリは以下を実行します:

1. シングルサインオン中にスマートカード PIN を取得します。
2. IWA（Kerberos）を使用して StoreFront へのユーザー認証を行います。これによって StoreFront は、使用可能な Citrix Virtual Apps and Desktops および Citrix DaaS の情報を Workspace アプリに提供します。

   > 注
   >
   > 追加の PIN プロンプトが表示されるのを回避するために Kerberos を有効にします。Citrix Workspace アプリで Kerberos 認証を使用しない場合、StoreFront への認証にはスマートカード資格情報が使用されます。

3. HDX エンジンがスマートカードの PIN を VDA に渡します。これにより、ユーザーが Citrix Workspace アプリセッションにログオンできます。Citrix Virtual Apps and Desktops および Citrix DaaS が、要求されたリソースを配信します。

Citrix Workspace アプリで Kerberos 認証を使用する場合は、以下のように構成する必要があります。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Kerberos を使用するには、サーバーと Citrix Workspace アプリを、同じまたは信頼されている Windows Server ドメイン内に設置する必要があります。さらに、管理タスクを割り当てられるように、［Active Directory ユーザーとコンピューター］を使ってサーバーの信頼関係を構成する必要があります。
- ドメイン、Citrix Virtual Apps and Desktops および Citrix DaaS で Kerberos が有効になっている必要があります。セキュリティを強化するには、Kerberos 以外の IWA オプションを無効にして、ドメインで必ず Kerberos が使用されるようにします。
- リモートデスクトップサービス接続で、基本認証や保存されたログオン情報の使用、または常にユーザーにパスワードを入力させたりする場合、Kerberos によるログオンは使用できません。

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

スマートカードを使用する環境で **Kerberos** によるドメインパススルー認証

Citrix Virtual Apps and Desktops ドキュメントの「展開環境の保護」セクションでスマートカード情報を参照してください。

Windows 向け Citrix Workspace アプリのインストール時に、以下のコマンドラインオプションを指定します。

- `/includeSSON`

  これにより、ドメインに参加しているコンピューターにシングルサインオンコンポーネントがインストールされ、ワークスペースの IWA（Kerberos）による StoreFront への認証が有効になります。シングルサインオンコンポーネントは、スマートカードの PIN を格納します。次に、HDX エンジンがこの PIN を使用して、Citrix Virtual Apps and Desktops および Citrix DaaS がスマートカードハードウェアと資格情報にアクセスできるようにします。Citrix Virtual Apps and Desktops および Citrix DaaS は、自動的にスマートカードから証明書を選択して、HDX エンジンから PIN を取得します。

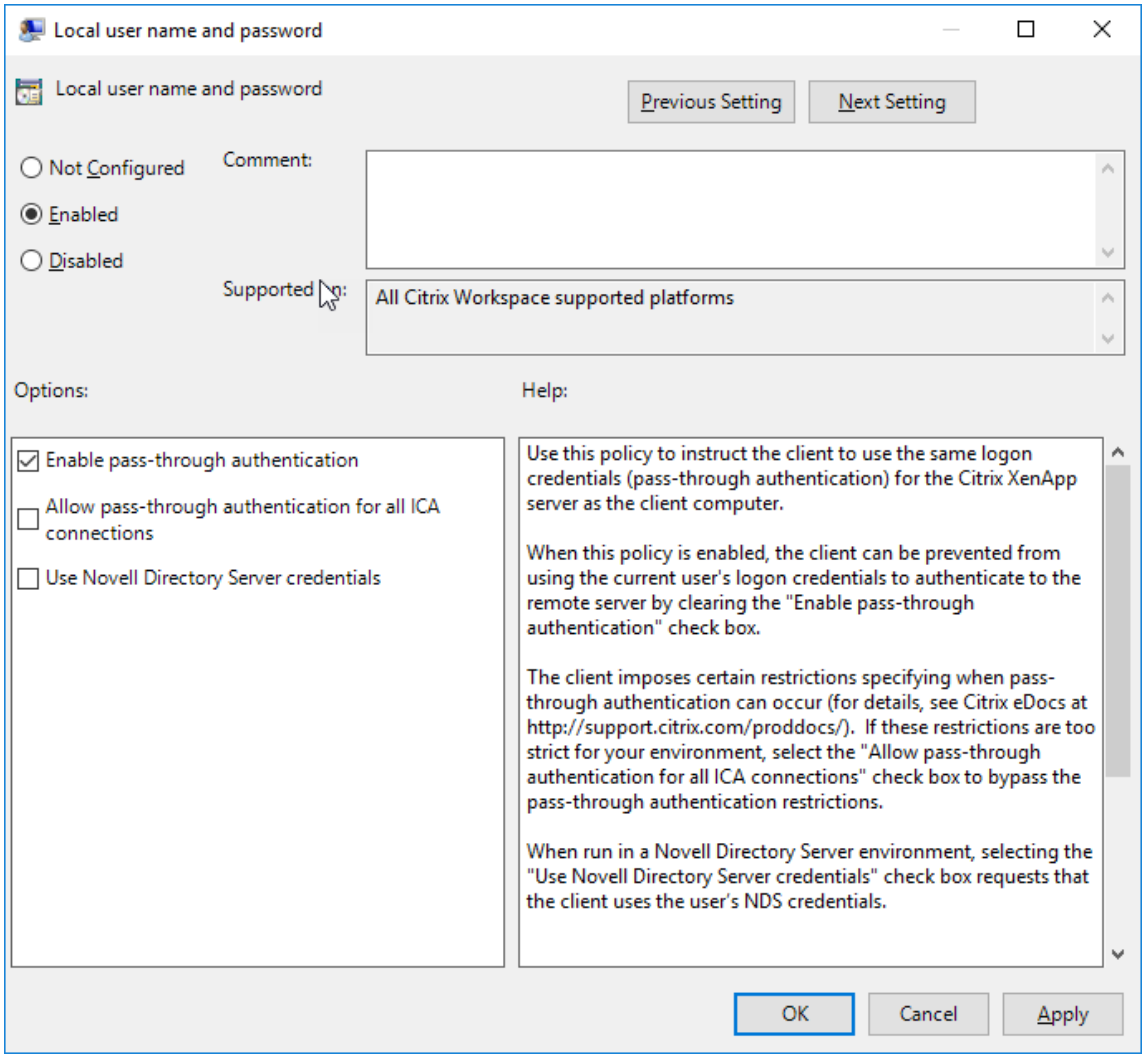
  関連オプション「`ENABLE\\_SSON`」は、デフォルトで有効になっています。

セキュリティポリシーにより、デバイスでシングルサインオンを有効にできない場合は、グループポリシーオブジェクト管理用テンプレートを使用して Citrix Workspace アプリを構成します。

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. ［管理用テンプレート］>［**Citrix** コンポーネント］>［**Citrix Workspace**］>［ユーザー認証］>［ローカルユーザー名とパスワード］を選択します。
3. ［パススルー認証を有効にします］チェックボックスをオンにします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

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



StoreFront を構成するには:

StoreFront サーバーの認証サービスを構成するときに、［ドメインパススルー］オプションをオンにします。これにより、統合 Windows 認証が有効になります。［スマートカード］オプションは、スマートカードを使用して StoreFront に接続する非ドメイン参加のクライアントをサポートする場合のみオンにします。

StoreFront でスマートカードを使用する場合は、StoreFront ドキュメントの「認証サービスの構成」を参照してください。

スマートカード

Windows 向け Citrix Workspace アプリでは、以下のスマートカード認証がサポートされます:

- パススルー認証（シングルサインオン） - ユーザーが Citrix Workspace アプリにログオンするときに使用するスマートカードの資格情報を取得します。取得した資格情報は以下のように使用されます:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - ドメインに属しているデバイスのユーザーがスマートカードの資格情報で Citrix Workspace アプリにログオンした場合、仮想デスクトップやアプリケーションの起動時に資格情報を再入力する必要はありません。
  - ドメインに属していないデバイスで実行している Citrix Workspace アプリがスマートカードの資格情報を使用している場合、デスクトップやアプリの起動時に資格情報を再入力する必要があります。

  パススルー認証を使用するには、StoreFront および Citrix Workspace アプリ両方での構成が必要です。

- **2** モード認証 - 認証方法として、スマートカードと、ユーザー名およびパスワードの入力を選択できます。この機能は、スマートカードを使用できない場合に有効です。たとえば、ログオン証明書が期限切れになった場合などです。これを実行できるようにするには、スマートカードを許可するため **False** に設定した **DisableCtrlAltDel** メソッドを使って、サイトごとに専用ストアをセットアップする必要があります。2 モード認証には StoreFront 構成が必要です。

  また 2 モード認証により、StoreFront 管理者はユーザーが StoreFront コンソールでユーザー名とパスワード、およびスマートカード認証の両方を選択して同じストアで使用できるようにします。StoreFrontのドキュメントを参照してください。

- 複数の証明書 - 単一または複数のスマートカードを使用する場合、複数の証明書を使用できます。
- クライアント証明書による認証 - この機能を使用するには、Citrix Gateway および StoreFront での構成が必要です。

  - Citrix Gateway を使って StoreFront にアクセスする場合、ユーザーがスマートカードを取り外した後で再認証が必要になることがあります。
  - Citrix Gateway の SSL 構成で常にクライアント証明書による認証が使用されるようにすると、より安全になります。ただし、この構成では 2 モード認証を使用できません。

- ダブルホップセッション - ダブルホップセッションでは、Citrix Workspace アプリとユーザーの仮想デスクトップとの間に接続が確立されます。ダブルホップセッションをサポートする展開方法については、Citrix Virtual Apps and Desktops のドキュメントを参照してください。
- スマートカード対応のアプリケーション - 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、仮想アプリと仮想デスクトップの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。

制限事項:

- 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。
- Citrix Workspace アプリはユーザー証明書の選択を保存しませんが、構成時に PIN を格納します。PIN は非ページ化メモリにのみキャッシュされ、ディスクには格納されません。
- 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が構成されている場合、Citrix Workspace アプリでは仮想プライベートネットワーク（VPN：Virtual Private Network）のシングルサインオンやセッションの事前起動がサポートされません。ス

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

マートカード認証で VPN 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 による認証が必要になります。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。

- Citrix Workspace アプリ更新ツールと citrix.com や Merchandising Server 間の通信では、Citrix Gateway 上のスマートカード認証を使用できません。

> 警告
>
> 一部の構成では、レジストリの編集が必要です。レジストリエディターの使用を誤ると、問題が発生する可能性があり、Windows のインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

スマートカード認証のシングルサインオンを有効にするには:

Windows 向け Citrix Workspace アプリのインストール中に、以下のコマンドラインオプションを指定します:

- `ENABLE\\_SSON=Yes`

  シングルサインオンは、「パススルー認証」と呼ばれることもあります。このオプションを指定すると、Citrix Workspace アプリで PIN を繰り返し入力する必要がなくなります。

- シングルサインオンコンポーネントをインストールしていないデバイス上で、**SSONCheckEnabled** を false に設定します。これにより、Citrix Workspace アプリの Authentication Manager でシングルサインオンコンポーネントがチェックされなくなり、Citrix Workspace アプリで StoreFront への認証が可能になります。

  ```
  HKEY\\_CURRENT\\_USER\Software\Citrix\AuthManager\protocols\
  integratedwindows\
  ```

  ```
  HKEY\\_LOCAL\\_MACHINE\Software\Citrix\AuthManager\protocols\
  integratedwindows\
  ```

Kerberos の代わりに StoreFront に対してスマートカード認証を有効にするには、次のコマンドラインオプションで Citrix Workspace アプリをインストールします:

- `/includeSSON` を指定すると、シングルサインオン認証（パススルー認証）がインストールされます。資格情報のキャッシュおよびパススルードメインベース認証の使用を有効にします。
- Windows 向け Citrix Workspace アプリのスマートカード認証とは別の方法（ユーザー名とパスワードなど）でユーザーがエンドポイントにログオンしている場合、コマンドラインは次のようになります:

  ```
  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
  ```

これによりログオン時に資格情報がキャプチャされるのを防ぎ、Citrix Workspace アプリへのログオン時に PIN を格納することができます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. ［管理用テンプレート］>［**Citrix** コンポーネント］>［**Citrix Workspace**］>［ユーザー認証］>［ローカルユーザー名とパスワード］に移動します。
3. ［パススルー認証を有効にします］チェックボックスをオンにします。構成およびセキュリティ設定によっては、パススルー認証を実行するために ［すべての **ICA** 接続にパススルー認証を許可します］チェックボックスをオンにします。

StoreFront を構成するには:

- 認証サービスを構成する場合、［スマートカード］チェックボックスをオンにします。

StoreFront でスマートカードを使用する場合は、StoreFront ドキュメントの「認証サービスの構成」を参照してください。

ユーザーデバイスでスマートカードを使用できるようにするには:

1. デバイスのキーストアに、証明機関のルート証明書をインポートします。
2. ベンダーが提供する暗号化ミドルウェアをインストールします。
3. Citrix Workspace アプリをインストールして構成します。

証明書の選択方法を変更するには:

複数の証明書が有効な場合、Citrix Workspace アプリではデフォルトでそれらの証明書の一覧が表示され、ユーザーは使用する証明書を選択できます。管理者は、デフォルトの証明書（スマートカードプロバイダー指定の証明書）、または有効期限が最も残っている証明書が使用されるように Citrix Workspace アプリを構成できます。有効なログオン証明書がない場合はユーザーにメッセージが表示され、使用可能なほかのログオン方法が提示されます。

有効な証明書とは、以下のものを指します:

- ローカルコンピューターの現在時刻に基づき、証明書が有効期限内である。
- サブジェクトの公開キーで RSA アルゴリズムが使用されており、キーの長さが 1024 ビット、2048 ビット、または 4096 ビットである。
- キー使用法にデジタル署名が含まれている。
- Subject Alternative Name フィールドにユーザープリンシパル名（UPN）が含まれている。
- Enhanced Key Usage フィールドに Smart Card Logon および Client Authentication、または All Key Usages が含まれている。
- 証明書の発行者チェーンに含まれる証明機関の 1 つが、TLS ハンドシェイク時にサーバーから送信される、許可される識別名（DN）の 1 つに合致している。

証明書の選択方法を変更するには、以下のいずれかの構成を行います:

- Citrix Workspace アプリのコマンドラインで、オプション`AM\\_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }`を指定します。

  デフォルト値は、Prompt です。SmartCardDefault または LatestExpiry を指定して複数の証明書が該当する場合は、ユーザーが証明書を選択するための一覧が表示されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

次のようにレジストリキーに値を追加します: HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\AuthManager: CertificateSelectionMode={ Prompt	SmartCardDefault	LatestExpiry }。

-

最適な証明書をユーザーが選択できるように、HKEY_CURRENT_USER での設定は、HKEY_LOCAL_MACHINE の設定よりも優先されます。

CSP の **PIN** 入力メッセージを使用するには:

Windows 向け Citrix Workspace アプリのデフォルトでは、スマートカードの Cryptographic Service Provider（CSP）ではなく PIN 入力用のメッセージが表示されます。PIN の入力が必要な場合、Citrix Workspace アプリがメッセージを表示して、ユーザーにより入力された PIN をスマートカードの CSP に渡します。プロセスごとやセッションごとの PIN のキャッシュが禁止されているなど、環境やスマートカードでより厳格なセキュリティが求められる場合は、CSP コンポーネントを使用して PIN 入力用のメッセージを表示して PIN を処理するように Citrix Workspace アプリを構成できます。

PIN 入力の処理方法を変更するには、以下のいずれかの構成を行います:

- Citrix Workspace アプリのコマンドラインで、オプション`AM\\_SMARTCARDPINENTRY=CSP`を指定します。
- 次のようにレジストリキーに値を追加します:HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\AuthMana SmartCardPINEntry=CSP

スマートカードのサポートおよび取り出しの変更

XenApp 6.5 PNAgent サイトに接続する場合は次の点に注意してください。

- スマートカードによるログインは、PNAgent サイトのログインでサポートされています。
- PNAgent サイトでのスマートカードの取り出しポリシーは変更されました:

スマートカードを取り外すと Citrix Virtual Apps セッションからログオフされます。ただし、PNAgent サイトの認証方法をスマートカードに設定している場合、Citrix Virtual Apps セッションからのログオフを有効にするには Windows 向け Citrix Workspace アプリで対応するポリシーを構成する必要があります。XenApp PNAgent サイトでスマートカード認証のローミングを有効にして、Citrix Workspace アプリセッションから Citrix Virtual Apps をログオフするスマートカードの取り出しポリシーを有効にします。ユーザーは Citrix Workspace アプリセッションにログインしたままになります。

制限事項:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

スマートカード認証を使用して PNAgent サイトにログインした場合、ユーザー名が ［ログオン済み］と表示されます。

セキュリティで保護された通信

April 22, 2024

Citrix Virtual Apps and Desktops サーバーと Citrix Workspace アプリ間の通信を保護するには、以下のセキュリティ保護技術をセットで使用します。

- Citrix Gateway：詳しくは、このセクションのトピックと、Citrix Gateway および 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に Citrix Gateway を使用することをお勧めします。

- ファイアウォール：ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。サーバーの内部 IP アドレスを外部インターネットアドレスにマップするネットワークファイアウォール（つまり NAT（Network Address Translation：ネットワークアドレス変換））を介して Citrix Workspace アプリを使用する場合は、外部アドレスを構成します。
- 信頼されたサーバー。
- Citrix Virtual Apps または Web Interface 展開環境でのみ（XenDesktop 7 には適用されません）：SOCKS プロキシサーバーまたはセキュアプロキシサーバー（セキュリティプロキシサーバー、HTTPS プロキシサーバーとも呼ばれます）。プロキシサーバーでネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、Citrix Workspace アプリとサーバー間の接続を制御できます。Citrix Workspace アプリは、SOCKS プロトコルとセキュアプロキシプロトコルをサポートしています。
- Citrix Virtual Apps または Web Interface 展開環境では、TLS（Transport Layer Security）プロトコルを使用する Citrix SSL Relay（XenDesktop 7、XenDesktop 7.1、XenDesktop 7.5、または XenApp 7.5 には適用されません）。
- Citrix Virtual Apps and Desktops 7.6 の場合、ユーザーと VDA 間で直接 SSL 接続を有効にできます

送信プロキシのサポート

スマートコントロールを使用すると、管理者は詳細なポリシーを定義して、Citrix Gateway を使用して Citrix Virtual Apps and Desktops および Citrix DaaS（Citrix Virtual Apps and Desktops サービスの新名称）のユーザー環境属性を構成および適用できます。たとえば、ユーザーがドライブをリモートデスクトップにマップできないようにしたい場合があります。Citrix Gateway のスマートコントロール機能を使用してこれを実現できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ただし、Citrix Workspace アプリと Citrix Gateway が別々のエンタープライズアカウントに属している場合には、シナリオは変わります。このようなシナリオでは、クライアントドメインに Gateway が存在しないため、クライアントドメインはスマートコントロール機能を適用できません。代わりに、送信 ICA プロキシを利用できます。送信 ICA プロキシを使用すると、Citrix Workspace アプリと Citrix Gateway が異なる組織に展開されている場合でも、スマートコントロール機能を使用できます。

Citrix Workspace アプリは、NetScaler LAN プロキシを使用したセッションの起動をサポートします。単一の静的プロキシを設定することも、送信プロキシプラグインを使用して実行時にプロキシサーバーを選択することもできます。

送信プロキシは、次の方法を使用して構成できます:

- 静的プロキシ: プロキシのホスト名とポート番号を指定してプロキシサーバーを構成します。
- 動的プロキシ: プロキシプラグイン DLL を使用して、1 つ以上のプロキシサーバーから 1 つのプロキシサーバーを選択できます。

グループポリシーオブジェクト管理用テンプレートとレジストリエディターを使用して、送信プロキシを構成できます。

送信プロキシについて詳しくは、Citrix Gateway のドキュメントの「送信 ICA プロキシのサポート」を参照してください。

送信プロキシのサポート - 構成

> 注:
>
> 静的プロキシと動的プロキシの両方が構成されている場合は、動的プロキシの構成が優先されます。

GPO 管理用テンプレートを使用した送信プロキシの構成:

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. [コンピューターの構成] ノードで、[管理用テンプレート] > [**Citrix Workspace**] > [ネットワークルーティング] の順に移動します。
3. 次のいずれかのオプションを選択します:
   - 静的プロキシの場合: [**NetScaler LAN** プロキシを手動で構成する] ポリシーを選択します。[有効] を選択して、ホスト名とポート番号を入力します。
   - 動的プロキシの場合: [**NetScaler LAN** プロキシを **DLL** を使用して構成する] ポリシーを選択します。[有効] を選択して、DLL ファイルのフルパスを入力します。例: `C:\Workspace\Proxy\ProxyChooser.dll`。
4. [適用]、[**OK**] の順にクリックします。

レジストリエディターを使用して、次のように送信プロキシーを構成します:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 静的プロキシの場合:
  - レジストリエディターを起動して、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScalerに移動します。
  - DWORD 値キーを次のように作成します:

```
"StaticProxyEnabled"=dword:00000001
"ProxyHost"="testproxy1.testdomain.com
"ProxyPort"=dword:000001bb
```

- 動的プロキシの場合:
  - レジストリエディターを起動して、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler LAN Proxyに移動します。
  - DWORD 値キーを次のように作成します:

```
"DynamicProxyEnabled"=dword:00000001
"ProxyChooserDLL"="c:\\Workspace\\Proxy\\ProxyChooser.dll"
```

TLS

このトピックは、Citrix Virtual Apps and Desktops のバージョン 7.6 以降に適用されます。

サーバーのすべての Citrix Workspace アプリ通信を TLS で暗号化するには、ユーザーデバイス、Citrix Workspace アプリ、および Web Interface サーバー（使用している場合）を構成します。StoreFront 通信の保護については、StoreFront のドキュメントのセキュリティに関するセクションを参照してください。

前提条件:

ユーザーデバイスは、「システム要件」で指定された要件を満たす必要があります。

このポリシーを使用して TLS オプションを構成します。このオプションにより、Citrix Workspace アプリで接続先のサーバーをセキュアに識別して、サーバーとのすべての通信を暗号化できます。

このオプションで、以下が可能になります:

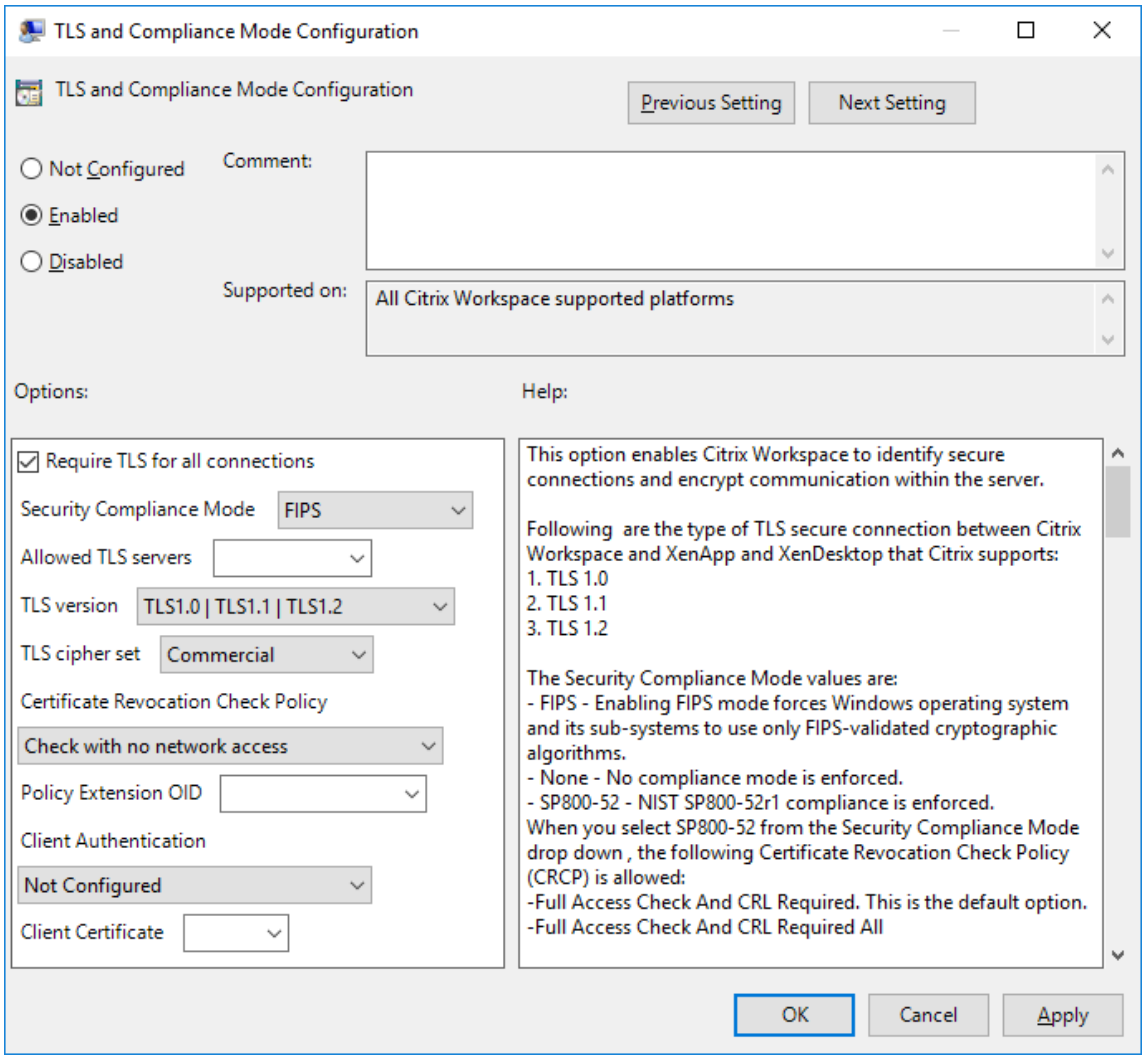
- TLS の使用を適用する: インターネットを含めて、信頼されていないネットワークを介するすべての接続で、TLS の使用をお勧めします。
- FIPS（Federal Information Processing Standards）の使用を適用する: FIPS 準拠の暗号化で、NIST SP 800-52 の推奨セキュリティへの準拠を可能にします。デフォルトでは、これらのオプションは無効になっています。
- TLS の特定のバージョンおよび特定の TLS 暗号の組み合わせの使用を適用する: Windows 向け Citrix Workspace アプリと Citrix Virtual Apps and Desktops および Citrix DaaS 間で TLS 1.0、TLS 1.1、TLS 1.2 プロトコルがサポートされます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 特定のサーバーのみに接続する。
- サーバー証明書の失効を確認する。
- 特定のサーバー証明書発行ポリシーを確認する。
- 特定のクライアント証明書を選択する（サーバーが要求するよう構成されている場合）。

TLS のサポート

1. gpedit.msc を実行して、Citrix Workspace アプリの GPO 管理用テンプレートを開きます。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］>［**Citrix Workspace**］>［ネットワークルーティング］の順に移動して、［**TLS** およびコンプライアンスモードの構成］ポリシーを選択します。



3. ［有効］を選択してセキュリティで保護された接続を有効にし、サーバー上の通信を暗号化します。次のオプションを設定します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> セキュリティで保護された接続で、TLS を使用することを Citrix ではお勧めします。

a) ［すべての接続で **TLS** が必要］を選択することによって、公開アプリケーションおよびデスクトップに対する Citrix Workspace アプリのすべての通信で強制的に TLS を使用させることができます。

b) ［セキュリティコンプライアンスモード］メニューから、適切なオプションを選択します:

i. なし - コンプライアンスモードが適用されません。
ii. **SP800-52** - **SP800-52** を選択して NIST SP800-52 に準拠します。このオプションは、サーバーまたはゲートウェイを NIST SP 800-52 推奨セキュリティに準拠させる場合にのみ選択してください。

> 注:
>
> ［**SP800-52**］を選択すると、［**FIPS** を有効にします］が選択されていない場合でも、自動的に FIPS 準拠の暗号化が使用されます。Windows セキュリティオプションの ［システム暗号化：暗号化、ハッシュ、署名のための **FIPS** 準拠アルゴリズムを使う］も有効にする必要があります。有効にしない場合、Citrix Workspace アプリが公開アプリケーションおよびデスクトップに接続できないことがあります。

［**SP800-52**］を選択した場合、［証明書失効チェックのポリシー］で ［完全なアクセス権のチェック］または ［完全なアクセス権のチェックと **CRL** が必要です］のいずれかも選択する必要があります。

［**SP800-52**］を選択すると、Citrix Workspace アプリはサーバー証明書が NIST SP 800-52 の推奨セキュリティに準拠しているかを検証します。サーバー証明書が準拠していない場合、Citrix Workspace アプリが接続できないことがあります。

i. **FIPS** を有効にします - FIPS 準拠の暗号化の使用を適用するには、このオプションを選択します。オペレーティングシステムのグループポリシーから Windows セキュリティオプションの ［システム暗号化：暗号化、ハッシュ、署名のための **FIPS** 準拠アルゴリズムを使う］も有効にする必要があります。有効にしない場合、Citrix Workspace アプリが公開アプリケーションおよびデスクトップに接続できないことがあります。

c) ［許可された **TLS** サーバー］ドロップダウンリストから、ポート番号を選択します。Citrix Workspace アプリがコンマ区切りの一覧で指定されたサーバーにのみ接続できるようにします。ワイルドカードおよびポート番号を指定できます。たとえば、「*.citrix.com: 4433」により、共通名が「.citrix.com」で終わるどのサーバーともポート 4433 での接続が許可されます。セキュリティ証明書の情報の正確さは、証明書の発行者によって異なります。Citrix Workspace が証明書の発行者を認識して信頼しないと、接続は拒否されます。

d) ［**TLS** バージョン］メニューから、次のいずれかのオプションを選択します:

- **TLS 1.0**、**TLS 1.1**、または **TLS 1.2** - これはデフォルトの設定です。このオプションは、業務上 TLS 1.0 との互換性が必要な場合のみお勧めします。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **TLS 1.1** または **TLS 1.2** - このオプションで ICA 接続が TLS 1.1 または TLS 1.2 を使用するようにします。
- **TLS 1.2** - このオプションは、業務上 TLS 1.2 が必要な場合のみお勧めします。

a) **TLS** 暗号セット - 特定の TLS 暗号セットの使用を適用するには、GOV（行政機関）、COM（営利企業）、ALL（すべて）の中から選択します。一部の Citrix Gateway 構成では、**COM** の選択が必要になることがあります。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:
>
> ビット長 1024 の RSA キーの使用はお勧めしません

- 任意:「任意」が設定されると、ポリシーは構成されず次のいずれかの暗号の組み合わせが許可されます:
  a) TLS_RSA_WITH_RC4_128_MD5
  b) TLS_RSA_WITH_RC4_128_SHA
  c) TLS_RSA_WITH_3DES_EDE_CBC_SHA
  d) TLS_RSA_WITH_AES_128_CBC_SHA
  e) TLS_RSA_WITH_AES_256_CBC_SHA
  f) TLS_RSA_WITH_AES_128_GCM_SHA256
  g) TLS_RSA_WITH_AES_256_GCM_SHA384
- 商用:「商用」が設定されると、次の暗号の組み合わせのみが許可されます:
  a) TLS_RSA_WITH_RC4_128_MD5
  b) TLS_RSA_WITH_RC4_128_SHA
  c) TLS_RSA_WITH_AES_128_CBC_SHA
  d) TLS_RSA_WITH_AES_128_GCM_SHA256
- 自治体:「自治体」が設定されると、暗号の組み合わせのみが許可されます:
  a) TLS_RSA_WITH_AES_256_CBC_SHA
  b) TLS_RSA_WITH_3DES_EDE_CBC_SHA
  c) TLS_RSA_WITH_AES_128_GCM_SHA256
  d) TLS_RSA_WITH_AES_256_GCM_SHA384

a)［証明書失効チェックのポリシー］メニューから、次の任意のオプションを選択します:

- ネットワークアクセスなしでチェックします - 証明書失効一覧チェックが実行されます。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/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必須ではありません。
- 完全なアクセス権のチェック - 証明書失効一覧チェックが実行されます。ローカル証明書失効一覧のストアとすべての配布ポイントが使用されます。証明書の失効情報が検出されると、接続は拒否されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

証明書失効一覧を検出することは、ターゲットサーバーで提示されるサーバー証明書の検証では重要ではありません。

- 完全なアクセス権と **CRL** のチェックが必要です - ルート CA を除いて証明書失効一覧チェックが実行されます。ローカル証明書失効一覧のストアとすべての配布ポイントが使用されます。証明書の失効情報が検出されると、接続は拒否されます。証明書失効一覧をすべて検出することが、検証では重要です。
- すべてに完全なアクセス権と **CRL** のチェックが必要です - ルート CA を含めた証明書失効一覧チェックが実行されます。ローカル証明書失効一覧のストアとすべての配布ポイントが使用されます。証明書の失効情報が検出されると、接続は拒否されます。証明書失効一覧をすべて検出することが、検証では重要です。
- チェックなし - 証明書失効一覧チェックは実行されません。

a) ［ポリシーの拡張 **OID**］を使用して、Citrix Workspace アプリが特定の証明書の発行ポリシーがあるサーバーにのみ接続するように制限できます。［ポリシーの拡張 **OID**］を選択すると、Citrix Workspace アプリはポリシーの拡張 OID があるサーバー証明書のみを受け入れます。

b) ［クライアント認証］メニューから、以下の任意のオプションを選択します：

- 無効 - クライアント認証が無効になります。
- 証明書セレクタを表示します - 常にユーザーが証明書を選択するよう求めます。
- 可能な場合、自動的に選択します - 特定する証明書に選択肢がある場合のみ、ユーザーに表示します。
- 未構成 - クライアント認証が構成されていないことを意味します。
- 指定された証明書を使用します - ［クライアント証明書］オプションの設定で指定された「クライアント証明書」を使用します。

a) ［クライアント証明書］設定を使用して、識別証明書の拇印を指定します。これにより、ユーザーに不要なプロンプトを表示しないようにすることができます。

b) ［適用］および ［**OK**］をクリックしてポリシーを保存します。

次の表は、各セットの暗号の組み合わせを示しています：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Ciphersuite	Native Cyrpto Kit mode and cipher set								
	Open			FIPS			SP800-52		
	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y		Y	Y		Y	Y	
TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2)	X								
TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2)	X	X							
TLS_RSA_WITH_AES_256_CBC_SHA256 (1) (2)	X								
TLS_RSA_WITH_AES_256_CBC_SHA (2)	X								
TLS_RSA_WITH_AES_128_CBC_SHA (2)	X	X							
TLS_RSA_WITH_RC4_128_SHA (2) (3)	X	X							
TLS_RSA_WITH_RC4_128_MD5 (2) (3)	X	X							
TLS_RSA_WITH_3DES_EDE_CBC_SHA (2)	X								
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	Y	Y	Y	Y	Y	Y	Y	Y	Y
Notes									
(1) Ciphersuites that require TLS1.2/DTLS 1.2									
(2) Ciphersuites disabled by default									
(3) Ciphersuites not available for DTLS protocol									
Y - Supported ciphersuites									
X-Deprecated ciphersuites									

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。ファイアウォールが使用されている環境では、Windows 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。

共通の **Citrix** 通信ポート

接続元	種類	ポート	詳細
Citrix Workspace アプリ	TCP	80/443	StoreFront との通信
ICA/HDX	TCP	1494	アプリケーションおよび仮想デスクトップへのアクセス
ICA/HDX（セッション画面の保持機能）	TCP	2598	アプリケーションおよび仮想デスクトップへのアクセス
ICA/HDX（SSL 経由）	TCP	443	アプリケーションおよび仮想デスクトップへのアクセス

ポートについて詳しくは、Knowledge Center のCTX101810を参照してください。

ファイヤウォールによるネットワークアドレス変換（NAT：Network Address Translation）を使用している場合は、Web Interface を使って内部アドレスから外部アドレスおよびポートへのマッピングを定義できます。たとえ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ば、Citrix Virtual Apps and Desktops サーバーに代替アドレスが設定されていない場合は、Web Interface から Citrix Workspace アプリに代替アドレスが提供されるように設定できます。これにより、Citrix Workspace アプリでのサーバー接続で、外部アドレスおよびポート番号が使用されるようになります。

プロキシサーバー

プロキシサーバーは、ネットワーク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、Windows 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。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 Workspace アプリでサーバーと通信する場合、Web 向け Workspace または Web Interface サーバー上でリモート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。プロキシサーバーの構成については、StoreFront または Web Interface のドキュメントを参照してください。

また、Citrix Workspace アプリが Web サーバーと通信するときは、ユーザーデバイス上でデフォルトの Web ブラウザーのインターネット設定で構成した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、インターネット設定を構成する必要があります。

接続中に Citrix Workspace アプリがプロキシサーバーを優先するか無視するかについて、レジストリエディターでプロキシ設定を構成します。

> 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrix では一切責任を負いません。

1. `\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\AuthManager`にアクセスします。
2. **ProxyEnabled**（REG_SZ）を設定します。
   - True –Citrix Workspace アプリは接続でプロキシサーバーを優先します。
   - False –Citrix Workspace アプリは接続でプロキシサーバーを無視します。
3. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

信頼されたサーバー

信頼済みサーバー構成を使用して、Citrix Workspace アプリの接続で信頼関係を識別し適用できます。

信頼済みサーバーを有効にすることで、Citrix Workspace アプリは要件を指定し、サーバーへの接続が信頼済みかどうかを判断できます。たとえば、特定のアドレス（`https://\*.citrix.com`など）に特定の接続の種類（TLS など）を使用して接続する Citrix Workspace アプリは、サーバーの信頼済みゾーンに接続されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

この機能を有効にすると、接続されたサーバーは Windows の信頼済みサイトゾーンに配置されます。Windows の信頼済みサイトゾーンにサーバーを追加する手順について詳しくは、Internet Explorer のオンラインヘルプを参照してください。

グループポリシーオブジェクト管理用テンプレートを使用して信頼済みサーバーの構成を有効にするには

前提要件:

コネクションセンターなどの Citrix Workspace アプリコンポーネントを終了します。

1. gpedit.msc を実行して、Citrix Workspace アプリの GPO 管理用テンプレートを開きます。
2. [コンピューターの構成] ノードで、[管理用テンプレート] > [従来の管理用テンプレート (**ADM**)] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [ネットワークルーティング] > [信頼済みサーバーの構成を構成します] の順に選択します。
3. [有効] を選択して、Citrix Workspace アプリに領域の識別を適用します。
4. [信頼済みサーバーの構成を適用します] を選択します。これによって、クライアントに信頼済みサーバーを使用した識別を適用します。
5. [**Windows** インターネットゾーン] ドロップダウンリストから、クライアントのサーバーアドレスを選択します。この設定は Windows の信頼済みサイトにのみ適用できます。
6. [アドレス] フィールドで、Windows 以外の信頼済みサイトゾーンのクライアントサーバーアドレスを設定します。コンマ区切り一覧を使用できます。
7. [**OK**] および [適用] をクリックします。

ICA ファイルの署名

ICA ファイル署名機能は、認証していないアプリケーションやデスクトップの起動を回避するために役立ちます。Citrix Workspace アプリは、信頼できるソースからアプリケーションまたはデスクトップが起動されることを管理ポリシーに基づいて検証し、信頼されていないサーバーからの起動を防ぎます。グループポリシーオブジェクトの管理用テンプレートまたは StoreFront を使用して、ICA ファイルの署名を構成できます。ICA ファイル署名はデフォルトで無効になっています。

StoreFront に対する ICA ファイル署名については、StoreFront のドキュメントの「ICA ファイル署名の有効化」を参照してください。

Web Interface 展開の場合、Web Interface でこの機能を有効にして構成し、Citrix ICA File Signing Service を使用して起動処理中にアプリケーションまたはデスクトップの起動に署名を含めることができます。このサービスにより、コンピューターの個人証明書ストアにある証明書を使用して ICA ファイルに署名できます。

ICA ファイルの署名の構成

> 注:
>
> CitrixBase.admx\adml がローカル GPO に追加されないと、[**ICA** ファイルの署名を有効にします] ポリシ

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ーが表示されないことがあります。

1. gpedit.msc を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］>［**Citrix** コンポーネント］に移動します。
3. ［**ICA** ファイルの署名を有効にします］を選択し、必要に応じて次のいずれかのオプションを選択します。

    a) 有効 - 署名証明書の拇印を信頼された機関からの証明書の拇印のホワイトリストに追加できます。
    b) 信頼証明書 - ［表示］をクリックして、ホワイトリストから既存の署名証明書の拇印を削除します。署名証明書のサムプリントは署名証明書のプロパティからコピーして貼り付けることができます。
    c) セキュリティポリシー - メニューから次のいずれかのオプションを選択します。
        i. 署名による起動のみを許可します（安全性が高い）：信頼できるサーバーからの署名されたアプリケーションまたはデスクトップの起動のみを許可します。無効な署名の場合、セキュリティ警告が表示されます。認証されていないため、セッションを開始できません。
        ii. 署名されていない起動（安全性が低い）でユーザーにプロンプトを表示します：署名されていないセッション、または署名が無効なセッションが開始されると、メッセージが表示されます。起動を続行するか、起動をキャンセルするか（デフォルト）を選択できます。

4. ［適用］および ［**OK**］をクリックしてポリシーを保存します。
5. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

デジタル署名証明書を選択して配布するには：

デジタル署名証明書を選択するときは、次の一覧の上位のオプションから順にお勧めします：

1. 周知の証明機関からコード署名証明書または SSL 署名証明書を購入する。
2. 社内に証明機関がある場合はその証明機関を使用して、コード署名証明書または SSL 署名証明書を作成する。
3. Web Interface のサーバー証明書などの既存の SSL 証明書を使用する。
4. ルート証明書を作成して、GPO または手動インストールによりユーザーデバイスに配布する。

Storebrowse

April 22, 2024

Storebrowse は、クライアントとサーバー間の相互通信に使用される軽量のコマンドラインユーティリティです。StoreFront 内および Citrix Gateway 内のすべての操作を認証するために使用されます。

Citrix Receiver for Windows の古いバージョンの Storebrowse ユーティリティに関するドキュメントは、Storebrowse for Citrix Receiverfor Windowsを参照してください。

Storebrowse ユーティリティを使用すると、管理者は以下のような日常的な操作を自動化できます：

- ストアを追加します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 構成済みのストアから公開された Citrix Virtual Apps and Desktops および Citrix DaaS（Citrix Virtual Apps and Desktops サービスの新名称）を列挙します。
- 公開された Citrix Virtual Apps and Desktops および Citrix DaaS を選択して、ICA ファイルを手動で生成します。
- Storebrowse コマンドラインを使用して ICA ファイルを生成します。
- 公開アプリケーションを起動します。

Storebrowse ユーティリティは、Authmanager コンポーネントに導入されました。Citrix Workspace アプリのインストール後、Storebrowse ユーティリティは`AuthManager`インストールフォルダーに格納されます。

Storebrowse ユーティリティが`Authmanager`コンポーネントにインストールされているかどうかは、次の方法でレジストリパスを確認してください:

管理者が **Citrix Workspace** アプリをインストールする場合:

32 ビットマシンの場合	[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\Inst
64 ビットマシンの場合	[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\A

ユーザー（管理者以外）が **Citrix Workspace** アプリをインストールする場合:

32 ビットマシンの場合	[HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Insta
64 ビットマシンの場合	[HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\Au

要件

Storebrowse ユーティリティが StoreFront と Citrix Gateway 間でシームレスに動作するには、Windows 向け Citrix Workspace アプリバージョン 1808 以降をインストールします。Citrix Workspace アプリバージョン 1809 には、少なくとも 530MB のディスク空き容量と 2GB の RAM が必要です。

互換性マトリックス

Storebrowse ユーティリティは、以下のオペレーティングシステムと互換性があります:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

オペレーティングシステム
Windows 10 32 ビット版および 64 ビット版
Windows 8.1 32 ビット版および 64 ビット版
Windows 7 SP1 32 ビット版および 64 ビット版
Windows Thin PC
Windows Server 2016
Windows Server 2012 R2、Standard および Datacenter エディション
Windows Server 2012、Standard および Datacenter エディション
Windows Server 2008 R2（64 ビット版）
Windows Server 2008 R2（64 ビット版）

接続

Storebrowse ユーティリティは、以下の接続の種類をサポートします:

- HTTP ストア
- HTTPS ストア
- Citrix Gateway 11.0 以降

> 注:
>
> Storebrowse ユーティリティは、HTTP ストア上でコマンドラインを使用した資格情報を承認しません。

認証方法

StoreFront サーバー　StoreFront は、ストアにアクセスするためのさまざまな認証方法をサポートしますが、すべてが推奨されるわけではありません。セキュリティ上の理由により、ストアの作成時には一部の認証方法がデフォルトで無効になります。

- ユーザー名とパスワード：ユーザーは、ストアにアクセスするときに、資格情報を入力でき認証されます。最初のストアの作成時に、指定ユーザー認証がデフォルトで有効になります。指定ユーザー認証は、すべてのアクセス方法でサポートされます。
- ドメインパススルー：この場合、ユーザーはドメインに参加している Windows コンピューターにログオンする時に認証されるため、ストアにアクセスするときは自動的にログオンできます。このオプションを使用するには、Citrix Workspace アプリがユーザーデバイスにインストールされているときに、パススルー認証を有効にする必要があります。ドメインパススルーを構成する方法については、「パススルー認証の構成」を参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- **HTTP** 基本：Storebrowse ユーティリティが StoreFront サーバーと通信するには、HTTP 基本認証を有効にする必要があります。デフォルトでは、このオプションは StoreFront サーバーで無効になっています。HTTP 基本認証方式を有効にする必要があります。

Storebrowse ユーティリティは、以下のいずれかの方式の認証方法をサポートします：

- Storebrowse ユーティリティに組み込みの`AuthManager`を使用します。注：Storebrowse ユーティリティを使用する場合、StoreFront で HTTP 基本認証方式を有効にする必要があります。これは、ユーザーが Storebrowse コマンドを使用して資格情報を提供する場合に適用されます。
- Windows 向け Citrix Workspace アプリに外部`Authmanager`を含めることができます。

Citrix Gateway のサポート

Storebrowse ユーティリティの最新リリースでは、Citrix Gateway URL を追加できるようになりました。Storebrowse ユーティリティで Citrix Gateway と通信するための追加の構成は必要ありません。

Citrix Gateway でのシングルサインオン

Citrix Gateway のサポートに加えて、シングルサインオンを使用できるようになりました。ユーザー資格情報を提供することなく、新しいストアを追加し、公開リソースを列挙することができます。

Citrix Gateway でシングルサインオンを使用する方法については、「Citrix Gateway でのシングルサインオンのサポート」を参照してください。

> 注：
>
> この機能は、Citrix Gateway でシングルサインオン認証が構成されているドメイン参加のマシンでのみサポートされます。

公開デスクトップまたはアプリケーションからの起動

ICA ファイルを使用せずに、ストアから直接リソースを起動できるようになりました。

コマンドの使用方法

以下のセクションでは、Storebrowse ユーティリティで使用できるコマンドについて詳しく説明します。

-a、**-addstore**

説明：

新しいストアを追加します。ストアの完全な URL を返します。失敗するとエラーが表示されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> Storebrowse ユーティリティを使用して複数のストアを追加できます。

StoreFront のコマンド例:

コマンド:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of Storefront*
```

例:

‘.\storebrowse.exe –U {Username} –P {Password} –D {Domain} –a https://my.firstexamplestore.net‘

Citrix Gateway のコマンド例:

コマンド:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of CitrixGateway*
```

例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -a <https://mysecondexample.com>
```

/?

説明:

Storebrowse ユーティリティの使用方法の詳細を提供します。

(-l)、-liststore

説明:

ユーザーが追加したストアを一覧表示します。

StoreFront のコマンド例:

```
.\storebrowse.exe -l
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -l
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

(-M 0x2000 -E)

説明:

使用可能なリソースが列挙されます。

StoreFront のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0
x2000 -E <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0
x2000 -E <https://my.secondexample.net>
```

-q、-quicklaunch

説明:

Storebrowse ユーティリティを使用して、公開アプリおよび公開デスクトップに必要な ICA ファイルを生成します。クイック起動オプションを使用するには、起動 URL とストア URL の入力が必要です。ストア URL は、StoreFront サーバーまたは Citrix Gateway URL のいずれかになります。ICA ファイルは、%LocalAppData%\Citrix\Storebrowse\cacheディレクトリに生成されます。

以下のコマンドを実行して、公開されているすべてのアプリとデスクトップの起動 URL を取得できます。

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/
Second/discovery
```

以下は、一般的な起動 URL の例です:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix
/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

StoreFront のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q {
Launch_URL_of_published_ apps and desktops } <https://my.firstexamplestore
.net/Citrix/Store/resources/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https
://my.firstexamplestore.net/Citrix/Store/discovery>
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q {
Launch_URL_of_published_ apps and desktops } <https://my.secondexmaplestore
.com>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

-L、-launch

説明:

Storebrowse ユーティリティを使用して、公開アプリおよび公開デスクトップに必要な ICA ファイルを生成します。起動オプションを使用するには、リソース名とストア URL が必要です。ストア URL は、StoreFront サーバーまたは Citrix Gateway URL のいずれかになります。ICA ファイルは、%LocalAppData%\Citrix\Storebrowse\cacheディレクトリに生成されます。

以下のコマンドを実行して、公開アプリや公開デスクトップの表示名を取得できます。

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

以下は、このコマンドの結果です:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

上記の結果で太字の名前は、起動オプションの入力パラメーターとして使用されます。

StoreFront のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L “{ Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Citrix Gateway のコマンド例:

```
<.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L { Resource_Name } https://my.secondexamplestore.com>
```

-S、-sessionlaunch

説明:

単一のコマンドでストアを追加し、公開リソース（アプリとデスクトップ）を列挙し、リソースを起動することができます。このオプションでは、ユーザー名、パスワード、ドメイン、起動するリソースのフレンドリ名、ストア URL の各パラメーターを指定します。ただし、ユーザーが資格情報を指定しない場合、資格情報を入力するためのAuthManagerプロンプトが表示され、リソースが起動されます。

以下のコマンドを実行して、公開アプリや公開デスクトップのリソース名を取得できます。

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

以下は、このコマンドの結果です:

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

上記の結果で太字の名前は、-Sオプションの入力パラメーターとして使用されます。

StoreFront のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S “
{ Friendly_Resource_Name } <https://my.firstexamplestore.net/Citrix/
Store/discovery >
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S {
Friendly_Resource_Name } <https://my.secondexamplestore.com>
```

-f、-filefolder

説明:

Storebrowse ユーティリティを使用して、公開されたすべてのアプリおよびデスクトップの-f オプションで定義されたカスタムパスに必要な ICA ファイルを生成します。

起動オプションを使用するには、フォルダー名およびリソース名とストア URL の入力が必要です。ストア URL は、StoreFront サーバーまたは Citrix Gateway URL のいずれかになります。

StoreFront のコマンド例:

```
.\storebrowse.exe -f “C:\Temp\Launch.ica” -L “Resource_Name” { Store
 }
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -f “C:\Temp\Launch.ica” -L “Resource_Name” {
NSG_URL }
```

-t、-traceauthentication

説明:

Storebrowse ユーティリティで組み込みのAuthManagerコンポーネントのログを生成します。ログは、Storebrowse ユーティリティが組み込みのAuthManagerを使用している場合にのみ生成されます。localappdata%\Citrix\Storebrowse\logsディレクトリに生成されます。

注: このオプションを、ユーザーのコマンドラインに表示される最後のパラメーターにすることはできません。

StoreFront のコマンド例:

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a
{ StoreURL }
```

Citrix Gateway のコマンド例:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a
{ NSG_URL }
```

-d、-deletestore

説明:

既存の StoreFront または Citrix Gateway ストアを削除します。

StoreFront のコマンド例:

```
.\storebrowse.exe -d https://my.firstexamplestore.net/Citrix/Store/
discovery
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -d https://my.secondexmaplestore.com
```

Citrix Gateway でのシングルサインオンのサポート

シングルサインオンを使用すると、ドメインに対して認証することで、そのドメインで提供されている Citrix Virtual Apps and Desktops および Citrix DaaS を再認証する必要なく使用できます。Storebrowse ユーティリティでストアを追加すると、スタートメニューの設定を含め、列挙された仮想アプリと仮想デスクトップとともに資格情報が Citrix Gateway サーバーにパススルーされます。シングルサインオンの構成後、資格情報を何度も入力しなくても、ストアを追加したり、仮想アプリと仮想デスクトップを列挙したり、必要なリソースを起動することができます。

この機能は、Citrix Gateway バージョン 11 以降でサポートされています。

前提条件:

Citrix Gateway のシングルサインオンを構成するための前提条件については、「ドメインパススルー認証の構成」を参照してください。

グループポリシーオブジェクト（GPO）管理用テンプレートを使用して Citrix Gateway でシングルサインオン機能を有効にできます。

> 注:
>
> Citrix Receiver から Citrix Workspace アプリをアップグレードする場合、または初めて新規にインストールする場合、最新のテンプレートファイルをローカル GPO に追加する必要があります。テンプレートファイルをローカル GPO に追加する方法について詳しくは、「グループポリシーオブジェクト管理用テンプレートの構成」を参照してください。アップグレードの場合、最新のファイルをインポートする時に既存の設定が保持されます。

1. gpedit.msc を実行して、Citrix Workspace アプリ GPO 管理用テンプレートを開きます。
2. [コンピューターの構成] ノードで、[管理用テンプレート] > [**Citrix** コンポーネント] > [**Citrix Workspace**] > [ユーザー認証] > [**Citrix Gateway** のシングルサインオン] に移動します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. シングルサインオンオプションで［有効］または［無効］に切り替えます。
4. ［適用］、［**OK**］の順にクリックします。
5. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

制限事項:

- Storebrowse ユーティリティでの資格情報入力操作のために、StoreFront サーバーで HTTP 基本認証を有効にする必要があります。
- 仮想アプリと仮想デスクトップを列挙または起動するためにユーティリティを使用して HTTP ストアに接続しようとする場合、コマンドラインオプションを使用した資格情報の入力はサポートされません。この問題を回避するには、コマンドラインで資格情報を提供しないときに使用される外部`AuthManager`モジュールを使用します。
- Storebrowse ユーティリティは、現在、StoreFront サーバー上の Citrix Gateway で構成された単一ストアのみをサポートしています。
- Storebrowse ユーティリティの資格情報の入力は、Citrix Gateway が単一要素認証で構成されている場合にのみ機能します。
- Storebrowse ユーティリティのコマンドラインオプション`Username` (`-U`)、`Password` (`-P`) `Domain` (`-D`) では大文字小文字が区別され、大文字のみを使用する必要があります。

Citrix Workspace アプリ Desktop Lock

January 17, 2024

ローカルのデスクトップを操作する必要がない場合は、Citrix Workspace アプリ Desktop Lock を使用できます。Desktop Viewer（有効な場合）を使用することはできますが、ツールバー上には次の必須オプションしか表示されません:

- Ctrl+Alt+Del
- 基本設定
- デバイス
- 切断。

Windows 向け Citrix Workspace アプリ Desktop Lock は、SSON（Single Sign-On：シングルサインオン）が有効でありストアが構成済みのドメイン参加マシンで機能します。Program Neighborhood エージェント（PNA）サイトはサポートしません。以前のバージョンの Desktop Lock は、Citrix Receiver for Windows 4.2 以降へアップグレードするとサポートされません。

コマンドラインインターフェイスを使用した **Desktop Lock** のインストール

前提条件:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- ドメイン参加マシンの管理者である必要があります。
- シングルサインオンを有効にする必要があります。
- ストアを構成する必要があります。

1. 次のコマンドを実行して、Citrix Workspace アプリをインストールします:

```
`CitrixWorkspaceApp.exe /includeSSON /Silent STORE0= “AppStore;
   https://testserver.net/Citrix/MyStore/discover;on;Desktop App
   Store” `
```

2. Citrix ダウンロードページで入手できるCitrixWorkspaceDesktopLock.msiをダウンロードします。
3. 次のコマンドを実行して、Desktop Lock をインストールします:

   ```
   installationSilent : msiexec /i CitrixWorkspaceDesktopLock.msi /
   qn
   ```

公開デスクトップは、ユーザーとしてログインすると自動的に起動します。

システム要件

- Microsoft Visual C++ 2005 Service Pack 1 再頒布可能パッケージ。詳しくは、Microsoft のダウンロードページを参照してください。
- Windows 7 (Embedded Edition を含む)、Windows 7 Thin PC、Windows 8、Windows 8.1、Windows 10（Anniversary Update を含む）でサポートされます。
- ネイティブプロトコルのみを介して StoreFront に接続します。
- ユーザーデバイスをローカルエリアネットワーク（LAN）またはワイドエリアネットワーク（WAN）に接続する必要があります。

ローカルアプリアクセス

> 重要
>
> ローカルアプリアクセスを有効にすると、グループポリシーオブジェクトテンプレートまたは同様のポリシーでフルロックダウンが適用されていない限り、ローカルデスクトップアクセスを実行できます。詳しくは、Citrix Virtual Apps and Desktops のドキュメントで「ローカルアプリアクセスと URL リダイレクト」セクションを参照してください。

Citrix Workspace アプリ Desktop Lock の使用

- Citrix Workspace アプリ Desktop Lock では次の Citrix Workspace アプリの機能を実行できます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 3Dpro、Flash、USB、HDX Insight、Microsoft Lync 2013 プラグイン、およびローカルアプリアクセス
  - ドメイン、2 要素、またはスマートカード認証のみ

- Citrix Workspace アプリ Desktop Lock セッションを切断すると、エンドデバイスがログアウトされます。
- Flash のリダイレクトは Windows 8 以降では無効です。Windows 7 では有効です。
- Desktop Viewer は Home、Restore、Maximize、および Display の各プロパティが未設定の Citrix Workspace アプリ Desktop Lock に最適化されています。
- Desktop Viewer のツールバーでは、Ctrl+Alt+Del キーの組み合わせを使用できます。
- Windows+L キー以外のほとんどの Windows ショートカットキーをリモートセッションで実行できます。
- 接続を無効にするまたはデスクトップ接続の Desktop Viewer を無効にする場合、Ctrl+F1 キーを押すと Ctrl+Alt+Del を押すのと同じように動作します。

> 注:
>
> Desktop Lock がインストールされ、`LiveInDesktopDisconnectOnLock`がレジストリパス`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`または`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`で **False** に設定されている場合、エンドポイントが休止状態またはスタンバイモードから復帰すると、アクティブなセッションが切断されます。

Citrix Workspace アプリ Desktop Lock のインストール

この手順では、Citrix Workspace アプリ Desktop Lock を使用して仮想デスクトップが表示されるように、Windows 向け Citrix Workspace アプリをインストールします。スマートカードを使用する展開については、「スマートカード」を参照してください。

1. ローカルの管理者アカウントを使用してログオンします。
2. コマンドプロンプトで次のコマンドを実行します（インストールメディアの Citrix Workspace アプリおよびプラグイン > Windows > Citrix Workspace アプリフォルダーにあります）。

   例:

```
CitrixWorkspaceApp.exe /includeSSON STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/discovery;on;Desktop Store"
```

コマンドについて詳しくは、「インストール」を参照してください。

1. インストールメディアの同じフォルダーにある`CitrixWorkspaceDesktopLock.msi`をダブルクリックします。Desktop Lock ウィザードが開きます。画面の指示に従って操作します。
2. インストールが完了したら、ユーザーデバイスを再起動します。デスクトップへのアクセスが許可されていて、ドメインユーザーとしてログオンすると、Citrix Workspace アプリ Desktop Lock でデスクトップが表示されます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ただし、インストールの完了後にユーザーデバイスを管理できるようにするため、CitrixWorkspaceDesktopLock.msiをインストールしたときのアカウントでは代替シェルが使用されません。このアカウントを削除すると、デバイスにログオンして管理することができなくなります。

Citrix Workspace アプリ Desktop Lock のサイレントインストールを実行するには、次のコマンドラインを使用します。

```
msiexec /i CitrixWorkspaceDesktopLock.msi /qn
```

Citrix Workspace アプリ Desktop Lock の構成

Citrix Workspace アプリ Desktop Lock を使用するユーザーには、単一の仮想デスクトップだけのアクセスを付与します。

Active Directory ポリシーを使用して、ユーザーが仮想デスクトップを休止状態にできないようにします。

Citrix Workspace アプリ Desktop Lock を構成するときは、インストール時に使用した管理者アカウントを使用します。

- receiver.admx（または receiver.adml）と receiver_usb.admx（.adml）ファイルがグループポリシーにロードされていることを確認します（ポリシーは［コンピューターの構成］または［ユーザーの構成］>［管理用テンプレート］>［従来の管理用テンプレート（ADMX）］>［Citrix コンポーネント］の順に展開すると表示されます）。これらの.admx ファイルは、%Program Files%\Citrix\ICA Client\Configuration\にインストールされています。
- USB 基本設定 - ユーザーが USB デバイスを接続すると、そのデバイスは自動的に仮想デスクトップで使用可能になります。このとき、ユーザーが何らかの操作を行う必要はありません。USB ドライブの制御と表示は、仮想デスクトップにより処理されます。
  - USB ポリシー規則を有効にします。
  - ［Citrix Workspace アプリ］、［クライアントデバイスをリモート処理します］、［一般的な USB のリモート処理］の順に選択して、Existing USB Devices と New USB Devices ポリシーを有効にして構成します。
- ドライブマッピング - ［Citrix Workspace アプリ］、［クライアントデバイスをリモート処理します］の順に選択して、Client drive mapping ポリシーを有効にして構成します。
- マイク - ［Citrix Workspace アプリ］、［クライアントデバイスをリモート処理します］の順に選択して、Client microphone ポリシーを有効にして構成します。

Desktop Lock を実行する Windows デバイスでのスマートカードの使用を構成

1. StoreFront を構成します。
   a) Citrix XML Service の DNS アドレス解決を有効にして、Kerberos 認証を使用できるように構成します。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) StoreFront サイトの HTTPS アクセスを構成して、ドメインの証明機関による署名付きのサーバー証明書を作成し、デフォルトの Web サイトに HTTPS バインドを追加します。
c) ［スマートカードパススルー認証］が有効になっていることを確認します（デフォルトで有効になっています）。
d) ［Kerberos］を有効にします。
e) ［Kerberos］および［スマートカードパススルー認証］を有効にします。
f) IIS の Default Web Site で［匿名アクセス］を有効にして、［統合 Windows 認証］を使用します。
g) IIS の Default Web Site の SSL 設定で［SSL が必要］チェックボックスがオフで、［クライアント証明書］で［無視］が選択されていることを確認します。

2. グループポリシー管理コンソールを使用して、ユーザーデバイスでローカルコンピューターのポリシーを構成します。

a) %Program Files%\Citrix\ICA Client\Configuration\から Receiver.admx テンプレートをインポートします。
b) ［管理用テンプレート］>［従来の管理用テンプレート（ADMX）］>［Citrix コンポーネント］>［Citrix Workspace］>［ユーザー認証］の順に展開します。
c) ［スマートカード認証］を有効にします。
d) ［ローカルユーザー名とパスワード］を有効にします。

3. Citrix Workspace アプリ Desktop Lock をインストールする前に、ユーザーデバイスを構成します。

a) Windows Internet Explorer の信頼済みサイトの一覧に、Delivery Controller の URL を追加します。
b) Windows Internet Explorer の信頼済みサイトの一覧に、最初のデリバリーグループの URL を「desktop://delivery-group-name」形式で追加します。
c) 信頼済みサイトに対する Internet Explorer の自動ログオン機能を有効にします。

Citrix Workspace アプリ Desktop Lock がユーザーデバイスにインストールされている場合、スマートカード取り出し時の動作に競合が生じないようにポリシーが適用されます。たとえば、Windows のスマートカードの取り出しポリシーがデスクトップで強制ログオフに設定されている場合、Windows のスマートカードの取り出しポリシーが設定されているかどうかにかかわらず、ユーザーはユーザーデバイスからもログオフする必要があります。これにより、ユーザーデバイスの整合性が維持されます。これは、Citrix Workspace アプリ Desktop Lock が有効なユーザーデバイスにのみ適用されます。

Desktop Lock の削除

以下のコンポーネントを両方ともアンインストールする必要があります。

1. Citrix Workspace アプリ Desktop Lock のインストールと構成に使用したローカル管理者アカウントでログオンします。
2. プログラムの削除や変更を行うための Windows 機能（コントロールパネルの［プログラムと機能］など）を開き、以下の操作を行います：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Workspace アプリ Desktop Lock をアンインストールします。
- Windows 向け Citrix Workspace アプリをアンインストールします。

リモートセッションでの **Windows** ショートカットキーの実行

ほとんどの Windows ショートカットキーはリモートセッションで実行できます。このセクションでは、一般的なものについていくつか説明します。

Windows

- Win+D - すべてのウィンドウをデスクトップ上で最小化します。
- Alt+Tab - アクティブなウィンドウを変更します。
- Ctrl+Alt+Delete - Ctrl+F1 および Desktop Viewer ツールバーを介します。
- Alt+Shift+Tab
- Windows+Tab
- Windows+Shift+Tab
- Windows+ すべての文字キー

Windows 8

- Win+C - チャームを開きます。
- Win+Q - チャームを検索します。
- Win+H - チャームを共有します。
- Win+K - デバイスのチャーム。
- Win+I - 設定のチャーム。
- Win+Q - アプリを検索します。
- Win+W - 設定を検索します。
- Win+F - ファイルを検索します。

Windows 8 のアプリ

- Win+Z - アプリのオプションを開きます。
- Win+. - アプリを左にスナップします。
- Win+Shift+. - アプリを右にスナップします。
- Ctrl+Tab - アプリ履歴を循環させます。
- Alt+F4 - アプリを閉じます。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

デスクトップ

- Win+D - デスクトップを開きます。
- Win+, - デスクトップでプレビューします。
- Win+B - デスクトップに戻ります。

その他

- Win+U - コンピューターの簡単操作センターを開きます。
- Ctrl+Esc - 画面を開始します。
- Win+Enter - Windows ナレーターを開きます。
- Win+X - システムユーティリティ設定メニューを開きます。
- Win+PrintScrn - スクリーンショットを取りピクチャに保存します。
- Win+Tab - スイッチ一覧を開きます。
- Win+T - タスクバーの開いているウィンドウをプレビューします。

SDK および API

June 16, 2023

Certificate Identity Declaration SDK

Certificate Identity Declaration SDK（CID）を使用すると、Citrix Workspace アプリがクライアントマシンにインストールされている証明書を使用して StoreFront サーバーに認証できるプラグインを開発者が作成できます。CID は、スマートカードベースの認証を実行せずに、ユーザーのスマートカード ID を StoreFront サーバーに宣言します。

詳しくは、「Certificate Identity Declaration SDK for Citrix Workspace app for Windows」のドキュメントを参照してください。

Citrix Common Connection Manager SDK

Common Connection Manager（CCM）SDK は、基本的な操作をプログラム的にやりとりして実行できるネイティブ API のセットを提供します。この SDK は、Windows 向け Citrix Workspace アプリインストールパッケージの一部であるため、別途ダウンロードする必要はありません。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注:
>
> 起動に関連する API によっては、仮想アプリと仮想デスクトップのセッションの起動プロセスの開始に ICA ファイルが必要な場合があります。

CCM SDK の機能は次のとおりです。

- セッションの起動
  - 生成された ICA ファイルを使用してアプリケーションおよびデスクトップを起動できます。
- セッションの切断
  - コネクションセンターを使用した切断と同様の操作です。切断は、すべてのセッションまたは特定のユーザーに対して行うことができます。
- セッションのログオフ
  - コネクションセンターを使用したログオフと同様の操作です。ログオフは、すべてのセッションまたは特定のユーザーに対して行うことができます。
- セッション情報
  - 起動されたセッションの接続関連情報を取得するさまざまな方法を提供します。対象となるのは、デスクトップセッション、アプリケーションセッション、リバースシームレスアプリケーションセッションなどです。

SDK のドキュメントについては、Programmers guide to Citrix CCM SDKを参照してください。

Citrix 仮想チャネル SDK

Citrix 仮想チャネルソフトウェア開発キット（SDK）は、ICA プロトコルを使用する追加の仮想チャネルのための、サーバー側アプリケーションやクライアント側ドライバーの作成をサポートします。サーバー側仮想チャネルアプリケーションは、Citrix Virtual Apps and Desktops 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。

詳しくは、Citrix Virtual Channel SDK for Citrix Workspace app for Windowsのドキュメントを参照してください。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Fast Connect 3 Credential Insertion API

Fast Connect 3 Credential Insertion API は、Windows 向け Citrix Workspace アプリ 4.2 以降のシングルサインオン（SSON）機能に対してユーザーの資格情報を提供するインターフェイスです。この API を使用すると、Citrix パートナーは、StoreFront または Web Interface を使用して仮想アプリケーションまたはデスクトップにユーザーをログオンさせ、その後でそれらのセッションからユーザーを切断する、認証や SSO にかかわる製品を提供できます。

詳しくは、「Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows」のドキュメントを参照してください。

ICA 設定リファレンス

June 16, 2023

ICA 設定リファレンスファイルは、レジストリ設定および ICA ファイル設定のリストを提供し、管理者は環境に対して Citrix Workspace アプリの動作を高度にカスタマイズできます。また、ICA 設定リファレンスを使用して、予期しない Citrix Workspace アプリの動作をトラブルシューティングできます。

ICA 設定リファレンス（PDF のダウンロード）

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).