新機能

Sep 25, 2017

12.7の新機能

macOS 10.13（High Sierra）のサポート

このリリースでは、macOS 10.13を使用してCitrix Receiver for Macの一般的なUSBリダイレクトを有効にする方法が変更されています。macOS 10.13を使用して一般的なUSBリダイレクトを構成するには、CTX228208を参照してください。

StoreFrontを使用したスマートカードのサポート

Citrix Receiver for Webだけでなく、Citrix Receiver for Macも、NetScaler GatewayまたはStoreFrontへの接続でネイティブスマートカード認証をサポートするようになりました。

SNI（Server Name Indication）のサポート

Citrix Receiver for Macは、SNI（Server Name Indication）を構成済みのNetScaler Gatewayをサポートするようになりました。これによって、ユーザーはデスクトップおよびアプリケーションを正常に起動できます。SNIについて詳しくは、Knowledge CenterのCTX125798を参照してください。

解決された問題

Sep 25, 2017

Citrix Receiver for Mac 12.6との比較

Citrix Receiver for Mac 12.7には、バージョン12、12.1、12.1.100、12.2、12.3、12.4、12.5、12.6に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

- NetScalerを使用すると、スマートカードでVDAを起動できないことがあります。Citrix Viewerが応答しなくなり、再起動が必要になります。

  [#RFMAC-445]

- XenApp Essentialsにログオンして2要素認証を使用すると、セキュリティコードを求めるメッセージが表示されないことがあります。

  [#RFMAC-976]

- Citrix Receiver for Macを更新すると、USBリダイレクトの構成ファイルが正しく保存されないことがあります。

  [#RFMAC-981]

- 公開アプリケーションが内部URLをリダイレクトしないことがあります。

  [#RFMAC-982]

- Citrix Viewerが応答しなくなることがあります。

  [#RFMAC-1050]

- High Sierraを実行しているMacでスワイプジェスチャを使用すると、画面が乱れることがあります。

  [#RFMAC-1073]

Citrix Receiver for Mac 12.5との比較

Citrix Receiver for Mac 12.6には、バージョン12、12.1、12.1.100、12.2、12.3、12.4、12.5に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

- WebExで画面を共有すると、共有された画面で黒い画面が表示されることがあります。

  [#RFMAC-689、#LC6462]

- WebExで画面共有を停止すると、アプリケーションがデスクトップ画面の最前面に表示されないことがあります。

[#RFMAC-690、#LC6255]

- macOS Sierraで、Shift+Insキーの組み合わせが機能しないことがあります。

  [#RFMAC-696]

- WebExを最小化した後再度表示しようとすると、アプリケーションが正しく表示されないことがあります。

  [#RFMAC-742、#LC6840]

- Google Chromeを使用してCitrix Receiverでアプリケーションを起動すると、［アプリケーションを起動中...］画面が表示されないことがあります。

  [#RFMAC-744]

- 仮想マシンの実行中、XenDesktopセッションが黒い画面で表示されることがあります。

  [#RFMAC-808]

- アプリケーションが起動された後も、ロード中の画面が開かれたままになります。［キャンセル］をクリックすると、Citrix Receiverが予期せず終了します。

  [#RFMAC-832、#LC7682]

- サーバーからクライアントへのURLリダイレクトを使用すると、「ワンタイムアクセストークン」を含むURLが、期限切れのトークンで起動されることがあります。

  [#RFMAC-856]

- macOS Sierra 10.12.6パブリックベータ版またはmacOS High Sierra Developer PreviewビルドでSafariを使用すると、アプリおよびデスクトップが起動されないことがあります。

  [#RFMAC-869]

Citrix Receiver for Mac 12.4との比較

Citrix Receiver for Mac 12.5には、バージョン12、12.1、12.1.100、12.2、12.3、12.4に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

- リモートデスクトップクライアントのログオンにスマートカードを使用すると、「カードに証明書がありません」というエラーメッセージが表示されることがあります。

  [#RFMAC-432、#650298]

- サーバーがUTF-8形式以外を使用して応答すると、ストアの検出が失敗します。

  [#RFMAC-565]

- SAMLアプリケーションを起動すると、「無効な要求」というエラーメッセージが表示されることがあります。

  [#RFMAC-598、#LC6558]

- ReceiverHelperが予期せず終了することがあります。この問題は、CEIPRegistry.jsonに無効なJSONが含まれる場合に発生します。

  [#RFMAC-639]

- Citrix ReceiverからログアウトしたあとにLaunchpadまたはFinderから公開アプリケーションを起動できず、次のエラーメッセージが表示されます。「接続エラーです。Authentication Managerサービスと通信できません」。

  [#RFMAC-648]

Citrix Receiver for Mac 12.3との比較

Citrix Receiver for Mac 12.4には、バージョン12、12.1、12.1.100、12.2、12.3に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

- Citrix Viewerが正しいキーボードレイアウトをサーバーに送信しません。

  [#581829]

- Citrix Receiver for Mac 12.1を使用すると、ホストされているデスクトップのSplit Viewでサイズ変更やスワップが機能しないことがあります。

  [#604943]

- プライマリディスプレイが一番下にある構成で複数のディスプレイを使用すると、Citrix Receiver for Macの公開アプリケーションの画面でちらつきが発生することがあります。

  [#652254]

- 公開アプリケーションを使用すると、ネットワークドライブでファイルの編集や保存ができないことがあります。

  [#660657]

- ネットワークドライブでファイルを保存すると、VDAセッションが切断されることがあります。

  [#660661]

- VDAセッションまたは公開アプリケーションのどちらかで外部キーボードを使用すると、Insキーが機能しません。

  [#660669]

- 使用可能でもセッションに表示されないプリンターがあります。

  [#667462]

Citrix Receiver for Mac 12.2との比較

Citrix Receiver for Mac 12.3には、バージョン12、12.1、12.1.100、12.2に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

- Citrix Receiver for Macがプロキシサーバーを使用するように構成されている場合、SSL（Secure Socket Layer）接続が失敗することがあります。

  [#640652]

Citrix Receiver for Mac 12.1.100との比較

Receiver for Mac 12.2には、バージョン12、12.1、12.1.100に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

- ドイツ語/オーストリア語対応キーボードで、Alt+Iを使用後、ALTキーが解放されない問題が解決されました。

  [#LC3796]

- URLが非ASCII文字を含むコンテンツにリダイレクトされると、サーバーからコンテンツへのリダイレクトが失敗する問題は解決されました。

  [#LC4470]

- このリリースでは、HDXアプリ画面の最小化および最大化後、描画アーティファクトを表示する問題が解決されました。

  [#LC4668]

- スマートカードのパススルー認証が失敗する問題が解決されました。

  [#LC4907]

- オーディオをマイクからサーバーにリモート接続すると、音声が途切れる問題が解決されました。

  [#LC5157]

- CtrlキーとTabキーの組み合わせがアクティブなデスクトップセッションに正しく渡されなかった問題が解決されました。

  [#LC5367]

- 現在のセッションに再接続すると、セッションのキーボードマッピングが間違ったものになる問題が解決されました。

[#LC5395]

- スマートカードが、HDXセッション内で実行されているMicrosoftリモートデスクトップクライアントに接続できない問題が解決されました。

  [#LC5454]

- このリリースでは、ユーザー証明書の認証がNetScaler Gatewayで構成されると、セッションが接続できない問題が解決されました。

  [#LC5455]

- ICAファイルでScreenPercentパラメーターが指定されると、Receiver for Macが全画面モードでセッションを起動する問題が解決されました。

  [#605353]

- Webカメラがアクティブなセッションにリモート接続されている間にセッションが切断されると、Receiver for Macがクラッシュする問題は解決されました。

  [#612051]

- このリリースでは、証明書失効一覧をダウンロード中、Receiver or Macがシステムプロキシ構成を使用しない問題は解決されました。

  [#638176]

Citrix Receiver for Mac 12.1との比較

Receiver for Mac 12.1.100には、バージョン12および12.1に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

- Cisco ASA 9.32 SSL VPNを介して接続するとReceiver for Macセッションが失敗する問題が解決しました。

  [#LC3887]

- 名前が「@」で始まるアプリケーションまたはデスクトップを起動するとセッションがクラッシュする問題が解決しました。

  [#LC4296]

- セッションが切断されると「リモートSSLピアがbad MACアラートを送信しました。」というエラーメッセージが表示される問題が解決しました。

  [#LC4367]

- NetScaler GatewayにIPV6接続が失敗する問題が解決しました。

[#LC4512]

- 単一の日本語または簡体中国語を入力しようとするとセッションデスクトップには文字が表示されない問題が解決しました。

  [#603635]

Citrix Receiver for Mac 12との比較

Receiver for Mac 12.1には、バージョン12に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

- OS Xに組み込まれているVPNサポートを使用している場合、VPNがアクティブな間にCitrix Receiverが構成済みのアカウントに接続できなかったことがある問題が解決されました。
- セッションが分割ビューになった場合にセッションの表示が乱れるOS X El Capitanの問題が解決しました。

  [#582397]

- F5プロキシを使って外部接続しようとするとビーコンの検出に失敗する問題が解決されました。

  [#582885]

- システム環境設定で構成されたキーボードショートカットがセッションに適用されなかった問題が解決されました。

  [#583033]

- ビューアーがクラッシュする原因であった、Citrix Receiver for Mac 11.9.15および12の「+」キーボード記号の問題が解決されました。

  [#586179, #577922]

- あるアプリケーションを起動後に、Citrix Receiverにより別のアプリケーションに対する認証を求められる問題が解決されました。

  [#592460]

- キーボードの組み合わせCtrl + Qキーが正しく渡されなかったデスクトップセッションの問題が解決されました。

  [#600601]

このリリースではスマートカード統合に関する多くの問題が解決されています。一部の問題については未解決で、引き続き調査が実行されます。

このリリースで解決されたそのほかの問題：

- 日本語環境で、資格情報を入力するダイアログボックスに正しくないメッセージ「デモアカウントにログオンしてください」が表示されました。正しくは「仮想デスクトップにログオンしてください」でした。

  [#LC2682]

- Receiverの複数のディスクイメージを同時にマウントすると、間違ったインストーラーが起動することがありました。

  [#551605]

- CIDR表記のOS Xプロキシバイパスエントリが無視されました。

  [#564250]

- OS Xバイパス一覧の最初の256文字のみが使用されました。

  [#567089]

- 内部ビーコンの誤検知チェックが特定のISPで失敗することがありました。これらのISPはBarefruitのDNSエラーリダイレクトソフトウェアをインストールしていました。

  [#572456]

既知の問題

Sep 25, 2017

このリリースでは、以下の既知の問題が確認されています。

- 全画面セッションで「デスクトップコンポジションリダイレクトを有効にする」ポリシーを有効にすると、Citrix Viewerの画面が乱れることがあります。

  [＃RFMAC-1078]

- 韓国語のローカルIMEで文字をICAセッションに送信すると、Citrix Viewerが予期せず終了することがあります。

  [#RFMAC-1079]

- Macでカナダフランス語キーボードを使用してWindows 7 VDAに接続すると、曲折アクセント（^）が意図したとおりにマップされません。

  [#RFMAC-1107]

- 英語以外の言語のデバイスで、環境設定ペインのUI要素が省略して表示されることがあります。

  [#RFMAC-1113]

このリリースでは、以下の既知の問題が確認されています。

- プロキシ接続を使用すると、EDT経由で通信できません。

  [#664725、#RFMAC-464]

- メニューバーでデスクトップを切断すると、macOS 10.12上でCitrix Viewerが予期せず終了することがあります。デスクトップセッションをログオフする時に、「すべての画面を全画面で使用する」モードが選択されている場合にも、この問題が発生します。

  [#RFMAC-618]

このリリースでは、以下の既知の問題が確認されています。

- プロキシ接続を使用すると、Enlightened Data Transport（EDT）経由で通信できません。

  [#664725]

- VDAのバージョン7.11以前でEDT用に構成されたNetScaler Gatewayを使用すると、TCPへのフォールバックメカニズムが機能しないため、TCPへの接続が失敗します。

[#665617]

このリリースでは、以下の既知の問題が確認されています。

- ユーザーデバイスでプロキシサーバーを構成すると、VDA for Desktop OSでクライアント自動再接続が失敗することがあります。

  [#659683]

- IPV6環境で、SSL（Secure Socket Layer）を有効にした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。

  [#659700]

このリリースでは、以下の既知の問題が確認されています。

- スマートカードへのリダイレクト中、同時接続セッションが同時に実行されていると、Receiverがハングする可能性があります。

  [#511140]

- HDXアプリ画面で、OS XのSplit View機能を使用できないことがあります。

  [#637963]

- USB CD/DVDドライブを一般的なUSBリダイレクトでリダイレクトすると、ドライブがイジェクトされることがあります。

  [#645484]

- USB Optimizationポリシーを［Capture］に設定すると、機能しなくなるUSBデバイスもあります。

  [#649082]

- クライアントの自動再接続プロセス中にUSBデバイスが接続されると、誤って新しいUSBデバイス通知画面が表示されることがあります。

  [#649714]

- Receiver for Mac 12.2にアップグレード後アカウントに接続すると、キーチェーンのメッセージが表示されることがあります。

  [#649885]

- Mac OS X 10.9を実行しているシステムで、HDXセッションで実行されているMicrosoftリモートデスクトップクライアントにスマートカードがアクセスできないことがあります。

[#650298]

- セッションの保持による再接続プロセス中にキーボード入力しても、セッションが再接続されると再生できないことがあります。

  [#652154]

このリリースでは、以下の既知の問題が確認されています。

- Windowsのログオンメッセージの表示中にデスクトップウィンドウのサイズを変更すると、セッションが応答しなくなります。

  [#525833]

- Chromeから仮想デスクトップを起動すると、エラーメッセージが表示されることがあります。

  [#564961]

- ビューアーは正しいキーボードレイアウトをサーバーに送らず、キーボードマッピングの問題が発生します。

  [#581829]

- OS X 10.11（El Capitan）マシンへのセッションでスムースローミングを実行すると、セッションが再接続に成功しないことがあります。最初の再接続に失敗した後、［アプリの更新］メニューコマンドを使って、セッションに再接続します。

  [#601542]

このリリースでは、以下の既知の問題が確認されています。

- セッションからの切断時に公開コマンドプロンプトが最小化されていると、再接続時にコマンドプロンプトが再表示されない可能性があります。

  [#411702]

- HDXアプリが黒色表示となることがあります。この問題が発生したら、アプリケーションをドラッグし、［閉じる］ボタンがあるべき場所をクリックしてそれを閉じます。

  [#426991]

- Mac OS X Mountain Lion（10.8）が動作するコンピューターのユーザーには、Receiverのユーザーインターフェイス上でログオンという文字列とダウンアイコンが重なって表示されることがあります。この場合、ダウンアイコンをクリックする代わりに［ログオン］またはユーザー名の文字列アイコンをクリックできます。

  [#504302]

- マルチモニター構成では、表示が再構成されるとシームレスアプリがプライマリ表示に移動することがあります。

  [#506532]

- DirectXまたはOpenGLアプリケーションを実行中にフルスクリーンに変更すると、カーソルが非表示となります。

  [#510745]

- 複数の証明書がインストールされていて一部の証明書が失効していると、SSL SDKで、証明書チェーンを失効済みと誤ったフラグが設定される可能性があります。キーチェーンアクセスから失効証明書を削除すると、この問題は解決されます。

  [#511574]

- サーバーの言語が繁体字中国語に設定されると、セッション内で"["または"]"を入力できなくなります。

  [#511877]

- 状態の変更がユーザーのアイドル状態に起因する場合、カーソルを移動してもLyncの状態は［退席中］から［連絡可能］に変更されません。この場合、ユーザーは手動で［連絡可能］に状態を変更する必要があります。

  [#512074]

- 更新の前にユーザーがアプリをサブスクライブすると、Receiverで表示されるアプリケーション名はBrokerおよびStoreFrontで更新が反映されません。この問題が発生する場合、ユーザーはアプリを削除してから再度サブスクライブできます。

  [#515097]

- Windowsのログオンメッセージの表示中にデスクトップウィンドウのサイズを変更すると、セッションが応答しなくなる可能性があります。

  [#525833]

- XenDesktop 5.6の認証にGemalto .NETカードのスマートカードを使用すると、セッションを起動できません。

  [#550781]

- PIVスマートカードを使用する場合、ReceiverはXenDesktop 5.6セッションに再接続できません。

  [#550986]

- OS X Mountain Lion（10.8）を使用していて、Receiver 11.9または11.9.15からReceiver 12.0にアップグレードしている場合、Receiverの起動時に新しいバージョンと古いバージョンの両方のReceiverが開く可能性があります。

  [#552496]

- Mac OS X向けのGoogle Chromeブラウザーでダウンロードバーのファイルをダブルクリックすると、複数のICAファイルが起動し、エラーメッセージが表示される可能性があります。

  [#564961]

- Web InterfaceのPNAアカウントへのログオン時に、ユーザーが失効したパスワードを変更できない可能性があります。
  [#568394]
  ビデオ通話セッション中に全画面モードにすると、XenDesktopツールバーのボタン下側が欠ける可能性があります。

  [#570480]

- OS X El Capitan（10.11）では、仮想デスクトップとアプリは通常スプリットビューでは表示されません。

  [#582397]

- OS X Yosemite（10.10）では、Safariのアップグレードバージョンによりポップアップウィンドウとして Receiverがブロックされることがあります。アプリやデスクトップを開くためのポップアップウィンドウを有効にすると、問題が解決します。

システム要件

Sep 25, 2017

Citrix Receiver for Macは、以下のオペレーティングシステムをサポートします。

- macOS High Sierra（10.13）
- macOS Sierra（10.12）
- Mac OS X El Capitan（10.11）
- Mac OS X Yosemite（10.10）

> **注意**
>
> Mac OS X Yosemiteより前のMac OS Xリリースは、サポートされていません。

互換性のあるCitrix製品

Citrix Receiver for Macは、以下のCitrix製品の現在サポートされているバージョンと互換性があります。Citrix製品のライフサイクル、および製品のバージョンごとのサポートが停止される時期について詳しくは、Citrix製品マトリクスを参照してください。

Citrix Receiver for Macは、次のブラウザーと互換性があります。

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

ハードウェア要件

- 140.7MB以上の空きディスク領域
- サーバーに接続するためのネットワークまたはインターネット接続

- Web Interface：
  - アプリケーションに（Webブラウザーからではなく）Citrix Receiver for Macでアクセスする場合は、Web Interface 5.4 for WindowsとXenApp Servicesサイト（Program Neighborhoodエージェントサービスサイト）。
- Citrix Receiver for Macを展開するには
  - Citrix Receiver for Web 2.1、2.5、および2.6
  - Citrix Web Interface 5.4
- StoreFront：
  Citrix Receiver for MacまたはWebブラウザーからアプリケーションにアクセスする場合は、StoreFront 2.x以降。

OS X El CapitanでユーザーがCitrix Receiver for Macを実行していて、また接続に問題がある場合、NetScaler Gateway Plugin をアップグレードします。詳しくは、Citrixダウンロードページのアーティクル「NetScaler Gateway Plug-in v3.1.4 for Mac OS X (El Capitan Support)」を参照してください。

Citrix Receiver for Macは、XenAppまたはXenDesktopへの以下の接続をサポートします。

- HTTP
- HTTPS
- ICA-over-TLS

Citrix Receiver for Macは以下の構成をサポートします。

LAN接続	セキュリティ保護されたリモートまたはローカルの接続
• StoreFront ServicesサイトまたはCitrix Receiver for Mac for Webサイトを使用するStoreFront • Web Interface 5.4 for WindowsとXenApp Servicesサイト	Citrix NetScaler Gateway： • VPXを含む12.0 • VPXを含む11.1 • VPXを含む11.0 • VPXを含む10.5 • VPXを含むEnterprise Edition 10.x • VPXを含むEnterprise Edition 9.x • VPX Citrix Secure Gateway 3.x（Web Interfaceを使用する環境でのみ）

StoreFrontとNetScaler Gatewayの展開については、NetScaler GatewayとStoreFrontのドキュメントを参照してください。

StoreFrontへの接続では、Citrix Receiver for Macで以下の認証方法がサポートされます。

	ブラウザーを使ったReceiver for Web	StoreFront Servicesサイト（ネイティブ）	StoreFront XenApp Servicesサイト（ネイティブ）	NetScalerからReceiver for Web（ブラウザー）	NetScalerからStoreFront Servicesサイト（ネイティブ）
匿名	はい	はい			
ドメイン	はい	はい		はい *	はい *
ドメインパススルー					
セキュリティトークン				はい *	はい *
2要素（セキュリティトークンがあるドメイン）*				はい *	はい *
SMS				はい *	はい *

	ブラウザーを使ったReceiver for Web	StoreFront Servicesサイト（ネイティブ）	StoreFront XenApp Servicesサイト（ネイティブ）	NetScalerからReceiver for Web（ブラウザー）	NetScalerからStoreFront Servicesサイト（ネイティブ）
スマートカード**	はい	はい	はい	はい	はい
ユーザー証明書				はい	はい（NetScaler Gateway Plugin）

*Receiver for WebサイトおよびNetScaler Gatewayを含む展開に対してのみ使用できます（デバイスへの関連プラグインのインストールは関係なし）。

**OS X 10.10でスマートカードを使用するには、OS X 10.10.2以上をインストールする必要があります。

Web Interface 5.4への接続では、Citrix Receiver for Macで以下の認証方法がサポートされます。
注：（Web Interfaceでは、指定ユーザーによる認証がドメイン+セキュリティトークン認証に相当します）。

	Web Interface（ブラウザー）	Web Interface XenApp Servicesサイト	NetScalerからWeb Interface（ブラウザー）	NetScalerからWeb Interface XenApp Servicesサイト
匿名	はい			
ドメイン	はい	はい	はい	はい
ドメインパススルー				
セキュリティトークン			はい *	はい
2要素（セキュリティトークンがあるドメイン）*			はい *	はい
SMS			はい *	はい
スマートカード**	はい		はい	
ユーザー証明書			はい（NetScaler Gateway Pluginが必要）	はい（NetScaler Gateway Pluginが必要）

* NetScaler Gatewayを展開する環境でのみ使用できます（デバイスへの関連プラグインのインストールは関係なし）。

Citrix Receiver for Macは次の構成においてスマートカード認証をサポートします。

- Receiver for Web/StoreFront 2.x以降、XenDesktop 7.1以降、XenApp 6.5以降に対して、スマートカード認証を提供します。

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

NetScalerに対するスマートカード認証について

スマートカードを使って接続を認証する場合、スマートカードに複数の使用可能な証明書が入っていると、証明書を選択するようCitrix Receiver for Macがプロンプトを表示します。証明書を選択したら、スマートカードのパスワードを入力するようにCitrix Receiver for Macからプロンプトが表示され、認証が実行されてセッションが開始します。

スマートカードにある証明書のうち適切なものが1つだけの場合は、Citrix Receiver for Macはその証明書を使用し、選択を求めるプロンプトは表示されません。ただし、接続を認証してセッションを開始するために、スマートカードに割り当てられたパスワードを入力する必要はあります。

スマートカード認証用のPKCS#11モジュールの指定

注：IPKCS#11モジュールのインストールは必須ではありません。

スマートカード認証用のPKCS#11モジュールを指定するには

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

サポートされるリーダー、ミドルウェア、スマートカードプロファイル

Citrix Receiver for Macは多くのMac OS X互換スマートカードリーダーおよび暗号化ミドルウェアをサポートします。Citrixは次の操作について検証済みです。

サポートされるスマートカードリーダー：

- 一般的なUSB接続スマートカードリーダー

サポートされるミドルウェア：

- Clariify
- Activeidentityクライアントのバージョン
- Charismathicsクライアントのバージョン

サポートされているスマートカード：

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

ユーザーデバイスを構成するため、ベンダーのMac OS X互換スマートカードリーダーおよび暗号化ミドルウェアにより提供

された指示に従います。

制限事項

- 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 Receiver for Macでは、ユーザーの選択した証明書が保存されません。
- Citrix Receiver for Macでは、ユーザーのスマートカードPINが格納または保存されません。PINの取得はオペレーティングシステムにより処理され、独自のキャッシングメカニズムがある場合があります。
- Citrix Receiver for Macでは、スマートカードが挿入された時に自動的には切断セッションに再接続されません。
- スマートカード認証でVPNトンネルを使用するには、ユーザーがNetScaler 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、NetScaler 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。

追加情報

詳しくは、次のトピックを参照してください。

- Configuring Citrix XenDesktop 7.6 and NetScaler Gateway 10.5 with PIV SmartCard Authentication（PDF）
- Smart Card Support with Citrix Receiver for Mac 11.9.15 on OS X 10.10.2

スマートカード認証用の要件

Sep 25, 2017

Citrix Receiver for Macは次の構成においてスマートカード認証をサポートします。

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

NetScalerに対するスマートカード認証について

スマートカードを使って接続を認証する場合、スマートカードに複数の使用可能な証明書が入っていると、証明書を選択するようCitrix Receiver for Macがプロンプトを表示します。証明書を選択したら、スマートカードのパスワードを入力するようにCitrix Receiver for Macからプロンプトが表示され、認証が実行されてセッションが開始します。

スマートカードにある証明書のうち適切なものが1つだけの場合は、Citrix Receiver for Macはその証明書を使用し、選択を求めるプロンプトは表示されません。ただし、接続を認証してセッションを開始するために、スマートカードに割り当てられたパスワードを入力する必要はあります。

スマートカード認証用のPKCS#11モジュールの指定

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

スマートカード認証用のPKCS#11モジュールを指定するには

1. Citrix Receiverで **[基本設定]** を選択します。
2. **[Security & Privacy]** をクリックします。
3. **[Security & Privacy]** セクションで、**[スマートカード]** をクリックします。
4. **PKCS#11**フィールドで適切なモジュールを選択します。一覧に必要なモジュールがない場合は、**[その他]** をクリックしてPKCS#11モジュールの場所を参照します。
5. 適切なモジュールを選択したら、**[追加]** をクリックします。

Citrix Receiver for Macは多くのmacOS互換スマートカードリーダーおよび暗号化ミドルウェアをサポートします。Citrixは次の操作について検証済みです。

サポートされるスマートカードリーダー：

- 一般的なUSB接続スマートカードリーダー

サポートされるミドルウェア：

- Clariify
- Activeidentityクライアントのバージョン
- Charismathicsクライアントのバージョン

サポートされているスマートカード：

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

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

- 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 Receiver for Macでは、ユーザーの選択した証明書が保存されません。
- Citrix Receiver for Macでは、ユーザーのスマートカードPINが格納または保存されません。PINの取得はオペレーティングシステムにより処理され、独自のキャッシングメカニズムがある場合があります。
- Citrix Receiver for Macでは、スマートカードが挿入されたときに自動的には切断セッションに再接続されません。
- スマートカード認証でVPNトンネルを使用するには、ユーザーがNetScaler 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、NetScaler 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。

以下の情報も参照してください。

- Smart Card Support with Citrix Receiver for Mac 11.9.15 on OS X 10.10.2

Citrix Receiver for Macのインストール、セットアップ、アップグレード、展開、またはアンインストール

Sep 25, 2017

Citrix Receiver for Macのこのリリースは単一のインストールパッケージCitrixReceiver.dmgで提供されており、NetScaler GatewayおよびSecure Gatewayを使用したリモートアクセスをサポートしています。

ここでは次のことについて説明します。

Citrix Receiver for Macは、Citrix WebサイトでReceiver for WebまたはWeb Interfaceから自動的に、またはElectronic Software Distribution（ESD）ツールを使用してインストールできます。

ユーザーによるCitrix.comからのインストール:

- Citrix Receiver for Macを初めて使用するユーザーがCitrix Receiver for Macのインストールファイルを Citrix.comなどのダウンロードサイトから入手した場合は、サーバーURLの代わりにメールアドレスを入力してアカウントをセットアップできます。これにより、メールアドレスに関連付けられたNetScaler GatewayやStoreFrontサーバーが識別され、ログオン用のメッセージが表示されてインストールを続行します。この機能は、メールベースのアカウント検出と呼ばれます。

> **注意**
>
> 初めて使用するユーザーとは、デバイスにCitrix Receiver for Macをインストールしていないユーザーを指します。

- Citrix.com以外の場所（Receiver for Webサイトなど）からCitrix Receiver for Macをダウンロードした場合は、メールアドレスによるアカウントセットアップを使用できません。
- Receiverの構成が必要な環境では、ほかの方法でReceiverをユーザーに配布してください。

Receiver for WebサイトまたはWeb Interfaceからの自動インストール

- Citrix Receiver for Macを初めて使用するユーザーがアカウントをセットアップするには、サーバーのURLを入力するかプロビジョニングファイルをダウンロードします。

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

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

ユーザーは、管理者が用意したWeb Interfaceやネットワーク共有を使用したり、Citrix社のWebサイト（http://www.citrix.com）からCitrixReceiver.dmgを直接ダウンロードしたりして、Citrix Receiver for Macをインストールできます。

Citrix Receiver for Macをインストールするには

1. Citrix社のWebサイトから、適切なバージョンのCitrix Receiver for MacのDMGファイルをダウンロードして開きます。
2. ［はじめに］ページで **[続ける]** をクリックします。
3. **［使用許諾契約］**ページで **[続ける]** をクリックします。
4. 使用許諾契約の内容を確認して、 **[同意する]** をクリックします。
5. **［インストールの種類］**ページで、 **［インストール］** をクリックします。
6. ローカルデバイスに管理者のユーザー名とパスワードを入力します。

Online Plug-in for Mac Version 11.xからのアップグレードがサポートされています。また、Citrix Receiver for Macは、以前のどのバージョンからもアップグレードできます。

> ## Important
>
> ShareFileとの統合機能は、バージョン11.8から削除されています。Receiver for MacとShareFileを統合した場合は、アップグレード時にShareFileアプリケーションのダウンロードを確認するメッセージが表示されます。このアプリケーションを使用して、引き続きリモートデータにアクセスできます。

StoreFront環境：

- Netscaler GatewayおよびStoreFrontのドキュメントを参照して、NetScaler GatewayおよびStoreFront 3.xを構成してください。StoreFrontにより作成されたプロビジョニングファイルをメールに添付して、アップグレード方法およびCitrix Receiver for Macのインストール後にプロビジョニングファイルを開く方法をユーザーに通知します。
- プロビジョニングファイルを使用する代わりに、どちらかのNetScaler GatewayのURLを入力するようユーザーに指示します。StoreFrontのドキュメントで説明されているメールアドレスによるアカウント検出を構成済みの場合は、自分のメールアドレスを入力するようにユーザーに指示します。
- また、Receiver for Webサイトを構成する方法もあります。詳しくは、StoreFrontのドキュメントを参照してください。Citrix Receiver for Macのアップグレード方法、Receiver for Webサイトへのアクセス方法、Receiver for Webサイトからのプロビジョニングファイルのダウンロード方法（ユーザー名をクリックしてから［アクティブ化］をクリック）をユーザーに通知します。

Web Interfaceで展開する場合：

- Web InterfaceサイトをReceiver for Macでアップグレードして、ユーザーにCitrix Receiver for Macのアップグレード方法を通知します。たとえば、ユーザーの［メッセージ］画面に、Citrix Receiver for Macのアップグレードを確認するメッセージを表示できます。

Citrix Receiver for MacをReceiver for Webサイトからユーザーに配布すると、Webブラウザーからアプリケーションにアクセ

スするユーザーに確実にReceiverをインストールさせることができます。Receiver for Web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。Receiver for Webサイトで適切なバージョンのCitrix Receiver for Macがインストールされていないことが検出されると、Citrix Receiver for Mac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。詳しくは、StoreFrontのドキュメントを参照してください。

この機能は、Web InterfaceをサポートしているXenDesktopおよびXenAppリリースでのみ使用できます。

Web Interfaceのログオン画面でReceiverをユーザーに配布すると、ユーザーがWeb Interfaceを使用する前に確実にCitrix Receiver for Macをインストールできます。Web Interfaceでは、Citrixクライアントソフトウェアを検出して必要に応じてインストールするための機能が提供されます。この機能により、ユーザーは自分の環境に適したソフトウェアをインストールできます。

管理者は、ユーザーがXenApp Webサイトにアクセスしたときに自動的にクライアント検出および展開処理が実行されるように構成できます。Web Interfaceで適切なバージョンのReceiverがインストールされていないことが検出されると、Receiver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。

詳しくは、Web Interfaceのドキュメントの「クライアント展開の構成」を参照してください。

Citrix Receiver for Macをアンインストールするには、CitrixReceiver.dmgを開き、**[Uninstall Citrix Receiver]** をダブルクリックして、画面に表示される指示に従って操作します。

Citrix Receiver for Macの構成

Sep 25, 2017

ホストされているアプリケーションやデスクトップにユーザーがアクセスできるようにするには、Citrix Receiver for Macソフトウェアをインストールした後で、以下の構成を行う必要があります。

- USBリダイレクトの設定
- セッション画面の保持の構成
- CEIPの構成
- アプリケーション配信の構成 - XenApp環境を正しく構成します。オプションについて理解し、ユーザーに対しわかりやすいアプリケーションについての説明を提供します。
- セルフサービスモードの構成 - セルフサービスモードを構成します。これにより、ユーザーがCitrix Receiver for Mac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。
- StoreFrontの構成 - このストアにより、XenDesktopサイトおよびXenAppファームからデスクトップとアプリケーションが列挙および集約され、これらのリソースをユーザーが使用できるようになります。
- ユーザーへのアカウント情報の提供 - ユーザーがアカウントをセットアップするための情報を提供します。ユーザーは、このアカウントを使用してアプリケーションやデスクトップにアクセスします。環境によっては、ユーザーが手作業でアカウントをセットアップする必要があります。
- 自動更新の構成
- 外部から接続するユーザー（遠隔地からまたはインターネット経由で接続するユーザーなど）にアクセスを提供するには、NetScaler Gatewayを使用した認証を構成します。詳しくは、「Netscaler Gateway」を参照してください。

HDX USBデバイスリダイレクト機能を使用すると、USBデバイスのクライアント側へのリダイレクトおよびクライアント側からのリダイレクトが有効になります。たとえば、ユーザーがデスクトップでホストされるアプリケーションや仮想デスクトップを使用している時に、ローカルのユーザーデバイスに装着したUSBフラッシュドライブにアクセスできるようになります。セッション内で、デジタルカメラなどの画像転送プロトコル（PTP）デバイス、デジタルオーディオプレーヤーやポータブルメディアプレーヤーなどのメディア転送プロトコル（MTP）デバイス、POS（Point-Of-Sale）デバイス、3D SpaceMouse、スキャナー、署名パッドなどの他のデバイスをユーザーデバイスに接続して使用できます。

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

以下のCitrix Receiver for MacでUSBリダイレクトを使用できます。

- Windows：
- Linux：
- Macintosh

USBリダイレクトのデフォルトでは、特定のクラスのUSBデバイスでのみ許可され、ほかのクラスのデバイスはリダイレクトされません。管理者は、リダイレクトするUSBデバイスの一覧を変更して、仮想デスクトップで使用可能になるUSBデバイスの種類を制限できます。詳しくは、このセクションで後述する説明を参照してください。

> **ヒント**
>
> ユーザーデバイスとサーバー間でセキュリティ境界による分離が必要な環境では、使用を禁止するUSBデバイスの種類についてユー

ザーに通知することをお勧めします。

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

注意

Citrix Receiver for MacのUSBリダイレクトでSMARTボードを使用する場合、マウスとして処理されます。

ただし、最適化された仮想チャネルでUSB 3.0デバイスおよびUSB 3.0ポートを使用して、CDM仮想チャネルを使用してカメラ内のファイルを表示したり、ヘッドセットでオーディオを再生したりできます。USB 3.0デバイスをUSB 2.0ポートに接続した場合も、汎用USBリダイレクトがサポートされます。

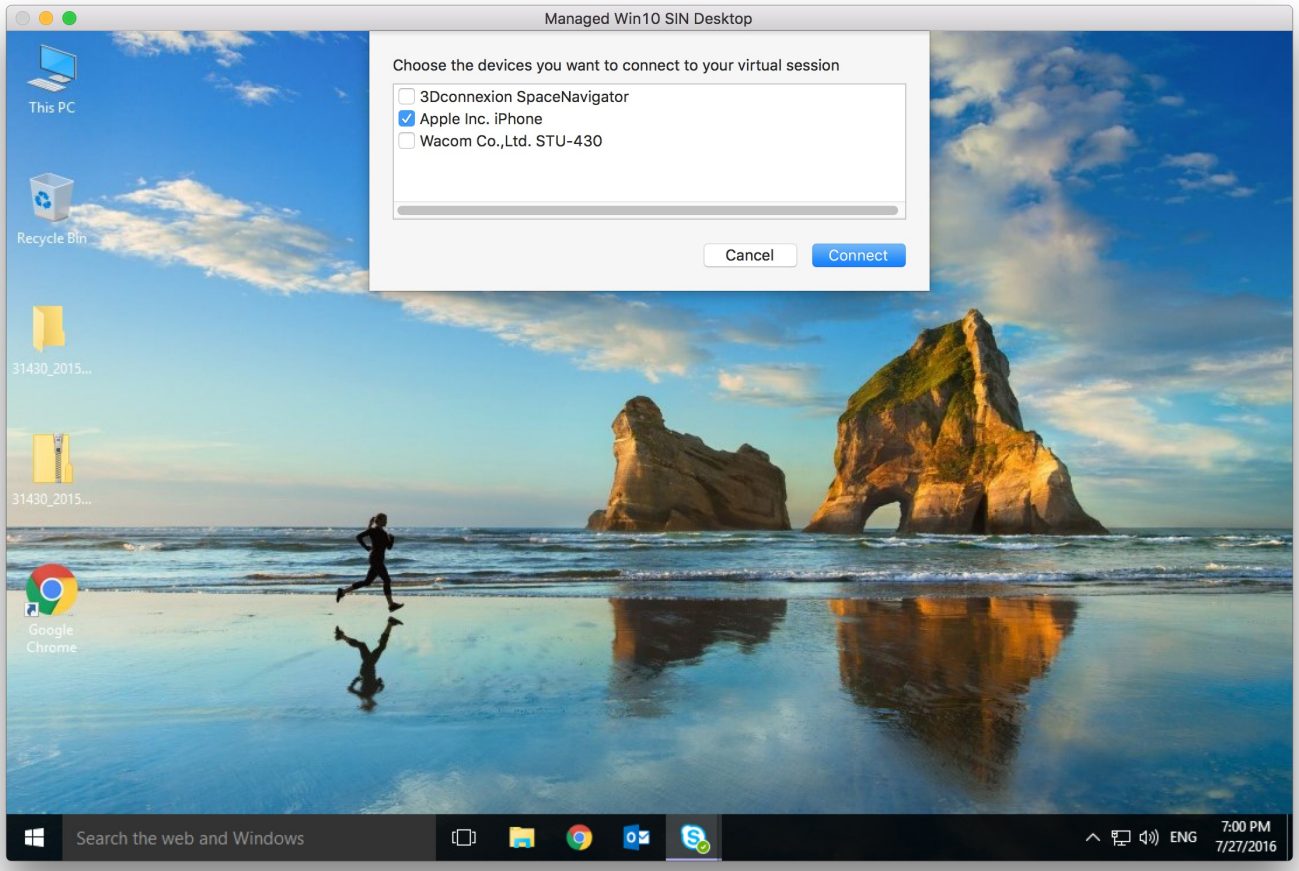
Webカメラのヒューマンインターフェイスデバイス（HID）ボタンなど、一部のデバイス固有の機能は、最適化された仮想チャネルで正しく動作しない場合があります。問題が発生する場合は、汎用USB仮想チャネルを使用してください。

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

USBリダイレクトを使用するには

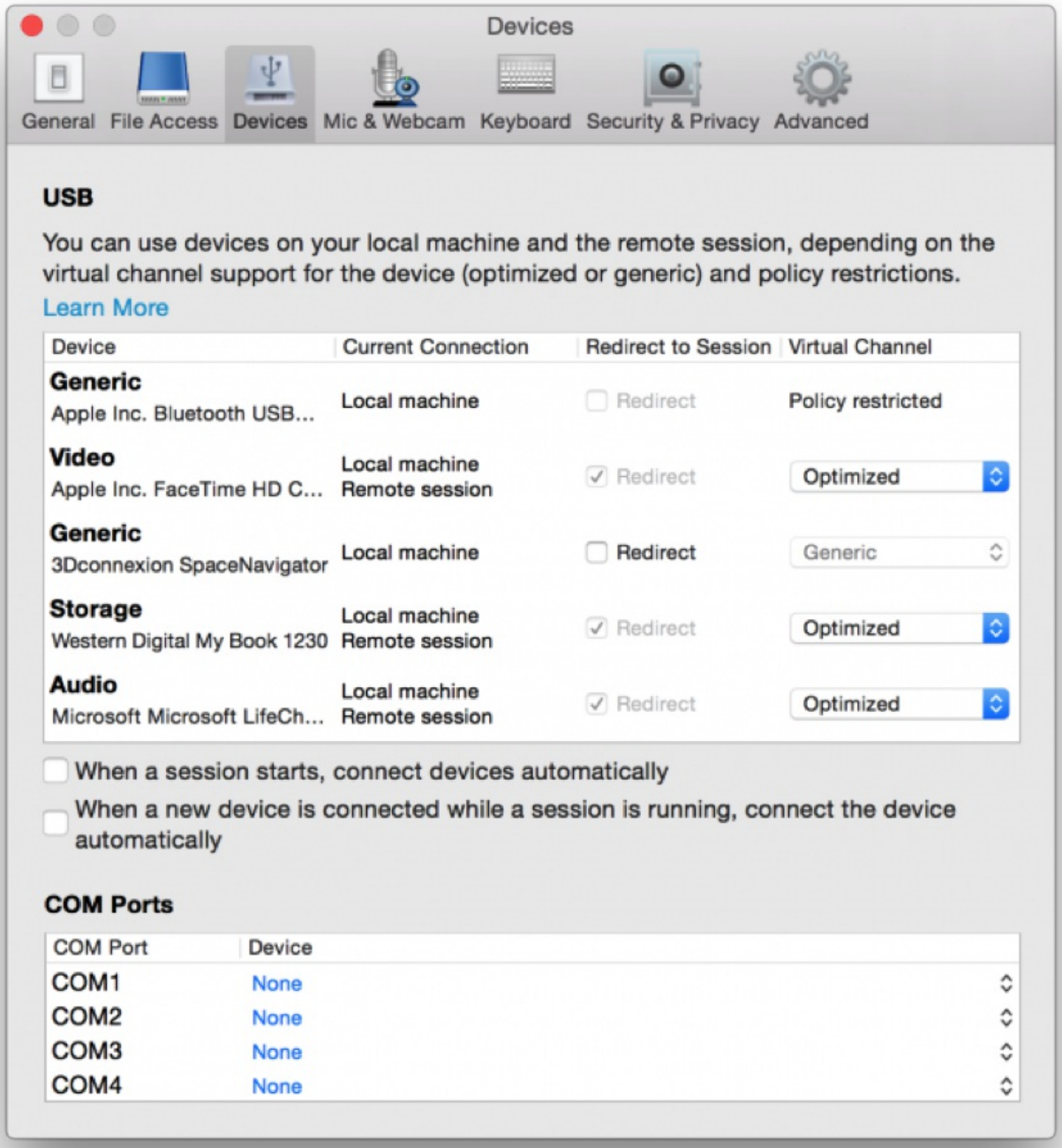
1. USBデバイスをReceiverがインストールされたデバイスに接続します。

2. ローカルシステムで、使用できるUSBデバイスを選択するメッセージが表示されます。



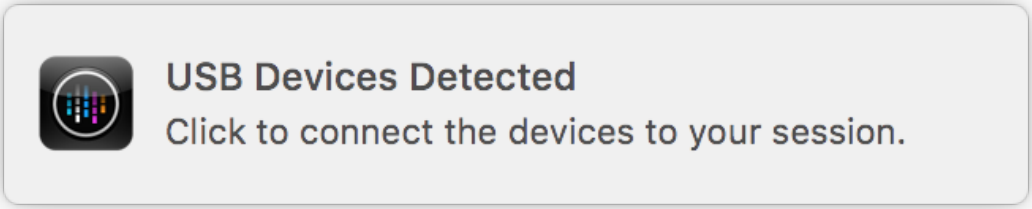
3. 接続するデバイスを選択して、**[接続]**をクリックします。接続できない場合は、エラーメッセージが表示されます。

4. **[環境設定]**画面の**[デバイス]**タブで、接続されたUSBデバイスがUSBパネルに一覧表示されます。



5. USBデバイスの仮想チャネルの種類で*汎用*または*最適化*を選択します。

6. メッセージが表示されます。クリックしてUSBデバイスをセッションに追加します。



USBデバイスの装着と取り外し

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

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

Enlightened Data Transport（EDT）の構成

Citrix Receiver for Macでは、デフォルトでEDTが有効になっています。

Citrix Receiver for Macは、デフォルトの.icaファイルに設定されたEDT設定を読み取り、適切に適用します。

EDTを無効にするには、ターミナルで次のコマンドを実行します。

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

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

セッション画面の保持機能を有効にすると、データを損失することなく、サーバー上のセッションがアクティブのまま保持されます。ネットワークが中断されると、セッション画面が停止するため、ユーザーにもネットワークが切断されていることがわかります。この時、セッションウィンドウが閉じたりエラーメッセージが表示されたりする代わりに画面表示が保持され、バックグラウンドで再接続が試行されます。ネットワーク接続が回復すると、自動的にセッションでの作業を再開できるようになります。また、セッションに再接続する時に再認証用のログオン画面が表示されないため、ユーザーは即座に作業を再開できます。

> **Important**
>
> Citrix Receiver for Macのユーザーは、サーバー側の設定を上書きできません。

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

> **注意**
>
> TLSはユーザーデバイスとNetScaler Gateway間で送信されるデータのみを暗号化します。

セッション画面の保持ポリシーを使用する

[セッション画面の保持] ポリシー設定により、セッション画面の保持を許可または禁止します。

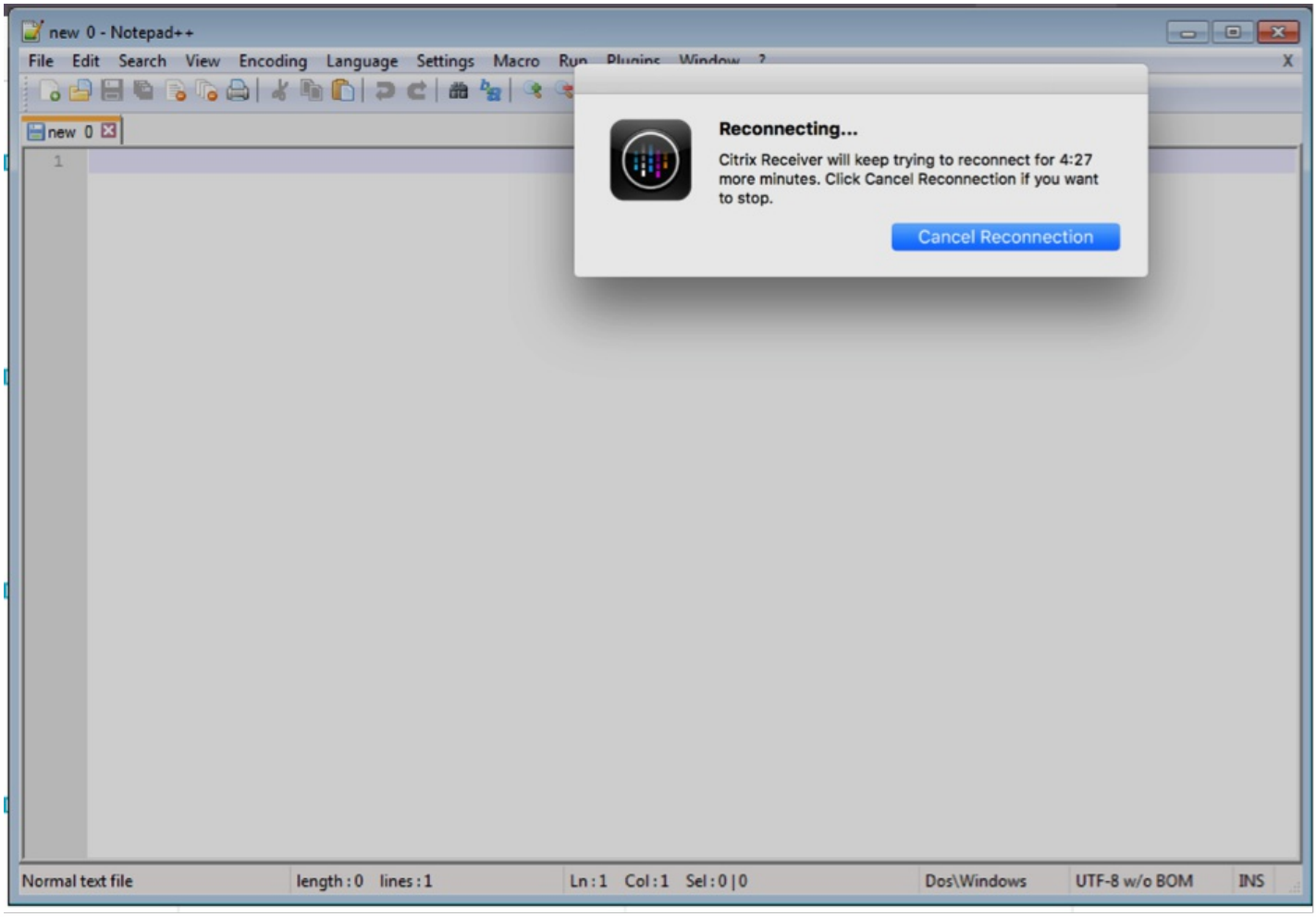
[セッション画面の保持のタイムアウト] ポリシー設定は、デフォルトで180秒つまり3分です。この時間を長く設定することもできますが、この機能の本来の目的は、ネットワークから切断されたユーザーを再認証することなくセッションに再接続することにあるので注意が必要です。

> **ヒント**
>
> 必要以上に長い時間を設定すると、接続の再開を待ちきれないユーザーが席を離れてしまい、その間に不正なユーザーがセッションにアクセスしてしまう危険性があります。

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

切断したセッションに再接続するユーザーを再認証する場合は、クライアントの自動再接続機能を使用します。［クライアントの自動再接続時の認証］設定を構成して、中断されたセッションにユーザーが再接続する時に再認証を要求することができます。

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



注意

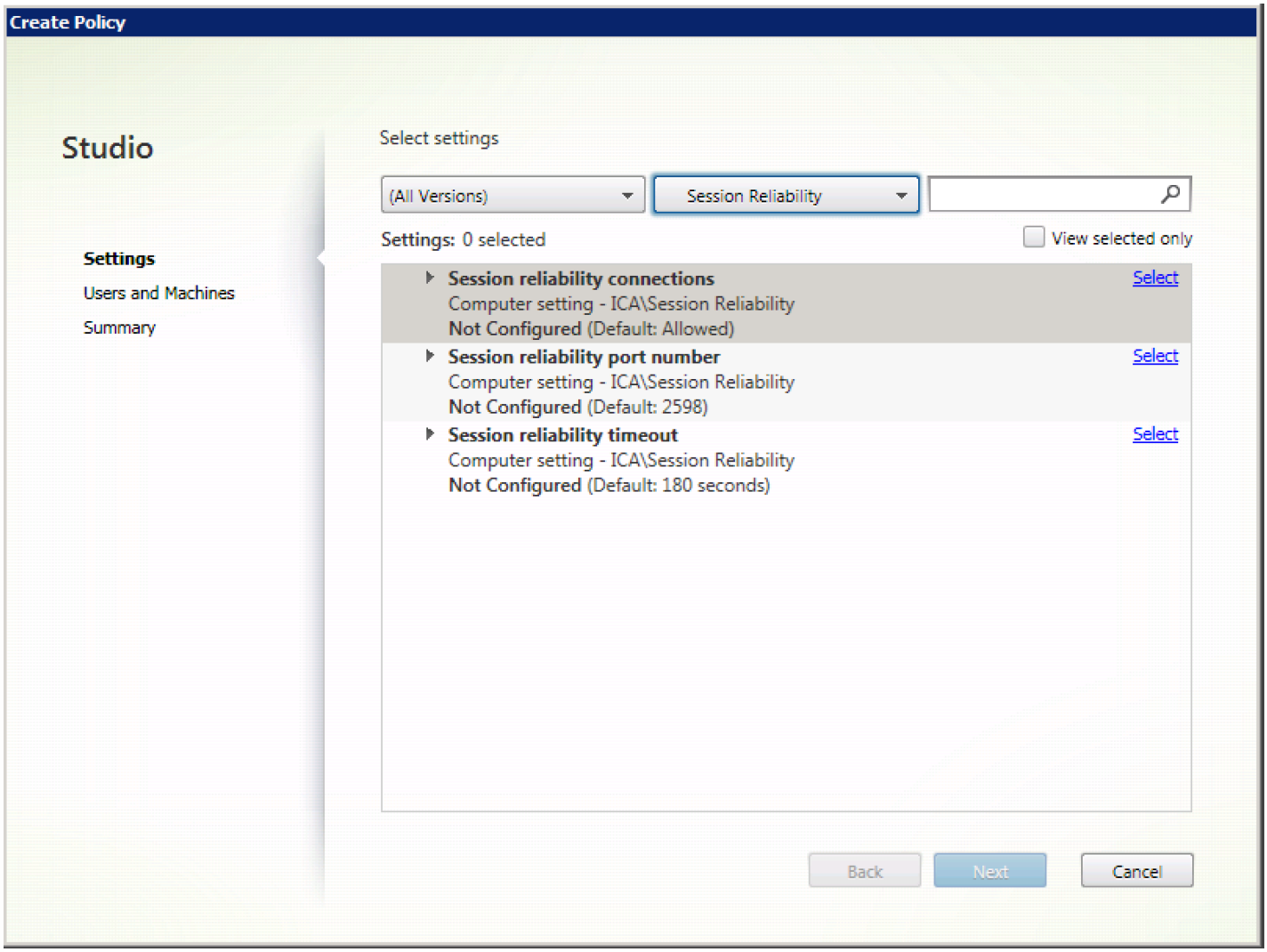
セッション画面の保持は、サーバーでデフォルトで有効になっています。この機能を無効にするには、サーバーで管理するポリシーを構成します。

セッション画面の保持を設定する

デフォルトでは、セッション画面の保持機能は有効になっています。

セッション画面の保持を無効にするには

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



セッション画面の保持のタイムアウトを設定する

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

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

セッション画面の保持のタイムアウトを変更するには

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

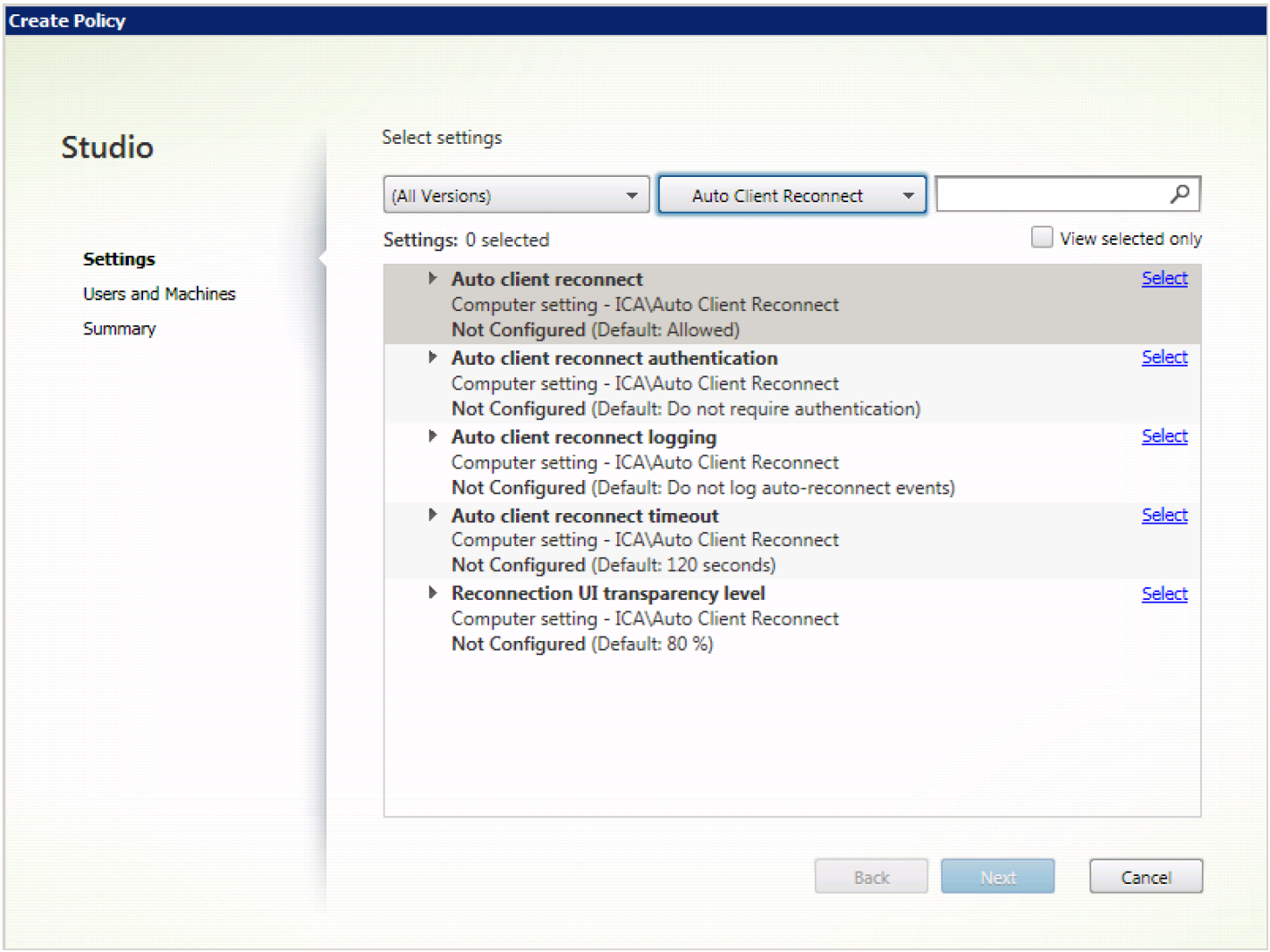
クライアントの自動再接続を設定する

デフォルトでは、自動再接続機能は有効になっています。

自動再接続を無効にするには

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

3. ポリシーを［禁止］に設定します。



クライアントの自動再接続のタイムアウトを設定する

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

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

クライアントの自動再接続のタイムアウトを変更するには

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

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

再接続ユーザーインターフェイスの透明度レベルの設定

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

デフォルトでは、再接続UIの透明度は、80に設定されています。

再接続ユーザーインターフェイスの透明度レベルを変更するには

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

クライアントの自動再接続とセッション画面の保持の操作

さまざまなアクセスポイント間での切り替え、ネットワークの中断、遅延による表示のタイムアウトなど、モバイルに伴う課題は、アクティブなCitrix Receiverセッションのリンクの整合性を保持しようとする時に問題になります。この問題を解決するために、Receiver for Macのこのバージョンでは、セッション画面の保持および自動再接続テクノロジが強化されました。

自動再接続およびセッション画面の保持機能によって、ネットワークの中断からの回復後、Citrix Receiverセッションに自動的に再接続できます。これらの機能は、Citrix Studioのポリシーで有効にでき、ユーザーエクスペリエンスを大幅に向上できます。

> **注意**
>
> クライアントの自動再接続およびセッション画面の保持のタイムアウト値は、StoreFrontの**default.ica**ファイルを使用して変更できます。

クライアントの自動再接続

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

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

設定	例	デフォルト
TransportReconnectRetryMaxTimeSeconds	TransportReconnectRetryMaxTimeSeconds=60	120

セッション画面の保持

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

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

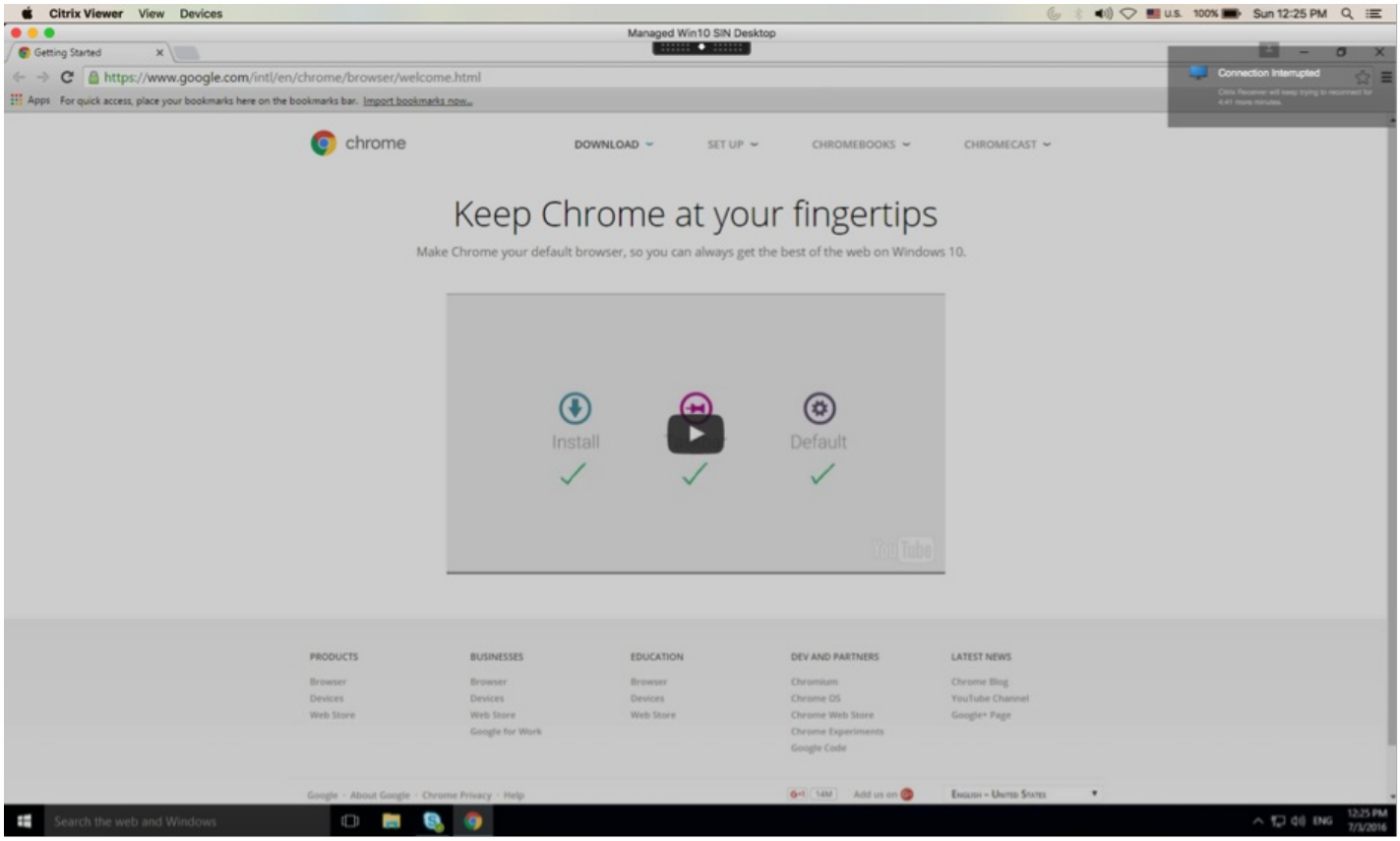
設定	例	デフォルト
SessionReliabilityTTL	SessionReliabilityTTL=120	180

クライアントの自動再接続およびセッション画面の保持の仕組み

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

- 再接続の進行中は、アクティブなセッション画面は淡色表示され、カウントダウンタイマーがセッションが切断されるまでの残り時間を表示します。セッションがタイムアウトになると、接続は切断されます。

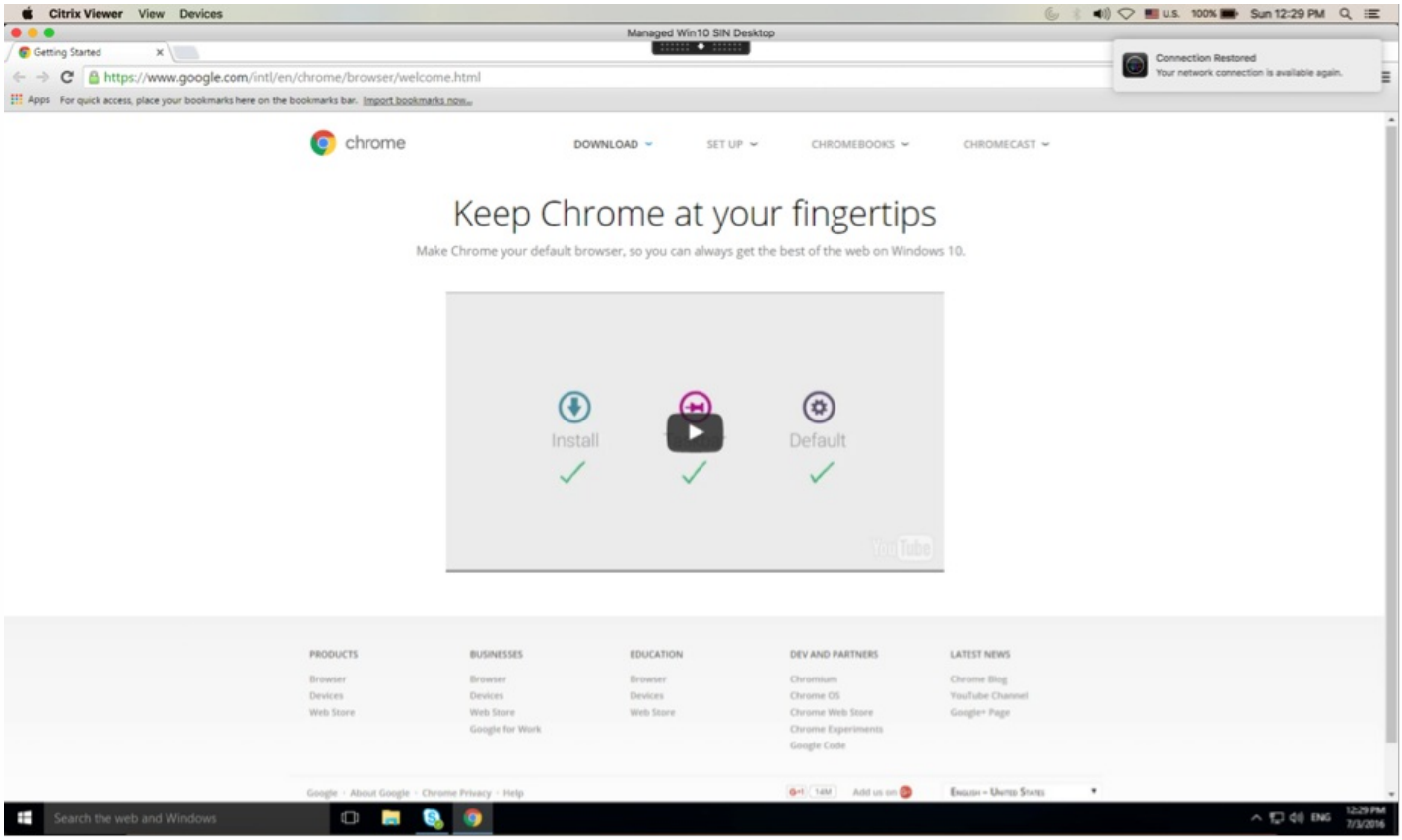
デフォルトでは、再接続のカウントダウンタイマーの通知は5分です。これは、自動再接続のデフォルトの値（2分）およびセッション画面の保持のデフォルトの値（3分）を組み合わせた値です。以下の図は、セッションインターフェイスの右上に表示されるカウントダウンタイマーの通知です。



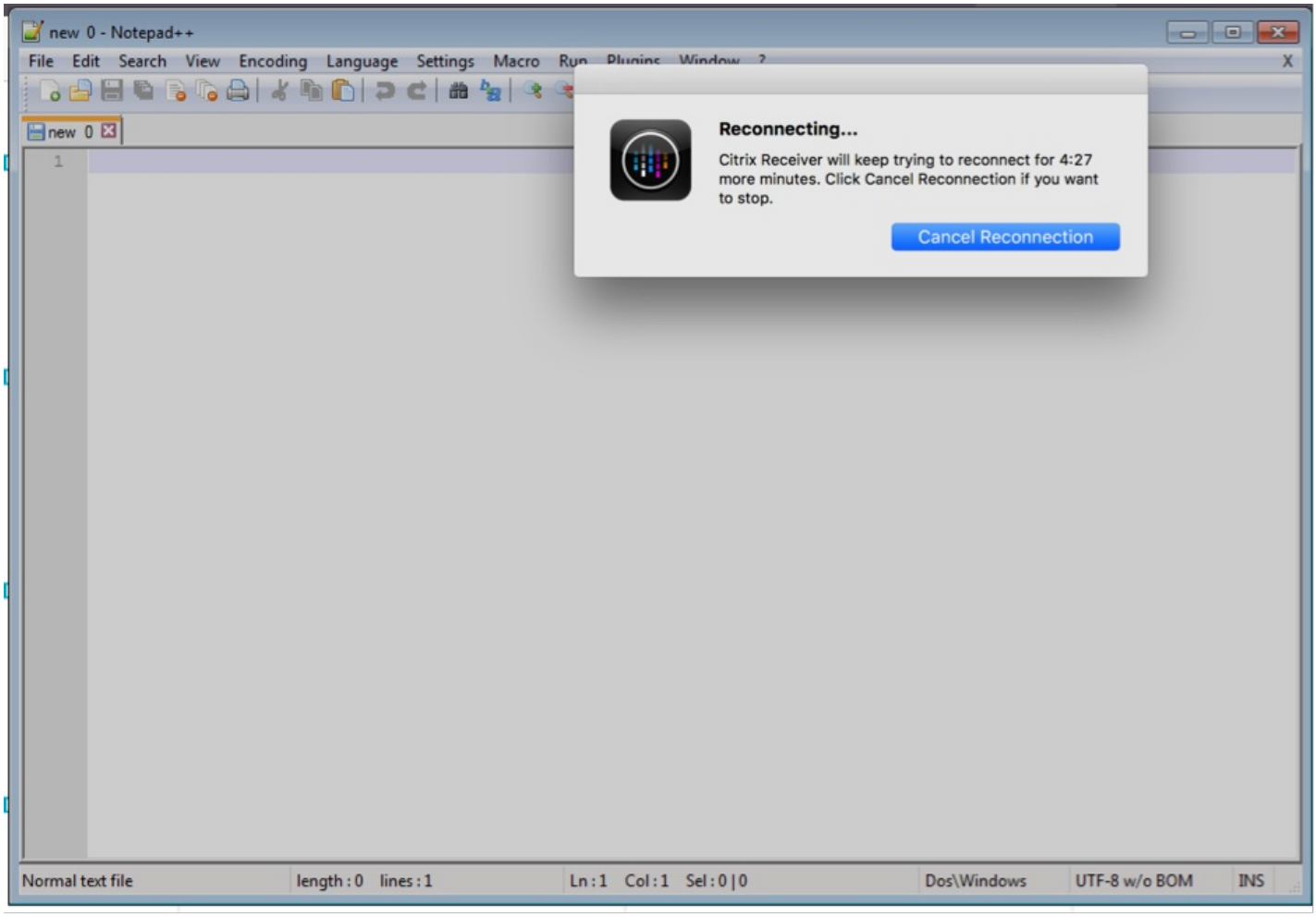
ヒント

非アクティブなセッションに使用されるグレースケールの明るさは、コマンドプロンプトを使用して変更できます。たとえば、次のようになります。defaults write com.citrix.receiver.nomas NetDisruptBrightness 80。デフォルト値は、80に設定されています。最大値は100（半透明の画面）より上に設定できません。最小値は0（完全に黒くなった画面）に設定できます。

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



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



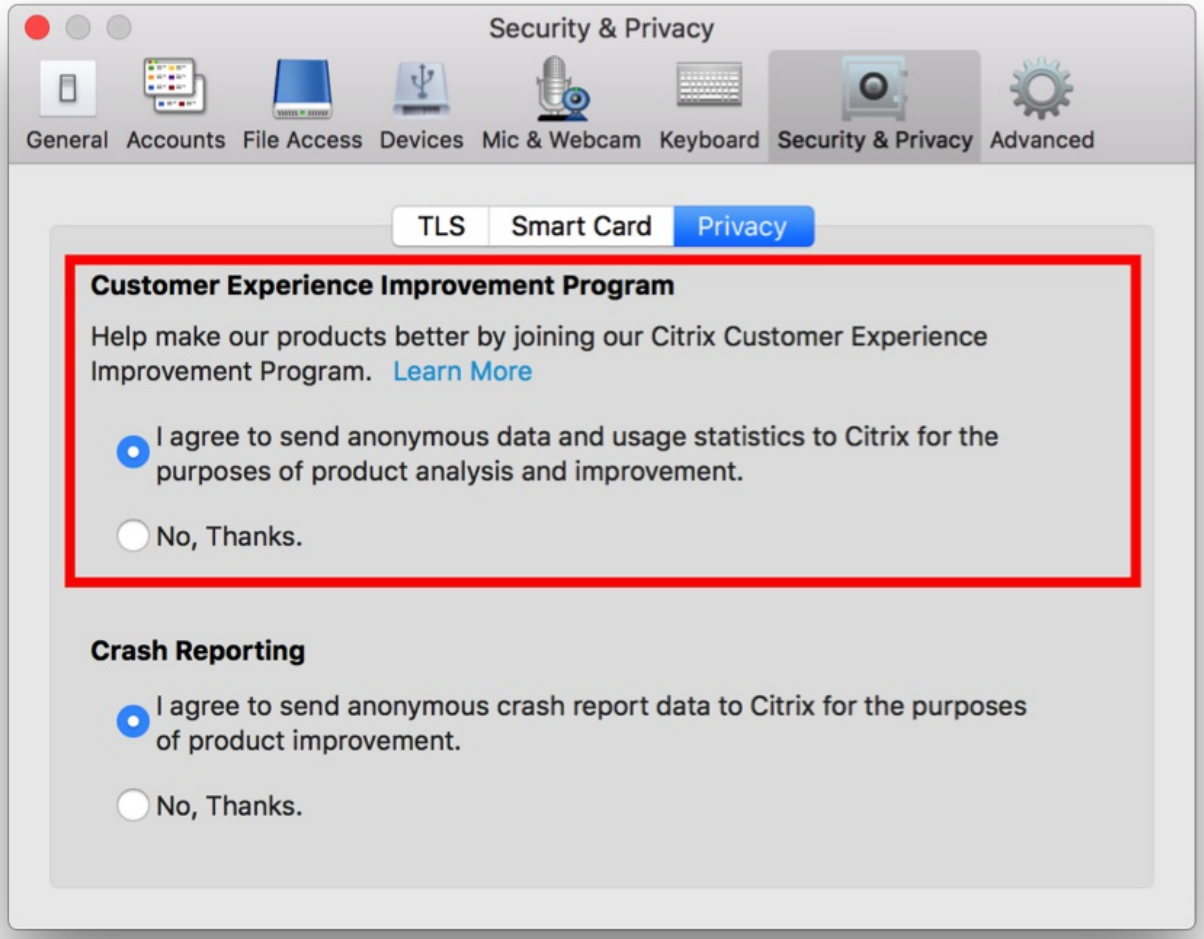
CEIPは、7日ごとにデータを収集してからCitrixに安全にアップロードするように、デフォルトでスケジュールされています。CEIPに参加するかどうかは、［Citrix Receiver for Mac］>> **[セキュリティ] > [基本設定]** 画面でいつでも変更できます。

ヒント

CEIPが無効になると、インストールされたCitrix Receiver for Macバージョンの最小限の情報のみが、一度だけアップロードされます。この最小限の情報は、お客様が使用されているさまざまなバージョンの分布状況を把握する上で、大変に貴重です。これは、CEIPが無効にされた直後の一度しか機能しません。

CEIPを無効にする、または参加をやめるには

1. **[環境設定]** ウィンドウで **[セキュリティとプライバシー]** を選択します。
2. **[Privacy]** タブを選択します。
3. 適切なラジオボタンを変更します。たとえば、CEIPを無効にするには、**[いいえ]** をクリックします。
4. **[OK]** をクリックします。



XenDesktopまたはXenAppでアプリケーションをユーザーに配信する時は、ストアのアプリケーションにアクセスするユーザーのエクスペリエンスを向上させるために、次のオプションについて検討します。

Webアクセスモード

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

セルフサービスモード

StoreFrontアカウントをCitrix Receiver for Macに追加したり、StoreFrontサイトをポイントするようにCitrix Receiver for Maを構成して、セルフサービスモードを構成できます。これにより、ユーザーはCitrix Receiver for Mac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、お勧めのアプリケーションキーワード設定を

構成できます。いずれかのユーザーがアプリケーションを選択すると、そのアプリケーションに対するショートカットがユーザーデバイスのアプリケーションフォルダーに置かれます。

StoreFront 3.0サイトにアクセスすると、Citrix Receiver for Mac Tech Previewユーザーエクスペリエンスを実行できます。Citrix Receiver for Mac Tech Previewユーザーエクスペリエンスについて詳しくは、「ReceiverおよびStoreFront 3.0 Technology Preview」を参照してください。

XenAppファームでアプリケーションを公開する場合、StoreFrontストアを介したアプリケーションへのユーザーアクセスの利便性を高めるため、公開アプリケーションについてわかりやすい説明を付加してください。この説明は、Citrix Receiver for Macを介してユーザーに表示できます。

前述のとおり、StoreFrontアカウントをCitrix Receiver for Macに追加したり、StoreFrontサイトをポイントするようにCitrix Receiver for Macを構成して、セルフサービスモードを構成できます。これにより、ユーザーはCitrix Receiver for Mac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、お勧めのアプリケーションキーワード設定を構成できます。

- アプリケーションがストアのユーザー全員に自動的にサブスクライブされるようにするには、XenAppでそのアプリケーションを公開する時に、説明にKEYWORDS:Auto という文字列を追加します。ユーザーがストアにログオンすると、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 Receiver for Mac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。

詳しくは、StoreFrontのドキュメントを参照してください。

XenApp展開環境のWeb Interfaceで、XenApp Servicesサイトを作成します。サイト名およびその作成方法は、インストールしているWeb Interfaceのバージョンにより異なります。詳しくは、Web Interfaceのドキュメントを参照してください。

StoreFrontで作成するストアは、Citrix Receiver for Macのリソース配信インフラストラクチャと認証を提供するサービスにより構成されます。このストアにより、XenDesktopサイトおよびXenAppファームからデスクトップとアプリケーションが列挙および集約され、これらのリソースをユーザーが使用できるようになります。

1. StoreFrontをインストールして構成します。詳しくは、StoreFrontのドキュメントを参照してください。

   注：独自のCitrix Receiver for Mac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。
2. XenAppやXenDesktopのアプリケーションと同様の手順で、CloudGateway用にストアを構成します。ユーザーのCitrix Receiver for Mac側で特別な設定を行う必要はありません。詳しくは、StoreFrontのドキュメントの「*ストアの構成*」を参照してください。

管理者は、ユーザーにアカウントの情報を提供します。ユーザーは、この情報を使用してアプリケーションやデスクトップにアクセスします。次の方法でユーザーに情報を提供できます。

- メールアドレスによるアカウント検出を構成する
- ユーザーにプロビジョニングファイルを提供する
- ユーザーにセットアップ用のURLを提供する

- アカウント情報をユーザーに手入力させる

メールアドレスによるアカウント検出を構成する

管理者は、メールアドレスによるCitrix Receiver for Macアカウントの検出機能を構成できます。この機能を有効にした場合、ユーザーはCitrix Receiver for Mac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。DNS（Domain Name System）サービス（SRV）レコードにより、そのメールアドレスに関連付けられているNetScaler Gateway、またはStoreFrontサーバーが自動的に検出され、ホストされているアプリケーションやデスクトップ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。

メールアドレスによるReceiverアカウントの検出機能が正しく動作するようにDNSサーバーを構成する方法については、StoreFrontドキュメントの「*— メールアドレスによるアカウント検出を構成する*」を参照してください。

ユーザーが入力したメールアカウントによりStoreFrontまたはNetScaler Gatewayが正しく検出され、NetScaler Gatewayに接続できるように構成する方法については、NetScaler Gatewayドキュメントの「*— Connecting to StoreFront by Using Email-Based Discovery*」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

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、Receiverを自動的に構成できるようにします。Citrix Receiver for Macをインストールした後で、提供されたファイルをユーザーが開くとCitrix Receiver for Macが自動的に構成されます。Receiver for Webサイトを構成する場合は、そのサイトからユーザーにCitrix Receiver for Macのプロビジョニングファイルを提供することもできます。

詳しくは、StoreFrontのドキュメントを参照してください。

ユーザーにセットアップ用のURLを提供する

管理者は、Citrix Receiver for Mac Setup URL Generatorを使用して、必要なアカウント情報を含んでいるURLを生成できます。Citrix Receiver for Macをインストールした後で、管理者から提供されたURLをユーザーがクリックしてアカウントを構成し、リソースにアクセスできます。Setup URL Generatorユーティリティで生成したURLは、すべてのユーザーにメールで送信したりWebサイトに掲載したりできます。

アカウント情報をユーザーに手入力させる

ユーザーにアカウント情報を入力させる場合は、以下の情報を提供する必要があります。

- StoreFrontストアやXenApp ServicesサイトのURL（https://servername.example.comなど）
- NetScaler Gatewayを使用する環境では、そのアドレスと製品エディション、および使用する認証方法
  NetScaler Gatewayの構成について詳しくは、「NetScaler Gateway」を参照してください。

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

自動更新の構成

各ユーザーが **[環境設定]** ダイアログボックスで［Citrix Receiver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。

1. Citrix Receiver for Macの **[環境設定]** に移動します。
2. **[詳細]** ペインで、 **[自動更新]** を選択します。［Citrix Receiverの更新］ダイアログボックスが開きます。
3. 次のいずれかのオプションを選択します。
   - はい。通知します
   - いいえ。通知しません
   - 管理者指定の設定を使用する
4. 変更を保存するには、ダイアログボックスを閉じます。

管理者は、StoreFrontを使用して［Citrix Receiverの更新］を構成できます。Citrix Receiverは、［管理者指定の設定を使用する］を選択したユーザーに対してのみこの構成を使用します。以下の手順で、自動更新を手動で構成します。

1. テキストエディタでweb.configファイルを開きます。ファイルのデフォルトの場所は、C:\inetpub\wwwroot\Citrix\Roaming\web.configです。
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）。

   例：

   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。

3. タグの後に、自動更新タグを追加します。

auto-update-Check

このコマンドは、更新が利用可能かを検出します。

有効な値は次のとおりです。

- Auto – このオプションは、更新が利用可能な時に通知します。
- Manual – このオプションは、更新が利用可能であっても通知しません。ユーザーは、**[更新の確認]** を選択して手動で更新を確認します。
- Disabled – このオプションは、［Citrix Receiverの更新］を無効にします。

auto-update-DeferUpdate-Count

このコマンドは、最新バージョンのCitrix Receiverに強制的に更新される前に、エンドユーザーに送信される更新通知の回数を設定します。デフォルト値は、7です。

有効な値は次のとおりです。

- -1 – エンドユーザーは、更新が利用可能になった時に、後で通知するオプションを選択できます。
- 0 – エンドユーザーは、更新が利用可能になった時に、すぐに最新バージョンのCitrix Receiverに更新するよう強制されます。
- 正の整数 – エンドユーザーが更新を強制される前に更新通知を受信する回数を指定します。この値は、8以上に設定しないでください。

auto-update-Rollout-Priority

このコマンドは、更新が利用可能であることがデバイスに表示されるタイミングを指定します。

有効な値は次のとおりです。

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

Citrix Receiver for Mac環境の最適化

Sep 25, 2017

Citrix Receiver for Mac環境を以下のように最適化できます。

- ユーザーの自動再接続
- デスクトップの再起動
- セッション画面の保持機能の提供
- ローミングユーザーのセッションの維持
- クライアント側デバイスのマッピング
- クライアント側ドライブのマッピング
- クライアント側COMポートのマッピング

ネットワークの状態が不安定であったり、待ち時間が非常に変わりやすかったりする場合、また、無線デバイスの伝送距離に制限がある場合に、セッションが切断されてしまうことがあります。クライアントの自動再接続機能では、ネットワークの問題などによって切断されたセッションをCitrix Receiver for Macが検出して、そのセッションに自動的に再接続します。

この機能がサーバーで有効になっていると、ユーザーは作業を続けるために手動で再接続する必要がありません。再接続は、接続に成功するかユーザーがキャンセルするまで繰り返し試行されます。サーバー側でユーザー認証を要求する設定になっている場合、再接続時にユーザーの資格情報を入力するためのダイアログボックスが開きます。ユーザーがセッションからログオフしないでアプリケーションを終了してセッションを切断した場合、自動再接続は行われません。

管理者は、サーバーのポリシーを使用してクライアント自動再接続機能を構成します。詳しくは、XenAppおよびXenDesktopのドキュメントを参照してください。

仮想デスクトップで起動しない、接続に時間がかかる、または破損したなどの問題が生じた場合、ユーザーはそのデスクトップを再起動できます。管理者は、XenDesktopでこの機能を構成する必要があります。

ユーザーがサブスクライブしたデスクトップやユーザーの［アプリ］ページには、状況依存型のメニュー項目**[再起動]** が表示されます。デスクトップの再起動が無効に設定されている場合、このメニュー項目は使用できません。ユーザーが［再起動］を選択すると、Citrix Receiver for Macがそのデスクトップをシャットダウンしてから起動します。

> **Important**
>
> デスクトップの再起動により、未保存のデータが失われる場合があることをユーザーに説明してください。

セッション画面の保持機能を有効にすると、公開アプリケーションへの接続が中断しても、ユーザーのセッション画面には作業中の画面が保持され、表示されたままになります。たとえば、ワイヤレス接続でのセッション中にトンネルや障害物などの影響で接続に障害が生じた場合、ユーザーデバイス上の画面表示が停止します。トンネルから出るなどして再接続されると、ユーザーはそのまま作業を続行できます。セッション画面の保持を有効にしておくと、このような接続の中断時にセッション画面が表示されたままになり、接続が回復するまで維持されるようになります。

セッションに接続できないときに、ユーザーに警告ダイアログボックスが表示されるように構成できます。

管理者は、サーバーのポリシーを使用してセッション画面の保持機能を設定します。セッション画面の保持機能とReceiverの操作について詳しくは、高い品質のサービスおよび保持機能を確保する方法に関するドキュメントを参照してください。

また、ポリシーに関して詳しくは、「クライアントの自動再接続のポリシー設定」および「セッション画面の保持のポリシー設定」を参照してください。

> **ヒント**
>
> Citrix Receiver for Macのユーザーは、サーバー側のセッション画面の保持設定を変更できません。

> **Important**
>
> セッション画面の保持を有効にすると、セッションの通信に使用されるデフォルトのポートは、1494から2598に変更されます。

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

ポリシーおよびクライアント側ドライブのマッピングの構成は、ユーザーがほかのデバイスに移動したときに、そのデバイスに適したものに自動的に切り替わります。ポリシーおよびマッピングの構成は、ユーザーがログオンするデバイスに応じて動的に適用されます。たとえば、医療従事者が緊急治療室のユーザーデバイスからログオフして、レントゲン室で別のワークステーションにログオンした場合、そのワークステーションでのセッション用に設定されたポリシー、プリンターマッピング、およびクライアント側ドライブマッピングが自動的に適用されます。

ワークスペースコントロール設定を構成するには

1. Receiver for Macウィンドウで下向き矢印のアイコンをクリックして、**[環境設定]**を選択します。
2. **[一般設定]**タブをクリックします。
3. 次のいずれかのオプションを選択します。
   - Receiverへのログオン時にアプリケーションに再接続する：ユーザーがReceiverを起動してログオンしたときに、切断セッションに再接続されます。
   - アプリケーションの起動時または更新時に再接続する：ユーザーがReceiverを起動したとき、およびCitrix Receiverのメニューで［アプリケーション一覧の更新］を選択したときに、切断セッションに再接続されます。

Citrix Receiver for Macでは、ローカルのドライブやデバイスがセッション内で自動的にマップされます。これにより、セッション内でクライアント側のドライブやデバイスにアクセスできるようになります。クライアント側デバイスのマッピング機能をサーバー側で有効にすると、サーバー上で動作するリモートのアプリケーションやデスクトップで、ユーザーデバイスに接続されているローカルのデバイスを使用できるようになります。マシンの追加方法

- ローカルのドライブ、COMポート、およびプリンターにアクセスする。
- セッション内で、サーバー上のシステムサウンドやオーディオファイルを再生する。

> **注意**
>
> クライアント側オーディオのマッピングおよびクライアント側プリンターのマッピングでは、ユーザーデバイス側での設定が不要です。

クライアント側ドライブのマッピング機能を有効にすると、セッション内でユーザーデバイス上のローカルドライブ（CD-ROMドライブ、DVDドライブ、USBメモリスティックなど）にアクセスできるようになります。サーバーでクライアント側ドライブのマッピングが許可されている場合、ユーザーはセッション内で各自のローカルファイルを読み込んで、再びローカルドライブに保存したり、サーバーのドライブに保存したりできます。

Citrix Receiver for Macは、CD-ROMドライブ、DVDドライブ、USBメモリスティックなどのハードウェアデバイスがマウントされるユーザーデバイス上のディレクトリを監視して、セッション内で追加された新しいディレクトリを、サーバーで使用可能な最初のドライブ文字に自動的にマップします。

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

マップされたドライブの読み取りと書き込みアクセスを制御するには

1. Receiver for Macのホームページで下向き矢印のアイコンをクリックし、**［環境設定］**を選択します。
2. **［デバイス］**をクリックします。
3. 以下のいずれかのアクセスレベルを選択します。
   - 読み出し/書き込み
   - 読み取り専用
   - アクセスなし
   - 毎回確認する
4. 変更内容を適用するには、既存のセッションからログオフして、再接続します。

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。

Macintoshのシリアルポートでは、Windowsアプリケーションで使用される一部の制御信号線が提供されません。具体的には、DSR（Data Set Ready）、DCD（Device Carrier Detect）、RI（Ring Indicator）、およびRTS（Request To Send）線がありません。これらの信号によりハードウェアハンドシェイクやフロー制御を行うWindowsアプリケーションでは、Macintoshのシリアルポートを使用できない場合があります。Macintoshのシリアル通信では、CTS（Clear To Send）とDTR（Data Terminal Ready）により入力および出力のハードウェアハンドシェイクが行われます。

クライアント側COMポートをマップするには

1. Receiver for Macのホームページで下向き矢印のアイコンをクリックし、**［環境設定］**を選択します。
2. **［デバイス］**をクリックします。
3. ［マップされたCOMポート］の一覧から、マップするCOMポートを選択します。これはセッション内で表示される仮想COMポートであり、ローカルマシン上の物理ポートではありません。
4. ［デバイス］列のポップアップメニューから、その仮想COMポートに割り当てるデバイスを選択します。
5. Citrix Receiver for Macを起動して、サーバーにログオンします。

6. コマンドプロンプトを開きます。コマンドプロンプトで、次のコマンドを実行します。
   net use comx: \\client\comz：

   ここで、xにサーバー側のCOMポート番号（ポート1～9）を指定し、にクライアント側のCOMポート番号（ポート1～4）を指定します。

7. 正しくマッピングされていることを確認するには、コマンドプロンプトでnet useを実行します。これにより、マップされたドライブ、LPTポート、およびCOMポートの一覧が表示されます。

Citrix Receiver for Macでのユーザーエクスペリエンスの向上

Sep 25, 2017

Receiverには、ユーザーエクスペリエンスを向上させるための以下の機能が用意されています。

- カスタマーエクスペリエンス向上プログラム（CEIP）
- ClearTypeフォントスムージング
- クライアント側のマイク入力
- Windows特殊キー
- Windowsのショートカットやキーの組み合わせ
- IME（Input Method Editor）とインターナショナルキーボードレイアウトの使用
- 複数モニターの使用
- デスクトップツールバーの使用

Ctrixカスタマーエクスペリエンス向上プログラム（CEIP）では、Citrix Receiver for Macの構成および使用に関するデータが匿名で収集され、そのデータがCitrixに自動的に送信されます。このデータは、Citrix Receiver for Mac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。詳しくは「CEIPの構成」を参照してください。

ClearTypeフォントスムージング（サブピクセルのフォントレンダリング）は、従来のフォントスムージングやアンチエイリアスに比べて表示フォントの質を向上させます。

サーバー側でClearTypeフォントスムージングを有効にしても、ユーザーデバイスで強制的にClearTypeフォントスムージングが使用されるわけではありません。管理者がサーバー側でClearTypeフォントスムージングのサポートを有効にすると、ユーザーデバイス側でこの機能が有効な場合のみフォントスムージングが使用されます。

Citrix Receiver for Macはユーザーデバイスのフォントスムージング設定を自動的に検出し、それをサーバーに送信します。セッションはこの設定を使って接続されます。セッションが切断または終了すると、サーバー側の設定が元に戻ります。

Citrix Receiver for Mac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 Receiver for Macでは、デジタルディクテーションがサポートされます。サーバー上でのこの機能を構成する方法について詳しくは、製品ドキュメントサイトで「オーディオ機能」の情報を参照してください。

ユーザーは、ユーザーデバイスに接続されたマイクをセッションで使用するかどうかを、Citrix Receiver for Macの［環境設定］の［マイクとWebカメラ］タブで設定できます。

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

[毎回確認する]を選択すると、ホストされているアプリケーションやデスクトップに接続するたびに、そのセッションでマイクを使用するかどうかを確認するダイアログボックスが開きます。

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

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

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

テンキーが付属しているキーボードでは、さらに以下のキー操作を使用できます。

PCキー	Macキー操作
挿入	テンキーの0キー0。Macキーボードのnum lockはオフである必要があります（オン/オフを切り替えるにはclearキーを使用します） option+help
削除	テンキーの小数点キー。Macキーボードのnum lockはオフである必要があります（オン/オフを切り替えるにはclearキーを使用します） クリア
F1からF9	option+1～9（テンキー）
F10	option+0（テンキー）
F11	option+テンキーの負符号（-）キー

PC	Macキー操作
F12	option+テンキーの正符号（+）キー

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

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

キーボードやキー操作の構成は、デバイスにより大きく異なることがあります。このため、Citrix Receiver for Macには、セッション内のアプリケーションやデスクトップにキー操作を正しく転送するためのオプションが用意されています。これらのオプションについては、下の表を参照してください。Receiverでのデフォルトの動作についても説明します。Citrix Receiver for Macやそのほかの設定でデフォルトの動作を変更すると、リモートのデスクトップやアプリケーションに異なるキー操作が送信される場合があります。

Important

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

下の表について、以下の点に注意してください。

- Macキーボードの特殊キーは小文字で示します（ファンクションキーを除くcontrol、command、optionなど）。また、英字キーは大文字で表記されていますが、Shiftキーを同時に押すという意味ではありません。
- キー名の間のプラス記号（+）は、それらのキーを同時に押すことを示します（control+Cなど）。
- 文字キーは、英数字および句読点のキーを指します。特殊キーは単独では文字を入力しない修飾キーや制御キーを指し、Ctrl（control）、Alt、Shift（shift）、command、option、方向キー、およびファンクションキーが含まれます。
- 使用するメニューは、そのセッションのCitrix Viewerメニューを指します。
- ユーザーデバイスの構成によっては、一部のキーの組み合わせが意図したとおりに機能しない場合があります。この場合、その代替操作を示します。
- fnキーはMacキーボードの修飾キーのうちの1つで、F1～F12キーはPCまたはMacキーボードの各ファンクションキーに相当します。

Windowsキー	Macキー操作
Alt+文字キー	command+option+文字キー（たとえば、セッションでＡｌｔ+Cキー操作を使用するには、command+option+Cを押します）
Alt+特殊キー	option+特殊キー（option+tabなど）

	command+option+特殊キー（command+option+tabなど）
Ctrl+文字キー	command+文字キー（command+Cなど） control+文字キー（control+Cなど）
Ctrl+特殊キー	control+特殊キー（control+F4など） command+特殊キー（command+F4など）
Ctrl/Alt/Shift/Windowsロゴ+ファンクションキー	［キーボード］メニューの［ファンクションキーを送信］>（control/option/shift/commandを押しながら）［F1～F12］
Ctrl+Alt	control-option-command
Ctrl+Alt+Del	control+option+Forward Delete control+option+fn+delete（MacBookキーボード） ［キーボード］メニューの［Ctrl+Alt+Delを送信］
削除	削除 ［キーボード］メニューの［キーを送信］>［Del］ fn+backspace（一部のUSキーボードではfn+delete）
終了日	終了日 fn+右方向キー
Esc	Esc ［キーボード］メニューの［キーを送信］>［Esc］
F1～F12	F1～F12 ［キーボード］メニューの［ファンクションキーを送信］>［F1～F12］
ホーム	ホーム fn+左方向キー
Ins	［キーボード］メニューの［キーを送信］>［Ins］

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

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

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

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

クライアント側のIMEを有効にするには

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

IME入力時の確定前文字列の挿入ポイント（`）を表示するには

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

サーバー側のIMEを使用するには

- クライアント側のIMEが半角英数モードになっていることを確認します。

サーバー側IMEの入力モードキーの割り当て

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

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

インターナショナルキーボードレイアウトを使用するには

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

Citrix Receiver for Macのメニューオプションである **[フルスクリーンのすべてのディスプレイを使用する]** を使って、複数のモニターを使ったフルスクリーンモードを実行できます。

既知の制限事項

単一モニターのフルスクリーンまたはすべてのモニターを使ったフルスクリーンモードのみがサポートされています。これはメニューアイテムを使って構成できます。

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

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

れています。

Citrix Receiver for Mac通信のセキュリティ保護

Sep 25, 2017

ここでは、Citrix Receiver for Macでのセキュアな通信に関する情報について説明します。

サーバーファームとCitrix Receiver for Mac間の通信を保護するには、Citrix NetScaler Gatewayなど、以下の一連のセキュリティ技術を使用します。このゲートウェイ製品とStoreFrontの構成について詳しくは、「StoreFront」のドキュメントを参照してください。

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

- SOCKSプロキシサーバーまたはSecure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 Receiverとサーバー間の接続を制御できます。Citrix Receiver for Macは、SOCKSプロトコルとSecureプロキシプロトコルをサポートしています。
- Secure Gateway Secure GatewayをWeb Interfaceと一緒に使うと、社内ネットワーク上のサーバーにインターネットを介して接続できる、暗号化された安全な単一のアクセスポイントをユーザーに提供できます。
- Transport Layer Security（TLS）プロトコルによるSSL Relayソリューション
- ファイアウォール。ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。サーバーの内部IPアドレスを外部インターネットアドレスにマップするネットワークファイアウォール（つまりNAT（Network Address Translation：ネットワークアドレス変換））を介してCitrix Receiver for Macを使用する場合は、外部アドレスを構成します。

プライベート（自己署名）証明書

リモートゲートウェイにプライベート証明書がインストールされている場合は、組織の証明機関のルート証明書をユーザーデバイスにインストールしないと、Citrix Receiver for Macを使用してCitrixリソースにアクセスできません。

> **注意**
>
> 接続時にリモートゲートウェイの証明書を検証できない場合（ローカルのキーストアにルート証明書が含まれていないため）、信頼

されていない証明書の警告が表示されます。ユーザーが警告に対してそのまま続行することを選択した場合、アプリケーションの一覧が表示されますが、アプリケーションの起動に失敗します。

Receiver for Macデバイスへのルート証明書のインポート

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

ワイルドカード証明書

ワイルドカード証明書は、同一ドメイン内の任意のサーバーで個別のサーバー証明書の代わりに使用します。Citrix Receiver for Macでは、ワイルドカード証明書がサポートされています。

NetScaler Gatewayの中間証明書

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NetScaler Gatewayのサーバー証明書にマップする必要があります。方法については、NetScaler Gatewayのドキュメントを参照してください。中間証明書をNetScaler Gatewayアプライアンスにインストールして、プライマリCAとリンクする方法については、「How to Install and Link Intermediate Certificate with Primary CA on NetScaler Gateway」を参照してください。

サーバー証明書検証ポリシー

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

Important

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

- サーバーまたはゲートウェイの構成に不適切なルート証明書が含まれている
- サーバーまたはゲートウェイの構成にすべての中間証明書が含まれていない
- サーバーまたはゲートウェイの構成に有効期限切れの証明書や無効な中間証明書が含まれている
- サーバーまたはゲートウェイの構成にクロスルート用中間証明書が含まれている

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

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

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

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

- 「サーバー証明書サンプル」
- 「中間証明書サンプル」

- 「ルート証明書サンプル」

次に、Citrix Receiver for Macはこれらすべての証明書が有効であることを確認します。Citrix Receiver for Macが「ルート証明書サンプル」を信頼済みであることも確認します。Citrix Receiver for Macが「ルート証明書サンプル」を信頼していない場合、接続に失敗します。

Important

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

注意

サーバーやゲートウェイによっては、ルート証明書が構成されていても、送信しないことがあります。この場合、より厳格な検証は機能しません。

以下は、ゲートウェイがこのような有効な証明書で構成されていることを前提としています。通常は、このルート証明書を省略した構成が推奨されます。

- 「サーバー証明書サンプル」
- 「中間証明書サンプル」

Citrix Receiver for Macはこの2つの証明書を使用します。次に、ユーザーデバイスでルート証明書を検索します。正しく検証される証明書が見つかり、信頼済みである場合（「ルート証明書サンプル」など）、接続は成功します。信頼済みの証明書が見つからない場合は、失敗します。この構成では、Citrix Receiver for Macが必要とする中間証明書が提供されますが、Citrix Receiver for Macは任意の有効な、信頼済みのルート証明書を選択できます。

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

- 「サーバー証明書サンプル」
- 「中間証明書サンプル」
- 「不正なルート証明書」

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

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

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

Important

証明機関によっては、クロスルート用中間証明書を使用します。これは、複数のルート証明書があり、以前のルート証明書が最新のルート証明書と同時に使用中の状況を想定しています。この場合、少なくとも2つの中間証明書が存在します。たとえば、以前のルート証明書「Class 3 Public Primary Certification Authority」には、関連するクロスルート用中間証明書「VeriSign Class 3 Public Primary Certification Authority - G5」があります。ただし、最新のルート証明書「VeriSign Class 3 Public Primary Certification Authority - G5」も利用可能であり、「Class 3 Public Primary Certification Authority」に置き換わります。このルート証明書はクロスルート用中間証明書を使用しません。

注意

クロスルート用中間証明書およびルート証明書は、同じサブジェクト名（発行先）ですが、クロスルート中間証明書には異なる発行者名（発行元）があります。これによって、クロスルート用中間証明書と通常の中間証明書（「中間証明書サンプル2」など）を区別できます。

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

- 「サーバー証明書サンプル」
- 「中間証明書サンプル」

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

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

ゲートウェイでサーバー証明書のみを構成しないでください。

- 「サーバー証明書サンプル」

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

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

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

NetScaler Gatewayでの構成について詳しくは、「Integrating with NetScaler Gateway and NetScaler」のドキュメントを参照してください。

このトピックの内容は、Web Interface環境にのみ適用されます。

Secure Gatewayを通常モードまたはリレーモードのどちらかで使用して、Citrix Receiver for Macとサーバーの間に保護された通信チャネルを提供できます。Secure Gatewayを通常モードで使用し、ユーザーがWeb Interface経由で接続する場合は、Citrix Receiver for Mac側での構成は不要です。

Citrix Receiver for MacがSecure Gatewayサーバーに接続する時は、リモートのWeb Interfaceサーバーで構成されている設定が使用されます。Citrix Receiver for Macをサポートするプロキシサーバー設定の構成については、Web Interfaceのドキュメントを参照してください。

Secure Gateway Proxyがセキュリティで保護されたネットワーク内のサーバーにインストールされている場合は、Secure Gateway Proxyをリレーモードで使用できます。リレーモードについて詳しくは、XenAppおよびSecure Gatewayのドキュメントを参照してください。

ただし、リレーモードで使用する場合、Secure Gatewayサーバーはプロキシサーバーとして機能するため、Citrix Receiver for Macで次の項目を構成する必要があります。

- Secure Gatewayサーバーの完全修飾ドメイン名。
- Secure Gatewayサーバーのポート番号。Secure Gateway, Version 2.0では、リレーモードはサポートされていません。

完全修飾ドメイン名には、以下の3つの要素を順に指定する必要があります。

- ホスト名
- サブドメイン名
- 最上位ドメイン名

たとえば、my_computer.example.comは完全修飾ドメイン名です。ホスト名（my_computer）、サブドメイン名（example）、最上位ドメイン名（com）が順に指定されています。一般的には、サブドメイン名と最上位ドメイン名の組み合わせ（example.com）をドメイン名といいます。

プロキシサーバーは、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、Citrix Receiver for Macとサーバー間の接続を制御するために使います。Citrix Receiver for Macは、SOCKSプロトコルとSecureプロキシプロトコルの両方をサポートしています。

Citrix Receiver for MacでXenAppサーバーまたはXenDesktopサーバーと通信する場合、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。Receiverをサポートするプロキシサーバー設定の構成については、Web Interfaceのドキュメントを参照してください。

Citrix Receiver for MacでWebサーバーと通信する場合は、ユーザーデバイス上のデフォルトのWebブラウザーで構成されているプロキシサーバー設定が使用されます。各ユーザーデバイス上のデフォルトのWebブラウザーで、プロキシサーバー設定を構成する必要があります。

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

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。たとえば、XenAppサーバーやXenDesktop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 Receiver for Mac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 Receiver for Mac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。詳しくは、Web Interfaceのドキュメントを参照してください。

Citrix Receiver for Mac 12.3はXenApp/XenDesktopとのTLS接続に、以下の暗号の組み合わせを使用したTLS 1.0、1.1、1.2をサポートします。

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

注：Mac OS Sierra上で実行されているCitrix Receiver for Macは、以下のTLS暗号の組み合わせをサポートしません。

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

Transport Layer Security（TLS）は、SSLプロトコルの最新の標準化バージョンです。IETF（Internet Engineering TaskForce）が、TLSの公開標準規格の開発をNetscape Communications社から引き継いだ時に、SSLという名前をTLSに変更しました。

TLSは、サーバーの認証、データの暗号化、メッセージの整合性の確認を行って、データ通信を保護します。米国政府機関をはじめとする組織の中には、データ通信を保護するためにTLSの使用を義務付けているところもあります。このような組織では、さらにFIPS 140（Federal Information Processing Standard）などのテスト済み暗号化基準の使用を義務付けられる場合があります。FIPS 140は、暗号化の情報処理規格です。

Citrix Receiver for Mac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。

SSL Relayを構成して使用する安全なインストールについては、XenDesktopおよびStoreFrontのドキュメントを参照してください。

> **注意**
>
> Citrix Receiver for Macは、プラットフォーム（OS X）の暗号化機能をCitrix Receiver for MacとStoreFrontの接続に使用します。

Citrix Receiver for MacのTLSの構成と有効化

TLSのセットアップは、以下の2つの手順で行います。

1. XenAppサーバー、XenDesktopサーバー、およびWeb Interfaceサーバー上でSSL Relayをセットアップし、必要なサーバー証明書を入手してインストールします。詳しくは、XenAppおよびWeb Interfaceのドキュメントを参照してください。
2. ユーザーデバイス上で、ルート証明書をインストールします。

ユーザーデバイスへのルート証明書のインストール

TLS機能が有効になっているCitrix Receiver for Macとサーバーファーム間の通信をTLSで保護するには、サーバー証明書の証明機関の署名を認証するためのルート証明書がユーザーデバイスにインストールされている必要があります。

Mac OS Xには約100の商用ルート証明書が付属していますが、ほかの証明書を使用する場合は、証明機関から証明書を入手して、それを各ユーザーデバイスにインストールします。

企業の方針によっては、ルート証明書のインストールはエンドユーザーではなく管理者が行う場合があります。ルート証明書を簡単および確実にインストールするには、Mac OS Xのキーチェーンにその証明書を追加します。

ルート証明書をキーチェーンに追加するには

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

ルート証明書は、TLSが有効なクライアントと、TLSを使用するその他のアプリケーションでインストールされ、使用可能になります。

TLSポリシーについて

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

> ### 注意
> デバイスがOS Xサーバーなどのモバイルデバイス管理ソリューションで制御されている場合は、TLSポリシーはほかの方法でも管理できます。

TLSポリシーには以下の設定が含まれます。

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

- **None**。コンプライアンスモードは適用されません。
- **FIPS**。FIPS暗号モジュールが使用されます。
- **SP800-52**。NIST SP800-52r1コンプライアンスが適用されます。

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

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

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

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

SSLCertificateRevocationCheckPolicy。この機能により、Citrixサーバーの暗号化認証機能が強化され、クライアントとサーバーの間のSSL/TLS接続の全体的なセキュリティが向上します。この設定により、OS XクライアントでSSL経由のリモートセッションを開く時に、所与の信頼されたルート証明機関を扱う方法を制御します。

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

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

この設定に適用できる値は以下のとおりです。

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

味を持ちます。

> **注意**
>
> SSLCertificateRevocationCheckPolicyを設定しない場合は、デフォルト値としてFullAccessCheckが使用されます。

```
defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy FullAccessCheckAndCRLRequired
```

TLSポリシーの構成

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

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

設定を変更するには

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

   defaults write com.citrix.receiver.nomas

場所:

：前述のように設定の名前です。

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

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

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

デフォルト構成へのリセット

設定をデフォルトに戻すには

1. ［アプリケーション］、［ユーティリティ］、［ターミナル］の順に選択します。

2. ターミナルで以下のコマンドを実行します。

   defaults delete com.citrix.receiver.nomas

場所:

：前述のように設定の名前です。

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

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

- セキュリティ構成のユーザーインターフェイスが強化されました。以前のリリースでは、セキュリティ関連の変更を実施する場合、コマンドラインが優先される方法でしたが、セッションセキュリティ関連の構成設定は、UIから簡単にアクセスしやすくなりました。これによってユーザーエクスペリエンスが向上し、シームレスにセキュリティ関連の基本設定を採用するための方法が提供されます。
- TLS接続の表示。Citrix Receiver for Macでは、情報を追加して、特定のTLSバージョンを使用したサーバーへの接続を検証できます。この情報には、接続に使用される暗号化アルゴリズム、モード、キーサイズ、SecureICAが有効になっているかどうかなどが含まれます。また、TLS接続のサーバー証明書も表示できます。

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

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

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