

Citrix Receiver for Android 3.7.xについて

Nov 20, 2015

Google playからダウンロードできる最新のバージョンのCitrix Receiver for Androidは3.7.3です。以前のバージョンを実行しているユーザーはこの最新バージョンに更新する必要があります。

Citrix Receiver for Android 3.7.3には、Android M (6.0) をサポートします。

Version 3.7.3で解決された問題

Citrix Receiver for Android 3.7.3は、Nexus 9 BluetoothでCitrix Receiverを使用する場合の断続的なクラッシュを処理します。

このリリースでは、以下の機能が追加されました。

- **ディスプレイとの合致**。特定の解像度のアプリを公開する場合、Receiverはそのアプリを中央部分に表示させて、アスペクト比に合わせてその表示サイズを拡大するようになりました。ソース（アプリ）と対象（ディスプレイ）間の関係を適切に解釈します。
- **セッション表示のミラー化の拡張サポート**。Receiver for Androidでは画面ディスプレイとAndroidデバイス間でディスプレイ特性を一致させて、ユーザーエクスペリエンス強化します。
- **Transport Layer Security (TLS) のサポート**。Receiver for AndroidはTLS 1.1およびTLS 1.2プロトコルをサポートするようになりました。これを有効にすると、TLSによりサーバーとクライアント間におけるセキュリティで保護された通信が提供されます。この機能は、Receiver for Androidのインターフェイスまたはreceiverconfigファイルを介して構成できません。
- タッチ画面をサポートしないデバイスに対するインセッションメニューバーの非表示をサポートします。
- 強化された韓国ハングルのキーボード処理。

このリリースのReceiver for Androidには、次の既知の問題と制限があります。

- 以前のリリースでは、セッションディスプレイをセカンダリディスプレイにミラーリングする機能のサポートは限定的でした。Androidデバイスのディスプレイと解像度が一致するデバイスでのみこの機能がサポートされました。このリリースのReceiver for Androidではこの限定条件はなくなりました。Androidデバイスの解像度とは異なる解像度のディスプレイデバイスがサポートされます。ただし、次の制限はあります。[#549471]
 - セッションサイズは、接続されているディスプレイデバイスのナチュラル解像度により決まります。セカンダリディスプレイはセッションイメージのサイズを変えることができないため、そのほかすべての設定は無視されます。さらに、接続されているディスプレイの解像度と一致するようにセッション解像度を動的に調整する要求は一部のみサポートされます。このような環境では、セカンダリディスプレイを接続および切断しても、標準のユーザー設定を遵守するセッションのサイズ変更要求は許可されません。
 - セカンダリディスプレイを切断すると不安定となり、Receiverがクラッシュすることがあります。セカンダリディスプレイを使用する場合は、セッションを開始する前にAndroidデバイスに接続してください。
 - 接続されたディスプレイにおいて表示パフォーマンスが否定的な影響を受けることがあります。場合によっては、マウスポインターの表示障害やウィンドウを移動する間の表示の乱れなど、接続されたデバイスで表示上の問題が起こることがあります。
 - Androidデバイスのプライマリディスプレイ上で表示されるため、ユーザーインターフェイスにはいくつかの制限が適用されます。たとえば、マウスはデバイスの画面サイズに合わせて機能し、セカンダリ画面のサイズとは合致しません。

また画面のミラー化が有効な場合、デバイス画面にツールバーは表示されません。[#549471]

- セカンダリディスプレイを接続する場合、新しく接続されたディスプレイの画面解像度はデバイスの解像度と同じとなります。この問題は、接続されたデバイスがセッションの初期化後にドッキングされて、マウスはドックに接続されていない場合に発生します。この問題を解決するには、2つ目のセッション用のマウスを接続し、正しい解像度に戻します。この問題は、Samsung Galaxy Note II Multimedia Dockに特定のものです。[#541028]
- ドッキングされたセッションからマウスを取り外すと、デバイス上のセッションの表示が時計回りに90度回転します。セッションの方向はその後すぐに通常の状態に戻ります。この問題は、Samsung Galaxy Note II Multimedia Dockに特定のものです。[#541032]
- AllCast Dongleを使用する外部モニターを画面ミラーリング機能で使用する場合、メディアファイルを再生してもオーディオは再生されません。この問題は、ディスプレイデバイスの性能に関係するものと思われます。スピーカー内蔵のテレビを使用すると、テレビを介してオーディオが再生されます。スピーカーが内蔵されていないモニターを使用する場合、Androidデバイスのスピーカーからも音はなりません。[#544330]
- 虫眼鏡をセッションイメージの端よりも外に移動させると、虫眼鏡内に背景イメージの一部が拡大表示されないままに表示されることがあります。[#542299]
- セッションを閉じるとランタイム例外が生じることがあります。[#523824]
- 画面を回転した後は、最大「ピンチアウト」レベルを維持できません。この問題は、セッションを起動して「ピンチイン」を使って必要な最大ビューにした後、デバイスを90度回転させた後で起こることがあります。デバイスをもう一度回転させた後は、選択していた「ピンチレベル」の設定は無効になります。[#538638]
- 特定の条件においては、拡張キーボードが間違っ​​てアクティブになります。たとえば、画面のミラーリングを停止してデバイスを回転させるとこの問題が起こります。また、画面のミラーリングが有効な間にデバイス画面に触ってもこの問題が発生します。この問題は、ソフトキーボードを表示しているかどうかをAndroidデバイスが判別できない場合に発生します。つまり、別のモニターに接続してミラーモードに入ると、拡張キーボードの表示操作の解釈に失敗します。[#545231]
- Android Version 4.1.1が動作するASUS Nexus 7デバイスでは、アカウントの作成に失敗します。この問題を回避するには、Androidオペレーティングシステムを最新バージョン（Version 4.2.2など）にアップデートしてください。
- 一部のAndroidデバイスで、Bluetooth接続のマウスの右クリックにより「戻る」処理が実行され、「終了」ダイアログボックスが開くことがあります。この問題は、マウスの右クリックをサポートしないファームウェアが動作するデバイスで発生します。[#331168]
- Receiver for Android 3.5では、スマートカード認証を使用するとフルVPNトンネル機能はサポートされません。[#456657]
- "denyslreneg"ポリシーをNoに設定して、またはFrontend Clientおよび"Client Authentication"をOptionalに設定してFIPS NetScalerに接続する場合、Receiverにログインすると次のエラーが発生することがあります。
 - ユーザー名フィールドに「ドメイン\ユーザー名」形式で入力してReceiverにログインする場合、ユーザー名またはパスワードを間違っ​​て入力すると「ドメイン\ドメイン\ユーザー名」形式での入力を確認するメッセージが表示されることがあります。この問題を解決するには、ドメイン名エントリを1つ削除して、「ドメイン\ユーザー名」形式でログインし直してください。[#466022]

Receiver for Androidのシステム要件

Nov 20, 2015

- Citrix Receiver for Android 3.7.6.1は、Androidのバージョン4、5、および6（Android M）をサポートします。
- Citrix Receiver for Android 3.7、3.7.1、および3.7.2はAndroidバージョン4および5をサポートします。
- デバイスのAndroidオペレーティングシステムを最新バージョンにアップデートしてください。
- Receiver for AndroidはReceiver for Webからのセッションの開始をサポートし、Webブラウザを使ってReceiver for Webを実行できるようになります。セッションが開始しない場合、Receiver for Androidを介して直接アカウントを構成してください。
- Citrix ReceiverのTechnology Preview版がインストールされている場合は、これをアンインストールしてから新しいバージョンをインストールします。

重要：接続を保護する場合については、下記の「[接続](#)」を参照してください。

Citrix Receiverで仮想デスクトップやアプリケーションに接続する場合、Citrix StoreFront、およびWeb Interfaceがサポートされます。

StoreFront：

- StoreFront 3.0（推奨）
StoreFrontストアへの直接アクセスを提供します。Receiverでは、前バージョンのStoreFrontもサポートされます。
- Receiver for Webサイトが構成されたStoreFront
StoreFrontストアへのWebブラウザからのアクセスを提供します。この展開方法での制限事項については、StoreFrontのドキュメントを参照してください。

Web Interface（XenDesktop 7環境ではサポートされません）：

- Web Interface 5.4とWeb Interfaceサイト。
- Web Interface 5.4とXenApp Servicesサイト。
- NetScaler上のWeb Interface
NetScalerで提供されるリライトポリシーを有効にする必要があります。
- XenAppおよびXenDesktopの以下のバージョン
 - XenApp 7.x
 - XenApp 6.5 for Windows Server 2008 R2
 - XenApp 6 for Windows Server 2008 R2
 - XenApp Fundamentals 6.0 for Windows Server 2008 R2
 - XenApp 5 for Windows Server 2008
 - XenApp 5 for Windows Server 2003
 - Citrix Presentation Server 4.5
 - XenDesktop 7.x
 - XenDesktop 7
 - XenDesktop 5、5.5、および5.6

Citrix Receiverでは、以下の設定のいずれかを使用して、XenAppサーバーファームにHTTP、HTTPS、およびICA-over-TLS接

続を確立できます。

LAN接続の場合：

- StoreFront 2.xまたは2.6（推奨）、Web Interface 5.4、またはXenApp Servicesサイト（旧称「Program Neighborhood エージェントサイト」）

安全なリモート接続の場合（次のいずれかのバージョン）

- Citrix NetScaler Gateway 10（VPX、MPX、およびSDXバージョンを含む）
- Citrix Access Gateway Enterprise Edition 9.x、10.x（VPX、MPX、およびSDXバージョンを含む）
 - CloudGatewayはバージョン9.3以降でのみサポートされます

セキュリティが保護された接続とTLS証明書について

TLSを使用してリモート接続を保護する場合、モバイルデバイスはリモートゲートウェイのTLS証明書の信頼性を、信頼されたルート証明機関のローカルストアと照合することで検証します。証明機関のルート証明書がローカルのキーストアに存在する場合は、民間の証明機関（VeriSignおよびThawteなど）が発行した証明書が自動的に検出されます。

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モバイルデバイスにインストールしないと、Citrix ReceiverでCitrixリソースにアクセスできません。

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は、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が起動しません。

Androidデバイスへのルート証明書のインポート

Android 4.xデバイスでは、デバイスのルートアクセスがなくてもルート証明書をインポートできます。Android 4.0以前のデバイスでは、ルート証明書の自動インポートはサポートされていません。

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 Androidでは、ワイルドカード証明書がサポートされています。

中間証明書とAccess Gateway

証明書チェーンに中間証明書が含まれる場合は、中間証明書をAccess Gatewayのサーバー証明書に追加する必要があります。使用するAccess Gatewayのエディションに関するKnowledge Baseアートを参照してください。

[CTX114146 : How to Install an Intermediate Certificate on Access Gateway Enterprise Edition](#)

eDocsのこのセクションの設定のトピックに加えて、次のトピックも参照してください。

[CTX124937 : How to Configure Citrix Access Gateway Enterprise Edition for Use with Citrix Receiver for Mobile Devices](#)

注：RSA SecurID認証は、Secure Gatewayを使用する構成ではサポートされません。RSA SecurIDを使用するにはAccess Gatewayを使用してください。

Citrix Receiverでは、使用するAccess Gatewayのエディションに応じて以下の認証がサポートされます。

- 認証なし（StandardおよびEnterprise Editionのみ）
- ドメイン認証

- RSA SecurID (WiFi接続および非WiFi接続でのソフトウェアトークンを含む)
- RSA SecurIDを組み合わせたドメイン認証
- SMSパスコード (OTP) 認証
- スマートカード認証*

Receiver for Androidは次の製品および構成をサポートするようになりました。

注：Web Interfaceサイトでは、スマートカードによる認証がサポートされていません。

サポートされるスマートカードリーダー：

- BaiMobile 3000MP Bluetoothスマートカードリーダー

サポートされるスマートカード：

- PIVカード
- Common Access Card

サポートされる構成：

- StoreFront 2.xおよびXenDesktop 5.6以降またはXenApp 6.5以降があるNetScaler Gatewayに対するスマートカード認証
- Web Interface 5.4.2およびXenDesktop 5.6以降またはXenApp 6.5以降があるNetScaler Gatewayに対するスマートカード認証

注：RADIUSを使用してほかのトークンベースの認証ソリューションを設定できる場合があります。SafeWordトークン認証について詳しくは、eDocsで適切なAccess Gatewayエディションの「SafeWord認証の構成」に関するトピックを参照してください。

管理

Nov 20, 2015

Receiverを使用するには、環境でWeb Interfaceを構成する必要があります。Web Interfaceでは、XenApp Servicesサイト（旧称「Program Neighborhoodエージェントサービスサイト」）とXenApp Webサイトという2種類のWebサイトを作成できます。これらのWeb Interfaceサイトにより、ユーザーデバイスがサーバーファームに接続できるようになります。ReceiverとWeb Interfaceサイト間の認証は、このセクションで説明されているいくつかの方法で処理されます。

また、StoreFrontがReceiverへの認証およびリソース配信を提供するように構成して、デスクトップ、アプリケーション、およびその他のリソースをユーザーに配信する一拠点のエンタープライズリソースストアを作成することもできます。

接続の構成については、<http://community.citrix.com>を参照してください。ビデオ、ブログ、サポートフォーラムなどを利用できます。

SDカードへのReceiverのインストール

Nov 20, 2015

Receiver for Mobile Devicesは、ユーザーデバイスへのローカルインストールに最適です。ただし、デバイス上のストレージ領域が不足している場合は、外部SDカード上にReceiverをインストールできます。この場合、そのSDカードをモバイルデバイスにマウントして、公開アプリケーションを起動します。この機能はデフォルトでサポートされており、追加構成は不要です。

SDカードを使用してアプリを起動するには、ユーザーデバイスでReceiverアプリ一覧から起動するアプリを選択して、[SDカードへ移動] を選択します。

外部SDカード上にReceiverをインストールしてアプリを起動する場合、以下の問題が生じることがあります。

- モバイルデバイス上にSDカードをマウントした状態でUSBストレージデバイスをマウントすると、SDカードを使用できなくなります。このため、実行中のアプリが停止します。
- SDカードからアプリを実行している間、一部のApp Widget（ホーム画面のウィジェットなど）を使用できなくなります。ユーザーは、SDカードのマウントを解除した後で、App Widgetを再起動する必要があります。

ユーザーがReceiverをローカルにインストールした場合、必要に応じてReceiverをSDカード上に移動することができます。

Access Gateway Enterprise EditionをCitrix Receiver for Android用に構成するには

Nov 20, 2015

重要：

- Receiver for AndroidでXenApp Servicesサイトを使用する場合は、Access Gateway Enterprise Edition 9.xおよび10.xがサポートされます。
- Receiver for AndroidでXenApp Webサイトを使用する場合は、Access Gateway Enterprise Edition 9.xおよび10.xがサポートされます。
- Receiver for Webは、Receiver for Androidではサポートされません。
- Receiver for AndroidでStoreFrontストアにアクセスする場合は、Access Gateway Enterprise Edition 9.xおよび10.xがサポートされます。
- Web InterfaceサイトおよびStoreFrontでは、1要素認証および2要素認証がサポートされます。
- デバイ스에組み込まれているすべてのWebブラウザでサポートされている、Web Interface 5.4を使用する必要があります。
- 単一の仮想サーバー上で複数のセッションポリシーを作成して、接続の種類（ICA、CVPN、またはVPN）やReceiverの種類（Web ReceiverまたはローカルインストールのReceiver）に応じて異なる設定を適用できます。すべてのポリシーを単一の仮想サーバーで作成できます。
- ユーザーがReceiver上でアカウントを作成するときに、アカウントの資格情報としてメールアドレスまたはAccess GatewayサーバーのFQDNを入力する必要があります。たとえば、デフォルトのパスで接続できない場合、ユーザーはAccess Gatewayサーバーのフルパスを入力する必要があります。

リモートのユーザーがAccess Gatewayを介してCloudGateway環境に接続できるようにするには、CloudGatewayのコンポーネントであるAppControllerまたはStoreFrontと通信するようにAccess Gatewayを構成します。このアクセスを有効にする方法は、CloudGatewayのエディションによって異なります。

- CloudGateway Enterpriseエディションでは、Access GatewayとAppControllerを統合することでリモートユーザーのAppControllerへの接続を有効にします。ユーザーは、AppControllerに接続してWebアプリケーション、SaaS（Software as a Service）アプリケーション、およびモバイルアプリケーションを取得したり、ShareFileで共有されているドキュメントにアクセスしたりします。ユーザーは、Citrix ReceiverまたはAccess Gateway Plug-inを使用して接続を行います。
- CloudGateway Expressエディションでは、Access GatewayとStoreFrontを統合することで内部ユーザーやリモートユーザーのStoreFrontへの接続を有効にします。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。

接続の構成方法については、「Integrating Access Gateway with CloudGateway」と[Access Gateway 10のドキュメント](#)のその他のトピックを参照してください。

Receiver for Mobile Devicesに必要な設定については、[Access Gateway 10のドキュメント](#)のトピックも参照してください。

- [Creating the Session Profile for Receiver for CloudGateway Enterprise](#)
- [Creating the Session Profile for Receiver for CloudGateway Express](#)
- [Configuring Custom Clientless Access Policies for Receiver](#)
- [Allowing Access from Mobile Devices](#)

および、XenMobileのドキュメントの以下のトピック：

- [App Preparation Tool for Mobile Apps](#)

リモートのユーザーがAccess Gatewayを介してWeb Interface環境に接続できるようにするには、Web Interfaceと通信するようにAccess Gatewayを構成します。詳しくは、「Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface」および[Access Gateway 10のドキュメント](#)を参照してください。

Web InterfaceをCitrix Receiver for Android用に構成するには

Nov 20, 2015

Citrix Receiverでは、既存のWeb Interfaceサイトを使用してアプリケーションを起動できます。管理者は、ほかのXenAppアプリケーションと同じ方法でWeb Interfaceサイトを設定できます。ユーザーのモバイルデバイス側で特別な構成を行う必要はありません。

Receiverは、Web Interface Versions 5.4のみをサポートします。Web Interface 5.4を使用する場合、ユーザーはモバイル版のFirefoxからアプリケーションを起動できます。

デバイスから、通常のアカウント情報を入力してWeb Interfaceサイトにログインします。

Receiver for Androidを使用しているときにWeb Interfaceサイトからアプリケーションを起動する場合、デバイス上のSDカードが使用可能である必要があります。SDカードが使用不能である場合（ほかで使用されていたりマウントされていない場合）、セッションの起動に失敗します。

スマートカードサポートの有効化

Nov 20, 2015

Receiver for Androidでは、Bluetoothで接続したスマートカードリーダーを使用してPNAサイトにアクセスできます。スマートカードのサポートを有効にすると、以下の機能が有効になります。

- スマートカードによるログオン認証。Receiverのユーザーをスマートカードを使って認証します。
- スマートカード対応アプリケーションのサポート。スマートカード対応の公開アプリケーションを使って、ローカルのスマートカードリーダーにアクセスできます。
- ドキュメントおよび電子メールへの署名ICAセッション内で起動するMicrosoft WordやOutlookなどのアプリケーションからスマートカードにアクセスして、ドキュメントやメールにデジタル署名を追加できます。

サポートされているスマートカード：

- PIVカード
- Common Access Card

デバイス上でスマートカードサポートを有効にするには

1. ユーザーは、モバイルデバイスでスマートカードリーダーを使用できるように構成する必要があります。構成方法については、スマートカードリーダーのドキュメントを参照してください。たとえば、baiMobile Bluetooth Smart Card Reader 製品をAndroidデバイスで使用できるようにする方法については、<http://www.biometricassociates.com/downloads/user-guides/baiMobile-3000MP-User-Guide-for-Android-v2.0.pdf>を参照してください。

Androidデバイスでのスマートカードのサポートでは、以下の要件および制限事項があります。

- Receiverでスマートカードを使用する場合、Biometric Associates社でサポートされるすべてのAndroidデバイスがReceiverでもサポートされます。詳しくは、<http://www.biometricassociates.com/products/smart-card-readers/android-supported-devices/>を参照してください。
 - スマートカードを使用する場合、グローバルPINを使用することはできません。PIV PINを入力してください。これはサードパーティの制限事項によるものです。
 - スマートカードでの認証にパスワード認証よりも時間がかかることがあります。このため、セッションから切断した後再接続する場合は、切断後約30秒待機してください。セッションからの切断直後に再接続を試行すると、Receiverが動作しなくなることがあります。
 - WebブラウザやXenAppサイトを使用したアクセスでスマートカード認証はサポートされません。
2. スマートカードを使用するPNAgentアカウントを追加する前に、AndroidデバイスにAndroid PC/SC-Liteサービスをインストールします。このサービスは、baiMobile SDKにAPK (.apk) ファイルとして付属しています。Androidの場合、Google Play StoreからPC/SC-Liteのapkファイルをダウンロードできます。
 3. Receiverの [設定] アイコンをタップして、[アカウント]、[アカウントの追加] の順に選択するか、既存のアカウントを編集します。
 4. 接続を構成し、スマートカードのオプションを有効にします。

RSA SecurID認証のAndroidデバイス用の設定

Nov 20, 2015

Access GatewayのRSA SecurID認証を設定すると、Receiverで「次のトークン」モードがサポートされます。このモードを有効にすると、ユーザーが不正なパスワードを3回（デフォルト設定）入力したときに、Access Gateway Plug-inによりメッセージが表示され、次のトークンが表示されるまで待機すればログオンできるようになります。ユーザーが不正なパスワードで何度もログオンしようとした場合に、そのユーザーのアカウントが無効になるようにRSAサーバーを設定できます。

RSA SecurID認証の構成手順については、Citrix eDocsで、対応する[Access Gateway](#)バージョンの

— *RSA SecurID認証の構成*

に関するトピックを参照してください。

RSA SecurID認証は、Secure Gatewayを使用する構成ではサポートされません。RSA SecurIDを使用するにはAccess Gatewayを使用してください。

RSA SecurID Software Authenticatorファイルの拡張子は、「.sdtid」です。このファイルを、RSA社の変換ツール（RSA SecurID Software Token Converter）を使用してXML形式の81桁の数値に変換します。RSA SecurID Software Token Converterのダウンロードおよび使用方法については、RSA社のWebサイトを参照してください。

以下の手順でトークンファイルを変換します。

1. モバイルデバイスではなくコンピューターを使用して、<http://www.rsa.com/node.aspx?id=2521>からRSA SecurID Software Token Converterをダウンロードします。Webサイトおよび変換ツールに付属のReadmeの説明に従って、トークンファイルを数値に変換します。
2. 変換された数値をメールにコピーして、ユーザーのモバイルデバイスに送信します。
3. デバイスの日時設定が正確であることを確認してください。この設定が正確でないと、認証が行われません。
4. デバイスでメールを開き、ソフトウェアトークンをインポートするためのリンクをクリックします。

デバイスにソフトウェアトークンをインストールすると、[設定] にトークンを管理するためのオプションが追加されます。

注：SDTID (.sdtid) ファイルをReceiverに関連付けられないモバイルデバイスでは、拡張子を.xmlに変更してからインポートしてください。

Androidユーザーへのアクセス情報の提供

Nov 20, 2015

管理者は、ユーザーにReceiver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、デスクトップ、およびデータにアクセスします。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
- アカウント情報をユーザーに手入力させる

管理者は、メールアドレスによるReceiver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Receiver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Access 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、デスクトップ、およびデータにアクセスするためのログオンを求めメッセージが表示されます。

注：ReceiverでWeb Interfaceに接続する環境では、メールアドレスによるアカウント検出がサポートされません。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ドレスによりStoreFrontまたはAccess GatewayのURLが正しく検出され、Access Gatewayに接続できるように構成する方法については、Access 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。

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。デバイスにReceiverをインストールした後で、提供されたCRファイルをユーザーが開くとReceiver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Receiver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。

ユーザーが手動で入力するアカウント情報を提供している場合は、以下の情報を指定しておく必要があります。

- StoreFront URLまたはXenApp Servicesサイトホスティングリソース。例：servername.company.com。
- Access Gatewayを使用する場合は、そのアドレスと認証方法。
Access GatewayまたはSecure Gatewayの構成について詳しくは、「[Access Gateway](#)」または「[XenApp \(Secure Gatewayの場合\)](#)」のドキュメント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。

パスワードの保存

Nov 20, 2015

Citrix Web Interface管理コンソールでは、認証時にユーザーがパスワードを保存することを許可できます。管理者がユーザーのアカウントを設定すると、パスワードが暗号化され、そのユーザーの初回接続時まで保存されます。

- ユーザーによるパスワードの保存を許可すると、パスワードがデバイス上に格納され、アプリケーションへの再接続時にパスワードの再入力が必要になります。
注：パスワードが保存されるのは、ユーザーがアカウントを作成するときにパスワードを入力した場合のみです。アカウントのパスワードが入力されていない場合は、サーバー側の設定にかかわらずパスワードは保存されません。
- 管理者がパスワードの保存を無効（デフォルト設定）にすると、接続時に常にパスワードの入力が必要になります。

注：StoreFront接続では、パスワードを保存することはできません。

サーバー側でパスワードの保存を有効にしても、ユーザーは以下の方法でパスワードの入力が毎回要求されるように設定できます。

- アカウント作成時に、パスワードフィールドを空白のままにする。
- アカウント編集時に、パスワードを削除して設定を保存する。

Citrix Receiver設定の変更

Nov 20, 2015

Citrix Receiver for Androidの [設定] タブで、次の設定をカスタマイズできます。

- **表示**
 - セッションの解像度：セッションの解像度を選択します。デフォルトは [画面に合わせる] です。
- **キーボード**
 - 予測入力：文字列の予測入力を有効または無効にします。デフォルトは、 [Off] です。
 - 拡張キーボード：拡張キーボードを有効または無効にします。デフォルトは、 [Off] です。
 - 拡張キー：AltやCtrlなど、特殊キーを拡張キーボードの一部として表示するように構成します。
 - クライアント側IME：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。デフォルトは、 [Off] です。
- **オーディオ**
 - オーディオストリーム：セッション内でのオーディオ設定を [オーディオ:オフ]、 [再生]、 [再生と録音] のいずれかとして構成します。デフォルトは [再生] です。
- **上級**
 - デバイスストレージの使用：デバイスストレージへのアクセスを許可します。デフォルトは、 [アクセスなし] です。
 - 終了する前に確認：終了する前の確認について構成します。デフォルトは [On] です。
 - クリップボード：クリップボードの使用を有効または無効にします。デフォルトは、 [Off] です。
 - 画面の向き：表示の向きを [横]、 [縦]、または [自動] (動的) に構成します。デフォルトは [自動] です。
 - 画面の常時表示：デバイスの表示をオンのままにします。デフォルトは、 [Off] です。
- **ShareFile**：この機能のサポートはなくなっていて、将来の更新から削除されます。ShareFileアプリを使用してください。
- **バージョン情報**：Citrix Receiverのバージョンおよび著作権情報です。

デモ用のサイトを試用する

Nov 20, 2015

Citrix Receiverを初めて起動すると、[ようこそ] ページが開き、Citrix Cloudのデモ用アカウントを作成するためのオプションが表示されます。このアカウントを使用して、Citrix Cloudを試用できます。

デモ用アカウントを作成するには、ユーザーが名前およびメールアドレスを入力して登録操作を行う必要があります（一部のデバイスではメールアドレスが自動的に入力されます）。Citrix Cloudのデモサイトにはいくつかの構成済み公開アプリケーションが用意されており、Citrix Receiverですぐにそれらのアプリケーションを使用できます。

ユーザーは、Receiverを使用してアカウントを追加、変更、および削除できます。