Web Interface 5.4

2015-05-07 20:30:43 UTC

目次

Web Interface 5.4

更新日： 2014-11-25

Web Interfaceにより、XenAppアプリケーションやコンテンツ、およびXenDesktop仮想デスクトップへのアクセスがユーザーに提供されます。 ユーザーは、標準のWebブラウザーまたはCitrix Online Plug-inを使用してリソースにアクセスします。

このセクションの内容

このセクションでは、Web Interfaceのインストール、構成、および管理に関する、以下の最新情報について説明します。

Readme - Web Interface 5.4	最新のアップデートおよび既知の問題についての情報です。
Web Interface 5.4で解決された問題	Web Interfaceの前回のリリース以降に解決された問題に関する詳細です。
Web Interfaceの機能	Web Interfaceを紹介します。
新機能	新機能の概要です。
Web Interfaceのコンポーネント	Web Interfaceの展開について説明します。
Web Interfaceで必要なシステム環境	ソフトウェア、構成、Webサーバー、ユーザー、およびデバイスの要件について説明します。
Web Interfaceのインストール	Web InterfaceをインストールしてWebサーバーを構成します。
はじめに	Web Interfaceサイトを作成して構成します。
サーバーとサーバーファームの管理	サーバーおよびサーバーファームとの通信を構成して管理します。
Web Interfaceの認証方法の構成	Web Interface、サーバーファーム、およびCitrixのプラグイン間の認証を構成します。
クライアントの管理	CitrixのプラグインをWeb Interfaceと共に展開して使用します。
セキュアなアクセスの管理	サイトへのアクセスを構成して管理します。
クライアント側のプロキシ設定の編集	Citrixのクライアントおよびプロキシサーバーを経由してアクセスするXenAppまたはXenDesktopサーバーを構成します。
ユーザーページの外観のカスタマイズ	ユーザーがWeb Interfaceを使用するときの外観をカスタマイズします。
セッション基本設定の管理	ユーザーが調整できる設定を指定します。
ワークスペースコントロールの構成	ユーザーがすばやくリソースから切断したり、リソースに再接続したり、ログオフしたりできるようにします。

Web Interfaceのセキュリティ構成	Web Interface環境で通信されるデータをセキュリティで保護します。
構成ファイルを使用したサイトの構成	構成ファイルでWeb Interfaceサイトを管理します。
Web Interfaceに対するActive Directoryフェデレーションサービスのサポートの構成	Microsoft Active Directoryフェデレーションサービス（AD FS）を作成して構成し、Web Interfaceサイトに統合します。

Readme - Web Interface 5.4

Readme Version : 1.0

目次

関連ドキュメント

Web Interfaceのユーザーに影響を与える可能性があるクライアント関連の問題については、ユーザーに対して現在配信しているCitrixのクライアントのReadmeファイルを参照してください。

このリリースで解決された問題の一覧については、Citrix Knowledge Centerの技術文書http://support.citrix.com/article/CTX124164を参照してください。

Citrix製品のライセンスのドキュメントは、Citrix eDocsの「製品ライセンスの有効化」を参照してください。

テクニカルサポートについて

Citrixでは、主にCitrix Solution Advisor（CSA）のパートナー各社を通して、テクニカルサポートを提供しています。 Citrix製品のサポートについては、Citrix製品の販売代理店にお問合せください。また、Citrix社のWebサイト（http://www.citrix.co.jp/partners/）にて、最寄りのCitrix Solution Advisorを検索することができます。

Citrixオンラインテクニカルサポートのサービスは、CitrixサポートWebサイトで提供されています。 ここでは、ダウンロードページ、Citrix Knowledge Center、Citrix Consulting Services、およびそのほかの有用な情報の参照先が説明されています。

このリリースの既知の問題について

ここでは、このリリースで確認されている既知の問題について解説します。 この情報をよく読んでから、製品をインストールしてください。

- WinCE 6.0 WFR3が動作するデバイス上のInternet Explorer 6で、アイコンが正しく表示されない
- Internet Explorerの［お気に入り］に公開デスクトップおよび公開アプリケーションを追加するとユーザーエラーが発生する

- サポートされないクライアントを使って接続しようとする場合のエラーメッセージ
- Windows Embeddedが動作するデバイスでCitrix Online Plug-inをアップグレードできない
- Windows Server 2008が動作するXenAppサーバーで委任を構成する場合はKerberosを使用できない
- Windows Embedded CE 6.0が動作する一部のデバイスからWeb Interfaceにアクセスする場合、仮想デスクトップを開始できない
- Firefox 3.6ユーザーはワークスペースコントロールおよびクライアントのアップグレードを実行できない
- Windows Mobile 6.1が動作する一部のデバイスではワークスペースコントロールを実行できない
- Windows Embedded CE 6.0 R2が動作する一部のデバイスではワークスペースコントロールを断続的に実行できない
- XenApp 6.0では、Access Gatewayからのスマートカードパススルー認証を使用できない

WinCE 6.0 WFR3が動作するデバイス上のInternet Explorer 6で、アイコンが正しく表示されない

WinCE 6.0 WFR3（Hot Fix 3 build 664）が動作するデバイスのInternet Explorer 6で表示すると、PNG形式のアイコンは正しく表示されません。 この問題を解決するには、Internet Explorer 5以前を使用してください。 または、Internet Explorer 6でPNGファイルを表示するには、Microsoftのサポート技術情報の文書番号 http://support.microsoft.com/kb/294714に記載されている回避策を参照してください。

[#41839]

Internet Explorerの［お気に入り］に公開デスクトップおよび公開アプリケーションを追加するとユーザーエラーが発生する

Internet Explorerの［お気に入り］に公開デスクトップおよび公開アプリケーションを追加すると、問題が発生することがあります。 ［お気に入り］リンクのタイトルが間違って作成され、クリックしても正しく動作しないことがあります。 ［お気に入り］にアプリケーションを追加するには、アプリケーションのアイコンを右クリックしてください。 デスクトップを追加するには、デスクトップのタイトルテキストを右クリックしてください。

[#244446]

サポートされないクライアントを使って接続しようとする場合のエラーメッセージ

Web Interfaceのこのリリースでは、Version 7.0より古いクライアントの使用をサポートしていません。 サポートされないバージョンのクライアントを使ってリモートアプリケーションに接続しようとすると、「50：サーバーに接続できません」というエラーメッセージが表示されます。クライアントソフトウェアを最新のバージョンにアップグレードして、この問題を防ぐことができます。 アップグレードすることができない場合は、テンプレートICAファイルを次のように編集してエラーの発生を防ぐことができます。

1. メモ帳などのテキストエディターを使って、default.ica、bandwidth_high.ica、bandwidth_low.ica、bandwidth_medium.ica、およびbandwidth_medium_high.ica

ファイルを開きます。 通常これらのファイルは、IIS上では C:¥inetpub¥wwwroot¥Citrix¥SiteName¥confに、Java Application Server上では Web InterfaceサイトのWEB-INFディレクトリにあります。

2. 各ファイルで次の行を削除します。

   DoNotUseDefaultCSL=On
   BrowserProtocol=HTTPonTCP
   LocHttpBrowserAddress=!

[#163695]

Windows Embeddedが動作するデバイスでCitrix Online Plug-inをアップグレードできない

Windows Embeddedオペレーティングシステムが動作するデバイスにおいて、Citrix Online Plug-inのインストールまたはアップグレードを求めるメッセージがWeb Interfaceにより表示される場合がありますが、このインストールは失敗します。 Windows XP Embeddedが動作するデバイスに最新バージョンのCitrix Online Plug-inを手動でインストールすることで、この問題を防ぐことができます。 手動でのインストールができない場合は、このメッセージを表示しないよう次の手順で、サイトの設定を変更できます。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。

3. ［操作］ペインで［クライアントの展開］をクリックします。 オンラインアプリケーションのみを公開するサイトの場合、［ネイティブクライアント］チェックボックスをオンにして、［プロパティ］をクリックします。

4. ［クライアント検出］をクリックします。

5. ［クライアントのアップグレードを要求する］チェックボックスをオフにして、［リソースにアクセスできないときのみ］または［表示しない］を選択します。

[#164709]

Windows Server 2008が動作するXenAppサーバーで委任を構成する場合はKerberosを使用できない

Windows Server 2008による問題のため、委任のためXenAppサーバーの信頼関係を設定する際に、認証にKerberosのみを使用するようActive Directoryを構成すると認証に失敗します。 この問題は、Windows Server 2008 with Service Pack 2、Windows Server 2008 x64 Edition with Service Pack 2、およびWindows Server 2008 R2が動作するXenAppサーバーで発生します。 Windows Server 2008が動作するXenAppサーバーでAD FS統合およびAccess Gatewayからのスマートカードパススルーを有効にするには、ドキュメントで説明されている［Kerberosのみを使用する］設定ではなく、［任意の認証プロトコルを使う］設定を選択します。 [#169269]

Windows Embedded CE 6.0が動作する一部のデバイスからWeb Interfaceにアクセスする場合、仮想デスクトップを開始できない

Windows Embedded CE 6.0とInternet Explorer 6.xが動作するWYSE V30LEシンクライアントでXenApp Webサイトにログオンして仮想デスクトップへのリンクをクリックした場合、デスクトップの起動に失敗することがあります。 この問題を避けるには、リンク文字列

の横に表示されるアイコンをクリックしてください。 [#218317]

Firefox 3.6ユーザーはワークスペースコントロールおよびクライアントのアップグレードを実行できない

Mozilla Firefox 3.6の変更のため、このWebブラウザーを使ってWeb Interfaceにアクセスするユーザーに対してワークスペースコントロールは自動的に無効になります。 また、Firefox 3.6ユーザーによりインストールされたCitrixのクライアントは、クライアントの検出と展開処理によってバージョン番号を検出できないため、これらのユーザーに対してクライアントのアップグレードを提供することができません。 [#230068]

Windows Mobile 6.1が動作する一部のデバイスではワークスペースコントロールを実行できない

Windows Mobile 6.1 Professional とInternet Explorer Mobileが動作するHP iPAQ 910cハンドヘルドデバイスでXenApp Webサイトにログオンした場合、ワークスペースコントロールが正常に機能しないことがあります。 [#230580]

Windows Embedded CE 6.0 R2が動作する一部のデバイスではワークスペースコントロールを断続的に実行できない

Windows Embedded CE 6.0 R2とInternet Explorer 6.xが動作するHP t5540シンクライアントでXenApp Webサイトにログオンすると、［再接続］ボタンをクリックしたときにワークスペースコントロールが正常に機能しないことがあります。 [#230654]

XenApp 6.0では、Access Gatewayからのスマートカードパススルー認証を使用できない

XenApp 6.0による問題のため、Access Gatewayからのスマートカードパススルー認証を有効にすると、Access Gateway統合サイトにスマートカードでログオンするユーザーはリソースにアクセスできなくなります。 ユーザーがXenApp 6.0により配信されたリソースにアクセスするためにリンクをクリックすると、「必要な接続を実行中にエラーが発生しました。」というエラーメッセージが表示されます。スマートカードユーザーに対してリソースへアクセスするたびにPINの入力を求めるようにサイトを構成して、この問題を防ぐことができます。 [#230942]

http://www.citrix.co.jp/

Web Interfaceの管理

Web Interfaceにより、XenAppアプリケーションやコンテンツ、およびXenDesktop仮想デスクトップへのアクセスがユーザーに提供されます。 ユーザーは、標準のWebブラウザーまたはCitrix Online Plug-inを使用してリソースにアクセスします。

Web Interfaceは、Webサーバー上でJavaおよび.NETの技術を実行して、XenApp Webサイトに表示するサーバーファームのHTMLリンクを動的に作成します。 各ユーザーに表示されるWebページには、サーバーファーム内でそのユーザーに公開されているすべてのリソース（アプリケーション、コンテンツ、およびデスクトップ）が表示されます。 Web Interfaceでは、リソースにアクセスするための独立したWebサイトや、既存の企業ポータルサイトに統合可能なWebサイトを作成できます。 またWeb Interfaceを使って、Citrix Online Plug-inを介したリソースへのユーザーアクセス設定を構成できます。

Citrix Web Interface管理コンソールを使って、Microsoftインターネットインフォメーションサービス（IIS）上にWeb Interfaceサイトを作成して構成できます。 このコンソールは、Web Interface for Microsoft Internet Information Servicesでのみインストールされます。 コンソールの使用については、「Citrix Web Interface管理コンソールでのサイトの構成」を参照してください。

また、サイト構成ファイル（WebInterface.conf）を使用してWeb Interfaceサイトの管理を行うこともできます。 詳しくは、「構成ファイルを使用したサイトの構成」を参照してください。

XenApp Webサイトをカスタマイズしたり、拡張したりすることもできます。 これらの構成方法については、Web Interface SDKを参照してください。

Web Interfaceの機能

Web Interfaceでは、必要に応じて、リソースへのアクセス方法が異なる2種類のサイトを作成してユーザーに提供できます。

XenApp Webサイト： ユーザーは、Webブラウザーを使ってこのWebサイトにログオンします。 認証されたユーザーは、Citrixのクライアントを使用してオンラインリソースやオフラインアプリケーションにアクセスできます。

XenApp Servicesサイト： Citrix Online Plug-inをWeb Interfaceと組み合わせて使用することで、ユーザーのデスクトップにリソースのショートカットを組み込むことができます。 ユーザーは、デスクトップまたは［スタート］メニューにあるアイコン、またはデスクトップ内の通知領域をクリックして、アプリケーション、仮想デスクトップ、およびオンラインコンテンツにアクセスします。 音声、表示、ログオンなどの構成オプションにユーザーがアクセスして変更できるようにする場合は、管理者はどのオプションを表示するかを指定できます。

管理機能

更新日： 2014-11-24

複数のサーバーファームのサポート： 複数のサーバーファームを構成して、ユーザーの画面からすべてのサーバーファームのリソースにアクセスできるように設定できます。 Citrix Web Interface管理コンソールの［サーバーファーム］タスクを使って各サーバーファームを個々に構成できます。 詳しくは、「構成ファイルを使用したサイトの構成」を参照してください。

障害復旧： 停電またはネットワーク障害などにより、ユーザーが運用環境のサーバーファームにアクセスできない場合に備えて緊急用のXenAppおよびXenDesktopサーバーファームを指定できます。 これにより、すべての実務環境のサーバーへのアクセス障害に対して対策し、基幹業務アプリケーションやデスクトップが突如として使用不可状態になるのを防ぐことができます。

共有サイト構成： Web Interface for Microsoft Internet Information Servicesでは、ネットワーク上で構成ファイルを共有するマスターサイトを指定できます。 共通の構成を使用するほかのサイトでは、ローカルファイルではなく、マスターサイトの構成ファイルを使用するように設定できます。

広く利用されているWeb技術との統合： Microsoft社のASP.NETおよびSun Microsystems社のJavaServer Pages（JSP）から、Web InterfaceのAPIにアクセスすることができます。 Web Interface for Java Application Serversはプラットフォームから独立しており、Microsoftインターネットインフォメーションサービスが Webサーバーとして使用されていないWindowsオペレーティングシステム上にインストールできます。

リソースアクセス機能

XenApp VM Hosted Apps： XenAppにより、仮想マシンからオンラインアプリケーションを配信できます。 これにより、リモートデスクトップサービスと互換性がないまたは未検証のアプリケーション、またWindows Serverオペレーティングシステム上へのインストールがサポートされていないアプリケーションを公開できます。

ユーザーローミング。 ユーザーグループを特定のサーバーファームに割り当てて、場所やログオンしているサーバーに関係なく、ユーザーに一貫性のある操作性を提供できます。 これにより、たとえば海外出張中にも、出張先の国のローカルのWeb Interfaceサーバーにログオンし、母国のサーバーファームから母国語のリソースを自動的に受信することができます。

UNIXサーバーファームのサポート： XenApp for UNIX（日本語版はリリースされていません）動作するサーバー上のアプリケーションを、ユーザーのデバイスに表示して実行できます。

Active Directoryとユーザープリンシパル名（UPN）のサポート： Web Interfaceのすべてのコンポーネントで、Microsoft Active Directoryがサポートされています。 XenApp Webサイトにアクセスするユーザーは、Active Directory環境内のサーバーファームにログオンして、アプリケーションとコンテンツをシームレスに実行できます。 ［ログオン］画面では、Active Directory用のログオン情報をUPN形式（user@domainなど）で入力します。

匿名ユーザー： Web Interfaceにより、ユーザーは匿名ユーザーとしてXenApp Webサイトにログオンし、XenAppで公開しているアプリケーションにアクセスできます。

セキュリティ機能

SSL（Secure Sockets Layer）/TLS（Transport Layer Security）のサポート： Web Interfaceは、Web Interfaceサーバーとサーバーファーム間の通信を保護するための、SSL/TLSをサポートしています。 SSLをWebサーバーに実装し、SSLをサポートするWebブラウザーと一緒に使用することにより、ネットワークで送受信されるデータのセキュリティが保護されます。 Web InterfaceはMicrosoftの.NET Frameworkを使ってSSLおよび暗号化を導入します。

Access Gatewayのサポート： Citrix Access Gatewayは、Web Interfaceと連動して、データや音声などのあらゆる情報リソースに安全に接続できる単一のアクセスポイントを提供する、ユニバーサルSSL仮想プライベートネットワーク（VPN：Virtual Private Network）アプライアンスです。 IPSec（Internet Protocol Security）とSSL VPNの両方の利点をすべて活かしながら、複雑な導入および管理作業を排除し、どのようなファイアウォールを使用した環境でも、すべてのリソースとプロトコルに対応できます。

Secure Gatewayのサポート： Secure Gatewayは、Web Interfaceと連携動作することによって、企業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アクセスするための、暗号化された安全な単一のネットワークポイントを提供します。 Secure Gatewayを使用すると、サーバー証明書をSecure Gatewayサーバーにだけインストールし、サーバーファーム内の各サーバーへのインストールが不要になるため、証明書管理が簡素化されます。

スマートカードのサポート： Web Interfaceは、ユーザー認証に対するスマートカードの使用をサポートし、アプリケーション、コンテンツ、およびデスクトップへのセキュアなアクセスを提供します。 スマートカードを使用すると、ログオンセキュリティを向上させるとともに、ユーザーの認証プロセスを簡素化します。

チケット機能： チケットは認証セキュリティを向上させる機能で、 Web Interfaceでチケットを取得し、リソースに対してユーザーを認証します。 チケットは、1回のログオンでのみ有効で、有効期限を構成できます。 使用済みのチケットや、有効期限が切れたチケットは無効になり、ユーザーはリソースにアクセスできなくなります。 チケットを使用すると、リソースへの接続するためにWeb Interfaceで使われるICAファイルに、ユーザーのアカウント情報を明示的に指定する必要がなくなります。

Secure Ticket Authority冗長： Access Gatewayを介してリソースにアクセスするユーザーに対して、複数の冗長なSecure Ticket Authorities（STA）を構成できます。 これにより、ユーザーセッションの実行中にSTAが使用できなくなり、セッションへの再接続を妨げる可能性を小さくできます。 冗長性が有効な場合、Web Interfaceは2つの異なるSTAから2つのチケットを取得してゲートウェイに配信しようとします。 ユーザーセッション中にいずれかのSTAにアクセスできない場合、セッションは2つ目のSTAを使い途切れることなく実行されます。

パスワードの変更： ドメインアカウント情報を使い指定ユーザーとしてWeb InterfaceまたはCitrix Online Plug-inにログオンするユーザーは、Windowsパスワードの有効期限が切れた場合にこれを変更することができます。 パスワードを変更する場合、認証しようとするドメイン内にユーザーのコンピューターがある必要はありません。

アカウントセルフサービス： Web InterfaceにPassword Managerのアカウントセルフサービス機能を統合すると、ユーザーは管理者が設定した質問に回答することで、自分のネットワークパスワードをリセットしたりアカウントのロックを解除したりできるようになります。

クライアント展開機能

Webベースのクライアントインストール： ユーザーがXenApp Webサイトにアクセスすると、Web Interfaceによって、デバイスとWebブラウザーの種類が検出され、適切なCitrixのクライアントをインストールするようにメッセージが表示されます。 近年のオペレーティングシステムおよびWebブラウザーにおけるセキュリティ強化の結果、ユーザーによるCitrixのクライアントのダウンロードおよび展開作業の難易度が増してきています。Web Interfaceのクライアント検出および展開処理機能により、ユーザーは簡単にクライアントを展開し、Webブラウザーの再構成を含む展開処理を実行することができます。 これにより、ユーザーは最もセキュリティに制限がある環境においても、サーバーで公開されているリソースにアクセスしてそれを起動することができます。

Citrix Online Plug-inのサポート： Citrix Online Plug-inにより、Webブラウザーを使わずにデスクトップから直接リソースにアクセスできます。 また、Citrix Online Plug-inのユーザーインターフェイスをユーザー側で変更できないようにして、ユーザーの構成ミスを防ぐこともできます。

Citrix Offline Plug-inのサポート： Citrix Offline Plug-inにより、XenAppアプリケーションをユーザーのデスクトップにストリーム配信し、ユーザーはローカルでそれを起動できます。 Citrix Offline Plug-inをCitrix Online Plug-inと一緒にインストールして、クライアント側のアプリケーション仮想化のすべての機能を提供したり、Citrix Offline Plug-inだけをインストールして、XenApp Webサイトを介したアプリケーションへのアクセスを提供したりできます。

新機能

更新日： 2014-12-02

このリリースの新機能および強化された機能を以下に示します。

新しいユーザーインターフェイス。 エンドユーザー向けのレイアウトと配色が新しくなり、ナビゲーションと見やすさが向上しました。

VM Hosted Appsセッションの共有。 Web InterfaceでVM（Virtual Machine：仮想マシン）Hosted Appsセッションを共有できるようになりました。 この機能は、シームレスアプリケーションを匿名ではないユーザーが実行する場合にのみ使用できます。

複数のデスクトップへのユーザーアクセス。 以前のバージョンのWeb Interfaceでは、ユーザーは1つのデスクトップグループにつき1つのデスクトップの単一のインスタンスにのみアクセスできました。 このリリースでは、ユーザーはデスクトップグループ内の複数のデスクトップの複数のインスタンスにアクセスできます。 ユーザーへのデスクトップの割り当てについて詳しくは、XenDesktop 5のドキュメントを参照してください。

Access Gateway用のスマートカードサポートの向上。 Web Interfaceでのスマートカード認証を、より多くの環境で使用できるようになりました。 Access Gatewayから送信されるユーザー名とドメインのほかに、ユーザープリンシパル名もWeb Interfaceで受け入れられるようになりました。 さらに、Web InterfaceはFIPSに準拠するように更新されました。この新機能はスマートカードオプションのパススルー認証でのみ使用できます。そして、管理者はドメイン管理者としてログオンする必要があります。 Access Gateway用のスマートカードサポートの構成について詳しくは、Access Gatewayのドキュメントを参照してください。

追加のデフォルト値の設定。 管理者は、音質、色数、帯域幅プロファイル、プリンターマッピング、およびウィンドウのサイズのような、帯域幅関連のすべての設定にデフォルト値を構成できます。

ICAファイルの署名。 生成されるICAファイルがWeb Interfaceによりデジタル署名され、そのファイルが信頼された発行元から送信されたことを互換性のあるCitrixのクライアントとプラグインで検証できます。

Web Interfaceのコンポーネント

Web Interface環境では、次の3つのネットワークコンポーネントが相互に作用して実行されます。

- 1つ以上のサーバーファーム
- Webサーバー
- WebブラウザーおよびCitrixのクライアントをインストールしたユーザーデバイス

サーバーファーム

単一のエンティティとして管理され、共に動作してリソースをユーザーに提供するサーバーのグループをサーバーファームと呼びます。 サーバーファームは、XenAppまたはXenDesktopのいずれかが動作する複数のサーバーにより構成され、これらを混在させることはできません。

サーバーファームの最も重要な機能の1つは、リソースの公開です。 これは管理者が、サーバーファームから配信される特定のリソース（アプリケーション、コンテンツ、およびデスクトップ）をユーザーが使用できるようにするプロセスです。 管理者がリソースをユーザーやユーザーグループに公開すると、そのリソースはオブジェクトとして使用可能になり、ユーザーはCitrixのクライアントを使ってこれらのオブジェクトに接続し、セッションを開始します。

Web Interfaceによって、サーバーファームにログオンしたユーザーのアカウント情報に従って、そのユーザーがアクセスできるリソースの一覧が表示されます。 このリソースの一覧をリソースセットといいます。 Web Interfaceサーバーは、1つまたは複数のサーバーファームに接続するときのアクセスポイントとして機能します。 Web Interfaceサーバーは、サーバーファームからリソースセット情報を取得し、それをWebブラウザーで表示可能なHTMLページに変換してユーザーに提供します。

Web Interfaceサーバーは、サーバーファームから情報を取得するために、要求をサーバーファームの1つ以上のサーバー上のCitrix XML Serviceに送信します。 Citrix XML Serviceは、XenAppおよびXenDesktopのコンポーネントの1つで、TCP/IPおよびHTTPを使用してリソースの情報をCitrixのクライアントとWeb Interfaceサーバーに送ります。 Citrix XML Serviceは、サーバーファームとWeb Interfaceサーバーの中継点として機能します。 Citrix XML ServiceはXenAppおよびXenDesktopと一緒にインストールされます。

Webサーバー

Web Interfaceは、Webサーバーによりホストされます。 Web Interfaceは、次のサービスを提供します。

- サーバーファームにアクセスするユーザーを認証します。
- ユーザーがアクセスできるリソースの一覧を含む、使用できるリソースに関する情報を取得します。

ユーザーデバイス

ユーザーデバイスとは、CitrixのクライアントとWebブラウザーを実行できるあらゆるコンピューターやデバイスを指します。 ユーザーデバイスには、デスクトップコンピューター、ラップトップコンピューター、ネットワークコンピューター、ターミナル、およびハンドヘルドコンピューターなどが含まれます。

ユーザーデバイスでは、WebブラウザーとCitrixのクライアントが、Web Interfaceにより提供されるリソースセットを表示するためのビューアーとエンジンとして機能します。 Webブラウザーは、Web Interfaceサーバー側で実行されるスクリプトによって作成されたリソースセットをユーザーに表示し、Citrixのクライアントは、ユーザーがリソースにアクセスするためのエンジンになります。

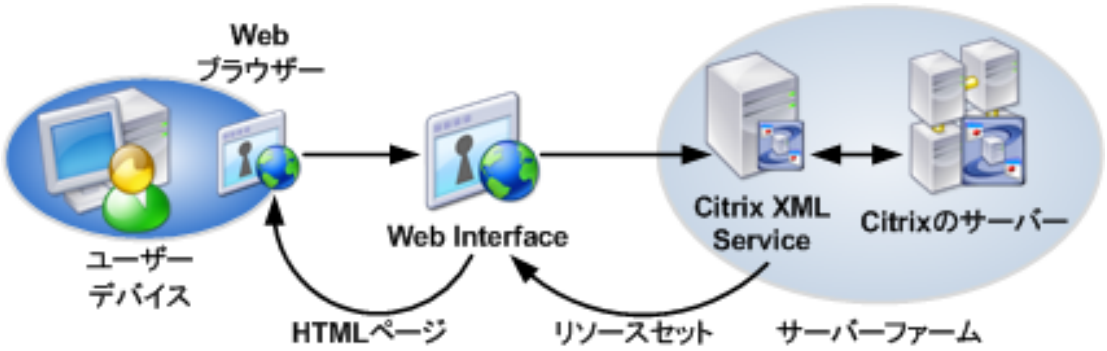
Web Interfaceには、WebサイトからCitrixのプラグインをユーザーに配布するための、Webベースクライアント展開機能があります。 Web Interfaceで作成したサイトにユーザーがアクセスすると、Webベースのクライアント検出および展開処理によってユーザーデバイスの種類が検出され、そのデバイスに適したCitrixのクライアントをインストールするようにメッセージが表示されます。 一部のプラットフォームでは、クライアント検出および展開処理により既存のクライアントインストールの有無も検出され、必要な場合にのみクライアントのインストールを求めるメッセージが表示されます。 詳しくは、「クライアント展開およびインストールキャプションの構成」を参照してください。

Web Interfaceは、WebブラウザーとCitrixのクライアントのさまざまな組み合わせをサポートしています。 サポートされているWebブラウザーとクライアントの組み合わせについては、「ユーザーデバイスの要件」を参照してください。

Web Interfaceのしくみ

次の図は、サーバーファーム、Web Interfaceサーバー、およびユーザーデバイス間の一般的な関係を示しています。

この図は、Web Interfaceを使用した一般的なサーバーファーム構成を示しています。 ユーザーデバイス上のWebブラウザーがWebサーバーに情報を送信し、Webサーバーがサーバーファームと通信して、リソースへのアクセスを許可します。



- Webブラウザーを介してWeb Interfaceへの認証を行います。
- Webサーバーはユーザーのアカウント情報を読み取り、ファームサーバーのサーバー上のCitrix XML Serviceにこの情報を送ります。 このサーバーは、Webサーバーとサーバーファーム内のほかのサーバー間のブローカーとして動作します。
- このサーバー上のCitrix XML Serviceが、ユーザーがアクセスできるリソースの一覧をサーバーから取得します。 クライアント側には、この一覧がリソースセットとして表示されます。 Citrix XML Serviceは、IMA（Independent Management Architecture）システムからリソースセットの情報を取得します。
- XenApp for UNIX（日本語版はリリースされていません）のサーバーファームでは、サーバー上のCitrix XML ServiceがICAブラウザーから収集した情報を使って、ユーザーがアクセス可能なアプリケーションを決定します。
- 次にCitrix XML Serviceが、ユーザーのリソースセット情報をサーバー上で動作するWeb Interfaceに返します。
- ユーザーが、HTMLページ上でリソースのアイコンをクリックします。
- Citrix XML Serviceは、サーバーファーム内で最も負荷の低いサーバーを特定してアクセスし、 そのサーバーのアドレスをWeb Interfaceに返します。
- Web Interfaceが、Citrixのクライアントと通信します（Webブラウザーを仲介役として使用することもあります）。
- Citrixのクライアントが、Web Interfaceにより提供された接続情報に従って、サーバーファームのサーバーとのセッションを開始します。

Web Interfaceで必要なシステム環境

更新日： 2014-11-24

Web Interfaceを実行するサーバーでは、以下のいずれかのCitrix製品を実行する必要があります。

Web Interfaceは、次の製品バージョンをサポートします。

- Citrix XenApp 7.6およびXenDesktop 7.6
- Citrix XenApp 7.5およびXenDesktop 7.5
- Citrix XenDesktop 7.1
- Citrix XenDesktop 7
- Citrix XenDesktop 5.6 Service Pack 1
- Citrix XenDesktop 5.6
- Citrix XenDesktop 5.5
- Citrix XenDesktop 5.0 Service Pack 1
- Citrix XenDesktop 5.0
- Citrix XenDesktop 4.0
- Citrix XenApp 6.5 for Microsoft Windows Server 2008 R2
- Citrix XenApp 6.0 for Microsoft Windows Server 2008 R2
- Citrix XenApp 5.0, with Feature Pack 2, for Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0, with Feature Pack 2, for Microsoft Windows Server 2003
- Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2008 x64 Edition
- Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2008
- Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0, with Feature Pack 1, for Microsoft Windows Server 2003
- Citrix XenApp 5.0 for Microsoft Windows Server 2008 x64 Edition
- Citrix XenApp 5.0 for Microsoft Windows Server 2008

- Citrix XenApp 5.0 for Microsoft Windows Server 2003 x64 Edition
- Citrix XenApp 5.0 for Microsoft Windows Server 2003
- Citrix XenApp 4.0, with Feature Pack 1, for UNIX Operating Systems
- Citrix Presentation Server 4.5, with Feature Pack 1, for Windows Server 2003 x64 Edition
- Citrix Presentation Server 4.5, with Feature Pack 1, for Windows Server 2003
- Citrix Presentation Server 4.5 for Windows Server 2003 x64 Edition
- Citrix Presentation Server 4.5 for Windows Server 2003

重要： XenApp 4.0 with Feature Pack 1 for UNIXとの互換性を維持する場合は、追加のサイト構成が必要となります。 詳しくは、「XenApp 4.0 with Feature Pack 1 for UNIXのサポートを構成するには」を参照してください。

Web Interfaceは、これらの製品でサポートされるすべてのプラットフォームをサポートしています。 サポートされるプラットフォームの一覧については、Citrixサーバーのドキュメントを参照してください。 また、サーバーにオペレーティングシステムの最新のService Packをインストールすることをお勧めします。

構成に関する一般的な要件

サーバーは、サーバーファームのメンバーである必要があります。 サーバーファームのサーバーは、リソース（アプリケーション、コンテンツ、デスクトップ）を公開している必要があります。 サーバーファームのメンバーシップとリソースの公開については、Citrixサーバー製品のドキュメントを参照してください。

XenApp for UNIX（日本語版はリリースされていません）サーバーの場合も、公開アプリケーションを設定しておく必要があります。 また、これらのアプリケーションをWeb Interfaceで使えるように構成する必要があります。 Citrix XML Service for UNIXのインストール方法、およびアプリケーションをWeb Interfaceで使えるように構成する方法については、XenApp for UNIXのドキュメントを参照してください。

必要なソフトウェア

最新のリリースがインストールされてない場合は、一部の新機能は使用できません。 たとえば、シームレスなサーバーファームの移行はXenApp 6.0にアップグレードする場合にのみ実行できます。

次に、Web Interfaceの主な機能を実行するために必要となるソフトウェアの最低要件を示します。

注： Citrix製品の特定のリリースでWeb Interface 5.4をサポートしているか確認するには、その製品のシステム要件を参照してください。

Web Interfaceの機能	ソフトウェア要件
XenAppサーバーファーム移行	Citrix XenApp 6.0
ユーザーローミング	Citrix XenDesktop 4.0 Citrix XenApp 6.0
XenApp VM Hosted Apps	Citrix XenApp 5.0 with Feature Pack 2
障害復旧	Citrix XenDesktop 4.0 Citrix XenApp 5.0 with Feature Pack 2
Secure Ticket Authority冗長	Citrix XenDesktop 4.0 Citrix XenApp 5.0 with Feature Pack 2 Citrix Access Gateway 4.6, Standard Edition
Windows 7およびInternet Explorer 8.0のサポート	Citrix XenDesktop 4.0 Citrix XenApp 5.0 with Feature Pack 2 Citrix Online Plug-in 11.2 Citrix Online Plug-in 5.2
仮想デスクトップ再起動	Citrix XenDesktop 3.0 Citrix Desktop Receiver 11.1
ユーザーフォルダーのリダイレクト	Citrix XenApp 5.0 Citrix XenApp Plugin for Hosted Apps 11.0 forWindows
フォントスムージング	Citrix XenApp 5.0 Citrix XenApp Plugin for Hosted Apps 11.0 forWindows

XenDesktopのサポート	Citrix XenDesktop 2.0 Citrix Desktop Receiver Embedded Edition10.250
Windows VistaおよびInternet Explorer 7.0のサポート	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Presentation Server Windowsクライアント10.1
オフラインアプリケーションのサポート	Citrix Presentation Server 4.5 Citrix Streamingクライアント1.0 Citrix Program Neighborhoodエージェント10.0
AD FSのサポート	Citrix Presentation Server 4.5
アクセス制御ポリシーのサポート	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Access Gateway 4.2 with Advanced AccessControl Citrix MetaFrame Presentation Server Win32クライアントVersion 9.0
アカウントセルフサービス	Citrix Password Manager 4.0
ユーザーによるパスワードの変更	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix Program Neighborhoodエージェント10.1
セッション画面の保持	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix MetaFrame Presentation Server Win32クライアントVersion 9.0
ワークスペースコントロール	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix MetaFrame Presentation Server Win32クライアントVersion 8.0
スマートカードのサポート	Citrix XenDesktop 3.0 Citrix Presentation Server 4.5 Citrix Desktop Receiver 11.1 Citrix Presentation Server Win32クライアント7.0

Secure Gatewayのサポート	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, with Feature Pack 1, for UNIX Operating Systems Citrix Presentation Server Win32クライアント7.0
NDS認証	Citrix Presentation Server 4.5 Citrix Presentation Server Win32クライアント7.0
DNSアドレス解決	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, with Feature Pack 1, for UNIX Operating Systems Citrix Presentation Server Win32クライアント7.0
コンテンツ公開機能の強化	Citrix Presentation Server 4.5 Citrix Presentation Server Win32クライアント7.0
負荷分散	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, with Feature Pack 1, for UNIX Operating Systems
サーバー側でのファイアウォールのサポート	Citrix XenDesktop 2.0 Citrix Presentation Server 4.5 Citrix XenApp 4.0, with Feature Pack 1, for UNIX Operating Systems
クライアント側でのファイアウォールのサポート	Citrix Presentation Server Win32クライアント7.0
パススルー認証	Citrix Presentation Server 4.5 Program Neighborhood 32ビットWindows（完全版） Citrix Program Neighborhoodエージェント7.0
リモートデスクトップ接続（RDP）	Citrix XenDesktop 4.0 Citrix Presentation Server 4.5

Webサーバーの要件

更新日： 2014-09-24

Webベースのクライアント展開を実行するには、Citrixのクライアントのインストールファイルをwebサーバーにコピーしておく必要があります。 サポートされるクライアントのバージョンについては、「ユーザーデバイスの要件」を参照してください。 Web Interfaceサーバーへのクライアントファイルのコピーについては、「Web Interfaceへのクライアントインストールファイルのコピー」を参照してください。

Windowsプラットフォーム

Web Interfaceは、次のWindowsプラットフォームにインストールできます。

オペレーティングシステム	Webサーバー	Runtime/JDK	サーブレットエンジン

Windows Server 2008 R2 x64 Windows Server 2008 R2（Service Pack 1インストール済み）	Internet Information Services 7.5	.NET Framework 3.5 with Service Pack 1 Visual J#.NET 2.0 Second Edition ASP.NET 2.0	-
Windows Server 2008 x64（Service Pack 2インストール済み） Windows Server 2008 x86（Service Pack 2インストール済み）	Internet Information Services 7.0		
Windows Server 2003 R2 x86（Service Pack 2インストール済み） Windows Server 2003 Standard Edition x86（Service Pack 2インストール済み） Windows Server 2003 Enterprise Edition x86（Service Pack 2インストール済み） Windows Server 2003 R2 Standard Edition x86（Service Pack 2インストール済み） Windows Server 2003 R2 Standard Edition x64（Service Pack 2インストール済み）	Internet Information Services 6.0		
Windows Server 2003 Standard Edition x86（Service Pack 2インストール済み）	Apache 2.2.x	Java 1.6.x	Apache Tomcat 6.0.x

Microsoftインターネットインフォメーションサービス（IIS）を使用する場合、サーバーを構成して適切なサーバーの役割を追加し、IISおよびASP.NET（IISのサブコンポーネント）をインストールする必要があります。 .NET Frameworkのインストール時にIISがまだインストールされていない場合は、IISをインストールしてからFrameworkを再インストールするか、IISをインストールしてからC:¥Windows¥Microsoft.NET¥Framework¥<Version>ディレクトリでaspnet_regiis.exe -iコマンドを実行します。 .NET FrameworkとVisual J# .NETの再配布ファイルは、XenAppおよびXenDesktopのインストールメディアのSupportフォルダーに収録されています。

ユーザー側の要件

更新日： 2014-05-23

次に、ユーザーがWeb Interfaceサイトにアクセスするために必要なWebブラウザーとオペレーティングシステムの組み合わせを示します。

Webブラウザー	オペレーティングシステム
Internet Explorer 11	Windows 8.1 32ビット Windows 8.1 64ビット Windows 8 32ビット Windows 8 64ビット Windows Server 2012 64ビット Windows Server 2012 R2 64ビット Windows 7 32ビット（Service Pack 1インストール済み） Windows 7 64ビット（Service Pack 1インストール済み） Windows Server 2008 R2 64ビット（Service Pack 1インストール済み）
Internet Explorer 10	Windows 7 32ビット（Service Pack 1インストール済み） Windows 7 64ビット（Service Pack 1インストール済み） Windows Server 2008 R2 64ビット（Service Pack 1インストール済み）
Internet Explorer 9.x （32ビットモード）	Windows Vista 32ビット（Service Pack 2以降インストール済み） Windows Vista 64ビット（Service Pack 2以降インストール済み） Windows 7 32ビット RTM以降 Windows 7 64ビット RTM以降 Windows Server 2008 32ビット（Service Pack 2以降インストール済み） Windows Server 2008 64ビット（Service Pack 2以降インストール済み） Windows Server 2008 R2 64ビット

Internet Explorer 8.x （32ビットモード）	Windows 7 64ビット Windows 7 32ビット Windows XP Professional（Service Pack 3インストール済み） Windows XP Professional x64 Edition（Service Pack 2インストール済み） Windows Vista 32ビット（Service Pack 2インストール済み） Windows Vista 64ビット（Service Pack 2インストール済み） Windows Server 2008 R2 Windows Server 2008（Service Pack 2インストール済み） Windows Server 2003（Service Pack 2インストール済み）
Internet Explorer 7.x （32ビットモード）	Windows Vista 64ビット（Service Pack 2インストール済み） Windows Vista 32ビット（Service Pack 2インストール済み） Windows Server 2008（Service Pack 2インストール済み） Windows Server 2003（Service Pack 2インストール済み）
Safari 5.x	Mac OS X Snow Leopard 10.6
Safari 4.x	Mac OS X Leopard 10.5

Mozilla Firefox 4.x （32ビットモード）	Windows 7 64ビット Windows 7 32ビット Windows XP Professional（Service Pack 3インストール済み） Windows XP Professional x64 Edition（Service Pack 2インストール済み） Windows Vista 32ビット（Service Pack 2インストール済み） Windows Vista 64ビット（Service Pack 2インストール済み） Windows Server 2003（Service Pack 2インストール済み）
Mozilla Firefox 3.x	Mac OS X Snow Leopard 10.6 Mac OS X Leopard 10.5 Windows XP Professional x32 Edition（Service Pack 3インストール済み） Windows Vista 32ビット（Service Pack 2インストール済み） Windows 7 32ビット Red Hat Enterprise Linux 5.4 Desktop Windows Server 2003（Service Pack 2インストール済み）
Mozilla 1.7	Solaris 10

注： Web Interface 5.4は、このページで示されているソフトウェアバージョンでのみサポートされます。 より新しいバージョンでも動作する場合がありますが、動作確認が実施されていないためサポートされません。

オフラインアプリケーションにアクセスするための要件

次に、オフラインアプリケーションにユーザーがアクセスするために必要なWebブラウザーとオペレーティングシステムの組み合わせを示します。

Webブラウザー	オペレーティングシステム
Internet Explorer 8.x （32ビットモード）	Windows 7 64ビット Windows 7 32ビット Windows Vista 64ビット（要Service Pack 2） Windows Vista 32ビット（要Service Pack 2） Windows XP Professional x64 Edition（要Service Pack 2） Windows XP Professional（要Service Pack 3） Windows Server 2008 R2 Windows Server 2008 x64（要Service Pack 2） Windows Server 2008（要Service Pack 2） Windows Server 2003 x64エディション（Service Pack 2適用済み） Windows Server 2003（要Service Pack 2）
Internet Explorer 7.x （32ビットモード）	Windows Vista 64ビット（要Service Pack 2） Windows Vista 32ビット（要Service Pack 2） Windows XP Professional x64 Edition（要Service Pack 2） Windows XP Professional（要Service Pack 3） Windows Server 2008 x64（要Service Pack 2） Windows Server 2008（要Service Pack 2） Windows Server 2003 x64エディション（Service Pack 2適用済み） Windows Server 2003（要Service Pack 2）

Mozilla Firefox 3.x	Windows 7 64ビット Windows 7 32ビット Windows Vista 64ビット（要Service Pack 2） Windows Vista 32ビット（要Service Pack 2） Windows XP Professional x64 Edition（要Service Pack 2） Windows XP Professional（要Service Pack 3） Windows Server 2003（要Service Pack 2）

そのほかのユーザーデバイスの要件

ユーザーは次の構成のシンクライアント、PDA（Personal Digital Assistant）、およびハンドヘルドデバイスを使ってWeb Interfaceにアクセスできます。

デバイス	オペレーティングシステム	Webブラウザー
iPhone	-	Safari 5.x
iPad	-	Safari 5.x
HTC Touch2	Windows Mobile 6.5 Professional	Pocket/WinCE Internet Explorer Opera Mobile 10
HP GY227 WYSE V90	Windows XP Embedded（Service Pack 2インストール済み）	Internet Explorer 6.x
HP T5730	Windows Embedded Standard 2009	Internet Explorer 7.x
HP T5540	Windows Embedded CE 6.0 R2	Internet Explorer 6.x
HP RK270 WYSE V30	Windows Embedded CE 6.0	Internet Explorer 6.x
HP GY231	Debian Linux 4.0	Debian Iceweasel 2.0
Symbian E61/E70	Symbian	SymbianのWebブラウザー

ユーザーデバイスの要件

ユーザーがWeb Interfaceを使用するには、サポートされるCitrixのクライアント、またはJava Runtime EnvironmentとサポートされるWebブラウザーのいずれかがユーザーのデバイスにインストールされている必要があります。 XenAppおよびXenDesktopのインストールメディアに収録されているすべてのクライアントは、Web Interfaceと互換性があります。 これらのクライアントは、Citrix社のWebサイトからダウンロードすることもできます。

より新しい機能を利用できるように、ユーザーに最新のクライアントを配布することをお勧めします。 クライアントの機能やオプションは、バージョンによって異なります。クライアントがサポートしている機能については、各クライアントのドキュメントを参照してください。

Web Interfaceのインストール

Web Interfaceをインストールするには、XenAppまたはXenDesktopのインストールメディアを使用します。

Web Interfaceは、次のプラットフォームにインストールできます。

- サポートするWindowsオペレーティングシステム
  - Microsoftインターネットインフォメーションサービス（IIS）
  - Apache Tomcat
- サポートするUNIXオペレーティングシステム
  - Apache Tomcat
  - IBM WebSphere
  - Sun GlassFish Enterprise Server

Webサーバー要件のインストール手順については、「Webサーバーの要件」を参照してください。

コマンドラインからスクリプトを実行して、無人インストールとサイト管理を行うことができます。 Web Interfaceでのコマンドラインの使用方法について詳しくは、Knowledge Centerを参照してください。

Web Interfaceのインストール手順については、「Microsoftインターネットインフォメーションサービス（IIS）上にWeb Interfaceをインストールするには」および「Java Application Server上へのWeb Interfaceのインストール」を参照してください。

セキュリティに関する注意事項

WindowsベースのサーバーにWeb Interfaceをインストールする場合、Microsoft社の標準のガイドラインに従って、Windowsサーバーを構成してください。 UNIXの場合は、そのオペレーティングシステムのガイドラインに従ってください。

Citrix XML Serviceで使用するポート番号の確認

Web Interfaceサイトの作成時（IISの場合）またはWARファイルの生成時（Java Application Serverの場合）に、Citrix XML Serviceが使用しているポートの確認が求められます。 Citrix XML Serviceは、サーバーファームとWeb Interfaceサーバー間の通信リンクになります。

Windowsプラットフォームでは、インターネットインフォメーションサービスのTCP/IPポートを共有するようにCitrix XML Serviceを構成できます。 この場合、インターネットインフォメーションサービスのWWWサービスにより使用されるポートを検索して、Citrix XML Serviceポートを決定する必要があります。 デフォルトでは、WWWサービスはポート80を使用します。 Citrix XML Serviceの専用のポートが必要な場合は、ポート8080を使用することをお勧めします。

Windowsプラットフォーム使用中のポート一覧を表示するには、コマンドプロンプトで netstat -aと入力します。 XenApp for UNIXサーバーでは、コマンドプロンプトで ctxnfusesrv -lと入力してポート情報を表示します。

注： 必要に応じて、サーバー上のCitrix XML Serviceが使用するポートを変更できます。詳しくは、サーバー製品のドキュメントを参照してください。

Microsoftインターネットインフォメーションサービス（IIS）上にWeb Interfaceをインストールするには

Web Interfaceをインストールする前に、サーバーにWebサーバーの役割を追加して、IISとASP.NET（IISのサブコンポーネント）をインストールする必要があります。

Windows Server 2008でIIS 7.xを使用するには、［Webサーバー（IIS）］の役割をインストールして、次の役割サービスを有効にします。

- ［Webサーバー］>［アプリケーション開発］>［ASP.NET］
- ［管理ツール］>［IIS 6管理互換］>［IIS 6メタベース互換］

パススルー認証、スマートカードパススルー認証、およびスマートカード認証を有効にする場合は、次の役割サービスもインストールする必要があります。

- パススルー認証およびスマートカードパススルー認証では、［Webサーバー］>［セキュリティ］>［Windows認証］
- スマートカード認証では、［Webサーバー］>［セキュリティ］>［クライアント証明書のマッピング認証］

Windows Server 2003でIIS 6.0を使用するには、［アプリケーションサーバー（IIS、ASP.NET）］の役割を追加して、ASP.NETを有効にします。

IISで、各サイトをアプリケーションプールに割り当てます。 アプリケーションプール構成には、ワーカープロセスの最大数を制御する設定が含まれています。 デフォルト値の1を変更すると、Web Interfaceを実行できない場合があります。

サーバーの役割を構成後、.NET Framework 3.5 with Service Pack 1およびVisual J#.NET 2.0 Second Editionをインストールします。

Web Interface Version 4.5またはそれ以降のバージョンからアップグレードする場合は、既存のサイトのバックアップを確認するメッセージが表示されます。

重要： 集中管理構成サイトおよびConferencing Managerゲスト出席者サイトはサポートされません。 以前のバージョンからアップグレードする場合は、サーバー上の既存のConferencing Managerゲスト出席者サイトがインストーラーにより削除されます。 既存の集中管理構成サイトは、アップグレードされてローカル構成を使用するように変換されます。

1. 管理者としてログオンします。

   XenAppまたはXenDesktopのインストールメディアからインストールする場合は、Webサーバーにディスクを挿入します。

Web InterfaceをCitrixのWebサイトからダウンロードした場合は、WebInterface.exeファイルをWebサーバーにコピーします。

2. WebInterface.exeを検索してダブルクリックします。

3. 使用する言語を一覧から選択します。 使用しているオペレーティングシステムの言語設定が検出され、デフォルトとして選択されます。 ［OK］をクリックします。

4. ［ようこそ］ページで［次へ］をクリックします。

5. ［ライセンス契約書］ページで、［ライセンス契約に同意します］をクリックし、［次へ］をクリックします。

6. ［インストールフォルダー］ページでWeb Interfaceをインストールする場所を指定します（デフォルトは、C:¥Program Files (x86)¥Citrix¥Web Interface¥）。 ［次へ］をクリックします。

7. ［クライアントの場所］ページで［このコンピューターにクライアントをコピーする］を選択します。 ［参照］をクリックして、インストールメディアまたはネットワーク上のCitrixのクライアントのセットアップファイルを選択します。

   セットアップにより、インストールメディアまたはネットワーク共有の¥Citrix Receiver and Plug-insフォルダーの内容がWeb InterfaceのClientsフォルダー（通常C:¥Program Files (x86)¥Citrix¥Web Interface¥Version¥Clients）にコピーされます。 このインストール処理で作成されるすべてのWebサイトでは、Webサーバーのこのディレクトリ内にクライアントファイルが格納されていることを前提としています。

   Web Interfaceのインストール時にクライアントファイルをWebサーバーにコピーしない場合は、［この手順をスキップする］を選択します。 クライアントファイルは後でWebサーバーにコピーできます。

8. ［次へ］をクリックして続行し、［次へ］をクリックしてインストールを開始します。

9. インストールが完了したら、［完了］をクリックします。

10. Windowsの［スタート］メニューをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択してWeb Interface管理コンソールにアクセスし、サイトの作成および構成を開始します。

Windows Server 2003 x64 Edition上のほかのコンポーネントとの互換性

Windows Server 2003の64ビットバージョン上にWeb Interface for Microsoft Internet Information Servicesをインストールすると、IIS 6.0の32ビットWeb拡張のサポートが有効になり、これにより64ビット拡張のサポートが無効になります。 Windows Server 2003の64ビットバージョン上にWeb Interface for Microsoft Internet Information Servicesをインストールする場合は、XenApp、XenDesktop、およびライセンス管理コンソールを含むほかのCitrixソフトウェアをインストールする前に、Web Interfaceをインストールする必要があります。 これにより、IIS 6.0の32ビットサポートをCitrixソフトウェアに適用できます。これらのソフトウェア製品のインストール順を間違うと、Webサーバーへのアクセス時に「Internet Explorerではこのページは表示できません」という内容のエラーメッセージが表示される場合があります。

Windows Server 2003 x64 Edition上にインストールした場合、Web Interface for Microsoft Internet Information Servicesは、WindowsコンポーネントのRPC over HTTP proxyなど64ビットISAPIフィルターを使用する製品と互換性を持たない場合があります。このため、Web Interfaceをインストールする前に、RPC over HTTP proxyをアンインストールする必要があります。

RPC over HTTP proxyをアンインストールするには

1. ［スタート］ボタンをクリックし、［コントロールパネル］>［プログラムの追加と削除］の順に選択します。
2. ［Windowsコンポーネントの追加と削除］を選択します。
3. ［ネットワークサービス］を選択して［詳細］をクリックします。
4. ［HTTPプロキシを経由したRPC］チェックボックスをオンにして、［OK］をクリックします。
5. ［次へ］をクリックして、HTTPプロキシを経由したRPCをアンインストールし、サーバーを再起動します。

Java Application Server上へのWeb Interfaceのインストール

注： IBM WebSphere上にWeb Interfaceをインストールする場合は、was.policyファイルのコンテンツの問題を示す、アプリケーションセキュリティ警告メッセージが表示されます。 このポリシーファイルは、WebSphereで［Security］>［Global Security］>［Enforce Java 2 Security］の順に選択すると作成されます。 WebSphere Java 2 Securityポリシーファイルに従ってwas.policyを編集する必要があります。このポリシーに準拠しない場合は、Web Interfaceが正しく機能しない可能性があります。 このポリシーファイルは、WEBSPHERE_HOME/AppServer/installedApps/NodeName/WARFileName.ear/META-INFにあります。

Web Interface for Java Application Serversを実行するには、サーブレットエンジンが必要です。 Apache WebサーバーでWeb Interfaceをサポートするには、Tomcatなどのサーブレットエンジンが必要です（Tomcatは、スタンドアロンのWebサーバーまたはサーブレットエンジンとして使用できます）。

Tomcat上にWeb Interfaceをインストールするには

1. インストールメディアのWeb InterfaceディレクトリからWebInterface.jarファイルを任意の一時フォルダーにコピーします。
2. コマンドプロンプトで上記の一時ディレクトリ移動して、java -jar WebInterface.jarと入力してインストーラーを起動します。
3. Enterキーを押して、ライセンス契約の内容を確認します。
4. Yと入力して、ライセンス契約に同意します。
5. 一覧からサイトの種類を選択します。
6. 画面上に表示される質問に答えて、サイトの初期構成を指定します。
7. 選択したオプションの概要が表示されます。 表示された内容が正しければ、Yを入力してWARファイルを作成します。 WARファイルが作成され、必要に応じてCitrixのクライアントがインストールメディアからコピーされます。
8. 画面の指示に従って、WARファイルのインストールを終了します。

Sun GlassFish Enterprise Serverが動作するサーバー上でセキュリティポリシーを構成するには

Sun GlassFish Enterprise Serverが動作するサーバー上でアカウントセルフサービスが有効なXenApp Webサイトを作成するには、まずそのサーバーのセキュリティポリシーを手動で構成する必要があります。

1. サイトのWARファイルをサーバーに配布します。
2. Webサーバーを停止します。
3. ドメイン構成フォルダーにあるserver.policyファイルを編集します。 Sun GlassFish Enterprise ServerがSunGlassFishEnterpriseServerRoot/AppServerにインストールされており、サイトがdomain1に保存されている場合、このファイルはSunGlassFishEnterpriseServerRoot/AppServer/domains/domain1/configにあります。
4. 一般的なgrantブロックの前に、以下の構成を追加します。

   ```
   grant codeBase
   "file:${com.sun.aas.instanceRoot}/applications/
   j2ee-modules/WARFileName/-"{
   permission java.lang.RuntimePermission
   "getClassLoader";
   permission java.lang.RuntimePermission
   "createClassLoader";
   permission java.util.PropertyPermission
   "java.protocol.handler.pkgs", "read, write";
   };
   ```

   ここで、WARFileNameには、サイトのWARファイルの名前の最初の部分（「XenApp」など）を指定します。
5. SunGlassFishEnterpriseServerRoot/ApplicationServer/libにあるLauncher.xmlファイルのsysproperty key="com.sun.enterprise.overrideablejavaxpackages"要素の値一覧にelement.javax.wsdlを追加します。
6. Webサーバーを起動します。

言語パックの使用

言語パックには、特定の言語（日本語、英語、ドイツ語、スペイン語、フランス語、中国語（簡体、繁体）、韓国語）にサイトをローカライズするために必要なすべての情報が含まれており、以下のファイルで構成されています。

- サイトのリソースファイル
- ユーザーヘルプ
- ローカライズされたアイコンおよびイメージ

IISでは、Web Interfaceに言語パックを追加するにはツリーをコピーするか、またはlanguagesフォルダー（通常は、C:¥Program Files (x86)¥Citrix¥Web Interface¥Version¥languages）にファイルを展開します。 特定のサイトの言語をカスタマイズするには、言語パックをそのサイトのディレクトリにコピーして変更を加えます。 これにより、このサイトでのみ変更した言語パックが使用され、そのほかのサイトではデフォルト設定が使用されるようになります。

注： IIS上でWindowsエラーメッセージを適切な言語で表示させるには、Microsoft .NET Frameworkの適切な言語パックをインストールする必要があります。

Java Application Server上では、追加の言語パックをインストールするにはサイト内の適切なディレクトリに移動してファイルを展開します。

適切な言語を表示できない場合に常に英語が使用されるため、Webサーバーに必ず英語の言語パックをインストールしておく必要があります。 言語パックは、Web Interfaceのバージョン固有であり、ほかのバージョンには使用できません。 言語パックの使用について詳しくは、Web Interface SDKを参照してください。

言語パックの削除

Windows CEが動作するデバイスなど一部のデバイスでは、日本語など、特定の言語を表示できない場合があります。 この場合、ユーザーインターフェイスの言語選択一覧に、使用できない言語の名前が正しく表示されません。 これを防ぐには、すべてのサイトまたは特定のサイトから問題の言語を削除します。

IIS上のサイトでは、languagesフォルダー（通常はC:¥Program Files (x86)¥Citrix¥Web Interface¥Version¥languages）からLanguageCode.lang（ja.langなど）を削除します。 これにより、この言語がサーバー上のすべてのサイトから削除されます。 特定のサイトでこの言語を有効にする場合は、そのサイトのlanguagesフォルダーに.langファイルを移動します。

Java Application Server上のサイトの場合は、WARファイルの作成後に、適切なツールでWARファイルを開き、LANGファイルを削除してから再パッケージ化します。 これにより、そのWARファイルによって展開されるサイトからその言語が削除されます。

旧バージョンのWeb Interfaceのアップグレード

Version 4.5 以降のWeb Interfaceを最新バージョンにアップグレードするには、XenAppまたはXenDesktopのインストールメディアからインストールするか、ダウンロードサイトから入手したファイルを使用します。

Web Interfaceを以前のバージョンにダウングレードすることはできません。

重要： 集中管理構成サイトおよびConferencing Managerゲスト出席者サイトはサポートされません。 以前のバージョンからアップグレードする場合は、サーバー上の既存のConferencing Managerゲスト出席者サイトがインストーラーにより削除されます。 既存の集中管理構成サイトは、アップグレードされてローカル構成を使用するように変換されます。

ユーザーに対するWebベースのクライアント展開に使用されるClientsフォルダーのディレクトリ構造は、Web Inrterfaceのバージョン5.1以前のものとは異なります。 XenAppまたはXenDesktopのインストールメディアを使用してWeb Interfaceをアップグレードする場合、アップグレードの際にインストールメディアからディレクトリ構造をコピーします。 Webダウンロードによりアップグレードする場合、必要なディレクトリ構造を手動で再生成する必要があります。 次に、必要なクライアントをCitrixのWebサイトからダウンロードできます。 Clientsディレクトリ構造については、「Web Interfaceへのクライアントインストールファイルのコピー」を参照してください。

デフォルトでは、クライアントインストールファイルのファイル名はXenAppまたはXenDesktopのインストールメディアで提供されているファイル名と同じであると仮定しています。 クライアントのインストールファイルをCitrixのWebサイトからダウンロード、または古いバージョンのクライアントソフトウェアを展開する場合は、XenApp Webサイトの構成ファイルでClientIcaLinuxX86、ClientIcaMac、ClientIcaSolarisSparc、ClientIcaSolarisX86、ClientIcaWin32、およびClientStreamingWin32パラメーターに対して適切なクライアントインストールファイル名が指定されているかチェックします。 Web Interface構成ファイルのパラメーターについては、「WebInterface.confのパラメーター」を参照してください。

インストール後の作業

Web Interfaceをインストールしたら、次に、ユーザーがWeb Interfaceを使用できるようにする必要があります。 これを実行するには、Citrix Web Interface管理コンソールを使用するか、またはWebInterface.confファイルを直接編集して、サイトの作成と構成を行います。

また、インストールされているほかのコンポーネントに合わせてWeb Interfaceを構成したり、必要に応じてWeb Interfaceの機能をカスタマイズまたは拡張したりする必要があります。

- Citrix Web Interface管理コンソールまたはWebInterface.confファイルを使用してWeb Interfaceを構成する方法については、それぞれ「Citrix Web Interface管理コンソールでのサイトの構成」または「構成ファイルを使用したサイトの構成」を参照してください。
- Access GatewayまたはSecure GatewayをサポートするようにCitrix Web Interface管理コンソールでWeb Interfaceを構成する方法については、「ゲートウェイ設定を構成するには」を参照してください。
- Web InterfaceでAD FSを使用する構成については、「Web Interfaceに対するActive Directoryフェデレーションサービスのサポートの構成」を参照してください。
- セキュリティに関する注意事項については、「Web Interfaceのセキュリティ構成」を参照してください。
- Web Interfaceの機能の拡張とカスタマイズについては、Web Interface SDKを参照してください。

Web Interfaceのインストール環境のトラブルシューティング

IISが動作するWindowsプラットフォームでは、［修復］オプションを使ってWeb Interfaceのトラブルシューティングを実行できます。 ［修復］オプションを使用しても問題が解決されない場合や、このオプションが使用できない場合（Java Application Serverを使用する場合など）は、いったんWeb Interfaceをアンインストールしてから Web Interfaceを再インストールしてください。 詳しくは、「Web Interfaceのアンインストール」を参照してください。 Web Interfaceを再インストールした場合は、すべてのサイトを再度作成する必要があります。

［修復］オプションを使用するには

Web Interfaceのインストール環境で問題が発生した場合は、［修復］オプションを使って問題を解決できることがあります。 ［修復］オプションを使用すると、共通ファイルが再インストールされますが、既存のサイトが修復されたり、上書きされたりすることはありません。

重要： インストールされているWeb interfaceにカスタマイズされたコードがあり、［修復］オプションを選択した場合は、このカスタマイズされたコードは削除されます。 このオプションを実行する前に、すべてのカスタマイズされたファイルのバックアップを取ることをお勧めします。

1. WebInterface.exeファイルをダブルクリックします。
2. ［修復］をクリックして、［次へ］をクリックします。
3. 画面に表示される指示に従います。

Web Interfaceのアンインストール

Web Interfaceをアンインストールすると、Clientsフォルダーを含むすべてのWeb Interfaceファイルが削除されます。 したがって、Web Interfaceのファイルを保存しておきたい場合は、Web Interfaceをアンインストールする前にこれらのファイルをコピーしておいてください。

まれに、Web Interfaceをアンインストールできないことがあります。 この場合、次のような原因が考えられます。

- アンインストーラーを実行するために必要なレジストリへのアクセス権がない
- Web Interfaceのインストール後にシステムからIISが削除されている

Micorosoftインターネットインフォメーションサービス（IIS）上のWeb Interfaceをアンインストールするには

1. ［スタート］ボタンをクリックし、［コントロールパネル］>［プログラムと機能］の順に選択します。
2. ［Citrix Web Interface］を選択して、［アンインストール］をクリックします。
3. 画面に表示される指示に従います。

Java Application Server上のWeb Interfaceのアンインストール

WebアプリケーションをアンインストールするためのツールがWebサーバーソフトウェアにより提供されている場合は、そのツールの手順に従ってWeb Interfaceをアンインストールしてください。 または、手動でWeb Interfaceをアンインストールすることもできます。

1. コマンドプロンプトを開き、WARファイルをコピーしたディレクトリに移動します。
2. Webサーバーを停止し、WARファイルを削除します。

   WARファイルの解凍先ディレクトリも削除する必要があります。 このディレクトリの名前は、通常、WARファイルのファイル名と同じ名前です。 たとえば、「mysite.war」というWARファイルを展開すると、「mysite」というディレクトリにWARファイルの内容が展開されます。

   注： Web Interfaceをアンインストールしても、削除されずにサーバーに残るファイルがいくつかあります。 削除されないファイルの種類については、Citrix XenAppのReadmeファイルを参照してください。

はじめに

更新日： 2014-11-24

Web Interfaceの構成方法の決定

Citrix Web Interface管理コンソールを使用するか、またはWeb terfaceの構成ファイルを編集して、Web Interfaceを構成およびカスタマイズすることができます。

Citrix Web Interface管理コンソールの使用

Citrix Web Interface管理コンソールはMicrosoft管理コンソール（MMC）3.0のスナップインで、これを使ってMicrosoftインターネットインフォメーションサービス（IIS）上にXenApp WebサイトおよびXenApp Servicesサイトを作成して構成できます。 コンソールの左側のペインには、Web Interfaceサイトの種類が表示されます。 中央の結果ペインには、左側のペインで選択されたサイト種類のコンテナー内で使用できるサイトが表示されます。

管理者は、Citrix Web Interface管理コンソールを使って日常的な管理作業をすばやく簡単に実行できます。 ［操作］ペインには、現在使用できるタスクが一覧で表示されます。 左側のペインで選択されたアイテムに関連するタスクは上に、結果ペインで選択されたアイテムに対して実行できる操作は下に表示されます。

管理者による構成は、Web Interface管理コンソールで変更を確定した時点で有効になります。 このため、その環境に適切でない値をCitrix Web Interface管理コンソールで指定するとその構成は適用されず、WebInterface.confの値がデフォルトにリセットされることがあります。 このような場合に備えて、定期的にWebInterface.confとConfig.xmlファイルのバックアップを作成してください。

Web Interface for Microsoft Internet Information Servicesをインストールすると、Citrix Web Interface管理コンソールが自動的にインストールされます。 ［スタート］をクリックし、［（すべての）プログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択してコンソールを起動します。

注： Web Interfaceをインストールするサーバー上には、Citrix Web Interface管理コンソールに必要なMMC 3.0がインストールされている必要があります。 MMC 3.0は、Web InterfaceのホストをサポートするすべてのWindowsプラットフォームでデフォルトで使用できます。

構成ファイルの使用

次の構成ファイルを編集して、Web Interfaceのサイトを構成することができます。

- Web Interface構成ファイル： このWebInterface.confファイルでWeb Interfaceの設定の大半を変更できます。このファイルは、Microsoftインターネットインフォメーションサービス（IIS）とJava Application Serverの両方で使用できます。 このファイルを使い、日常の管理業務を実行したり、数多くの設定をカスタマイズしたりできます。 編

集したWebInterface.confファイルを保存した時点で、変更が有効になります。WebInterface.confを使用してWeb Interfaceを構成する方法については、「構成ファイルを使用したサイトの構成」を参照してください。

- Citrix Online Plug-in構成ファイル： Citrix Online Plug-inの構成は、Web Interfaceサーバー上のConfig.xmlファイルで行います。

Java Application Server上でのサイトの作成

Java Application Serverで、Web Interfaceインストーラーを実行してサイトを作成します。インストーラーによりサイト用にカスタマイズされたWARファイルが作成され、（一般的には、サーブレットエンジンの適切な場所にWARファイルを置くことにより）それをインストールできます。 WARファイルから展開されたファイルの内容を編集して、サイトに変更を加えることができます。また、サイトを削除するには、WARファイルを削除します。

Citrix Web Interface管理コンソールでのサイトの構成

Citrix Web Interface管理コンソールはMicrosoft管理コンソール（MMC）3.0のスナップインで、これを使ってMicrosoftインターネットインフォメーションサービス（IIS）上にXenApp WebサイトおよびXenApp Servicesサイトを作成して構成できます。 コンソールの左側のペインには、Web Interfaceサイトの種類が表示されます。 中央の結果ペインには、左側のペインで選択されたサイト種類のコンテナー内で使用できるサイトが表示されます。

管理者は、Citrix Web Interface管理コンソールを使って日常的な管理作業をすばやく簡単に実行できます。 ［操作］ペインには、現在使用できるタスクが一覧で表示されます。 左側のペインで選択されたアイテムに関連するタスクは上に、結果ペインで選択されたアイテムに対して実行できる操作は下に表示されます。

管理者による構成は、Web Interface管理コンソールで変更を確定した時点で有効になります。 このため、その環境に適切でない値をCitrix Web Interface管理コンソールで指定するとその構成は適用されず、WebInterface.confの値がデフォルトにリセットされることがあります。 このような場合に備えて、定期的にWebInterface.confとConfig.xmlファイルのバックアップを作成してください。

Web Interface for Microsoft Internet Information Servicesをインストールすると、Citrix Web Interface管理コンソールが自動的にインストールされます。 ［スタート］をクリックし、［（すべての）プログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択してコンソールを起動します。

注： Web Interfaceをインストールするサーバー上には、Citrix Web Interface管理コンソールに必要なMMC 3.0がインストールされている必要があります。 MMC 3.0は、Web InterfaceのホストをサポートするすべてのWindowsプラットフォームでデフォルトで使用できます。

構成ファイルを使用したサイトの構成

次の構成ファイルを編集して、Web Interfaceのサイトを構成することができます。

- Web Interface構成ファイル： このWebInterface.confファイルでWeb Interfaceの設定の大半を変更できます。このファイルは、Microsoftインターネットインフォメーションサービス（IIS）とJava Application Serverの両方で使用できます。 このファイルを使い、日常の管理業務を実行したり、数多くの設定をカスタマイズしたりできます。 編集したWebInterface.confファイルを保存した時点で、変更が有効になります。 WebInterface.confを使用してWeb Interfaceを構成する方法については、「構成ファイルを使用したサイトの構成」を参照してください。

- Citrix Online Plug-in構成ファイル： Citrix Online Plug-inの構成は、Web Interfaceサーバー上のConfig.xmlファイルで行います。

共有構成

IIS上でホストされるサイトの場合、ネットワーク上で構成ファイルを共有する「マスター」サイトを設定して、ほかのWeb Interfaceサイトがマスターサイトの設定を取得するように構成できます。 適切なファイル権限を設定したら、ローカルサイトのbootstrap.confファイルにマスターサイト構成ファイル（WebInterface.conf）の絶対パスを指定して、ほかのサイトがマスターサイトの構成を共有するようにします。 共有構成を使用するXenApp Servicesサイトの場合、Web InterfaceはWebInterface.confに対して指定したのと同じディレクトリからCitrix Online Plug-in構成ファイル（config.xml）を読み取ろうとします。

共有ファイルから構成を取得するようにサイトを変更したら、そのサイトの構成を直接管理することはできなくなります。 その代わりにCitrix Web Interface管理コンソールを使うか、またはマスターサイトをホストするWebサーバー上の構成ファイルを直接変更して、マスターサイトの構成を変更する必要があります。 マスターサイトの構成に対する変更はすべて、マスターサイトの構成ファイルを共有するほかのサイトに適用されます。 共有構成は、Java Application Server上でホストされるサイトでは使用できません。

サイト構成を共有するには

1. 適切なファイル共有を設定して、マスターサイトのconfフォルダー（通常、C:¥inetpub¥wwwroot¥Citrix¥SiteName¥conf）およびサイト構成ファイルWebInterface.conf（通常、confフォルダー内にある）へのネットワークを介したアクセスを許可します。 XenApp Servicesマスターサイトの場合、Citrix Online Plug-in構成ファイルconfig.xml（通常、confフォルダー内にある）に対して同じ権限を設定する必要があります。

2. テキストエディターを使い、共有構成ファイルから構成を取得するサイトのbootstrap.confファイル（通常confフォルダー内にある）を開きます。

3. ConfigurationLocationパラメーターの設定を変更して、以下のようにマスターサイトの構成ファイルの絶対ネットワークパスを指定します。

   ConfigurationLocation=¥¥ServerName¥ShareName¥WebInterface.conf

Microsoftインターネットインフォメーションサービス（IIS）上にサイトを作成するには

Citrix Web Interface管理コンソールの［サイトの作成］タスクを使って、次のサイトのいずれか1つを作成します。

- XenApp Webサイト： Webブラウザーを使ってリソースにアクセスするユーザーのためのサイトです。
- XenApp Servicesサイト： Citrix Online Plug-inを使ってリソースにアクセスするユーザーのためのサイトです。

このタスクでは、サイトをホストするIISの場所、変更の適用先URL、およびサイトの認証設定を指定します。 これらのオプションは、あとで［サイトメンテナンス］タスクを使って更新できます。 サイトを作成する場合は、Web Interfaceを実行するサーバーにローカル管理者の権限でログオンする必要があります。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで［Web Interface］コンテナーをクリックします。
3. ［操作］ペインで、［サイトの作成］をクリックします。
4. 作成するサイトの種類を選択します。
5. サイトのURLおよび名前を指定します。
6. 画面に表示される指示に従って、サイトを作成します。

Microsoftインターネットインフォメーションサービス（IIS）のホスト

Citrix Web Interface管理コンソールで［サイトメンテナンス］の［IISホストの管理］タスクを使用して、IIS上のWeb Interfaceサイトの場所を変更します。

認証ポイントの指定

更新日： 2014-12-02

Citrix Web Interface管理コンソールを使ってXenApp Webサイトを作成する場合、環境内のユーザー認証を実行する認証ポイントを指定する必要があります。

Web Interfaceでの認証

指定ユーザー、パススルー、およびスマートカードなどのビルドイン認証方法を使用して、Web Interfaceによるユーザー認証を有効にできます。 Web Interfaceでの認証方法について詳しくは、「Web Interfaceの認証方法の構成」を参照してください。

Active Directoryフェデレーションサービスアカウントパートナーでの認証

Active Directoryフェデレーションサービス（AD FS）環境のアカウントパートナーを有効にして、XenAppアプリケーションにアクセスできます。 これにより、アカウントパートナーにもアプリケーションへのアクセスを許可できます。

AD FS統合サイトを作成する場合は、次の点に注意してください。

- XenDesktopはAD FS認証をサポートしません。
- AD FSはWeb Interface for Java Application Serversの使用をサポートしません。
- Client for Javaおよび埋め込みリモートデスクトップ接続（RDP）ソフトウェアはAD FS統合サイトへのアクセスをサポートしません。
- AD FS統合サイトではAD FSを使った認証のみをサポートします。 ほかの認証方法はサポートされていません。
- AD FS統合サイトを作成した後で、AD FSの代わりにビルトイン認証またはAccess Gatewayによる認証を使用するように構成できません。

詳しくは、「Web InterfaceにするActive Directoryフェデレーションサービスのサポートの構成」を参照してください。

Access Gatewayでの認証

指定ユーザーおよびスマートカード認証のため、Access Gatewayによるユーザーのアカウント情報の認証およびパススルーを有効にできます。 リソースへのユーザーアクセスは、ポリシーの使用を介して制御されます。

ユーザーがアカウント情報を使ってAccess Gatewayにログオンする場合、パススルー認証がデフォルトで有効になります。 Access Gatewayにログオンしたユーザーは、Web

Interfaceで再度認証を実行することなくリソースにアクセスできます。 セキュリティを強化するために、パススルー認証を無効にして、リソースセットが表示される前にユーザーにパスワードの入力を求めることができます。

ユーザーがスマートカードを使ってAccess Gatewayにログオンする場合、Web Interfaceで再度認証を実行する必要はありません。 ただしデフォルトでは、リソースにアクセスする際にPINの入力を求められます。 ユーザーがPINを指定することなくXenAppリソースにアクセスできるようサイトを構成できます。 この機能は、XenDesktopではサポートされていません。

Citrix Web Interface管理コンソールの［認証方法］タスクを使って設定をいつでも更新できます。

Kerberosを使ったサードパーティでの認証

サードパーティのフェデレーションまたはシングルサインオン製品を使ってユーザーを認証し、Active Directoryユーザーアカウントにユーザーの IDをマップできます。 これにより、Web InterfaceにKerberosを使用してシングルサインオンできます。 Kerberosについては、「Kerberosログオンを設定する」を参照してください。

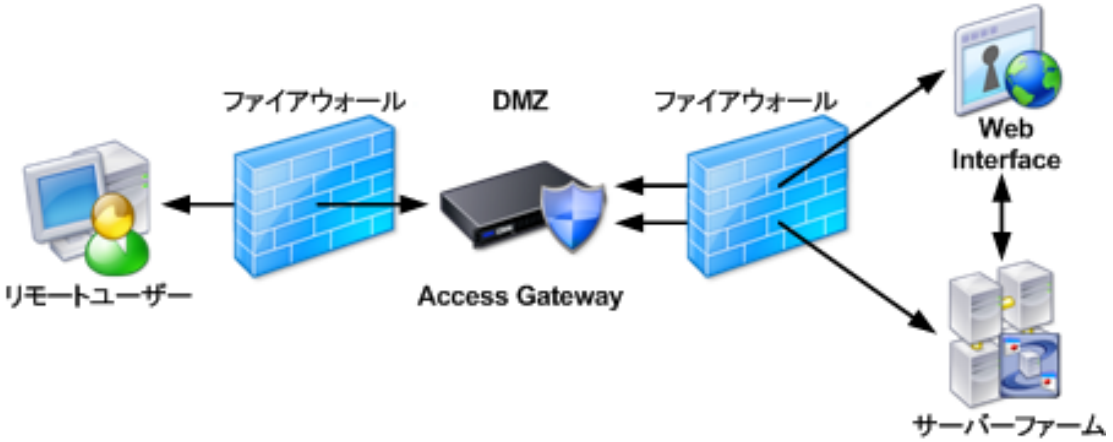
Webサーバーでの認証

Kerberosを使用するWebサーバーでのユーザー認証を有効にできます。 Kerberosについては、「Kerberosログオンを設定する」を参照してください。

Access GatewayとWeb Interfaceの展開

Access GatewayとWeb Interfaceを組み合わせて展開する場合、XenApp/XenDesktopおよびWeb Interfaceをすべて内部ネットワーク内のサーバーにインストールし、Access Gatewayアプライアンスを非武装地帯（DMZ）に置くことをお勧めします。

次の図は、Access GatewayとWeb Interfaceの組合せの推奨構成を示しています。



DMZは、保護された内部ネットワークとインターネット（または任意の外部ネットワーク）間にあるサブネットです。 Access GatewayをDMZに展開する場合、ユーザーはCitrix Secure Access Plug-inまたはCitrixのクライアントを使ってこれにアクセスします。 ユーザーのログオンはAccess Gatewayにより認証され、構成するアクセスポリシーに基づいてリソースが表示されます。

ユーザーに対するリソースの提供

Access Gatewayを使い、ユーザーは領域（Access Gateway Standard Editionの場合）、ログオンポイント（Access Gateway Advanced EditionおよびAccess Gateway 5.0の場合）、または仮想サーバー（Access Gateway Enterprise Editionの場合）にログオンして、リソースにアクセスします。 管理者はXenApp Webサイトにアクセスするための領域、ログオンポイント、または仮想サーバーを構成してユーザーがリソースを使用できるようにします。

Access Gatewayでは、Web Interfaceを使用して作成したXenApp Webサイトを、次のいずれかの方法で統合できます。

- 領域、ログオンポイント、または仮想サーバーのデフォルトのホームページとしてXenApp Webサイトを構成します。 この場合、ユーザーがログオンすると、XenApp Webサイトが表示されます。
- Access Interface内にXenApp Webサイトを埋め込みます。 この場合、Access Interfaceをデフォルトのホームページとして指定すると、共有ディレクトリや、アクセスセンター、Webアプリケーションと一緒にXenApp Webサイトが表示されます。 ア

クセスインターフェイスは、Access Gateway Advanced EditionおよびEnterpriseEditionで使用できます。

XenApp WebサイトとAccess Gatewayの統合

更新日： 2014-10-30

サイトをAccess Gatewayに統合するには、XenApp Webサイトを作成し、Access Gatewayのサイトに対してWebリソースを構成します。

Access Gateway統合サイトを作成するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで［Web Interface］コンテナーをクリックします。

3. ［操作］ペインで、［サイトの作成］をクリックします。

4. ［XenApp Web］をクリックして、［次へ］をクリックします。

5. ［IISの場所の指定］ページで、IISの場所、パス、およびサイト名を指定します。［次へ］をクリックします。

6. ［認証のポイントの指定］ページで、［Access Gateway］を選択し［次へ］をクリックします。

7. ［Access Gateway設定の指定］ページで、Access Gateway認証サービスのURLを［認証サービスURL］に入力します。

8. ユーザーによるAccess Gatewayへのログオン方法を指定して、［次へ］をクリックします。

   - ユーザーがユーザー名およびパスワードを使ってAccess Gatewayにログオンする場合は、［指定ユーザー］を選択します。 Access GatewayからWeb Interfaceへのユーザーのアカウント情報のパススルーを無効にしてセキュリティを強化するには、［アプリケーションやデスクトップを表示する前にユーザーにパスワードを求める］チェックボックスをオンにします。

   - ユーザーがスマートカードを使ってAccess Gatewayにログオンする場合は、［スマートカード］を選択します。 スマートカードオプションのパススルー認証を有効にする前に、ドメイン管理者としてログオンしていることを確認します。

   重要： XenApp Webサイトを統合したAccess Gatewayは、指定ユーザーまたはスマートカード認証のいずれか一方だけをサポートできます。 指定ユーザーとスマートカード認証の両方でAccess Gatewayにログオンするユーザーがいる場合、各認証方法に対して別々のサイトを作成して構成する必要があります。 次にユーザーが認証方法に合った適切なサイトに振り分けられるようAccess Gatewayを構成する必要があります。

9. 指定ユーザー認証のサイトを構成する場合は、手順10.に移動します。 スマートカード認証を構成する場合は、［スマートカード設定の指定］ページでユーザーがリソースにアクセスする前にPINの入力を求めるかどうかを指定します。

   - ユーザーがリソースにアクセスするたびにPINの入力を求める場合は、［ユーザーにPINの入力を求める］を選択します。 この機能を有効にするには、追加の構成が必要となります。 詳しくは、「スマートカードユーザーに対し、PINを指定してAccess Gatewayを介したリソースへのアクセスを有効にするには」を参照してください。

     注： PINを入力することなくリソースにアクセスするために、Access Gatewayへのログオンに使用するスマートカードを使ってデスクトップにログオンするWindows XPユーザーを有効にできます。 詳しくは、「スマートカードユーザーに対し、PINを指定してAccess Gatewayを介したリソースへのアクセスを有効に

するには」を参照してください。

- すべてのユーザーがPINを入力することなくXenAppリソースにアクセスできるようにするには、［スマートカードパススルーを有効にする］を選択します。 この機能はXenDesktopではサポートされず、Webサーバーがユーザーと同じドメインにある場合にのみ使用できます。 Access Gatewayサービスからのスマートカードパススルーを有効にするには、Webサーバーを再起動する必要があることがあります。 この機能を有効にするには、追加の構成が必要となります。 詳しくは、「スマートカードを使ってPINを指定することなくAccess Gatewayを介したリソースへのアクセスを有効にするには」を参照してください。

  注： デフォルトでは、Access Gatewayからのスマートカードパススルーがすべてのドメインユーザーに対して有効になっています。 これを有効にするユーザーを制限するには、PTSAccess.txtファイルに対するユーザー権限を変更します。このファイルは、通常C:¥Program Files (x86)¥Citrix¥DeliveryServices¥Protocol TransitionService¥ディレクトリにあります。

10. 新しいサイトの設定を確認し、［次へ］をクリックしてサイトを作成します。

Access Gatewayを介してサイトにアクセスするには

ここでは、Access Gatewayを介したサイトへのアクセス方法について概要を説明します。詳しくは、ここにアーカイブ化されているAccess Gatewayエディションのドキュメントを参照してください。

1. Access Gatewayと通信するようにXenAppまたはXenDesktopを構成します。
2. XenApp Webサイトにアクセスするように Access Gatewayを構成します。

   重要： domain.comではなく、domainの形式でドメインを指定します。 Access GatewayからのWeb Interfaceスマートカードパススルーはdomain.com形式のドメインでは認識されないため、この形式でドメインを指定するとユーザーはログオンできません。
3. ワークスペースコントロール（Access Gateway Advanced Editionのみ）およびセッションタイムアウト設定をAccess GatewayおよびWeb Interfaceの両方に対して正しく構成する必要があります。

スマートカードを使ってPINを指定することなくAccess Gatewayを介したリソースへのアクセスを有効にするには

PINを指定せずにすべてのユーザーがXenAppリソースへアクセスできるようにする場合、XenApp Webサイトをホストしている IISサイトでSSL（Secure Sockets Layer）を有効にする必要があります。 詳しくは、IIS 7.xおよびIIS 6.0に関するMicrosoftのドキュメントを参照してください。

SSLを有効にした後、Webサーバーがユーザーと同じドメイン内にあり、Active Directoryを構成して制約された委任を許可する必要があります。

ドメインを正しい機能レベルにするには

重要： ドメインの機能レベルを上げるには、ドメイン内のすべてのドメインコントローラーがWindows Server 2008またはWindows Server 2003を実行している必要があります。 また、Windows Server 2003を実行するドメインコントローラーがある場合、またはそれを追加する予定がある場合は、ドメインの機能レベルをWindows Server 2008レベルに上げないでください。 ドメイン機能レベルを上げた後、それを低いレベルに戻すことはできません。

1. ドメイン管理者としてドメインにログオンし、MMCでActive Directoryドメインと信頼関係スナップインを開きます。
2. 左側のペインで、ドメイン名を選択し、［操作］ペインの［プロパティ］を選択します。
3. ドメインの機能レベルが最上位のレベルでない場合は、ドメイン名を選択して［操作］ペインの［ドメインの機能レベルを上げる］を選択します。
4. ドメインの機能レベルを上げるには、適切なレベルをクリックして［上げる］をクリックします。

委任のためWeb InterfaceおよびCitrix XML Serviceを実行するサーバーを信頼するには

1. ドメイン管理者としてドメインにログオンし、MMCでActive Directoryユーザーとコンピュータースナップインを開きます。
2. ［表示］メニューで［詳細］を選択します。
3. 左側のペインで、［コンピューター］をクリックして、Webサーバーを選択します。
4. ［操作］ペインの［プロパティ］を選択します。
5. ［委任］タブで、［指定されたサービスへの委任でのみこのユーザーを信頼する］、［任意の認証プロトコルを使う］の順にクリックし、［追加］をクリックします。
6. ［サービスの追加］ダイアログボックスで、［ユーザーまたはコンピューター］をクリックします。
7. ［ユーザーまたはコンピューターの選択］ダイアログボックスの［選択するオブジェクト名を入力してください］ボックスに、Citrix XML Serviceを実行しているサーバーの名前を入力し、［OK］をクリックします。
8. 一覧からhttpサービスタイプを選択し、［OK］をクリックします。
9. ［委任］タブの［このアカウントが委任された資格情報を提示できるサービス］の一覧に、Citrix XML Serviceを実行するサーバー用に選択したhttpサービスタイプが表示されていることを確認し、［OK］をクリックします。
10. Web Interfaceの通信先として構成されているCitrix XML Serviceを実行しているサーバーごとに、手順3.～9.を繰り返します。
11. 左側のペインで［コンピューター］から、Web Interfaceが接続するように構成されるCitrix XML Serviceを実行するサーバーを選択します。
12. ［操作］ペインの［プロパティ］を選択します。
13. ［委任］タブで、［指定されたサービスへの委任でのみこのユーザーを信頼する］、［Kerberosのみを使う］の順にクリックし、［追加］をクリックします。
14. ［サービスの追加］ダイアログボックスで、［ユーザーまたはコンピューター］をクリックします。
15. ［ユーザーまたはコンピューターの選択］ダイアログボックスの［選択するオブジェクト名を入力してください］ボックスに、Citrix XML Serviceを実行しているサーバーの名前を入力し、［OK］をクリックします。
16. 一覧からHOSTサービスタイプを選択し、［OK］をクリックします。
17. ［委任］タブの［このアカウントが委任された資格情報を提示できるサービス］の一覧に、Citrix XML Serviceを実行するサーバー用に選択したHOSTサービスタイプが表示されていることを確認し、［OK］をクリックします。

18. Web Interfaceの通信先として構成されているCitrix XML Serviceを実行しているサーバーごとに、手順11.～17.を繰り返します。

19. セキュリティ上の理由から、サーバーファームのすべてのサーバーに、制約付き委任を構成する必要があります。 これらのサーバー上のリソースへのアクセスをユーザーに提供するには、Webサーバーに対するhttpサービスなどの関連のサービスを［このアカウントが委任された資格情報を提示できるサービス］の一覧に追加する必要があります。

    詳しくは、Citrix Knowledge CenterのCTX112972の「Presentation Serverでのサービスプリンシパル名（SPN）と委任」を参照してください。

サーバーファームからのアクセスを許可するリソースを決定するには

1. ドメイン管理者としてドメインにログオンし、MMCでActive Directoryユーザーとコンピュータースナップインを開きます。

2. 左側のペインで、［コンピューター］をクリックして、サーバーファームからサーバーを選択します。

3. ［操作］ペインの［プロパティ］を選択します。

4. ［委任］タブで、［指定されたサービスへの委任でのみこのユーザーを信頼する］、［Kerberosのみを使う］の順にクリックし、［追加］をクリックします。

5. ［サービスの追加］ダイアログボックスで、［ユーザーまたはコンピューター］をクリックします。

6. ［ユーザーまたはコンピューターの選択］ダイアログボックスの［選択するオブジェクト名を入力してください］ボックスにサーバーの名前を入力し、［OK］をクリックします。

7. 一覧からcifsおよびldapサービスタイプを選択し、［OK］をクリックします。

   注： ldapサービスが2つある場合は、使用するドメインコントローラーの完全修飾ドメイン名（FQDN）に一致する方を選択します。

8. ［委任］タブの［このアカウントが委任された資格情報を提示できるサービス］の一覧に、ドメインコントローラー用に選択したcifsおよびldapサービスタイプが表示されていることを確認し、［OK］をクリックします。

9. サーバーファームの各サーバーで、この処理を繰り返します。

リソースへのアクセス制限時間をドメインレベルで構成するには

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。

デフォルトでは、ユーザーはネットワーク上のリソースに15分間アクセスできます。 この制限時間を延長する場合は、Citrix XML Serviceを実行しているサーバーで次のレジストリエントリを変更します。

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Lsa¥Kerberos¥Parameters¥S4UTicketLifetime

このレジストリ値に、リソースのアクセス制限時間を分単位で指定します。ユーザーがセッションを開始してから、ここで指定した時間が経過するまでリソースへのアクセスが許可されます。

S4ULifetimeに指定できる最大値は、ドメインセキュリティポリシーによって制限されます。つまり、S4UTicketLifetimeの値が、ドメインレベルで指定した値よりも大きい場合、ドメインレベルの値が優先されます。

1. ドメイン管理者としてドメインにログオンし、MMCでドメインセキュリティポリシースナップインを開きます。
2. コンソールツリーで、［アカウントポリシー］>［Kerberosポリシー］の順に選択します。
3. 結果ペインで、［サービスチケットの最長有効期間］を選択します。
4. ［操作］ペインの［プロパティ］を選択します。
5. ［チケットの有効期間］に必要とされる時間を分単位で入力し、［OK］をクリックします。

リソースへのアクセス制限時間を構成しない場合は、サーバーファームからアクセスできるリソースを決定するときに、MMCのActive Directoryユーザーとコンピュータースナップインで［任意の認証プロトコルを使う］を選択します。 このオプションを選択すると、S4UTicketLifetimeに設定した値はすべて無視されます。 詳しくは、Microsoft社のWebサイト（http://support.microsoft.com/）を参照してください。

スマートカードユーザーに対し、PINを指定してAccess Gatewayを介したリソースへのアクセスを有効にするには

更新日： 2014-07-04

スマートカードユーザーがAccess Gatewayを介してリソースにアクセスするたびにPINを入力するように設定する場合、Citrix XML Service上でユーザーのセキュリティID（SID）の列挙を有効にする必要があります。

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。

1. ユーザーアカウントがサーバーファームを含むドメインとは異なるドメインにある場合、ドメインが2通りの信頼関係を共有する必要があります。

2. Citrix XML ServiceがIPアドレスを解決でき、ユーザーアカウントドメインのドメインコントローラーにアクセスできるかを検証します。 ドメインコントローラーと通信できない場合は、Citrix XML Serviceへの要求がタイムアウトになる可能性があります。

3. 各ドメインに対して、Citrix XML ServiceがActive DirectoryのTGGAU属性への読み取りアクセスを実行するWindowsアカウントを許可します。 TGGAU属性について詳しくは、Microsoft Knowledge Baseアーティクル331951を参照してください。 デフォルトでは、Network Serviceアカウントとして実行するようCitrix XML Serviceが構成されます。 このアカウントを次のビルトインActive Directoryグループに追加して、必要な許可を付与できます。

   - Pre-Windows 2000 Compatibility Access

   - Windows Authorization Access

4. Citrix XML Serviceを実行するサーバーで、システムレジストリのHKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Citrix¥XMLService¥に移動します。

5. ［XMLService］ノードに、EnableSIDEnumerationという名のDWORD値を追加し、値を1に設定します。

   注： XenDesktop 5移行の場合、レジストリキーは次のようになります。
   [HKEY_LOCAL_MACHINE¥SOFTWARE¥Citrix¥DesktopServer] "EnableXmlServiceSidEnumeration"=REG_DWORD:1

6. WebサーバーでIISを再開します。 Kerberosチケットのキャッシュ機関が期限切れとなるのを待たずに新しい権限を即座に適用する場合、Citrix XML Serviceを実行しているサーバーを再起動します。

7. Access Gatewayへのログオンに使用するのと同じスマートカードを使ってデスクトップにログオンするWindows XPユーザーの場合、スマートカードパススルー認証を構成して、PINを指定することなくリソースにアクセスできるように設定できます。

   a. Citrix Online Plug-inまたはCitrix Desktop Viewerを管理者アカウントを使ってユーザーのデバイスにインストールします。

   b. クライアントテンプレートをグループポリシーオブジェクトエディターに追加します。 詳しくは、「手順1：スマートカード認証を使用するプラグインのインストール」を参照してください。

   c. グループポリシーを使用して、すべてのCitrixのクライアントに対するパススルー認証を有効にします。 詳しくは、「手順1：スマートカード認証を使用するプラグインのインストール」を参照してください。

Web InterfaceとAccess Gatewayの設定の調整

XenAppおよびXenDesktopの特定の設定を、Web InterfaceとAccess Gatewayで構成できます。 ただしAccess Gatewayに統合されたXenApp Webサイトは、1つ以上の領域（Access Gateway Standard Editionの場合）、ログオンポイント（Access Gateway Advanced Editionの場合）、仮想サーバー（Access Gateway Enterprise Editionの場合）により参照できるため、ある1つの範囲、ログオンポイント、または仮想サーバーでデフォルトのホームページとしてサイトを表示しつつ、別の範囲、ログオンポイント、または仮想サーバーを1つAccess Interface内のXenApp Webサイトに埋め込むことができます。 これにより、一部のリソースの設定で競合が生じることがあります。

設定した機能を問題なく実行するには、次の作業を実行します。

- セッションのタイムアウト： すべての範囲、ログオンポイント、仮想サーバーがXenApp Webサイトと同じ設定を使用するようにします。
- ワークスペースコントロール。 Access Gateway Advanced Editionの場合、XenApp Webサイトをホームページとするすべてのログオンポイントに対して、Access Gatewayのワークスペースコントロールのすべての設定を無効にします。 これにより、Web Interface内で構成した設定が使用されます。 これ以外のログオンポイントでは、必要に応じてワークスペースコントロールを構成できます。

サイトの初期構成設定の指定

サイトの作成ウィザードでサイトを作成した後に、最後のページで［すぐにこのサイトを構成する］チェックボックスをオンにすると、そのサイトの初期構成設定を指定できます。 初期構成の指定ウィザードを使って、1つ以上のサーバーファーム間の通信を構成し、ユーザーが使用できるリソースの種類を指定します。

サーバーファームの指定

新しいサイトを構成する場合、サイトのユーザーに対してリソースを提供するサーバーファームの詳細を入力する必要があります。

Citrix Web Interface管理コンソールの［サーバーファーム］タスクを使って設定をいつでも更新できます。 サーバーファームとの通信方法を構成する方法については、「サーバーとサーバーファームの管理」を参照してください。

重要： XenApp 4.0 with Feature Pack 1 for UNIXとの互換性を維持する場合は、追加のサイト構成が必要となります。 詳しくは、「XenApp 4.0 with Feature Pack 1 for UNIXのサポートを構成するには」を参照してください。

認証方法の指定

認証ポイントとして［Web Interface］を選択した新しいXenApp Webサイトを構成する場合、ユーザーがWeb Interfaceにログオンする場合にどのようにユーザーを認証するかを指定できます。

Citrix Web Interface管理コンソールの［認証方法］タスクを使って設定をいつでも更新できます。 認証の構成について詳しくは、「Web Interfaceの認証方法の構成」を参照してください。

ドメイン制限の指定

Web Interface認証ポイントで作成された新しいXenApp Webサイトを構成する場合、ユーザーアクセスを特定のドメインに制限できます。

Citrix Web Interface管理コンソールの［認証方法］タスクを使って設定をいつでも更新できます。 ドメイン制限の構成について詳しくは、「ドメインの制限を構成するには」を参照してください。

ログオン画面の外観の指定

新しいXenApp Webサイトを構成するときに、ユーザーの［ログオン］画面の外観を指定できます。 ログオンフィールドのみを表示する最小限のレイアウトや、ナビゲーションバーを含むレイアウトを選択します。

Citrix Web Interface管理コンソールの［Webサイトの外観］タスクを使ってこの設定をいつでも更新できます。 ユーザーインターフェイスの外観のカスタマイズについて詳しくは、「ユーザーページの外観のカスタマイズ」を参照してください。

ユーザーが使用できるリソースの種類の指定

新しいサイトを構成するときに、ユーザーに提供するリソースの種類を指定する必要があります。 Web Interfaceは、ユーザーがWebブラウザーまたはCitrix Online Plug-inを使ってリソース（アプリケーション、コンテンツ、およびデスクトップ）にアクセスできるようにするためのプログラムです。 オフラインアプリケーションの機能と一緒に使用すると、アプリケーションがユーザーのコンピューターにストリーム配信されるため、ユーザーはそのアプリケーションをローカルで実行できるようになります。

ユーザーに提供するリソースの種類として、次のものがあります。

- オンライン： ユーザーは、リモートサーバーでホストされるアプリケーション、コンテンツ、およびデスクトップにアクセスします。 ユーザーは、リソースにアクセスするためにネットワーク接続が必要です。

- オフライン： ユーザーは、デスクトップにアプリケーションをストリーム配信し、ローカルで開きます。 XenApp Servicesサイトの場合、いったんアプリケーションを配信したら、ユーザーはネットワークに接続せずにいつでもそのアプリケーションを実行できます。 XenApp Web サイトの場合、ユーザーはサイトにログオンしてアプリケーションを起動するためにネットワーク接続が必要です。 いったんアプリケーションを実行したら、接続を維持する必要はありません。

- デュアルモード： ユーザーは同じサイト上のすべてのオフラインアプリケーションとオンラインアプリケーション、コンテンツ、デスクトップの両方にアクセスします。 オフラインアプリケーションを実行できない場合に、オンラインアプリケーション、コンテンツ、およびデスクトップを配信します。

Citrix Web Interface管理コンソールの［リソースの種類］タスクを使って設定をいつでも更新できます。 Citrixのクライアントの種類については、「クライアントの管理」を参照してください。

既存のサイトのアップグレード

Web Interface 4.5またはそれ以降のバージョンからアップグレードする場合、既存のサイト（Conferencing Managerゲスト出席者サイトを除く）がサポートされます。

重要： Conferencing Managerゲスト出席者サイトはサポートされません。 以前のバージョンからアップグレードする場合は、サーバー上の既存のConferencing Managerゲスト出席者サイトがインストーラーにより削除されます。

既存のAccess Platform/XenApp WebサイトおよびProgram Neighborhoodエージェントサービス/XenApp Servicesサイトは次のように処理されます。

- ローカル構成サイト： Web Interfaceのインストール時に、すべてのローカル構成サイトが自動的に最新バージョンにアップグレードされます。
- 集中管理構成およびグループサイト： Web Interfaceのインストール時に、すべての既存の集中管理構成サイトまたはグループサイトがローカル構成を使用するように自動的に変換されます。 次に、変換されたサイトは最新のバージョンにアップグレードされます。

デフォルトでは、クライアントインストールファイルのファイル名はXenAppまたはXenDesktopのインストールメディアで提供されているファイル名と同じであると仮定しています。 クライアントのインストールファイルをCitrixのWebサイトからダウンロード、または古いバージョンのクライアントソフトウェアを展開する場合は、XenApp Webサイトの構成ファイルでClientIcaLinuxX86、ClientIcaMac、ClientIcaSolarisSparc、ClientIcaSolarisX86、ClientIcaWin32、およびClientStreamingWin32パラメーターに対して適切なクライアントインストールファイル名が指定されているかチェックします。 Web Interface構成ファイルのパラメーターについては、「WebInterface.confのパラメーター」を参照してください。

サイトタスクの使用

サイトを構成するには、Citrix Web Interface管理コンソールの左側のペインでサイトの種類を選択し、結果ペインでサイトをクリックして［操作］ペインまたは［操作］メニューで使用可能なタスクを選択します。 または、結果ペインでサイト名をマウスの右ボタンでクリックし、表示されるメニューからタスクを選択します。

特定の種類のサイト専用のタスクや、特定の構成でのみ表示されるタスクもあります。 次の表に、どの種類のサイトでどのタスクを実行できるかを示します。

フ	XenApp Webサイト		XenApp Servicesサイト	
	オンライン/デュアルモード	オフラインのみ	オンライン/デュアルモード	オフラインのみ
entication Method	*	*		
方法	*	*	*	*
イアント側のプロキシ	*		*	
イアントの展開	*	*		
ース更新			*	*
ースの種類	*	*	*	*
ュアなアクセス	*		*	
バーファーム	*	*	*	*
バーの設定			*	*
ションオプション			*	
ション基本設定	*	*		
ートカット			*	*
トメンテナンス	*	*	*	*
サイトの外観	*	*		
クスペースコントロール	*			

サイトの修復とアンインストール

Citrix Web Interface管理コンソールの［サイトメンテナンス］の［サイトの修復］および［サイトのアンインストール］タスクを使ってサイトをここに修復および削除できます。 サイトを完全にアンインストールすると、Web Interfaceのシステムからそのサイトが削除され、それ以降そのサイトではタスクを実行できなくなります。

重要： ［サイトの修復］タスクを実行すると、そのサイトでそれまでに作成したカスタムスクリプトやカスタムイメージは削除されます。 また、［IISホストの管理］タスクを実行したときも、カスタマイズしたファイルが削除されます。 これらのタスクは、作成したファイルをバックアップしてから実行することをお勧めします。

ユーザーがWeb Interfaceを使用できるようにする

Web Interfaceをインストールして構成したら、Web Interfaceの［ログオン］画面のURLをユーザーに知らせます。 ユーザーが［ログオン］画面をWebブラウザーにブックマーク登録する場合は、http://ServerName/SitePathというURLを使用することをお勧めします（login.aspxなどの特定のページは指定しないようにします）。

Java Application Serverでは、サイトのパス（URLのホスト名とポート番号の後の部分）はサーブレットエンジンによって決められます。 サーブレットエンジン内でWARファイルをインストールするときに、このパスを変更することができます。 デフォルトは、/WARFileNameです。ここで、WARFileNameはサイトのWARのファイル名の最初の部分です。

サイトへの直接アクセス

XenApp WebサイトにCitrixセキュアアクセスプラグインを使ってAccess Gateway Enterprise Editionを介してアクセスする場合、リソースURLのサポートを有効にできます。 これにより、ユーザーはWeb Interface使ってアクセスするリソースへの固定リンクを作成できます。

注： Access Gateway Standard EditionまたはAdvanced Editionを介してアクセスするユーザー、またはAccess Gateway Enterprise Editionを介するクライアントレスアクセスを使用するユーザーに対しては、リソースURLはサポートされません。

ユーザーは、ショートカットの一覧やデスクトップに固定リンクを追加できます。 Citrix Web Interface 管理コンソールを使ってリソースURLのサポートを有効にするには、左側のペインで［XenApp Webサイト］をクリックし、結果ペインでサイトを選択してから［操作］ペインで［セッション基本設定］をクリックして［固定URL］を選択し、［ブラウザーのブックマーク機能を使ったリソースへのアクセスを許可する］チェックボックスをオンにします。

重要： この機能を有効にすると、サイト間の偽装要求（クロスサイトリクエストフォージェリ）から保護する機能が無効になります。

Web Interfaceの［ログオン］画面をMicrosoftインターネットインフォメーションサービス（IIS）のデフォルトのWebページに設定する

Web Interfaceの［ログオン］画面が、そのWebサーバーのデフォルトページになるように、［ログオン］画面のURLをhttp://ServerName/として設定できます。 これを行なうには、サイトの作成時に［IISサイトのデフォルトのページとして設定する］チェックボックスをオンにします。または、サイトの作成後にCitrix Web Interface管理コンソールの［サイトメンテナンス］の［IISホストの管理］タスクを使用します。

サーバーとサーバーファームの管理

更新日： 2014-11-24

ここでは、サーバーファームと正しく通信できるようにWeb Interfaceを構成する方法について説明します。 また、サーバーを構成して管理する方法と、Citrix XML Serviceを実行しているサーバー間の負荷分散を有効にする方法についても説明します。

パスワードの変更に関する考慮事項

複数のサーバーファーム間で設定やバージョンに違いがあると、ユーザーがパスワードを変更できなくなることがあります。 次に例を示します。

- ドメインのポリシーによってパスワードの変更が禁止されることがあります。
- 1つのサイトでXenApp for UNIX（日本語版はリリースされていません）が動作するサーバーファームと、XenApp for WindowsおよびXenDesktopの両方またはその一方が動作するサーバーファームを使用している場合は、Windowsのパスワードしか変更できません。

このような環境では、ユーザーによるパスワードの変更を許可しないことをお勧めします。

複数のサーバーファームを統合する場合、サイト構成ファイル内に一覧表示されている最初のサーバーファームでPresentation Server 4.5以降、またはXenDesktopのいずれかを実行している必要があります。

サーバーファームを混在モードで運用している場合は、必要に応じてパスワードの変更を有効にできます。 Web Interfaceは、サーバーファームの定義順に各サーバーファームと通信を行い、パスワードが変更されたサーバーファームを検出すると通信を停止します。 これで、どのサーバーファームにパスワードの変更要求を送信すればいいかがわかります。 パスワードの変更が正常に行われなかった場合は、次のサーバーファームにパスワードの変更要求が送信されます。 サーバーファーム間でパスワードを複製するときに、すべてのユーザーのパスワードの一貫性が損なわれないように注意してください。

サーバーファームを追加するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで［サーバーファーム］をクリックします。

4. ［Add］をクリックします。

5. ［ファーム名］ボックスに、サーバーファームの名前を入力します。

6. ［サーバー設定］の一覧の［追加］をクリックして、追加するサーバーの名前を指定します。 サーバー名を変更するには、一覧からサーバー名を選択し、［編集］をクリックします。 サーバー名を削除するには、サーバー名を選択し、［削除］をクリックします。

7. 複数のサーバー名を一覧に追加した場合は、サーバーの優先順位を設定できます。これを行うには、［サーバー］の一覧でサーバー名を選択し、［上に移動］または［下に移動］をクリックして適切なフェールオーバー順に並べ替えます。

重要： XenApp 4.0 with Feature Pack 1 for UNIXとの互換性を維持する場合は、追加のサイト構成が必要となります。 詳しくは、「XenApp 4.0 with Feature Pack 1 for UNIXのサポートを構成するには」を参照してください。

フォールトトレランスを構成するには

Web Interfaceでは、Citrix XML Serviceを実行している複数のサーバー間でのフォールトトレランスを設定できます。 Citrix Web Interface管理コンソールの［サーバーファーム］タスクを使って、フォールトトレランスを構成します。 サーバーとの通信中にエラーが発生した場合、［接続できないサーバーを無視する期間］ボックスに指定した時間が経過するまでWeb Interfaceはそのサーバーにアクセスせず、［サーバー］の一覧に追加されているほかのサーバーとの通信を継続します。

デフォルトでは、障害が発生したサーバーは1時間無視されます。 一覧内のどのサーバーも応答しない場合は、Web Interfaceは各サーバーへの通信を10秒ごとに再試行します。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで［サーバーファーム］をクリックします。

4. ［追加］をクリックしてサーバーファームを追加するか、既存のサーバーファームを選択し、［編集］をクリックします。

5. ［サーバー］の一覧で、サーバーを適切な優先順位に並べ替えます。 サーバーを並べ替えるには、サーバー名を選択してから、［上に移動］または［下に移動］をクリックします。

6. 障害が発生したサーバーを無視する時間を変更するには、［接続できないサーバーを無視する期間］に時間を指定します。

サーバー間の負荷分散を有効にするには

更新日： 2014-11-25

Citrix XML Serviceを実行しているサーバー間で負荷が分散されるように設定できます。 負荷分散を有効にすると、サーバー間の接続負荷が均等に分散されるため、サーバーが負荷限界状態になることを防ぐことができます。 デフォルトでは、負荷分散は無効になっています。

あるサーバーと通信しているときにエラーが発生した場合、それ以降のすべての通信は残りのサーバーで負荷分散されます。 障害が発生したサーバーは、指定した時間（デフォルトでは1時間）無視されますが、Citrix Web Interface管理コンソールの［サーバーファーム］タスクを使ってこれを変更できます。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで［サーバーファーム］をクリックします。

4. ［追加］をクリックしてサーバーファームを追加するか、既存のサーバーファームを選択し、［編集］をクリックします。

5. ［サーバー］の一覧に、負荷を分散させるサーバーを追加します。

6. ［負荷分散にサーバーの一覧を使用する］チェックボックスをオンにします。

7. 障害が発生したサーバーを無視する時間を変更するには、［接続できないサーバーを無視する期間］に時間を指定します。

サーバーファーム内のすべてのサーバー設定の構成

Citrix Web Interface管理コンソールの［サーバーファーム］タスクを実行して、XenAppまたはXenDesktopのサーバーとWeb Interface間をCitrix XML Serviceがどのようにデータを転送するかを指定できます。 Citrix XML Serviceは、サーバーファームとWeb Interfaceサーバーの中継点として機能するXenAppおよびXenDesktopのコンポーネントです。 デフォルトでは、このポート番号はサイト作成時に指定した値になっています。 このポート番号は、Citrix XML Serviceで使用されるポートと同じである必要があります。

また、サーバーで生成されるチケットの有効時間も指定できます。 チケットを使用すると、Webサーバーからユーザーのデバイスに送られるICAファイルにユーザーのアカウント情報が含まれないようになり、指定ユーザーによるログオンのセキュリティが向上します。

Web Interfaceの各チケットには、有効時間（デフォルトで200秒）が設定されています。この有効時間が短すぎるためにサーバーファームにアクセスするユーザーを認証できない場合は、ネットワークのパフォーマンスに応じてこの値を調整します。 Citrix XML Serviceを実行しているサーバーのIPアドレスやアドレスを変更した場合は、そのサーバーを再起動するまでチケット機能が無効になります。 サーバーのIPアドレスやアドレスを変更した場合は、必ずサーバーを再起動してください。

すべてのサーバーに対する設定を指定するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで［サーバーファーム］をクリックします。

4. ［追加］をクリックしてサーバーファームを追加するか、既存のサーバーファームを選択し、［編集］をクリックします。

5. ［通信設定］の［XML Serviceポート］ボックスに、ポート番号を入力します。 このポート番号は、Citrix XML Serviceで使用されるポートと同じである必要があります。

6. ［トランスポートタイプ］の一覧から、次のいずれかのオプションを選択します。

   - HTTP。 標準のHTTP接続を介してデータを送信します。 サーバー間でほかのセキュリティ対策を設定している場合は、このプロトコルを使用します。

   - HTTPS。 SSL（Secure Sockets Layer）またはTLS（Transport Layer Security）を使って、セキュリティレベルの高いHTTP接続を介してデータを送信します。 Citrix XML Serviceがインターネットインフォメーションサービス（IIS）とポートを共有し、IISがHTTPSをサポートするように構成する必要があります。

   - SSL Relay。 ホスト認証やデータの暗号化を行うSSL Relayを実行しているサーバー（XenAppまたはXenDesktopが動作するサーバー）を介してセキュリティレベルの高いデータを送信します。

7. ［SSL Relay］を選択した場合は、［SSL Relayポート］ボックスにSSL RelayのTCPポートを指定します（デフォルトのポートは443）。 Web Interfaceでは、SSL Relayを実行するサーバーを認証するときに、ルート証明書を使用します。 SSL Relayを実行しているすべてのサーバーのリスナーポートが同じポートになっていることを確認してください。

   注： ［SSL Relay］または［HTTPS］を使用する場合は、指定する名前はXenAppまたはXenDesktopが動作するサーバーの証明書で使用されているサーバー名と（大文字小文字に区別も含めて）同じである必要があります。

8. チケット機能を構成するには、［チケット設定］をクリックします。

9. ［ICAチケット有効期間］ボックスに、オンラインリソースのCitrix のクライアントのチケットの有効期間を入力します。

10. ［Streamingチケット有効期間］ボックスに、Citrix Online Plug-inのチケットの有効期間を入力します。

サーバーの詳細設定の指定

更新日： 2014-12-02

［サーバーファームの詳細設定］ダイアログボックスを使って、ソケットプールやコンテンツのリダイレクト機能を有効にしたり、Citrix XML Serviceのタイムアウトおよびcitrix XML Serviceとの通信試行回数（通信エラーとみなす基準）を指定したりできます。

ソケットプール機能を有効にするには

ソケットプール機能を有効にすると、Web Interfaceは、ソケットを必要に応じて作成して接続が閉じたときにそれをオペレーティングシステムに戻す代わりに、ソケットのプールを保持します。 この機能を有効にすると、特にSSL接続でパフォーマンスが向上します。

ソケットプールは、認証ポイントが［Web Interface］または［Access Gateway］で作成されたサイトでのみ使用でき、デフォルトで有効です。 XenApp for UNIXが動作するサーバーを使用するようにWeb Interfaceを構成している場合は、ソケットプール機能を使用する必要はありません。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。
3. ［操作］ペインで［サーバーファーム］をクリックします。
4. ［Advanced］をクリックします。
5. ［ソケットプール］の［ソケットプールを有効にする］チェックボックスをオンにします。

コンテンツのリダイレクトを有効にするには

Citrix Web Interface管理コンソールの［サーバーファーム］タスクを使って個々のXenApp Servicesサイトに対するプラグインからサーバーへのコンテンツリダイレクト機能を有効および無効にできます。 この設定は、XenAppに構成するコンテンツリダイレクト設定よりも優先されます。

プラグインからサーバーへのコンテンツリダイレクト機能を有効にすると、Citrix Online Plug-inユーザーがオンラインコンテンツやローカルファイルを開くときに、サーバー上のアプリケーションが使用されるようになります。 たとえば、Citrix Online Plug-inのユーザーがローカルデバイス上の電子メールプログラムで電子メールの添付ファイルを受信し、その添付ファイルをオンラインアプリケーションで開きます。 コンテンツリダイレクト機能を無効にすると、ユーザーはオンライコンテンツやローカルファイルをローカルデバイス上のアプリケーションで開きます。

XenApp Servicesサイトでは、デフォルトでプラグインからサーバーへのコンテンツリダイレクト機能が有効になっています。

ファイルタイプをアプリケーションに関連付けて、プラグインからサーバーへのコンテンツリダイレクト機能を構成できます。 ファイルタイプの関連付けについては、「ファイルタイプに公開アプリケーションを関連付けるには」を参照してください。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Servicesサイト］をクリックして結果ペインでサイトを選択します。
3. ［操作］ペインで［サーバーファーム］をクリックします。
4. ［Advanced］をクリックします。
5. ［コンテンツのリダイレクト］の［コンテンツのリダイレクトを有効にする］チェックボックスをオンにします。

Citrix XML Service通信を構成するには

デフォルトでは、Citrix XML Serviceとの通信は1分でタイムアウトし、2回の通信試行に失敗した場合に障害が発生しているとみなされます。 Citrix Web Interface管理コンソールの［サーバーファーム］ タスクを使ってデフォルト設定を変更できます。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。
3. ［操作］ペインで［サーバーファーム］をクリックします。
4. ［Advanced］をクリックします。
5. Citrix XML Serviceのタイムアウトを構成するには、［ソケットタイムアウト］ボックスに適切な値と単位を指定します。
6. ［XML Serviceへのアクセスを試みる回数］には、Citrix XML Serviceとの通信試行回数を入力します。ここで指定した回数XML Serviceにアクセスしても通信が確立されない場合は、そのCitrix XML Serviceで障害が発生しているとみなされ、無視されます。

サーバー設定の管理

Citrix Web Interface管理コンソールの［サーバー設定］タスクを使って、Citrix Online Plug-inがどのようにサイトと通信するか、またイベントの障害時にユーザーが代替サイトにリダイレクトされるかどうかを構成します。

サーバーの通信方法を構成するには

サーバーの通信方法には、次のオプションがあります。

- 通信にSSL/TLSを使用する： デフォルトでは、スマートカードを使ったログオンと、プラグインとWeb Interfaceサーバー間の通信でSSL/TLSを使用するオプションは無効になっています。 ここでSSL/TLS通信を有効にすると、サイトのURLで自動的にHTTPSプロトコルが使用されます。 また、このオプションを有効にする場合は、XenAppまたはXenDesktopが動作するサーバーでもSSLを有効にする必要があります。

- ユーザーにサーバーURLのカスタマイズを許可する： サーバーのURLには、Citrix Online Plug-inによって参照される構成ファイルのパスが設定されています。 デフォルトのパスは、Citrix Online Plug-inのインストール時に指定したサーバーのアドレスに基づいて決定されます。 このオプションを有効にすると、ユーザーがCitrix Online Plug-inの［オプション］ダイアログボックスの［サーバーオプション］ページで［サーバーのURL］ボックスを編集できるようになります。

- 次の時間ごとに自動更新する： プラグインの構成の更新頻度を定義できます。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Servicesサイト］をクリックして結果ペインでサイトを選択します。

3. ［操作］ペインで［サーバー設定］をクリックします。

4. Citrix Online Plug-inとサイト間の通信を保護するには、［プラグインとこのサイト間の通信にSSL/TLSを使用する］チェックボックスをオンにします。

5. Citrix Online Plug-inによって参照される構成ファイルのURLをユーザーが変更できるようにするには、［ユーザーによるカスタマイズを許可する］チェックボックスをオンにします。

6. Citrix Online Plug-inが設定を更新する間隔を構成するには、［次の時間ごとに自動更新する］チェックボックスをオンにして、その間隔を時間、日、週、または年で指定します。

Citrix Online Plug-inバックアップURLを指定するには

Web Interfaceのプライマリサーバーが使用できなくなったときにCitrix Online Plug-inがアクセスするバックアップサーバーを指定できます。 Citrix Web Interface管理コンソールの［サーバー設定］タスクを使ってバックアップサーバーのURLを指定します。 Web Interfaceサーバーで障害が発生すると、Online Plug-inは［バックアップサイトパス］の一覧の先頭のバックアップサーバーに自動的に接続されます。 このサーバーでも障害が発生した場合は、一覧の2番目のサーバーとの接続が試みられます。

重要： バックアップURLには、プライマリサイトと同じ種類WebサーバーでホストされるサイトへのURLを指定する必要があります。 たとえば、プライマリサイトがWeb Interface for Microsoft Internet Information Servicesサイトの場合、指定したバックアップサイトもWeb Interface for Microsoft Internet Information Servicesサイトである必要があります。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Servicesサイト］をクリックして結果ペインでサイトを選択します。
3. ［操作］ペインで［サーバー設定］をクリックします。
4. ［バックアップ］をクリックします。
5. ［Add］をクリックします。
6. ［バックアップURL］ボックスに、接続先のサイトのURLを入力します。 1つのサイトにつき最大5つのバックアップURLを指定できます。
7. ［OK］をクリックします。
8. 複数のバックアップURLを指定する場合は、［バックアップURL］の一覧からURLを選択し、［上に移動］または［下に移動］をクリックして適切なフェールオーバー順にURLを並べます。

サイトのリダイレクトを構成するには

ユーザーのアクセスを別のサイトにリダイレクトするように指定するには、リダイレクト設定を使用します。 たとえば、人事部用の新しいサイトを作成した場合に、以前のサイトへのユーザーアクセスが、自動的に新しいサイトにリダイレクトされるように設定できます。これにより、ユーザーが自分で新しいサイトのURLを入力する必要がなくなります。 Citrix Web Interface管理コンソールの［サーバー設定］タスクを使って新しいサイトの詳細を指定します。 ユーザーのアクセスを直ちにリダイレクトするのか、次にCitrix Online Plug-inを起動したときにリダイレクトするのかを指定できます。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Servicesサイト］をクリックして結果ペインでサイトを選択します。

3. ［操作］ペインで［サーバー設定］をクリックします。

4. ［リダイレクト］をクリックします。

5. 次のいずれかを選択します。

   - サイトのリダイレクトを構成しない場合は、［リダイレクトしない］を選択します。

   - ユーザーをほかのサイトにすぐにリダイレクトする場合は、［Citrix Online Plug-in 構成を更新した時にリダイレクトする］を選択します。

   - ユーザーが次回プラグインを起動したときにほかのサイトにリダイレクトする場合は、［Citrix Online Plug-inを次に起動した時にリダイレクトする］を選択します。

6. ［リダイレクトURL］ボックスに、代替サイトのURLを入力します。

Web Interfaceの認証方法の構成

更新日： 2014-11-25

認証方法

ユーザーがリソース（アプリケーション、コンテンツ、およびデスクトップ）にアクセスすると、認証が行われます。 ユーザーが正しく認証されると、リソースセットが表示されます。

Web Interfaceでは、次の認証方法を構成できます。

- （XenApp WebサイトおよびXenApp Servicesサイトともに）指定ユーザーによる認証 ： ユーザーはユーザー名とパスワードを入力してログオンします。 UPN（ユーザープリンシパル名）、Microsoftのドメインベースの認証、およびNDS（Novell Directory Service）を使用できます。 XenApp Webサイトの場合、RSA SecurIDおよびSafeWord認証も使用できます。

  注： Web Interface for Java Application ServersではNovell認証は実行できず、またはXenApp 6.0、XenApp 5.0 for Windows Server 2008、またはXenDesktopでサポートされていません。 ただし、XenApp 6.0はNovell Domain Services for Windowsと互換性があります。

- パススルー認証： ユーザーは、物理的なWindowsコンピューターにログオンしたときに入力したアカウント情報によって認証されます。 つまり、Web Interfaceへのログオン時にアカウント情報を入力しなくても、自動的にリソースセットが表示されます。 また、Kerberos統合Windows認証を使ってサーバーファームに接続できます。 Kerberos認証を使用するように指定した場合は、Kerberos認証に失敗するとパススルー認証にも失敗し、ユーザーはログオンできません。 Kerberosについては、「Kerberosログオンを設定する」を参照してください。

- スマートカードパススルー認証： ユーザーは、ユーザーデバイスに接続されたスマートカードリーダーにスマートカードを挿入することによって認証されます。 Citrix Online Plug-inをインストールしている場合、ユーザーデバイスへのログオン時にスマートカードのPINの入力が求められます。 ログオン後、ユーザーはリソースに再度ログオンを求められることなくアクセスできます。 XenApp Webサイトにアクセスする場合は、PINの入力画面は表示されません。 XenApp Servicesサイトを構成している場合、サーバーファームへの認証にスマートカードを使い、Kerberos統合Windows認証を使ってWeb Interfaceに接続できます。 Kerberos認証を使用するように指定した場合は、Kerberos認証に失敗するとパススルー認証にも失敗し、ユーザーはログオンできません。

  注： Windows Vistaの向上したセキュリティ機能により、Wndows VistaまたはWindows 7を実行するスマートカードユーザーは、スマートカードパススルー認証が有効になっている場合でもアプリケーションへのアクセス時にはPINの入力が必要になります。

- スマートカード： ユーザーは、スマートカードを使ってWeb Interfaceにログオンできます。 この認証方法では、スマートカードのPINを入力する必要があります。

  注： パススルー認証、スマートカードパススルー認証、およびスマートカード認証は、Web Interface for Java Application Serversでは使用できません。

- 匿名ユーザーとしてログオン： 匿名ユーザーは、ユーザー名とパスワードを入力せずにログオンして、匿名ユーザー用に公開されているリソースにアクセスできます。

  重要： 匿名ユーザーとしてログオンできるようにすると、Web Interfaceで認証されなくても、ユーザーがSecure Gatewayチケットを入手できるようになります。Secure Gatewayは、認証ユーザーに対するチケットの発行に関してのみWeb Interfaceに依存するため、匿名ユーザーを設定するとSecure Gatewayのセキュリティ機能のメリットの一部が損なわれます。

  注： XenDesktopは匿名ユーザーをサポートしていません。

認証に関する推奨事項

パススルー、スマートカードパススルー、またはスマートカード認証を有効にする場合は、次の点に注意してください。

- ユーザーがユーザーデバイスにスマ―トカードを使ってログオンし、パススルー認証を有効にする場合、Kerberos認証を使用するオプションを選択します。

- ユーザーがユーザーデバイスに指定ユーザーとしてログオンする場合は、これらのユーザーのWeb Interfaceへのアクセスに対してスマートカードまたはスマートカードパススルー認証を有効にしないでください。

  注： 指定ユーザー認証を使ってWindowsにログオンしたユーザーが、次にスマートカードパススルー認証が構成されたサイトにアクセスすると、リソースへのアクセス時に［Windowsへようこそ］ダイアログボックスが開きます。 このダイアログボックスを閉じるには、Ctrl+F1キーを押す必要があります。 スマートカード認証および指定ユーザー認証を使用するユーザー用に別のサイトを作成することをお勧めします。

Web Interfaceの認証方法を変更すると、既にWeb Interfaceにログオンしているユーザーの画面にエラーメッセージが表示される場合があります。 これらのユーザーがWebブラウザーを使ってWeb Interfaceにアクセスしている場合、再度ログオンする前にWebブラウザーをいったん閉じてから再度開く必要があります。

認証の構成

Citrix Web Interface管理コンソールの［認証方法］タスクでは、XenApp、XenDesktop、およびCitrix Online Plug-inにアクセスするユーザーの認証方法を構成します。

ドメインの制限を構成するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで［認証方法］をクリックし、認証方法として匿名ユーザー認証以外のオプションが有効になっていることを確認します。

4. ［プロパティ］をクリックし、［ドメイン制限］を選択します。

5. 特定のドメインに属するユーザーからのアクセスを制限するかどうかを指定します。 次のいずれかを選択します。

   - ドメイン単位でアクセスを制限しない場合は、［すべてのドメイン］をクリックします。

   - 選択したドメインからのアクセスを制限する場合は、［次のドメインに制限する］をクリックします。

6. ［追加］をクリックします。

7. ［ログオンドメイン］ボックスに、アクセスを許可するドメインの名前を入力します。

   注： 特定のドメインのユーザーからのアクセスを制限するには、［ドメイン］および［UPN制限］の一覧の両方に同じドメイン名を入力する必要があります。 詳しくは、「ドメインベースの認証を使用するには」を参照してください。

自動ログオン設定を構成するには

Citrix Web Interface管理コンソールの［認証方法］タスクを使って、パススルー認証、スマートカードパススルー認証、およびスマートカード認証を使ってリソースにアクセスするユーザーの自動ログオン設定を構成できます。

ユーザーに対して有効な認証方法が匿名ユーザー認証のみの場合、管理者またはユーザーが構成する設定にかかわらず自動的にログオンします。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。

3. ［操作］ペインで［認証方法］をクリックして［パススルー認証］、［スマートカードパススルー認証］、［スマートカード］の中から1つ以上のチェックボックスをオンにします。

4. ［プロパティ］をクリックし、［自動ログオン］を選択します。

5. ユーザーに自動ログオンを許可するかどうか、またユーザーの［アカウント設定］画面に自動ログオンの有効/無効を指定するオプションを表示するかどうかを指定します。

ドメインベースの認証を使用するには

指定ユーザー認証を選択した場合は、Citrix Web Interface管理コンソールの［認証方法］タスクでユーザー認証にWindowsまたはNovell Directory Services（NDS）のどちらを使用するかを指定します。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで、［認証方法］をクリックし、必要に応じて［指定ユーザーとしてログオン］や［パススルー認証］チェックボックスをオンにします。

4. ［プロパティ］をクリックして、ダイアログボックス左側で［認証の種類］を選択します。

5. ［WindowsまたはNIS（UNIX）］をクリックします。

6. ログオン情報の入力形式を指定します。 次のいずれかを選択します。

   · ユーザーがログオン情報をUPN形式とドメインユーザー名形式のどちらでも入力できるようにする場合は、［ドメインユーザー名およびUPN］をクリックします。

   · ユーザーがログオン情報をドメインユーザー名形式でしか入力できないようにする場合は、［ドメインユーザー名のみ］をクリックします。

   · ユーザーがログオン情報をUPN形式でしか入力できないようにする場合は、［UPNのみ］をクリックします。

7. ［設定］をクリックします。

8. ［ドメインの表示］で、次のオプションを構成します。

   · ［ログオン］画面に［ドメイン］ボックスを表示するかどうかを指定します。

   · ［ドメイン］ボックスにドメインの一覧を表示してユーザーが選択できるようにするか、ユーザーがドメイン名を入力するようにするかを指定します。

     注： ログオン時に「ドメインを指定する必要があります」という内容のエラーメッセージが表示される場合は、ユーザーが［ドメイン］ボックスでドメイン名を指定していない可能性があります。 このような問題を避けたい場合は、［ドメインボックスを非表示にする］を選択します。 XenApp for UNIXサーバーだけで構成されるサーバーファームでは、［ドメインの一覧］ボックスで［事前設定］を選択して、ドメイン名として［UNIX］を追加します。

   · ［ログオン］画面の［ドメイン］ボックスに表示するドメインを指定します。

9. ［UPN制限］で、次のオプションを構成します。

   · すべてのUPNサフィックスを受け付けるかどうかを指定します。 デフォルトでは、すべてのUPNサフィックスを使用できます。

- ユーザーに許可するUPNサフィックスを指定します。

  注： 特定のドメインのユーザーからのアクセスを制限するには、［ドメイン］および［UPN制限］の一覧の両方に同じドメイン名を入力する必要があります。 詳しくは、「認証の構成」を参照してください。

Novell Directory Services認証を使用するには

指定ユーザー認証を選択した場合は、Citrix Web Interface管理コンソールの［認証方法］タスクでユーザー認証にWindowsまたはNovell Directory Services（NDS）のどちらを使用するかを指定します。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで、［認証方法］をクリックし、必要に応じて［指定ユーザーとしてログオン］や［パススルー認証］チェックボックスをオンにします。

4. ［プロパティ］をクリックして、ダイアログボックス左側で［認証の種類］を選択します。

5. ［NDS］を選択します。

6. ［デフォルトのツリー名］ボックスに、ツリーの名前を入力します。

7. ［設定］をクリックして、コンテキスト制限またはコンテキストレス認証を構成します。

   注： eDirectoryのデフォルトでは、コンテキストレス認証に必要なcn属性への匿名アクセスが許可されていません。 eDirectoryを構成する方法については、http://developer.novell.com/wiki/index.php/Developer_Homeを参照してください。

8. XenApp Servicesサイトでは、Novellクライアントをインストールしているユーザーに Citrix Online Plug-inユーザーにWindowsのアカウント情報によるパススルー認証を許可する場合、［Windowsアカウントを使用する］を選択します。

XenApp Webサイトに対する指定ユーザー認証の有効化

指定ユーザー認証を有効にした場合、ユーザーはユーザーアカウントを持ち、適切なアカウント情報を入力してログオンする必要があります。

指定ユーザー認証の設定は、Citrix Web Interface管理コンソールで変更できます。 たとえば、ユーザーがセッション内でパスワードを変更できるかどうかを構成できます。

指定ユーザー認証は、XenApp Webサイトでのみ使用できます。

指定ユーザー認証を有効にするには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。
3. ［操作］ペインで［認証方法］をクリックし、［指定ユーザーとしてログオン］チェックボックスをオンにします。
4. ［プロパティ］をクリックして、指定ユーザー認証の詳細を指定します。

指定ユーザー認証のパスワード設定を構成するには

Citrix Web Interface管理コンソールの［認証方法］タスクを使って、パスワード変更やユーザーに対するパスワードの有効期限切れ警告を構成します。 一部のパスワード設定は、サイトに対して構成するほかの認証設定により影響を受けます。

- ［2要素認証］ページで［RSA SecurID］および［Windowsパスワード統合を使用する］オプションを選択する場合、［常時］オプションは無効になります。

- ［Active Directoryグループポリシーの警告メッセージ設定を使用する］チェックボックスをオンにすると、現在のWindowsのポリシーに基づいて警告メッセージが表示されます。 現在のWindowsポリシーに警告メッセージの表示期間が設定されていない場合、パスワードの有効期限が切れる前に変更を求めるメッセージがユーザーに表示されません。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。

3. ［操作］ペインで［認証方法］をクリックし、［指定ユーザーとしてログオン］チェックボックスをオンにします。

4. ［プロパティ］をクリックして、ダイアログボックス左側で［パスワード設定］を選択します。

5. ユーザーがWeb Interfaceセッションでパスワードを変更できるようにするには、［ユーザーによるパスワードの変更を許可する］チェックボックスをオンにします。

6. ユーザーがいつパスワードを変更できるかを指定します。

   - パスワードの有効期限が切れたときにユーザーがログオンパスワードを変更できるようにするには、［有効期限の満了時のみ］を選択します。 このオプションを選択すると、パスワードの期限切れでWeb Interfaceにログオンできなくなったときに［パスワードの変更］ページが開きます。 パスワードの変更後は、新しいパスワードで自動的にログオンできます。

   - ユーザーがWeb Interfaceの使用中にいつでもパスワードを変更できるようにするには、［常時］を選択します。 このオプションを選択すると、［パスワードの変更］ボタンがユーザーの［アプリケーション］および［アカウント設定］画面に表示されます。 ユーザーがこのボタンをクリックすると、新しいパスワードの入力画面が表示されます。

7. パスワードの有効期限が切れたことを知らせるメッセージを構成する場合は、次のいずれかのオプションを選択します。

   - パスワードが期限切れになる前に警告メッセージを表示しない場合は、［警告メッセージを表示しない］を選択します。

- 現在のWindowsポリシーの警告メッセージ設定を使用する場合は、［Active Directoryグループポリシーの警告メッセージ設定を使用する］を選択します。
- パスワードが期限切れになる前にユーザーに警告メッセージを表示する場合は、［カスタム警告メッセージ設定を使用する］を選択し、 メッセージを表示してから期限切れになるまでの期間を指定します。

2要素認証を有効にするには

必要に応じて、Citrix Web Interface管理コンソールの［認証方法］タスクを使ってユーザーに対する2要素認証を有効にします。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。
3. ［操作］ペインで［認証方法］をクリックし、［指定ユーザーとしてログオン］チェックボックスをオンにします。
4. ［プロパティ］をクリックして、ダイアログボックス左側で［2要素認証］を選択します。
5. 使用する2要素認証の種類を［2要素設定］の一覧から選択し、必要に応じて追加設定を構成します。

SafeWord、RSA SecurID、およびRADIUS認証の構成方法については、「Two-Factor認証の構成」を参照してください。

アカウントセルフサービスの構成

Web InterfaceにPassword Managerのアカウントセルフサービス機能を統合すると、ユーザーは管理者が設定した質問に回答することで、自分のネットワークパスワードをリセットしたりアカウントのロックを解除したりできるようになります。

サイトに対してアカウントセルフサービスを有効にすると、サイトにアクセスできるアカウントに対してセキュリティが無条件で危険にさらされることになります。 インターネットからサイトにアクセスできる場合、セキュリティ機能が無効となります。 組織のセキュリティポリシーでアカウントセルフサービスの使用を内部使用のみに制限している場合、内部ネットワーク外からサイトにアクセスできないことを確認する必要があります。

重要： Password Managerのセットアップ時に、パスワードのリセットとアカウントのロック解除を許可するユーザーを指定します。 Web Interfaceでこれらの機能を有効にしても、Password Managerで許可されていないユーザーは、これらの操作を行うことができません。

アカウントセルフサービスは、ユーザーがHTTPS接続を使ってWeb Interfaceにアクセスする場合にのみ使用できます。 ユーザーがHTTP接続を使ってWeb Interfaceにアクセスする場合は、アカウントセルフサービスを使用できません。 アカウントセルフサービスは、Access Gateway統合サイトに対しては実行できません。

アカウントセルフサービスは、username@domain.comなどのUPNログオンをサポートしません。

サイトのアカウントセルフサービスを設定する前に、次のことを確認する必要があります。

- サイトが、Windowsベースの指定ユーザー認証を使用するように設定されている。
- サイトが、1つのPassword Manager Serviceのみを使用するように設定されている。 Web Interfaceが、複数の同じドメインまたは信頼されているドメイン内にある複数のサーバーファームを使用するように設定されている場合は、これらのすべてのドメインからのログオン情報を受信するようにPassword Managerを設定する必要があります。
- サイトのパスワードもユーザーが常時変更できるように設定されている（パスワードのリセット機能を有効にする場合）。

アカウントセルフサービスを構成するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。

3. ［操作］ペインで［認証方法］をクリックし、［指定ユーザーとしてログオン］チェックボックスをオンにします。

4. ［プロパティ］をクリックして、ダイアログボックス左側で［アカウントセルフサービス］を選択します。

5. 適切なチェックボックスをオン／オフにして、ユーザーにネットワークパスワードのリセットとアカウントのロック解除を許可するかどうかを指定します。

6. ［Password Manager Service URL］ボックスに、Password ManagerのURLを入力します。

XenApp Servicesサイトに対する指定ユーザー認証の有効化

更新日： 2014-11-24

指定ユーザー認証を有効にする場合、ユーザーはユーザーアカウントを持ち、適切なアカウント情報を入力してログオンする必要があります。

指定ユーザー認証は、XenApp Servicesサイトに対して実行できます。

指定ユーザー認証を有効にするには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Servicesサイト］をクリックして結果ペインでサイトを選択します。
3. ［操作］ペインで［認証方法］をクリックし、［指定ユーザーとしてログオン］チェックボックスをオンにします。
4. ［プロパティ］をクリックして、指定ユーザー認証の詳細を構成します。

指定ユーザー認証のパスワード設定を構成するには

Citrix Web Interface管理コンソールの［認証方法］タスクを使って、ユーザーによるパスワードの保存を許可するかどうかを指定したり、ユーザーによるパスワード変更オプションを構成したりできます。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Servicesサイト］をクリックして結果ペインでサイトを選択します。
3. ［操作］ペインで［認証方法］をクリックし、［指定ユーザーとしてログオン］チェックボックスをオンにします。
4. ［プロパティ］をクリックして、ダイアログボックス左側で［パスワード設定］を選択します。
5. ユーザーがパスワードを保存できるようにするには、［ユーザーによるパスワードの保存を許可する］チェックボックスをオンにします。

6. パスワードの有効期限が切れた場合にユーザーがパスワードを変更できるようにするには、［以下に接続した、ユーザーによる有効期限の切れたパスワードの変更を許可する］チェックボックスをオンにします。

7. 次のいずれかのオプションを選択して、パスワード変更要求を送信するオプションを指定します。

   - Citrix Online Plug-inのユーザーがドメインコントローラーに直接接続してパスワードを変更できるようにするには、［ドメインコントローラーに直接］を選択します。 Citrix Online Plug-inからのパスワード変更要求が、Web InterfaceやXenApp/XenDesktopを介さずに直接ドメインコントローラーに送られるため、このオプションが最も安全な方法になります。

   - Citrix Online Plug-inのユーザーがドメインコントローラーに直接接続し、接続に失敗した場合にWeb InterfaceおよびXenApp/XenDesktopを介してパスワードを変更できるようにするには、［サーバーファームにフォールバックして、ドメインコントローラーに直接］を選択します。

   - Citrix Online Plug-inのユーザーがWeb InterfaceおよびXenApp/XenDesktopを介してドメインコントローラーに接続してパスワードを変更できるようにするには、［サーバーファーム］を選択します。 このオプションでは、ユーザーによるパスワード変更が、Web InterfaceおよびXenApp/Desktopに確実に反映されます。 ただし、新しいパスワードが多くのネットワーク接続を経由するため、セキュリティ上の問題が高くなります。

Pass-Through認証の有効化

更新日： 2013-02-21

管理コンソールにより、ユーザー名、パスワード、およびドメイン名を使ってローカルのデスクトップにログオンするユーザーに対してパススルー認証を有効にできます。 パススルー認証を有効にすると、ユーザーがローカルのWindowsデスクトップにログオンするときに入力したアカウント情報をWeb Interfaceのユーザー認証に使用できるようになります。 アカウント情報の再入力は必要なく、リソースセットが自動的に表示されます。

パススルー認証の要件

パススルー認証機能を使用するには、Web InterfaceをIIS上で実行する必要があり、ユーザーはサポートされているバージョンのInternet Explorerを実行する必要があります。
XenApp Webサイトの場合、Internet Explorerを使ってサイトをWindows信頼済みサイトまたはローカルイントラネットゾーンに追加する必要があります。

Internet Explorerバージョン7以降を使っている場合は、次のように設定します。

1. サイトをWindows信頼済みサイトに追加し、［インターネットオプション］をクリックして［セキュリティ］タブに移動します。

2. ［信頼済みサイト］ゾーンを強調表示させて［レベルのカスタマイズ］をクリックします。

3. ［セキュリティ設定］ウィンドウ 内の一番下にある［ユーザー認証］に移動し、［ログオン］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］をクリックします。

Windows Server 2008で実行するIIS 7.xの場合、［Webサーバー］>［セキュリティ］>［Windows認証］役割サービスを［Webサーバー（IIS）］役割に対して有効にします。

重要： サーバーでCitrix MetaFrame XP Feature Release 2よりも古いバージョンが動作している場合、ユーザーがパススルー認証でログオンすると、サーバーで公開されているすべてのアプリケーションおよびコンテンツが表示されることがあります。

ユーザーがVersion 6.30より前のWindows用のクライアントを使用し、ICA暗号化（SecureICA）を有効にしている場合は、パススルー認証を使用できません。 ICA暗号化とパススルーを使用するには、ユーザーは最新のCitrixのクライアントをインストールする必要があります。 パススルー認証はWeb Interface for Java Application Serversでは使用できません。

重要： ユーザーがリソースにアクセスすると、ファイルが（一部Webブラウザーを介して）Citrixのクライアントに送信されます。 このファイルには、ユーザーのローカルのログオンアカウント情報をサーバーに送信するための設定が含まれることもあります。 デフォルトでは、クライアントにこの設定は適用されません。ただし、Citrix Online Plug-inでパススルー認証が有効になっている場合、攻撃者により不正なファイルが送信され、認証されていないサーバーや偽装サーバーにユーザーのアカウント情報が転送される危険性もあります。 このようなリスクを回避するため、パススルー認証は、セキュリティで保護された信頼できる環境でだけ使用してください。

手順1：パススルー認証を使用するプラグインのインストール

更新日： 2014-12-02

Citrix Online Plug-inまたはCitrix Desktop Viewerを管理者アカウントを使ってユーザーのデバイスにインストールする必要があります。 パススルー認証機能は、XenAppおよびXenDesktopインストールメディアに収録されているこれらのプラグインでのみ使用できます。 セキュリティ上の理由から、Citrix Online Plug-in - Webにはこの機能は含まれていません。 つまり、Webインストールを使って、この機能を含むCitrixのプラグインをユーザーに配布することはできません。

クライアントをインストールしたら、グループポリシーを使ってすべてのCitrixのクライアントに対してパススルー認証を有効にする必要があります。 詳しくは、http://support.citrix.com/article/CTX122676およびOnline Plug-in for Windowsのドキュメントを参照してください。

手順2：プラグインに対するパススルーの有効化

クライアントに対するパススルー認証は、2つの手順で有効にします。 まず、クライアントテンプレートをグループポリシーオブジェクトエディターに追加します。 次に、このテンプレートを使ってすべてのクライアントに対してパススルー認証を有効にします。

パススルー認証用にクライアントテンプレートをグループポリシーオブジェクトエディターに追加するには

1. MMCでグループポリシーオブジェクトエディタースナップインを開きます。
2. 編集するグループポリシーオブジェクトを選択します。
3. ［管理用テンプレート］ノードを選択し、［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］をクリックして、クライアントテンプレートファイルのicaclient.admを指定します。 このファイルは、クライアントのConfigurationフォルダー（通常はC:¥Program Files (x86)¥Citrix¥ClientName¥Configuration）にインストールされています。
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オブジェクトエディターに戻ります。

すべてのクライアントに対してパススルー認証を有効にするには

1. MMCでグループポリシーオブジェクトエディタースナップインを開きます。
2. 編集するグループポリシーオブジェクトを選択します。
3. 管理コンソールの左側のペインで、［管理用テンプレート］ノードを展開します。
4. ［従来の管理用テンプレート（ADM）］>［Citrixコンポーネント］の順に選択します。インストールしたクライアントのノードを展開し、［ユーザー認証］を選択します。
5. 結果ペインで［Local user name and password］を選択します。
6. ［操作］メニューの［編集］を選択します。
7. ［有効］をクリックして、［Enable pass-through authentication］チェックボックスをオンにします。
8. グループポリシーオブジェクトエディター内のユーザーおよびコンピューターの両方で、これらすべての手順を完了させる必要があります。
9. いったんログオフしてから再度ログオンすると、ポリシーに対する変更が有効になります。

手順3：コンソールを使ったパススルーの有効化

次は、Citrix Web Interface管理コンソールを使って、サイトのパススルー認証を有効にします。 パススルー認証を有効にした場合、ユーザーはアカウント情報を再入力する必要がなく、リソースセットは自動的に表示されます。

XenApp WebサイトおよびXenApp Servicesサイトでは、パススルー認証と一緒にKerberos認証も使用できます。 またXenApp Servicesサイトでは、スマートカードパススルー認証でもKerberos認証を使用できます。

パススルー認証を有効にするには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ ペインで［認証方法］をクリックし、［パススルー認証］チェックボックスをオンにします。

4. ［プロパティ］をクリックして、ダイアログボックス左側で［Kerberos認証］を選択します。

5. Kerberos認証を有効にする場合は、XenApp Webサイトでは［Kerberos認証を使ってサーバーに接続する］チェックボックスを、XenApp Servicesサイトでは［Kerberosを使用する］チェックボックスをオンにします。

スマートカード認証の有効化

更新日： 2014-12-02

スマートカード認証を使用するには、Web InterfaceがIIS上で動作しており、ユーザーのWebブラウザーがサポートされているバージョンのInternet ExplorerまたはFirefoxである必要があります。 スマートカードパススルー認証の場合、Internet Explorerのサポートされているバージョンを実行している必要があります。スマートカードパススルー認証はFirefox をサポートしていません。

XenApp Webサイトに対するスマートカードパススルー認証を有効にしない場合、ユーザーはInternet Explorerを使ってサイトをWindows信頼済みサイトまたはローカルイントラネットゾーンに追加する必要があります。

Windows Server 2008で実行するIIS 7.xの場合、［Webサーバー］>［セキュリティ］>［クライアント証明書のマッピング認証］役割サービスを［Webサーバー（IIS）］役割に対して有効にします。 スマートカードパススルー認証を有効にする場合は、［Webサーバー］>［セキュリティ］>［Windows認証］役割サービも有効にします。

マートカード認証はWeb Interface for Java Application Serversではサポートされていません。

Secure Sockets Layer（SSL）はWebブラウザーとサーバー間の通信の保護に使用されるため、Webサーバー上でSSLが有効である必要があります。 詳しくは、Webサーバーのドキュメントを参照してください。

スマートカード認証を有効にするには（ほかの認証方法と組み合わせる場合もそうでない場合も）、［ログオン］画面にHTTPS接続でのみアクセスできるように構成する必要があります。 ユーザーが通常のHTTPでアクセスしたり、HTTPSの構成が間違っていたりすると、エラーメッセージが表示され、ユーザーはログオンできなくなります。 この問題を防ぐには、すべてのユーザーに、https://www.MyCompany.com:443/Citrix/XenAppなどの完全なHTTPS URLを提供します。

スマートカード認証を使用するためにユーザーデバイスやサーバーで必要なシステム環境については、「Citrix XenAppでスマートカードを使用する」を参照してください。

手順1：スマートカード認証を使用するプラグインのインストール

スマートカード認証を使用するには、ユーザーはCitrix Online Plug-inまたは Citrix Desktop Viewerをインストールする必要があります。 またはWebベースのクライアントインストールを使って、適切に構成されたXenApp WebサイトからCitrix Online Plug-in – Webをダウンロードしてインストールできます。 ただし、スマートカードパススルー認証を使用するには、Citrix Online Plug-inまたはCitrix Desktop Viewerを管理者アカウントを使ってユーザーのデバイスにインストールする必要があります。 パススルー認証機能は、XenAppおよびXenDesktopインストールメディアに収録されているこれらのプラグインでのみ使用できます。 セキュリティ上の理由から、Citrix Online Plug-in - Webにはこの機能は含まれていません。

スマートカードパススルー認証を有効にする場合、プラグインをインストールした後で最初にグループポリシーを使ってすべてのCitrixのクライアントに対してパススルー認証を有効にする必要があります。 クライアントに対するパススルー認証は、2つの手順で有効にします。まず、クライアントテンプレートをグループポリシーオブジェクトエディターに追加します。次に、このテンプレートを使ってすべてのクライアントに対してパススルー認証を有効にします。

パススルー認証用にクライアントテンプレートをグループポリシーオブジェクトエディターに追加するには

1. MMCでグループポリシーオブジェクトエディタースナップインを開きます。
2. 編集するグループポリシーオブジェクトを選択します。
3. ［管理用テンプレート］ノードを選択し、［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］をクリックして、クライアントテンプレートファイルのicaclient.admを指定します。 このファイルは、クライアントのConfigurationフォルダー（通常はC:¥Program Files (x86)¥Citrix¥ClientName¥Configuration）にインストールされています。
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オブジェクトエディターに戻ります。

すべてのクライアントに対してスマートカードによるパススルー認証を有効にするには

1. MMCでグループポリシーオブジェクトエディタースナップインを開きます。
2. 編集するグループポリシーオブジェクトを選択します。
3. 管理コンソールの左側のペインで、［管理用テンプレート］ノードを展開します。
4. ［従来の管理用テンプレート（ADM）］>［Citrixコンポーネント］の順に選択します。インストールしたクライアントのノードを展開し、［ユーザー認証］を選択します。
5. 結果ペインで［スマートカード認証］を選択します。
6. ［操作］メニューの［編集］を選択します。
7. ［有効］をクリックして［Allow smart card authentication］および［Use pass-through authentication for PIN］チェックボックスをオンにします。

手順2：Windowsディレクトリサービスマッパーの有効化

スマートカード認証を有効にするには、Web InterfaceサーバーでWindowsディレクトリサービスマッパーを有効する必要があります。

Web Interfaceの認証では、Windowsのドメインアカウント、つまりユーザー名とパスワードを使用します。 ただし、スマートカードには証明書が含まれます。 ディレクトリサービスマッパーは、Windows Active Directoryを使って、証明書をWindowsドメインアカウントにマップします。

Microsoft Internet Information Services 7.xのWindowsディレクトリサービスマッパーを有効にするには

1. Web Interfaceサーバーで、［Webサーバー］>［セキュリティ］>［IISクライアント証明書のマッピング認証］役割サービスを［Webサーバー（IIS）］役割サービスにインストールしないようにします。
2. MMCインターネットインフォメーションサービス（IIS）マネージャープラグインを開きます。
3. 左側のペインでWebサーバーを選択し、［機能ビュー］で［認証］をダブルクリックします。
4. ［認証］ページで、［Active Directoryクライアント証明書の認証］を有効にします。

Microsoft Internet Information Services 6.0のWindowsディレクトリサービスマッパーを有効にするには

1. Web Interfaceサーバーで、インターネットインフォメーションサービス（IIS）マネージャーを開きます。
2. Web Interfaceサーバーのコンピューター名の下のWebサイトを選択し、［操作］ペインで［プロパティ］を選択します。
3. ［ディレクトリセキュリティ］タブで、［セキュリティ保護された通信］の［Windowsディレクトリサービスマッパーを有効にする］チェックボックスをオンにします。

手順3：Web Interface上でのスマートカード認証の有効化

スマートカード認証を有効にし（これによりユーザーがWeb Interfaceにアクセスしてリソースセットを取得できます）、またサーバーに対する認証を有効にする（これによりユーザーはWeb Interfaceを使ってセッションのリソースにアクセスできます）ために、Web Interfaceを構成する必要があります。

XenApp Webサイトでスマートカード認証を有効にするには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。
3. ［操作］ペインで［認証方法］をクリックし、必要に応じて［スマートカード］または［スマートカードパススルー認証］チェックボックスをオンにします。
4. ［プロパティ］をクリックして、スマートカード認証の詳細を構成します。

XenApp Servicesサイトでスマートカード認証を有効にするには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Servicesサイト］をクリックして結果ペインでサイトを選択します。

3. ［操作］ペインで［認証方法］をクリックし、必要に応じて［スマートカード］または［スマートカードパススルー認証］チェックボックスをオンにします。

4. ［プロパティ］をクリックして［ローミング］を選択します。

5. スマートカードを取り出した場合のWeb Interfaceの動作を構成するには、［ローミングを有効にする］チェックボックスをオンにして、次のいずれかのオプションを選択します。

   - ユーザーがスマートカードを取り出した場合にセッションを切断するには、［スマートカードの取り出し時にセッションを切断する］を選択します。

   - ユーザーがスマートカードを取り出した場合にセッションからログオフするには、［スマートカードの取り出し時にセッションをログオフする］を選択します。
6. スマートカードパススルー認証を有効にし、Citrix Online Plug-inとXenApp Servicesサイト間でKerberos認証を使用する場合は、［Kerberos認証］を選択して［XenApp ServicesサイトにKerberos認証を使用する］チェックボックスをオンにします。

例：ユーザーのスマートカード認証の有効化

ユーザーに対するスマートカードパススルー認証を有効にします。 ユーザーのコンピューターはWindows XPを実行しています。 スマートカードリーダーはユーザーのコンピューターに接続されており、サーバーファームでスマートカードのサポートが構成されています。 現在Web Interfaceでは、ユーザー名とパスワードを使用する指定ユーザー認証だけが構成されています。

スマートカードパススルー認証を有効にするには

1. 適切なインストールメディアを使ってCitrix Online Plug-inまたはCitrix Desktop Viewerをユーザーのコンピューターにインストールします。 プラグインのインストールは、管理者アカウントで実行します。 XenApp Webサイトの場合、ユーザーのコンピューター上のInternet Explorerを使ってサイトをWindows信頼済みサイトまたはローカルイントラネットゾーンに追加します。

2. グループポリシーを使用して、すべてのCitrixのクライアントに対するパススルー認証を有効にします。 詳しくは、「手順1：スマートカード認証を使用するプラグインのインストール」を参照してください。 また、パススルー認証をサーバーファームで有効にする必要があります。 詳しくは、サーバー製品のドキュメントを参照してください。

3. Windowsディレクトリサービスマッパーが有効になっていることを確認します。 詳しくは、「手順2：Windowsディレクトリサービスマッパーの有効化」を参照してください。

4. Citrix Web Interface管理コンソールの［認証方法］タスクを使って、スマートカードパススルー認証を有効にします。 詳しくは、「手順3：Web Interface上でのスマートカード認証の有効化」を参照してください。 スマートカードを使って物理的なWindowsデスクトップにログオンします。 リソースにアクセスすると、自動的にログオンします。 パスルーなしでスマートカードが有効になっている場合、リソースへのアクセス時にPINの入力が必要となります。

Two-Factor認証の構成

XenApp Webサイトでは、次の2要素認証を構成できます。

- Aladdin SafeWord for Citrix： SafeWordトークンで生成される英数字コードとPIN番号（オプション）を組み合わせたパスコードを使用する認証技術です。 ユーザーは、Web Interfaceの［ログオン］画面で、ドメインのアカウント情報とSafeWordパスコードを入力して、サーバーの公開アプリケーションにアクセスします。

- RSA SecurID： RSA SecurIDトークンで生成される番号（トークンコード）とPIN番号を組み合わせたパスコードを使用する認証方法です。 ユーザーは、Web Interfaceの［ログオン］画面で、ユーザー名、パスワード、ドメイン、およびRSA SecurIDパスコードを入力して、サーバーのリソースにアクセスします。 RSA ACE/Server上でユーザーを作成する場合、ドメインユーザー名と同じ名前をユーザーログイン名として指定する必要があります。

  注： RSA SecurID認証を使用する場合、システムにより新しいPINが生成され、ユーザーに表示されます。 このPINは、10秒間、またはユーザーが［ログオン］または［キャンセル］をクリックするまで表示されます。これは、ほかのユーザーにPINを見られるのを防ぐためです。 この機能は、PDAデバイスでは使用できません。

- RADIUSサーバー： 専用のエージェントソフトウェアではなく、RADIUS（Remote Authentication Dial-in User Service）認証プロトコルを使用する認証方法です。 SafeWordとSecurIDは、RADIUSサーバーとして動作するためのインストールおよび構成が可能です。 Web Interface for Java Application Serversの場合、2要素認証としてはRADIUS認証のみを使用できます。

Microsoftインターネットインフォメーションサービス（IIS）でのSafeWord認証の有効化

ここでは、RSA SecurID 6.0のサポートを有効にする方法について説明します。

SafeWordの要件

Web Interface for Microsoft Internet Information ServicesでSafeWord認証を使用するには次のことが必要です。

- SafeWord Agentの最新バージョンをAladdin Knowledge Systems社から入手する。UPN認証をサポートするには、最新のSafeWord Agent for the Web InterfaceおよびSafeWordサーバーを適用する必要があります。
- SafeWord Agent for the Web Interfaceをインストールする前に、Web Interfaceをインストールする。
- Web InterfaceサーバーにSafeWord Agent for the Web Interfaceをインストールする。

SafeWord製品の構成方法について詳しくは、http://www.aladdin.com/safeword/default.aspxを参照してください。

コンソールを使ったRSA SecurID認証の有効化

ユーザーがリソースセットにアクセスして表示できるように、Web InterfaceでRSA SecurID認証を有効にする必要があります。 これを実行するには、Citrix Web Interface管理コンソールの［認証方法］タスクを使用します。

Microsoftインターネットインフォメーションサービス（IIS）でのRSA SecurID認証の有効化

更新日： 2014-11-24

ここでは、RSA SecurID 7.0のサポートを有効にする方法について説明します。

SecurIDの要件

Web Interface for Microsoft Internet Information ServicesでSecurID認証を使用するには次のことが必要です。

- WebサーバーにRSA ACE/Agent for Windows 7.0以降をインストールする。
- RSA ACE/Agentをインストールした後に、Web Interfaceをインストールする。
- Web InterfaceをMicrosoftインターネットインフォメーションサービス（IIS）6.0上でホストする。

Agent HostとしてのWeb Interfaceサーバーの追加

RSA ACE/Serverが、Webサーバーからの認証要求を認識し、許可できるようにするには、事前にRSA ACE/ServerデータベースにWebサーバーのAgent Hostを作成しておく必要があります。 Agent Hostを作成する場合、Web InterfaceをNetOS Agentとして構成します。この設定は、Web Interfaceとどのように通信するかを決定するためにRSA ACE/Serverによって使用されます。

sdconf.recファイルのコピー

RSA ACE/Server上でsdconf.recファイルを検索（または必要な場合は作成）し、このファイルをWeb Interfaceサーバー上の¥System32フォルダー（通常はC:¥Windows¥System32）にコピーします。 このファイルには、Web InterfaceがRSA ACE/Serverに接続するときに必要な情報が指定されています。

コンソールを使ったRSA SecurID認証の有効化

ユーザーがリソースセットにアクセスして表示できるように、Web InterfaceでRSA SecurID認証を有効にする必要があります。 これを実行するには、Citrix Web Interface管理コンソールの［認証方法］タスクを使用します。

RSA SecurIDでの複数ドメインのサポート

同じユーザー名を共有し、異なるWindowsドメインにあるユーザーアカウントがある場合、RSA ACE/Serverデータベースで［Default Login］にユーザー名形式ではなく、DOMAIN¥usernameの形式を使用し、Citrix Web Interface管理コンソールの［認証方法］タスクでRSA ACE/Serverにドメインおよびユーザー名を送るよう構成する必要があります。

RSA SecurID のWindowsのパスワード統合の有効化

Web Interfaceは、RSA SecurIDのWindowsパスワード統合機能をサポートします。 この機能を有効にすると、Web Interfaceのユーザーは、SecurIDパスコードを使ってログオンし、リソースにアクセスできます。 ユーザーがWindowsのパスワードを入力するのは最初のWeb Interfaceへのログオン時、またはパスワードを変更する必要がある場合のみです。

Web Interface for Microsoft Internet Information ServicesでSecurID Windowsパスワード統合を使用するには、次のことを実行する必要があります。

- Web InterfaceサーバーにRSA ACE/Agent Local Authentication Client for Windowsをインストールする（管理者は、ローカルの管理者アカウント情報でWeb Interfaceにログオンする必要がある）。
- RSA ACE/Agentをインストールした後に、Web Interfaceをインストールする。
- WebサーバーでRSA Authentication Agent Offline Local Serviceを実行する。
- RSA ACE/Serverデータベースで、WebサーバーのAgent HostのWindowsパスワード統合機能を有効にする。
- データベースのシステムパラメーターを構成して、システムレベルでのWindowsパスワード統合を有効にする。

Webサーバー上のノードシークレットのレジストリキーをリセットするには

ノードシークレットは、Web InterfaceとRSA ACE/Server間の通信を保護するために使用されます。

次のような場合は、これらの2つのサーバーのノードシークレットが非同期状態となります。

- Web Interfaceを再インストールした場合
- RSA ACE/Serverを再インストールした場合
- WebサーバーのAgent Host情報をデータベースから削除し、その後で再度追加した場合
- WebサーバーのNodeSecretレジストリキーが削除された場合
- RSA ACE/Serverで、［Edit Agent Host］ダイアログボックスの［Node Secret Created］チェックボックスがオフの場合

Web InterfaceサーバーとRSA ACE/Serverのノードシークレットが一致しない場合、SecurIDは失敗します。 Web InterfaceサーバーとRSA ACE/Serverでノードシークレットをリセットする必要があります。

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。

1. システムレジストリで、次の場所に移動します。
   - 32ビットサーバー上のHKEY_LOCAL_MACHINE¥SOFTWARE¥SDTI¥ACECLIENT
   - 64ビットサーバー上のHKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥SDTI¥ACECLIENT
2. NodeSecretキーを削除します。

注： Web Interfaceを再インストールしても、NodeSecretキーは削除されません。 RSA ACE/ServerのAgent Host情報を変更しない限り、同じノードシークレットを使用できます。

RADIUS認証の有効化

更新日： 2014-11-24

ここでは、Aladdin SafeWordおよびRSA SecurIDをインストールおよび構成して、RADIUSサーバーとして表示させる方法について説明します。 RADIUS認証は、Web Interface for Java Application Serversで使用できる唯一の2要素認証オプションです。

SafeWordでのRADIUSの有効化

SafeWordサーバーソフトウェアをインストールする場合、IAS RADIUS Agentのインストールを選択します。

画面上の指示に従って、RADIUSクライアントと、Microsoft管理コンソールのWindows Internet Authentication Service（IAS）スナップインをインストールします。 新しいRADISUクライアントは、SafeWordサーバーでユーザーを認証する各Web Interfaceサーバーについて構成する必要があります。

各RADIUSクライアントについて、次の設定が必要です。

- RADIUSクライアントが関連付けられるWeb Interfaceサーバーの完全修飾ドメイン名またはIPアドレスを指定します。
- 関連付けられるWeb Interfaceサーバーで使用できる共有シークレットを指定します。
- クライアント製造元を［RADIUS standard］に設定する必要があります。
- セキュリティを強化するため、［クライアントは要求時に常に署名属性を送信する］オプションを有効にする必要があります。

RSA SecureIDによるRADIUSの有効化

SecurID Configuration Management Toolを使い、RADIUSをRSA Authentication Managerで有効にします。 このツールについて詳しくは、RSA Authentication Managerのドキュメントを参照してください。

Authentication ManagerとしてのWeb InterfaceおよびRADIUSサーバーの追加

ユーザー認証を行なうRSA Authentication ManagerをRADIUSサーバーとして動作させるには、RSA Authentication Managerデータベースでローカルの RADIUSサーバーに対するAuthentication Agent記録を作成する必要があります。 Authentication Agent記録を作成する場合、ローカルサーバーの名前とIPアドレスを設定し、このサーバーをNetOS Authentication Agentとして構成します。 ローカルサーバーは［Acting Server］として割り当てる必要があります。

これに加えて、RSA Authentication Managerデータベースで各Web Interfaceサーバーに対するAuthentication Agent記録を作成する必要があります。これにより、RSA Authentication Managerは、RADIUSサーバーを介したWeb Interfaceからの認証要求を認識して受け入れます。 Authentication Agent記録を作成する場合、Web Interfaceを［Communication Server］として構成し、Web Interfaceと共有されるシークレット値に対する暗号キーを設定します。

RADIUSチャレンジモードの使用

デフォルトでは、SecurID RADIUSサーバーはRADIUSチャレンジモードで動作します。 このモードは、次のように動作します。

- Web Interfaceは、汎用的なチャレンジ用画面を表示します。この画面には、メッセージ、HTMLパスワードボックス、および［OK］ボタンと［キャンセル］ボタンが表示されます。
- Web Interfaceは、チャレンジメッセージをローカライズしません。 メッセージは、SecurID RADIUSサーバーで設定されているチャレンジメッセージの言語で表示されます。

ユーザーが応答を送信しなかった場合（たとえば［キャンセル］をクリックした場合）は、［ログオン］画面に戻ります。

このモードは、認証にRADIUSサーバーも使用するWeb Interfaceでは使用せず、それ以外のソフトウェアコンポーネントまたは製品でのみ使用することをお勧めします。

独自のチャレンジメッセージの使用

SecurID RADIUSサーバーに独自のチャレンジメッセージを構成することができます。 この機能を使用すると、RADIUSサーバーはWeb Interface for Microsoft Internet Information Servicesのユーザーインターフェイスのページを別の言語で作成して表示することができます。

この機能を使用するにはRADIUSサーバーの構成を変更する必要があるため、Web Interfaceのユーザーを認証する目的でのみRADIUSサーバーを使用している場合以外は、この機能を使用しないでください。

チャレンジメッセージを変更するには、RSA RADIUS Configuration Utilityを使用します。このツールの使用方法について詳しくは、RSA SecurIDソフトウェアに付属のドキュメントを参照してください。 IISとJava Application Serverのユーザーに同じメッセージを表示するには、以下のチャレンジメッセージを変更する必要があります。

メッセージ	パケット	変更後の値
Does User Want a System PIN（ユーザーがシステムPINを必要としているか）	Challenge	CHANGE_PIN_EITHER
Is User Ready to Get System PIN（ユーザーがシステムPINを取得できる状態か）	Challenge	SYSTEM_PIN_READY
Is User Satisfied with System PIN（ユーザーがシステムPINに満足しているか）	Challenge	CHANGE_PIN_SYSTEM_[%s]
New Numeric PIN of Fixed Length（新しい固定長の数値PIN）	Challenge	CHANGE_PIN_USER

New Alphanumeric PIN of Fixed Length（新しい固定長の英数字PIN）	Challenge	CHANGE_PIN_USER
New Numeric PIN of Variable Length（新しい可変長の数値PIN）	Challenge	CHANGE_PIN_USER
New Alphanumeric PIN of Variable Length（新しい可変長の英数字PIN）	Challenge	CHANGE_PIN_USER
New PIN Accepted（新しいPINが受け入れられた）	Challenge	SUCCESS
Enter Yes or No（YesまたはNoを入力）	Challenge	FAILURE
Next Token Code Required（次のトークンコードが必要）	Challenge	NEXT_TOKENCODE

RADIUSの共有シークレットの作成

RADIUSプロトコルでは、共有シークレットを使用する必要があります。共有シークレットとは、RADIUSクライアント（ここではWeb Interface）と認証先RADIUSサーバーだけが使用できるデータです。 Web Interfaceは、この共有シークレットをテキストファイル形式でローカルのシステム上に保存します。 このファイルの場所は、web.configファイル（IISでホストされるサイトの場合）またはweb.xmlファイル（Java Application Serverでホストされるサイトの場合）のRADIUS_SECRET_PATH構成値で指定されます。 指定された場所は、IISでホストされるサイトの¥confフォルダーおよびJava Application Serverでホストされるサイトの/WEB_INFディレクトリに相対します。

共有シークレットを作成するには、任意の文字列を記述したradius_secret.txtというファイル名のテキストファイルを作成します。 このファイルを構成ファイルで指定されている場所に移動してロックし、適切なユーザーまたはプロセスだけがアクセスできるようにする必要があります。

RADIUSのネットワークアクセスサーバー識別子の指定

RADIUSプロトコルでは、RADIUSサーバーへのアクセス要求にRADIUSクライアントのIPアドレスまたはほかの識別子（つまりWeb Interface）が含まれる必要があります。 RADIUS認証を有効にするには、WebサーバーのIPアドレスを指定するか、またはRADIUSネットワークアクセスサーバー（NAS）識別子属性の値を指定する必要があります。 NAS識別子属性の値は、3文字以上の任意の文字列にすることができます。 この属性は各RADIUSクライアントに対して必ずしも一意である必要はありませんが、クライアントごとに一意の識別子を設定すると、RADIUS通信の問題を診断する際に役に立ちます。

RADIUSクライアントのIPアドレスを指定するには、web.configファイル（IISでホストされているサイトの場合）またはweb.xmlファイル（Java Application Serverでホストされているサイトの場合）のRADIUS_IP_ADDRESS構成パラメーターの値としてWebサーバーのIPアドレスを入力します。 RADIUS NAS識別子を設定するには、web.configまたはweb.xmlでRADIUS_NAS_IDENTIFIERの値を指定します。

コンソールを使ったRADIUSの2要素認証の有効化

ユーザーがリソースセットにアクセスして表示できるように、Web Interfaceへの2要素認証を有効にする必要があります。 これを実行するには、Citrix Web Interface管理コンソールの［認証方法］タスクを使用します。 2要素認証のほかに、RADIUSサーバーアドレス（および必要な場合はポート番号）、サーバーの負荷分散またはフェールオーバー、およびタイムアウトを指定できます。

重要： RADIUS認証を有効にしたら、RADIUSクライアントのIPアドレスを指定するか、またはRADIUSネットワークアクセスサーバー識別子属性の値をサイトのweb.configファイル（IIS）またはweb.xmlファイル（Java Application Server）で指定する必要があります。

クライアントの管理

更新日： 2014-11-24

ここでは、Web InterfaceによるCitrixのクライアントの配布および使用について説明します。 また、セキュアなアクセスをセットアップする方法についても説明します。

オンラインリソース用のクライアント

次のCitrixのクライアントは、オンラインリソースへのアクセスに使用できます。

- ネイティブクライアント： 管理者は、適切なネイティブクライアントをユーザーのデバイスにインストールします。 ユーザーデバイス上にネイティブクライアントがインストールされていない場合、クライアント検出および展開処理を使用してCitrix Online Plug-inをダウンロードしてインストールできます。 ネイティブクライアントは、リソースをデスクトップ上のサイズ変更可能なウィンドウに表示できる、シームレスウィンドウに対応しています。 ユーザーがPDA（Personal Digital Assistant）デバイスからリソースにアクセスする場合は、ネイティブクライアントを有効にする必要があります。

- Client for Java： リソースへのアクセス時に、ユーザーはClient for Javaを実行します。 ネイティブクライアントがインストールされておらず、ユーザーがCitrix Online Plug-inをインストールできない場合、またはデバイスやXenApp Webサイトの構成によりインストールが禁止されている場合、このクライアントが使用されます。 Client for Javaは、リソースをデスクトップ上のサイズ変更可能なウィンドウに表示できる、シームレスウィンドウに対応しています。

- 埋め込みリモートデスクトップ接続（RDP）ソフトウェア： このオプションを使用できる場合は、Windowsオペレーティングシステムの一部としてインストール済みのリモートデスクトップ接続（RDP）ソフトウェアを使用できます。 クライアント検出および展開処理により、リモートデスクトップ接続（RDP）ソフトウェアがインストールされていないユーザーに対してこれを有効にすることができません。 シームレスウィンドウには対応していないため、リソースはWebブラウザーウィンドウに表示されます。

  注： Client for Javaおよび埋め込みリモートデスクトップ接続（RDP）ソフトウェアは、Windows CEまたはWindows Mobileを実行するデバイスでは使用できません。 Client for Javaおよび埋め込みリモートデスクトップ接続（RDP）ソフトウェアはAD FS統合サイトでの使用をサポートしません。

Citrix Online Plug-inの構成

Citrix Online Plug-inにより、ユーザーは物理的なWindowsデスクトップからWebブラウザーを使用することなくアプリケーション、コンテンツ、仮想デスクトップに直接アクセスできます。 管理者は、［スタート］メニュー、Windowsデスクトップ、またはWindowsの通知領域に、これらのリソースへのショートカットを配置できます。 また、Citrix Online Plug-inのユーザーインターフェイスをユーザー側で変更できないようにして、ユーザーの構成ミスを防ぐこともできます。 Citrix Online Plug-inを構成するには、Citrix Web Interface管理コンソールまたはconfig.xmlファイルを使用します。

Citrix Web Interface管理コンソールを使った構成

Citrix Online Plug-inは、デフォルトの表示オプション、認証方法、およびサーバー接続オプションを使用するように構成されています。 Citrix Web Interface管理コンソールを使って、これらのデフォルト設定をユーザーが変更できないように設定できます。

構成ファイルの使用

Citrix Online Plug-inをconfig.xmlおよびWebInterface.confファイルを使って構成することもできます。通常、これらのファイルは、Web Interfaceサーバーの C:¥inetpub¥wwwroot¥Citrix¥PNAgent¥confにあります。

プラグイン構成ファイルの管理

コンソールで構成したCitrix Online Plug-inオプションは、Web Interfaceサーバー上の構成ファイルに保存されます。 この構成ファイルによって、ユーザーのCitrix Online Plug-inの［オプション］ダイアログボックスに表示されるさまざまなオプション（パラメーター）が制御されます。 ユーザーは、ログオンモード、ウィンドウのサイズ、音質、リソースへのショートカットの表示位置など、ICAセッションに関するさまざまなオプションを指定できます。

新しいサイトでは、インストール直後の構成ファイル（config.xml）には各種オプションのデフォルト値が定義されており、多くのネットワーク環境ではこの値を特に編集せずにそのまま使用できます。 config.xmlファイルは、サイトのConfフォルダーにインストールされます。

Web Interfaceへのクライアントインストールファイルのコピー

更新日： 2014-11-24

Webベースのクライントインストールを使用するには、Web Interfaceサーバーでクライアントインストールファイルを使用できる必要があります。

Web Interfaceのインストール時に、XenAppまたはXenDesktopインストールメディアへのアクセスを求めるメッセージが表示されます。 IISでは、インストールメディアのCitrix Receiver and Plug-insフォルダー内のファイルが、ルートディレクトリのClientsフォルダー（例：C:¥Program Files (x86)¥Citrix¥Web Interface¥Version¥Clients）にコピーされます。 Java Application Serverでは、インストールメディアからクライアントがコピーされ、WARファイルにパッケージ化されます。

Web Interfaceのインストール時にクライアントインストールファイルをWebサーバーにコピーしなかった場合は、Webベースのクライアントインストール機能を使用する前に、必ずこれらのファイルをWebサーバーにコピーしてください。例えば、Citrix Receiver and Plug-ins/Windowsフォルダーからファイルをコピーします。 XenAppまたはXenDesktopのインストールメディアを使用できない場合は、必要なディレクトリ構成を手作業で再作成し、Citrix Webサイトから必要なクライアントソフトウェアをダウンロードする必要があります。

デフォルトでは、クライアントインストールファイルのファイル名はXenAppまたはXenDesktopのインストールメディアで提供されているファイル名と同じであると仮定しています。 Iクライアントのインストールファイルをを Citrix Webサイトからダウンロード、または古いバージョンのクライントソフトウェアを展開する場合は、XenApp Webサイトの構成ファイルで適切なクライアントインストールファイル名が指定されているかチェックします。

Microsoftインターネットインフォメーションサービス（IIS）上のWeb Interfaceにクライアントファイルをコピーするには

1. Web Interfaceのインストール先にあるClientsフォルダーを探します（例：C:¥Program Files (x86)¥Citrix¥Web Interface¥Version¥Clients）。

2. インストールメディアをWebサーバーのドライブに挿入するか、ネットワーク上の共有ディレクトリに保存されているインストールメディアのイメージにアクセスします。

3. インストールメディアのCitrix Receiver and Plug-insフォルダーに移動します。 その内容をWeb Interfaceサーバー上のClientsフォルダーにコピーします。 フォルダー内のファイルのみをコピーし、Citrix Receiver and Plug-insフォルダー自体はコピーしないようにします。

   XenAppまたはXenDesktopのインストールメディアを使用できない場合は、次のディレクトリ構成を手作業で再作成し、Citrix Webサイトから必要なクライアントソフトウェアをダウンロードする必要があります。

   C:¥Program Files (x86)¥Citrix¥Web Interface¥Version¥Clients

   - ¥de
     - ¥Unix

       ドイツ語をサポートするClients for UNIXインストールファイル（solaris.tar.Z、sol86.tar.Z）をこのフォルダーに置きます。
   - ¥en
     - ¥Unix

       英語をサポートするClients for UNIXインストールファイル（solaris.tar.Z、sol86.tar.Z）をこのフォルダーに置きます。
   - ¥es
     - ¥Unix

       スペイン語をサポートするClients for UNIXインストールファイル（solaris.tar.Z、sol86.tar.Z）をこのフォルダーに置きます。
   - ¥fr
     - ¥Unix

       フランス語をサポートするClients for UNIXインストールファイル（solaris.tar.Z、sol86.tar.Z）をこのフォルダーに置きます。
   - ¥ja
     - ¥Unix

       日本語をサポートするClients for UNIXインストールファイル（solaris.tar.Z、sol86.tar.Z）をこのフォルダーに置きます。
   - ¥Java

Client for Javaファイルをこのフォルダーに置きます。

- ¥Linux

  Citrix Receiver for Linuxインストールファイル（linuxx86-Version.tar.gz）をこのフォルダーに置きます。

- ¥Mac

  - ¥Web Online Plug-in

    Citrix Online Web Plug-in for Macintoshインストールファイル（Citrix online plug-in (web).dmg）をこのフォルダーに置きます。
- ¥Windows

  - ¥Offline Plug-in

    Citrix Offline Plug-inインストールファイル（CitrixOfflinePlugin.exe）をこのフォルダーに置きます。

  - ¥Online Plug-in

    Citrix Onine Plug-in - Webインストールファイル（CitrixOnlinePluginWeb.exe）をこのフォルダーに置きます。

デフォルトでは、クライアントインストールファイルのファイル名はXenAppまたはXenDesktopのインストールメディアで提供されているファイル名と同じであると仮定しています。 クライアントのインストールファイルをCitrixのWebサイトからダウンロード、または古いバージョンのクライアントソフトウェアを展開する場合は、XenApp Webサイトの構成ファイルでClientIcaLinuxX86、ClientIcaMac、ClientIcaSolarisSparc、ClientIcaSolarisX86、ClientIcaWin32、およびClientStreamingWin32パラメーターに対して適切なクライアントインストールファイル名が指定されているかチェックします。

クライアントインストールファイルを上記のディレクトリ構造にコピーしたら、Webベースのクライアントインストールを実行するように構成されたXenApp Webサイトで、それを必要とするユーザーにクライアントが自動的に配布されるようになります。

Java Application Server上のWeb Interfaceにクライアントファイルをコピーするには

1. サイトのWARファイルを展開し、Clientsディレクトリに移動します。

2. インストールメディアをWebサーバーのドライブに挿入するか、ネットワーク上の共有ディレクトリに保存されているインストールメディアのイメージにアクセスします。

3. ディレクトリをインストールメディアの/Citrix Receiver and Plug-insディレクトリに変更します。 その内容をWeb Interfaceサーバー上のClientsディレクトリにコピーします。 ディレクトリ内のファイルのみをコピーし、Citrix Receiver and Plug-insディレクトリ自体はコピーしないようにします。

   XenAppまたはXenDesktopのインストールメディアを使用できない場合は、次のディレクトリ構成を手作業で再作成し、Citrix Webサイトから必要なクライアントソフトウェアをダウンロードする必要があります。

   XenAppWebSiteRoot/Clients

   - /de
     - /Unix

       ドイツ語をサポートするClients for UNIXインストールファイル（solaris.tar.Z、sol86.tar.Z）をこのディレクトリに置きます。
   - /en
     - /Unix

       英語をサポートするClients for UNIXインストールファイル（solaris.tar.Z、sol86.tar.Z）をこのディレクトリに置きます。
   - /es
     - /Unix

       スペイン語をサポートするClients for UNIXインストールファイル（solaris.tar.Z、sol86.tar.Z）をこのディレクトリに置きます。
   - /fr
     - /Unix

       フランス語をサポートするClients for UNIXインストールファイル（solaris.tar.Z、sol86.tar.Z）をこのディレクトリに置きます。
   - /ja
     - /Unix

       日本語をサポートするClients for UNIXインストールファイル（solaris.tar.Z、sol86.tar.Z）をこのディレクトリに置きます。
   - /Java

     Client for Javaファイルをこのディレクトリに置きます。

- /Linux

  Citrix Receiver for Linuxインストールファイル（linuxx86-Version.tar.gz）をこのディレクトリに置きます。

- /Mac

  - /Web Online Plug-in

    Citrix Online Web Plug-in for Macintoshインストールファイル（Citrix online plug-in (web).dmg）をこのディレクトリに置きます。

- /Windows

  - /Offline Plug-in

    Citrix Offline Plug-inインストールファイル（CitrixOfflinePlugin.exe）をこのディレクトリに置きます。

  - /Online Plug-in

    Citrix Onine Plug-in - Webインストールファイル（CitrixOnlinePluginWeb.exe）をこのディレクトリに置きます。

デフォルトでは、クライアントインストールファイルのファイル名はXenAppまたはXenDesktopのインストールメディアで提供されているファイル名と同じであると仮定しています。 クライアントのインストールファイルをCitrixのWebサイトからダウンロード、または古いバージョンのクライアントソフトウェアを展開する場合は、XenApp Webサイトの構成ファイルでClientIcaLinuxX86、ClientIcaMac、ClientIcaSolarisSparc、ClientIcaSolarisX86、ClientIcaWin32、およびClientStreamingWin32パラメーターに対して適切なクライアントインストールファイル名が指定されているかチェックします。

4. クライアントインストールファイルを上記のディレクトリ構造内にコピーしたら、Webサーバーを再起動します。

   Webベースのクライアントインストールを実行するようにXenApp Webサイトを構成している場合は、それを必要とするユーザーにクライアントが提供されます。

クライアント展開およびインストールキャプションの構成

更新日： 2014-11-24

Web Interfaceでは、Citrixのクライアントを検出して展開するための機能を提供しています。この機能により、ユーザーは自分の環境に適したCitrixのクライアントをインストールして、必要に応じてWebブラウザーを再構成できます。

クライアント検出および展開処理をユーザーが実行できるようにするには、3つの方法があります。

- 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。 クライアント検出および展開処理が自動的に開始され、リソースへのアクセスに適したCitrixのクライアントを識別してインストールすることができます。 一部のプラットフォームでは、既存のクライアントの有無も検出され、必要な場合にのみクライアントのインストールを求めるメッセージが表示されます。

- 管理者は、オンラインリソースにアクセスするときに使用するクライアントをユーザーが選択できるように設定できます。 これにより、［設定］画面に［クライアント検出の実行］ボタンが追加され、ユーザーはクライアントの検出と展開処理を手動で実行できるようになります。

- 管理者は、リンクを設定したインストールキャプションをユーザーの［メッセージ］画面に表示できます。 ユーザーがこのリンクをクリックすると、クライアント検出および展開処理が開始されます。

ユーザーがXenApp Webサイトにアクセスすると、Webベースのクライアント検出および展開処理により、適切なCitrixのクライアントがユーザーのコンピューターにインストールされているかどうかが検出されます。 ユーザーがクライアントの自動検出および展開が構成されているXenApp Webサイトにログオンする前に、クライアント検出および展開処理が自動的に開始され、リソースへのアクセスに適したCitrixのクライアントを識別してインストールし、必要に応じてWebブラウザーを再構成できます。

また、ユーザーは［メッセージ］画面に表示されるリンクを使って、クライアント検出および展開処理を実行することもできます。 ユーザーがこのリンクをクリックすると、クライアント検出および展開処理が開始されます。 このリンクを、インストールキャプションと呼びます。

インストールキャプションは、適切なクライアントをインストールしていないユーザーだけに表示させることができます。また、既にクライアントをインストール済みのユーザーはこのキャプションを使って新しいバージョンのクライアントへアップグレードしたり、機能の優れた別の種類のCitrixのクライアントを検出して展開したりできます。

Citrix Web Interface管理コンソールの［クライアントの展開］タスクを使って、ユーザーがクライアント検出および展開処理にアクセスできる環境を指定できます。

クライアント展開およびインストールキャプションを構成するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。

3. ［操作］ペインで［クライアントの展開］をクリックします。 オンラインアプリケーションのみを公開するサイトの場合、［ネイティブクライアント］チェックボックスをオンにして、［プロパティ］をクリックします。

4. ［クライアント検出］をクリックします。

5. 適切なCitrixのクライアントをインストールしていないユーザーが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を開始する場合は、［ログオン時にクライアント検出を実行する］チェックボックスをオンにします。

6. クライアント検出および展開処理により新しいバージョンのクライアントをXenApp Webサイトからダウンロードできることが検出された場合、ユーザーにクライアントのアップグレードを求めるメッセージを表示するには、［クライアントのアップグレードを要求する］チェックボックスをオンにします。

7. 次のいずれかを選択して、ユーザーにインストールキャプションをいつ表示するかを指定します。

   - 適切なクライアントを検出できない場合、またはより適したクライアントを利用できる場合にユーザーにそれを通知するには、［クライアントが必要なとき］を選択します。 これがデフォルトの設定です。

   - 適切なクライアントを検出できない場合にのみユーザーにそれを通知するには、［リソースにアクセスできないときのみ］を選択します。

   - いずれの状況においてもインストールキャプションを表示しない場合は、［通知しない］を選択します。

ICAファイルの署名機能の構成

更新日： 2014-12-02

Web Interfaceでは生成されるICAファイルを選択した証明書でデジタル署名して、そのファイルが組織内から送信されたことを互換性のあるCitrixのクライアントとプラグインで検証できます。

ICAファイルの署名機能を使用するには、次のコンポーネントが必要です。

- Web Interface 5.4以降
- Merchandising Server 1.2以降（クライアントのセキュリティポリシーを管理しない展開環境の場合）
- グループポリシーオブジェクト（クライアントのセキュリティポリシーを管理する展開環境の場合）
- Windows Server 2003以降の管理用テンプレート

次の一覧の上位のオプションから順にお勧めします。

- 周知の証明機関（VeriSignなど）からコード署名証明書またはSSL署名証明書を購入する。
- 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。
- Web InterfaceまたはDazzleのサーバー証明書などの既存のSSL証明書を使用する。
- 新しいルート証明書を作成して、グループポリシーオブジェクトでクライアントに配布する。

証明書は、次の要件を満たしている必要があります。

- 証明書に秘密キーが含まれている。
- 証明書の有効期間が無期限である。
- 次のいずれかが真である。
    - 証明書にキー使用法または拡張キー使用法フィールドがない。
    - キー使用法フィールドで、キーをデジタル署名に使用することが許可されている。
    - 拡張キー使用法フィールドが、［コード署名］または［サーバー認証］に設定されている。

Web Interfaceにより、SHA-1またはSHA-256ハッシュアルゴリズムを使用してICAファイルが署名されます。 SHA-256ハッシュアルゴリズムは新しくセキュリティの高いアルゴリズムですが、Windows 2008以降のサーバーとWindows Vista以降のクライアントでのみサポートされます。 SHA-1ハッシュアルゴリズムは、サポートされるすべてのサーバーおよび

クライアントのオペレーティングシステムで使用できます。

ICAファイル署名機能は、Client for Java、RDPクライアント、Citrix Offline Plug-in、およびネットワーク共有からダウンロードする公開ドキュメントでは使用できません。

ICAファイルの署名機能を有効にするには、ユーザーがネイティブクライアントを使用することとオンラインアプリケーションを表示することをサイトに構成して、WebinterfaceのEnableLegacyIcaClientSupportをOffに設定する必要があります。

Citrix Online Plug-inのためにに関する詳しくは、Citrix Merchandising Serverのドキュメントを参照してください。

Web Interface管理コンソールでICAファイルの署名機能を有効にするには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。
3. ［操作］ペインで［クライアントの展開］をクリックします。
4. ［ICAファイル署名］をクリックします。
5. ［ICAファイル署名を有効にする］チェックボックスをオンにして、ボックスの一覧から証明書を選択します。 必要な証明書が一覧にない場合、［インポート］をクリックして個人証明書ストアに証明書をインポートします。
6. Windows Server 2008以降を実行する場合は、使用するハッシュアルゴリズムを選択できます。 そうでなければ、SHA-1が使用されます。 Windows Server 2003でICAファイルの署名機能を構成した後は、コンピューターを再起動する必要があります。

ストリーム配信セッションの監視の構成

Citrix Web Interface管理コンソールの［クライアントの展開］タスクを使用して、Citrix管理者はユーザーのセッション情報をチェックできるようにWeb Interfaceを構成できます。セッションの情報は、Citrix Offline Plug-inとの通信を提供するURLを使って表示されます。通常、このURLは自動的に検出されますが、 クライアント側でプロキシ機能を使用している場合などは、使用するURLを手動で指定する必要があります。

セッション情報は、デリバリーサービスコンソールに表示されます。 複数のサーバーファームのすべてのユーザーセッションの情報を表示したり、特定のアプリケーションやサーバーのセッション情報、および特定のユーザーのセッションやアプリケーションの情報を表示したりできます。

ストリーム配信セッションの監視を構成するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。
3. ［操作］ペインで［クライアントの展開］をクリックします。
4. ［Citrix Offline Plug-in］をクリックします。
5. Web InterfaceがCitrix Offline Plug-inとどのように通信するかを選択します。 次のいずれかを選択します。
   - Citrix Offline Plug-inとの通信に使用されるセッションURLを自動的に検出する場合は、［セッションURLを自動検出する］を選択します。
   - 特定のセッションURLを指定する場合は、［セッションURLを指定する］を選択して、指定するURLを入力します。

リモートデスクトップ接続ソフトウェアの展開

リモートデスクトップ接続（RDP）機能は、Internet Explorerが動作する32ビットのWindowsシステム環境で使用できます。 Microsoftリモートデスクトップ接続（RDP）ソフトウェアのVersion 6.0（Windows XP Service Pack 3に付属）以降をインストールしているユーザーは、これを使ってリソースにアクセスできます。 ほかのクライアントソフトウェアを使用できない場合、クライアントの検出と展開処理によりリモートデスクトップ接続（RDP）ソフトウェアが使用可能かどうかがチェックされ、必要に応じてターミナルサービスActiveXコントロールが有効になります。 単にオンラインアプリケーションを提供するサイトに対してのみ、リモートデスクトップ接続（RDP）ソフトウェアを使用できます。

注： Internet Explorerで、XenApp Webサイトがローカルイントラネットまたは信頼済みゾーンに追加されていない場合には、エラーメッセージが表示されます。 ユーザーには、Web Interfaceのクライアント検出および展開処理により、適切なWindowsセキュリティゾーンにXenApp Webサイトを追加する方法が示されます。

Client for Javaの配布

低帯域幅ネットワーク上でCitrixのクライアントを配布する場合、またはユーザーがどのプラットフォームを使用するかがわからない場合は、ユーザーにClient for Javaを配布することを検討します。 Client for Javaは、クロスプラットフォーム互換のJavaアプレットであり、Web Interfaceサーバーを使用してユーザーのJava互換のWebブラウザーに配布できます。

Client for Javaは、ユーザー環境、デバイス、オペレーティングシステム、およびWebブラウザーを広範囲にサポートしているため、ネイティブクライアントを使用できない環境での次善の策として使用できます。 管理者は、クライアントの検出および展開処理を構成して、ネイティブクライアントをインストールしていないユーザーやXenApp Webサイトからインストールが必要なクライアントのダウンロードを実行できないユーザーに対して、Client for Javaを提供できます。

ユーザーにClient for Javaを配布できるようにするには、このプラグインがXenApp WebサイトのClientsフォルダーに格納されている必要があります。

Client for Javaへのフォールバックを構成するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。

3. ［操作］ペインで［クライアントの展開］をクリックします。 オンラインアプリケーションのみを公開するサイトの場合、［ネイティブクライアント］チェックボックスをオンにして、［プロパティ］をクリックします。

   注： フォールバック機能を提供するために、ここでClient for Javaを使用できるよう設定する必要はありません。

4. ［フォールバック動作］をクリックします。

5. 次のいずれかのオプションを選択して、ネイティブクライアントがインストールされていないユーザーにClient for Javaを提供するときの設定を指定します。

   - ネイティブクライアントをインストールしていないユーザーに適切なCitrixのクライアントをダウンロードおよびインストールさせる場合は、［ネイティブクライアントを配布する］を選択します。 これがデフォルトの設定です。

   - ネイティブクライアントをインストールしていないユーザーにClient for Javaを提供し、Client for Javaを使用できない場合にのみネイティブクライアントのインストールを求める場合は、［ネイティブクライアントを配布し、ネイティブクライアントとClient for Javaの選択をユーザーに許可する］を選択します。

   - ネイティブクライアントをインストールしていないユーザーに、Client for Javaに加えて適切なクライアントのインストールを求めるメッセージを表示する場合は、［Client for Javaへ自動的にフォールバックする］を選択します。

Client for Javaの配布のカスタマイズ

更新日： 2014-11-25

Client for Javaの配布パッケージに含めるコンポーネントを構成することができます。

Client for Javaのサイズは、パッケージにどのコンポーネントを含めるかにより異なります。 パッケージに含めるコンポーネントが少ないほど、サイズが小さくなります（最小サイズは540KB)。 帯域幅が狭い接続を使用しているユーザーのために、必要最低限のコンポーネントだけを含む配布パッケージを設定できます。 または、必要なコンポーネントをユーザー側で選択できるようにすることもできます。 Client for Javaとそのコンポーネントについて詳しくは、Client for Javaのドキュメントを参照してください。

注： Client for Javaの配布パッケージに含めるコンポーネントには、ユーザーのデバイスまたはサーバー上で追加の構成が必要なものもあります。

次の表に、パッケージに含むことができるコンポーネントを示します。

Package	説明
オーディオ	サーバー上で実行中のリソースを有効にして、ユーザーのコンピューターにインストールされているサウンドデバイスを介してサウンドを再生できます。 サーバー上でクライアントオーディオマッピングにより使用される帯域幅の量を制御するには、Citrixユーザーポリシーを構成します。
クリップボード	オンラインリソースとユーザーデバイス上でローカルに実行されているアプリケーション間で、文字列やグラフィックのコピーが可能になります。
ローカルテキストエコー	ローカルテキストエコー機能を有効にすると、速度の遅い接続でのセッションで、入力文字がフィールド内に高速に表示されます。
SSL/TLS	SSLおよびTLSを使って通信を保護します。 SSLおよびTLSでは、サーバーの認証、データストリームの暗号化、およびメッセージの整合性チェックが提供されます。
暗号化	強力な暗号化を提供して、Citrixのクライアントコネクションの機密性を高めます。
クライアント側ドライブのマッピング	セッション内でローカルのドライブにアクセスできるようにします。 ユーザーがサーバーに接続すると、フロッピーディスク、ネットワークドライブ、CD-ROMドライブなどのクライアント側のドライブが自動的にマッピングされます。 ユーザーは、セッション内で各自のローカルファイルにアクセスして、それらをセッションで編集し、ローカルドライブやサーバー上のドライブに保存することができます。 この設定を有効にするには、Client for Javaの［設定］ダイアログボックスでもクライアントドライブマッピングを構成する必要があります。 詳しくは、Client for Javaのドキュメントを参照してください。

プリンターマッピング	セッション内で、ローカルプリンターまたはネットワークプリンターに出力できるようになります。
構成UI	Client for Javaの［設定］ダイアログボックスを有効にします。 ユーザーは、このダイアログボックスを使ってClient for Javaを構成できます。

Client for JavaのVersion 9.xでのプライベートルート証明書の使用

Microsoft証明書サービスを使って発行した独自の証明書など、プライベート証明機関から取得したサーバー証明書を使用するようにCitrix Secure GatewayまたはSSL Relayサービスを構成した場合は、各ユーザーのデバイスのJavaキーストアにルート証明書をインポートする必要があります。 詳しくは、Client for Javaのドキュメントを参照してください。

セキュアなアクセスの管理

Web Interfaceサイトを作成すると、デフォルトで直接アクセス用に構成されます。つまり、すべてのCitrixのクライアントにWebサーバーの実際のアドレスが提供されます。 ただし、Access Gateway、Secure Gateway、またはファイアウォールを使用している環境では、Citrix Web Interface管理コンソールの［セキュアなアクセス］タスクを使ってWeb Interfaceを適切に構成できます。 また、異なるユーザーのグループに対しては異なるアクセス方法を構成できます。 たとえば、企業LANでログオンする社内ユーザーに対しては直接アクセスを構成し、インターネットを介してログオンする外部ユーザーはAccess Gatewayを介してWeb Interfaceにアクセスします。

ここでは、［セキュアなアクセス］タスクを使ったアクセス設定の指定、アドレス変換の変更、およびゲートウェイ設定の構成の方法について説明します。

直接アクセスルートを構成するには

特定のCitrixのクライアントセットに対してサーバーの実際のアドレスを提供する場合は、Citrix Web Interface管理コンソールの［セキュアなアクセス］タスクを使ってユーザーデバイスアドレスとマスクを指定できます。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで［セキュアなアクセス］をクリックします。

4. ［アクセス方法の指定］ページで［追加］をクリックして新しいアクセスルートを追加するか、一覧からエントリを選択して［編集］をクリックし、既存のルートを編集します。

5. ［アクセス方法］の一覧から［直接］を選択します。

6. クライアントネットワークを識別するためのネットワークアドレスとサブネットマスクを入力します。

7. ［ユーザーデバイスのアドレス］の一覧で、［上に移動］および［下に移動］ボタンを使ってアクセスルートの優先順位を指定します。

代替アドレスを構成するには

特定のCitrixのクライアントセットに対してサーバーの代替アドレスを提供する場合は、Citrix Web Interface管理コンソールの［セキュアなアクセス］タスクを使ってユーザーデバイスアドレスとマスクを指定できます。 サーバーに代替アドレスを構成して、ファイアウォールでネットワークアドレス変換を行うように構成する必要があります。

注： 代替アドレスを使用する場合、XenDesktop仮想デスクトップにはアクセスできなくなります。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。
3. ［操作］ペインで［セキュアなアクセス］をクリックします。
4. ［アクセス方法の指定］ページで［追加］をクリックして新しいアクセスルートを追加するか、一覧からエントリを選択して［編集］をクリックし、既存のルートを編集します。
5. ［アクセス方法］の一覧から［代替］を選択します。
6. クライアントネットワークを識別するためのネットワークアドレスとサブネットマスクを入力します。
7. ［ユーザーデバイスのアドレス］の一覧で、［上に移動］および［下に移動］ボタンを使ってアクセスルートの優先順位を指定します。

内部ファイアウォールアドレス変換を構成するには

展開環境内でファイアウォールを使用している場合、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、サーバーが代替アドレスを使って構成されていない場合は、Citrixのクライアントに代替アドレスを提供するようにWeb Interfaceを構成できます。 これを実行するには、Citrix Web Interface管理コンソールの［セキュアなアクセス］タスクを使用します。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで［セキュアなアクセス］をクリックします。

4. ［アクセス方法の指定］ページで［追加］をクリックして新しいアクセスルートを追加するか、一覧からエントリを選択して［編集］をクリックし、既存のルートを編集します。

5. ［アクセス方法］の一覧から［変換］を選択します。

6. クライアントネットワークを識別するためのネットワークアドレスとサブネットマスクを入力します。 ［ユーザーデバイスのアドレス］の一覧で、［上に移動］および［下に移動］ボタンを使ってアクセスルートの優先順位を指定して、［次へ］をクリックします。

7. ［アドレス変換の指定］ページで［追加］をクリックして新しいアドレス変換を追加するか、一覧からエントリを選択して［編集］をクリックし、既存のルートを編集します。

8. ［アクセスの種類］で、次のいずれかを選択します。

   - Citrixのクライアントで変換アドレスを使用してサーバーに接続する場合は、［ユーザーデバイスルート変換］を選択します。

   - ［ユーザーデバイスのアドレス］の一覧でゲートウェイ変換ルートを構成済みで、クライアントおよびゲートウェイサーバーの両方で変換アドレスを使用してサーバーに接続する場合は、［ユーザーデバイスおよびゲートウェイルート変換］を選択します。

9. 内部および外部（変換済み）のポートとサーバーのアドレスを入力します。 サーバーに接続しているクライアントは外部ポート番号とアドレスを使用します。 作成するマッピングは、サーバーにより使用されているアドレスの種類と一致する必要があります。

ゲートウェイ設定を構成するには

更新日： 2014-11-25

環境でAccess GatewayまたはSecure Gatewayを使用している場合は、これらのゲートウェイに対応するようにWeb Interfaceを構成する必要があります。 これを実行するには、Citrix Web Interface管理コンソールの［セキュアなアクセス］タスクを使用します。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで［セキュアなアクセス］をクリックします。

4. ［アクセス方法の指定］ページで［追加］をクリックして新しいアクセスルートを追加するか、一覧からエントリを選択して［編集］をクリックし、既存のルートを編集します。

5. ［アクセス方法］の一覧で、次のいずれかを選択します。

   - サーバーの実際のアドレスをゲートウェイに提供する場合は、［ゲートウェイ直接］を選択します。

   - XenAppサーバーの代替アドレスをゲートウェイに提供する場合は、［ゲートウェイ代替］を選択します。 この場合、XenAppサーバーに代替アドレスを構成し、ファイアウォールでネットワークアドレス変換を行うように構成する必要があります。

     注： 代替アドレスを使用する場合、XenDesktop仮想デスクトップにはアクセスできなくなります。

   - Web Interfaceに設定されているアドレス変換のマッピングに基づいたアドレスをゲートウェイに提供する場合は、［ゲートウェイ変換］を選択します。

6. クライアントネットワークを識別するためのネットワークアドレスとサブネットマスクを入力します。 ［ユーザーデバイスのアドレス］の一覧で、［上に移動］および［下に移動］ボタンを使ってアクセスルートの優先順位を指定して、［次へ］をクリックします。

7. ゲートウェイアドレス変換を使用しない場合は、手順10.に進みます。 ゲートウェイアドレス変換を使用している場合は、［アドレス変換の指定］ページで［追加］をクリックして新しいアドレス変換を追加するか、一覧からエントリを選択して［編集］をクリックし既存のアドレス変換を編集します。

8. ［アクセスの種類］で、次のいずれかを選択します。

   - ゲートウェイで変換アドレスを使用してサーバーに接続する場合は、［ゲートウェイルート変換］を選択します。

   - ［ユーザーデバイスのアドレス］の一覧でゲートウェイ変換ルートを構成済みで、Citrixのクライアントおよびゲートウェイの両方で変換アドレスを使用してサーバー

に接続する場合は、［ユーザーデバイスおよびゲートウェイルート変換］を選択します。

9. 内部および外部（変換済み）のポートとサーバーのアドレスを入力し、［OK］をクリックします。 ゲートウェイでCitrixのサーバーに接続する場合、外部ポート番号とアドレスを使用します。 作成するマッピングは、サーバーファームにより使用されているアドレスの種類と一致する必要があります。 ［次へ］をクリックします。

10. ［ゲートウェイ設定の指定］ページで、クライアントが使用するゲートウェイの完全修飾ドメイン名（FQDN）とポート番号を指定します。 このFQDNは、ゲートウェイにインストールされている証明書のFQDNと同じでなければなりません。

11. クライアントが自動的に再接続を実行する間に切断したセッションを開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。

12. セッション画面の保持を有効にして、2つのSecure Ticket Authority（STA）からの同時チケットを使用する場合、［2つのSTAからチケットを要求する］チェックボックスをオンにします。 このオプションを有効にすると、Web Interfaceは2つのSTAからチケットを取得して、一方のSTAがセッション中に使用できなくなってもユーザーセッションが中断されません。 Web InterfaceがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。 ［次へ］をクリックします。

    注： この機能を使うには、Access Gatewayを展開する必要があります。 Secure Gatewayは現在、複数の冗長STAをサポートしていません。

13. ［Secure Ticket Authority設定の指定］ページで［追加］をクリックして、Web Interfaceが一覧内のエントリを使用または選択できるSecure Ticket Authority（STA）のURLを指定するか、一覧のエントリを選択して［編集］をクリックし既存のSTAの詳細を編集します。 Secure Ticket Authorityは、http[s]://servername.domain.com/scripts/ctxsta.dllのようにCitrix XML Serviceに含まれています。 フォールトトレランス用に複数のSecure Ticket Authorityを指定できますが、外部の負荷分散装置を使用することは推奨されません。 ［上に移動］および［下に移動］ボタンを使ってSTAを優先順位で並べ替えます。

14. ［負荷分散を使用する］チェックボックスで、Secure Ticket Authority間の負荷分散を有効にするかどうかを指定します。 負荷分散を有効にすることによって、サーバー間の接続負荷を均等に分散させることができ、その結果、負荷限界状態になるサーバーがなくなります。

15. 到達できないSTAを無視する時間の長さを［接続できないサーバーを無視する期間］に指定します。 Web Interfaceは、［Secure Ticket Authority URL］の一覧にあるサーバー間でフォールトトレランスを実行します。そのため通信エラーが生じると、障害の発生したサーバーは指定した期間使用されなくなります。

デフォルトのアクセス方法を構成するには

このタスクで設定する［ユーザーデバイスのアドレス］の一覧の表示順に基づいて、規則が適用されます。 ユーザーデバイスのアドレスが、明示的に定義されている規則と一致しない場合は、デフォルトの規則が適用されます。 サイトを作成するときは、直接アクセス用にデフォルトのルートが自動的に構成されます。 Citrix Web Interface管理コンソールの［セキュアなアクセス］タスクを使って環境に対するデフォルトのアクセス方法を指定できます。

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで［セキュアなアクセス］をクリックします。

4. ［アクセス方法の指定］ページで、一覧から［デフォルト］と指定されているエントリを選択し、［編集］をクリックします。

5. ［アクセス方法］の一覧で、次のいずれかを選択します。

   - サーバーの実際のアドレスをCitrixのクライアントに提供する場合は、［直接］を選択します。

   - XenAppサーバーの代替アドレスをクライアントに提供する場合は、［代替］を選択します。 この場合、XenAppサーバーに代替アドレスを構成し、ファイアウォールでネットワークアドレス変換を行うように構成する必要があります。

     注： 代替アドレスを使用する場合、XenDesktop仮想デスクトップにはアクセスできなくなります。

   - Web Interfaceに設定されているアドレス変換のマッピングに基づいたアドレスをクライアントに提供する場合は、［変換］を選択します。

   - サーバーの実際のアドレスをゲートウェイに提供する場合は、［ゲートウェイ直接］を選択します。

   - XenAppサーバーの代替アドレスをゲートウェイに提供する場合は、［ゲートウェイ代替］を選択します。 この場合、XenAppサーバーに代替アドレスを構成し、ファイアウォールでネットワークアドレス変換を行うように構成する必要があります。

     注： 代替アドレスを使用する場合、XenDesktop仮想デスクトップにはアクセスできなくなります。

   - Web Interfaceに設定されているアドレス変換のマッピングに基づいたアドレスをゲートウェイに提供する場合は、［ゲートウェイ変換］を選択します。
6. クライアントネットワークを識別するためのネットワークアドレスとサブネットマスクを入力します。 ［ユーザーデバイスのアドレス］の一覧で、［上に移動］および［下に

移動］ボタンを使ってアクセスルートの優先順位を指定します。

7. アドレス変換またはゲートウェイを使用している環境では、［次へ］をクリックし、デフォルト構成に対して適切な設定を指定します。 詳しくは、「内部ファイアウォールアドレス変換を構成するには」および「ゲートウェイ設定を構成するには」を参照してください。

クライアント側のプロキシ設定の編集

Web Interface環境のクライアント側でプロキシサーバーを使用している場合は、Citrixのクライアントが XenAppまたはXenDesktopの実行サーバーと通信するときにプロキシサーバーを使用することを要件にするかどうかを構成できます。 Citrix Web Interface管理コンソールの［クライアント側のプロキシ］タスクを使用してこれを実行します。

Web Interface環境のクライアント側でプロキシサーバーを使用すると、次のようなセキュリティ上の利点があります。

- ファイアウォール内のシステム名が、DNSを介してファイアウォールの外側に漏れることがないため、情報を保護できます。

- 1つの接続を介して、複数のTCP接続をチャネル化できます。

Citrix Web Interface管理コンソールでは、Citrixのクライアントのデフォルトのプロキシ規則を設定できます。 ただし、ユーザーデバイスごとにこの動作に対する例外を構成することもできます。 例外を構成するには、プロキシサーバーの外部IPアドレスをWeb Interfaceのプロキシ設定に関連付けます。

また、プロキシ動作がクライアントによって制御されるように指定することもできます。 たとえば、XenAppおよびXenDesktopのSecure Proxy機能を使用するには、プラグイン側で指定されているプロキシ設定を使用するようにWeb Interfaceを構成し、クライアントのSecure Proxy機能を有効にします。 Citrixのクライアントを使ってプロキシ動作を制御する方法については、使用するクライアントのドキュメントを参照してください。

デフォルトのプロキシを構成するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで［クライアント側のプロキシ］をクリックします。

4. ［追加］をクリックして新しいマッピングを作成するか、一覧からエントリを選択して［編集］をクリックし、既存のマッピングを編集します。

5. ［IPアドレス］および［サブネットマスク］にそれぞれ、プロキシの外部アドレスとユーザーデバイスのサブネットマスクを入力します。

6. ［プロキシ］の一覧から、次のいずれかを選択します。

   - CitrixのクライアントでユーザーのWebブラウザーで構成されているWebプロキシを自動的に検出する場合は、［ユーザーのブラウザー設定］を選択します。

   - Webプロキシ自動検出プロトコル（WPAD）でWebプロキシを自動的に検出する場合は、［Webプロキシ自動検出］を選択します。

   - ユーザーがクライアントに構成したプロキシを使用する場合は、［クライアントの定義］を選択します。

   - SOCKSプロキシサーバーを使用する場合は、［SOCKS］を選択します。 このオプションを選択した場合は、プロキシサーバーのアドレスとポート番号を入力する必要があります。 プロキシアドレスとしては、IPアドレスまたはDNS名を指定できます。

   - Secureプロキシサーバーを使用する場合は、［Secure（HTTPS）］を選択します。 このオプションを選択した場合は、プロキシサーバーのアドレスとポート番号を入力する必要があります。 プロキシアドレスとしては、IPアドレスまたはDNS名を指定できます。

   - プロキシを使用しない場合は、［なし］を選択します。
7. 複数のマッピングを入力した場合は、［上に移動］および［下に移動］ボタンを使って表内のエントリを並べ替えます。この順番に従ってマッピングが使用されます。

ユーザーページの外観のカスタマイズ

Webページに表示されるユーザーインターフェイスの外観をカスタマイズして、たとえば固有の「外観と操作性」を備えたサイトを作成できます。

Web Interface管理コンソールの［Webサイトの外観］タスクを使って、つぎのカスタマイズを実行します。

- レイアウト。 ユーザーに提供するコントロールを指定して、Webサイトの表示方法を定義します。 マシンの追加方法
    - XenApp Webサイトのレイアウトとしては［自動］、［背景イメージをすべて表示］、［背景イメージを限定して表示］を選択できます。 背景イメージを限定して表示するユーザーインターフェイスは、小型デバイスや低速ネットワーク接続を使用してリソースにアクセスするユーザーを対象としたコンパクトなユーザーインターフェイスです。 ［自動］を選択すると、ユーザーのコンピューターの画面サイズに適したサイトレイアウトがシステムにより選択されます。
    - 検索やヒントの表示など、ユーザーが［アプリケーション］画面で設定できる機能やコントロールを構成し、ユーザーによる画面のカスタマイズを許可するかどうかを指定します。
    - ［背景イメージをすべて表示］ビューおよび［背景イメージを限定して表示］ビューにおいて、ユーザーリソースセットに対するデフォルトのビュースタイルを設定します。 また、ユーザーがどのビュースタイルを使用できるかを指定できます。
    - ユーザーの［アプリケーション］画面でリソースをどのようにグループ化するのかを指定します。 アプリケーション、コンテンツ、およびデスクトップを個別のタブで表示したり、すべてのリソースを一緒に単一のタブに統合したりできます。
- 外観。 サイト全体で使用されるイメージや色を設定して、ユーザーインターフェイスの「外観と操作性」をカスタマイズします。 マシンの追加方法
    - ユーザーの［ログオン］画面のスタイルを指定します。 適切なログオンフィールドのみが表示される最小レイアウトと、［メッセージ］や［設定］画面にアクセスできるナビゲーションバー付きのレイアウトのいずれかを選択します。
    - ［背景イメージをすべて表示］ビューおよび［背景イメージを限定して表示］ビューに対してカスタマイズしたサイトイメージを指定し、またオプションでそのイメージにハイパーリンクを設定します。 また、サイトのヘッダー領域に表示される背景イメージを変更したり、特定の色を使用したりできます。
- コンテンツ。 メッセージや画面の文字列を変更し、ユーザーがサイトにアクセスした場合に使用する可能性がある言語を指定します。 ユーザーの［ログオン］画面および［アプリケーション］画面のページタイトルやメッセージ、およびすべての画面に共通で表示されるフッター文字列を指定できます。 さらに、ユーザーがログオン前に受け入れる必要がある警告メッセージを構成できます。

リソースショートカットおよび更新オプションの管理

更新日： 2014-11-24

Citrix Web Interface管理コンソールの［ショートカット］タスクを使ってCitrix Online Plug-inがリソースのショートカットをどのように表示するかを指定します。

以下の種類のショートカットを作成できます。

- ［スタート］メニューショートカット： ［ショートカット］タスクで指定する設定、XenAppおよびXenDesktopでリソースを公開するときに定義する設定、およびその両方を使用できます。 ［スタート］メニューでのショートカットの表示方法を定義し、その設定をユーザーが指定できるようにすることもできます。 また、［すべてのプログラム］メニューのショートカットやサブメニューを作成したり、ユーザーがサブメニューの名前を指定できるようにしたりすることもできます。

- Desktop ［ショートカット］タスクで指定する設定、XenAppおよびXenDesktopでリソースを公開するときに定義する設定、およびその両方を使用できます。 デスクトップでのショートカットの表示方法を定義し、その設定をユーザーが指定できるようにすることもできます。 また、カスタムフォルダー名を作成したり、ユーザーが名前を選択できるようにしたりすることができます。

- 通知領域： ユーザーが選択できるようにするオプションを有効にします。通知領域にリソースを表示したり、ユーザーがリソースの表示方法を指定できるようにしたりすることができます。

［ショートカット］タスクでは、ショートカットの削除を設定することもできます。 ショートカットを削除するタイミング（Citrix Online Plug-inを閉じる時またはユーザーがXenAppからログオフした時）や、Windows CEまたはLinuxを実行するユーザーの場合は、Citrix Online Plug-inショートカットに加えてユーザー作成のショートカットを削除するかどうかを指定できます。 Citrix Online Plug-inおよびユーザー作成ショートカットの削除を選択すると、検索するフォルダー階層を制限してパフォーマンスを向上させることができます。

リソース更新オプションの指定

Citrix Web Interface管理コンソールで［リソースの更新］タスクを使って、ユーザーのリソースの一覧をいつ更新するのか、またこれらの設定のカスタマイズをユーザーに許可するかどうかを指定します。 管理者は、ユーザーがCitrix Online Plug-inを起動したとき、またはリソースにアクセスしたときに一覧が更新されるように設定できます。また、更新頻度も指定できます。

セッション基本設定の管理

Citrix Web Interface管理コンソールの［セッション設定］タスクを使ってユーザーが変更できる設定を指定します。 また、アクティブでないユーザーがWeb Interfaceからログオフされる時間と、オンラインリソースのクライアントの場合にWeb Interfaceでユーザーデバイス名を上書きするかどうかも指定できます。

XenApp Webサイトの場合、ユーザーセッションに対して次の設定を構成できます。

- ユーザーによるカスタマイズ。 キオスクモードの有効/無効を設定し、［アプリケーション］画面に［設定］ボタンを表示するかどうかを指定します。
- Webセッション。 アクティブでないユーザーがWeb Interfaceからログオフされる時間を指定します。
- 固定URL。 ユーザーがサイトへのアクセスにブラウザーのブックマーク機能を使用できるかどうかを指定します。
- 接続パフォーマンス。 事前設定のデフォルト値を指定するか、帯域幅の制御、色数、音質、およびプリンターマッピング設定のカスタマイズをユーザーに許可するかどうかを指定します。
- 表示。 ホストセッションのウィンドウサイズの変更をユーザーに許可するかどうか、またWeb InterfaceでClearTypeフォントスムージングを使用するかどうかを指定します（ユーザーのWindowsオペレーティングシステム、ユーザーのCitrixのクライアントソフトウェア、およびサーバーファーム側で対応する設定が構成されている場合）。
- ローカルリソース。 Windowsショートカットキーの適用先、PDA同期、およびユーザーフォルダーのリダイレクト機能を構成します。
- ユーザーデバイス名。 オンラインリソースの場合に、Web Interfaceがユーザーデバイス名を上書きするかどうかを指定します。

  重要： Windows用のクライアントVersion 8.xおよび9.xでワークスペースコントロールを使用する場合は、［ユーザーデバイス名を上書きする］チェックボックスをオンにする必要があります。

オンラインリソースを提供するXenApp Servicesサイトの場合、Citrix Web Interface管理の［セッションオプション］タスクを使って次のユーザーセッションを構成できます。

- 表示。 ICAセッションで使用できるようにするウィンドウのサイズを選択します。カスタムサイズをピクセル数または画面に対する割合で定義できます。 また、Web InterfaceでClearTypeフォントスムージングを使用するかどうかを指定します（ユーザーのWindowsオペレーティングシステム、ユーザーのCitrix Online Plug-in、およびサーバーファーム側で対応する設定が構成されている場合）。
- 色数とサウンド。 ユーザーが選択できるようにするオプションを有効にします。
- ローカルリソース。 ユーザーが選択できるWindowsショートカットキーの適用先を指定します。 Windowsショートカットキーは、シームレスウィンドウモードのコネクション

には影響しません。 次の適用先を指定できます。

- ローカルデスクトップ上。 ローカルデスクトップにのみ適用するショートカットキー。これらのショートカットキーはICAセッションに渡されません。
- リモートデスクトップ上。 ICAセッション内の仮想デスクトップに適用するショートカットキー。
- 全画面デスクトップのみ。 ICAセッション内の全画面モードの仮想デスクトップにのみ適用するショートカットキー。

ユーザーフォルダーのリダイレクトを有効にし、これによりユーザーはオンラインリソースでドキュメントまたはデスクトップフォルダーでファイルを開く、閉じる、または保存する場合に、ローカルコンピューター上のフォルダーにリダイレクトされます。 詳しくは、「ユーザーフォルダーのリダイレクト」を参照してください。

- ワークスペースコントロール。 再接続およびログオフ時の動作を構成します。 詳しくは、「ワークスペースコントロールの構成」を参照してください。

帯域幅の制御

帯域幅の制御機能により、接続帯域幅に基づいてユーザーがセッション設定を選択できるようにすることができます。 これらのオプションは、ログオンの前または後に［設定］画面に表示されます。 帯域幅の制御機能では、ウィンドウの色数、音質、プリンターマッピングを調整できます。 さらに、Web Interface管理コンソールを使用して、ユーザーのデフォルト設定またはカスタム設定を指定できます。 ［セッション設定の管理］ダイアログボックスの［接続パフォーマンス］ページを使用して、帯域幅の設定をカスタマイズします。 ［接続速度］ボックスの一覧から［カスタム］を選択すると、［色数の設定］ボックスの一覧、［音質］ボックスの一覧、および［プリンターマッピングを有効にする］チェックボックスを使用できるようになります。

Client for Javaを使用している場合は、帯域幅の制御機能によって、サウンドのサポートおよびプリンターマッピングのパッケージを使用できるかどうかが判断されます。 リモートデスクトップ接続（RDP）ソフトウェアを使用している場合は、音質設定がオンまたはオフにマップされ、それ以外の音質設定は使用できません。 ワイヤレスWAN接続には、狭帯域幅設定が適しています。

注： 帯域幅の制御機能と一緒にリモートデスクトップ接続（RDP）ソフトウェアを使用している場合は、選択した帯域幅に適したパラメーターがWeb Interfaceによって指定されます。 ただし、実際の動作は、使用されるリモートデスクトップ接続（RDP）ソフトウェアのバージョン、ターミナルサーバー、およびサーバー構成に依存します。

デフォルトでは、ユーザーはセッションのウインドウのサイズを調整できます。

ユーザーが設定を調整できないようにした場合は、ユーザーインターフェイスに設定が表示されず、リソース用に指定したサーバーの設定が使用されます。

ClearTypeフォントスムージング

ClearTypeは、Microsoft社により開発されたサブピクセルのアンチエイリアステクノロジーで、液晶モニター上の文字のレンダリングを向上させて、文字をはっきりと滑らかに表示します。 ClearTypeフォントスムージングはWindows XP以降で提供されています。 フォントスムージングは、Windows 7およびWindows Vistaはデフォルトで装備されていますが、Windows XPではオプションとなります。

Web InterfaceおよびCitrix Online Plug-inでは、ICAセッションでのClearTypeフォントスムージングがサポートされます。 Windows XP以降を実行するユーザーがサーバーに接続する場合、プラグインがユーザーのコンピューター上のフォントスムージング設定を自動的に検出してサーバーに送信します。 これにより、同じ設定がセッションに適用されます。

フォントスムージングは、ユーザーのオペレーティングシステム、Citrix Online Plug-in、Web Interfaceサイト、およびサーバーファームで有効にする必要があります。 フォントスムージングを有効にするには、XenApp Webサイトの場合はCitrix Web Interface管理コンソールの［セッション設定］タスクを使用し、XenApp Servicesサイトでは［セッションオプション］タスクを使用します。

フォントスムージングはオンラインリソースにのみ適用されます。 オフラインアプリケーションには適用されません。

ユーザーフォルダーのリダイレクト

更新日： 2014-11-24

ユーザーフォルダーのリダイレクト機能により、サーバー上のWindowsの特殊フォルダーがローカルコンピューター上のフォルダーにマップされるため、ユーザーはオンラインリソースでこれらのフォルダーを簡単に使用できるようになります。 ユーザーフォルダーという用語は、［ドキュメント］、［コンピューター］、［デスクトップ］など、ユーザー固有のWindowsフォルダー（特殊フォルダー）を指すもので、Windowsのバージョンが異なっていても同様のフォルダーが存在します。

注： Windows Vistaよりも前のバージョンのWindowsでは、これらの特殊フォルダーには「マイ」という用語が付いていました。このため、たとえば「ドキュメント」フォルダーはWindow XPの「マイドキュメント」フォルダーに相当します。

ユーザーフォルダーのリダイレクトが無効な場合、セッション内でファイルを開いたり保存したりするときのダイアログボックスに表示される［ドキュメント］や［デスクトップ］などのアイコンは、サーバー上のユーザーフォルダーを示しています。 ユーザーフォルダーのリダイレクトを有効にすると、これらのアイコンへのアクセスがクライアントコンピューター上の各ユーザーフォルダーにリダイレクトされます。このため、ユーザーがファイルをドキュメントフォルダーやデスクトップフォルダーから開いたり保存したりする場合にアクセスするのは、ローカルコンピューター上のフォルダーということになります。 現在、このリダイレクト機能は［ドキュメント］および［デスクトップ］フォルダーのみをサポートしています。

ユーザーフォルダーのリダイレクトはオンラインリソースにのみ適用されます。 オフラインアプリケーションには適用されません。

ユーザーフォルダーのリダイレクトの有効化

XenApp WebサイトおよびXenApp Servicesサイトともにユーザーフォルダーのリダイレクトはデフォルトでは無効になっています。 サイトでユーザーフォルダーのリダイレクトを有効にする場合は、サーバーファーム内の既存のポリシー規則がユーザーによるローカルドライブへのアクセスやローカルドライブへの保存を妨げないようにする必要があります。

ユーザーフォルダーのリダイレクトを有効にするには、XenApp Webサイトの場合はCitrix Web Interface管理コンソールの［セッション設定］タスクを使用し、XenApp Servicesサイトでは［セッションオプション］タスクを使用します。 また、ユーザーが［設定］画面でこの機能を有効にできるかどうかを指定することができます。

ユーザーフォルダーのリダイレクトを有効にする場合、ユーザーがCitrixコネクションセンターの［クライアント側ファイルのセキュリティ］ダイアログボックスで［フルアクセス］を選択して、リソースがローカルファイルおよびフォルダーへの完全な読み取りおよび書き込みアクセスを持つようにする必要があります。 ユーザーは、ほかのデバイスで新しいセッションを始める前に、アクティブなセッションをすべてログオフする必要があります。 複数のデバイスから同時に同じセッションに接続するユーザーに対しては、ユーザーフォルダーのリダイレクトを有効にしないことをお勧めします。

ワークスペースコントロールの構成

ワークスペースコントロール機能を有効にすると、ユーザーは簡単にすべてのリソース（アプリケーション、コンテンツ、およびデスクトップ）から切断したり、切断されたリソースに再接続したり、すべてのリソースからのログオフしたりできます。 これにより、ユーザーが別のデバイスから再ログオンしたときに、ほかのディバイス上で使用していたリソース（切断したリソースおよびアクティブなリソース）に自動的または手作業で再接続できます。 たとえば、病院内の複数のコンピューター間を移動しながら、常に同じリソースセットにアクセスしなければならない医療スタッフをサポートするために、この機能を利用できます。

ワークスペースコントロールの要件

次に、ワークスペースコントロール機能を使用するのに必要な条件と推奨事項を示します。

- ワークスペースコントロール機能をWindows用のクライアントのVersions 8.xおよび9.xで使用するには、Citrix Web Interface管理者コンソールの［セッション基本設定］タスクで［ユーザーデバイス名を上書きする］チェックボックスをオンにする必要があります。

- Citrixセッション内でWeb Interfaceにアクセスしていることが検出されると、ワークスペースコントロール機能は無効になります。

- セキュリティ設定によっては、ユーザーが直接初期化しないファイルのInternet Explorerを介したダウンロードをブロックすることができ、このためネイティブクライアントを使ったリソースへの再接続をブロックすることができます。 再接続できない状況では、警告メッセージが表示され、ユーザーはInternet Explorerのセキュリティ設定を再構成するオプションが表示されます。

- 各Webセッションは、非アクティブの状態が一定時間（通常は20分）続くと、タイムアウトになります。 HTTPセッションがタイムアウトになると、［ログオフ］画面が表示されますが、そのセッションでアクセスまたは再接続したリソースは切断されません。 その場合手動で接続を切断する、ログオフする、またはWeb Interfaceにログオンし直し、［ログオフ］または［切断］をクリックする必要があります。

- Web Interfaceのアカウント情報を信頼するようにCitrix XML Serviceを設定した場合は、匿名ユーザー用のリソースは、匿名ユーザーと認証済みユーザーの両方が接続を切断した時点で終了します。 そのため、ユーザーは、切断後に匿名ユーザー用のリソースに再接続することはできません。

- パススルー認証、スマートカード認証、またはスマートカードパススルー認証を使用するには、Web InterfaceサーバーとCitrix XML Service間に信頼関係を設定する必要があります。 詳しくは、「XenApp Webサイトでのワークスペースコントロールおよび統合された認証方法の併用」を参照してください。

- XenApp Servicesサイトに対してアカウント情報によるパススルー認証が無効に設定されている場合は、スマートカードのユーザーは、Citrixセッションに再接続するたびにPINを入力する必要があります。 これに対し、XenApp Servicesサイトでのパススルー認証またはスマートカードパススルー認証では、アカウント情報によるパススルー認証が有効に設定されているため、再接続時にPINを入力する必要がありません。

ワークスペースコントロールの制限事項

ワークスペースコントロールを有効にする場合は、次の点に注意してください。

- ワークスペースコントロール機能は、オフラインアプリケーションを配信するように構成されたサイトでは使用できません。 デュアルモード配信をサイトに構成する場合は、ワークスペースコントロールはオンラインリソースでのみ実行されます。
- ワークスペースコントロール機能は、Version 8より前の32ビットWindows用のクライアントやリモートデスクトップ接続（RDP）ソフトウェアでは使用できません。 また、この機能は、Citrix Presentation Server Version 4.5以降を実行しているサーバーでのみ動作します。
- ワークスペースコントロールでは、切断されたXenDesktop仮想デスクトップにのみ再接続できます。 中断された仮想デスクトップには再接続できません。

XenApp Webサイトでのワークスペースコントロールおよび統合された認証方法の併用

次のセクションはXenApp Webサイトにのみ当てはまります。 ユーザーがパススルー認証、スマートカード、またはスマートカードパススルー認証を使ってログオンする場合は、Web Interfaceサーバーと、Web Inerfaceでアクセスするcitrix XML Serviceの実行サーバーとの間に信頼関係を設定する必要があります。 Citrix XML Serviceは、XenAppまたはXenDesktopが動作するサーバーとWeb Interfaceとの間でリソースに関する情報をやり取りするための通信インターフェイスとして機能します。 信頼関係を設定しないと、スマートカードまたはパススルー認証を使ってログオンしたセッションでは、［切断］、［再接続］、および［ログオフ］ボタンが正しく動作しません。

ユーザーがサーバーファームによって認証されている場合（ログオン時にスマートカード認証またはパススルー認証を使用していない場合）は、信頼関係を設定する必要はありません。

信頼関係を設定するには

Citrix XML Serviceに送られる要求を信頼するようにサーバーを設定する場合は、次の点を考慮してください。

- 信頼関係を設定すると、ユーザーの認証はWeb Interfaceサーバーによって管理されます。 セキュリティに関わるリスクを回避するには、IPSecやファイアウォールなどの技術を使用して、信頼されるサービスだけがCitrix XML Serviceと通信するようにします。IPSecやファイアウォールなどのセキュリティ技術を使用しないで信頼関係を設定した場合は、どのネットワークデバイスからでもセッションを切断したり終了したりできてしまう危険性があります。 サイトに指定ユーザー認証だけを構成している場合は、信頼関係の設定は不要です。

- 信頼関係は、Web Inerfaceが直接アクセスするサーバー上でのみ有効にします。 これらのサーバーは、Citrix Web Interface管理コンソールの［サーバーファーム］タスクで表示されます。

- Citrix XML ServiceへのアクセスがWeb Interfaceサーバーだけに制限されるように、使用するセキュリティ技術を構成してください。 たとえば、Citrix XML ServiceがIIS（インターネットインフォメーションサービス）とポートを共有している場合に、IISのIPアドレス制限機能を使ってCitrix XML Serviceへのアクセスを制限できます。

1. サーバーファームのサーバーにログオンし、［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrixデリバリーサービスコンソール］の順に選択します。

2. コンソールの左側で、［Citrixリソース］>［XenApp］の順に展開し、サーバーファームのノードを展開して、［ポリシー］をクリックします。

3. コンソールの詳細ペインで、［コンピューター］タブを選択し、［新規］をクリックします。

4. 新しいポリシーの名前と（任意で）説明を入力し、［次へ］をクリックします。

5. ［カテゴリ］の一覧で、［XML Service］をクリックし、［設定］の［XML要求を信頼する］を選択して［追加］をクリックします。

6. ［有効］をクリックして［OK］をクリックします。 ［次へ］をクリックします。

7. 必要な場合はポリシーにフィルターを適用し、そのポリシーが適用される環境を指定して［次へ］をクリックします。

8. ［このポリシーを有効にする］チェックボックスがオンになっていることを確認して、［保存］をクリックします。

Web Interfaceへのログオン時に自動的に再接続するように設定するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで、サイトの種類に合わせて適切なタスクを選択します。

   - XenApp Webサイトでは、［ワークスペースコントロール］をクリックします。

   - XenApp Servicesサイトでは、［セッションオプション］をクリックし、［ワークスペースコントロール］を選択します。
4. ［ログオン時に自動的にセッションに再接続する］チェックボックスをオンにします。

5. 次のいずれかを選択します。

   - 切断したセッションとアクティブなセッションの両方に自動的に再接続するようにするには、［すべてのセッションに再接続する］をクリックします。

   - 切断したセッションだけに自動的に再接続するようにするには、［切断されたセッションにのみ再接続する］をクリックします。
6. ［ユーザーによるカスタマイズを許可する］チェックボックスをオンにすると、 ユーザーがXenApp Webサイトの［設定］画面、またはCitrix Online Plug-inの［オプション］ダイアログボックスでこの設定を変更できるようになります。

［再接続］ボタンを有効にするには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、必要に応じて［XenApp Webサイト］または［XenApp Servicesサイト］をクリックして、結果ペインでサイトを選択します。

3. ［操作］ペインで、サイトの種類に合わせて適切なタスクを選択します。

   - XenApp Webサイトでは、［ワークスペースコントロール］をクリックします。

   - XenApp Servicesサイトでは、［セッションオプション］をクリックし、［ワークスペースコントロール］を選択します。
4. ［再接続ボタンを有効にする］チェックボックスをオンにます。

5. 次のいずれかを選択します。

   - ［再接続］ボタンでアクティブなセッションと切断されたセッションの両方に再接続できるようにするには、［すべてのセッションに再接続する］をクリックします。

   - ［再接続］ボタンで切断されたセッションのみに再接続できるようにするには、［切断されたセッションにのみ再接続する］をクリックします。
6. ［ユーザーによるカスタマイズを許可する］チェックボックスをオンにすると、 ユーザーがXenApp Webサイトの［設定］画面、またはXenApp Servicesの場合はCitrix Online Plug-inの［オプション］ダイアログボックスでこの設定を変更できるようになります。

ログオフ時の動作を構成するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。

2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでサイトを選択します。

3. ［操作］ペインで［ワークスペースコントロール］をクリックします。

4. ［サイトからログオフする場合にアクティブなセッションをログオフする］チェックボックスをオンにすると、ユーザーのログオフ操作により、Web Interfaceおよびすべてのアクティブなセッションからログオフします。 このチェックボックスをオフにすると、ログオフ後もユーザーセッションはアクティブのままになります。

5. ［ユーザーによるカスタマイズを許可する］チェックボックスをオンにすると、ユーザーはサイトの［設定］画面でこの設定を構成できます。

Web Interfaceのセキュリティ構成

総合的なセキュリティを確立するには、リソースを配信するどの過程においてもデータが不正に利用されないようにする必要があります。 ここでは、Web Interfaceの次の通信リンクにおける、Web Interfaceのセキュリティに関わる問題とその対策を示します。

- ユーザーデバイスとWeb Interface間の通信： WebブラウザーとWeb Interfaceサーバー間のデータの受け渡しに関連する問題、および転送中のデータやユーザーデバイスに書き込まれるデータを保護する方法を説明します。
- Web Interfaceとサーバー間の通信： Web Interfaceサーバーとサーバーファーム間の認証情報およびリソース情報を保護する方法を説明します。
- セッションとサーバー間の通信： Citrixのクライアントとサーバー間でのセッション情報の受け渡しに関連する問題について説明します。 また、データなどを保護する、Web InterfaceおよびXenApp/XenDesktopのセキュリティ機能の実装について説明します。

この図は、ユーザーデバイス、XenAppまたはXenDesktopが動作するサーバー、およびWeb Interfaceサーバー間での通信を示しています。

セキュリティに関する一般的な注意事項

ほかのWindowsベースのサーバーの場合と同様に、Windowsサーバーを構成するためのMicrosoft社の標準ガイドラインに従うことをお勧めします。

すべてのコンポーネントに最新の修正プログラムがすべて適用済みであることを常に確認してください。 詳しくは、MicrosoftのWebサイト（http://support.microsoft.com/）を参照して、最新の推奨ダウンロードプログラムについて確認してください。

SSLおよびTLS

更新日： 2014-12-02

Secure Sockets Layer（SSL）は、ネットワーク間で送受信されるデータを保護するためのプロトコルです。 SSLでは、サーバーの認証、データストリームの暗号化、およびメッセージの整合性のチェックを行います。

SSLは、暗号化を使用してメッセージをエンコードし、その識別情報を認証して、コンテンツの整合性をチェックします。 これによって、盗聴、悪意のある経路変更、データの改ざんなどのリスクから保護されます。 SSLでは、識別情報の身元を証明するために、証明機関により発行される公開キー証明書を使用します。 SSL、暗号化、および証明書については、「サーバーファームのセキュリティを保護する」および「組織内ネットワークの保護」の説明を参照してください。

Transport Layer Security

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 Task Force）が、SSLの公開標準規格の開発をNetscape Communications社から引き継いだときに、SSLという名前をTLSに変更しました。 TLSでは、SSLのように、サーバーの認証、データストリームの暗号化、およびメッセージの整合性のチェックを行います。

XenApp for WindowsおよびXenDesktopのすべてのサポートされているバージョンでTLS Version 1.0をサポートします。 SSL Version 3.0は、技術的にはTLS Version 1.0とそれほど変わらないため、インストール時にSSL用に使用したサーバー証明書をTLSでも使用することができます。

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。

注： Web Interface for Java Application Serversでサポートする最大SSL/TLS証明書キーサイズは2048ビットです。

SSL Relay

SSL Relayは、Web Interfaceサーバーとサーバーファーム間の通信データをSSLにより保護するコンポーネントです。 SSL Relayには、TCP/IP接続でのサーバーの認証、データの暗号化、メッセージの整合性チェックなどの機能があります。 SSL Relayは、Citrix XTE Serviceによって提供されています。

SSL Relayは、Web InterfaceサーバーとCitrix XML Service間の通信を仲介するコンポーネントです。 SSL Relayを使用する環境では、まずWebサーバーがSSL Relayサーバー上のサーバー証明書を正規の証明機関の一覧と照合して、SSL Relayサーバーを認証します。

認証が終わると、WebサーバーとSSL Relayはセッションの暗号化の方法をネゴシエートします。 次に、Webサーバーはすべての情報要求を暗号化して、SSL Relayに送信します。 SSL Relayはその要求を解読し、解読した要求をCitrix XML Serviceに渡します。 Citrix XML ServiceからWebサーバーに情報を戻すときは、Citrix XML Serviceがすべての情報をSSL Relayが動作するサーバーを介して送り、このサーバーはデータを暗号化してWebサーバーに転送します。Webサーバーはその情報を解読します。 メッセージの整合性チェックでは、通信情報が不正に変更されていないことを確認します。

ICA暗号化

ICA暗号化を使うと、サーバーとCitrixのクライアント間で送受信される情報を暗号化できます。 これにより、認証されていないユーザーが暗号化された転送データを読み取ることはできなくなります。

ICA暗号化により、盗聴の脅威から機密情報を保護できます。 ただしセキュリティに関するリスクはほかにもあり、暗号化の使用は総合的なセキュリティポリシーの1つの側面でしかありません。 SSLやTLSとは異なり、ICA暗号化はサーバーの認証を行いません。 したがって理論的には、ネットワークを横断するときに情報が傍受されたり、偽装サーバーに経路変更される可能性があります。 また、ICA暗号化は整合性のチェックも行いません。

ICA暗号化は、XenApp for UNIX（日本語版はリリースされていません）では使用できません。

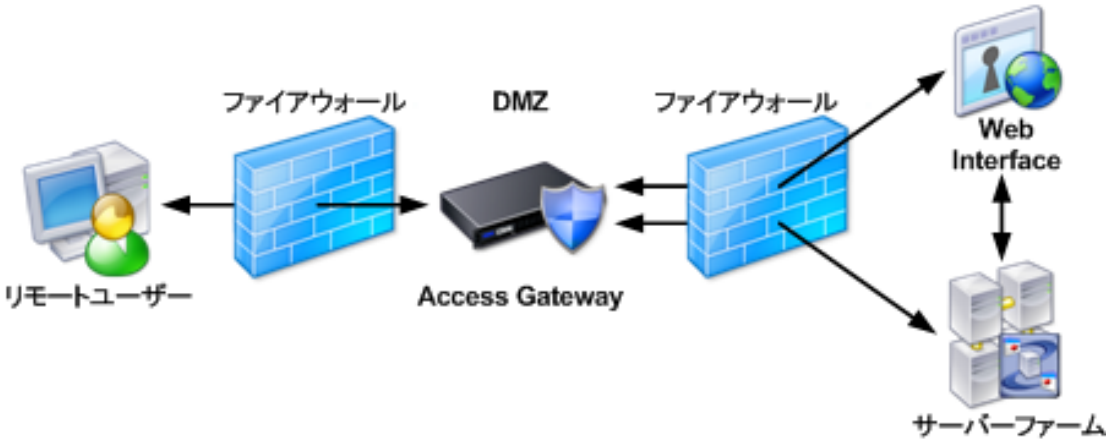
Access Gateway

Access GatewayをWeb InterfaceおよびSecure Ticket Authority（STA）と一緒に使用すると、XenAppまたはXenDesktopが動作するサーバー上のリソース（アプリケーション、コンテンツ、およびデスクトップ）の認証、認可、およびリダイレクトできます。

Access Gatewayは、データや音声などのあらゆる情報リソースに対する安全で単一のポイントからのアクセスを提供するユニバーサルSSL仮想プライベートネットワーク（VPN：Virtual Private Network）アプライアンスです。 Access Gatewayは、あらゆるリソースとプロトコルの暗号化に対応します。

Access Gatewayにより、リモートユーザーは社内で許可されているアプリケーション、コンテンツ、デスクトップ、およびネットワークリソースにシームレスかつ安全にアクセスでき、ファイアウォールの内側で作業しているような感覚で、ネットワークドライブ上のファイルや、電子メール、イントラネットサイト、リソースを利用できます。

この図は、SSL/TLSが有効なCitrixのクライアントとサーバー間の通信をAccess Gatewayで保護するしくみを示しています。



Access Gatewayについて詳しくは、Access Gatewayのドキュメントを参照してください。 Web InterfaceがAccess Gatewayと連動するようにCitrix Web Interface管理コンソールで設定する方法については、「ゲートウェイ設定を構成するには」を参照してください。

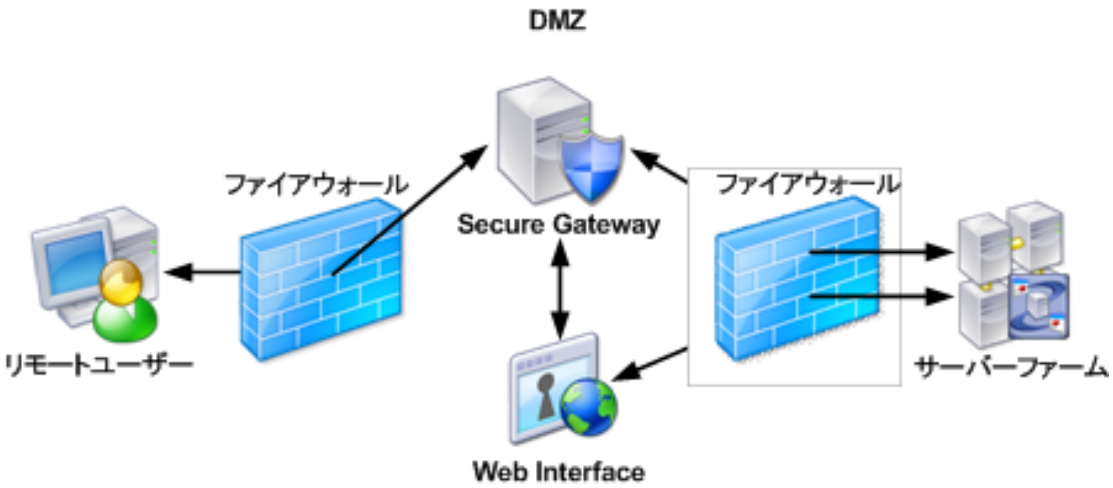
Secure Gateway

更新日： 2014-11-25

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。

Secure Gatewayは、SSL/TLSが有効なCitrixのクライアントとサーバー間の通信の安全なインターネットゲートウェイとして機能します。 ユーザーのデバイスとSecure Gatewayサーバー間のトラフィックのインターネット部分は、SSLまたはTLSによって暗号化されます。つまり、セキュリティが侵害されることなく、ユーザーは情報にリモートアクセスできます。また、Secure Gatewayによって、サーバー証明書がSecure Gatewayサーバー上でのみ必要になり、サーバーファーム内のサーバーでは不要になるため、証明書管理が簡素化されます。

この図は、SSL/TLSが有効なCitrixのクライアントとサーバー間の通信をSecure Gatewayで保護するしくみを示しています。



Web InterfaceがSecure Gatewayと連動するようにCitrix Web Interface管理コンソールで構成する方法については、「ゲートウェイ設定を構成するには」を参照してください。

SSLによるCitrix Online Plug-inの保護

Citrix Web Interface管理コンソールで、SSLを使ったCitrix Online Plug-inとWeb Interfaceサーバー間の通信の保護を設定するには、左側のペインで［XenApp Servicesサイト］をクリックして結果ペインでサイトを選択し、［操作］ペインで［サーバー設定］をクリックして［プラグインとこのサイト間の通信にSSL/TLSを使用する］チェックボックスをオンにします。

各アプリケーションに対して、デリバリーサービスコンソールで［アプリケーションプロパティ］ダイアログボックスを開き、［クライアントオプション］ページの［SSLおよびTLSを有効にする］チェックボックスをオンにする必要があります。

ユーザーデバイスとWeb Interface間の通信

CitrixのクライアントとWeb Interfaceサーバー間の通信では、さまざまな種類のデータが送信されます。 ユーザーがアカウント情報を入力し、リソースの一覧からアクセスするリソースを選択するときに、WebブラウザーとWebサーバー間で、ユーザーのアカウント情報、リソースセットの一覧、セッションの初期化ファイルなどのデータが転送されます。 このネットワークトラフィックには、次のデータが含まれます。

- HTMLフォームデータ。 Web Interfaceでは、ユーザーのログオン時に、標準のHTMLフォームを使ってアカウント情報がWebブラウザーからWebサーバーに送信されます。 Web Interfaceフォームでは、ユーザー名と認証情報はテキスト形式で渡されます。

- HTMLのページおよびセッションCookie。 Web Interfaceの［ログオン］画面にユーザーがアカウント情報を入力すると、その情報はWebサーバー上に保存され、セッションCookieによって保護されます。 WebサーバーからWebブラウザーに送られるHTMLページには、リソースセットが表示されます。 これらのHTMLページには、ユーザーが使用できるリソースが一覧表示されます。

- ICAファイル。 ユーザーがリソースを選択すると、WebサーバーがCitrixのクライアントにそのリソースのICAファイルを（一部Webブラウザーを介して）送信します。 ICAファイルには、サーバーへのログオン時に使用されるチケットが含まれています。 パススルー認証およびスマートカード認証用のチケットは含まれていません。

  クライアントを起動するときに、ICAファイルがユーザーのハードディスク上にテキスト形式のファイルとして保存される場合があります。 ただし、これによりクライアントの起動に問題が起きることはありません。

  ICAファイルの署名機能により、ユーザーは信頼済みのWebサーバーからアプリケーションまたはデスクトップを起動していることを検証できます。 詳しくは、「ICAファイルの署名機能の構成」を参照してください。

ユーザーデバイスとWeb Interface間の通信におけるセキュリティ上の問題

Web InterfaceデータがWebサーバーとWebブラウザー間でネットワーク上に転送されているときや、ユーザーデバイスに書き込まれているときに、Web Interfaceデータが攻撃者に悪用される可能性があります。たとえば、次の潜在的な危険性が考えられます。

- WebサーバーとWebブラウザー間で通信されるログオンデータ、セッションCookie、およびHTMLページが攻撃者により傍受される可能性があります。
- Cookieおよびそこに記録されているアカウント情報が攻撃者に不正に取得される可能性があります。Web Interfaceで使用されるセッションCookieは一時的で、ユーザーがWebブラウザーを閉じると消去されますが、攻撃者がユーザーのWebブラウザーにアクセスできる場合にこの危険性が生じます。
- ICAファイルにユーザーのアカウント情報は含まれていませんが、デフォルトで200秒で有効期限が切れる、1回だけ使用可能なチケットが含まれています。 認証されたユーザーがこのチケットを使用してサーバーに接続する前に、攻撃者がICAファイルを傍受し、サーバーに接続する可能性があります。
- ユーザーがInternet ExplorerでHTTPS接続を使用する場合、暗号化されたページをキャッシュしないように設定していると、ICAファイルがプレーンテキストとして一時フォルダーに保存されます。 攻撃者がユーザーのInternet Explorerのキャッシュにアクセスできる場合、ICAファイルからネットワーク情報が漏洩する危険性があります。
- Citrixのクライアント側でパススルー認証が有効になっている場合、攻撃者により不正なファイルが送信され、認証されていないサーバーや偽装サーバーにユーザーのアカウント情報が転送される危険性があります。 これは、ユーザーがユーザーデバイスへのログオン時に入力したアカウント情報がクライアントに残り、その情報がICAファイルとしてサーバーに転送されるときに発生します。

ユーザーデバイスとWeb Interface間の通信のセキュリティに関する推奨事項

ここでは、ユーザーのデバイスとWebサーバー間で送信されるデータとユーザーのデバイスに書き込まれるデータを保護するための、標準的なセキュリティ対策とCitrix製品のセキュリティ機能の組み合わせについて説明します。

SSL/TLSに対応したWebサーバーとWebブラウザーの導入

Web Interfaceで、WebサーバーとWebブラウザー間の通信を保護するには、まずセキュリティ機能が組み込まれたWebサーバーとWebブラウザーを導入するところから始めます。セキュリティ機能が組み込まれたWebサーバーの多くは、SSLまたはTLS技術を使ってトラフィックを保護しています。

通常のWebサーバーからWebブラウザーへの通信トランザクションでは、最初にWebブラウザーがWebサーバーのサーバー証明書を正規の証明機関の一覧と照合して、Webサーバーの同一性を検証します。 検証が終わると、WebブラウザーはユーザーのWebページへの要求を暗号化し、Webサーバーから戻されたデータを復号化します。 トランザクションの終了時には必ず、TLSまたはSSLによるメッセージの整合性チェックが実行され、通信中にデータが不正に変更されていないかどうかを確認します。

Web Interface環境では、SSLまたはTLSの認証と暗号化機能により安全な接続が作成され、その接続を使用してWeb Interfaceの［ログオン］画面にユーザーが入力するアカウント情報が転送されます。 アカウント情報、セッションCookie、ICAファイル、リソースセットのHTMLページなど、Webサーバーから送られるデータも、同様の方法で保護されます。

ネットワーク上にSSL/TLS技術を実装するには、SSL/TLSに対応したWebサーバーおよびWebブラウザーが必要です。 これらの製品は、Web Interfaceに対して透過的に使用できます。 つまり、これらのWebサーバーやWebブラウザーでは Web Interface用の構成を行う必要はありません。 WebサーバーでSSLまたはTLSを使用するように構成する方法については、Webサーバー製品のドキュメントを参照してください。

重要： SSL/TLSに対応したWebサーバーでは、ほとんどの場合HTTP通信にTCP/IPポート443を使用します。 デフォルトでは、SSL Relayもこのポートを使用します。 Webサーバーが、SSL Relayを実行するサーバーも兼ねている場合は、WebサーバーまたはSSL Relayのどちらかが TCP/IPポート443以外のポートを使用するように構成する必要があります。

パススルー認証の無効化

高度なセキュリティが要求される環境では、認証を受けてないサーバーや偽のサーバーにユーザーのアカウント情報が送信されることを防ぐため、パススルー認証機能を有効にしないでください。 パススルー認証機能は、信頼できる小規模な環境でのみ使用してください。

Web InterfaceとCitrixサーバー間の通信

Web InterfaceとCitrixサーバー（XenAppまたはXenDesktopが動作するサーバー）間の通信には、Web InterfaceとサーバーファームのCitrix XML Service間における、ユーザーアカウント情報やリソースセット情報のやり取りが含まれています。

通常のWeb Interfaceセッションでは、Web Interfaceがユーザー認証用のアカウント情報をXML Serviceに渡し、XML Serviceがリソースセット情報を返します。 サーバーとサーバーファームは、TCP/IP接続とCitrix XMLプロトコルを使用して情報を渡します。

Web InterfaceとCitrixサーバー間の通信におけるセキュリティ上の問題

Web InterfaceのXMLプロトコルでは、難読化されるパスワードを除いてすべてのデータがクリアテキスト形式で通信されます。 そのため次のように、通信データが傍受される危険性があります。

- 攻撃者がXMLトラフィックを傍受し、リソースセット情報やチケットを読み取る可能性があります。 難読化データを攻撃者が解読できる場合は、ユーザーのアカウント情報が不正に取得される可能性があります。
- 攻撃者が、サーバーを偽装して、認証要求を傍受する可能性があります。

Web InterfaceとCitrixサーバー間の通信を保護するための推奨事項

Web Interfaceサーバーとサーバーファーム間で送受信されるXMLトラフィックを保護するには、次のいずれかのセキュリティ対策を施す必要があります。

- SSL Relayを使用して、Web Interfaceサーバーとサーバーファーム間の通信データを保護します。 SSL Relayは、ホストの認証とデータの暗号化を行います。
- SSL Relayを使用できない環境では、XenAppまたはXenDesktopが動作するサーバー上にWeb Interfaceをインストールします。
- IISがXenAppまたはXenDesktopが動作するサーバーにインストールされている場合は、SSLで保護されたHTTPSプロトコルを使用してWeb Interfaceデータを送信します。

SSL Relayの使用

更新日： 2014-12-02

SSL Relayは、XenAppおよびXenDesktopのインストール時にデフォルトでインストールされるコンポーネントです。

サーバー側でSSL Relayのセキュリティ機能を使用するには、SSL Relayが動作するサーバーにサーバー証明書をインストールして、正しく構成しておく必要があります。 サーバー証明書をインストールしてSSL Relayを設定する方法については、「サーバーとクライアント間のSSL/TLSを設定する」の説明を参照してください。 また、SSLリレー構成ツールのオンラインヘルプも参照してください。 XenApp for UNIXサーバーについては、「SSL Relay for UNIX Administration」を参照してください。

SSL Relayの構成を行う前に、SSL Relayが動作するサーバーがCitrix XML Serviceを実行するサーバーにSSLトラフィックを転送できることを確認してください。 デフォルトでは、SSL Relayがインストールされているサーバーにだけデータが転送されます。 ただし、トラフィックをほかのサーバーに転送するようにSSL Relayを構成することも可能です。 Web Interfaceデータの送信先サーバーとは異なるサーバーにSSL Relayをインストールする場合は、SSL Relayのサーバーの一覧に、Web Interfaceデータの転送先サーバーを追加します。

SSL Relayを使用するようにWeb Interfaceを構成するには、Citrix Web Interface管理コンソールまたはWebInterface.confファイルを使います。 コンソールを使って、SSL Relayを使用するようにWeb Interfaceを構成する方法について詳しくは、「サーバーファーム内のすべてのサーバー設定の構成」を参照してください。

Web InterfaceがSSL Relayを使用するようにWebInterface.confファイルで構成するには

1. テキストエディターを使って、Webinterface.confファイルを開きます。
2. FarmnパラメーターのSSLRelayPortの値を、サーバー上のSSL Relayのポート番号に変更します。
3. FarmnパラメーターのTransportの値を、SSLに変更します。

新しいルート証明書をWeb Interfaceサーバーに追加するには

証明機関のサポートを追加するには、その証明機関のルート証明書をWeb Interfaceサーバーに追加する必要があります。

ルート証明書をWebサーバーにコピーします。

- IISの場合は、Microsoft管理コンソール（MMC）のスナップインを使って証明書をコピーします。
- Java Application Serverの場合は、keytoolコマンドラインツールを使用して、適切なキーストアディレクトリに証明書をコピーします。 証明書は、Webページを提供するJava仮想マシンに関連付けられたキーストアに追加する必要があります。 通常、次のキーストアが使用されます。
  - {javax.net.ssl.trustStore}
  - {java.home}/lib/security/jssecacerts
  - {java.home}/lib/security/cacerts

XenAppまたはXenDesktopが動作するサーバーでのWeb Interfaceの有効化

SSL Relayを使用できない環境では、Web Interfaceデータを提供するサーバー上でWebサーバーを実行して、ネットワークへの不正アクセスを防ぐことができます。 このようなWebサーバー上でWeb Interfaceサイトをホストすると、Web Interface要求はすべてローカルホスト上のCitrix XML Serviceに送られるので、ネットワーク上にWeb Interfaceデータを転送する必要がなくなります。 ただし、ネットワークでのデータ転送が不要であるという利点と、Webサーバーへの不正アクセスのリスクを比較検討してください。

まず、Webサーバーと、XenAppまたはXenDesktopが動作するサーバーをファイアウォールの内側に設置します。これにより、WebサーバーとXenAppやDesktop Delivery Controllerとの通信がインターネット側にさらされることを防ぐことができます。 この場合、ユーザーデバイスが、ファイアウォールを介してWebサーバーおよびXenAppやXenDesktopのサーバーと通信できることが必要です。 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、クライアントとサーバー間の通信では、ポート1494とポート2598の着信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。 ネットワークファイアウォールでICAを使用する方法については、Webサーバーのドキュメントを参照してください。 Web Interfaceでネットワークアドレスを変換する方法については、Web Interface SDKを参照してください。

注： XenAppのインストール時のデフォルトでは、Citrix XML ServiceとIISがTCP/IPポートを共有するように設定できます。 XenDesktopで、インストーラーはポート共有を自動的有効にします。 ポート共有が有効な場合、デフォルトでCitrix XML ServiceとWebサーバーで同じポート番号が使用されます。

HTTPSプロトコルの使用

HTTPSプロトコルを使って、XenAppまたはXenDesktopが動作するサーバーとWebサーバーとの間で通信されるWeb Interfaceデータを保護できます。 HTTPSは、SSLまたはTLSを使って強力なデータ暗号化を提供します。

Webサーバーは、XenAppまたはXenDesktopが動作するサーバー上で実行しているIISとのHTTPS接続を確立します。 これには、XenAppまたはXenDesktopが動作するサーバー上のIISがポートを共有し、IISでSSLが有効になっている必要があります。 Citrix Web Interface管理コンソールまたはWebInterface.confのFarmnパラメーターで指定するサーバー名は、IIS SSLサーバー証明書と同じ完全修飾DNS名でなければなりません。

XML Serviceには、https://ServerName/scripts/wpnbr.dllでアクセスできます。 Web InterfaceがHTTPSプロトコルを使用するようにCitrix Web Interface管理コンソールで構成する方法については、「セキュアなアクセスの管理」を参照してください。

HTTPSプロトコルを使用するようにWebInterface.confファイルでWeb Interfaceを構成するには

1. テキストエディターを使って、Webinterface.confファイルを開きます。
2. FarmnパラメーターのTransportの値を、HTTPSに変更します。

ユーザーセッションとサーバー間の通信

Web Interfaceを使用するときのユーザーのデバイスとサーバー間の通信では、初期化要求やセッション情報などの異なる種類のセッションデータが転送されます。

- 初期化要求： 初期化は、セッションを確立する最初のプロセスです。 このときCitrixのクライアントはセッションを要求して、ログオンするユーザー、ウィンドウのサイズ、セッションで実行するアプリケーションなど、セッションを制御するセッション構成パラメーターを作成します。

- セッション情報： セッションの初期化後、（Citrixのクライアントからサーバーへの）マウス入力および（サーバーからクライアントへの）グラフィカル更新など、多数の仮想チャネルを介してCitrixのクライアントとサーバー間で情報が送受信されます。

ユーザーセッションとサーバー間の通信におけるセキュリティ上の問題

クライアントとサーバー間のネットワーク通信を傍受して不正利用するには、バイナリ形式のクライアントプロトコルを解読する必要があります。 攻撃者がクライアントプロトコルを解読できる場合、以下のセキュリティ上のリスクが生じます。

- Citrixのクライアントが送信する初期化要求に含まれるユーザーのアカウント情報などを傍受される。

- ユーザーが入力したテキストやマウスのクリック操作、サーバーから送られる更新画面情報などのセッション情報を傍受される。

ユーザーセッションとサーバー間の通信のセキュリティに関する推奨事項

更新日： 2014-12-02

ユーザーデバイスとサーバー間で通信されるデータを保護するため、トラフィックを暗号化するか、またはAccess Gatewayを使用することをお勧めします。

SSL/TLSまたはICA暗号化の使用

SSL/TLS、またはICA暗号化を使用して、Citrixのクライアントとサーバー間のトラフィックを保護することをお勧めします。 どちらの方法でも、クライアントとサーバー間のデータストリームに128ビット暗号化を適用できます。また、SSL/TLSではサーバーの識別も行われます。

XenAppおよびXenDesktopのすべてのサポートされているバージョンでSSLをサポートします。 XenApp for WindowsおよびXenDesktopのすべてのサポートされているバージョンでSSL/TLSおよびICA暗号化をサポートします。 これらの機能をサポートしているCitrixのクライアントの一覧については、クライアントのドキュメント、またはCitrixのWebサイトを参照してください。 ICA暗号化について詳しくは、「XenAppの管理」を参照してください。

Access Gatewayの使用

Access Gatewayを使うと、Citrixのクライアントとサーバー間のインターネットを介したトラフィックを保護できます。 Access Gatewayは、すべてのリソースに対する安全で単一のポイントからのアクセスを提供するユニバーサルSSL VPNアプライアンスです。 Access Gatewayについて詳しくは、Access Gatewayのドキュメントを参照してください。 Web InterfaceがAccess Gatewayと連動するようにCitrix Web Interface管理コンソールで設定する方法については、「ゲートウェイ設定を構成するには」を参照してください。

診断ログの管理

Citrix Web Interface管理コンソールの［サイトメンテナンス］の［診断ログ］タスクを使って、エラーログに対するシステムセキュリティを強化します。 重複するイベントが繰り返しログに記録されないようにしたり、重複イベントをログに記録する回数と頻度を構成したりできます。

このタスクでは、エラー時のリダイレクト先URLを指定することもできます。 カスタマイズしたエラーコールバックURLを使用する場合は、すべてのエラーIDをそのURLで処理し、ユーザーに適切なエラーメッセージを提供する必要があります。 またユーザーがエラーなく正常にログオフした場合でも、このエラーコールバックURLはユーザーのログオフ画面に表示されます。

構成ファイルを使用したサイトの構成

更新日： 2014-11-24

サイト構成ファイル

Web Interfaceサイトには、そのサイトの構成データを定義する構成ファイル（WebInterface.conf）が含まれています。 管理者は、このファイルを使ってサイトの日常的な管理作業を行ったり、サイトの設定をカスタマイズしたりできます。 たとえば、ユーザーが変更できる設定を指定したり、Web Interfaceへの認証を構成したりできます。

構成ファイルに無効な値を指定し、その後でCitrix Web Interface管理コンソールを使用すると、構成ファイルの値がデフォルトの値に戻されます。

サイト構成ファイルを手作業で編集しているときにCitrix Web Interface管理コンソールを実行している場合、このコンソール上で何らかの構成を変更すると、構成ファイル上でのすべての変更内容が上書きされます。 サイト構成ファイルを編集する前に、Citrix Web Interface管理コンソールを閉じるようにしてください。 これを実行できない場合は、コンソールを使ってほかの変更を入れる前に、コンソール上で更新を実行して構成ファイルの編集を手動でコミットします。

WebInterface.confファイルは、次のサイト構成ディレクトリにあります。

- Microsoftインターネットインフォメーションサービス（IIS）では通常、C:¥inetpub¥wwwroot¥Citrix¥SiteName¥confにあります。
- Apache TomcatなどJava Application Serverでは、./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INFなどのディレクトリにあります。

Webサーバースクリプトを使用すると、WebInterface.confファイルで構成されている値を、特定のWebページで無効にすることができます。 Webサーバースクリプトについて詳しくは、Web Interface SDKを参照してください。

注： Java Application ServerでWeb Interface.confの変更を有効にするには、Webサーバーをいったん停止してから再起動する必要があります。 また、変更は必ずUTF-8エンコードを使用して保存してください。

サーバーとの通信を構成するには

この例では、Citrix XML Serviceを実行している追加サーバーの名前を指定します。 Citrix XML Serviceは、サーバーファームとWeb Interfaceサーバー間の通信リンクとして機能します。

現在、Citrix XML Serviceを実行しているサーバー「rock」と通信していますが、rockがダウンした場合に備えて「roll」を追加することにします。 これを行うには、次の操作を行います。

1. テキストエディターを使ってWebInterface.confファイルを開き、次の行に移動します。

Farm1=rock,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443,…

2. この行を次のように編集して、サーバーrollを追加します。

Farm1=rock,roll,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443,…

SSL Relay通信を構成するには

この例では、Webサーバーと、XenAppまたはXenDesktopのサーバー間の通信をSSL（Secure Sockets Layer）を使って保護します。 SSL Relayは、XenAppまたはXenDesktopが動作するサーバーにインストールされており、このサーバーの完全修飾ドメイン名はblues.mycompany.comです。また、SSL Relayは、TCPポート443で接続を待機しています。

現在、「rhythm」という名前のサーバーを使用していますが、上記のXenAppサーバーに置き換えることにします。 これを行うには、次の操作を行います。

1. テキストエディターを使ってWebInterface.confファイルを開き、次の行に移動します。

Farm1=rhythm,Name:Farm1,XMLPort:80,Transport:HTTP, SSLRelayPort:443

2. この行のTransportの値を、次のようにSSLに変更します。

Farm1=blues.mycompany.com,Name:Farm1,XMLPort:80, Transport:SSL,SSLRelayPort:443

注： サーバー名には、サーバーの証明書で使われているサーバー名と同じ名前を指定する必要があります。

Secure Gatewayのサポートを構成するには

この例では、以下の2つのSecure Ticket Authorityアドレスを使って、Citrixのクライアントがポート443を使用するSecure Gatewayサーバー「csg1.mycompany.com」を指定します。

- http://country.mycompany.com/scripts/ctxsta.dll
- http://western.mycompany.com/scripts/ctxsta.dll

WebInterface.confで次の行を追加します。

AlternateAddress=Mapped

CSG_STA_URL1=http://country.mycompany.com/scripts/ctxsta.dll

CSG_STA_URL2=http://western.mycompany.com/scripts/ctxsta.dll

CSG_Server=csg1.mycompany.com

CSG_ServerPort=443

ClientAddressMap=*,SG

最後の行により、すべてのユーザに対してSecure Gatewayが有効になります。

障害復旧サーバーファームを構成するには

この例では、2つのサーバーファームを確保して、電源障害やネットワーク障害などによりユーザーが実務環境へのアクセスを阻害される場合にのみ使用するとします。

サーバーファームでCitrix XML Serviceを実行するサーバーの名称は、“jazz”および“fusion”です。これらのサーバーファームを障害復旧用とします。 これを実行するには、テキストエディターを使ってWebInterface.confファイルを開き、次の行を追加して環境に合わせてこのパラメーターの設定を構成します。

RecoveryFarm1=jazz,Name:RecoveryFarm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443,Bypassl
RecoveryFarm2=fusion,Name:RecoveryFarm2,XMLPort:80,Transport:HTTP,SSLRelayPort:443,Bypas

2つ目のサーバーファームは、最初の障害復旧サーバーファームにアクセスできない場合にのみ使用されることに留意してください。 リソースは実稼働サーバファーム用のため、両方の障害復旧サーバーファームでは集計されません。 代わりに、Web Interfaceは各障害復旧サーバーファームに順にアクセスして、通信が確立した最初のサーバーファームからリソースを列挙します。

WebInterface.confのパラメーター

更新日： 2014-11-25

次の表に、WebInterface.confに指定できるパラメーターをアルファベット順に示します。 太字はデフォルト値を表します。 WebInterface.confでパラメーターを指定しない場合は、デフォルト値が使用されます。

AccountSelfServiceUrl

- 説明：Password Manager ServiceのURLを指定します。
- 値：HTTPSを使用する有効なURL
- サイトの種類： XenApp Web

AdditionalExplicitAuthentication

- 説明：Secure Access Manager、Active Directoryサービス、またはNDS（Novell Directory Services）と一緒に行う必要がある2つの認証を指定します。
- 値：None | SecurID | SafeWord | RADIUS
- サイトの種類： XenApp Web

AddressResolutionType

- 説明：ICA起動ファイルで使用するアドレスの種類を指定します。
- 値：dns-port | dns | ipv4-port | ipv4
- サイトの種類： XenApp WebおよびXenApp Services

AGAuthenticationMethod

- 説明：Access Gateway統合サイトに対する許可された認証方法を指定します。 ユーザー名とパスワードを使ってAccess Gatewayにログオンしている場合は、このパラメーターはExplicitに設定する必要があります。 スマートカードを使ってAccess Gatewayにログオンしている場合は、このパラメーターをSmartCardに設定します。この場合、ユーザーはリソースにアクセスするたびにPINの入力が必要となります。 SmartCardKerberosに設定すると、スマートカードを使ってAccess Gatewayにログオンし、PINを入力することなくリソースにアクセスできます。
- 値：Explicit | SmartCard | SmartCard Kerberos
- サイトの種類： XenApp Web

AGEPromptPassword

- 説明：ユーザーがAccess Gatewayのログオンページからログオンするときにパスワード入力画面を再度表示するかどうかを指定します。

- 値：Off | On
- サイトの種類： XenApp Web

AGEWebServiceURL

- 説明：Access Gateway認証サービスのURLを指定します。
- 値：Valid URL
- サイトの種類： XenApp Web

AllowBandwidthSelection

- 説明：ユーザーがネットワーク接続速度を指定し、ICA設定を最適化できるかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowCustomizeAudio

- 説明：ICAセッションの音質設定をユーザーが変更できるようにするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowCustomizeAutoLogin

- 説明：自動ログオンの有効/無効をユーザーが切り替えられるようにするかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

AllowCustomizeClientPrinterMapping

- 説明：クライアントプリンターマッピングの有効/無効をユーザーが切り替えられるようにするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowCustomizeJavaClientPackages

- 説明使用するClient for Javaのパッケージをユーザーが選択できるようにするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowCustomizeLayout

- 説明：ユーザーインターフェイスの背景イメージ表示（すべて表示、または限定して表示）の選択をユーザーに許可するかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowCustomizeLogoff

- 説明：ログオフ時のワークスペースコントロールの動作をユーザーが変更できるようにするかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

AllowCustomizePersistFolderLocation

- 説明：再ログオン時に、［アプリケーション］画面の前のセッションの最後に表示していたフォルダーに戻ることができる機能をユーザーが有効/無効にできるかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowCustomizeReconnectAtLogin

- 説明：ログオン時のワークスペースコントロールの動作をユーザーが変更できるようにするかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

AllowCustomizeReconnectButton

- 説明：［再接続］ボタンをクリックしたときのワークスペースコントロールの動作をユーザーが変更できるようにするかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

AllowCustomizeSettings

- 説明：ユーザーによるWeb Interfaceセッションのカスタマイズを許可するかどうかを指定します。 Offを指定すると、ユーザーの［ログオン］および［アプリケーション］画面に［基本設定］ボタンが表示されません。
- 値：On | Off
- サイトの種類： XenApp Web

AllowCustomizeShowHints

- 説明：［アプリケーション］画面のヒントの表示/非表示の選択をユーザーに許可するかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

AllowCustomizeShowSearch

- 説明：［アプリケーション］画面の検索の有効/無効の選択をユーザーに許可するかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowCustomizeSpecialFolderRedirection

- 説明：ユーザーフォルダーのリダイレクトの有効/無効をユーザーが切り替えられるようにするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowCustomizeTransparentKeyPassthrough

- 説明：ショートカットキーの適用先をユーザーが変更できるようにするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowCustomizeVirtualCOMPortEmulation

- 説明：PDA同期の有効/無効をユーザーが切り替えられるようにするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowCustomizeWinColor

- 説明：ICAセッションの色数をユーザーが変更できるようにするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowCustomizeWinSize

- 説明：ICAセッションのウィンドウのサイズをユーザーが変更できるようにするかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

AllowDisplayInFrames

- 説明：XenApp Webサイトについて、サードパーティ製のWebページに埋め込まれたフレーム内での表示を許可するかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

AllowFontSmoothing

- 説明：フォントスムージングをICAセッションで許可するかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp WebおよびXenApp Services

AllowUserAccountUnlock

- 説明：アカウントセルフサービスを使用したアカウントのロックを解除をユーザーに許可するかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AllowUserPasswordChange

- 説明：ユーザーがパスワードを変更できる条件を指定します。
- 値：Never | Expired-Only | Always（XenApp Webサイトのみ）
- サイトの種類： XenApp WebおよびXenApp Services

AllowUserPasswordReset

- 説明：アカウントセルフサービスを使用したパスワードのリセットをユーザーに許可するかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

AlternateAddress

- 説明：サーバーの代替アドレスをICAファイルに返すかどうかを指定します。
- 値：Off | Mapped | On

- サイトの種類： XenApp WebおよびXenApp Services

ApplicanceEmbeddedSmartCardSSO

- 説明：スマートカード認証でシングルサインオンに埋め込みActiveXコントロールを使用するかどうかを指定します。
- 値：Off | On
- サイトの種類：Desktop Appliance Connector

ApplianceEmbeddedSmartCardSSOPinTimeout

- 説明：埋め込まれたスマートカード認証の暗証番号入力画面に入力がない場合、ログオン画面に戻る前に待機する秒数です。
- 値：20
- サイトの種類：Desktop Appliance Connector

ApplianceMultiDesktop

- 説明：ユーザーに複数のデスクトップが割り当てられている場合、デスクトップの一覧を表示するかどうかを指定します。
- 値：Off | On
- サイトの種類：Desktop Appliance Connector

ApplicationAccessMethods

- 説明：ユーザーが、オンラインリソース用のクライアント、またはCitrix Offline Plug-in、またはその両方を使ってアプリケーションにアセクスできるかどうかを指定します。
- 値：Remote、Streaming
- サイトの種類： XenApp WebおよびXenApp Services

AppSysMessage_<Language Code >

- 説明：［アプリケーション］画面のメインコンテンツ領域に表示されるボタンのローカライズ文字列を指定します。 LanguageCodeは、ja、en、fr、de、es、またはそのほかのサポートされている言語の識別子です。
- 値：なし。 テキスト形式の文字列と、任意の数の改行タグ（
）とハイパーリンク
- サイトの種類： XenApp Web

AppTabn

- 説明：［アプリケーション］画面上に表示させるタブを指定します。 複数指定することで複数のタブを定義できます。 AllResources値を指定すると、ユーザーが使用できるすべてのリソースを含む単一のタブを定義できます。
- 値：Applications | Desktops | Content | AllResources

- サイトの種類： XenApp Web

AppWelcome Message_<Language Code >

- 説明：［アプリケーション］画面のメインコンテンツ領域上部に表示されるローカライズ文字列を指定します。 LanguageCodeは、ja、en、fr、de、es、またはそのほかのサポートされている言語の識別子です。
- 値：なし。 テキスト形式の文字列と、任意の数の改行タグ（
）とハイパーリンク
- サイトの種類： XenApp Web

AuthenticationPoint

- 説明：ユーザー認証を実行する場所を指定します。
- 値：WebInterface | ADFS | AccessGateway | 3rdParty | WebServer
- サイトの種類： XenApp Web

AutoLaunchDesktop

- 説明：デスクトップへの自動アクセスを有効にするかどうかを指定します。 このパラメーターをOnに設定すると、デスクトップがすべてのサーバーファームでの唯一のリソースである場合は、Web Interfaceは自動的にユーザーのデスクトップを開始します。
- 値：Off | On
- サイトの種類： XenApp Web

AutoLoginDefault

- 説明：パススルー認証、スマートカードパススルー認証、およびスマートカード認証を使ってリソースにアクセスするユーザーの自動ログオンをデフォルトで有効にするか無効にするかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

BrandingColor

- 説明：ヘッダーおよびフッター領域の色を指定します。
- 値：16進表記の色番号、または色名
- サイトの種類： XenApp Web

BrandingImage

- 説明：ヘッダーおよびフッターのブランドイメージのURLを指定します。
- 値：Valid URL
- サイトの種類： XenApp Web

BypassFailedRadiusServerDuration

- 説明：障害が発生したRADIUSサーバーの使用を再開するまでの時間を指定します。
- 値：分数（60）
- サイトの種類： XenApp Web

BypassFailedSTADuration

- 説明：障害が発生したゲートウェイデバイス用のSecure Ticket Authorityが動作するサーバーの使用を再開するまでの時間を指定します。
- 値：分数（60）
- サイトの種類： XenApp Web

ClientAddressMap

- 説明：サーバー側のファイアウォール構成に対するクライアントのアドレスおよびアドレスの種類を指定します。 エントリの最初のフィールドはサブネットアドレスおよびマスクで、2つ目の値はNormal、Alternate、Translated、SG、SGAlternate、SGTranslatedのいずれかになります。 特に指定のないすべてのCitrixのクライアントでデフォルト値を使用する場合は、プラグインアドレスまたはサブネット部分にワイルドカード文字のアスタリスク（*）を使用します。
- 値：SubnetAddress/SubnetMask |*, Normal | Alternate |Translated | SG | SGTranslated |SGAlternate, ...
- サイトの種類： XenApp Web

ClientDefaultURL

- 説明：適切なクライアントをダウンロードできない場合に、クライアント検出および展開プロセスによりユーザーがリダイレクトされるURLを指定します。
- 値：http://www. citrix.com/ download 有効なURL
- サイトの種類： XenApp Web

ClientIcaLinuxX86

ClientIcaMac

ClientIcaSolarisSparc

ClientIcaSolarisX86

ClientIcaWin32

ClientStreamingWin32

- 説明：指定のプラットフォームに対するクライアント検出および展開処理を構成します。適切なパラメーターが構成されていない場合、ユーザーはClientDefaultURLパラメーターで指定されたWebページにリダイレクトされます。 デフォルトでは、これらのパラメーターはXenApp 6.0インストールメディアに収録されているネイティブクライアント用に

構成されています。

最初の2つのフィールドは、クライアントインストーラーの場所とファイル名を指定します。 ファイルが見つからない場合、ユーザーはClientDefaultURLパラメーターで指定されたWebページにリダイレクトされます。

MuiフィールドはDirectoryおよびFilenameフィールドで指定されるクライアントが複数言語をサポートするかどうかを指定します。 Noに設定すると、クライアント検出および展開処理により指定のファイルに対してLanguageCode¥FolderNameフォルダーがチェックされます。

Versionフィールドは、DirectoryおよびFilenameフィールドで指定されたクライアントのバージョン番号をコンマ区切りで示します。 バージョン番号が指定されていないと、クライアント検出および展開処理により指定のファイルからバージョン番号が推測されます。

ShowEULAフィールドは、指定のクライアントをインストールするためにユーザーがCitrixライセンス契約に同意する必要があるかどうかを指定します。

ClassIDフィールドは、Windows用のクライアントのクラスIDおよびそのクライアントで必要な設定を指定します。

Urlフィールドは、［ダウンロード］ボタンをクリックし、またDirectoryおよびFilenameフィールドを使ってクライアントファイルが指定されていない場合にユーザーがリダイレクトされるWebページを指定します。 この設定は、クライアントファイルを使用できない場合に限り使用する必要があります。

Descriptionフィールドは、［ダウンロード］ボタンの上に表示されるカスタムメッセージを指定します。 このメッセージは指定の言語以外にはローカライズされません。

- 値：Directory: <FolderName>, Filename: <FileName>, [Mui:Yes | No,] [Version: <Version Number>,] [ShowEULA: Yes | No,] [ClassID: <Value>,] [Url: <ValidURL>,] [Description: <Caption>]
- サイトの種類： XenApp Web

ClientProxy

- 説明：サブネットアドレスとマスク、およびクライアント側のファイアウォールの割り当てられたプロキシ設定を指定します。 返されるICAファイル内のアドレスは、これらの設定によって決まります。 各エントリは、3つのフィールドで構成されます。 1番目のフィールドは、サブネットアドレスとサブネットマスクです。 特に指定のないCitrixのクライアントではデフォルト値を使う場合は、ワイルドカード文字のアスタリスク（*）を挿入します。 2番目のフィールドには、6つのプロキシの種類のいずれか1つを指定します。 3つのフィールドの各組み合わせの第3フィールド（プロキシアドレス）は、第2フィールド（プロキシの種類）にプロキシの種類が明示的に指定されている場合（SOCKSまたはSecure）を除き無視されますが、必ず指定しなければなりません。第3フィールドのデフォルト値はマイナス記号（-）です。
- 値：<Subnet Address>/ <SubnetMask> |*, Auto | WpadAuto | Client | None | SOCKS | Secure, - | <Proxy Address> | <ProxyAddress>: <ProxyPort>, …
- サイトの種類： XenApp WebおよびXenApp Services

CompactHeaderImage

- 説明：背景イメージを限定して表示するユーザーインターフェイスのヘッダーイメージのURLを指定します。
- 値：Valid URL
- サイトの種類： XenApp Web

CompactViewStyles

- 説明：背景イメージを限定して表示するユーザーインターフェイスの［アプリケーション］画面でユーザーが使用できる表示スタイルを指定します。
- 値：Icons, List
- サイトの種類： XenApp Web

CredentialFormat

- 説明：WindowsおよびNISの指定ユーザー認証で使用するアカウント情報の形式を指定します。
- 値：All | UPN | DomainUsername
- サイトの種類： XenApp WebおよびXenApp Services

CSG_EnableSessionReliability

- 説明：Access GatewayまたはSecure Gatewayでセッション画面の保持を使用するかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp WebおよびXenApp Services

CSG_Server

- 説明：Access Gatewayアプライアンスまたは Secure Gatewayサーバーのアドレスを指定します。
- 値：なし。 サーバーのFQDN
- サイトの種類： XenApp WebおよびXenApp Services

CSG_ServerPort

- 説明：Access Gatewayアプライアンスまたは Secure Gatewayサーバーのポートを指定します。
- 値：なし。 サーバーポート
- サイトの種類： XenApp WebおよびXenApp Services

CSG_STA_URLn

- 説明：ゲートウェイデバイス用のSecure Ticket Authorityを実行するサーバーのURLを指定します。

- 値：なし。 STAのURL
- サイトの種類： XenApp WebおよびXenApp Services

CSG_UseTwoTickets

- 説明：Access Gatewayを介してリソースにアクセスした際に、Web Interfaceが2つの別のSecure Ticket Authorityからのチケットを必要とするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp WebおよびXenApp Services

DefaultAudioQuality

- 説明：ICAコネクションで使用するデフォルトの音質を指定します。
- 値：NoPreference | High | Medium | Low | Off
- サイトの種類： XenApp Web

DefaultBandwidthProfile

- 説明：ICAコネクションで使用するデフォルトの帯域幅プロファイル（音質や色数などのはい域幅に関連する設定のコレクション）を指定します。
- 値：Custom | High | Medium High | Medium | low
- サイトの種類： XenApp Web

DefaultColorDepth

- 説明：ICAコネクションで使用するデフォルトの色数を指定します。
- 値：NoPreference | TrueColor | HighNoPreferenceColor
- サイトの種類： XenApp Web

DefaultCompactViewStyle

- 説明：背景イメージを限定して表示するユーザーインターフェイスの［アプリケーション］画面のデフォルトの表示スタイルを指定します。
- 値：List | Icons
- サイトの種類： XenApp Web

DefaultCustomTextLocale

- 説明：インストールキャプションとして使用するメッセージのデフォルトの言語コード（ロケール）を指定します。 同じロケールを、定義したすべてのカスタム文字列パラメーター（*_LanguageCode）に指定する必要があります。
- 値：なし。en | fr | de | es | ja | そのほかのサポートされている言語の識別子
- サイトの種類： XenApp Web

DefaultPrinterMapping

- 説明：ICAコネクションに対してプリンターマッピングをデフォルトで有効にするかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

DefaultViewStyle

- 説明：背景イメージをすべて表示するユーザーインターフェイスの［アプリケーション］画面のデフォルトの表示スタイルを指定します。
- 値：Icons | Details | Groups | List | Tree
- サイトの種類： XenApp Web

DefaultWindowSize

- 説明：ICAセッションで使用するデフォルトのウィンドウモードを指定します。 このパラメーターには、画面領域全体に対する割合をX%の形式で指定したり、固定のカスタムサイズをXxYの形式で指定したりできます。
- 値：FullScreen | Seamless | X% | XxY
- サイトの種類： XenApp Web

DisplayBrandingImage

- 説明：ヘッダーおよびフッター領域にブランドイメージを表示するかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

DomainSelection

- 説明：指定ユーザー認証用の［ログオン］画面に一覧表示するドメイン名を指定します。
- 値：NetBIOSドメイン名のリスト
- サイトの種類： XenApp WebおよびXenApp Services

DuplicateLogInterval

- 説明：DuplicateLogLimitに指定したログエントリを監視する時間を指定します。
- 値：秒数（60）
- サイトの種類： XenApp WebおよびXenApp Services

DuplicateLogLimit

- 説明：DuplicateLogIntervalにより指定された時間内に、何個の重複ログエントリを許可するかを指定します。
- 値：1以上の整数（10）
- サイトの種類： XenApp WebおよびXenApp Services

EnableFileTypeAssociation

- 説明：サイトのファイルタイプの関連付けを有効にするかどうかを指定します。 Offを指定すると、コンテンツのリダイレクトをサイトでは使用できません。
- 値：On | Off
- サイトの種類： XenApp WebおよびXenApp Services

EnableKerberosToMPS

- 説明：Kerberos認証を有効にするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp WebおよびXenApp Services

EnableLegacyICAClientSupport

- 説明：UTF-8形式のICAファイルを読み込むことができない旧バージョンのCitrixのクライアントをサポートするかどうかを指定します。 Offを指定すると、サーバーはUTF-8エンコードでICAファイルを生成します。
- 値：Off | On
- サイトの種類： XenApp WebおよびXenApp Services

EnableLogoffApplications

- 説明：ユーザーがサーバーからログオフするときに、ワークスペースコントロール機能を使ってアクティブなリソースもログオフするかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

EnablePassthroughURLs

- 説明：Web Interfaceを使用してアクセスするリソースへのリンクの作成をユーザーに許可するかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

EnableRadiusServerLoadBalancing

- 説明：構成したRADIUSサーバー間でセッションの負荷分散をするかどうかを指定します。 このパラメーターの設定に関係なく、サーバー間のフェールオーバーは実行されま

す。

- 値：Off | On
- サイトの種類： XenApp Web

EnableSTALoadBalancing

- 説明：ゲートウェイデバイスに対して構成されたSecure Ticket Authorityサーバー間で要求の負荷分散をするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp WebおよびXenApp Services

EnableVirtualCOMPortEmulation

- 説明：USB接続によるPDA同期を有効にするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

EnableWizardAutoMode

- 説明：クライアント検出および展開処理を自動モードで実行するかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

EnableWorkspaceControl

- 説明：ユーザーにワークスペースコントロール機能の使用を許可するかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

ErrorCallbackURL

- 説明：エラー発生時のWeb Interfaceのリダイレクト先URLを指定します。 URLが参照するWebページは、次の4つのクエリ文字列パラメーターを受け入れて処理する必要があります。

  CTX_MessageType

  CTX_MessageKey

  CTX_MessageArgs

  CTX_LogEventID

- 値：Valid URL

- サイトの種類： XenApp Web

Farmn

- 説明：サーバーファームのすべての情報を指定します。 最大512のサーバーファームを構成できます。
- 値：Citrix XML Service address [,Citrix XML Service address,] [,Name:<Name>] [,XMLPort: <Port>] [,Transport: <HTTP | HTTPS | SSL>] [,SSLRelayPort: <Port>] [,Bypass Duration: <TimeInMinutes (60)>] [,LoadBalance: <off | on>] [,TicketTime ToLive: <TimeInSeconds (200)>] [,RADETicket TimeToLive: <TimeInSeconds (200)>]
- サイトの種類： XenApp WebおよびXenApp Services

FarmnGroups

- 説明：サーバーファームからリソースを表示できるActive Directoryグループを指定します。 このパラメーター設定を含めると、ユーザーローミング機能がアクティブになります。 Farmnパラメーターで定義する各サーバーファームに対して最大512のユーザーグループを指定できます。
- 値：なし。 Domain¥ UserGroup[,...]
- サイトの種類：XenApp Web、XenApp Services、およびXenDesktop

FooterText _LanguageCode

- 説明：すべてのページのフッター領域にローカライズしたフッター文字列を指定します。 LanguageCodeは、ja、en、fr、de、es、またはそのほかのサポートされている言語の識別子です。
- 値：なし。 テキスト形式の文字列と、任意の数の改行タグ（
）とハイパーリンク
- サイトの種類： XenApp Web

HeaderFontColor

- 説明：ヘッダー領域のフォント色を指定します。
- 値：16進表記の色番号、または色名
- サイトの種類： XenApp Web

HeadingHomePage

- 説明：ホームページの見出しとして表示するイメージのURLを指定します。
- 値：Valid URL
- サイトの種類： XenApp Web

HeadingImage

- 説明：Web Interfaceの見出しとして表示するイメージのURLを指定します。

- 値：Valid URL
- サイトの種類： XenApp Web

HideDomainField

- 説明：［ログオン］画面にドメインフィールドを表示するかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

IcaFileSigningCertificateThumbprint

- 説明：ICAファイルの署名に使用する証明書の拇印です。
- 値：なし。 拇印にはスペースを含めることができます。
- サイトの種類： XenApp WebおよびXenApp Services

IcaFileSigningEnabled

- 説明：ICAファイルの署名機能を有効または無効にします。
- 値：Off | On
- サイトの種類： XenApp WebおよびXenApp Services

IcaFileSigningHashAlgorithm

- 説明：ICAファイルの署名に使用するハッシュアルゴリズムです。
- 値：SHA1 | SHA256
- サイトの種類： XenApp WebおよびXenApp Services

IgnoreClientProvidedClientAddress

- 説明：Citrixのクライアント指定のアドレスを無視するかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp WebおよびXenApp Services

InternalServerAddressMap

- 説明：通常/変換済みのアドレスペアを指定します。 通常のアドレスは、ゲートウェイが通信するサーバーを識別し、変換済みのアドレスはCitrixのクライアントに戻されます。
- 値：NormalAddress = Translated Address, ...
- サイトの種類： XenApp WebおよびXenApp Services

JavaClientPackages

- 説明：ユーザーが使用できるようにするClient for Javaのパッケージのデフォルトのセットを指定します。
- 値：ClipBoard、ConfigUI、PrinterMapping、SecureICA、SSL、Audio、ClientDriveMapping、ZeroLatency
- サイトの種類： XenApp Web

JavaFallbackMode

- 説明：ユーザーがネイティブクライアントをインストールできない場合に、Client for Javaにフォールバックするかどうかを指定します。 このパラメーターは、LaunchClientsパラメーターにIca-Local値が含まれている場合にのみ適用されます。Manual設定により、ユーザーがClient for Javaの使用を選択できるようにできます。
- 値：None | Manual | Auto
- サイトの種類： XenApp Web

KioskMode

- 説明：ユーザー設定を永続的に維持するか、セッション内でのみ維持するかを指定します。 キオスクモードを有効にすると、ユーザー設定はセッション間で維持されなくなります。
- 値：Off | On
- サイトの種類： XenApp Web

LaunchClients

- 説明：ユーザーが選択できるCitrixのクライアントを指定します。 このパラメーターはデュアルモードサイトでは無視され、設定は常にIca-Localです。Ica-Javaを省略しても、Client for Javaの使用が禁止されるわけではありません。 Client for Javaの使用を許可しない場合は、JavaFallbackModeパラメーターにもNoneを指定します。
- 値：Ica-Local、Ica-Java、Rdp-Embedded
- サイトの種類： XenApp Web

LoginDomains

- 説明：アクセスを制限するドメインの名前を指定します。
- 値：NetBIOSドメイン名のリスト
- サイトの種類： XenApp WebおよびXenApp Services

LoginSys Message _LanguageCode

- 説明：［ログオン］画面のメインコンテンツのボタンを表示するローカライズされた文字列を指定します。 LanguageCodeは、ja、en、fr、de、es、またはそのほかのサポートされている言語の識別子です。
- 値：なし。 テキスト形式の文字列と、任意の数の改行タグ（
）とハイパーリンク

- サイトの種類： XenApp Web

LoginTitle _LanguageCode

- 説明：［ログオン］画面のウェルカムメッセージの上に表示させるローカライズされた文字列を指定します。 LanguageCodeは、ja、en、fr、de、es、またはそのほかのサポートされている言語の識別子です。

- 値：なし。 テキスト形式の文字列と、任意の数の改行タグ（
）とハイパーリンク

- サイトの種類： XenApp Web

LoginType

- 説明：ユーザーに表示する［ログオン］画面の種類を指定します。 ［ログオン］画面は、ドメインベースまたはNDSベースのいずれかにできます。

- 値：Default | NDS

- サイトの種類： XenApp WebおよびXenApp Services

LogoffFederationService

- 説明：AD FS統合サイトで［ログオフ］ボタンをクリックする場合に、XenApp Webサイトからのみログオフするのかフェデレーションサービス全体からログオフするのかを指定します。

- 値：On | Off

- サイトの種類： XenApp Web

MultiFarmAuthenticationMode

- 説明：3つのオプションで、許可される認証モードを指定します。 デフォルトのAllオプションでは、任意のアプリケーションの列挙時にすべてのファームで認証されます。 Anyオプションでは、認証された任意のファームでアプリケーションが列挙されますが、ユーザーが資格情報を誤って入力するとその情報が各ファームに送信されてしまいます。これにより、そのアカウントが直ちにロックされてしまう場合があります。 Primaryオプションでは、最初にプライマリファーム（Web Interfaceで構成されたファーム一覧の最上位ファーム）で認証され、その後でAnyモードにフォールバックします。このため、アカウントがロックされる危険性が低くなります。

- 値：All | Any | Primary

- サイトの種類： XenApp Web

MultiLaunchTimeout

- 説明：リソースを開始するためにユーザーがリソースアイコンを最初にクリックした後に、そのアイコンを無効にする時間を指定します。

- 値：秒数（2）

- サイトの種類： XenApp Web

NDSContextLookupLoadbalancing

- 説明：構成したLDAPサーバー間でNDS要求の負荷分散をするかどうかを指定します。 このパラメーターの設定に関係なく、サーバー間のフェールオーバーは実行されます。
- 値：Off | On
- サイトの種類： XenApp Web

NDSContextLookupServers

- 説明：使用するLDAPサーバーを指定します。 ポートが指定されていない場合は、プロトコルから推測されます。ldapを指定すると、デフォルトのLDAPポート（389）が使用されます。ldapsを指定すると、デフォルトのSSL経由LDAPポート（636）が使用されます。 最大512のLDAPサーバーを構成できます。

  パラメーターが非定義または存在しない場合、コンテキストレスログオン機能は無効になります。
- 値：None. ldap://[:] | ldaps://[:],
- サイトの種類： XenApp Web

NDSTreeName

- 説明：NDS認証を使用する場合に必要なNDSツリーを指定します。
- 値：なし。 NDSツリー名
- サイトの種類： XenApp WebおよびXenApp Services

OverlayAutologonCredsWithTicket

- 説明：ログオンチケットを1つのログオンチケットエントリで複製するのか、別のICA起動ファイルチケットエントリのみに置くのかを指定します。 Onを指定すると、ログオンチケットが複製されます。
- 値：On | Off
- サイトの種類： XenApp Web

OverrideIcaClientname

- 説明：Web Interfaceで生成するIDをICA起動ファイルのClientnameエントリに渡すかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

PasswordExpiryWarningPeriod

- 説明：パスワードの有効期限が切れる何日前に、警告メッセージをユーザーに表示するかを指定します。
- 値：0～999の整数（14）
- サイトの種類： XenApp Web

PersistFolderLocation

- 説明：再度ログオンした場合、［アプリケーション］画面に前のセッションの最後に表示していたフォルダーを表示させるかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

PNAChangePasswordMethod

- 説明：Citrix Online Plug-inがユーザーからのパスワード変更要求をどのように処理するかを指定します。 Direct-Onlyを指定すると、プラグインはドメインコントローラーと直接通信してパスワードを変更します。 Direct-With-Fallbackは、ドメインコントローラーに最初にアクセスしようとしたプラグインを示しますが、これに失敗する場合は、XenApp Servicesサイトを使用します。 プロキシオプションは、XenApp Servicesサイトにアクセスしてプラグインがパスワードを変更することを示します。
- 値：Direct-Only | Direct-With-Fallback | Proxy
- サイトの種類：XenApp Services

PooledSockets

- 説明：ソケットプール機能を使用するかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp WebおよびXenApp Services

PreLoginMessageButton_<Language Code >

- 説明：ログオン前に表示するメッセージの確認ボタンのローカライズされた名前を指定します。 LanguageCodeは、ja、en、fr、de、es、またはそのほかのサポートされている言語の識別子です。
- 値：なし。 テキスト形式の文字列と、任意の数の改行タグ（
）とハイパーリンク
- サイトの種類： XenApp Web

PreLoginMessageText_<Language Code >

- 説明：ログオン前に表示するメッセージページのローカライズされた文字列を指定します。 LanguageCodeは、ja、en、fr、de、es、またはそのほかのサポートされている言語の識別子です。
- 値：なし。 テキスト形式の文字列と、任意の数の改行タグ（
）とハイパーリンク
- サイトの種類： XenApp Web

PreLoginMessageTitle_<Language Code >

- 説明：ログオン前に表示するメッセージページのローカライズされたタイトルを指定します。 LanguageCodeは、ja、en、fr、de、es、またはそのほかのサポートされている言語の識別子です。

- 値：なし。 テキスト形式の文字列と、任意の数の改行タグ（
）とハイパーリンク
- サイトの種類： XenApp Web

RADERequestValidation

- 説明：Citrix Offline Plug-inから受信する要求に対してテキスト検証を実行するかどうかを指定します。
- 値のデータ：
- サイトの種類： XenApp WebおよびXenApp Services

RADESessionURL

- 説明：RADEセッションページのURLを指定します。 Autoを指定すると、URLは自動的に生成されます。
- 値：Auto 有効なURL
- サイトの種類： XenApp WebおよびXenApp Services

RadiusRequestTimeout

- 説明：セッションのRADIUSサーバーからの応答を待機するタイムアウトを指定します。
- 値：秒数（30）
- サイトの種類： XenApp Web

RadiusServers

- 説明：使用するRADIUSサーバー、およびオプションでそれがリスンするポートを指定します。 サーバーはIPアドレスまたはサーバー名で指定します。サーバーとポートの間はコロン（:）で区切ります。 ポートが指定されていない場合、デフォルトのRADIUSポート（1812）が採用されます。 最大512のサーバーを構成できます。
- 値：Server [:Port] [,...]
- サイトの種類： XenApp Web

ReconnectAtLogin

- 説明：ログオン時にワークスペースコントロール機能を使ってリソースに再接続するかどうかを指定します。再接続する場合は、すべてのリソースに再接続するのか、それとも切断したリソースだけに再接続するのかを指定します。
- 値：Disconnected AndActive | Disconnected | None
- サイトの種類： XenApp Web

ReconnectButton

- 説明：ユーザーが［再接続］をクリックしたときにワークスペースコントロール機能を使ってリソースに再接続するかどうかを指定します。再接続する場合は、すべてのリソースに再接続するのか、それとも切断したリソースだけに再接続するのかを指定します。

- 値：Disconnected AndActive | Disconnected | None
- サイトの種類： XenApp Web

RecoveryFarmn

- 説明：障害復旧サーバーファームのすべての情報を指定します。 最大512のサーバーファームを構成できます。
- 値：Citrix XML Service address [,Citrix XML Service address,] [,Name:<Name>] [,XMLPort: <Port>] [,Transport: <HTTP | HTTPS | SSL>] [,SSLRelayPort: <Port>] [,Bypass Duration: <TimeInMinutes (60)>] [,LoadBalance: <off | on>] [,TicketTime ToLive: <TimeInSeconds (200)>] [,RADETicket TimeToLive: <TimeInSeconds (200)>]
- サイトの種類：XenApp Web、XenApp Services、およびXenDesktop

RequestedHighColorIcons

- 説明：Citrix XLM Serviceから色数32ビットのアイコンを要求するかどうかを指定します。要求する場合は、アイコンサイズをピクセルで指定します。 Noneを指定すると、標準の4ビット32×32のアイコンだけが要求されます。 デフォルト設定は、サイトの種類およびその構成により異なります。
- 値：16, 32, 48 | None

  XenApp Servicesサイトの場合、デフォルトではすべてのアイコンが要求されます。 XenApp Webサイトの場合、16×16および32×32サイズのみがデフォルトで要求されます。
- サイトの種類： XenApp WebおよびXenApp Services

RequestICAClientSecureChannel

- 説明：TLS設定を指定します。
- 値：Detect-Any Ciphers、TLS- GovCiphers、SSL-AnyCiphers
- サイトの種類： XenApp WebおよびXenApp Services

RequireLaunchReference

- 説明：起動リファレンスを強制的に使用するかどうかを指定します。 XenApp VM Hosted Appsへのパススルー認証には、起動リファレンスが必要です。 XenApp 4.0 with Feature Pack 1 for UNIXとの互換性が必要な場合は、このパラメーターをOffに設定する必要があります。
- 値：On | Off
- サイトの種類： XenApp WebおよびXenApp Services

RestrictDomains

- 説明：LoginDomainsパラメーターを使用してユーザーのアクセスを制限するかどうかを指定します。

- 値：Off | On
- サイトの種類： XenApp WebおよびXenApp Services

SearchContextList

- 説明：NDS認証で使用するコンテキスト名を指定します。
- 値：なし。 コンテキスト名のカンマ区切りの一覧
- サイトの種類： XenApp WebおよびXenApp Services

ServerAddressMap

- 説明：サーバー側のファイアウォール構成とペアになる通常/変換済みアドレスを指定します。 標準アドレスはサーバーを識別し、変換アドレスはCitrixのクライアントに返されます。
- 値：NormalAddress、Translated Address、…
- サイトの種類： XenApp WebおよびXenApp Services

ServerCommunicationAttempts

- 説明：Citrix XML Serviceで障害が発生した場合に、接続を試みる回数を指定します。
- 値：1以上の整数（2）
- サイトの種類： XenApp WebおよびXenApp Services

ShowClientInstallCaption

- 説明：インストールキャプションをどのように、いつ表示するかを指定します。 Autoを指定すると、ユーザーにインストール済みのCitrixのクライアントがない、またはインストールされているものよりも機能的に優れたクライアントをダウンロードできる場合に、インストールキャプションが表示されます。 Quietを指定すると、インストール済みのクライアントがない場合にのみインストールキャプションが表示されます。 ［ログオン］画面には、オンラインリソース用のクライアントが検出されなかったときにのみキャプションが表示され、古いバージョンに対するメッセージは表示されません。 このため、［ログオン］画面に表示されるインストールキャプションついては、AutoとQuietで差異は生じません。
- 値：Auto | Quiet | Off
- サイトの種類： XenApp Web

ShowDesktopViewer

- 説明：ユーザーがデスクトップにアクセスしする際に、Citrix Desktop Viewerウィンドウおよびツールバーを有効にするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp WebおよびXenApp Services

ShowHints

- 説明：［アプリケーション］ 画面にヒントを表示するかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

ShowPasswordExpiryWarning

- 説明：パスワードの有効期限に関する警告をユーザーに表示する条件を指定します。
- 値： Never | WindowsPolicy | Custom
- サイトの種類： XenApp Web

ShowRefresh

- 説明：［アプリケーション］画面で［更新］ボタンをユーザーが使用できるかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

ShowSearch

- 説明：［アプリケーション］画面で［検索］をユーザーが使用できるかどうかを指定します。
- 値：On | Off
- サイトの種類： XenApp Web

SpecialFolderRedirection

- 説明：ユーザーフォルダーのリダイレクト機能を有効にするかどうかを指定します。 Onを指定すると、リソースでユーザーのローカルコンピューター上のドキュメントフォルダーおよびデスクトップフォルダーが表示されます。 Offを指定すると、アプリケーションが表示するドキュメントフォルダーおよびデスクトップフォルダーはサーバー上のものになります。
- 値：Off | On
- サイトの種類： XenApp WebおよびXenApp Services

SuppressDuplicateResources

- 説明：異なるサーバーファーム上で公開された識別名およびフォルダーの場所があるリソースの存在をユーザーに表示するかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp WebおよびXenApp Services

Timeout

- 説明：Citrix XML Serviceとの通信のタイムアウト（時間切れ）を指定します。

- 値：秒数（60）
- サイトの種類： XenApp WebおよびXenApp Services

TransparentKeyPassthrough

- 説明：Windowsショートカットキーの適用先を指定します。
- 値：FullScreen Only | Local | Remote
- サイトの種類： XenApp WebおよびXenApp Services

TwoFactorPasswordIntegration

- 説明：RSA SecurID 6.0とのパスワード統合を有効にするかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

TwoFactorUseFullyQualifiedUserNames

- 説明：2要素認証時に完全修飾ユーザー名を認証サーバーに渡すかどうかを指定します。
- 値：Off | On
- サイトの種類： XenApp Web

UpgradeClientsAtLogin

- 説明：適切なネイティブクライアントまたはCitrix Offline Plug-inのより新しいバージョンを使用できる場合に、ユーザーのログオン時にクライアント検出および展開処理を自動的に実行するかどうかを指定します。 このパラメーターは、EnableWizardAutoModeがOnの場合にのみ適用されます。
- 値：Off | On
- サイトの種類： XenApp Web

UPNSuffixes

- 説明：指定ユーザーによる認証にUPN認証が制限されるサフィックスを指定します。
- 値：UPNサフィックスのリスト
- サイトの種類： XenApp WebおよびXenApp Services

UserInterfaceBranding

- 説明：XenAppユーザーまたはXenDesktopユーザー向けにサイトを最適化します。 Desktopsを指定すると、XenDesktopユーザーが操作しやすいようにサイトの機能が変更されます。 XenDesktopを運用するすべての環境でこの設定を使用することをお勧めします。
- 値：Applications | Desktops

- サイトの種類： XenApp Web

UserInterfaceLayout

- 説明：コンパクトなユーザーインターフェイスを使用するかどうかを指定します。
- 値：Auto | Normal | Compact
- サイトの種類： XenApp Web

UserInterfaceMode

- 説明：［ログオン］画面の外観を指定します。 Simpleを指定すると、選択した認証方法のログオンフィールドのみが表示されます。 Advancedを指定すると、ログオン前の［メッセージ］画面や［設定］画面にアクセスできるナビゲーションバーが表示されます。
- 値：Simple | Advanced
- サイトの種類： XenApp Web

ViewStyles

- 説明：背景イメージをすべて表示する場合の［アプリケーション］画面の表示スタイルを指定します。
- 値：Details | Groups | Icons | List | Tree
- サイトの種類： XenApp Web

WebSessionTimeout

- 説明：アイドル状態のWebブラウザーセッションのタイムアウトを指定します。
- 値：分数（20）
- サイトの種類： XenApp Web

Welcome Message_LanguageCode

- 説明：［ログオン］画面のウェルカム領域に表示されるローカライズされたウェルカムメッセージを指定します。 LanguageCodeは、ja、en、fr、de、es、またはそのほかのサポートされている言語の識別子です。
- 値：なし。 テキスト形式の文字列と、任意の数の改行タグ（
）とハイパーリンク
- サイトの種類：XenApp Web

WIAuthenticationMethods

- 説明：Access Gatewayに統合されないサイトに対する許可された認証方法を指定します。 これはコンマ区切りの一覧で、指定できる値を任意の数だけ、任意の順序で指定できます。
- 値：Explicit、Anonymous、Certificate SingleSignOn、Certificate、SingleSignOnの組み合わせ

- サイトの種類：XenApp Web、XenApp Services、およびDesktop Appliance Connector

config.xmlファイルのパラメーター

更新日： 2014-12-02

config.xmlファイルには、多数のパラメーターが含まれており、複数のカテゴリに分類されています。 次のカテゴリに含まれるパラメーターを編集できます。

- FolderDisplay： ソースのアイコンを表示する場所を［スタート］メニュー、ローカルのWindowsデスクトップ、または通知領域で指定します。 ［スタート］メニューの特定のフォルダーを指定する追加パラメーターがあります。 これのパラメーターは、Citrix Online Plug-inの［オプション］ダイアログボックスの［アプリケーションの表示］ページで設定するオプションに相当します。

- DesktopIntegration： アプリケーションのショートカットを［スタート］メニュー、Windowsデスクトップ、または通知領域に表示するかどうかを指定します。

- ConfigurationFile： 別の場所にあるconfig.xmlを使用させる場合は、そのURLを指定します。 これにより、ユーザーを別のWeb Interfaceサーバーに移行できます。

- Request： ユーザーがアクセスするリソースの一覧の取得先と、その一覧の更新間隔を指定します。

- Failover： プライマリサーバーが使用できなくなったときに接続するバックアップサーバーのURLを指定します。

- ログオン。使用するログオン方法を指定します。

- ChangePassword： ユーザーによるパスワード変更を許可するかどうか、および要求の転送パスを指定します。

- UserInterface： Citrix Online Plug-inの画面に表示するオプションを指定します。

- ReconnectOptions： ユーザーにワークスペースコントロール機能の使用を許可するかどうかを指定します。

- FileCleanup： ユーザーがCitrix Online Plug-inからログオフしたときに、アプリケーションのショートカットを削除するかどうかを指定します。

- ICA_Options： プラグインコネクションで使用可能な表示およびサウンドオプションを定義します。 このパラメーターは、Citrix Online Plug-inの［オプション］ダイアログボックスの［セッションオプション］ページの設定に相当します。

- AppAccess： ユーザーが使用できるアプリケーションの種類を指定します。

config.xmlファイルの使用について詳しくは、「Online Plug-in for Windows」を参照してください。

Citrix Online Plug-inに関する注意事項

WebInterface.confパラメーターの設定には、Citrix Online Plug-in要求の検証に影響を与えるものがあります。 WebInterface.confファイルの設定とCitrix Online Plug-inのconfig.xmlファイルの設定に一貫性を持たせることをお勧めします。

WebInterface.confファイルのパラメーター

次の表に、config.xmlファイルのパラメーターと整合性がある必要があるWebInterface.confのパラメーターを示します。 また、Citrix Online Plug-inに影響するパラメーターおよびその推奨設定も示します。

パラメーター	推奨設定
LoginType	NDSに設定する場合、config.xmlでNovell認証を有効にする必要があります。
NDSTreeName	config.xmlファイルのLogonセクションのDefaultTreeに同じ値を設定する必要があります。
PNAChangePasswordMethod	config.xmlファイルのChangePasswordセクションのMethodに同じ値を設定する必要があります。
WIAuthenticationMethods	WebInterface.confファイルで構成されている認証方法と同じ方法を使用します。 config.xmlでの認証方法がWeb Interfaceと異なると、認証エラーが発生します。

Citrix Online Plug-in用にWeb Interfaceを構成するには

1. テキストエディターを使って、Webinterface.confファイルを開きます。
2. 以下のパラメーターを見つけます。
   - LoginType
   - NDSTreeName
   - PNAChangePasswordMethod
   - WIAuthenticationMethods
3. 「config.xmlファイルのパラメーター」を参照して、これらのパラメーターの設定を必要に応じて変更します。
4. Web Interfaceサーバーを再起動すると、変更が適用されます。

WebInterface.confファイルのパラメーターについて詳しくは、「WebInterface.confのパラメーター」を参照してください。

bootstrap.confファイルの設定

次の表に、bootstrap.confファイルのパラメーターを示します。

パラメーター	説明	値	サイトの種類
ConfigurationLocation	Web Interfaceサイトが構成を取得するファイルを指定します。 これはローカルファイル、またはIISでホストされるサイトの場合はネットワークで共有されるリモートファイルです。	WebInterface.confの絶対パス	XenApp Web XenApp Services
DefaultLocale	ユーザーのWebブラウザーから未対応の言語が要求されたときに使用するデフォルトの言語を指定します。	en | fr | de | es | ja | そのほかのサポートされている言語の識別子	XenApp Web XenApp Services
SiteName	Citrix Web Interface管理コンソールに表示されるサイト名を指定します。 デフォルトの設定はサイトのURLです。	有効な文字列	XenApp Web XenApp Services

XenApp 4.0 with Feature Pack 1 for UNIXのサポートを構成するには

この例では、XenApp 4.0 with Feature Pack 1 for UNIXと互換性があるサイトを構成します。 新しいバージョンのWeb Interfaceで作成されるサイトは、そのままではこの製品で使用できません。以下の追加構成が必要です。

1. テキストエディターを使ってWebInterface.confファイルを開き、次の行に移動します。

   OverrideIcaClientname=Off

   RequireLaunchReference=On

2. Change the settings as shown below:

   OverrideIcaClientname=On

   RequireLaunchReference=Off

   注： RequireLaunchReferenceパラメーターをOffにすると、XenApp VM Hosted Appsでのパススルー認証が無効になります。 つまり、このサイトからログオンするユーザーは、XenApp VM Hosted Appsで公開されているアプリケーションにアクセスするたびにアカウント情報を入力する必要があります。

ユーザーローミングを構成するには

この例では、アメリカオフィスのユーザーグループを特定のサーバーファームに割り当て、これによりこのユーザーグループのメンバーは日本オフィスからローカルのWeb Interfaceサーバーにログオンして自動的にアメリカオフィスのサーバーファームから英語版のリソースを受信できます。

サーバー“waltz”で実行中のCitrix XML Serviceがある既存のサーバーファームは、すでに構成ファイル内でFarm1として定義されており、アメリカのWeb Interfaceサーバーにログオンするすべてユーザーが使用できます。 ユーザーグループ“SalesMgrs”および“SalesTeam”は、ドメイン“ussales.mycompany.com”で、ユーザーグループ“Accounts”はドメイン“finance.mycompany.com”です。 これらのグループのユーザーをCitrix XML Serviceを実行するサーバー名が“foxtrot”および“tango”のサーバーファームに割り当てるには、次のようにします。

1. テキストエディターを使って、アメリカのWeb Interfaceサーバーの WebInterface.confファイルを開き、次の行に移動します。

   ```
   Farm1=waltz,Name:Farm1,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,L
   ```

   > 重要： ユーザーローミングが有効な場合、構成ファイル内で最初に定義されているサーバーファームは、XenApp 6.0以降またはXenDesktop 4.0以降を実行している必要があります。 最初のサーバーファームで以前のバージョンを実行している場合は、ユーザーに対してリソースが表示されません。

2. 次の行を追加して、新しいサーバーファームを定義します。

   ```
   Farm2=foxtrot,Name:Farm2,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,
   Farm3=tango,Name:Farm3,XMLPort:80,Transport:HTTP,SSLRelayPort:443,BypassDuration:60,L
   ```

3. 次の行を追加して、新しいサーバーファームにユーザーグループを割り当てます。

   ```
   Farm2Groups=ussales.mycompany.com¥SalesMgrs,ussales.mycompany.com¥SalesTeam,financ
   Farm3Groups=ussales.mycompany.com¥SalesMgrs
   ```

   Farm*n*Groups[redacted]**Farm*n***[redacted]

4. 次の行を追加して、ユーザーが既存のサーバーファームに引き続きアクセスできるようにします。

   ```
   Farm1Groups=mycompany.com¥DomainUsers
   ```

   [redacted]Web Interface[redacted]

5. テキストエディターを使用して日本のWeb InterfaceサーバーのWebInterface.confファイルを開き、手順2.と3.で示した行を追加します。 ローカルユーザーが引き続きアクセスできるように、ユーザーグループを既存の日本のサーバーファームに割り当てる必要があります。

ログメッセージとイベントID

更新日： 2014-11-25

Web Interfaceは、すべてのサイトの種類およびプラットフォームのイベントIDのログを記録します。 Windowsオペレーティングシステムでは、イベントビューアーを使ってイベントIDを確認し、これをCitrix EdgeSightまたはサードパーティの管理とレポートツールで使用できます。 Java Application Serverの場合、Webサーバーのログファイルに書き込まれるログメッセージの一部としてイベントIDが含まれます。

次に表は、Web InterfaceイベントIDおよびそれに割り当てられたログメッセージを示しています。 また問題についての簡単な説明と、その解決策について示しています。

イベントID	メッセージ	重要度	説明
10001	構成解析エラー<エラーの説明>が発生しました。	エラー	サイト構成ファイルに問題があります。 WebInterface.confでエラーをチェックしてください。
10002	構成読み込みエラーが発生しました。	エラー	サイト構成ファイルがないか、またはアクセスできません。 WebInterface.confが削除されていないか、またこのファイルを読み取ることができる適切な権限が構成されているか、チェックしてください。
10003	Citrix Online Plug-in構成を取得できませんでした。	エラー	Citrix Online Plug-in構成ファイルがないか、またはアクセスできません。 config.xmlが削除されていないか、またこのファイルを読み取ることができる適切な権限が構成されているか、チェックしてください。
10004	構成データが正常にリロードされました。	情報	サイト構成ファイル（WebInterface.conf）またはOnline Plug-in構成ファイル（config.xml）に対する最近の変更が検証され、受け入れられました。
10005	次のキーは、構成ファイルで複製されます：<キー名>	警告	サイト構成ファイルに重複パラメーターがあります。 WebInterface.confのエラーを修正してください。
10006	不明な認証ポイントの種類：<認証ポイント>	エラー	サイト構成ファイルのAuthenticationPointパラメーターに不正な値が指定されています。 WebInterface.confのエラーを修正してください。

10007	ユーザーのローミングが有効な場合、匿名ユーザーによるログオンは許可されていません。	エラー	XenDesktopは匿名ユーザーをサポートしていません。XenDesktopでユーザーのローミングを使用するには、匿名ユーザー認証を無効にします。
10008	構成が無効です：このバージョンのWeb Interfaceでは、NDS認証がサポートされていません。	エラー	サイトの認証方法を再構成して、ユーザープリンシパル名またはMicrosoftドメインベースの認証を選択します。
10009	構成が無効です：このバージョンのWeb Interfaceでは、スマートカード認証またはパススルー認証がサポートされていません。	エラー	UNIX/JSPバージョンのWeb Interfaceにおいて、Web Interfaceの認証ポイントでパススルー認証、スマートカード認証、またはスマートカードパススルー認証を使用する、またはAccess Gatewayの認証ポイントでスマートカード認証またはスマートカードパススルー認証を使用する場合に、このエラーが表示されます。
10010	2要素認証の構成に問題があります。	エラー	Aladdin SafeWord for Citrix、RSA SecurID、またはRADIUSサーバー認証が正しく構成されているかチェックしてください。
10011	現在有効な認証の方法はありません。	エラー	サイトが正しく構成されていることと、有効な認証方法が指定されていることをチェックしてください。
10101	Protocol Transition Serviceは不正に構成されています。web.configでtokenManagerが定義されていて、1つ以上のトークンサービスを定義しているか確認してください。	エラー	XenApp Webサイトのweb.configファイルが、割り当てられた証明書リファレンスがある1つ以上のトークン発行者を指定しているかチェックしてください。このリファレンスは、Access Gatewayサービスからのスマートカードパススルーによる信頼関係を保護するために使用できます。
10201	構成が無効です。ICAファイル署名は、このバージョンのWeb Interfaceではサポートされていません。	エラー	ICAファイルの署名機能を使用するにはWeb Interface 5.4以降を実行する必要があります。
10202	古いバージョンのクライアントのサポートが有効な場合は、ICAファイル署名を使用できません。	エラー	ICAファイルの署名機能を有効にするには、ユーザーがネイティブクライアントを使用するようにサイトを構成して、Webinterface.confファイルのEnableLegacyIcaClientSupportをOffに設定する必要があります。

10203	ICAファイル署名は、オフラインアプリケーションでは使用できません。	エラー	オンラインアプリケーションまたはデュアルモードアプリケーションを表示するようにサイトが構成されているかチェックしてください。
10204	ICAファイル署名を使用するために、ユーザーによるネイティブクライアントの選択を許可する必要があります。	情報	ICAファイルの署名機能を有効にするには、ネイティブクライアントを使用するようにサイトを構成する必要があります。
10205	ICAファイルに署名しようとしてエラーが発生しました：<エラーメッセージ>。	エラー	実行すべき作業について詳しくは、エラーメッセージの内容を参照してください。
10206	ICAファイルに署名しようとしてエラーが発生しました：<>。 Webサーバーを再起動して、ICA File Signingサービスを有効にする必要があります。	エラー	Webサーバーを再起動して、Web Interface管理コンソールでICAファイルの署名機能が有効になっていることを確認します。
11001	クライアント検出および展開処理に無効なリダイレクト先URLが渡されました。	エラー	リダイレクト先URLは、ユーザーがクライアント検出および展開処理を完了した際に転送されるWebページを指定します。 このエラーは、リダイレクト先URLがサイトのコードで変更されたことを示しています。
11002	クライアント検出および展開処理により、有効なクライアントを展開できませんでした。 XenApp WebサイトのClientsフォルダーに、ユーザーのWebブラウザー、オペレーティングシステム、およびアクセス方法に対応したクライアントがあることを確認してください。	エラー	ユーザーがサイトからクライアントを取得できませんでした。 ユーザーデバイス、オペレーティングシステム、Webブラウザー、およびアクセス方法に対して適切なクライアントが、Webサーバーで使用でき、サイトで有効になっているかチェックしてください。
11003	ユーザーのコンピューターのオペレーティングシステムは、クライアント検出および展開処理をサポートしていません。	エラー	クライアント検出および展開処理がユーザーデバイス上のオペレーティングシステムを識別できなかったため、ユーザーがサイトからクライアントを取得できませんでした。
11004	プラットフォーム情報を提供するUser-Agent HTTPヘッダーがないため、ユーザーデバイス<IPアドレス>で実行中のブラウザーからの要求を処理できません。	エラー	ブラウザーにより送信された要求にユーザーのブラウザーとプラットフォームを識別するUser-Agent HTTPヘッダーがないため、ユーザーがサイトにアクセスできませんでした。 ユーザー要求からUser-Agentヘッダーが取り除かれていないか、ネットワーク環境をチェックしてください。

12001	Web Interfaceにより、一意のログID<ID>があるログメッセージが<数>回記録されませんでした。 レポート率は下がっています。Web Interfaceはこれらのメッセージのログの記録を再開します。	情報	Citrix Web Interface管理コンソールの［サイトメンテナンス］の［診断ログ］タスクを使って、重複するイベントが繰り返しログに記録されないようにしたり、重複イベントをログに記録する回数と頻度を構成したりします。
12002	レポート率が下がるまで、一意のログID<ID>があるログメッセージは記録されません。	情報	Citrix Web Interface管理コンソールの［サイトメンテナンス］の［診断ログ］タスクを使って、重複するイベントが繰り返しログに記録されないようにしたり、重複イベントをログに記録する回数と頻度を構成したりします。
12003	イベントIDファイルをロードできませんでした。 イベントIDファイルへのパスが正しいか<ファイル名>をチェックしてください。	警告	イベントIDファイルがないか、またはアクセスできません。web.config（IISでホストされるサイト）またはweb.xml（Java Application Serverでホストされるサイト）で指定されたパスが正しいかチェックしてください。 また、WebInterfaceEventIds.txtが削除されていないか、またこのファイルを読み取ることができる適切な権限が構成されているか、チェックしてください。
12004	メッセージキー<キー名>は有効なイベントIDと対応していません。 イベントIDファイルに<キー名>に対する有効なエントリがあるかチェックしてください。 イベントIDは65535未満の整数である必要があります。	警告	指定したイベントIDがイベントIDファイルで見つかりません。このイベントIDがWebInterfaceEventIds.txtから削除されてないかチェックしてください。
13001	SSL接続は、<サーバーアドレス>でWebサービスとの通信を確立できませんでした：<ポート>。 基になるプラットフォームから、次のメッセージが報告されました：<エラーの説明>	エラー	SSLエラーが発生しました。エラーメッセージの最後に詳細があります。 Web InterfaceがSSLを介してAccess GatewayまたはPassword Managerと正常に統合するよう構成されているかチェックしてください。
13002	1つ以上のグループに対してセキュリティIDを取得できませんでした。 Citrix XML Serviceがアクセス可能で、ユーザーローミングをサポートし、また構成ファイル内のグループが正しいかを確認してください。	エラー	ユーザーのローミング機能に対して構成されている1つ以上のユーザーグループに問題があります。 サーバーファームのすべてのサーバーでユーザーのローミング機能をサポートするバージョンのXenAppまたはXenDesktopを実行しているかチェックしてください。 また、指定のグループ名が有効で、Citrixサーバーとの通信を実行できるかチェックしてください。

14001	RSA SecurID ACE/Agentに問題があります。 ACE/Agentが正常にインストールされているか、aceclnt.dllファイルへのパスがPATH環境変数に追加されたかをチェックしてください。	エラー	Web Interface for Microsoft Internet Information ServicesでSecurID認証を使用するには、RSA Authentication Agent for Web for Internet Information Servicesをインストールしてから Web Interfaceをインストールする必要があります。
14002	RSA SecurID ACE/Agentに問題があります。 正しいバージョンのRSA SecurID ACE/Agentをインストールしているかチェックしてください。	エラー	サポートされているバージョンのRSA Authentication Agent for Web for Internet Information ServicesがWebサーバーにインストールされているかチェックしてください。
14003	Aladdin SafeWord Agentに問題があります。 Aladdin SafeWord Agentが正常にインストールされているかどうかチェックしてください。	エラー	WebサーバーにSafeWord Agent for the Web Interfaceがインストールされているかチェックしてください。 SafeWord Agentをインストールしてから、Web Interfaceをインストールする必要があります。
14004	RSA SecurID ACE/Agentによりキャッシュされたパスワードを更新できません。 RSA SecurID ACE/AgentとACE/Serverのバージョンに互換性があるか、またACE/AgentとACE/Serverの両方がWindowsパスワード統合機能を使用するために構成されているかをチェックしてください。	エラー	RSA Authentication ManagerとRSA Authentication Agent for Web for Internet Information Servicesのバージョンに互換性があるかチェックしてください。 また、RSA Authentication Managerデータベースのシステムパラメーターを構成して、システムレベルでのWindowsパスワード統合が有効かチェックしてください。
14005	RSA SecurID ACE/Agentによりキャッシュされたパスワードを取得できません。 RSA SecurID ACE/AgentとACE/Serverのバージョンに互換性があるか、またACE/AgentとACE/Serverの両方がWindowsパスワード統合機能を使用するために構成されているかをチェックしてください。	エラー	RSA Authentication ManagerとRSA Authentication Agent for Web for Internet Information Servicesのバージョンに互換性があるかチェックしてください。 また、RSA Authentication Managerデータベースのシステムパラメーターを構成して、システムレベルでのWindowsパスワード統合が有効かチェックしてください。
14006	ユーザーを認証する際、SafeWord認証システムに問題がありました。	エラー	SafeWordサーバーに問題があります。 詳しくは、SafeWordサーバーのログファイルを参照してください。

14007	RSA SecurID ACE/Agentに問題があります。 Web Interfaceアプリケーションプールが、インストールされたACE/Agentのバージョンに対する適切な32ビットまたは64ビットのアプリケーションに対して構成されているかチェックしてください。	エラー	使用しているバージョンのACE/Agentのアプリケーション要件をチェックしてください。
15001	<ファイルパス>からのクライアントバージョンの読み取りに問題がありました。 ユーザーには、このクライアントの新しいバージョンへのアップグレードメッセージが表示されません。	エラー	指定したクライアントのインストーラーファイルを読み取ることができる適切な権限が構成されているか、チェックしてください。
15002	言語パックファイル<ファイル名>の読み取りに問題があります。 ファイルにアクセスでき、ファイル形式が正しいかをチェックしてください。	エラー	指定したファイルが削除されていないか、またこのファイルを読み取ることができる適切な権限が構成されているか、チェックしてください。
15003	<ディレクトリ名>にアクセスできませんでした。 ユーザーは、このディレクトリ内のクライアントを使用できません。 Network Serviceアカウントに、このディレクトリへアクセスできる適切な権限があることを確認し、Webサーバーを再開してください。	エラー	指定したディレクトリが削除されていないか、またこのディレクトリにアクセスすることができる適切な権限が構成されているか、チェックしてください。
15004	言語パックファイル<ファイル名>の読み取りに問題があります。 ファイルにバージョン宣言がないため、言語パックを使用できません。	エラー	言語パックファイルにバージョン番号がありません。 指定したファイルのエラーを修正してください。
15005	言語パックファイル<ファイル名>の読み取りに問題があります。 言語パックのバージョンは<バージョン番号>で、現在のバージョンのWeb Interfaceと互換性がありません。	エラー	Web Interfaceと言語パックファイルのバージョンに不一致があります。 言語パックは、Web Interfaceのバージョン固有であり、ほかのバージョンには使用できません。 指定したファイルを適切にアップグレードまたはリバートしてください。
15006	言語パックは、デフォルトのロケール<インストールロケール>に対して見つかりませんでした。 言語パック<ファイル名>が見つかりました。これがデフォルトとして使用されます。	警告	Web Interfaceがインストール時に選択したローケルに対する言語パックを見つけることができない場合、Web Interfaceは最初に互換性がある言語パックにフォールバックします。

16001	RADIUSシークレットファイル <ファイルパス>を読み取れません。	エラー	RADIUSシークレットファイルがないか、またはアクセスできません。 web.config（IISでホストされるサイト）または web.xml（Java Application Serverでホストされるサイト）で指定されたパスが正しいかチェックしてください。 また、RADIUSシークレットファイルが削除されていないか、またこのファイルを読み取ることができる適切な権限が構成されているか、チェックしてください。
16002	RADIUSシークレットファイル <ファイルパス>は空です。	エラー	RADIUSプロトコルでは、共有シークレットを使用する必要があります。共有シークレットとは、RADIUSクライアント（Web Interface）と認証先RADIUSサーバーだけが使用できるデータです。 RADIUSシークレットファイルには文字列を含めることができますが、空です。
16003	ユーザーを認証する際、RADIUS認証システムに問題がありました。	エラー	RADIUSサーバーに問題があります。 詳しくは、RADIUSサーバーのログファイルを参照してください。
16004	RADIUS_NAS_IDENTIFIER値とRADIUS_IP_ADDRESS値の両方またはその一方がサイトのWeb構成ファイルにある必要があります。 RADIUS_NAS_IDENTIFIER値には3文字以上含まれる必要があります。 RADIUS_IP_ADDRESSは有効なIPアドレスである必要があります。	エラー	RADIUSプロトコルでは、RADIUSサーバーへのアクセス要求にRADIUSクライアントのIPアドレスまたはほかの識別子（Web Interface）が含まれる必要があります。 web.config（IISでホストされるサイト） web.xml（Java Application Serverでホストされるサイト）に有効なRADIUS NAS IDまたはIPアドレスがあるかチェックしてください。
17001	サーバー<サーバーアドレス> 上のコンテキストルックアップエラー：<例外>。 このサーバーは、アクティブなサーバーの一覧から一時的に削除されました。	エラー	指定したNDSサーバーに問題があります。 問題が解決されるまで、このサーバーは無視されます。 詳しくは、NDSサーバーのログファイルを参照してください。
17002	すべてのNDSサーバーが無効なため、コンテキストルックアップを実行できません。 完全修飾ユーザー名（例：.username.mycompany.com）を使ってログオンしてみてください。	エラー	NDSサーバーにアクセスできませんでした。 .username.mycompany.comの形式で、アカウント情報を入力してみてください。 詳しくは、NDSサーバーのログファイルを参照してください。

18001	<URL>のAdvanced Access Control認証サービスにアクセスしようとして、通信エラーが発生しました。 認証サービスが実行中かチェックしてください。基になるプラットフォームにより、次のメッセージが報告されました：<エラーの説明>。	エラー	Access Gateway認証サービスへのアクセスに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Access Gatewayアプライアンスのログファイルを参照してください。
18002	<URL>のAdvanced Access Control認証サービスを使ってセッションを閉じようとして通信エラーが発生しました。 認証サービスが実行中かチェックしてください。 基になるプラットフォームにより、次のメッセージが報告されました：<エラーの説明>。	エラー	Access Gateway認証サービスへのアクセスに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Access Gatewayアプライアンスのログファイルを参照してください。
18003	Access Gateway認証サービスがユーザーの認証に失敗しました。 サービスにより、次のメッセージが報告されました：<エラーの説明>[状態コード：<コード番号>]。	エラー	Access Gateway認証サービスへのアクセスに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Access Gatewayアプライアンスのログファイルを参照してください。
18004	Access Gateway認証サービスがセッションを閉じることができませんでした。 サービスにより、次のメッセージが報告されました：<エラーの説明>[状態コード：<コード番号>]。	エラー	Access Gateway認証サービスへのアクセスに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Access Gatewayアプライアンスのログファイルを参照してください。
18005	サイト構成の無効なAccess Gateway認証サービスURL：<URL>	エラー	サイト構成ファイルのAGEWebServiceURLパラメーターに不正なURLが指定されています。 WebInterface.confのエラーを修正してください。
18006	ユーザー<ユーザー>はサイト<サイト>にログオンできませんでした。 Webサーバーを再起動して、Access Gatewayサービスからのスマートカードパススルーを有効にする必要があります。	エラー	スマートカードユーザーはAccess Gateway統合サイトにログオンできませんでした。 Webサーバーを再起動して、Access Gatewayサービスからのスマートカードパススルーを実行中にする必要があります。

18007	このバージョンのAccess Gatewayは、Web Interfaceのパスワード変更要求をサポートしていません。 ユーザーによるパスワードの変更を有効にするには、Access Gatewayをこの機能をサポートするバージョンにアップグレードする必要があります。	エラー	サイトではパスワードの変更機能が有効になっているにも関わらずこの機能をサポートするバージョンのAccess Gatewayを使用していない場合に、このエラーが表示されます。 パスワードの変更を無効にするか、またはAccess Gatewayをこの機能をサポートするバージョンにアップグレードします。
19001	ユーザーのリソースから切断中にエラーが発生しました。 ワークスペースコントロールが無効になっているか、匿名ユーザーとしてログオンしているか、またはユーザーのアカウント情報やクライアント名の取得中にエラーが発生しました。	エラー	ワークスペースコントロールに問題があります。 サイトに対してワークスペースコントロールが有効になっているか、またユーザーが匿名ユーザー認証以外の認証方法を使ってログオンしてるかをチェックしてください。
19,002	ユーザーのリソースへの再接続中にエラーが発生しました。 ワークスペースコントロールが無効になっているか、匿名ユーザーとしてログオンしているか、またはユーザーのアカウント情報やクライアント名の取得中にエラーが発生しました。	エラー	ワークスペースコントロールに問題があります。 サイトに対してワークスペースコントロールが有効になっているか、またユーザーが匿名ユーザー認証以外の認証方法を使ってログオンしてるかをチェックしてください。
20001	<URL>のPassword Manager Serviceへアクセスしようとして通信エラーが発生しました。 このサービスが実行中かチェックしてください。 基になるプラットフォームにより、次のメッセージが報告されました：<エラーの説明>。	エラー	Password Manager Serviceへのアクセスに問題があります。 エラーメッセージの最後に詳細があります。 詳しくは、Password Managerサーバーのログファイルを参照してください。
20002	サイト構成の無効なPassword Manager Service URL：<URL>	エラー	サイト構成ファイルのAccount SelfServiceUrlパラメーターに不正なURLが指定されています。 WebInterface.confのエラーを修正してください。
21001	重要なサーバーエラーが発生しました。	エラー	Webページで実行中のスクリプトの1つでJava例外が発生しました。 ページをリロードしてみてください。 または、Citrix Web Interface管理コンソールで［サイトメンテナンス］の［サイトの修復］タスクを使ってサイトのスクリプトを再インストールします。

21002	重要なサーバーエラーが発生しました：<.NETエラーの説明>	エラー	Webページで実行中のスクリプトの1つで.NET例外が発生しました。 ページをリロードしてみてください。 または、Citrix Web Interface管理コンソールで［サイトメンテナンス］の［サイトの修復］タスクを使ってサイトのスクリプトを再インストールします。
21003	エラーのため、パス<サイト構成ディレクトリ>にファイルウオッチャーを作成できませんでした。	エラー	サイト構成フォルダーのパスが正しいか、またこのディレクトリを読み取ることができる適切な権限が構成されているか、チェックしてください。 またはIISを再開し、サイトを更新して最新の構成の変更を適用してください。
21004	Webサーバーの完全修飾ドメイン名にアンダースコア（_）が含まれているため、ユーザーはサイトにアクセスできませんでした。 Webサーバーまたはドメイン、あるいはその両方の名前を変更して、アンダースコアを削除してください。 名前を変更できない場合は、アンダースコアを含まないWebサーバーの代替アドレスを構成するか、WebサーバーのIPアドレスを使ってサイトにアクセスするようユーザーに指示します。	エラー	サイト名にアンダースコアなどの認識できない文字が含まれていると、サイトにアクセスできません。 Webサーバーの名前にアンダースコアが含まれていないか確認し、サーバー名を変更する必要がある場合はWeb Interface管理コンソールを使用します。
21005	クラスID<ID番号>がある Citrix Online Plug-in ActiveX コントロールを開始できませんでした。 サイト構成ファイルで正しいクラスIDが指定されているかチェックしてください。	エラー	ActiveXクラスIDがWebinterface.confファイルのID番号と一致するかチェックしてください。
21006	クラスID<ID番号>がある Citrix Online Plug-in ActiveX コントロールを開始できませんでした。 サイト構成ファイルで正しいクラスIDが指定されているかチェックしてください。	エラー	ActiveXクラスIDがWebinterface.confファイルのID番号と一致するかチェックしてください。
22001	サーバー上で、Client for Java ファイルが見つかりませんでした。 XenApp Webサイトの Clientsフォルダーでこれらのファイルを使用できるか確認してください。	エラー	Client for Javaがないか、またはアクセスできません。 ファイルが削除されていないか、またこのファイルを読み取ることができる適切な権限が構成されているか、チェックしてください。

23001	ユーザー<ユーザー名>のデスクトップにアクセスしようとしてICAエラーが発生しました。	エラー	Citrix Online Plug-inはユーザーのデスクトップにアクセスできませんでした。 デスクトップが実行中でアクセスできるかチェックしてください。
23002	Internet Explorerでユーザー<ユーザー名>のデスクトップにアクセスできませんでした。 ユーザーデバイスにCitrix Desktop Appliance Lockがインストールされていて、Desktop Appliance ConnectorがInternet Explorerの適切なWindowsセキュリティゾーンに追加されているかチェックしてください。	エラー	デスクトップアプライアンスユーザーが全画面のみを実行するモードのデスクトップにアクセスできませんでした。 ユーザーデバイスにCitrix Offline Plug-inが正常にインストールされて構成されているかチェックしてください。
23003	ユーザー<ユーザー名>は、<数>デスクトップへのアクセスを許可されました。 Desktop Appliance Connectorを介して全画面のみを実行するモードのデスクトップにアクセスしているユーザーは、単一のデスクトップへのアクセスのみが許可される必要があります。	警告	1つ以上のデスクトップをデスクトップアプライアンスユーザーが使用できます。 ユーザーはデスクトップにアクセスできます。ただし、必要なデスクトップを選択する方法がないため、ユーザーは次にログオンした際に同じデスクトップには接続できない可能性があります。 ユーザーが単一のデスクトップへのアクセスのみを許可されるよう、Desktop Appliance Connectorを構成してください。
23004	指定の認証方法は無効です。 ExplicitまたはCertificateのいずれかを指定する必要があります。	エラー	ExplicitおよびCertificateの両方の値は、サイト構成ファイルのWIAuthenticationMethodsパラメーターに対して指定されています。 同じDesktop Appliance Connectorに対して指定ユーザーおよびスマートカード認証の両方を有効にすることはできません。 WebInterface.confのエラーを修正してください。
23005	埋め込みスマートカードSSO認証構成が無効です。 認証方法には、Certificateを含める必要があります。	エラー	Desktop Appliance Connectorのサイト構成ファイルのWIAuthenticationMethodsパラメーターに、Certificateを指定する必要があります。 WebInterface.confのエラーを修正してください。

23006	指定の認証方法は無効です。 認証方法の組み合わせはサポートされていません。	エラー	サイト構成ファイルのWIAuthenticationMethodsパラメーターに指定されているDesktop Appliance Connectorの認証方法は共に使用できません。 WebInterface.confのエラーを修正してください。
24001	認証されていないユーザーによるログオンが試みられました。 シャドウアカウントがシステムのすべての指定のユーザーに対して作成されたか検証してください。 問題が続く場合は、Web Interface管理コンソールを使ってサイトの修正を試みてください。	エラー	AD FS統合サイトに問題があります。 ユーザーを認証できませんでした。 リソースパートナードメインのユーザーに対してシャドウアカウントが作成されたかチェックしてください。 または、Citrix Web Interface管理コンソールで［サイトメンテナンス］の［サイトの修復］タスクを使ってサイトを再インストールします。
24002	認証されていないユーザーによるログオンが試みられました。 問題が続く場合は、Web Interface管理コンソールを使ってサイトの修正を試みてください。	エラー	XenApp WebサイトまたはXenApp Servicesサイトに問題があります。 ユーザーを認証できませんでした。 ドメインのユーザーに対してユーザーアカウントが作成されたかチェックしてください。 または、Citrix Web Interface管理コンソールで［サイトメンテナンス］の［サイトの修復］タスクを使ってサイトを再インストールします。
30001	サーバー<サーバーファーム名>からの読み取り処理中にエラーが発生しました。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30002	サーバー<サーバーファーム名>への情報の書き込み中にエラーが発生しました。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。

30003	ポート<ポート>のサーバー<サーバーアドレス>への接続処理中にエラーが発生しました。 Citrix XML Serviceが実行中で、適切なポートが使用中であることを確認してください。 Citrix XML ServiceがIISとポートを共有している場合は、Microsoft インターネットインフォメーションサービス（IIS）が実行中であることを確認してください。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 Citrix XML ServiceとIISとTCP/IPポートを共有するように構成されているかをチェックし、共有している場合はIISが実行中かをチェックします。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30004	サーバー名<サーバーアドレス>を解決できません。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30005	サーバーが送信したHTTP構文にエラーがあります。 現在のWeb Interfaceのバージョンと使用中のサーバーとに互換性があるか確認してください。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 サーバーファームでXenDesktopまたはPresentation Server 4.5以降が実行されているかチェックしてください。 サーバーファーム内のすべてのサーバーで同じ製品およびバージョンを使用することをお勧めします。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30006	サーバーが、形式の正しくない、または予期しない応答を返しました。 現在のWeb Interfaceのバージョンと使用中のサーバーとに互換性があるか確認してください。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 サーバーファームでXenDesktopまたはPresentation Server 4.5以降が実行されているかチェックしてください。 サーバーファーム内のすべてのサーバーで同じ製品およびバージョンを使用することをお勧めします。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30008	サーバーが予期せず接続を閉じました。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。

30009	サーバーが、エラー<詳細>の発生を示すHTTPヘッダーを送信しました。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30010	現在、サーバーは要求を処理できません。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30011	要求の処理中にサーバーでエラーが発生しました。エラー：<詳細> このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30012	サーバーでバージョンの不一致エラーが発生しました。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30013	サーバーが不正な要求を受け取りました。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30014	サーバーで要求の解析中にエラーが発生しました。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30015	アドレス<ファイルパス>のCitrix XML Serviceは要求を処理できません。	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30016	Citrix XML Serviceオブジェクトが見つかりません：<詳細>。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30017	Citrix XML Serviceメソッドがサポートされていません：<詳細>。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。

30018	受け入れ可能なCitrix XML Serviceがありません：<詳細>。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30019	Citrix XML Serviceの要求の長さが必要です：<詳細>。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30020	Citrix XML Serviceの要求が短すぎます：<詳細>。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30021	Citrix XML Serviceの要求が最大サイズを越えています：<詳細>。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30022	Citrix XML Serviceまたはサーバーを使用できないか、過負荷状態です：<詳細>。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30023	サーバーが送信したXML文書を処理できません。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30024	無効なXMLを含んでいるため、サーバーが送信したXML文書を処理できません。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30025	サーバー<サーバーファーム名>からの読み取り処理中にエラーが発生しました。 SSL接続を使用するように構成されていますが、SSL Relayでないサーバーと通信したためにエラーが発生した可能性があります。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 サーバーファームへの接続でSSL/TLS暗号化を使用するには、各サーバー上でCitrix SSL Relayを使用して必要な構成を行います。 詳しくは、Citrixのサーバーのログファイルを参照してください。

30026	Citrix SSL Relay<サーバーアドレス>：<ポート>による接続中にエラーが発生しました。 Citrix SSL Relayが実行中で、有効なリスナーポートが割り当てられていることを確認してください。 また、Citrix SSL Relayアクセスのために構成されるサーバー証明書内の名前は、接続しようとしたサーバー名と完全に一致している必要があります。 このメッセージは、アドレス<ファイルパス>のCitrix XML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 SSL Relayが実行中で適切なポート（通常はポート443）をリスンしており、またSSL Relayサーバー証明書に接続が試みられたサーバーの（大文字小文字の別も一致する）完全修飾名を含まれているかをチェックします。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30027	サーバーのいずれかのサーバーでチケット機能がサポートされていない可能性があります。 この機能を使用するには、XML Serviceを実行中のサーバーをアップグレードするか、チケット機能を無効にしてください。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 サーバーファームのすべてのサーバーでXenDesktopまたはMetaFrame XP 1.0以降が実行されているかチェックしてください。 サーバーファーム内のすべてのサーバーで同じ製品およびバージョンを使用することをお勧めします。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30028	Citrix SSL Relay名<サーバーアドレス>を解決できません。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30029	SSL接続を確立できません：<SSLエラーの説明>。 このメッセージは、アドレス<ファイルパス>のCitrix XML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30030	Citrix SSL Relay接続を確立できません：<SSLエラーの説明>。 このメッセージは、アドレス<ファイルパス>のCitrix XML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30031	アドレス<ファイルパス>のCitrix XML Serviceは機能<機能名>をサポートしません。	エラー	サーバーファームのすべてのサーバーで指定の機能をサポートするバージョンのXenAppまたはXenDesktopを実行していることをチェックしてください。 詳しくは、「必要なソフトウェア」を参照してください。

30101	パスワードの変更は無効になりました。	エラー	セキュリティ上の理由から、ユーザーはWindowsパスワードを変更できませんでした。 詳しくは、Citrixのサーバーまたはドメインコントローラー、またはその両方のログファイルを参照してください。
30102	アドレス<ファイルパス>のXML Serviceから原因不明のエラーが発生しました。	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30103	代替アドレスが見つかりませんでした。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30104	リソースにアクセスするためにサーバーへ接続しようとしてエラーが発生しました。 接続先のサーバーが動作しており、ネットワークが正しく機能していることを確認してください。 このエラーは、アドレス<ファイルパス>のCitrix XML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 問題に対して、サーバーファームおよびネットワークをチェックしてください。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30105	サーバーファームがサーバーを信頼していません。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Web InterfaceサーバーとCitrix XML Service間に信頼関係があるかチェックしてください。 詳しくは、「XenApp Webサイトでのワークスペースコントロールおよび統合された認証方法の併用」を参照してください。
30106	Citrixサーバーは、必要な操作をサポートするためにライセンスされていません。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 Citrixライセンスサーバーが実行中で、アクセスできることをチェックしてください。 最新の製品との互換性を維持するため、ライセンスサーバーを最新のバージョンにアップグレードすることをお勧めします。 詳しくは、Citrixのサーバーまたはライセンスサーバー、またはその両方のログファイルを参照してください。

30107	サーバーが過度にビジー状態になっているため、選択したリソースにアクセスできないことが報告されました。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 サーバーファームが過負荷状態になってないかチェックしてください。詳しくは、Citrixのサーバーのログファイルを参照してください。
30108	サーバーでチケット機能が無効になっています。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 サーバーファーム内のすべてのサーバーで、Citrix XML Serviceと通信するために同じポートを使用しているかチェックしてください。詳しくは、Citrixのサーバーのログファイルを参照してください。
30109	アドレス<ファイルパス>のCitrix XML Serviceが未登録エラーを報告しました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30110	アドレス<ファイルパス>のCitrix XML Serviceにより、エラーID<エラーID>で種類<エラーの種類>のエラーが報告されました。 XML Serviceを実行しているサーバーによっては、サーバーのイベントログで有効な追加情報があることがあります。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30111	Citrixの製品が動作するサーバーは指定のアドレスの種類をサポートしていません。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30112	デスクトップグループ<グループ名>にアクセスする場合、ユーザー<ユーザー名>が使用できるリソースがありません。 このメッセージは、アドレス<ファイルパス>のCitrix XML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 ユーザーに指定のデスクトップグループが割り当てられていて、グループに使用可能な未使用のデスクトップがあるかチェックしてください。 詳しくは、Citrixのサーバーのログファイルを参照してください。

30113	ユーザー<ユーザー名>のデスクトップグループ<グループ名>を初期化中に、Citrix製品が動作するサーバーからの接続要求が拒否されました。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30114	Citrixの製品が動作するサーバーは、ユーザーのセキュリティIDを取得するためのアクセスが拒否されました。 Active DirectoryのToken-Groups-Global-And-Universal属性に対するXML Service読み取り許可を認めるか、XML Serviceのセキュリティ IDエミュレーションを無効にします。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 ユーザーのセキュリティIDを列挙するようにCitrix XML Serviceが構成される場合、Active Directoryで適切な権限が付与されているかをチェックしてください。 詳しくは、CTX118708およびCitrixのサーバーのログファイルを参照してください。
30115	Citrixの製品が動作するサーバーは、ユーザーのセキュリティIDを取得できませんでした。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、CTX118708およびCitrixのサーバーのログファイルを参照してください。
30116	デスクトップグループ<グループ名>を初期化している場合、ユーザー<ユーザー名>のメンテナンスモードのデスクトップに接続できません。 このメッセージは、アドレス<ファイルパス>のCitrix XML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 ユーザーのデスクトップがメンテナンスモードになっていないかチェックしてください。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30117	サーバーはデスクトップ再起動操作をサポートしていません。このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 サーバーファームでXenDesktop 3.0以降が実行されているかチェックしてください。 サーバーファーム内のすべてのサーバーで同じ製品およびバージョンを使用することをお勧めします。 詳しくは、Citrixのサーバーのログファイルを参照してください。

30118	ユーザー<ユーザー名>のデスクトップグループ<グループ名>のマシンの電源がオフになるのを待っている間に、Citrixサーバーがタイムアウトしました。このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30119	ユーザー<ユーザー名>のデスクトップグループ<グループ名>のメンテナンスモードになっているマシンの電源をオフにできません。 このメッセージは、アドレス<ファイルパス>のCitrix XML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 ユーザーのデスクトップがメンテナンスモードになっていないかチェックしてください。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30120	ユーザー<ユーザー名>を見つけることができません。 このメッセージは、アドレス<ファイルパス>のCitrix XML Serviceから報告されました。 <エラーの説明>	エラー	Citrix XML Serviceに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30201	無効なSecure Ticket Authorityアドレス：<URL>。 <エラーの説明>	エラー	サイト構成ファイルのCSG_STA_ URLnパラメーターに不正なURLが指定されています。 WebInterface.confのエラーを修正してください。
30202	Secure Ticket Authority<URL>は、バージョン4要求をサポートしません。 すべてのSecure Ticket Authority通信は、バージョン1に戻されます。 Secure Gateway を介する新しい接続ではセッション画面の保持を実行できません。	エラー	使用中のSecure Gatewayのバージョンは、Secure Ticket Authority冗長機能をサポートしません。 そのため、この機能は無効となっています。
30203	Secure Ticket Authority<URL>は、予期しない認証または種類（<エラーの種類>、<エラーID>、<SSLエラーの説明>、<詳細>）とチケットを返しました。 <エラーの説明>	エラー	Secure Ticket Authorityに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30204	指定したSecure Ticket Authorityにアクセスできませんでした。このSecure Ticket Authorityは、アクティブなサービスの一覧から一時的に削除されました。	エラー	Secure Ticket Authorityに問題があります。 問題が解決されるまで、このサービスは無視されます。 詳しくは、Citrixのサーバーのログファイルを参照してください。

30205	すべての構成されたSecure Ticket Authorityは、このXMLトランザクションへの応答に失敗しました。	エラー	Secure Ticket Authorityにアクセスできませんでした。 Webサーバーを再起動してみてください。 詳しくは、Citrixのサーバーのログファイルを参照してください。
30301	HTTP応答は、この接続が閉じられたことを示しています。	エラー	サーバーファームでXenDesktopまたはPresentation Server 4.5以降が実行されているかチェックしてください。 サーバーファーム内のすべてのサーバーで同じ製品およびバージョンを使用することをお勧めします。
30401	プールされたソケットは、トランザクション層により強制的に破棄されました。	エラー	破損アプリケーションについてファームデータストアをチェックしてください。 詳しくは、CTX114769を参照してください。
31001	指定したCitrix XML Serviceと通信できませんでした。このサービスはアクティブなサービスの一覧から一時的に削除されました。	エラー	Citrix XML Serviceに問題があります。 問題が解決されるまで、このサーバーは無視されます。 詳しくは、Citrixのサーバーのログファイルを参照してください。
31002	Citrix XML Serviceトランザクションに失敗しましたが、XML Serviceはアクティブなサーバーの一覧から削除されませんでした。	エラー	Citrix XML Serviceにはアクセスできますが、要求またはインストラクションを完了できませんでした。 詳しくは、Citrixのサーバーのログファイルを参照してください。
31003	サーバーファーム<サーバーファーム名>に対して構成されたすべてのCitrix XML Serviceは、このXML Serviceトランザクションに応答できませんでした。	エラー	指定のサーバーファームに対するCitrix XML Serviceホストにアクセスできませんでした。 Webサーバーを再起動してみてください。 詳しくは、Citrixのサーバーのログファイルを参照してください。
31004	XMLプロトコルエラー<エラーID>をアクセス状態エラーに変換できませんでした。	エラー	ユーザーにCitrixのサーバーに対するActive Directoryログオン権限があるかチェックしてください。
31005	<数>のうち<数>のリソースが無効なため無視されます。	エラー	Citrix XML Serviceは使用できるリソースのすべてを列挙できませんでした。 詳しくは、Citrixのサーバーのログファイルを参照してください。

31006	ユーザー<ユーザー名>にはライセンスがないため、このユーザーのログオンは拒否されました。	エラー	使用できるCitrixライセンスまたはMicrosoftリモートデスクトップサービスのクライアントアクセスライセンスがないため、ユーザーはログオンできませんでした。 Citrixライセンスサーバーが実行中で、アクセスできることをチェックしてください。 最新の製品との互換性を維持するため、ライセンスサーバーを最新のバージョンにアップグレードすることをお勧めします。 詳しくは、Citrixのサーバーまたはライセンスサーバー、またはその両方のログファイルを参照してください。
31007	Citrixのサーバーはワークスペースコントロールをサポートするようにライセンスされていません。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。	エラー	ワークスペースコントロール機能を装備した製品エディションでCitrixライセンスが有効かチェックしてください。 また、Citrixライセンスサーバーが実行中で、アクセスできることをチェックしてください。 最新の製品との互換性を維持するため、ライセンスサーバーを最新のバージョンにアップグレードすることをお勧めします。 詳しくは、Citrixのサーバーまたはライセンスサーバー、またはその両方のログファイルを参照してください。
31008	Citrixのサーバーはリソース<リソース名>を起動するようにライセンスされていません。 このメッセージは、アドレス<ファイルパス>のXML Serviceから報告されました。	エラー	この種類のリソースを含む製品エディションでCitrixライセンスが有効かチェックしてください。 また、Citrixライセンスサーバーが実行中で、アクセスできることをチェックしてください。 最新の製品との互換性を維持するため、ライセンスサーバーを最新のバージョンにアップグレードすることをお勧めします。 詳しくは、Citrixのサーバーまたはライセンスサーバー、またはその両方のログファイルを参照してください。

31009	次のアカウントのアカウントデータを取得できません：<アカウント名の一覧>名前のスペルが正しいかチェックしてください。このメッセージは、アドレス<ファイルパス>のCitrix XML Serviceから報告されました。	エラー	Citrix XML Serviceは指定のアカウントにアクセスできません。アカウントが削除されていないか、またCitrix XML Serviceで読み取ることができる適切な権限が構成されているか、チェックしてください。 また、アカウント名が正しく入力されているかチェックしてください。 詳しくは、Citrixのサーバーのログファイルを参照してください。
31101	ユーザー<ユーザー名>は、サーバーセッション<セッションID>を実行していますが、このユーザーにはセッションを作成したリソース<リソース名>へのアクセス権がありません。 このため、ユーザーはこのセッションにアクセスできません。	エラー	ユーザーのセッションがアクティブな間に、ユーザーのアクセス権限が変更されました。 セッションをリセットしてください。 これにより、ユーザーの作業データが失われます。 詳しくは、Citrixのサーバーのログファイルを参照してください。
31201	チケット機能を使用するようにサーバーファーム<サーバーファーム名>が構成されましたが、チケットタグを受信していません。 サーバーファームがチケット機能をサポートしているかをチェックしてください。	エラー	指定したサーバーファームのすべてのサーバーでXenDesktopまたはMetaFrame XP 1.0以降が実行されているかチェックしてください。 サーバーファーム内のすべてのサーバーで同じ製品およびバージョンを使用することをお勧めします。 詳しくは、Citrixのサーバーのログファイルを参照してください。
31202	現在無効なリソース<リソース名>を起動しようとしました。	エラー	指定のリソースがホストされてるサーバー上で有効かチェックしてください。
31203	起動リファレンスを使用するようにサーバーファーム<サーバーファーム名>は構成されていますが、Citrix XML Serviceから起動リファレンスが受信されませんでした。 サーバーファームが起動リファレンスをサポートしているか、または起動リファレンス要求が無効になっているかチェックしてください。	エラー	起動リファレンスを使用するには、サーバーファーム内のすべてのサーバーでXenDesktopまたはPresentation Server 4.5以降を実行する必要があります。サーバーファーム内のすべてのサーバーで同じ製品およびバージョンを使用することをお勧めします。 サーバーファームにXenApp 4.0 with Feature Pack 1 for UNIXまたはPresentation Server 4.0以前が動作するサーバーがある場合、XenApp WebサイトのWebInterface.confで、RequireLaunchReferenceパラメーターをOffに設定して、OverrideIcaClientnameパラメーターをOnに設定します。

31301	サーバーファーム<サーバーファーム名>の構成は無効です。	エラー	指定したサーバーファームに問題があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
32001	構成には、Citrixのサーバーの詳細情報は含まれていません。	エラー	XenApp Servicesサイト構成ファイルのFarmnパラメーターに対してサーバーファームが指定されていません。 WebInterface.confのエラーを修正してください。
32002	プロバイダーチェーン構成を解析できません。	エラー	XenApp Servicesサイトに問題があります。 サイト構成ファイルでエラーをチェックしてください。
32003	<エラーの原因>次のシステムエラーが発生しました：<エラーの説明>	エラー	XenApp Serviceサイトに問題があります。エラーメッセージの最後に詳細があります。 サイト構成ファイルでエラーをチェックしてください。
33001	Citrix Streaming Service：指定したCitrix XML Serviceにはアクセスできず、アクティブなサービスの一覧から一時的に削除されました。	エラー	Citrix Offline Plug-inでCitrix XML Serviceの問題が発生しました。 問題が解決されるまで、このサービスは無視されます。詳しくは、Citrixのサーバーのログファイルを参照してください。
33002	Citrix Streaming Service：このCitrix XML Serviceトランザクションは失敗しましたが、Citrix XML Serviceはアクティブなサービスの一覧から削除されませんでした。	エラー	Citrix XML ServiceはCitrix Offline Plug-inにアクセスできますが、要求またはインストラクションを完了できませんでした。 詳しくは、Citrixのサーバーのログファイルを参照してください。
33003	Citrix Streaming Service：サーバーファーム<サーバーファーム名>に対して構成されたすべてのCitrix XML Serviceは、このXML Serviceトランザクションへの応答に失敗しました。	エラー	Citrix Offline Plug-inは、指定のサーバーファームに対するCitrix XML Serviceホストにアクセスできませんでした。 Webサーバーを再起動してみてください。 詳しくは、Citrixのサーバーのログファイルを参照してください。
33004	Citrix Streaming Service：サーバーファーム<サーバーファーム名>の構成は無効です。	エラー	Citrix Offline Plug-inで指定したサーバーファームの問題が発生しました。 詳しくは、Citrixのサーバーのログファイルを参照してください。
33005	Citrix Streaming Service：構成には、Citrixのサーバーの詳細情報がありません。	エラー	サイト構成ファイルのFarmnパラメーターに対してサーバーファームが指定されていません。 WebInterface.confのエラーを修正してください。

33006	構成ファイルRadeValidationRules.confを読み込めませんでした。 サイト構成フォルダーでファイルを使用できるかチェックしてください。	エラー	構成ファイルRadeValidationRules.confがないか、またはアクセスできません。 ファイルが削除されていないか、またこのファイルを読み取ることができる適切な権限が構成されているか、チェックしてください。
33007	構成ファイルRadeValidationRules.confに無効な規則が含まれているため、このファイルを使用できません。 すべての規則が有効な正規表現構文を使用しているかチェックしてください。	エラー	構成ファイルRadeValidationRules.confに問題があります。 正規表現構文を使って、このファイルのすべての規則を指定する必要があります。 ファイルでエラーをチェックしてください。 または、Citrix Web Interface管理コンソールで［サイトメンテナンス］の［サイトの修復］タスクを使ってサイトを再インストールします。 ファイルに追加した変更はすべて破棄されます。
34001	構成には、Citrixのサーバーの詳細情報は含まれていません。	エラー	Desktop Appliance ConnectorまたはXenApp Webサイト構成ファイルのFarmnパラメーターに対してサーバーファームが指定されていません。 WebInterface.confのエラーを修正してください。
34002	プロバイダーチェーン構成を解析できません。	エラー	Desktop Appliance ConnectorまたはXenApp Webサイトに問題があります。 WebInterface.confでエラーをチェックしてください。
34003	<エラーの原因>次のシステムエラーが発生しました：<エラーの説明>	エラー	XenApp Serviceサイトに問題があります。エラーメッセージの最後に詳細があります。 WebInterface.confでエラーをチェックしてください。
40001	ユーザーのリソースを取得中に、エラーが発生しました。 ユーザーデバイスから、認識できないXMLメッセージを受け取りました。	エラー	Citrixのサーバーに接続する際に、Citrix Online Plug-inで問題が発生しました。 ユーザーデバイスでCitrix Online Plug-inが正常に構成されているかチェックしてください。
40002	ユーザーのリソースを取得中に、エラーが発生しました。 ユーザーデバイスから、認識できないXMLメッセージを受け取りました。	エラー	Citrixのサーバーに接続する際に、Citrix Online Plug-inで問題が発生しました。 ユーザーデバイスでCitrix Online Plug-inが正常に構成されているかチェックしてください。

40003	ユーザーのリソースへの再接続中にエラーが発生しました。 ユーザーデバイスから、認識できないXMLメッセージを受け取りました。	エラー	Citrixのサーバーに接続する際に、Citrix Online Plug-inで問題が発生しました。 ユーザーデバイスでCitrix Online Plug-inが正常に構成されているかチェックしてください。
40004	<IPアドレス>が必要とするCitrix Online Plug-in構成<ファイル名>は存在しません。	エラー	Citrix Online Plug-inの［オプション］ダイアログボックスに構成ファイルのURLが正しく入力されているか、ユーザーのデバイスをチェックしてください。
40005	ユーザーのリソースを起動中にエラーが発生しました：<エラーの説明>	エラー	Citrix Online Plug-inに問題があります。エラーメッセージの最後に詳細があります。 詳しくは、Citrixのサーバーのログファイルを参照してください。
40006	デスクトップ操作を実行中に、エラーが発生しました。 ユーザーデバイスから、認識できないXMLメッセージを受け取りました。	エラー	ユーザーのデスクトップを再開する際に、Citrix Online Plug-inで問題が発生しました。 ユーザーデバイスでCitrix Online Plug-inが正常に構成されているかチェックしてください。

エラーメッセージの無効化

IISでは、Web Interfaceのエラーメッセージを無効にして、発生した根本的なエラーのメッセージを表示するように設定することができます。 これを行うには、サイトのルートディレクトリにあるweb.configファイルを次のように変更します。 変更前

<customErrors mode="On" defaultRedirect="~/html/serverError.html">

新しい場所

<customErrors mode="Off" defaultRedirect="~/html/serverError.html">

また、独自のエラーメッセージを表示させることもできます。 これを行うには、次のように行を変更します。

<customErrors mode="On" defaultRedirect="~/html/CustomErrorPage">

ここで、CustomErrorPageは独自のエラーページのファイル名です。

Web InterfaceにするActive Directoryフェデレーションサービスのサポートの構成

更新日： 2014-11-24

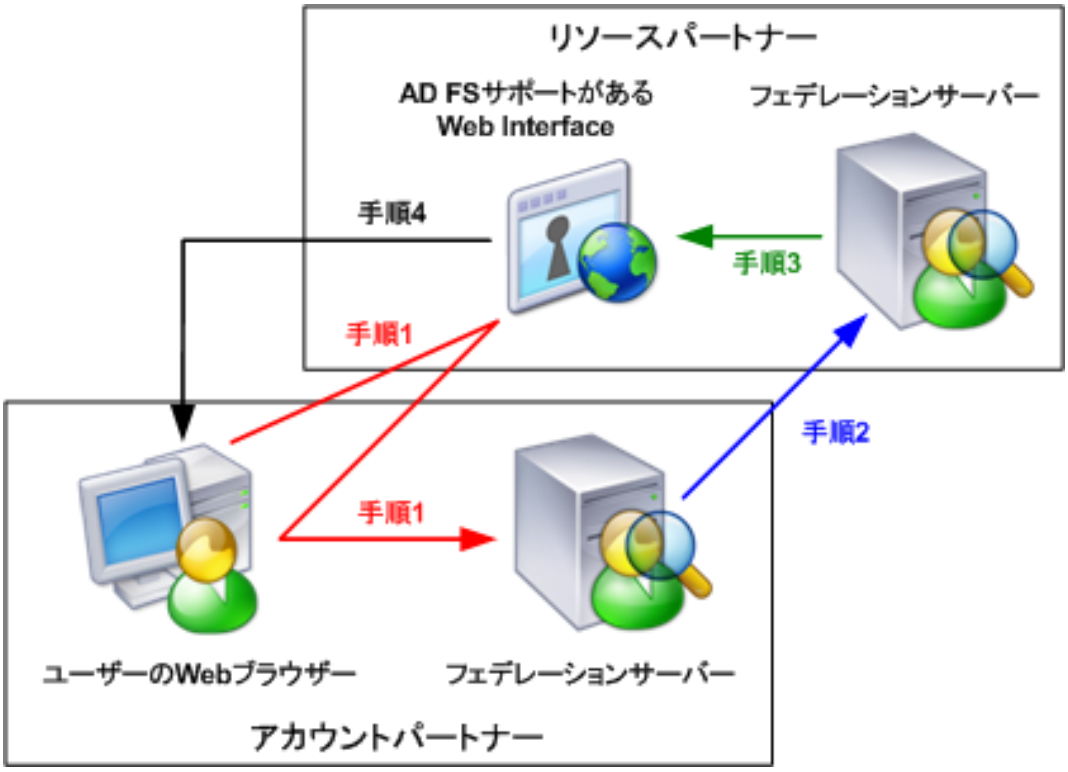
Web InterfaceでMicrosoft Active Directoryフェデレーションサービス（AD FS）を使うことにより、提携企業などのパートナーも、XenAppを使用してネットワーク上のリソースにアクセスできるようになります。 管理者は、リソースパートナーにアプリケーションやコンテンツへのアクセスを許可できるAD FSを統合したサイトを事前に作成しておきます。

重要： AD FSを使用する場合は、Webブラウザー、Webサーバー、フェデレーションサーバー間の通信を保護する必要があります。 また、Web Interfaceユーザーは、HTTPS/SSLを使ってAD FS統合サイトにアクセスする必要があります。

Active Directoryフェデレーションサービスを統合したサイトの動作

アカウントパートナー側のユーザーがリソースパートナー上のアプリケーションにアクセスすると、次の処理が行われます。

- 手順1： リソースパートナー側のWeb Interfaceホームページを開く要求が、アカウントパートナーの認証ページに転送されます。
- 手順2： アカウントパートナーは、そのユーザーを認証し、セキュリティトークンをリソースパートナーに送り返します。
- 手順3： リソースパートナー側のAD FSが、そのセキュリティトークンを検証してWindows識別情報に変換し（これがシャドウアカウントになります）、ユーザーの画面にWeb Interfaceの［ログオン］画面を表示します。

- 

  手順4： Web Interfaceは、そのユーザーがアクセスできるアプリケーションセットを表示します。 この図は、アカウントパートナードメインのユーザーがログオンし、アプリケーションセットにアクセスするときの手順を示しています。

- 手順5： ユーザーが、アプリケーション一覧のリンクをクリックしてアプリケーションにアクセスします。 Web Interfaceが、アクセス要求をCitrix XML Serviceに送信します。

- 手順6： Citrix XML Serviceが、SSPI（Security Support Provider Interface）データを生成し、XenAppサーバーに送信します。

- 手順7： XenAppサーバーが、SSPIデータを使用してユーザーを認証し、次回の認証用にログオントークンを保存します。

- 手順8： XenAppサーバーが、保存したログオントークン専用の起動チケットを生成して、そのチケットをCitrix XML Serviceに返します。

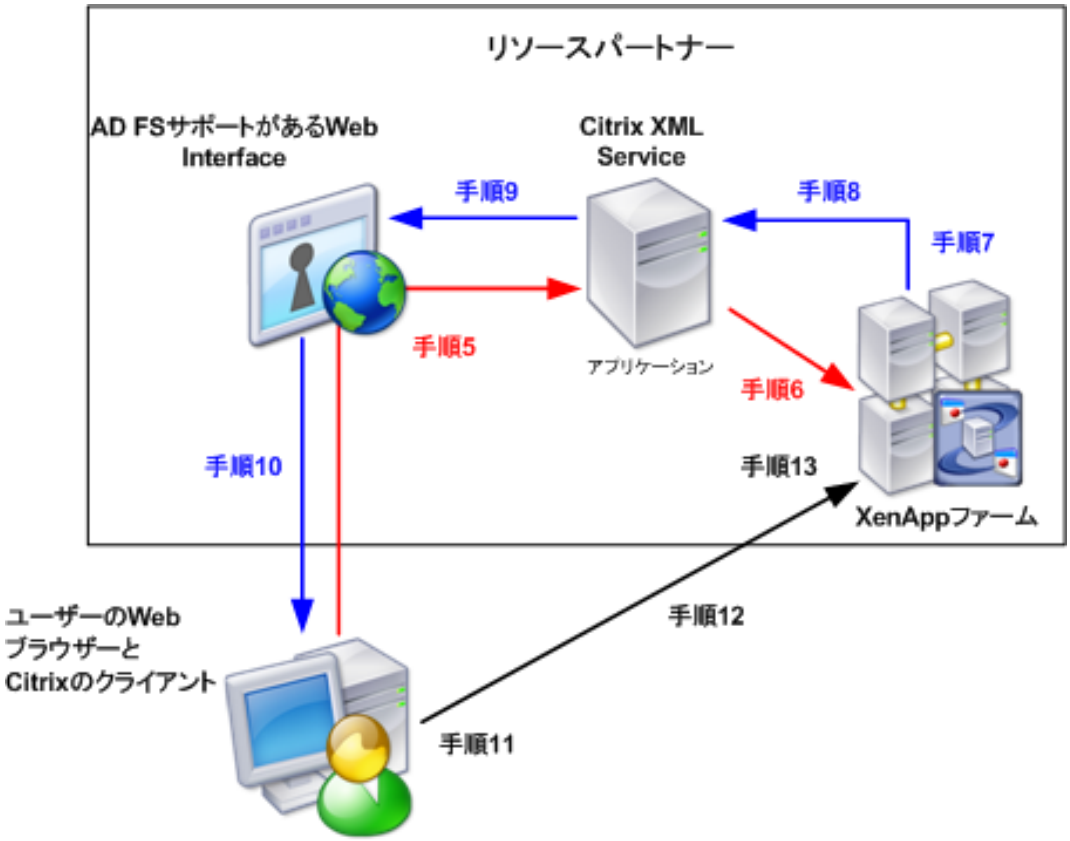
- 手順9： Citrix XML Serviceが、起動チケットをWeb Interfaceに送信します。

- 手順10： Web Interfaceが、その起動チケットを格納したICAファイルを作成して、ユーザーのWebブラウザーに送信します。

- 手順11： ユーザーのデバイスがICAファイルを開き、サーバーへのICAコネクションを試みます。

- 手順12： Citrixのクライアントが、起動チケットをXenAppサーバーに送信します。

.



手順13： XenAppサーバーが起動チケットを受け取り、そのチケットを前の手順で作成したログオントークンと照合します。次に、そのトークンを使って、そのサーバー上のICAセッションにユーザーがログオンできるようにします。 ICAセッションは、シャドウアカウントの識別情報を使って実行されます。この図は、アカウントパートナードメインのユーザーがアプリケーションにアクセスするときの手順を示しています。

サイトの構成により、ユーザーがログオフ操作を行うと、Web Interfaceから、またはWeb InterfaceとAD FSの両方からログオフします。 Web InterfaceおよびAD FSからログオフした場合は、すべてのAD FSアプリケーションからもログオフします。

Active Directoryフェデレーションサービスサイトの作成前の作業

Active Directoryフェデレーションサービス（AD FS）サイトを作成する前に、次の操作をすべて実行する必要があります。 1つでも欠けると、正常に機能しません。

- アカウントパートナー側とリソースパートナー側のフェデレーションサーバーのシステムクロックの誤差が5分以内になるように同期します。 これ以上の誤差があると、アカウントパートナー側で生成されるセキュリティトークンが、リソースパートナーに届く前に期限切れになってしまいます。 この問題を避けるためにも、両方の組織で同じインターネットタイムサーバーを使ってフェデレーションサーバーを同期してください。 詳しくは、「ドメイン間の関係の設定」を参照してください。

- リソースパートナー側のフェデレーションサーバーとWebサーバーが、確実に証明機関の証明書失効リスト（Certificate Revocation Lists：CRL）にアクセスできるようにする必要があります。 これらのサーバーで証明書が失効していないことを確認できないと、AD FSでエラーが発生することがあります。 詳しくは、「ドメイン間の関係の設定」を参照してください。

- Web Interface環境内にあるすべてのサーバーが委任処理を実行できるように信頼関係を設定する必要があります。 詳しくは、「展開環境内のサーバーに対する委任の構成」を参照してください。

- AD FSを介してWeb Interfaceにアクセスする外部ユーザーを認証するために、リソースパートナー側のドメイン内にこれらのすべてのユーザーのシャドウアカウントを作成する必要があります。 詳しくは、「シャドウアカウントの設定」を参照してください。

- XenAppをインストールし、Citrix XML ServiceがIISとポートを共有するように設定され、IISでHTTPSを使用できるように構成されている必要があります。

- Web Interfaceサーバーと、サーバーファーム内でWeb Interfaceの通信先となるCitrix XML Serviceを実行しているサーバーとの信頼関係を設定します。 詳しくは、「XenApp Webサイトでのワークスペースコントロールおよび統合された認証方法の併用」を参照してください。

重要： ここでは、AD FSのインストール方法については説明しません。 AD FSをインストールしたら、AD FSサイトを作成する前に、リソースパートナー側でAD FSが有効になっているアプリケーションに外部ユーザーがアクセスできることを確認してください。

Active Directoryフェデレーションサービス（AD FS）に必要なソフトウェア

Web InterfaceでAD FSを使用するには、次のソフトウェアが必要です。

- フェデレーションサーバーおよびWebサーバーとして、Windows Server 2008またはWindows Server 2003 R2。 Webサーバーの場合、32ビット版のWindows Server 2008およびWindows Server 2003 R2のみがサポートされています。

- リソースパートナーおよびアカウントパートナー上のActive Directoryフェデレーションサービス。 要求に対応するWebエージェントとWindowsトークンベースのAD FS Webエージェントの両方がインストールされている必要があります。

ドメイン間の関係の設定

以下の説明は、AD FS環境が、アカウントパートナー側のドメイン1つと、リソースパートナー側のドメイン1つの、合計2つのドメインで構成されていることを想定しています。どちらのドメインも、それぞれの組織のフォレスト内にあります。 AD FS環境に必要なコンポーネントを、別々のコンピューターにインストールする必要はありません。

2つのドメイン間の関係を設定するには

1. 次のコンポーネントが揃っていることを確認します。 アカウントパートナー：

   - Domain controller
   - フェデレーションサーバー
   - ユーザーデバイス

   リソースパートナー：

   - Domain controller
   - フェデレーションサーバー
   - Webサーバー
   - 1台以上のXenAppサーバー

   フェデレーションサーバーは、Windows Server 2008またはWindows Server 2003 R2が動作するコンピューターでホストされ、そのコンピューターにActive Directoryフェデレーションサービスサーバー役割をインストールする必要があります。

   Webサーバーは、32ビット版のWindows Server 2008またはWindows Server 2003 R2を実行するコンピューターでホストされる必要があります。 Web Server (IIS)サーバー役割に対するすべての役割サービスに加えて、要求に対応するエージェントおよびWindowsトークンベースのエージェント役割サービスをインストールする必要があります。

2. Webサーバーと両方のパートナーのフェデレーションサーバーのサーバー証明書を取得します。

   - 証明書には、信頼のおける証明機関の署名が入っている必要があります。
   - サーバー証明書は、特定の1台のコンピューターを識別します。このため、管理者は各サーバーの完全修飾ドメイン名（FQDN：Fully Qualified Domain Name。xenappserver1.mydomain.comなど）を把握している必要があります。
   - Webサーバーの証明書をIISにインストールして、SSLトラフィック用のデフォルトのIIS Webサイトを有効にします。
   - Microsoft管理コンソール（MMC）のスナップインを使って、フェデレーションサーバーの証明書をインストールします。 この手順については、Microsoft社のWebサイト（http://technet.microsoft.com/ja-jp/default.aspx）でMMCのドキュメントを参照してください。

3. リソースパートナーのフェデレーションサーバーが、アカウントパートナーのフェデレーションサーバーを信頼するようにするには、アカウントパートナーのフェデレーションサーバーの証明書をリソースパートナーのフェデレーションサーバーの信頼されたルート証明機関のストアにインストールします。

4. Webサーバーがリソースパートナーのフェデレーションサーバーを信頼するようにするには、リソースパートナーのフェデレーションサーバーの証明書を、Webサーバーの信頼されたルート証明機関のストアにインストールします。

   重要： リソースパートナーのフェデレーションサーバーとWebサーバーは、証明機関の証明書失効リストにアクセスできる必要があります。 そのためには、リソースパー

トナーのフェデレーションサーバーがアカウントパートナーの証明機関にアクセスできるようにして、Webサーバーがリソースパートナーの証明機関にアクセスできるようにします。 これらのサーバーで証明書が失効していないことを確認できないと、AD FSでエラーが発生することがあります。

5. リソースパートナーのフェデレーションサーバーで、MMCのActive Directoryフェデレーションサービススナップインを開きます。

6. コンソールツリーで、［フェデレーションサービス］>［信頼ポリシー］>［パートナーの組織］>［アカウントパートナー］の順に選択して、アカウントパートナーの名前を選択します。

7. ［操作］ペインの［プロパティ］を選択します。

8. ［リソースアカウント］タブで、［すべてのユーザーについてリソースアカウントが存在する］をクリックして、［OK］をクリックします。

9. リソースパートナーとアカウントパートナーの両方で同じインターネットタイムサーバーを使って、両方のフェデレーションサーバーのシステムクロックの誤差が5分以内になるように同期します。 これ以上の誤差があると、アカウントパートナー側で生成されるセキュリティトークンが、リソースパートナーに届く前に期限切れになってしまいます。 リソースパートナーとアカウントパートナーが異なるタイムゾーンに属していても構いませんが、クロックは同期させる必要があります。 たとえば、ニューヨークにあるアカウントパートナー側でクロックを東部標準時の16：00に設定した場合は、 カリフォルニアにあるリソースパートナー側のクロックが太平洋標準時の12:55～13:05である必要があります （東部標準時と太平洋標準時の時差は3時間です）。

10. Webサーバーで、MMCのインターネットインフォメーションサービス（IIS）マネージャースナップインを開きます。

11. 左側のペインでWebサーバーを選択し、［機能ビュー］で［フェデレーションサービスのURL］をダブルクリックします。

12. ［フェデレーションサービスのURL］ページで、リソースパートナーフェデレーションサービスのURLを入力し、［操作］ペインで［適用］をクリックします。

展開環境内のサーバーに対する委任の構成

更新日： 2014-11-24

展開環境内のすべてのサーバーに対して、委任のために信頼関係を設定する必要があります。これを行うには、リソースパートナードメインのドメインコントローラーにドメイン管理者としてログオンし、次のタスクを完了します。

リソースパートナードメインを正しい機能レベルにするには

重要： ドメインの機能レベルを上げるには、ドメイン内のすべてのドメインコントローラーがWindows Server 2008またはWindows Server 2003を実行している必要があります。 また、Windows Server 2003を実行するドメインコントローラーがある場合、またはそれを追加する予定がある場合は、ドメインの機能レベルをWindows Server 2008レベルに上げないでください。 ドメイン機能レベルを上げた後、それを低いレベルに戻すことはできません。

1. リソースパートナーのドメインコントローラーで、MMCのActive Directoryドメインと信頼関係スナップインを開きます。
2. 左側のペインで、リソースパートナーのドメイン名を選択し、［操作］ペインの［プロパティ］を選択します。
3. ドメインの機能レベルが最上位のレベルでない場合は、ドメイン名を選択して［操作］ペインの［ドメインの機能レベルを上げる］を選択します。
4. ドメインの機能レベルを上げるには、適切なレベルをクリックして［上げる］をクリックします。

委任のためWeb Interfaceサーバーを信頼するには

1. リソースパートナーのドメインコントローラーで、MMCのActive Directoryユーザーとコンピュータースナップインを開きます。
2. ［表示］メニューで［詳細］を選択します。
3. コンソールツリーで、リソースパートナードメイン名の下の［コンピューター］から、Web Interfaceサーバーを選択します。
4. ［操作］ペインで［プロパティ］をクリックします。
5. ［委任］タブで、［指定されたサービスへの委任でのみこのユーザーを信頼する］、［任意の認証プロトコルを使う］の順にクリックし、［追加］をクリックします。
6. ［サービスの追加］ダイアログボックスで、［ユーザーまたはコンピューター］をクリックします。
7. ［ユーザーまたはコンピューターの選択］ダイアログボックスの［選択するオブジェクト名を入力してください］ボックスに、Citrix XML Serviceを実行しているサーバーの名前を入力し、［OK］をクリックします。
8. 一覧からhttpサービスタイプを選択し、［OK］をクリックします。
9. ［委任］タブの［このアカウントが委任された資格情報を提示できるサービス］の一覧に、XenAppサーバー用に選択したhttpサービスタイプが表示されていることを確認し、［OK］をクリックします。
10. Web Interfaceの通信先として構成されているサーバーファームのCitrix XML Serviceを実行しているサーバーごとに、この手順を繰り返します。

委任のためCitrix XML Serviceを実行するサーバーを信頼するには

1. リソースパートナーのドメインコントローラーで、MMCのActive Directoryユーザーとコンピュータースナップインを開きます。
2. コンソールツリーで、リソースパートナードメイン名の下の［コンピューター］から、Web Interfaceが接続するように構成されるCitrix XML Serviceを実行するサーバーを選択します。
3. ［操作］ペインの［プロパティ］を選択します。
4. ［委任］タブで、［指定されたサービスへの委任でのみこのユーザーを信頼する］、［Kerberosのみを使う］の順にクリックし、［追加］をクリックします。
5. ［サービスの追加］ダイアログボックスで、［ユーザーまたはコンピューター］をクリックします。
6. ［ユーザーまたはコンピューターの選択］ダイアログボックスの［選択するオブジェクト名を入力してください］ボックスに、Citrix XML Serviceを実行しているサーバーの名前を入力し、［OK］をクリックします。
7. 一覧からHOSTサービスタイプを選択し、［OK］をクリックします。
8. ［委任］タブの［このアカウントが委任された資格情報を提示できるサービス］の一覧に、Citrix XML Serviceを実行するサーバー用に選択したHOSTサービスタイプが表示されていることを確認し、［OK］をクリックします。
9. Web Interfaceの通信先として構成されているサーバーファームのCitrix XML Serviceを実行しているサーバーごとに、この手順を繰り返します。

XenAppサーバーからのアクセスを許可するリソースを決定するには

1. リソースパートナーのドメインコントローラーで、MMCのActive Directoryユーザーとコンピュータースナップインを開きます。
2. コンソールツリーで、リソースパートナードメイン名の下の［Computers］から、XenAppサーバーを選択します。
3. ［操作］ペインの［プロパティ］を選択します。
4. ［委任］タブで、［指定されたサービスへの委任でのみこのユーザーを信頼する］、［Kerberosのみを使う］の順にクリックし、［追加］をクリックします。
5. ［サービスの追加］ダイアログボックスで、［ユーザーまたはコンピューター］をクリックします。
6. ［ユーザーまたはコンピューターの選択］ダイアログボックスの［選択するオブジェクト名を入力してください］ボックスに、リソースパートナーのドメインコントローラーの名前を入力し、［OK］をクリックします。
7. 一覧からcifsおよびldapサービスタイプを選択し、［OK］をクリックします。

   注： ldapサービスが2つある場合は、使用するドメインコントローラーの完全修飾ドメイン名（FQDN）に一致する方を選択します。
8. ［委任］タブの［このアカウントが委任された資格情報を提示できるサービス］の一覧に、リソースパートナーのドメインコントローラー用に選択したcifsおよびldapサービスタイプが表示されていることを確認し、［OK］をクリックします。
9. サーバーファームの各XenAppサーバーで、この手順を繰り返します。

制約付き委任のためのサーバー構成

セキュリティ上の理由から、すべてのXenAppサーバーに、制約付き委任を構成する必要があります。 これらのサーバー上のリソースにユーザーがアクセスできるようにするには、MMCのActive Directoryユーザーとコンピュータースナップインを使って［このアカウントが委任された資格情報を提示できるサービス］に適切なサービスを追加する必要があります。 たとえば、サーバー「adam」上のWebサーバーにアクセスするユーザーを認証するには、adam用のhttpサービスを追加し、サーバー「eve」上のSQLサーバーにアクセスするユーザーを認証するには、eve用のMSSQLSvcサービスを追加します。

詳しくは、Citrix Knowledge CenterのCTX112972の「Presentation Serverでのサービスプリンシパル名（SPN）と委任」を参照してください。

リソースへのアクセス制限時間の構成

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。

デフォルトでは、AD FSユーザーはネットワーク上のリソースに15分間アクセスできます。この制限時間を延長する場合は、Citrix XML Serviceを実行しているサーバーで次のレジストリエントリを変更します。

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Lsa¥Kerberos¥Parameters¥S4UTicketLifetime

このレジストリ値に、リソースのアクセス制限時間を分単位で指定します。ユーザーがセッションを開始してから、ここで指定した時間が経過するまでリソースへのアクセスが許可されます。

S4ULifetimeに指定できる最大値は、ドメインセキュリティポリシーによって制限されます。つまり、S4UTicketLifetimeの値が、ドメインレベルで指定した値よりも大きい場合、ドメインレベルの値が優先されます。

リソースへのアクセス制限時間をドメインレベルで構成するには

1. リソースパートナーのドメインコントローラー上で、MMCのドメインセキュリティポリシースナップインを開きます。
2. コンソールツリーで、［アカウントポリシー］>［Kerberosポリシー］の順に選択します。
3. 結果ペインで、［サービスチケットの最長有効期間］を選択します。
4. ［操作］ペインの［プロパティ］を選択します。
5. ［チケットの有効期間］に必要とされる時間を分単位で入力し、［OK］をクリックします。

リソースへのアクセス制限時間を構成しない場合は、XenAppサーバーからアクセスできるリソースを決定するときに、MMCのActive Directoryユーザーとコンピュータースナップインで［任意の認証プロトコルを使う］を選択します。 このオプションを選択すると、S4UTicketLifetimeに設定した値はすべて無視されます。 詳しくは、Microsoft社のWebサイト（http://support.microsoft.com/）を参照してください。

シャドウアカウントの設定

XenAppサーバー上のアプリケーションにアクセスするには、Windowsの正規アカウントが必要です。 そのため、AD FSを介してWeb Interfaceにアクセスする外部ユーザーごとに、リソースパートナー側のドメイン内にシャドウアカウントを手動で作成する必要があります。

リソースパートナー側のドメイン内のアプリケーションおよびコンテンツにアクセスするユーザーが、アカウントパートナー側のドメイン内に多数いる場合は、Active Directory内にユーザーのシャドウアカウントをすばやく作成できるサードパーティ製のアカウント作成プログラムを使用することもできます。

シャドウアカウントを作成するには、リソースパートナー側のドメイン内にあるドメインコントローラーに管理者としてログオンし、次の作業を行います。

ユーザープリンシパル名サフィックスを追加するには

1. リソースパートナーのドメインコントローラーで、MMCのActive Directoryドメインと信頼関係スナップインを開きます。
2. コンソールツリーで、［Active Directoryドメインと信頼関係］を選択します。
3. ［操作］ペインの［プロパティ］を選択します。
4. すべての外部アカウントパートナーのUPNサフィックスを追加します。 たとえば、アカウントパートナーのActive Directoryドメインが「adomain.com」の場合は、UPNサフィックスとしてadomain.comを追加します。

シャドウアカウントユーザーを定義するには

1. リソースパートナーのドメインコントローラーで、MMCのActive Directoryユーザーとコンピュータースナップインを開きます。
2. コンソールツリーで、リソースパートナードメイン名を選択します。
3. ［操作］ペインで、［新規作成］>［ユーザー］の順に選択します。
4. 該当するボックスに、ユーザーの姓、名、頭文字を入力します。
5. ［ユーザーログオン名］ボックスに、アカウント名を入力します。 ここには、必ずアカウントパートナードメインコントローラーと同じ名前を入力してください。
6. 一覧で、アカウントパートナーのUPNサフィックスを選択し、［次へ］をクリックします。
7. 所属組織のパスワードポリシーに従って、［パスワード］および［パスワードの確認入力］ボックスにパスワードを入力します。 ユーザーはAD FSを介して認証されるため、このパスワードが使われることはありません。
8. ［ユーザーは次回ログオン時にパスワード変更が必要］チェックボックスをオフにします。
9. ［ユーザーはパスワードを変更できない］および［パスワードを無制限にする］チェックボックスをオンにします。
10. ［次へ］をクリックし、［完了］をクリックします。

Active Directoryフェデレーションサービス統合サイトの作成

Citrix Web Interface管理コンソールの［サイトの作成］タスクを実行して、Web Interfaceのサイトが認証にAD FSを使用するように構成します。

注： AD FS環境でのXenDesktop仮想デスクトップの配信はサポートされません。 また、Client for Javaや埋め込みリモートデスクトップ接続（RDP）ソフトウェアでAD FS統合サイトにアクセスすることはできません。

Active Directoryフェデレーションサービス統合サイトを作成するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで［Web Interface］コンテナーをクリックします。
3. ［操作］ペインで、［サイトの作成］をクリックします。
4. ［XenApp Web］をクリックして、［次へ］をクリックします。
5. ［IISの場所の指定］ページで、IISの場所、パス、およびサイト名を指定します。 ［次へ］をクリックします。
6. ［認証ポイントの指定］ページで［Microsoft AD FSアカウントパートナー］を選択します。 Web Interfaceに対する応答URLを設定し、［次へ］をクリックします。
7. 新しいサイトの設定を確認し、［次へ］をクリックしてサイトを作成します。

Active Directoryフェデレーションサービス（AD FS）アプリケーションとしてのサイトの構成

サイトを作成したら、そのサイトをフェデレーションサーバーが認識できるようにAD FSアプリケーションとして構成します。

Active Directoryフェデレーションサービス（AD FS）アプリケーションとしてサイトを構成するには

1. リソースパートナーのフェデレーションサーバーで、MMCのActive Directoryフェデレーションサービススナップインを開きます。
2. コンソールツリーで、［フェデレーションサービス］>［信頼ポリシー］>［自分の組織］>［アプリケーション］の順に選択します。
3. ［操作］ペインで、［新規作成］>［ユーザー］の順に選択します。
4. ［次へ］をクリックし、［要求に対応するアプリケーション］を選択して［次へ］をもう一度クリックします。
5. ［アプリケーション表示名］にサイトの名称を入力します。
6. ［アプリケーションURL］に、Web Interfaceサイトの作成時に［Web Interface応答URL］に表示されるとおりにURLを正確に入力し、［次へ］をクリックします。

   注： URLには、必ずHTTPSとWebサーバーのFQDNを使用してください。
7. ［ユーザープリンシパル名（UPN）］チェックボックスをオンにして、［次へ］をクリックします。
8. ［このアプリケーションを有効にする］チェックボックスをオンにして、［次へ］をクリックします。
9. ［完了］をクリックし、AD FSアプリケーションとしてサイトを追加します。

展開環境のテスト

更新日： 2014-12-02

サイトをAD FSアプリケーションとして構成したら、アカウントパートナーとリソースパートナー間ですべてが正常に機能するかどうかテストします。

Web Interface Active Directoryフェデレーション環境をテストするには

1. アカウントパートナードメインのユーザーデバイスにログオンします。
2. Webブラウザーを開き、前の手順で作成したAD FS統合Web InterfaceサイトのURLを完全修飾ドメイン名（FQDN）形式で入力します。

   アプリケーションセットが表示されます。

   注： 統合認証のためにAD FSを構成していない場合は、アカウント情報を入力するか、スマートカードを挿入するよう求めるメッセージが表示されます。
3. Citrix Online Plug-inをインストールしていない場合は、これをインストールします。詳しくは、Online Plug-in for Windowsのドキュメントを参照してください。
4. アクセスするアプリケーションをクリックします。

Active Directoryフェデレーションサービス（AD FS）統合サイトからのログオフ

Citrix Web Interface管理コンソールの［認証方法］タスクを使って、ユーザーがWebサイトで［ログオフ］または［切断］ボタンをクリックしたときに、次のどちらからログオフするかを指定します。

- Web Interfaceのみ
- Web InterfaceおよびAD FSフェデレーションサービスの両方

Web Interfaceのみからログオフするように設定した場合、ユーザーにWeb Interfaceの［ログオフ］画面が表示されます。 Web InterfaceとAD FSの両方からログオフするように設定した場合、ユーザーにAD FSのログオフページが表示され、すべてのAD FSアプリケーションからログオフされます。

注： AD FSを使って認証するユーザーはパスワードを知らないため、XenAppセッションのロックを解除できません。 セッションのロックを解除するには、ユーザーはWeb Interfaceからログオフし、次にAD FS認証を使用して再度ログオンし、アプリケーションをもう一度起動する必要があります。 これにより、前のセッションのロックが解除され、新しい起動ウィンドウが閉じます。

ユーザーがログオフするサービスを指定するには

1. ［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順に選択します。
2. Citrix Web Interface管理コンソールの左側のペインで、［XenApp Webサイト］をクリックして結果ペインでAD FS統合サイトを選択します。
3. ［操作］ペインで［認証方法］をクリックします。
4. ユーザーがWeb InterfaceとAD FSの両方からログオフするように設定する場合は、［総合的なログオフを実行する］チェックボックスをオンにします。 ユーザーがWeb Interfaceだけからログオフするように設定する場合は、［総合的なログオフを実行する］チェックボックスをオフにします。