Single Sign-On 5.0

Dec 11, 2015

このリリースについて

導入

評価

システム要件

計画

中央ストアの種類

パスワードポリシー

アプリケーション定義

スマートカード

ユーザーの同一性検証を要求する

Single Sign-On Plug-inユーザー構成の作成計画

複数ユーザーでのワークステーションの共有（Hot Desktop）

オプションのSingle Sign-Onサービス機能の計画

Single Sign-On Plug-inの展開シナリオ

複数のプライマリ認証とデータの保護方法

インストールとアップグレード

Single Sign-Onのインストールに必要なセキュリティとアカウントの設定

JRE（Java Runtime Environment）のインストール

中央ストアの作成

管理コンソールのインストール

サービスモジュールのインストールと設定

Single Sign-On Plug-inのインストール

管理

リファレンス

データの保護方法

アプリケーション定義

パスワードポリシー

運用

アプリケーション定義拡張機能

Windows、Web、およびターミナルエミュレーターベースのアプリケーション用の仮想キーコード

Single Sign-Onプロビジョニングソフトウェア開発キット（SDK）

ようこそ

Sep 30, 2015

新機能

Single Sign-On 5.0では、Single Sign-On Plug-inがCitrix Receiverに統合されています。これにより、シンプルなユーザーエクスペリエンスが提供され、Merchandising ServerによるSingle Sign-On Plug-inの配信が可能になりました。また、このバージョンのSingle Sign-On Plug-inでは、簡体字中国語の言語パックを使用できます。

- **ユーザーは、Citrix Receiverのアイコンから Single Sign-On Plug-inの機能にアクセスします。**Windows通知領域に複数のSingle Sign-On Plug-inアイコンを表示する代わりに、1つのCitrix Receiverアイコンだけが表示されます。ユーザーが複数のSingle Sign-Onセッションを使用している場合でも、Citrix Receiverアイコンは1つしか表示されません。ユーザーは、Citrix Receiverアイコンのメニューを使ってログオン情報を管理したり、Single Sign-Onを一時停止/再開したり、Single Sign-Onが一時停止中かどうかを確認したり、パスワードを手作業で送信したりできます。
  注：以前のバージョンのソフトウェアがインストールされている場合、Windows通知領域に複数のアイコンが表示されることがあります。詳しくは、「Single Sign-On Plug-inのインストール」を参照してください。
- **Single Sign-Onのすべての機能を使用するには、XenAppサーバーだけでなくユーザーデバイス上にもSingle Sign-On Plug-inをインストールする必要があります。**ユーザーデバイス上にSingle Sign-On Plug-inがインストールされていない場合、ログオン情報の管理、Single Sign-Onの一時停止/再開、Single Sign-Onが一時停止中かどうかの確認、およびパスワードの手作業での送信などの操作をユーザーが実行できなくなります。詳しくは、「Single Sign-On Plug-inの展開シナリオ」を参照してください。
- **ユーザーは、Citrix Receiverを終了することでSingle Sign-On Plug-inを終了します。**Citrix Receiverアイコンのメニューで［終了］を選択すると、Single Sign-Onが終了します。これにより、Citrix Receiverのユーザーインターフェイスが閉じて、このインターフェイスからアクセスできるすべてのプラグインソフトウェアが終了します。
- **ユーザーは、［パスワード管理］ダイアログボックスを使って自分のログオン情報を管理します。**このダイアログボックスは、以前のバージョンで使用されていた「ログオンマネージャー」に相当します。ただし、ユーザーエクスペリエンスをシンプルにするため、以下のように変更されています。
  - ［パスワード管理］ダイアログボックスを開くには、Citrix Receiverアイコンのメニューを使用します。1つの［パスワード管理］ダイアログボックスで、すべてのセッションでのアプリケーションに対するログオン情報を管理できます。
  - 管理者は、ユーザーの［パスワード管理］ダイアログボックスの一覧に表示するログオン情報の属性の列（名前、説明、グループ、最終使用日、更新日時）を制御できます。ユーザーは、各属性でこの一覧を並び変えることができます。
  - ［パスワード管理］ダイアログボックスには、ログオンマネージャーで使用されていたドロップダウンメニューがありません。ログオンマネージャーのメニューから選択していた以下の機能は、このバージョンで削除されたか、ほかの方法で選択できます。

メニュー	オプション	Single Sign-On 5.0での選択方法
ファイル	新規ログオン または 新規ログオン > ログオン情報の追	ユーザーがログオン情報を手作業で保存するには、Citrix Receiverアイコンのメニューの［パスワードの送信］オプションを使用します。

メニュー	オプション	Single Sign-On 5.0での選択方法
加	新規ログオン > 複数のログオン情報の追加	ユーザーが同一アプリケーションに対する複数のログオン情報を保存するには、最初のログオン情報を追加した後でそれをコピーし、必要に応じて編集します。
	コピー	［パスワード管理］ダイアログボックスの［コピー］ボタンを使用します。
	削除	［パスワード管理］ダイアログボックスの［削除］ボタンを使用します。
	プロパティ	［パスワード管理］ダイアログボックスの［編集］ボタンを使用します。
	Exit	［パスワード管理］ダイアログボックスの［X］（閉じる）ボタンを使用します。
表示	アイコン、一覧、および詳細	シンプルなユーザーエクスペリエンスを提供するため削除されました。
	アイコンの整列	削除されました。ただし、ユーザーは各属性の列見出しをクリックして［パスワード管理］ダイアログボックスの一覧を並び変えることができます。
	Refresh	［パスワード管理］ダイアログボックスの［更新］リンクを使用します。
	文字列の表示	［パスワード管理］ダイアログボックスの［文字列の表示］ボタンを使用します。ただし、一度に複数のパスワード文字列を表示することはできません。
ツール	アカウントの関連付け	Single Sign-On Plug-inでユーザーがアカウントの関連付けを有効にすることはできません。ユーザーがアカウントの関連付けを実行できるようにするには、AccAssoc.exeユーティリティを公開アプリケーションとして提供してください。
	セキュリティ用の質問の登録	Single Sign-On Plug-inでユーザーがセキュリティ用の質問に対する回答を登録することはできません。ユーザーが回答を登録できるようにするには、登録を求めるメッセージの表示を有効にするか、QBAEnroll.exeユーティリティを公開アプリケーションとして提供してください。
	オプション > 終了を確認する	終了時の確認機能は、Citrix Receiverで設定します。Single Sign-On Plug-inの終了時には確認メッセージは表示されません。
ヘルプ	ログオンマ	［パスワード管理］ダイアログボックスの［ヘルプ］リンクを使用します。

メニュー	ネージャーオプションのヘルプ	Single Sign-On 5.0での選択方法
	ようこそ	［パスワード管理］ダイアログボックスの［バージョン情報］リンクを使用します。

- ［パスワード管理］ダイアログボックスには、ログオンマネージャーで使用されていたコンテキストメニューがありません。ログオンマネージャーのコンテキストメニューから選択していた以下の機能は、このバージョンではほかの方法で選択できます。

オプション	Single Sign-On 5.0での選択方法
コピー	［パスワード管理］ダイアログボックスの［コピー］ボタンを使用します。
削除	［パスワード管理］ダイアログボックスの［削除］ボタンを使用します。
プロパティ	［パスワード管理］ダイアログボックスの［編集］ボタンを使用します。

- **Single Sign-Onの初回起動時にユーザーにログオン情報の一括登録を求める機能：**この機能は、このバージョンで削除されています。
- **Merchandising Serverを使用したSingle Sign-On Plug-inの配布：**ユーザーデバイス上にCitrix Receiver Updaterがインストールされている場合は、管理者がMerchandising Serverを使用してSingle Sign-On Plug-inをユーザーに配布し、それを管理できます。
- **Single Sign-On Plug-inを簡体字中国語ユーザーインターフェイスで使用できるようになりました。**

既知の問題

Single Sign-On 5.0で確認されている既知の問題については、「既知の問題 - XenApp 6.5 for Windows Server 2008 R2」を参照してください。

はじめに

Sep 30, 2015

Single Sign-Onは、以下の4つの主要コンポーネントで構成されます。

- 中央ストア
- Citrix AppCenterの［Single Sign-On］ノード
- Single Sign-On Plug-in
- Single Sign-Onサービス（オプション）

中央ストア

中央ストアは、Single Sign-Onによるユーザーデータや管理データを格納および管理する、集中リポジトリです。ユーザーデータには、ログオン情報、セキュリティ用の質問と回答、およびユーザーに関するそのほかのデータがあります。管理データには、パスワードポリシー、アプリケーション定義、セキュリティ用の質問などがあります。ユーザーがWindowsにログオンすると、ユーザーの入力したログオン情報が、中央ストアに格納されているログオン情報と比較されます。その後、ユーザーがパスワードで保護されたアプリケーションやWebページを開くと、登録済みのログオン情報が中央ストアから取得されます。

Citrix AppCenterの［Single Sign-On］ノード

Citrix AppCenterの［Single Sign-On］ノードは、Single Sign-Onの管理コンソールとして機能します。ここでは、Single Sign-Onの動作、機能、セキュリティ対策、およびパスワードに関するそのほかの重要な構成を行います。

このノードには、［ユーザー設定］、［アプリケーション定義］、［パスワードポリシー］、および［ユーザー識別処理］の4つのノードがあります。ノードを選択すると、そのノードに対して実行できるタスクが表示されます。各ノードの機能は、以下のとおりです。

- ［ユーザー設定］ノードでは、ユーザーの担当業務や作業場所の条件に基づいて、Single Sign-Onの各種設定をカスタマイズできます。
- ［アプリケーション定義］ノードでは、アプリケーションからのログオン要求やパスワードの変更要求に対して、Single Sign-On Plug-inがユーザーのログオン情報を提供したり、エラーを検出したりできるようにするための定義を作成できます。Single Sign-Onに組み込まれているテンプレートを利用したり、独自に定義を作成したりできます。
- ［パスワードポリシー］ノードでは、ユーザーが使用するパスワードの長さや種類、および使用可能な文字を制御するためのポリシーを作成できます。パスワードポリシーは、ユーザーが作成するパスワードと自動生成されるパスワードの両方に適用されます。また、パスワードに使用できない文字を特定したり、パスワードの再使用を可能にするかどうか指定することもできます。組織のパスワード規則に準拠したポリシーを作成して、ユーザーが使用するパスワードの安全性を高めることができます。
- ［ユーザー識別処理］ノードでは、ユーザーの同一性を検証するためのセキュリティ用の質問を作成できます。セキュリティ用の質問により、ほかのユーザーがそのユーザーになりすましたり、不正にパスワードを変更したり、アカウントのロックを解除したりすることを防ぐことができます。セキュリティ用の質問に対する回答を登録したユーザーは、同じ回答を入力することで自分の同一性を証明できます。ユーザーがプライマリパスワードを忘れたり、アカウントがロックされたりした場合は、登録した回答を正確に入力することでユーザーの同一性が検証され、パスワードをリセットしたりロックを解除したりできるようになります。セキュリティ用の質問は、暗号キーの復元処理でも使用されます。

Single Sign-On Plug-in

Single Sign-On Plug-inは、ユーザーのコンピューター上で動作するアプリケーションに適切なログオン情報を送信したり、パスワードポリシーを適用したり、セルフサービス機能を提供したりします。また、ユーザーはSingle Sign-On Plug-inの［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）を使用して、自分のログオン情報を管理できます。管理者が定義するユーザー構成により、ユーザーが使用できる機能は異なります。

Single Sign-Onサービス

Webサーバー上で実行されるSingle Sign-Onサービスにより、いくつかの追加機能が提供されます。以下のいずれかの追加機能を使用する場合は、Single Sign-Onサービスをインストールする必要があります。

- アカウントセルフサービスモジュール：ユーザーが自分のWindowsパスワードを再設定（リセット）したり、Windowsアカウントのロックを自分で解除したりできるようになります。
- データの整合性チェックモジュール：中央ストアとSingle Sign-On Plug-in間で通信されるデータが不正に改変されることを防ぐことができます。
- キー管理：ユーザーのプライマリパスワードが変更されたときに、暗号化されているセカンダリパスワード（Single Sign-Onに登録したログオン情報）を、自動的に、またはユーザーがセキュリティ用の質問に対する回答を入力することで復元します。
- プロビジョニング：Citrix AppCenterから、Single Sign-Onのユーザーデータやログオン情報を一括して追加、削除、または更新できます。
- ログオン情報の同期：Webサービスを使用して、ユーザーのログオン情報をドメインアカウント間で同期します。

これらの追加機能を使用しない場合は、Single Sign-Onサービスをインストールしないでください。

評価

Sep 30, 2015

XenApp 6.5 for Windows Server 2008 R2を使用してアプリケーションを公開しており、さらにSingle Sign-On 5.0を使用してパスワードの安全性とアプリケーションへのシングルサインオンアクセスを実現することを望んでいる場合は、このトピックにより、すばやくSingle Sign-Onを展開できます。ここで説明するSingle Sign-On環境は、Single Sign-Onの評価に使用したり、拡張により多くのユーザーやアプリケーションを含むことができるパイロット展開として使用することができます。

注：展開処理を単純化するために、ここで説明する展開では、Single Sign-On 5.0をXenApp 6.5と併用する場合に使用できる一部のコンポーネント、機能、オプションは除外されます。
ここで説明する展開には、以下のSingle Sign-Onコンポーネントが含まれます。

- **中央ストア。**中央ストアは、Single Sign-Onによるユーザーデータや管理データを格納および管理する、集中リポジトリです。ユーザーデータには、ログオン情報、セキュリティ用の質問と回答、およびユーザーに関するそのほかのデータがあります。管理データには、パスワードポリシー、アプリケーション定義、セキュリティ用の質問などがあります。ユーザーがWindowsにログオンすると、ユーザーの入力したログオン情報が、中央ストアに格納されているログオン情報と比較されます。その後、ユーザーがパスワードで保護されたアプリケーションやWebページを開くと、登録済みのログオン情報が中央ストアから取得されます。
- **Citrix AppCenterの［Single Sign-On］ノード。**この展開では、Citrix AppCenterの［Single Sign-On］ノードを使用して、パスワードポリシーの定義、アプリケーションを識別するためのSingle Sign-Onの構成、およびユーザー構成の作成を行うことができます。
- **アプリケーション定義ツール**アプリケーション定義ツールはCitrix AppCenterの［Single Sign-On］ノードの一部と同じ機能を備えており、アプリケーションを識別するようにSingle Sign-Onを構成できます。
- **Single Sign-On Plug-in**Single Sign-On Plug-inは、ユーザー対話型のSingle Sign-Onコンポーネントです。Single Sign-On Plug-inは、ユーザーのクライアントデバイスで実行されているアプリケーションに適切な資格情報を送信したり、パスワードポリシーを強制的に実行したりします。また、このコンポーネントによって、ユーザーは［Manage Passwords］ダイアログボックスで自身の資格情報を管理できるようになります。この展開では、各ユーザーデバイスにSingle Sign-On Plug-inがインストールされます。

この展開には、Single Sign-Onサービスとそれがサポートしている以下のオプション機能は含まれません。

- アカウントセルフサービスモジュール：ユーザーが自分のWindowsパスワードを再設定（リセット）したり、Windowsアカウントのロックを自分で解除したりできるようになります。
- データの整合性チェックモジュール：中央ストアとSingle Sign-On Plug-in間で通信されるデータが不正に改変されることを防ぐことができます。
- キー管理：ユーザーのプライマリパスワードが変更されたときに、暗号化されているセカンダリパスワード（Password Managerに登録したログオン情報）を、自動的またはユーザーがセキュリティ用の質問に対する回答を入力することで復元します。
- プロビジョニング：管理コンソール（Citrix AppCenterの［Single Sign-On］ノード）から、Single Sign-Onのユーザーデータやログオン情報を一括して追加、削除、または更新ができます。
- ログオン情報の同期：Webサービスを使用して、ユーザの資格情報をドメインアカウント間で同期します。

以下に示す順序でセクションを進み、このトピックのタスクを実行してください。

展開計画

- 中央ストア、管理コンソール（Citrix AppCenterの［Single Sign-On］ノード）、アプリケーション定義ツール、プラグインのシステム要件を確認します（「システム要件」を参照）。
- Single Sign-Onのライセンス要件を確認し、必要に応じて、ライセンスをインストールしてアップグレードします（「シス

テム要件」を参照）。

- 含めるアプリケーションを特定します。この展開では、XenAppで公開されたWindowsとWebアプリケーションのみを選択します。
  - Windowsアプリケーションの場合は、Microsoft Outlook、Lotus Notes、SAPなどのパスワードで保護された32ビットのWindowsアプリケーション（Javaアプリケーションを含む）を使用します。Single Sign-Onでは、「.exe」拡張子が付いたファイルにより起動されるアプリケーションはすべて、Windowsアプリケーションとして分類されます。
  - Webアプリケーションの場合は、Microsoft Internet ExplorerからアクセスするWebアプリケーション（JavaアプレットとSAPを含む）を使用します。通常、Single Sign-Onでは、ブラウザーで実行されるアプリケーションはすべて、Webアプリケーションとして分類されます。Single Sign-Onでは、Internet Explorer Versions 6.0、7.0、8.0、および9.0上で動作するWebアプリケーションがサポートされます。
- 含めるユーザーを特定します。ユーザーデバイスがSingle Sign-On Plug-inをサポートしていることを確認してください。
- 中央ストアのインストール先を決定します。この展開の中央ストアはNTFSネットワーク共有です。
- Citrix AppCenterの［Single Sign-On］ノードのインストール先を決定します。インストール済みのAppCenterを使用することもできますし、新しいAppCenterをインストールすることもできます。
- アプリケーション定義ツールをインストールするかどうか、およびそのインストール先を決定します。展開に含めるアプリケーションを実行しているコンピューターにCitrix AppCenterがインストールされていない場合は、そのコンピューターにアプリケーション定義ツールをインストールします。アプリケーションを識別するようにSingle Sign-Onを構成する場合は、アプリケーションを実行して、ツールのウィザードがアプリケーションに関する情報をキャプチャできるようにします。
- パスワードポリシーを計画します。パスワードポリシーは、パスワードを作成、送信、管理する方法を制御する規則です。アプリケーションのすべてのユーザーまたは特定のグループにパスワードポリシーを適用してください。Single Sign-Onには、デフォルトとドメインという2つの標準パスワードポリシーが用意されています。この展開に対して、標準ポリシーのデフォルト値が自身の要件に合致する場合は、標準ポリシーを変更することなく使用できます。それ以外の場合は、標準ポリシーに基づいて新しいポリシーを作成し、それらの値を変更することができます。
  - パスワードポリシーの概要については、「パスワードポリシー」を参照してください。
  - パスワードポリシーをセキュリティ保護して使用できるようにするためのガイドラインについては、「パスワードポリシー」を参照してください。
  - Single Sign-Onがパスワードポリシーを強制実行する仕組みについては、「パスワードの要件を適用する」を参照してください。
  - パスワードポリシー規則のデフォルト値がアプリケーションやユーザーに対して適切かどうかを判断するには、「パスワードポリシー」のリファレンストピックとそのサブトピックに記載されている各設定のデフォルト値を参照してください。標準パスワードポリシー（デフォルトとドメイン）はそれらのデフォルト値を備えています。
- ユーザー構成を計画します。ユーザー構成は、ユーザー固有の設定、パスワードポリシー、およびアプリケーションを定義したもので、Active Directory階層に関連付けられたユーザー（組織単位または個々のユーザー）またはActive Directoryグループに適用されます。ユーザー構成の内容により、ユーザーのSingle Sign-On Plug-inの動作やユーザーインターフェイスが制御されます。
  - ユーザー構成の概要について、またこの展開で使用されるユーザー構成設定とそのデフォルト値を確認するには、「Single Sign-On 5.0設定リファレンス」を参照してください。左記の参照トピックで説明されている一部のオプションと機能はこの展開では使用されないので注意してください。この概要には、次の情報が含まれています。
    - Plug-inの基本動作
    - Plug-inのユーザーインターフェイス
    - 同期

      注：［ログオン情報の同期モジュールがユーザーのログオン情報にアクセスすることを許可する］はオフにしてください。ユーザー構成展開にはログオン情報の同期モジュールは含まれません。
    - アプリケーションのサポート
    - ライセンス管理
  - ユーザー資格情報を保護するには、「データの保護方法」を参照してください。

注：［secondary data protection］の設定にはデフォルト値を使用してください。ほかの値にはキー管理モジュールが必要ですが、この展開には含まれません。
大部分の環境では、この展開を最初に使用するときにデフォルトのユーザー構成設定（ライセンス設定を除く）を使用できます。展開の使用を開始した後に要件が変化した場合は、ユーザー構成の値を編集できます。

この展開で使用されない機能の設定はデフォルトで無効になっています。

中央ストアの作成

Single Sign-On中央ストアの種類として、Active DirectoryまたはNTFSネットワーク共有のいずれかを選択できます。NTFSネットワーク共有はActive Directory形式の中央ストアよりもより少ない権限で作成できるため、この展開ではNTFSネットワーク共有を作成します。NTFSネットワーク共有の中央ストアの利点と考慮事項については、「NTFSネットワーク共有形式の中央ストア」を参照してください。

必要な場合は、後からユーザーをActive Directory形式の中央ストアに移行できます。

NTFSネットワーク共有の中央ストアを作成するには：

1. XenAppインストールメディアを挿入します。
2. XenAppインストールメディアの起動画面で、［コンポーネントの個別インストール］、［サーバーコンポーネント］、［追加機能］、［Single Sign-On］の順にクリックします。
3. ［中央ストア］をクリックします。
4. ［NTFS ネットワーク共有］を選択します。

中央ストアが%SystemDrive%\CITRIXSYNC$として作成されます。

管理コンソール（Citrix AppCenterの［Single Sign-On］ノード）をインストールします。

AppCenterには、インストール時にデフォルトでSingle Sign-Onコンポーネントが含まれます。

既存のAppCenterをSingle Sign-Onと共に使用する場合は、中央ストアの作成後に検出を設定して実行します。

新しいAppCenterをインストールしてSingle Sign-Onと共に使用する場合は、システム要件に記載されているように、必要なMicrosoft Visual C++再頒布可能パッケージとMicrosoftプライマリ相互運用アセンブリがインストールされていることを確認してください。

AppCenterをインストールするには：

1. XenAppインストールメディアを挿入します。
2. XenAppインストールメディアの起動画面で、［コンポーネントの個別インストール］、［共通コンポーネント］、［管理コンソール］の順にクリックします。 画面の指示に従って操作します。
3. AppCenterを開き、［検出の設定と実行］を選択し、ウィザードの指示に従って操作します。

構成後、管理コンソール（Citrix AppCenterの［Single Sign-On］ノード）が中央ストアに接続されます。それを使用して、パスワードポリシーを定義したり、アプリケーションを識別するようにSingle Sign-Onを設定したり、ユーザー構成を作成したりできます。

アプリケーション定義ツールのインストール

展開に含めるアプリケーションを実行しているコンピューターにCitrix AppCenterがインストールされていない場合は、そのコンピューターにアプリケーション定義ツールをインストールしてアプリケーションのアプリケーション定義を作成します。

1. XenAppインストールメディアを挿入します。
2. AdministrationフォルダーでASC_PasswordManagerファイルを検索し、それを実行します。
3. ［アプリケーション定義ツール］を選択します。 画面の指示に従って操作します。

パスワードポリシーの定義

この展開に対して、標準パスワードポリシーのデフォルト値が自身の要件に合致すると判断した場合は、別のポリシーを定義する必要はありません。それ以外の場合は、標準ポリシーに基づいて新しいポリシーを作成します。

新しいパスワードポリシーを作成するには：

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［パスワードポリシー］を選択します。
3. ［操作］メニューから、［パスワードポリシーの作成］を選択します。
4. パスワードポリシーウィザードの指示に従って操作します。

アプリケーションを識別するためのSingle Sign-Onの構成

Single Sign-Onでは、アプリケーション定義に設定されている条件に基づいてアプリケーションを識別し、ログオン処理を行います。アプリケーション定義により必要な情報を提供することで、Single Sign-On Plug-inがアプリケーションにユーザの資格情報を提供したり、エラーを検出したりできるようになります。

アプリケーション定義はフォーム定義から構成されています。Single Sign-On Plug-inは、アプリケーションの起動時にこれらのフォーム定義機能に基づいてアプリケーションを分析し、次のような処理が必要かどうかを判断します。

- ログオン要求に対してログオン情報を送信する。
- ログオン情報の変更用のインターフェイスとネゴシエートする。
- ログオン情報の確認用のインターフェイスを処理する。

多くのアプリケーションでは、ログオン情報の管理に2つのフォーム（ログオン用およびパスワード変更用）だけを使用しますが、必要に応じてほかのフォームをアプリケーション定義に追加して、使用することができます。

以下の種類のログオン情報用フォームを作成できます。

- ログオンフォーム
  アプリケーションのログオン用のインターフェイスを識別し、そのアプリケーションにアクセスするために必要なアクションを定義するために使用します。

- パスワード変更フォーム
  アプリケーションのパスワード変更用のインターフェイスを識別し、そのアプリケーションのユーザーパスワードを変更するために必要なアクションを定義するために使用します。

- パスワード変更の成功フォーム
  アプリケーションのパスワード変更用のインターフェイスを識別し、パスワードが変更されたことを確認するために必要なアクションを定義するために使用します。

- パスワード変更の失敗フォーム
  アプリケーションのパスワード変更失敗用のインターフェイスを識別し、パスワードの変更操作が失敗したときに行うアクションを定義するために使用します。

AppCenterまたはアプリケーション定義ツールからウィザードを使用して、アプリケーション定義を作成します。定義するアプリケーションが実行されているか、ブラウザーウィンドウで使用可能になっている場合は、これらのウィザードによってアプリケーション定義に必要な情報をキャプチャできます。アプリケーション定義を作成するには、アプリケーション定義を作成するコンピューターからそのアプリケーションにアクセスできる必要があります。

オペレーティングシステムによっては一部のアプリケーション署名が異なることがあるため、アプリケーション定義を実行するすべてのオペレーティングシステムでアプリケーション定義をテストする必要があります。

一部のアプリケーションではアプリケーションテンプレートを使用できます。これらのテンプレートによってアプリケーション定義の作成に必要な大部分の情報が提供されるため、Single Sign-On環境へのアプリケーション定義の追加が簡単になります。アプリケーションテンプレートについては、「アプリケーションテンプレート」を参照してください。

Windowsアプリケーション定義を作成するには

Windowsアプリケーション用のアプリケーション定義を作成するには、Citrix AppCenterまたはアプリケーション定義ツールからアプリケーション定義ウィザードを実行します。ウィザードを実行しながら、ログオン情報管理イベント（ユーザーログオン、パスワード変更、パスワード変更の成功、パスワード変更の失敗）を要求するアプリケーション内のフォームを開きます。

Windowsアプリケーション定義に関する考慮事項の概要については、「Windowsアプリケーションの定義」を参照してください。

1. 対象となるアプリケーションを起動しておきます。
2. アプリケーション定義ウィザードを起動する準備をします。
   - AppCenterの場合：［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 AppCenter］の順に選択します。［Single Sign-On］ノードを開き、［アプリケーション定義］を選択します。
   - アプリケーション定義ツールの場合：［AppCenter］から：［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［Single Sign-On］>［アプリケーション定義ツール］の順に選択します。
3. ［アプリケーション定義の作成］を選択します。
4. ［Windows］と［新規に作成する］が選択されていることを確認して、［ウィザードの起動］をクリックします。
5. 中央ストアで表示するアプリケーションの名前を入力します。 オプションとして、説明を入力します。［Next］をクリックします。
6. ［フォームの追加］をクリックします。フォーム定義ウィザードが起動します。
7. アプリケーションのログオンフォーム、パスワードの変更フォーム、パスワード変更の成功フォーム、またはパスワード変更の失敗フォームを開きます。
8. フォーム定義ウィザードの［フォームの識別］ページで、［選択］をクリックします。
9. 表示された［ウィンドウ セレクター］で、定義を作成するアプリケーションを選択します。アプリケーションのプロンプト付近に点滅する枠線が表示されます。
10. ［フォーム名］ページで、フォームの名前を入力し、フォームの種類を選択します。［Next］をクリックします。
11. ［ウィンドウ セレクター］で［OK］をクリックします。
12. ［フォームの識別］ページで［次へ］をクリックします。
13. ［フォーム アクションの定義］ページで、フォームに表示するログオン情報フィールドとボタンを構成します。
    1. 特定のログオン情報の右側の［設定/変更］のハイパーリンクをクリックします。 各ログオン情報の入力フィールドを特定するための［コントロールの文字列の設定］ダイアログボックスが開きます。
    2. ログオン情報の入力フィールドと送信ボタンを選択します。 異なる入力フィールドや送信ボタンを選択すると、対応する種類のコントロールがアプリケーション上で点滅する枠線によって強調表示されます。
    3. フォームで必要なすべてのログオン情報フィールドとフォームを送信するためのボタンについて、この操作を繰り返します。
       フォームの中には、ドメインやそのほかのログオン情報の入力が必要なものもあります。そのような場合に備えて、2つのカスタムフィールドが用意されています。これらのフィールドには、特別なログオン情報を割り当てます。フィールドの名前は、フォームを定義した後にアプリケーション定義ウィザードの［カスタムフィールドの名前］ページで定義します。

       注：［フォームアクションの定義］ページ上部に表示されるすべてのログオン情報用のフィールドを構成する必要はありません。

14. アプリケーションでそのほかのフォームが必要な場合は、ウィザードを使用してフォームを作成します。

Webアプリケーション定義を作成するには

Webアプリケーション用のアプリケーション定義を作成するには、Citrix AppCenterまたはアプリケーション定義ツールからアプリケーション定義ウィザードを実行します。ウィザードを実行しながら、ログオン情報管理イベント（ユーザーログオン、パスワード変更、パスワード変更の成功、パスワード変更の失敗）を要求するアプリケーション内のフォームを開きます。

1. 対象となるアプリケーションを起動しておきます。
2. アプリケーション定義ウィザードを起動する準備をします。
   - AppCenterの場合：［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 AppCenter］の順に選択します。［Single Sign-On］ノードを開き、［アプリケーション定義］を選択します。
   - アプリケーション定義ツールの場合：［AppCenter］から：［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［Single Sign-On］>［アプリケーション定義ツール］の順に選択します。
3. ［アプリケーション定義の作成］を選択します。
4. ［Web］と［新規に作成する］が選択されていることを確認して、［ウィザードの起動］をクリックします。
5. ［アプリケーションの識別］ページで、中央ストアで表示するアプリケーションの名前を入力します。 オプションとして、説明を入力します。 ［Next］をクリックします。
6. ［フォームの追加］をクリックします。フォーム定義ウィザードが起動します。
7. ［フォーム名］ページで［次へ］をクリックします。
   1. フォームの名前を入力します。
   2. フォームの種類を選択します。
   3. ［特殊操作なし］が選択されていることを確認します。
   4. ［Next］をクリックします。
8. アプリケーションのログオンフォーム、パスワードの変更フォーム、パスワード変更の成功フォーム、またはパスワード変更の失敗フォームを開きます。
9. ［フォームの識別］ページで［選択］をクリックします。Webフォームウィザードが起動します。
10. 表示された［Web ページ セレクター］で、定義を作成するアプリケーションを選択します。［OK］をクリックします。アプリケーションのログオン情報用フォームを表示しているWebページ付近に点滅する枠線が示されます。
11. フォームの名前を入力し、フォームの種類を選択します。［Next］をクリックします。
12. ［フォームの識別］ページでは、識別されたURLの解釈方法を管理する2つのチェックボックスを使用できます。 適切なチェックボックスを選択して、［次へ］をクリックします。
    - URLの完全マッチ
      このチェックボックスをオンにすると、指定したURLから開始されるWebアプリケーションのログオン情報管理イベントだけが認識されます。URLの中には、セッション管理識別子、アプリケーションパラメーター、またはインスタンスごとに変化する識別子などの動的データが含まれているものもあります。このような場合に完全マッチを使用すると、そのフォームが認識されなくなります。

    - URLの大文字/小文字を区別する
      このチェックボックスをオンにすると、URLの大文字と小文字が区別されます。

13. ［フォーム アクションの定義］ページで、フォームに表示するログオン情報フィールドとボタンを構成します。
    1. 特定のログオン情報の右側の［設定/変更］のハイパーリンクをクリックします。 各ログオン情報の入力フィールドを特定するための［フィールド文字列の設定］ダイアログボックスが開きます。 ログオン情報用のフォームが既に開いている場合は、ダイアログボックスには選択したログオン情報または送信ボタン（［OK］ボタンなど）に対応するフィールドの種類が表示されます。

2. アプリケーションのログオン情報用のフォームが開いていない場合は、アプリケーションを起動して目的のフォームを開いてから、［更新］を選択します。 アプリケーションフォームを選択すると、このダイアログボックスには、選択したログオン情報に応じた種類のコントロールが表示されます。
3. ログオン情報の入力フィールドと送信ボタンを選択します。 指定したログオン情報用のフィールドや送信ボタンを簡単に見分けられるように、対応するフィールドがアプリケーション上で強調表示されます。
4. フォームで必要なすべてのログオン情報フィールドとフォームを送信するためのボタンについて、この操作を繰り返します。
   フォームの中には、ドメインやそのほかのログオン情報の入力が必要なものもあります。そのような場合に備えて、2つのカスタムフィールドが用意されています。これらのフィールドには、特別なログオン情報を割り当てます。フィールドの名前は、フォームを定義した後にアプリケーション定義ウィザードの［カスタムフィールドの名前］ページで定義します。

   注：［フォームアクションの定義］ページ上部に表示されるすべてのログオン情報用のフィールドを構成する必要はありません。

14. アプリケーションでそのほかのフォームが必要な場合は、ウィザードを使用してフォームを作成します。

テンプレートを使用してアプリケーションのアプリケーション定義を追加するには

アプリケーション定義ウィザードを使用すると、簡単にアプリケーションテンプレートを検索して、それらを展開に追加できます。

1. アプリケーション定義ウィザードを起動する準備をします。
   - AppCenterの場合：［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 AppCenter］の順に選択します。［Single Sign-On］ノードを開き、［アプリケーション定義］を選択します。
   - アプリケーション定義ツールの場合：［AppCenter］から：［スタート］ボタンをクリックし、［すべてのプログラム］>［Citrix］>［Single Sign-On］>［アプリケーション定義ツール］の順に選択します。
2. ［テンプレートの管理］を選択します。
3. テンプレートのリストを表示して、必要なアプリケーションが表示されていることを確認します。 リンクをクリックしてWebからさらにアプリケーションをダウンロードし、それらをリストにインポートすることもできます。
4. 追加するアプリケーションテンプレートを選択し、［アプリケーション定義の作成］をクリックします。
5. ウィザードを使用してアプリケーション用のフォームを編集するか、デフォルト値を受け入れます。

ユーザー構成の作成

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］ノードを選択します。
3. ［ユーザー設定の追加］をクリックします。
4. 中央ストアで表示するアプリケーションの名前を入力します。 オプションとして、説明を入力します。
5. このユーザー構成をユーザーに関連付ける方法を指定します。
   ユーザー構成は、Active Directory階層に関連付けられたユーザー（組織単位または個々のユーザー）またはActive Directoryグループに割り当てることができます。必要に応じて、［操作］メニューから［ユーザー設定の移動］を選択して、ユーザー構成を別の階層やグループに割り当てることができます。

   重要：Active Directory環境の構成は、ユーザー構成の適用に影響します。 つまり、ユーザー構成をActive Directory階層（組織単位またはユーザー）に割り当てるか、Active Directoryグループに割り当てるかを考慮する必要があります。この両方（階層とグループ）を使用していてユーザーがどちらのコンテナーにも存在する場合、階層に割り当てられたユーザ-

構成が優先的に使用されます。このようなスキームは、混在環境とみなされます。
また、ユーザーが2つのActive Directoryグループに属しており、各グループともそれぞれユーザー構成に割り当てられている場合は、優先度の高いユーザー構成が適用されます。

ユーザー構成のグループへの割り当ては、Active Directory認証を使用するActive Directoryドメインでのみサポートされています。

6. ［アプリケーションの選択］ページで、ユーザー構成用のアプリケーションを追加します。［追加］をクリックすると、ダイアログボックスが開き、作成済みのアプリケーション定義が表示されます。
7. ［Single Sign-On Plug-in の動作の設定］ページを使用して、このユーザーエクスペリエンスでのPlug-inの動作を設定します。
8. ［ライセンスの設定］ページで、ライセンスサーバーとライセンスモデルを選択します。
9. ［データ保護方法の選択］ページを使用して、ユーザの資格情報を保護するためのデータ保護方法を選択します。さまざまな認証方法に基づいてユーザーは使用を許可されます。

Single Sign-On Plug-inのインストール

XenAppサーバー上で動作するSingle Sign-On Plug-inは、そのサーバー上で実行される公開アプリケーションへのシングルサインオンアクセスを提供します。Single Sign-On Plug-inは各ユーザーデバイス上でも実行され、資格情報をアプリケーションに送信したり、ユーザーが自身の資格情報を管理できるようにします。

インストール時の考慮事項

- インストール先のオペレーティングシステムでMicrosoft GINA（Graphical Identification and Authentication）が使用されている場合は、インストール完了後にコンピューターを再起動する必要があります。このようなオペレーティングシステムとして、Microsoft Windows XP、Microsoft Windows XP Embedded、Microsoft Windows Fundamentals for Legacy PCs、Microsoft Windows Server 2003 R2、およびMicrosoft Windows Server 2003 with Service Pack 2があります。WinLogonでは、ユーザーがCtrl + Alt + Delキーを押したときに表示されるダイアログボックスでGINAコントロールが使用されています。このダイアログボックスにより、認証に必要なデータが収集されます。XenApp、Single Sign-On Plug-in、およびNovell NetWare Clientは、GINAダイナミックリンクライブラリ（DLL）と連動したり、DLLを置き換えたりして、ユーザー認証の処理方法を変更します。特定の順番でソフトウェアをインストールまたはアンインストールしないと、GINAチェーンが不正に変更され、ユーザー認証用のダイアログボックスが正しく表示されなくなる場合があります。これらのソフトウェアよりも後にSingle Sign-On Plug-inインストールすることで、WinLogonプロセスがSingle Sign-OnのGINAを最初に呼び出すようになります。

- インストールが完了すると（必要な場合はデバイスを再起動した後）、通知領域にCitrix Receiverのアイコンが表示されます。
- インストール後にCitrixライセンス情報を構成したり変更したりした場合は、Single Sign-On Plug-inを再起動する必要があります。

ユーザーデバイスまたは既存のXenAppサーバー上にSingle Sign-On Plug-inをインストールするには：

1. ユーザーデバイスまたはXenAppサーバーのドライブにXenAppインストールメディアを挿入します。
2. XenAppインストールメディアの起動画面で、［コンポーネントの個別インストール］、［サーバーコンポーネント］、［追加機能］、［Single Sign-On］、［Single Sign-On Plug-in］の順にクリックします。
3. 画面の指示に従って操作します。

ユーザーによるSingle Sign-Onの使用開始

エンドユーザーがSingle Sign-Onの使用を開始する前に、Single Sign-Onインターフェイスからエンドユーザー用のヘルプを確認してください。Single Sign-Onの動作の仕組みとこの展開でユーザーが使用できる機能について、ユーザーに通知してください。

システム要件

Sep 30, 2015

Single Sign-Onコンポーネントを実行するには、以下のシステムソフトウェアが必要です。

ソフトウェアコンポーネント	左記を必要とするコンポーネント	入手先
Microsoft Windows Installer 3.0以降（Autorunにより自動的にインストールされます）	すべて	• Single Sign-Onインストールメディアのsupportフォルダー • http://www.microsoft.com
Microsoft .NET Framework 3.5 Service Pack 1（Autorunにより自動的にインストールされます）	• Single Sign-Onサービス • 管理コンソール（Citrix AppCenterの［Single Sign-On］ノード） • アプリケーション定義ツール	Single Sign-Onインストールメディアのsupportフォルダー
Microsoft Internet Explorer Version 6.0、7.0、8.0、または9.0（非保護モード）	Single Sign-On Plug-in（Webアプリケーションを使用する場合）	http://www.microsoft.com
ASP.NET	Single Sign-Onサービス	http://www.asp.net/

• 32ビットコンピューター：Microsoft Visual C++ 2005再頒布可能パッケージ（x86）Service Pack 1
  • vc80_vcredist_x86.exe
• 64ビットコンピューター：Microsoft Visual C++ 2005再頒布可能パッケージ（x64）Service Pack 1
  • vc80_vcredist_x86.exe
  • vc80_vcredist_x64.exe
	Single Sign-Onの管理コンソール、サービス、またはPlug-in - これらのコンポーネントをコマンドラインからWindows Vista、Windows Server 2008、またはWindows Server 2008 R2上にインストールする場合	Single Sign-Onインストールメディアのsupportフォルダー

• 32ビットコンピューター：Microsoft Visual C++ 2008再頒布可能パッケージ（x86）Service Pack 1
  • vc90_vcredist_x86.exe
• 64ビットコンピューター：Microsoft Visual C++ 2008再頒布可能パッケージ（x86）Service Pack 1
  • vc90_vcredist_x86.exe
  • vc90_vcredist_x64.exe
	Single Sign-Onの管理コンソール、サービス、またはPlug-in - これらのコンポーネントをコマンドラインからWindows Vista、Windows Server 2008、またはWindows Server 2008 R2上にインストールする場合	Single Sign-Onインストールメディアのsupportフォルダー

ソフトウェアコンポーネント	左記を必要とするコンポーネント	入手先
Microsoftプライマリ相互運用アセンブリ • vs90_piaredist.exe	Single Sign-Onの管理コンソール - このコンポーネントをコマンドラインからWindows Vista、Windows Server 2008、またはWindows Server 2008 R2上にインストールする場合	Single Sign-Onインストールメディアの Supportフォルダー
Internet Explorerセキュリティ強化の構成	Single Sign-On Plug-in - Plug-inをWindows Server 2003、Windows Server 2008、またはWindows Server 2008 R2上にインストールする場合は、Internet Explorerセキュリティ強化の構成を無効にする必要があります。無効にしないと、Single Sign-On Plug-inがWebアプリケーションを処理できなくなります。	

Single Sign-Onコンポーネントの要件

Single Sign-Onコンポーネント	**サポートする環境またはMicrosoft Windowsオペレーティングシステム**	**サポートされる言語**	**ハードウェア要件**
中央ストア	• Active Directory • NTFSネットワーク共有	• 英語 • ドイツ語 • フランス語 • スペイン語 • 日本語	ユーザーあたり30KBのディスク空き容量

管理コンソール（Citrix AppCenterの［Single Sign-On］ノード） **Single Sign-Onコンポーネント**	• Microsoft Windows 7 Service Pack 1 - 32ビットおよび64ビット **サポートする環境またはMicrosoft Windowsオペレーティングシステム** • Microsoft Windows 7 - 32ビットおよび64ビット • Microsoft Windows Vista Service Pack 2（Business Edition、Ultimate Edition、Enterprise Edition） - 32ビットおよび64ビット • Microsoft Windows Vista（Business Edition、Ultimate Edition、Enterprise Edition） - 32ビットおよび64ビット • Windows XP Service Pack 3 - 32ビット • Microsoft Windows XP Professional Service Pack 2 - 32ビット • Microsoft Windows XP Professional x64 Edition - 64ビット • Windows Server 2008 R2 Service Pack 1- 64ビット • Microsoft Windows 2008 R2 - 64ビット • Microsoft Windows Server 2008 （Standard Edition、Enterprise Edition、Datacenter Edition） - 32ビットおよび64ビット • Microsoft Windows Server 2003 R2（Standard Edition、Enterprise Edition、Datacenter Edition） - 32ビットおよび64ビット • Microsoft Windows Server 2003 with Service Pack 2（Standard Edition、Enterprise Edition、Datacenter Edition） - 32ビットおよび64ビット	• 英語 **サポートされる言語** • ドイツ語 • フランス語 • スペイン語 • 日本語	• 64MBのRAM **ハードウェア要件** • 60MBのディスク空き容量
プラグイン	• Microsoft Windows 7 Service Pack 1 - 32ビットおよび64ビット • Microsoft Windows 7 - 32ビットおよび64ビット • Microsoft Windows Vista Service Pack 2（Business Edition、Ultimate Edition、Enterprise Edition） - 32ビットおよび64ビット • Microsoft Windows Vista（Business Edition、Ultimate Edition、Enterprise Edition） - 32ビットおよび64ビット • Windows XP Service Pack 3 - 32ビット • Microsoft Windows XP Professional Service Pack 2 - 32ビット • Microsoft Windows XP Professional x64 Edition - 64ビット • Microsoft Windows XP Embedded • Windows Server 2008 R2 Service Pack 1- 64ビット • Microsoft Windows 2008 R2 - 64ビット • Microsoft Windows Server 2008 （Standard Edition、Enterprise Edition、Datacenter Edition） - 32ビットおよび64ビット • Microsoft Windows Server 2003 R2（Standard	• 英語 • ドイツ語 • フランス語 • スペイン語 • 日本語 • 簡体	• 10MBのRAM • 25MBのディスク空き容量（オプション機能をインストールしない場合） • 35MBのディスク空き容量（オプション機能をインストールする場合）

Single Sign-Onコンポーネント	サポートする環境またはMicrosoft Windowsオペレーティングシステム	サポートされる言語	ハードウェア要件
	Edition、Enterprise Edition、Datacenter Edition）- 32ビットおよび64ビット • Microsoft Windows Server 2003 with Service Pack 2（Standard Edition、Enterprise Edition、Datacenter Edition） - 32ビットおよび64ビット	中国語（簡体字）	
サービス	• Windows Server 2008 R2 Service Pack 1- 64ビット • Microsoft Windows 2008 R2 - 64ビット • Microsoft Windows Server 2008（Standard Edition、Enterprise Edition、Datacenter Edition） - 32ビット • Microsoft Windows Server 2003 R2（Standard Edition、Enterprise Edition、Datacenter Edition） - 32ビット • Microsoft Windows Server 2003 with Service Pack 2（Standard Edition、Enterprise Edition、Datacenter Edition） - 32ビット	• 英語 • ドイツ語 • フランス語 • スペイン語 • 日本語	• 128MBのRAM • 30MBのディスク空き容量
アプリケーション定義ツール	Single Sign-On Plug-inと同じ	• 英語 • ドイツ語 • フランス語 • スペイン語 • 日本語	Single Sign-On Plug-inと同じ

注：Single Sign-Onは、Microsoft Windows XP Home Editionをサポートしていません。
Hot Desktopは、以下のオペレーティングシステムのみをサポートしています。

- Microsoft Windows XP Professional Service Pack 2 - 32ビット
- Microsoft Windows XP Embedded

Hot Desktopは、64ビットのオペレーティングシステムでは使用できません。

ライセンスの要件

Single Sign-Onをインストールする前に、ライセンスサーバーをインストールして、ライセンスを追加します。

この製品を使用するには、最新バージョンのライセンスサーバーを使用する必要があります。以前のバージョンのライセンスサーバーを実行している場合は、最新バージョンにアップグレードしてください。
重要：ユーザーのコンピューター上にインストールされたSingle Sign-On Plug-inを使用してCitrix XenApp, Platinum Edition環境で公開されているアプリケーションにアクセスする場合、そのSingle Sign-On Plug-in用に個別のライセンスをインストールする必要はありません。

非接続期間の設定

ラップトップを使用するモバイルユーザーなど、長期間ライセンスサーバーに接続せずに作業するユーザーには、ライセンスの非接続期間を設定する必要があります。非接続期間は、ユーザー構成のライセンス設定の一部として定義します。非接続期間により、ライセンスに関する次の期間が定義されます。

- ライセンスサーバーに接続せずに、Single Sign-Onを使用できる期間。この間、ライセンス猶予期間（30日）の適用は開始されません。非接続期間の期限が切れると、ライセンス猶予期間の適用が開始されます。
- チェックアウトされたままライセンスサーバーから切断されたコンピューターのライセンスが、ライセンスサーバー上のライセンスプールに戻るまでの期間。ライセンスがチェックアウトされた後、再度チェックインされることなくそのライセンスの非接続期間が期限切れになった場合、ライセンスサーバーはライセンスを自動的に戻し、再び使用できるようにします。たとえば、Single Sign-On Plug-inを実行しているラップトップを紛失したために組織のネットワークに再接続できない場合、非接続期間の満了時にライセンスが自動的にライセンスプールに戻されます。

非接続期間を設定することで、ライセンスがライセンスのプールに戻るまでの待機時間が指定されます。

リモートで作業をする営業担当者など、組織のネットワークに定期的に接続しないユーザーには、長めの非接続期間を設定します。コンピューターを紛失したりコンピューターが壊れたりした場合でも、非接続期間が終了するまでそのライセンスを使用できなくなります。

ライセンスの種類が混在する環境

Single Sign-On環境および組織のニーズによっては、複数の種類のスタンドアロンSingle Sign-Onライセンスを使用している場合があります。たとえば、デスクトップコンピューターおよびラップトップコンピューターからSingle Sign-On Plug-inを使用するモバイルユーザーには、指定ユーザーライセンスを使用するユーザー構成を作成し、Hot Desktopユーザーには同時接続ユーザーライセンスを使用するユーザー構成を作成できます。

この場合、指定ユーザーライセンスがすべて使用され、一部のユーザーがSingle Sign-Onを使用できなくなることがあります。そのような場合は、使用可能な同時接続ユーザーライセンスをオフラインで使用できるようにユーザー構成を定義します。

計画

Sep 30, 2015

Single Sign-Onをインストールする前に、どのように環境を設定するかについて計画する必要があります。たとえば、作成する中央ストアの種類、シングルサインオンの対象アプリケーション、使用する機能、パスワードポリシーの内容などを検討します。

Single Sign-On環境は、以下の要素で構成されます。

- 中央ストアをホストする共有ネットワークフォルダーまたはActive Directory
- Single Sign-Onの管理コンソール（Citrix AppCenter）を実行するコンピューター
- Single Sign-On Plug-inを使用するユーザーのコンピューター
- 機能モジュールがインストールされたSingle Sign-Onサービスをホストする専用サーバー
- Single Sign-On Plug-inをホストするCitrix XenApp環境
- スマートカードなどの認証デバイス
- Hot Desktopやキー管理などのSingle Sign-On機能

中央ストアの種類

Sep 30, 2015

Single Sign-Onは、中央ストアと呼ばれるリポジトリを使用して、エンドユーザーやSingle Sign-On環境に関する情報の格納や検索を行います。中央ストアのデータに基づいて、Single Sign-Onのすべてのシングルサインオン機能が実行されます。中央ストアは、Single Sign-Onのインストール時に自動的に作成したり、中央ストアの設定ユーティリティを使用して手動で作成したりできます。

中央ストアには、ユーザーデータと管理データが格納されます。

- 中央ストアのユーザーデータには、ユーザーのログオン情報、セキュリティ用の質問と回答、サービス関連のデータ（プロビジョニングデータ、質問ベースの認証データ、暗号キーの自動復元機能のデータなど）のほか、Single Sign-Onに関連する、ユーザーのWindowsレジストリデータがあります。
- 中央ストアの管理データには、アプリケーション定義、パスワードポリシー、セキュリティ用の質問、および管理コンソールでの設定データなどがあります。

中央ストアにより、ユーザーのコンピューターやXenAppサーバー上で実行されるSingle Sign-On Plug-inで、中央ストアやSingle Sign-Onサービスと通信したり、ユーザーのログオン情報をアプリケーションに送信したりする機能が提供されます。

ユーザーのコンピューター上には、Single Sign-On Plug-inによりローカルストアが保持されます。ローカルストアには、ユーザーが登録したログオン情報、暗号キーの復元に関する情報、およびセキュリティ用の質問と回答（この機能を使用する場合）だけが格納されます。ローカルストアの情報は中央ストアと同期されるため、ユーザーが組織の環境内を移動しても、保存されているログオン情報にいつでもアクセスできます。

中央ストアには以下の種類があります。

- Active Directory
  Active Directory環境およびオブジェクトを使用して、Single Sign-Onデータを格納および更新します。
- NTFSネットワーク共有
  WindowsネットワークのファイルNTFS共有を使用してSingle Sign-Onデータを格納および更新します。

必要に応じて、ほかの種類の中央ストアにユーザーを移行することもできます。

Active Directory形式の中央ストア

Active Directory形式の中央ストアを使用すると、既存のActive Directoryユーザー認証およびオブジェクト管理を活用して、Single Sign-On設定を管理できます。たとえば、Single Sign-On Plug-inの設定を、ドメインレベル、組織単位（OU）レベル、ユーザーレベルなど、対象を特定して適用することができます。

Active Directory形式の中央ストアを作成すると、Active Directoryスキーマに2つのクラスと2つの属性が追加されます。

Class	説明
citrix-SSOConfig	Single Sign-On Plug-in設定、同期の状態、アプリケーション定義、および初回使用時の動作設定データを含んだオブジェクトが定義されています。このクラスには次の属性があります。citrix-SSOConfigData：実際の設定データが含まれます。citrix-SSOConfigType：データの種類が指定されます。
citrix-SSOSecret	Single Sign-Onユーザーを認証するための機密データオブジェクトが含まれています。このクラスには次の属性があります。citrix-SSOSecretData：暗号化されたログオン情報データ、およびアカウントセルフサービスパスワードリセットデータが含まれています。

Class	説明

注：これらのクラスと属性について詳しくは、インストールメディアのToolsフォルダーにあるCitrixMPMSchema.xmlファイルを参照してください。

一般的に、以下のような場合は中央ストアとしてActive Directoryを選択します。

- 組織に影響を与えることなくActive Directoryスキーマを適切に拡張できる場合
- Active Directoryのバックアップと復元をMicrosoftの推奨どおりに実装している場合（これは必須要件ではありません）
- Active Directoryの高可用性を中央ストアデータに拡張したい場合

Active Directory形式の中央ストアの利点

Active Directory形式の中央ストアには、以下の利点があります。

- Active Directoryにはフェールオーバーと冗長性が組み込まれているため、障害回復のための追加の対策が必要ありません。
- Active Directoryのレプリケーションは、中央ストアの管理データおよびユーザーデータを組織全体に配布するのに効果的です。
- Active Directory形式の中央ストアを使用するために、ハードウェアを追加する必要はありません。

Active Directory形式の中央ストアに関する注意事項

Active Directory形式の中央ストアを使用する場合は、以下の事項について考慮してください。

- Active Directory形式の中央ストアを使用する場合はスキーマを拡張する必要があります。これには慎重な計画と実装が求められます。
- スキーマの拡張はフォレスト全体に影響します。スキーマの拡張および中央ストアの作成は、オフピーク時に行うことをお薦めします。
- これらの変更がフォレスト内のすべてのドメインコントローラーにコピーされるまでの所要時間は、Active Directoryのレプリケーションサイクルの待ち時間により異なります。WAN（Wide Area Network：広域通信網）を介したサイト間レプリケーションでは、待ち時間を軽減するためにレプリケーションを正しく設定する必要があります（サイト内レプリケーションの待ち時間はさほど長くはありません）。

NTFSネットワーク共有形式の中央ストア

NTFSネットワーク共有を中央ストアとして使用する場合は、Active Directoryスキーマを拡張することなく、既存のActive Directoryユーザー認証およびツリー構造を活用して、Single Sign-On設定を管理できます。たとえば、Single Sign-On Plug-inの設定を、ドメインレベル、組織単位（OU）レベル、ユーザーレベルなど、対象を特定して適用することができます。

重要：NTFSネットワーク共有を使用する場合、中央ストアとして使用するフォルダーに対して隠し共有を設定します。Single Sign-Onでは、CITRIXSYNC$という名前の共有フォルダーが、PeopleおよびCentralStoreRootという2つのサブフォルダーと共に作成されます。

Peopleフォルダーには、各ユーザーのサブフォルダーがあり、サブフォルダーには適切なセキュリティとアクセス権が設定されます。CentralStoreRootフォルダーには管理データが含まれます。

NTFSネットワーク共有形式の中央ストアの利点

NTFSネットワーク共有形式の中央ストアには、以下の利点があります。

- Active Directoryスキーマを拡張せずに、Active Directory中央ストアと同じように使用できます。さらに、既存のActive Directory階層およびグループを利用することができます。
  注：ユーザー構成のグループへの割り当ては、Active Directory認証を使用するActive Directoryドメインでのみサポートさ

れています。
- Active Directoryで発生するデータレプリケーションの待ち時間がないため、常に最新のユーザーデータが一元的に格納されます。
- 複数のコンピューター上のNTFSネットワーク共有に中央ストアを作成することで、各中央ストア間で負荷を分散して可用性を向上させることができます。
- Active Directory環境の認証処理の負担を軽減できます。
- 必要に応じて、後でActive Directory形式の中央ストアに移行できます。

NTFSネットワーク共有形式の中央ストアに関する注意事項

NTFSネットワーク共有形式の中央ストアを使用する場合は、以下の事項について考慮してください。
- 中央ストアをホストするために追加のハードウェアが必要になる場合があります。
- 中央ストアのファイルおよびフォルダー（それらに関連する権限を含む）のバックアップを定期的に行う必要があります。また、サイト復旧のためにファイルおよびフォルダーをレプリケートする障害復旧計画の管理と実行が必要になります。
- ユーザー（およびSingle Sign-On Plug-in）は、組織のネットワークトポロジによっては、ユーザーデータをWANリンク間で転送する必要があります。この場合は、Microsoft Windows Server 2003および2008で提供されている分散ファイルシステム技術の使用を検討します。分散ファイルシステム技術について詳しくは、Microsoft社のWebサイト（http://support.microsoft.com）を参照してください。

複数ドメイン環境での中央ストアとアカウントの関連付け機能の使用

複数のドメインを持った組織内に複数の中央ストアを作成できます。このような環境では、異なる種類の中央ストアを使用することもできます。たとえば、ユーザー構成を、あるドメインではNTFSネットワーク共有の中央ストアに割り当てて、別のドメインではActive Directoryの中央ストアに割り当てることができます。

複数のWindowsドメインを持った組織では、ユーザーが複数のWindowsアカウントを使用している場合があります。Single Sign-Onのアカウントの関連付け機能を使用すると、ユーザーが登録したログオン情報を複数のWindowsアカウント間で共有して、どのアカウントからも同じログオン情報でアプリケーションに自動ログオンできます。アカウントの関連付け機能を使用しない場合、ユーザーのログオン情報は単一のWindowsアカウントに関連付けられるため、ユーザーの所有する複数のアカウント間でログオン情報が自動的に同期されることはありません。

管理者がログオン情報の同期モジュールを使用してアカウントの関連付けを構成すると、ユーザーのログオン情報を同期させることができます。ユーザーは異なるWindowsアカウントを使っているときでも、登録済みのログオン情報を使ってアプリケーションにログオンできます。ユーザーがログオン情報を変更、追加、または削除すると、関連付けられたすべてのアカウントでのログオン情報が自動的に同期されます。

アカウントの関連付けが設定されていない場合、複数のWindowsアカウントを持つユーザーは、各Windowsアカウントから個別にログオン情報を更新する必要があります。

ユーザーがアカウントの関連付け機能を使って複数のログオン情報を同期できるようにするには、AccAssoc.exeユーティリティを公開アプリケーションとして提供してください。

アカウントの関連付け機能の利点

- アカウントの関連付けによってユーザーのログオン情報が同期するため、ログオンの管理作業や障害が軽減し、生産性の向上、ヘルプデスクへの負担軽減につながります。
- 異なる種類の中央ストア間でもアカウントを同期させることができます。つまり、Active Directoryを中央ストアとして使用するユーザーアカウントは、それと関連付けられた、NTFSネットワーク共有を使用するユーザーアカウントと同期できます。

- 異なるユーザー構成のアカウント間でもアカウントを同期させることができます。たとえば、ユーザー構成をある特定のドメインのActive Directory階層（OUまたはユーザー）と、別のドメインのActive Directoryグループに関連付けることができます。
- 同じドメインおよび同じ中央ストア内の異なるユーザー構成のアカウント間でもアカウントを同期させることができます。
- アカウントの関連付け機能を使用するために、ドメインコントローラー間に信頼関係を設定する必要はありません。

アカウントの関連付けを構成する前に、次の点に注意してください。

- Windowsにログオンするときのプライマリの認証方法としてスマートカードを使用する場合、アカウントを関連付けることはできません。
  注：各ドメインのユーザー構成に設定されているパスワードポリシーが異なるために、共有したログオン情報で自動ログオンできない場合があります。アカウントの関連付け機能では、ユーザーのログオン情報だけが同期され、ユーザー構成やパスワードポリシーは同期されません。この点を考慮して組織のパスワードポリシーを設定してください。
- 関連付けられた各ドメインアカウントで、Single Sign-Onを使用する必要があります。
- アカウントの関連付け機能でログオン情報の同期を行うには、各ユーザー構成で同じアプリケーション定義名を使用する必要があります。
- 管理者が作成したアプリケーション定義で指定されているアプリケーションのログオン情報だけが共有されます。
- Single Sign-Onサービスのログオン情報の同期モジュールは、保護されたHTTP接続で提供されるWebサービスです。そのため、アカウントの関連付け機能を使用するすべてのコンピューターからこのモジュールにアクセスできるようにする必要があります。

パスワードポリシー

Sep 30, 2015

パスワードポリシーとは、パスワードの作成、送信、および管理方法を制御するための規則です。Single Sign-Onには、デフォルトのポリシーおよびドメインポリシーという2つの標準のパスワードポリシーがあらかじめ定義されており、これらを削除することはできません。ただし、これらのポリシーを編集したり、これらのポリシーの複製を作成したりして、独自のパスワードポリシーを定義できます。

デフォルトのパスワードポリシー

Single Sign-Onのデフォルトでは、アプリケーションで使用するポリシーにデフォルトのポリシーが適用されます（ドメインのログオン情報が必要なアプリケーションを除きます）。このポリシーは、管理者がアプリケーション定義ウィザードで定義していないすべてのアプリケーション、およびアプリケーショングループに属さないすべてのアプリケーションに適用されます。

ユーザー側の［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）では、管理者が定義していないアプリケーション用のログオン情報をユーザーが自分で登録できます。

ドメインパスワードポリシー

通常、管理者はアプリケーショングループを作成して、そのグループのアプリケーションに適用するドメインポリシーを選択します。ドメインポリシーが適用されたアプリケーションには、ユーザーのドメイン用のログオン情報が使用されます。組織のActive DirectoryまたはNTのドメインのポリシーに基づいて、ドメインポリシーを変更できます。

これらのアプリケーションには、デフォルトのポリシーが適用されます。アプリケーショングループをドメインパスワード共有グループとして設定するには、そのアプリケーショングループにドメインポリシーを適用します。アプリケーショングループとは、パスワードポリシーを含む、1つまたは複数のユーザー構成に関連付けられた既存のアプリケーション定義の集合です。アプリケーショングループのアプリケーションには、共通のパスワードポリシーが適用されます。

パスワードポリシーの設定

必要に応じて、独自のパスワードポリシーを作成できます。つまり、ドメインパスワード共有グループに1つのパスワードポリシーを適用して、ほかのアプリケーショングループにそれぞれ適切なパスワードポリシーを作成することができます。

独自のパスワードポリシーを作成したり、既存のポリシーを変更したりする場合は、組織とアプリケーションで、パスワードに対する要件が同一である必要があります。作成したポリシーとアプリケーションのパスワード要件に矛盾があると、ユーザーがそのアプリケーションにログオンできなくなることがあります。

一般的に、パスワードポリシーでは以下の制限を指定することができます。

- 最小文字数と最大文字数
- アルファベットと数字の使用
- 同じ文字を繰り返し使用できる回数
- 使用できる文字/使用できない文字（特殊文字を含む）の設定
- パスワードとして入力した文字列をユーザーが確認できるかどうか
- ログオンの試行回数
- パスワードの有効期限とその警告メッセージの表示
- パスワードの履歴と禁止文字列

パスワードポリシーに関する注意事項

パスワードポリシーを作成する場合は、以下の事項を考慮してください。

- ユーザーにとっての使いやすさを考慮したセキュリティ要件が必要です。ポリシーによる制限を過剰に厳しくすると、ユーザーによるパスワードの作成、使用、および記憶が難しくなります。
- Single Sign-On自体がセキュアに設計されており、デフォルトのパスワードポリシーでもCitrixが推奨する最低限のセキュリティレベルが定義されています。ポリシーに定義されている各設定は、組織のポリシーおよび規則に沿うように変更できます。
- ユーザーが自分で追加するアプリケーションには、デフォルトのパスワードポリシーが適用されます。そのため、デフォルトのポリシーに準拠するパスワードが、アプリケーションに組み込まれている標準的なポリシーにより拒否されないように考慮する必要があります。
- ユーザーがパスワードを変更する場合に、変更前のパスワードと変更後のパスワードが照合されるようにポリシーを構成できます。これにより、有効期限が切れたパスワードをユーザーが続けて使用できないように設定できます。
- 製品スイートに含まれるアプリケーションなど、複数のアプリケーションで同じパスワードが使用される場合があります。これはパスワード共有と呼ばれ、複数のアプリケーションで同一の認証先が使用されます。
  パスワード以外のログオン情報（ユーザー名やそのほかのカスタムフィールド用の情報など）がアプリケーションごとに異なっても、同じパスワードを使用することができます。この場合、アプリケーショングループをパスワード共有グループとして設定すると、そのグループのすべてのアプリケーションを単一のパスワードで管理できるようになります。ユーザーまたはSingle Sign-On Plug-inが、任意のアプリケーションでパスワードを変更した場合、同じグループに属するすべてのアプリケーションのパスワードにその変更が反映されます。

- ドメインパスワード共有グループでは、そのほかのパスワード共有グループとは異なり、ユーザーのドメインパスワードが各アプリケーションのマスターパスワードとして使用されます。ユーザーがドメイン用のパスワードを変更すると、ドメインパスワード共有グループに属するすべてのアプリケーションのパスワードにその変更が反映されます。ただし、ドメインパスワード共有グループに属する特定のアプリケーションのパスワードだけを変更するには、管理者がそのアプリケーションをドメインパスワード共有グループから削除する必要があります。

アプリケーション定義

Sep 30, 2015

管理者は、Single Sign-Onで管理するユーザーの各アプリケーションに合わせて、アプリケーション定義を作成したり、アプリケーション定義テンプレートを変更したりできます。アプリケーション定義を作成するには、管理コンソールかアプリケーション定義ツールを使用します。アプリケーション定義ツールは、管理コンソールをインストールできないワークステーション上に単独でインストールできます。

また、アプリケーションに対するログオン情報をユーザーが自分で登録できるようにユーザー構成を定義することもできます。Single Sign-On Plug-inは、次の種類のアプリケーションのログオン要求およびパスワードの変更要求を検出して処理できます。

アプリケーションの種類	説明
Windows	Microsoft Outlook、Lotus Notes、SAPなどのパスワードで保護された32ビットのWindowsアプリケーション（Javaアプリケーションを含む）
Web	Microsoft Internet ExplorerからアクセスするWebアプリケーション（JavaアプレットおよびSAPを含む）
ターミナルエミュレーター	HLLAPI（High-Level Language Application Programming Interface）を実装したターミナルエミュレーターでアクセスするメインフレームアプリケーション（64ビットのターミナルエミュレーターはサポートされません）

Single Sign-On Plug-inでは、管理者が作成するアプリケーション定義に基づいて処理が行われます。アプリケーション定義には以下の特徴があります。

- Single Sign-On Plug-inでは、アプリケーション定義に基づいてアプリケーションおよびそのログオン用フォーム（ログオン用のダイアログボックスやWebページなど）が認識され、処理されます。
- アプリケーション定義は、アプリケーションを認識しログオンを処理するためのパラメーターである識別子セットで構成されます。

各アプリケーション定義で、アプリケーションへのアクセスに必要なログオンフォームおよびパスワード関連のフォームを検出するための定義を作成します。アプリケーション定義ウィザードを使用するときに、対象となるアプリケーションを起動しておくと、より簡単にアプリケーション定義を作成できます。アプリケーション定義ウィザードでは、ウィンドウマッチ機能によりほとんどのアプリケーションのフォームおよびフィールドが認識されます。

ヒント：Single Sign-Onには、ほかのCitrixアプリケーションで使用できるデフォルトテンプレートが用意されています。追加のテンプレートは、CitrixのサポートWebサイトで検索できます。

スマートカード

Sep 30, 2015

Citrixでは、ISO（International Organization for Standardization：国際標準化機構）の7816に準拠したスマートカードのうち、スマートカードリーダーに挿入して電気的に接触させることで情報を読み取るコンタクトカードを使って、これらの認証機能の動作確認を行いました。スマートカードリーダーは、シリアルポート、USBポート、またはPCカード（PCMCIA）ポートを使って、コンピューターに接続できます。

Citrixでは、PC/SC仕様に準拠した暗号化スマートカードをサポートしています。これらのカードは、デジタル署名や暗号化などの暗号処理に対応しています。暗号化カードは、PKI（Public Key Infrastructure）セキュリティシステムで使用される秘密キーを、安全に格納するためのものです。

情報がスマートカード内で暗号化されるため、秘密キーが外に漏れる心配がありません。また、スマートカードにユーザーのPIN（Personal Identification Number：暗証番号）を組み合わせて、認証プロセスを2段階にすることでセキュリティをさらに強化できます。PINを認証プロセスに組み込むことで、スマートカードの不正利用を防ぐことができます。

スマートカードに必要なソフトウェア

スマートカード自体の設定については、スマートカードの製造元またはシステムインテグレーターに問い合わせてください。サーバーまたはクライアントコンピューターには、次のコンポーネントが必要です。

- PC/SCソフトウェア
- Cryptographic Service Provider（CSP）ソフトウェア
- スマートカードリーダーのドライバーソフトウェア

サーバーとクライアントコンピューターのWindowsオペレーティングシステムに、既にPC/SC、CSP、またはスマートカードリーダーのドライバーが組み込まれている場合があります。使用するスマートカードがこれらのソフトウェアコンポーネントをサポートしているかどうか、または代わりに専用のソフトウェアをインストールする必要があるかどうかについては、スマートカードの製造元に問い合わせてください。

Windows Server 2008またはWindows Vista環境でスマートカードを使用できるようにするには、中央ストアをSingle Sign-On（Password Manager）4.5またはそれ以降のバージョンで作成または更新し、ユーザー構成で［Microsoft Data Protection API（移動プロファイルが必要）］を選択する必要があります。

ユーザーの同一性検証を要求する

Sep 30, 2015

以下のイベントが発生したときに、ユーザーの同一性検証プロセスが開始されるようにユーザー構成を作成できます。ユーザーの同一性検証により、別のユーザーがSingle Sign-Onの機能を使って不正にログオン情報を使用することを防ぎます。

- スマートカードからパスワード認証への変更など、ユーザーがWindowsにログオンするときの認証の方法を変更した（認証の種類の変更について、最初のみ認証を求めるユーザー構成を作成することもできます）。
- 管理者がユーザーのプライマリパスワードを変更した。
- アカウントセルフサービス機能を使用して、ユーザーがプライマリパスワードをリセットした。
- アカウントセルフサービス機能を使用して、ユーザーがアカウントのロックを解除した。
- ユーザーが、Single Sign-On Plug-inが動作していないワークステーション上でプライマリパスワードを変更した後、Single Sign-On Plug-inが動作するワークステーションにログオンした。

Single Sign-Onでは、ユーザーがSingle Sign-Onで認証されたユーザーと同一であるかを検証するよう構成できます。次のユーザー再認証方法のいずれかを選択できます。

メソッド	説明
変更前のパスワード	ユーザーは、変更前のプライマリパスワードを入力して自分の同一性を証明します。
セキュリティ用の質問（質問ベースの認証とも呼ばれます）	管理者は、質問および質問グループを作成して、ユーザーに提示する質問リストを設定しておきます。Single Sign-Onにあらかじめ用意されている質問を使用することも、独自の質問を作成することもできます。

注意：変更前のパスワードの入力のみを再認証方法として設定した場合、変更前のパスワードを忘れたユーザーは、自分の同一性を証明できなくなります。その場合、管理者は管理コンソールの［ユーザーデータのリセット］を使用して、ユーザーの再登録を可能にする必要があります。また、管理者はユーザーのアプリケーションでパスワードをリセットする必要もあります。

セキュリティ用の質問を使用した同一性検証（質問ベースの認証）

質問ベースの認証では、ユーザーに質問を提示して、登録済みの回答を正しく入力させることでユーザーの同一性を確認します。Single Sign-Onには4つの質問があらかじめ設定されており、それぞれ日本語、英語、フランス語、ドイツ語、簡体字中国語、およびスペイン語に翻訳されています。

質問ベースの認証機能を有効にすると、次の処理が行われます。

- ユーザーがSingle Sign-On Plug-inを最初に起動したときに、セキュリティ用の質問の登録ウィザードで質問が提示され、ユーザーはそれらに対する回答を登録します。
- 登録後、アカウントセルフサービス機能によるプライマリパスワードの変更またはアカウントのロック解除をユーザーに許可している場合、不正なユーザーがプライマリパスワードを変更したりアカウントのロックを解除したりすることを避けるために、セキュリティ用の質問が提示されます。

プライマリパスワードを変更するユーザーの同一性を、質問ベースの認証方法を使って検証するには、いくつかのセキュリティ用の質問で構成される質問リストを作成して、ユーザーに回答させます。この質問リストは、ユーザーがSingle Sign-On Plug-inを初めて起動したときに表示されます。ユーザーは、質問リストから必要な数の質問を選択し、それに対する回答を登録します。後でユーザーの同一性検証が必要になると、質問リストが再度表示されます。ユーザーは、登録した回答を再入力

して、自分の同一性を証明します。

ユーザーが回答を登録できるようにするには、登録を求めるメッセージの表示を有効にするか、QBAEnroll.exeユーティリティを公開アプリケーションとして提供してください。

セキュリティ用の質問を有効にしない場合、ユーザーがWindowsに初めてログオンするとき、およびプライマリパスワードを変更するときに、同一性を検証するために変更前のパスワードを入力するためのダイアログボックスが開きます。同一性検証の方法（変更前のパスワードの入力またはセキュリティ用の質問）をユーザーが選択できるよう設定することもできます。

暗号キーの自動管理

重要：ここで説明する暗号キーの自動管理機能は、セキュリティ用の質問や変更前のパスワード入力による再認証方法ほど安全ではありません。
Single Sign-Onサービスのキー管理モジュールを使用すると、ユーザーの同一性検証を行わなくても、ユーザーのログイン情報を暗号化している暗号キーを復元できるように構成できます。

暗号キーの自動管理を使用する基本的なワークフローは、以下のとおりです。

1. Single Sign-Onサービスおよびキー管理モジュールをインストールします。
2. 管理コンソールでユーザー構成を作成して、暗号キーの復元方法を選択します。このオプションは、ユーザー構成の［データの保護方法（セカンダリ）］ページで設定します。

Single Sign-On Plug-inユーザー構成の作成計画

Sep 30, 2015

ユーザー構成は、ユーザー固有の設定、パスワードポリシー、およびアプリケーションを定義したもので、Active Directory階層に関連付けられたユーザー（組織単位または個々のユーザー）またはActive Directoryグループ（サポートされていないActive Directory混在モードの配布グループやドメインローカルグループを除く）に適用されます。ユーザー構成の内容により、ユーザーのSingle Sign-On Plug-inの動作やユーザーインターフェイスが制御されます。

ユーザー構成では、ユーザーの情報や、アプリケーション定義、パスワードポリシー、同一性の検証方法などを指定します。また、ライセンス情報（ライセンスサーバーおよびライセンスの種類）も指定する必要があります。このため、ユーザー構成設定を作成しないと、ユーザーがSingle Sign-On Plug-inを使用できません。

ユーザー構成を作成する前に、以下を作成または定義しておく必要があります。

- 中央ストア
- オプションのサービスモジュール
- アプリケーション定義
- パスワードポリシー
- セキュリティ用の質問（オプション）

ユーザー構成は以下で構成されます。

- Active Directoryドメイン階層に関連付けられたユーザー（組織単位または個々のユーザー）またはグループ。
- データの保護方法
- 作成済みのアプリケーション定義。ユーザー構成の作成時に、複数のアプリケーション定義を組み合わせてアプリケーショングループを作成できます。
- アプリケーショングループに関連付けられたパスワードポリシー。ユーザー構成の作成時にアプリケーショングループを作成してユーザー構成に関連付けたり、ユー構成の作成後にアプリケーショングループを追加したりできます。
- セルフサービス機能（アカウントのロック解除とパスワードのリセット）およびキー管理オプション（変更前のパスワード、セキュリティ用の質問、および暗号キーの自動管理）。
- そのほかの、Hot Desktop、プロビジョニング、アプリケーションのサポート設定など。

ユーザー構成のグループへの割り当ては、Active Directory認証を使用するActive Directoryドメインでのみサポートされています。

Single Sign-On Plug-inのユーザー環境を計画するときに、以下の事項について考慮します。

- 既存のユーザー構成を別のユーザーグループに割り当てるには、管理コンソールでユーザー構成の複製を作成し、必要に応じて設定を変更します。
- Single Sign-Onのユーザー環境の構成は、ユーザー構成の適用に影響します。つまり、ユーザー構成をActive Directory階層（組織単位またはユーザー）に割り当てるか、Active Directoryグループに割り当てるかを検討する必要があります。この両方（階層とグループ）を使用していてユーザーがどちらのコンテナーにも存在する場合、階層に割り当てられたユーザー構成が優先的に使用されます。このようなスキームは、混在環境とみなされます。
- 中央ストアに格納されたユーザー構成の情報は、ローカルストアに格納されたユーザー構成の情報（ユーザーのコンピューターに格納されたユーザーデータ）よりも優先されます。ローカルストアのユーザーデータは、中央ストアが使用できない場合、またはオフラインの場合に使用されます。

複数ユーザーでのワークステーションの共有（Hot Desktop）

Sep 30, 2015

Hot Desktopは、ワークステーションを複数のユーザーで効率よく安全に共有するための機能です。Hot Desktopを使用すると、Single Sign-Onによるシングルサインオン機能に加えて、ユーザーセッションを高速に切り替えることができるようになります。

Hot Desktop機能を導入する前に、以下の作業を行う必要があります。

- Hot Desktop関連のユーザー構成の作成
- Hot Desktop共有アカウントの構成
- Hot Desktopワークステーションで実行するアプリケーションと、その起動および終了方法を設定するスクリプトの作成

Hot Desktopは、デフォルトではインストールされません。Single Sign-On Plug-inのインストール時に選択してインストールする必要があります。また、インストール済みのSingle Sign-On Plug-inに、後からHot Desktop機能を追加することもできます。

Hot Desktop環境でスマートカードを使用してログオンするときに、ユーザー構成でキーソースに［DPAPIとプロファイル］を指定している場合、唯一のキー復元方法として［変更前のパスワードを入力させる］を選択しないでください。このような環境では、ユーザーが変更前のパスワードを入力することが不可能なため、システムのロックを解除することができません。この問題を解決するには、キー管理モジュールによる暗号キーの自動復元を有効にするか、ユーザーが質問ベースの認証オプションを選択できるように設定してください。

Hot Desktop環境でのアプリケーションの制御

Hot Desktop機能を有効にすると、Windowsアカウントやスマートカード認証を使用して、ユーザーが高速にセッションにアクセスできるようになります。管理者がHot Desktopセッションの開始時に特定のアプリケーションが起動するように構成すると、ユーザーがそのアプリケーションを探して起動を待機する必要がなくなります。

また、Hot Desktopセッションの終了時にすべてのアプリケーションを正しく終了させて、次のユーザー用にクリーンな環境が維持されるように構成することもできます。

Hot Desktopのユーザーエクスペリエンス

ワークステーションが起動して共有アカウントで自動的にログオンすると、そのコンピューターは「高速ユーザースイッチ」モードになり、標準的なWindowsログオン画面を表示します。Hot Desktopユーザーがログオンしているかいないかにかかわらず、共有アカウントは常にログオンした状態のまま維持されます。

ログオン画面で、ユーザーは自分のWindowsアカウント情報を使用して認証を行いますが、この作業は本来の意味でのログオンとは異なります。Hot Desktopでは、そのユーザーのWindowsアカウント情報を使用して、Hot Desktopセッションが開始されます。ユーザーは、ログオンしているのではなく認証を受けただけなので、通常のログオン時に実行される、時間のかかるイベント（グループポリシーの適用やプリンターの初期化など）は、Hot Desktopセッションの開始時には発生しません。これにより、Hot Desktopセッションでの「高速ユーザースイッチ」が可能になります。ユーザーがセッションを開始して、必要な実務タスクを行い、セッションを終了すると、次のユーザーがすぐにセッションを開始できるようになります。共有ワークステーション上で、高速で効率的にユーザーを切り替えることができます。

Hot Desktopセッションが開始されると、Single Sign-On Plug-inが起動します。セッションが確立されると、Hot Desktopがユーザーのアカウント情報にアクセスして、標準的なシェルインターフェイスを使ってアプリケーションを起動し

ます。通常、これらのクライアントアプリケーションは瞬時に起動して、ユーザーにログオン情報の入力を要求します。この場合、そのユーザーのWindowsアカウントに関連付けられた設定に従って、Single Sign-On Plug-inがログオン情報を自動的に入力します。

オプションのSingle Sign-Onサービス機能の計画

Sep 30, 2015

Single Sign-Onサービスは、専用のWebサーバー上で動作するWebサービスで、このサービスと管理コンソールおよびSingle Sign-On Plug-inで共有されるデータはSSL（Secure Sockets Layer）で暗号化されます。Single Sign-Onサービスにより、Single Sign-Onの追加機能が提供されます。

以下の追加機能を使用する場合は、Single Sign-Onサービスをインストールする必要があります。

- キー管理
- データの整合性チェック
- プロビジョニング
- セルフサービス
- ログオン情報の同期

重要：Single Sign-Onサービスをホストするサーバーには、機密性の高いユーザー情報が保持されます。このため、Single Sign-Onサービス用に専用のサーバーを設定して、物理的に安全な場所で運用することをお勧めします。

キー管理

キー管理機能によりユーザーの同一性を検証するための認証処理が省かれるため、ユーザーがアプリケーションに直ちにアクセスできるようになります。暗号キーの自動管理では秘密キーが2つに分割される（キースプリット処理）ため、悪意のあるユーザーからの不正アクセスの脅威を最小限に抑えることができます。

ただし、ユーザーのネットワークパスワードを保護する「秘密の鍵」がないため、ユーザーになりすました不正なアクセスを防ぐことはできません。このような問題が起こらないように、暗号キーの自動管理機能を、アカウントセルフサービス機能および質問ベースの認証と組み合わせて使用してください。

重要：採用しているセキュリティポリシーによっては、ユーザーがSingle Sign-On Plug-inで登録したログオン情報に管理者がアクセスすることを許可している場合があります。ユーザーが管理している個人的なパスワードをSingle Sign-Onで管理するかどうかを決定する前に、組織のセキュリティポリシーを確認してください。ユーザー構成の［データの保護方法］設定で暗号キーの自動管理機能の選択を解除することでも、不正なアクセスを回避できます。

データの整合性チェック

データの整合性チェックモジュールには公開キーファイルと秘密キーファイルが含まれており、これらのファイルを使用してデータに署名を追加します。このサービスモジュールを使用すると、RSA（Rivest Shamir Adleman）公開キー暗号化技術により、認証済みの情報源からのみ設定データが取得されます。データの整合性チェックモジュールの秘密キーが配布されることはありません。

管理コンソールで署名されたデータは、その署名と一緒に中央ストアに送信されます。Single Sign-On Plug-inは中央ストアからデータと署名を受信して、ローカルストアの情報と同期します。次に、Single Sign-On Plug-inはSingle Sign-Onサービスと通信して、受信した署名を検証するための公開キーを入手します。

信頼性のある、認証済みの情報源から提供されたデータだけがSingle Sign-Onのコンポーネント間で転送されるようにするには、データの整合性モジュールをインストールします。このモジュールはオプションの機能で、信頼関係が設定されていないネットワーク環境のユーザー向けに設計されています。

整合性チェック処理に失敗したデータがSingle Sign-On Plug-inにより使用されることはありません。整合性チェック処理の失敗イベントは、Windowsのイベントログに記録されます。 また、ユーザーには、管理者に連絡する必要があるという内容のメッセージが表示されます。この場合、Single Sign-On Plug-inでは、同期前の設定がそのまま使用されるか、オフライン状態に変更されます。

IPsec（Internet Protocol Security）やSMB（Server Message Block）署名など、転送データを保護するセキュリティフレーム

ワークを導入済みの環境では、データの整合性チェックモジュールをインストールする必要はありません。

プロビジョニング

ログオン情報のプロビジョニング機能により、一部の管理プロセスが自動化されます。マシンの追加方法
- 中央ストアにログオン情報を追加したり、中央ストアに格納されているログオン情報の変更や削除をする。
- ユーザーの設定をリセットする。
- ユーザーおよびそのログオン情報をSingle Sign-On環境から消去する。

プロビジョニングを実行するには、Single Sign-On環境の情報に基づいてプロビジョニング用のテンプレートを生成し、それを必要に応じて編集して、中央ストア内のログオン情報を追加、削除、または変更します。

セルフサービス

Single Sign-Onのアカウントセルフサービス機能を使用すると、管理者やヘルプデスクの手を煩わせずに、ユーザーが自分でプライマリパスワードをリセットしたり、Windowsドメイン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。組織ニーズに応じて、セルフサービスパスワードリセットとアカウントのロック解除のどちらかまたは両方の機能を、Single Sign-On環境に安全に実装することができます。
注：アカウントセルフサービス機能を使用できるのは、Active Directory環境のWindowsドメインアカウントのパスワードをリセットしたりロックを解除したりする場合のみです。
これらのセルフサービス機能のセキュリティは、質問ベースの認証により保護されるため、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するユーザーは、セキュリティ用の質問に正しく回答できなければなりません。アカウントセルフサービス機能を使うには、まず、管理者が設定したセキュリティ用の質問に対して、ユーザーが回答を登録します。ユーザーが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しようとすると、これらの質問がユーザーの画面に表示されます。ユーザーが事前に登録した回答を入力すると、パスワードをリセットしたりロックを解除したりできます。

ログオン情報の同期

ログオン情報の同期機能（「アカウントの関連付け機能」とも呼ばれます）により、異なるWindowsアカウントでユーザーがログオンしているときでも、Single Sign-Onに登録済みのログオン情報を使ってアプリケーションにログオンできます。通常、ユーザーのログオン情報は単一のWindowsアカウントに関連付けられ、ユーザーの複数のWindowsアカウント間で自動的にログオン情報が同期されることはありません。管理者がアカウントの関連付け機能を有効にすると、ユーザーは異なるWindowsアカウントを使っているときでも、登録済みのログオン情報を使ってアプリケーションにログオンできます。ユーザーがログオン情報を変更、追加、または削除すると、関連付けられたすべてのアカウントでのログオン情報が自動的に同期されます。

Single Sign-On Plug-inの展開シナリオ

Sep 30, 2015

Single Sign-Onは、XenAppサーバーでホストされる公開アプリケーションや、ユーザーデバイス上で実行されるローカルアプリケーションでのシングルサインオン機能を提供します。

XenApp環境では、認証が必要な公開アプリケーションをホストする各XenAppサーバー上にSingle Sign-On Plug-inをインストールします。この場合、ユーザーはCitrixコネクションを介してサーバー上のSingle Sign-On Plug-inを実行します。サーバー上のSingle Sign-On Plug-inは、アプリケーションの種類（Windowsベース、Webベース、またはターミナルエミュレーターベース）を特定し、ユーザープロファイル内に格納されたローカルの情報ストアからアプリケーションへのログオン情報を取得します。

Single Sign-On Plug-inは、各ユーザーデバイス上にもインストールできます。XenApp環境で使用する場合は、後述の考慮事項を参照してください。ユーザーデバイス上にローカルにインストールされたアプリケーションでSingle Sign-Onの機能を使用する場合は、そのユーザーデバイス上にSingle Sign-On Plug-inをインストールします。

Single Sign-On Plug-inがユーザーデバイス上にインストールされているかどうかにかかわらず、ユーザーが自分でセキュリティ用の質問に対する回答を登録したり、アカウントの関連付け機能を使って複数のログオン情報を同期したりできるようにするには、管理者がXenAppサーバー上にSingle Sign-On Plug-inをインストールし、専用のアプリケーションを公開する必要があります。

Single Sign-Onは、以下のCitrix製品と一緒に使用することができます。

- Access Gateway Advanced Edition（アプリケーションはWebブラウザーを介してXenAppにより提供されます）
- Citrix XenAppの機能：
  - Citrix Receiver for Windows
  - Citrix Offline Plug-in
  - Web Interface

XenApp環境のユーザーデバイスにSingle Sign-On Plug-inを展開する

XenApp環境では、ユーザーにどのような作業を許可するかによりSingle Sign-On Plug-inをユーザーデバイス上にインストールするか、公開アプリケーションとして提供するかを決定します。いずれの展開方法でも、公開アプリケーションへのシングルサインオン機能が提供されます。

- ユーザーデバイス上にSingle Sign-On Plug-inをインストールしない場合、ユーザーには以下の作業が許可されます。
  - セキュリティ用の質問への登録を求めるメッセージに応じて回答を入力する。
  - Single Sign-Onの確認メッセージに応じてログオン情報を保存する。
  - Single Sign-Onの確認メッセージに応じてプログラムやWebサイトのパスワードを変更する。
- Single Sign-On Plug-inと一緒にインストールされるLogonManager.exeをXenAppサーバー上で公開すると、ユーザーには以下の作業が許可されます。
  - セキュリティ用の質問への登録を求めるメッセージに応じて回答を入力する。
  - Single Sign-Onの確認メッセージに応じてログオン情報を保存する。
  - Single Sign-Onの確認メッセージに応じてプログラムやWebサイトのパスワードを変更する。
  - Single Sign-Onに保存されたパスワードを編集、削除、またはパスワード文字列を表示する。
- ユーザーデバイス上にSingle Sign-On Plug-inをインストールすると、ユーザーには以下のすべての作業が許可されます（管理者が個別に無効にしたものを除く）。
  - セキュリティ用の質問への登録を求めるメッセージに応じて回答を入力する。
  - Single Sign-Onの確認メッセージに応じてログオン情報を保存する。
  - Single Sign-Onの確認メッセージに応じてプログラムやWebサイトのパスワードを変更する。

- Single Sign-Onに保存されたパスワードを編集、削除、またはパスワード文字列を表示する。
- Single Sign-Onのメッセージが表示されていないときに必要に応じてログオン情報を送信する。
- Single Sign-Onに登録済みのアプリケーションやWebサイトにログオン情報をさらに追加する。
- Single Sign-Onを一時停止/再開したり、Single Sign-Onが一時停止中かどうかを確認したりする。
- アカウントセルフサービスの使用

複数のプライマリ認証とデータの保護方法

Sep 30, 2015

ユーザー構成を作成または編集するときに、環境で使用している認証スキームに応じて、ユーザーのログオン情報をどのように暗号化して保護するかを選択できます。

以下に説明するユーザー構成のプロパティページでは、ドメインパスワードとスマートカードを使用する場合など、ユーザーがWindowsにログオンするときに使用するプライマリな認証方法が複数ある場合のSingle Sign-On Plug-inの動作およびユーザーデータの保護方法を設定できます。

［データの保護方法］プロパティ

ユーザー構成の［データの保護方法］プロパティページでは、プライマリの認証データの保護方法を選択できます。また、管理者によるユーザーのログイン情報へのアクセスを制限して、管理者がユーザーになりすましてユーザー情報を不正に入手するのを防ぎます。

［データの保護方法（セカンダリ）］プロパティ

ユーザーが自分のプライマリな認証方法を変更した場合（たとえば、ドメインパスワードやスマートカードを変更した場合）の追加のセキュリティとして、［データの保護方法（セカンダリ）］プロパティページを使用して、ユーザーのログオン情報のロックを解除する前に、ユーザーの再認証および同一性の検証を行うように設定できます。

安全性と使いやすさの両立

これら2つのプロパティページでオプションを選択する際、次の点について考慮する必要があります。

- 組織の環境で使用される認証の種類
- 組織のセキュリティ要件とすべてのユーザーにとっての使いやすさとのバランス

データの保護方法として、これらを組み合わせて使用することも可能です。最終的には、セキュリティの必要性とユーザーの使いやすさとのバランスを考慮する必要があります。

ユーザーのなりすまし

管理者がユーザーのログオン情報にアクセスすることを禁止するには、［データの保護方法］プロパティページの[アカウント管理者がユーザーデータにアクセスすることを制限しますか?］で［はい］を選択します。これにより、管理者がユーザーになりすましてユーザー情報を不正に入手することを防ぐことができます。

［データの保護方法］プロパティページのこのオプションのデフォルトの設定は、［はい］です。この場合、管理者がユーザーのパスワードなどのログイン情報にアクセスすることはできません。これにより、管理者がユーザーを偽装することを防ぐことができます。つまり、管理者がユーザーとしてログオンしても、そのユーザーのローカルの情報ストアにある情報にアクセスすることはできません。

［はい］が設定されている場合、このページの［Microsoft Data Protection API］と［データの保護方法（セカンダリ）］ページの［同一性を検証せずにネットワーク経由でプライマリのデータ保護方法を自動的に復元する］を選択することはできません。この場合、スマートカードと移動プロファイルは使用できません。また、パスワードが変更された場合、ログオン情報は自動的には復元されず、必ず再認証またはユーザーの同一性の検証が行われます。

ここで［いいえ］を選択すると、このページおよび［データの保護方法（セカンダリ）］ページのオプションをすべて使用できるようになります（再認証または同一性の検証なしでログオン情報を復元できるようにするオプションを含む）。

ユーザー名とパスワード

パスワードのみの設定がデータを保護する上での最も簡単な設定であり、これは[データの保護方法] ページでのデフォルト設定でもあります。この設定ではユーザー名とパスワードのみを使用して、管理者によるユーザーのログオン情報への不正なアクセスを防止します。

重要：この設定のセキュリティは、組織のドメインパスワードポリシーの相対的な強度に依存します。パスワードの要件が厳しい、または複雑なほど、この設定のセキュリティは強固なものになります。

オプション	説明
アカウント管理者がユーザーデータにアクセスすることを制限しますか?	「*—ユーザーのなりすまし*」を参照してください。
ユーザーの認証データ	オン。ユーザーのログオン情報が、ユーザーのプライマリパスワードに基づいて暗号化されます。プライマリパスワードとは、ユーザーがWindowsにログオンするときのドメインパスワード、トークンからのワンタイムパスワード、スマートカードのPIN、バイオメトリクス認証に含まれるユーザー情報などです。

スマートカード証明書とユーザの認証データ

スマートカードを、埋め込みの証明書またはデジタル署名、およびユーザーのログオン情報と組み合わせて使用する場合は、［スマートカード証明書］と［ユーザーの認証データ］の2つを選択します。認証用のユーザー名とパスワードをスマートカードと組み合わせて使用することで、最も安全にユーザーのログオン情報を保護できます。

スマートカードをHot Desktop環境で使用する場合は、［スマートカード証明書］を選択します。

Windows Server 2008またはWindows Vista環境でスマートカードを使用できるようにするには、中央ストアをSingle Sign-On（Password Manager）4.5またはそれ以降のバージョンで作成または更新し、ユーザー構成で［Microsoft Data Protection API（移動プロファイルが必要）］を選択する必要があります。

オプション	説明
アカウント管理者がユーザーデータにアクセスすることを制限しますか?	「*—ユーザーのなりすまし*」を参照してください。
ユーザーの認証データ	オン。 ユーザーのログオン情報が、ユーザーのプライマリパスワードに基づいて暗号化されます。 プライマリパスワードとは、ユーザーがWindowsにログオンするときのドメインパスワード、トークンからのワンタイムパスワード、スマートカードのPIN、バイオメトリクス認証に含まれるユーザー情報などです。
スマートカード証明書	オン。 ユーザーのログオン情報が、スマートカードのセキュリティ証明書に基づいて暗号化されます。

スマートカードのPINの許可

Windowsドメインで、セキュリティ証明書をサポートしていないスマートカードをプライマリの認証方法として使用する場合、または移動プロファイルを使用しない場合、［スマートカードのPINを許可する］オプションを選択します。この設定では、スマートカードのPIN（暗証番号）で暗号キーを生成し、ユーザーのログオン情報を保護します。

このオプションを使用する場合は、より強力なPINを使用することをお勧めします。スマートカードのPINに4桁の数字を使用している企業もありますが、8文字のパスワードなどに比べるとセキュリティ面での信頼性が低く、盗用される可能性が高くなります。そのため、英数字を組み合わせた8文字以上のPINを必要とする環境で使用してください。

オプション	説明
アカウント管理者がユーザーデータにアクセスすることを制限しますか?	「*—ユーザーのなりすまし*」を参照してください。
ユーザーの認証データ	オン。ユーザーのログオン情報が、ユーザーのプライマリパスワードに基づいて暗号化されます。
スマートカードのPINを許可する	オン。ユーザーのログオン情報が、スマートカードのPINに基づいて暗号化されます。強力なPINを使用している環境でのみこのオプションを使用してください。

Single Sign-On Plug-in（Password Managerエージェント）Version 4.0および4.1でこのオプションを使用するには、［Password Manager 4.1以前で使用したデータ保護方法を使用する］および［PINパスワード］を選択する必要があります。

移動プロファイル（Microsoft DPAPI）

［アカウント管理者がユーザーデータにアクセスすることを制限しますか?]で［いいえ］を選択すると、移動プロファイルおよびMicrosoft Data Protection APIを使用できます。このオプションは、埋め込みの証明書またはデジタル署名、およびユーザーのログオン情報とスマートカードを組み合わせて使用する方法（［スマートカード証明書］と［ユーザの認証データ］の両方のチェックボックスをオンにする）の次に安全性が高いオプションです。

移動プロファイルを使ってユーザーにKerberosネットワーク認証プロトコルを提供している環境では、このオプションを選択します。このオプションは、移動プロファイルが使用できる場合にだけ機能します。また、ユーザーのコンピューターに移動プロファイルを格納する場合は、このオプションを使用する必要があります。

Single Sign-Onでは、ユーザーのログオン情報を保護する暗号キーを、ユーザーのプライマリパスワードから生成します。ただし、ユーザーがプライマリの認証方法としてスマートカードを使用する場合、プライマリパスワードがないため使用できません。その場合は、［Microsoft Data Protection API］を選択します。このオプションでは、Microsoft DPAPIを使用して暗号キーを生成し、ユーザーのログオン情報を保護します（Microsoft DPAPIでは、ユーザーのプライマリパスワードで暗号キーが生成されます）。

ユーザーが、自分のコンピューターにアクセスするときにパスワードを使用し、XenAppサーバーにアクセスするときにKerberosネットワーク認証プロトコルを使用する場合は、以下のオプションを選択します。

- ［アカウント管理者がユーザーデータにアクセスすることを制限しますか?]で［いいえ］
- ユーザーの認証データ
- Microsoft Data Protection API

この場合、ユーザーはプライマリパスワードとスマートカードを使用してログオンすることもできます。

Windows Server 2008またはWindows Vista環境でスマートカードを使用できるようにするには、中央ストアをSingle Sign-On（Password Manager）4.5またはそれ以降のバージョンで作成または更新し、ユーザー構成で［Microsoft Data Protection API（移動プロファイルが必要）］を選択する必要があります。

このオプションは、Password ManagerエージェントのVersion 4.1でサポートされ、Windows XP、Windows 2000、およびWindows 2003 Serverの各プラットフォームでサポートされます。上記のバージョンを使用する場合は、［Password Manager 4.1以前で使用したデータ保護方法を使用する］および［DPAPIとプロファイル］を選択します。

空白のパスワード

空白のパスワードの使用は、セキュリティ上の要件が低く、ログオンしやすいことが重視される環境でのみ許可してください。たとえば、工場現場などで多くのユーザーが使用するようなコンピューターまたはワークステーション環境などで使用します。ログオン情報に空白のパスワードが含まれていても、Single Sign-On Plug-inによるシングルサインオンは可能です。

重要：［空白のパスワードを許可する］チェックボックスをオフにした場合、ユーザーが空白のプライマリパスワードを使用すると、Single Sign-On Plug-inでは暗号キーの生成やデータの保護が行われません。

オプション	説明
アカウント管理者がユーザーデータにアクセスすることを制限しますか?	「*—ユーザーのなりすまし*」を参照してください。
ユーザーの認証データ	オン。 ユーザーのログオン情報が、ユーザーのプライマリパスワードに基づいて暗号化されます。
空白のパスワードを許可する	オン。 ユーザーが空白のプライマリパスワードを使用する場合、ユーザーのログオン情報がユーザーIDに基づいて暗号化されます。

インストールとアップグレード

Sep 30, 2015

推奨されるインストール手順は、次のとおりです。

1. 中央ストアを作成します。
2. Citrix AppCenterをインストールします。このコンソールを使用して、Single Sign-Onを管理します。
3. 以下のいずれかの追加機能を使用する場合は、Single Sign-Onサービスをインストールします。
   - キー管理
   - セルフサービス
   - プロビジョニング
   - ログオン情報の同期
   - データの整合性チェック
     データの整合性チェックモジュールを後から追加したり、Citrix AppCenterやSingle Sign-On Plug-inの後にインストールしたりする場合は、既存の中央ストアのデータにデジタル署名を添付する必要があります。これを行うには、データの整合性チェックモジュールと一緒にインストールされるCtxSignData.exeを使用します。また、データの整合性チェックモジュールをアンインストールした場合は、中央ストアのデータからデジタル署名を削除する必要があります。
4. AppCenterをインストールしないコンピューター上でアプリケーション定義を作成する必要がある場合は、そのコンピューターにアプリケーション定義ツールをインストールします。アプリケーション定義ツールは、XenAppサーバーの役割のデフォルトコンポーネントとしてインストールされます。
5. 各ユーザーのコンピューターおよびXenAppサーバー上に、Single Sign-On Plug-inをインストールします。

重要：Single Sign-OnサービスおよびNTFSネットワーク共有形式の中央ストアをホストするサーバーには、機密性の高いユーザー情報が保持されます。専用のサーバーを用意して、物理的に安全な場所に設置してください。
以下のインストール構成は推奨されず、サポートされません。

- 同じコンピューター上にサービスとPlug-inの両方をインストールしないでください。
- 同じコンピューター上にサービスとXenAppサーバーの役割の両方をインストールしないでください。
- ドメインコントローラーとして動作するコンピューター上にSingle Sign-Onをインストールしないでください。ドメインコントローラー上にAppCenter、サービス、またはPlug-inをインストールしたり、NTFSネットワーク共有形式の中央ストアを作成することはサポートされていません。

Single Sign-On 5.0へのアップグレード

Single Sign-On Version 5.0へのアップグレードは、環境全体に対して実施したり、段階的に実施したりできます。

環境全体をアップグレードするには

1. 必須条件ではありませんが、事前にライセンスサーバーを最新バージョンにアップグレードし、必要なライセンスを追加しておくことをお勧めします。
2. 以下のいずれかのモジュールを使用している場合は、Single Sign-Onサービスをアップグレードします。 Single Sign-Onサービスの新しいモジュールを追加する場合は、ここでインストールすることもできます。
   - キー管理
   - セルフサービス
   - プロビジョニング
   - ログオン情報の同期
   - データの整合性チェック

   注：データの整合性チェックモジュールを後から追加したり、Citrix AppCenterやSingle Sign-On Plug-inの後にインストー

ルしたりする場合は、既存の中央ストアのデータにデジタル署名を添付する必要があります。これを行うには、データの整合性チェックモジュールと一緒にインストールされるCtxSignData.exeを使用します。また、データの整合性チェックモジュールをアンインストールした場合は、中央ストアのデータからデジタル署名を削除する必要があります。

3. 既存の管理コンソールを、Single Sign-On管理コンソール（AppCenterの［Single Sign-On］ノード）にアップグレードします。
   注：
   - Single Sign-Onサービスと管理コンソールは、同じバージョンを使用することをお勧めします。
   - 管理コンソールをVersion 5.0にアップグレードすると、Single Sign-On中央ストアもアップグレードされます。Single Sign-On 4.8の管理コンソールをVersion 5.0にアップグレードすると、Single Sign-On 4.8の管理コンソールを使って中央ストアを変更することができなくなります。
4. アプリケーション定義の作成のみを行う場合は、アプリケーション定義ツールを環境内の任意のコンピューターにインストール（またはアップグレード）します。 アプリケーション定義ツールは、XenAppサーバーの役割のデフォルトコンポーネントとしてインストールされます。
5. Single Sign-On中央ストアをアップグレードします。
   - NTFSネットワーク共有ベースの中央ストア：
     - アップグレードを行う前に、中央ストアのネットワーク共有フォルダーをバックアップします。
     - 中央ストアをアップグレードするには、AppCenterの［Single Sign-On］ノードを選択して検出の設定と実行ウィザードを実行します。これにより、中央ストアが自動的にアップグレードされます。
     - 検出の設定と実行ウィザードで、既存のNTFSネットワーク共有のUNCパス（\\servername\CITRIXSYNC$など。servernameは中央ストアが存在するサーバーの名前）を入力します。
   - Active Directoryベースの中央ストアをアップグレードするには、AppCenterの［Single Sign-On］ノードを選択して検出の設定と実行ウィザードを実行します。これにより、中央ストアが自動的にアップグレードされます。
   - Novell共有フォルダー形式の中央ストアを使用していたPassword Manager（Version 4.6など）をアップグレードする場合は、その中央ストアをバックアップしてから管理データをエクスポートしておく必要があります。中央ストアのデータを移動する方法については、Password Manager 4.6の『管理者ガイド』および『インストールガイド』を参照してください。これらのドキュメントは、Citrix Knowledge Centerで公開されています。
6. Citrix AppCenter上でSingle Sign-On環境の設定を行ってから、ユーザーデバイス上にSingle Sign-On Plug-inをインストールします。

段階的にアップグレードするには

1. まず、Single Sign-On 5.0 Plug-inが動作するユーザーデバイスを、既存の（Single Sign-On 4.8）環境に追加します。
2. 次に、Single Sign-Onサービスおよび管理コンソールをVersion 5.0にアップグレードします。
3. ほかのユーザーデバイスにSingle Sign-On 5.0 Plug-inを配布します。

Single Sign-Onのインストールに必要なセキュリティとアカウントの設定

Sep 30, 2015

Single Sign-Onサービスをインストールする前に、このサービスに必要なアカウントとコンポーネントを用意します。また、Single Sign-Onサービスはセキュアなhttp（HTTPS）を使用するので、管理コンソールおよびSingle Sign-On Plug-inとのSSL（Secure Sockets Layer）通信のサーバー認証証明書が必要です。

サーバー認証証明書の入手とインストール

CA（Certificate Authority：証明機関）からSSL通信のサーバー認証証明書を入手します。 PKI（Public Key Infrastructure）が導入済みの場合は、サービスを実行するサーバーに証明書をダウンロードします。

Single Sign-Onサービスと管理コンソールおよびPlug-in間の通信のセキュリティを確立するため、また、Plug-inと管理コンソールが正しいサービスサーバーと通信するためには、SSL証明書が必要です。

- この証明書はSSL通信で使用されるため、証明書の一般名（Common Name）と、そのサーバーの完全修飾ドメイン名（FQDN：Fully Qualified Domain Name。 host.subdomain.co.jpなど）が一致している必要があります。また、最小キーサイズには1024を指定してください。
- 証明書をローカルコンピューターの証明書ストアにインストールして、管理コンソール（Citrix AppCenterの［Single Sign-On］ノード）とPlug-inの信頼関係を設定する必要があります。
- この証明書は、Citrix AppCenter、Plug-in、およびサービスを実行する各コンピューター上にインストールしてください。
- 負荷分散またはクラスター化が設定されたサービス環境では、SSL証明書の一般名にワイルドカード（通常はアスタリスク*）を使用して、1つの証明書を複数のサービスサーバーで使用できます。たとえば、server*.mycompanysname.comという一般名のSSL証明書を、server1.mycompanysname.com、server2.mycompanysname.com、およびserver3.mycompanysname.comという名前のサーバーに使用することができます。また、この場合、*.mycompanysname.comという一般名のSSL証明書を使用することもできます。

重要：所属組織で独自にインストールした証明期間など、オペレーティングシステムのデフォルトで信頼されていない証明機関から証明書を入手する場合は、ルート証明書をローカルコンピューターの信頼されたルート証明機関の証明書ストアにインストールして、信頼関係を設定する必要があります。
SSL障害の原因の多くは、サーバー証明書が信頼されていないことにあります。ルート証明書の取得と配布について詳しくは、Microsoft社のWebサイトを参照してください。

Single Sign-Onのインストール時に作成される証明書の署名および検証は、SSL証明書とは無関係です。

サービスモジュールに必要なアカウント

Single Sign-Onサービスを実行するには、データの読み書き用のシステムアカウントが最大3つ必要です。必要なアカウントの数と種類は、インストールするサービスモジュールによって異なります。次の表は、Single Sign-Onサービスの各モジュールで必要なアカウントを示します。複数のモジュールで同じ種類のアカウントが必要な場合は、同じアカウントを複数のモジュールに使用したり、モジュールごとに専用のアカウントを指定したりできます

モジュール	**必要なアカウント**		
	サービス	**データプロキシ**	**セルフサービス**
データの整合性チェック	はい	いいえ	いいえ

キー管理モジュール	はい	はい	いいえ
プロビジョニング	はい	はい	いいえ
セルフサービス	はい	はい	はい
ログオン情報の同期	はい	いいえ	いいえ

Single Sign-Onサービス用アカウント

Single Sign-Onサービスを実行するサーバー上の既存のNetwork ServiceアカウントまたはLocal Serviceアカウントを使用します。

このバージョンのSingle Sign-Onでは、サービス用のアカウントとしてローカルユーザーアカウントを指定することはできません。既存のLocal Serviceアカウントを指定できます。

ドメインアカウントをサービスアカウントとして作成する場合、setspn.exeユーティリティを使って、このドメインアカウントのサービスプリンシパル名（SPN）およびActive Directoryのサービスサーバーを登録する必要があります。ドメインユーザーアカウントを使用する場合は、そのアカウントに「サービスとしてログオン」アクセス許可が割り当てられている必要があります。サービスを実行するコンピューターでは、委任に対する信頼を設定する必要があります。

サービスプリンシパル名について詳しくは、Microsoft社のWebサイトを参照してください。

データプロキシ用アカウント

Single Sign-Onサービスを実行するサーバー上で、Single Sign-Onサービスとのデータプロキシ通信に使用するドメイン管理者アカウントを次の設定で作成します。

アカウントには、中央ストアへの読み書き用のアクセス権が必要です。必要なアカウントは、導入する中央ストアの種類によって異なります。

中央ストアの種類	アカウントの説明
NTFSネットワーク共有	アカウントの条件は、以下のとおりです。 • 中央ストアへの読み書き用のアクセス権を所有している。 • 同じドメインに属している。 中央ストアの作成後に、以下を行います。 • CITRIXSYNC$共有に対するフルコントロール共有アクセス許可を設定する。 • CITRIXSYNCフォルダーおよびそのサブフォルダー（CentralStoreRootフォルダーとPeopleフォルダー）に完全な共有権限を設定する。 • CITRIXSYNCフォルダーおよびそのサブフォルダーのすべてのファイルオブジェクトに対するフルコントロールアクセス許可を設定する。 • Authenticated Usersグループに、Peopleフォルダー内にフォルダーを作成する権限を付与する。
Active Directory	アカウントの条件は、以下のとおりです。 • 中央ストアへの読み書き用のアクセス権を所有している。 • 同じドメイン管理者グループに属している。

Self-Serviceの要件

アカウントセルフサービスモジュールのセルフサービスパスワードリセット機能またはセルフサービスロック解除機能を使用するには、ドメイン管理者グループに属しているアカウントを使用します。

Single Sign-Onで必要なアカウント

Single Sign-Onサービスをインストールしたり、サービス設定ウィザードを実行したりするには、ドメインのメンバー（ドメインユーザー）で、かつインストール先コンピューターのローカル管理者グループのメンバーである必要があります（ドメインユーザーアカウントをローカル管理者グループに追加します）。

管理コンソール（Citrix AppCenterの［Single Sign-On］ノード）をインストールしたり、管理コンソール上で検出を実行したりSingle Sign-On環境を管理したりするには、ドメイン管理者で、かつ管理コンソールが動作するコンピューターのローカル管理者グループのメンバーである必要があります。このユーザーアカウントには、中央ストアへの読み書き用のアクセス権が必要です。管理者以外のユーザーアカウントには、Active Directory委任または制約付き委任を介して管理コンソールおよびその関連の機能を管理できる権限を割り当てることができます。

Single Sign-On Plug-inをインストールするには、ドメインのメンバー（ドメインユーザー）で、かつインストール先コンピューターのローカル管理者グループのメンバーである必要があります。Single Sign-On Plug-inをインストールするには、ドメインのメンバー（ドメインユーザー）で、かつインストール先コンピューターのローカル管理者グループのメンバーである必要があります。また、Single Sign-On Plug-inを使用するユーザーは、ドメインのメンバー（ドメインユーザー）である必要があります。

JRE（Java Runtime Environment）のインストール

Sep 30, 2015

Single Sign-Onでは、Java Runtime Environment（JRE）, Versions 1.4.x、5（1.5.x）、および6（1.6.x）がサポートされます。これらのJREは、Sun Microsystems社のWebサイト（http://java.sun.com）から入手できます。

Single Sign-Onインストール後のJREのインストールまたはアップグレード

Single Sign-Onの管理コンソール（デリバリーサービスコンソール）、アプリケーション定義ツール、またはPlug-inのインストール後にJREをインストールしたりアップグレードしたりした場合は、Single Sign-Onコンポーネントを新しいJREに関連付け直す必要があります。

1. コントロールパネルの［プログラムと機能］（または［プログラムの追加と削除］）を開き、インストール済みのSingle Sign-Onコンポーネントを選択します。
2. ［変更］をクリックします。
3. セットアップのメンテナンス処理のオプションとして、［修復］をクリックします。

Single Sign-On Plug-inのインストール/アンインストール時にJava関連のエラーが発生する場合

Single Sign-On Plug-inのインストール時またはアンインストール時に、次のエラーメッセージが表示される場合があります。

「実行中のJavaソフトウェアプログラムがあります。すべてのアプリケーションとJava関連のサービスを停止してから再試行してください。」

このエラーは、通常、そのコンピューター上でApache Tomcat、Apache HTTPサーバーなどのWebサーバーサービスが実行されている場合に発生します。また、また、ライセンス管理コンソールがインストールされたXenAppサーバー上でも発生する場合があります。

このような場合は、以下の手順を行います。

1. 実行中のサービスを停止します。
2. Single Sign-On Plug-inをインストールまたはアンインストールします。
3. サービスを再起動します。

中央ストアの作成

Sep 30, 2015

1. XenAppインストールメディアを挿入します。
2. XenAppインストールメディアの起動画面で、［コンポーネントの個別インストール］、［サーバーコンポーネント］、［追加機能］、［Single Sign-On］の順にクリックします。
3. ［中央ストア］をクリックします。
4. 中央ストアの種類として、［NTFSネットワーク共有］または［Active Directory］を選択します。
   - ［NTFS ネットワーク共有］を選択した場合は、中央ストアが%SystemDrive%\CITRIXSYNC$フォルダーに作成されます。
   - ［Active Directory］を選択した場合は、以下の手順に従います。
     1. ［手順1：Active Directoryスキーマの拡張］を選択します。Active Directoryスキーマが拡張されます。
     2. ［手順2：中央ストアの作成］を選択します。
     3. 中央ストアが作成されたら、Single Sign-on管理コンソールがインストールされているサーバーを再起動してください。これにより、中央ストアが検出されます。

     重要：サーバーがActive Directoryドメインの一部で、Schema AdministratorsグループおよびドメインAdministratorsグループのメンバーでログオンしていることを確認してください。サーバーにActive Directoryスキーママスターが割り当てられており、更新が可能であることを確認してください。また、ドメインコントローラーでないサーバー上でActive Directoryスキーマを拡張する場合は、Microsoft WindowsユーティリティであるLdifde.exeがインストールされていることを確認してから、この手順を実行してください。このユーティリティは、Windowsのインストールメディアまたは Microsoft社のWebサイトから入手できます。Ldifde.exeがインストールされていないサーバーでは、この手順を実行できません。

管理コンソールのインストール

Sep 30, 2015

Single Sign-Onの管理コンソールは、Citrix AppCenterの一部としてインストールされます。

重要：管理コンソールをインストールした後で検出の設定と実行ウィザードを実行する前に、Single Sign-On中央ストアを作成しておく必要があります。

XenAppのインストール時にAppCenter（およびSingle Sign-Onの管理コンソール）をインストールするには

1. XenAppサーバーの役割のインストールを開始します。 この役割では、デフォルトでAppCenterも一緒にインストールされます。
2. AppCenterを開き、［検出の設定と実行］を選択し、ウィザードの指示に従って操作します。

AppCenter（およびSingle Sign-Onの管理コンソール）を単独でインストールするには

システム要件に記載されているように、必要なMicrosoft Visual C++再頒布可能パッケージとMicrosoftプライマリ相互運用アセンブリがインストールされていることを確認してください。

1. XenAppインストールメディアを挿入します。
2. XenAppインストールメディアの起動画面で、［コンポーネントの個別インストール］、［共通コンポーネント］、［管理コンソール］の順にクリックします。 画面の指示に従って操作します。
3. AppCenterを開き、［検出の設定と実行］を選択し、ウィザードの指示に従って操作します。

サービスモジュールのインストールと設定

Sep 30, 2015

インストールおよび設定プロセスは、次のとおりです。

1. SSL証明書を取得し、Single Sign-Onサービス、管理コンソール、およびSingle Sign-On Plug-inを実行する各コンピューターにインストールします。
2. インストールする各サービスに必要なアカウントの種類を作成します。
3. サービスモジュールをインストールします。
4. サービスモジュールを構成します。

以下の手順を実行するには、Single Sign-Onサービスをインストールするコンピューターに XenAppのインストールメディアを挿入し、起動画面を開きます。

サービスモジュールをインストールするには

1. XenAppインストールメディアを挿入します。
2. XenAppインストールメディアの起動画面で、［コンポーネントの個別インストール］、［サーバーコンポーネント］、［追加機能］、［Single Sign-On］、［Single Sign-Onサービス］の順にクリックします。
3. 画面の指示に従って操作します。

サービスモジュールを構成するには

Single Sign-Onサービスのインストールが完了すると、サービス設定ウィザードが起動します。このウィザードを後で起動するには、［スタート］、［すべてのプログラム］、［Citrix］、［Single Sign-On］、［サービスの設定］の順に選択します。

画面の指示に従って操作します。

- ［サービス設定］ページでは、以下の設定を行います。

接続設定	サービス接続のポート番号を指定します。デフォルトのポート番号は443です。必要に応じて、サービスを実行するサーバーで使用可能なほかのポートを指定します。 サービスモジュールを追加でインストールする場合は、Single Sign-Onサービスを最初にインストールしたときに指定したポート番号を使用します。 Single Sign-Onサービスを複数のポートで実行することはできません。このため、異なるポートを指定すると、Single Sign-Onサービスとの通信エラーが発生します。 コマンドプロンプトでデータ署名ツールCtxSignData.exeを使用するときは、正しいサービスポート番号を指定してください。
SSL証明書	サービスをホストするコンピューターにインストールされたSSL証明書を選択します。この証明書は、クライアントコンピューターとの通信に使用されます。 証明書のLDAP情報を表示するには、［長い名前を表示する］チェックボックスをオンにします。

仮想ホスト名	SSL証明書名と仮想ホスト名が同じ場合、［デフォルトのホスト名を使用する］がデフォルトで選択されています。仮想ホスト名はSSL証明書名と同じでなければなりません。 仮想ホストとは、証明書が作成されたときに表示されるコンピューター名で、実際のコンピューター名とは異なる場合があります。たとえば、証明書名にワイルドカード（*）が使用されていたり、ドメイン名の大文字/小文字の使用が異なっていたりする場合があります。 負荷分散またはクラスター化が設定されたサービス環境に便利な設定です。
アカウント情報	サービスで使用するローカルコンピューターのアカウントを選択します。通常は、Network Serviceアカウントを選択します。

- ［ドメインの設定］ページでは、以下の設定を行います。
  1. Single Sign-Onサービスの機能を使用するドメインのチェックボックスをオンにします。
  2. ドメインを選択（複数選択可）して［プロパティ］をクリックし、［設定変更］ダイアログボックスを開きます。
  3. Active Directoryの中央ストアを作成した場合は、［ドメインコントローラー］をクリックし、適切なドメインコントローラーを選択します。
  4. ［データプロキシアカウント］ページでは、中央ストアとの通信に使用するデータプロキシ用のアカウントのユーザー名、パスワード、およびドメインを入力します。
  5. セルフサービスモジュールをインストールした場合は、［アカウントセルフサービス機能用のアカウント］ページでこの機能で使用するアカウントの情報を入力します。［OK］をクリックして［設定変更］ダイアログボックスを閉じます。
     重要：Windows Server 2008またはWindows Server 2008 R2が動作するサーバー環境でNTFSネットワーク共有の中央ストアを使用する場合は、CtxFileSyncPrep.exeを使用して、データプロキシアカウントを管理者として中央ストアに追加する必要があります。以下のコマンドを入力します。
     CtxFileSyncPrep[/Admin:accountname]

     Windows Server 2008またはWindows Server 2008 R2が動作するサーバー環境でActive Directoryの中央ストアを使用する場合も同様に、データプロキシアカウントを管理者として中央ストアに追加する必要があります。方法については、Citrix社のWebサイト（http://support.citrix.com/article/CTX115127）を参照してください。

Single Sign-Onサービスの複数ドメインサポートを設定する

Single Sign-Onサービスでは、信頼関係が設定された異なるドメインに属するユーザーからのサービス要求を処理できます。管理者は、異なるドメインに属するコンピューター上にSingle Sign-On管理コンソール（Citrix AppCenter）をインストールして、それぞれのドメインのユーザー構成を作成できます。

たとえば、ドメインAに属するコンピューター上のSingle Sign-Onサービスでは、ドメインAのユーザー構成に関連付けられたユーザーがアカウントセルフサービス機能を使ってアカウントのロックを解除できます。複数ドメインでのサービスのサポートにより、ドメインBのユーザー構成に関連付けられたユーザーも、ドメインAに属するコンピューターで提供されるアカウントセルフサービス機能を使用できます。この場合、異なるドメインに属する複数のユーザー構成で、同じコンピューター上のサービスが使用されます。

複数ドメインサポートに必要な条件

Single Sign-Onサービスの複数ドメインサポート機能を使用するには、以下の条件を満たしている必要があります。

コンポーネント	条件
ドメイン	Single Sign-Onサービスを共有する各ドメインが、同じドメインフォレストに属している必要があります。 同じフォレスト内のドメイン間で、双方向の推移性の信頼関係が設定されている必要があります。
中央ストア	中央ストアの種類として、Active DirectoryまたはNTFSネットワーク共有を使用する必要があります。 Single Sign-Onサービスを共有するすべてのユーザーが、同じ種類の中央ストア（Active DirectoryまたはNTFSネットワーク共有）に関連付けられている必要があります。異なる種類の中央ストアはサポートされません。 この場合、ドメインごとに1つのNTFSネットワーク共有の中央ストアを使用することはできません。ただし、フォレストごとに1つのNTFSネットワーク共有の中央ストアを使用することは可能です。
データの整合性	データの整合性機能について、すべてのドメインで同じ設定を使用する必要があります。つまり、すべてのドメインのサービス設定とPlug-in設定でこの機能を有効にするか、またはすべてのドメインで無効にする必要があります。たとえば、Single Sign-Onサービスの設定でデータの整合性機能を有効にして、Single Sign-On Plug-inのインストール時にこの機能を無効にすることはできません。
管理コンソール（Citrix AppCenterの［Single Sign-On］ノード）	各管理コンソールに表示される中央ストアは1つのみです。1つの管理コンソールで複数の中央ストアを使用することはできません。 管理者は、各ドメインに、そのドメインの管理者権限で管理コンソールをインストールする必要があります。 または、いったんログオフしてからほかのドメインにログオンし直して、管理コンソールで表示するドメインを変更することもできます。
データプロキシとセルフサービスのアカウント	管理者は、データプロキシ用およびセルフサービス用のアカウントとして、中央ストアへの読み書きアクセスと、ユーザーのパスワードをリセットできる権限を持つ1つのアカウントを使用できます。 必要な場合は、サービスの設定ツールでこれらのアカウントを各ドメインについて指定できます。

Single Sign-Onサービスの複数ドメインサポートを構成するには

1. Single Sign-Onサービスがインストールされたコンピューターに、管理者権限でログオンします。
2. ［スタート］、［すべてのプログラム］、［Citrix］、［Single Sign-On］、［サービスの設定］の順に選択します。
3. ［サービス設定の編集］ダイアログボックス左側で、［ドメインの設定］をクリックします。
4. Single Sign-Onサービスの機能を使用するドメインのチェックボックスをオンにします。
5. ドメインを選択（複数選択可）して［プロパティ］をクリックし、［設定変更］ダイアログボックスを開きます。
6. ［設定変更］ダイアログボックスでは、以下の設定を行います。
    1. Active Directoryの中央ストアを作成した場合は、［ドメインコントローラー］をクリックし、中央ストアにデータを書

き込むときにバインドするドメインコントローラーを一覧から選択するか、［書き込み可能な任意のドメインコントローラー］を選択します。

2. ［データプロキシアカウント］ページでは、中央ストアとの通信に使用するデータプロキシ用のアカウントのユーザー名、パスワード、およびドメインを入力します。
3. セルフサービスモジュールをインストールした場合は、［アカウントセルフサービス機能用のアカウント］ページでこの機能で使用するアカウントの情報を入力します。

Single Sign-On Plug-inのインストール

Sep 30, 2015

XenAppサーバー上で動作するSingle Sign-On Plug-inは、そのサーバー上で実行される公開アプリケーションへのシングルサインオンアクセスを提供します。各ユーザーデバイス上で動作するSingle Sign-On Plug-inは、そのデバイス上でローカルに実行されるアプリケーションへのシングルサインオンアクセスを提供します。この場合、ユーザーがSingle Sign-Onの動作を制御することもできます。

注：このバージョンのSingle Sign-On Plug-inをXenApp上で使用して公開アプリケーションへのシングルサインオンを提供する場合は、ユーザーデバイス上にもSingle Sign-On Plug-inをインストールする必要があります。ユーザーデバイス上にSingle Sign-On Plug-inがインストールされていない場合、XenAppサーバー上で実行される公開アプリケーションへのシングルサインオン機能は提供されますが、パスワードの編集、削除、パスワード文字列の表示、Single Sign-Onの一時停止/再開、Single Sign-Onが一時停止中かどうかの確認、およびパスワードの手作業での送信などの操作をユーザーが実行できなくなります。

インストール時の考慮事項

- Single Sign-on Plug-in Version 4.8がインストールされているユーザーデバイスにこのバージョンをインストールすると、既存のSingle Sign-on Plug-inがアップグレードされます。
- インストール先のオペレーティングシステムでMicrosoft GINA（Graphical Identification and Authentication）が使用されている場合は、インストール完了後にコンピューターを再起動する必要があります。このようなオペレーティングシステムとして、Microsoft Windows XP、Microsoft Windows XP Embedded、Microsoft Windows Fundamentals for Legacy PCs、Microsoft Windows Server 2003 R2、およびMicrosoft Windows Server 2003 with Service Pack 2があります。WinLogonでは、ユーザーがCtrl + Alt + Delキーを押したときに表示されるダイアログボックスでGINAコントロールが使用されています。このダイアログボックスにより、認証に必要なデータが収集されます。XenApp、Single Sign-On Plug-in、およびNovell NetWare Clientは、GINAダイナミックリンクライブラリ（DLL）と連動したり、DLLを置き換えたりして、ユーザー認証の処理方法を変更します。特定の順番でソフトウェアをインストールまたはアンインストールしないと、GINAチェーンが不正に変更され、ユーザー認証用のダイアログボックスが正しく表示されなくなる場合があります。これらのソフトウェアよりも後にSingle Sign-On Plug-inインストールすることで、WinLogonプロセスがSingle Sign-OnのGINAを最初に呼び出すようになります。
- インストールが完了すると（必要な場合はデバイスを再起動した後）、通知領域にCitrix Receiverのアイコンが表示されます。
- インストール後にCitrixライセンス情報を構成したり変更したりした場合は、Single Sign-On Plug-inを再起動する必要があります。

XenAppのインストール時にSingle Sign-On Plug-inをインストールするには（インストールウィザード）

1. 「*— ウィザード形式のサーバーの役割マネージャーでXenAppをインストールする*」の手順に従って操作します。 オプションコンポーネントの一覧で、[Single Sign-On Plug-in]を選択します。
2. Citrix XenAppサーバー構成ツールでXenAppを構成するときに、中央ストアの種類として[Microsoft Active Directory]（デフォルト）または[NTFSネットワーク共有]を選択し、パスを指定します。

XenAppのインストール時にSingle Sign-On Plug-inをインストールするには（コマンドライン）

1. 「*— XenAppをコマンドラインからインストールする*」の手順に従って操作します。 SSONAgentFeatureオプションを指定します（/install:XenApp,SSONAgentFeature）。
2. コマンドラインでXenAppを構成するときに、中央ストアの種類としてNTFSネットワーク共有を使用する場合は/SSOPluginUncPath:pathオプションを指定します。ここで、pathは中央ストアのNTFSネットワーク共有のUNCパスを示します。 中央ストアの種類としてActive Directoryを使用する場合は、このオプションを省略します。

ユーザーデバイスまたは既存のXenAppサーバー上にSingle Sign-On Plug-inをインストールするには

1. ユーザーデバイスまたはXenAppサーバーのドライブにXenAppインストールメディアを挿入します。
2. XenAppインストールメディアの起動画面で、［コンポーネントの個別インストール］、［サーバーコンポーネント］、［追加機能］、［Single Sign-On］、［Single Sign-On Plug-in］の順にクリックします。
3. 画面の指示に従って操作します。中央ストアの種類と、インストールするコンポーネント（言語パック、セルフサービス、データの整合性チェックなど）を指定する画面が開きます。

Merchandising Serverを使ってSingle Sign-On Plug-inをユーザーデバイスにインストールするには

Merchandising Serverのドキュメントを参照して、Single Sign-On Plug-inをダウンロードまたは配信します。

Microsoft Windows通知領域に表示されるアイコンについて

このバージョンのSingle Sign-On Plug-inをXenAppサーバーやユーザーデバイスにインストールすると、各ユーザーデバイスのMicrosoft Windows通知領域にReceiverアイコンが1つだけ表示されます。このアイコンを使用して、すべてのセッション用のSingle Sign-Onメニューを表示できます。

ただし、XenAppサーバーまたはユーザーデバイス上に以前のバージョンのソフトウェアがインストールされていると、通知領域にSingle Sign-Onアイコンが表示されます。次の表は、XenAppサーバーとユーザーデバイス上にインストールされているソフトウェアのバージョンと、通知領域に表示されるアイコンの関係を示しています。

ユーザーデバイス		XenAppサーバー		Windows通知領域	Receiverアイコンからパスワード関連のメニューを使用できるかどうか
Citrix Receiver	Single Sign-On Plug-in	Citrix Receiver	Single Sign-On Plug-in		
現行 *	5.0	現行	5.0	Receiverアイコンのみ	はい
現行	-	現行	5.0	Receiverアイコンのみ	いいえ
現行	5.0	-	4.8	Receiverアイコンと、XenAppセッションと同数のSingle Sign-Onアイコン**	はい
現行	4.8	現行	5.0	ReceiverアイコンとSingle Sign-Onアイコン	いいえ
現行	4.8	現行	4.8	ReceiverアイコンとSingle Sign-Onアイコン、さらにXenAppセッションと同数のSingle Sign-Onアイコン**	いいえ
以前のバージョンのOnline Plug-in	4.8	現行	5.0	Single Sign-OnアイコンとOnline Plug-inアイコン	いいえ

* 「現行」とは、現行バージョンのReceiver for Windowsを指し、このソフトウェアには最新のOnline Plug-inの機能も含まれています。

** XenAppサーバー上に以前のバージョンのSingle Sign-On Plug-inがインストールされており、ユーザーデバイス上に現行のReceiverがインストールされている場合（Single Sign-On Plug-inがユーザーデバイス上にインストールされているかど

ユーザーデバイス		XenAppサーバー		Windows通知領域	Receiverアイコンからパスワード関連のメニューを使用できるかどうか
Citrix Receiver	Single Sign-On Plug-in	Citrix Receiver	Single Sign-On Plug-in		

うかにかかわらず）、ユーザーデバイスのWindows通知領域には接続先のXenAppサーバー（以前のバージョンのSingle Sign-On Plug-inがインストールされている）と同じ数のSingle Sign-Onアイコンが表示されます。

管理

Sep 30, 2015

管理者は、ユーザーがSingle Sign-Onに登録するパスワードに特定の規則を適用できます。これらの規則はパスワードポリシーとしてグループ化され、管理者はそのポリシーをすべてのユーザーに適用したり、特定のアプリケーショングループに適用したりできます。

注：Citrix XenAppのポリシー機能を使用すると、特定の条件に合致する接続でのみSingle Sign-Onが有効になるように構成できます。Single Sign-Onのパスワードポリシーは、XenAppのポリシーとは異なります。
Single Sign-Onには、デフォルトとドメインという2つの標準パスワードポリシーが用意されています。これらのポリシーは、必要に応じてそのまま使用したり、複製したり、変更したりできます。デフォルトポリシーおよびドメインポリシーを削除することはできません。

ユーザー側の［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）では、管理者が定義していないアプリケーション用のログオン情報をユーザーが登録できます。これらのアプリケーションには、デフォルトのポリシーが適用されます。アプリケーショングループをドメインパスワード共有グループとして設定するには、そのアプリケーショングループにドメインポリシーを適用します。

ユーザーがログオンマネージャーで追加するアプリケーションには、デフォルトのパスワードポリシーが適用されます。そのため、デフォルトのポリシーに準拠するパスワードが、アプリケーションに組み込まれている標準的なポリシーにより拒否されないようにする必要があります。

パスワードポリシーはいくつでも作成できます。たとえば、ドメインパスワード共有グループにドメインポリシーを適用して、ほかの個々のアプリケーショングループにはそれぞれ異なるパスワードポリシーを適用できます。パスワードポリシーには、以下の特長があります。

- アプリケーションのパスワードの変更を自動化できる。
- 複雑なパスワードを作成したり、特定のアプリケーションでユーザーに表示されないパスワードを使用したりして、セキュリティを強化できる。
- アプリケーション側でパスワードの有効期限が設定されていない場合でも、パスワードの有効期限を設定できる。
- 有効期限が切れたパスワードをユーザーが続けて使用できないように設定できる。

パスワード共有グループ

製品スイートに含まれるアプリケーションなど、複数のアプリケーションで同じパスワードが使用される場合があります。これはパスワード共有と呼ばれ、複数のアプリケーションに同一の認証機関が使用されます。

パスワード以外のログオン情報（ユーザー名やそのほかのカスタムフィールド用の情報など）がアプリケーションごとに異なっても、同じパスワードを使用することができます。この場合、アプリケーショングループをパスワード共有グループとして設定すると、そのグループのすべてのアプリケーションを単一のパスワードで管理できるようになります。ユーザーまたはSingle Sign-On Plug-inが、任意のアプリケーションでパスワードを変更した場合、同じグループに属するすべてのアプリケーションのパスワードにその変更が反映されます。

ドメインパスワード共有グループ

ドメインパスワード共有グループでは、そのほかのパスワード共有グループとは異なり、ユーザーのドメインパスワードがすべてのアプリケーションのマスターパスワードとして使用されます。ユーザーがドメイン用のパスワードを変更すると、ドメインパスワード共有グループに属するすべてのアプリケーションのパスワードにその変更が反映されます。ただし、ドメインパスワード共有グループに属する特定のアプリケーションのパスワードだけを変更するには、管理者がそのアプリケーションをドメインパスワード共有グループから削除する必要があります。

パスワードポリシーの動作

パスワードポリシーは、ユーザーが設定したパスワードおよびSingle Sign-Onにより自動生成されたパスワードの両方に適用されます。

以下の場合、パスワードポリシーは適用されません。

- ユーザーがSingle Sign-Onを初めて使用するとき（初回起動時設定）
- ユーザーが［パスワード管理］ダイアログボックスでパスワードを編集するとき
- 管理者がアプリケーション定義を作成するとき

また、Single Sign-Onの導入以前からユーザーにより使用されていたパスワードにも、パスワードポリシーは適用されません。このため、パスワードポリシーの導入により、以前から使用していたアプリケーションにアクセスできなくなることはありません。

Single Sign-Onがアプリケーションを識別できるようにする

Sep 30, 2015

Single Sign-Onでは、アプリケーション定義に設定されている条件に基づいてアプリケーションを識別し、ログオン処理を行います。

アプリケーション定義には、フォーム定義が含まれています。Single Sign-On Plug-inは、アプリケーションの起動時にこれらのフォーム定義に基づいてアプリケーションを分析し、次のような処理が必要かどうかを判断します。

- ログオン要求に対してログオン情報を送信する。
- ログオン情報の変更用のインターフェイスとネゴシエートする。
- ログオン情報の確認用のインターフェイスを処理する。

アプリケーション定義は、フォーム定義と呼ばれる、特定のログオン情報用フォームの認識およびアクションの特性のセットと、設定に含まれるすべてのフォームに適用される複数の設定オプションで構成されます。

アプリケーションによりログオン処理が要求されると、Single Sign-On Plug-inはフォーム定義の内容に基づいたアクションを実行します。

アプリケーション定義には、1つのアプリケーションに関連する、すべてのログオン情報用フォームの設定が定義されます。

多くのアプリケーションでは、ログオン情報の管理に2つのフォーム（ログオン用およびパスワード変更用）だけを使用しますが、必要に応じてほかのフォームをアプリケーション定義に追加して、使用することができます。

Single Sign-Onは、Windowsベース、Webベース、ターミナルエミュレーターベースのさまざまなアプリケーションをサポートします。JavaアプリケーションやSAPソリューション、またはメインフレーム、AS/400システム、UNIXサーバー上のアプリケーションにも使用できます。

テンプレートが用意されていないアプリケーションの定義を新規に作成するには、アプリケーション定義ウィザードを使用して、シングルサインオンに必要な各フォームを認識するための情報を追加します。各フォームの情報は、フォーム定義ウィザードの手順に従って追加します。このウィザードでは、Windowsベース、Webベース、ターミナルエミュレーターベースのさまざまなアプリケーションがサポートされます。

また、Single Sign-Onには、アプリケーションの検出とアクションの実行を外部プロセスを使用して行う機能があります。この機能は、Single Sign-On Plug-inによるアプリケーション検出とアクションの送信時に、外部処理へのアクセスを提供します。これにより、開発者がフォームに関連付けられているアプリケーション検出とログオン情報送信タスクを拡張できるようになります。

これらの機能により、柔軟性と順応性を備えたアプリケーション定義を作成する環境が提供されます。Single Sign-On管理者は、重要なアプリケーションへの安全で柔軟性のあるシングルサインオンアクセスを、ユーザーコミュニティに提供できます。

注意：Single Sign-Onの機能を正しく使用するには、この製品の各コンポーネントが動作するコンピューターの操作が安全に行われていることが不可欠です。ユーザーのコンピューターがウィルスなどの悪意のあるコードに感染すると、Single Sign-Onによるセキュリティが損なわれる場合があります。このような問題を避けるため、標準的なセキュリティガイドラインに基づいて、組織のコンピューティング環境のセキュリティを維持することをお勧めします。

アプリケーションテンプレート

アプリケーションテンプレートとは、異なるSingle Sign-On環境でアプリケーション定義を共有するために使用するXMLファ

イルです。管理者は、これらのテンプレートを簡単にアプリケーション定義に変換できます。変換時に必要な情報は、URLまたは実行可能ファイル名、パスワードの有効期限、および詳細な検出の設定だけです。

アプリケーションテンプレートは、Single Sign-On管理コンソール（Citrix AppCenterの［Single Sign-On］ノード）またはアプリケーション定義ツールを使用してインストールします。どちらのツールにも、一般的なWindowsアプリケーションおよびWebアプリケーションのアプリケーションテンプレートが組み込まれています。

重要：Active Directory形式の中央ストアを使用する環境でWindows Server 2008、Windows Server 2008 R2、Windows Vista、またはWindows 7上のアプリケーション定義ツールを実行する場合、このツールの整合性レベルが「高」である必要があります。このため、ローカルシステムおよびドメインの管理者であるアカウントか、中央ストアのActive Directoryオブジェクトに対する書き込み権限を持つアカウントを使用する必要があります。これらのアカウントでシステムにログオンしてアプリケーション定義ツールを起動するか、アプリケーション定義ツール起動時のユーザーアカウント制御のプロンプトに対してこれらの資格情報を入力します。これにより、このツールの整合性レベルが「高」になり、Active Directory形式の中央ストアにデータを書き込めるようになります。
必要なアプリケーションテンプレートが見つからない場合は、Single Sign-On管理コンソール（Citrix AppCenterの［Single Sign-On］ノード）またはアプリケーション定義ツールを使用してアプリケーション定義を作成できます。

アプリケーションとログオン情報管理イベントの識別方法

Sep 27, 2015

アプリケーションのユーザーインターフェイスには、そのアプリケーションで発生するログオン情報関連のイベントの処理に必要なさまざまなフォームが含まれています。

たとえば、ログオン情報を入力するためのフォーム、パスワードを変更するためのフォーム、パスワードが変更されたことを確認するフォームなどがあります。

アプリケーションの種類（Windows、Web、ターミナルエミュレーター）に応じて、Single Sign-Onはアプリケーション定義に指定されている識別条件に従ってフォームを識別し応答します。識別条件の例としては、アプリケーションの種類、ウィンドウタイトル、実行可能ファイル名などがあります。

Single Sign-On Plug-inがアプリケーションとそのフォームを検出すると、アプリケーション定義の内容に従って、ログオン情報の入力や登録をユーザーに要求したり、登録済みのログオン情報を自動入力したり、ログオン情報の更新をユーザーに促したりします。

アプリケーション定義は、AppCenterまたはアプリケーション定義ツールを使用して作成します。

1つのアプリケーション定義で、1つのアプリケーションで発生する、次のログオン情報管理イベントすべてに対応できます。

- ユーザーの認証
- ログオン情報の変更
- ログオン情報変更の確認

アプリケーション定義は、次の3種類に分類されます。

- Windowsアプリケーション（JavaアプリケーションとSAP LogonPadも含む）
- Webアプリケーション（Javaアプレットも含む）
- HLLAPI準拠のターミナルエミュレーターベースのアプリケーション

アプリケーション定義は、次の項目から構成されます。

- 定義に含まれるすべてのフォームに適用されるアプリケーション特性。アプリケーション定義ウィザードを使用して定義します。
- アプリケーションで発生するさまざまなログオン情報管理イベントを認識するために使用される、フォーム固有のデータ。これらのデータは、フォーム定義ウィザードを使用して定義します。フォーム定義ウィザードは、アプリケーション定義ウィザード内で起動します。

どの種類のアプリケーションでも、アプリケーション特性には類似の設定情報が含まれますが、アプリケーション定義に含まれるフォーム固有のデータは、定義するアプリケーションの種類によって大きく異なります。

アプリケーション定義を作成するには、アプリケーション定義を作成するコンピューターからそのアプリケーションにアクセスできる必要があります。オペレーティングシステムによっては一部のアプリケーション署名が異なることがあるため、組織内のすべてのオペレーティングシステム環境でアプリケーション定義をテストする必要があります。

アプリケーション定義を作成して配布した後に変更やアップグレードが行われた場合は、アプリケーション定義の変更を必要とするような変更がアプリケーション署名にないことをテストして確認します。

重要：Windows Server 2008、Windows Server 2008 R2、Windows Vista、およびWindows 7では、セキュリティ機能によりデフォルトでユーザーインターフェイス特権の分離（UIPI：User Interface Privilege Isolation）が有効になっています。この

UIPI機能により、アプリケーションが整合性レベルの高いほかのアプリケーションにメッセージを送ることが阻止されます。このため、デフォルトで整合性レベル「中」が割り当てられているSingle Sign-On Plug-inで、整合性レベル「高」のアプリケーションを認識したりログオン情報を送信したりすることができません。これは、これらのオペレーティングシステムやSingle Sign-Onのセキュリティ上の仕様であり、このデフォルトの動作を変更することはお勧めできません。

アプリケーションおよびフォーム定義ウィザードについて

Sep 27, 2015

すべてのアプリケーション定義は、アプリケーション定義ウィザードおよびこのウィザードから起動するフォーム定義ウィザードを使用して作成されます。

フォーム定義ウィザードでは、アプリケーション定義に含める各ログオン情報用フォームの特性を定義します。

アプリケーション定義ウィザードについて

アプリケーション定義ウィザードを起動するには、管理コンソールで［アプリケーション定義］ノードを選択し、［操作］メニューから［アプリケーション定義の作成］を選択します。

アプリケーション定義ウィザードでは、アプリケーションの種類（Windows、Web、またはターミナルエミュレーターベース）に応じて必要な情報が収集されます。

収集データ	Windows	Web	ターミナルエミュレーター
アプリケーションの識別	○	○	○
フォームの管理	○	○	○
カスタムフィールドの名前	○	○	○
アイコンの指定	○		
詳細な検出設定	○	○	○
パスワードの有効期限の構成	○	○	○
設定の確認	○	○	○

アプリケーション定義ウィザードでのフォーム管理

ほとんどのアプリケーションには、ログオン用とパスワードの変更用に個別のフォームがあります。また、パスワードが正常に変更されたことを知らせる、個別のフォームを備えているアプリケーションもあります。

［フォームの管理］ページでは、アプリケーション定義にフォームを追加します。このページでは、定義済みのフォームを編集したり削除したりすることもできます。

［追加］をクリックすると、フォーム定義ウィザードが起動して1つのフォームのデータが収集されます。アプリケーション定義にフォームを追加するたびに、フォーム定義ウィザードを使用します。

カスタムフィールドの名前

Single Sign-Onでは、ユーザー名とパスワードを入力するフィールドが、すべてのログオン情報用フォームに必要な標準情報として扱われます。一部のアプリケーションでは、ユーザー認証に必要なログオン情報として、データベース名、ドメイン名、システム名などのほかの情報も要求されます。

フォーム定義ウィザードでは、カスタムフィールドを2つまで追加できます。フォームの作成時にカスタムフィールドを定義する場合は、フィールドの内容を［カスタムフィールドの名前］ページで定義します。

カスタムフィールド名のアクセスキーを作成するには、フィールド名の中のアクセスキーとして指定する文字の直前に、アンパサンド（&）を挿入します。アクセスキーが指定されていない場合は、Single Sign-Onによって動的に番号が割り当てられます。定義されたカスタムフィールドの数に応じて、ボタン上に（1）または（2）と表示されます。

Windowsアプリケーションのアイコンの指定

ユーザーの［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）には、アプリケーションの種類（Windows、Web、またはターミナルエミュレーターベース）に応じて異なるアイコンが表示されます。ただし、Windowsアプリケーションの場合は、ユーザーが特定のアプリケーションを見つけやすいように、［アイコンの指定］ページでカスタムアイコンを定義することができます。カスタムアイコンを使用する場合は、そのアプリケーションと同じ場所にアイコンファイルを格納する必要があります。

ログオンループの回避

［詳細な検出設定］ページのオプションは、ログオン情報の送信ループとパスワードの変更ループを避けるために使用します。

ログオフ後にログオン用のフォームが再表示されるWebアプリケーションでは、ユーザーのログオン情報が自動的に再送信されてしまう場合があります。このようなWebアプリケーションに対しては、［初回のログオンのみを自動処理する］チェックボックスをオンにして、ログオン情報の送信ループを回避できます。

このように定義されたアプリケーションでは、初回だけSingle Sign-On Plug-inがログオンフォームにログオン情報を自動的に送信します。ユーザーがログオフしログオン画面が再表示されると、別のウィンドウが約10秒間表示されます。ユーザーには、次の3つ選択肢があります。

- ウィンドウを閉じる。ログオン情報は送信されません。
- ウィンドウを無視する。ログオン情報は送信されません。
- リンクをクリックする。ログオン情報が送信されます。

アプリケーションを閉じるとセッションが終了し、次にアプリケーションを起動したときにはSingle Sign-On Plug-inによりログオン情報が送信されます。

パスワード変更時のループを回避するには、［初回のパスワード変更のみを自動処理する］チェックボックスをオンにします。これにより、そのアプリケーションにアクセスするときにユーザーがパスワードの変更を繰り返し行うと、パスワードの変更を続行するかどうかを確認するメッセージが表示されます。

パスワードの有効期限の構成

［パスワードの有効期限の設定］ページでは、以下のオプションを設定できます。

- パスワードの有効期限が切れたときにスクリプトを実行する
- Citrix Single Sign-Onの有効期限警告機能を使用する

組織のセキュリティポリシーに応じて、スクリプトを使用してパスワードの変更を促すメッセージをユーザーに定期的に表示したり、パスワードを自動的に変更したり、それらを組み合わせたりできます。アプリケーション定義に関連付けられているパスワードの有効期限が切れたときにスクリプトを実行するには、［パスワードの有効期限が切れたときにスクリプトを実行する］チェックボックスをオンにし、実行するスクリプトを指定します。ただし、すべてのユーザーがそのスクリプトにアクセスできる必要があります。UNC（Universal Naming Convention）パスは使用できません。

通常、これらのスクリプトでは、コマンドラインでパスワード変更用のパラメーターを使用して、適切なアプリケーションを起動します。

また、［Citrix Single Sign-Onの有効期限警告機能を使用する］チェックボックスをオンにすると、アプリケーションに関連付けられているパスワードポリシーによってパスワードの有効期限が切れたことが示されたときに、Single Sign-Onに組み込まれている有効期限の警告が表示されます。この設定によって、期限が切れたことを知らせるメッセージが繰り返し表示されますが、ユーザーがパスワードの変更を強制されることはありません。

フォーム定義ウィザードについて

フォーム定義ウィザードは、以下の状況で使用します。

- アプリケーション定義ウィザード内でフォームを定義するとき。
- 既存のフォームを定義するとき。
- 既存のアプリケーション定義にフォームを追加するとき。

フォーム定義ウィザードを使用して定義できる、標準的なログオン情報用フォームの種類は次のとおりです。

- ログオンフォーム
  アプリケーションのログオン用のインターフェイスを識別し、そのアプリケーションにアクセスするために必要なアクションを定義するために使用します。

- パスワード変更フォーム
  アプリケーションのパスワード変更用のインターフェイスを識別し、そのアプリケーションのユーザーパスワードを変更するために必要なアクションを定義するために使用します。

- パスワード変更の成功フォーム
  アプリケーションのパスワード変更用のインターフェイスを識別し、パスワードが変更されたことを確認するために必要なアクションを定義するために使用します。

- パスワード変更の失敗フォーム
  アプリケーションのパスワード変更失敗用のインターフェイスを識別し、パスワードの変更操作が失敗したときに行うアクションを定義するために使用します。

Single Sign-On Plug-in（Password Managerエージェント）Version 4.0および4.1は、パスワード変更の成功フォームおよび失敗フォームをサポートしていません。このため、これらのフォーム定義を含むアプリケーション定義は無視されます。

各フォームについて収集されるデータに基づいて、次の2つの処理が行われます。

- アプリケーション固有のフォームが起動されたらフォームを識別する。
- フォームに関連付けられている適切なログオン情報処理アクションを実行する。

フォーム定義ウィザードを起動するには、アプリケーション定義ウィザードの［フォームの管理］ページで［追加］をクリックします。

フォーム定義ウィザードでは、各種類（Windows、Web、ターミナルエミュレーター）のアプリケーションについて次のフォーム情報が収集されます。

収集データ	Windows	Web	ターミナルエミュレーター
フォーム名	○	○	○

収集データ	Windows	Web	ターミナルエミュレーター
フォームの識別	○	○	○
フォームアクションの定義	○	○	
フィールドの検出規則の設定			○
そのほかの設定の構成	○	○	○
設定の確認	○	○	○

Windowsアプリケーションの定義

Sep 27, 2015

Windowsアプリケーション定義は、Windowsアプリケーション、Javaアプリケーション、そしてSAP LogonPadから起動されるアプリケーションの識別に使用します。

アプリケーション定義の作成では、通常、実行可能ファイル（拡張子が.exeのファイル）で起動されるアプリケーションがWindowsアプリケーションとして分類されます。

Windowsアプリケーションの定義に必要な情報を円滑かつ簡単に収集するには、管理コンソールまたはアプリケーション定義ツールからフォーム定義ウィザードを使用するときに、対象となるアプリケーションを起動しておき、ログオン情報管理イベント（ユーザーログオン、パスワード変更、パスワード変更の成功、およびパスワード変更の失敗）を要求するフォームを開きます。ウィザードの画面に、アプリケーションの該当部分を検索および識別する手順が表示されます。

フォームの識別

Windowsアプリケーション定義を作成するときは、Single Sign-On Plug-inが処理対象のフォームを識別するための条件を［フォームの識別］ページで指定します。

識別情報には、ウィンドウタイトルと実行可能ファイル名が含まれます。Single Sign-On Plug-inは、実行可能ファイル名を検出すると、アプリケーションによって表示される、ここで定義するウィンドウタイトルを監視します。

ウィンドウタイトルを検出すると、Single Sign-On Plug-inはフォームに対して定義されているアクションを実行します。

フォームを識別するには

1. 対象のWindowsアプリケーションを起動して、ログオンフォーム、パスワードの変更フォーム、パスワード変更の成功フォーム、またはパスワード変更の失敗フォームを開きます。
2. フォーム定義ウィザードの［フォームの識別］ページで、［選択］をクリックします。
3. 対象のアプリケーションが強調表示されない場合は、［ウィンドウセレクター］でそのアプリケーションを選択します。

動的なウィンドウタイトルの識別

日付やセッション識別子など、動的に変更されるタイトルが表示されるウィンドウでは、［フォームの識別］ページの［このフォームのウィンドウタイトル］のタイトルを編集して、動的に変更される部分にワイルドカード文字を使用します。

Wildcard	説明
?	ウィンドウタイトルの1文字が動的に変わる場合に使用します。
*	ウィンドウタイトルの1つまたは複数の文字が動的に変わる場合に使用します。ウィンドウタイトルがない場合は、このワイルドカードではなく、NULLを使用します。
NULL	ウィンドウタイトルがない場合に使用します。大文字で入力します。

実行可能ファイルのフルパスの指定

［実行可能ファイルの名前とパス］ボックスには、実行可能ファイル名とフルパス情報が表示されます。

ここで指定したパスから起動したプログラムのインスタンスだけが対象アプリケーションとして認識されます。1つまたは複

数のフルパスが識別されたとき、Single Sign-On Plug-inは、指定されたパスから実行され、そのほかのフォーム識別条件をすべて満たしているプログラムにだけログオン情報を送信します。

実行可能ファイルのフルパスを指定するには、［ウィンドウセレクター］で［実行可能ファイルのフルパスを使用する］チェックボックスをオンにします。

フルパスが指定されていない実行可能ファイルは、［フルパス］列に「指定なし」と表示されます。この場合、Single Sign-On Plug-inは、ほかのフォーム識別条件と一致するプログラムにログオン情報を送信します。

セミコロン（;）で区切って複数のパスを入力したり、絶対パスや環境変数を使用することもできます。

注：実行可能ファイルのフルパスが指定されたアプリケーション定義を使用してアプリケーション定義テンプレートを作成できますが、フルパスの情報はテンプレートから削除されます。

フォームアクションの定義

フォーム定義ウィザードの［フォームアクションの定義］ページでは、そのフォームにログオン情報を送信するためにSingle Sign-On Plug-inにより実行されるアクションを定義します。

ページの上部には、フォームの種類に応じて、次の表に示すログオン情報が表示されます。

	ログオン フォーム	**パスワード変更 フォーム**	**パスワード変更の成功 フォーム**	**パスワード変更の失敗 フォーム**
ユーザー名/ID	○	○	○	○
Password	○		○	○
現在のパスワード		○		
新しいパスワード		○		
パスワードの確認入力		○		
カスタムフィールド1	○		○	○
カスタムフィールド2	○		○	○
OK	○	○	○	○

ページ下部には、定義済みのアクションシーケンスが表示されます。

この［フォームアクションの定義］ページでは、認識されたフォームに必要なログオン情報を送信するときに、Single Sign-On Plug-inが実行する処理について定義します。

フォームアクションを定義するには

ほとんどのWindowsアプリケーションでは、以下の手順でフォームアクションを定義できます。

1. 特定のログオン情報の右側の［設定/変更］のハイパーリンクをクリックします。 各ログオン情報の入力フィールドを特定

するための［コントロールの文字列の設定］ダイアログボックスが開きます。
2. ログオン情報の入力フィールドと送信ボタンを選択します。 指定したログオン情報用のフィールドや送信ボタンを簡単に見分けられるように、対応するコントロールがアプリケーション上で強調表示されます。
3. フォームで必要なすべてのログオン情報フィールドとフォームを送信するためのボタンについて、この操作を繰り返します。
   フォームの中には、ドメインやそのほかのログオン情報の入力が必要なものもあります。そのような場合に備えて、2つのカスタムフィールドが用意されています。これらのフィールドには、特別なログオン情報を割り当てます。フィールドの名前は、フォームを定義した後にアプリケーション定義ウィザードの［カスタムフィールドの名前］ページで定義します。

   注：［フォームアクションの定義］ページ上部に表示されるすべてのログオン情報用のフィールドを構成する必要はありません。

ウィンドウの識別

［ウィンドウの識別］ページでは、定義したウィンドウタイトルと実行可能ファイル名だけを使用すると複数のウィンドウが識別されてしまう場合に、特定のフォームを識別できるウィンドウコントロールIDを定義します。この設定は、ウィンドウコントロールIDによって複数のフォームから特定のフォームを識別できる場合にだけ役立ちます。

［ウィンドウのコントロールIDによるマッチを有効にする］チェックボックスをオンにして、そのフォームのウィンドウをほかのフォームから区別するためのコントロールIDを入力します。

フォーム識別拡張機能

フォーム識別拡張機能は、アプリケーション定義の拡張機能の一部です。これにより、Single Sign-Onから外部プロセスを呼び出して、ログオン情報管理イベントを認識してログオン情報を送信できるようにします。

通常は、管理コンソールとアプリケーション定義ツールを使用してアプリケーション定義を作成できますが、一部のアプリケーションではアプリケーションの検出、ログオン情報の送信などを行うために別の方法が必要な場合があります。

このようなアプリケーションに対応するために、アプリケーション定義拡張機能を使用して、アプリケーションのコントロールとそのデータ入力メカニズムを抽出できます。

拡張機能は、サードパーティの開発者によって開発され、実装方法はアプリケーションごとに異なります。したがって、設定手順もアプリケーションごとに異なります。

通常、Single Sign-On管理者は、これらの拡張機能の開発には携わりません。拡張機能は、サードパーティの開発者によって作成されます。拡張機能の設定は拡張機能ごとに異なるため、多くの場合は拡張機能に設定手順が付属しています。

アクションエディターによるアクションシーケンスの定義（Windowsアプリケーション）

［フォームアクションの定義］ページでは、定義するログオン情報用フォームにログオン情報を送信するための処理を定義します。

多くのWindowsアプリケーションでは、フォーム定義ウィザードで収集される基本的な情報だけで正しくフォームが識別されます。ただし、ログオン情報の管理タスクを完了するために、そのほかの情報、手順、特別なキー、アクションなどを要求するフォームもあります。このようなフォームの場合は、［フォームアクションの定義］ページで［アクションエディター］をクリックします。［アクションエディター］ダイアログボックスが開きます。

［アクションエディター］ダイアログボックスは、次の項目で構成されています。

- アクションの選択
  アクションシーケンスに追加できるすべてのアクションが表示されます。

- アクションの構成
  アクションシーケンスに追加するアクションのオプションを定義します。

- アクションシーケンス
  特定のログオン情報用フォームを処理するために実行するアクションのシーケンスが表示されます。

［アクションエディター］ダイアログボックスの下には、［詳細設定］ダイアログボックスを開く［詳細設定］ボタンがあります。［詳細設定］ダイアログボックスには、次の2つのオプションがあります。

- コントロールの重ね順で指定する
  このチェックボックスをオンにすると、コントロールのIDではなく、重ね順（Zオーダー）が使用されます。コントロールの重ね順は定義プロセス時にSingle Sign-On Plug-inによって独立して列挙されるため、アプリケーションによって定義されるコントロールIDとは無関係にコントロールを識別できます。

  動的にコントロールIDが生成される.NETアプリケーションまたはコントロールIDが重複するアプリケーションに対して、この機能を使用することを検討してください。

- 待機時間
  ここでは、Single Sign-On Plug-inがアクションシーケンスを開始するまでの待機時間を定義できます。待機時間は、［待機時間の挿入］アクションを使用してアクションシーケンスを開始することでも構成できます。このアクションは、［アクションエディター］ダイアログボックスの［アクションの選択］で選択します。

  ただし、キー送信処理として定義される［待機時間の挿入］アクションを使用する場合と異なり、［詳細設定］ダイアログボックスで定義する待機時間はSingle Sign-On（Password Manager）Version 4.5、4.6、4.6 with Service Pack 1、および4.8のPlug-inでしか使用できません。

アクションシーケンスを定義するには

1. ［アクションの選択］の一覧からアクションを選択します。
2. ［アクションの設定］で、必要なアクションを構成します。 構成が終わったら、［挿入］をクリックします。 構成したアクションが［アクションシーケンス］に追加されます。
3. ログオン情報用フォームで実行するすべてのアクションについて、手順1.～2.を繰り返します。
4. アクションの実行順を変更するには、［アクションシーケンス］の一覧でアクションを選択して、［上へ移動］または［下へ移動］をクリックします。
5. アクションシーケンスを並べ替えたら、［OK］をクリックします。 ［フォームアクションの定義］ページの［アクションシーケンス］に、定義したアクションシーケンスが表示されます。
6. ［次へ］をクリックして［そのほかの設定］ページに進み、引き続きフォームの定義を行います。 Single Sign-On（Password Manager）4.5、4.6、4.6 with Service Pack 1、4.8、および5.0のPlug-inでしか使用できないシーケンスを定義した場合は、そのまま続行するか、戻って設定を変更するかを確認するメッセージが表示されます。

Windowsアプリケーションの定義における注意事項

Windowsアプリケーションの定義を作成する場合、次の点に注意してください。

- アプリケーションテンプレートを使用すると、アプリケーション定義を簡単に作成できます。
- アプリケーション定義は、Single Sign-On Plug-inでテストをしてからユーザーに提供してください。
- アプリケーション定義の多くは基本的な情報を入力するだけで動作します。アプリケーション定義がテスト環境で意図したとおりに機能しない場合は、動的なウィンドウタイトル、コントロールID、またはアプリケーションに組み込まれているそのほかの特殊な識別子やアクションなどの固有機能が原因である場合があります。
- アプリケーション定義をテスト環境から実稼働環境にエクスポートするには、Citrix AppCenterのコンソールツリーで

［Single Sign-On］ノードを選択し、操作タスクの［管理データのエクスポート］をクリックします。

- アプリケーション定義レベルで設定した設定は、アプリケーション定義に含まれるすべてのフォームに適用されます。
- アプリケーション定義レベルで設定したオプションの一部は、フォームレベルで設定したオプションにより無効になることがあります。たとえば、1つのアプリケーション定義に3つのフォーム定義を追加して、アプリケーション定義レベルでログオン情報の自動送信機能を有効にします。これにより、これら3つのフォームのどれかが開いたときに、Single Sign-On Plug-inが各フィールドにユーザーのログオン情報を入力して、それを自動的にアプリケーション側に送信します。たし、フォーム定義レベルで特定のフォームの自動送信機能を無効にすると、アプリケーション定義レベルの自動送信設定よりもフォーム定義レベルの設定が優先されるため、そのフォームのログオン情報が自動送信されなくなります。この場合、ユーザーは選択したフォームの［送信］ボタンまたは［OK］ボタンを自分でクリックする必要があります。
- カスタムフィールド名のアクセスキーを作成するには、フィールド名の中のアクセスキーとして指定する文字の直前に、アンパサンド（&）を挿入します。
  アクセスキーが指定されていない場合は、Single Sign-Onによって動的に番号が割り当てられます。定義されたカスタムフィールドの数に応じて、ボタン上に（1）または（2）と表示されます。

  作成したフォームを必ずテストし、定義した名前がカスタムフィールド名に割り当てられている長さ以内であることを確認してください。

Windowsアプリケーションにリダイレクトする設定

WebフォームウィザードでWebアプリケーションのフォームが認識されない場合は、フォーム定義をリダイレクトして、Windowsアプリケーションのフォーム定義を使用する必要があります。

Webアプリケーションで、ActiveXコントロール、Flashベースのコントロール、一部のAjaxコントロールなど、非HTMLベースのコントロールを使用してログオン情報管理イベントが処理される場合に、フォームが認識されないことがあります。

そのような場合には、フォーム定義ウィザードの［フォーム名］ページで［Windowsアプリケーションにリダイレクトする］をクリックします。［次へ］をクリックして、フォーム定義ウィザードの残りのページを終了し、［設定の確認］ページで［完了］をクリックします。

次に、Windowsアプリケーションの定義とキー送信処理を使用して、フォームの認識特性とログオン用アクションを定義する必要があります。

詳細マッチ設定によるWindowsフォームの識別

Sep 27, 2015

ほとんどのWindowsアプリケーションの場合、フォーム定義ウィザードの [フォームの識別] ページを使って、対象となるフォームを指定できます。ただし、一部のログオン情報用フォームでは、より詳細な識別条件を定義する必要があります。これを行うには、フォーム定義ウィザードの［フォームの識別］ページで［詳細マッチ設定］をクリックします。

［詳細マッチ設定］ダイアログボックスでは、以下の5つのWindows識別オプションを設定できます。

- ウィンドウクラスの情報
- コントロールマッチ
- SAPセッション情報
- ウィンドウの識別
- フォーム識別拡張機能

クラス情報による無視するフォームの指定

［ウィンドウクラスの情報］ページでは、Single Sign-Onで無視するフォームを定義します。［このウィンドウクラスを無視する］ボックスに無視するウィンドウクラスを入力すると、そのクラス情報を持つフォームが開いてもSingle Sign-Onは反応しません。

.NETアプリケーションまたはデフォルトの32770のウィンドウクラスを使用するアプリケーションには、このマッチング方法を使用しないでください。

この設定は、ウィンドウクラスが動的な場合に有効です。ウィンドウクラスが動的に変化する場合は、ワイルドカード文字を使用してウィンドウクラスを指定します。

Wildcard	説明
?	ウィンドウクラスの1文字が動的に変わる場合に使用します。
*	ウィンドウクラスの1つまたは複数の文字が動的に変わる場合に使用します。ウィンドウクラスがない場合は、 このワイルドカードではなく、NULLを使用します。
NULL	ウィンドウクラスがない場合に使用します。大文字で入力します。

この設定は、多数のウィンドウクラスの中からウィンドウクラスを特定しなければならない、以下のような場合に使用します。

- 指定したウィンドウタイトルと実行可能ファイルに一致するウィンドウクラスが複数ある場合。これはウィンドウタイトルに動的データが含まれるためにワイルドカードを使用してタイトルを指定した場合によく起こります。
- 対象のフォームに固有のウィンドウクラスを関連付けて、ほかのすべてのフォームでは異なるウィンドウクラスを使用する必要がある場合。

ウィンドウクラスを識別するには

以下の手順を実行するには、フォーム識別ウィザードの [フォームの識別] ページを開きます。

1. ［詳細マッチ設定］をクリックして、ダイアログボックス左側で [ウィンドウクラスの情報] をクリックします。
2. ［選択］をクリックし、コンピューター上で既に起動しているアプリケーションの中から対象のアプリケーションを選択します。

注：目的のアプリケーションが［プログラムウィンドウ］の一覧に表示されない場合は、［隠しウィンドウを表示する］チェックボックスまたは［子ウィンドウを表示する］チェックボックスをオンにします。

コントロールマッチを使用して同一識別子のフォームを区別する

一部のアプリケーションでは、コントロールのラベルに動的情報が割り当てられています。その場合、複数のログオン情報用フォームで、同じウィンドウタイトル、実行可能ファイル、コントロールIDが使用されていても、アプリケーション固有のイベントに応じて、フォームの文字列ラベルやほかのプロパティが変化することがあります。

このような種類のフォームについては、コントロールマッチの設定オプションを使用してコントロールIDの固有のクラス、スタイル、または文字列値をマッチ条件として定義して、Single Sign-Onに実行させるアクションと関連付けます。

マッチ条件を定義するには

以下の手順を実行するには、フォーム識別ウィザードの［フォームの識別］ページを開きます。

1. ［詳細マッチ設定］をクリックして、ダイアログボックス左側で［コントロールマッチ］をクリックします。
2. ［マッチの追加］をクリックします。
   注：ここでは、定義するログオン情報用フォームを識別するために必要な最低限のコントロールマッチ条件を定義します。
3. ［マッチ条件の定義］ダイアログボックスで、［選択］をクリックします。
4. 定義するコントロールIDを右クリックします。
5. 選択したコントロールIDのフォームを識別するためのコントロールIDの特性（［クラス］、［スタイル］、または［文字列］）を選択します。
6. フォームの識別に使用する各コントロールIDについて、手順4.～5.を繰り返します。

複数のSAPセッション実行時のフォームの識別

古いバージョンのSAPには、標準のWindowsおよびWebアプリケーション定義を使用できます。ただし、複数のSAPシステムがSAP Logon Padなどの共通のSAP GUIユーザーログオンインターフェイスを使用するように定義されている場合には、［詳細マッチ設定］ダイアログボックスの［SAPセッション情報］ページでこれに対応するように設定します。

SAPセッション情報を使用するには、SAP管理者がサーバーでGUIスクリプトを有効にする必要があります。これにより、Single Sign-On管理コンソールおよびSingle Sign-On Plug-inが、SAP Logon Padに問い合わせを行い、特定のログオン情報用フォームを識別するために必要なシステムIDやサーバー名を判断できるようになります。

［SAPセッション情報］ページのオプションを使用すると、既存のSAPウィンドウから、そのウィンドウを識別するためのセッション情報を抽出できます。

SAPセッション情報を手作業で入力するには

必要な場合は、SAPセッションのシステムIDやサーバー名の情報を手作業で入力できます。どちらのフィールドにも正規表現を使用できます。正規表現を使用して、複数のサーバー名にマッチする条件を定義できます。

サーバーのDNS名およびNetBIOS名の両方にマッチする条件を定義することもできます。

次の正規表現形式を使用すると、DNS名およびNetBIOS名の両方にマッチする条件を定義できます。

```
^servername(\.domain\.com)?$
```

SAP GUIスクリプトメッセージを無効にするには

プログラムがSAP GUIを使用してSAP LogonPadに接続しようするときに、SAP GUIスクリプトメッセージが表示されること

あります。メッセージが表示されないようにするは、レジストリ設定を変更します。

キーはHKEY_CURRENT_USER\Software\SAP\SAPGUI Front\SAP Frontend Server\Security\WarnOnAttachで、種類はREG_DWORDです。このキーの値を0に設定すると、メッセージは表示されません。デフォルト値は1です。

Webアプリケーションの定義

Sep 27, 2015

Webアプリケーション定義は、Javaアプレットなど、Webベースのアプリケーションの識別に使用します。

アプリケーション定義の作成では、通常、Webブラウザー内で実行されるアプリケーションをWebアプリケーションとして分類します。Single Sign-Onでは、Internet Explorer Versions 6.0、7.0、8.0、および9.0上で動作するWebアプリケーションがサポートされます。

Webアプリケーションの定義の作成手順には、アプリケーションを実行してアプリケーション上のフィールドを指定することも含まれます。Webアプリケーションの定義に必要な情報を円滑かつ簡単に収集するには、管理コンソールまたはアプリケーション定義ツールからフォーム定義ウィザードを開いて、アプリケーションを起動し、ログオン情報管理イベント（ユーザーログオン、パスワード変更、パスワード変更の成功、パスワード変更の失敗）を要求するフォームを開きます。ウィザードの画面に、アプリケーションの該当部分を検索および識別する手順が表示されます。

フォーム名

フォーム定義ウィザードの［フォーム名］ページでは、次の操作を行います。

- 作成するフォームに名前を割り当てる。
- 作成するフォームの種類を指定する。
- 特別なアクションを指定する。

フォームに割り当てる名前は、アプリケーション定義ウィザードの［フォームの管理］ページに表示されます。定義するフォームの種類がわかるような名前を割り当てます。

フォーム定義ウィザードを使用して定義できる、ログオン情報処理の標準フォームの種類は次のとおりです。

- ログオンフォーム
  アプリケーションのログオン用のインターフェイスを識別し、そのアプリケーションにアクセスするために必要なアクションを定義するために使用します。

- パスワード変更フォーム
  アプリケーションのパスワード変更用のインターフェイスを識別し、そのアプリケーションのユーザーパスワードを変更するために必要なアクションを定義するために使用します。

- パスワード変更の成功フォーム
  アプリケーションのパスワード変更用のインターフェイスを識別し、パスワードが変更されたことを確認するために必要なアクションを定義するために使用します。

- パスワード変更の失敗フォーム
  アプリケーションのパスワード変更失敗用のインターフェイスを識別し、パスワードの変更操作が失敗したときに行うアクションを定義するために使用します。

Single Sign-On Plug-in（Password Managerエージェント）Version 4.0および4.1は、パスワード変更の成功フォームおよび失敗フォームをサポートしていません。このため、これらのフォーム定義を含むアプリケーション定義は無視されます。

［特殊操作］で、定義するフォームに対する特殊な処理を次の中から選択します。

- 特殊操作なし
  このオプションをクリックすると、通常のWebフォーム処理が行われます。

- Windowsアプリケーションにリダイレクトする
  Webフォームウィザードでwebアプリケーションのフォームが認識されない場合に、このオプションをクリックします。これは、Webアプリケーションで、ActiveXコントロール、Flashベースのコントロール、一部のAjaxコントロールなど、非HTMLベースのコントロールを使用してログオン情報管理イベントが処理される場合に起こります。

- 検出されても無視する
  このオプションをクリックすると、フォームは無視されます。

フォームの識別

Webアプリケーションに対するフォーム定義ウィザードの［フォームの識別］ページでは、Single Sign-On Plug-inがそのフォームを識別するために必要な情報を入力します。

Webアプリケーションは、定義するログオン情報用フォームのURLアドレスにより識別されます。

［選択］をクリックすると、［Webページセレクター］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では、フォームに関連付けるWebページを指定できます。

［Webページセレクター］ダイアログボックスを閉じると、［フォームの識別］ページに戻ります。指定したURLのマッチ条件を選択する次の2つのチェックボックスがあります。

- URLの完全マッチ
  このチェックボックスをオンにすると、指定したURLから開始されるWebアプリケーションのログオン情報管理イベントだけが認識されます。URLの中には、セッション管理識別子、アプリケーションパラメーター、またはインスタンスごとに変化する識別子などの動的データが含まれているものもあります。このような場合に完全マッチを使用すると、そのフォームが認識されなくなります。

- URLの大文字/小文字を区別する
  このチェックボックスをオンにすると、URLの大文字と小文字が区別されます。

フォームアクションの定義

フォーム定義ウィザードの［フォームアクションの定義］ページでは、そのフォームにログオン情報を送信するためにSingle Sign-On Plug-inにより実行されるアクションを定義します。

ページの上部には、フォームの種類に応じて、次の表に示すログオン情報が表示されます。

	ログオンフォーム	パスワード変更フォーム	パスワード変更の成功フォーム	パスワード変更の失敗フォーム
ユーザー名/ID	○	○	○	○
Password	○		○	○
現在のパスワード		○		
新しいパスワード		○		
パスワードの確認入力		○		
カスタムフィール	○		○	○

ド1 カスタムフィールド2	ログオンフォーム	パスワード変更フォーム	パスワード変更の成功フォーム	パスワード変更の失敗フォーム
OK	○	○	○	○

ページ下部には、定義済みのアクションシーケンスが表示されます。

この［フォームアクションの定義］ページでは、認識されたフォームに必要なログオン情報を送信するときに、Single Sign-On Plug-inが実行する処理について定義します。

多くのWebアプリケーションでは、次の手順に従うだけで設定が完了します。

1. 特定のログオン情報の右側の［設定/変更］のハイパーリンクをクリックします。各ログオン情報の入力フィールドを特定するための［フィールド文字列の設定］ダイアログボックスが開きます。ログオン情報用のフォームが既に開いている場合は、ダイアログボックスには選択したログオン情報または送信ボタン（［OK］ボタンなど）に対応するフィールドの種類が表示されます。
   アプリケーションのログオン情報用のフォームが開いていない場合は、アプリケーションを起動して目的のフォームを開いてから、［更新］を選択します。アプリケーションフォームを選択すると、このダイアログボックスには、選択したログオン情報に応じた種類のコントロールが表示されます。
2. ログオン情報の入力フィールドと送信ボタンを選択します。指定したログオン情報用のフィールドや送信ボタンを簡単に見分けられるように、対応するフィールドがアプリケーション上で強調表示されます。
3. フォームで必要なすべてのログオン情報フィールドとフォームを送信するためのボタンについて、この操作を繰り返します。
   フォームの中には、ドメインやそのほかのログオン情報の入力が必要なものもあります。そのような場合に備えて、2つのカスタムフィールドが用意されています。これらのフィールドには、特別なログオン情報を割り当てます。フィールドの名前は、フォームを定義した後にアプリケーション定義ウィザードの［カスタムフィールドの名前］ページで定義します。

   注：［フォームアクションの定義］ページ上部に表示されるすべてのログオン情報用のフィールドを構成する必要はありません。

多くのWebアプリケーションでは、特定のログオン情報の入力フィールドとフォーム送信用のボタンを指定することで定義付けのプロセスが完了し、次に進むことができます。

ただし、ログオン情報の管理タスクを完了するために、そのほかの情報、手順、特別なキー、アクションなどが必要なフォームもあります。このようなフォームの場合は、［アクションエディター］をクリックします。［アクションエディター］ダイアログボックスが開きます。

アクションエディターによるアクションシーケンスの定義（Webアプリケーション）

［フォームアクションの定義］ページでは、定義するログオン情報用フォームにログオン情報を送信するための処理を定義します。

多くのWebアプリケーションでは、フォーム定義ウィザードで収集される基本的な情報だけで正しくフォームが識別されます。ただし、ログオン情報の管理タスクを完了するために、そのほかの情報、手順、特別なキー、アクションなどを要求するフォームもあります。このようなフォームの場合は、［フォームアクションの定義］ページで［アクションエディター］を

クリックします。［アクションエディター］ダイアログボックスが開きます。

［Webアプリケーションアクションエディター］ダイアログボックスは、次の項目で構成されています。

- アクションの選択
  アクションシーケンスに追加できるすべてのアクションが表示されます。
- アクションの構成
  アクションシーケンスに追加するアクションのオプションを定義します。
- アクションシーケンス
  特定のログオン情報用フォームを処理するために実行するアクションのシーケンスが表示されます。

そのほかの設定の構成

フォーム定義ウィザードの［そのほかの設定］ページでは、送信ボタンをSingle Sign-On Plug-inが自動的に押すのか、またはユーザー自身が押すのかを指定します。

フォームを自動的に送信する場合は、［ログオン情報の自動送信を有効にする］チェックボックスをオンにします。

Webアプリケーションの［詳細設定］ダイアログボックス

Sep 27, 2015

一部のWebアプリケーションでは、動的URLが使用されます。その場合には、そのほかのフォーム定義条件（検出マッチ条件）を使用して、特定のログオン情報用フォームを識別する必要があります。

検出マッチ条件は、［マッチの詳細］ダイアログボックスで定義し、［詳細設定］ダイアログボックスに表示されます。［マッチの詳細］ダイアログボックスを開くには、フォーム定義ウィザードの［フォームの識別］ページで［詳細マッチ設定］をクリックして［詳細設定］ダイアログボックスを開き、［追加］をクリックします。

［マッチの詳細］ダイアログボックスのオプションを使用して、特定のフォームを識別する条件を定義します。この方法では、HTMLタグに設定されている特定の値により、対象となるフォームが識別されます。ここでは、そのフォームを識別するために必要な最低限のマッチ条件を定義します。

［検索］ボックスに、Webページを識別するためのWeb要素を入力します。目的の要素が見つからない場合は、［そのほかの設定］を展開して詳細を指定します。

［そのほかの設定］セクションでは、以下の項目を指定できます。

- タグ
  検索するHTMLタグを指定します。そのタグの特定のインスタンスがわかっている場合は、［対象を指定する］チェックボックスをオンにして、評価対象のインスタンスを指定します。特定のインスタンスを指定しない場合は、文書中のすべてのインスタンスが検証されます。ここでは、区切り記号を含めずに、タグだけを入力する必要があります（

  ではなくpなど）。基本的には検出対象のコンテンツに最も近いタグを選択します。

  注：［対象を指定する］チェックボックスの動作はWebブラウザーによって異なることがあるため、この機能は必要な場合にだけ使用し、使用するときは設定をテストしてください。
- 値の種類
  マッチ条件の種類を指定します。次のいずれかの条件を選択します。

値	説明
テキスト	HTMLコードに含まれる特定の文字列を検索する場合
HTML	指定タグ内に含まれる特定のコードを検索する場合
属性	HTMLコードの任意の属性（formタグのname属性など）

- マッチする値
  マッチする条件を定義するために使用します。厳密にマッチさせるには、［完全マッチ］チェックボックスをオンにします。この場合、指定されていない文字列がタグ要素に含まれていると、一致していないものとして評価されます。必要に応じて、区切り記号や引用符を含めて指定します。

  注：［完全マッチ］チェックボックスは、類似するマッチ条件のインスタンスが複数存在する場合にだけオンにします。
- 演算子
  そのフォームに定義するほかの検出マッチ条件との関係を定義するために使用します。次のオプションがあります。

オプション	説明
AND	この検出マッチ条件が、そのフォームを識別するために必要な複数の条件の1つである場合に選択します。このオプションを選択すると、その条件の評価結果と次の条件の評価結果が両方とも真の場合に、マッチとして認識されます。
または	この検出マッチ条件だけでフォームを識別できる場合に選択します。このオプションを選択すると、その条件の評価結果と次の条件の評価結果のうち、どちらかが真の場合にマッチとして認識されます。このオプションは、単一のマッチ定義に使用されます。
NOT	演算子に負論理を適用する場合に選択します。この演算子は、ページ上に存在してはならないマッチ条件を定義するために使用します。

ターミナルエミュレーターベースのアプリケーションの定義

Sep 27, 2015

ターミナルエミュレーターベースのアプリケーションの定義は、メインフレーム、AS/400、OS/390、UNIX、またはそのほかのホストベースセッションなど、ホストベースのアプリケーションの識別に使用します。Single Sign-Onには、HLLAPI（High-Level Language Application Programming Interface）を実装したターミナルエミュレーター、またはダイアログボックスを表示できるスクリプトが組み込まれたターミナルエミュレーターを経由して、ホストベースのアプリケーションへのシングルサインオンを可能にする機能が搭載されています。

ターミナルエミュレーターアプリケーションの定義に必要な情報の収集

ターミナルエミュレーターベースのアプリケーションの定義に必要な情報を円滑かつ簡単に収集するには、そのアプリケーションを起動しておきます。

ターミナルエミュレーターベースのアプリケーションの定義は、フォーム定義ウィザードを使用して作成します。このウィザードでは、アプリケーションのログオン、パスワード変更、パスワード変更の成功、またはパスワード変更の失敗用の画面に表示されるべき文字列（または表示されてはならない文字列）を指定します。

定義するログオン情報用フォームを開き、フォームにアクセスするために必要なユーザーアクションをすべて記録します。管理コンソールまたはアプリケーション定義ツールからフォーム定義ウィザードを実行するときに、各フォーム定義にこのアクションを入力する必要があります。

正しいログオン情報用フォームを指定したら、適切なログオン情報をアプリケーションに送信するためのデータ入力フィールドの位置を定義します。この定義では、アクションシーケンス、またはフィールドや画面を移動して文字列を入力するために必要なキー操作を指定します。

フォームの定義プロセス

Sep 27, 2015

Webアプリケーションのフォームの定義プロセスでは、フォームを識別するための情報とPassword Managerに処理させるアクション情報を収集します。これらの情報は、フォーム定義ウィザードの次のページで指定します。

- フォーム名
- フォームの識別
- そのほかの設定の構成
- 設定の確認

ウィザードの各ページで必要な操作を完了したら、[次へ]をクリックして先に進みます。各ページの[戻る]をクリックすると、先に構成したオプションを変更することができます。ただし、既に構成したオプションを変更すると、それ以降の設定も変更することになる場合があります。

フォーム名

フォーム定義ウィザードの[フォーム名]ページでは、次の操作を行います。

- 作成するフォームに名前を割り当てる。
- 作成するフォームの種類を指定する。

フォームに割り当てる名前は、アプリケーション定義ウィザードの[フォームの管理]ページに表示されます。定義するフォームの種類がわかるような名前を割り当てます。

フォーム定義ウィザードを使用して定義できる、ログオン情報処理の標準フォームの種類は次のとおりです。

- ログオンフォーム
  アプリケーションのログオン用のインターフェイスを識別し、そのアプリケーションにアクセスするために必要なアクションを定義するために使用します。

- パスワード変更フォーム
  アプリケーションのパスワード変更用のインターフェイスを識別し、そのアプリケーションのユーザーパスワードを変更するために必要なアクションを定義するために使用します。

- パスワード変更の成功フォーム
  アプリケーションのパスワード変更用のインターフェイスを識別し、パスワードが変更されたことを確認するために必要なアクションを定義するために使用します。

- パスワード変更の失敗フォーム
  アプリケーションのパスワード変更失敗用のインターフェイスを識別し、パスワードの変更操作が失敗したときに行うアクションを定義するために使用します。

Single Sign-On Plug-in（Password Managerエージェント）Version 4.0および4.1は、パスワード変更の成功フォームおよび失敗フォームをサポートしていません。このため、これらのフォーム定義を含むアプリケーション定義は無視されます。

使用しているエミュレーターでログオン画面またはパスワードの変更画面が複数表示される場合は、画面ごとにフォームを定義する必要があります。

フォームの識別

ターミナルエミュレーターベースのアプリケーションに対するフォーム定義ウィザードの[フォームの識別]ページでは、Single Sign-Onがそのフォームを識別するために必要な情報を入力します。

アプリケーションのフォームは、ターミナルエミュレーターアプリケーション画面の特定の行と列に表示される文字列を検索することにより識別されます。ここでは、フォームを識別するために必要な最低限の文字列のマッチ条件を定義します。

文字列のマッチ条件を追加するには

1. ターミナルエミュレーターベースのアプリケーションが起動していることを確認し、そのフォームを識別するための文字列を確定します。
2. フォームを識別するための文字列の一覧に新しい文字列を追加するには、フォーム識別ウィザードの[フォームの識別]ページで［追加］をクリックします。［文字列］ダイアログボックスが開きます。
3. ［文字列］ダイアログボックスの以下のボックスに必要な値を入力します。
   - 文字列
     そのフォームを識別するための文字列を入力します。
   - 行
     文字列の行番号を入力します。
   - 列
     文字列の列番号を入力します。

   注：アプリケーションを識別するとき、Single Sign-Onは完全に一致する文字列が指定された行と列にあるかどうかを調べます。指定の位置にある文字列が指定の文字列と一致しない場合、その画面は無視されます。
4. ［OK］をクリックします。［文字列］ダイアログボックスで指定した文字列が、［フォームの識別］ページの一覧に追加されます。

多くの場合、アプリケーションの起動を正確に認識するには、複数の文字列を定義する必要があります。文字列を追加する場合は、各文字列について、手順2.～4.を繰り返します。

フィールドの検出規則の設定

フォーム定義ウィザードの［フィールドの検出規則の設定］ページでは、そのフォームの処理に必要な位置情報とキー操作を指定します。

このページでは、処理するログオン情報用のフィールド、画面上でログオン情報が挿入される位置（行と列の座標）、次のログオン情報フィールドに移動したり送信アクションを実行したりするためのキー操作を定義します。

フィールドを追加するには

1. ［追加］をクリックします。［フィールドの定義］ダイアログボックスが開きます。
2. ［フィールドの定義］ダイアログボックスの次のボックスに必要な値を入力します。
   - フィールドの機能
     そのフィールドの機能をボックスの一覧から選択します。
   - 行
     文字列の行番号を入力します。
   - 列
     文字列の列番号を入力します。
   - 後入力のキー
     次のログオン情報フィールドに移動したり送信アクションを実行したりするためのキーコードを入力します。

   注：［仮想キーコード］をクリックすると、有効なキーコードについてのヘルプトピックが表示されます。
3. ［OK］をクリックします。定義したフィールドが、［フィールドの検出規則の設定］ページの［定義済みのフィールド］

の一覧に追加されます。

4. そのフォームに必要な各ログオン情報について、手順1.～3.を繰り返します。
5. ［フィールドの検出規則の設定］ページの［定義済みのフィールド］の一覧に追加したフィールドは、上から順に処理されます。 矢印ボタンを使用して、定義するフォームに合わせて順番を並べ替えます。

そのほかの設定の構成

フォーム定義ウィザードの［そのほかの設定］ページでは、定義するフォームの詳細設定オプションを選択できます。詳細設定では、次の設定を行います。

- フォーム処理の待機時間
- そのログオン情報用フォームにアクセスするために必要なキー操作
- 無視するフォームを識別するための文字列のマッチ条件

定義するログオン情報用フォームにそのほかの詳細設定が必要な場合は、［詳細設定］をクリックします。［詳細設定］ダイアログボックスが開きます。

ターミナルエミュレーターベースのアプリケーションの［詳細設定］ダイアログボックス

Sep 27, 2015

一部のターミナルエミュレーターベースのアプリケーションでは、正しいログオン情報用フォームを正確に識別するために、次の追加設定が必要な場合があります。

- アプリケーションの識別を試行する前に、アプリケーションを一定時間待機する。
- ログオン画面またはパスワード変更画面を表示するための一連のキー入力を処理する。
- 特定の文字列が表示される場合は画面の処理を無視する。

定義するログオン情報用フォームに詳細構成設定が必要な場合は、フォーム定義ウィザードの［そのほかの設定］ページの［詳細設定］をクリックします。［詳細設定］ダイアログボックスが開きます。

［詳細設定］ダイアログボックスには、ダイアログボックス左側で選択できる以下の2つの設定ページがあります。

- ［ホストフォームのそのほかの設定］ページには、以下の［そのほかの設定］オプションが表示されます。
  - 待機時間：アプリケーションが完全に読み込まれるのを待つ間、フォーム処理の開始を遅らせる時間をミリ秒単位で入力します。
  - 前入力のキー：そのフォームの最初のフィールドに移動するために必要な仮想キーコードを入力します。［仮想キーコード］をクリックすると、有効なキーコードについてのヘルプトピックが表示されます。
- ［無視するためのマッチ条件］ページには、［ログオン情報の送信を停止するための文字列のマッチ条件］オプションが表示されます。ここでは、無視するフォームを識別するための条件として、アプリケーション画面に表示される文字列を指定します。

ターミナルエミュレーターベースのアプリケーションの定義における注意事項

Sep 27, 2015

ターミナルエミュレーター（HLLAPI）ベースのアプリケーションの定義を作成する場合、次の点に注意してください。

- そのアプリケーションを使用する各ユーザー構成で、ターミナルエミュレーターのサポートが有効になっている必要があります。
- ターミナルエミュレータープログラムがHLLAPI準拠であることを確認します。
- ターミナルエミュレータープログラムがSingle Sign-On Plug-inのmfrmlist.iniファイルに定義されていることを確認します。
- カーソル位置の行と列の座標を表示するターミナルエミュレーターを使用すると、アプリケーション定義を作成するときに便利です。アプリケーションと各ログオン情報用フォームの識別に使用する文字列とフィールドの位置を簡単に判断できます。
- ターミナルエミュレーターによって自動的に各セッションに割り当てられる名前が、短い形式の名前であることを確認します。短い名前でないと、Single Sign-Onでターミナルエミュレーターベースのアプリケーションを認識できません。
- ターミナルエミュレーターベースのアプリケーションのマニュアルには、ログオン情報の送信に使用する画面番号など、固有の識別子が記載されている場合があります。その場合は、Single Sign-Onがログオン情報を識別し、正しいフォームに送信できるように、画面番号を固有の識別子として使用します。

ターミナルエミュレーターのサポート機能

Sep 27, 2015

サポートされるターミナルエミュレーターは、mfrmlist.iniファイルに含まれています。このファイルには、Citrix社によってテスト済みのすべてのターミナルエミュレーターが定義されています。

mfrmlist.iniにほかのエミュレーターを追加することはできますが、その場合はエミュレーターを実稼働環境に展開する前にテストを行い、問題がないことを確認する必要があります。次に、mfrmlist.iniに定義されている[Emulators]セクションの例を示します。

[Emulators] Ver=20021101 EMU1=Rumba6 EMU2=Attachmate myExtra!EMU3=Attachmate Extra!6.3 EMU4=Attachmate Extra!6.4 EMU5=Attachmate Extra!6.5 EMU7=Attachmate Extra!7.1 EMU8=Reflec

[Emulators]セクションのターミナルエミュレーターエントリには、EMU1～EMU99の範囲で連続する番号を付ける必要があります。番号が連続していないエントリがあると、ssomho.exeプロセスがすべてのエントリを読み取る前に終了します。

使用しないエミュレーターのエントリがある場合は、そのエントリを削除するか、またはコメントアウトします。これにより、不要なDLLファイルの読み込みやHLLAPIのリソースの消費を避けることができるので、ssomho.exeプロセスが効率的に実行されます。

エミュレーターのエントリをコメントアウトするには、不要なエントリをリストの最後に移動して、エントリの前にセミコロン（;）を挿入し、そのほかのエントリが連番になるように番号を変更します。

Single Sign-Onですべてのコンピューター上のmfrmlist.iniファイルを一度に更新することはできません。mfrmlist.iniを変更した場合は、Single Sign-On Plug-inをインストールした後に、手作業で既存のmfrmlist.iniファイルを上書きする必要があります。大規模な環境で運用している場合は、Microsoft Systems Management Server（SMS）、CA Unicenter、またはActive Directoryでバッチファイルやスクリプトを実行してmfrmlist.iniファイルを更新することをお勧めします。

mfrmlist.iniのフィールド定義

Sep 27, 2015

mfrmlist.iniにエミュレーターのエントリを追加しても、機能するのはHLLAPをサポートするエミュレーターだけです。次の表は、mfrmlist.iniファイルのフィールド定義を示します。エミュレーターの定義を追加する場合は、エミュレーターの製造元にそのエミュレーターがHLLAPIをサポートしているかどうかを確認し、正しいフィールド定義エントリを取得します。また、Single Sign-Onでエミュレーターを使用できるかどうかを確認する場合は、実務環境外でテストします。

フィールド	定義
[EmulatorName]	このフィールドの値は、[Emulators]セクションのEMUnn=EmulatorName行の値と同じである必要があります。
GroupName	内部使用のみ（変更しないでください）。
DisplayName	エミュレーターのディスプレイ名。セッションを処理するための新しいプロセスを起動するときに使用される2つのパラメーターの1つです。mfrmlist.iniファイル内で、重複して使用することはできません。
RegistryLoc	HLLAPI DLLの場所を参照するHKEY_LOCAL_MACHINE\SOFTWARE内のレジストリキー。エミュレータープログラムがHKEY_LOCAL_MACHINE\SOFTWAREにこの情報を保存しないように設定されている場合は、このRegistryLocの設定ではなく、ExplicitPathの設定を使用します。RegistryLocとExplicitPathの両方の設定を定義した場合は、ExplicitPathの設定が優先されます。
ExplicitPath	エミュレーターが使用するHLLAPI DLLファイルの明示パス。この設定は、エミュレータープログラムがHLLAPI DLLの場所をシステムレジストリに保存しない場合に、RegistryLoc設定の代わりに使用されます。RegistryLocとExplicitPathの両方の設定を定義した場合は、ExplicitPathの設定が優先されます。
ValueName	エミュレータープログラムの実際の場所のパスを含むRegistryLocキー内の値の名前。
DLLFile	HLLAPI DLLファイルの名前。
StripFileName	ValueNameおよびDLLFileのエントリからHLLAPI DLLのパスを作成するときに、ValueNameから取得した値の最後の円記号（\）およびその後ろの部分を削除する必要がある場合に1を指定します。
IntSize	エミュレーターがサポートするシステムのビット数（16ビットまたは32ビット）を整数で指定します。
WindowClass	エミュレーターのウィンドウクラス名。管理コンソールまたはアプリケーション定義ツールを使用して取得します。
WindowTitle	エミュレーターに関連付けられているウィンドウタイトルの一部。Single Sign-Onは、この値を使用してエミュレーターのウィンドウを確認します。ウィンドウタイトルに含まれる単語を少なくとも1つ指定する必要があります。この値の前後にワイルドカード置かれているとみなされます。

UseSendKeys パラメーター	定義 Single Sign-Onがエミュレーターとの通信にSendKeysオプションを使用するかどうかを指定します。このオプションは、Windowsアプリケーション用のSendKeysオプションとは異なります。

ユーザー構成の作成

Sep 30, 2015

ユーザー構成の内容により、ユーザーのSingle Sign-On Plug-inの動作やユーザーインターフェイスが制御されます。ユーザー構成の作成は、環境内のユーザーにSingle Sign-On Plug-inを配布する直前に行います。ただし、新しいユーザー構成の追加や既存のユーザー構成の編集は、いつでも行うことができます。

ユーザー構成は、ユーザー固有の設定、パスワードポリシー、およびアプリケーショングループを定義したもので、Active Directory階層に関連付けられたユーザー（組織単位または個々のユーザー）またはActive Directoryグループに適用されます。

ユーザー構成は、以下の要素で構成されています。

- Active Directoryドメイン階層に関連付けられたユーザー（組織単位または個々のユーザー）またはActive Directoryグループ。
  重要：Active Directory混在モードの配布グループとドメインローカルグループはサポートされていません。
- ユーザーのライセンスの種類（同時接続ライセンスまたは指定ユーザーライセンス）および設定。
- データの保護方法
- 作成済みのアプリケーション定義。ユーザー構成の作成時に、複数のアプリケーション定義を組み合わせてアプリケーショングループを作成できます。
- アプリケーショングループに設定されているパスワードポリシー。
- アカウントセルフサービス機能（アカウントのロック解除とパスワードのリセット）とキー管理オプション（以前のパスワードの使用、セキュリティ用の質問、自動キー管理）。
- そのほかの設定。プロビジョニング、アプリケーションのサポート設定など。

ユーザー構成を作成する前に、以下を作成または定義しておく必要があります。

- 中央ストア
- アプリケーション定義
- パスワードポリシー
- セキュリティ用の質問

Single Sign-On Plug-inをユーザーのコンピューターにインストールする前に、必ずユーザー構成を作成してください。ユーザー構成には、Single Sign-On Plug-inの動作に必要なライセンスサーバー情報およびライセンス情報が含まれます。

各オプションのデフォルト設定や詳細については、
—「Single Sign-On設定リファレンス」の「ユーザー設定」
を参照してください。

ユーザー構成にドメインコントローラーを関連付けるには

Active Directory形式の中央ストアを使用している環境で、複数のドメインコントローラーがある場合は、中央ストアにデータを書き込むときにユーザー構成にバインドするドメインコントローラーを選択します。

このバインド設定により、Active Directory複製による同期処理の遅延を短縮できます。この遅延は、複数のActive Directoryサイトでユーザーが Single Sign-Onに同時にアクセスする環境で起こることがあります。

管理コンソールの検出プロセスで、Single Sign-Onはドメイン内にあるすべてのドメインコントローラーを検出できます。ユーザー構成の作成時に、特定のドメインコントローラーを選択し、ユーザー構成をこのドメインコントローラーにバインドできます。

たとえば、ユーザーのローカルネットワーク内のドメインコントローラーにバインドされるように設定できます。これによ

り、次回そのユーザーがSingle Sign-On環境にログオンしたときに、選択したドメインコントローラーにバインドされます。

デフォルトでは、書き込み可能な任意のドメインコントローラーにユーザーがバインドされます。必要に応じて、ユーザーデータの整合性を損なわずに、ユーザー構成を編集して、ユーザーのバインド先のドメインコントローラーを変更します。

注：特定のドメインコントローラーにユーザーを関連付ける場合は、そのドメインコントローラーがピーク時のユーザー接続で発生するトラフィックをサポートできることを確認してください。
指定したドメインコントローラーが使用できない、またはオフラインの場合は、Single Sign-Onはローカルストアのユーザーデータ（ユーザーのコンピューター上にあるユーザーデータ）を使用します。ドメインコントローラーが長時間（指定時間以上）オフラインの場合は、管理コンソールの操作ペインの［ユーザー設定の編集］を選択し、別のドメインコントローラーを選択するか、［書き込み可能な任意のドメインコントローラー］を選択します。

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］ノードを選択します。
3. 既存のユーザー構成を選択します。
4. ［操作］メニューから、［ユーザー設定の編集］を選択します。
5. ［ユーザー設定の編集］の左側の一覧で、［ドメインコントローラー］を選択します。
6. 一覧からドメインコントローラーを選択するか、［書き込み可能な任意のドメインコントローラー］を選択します。

ユーザー構成を作成するには

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デリバリーサービスコンソール］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］ノードを選択します。
3. ［操作］メニューから、［ユーザー設定の追加］を選択します。

ユーザー構成の名前

ユーザー設定ウィザードの［ユーザー設定の名前］ページでは、作成するユーザー構成の名前と、割り当て先のユーザーを指定します。

- 名前
  ユーザー構成には、「Marketing Users」、「Software Development Users」、「North AmericanUsers」など、ユーザーをどのようにグループ分けし、特定のアプリケーションに関連付けるかを考えて名前を付けます。

- ユーザー構成の割り当て
  ユーザー構成は、Active Directory階層に関連付けられたユーザー（組織単位または個々のユーザー）またはActive Directoryグループに割り当てることができます。必要に応じて、［操作］メニューから［ユーザー設定の移動］を選択して、ユーザー構成を別の階層やグループに割り当てることができます。

  重要：Active Directory環境の構成は、ユーザー構成の適用に影響します。 つまり、ユーザー構成をActive Directory階層（組織単位またはユーザー）に割り当てるか、Active Directoryグループに割り当てるかを考慮する必要があります。この両方（階層とグループ）を使用していてユーザーがどちらのコンテナーにも存在する場合、階層に割り当てられたユーザー構成が優先的に使用されます。このようなスキームは、混在環境とみなされます。
  また、ユーザーが2つのActive Directoryグループに属しており、各グループともそれぞれユーザー構成に割り当てられている場合は、優先度の高いユーザー構成が適用されます。

  ユーザー構成のグループへの割り当ては、Active Directory認証を使用するActive Directoryドメインでのみサポートされています。

ドメインコントローラーの指定

Active Directory形式の中央ストアを使用している場合は、ユーザー設定ウィザードの [ドメインコントローラーの指定] ページで、特定のドメインコントローラーまたは [書き込み可能な任意のドメインコントローラー] を選択します。

アプリケーションの選択とユーザー設定の構成

Sep 30, 2015

ユーザー設定ウィザードの［アプリケーションの選択］ページでは、このユーザー構成に関連付けるアプリケーション定義を選択します。［追加］をクリックすると、ダイアログボックスが開き、作成済みのアプリケーション定義が表示されます。これらのアプリケーション定義を追加して、アプリケーショングループを作成します。通常、アプリケーショングループには複数のアプリケーションを追加しますが、単一のアプリケーションでアプリケーショングループを構成することもできます。

また、パスワード共有グループを作成して、パスワードの変更プロセスを自動化および単純化することもできます。パスワード共有グループに属するアプリケーションのパスワードが変更された場合、その変更がグループ内のすべてのアプリケーションのログオン情報に反映されます。

パスワード共有グループを使用すると、同じ認証機関を使用する複数のアプリケーションのログオン情報をSingle Sign-On Plug-inで一括管理できるようになります。たとえば、同じOracleデータベースを使って認証する2つのアプリケーション（経理アプリケーションと人事アプリケーションなど）を、同じパスワード共有グループに追加します。ユーザーが一方のアプリケーションでパスワードを変更すると、他方のアプリケーション用のパスワードも自動的に更新されます。

重要：パスワード共有グループに属するすべてのアプリケーションのパスワードが、共通の認証機関で管理されることを確認してください。たとえば、パスワード共有グループに属するアプリケーションが、データベースなどの共通のバックエンド認証機関を共有し、ユーザーがデータベースで認証されるために各アプリケーションに同じログオン情報が送信される場合に、パスワード共有グループを作成します。電子メールプログラム、Webアプリケーション、イントラネット上のカスタムプログラムなど、3つの異なるログオン情報をユーザーが使用する可能性があるアプリケーションでは、同じログオン情報を使用したとしても、パスワード共有グループを作成できません。たとえば、認証機関が異なる3つのアプリケーションがパスワード共有グループに含まれている場合に、1つのアプリケーションの変更後のパスワードが、ほかのアプリケーションで無効である可能性があるためです。

ユーザー設定の構成

以下のページでは、ユーザー設定のオプションを構成します。各オプションについて詳しくは、
—「Single Sign-On設定リファレンス」の「ユーザー設定」
を参照してください。

- ユーザー設定ウィザードの［Plug-inの動作の設定］ページでは、このユーザーのSingle Sign-On Plug-inの動作を設定します。
- ユーザー設定ウィザードの［ライセンスの設定］ページでは、ライセンスサーバーとライセンスモデルを選択します。
  重要：ユーザー構成を編集して製品エディションを変更すると、ライセンスモデルも変更される場合があります。たとえば、製品エディションをSingle Sign-On EnterpriseからSingle Sign-On Advancedに変更すると、同時接続ユーザーライセンスモデルから指定ユーザーライセンスモデルに変更されます。
- ユーザー設定ウィザードの［データ保護方法の選択］ページでは、ユーザーのログオン情報を暗号化して保護するための方法について設定します。ユーザーのログオン情報は、ユーザーがWindowsにログオンするときに使用するプライマリな認証方法に基づいて暗号化され、中央ストアに格納されます。一部の環境では、ユーザーが複数の認証方法を使用することがあります。
- ユーザー設定ウィザードの［もう1つのデータ保護方法（セカンダリ）の設定］ページでは、ユーザーが自分のプライマリな認証方法を変更した場合（たとえば、ドメインパスワードやスマートカードを変更した場合）の追加のセキュリティとして、ユーザーのログオン情報のロックを解除する前に、ユーザーの再認証および同一性の検証を行うように設定できます。または、キー管理モジュールを使用して、ログオン情報の自動復元を設定することもできます。
- ユーザー設定ウィザードの［アカウントセルフサービス機能の設定］ページでは、ユーザーが自分でプライマリパスワードをリセットしたりロックされたアカウントを解除したりできるセルフサービス機能について設定します。この機能を使用するには、Single Sign-Onサービスのセルフサービスモジュールとキー管理モジュールをインストールする必要があります

す。アカウントセルフサービス機能を有効にすると、ユーザーがWindowsにログオンしたりコンピューターのロックを解除したりするためのダイアログボックスに [アカウントセルフサービス] ボタンが追加されます。

- ユーザー設定ウィザードの [キー管理モジュール] ページおよび [プロビジョニングモジュール] ページでは、インストールされているサービスモジュールのURLとサービスポートを指定します。

アカウントの関連付け機能によるログオン情報の同期

Sep 30, 2015

複数のWindowsドメインを持った組織では、ユーザーが複数のWindowsアカウントを使用している場合があります。Single Sign-Onには、アカウントの関連付けを有効にする、ログオン情報の同期サービスが含まれています。

アカウントの関連付け機能により、異なるWindowsアカウントでユーザーがログオンしているときでも、Single Sign-Onに登録済みのログオン情報を使ってアプリケーションにログオンできます。通常、ユーザーのログオン情報は単一のWindowsアカウントに関連付けられ、ユーザーの複数のWindowsアカウント間で自動的にログオン情報が同期されることはありません。管理者がアカウントの関連付け機能を有効にすると、ユーザーは異なるWindowsアカウントを使っているときでも、登録済みのログオン情報を使ってアプリケーションにログオンできます。ユーザーがログオン情報を変更、追加、または削除すると、関連付けられたすべてのアカウントでのログオン情報が自動的に同期されます。

管理者がアカウントの関連付け機能を有効にしていない場合、複数のWindowsアカウントを持つユーザーは、各Windowsアカウントから個別にログオン情報を変更する必要があります。

アカウントの関連付けを構成するには、組織のWindowsドメイン管理者は、次の手順を順番どおりに行う必要があります。

1. ログオン情報の同期モジュール（Single Sign-Onサービスの一部）をホストするドメインを選択します。
2. アカウントの関連付け機能を使用する組織内のすべてのコンピューターに、信頼されたルート証明書を配布します。
3. ドメイン間でアプリケーション定義を手作業で同期します。
4. ほかのドメインでアカウントの関連付け構成して、ログオン情報の同期モジュールへの接続を設定します。
5. アカウントの関連付けツールを、公開アプリケーションとしてユーザーに提供します。

各ユーザーは、Single Sign-On Plug-inでアカウントの関連付けを有効にする必要があります。

ログオン情報の同期モジュールをホストするドメインの選択と設定

アカウントの関連付け機能を使用するすべてのユーザーのアカウントが含まれているドメインを選択します。ログオン情報の同期モジュールは、組織内のすべてのログオン情報のハブとして機能します。選択したドメインにログオン情報の同期モジュールをインストールします。

重要：ファイアウォールの設定変更が必要かどうか、変更内容が会社のポリシーに準拠しているかどうかをネットワーク管理者に確認してください。
ログオン情報の同期モジュールをインストールしたら、管理コンソールでユーザー構成を作成または編集して、個々のユーザーアカウントにログオン情報の同期モジュールの使用を許可します。

ホストドメインでログオン情報の同期モジュールを構成するには

ログオン情報の同期モジュールをホストしているドメインで管理コンソールを開きます。一部のドメインは、複数の中央ストアにアクセスできる場合があります。管理コンソールが、ログオン情報の同期モジュールサービスと同じ中央ストアに接続するように構成されていることを確認してください。

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］を選択します。
3. 既存のユーザー構成を選択するか、新しいユーザー構成を作成します。
   - 新しいユーザー構成を作成する場合は、［Plug-inの動作の設定］ページの［詳細設定］をクリックして、次の手順に進みます。

- 既存のユーザー構成を編集する場合は、［ユーザー設定の編集］ページで、次の手順に進みます。

4. ［同期処理］をクリックして、［ログオン情報の同期モジュールがユーザーのログオン情報にアクセスすることを許可する］チェックボックスをオンにします。
5. ［OK］をクリックして、必要なユーザー構成で手順3.～4.を繰り返します。

ドメイン間でアプリケーション定義を手作業で同期するには

ユーザー構成の関連付けが異なるアカウントを同期することもできます。たとえば、ユーザー構成をある特定のドメインのActive Directory階層（組織単位またはユーザー）と、別のドメインのActive Directoryグループに関連付けることができます。各ユーザー構成でアプリケーション定義名が同じであれば、アカウントの関連付け機能によりログオン情報が同期されます。

ログオン情報は、Single Sign-On管理者が作成したアプリケーション定義のものだけが共有されます。また、管理者は、関連付けるドメイン間で同じアプリケーション定義名を使用する必要があります。

たとえば、SAPのアプリケーション定義の名前として、あるドメインは「SAP Logon」、別のドメインでは「SAP」、また別のドメインでは「SAP Launch Pad」が使用されている場合、これらのアプリケーションのログオン情報はドメイン間で同期されません。

複数のドメインで新しいアプリケーション定義を作成する場合は、管理コンソールの操作ペインの[アプリケーション定義のエクスポート］と［管理データのインポート］を使用すると、簡単にアプリケーション定義を複製できます。これらのタスクを使用して、新しく作成したアプリケーション定義をエクスポートし、各中央ストアにインポートします。既存のアプリケーション定義で名前が異なる場合は、手作業で名前を変更する必要があります。

ほかのドメインでアカウントの関連付けを構成するには

ログオン情報の同期モジュールをホストしていないドメインのコンピューターで、Single Sign-On管理コンソールを起動します。一部のドメインは、複数の中央ストアにアクセスできる場合があります。この場合、各中央ストアについてこの手順を実行する必要があります。

各ドメインの管理者は、ドメインユーザーのアカウントと、ログオン情報の同期モジュールをホストしているドメインのアカウントとの関連付けを許可する必要があります。これを行うには、次の手順に従って、ログオン情報の同期モジュールをホストしていない各ドメインの管理コンソールでアカウントの関連付けを有効にします。

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］を選択します。
3. 既存のユーザー構成を選択するか、新しいユーザー構成を作成します。
   - 新しいユーザー構成を作成する場合は、［Plug-inの動作の設定］ページの［詳細設定］をクリックして、次の手順に進みます。
   - 既存のユーザー構成を編集する場合は、［ユーザー設定の編集］ページで、次の手順に進みます。
4. ［アカウントの関連付け］をクリックします。
5. ［アカウントの関連付けをユーザーに許可する］チェックボックスをオンにします。
   必要に応じて、以下のオプションを設定します。

6. ［デフォルトのサービスアドレスを指定する］チェックボックスをオンにして、ログオン情報の同期モジュールをホストするドメインのSingle Sign-Onサービスのアドレスとポートを入力します。
7. ［サービスアドレスの変更をユーザーに許可する］チェックボックスをオフにします。
8. ［デフォルトのドメインを指定する］チェックボックスをオンにして、ログオン情報の同期モジュールをホストするドメインの名前を入力します。ここでドメイン名を指定しないと、どのドメインアカウントの情報を入力すべきか、ユーザー

が迷う場合があります。

9. ［ドメインの変更をユーザーに許可する］チェックボックスをオフにします。
10. 所属組織のセキュリティポリシーで許可される場合は、必要に応じて［パスワードの保存をユーザーに許可する］チェックボックスをオンにします。
11. ［OK］をクリックし、各ユーザー構成で各手順を繰り返します。

アカウントの関連付けツールを公開する

このバージョンのSingle Sign-On Plug-inでは、アカウントの関連付け機能を有効にするためのメニューオプションがユーザーに提供されていません。このため、管理者はこの機能を有効にするためのツールをユーザーに公開アプリケーションとして提供する必要があります。

1. XenAppサーバーにSingle Sign-On Plug-inをインストールします。
2. XenAppサーバー上で、AccAssoc.exeファイルを見つけます。
3. このAccAssoc.exeファイルをユーザーに公開します。
4. アカウントの関連付けツールの起動方法および使用方法をユーザーに通知します。

注：Single Sign-On Plug-in Versions 4.8およびそれ以前のバージョンのユーザーは、アカウントの関連付け機能を有効にするためのメニューオプションを使用できます。この場合、このツールの公開アプリケーションを使用する必要はありません。

Single Sign-On Plug-inでアカウントの関連付けを有効にするには

Sep 30, 2015

ログオン情報の同期モジュールをホストするドメインにログオンしているときは、ユーザーがアカウントの関連付け機能を有効にする操作を行う必要はありません。このドメインのアカウントは、各ユーザーのログオン情報を保持する中央リポジトリとして機能します。

ユーザーがほかのドメインにログオンしているときには、Single Sign-On Plug-inのバージョンにより、以下の2通りの方法でアカウントの関連付けを有効することができます。

- このバージョンのSingle Sign-On Plug-inのユーザーは、公開アプリケーションとしてアカウントの関連付けツールを起動します。管理者は、このツールを公開アプリケーションとしてユーザーに提供し、そのアプリケーションへのアクセス方法を通知しておく必要があります。
- Single Sign-On Plug-in Versions 4.8およびそれ以前のバージョンのユーザーには、ログオンマネージャーの[ツール]メニューに［アカウントの関連付け］コマンドが表示されます。ユーザーは、このコマンドを使用してアカウントの関連付けを有効にします。

1. プラグインソフトウェアのバージョンに応じて、ユーザーがアカウントの関連付けツールの公開アプリケーションにアクセスするか、ログオンマネージャーの［ツール］>［アカウントの関連付け］を選択します。［アカウントの関連付け］ダイアログボックスが開きます。
2. ユーザーが、［アカウントの関連付けを有効にする]チェックボックスをオンにします。
   注：管理者によりデフォルトのサービスアドレスが指定されていない場合は、ユーザーが［サービスアドレス］ボックスにログオン情報の同期モジュールのサービスアドレスを入力する必要があります。サービスアドレスが管理者により指定済みである場合、ユーザーはこのボックスに入力できません。
3. ユーザーが、［OK］をクリックします。［アカウントの関連付けの認証]ダイアログボックスが開きます。
4. ユーザーが、関連付けるWindowsアカウントのユーザー名とパスワードを入力します。管理者によりデフォルトのドメインが指定されていない場合は、ユーザーが［ドメイン］ボックスに関連付け先のドメインを入力する必要があります。
   注：ドメイン名が管理者により指定済みである場合、ユーザーはこのボックスに入力できません。
5. ユーザーが、［OK］をクリックします。これで、アカウントの関連付けが有効になりました。Single Sign-On Plug-inの同期処理が行われるときに、ユーザーのログオン情報も同期されます。

ユーザー構成の管理

Sep 30, 2015

Single Sign-Onによりユーザー構成を管理できます。次のことを実行できます。

- ユーザーデータのリセット
- ユーザーデータの削除
- ユーザーの再登録
- ユーザー構成の優先度の設定
- ユーザー構成の別のユーザーへの割り当て
- 既存のユーザーのユーザー構成のアップグレード

ユーザーデータをリセットするには

［ユーザーデータのリセット］タスクを使用するには、Single Sign-Onサービスのプロビジョニングモジュールがインストールされ、構成済みである必要があります。

［ユーザーデータのリセット］を使用すると、中央ストアのユーザー情報をリセットして、そのユーザーを初期状態に戻すことができます。

- Active Directory形式の中央ストアでは、ユーザーデータ（ログオン情報、セキュリティ用の質問と回答など）が削除され、そのユーザーにはデータがリセットされたことを示すフラグが付けられます。
- NTFSネットワーク共有の中央ストアでは、ユーザーフォルダーはそのまま残りますが、ユーザーデータはすべて削除され、そのユーザーにはデータがリセットされたことを示すフラグが付けられます。

［ユーザーデータのリセット］は、ユーザーがセキュリティ用の質問に対する回答を忘れた場合や、ユーザーのデータが何らかの理由で破損した場合に、ログオン情報データを初期化するために使用します。ユーザーが次にSingle Sign-On Plug-inを使用して中央ストアに接続したときに、ユーザーのローカルのログオン情報ストアにあるデータはすべて消去されます。ユーザーは、ログオン情報の設定を再度行う必要があります。

このタスクは、ユーザーがSingle Sign-On Plug-inにログオンできない場合にも使用できます。

重要：パスワードの履歴情報は、ユーザーごとに保持されます。ユーザーのパスワードデータをリセットすると、そのユーザーのパスワード履歴も削除されます。

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］ノードを選択します。
3. ［操作］メニューから、［そのほかのタスク］［ユーザーデータのリセット］の順に選択します。 ［ユーザーの選択］ダイアログボックスが開きます。
4. ユーザー名を入力して、［名前の確認］をクリックします。
5. ［OK］をクリックします。
6. 中央ストアでユーザーを選択し、［リセット］をクリックします。
7. ［OK］をクリックします。 ユーザーのログオフを確認するメッセージが表示されます。
8. リセット対象のユーザーがCitrix XenAppでホストされているSingle Sign-Onを実行していないことを確認して、［続行］をクリックします。
   注：ユーザーがログオフしていない場合は、［キャンセル］をクリックし、ユーザーのICAセッションをリセットしてから、もう一度この手順を行ってください。
9. ユーザー情報が確認され、リセット処理が完了したら、［ユーザーデータのリセット］ダイアログボックスの［OK］をクリックします。 この手順の後でそのユーザーがSingle Sign-On Plug-inを使用してログオンすると、そのユーザーのデータ

がリセットされます。

ユーザーデータを削除するには

［中央ストアからのユーザーデータの削除］タスクは、すべてのユーザーデータと情報を中央ストアから削除します。［中央ストアからのユーザーデータの削除］は、現在の環境からユーザーを完全に削除する場合に使用します。

ユーザーのコンピューター上にあるローカルのログオン情報ストアは、管理者またはユーザーによって明示的に削除されるまで変更されません。

ローカルのログオン情報ストアが明示的に削除されていない場合、そのユーザーがSingle Sign-On Plug-inを実行すると、ローカルのログオン情報ストアと中央ストアが同期されます。これを防止するには、環境内からユーザーアカウントを削除します（Active Directoryからユーザーを削除したり無効にしたりするなど）。

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］ノードを選択します。
3. ［操作］メニューから、［そのほかのタスク］［中央ストアからのユーザー設定の削除］の順に選択します。 ［ユーザーの選択］ダイアログボックスが開きます。
4. ユーザー名を入力して、［名前の確認］をクリックします。
5. ［OK］をクリックします。 ［Yes］をクリックして確定します。 確認のメッセージが表示されます。
6. ［OK］をクリックします。 中央ストアからユーザーデータが削除されます。

セキュリティ用の回答を再登録させるには

特定のユーザーまたはすべてのユーザーに、セキュリティ用の質問に対する回答の再登録を要求できます。次の機能はセキュリティ上の理由から、またはユーザーデータが破損した場合に使用します。

- ユーザーの回答を削除する
  このタスクでは、ユーザーのセキュリティ用の質問のデータを削除します。質問ベースの認証機能は、ユーザーが回答を再登録するまで使用できなくなります。

- すべてのユーザーに回答を再登録させる
  すべてのユーザーがSingle Sign-On Plug-inを次回起動したときに、セキュリティ用の質問に対する回答を再登録させる場合に、このタスクを選択します。このタスクを実行しても、ユーザーが回答を再登録するまでは現在のセキュリティ用の質問データが保持され、ユーザーは現在の回答で再認証できます。ユーザーが回答を再登録するまでは、再登録を確認するメッセージが表示されます。

登録用のダイアログボックスで［キャンセル］をクリックして、回答を再登録しないことを選択したユーザーは、再登録を行うまで、質問ベースの認証を使用する機能（アカウントセルフサービスなど）は使用できません。

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］を選択します。
3. ［操作］メニューの［そのほかのタスク］で、以下のいずれかを選択します。
   - ユーザーの回答を削除する
     ［ユーザーの選択］ダイアログボックスが開きます。ユーザーを指定して、［OK］をクリックします。

   - すべてのユーザーに回答を再登録させる
     確認のメッセージが表示されます。すべてのユーザーにセキュリティ用の回答を再登録させる場合は、［はい］をクリックし、［OK］をクリックします。

ユーザー構成の優先度を設定するには

ユーザー構成を作成または編集するときに、Active Directoryグループに属するユーザーをユーザー構成に割り当てることができます。グループ内のユーザーを複数のユーザー構成に割り当てることもできます。この場合、ユーザー構成の優先度を設定できます。

重要：Single Sign-Onのユーザー環境の構成は、ユーザー構成の適用に影響します。つまり、ユーザー構成をActive Directory階層（組織単位またはユーザー）に割り当てるか、Active Directoryグループに割り当てるかを検討する必要があります。この両方（階層とグループ）を使用していてユーザーがどちらのコンテナーにも存在する場合、階層に割り当てられたユーザー構成が優先的に使用されます。このようなスキームは、混在環境とみなされます。

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］ノードを選択します。
3. ［操作］メニューから、［そのほかのタスク］、［ユーザー設定の優先度設定］の順に選択します。［ユーザー設定の優先度設定］ダイアログボックスが開きます。
4. ユーザー構成を選択し、［上へ移動］または［下へ移動］をクリックして、優先度を変更します。

別のユーザーへのユーザー構成の割り当て

既存のユーザー構成を編集する場合、そのユーザー構成の割り当て先を変更することはできません。同様のユーザー構成をほかのユーザーに割り当てる場合、次のいずれかの操作を行うことができます。

- ユーザー構成を複製して、ほかのユーザーに適用する。
- ユーザー構成を移動して、ほかのユーザーに適用する。

ユーザー構成を複製するには

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］ノードを選択します。
3. 既存のユーザー構成を選択します。
4. ［操作］メニューから、［ユーザー設定の複製］を選択します。
5. 複製の名前を入力します。
6. 割り当て先のユーザーが含まれている組織単位、ユーザー、またはグループを指定します。

ユーザー構成を移動するには

Active Directoryグループに割り当てられているユーザー構成は移動できません。Active Directory階層（組織単位またはユーザー）にユーザー構成を割り当てるには、ユーザー構成を複製し、割り当て先を指定します。

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］ノードを選択します。
3. 既存のユーザー構成を選択します。
4. ［操作］メニューから、［ユーザー設定の移動］を選択します。
5. 割り当て先のユーザーが含まれている組織単位、ユーザー、またはグループを指定します。

既存のユーザー構成のアップグレード

Single Sign-On（Password Manager）4.0および4.1では、Active Directory階層（組織単位またはユーザー）単位でユーザーをユーザー構成に割り当てます。Single Sign-On（Password Manager）のVersions 4.6、4.6、4.8、および5.0では、さらにActive Directoryグループ単位でユーザーを割り当てることができます。

- 階層単位に割り当てられている既存のユーザー構成があり、新しいユーザー構成をグループ単位に割り当てる場合、どちらにも属しているユーザーには階層に割り当てられているユーザー構成が優先して適用されます。このようなスキームは、混在環境とみなされます。この場合、ユーザーのSingle Sign-On Plug-inで意図しない処理が行われることがあります。たとえば、グループ単位のユーザー構成に割り当てられているリソースではなく、階層単位のユーザー構成に割り当てられているリソースにアクセスできるようになります。
- 既存の階層単位のユーザー構成での設定を維持しながら割り当て先を変更する場合は、ユーザー構成を移動してください。この手順は、Single Sign-On 4.1、4.5、4.6、4.8、および5.0の階層単位のユーザー構成で使用できます。

組織単位またはユーザー単位で編成されているユーザーの既存のユーザー構成をアップグレードする場合は、次の点に留意してください。

Single Sign-Onサービスと管理コンソールをアップグレードしてPlug-in（エージェント）をアップグレードしない場合、Active Directory階層（組織単位やユーザー）に割り当てられたユーザー構成では、Single Sign-Onの基本的な機能が提供されます。ただし、Single Sign-Onの最新の機能を使用するには、Plug-inをアップグレードする必要があります。環境内のすべてのPlug-inを、管理コンソールやSingle Sign-Onサービスと同じバージョンにアップグレードしてください。

ユーザーの認証と同一性の検証

Sep 30, 2015

Single Sign-Onには、次の2つの種類の認証があります。

- プライマリ認証：社内ネットワークにアクセスするために、ユーザーがWindowsのログオン画面にプライマリのユーザー名、パスワード、およびオプションでドメイン名を入力するときの認証。既存のWindowsセキュリティサブシステムによって、ネットワーク認証が管理されます。
- セカンダリ認証：パスワードで保護されているアプリケーションなどのリソースに、ユーザーがアクセスするために行わる認証。ユーザーのログオン情報が送信されるように、管理者がSingle Sign-Onを設定します。このようなリソースには、企業アプリケーション、Webアプリケーション、アプリケーション内の保護されているフィールド、IPアドレス、およびURLなどがあります。

ネットワーク認証が成功すると、Single Sign-Onは、Windowsのログオンコンポーネントからプライマリパスワードを取得し、その情報を使用して、ユーザーのログオン情報（セカンダリパスワード）を保護する暗号キーを作成します。Single Sign On Plug-inがアプリケーションまたはリソースからのログオン要求を検出すると、この暗号キーを使ってログオン情報を取得し、復号化します。

重要：ユーザーのパスワードが不正に改変された場合は、パスワードを2回リセットしてください。これにより、不正なパスワードが「変更前のパスワード」としてシステムに残ることを避けることができます。この場合、Single Sign-On Plug-inがパスワードの変更を認識できるように、ユーザーはパスワードをリセットするたびにWindowsにログオンする必要があります。

ユーザーの同一性検証が必要な状況

ユーザーがネットワーク環境にログオンする場合、ユーザー名とパスワードを入力したり、スマートカードやそのほかの認証機器を使用したりして、そのユーザーが本人であることを証明します。

これに加えて、以下の特定の状況で、そのユーザーがSingle Sign-Onで認証されたユーザーと同一であることを確認するために、再認証を行う必要があります。

イベント	説明
管理者がユーザーのプライマリパスワードを変更した。	管理者がユーザーのプライマリパスワードを変更した場合、ログオンしたユーザーが本人であることを検証する必要があります。
アカウントセルフサービス機能を使用して、ユーザーがプライマリパスワードをリセットした。	ユーザーがアカウントセルフサービス機能を使ってプライマリパスワードをリセットする場合、そのユーザーが本人であることを証明する必要があります。アカウントセルフサービス機能を使ってプライマリパスワードをリセットするユーザーは、変更前のパスワードを忘れているため、［変更前のパスワードを入力させる］オプションを唯一のユーザー識別処理方法として設定しないでください。
アカウントセルフサービス機能を使用して、ユーザーがアカウントのロックを解除した。	ユーザーがアカウントセルフサービス機能を使ってアカウントのロックを解除する場合、そのユーザーがロック前のユーザーと同一であることを検証する必要があります。
ユーザーが認証方法を変更した。	たとえば、ユーザーが、スマートカードによる認証からパスワードによる認証に切り替える場合、そのユーザーが本人であることを検証する必要があります。

イベント	説明
Single Sign-On Plug-inが動作していないコンピューターでパスワードが変更された。	Single Sign-On Plug-inがインストールされていないコンピューター上でユーザーがプライマリパスワードを変更した後で、Single Sign-On Plug-inがインストールされている別のコンピューターに変更後のプライマリパスワードでログオンした場合、そのユーザーが本人であることを検証する必要があります。

管理者が管理コンソールで指定する認証方法に従って、ユーザーは自分の同一性を証明します。

ユーザーの同一性の検証方法について

Single Sign-Onには、ユーザーの同一性を検証する方法として以下の2つがあります。

- 変更前のパスワード
- セキュリティ用の質問

暗号キーの自動管理機能を使用すると、ユーザーの同一性の検証を省略することもできます。

認証時に使用する同一性の検証方法として、変更前のパスワードとセキュリティ用の質問のどちらかをユーザーが選択できるようにすることができます。このオプションは、ユーザー構成の［データの保護方法（セカンダリ）］ページで設定します。

変更前のパスワード

この方法を使用する場合は、ユーザーがプライマリパスワードを変更するときに、変更前のパスワードの入力が要求されます。これにより、ユーザーの同一性が検証されます。

注意：変更前のパスワード入力を唯一の方法として設定した場合、変更前のパスワードを忘れたユーザーは、システムのロックを解除できなくなります。この場合、そのユーザーのデータを中央ストアおよびすべてのクライアントコンピューターから削除して、ユーザーはアプリケーションへのログオン情報を再登録する必要があります。

セキュリティの質問

プライマリパスワードを変更するユーザーの同一性を、質問ベースの認証方法を使って検証するには、いくつかのセキュリティ用の質問で構成される質問リストを作成して、ユーザーに回答させます。この質問リストは、ユーザーがSingle Sign-On Plug-inを初めて起動したときに表示されます。ユーザーは、質問リストから必要な数の質問を選択し、それに対する回答を登録します。

後でユーザーの同一性検証が必要になると、質問リストが再度表示され、ユーザーは登録した回答を再入力します。質問を作成するときは、その質問に対する回答が、各ユーザー固有であり、本人にとって覚えやすく、ほかの人から推測されにくいものになるように配慮する必要があります。Single Sign-Onにあらかじめ用意されている質問を使用することも、独自の質問を作成することもできます。

ユーザーの同一性検証の省略

重要：ここで説明する暗号キーの自動管理機能は、セキュリティ用の質問や変更前のパスワード入力による再認証方法ほど安全ではありません。
ユーザーの同一性の検証を省略し、自動的にユーザーの暗号キーを取得するには、ユーザー構成の［データの保護方法（セカンダリ）］ページの［同一性を検証せずにネットワーク経由でプライマリのデータ保護方法を自動的に復元する］をクリックします。

この暗号キーの自動管理機能は、キー管理モジュールをインストールし、このオプションを有効にしてユーザー構成を作成すると使用できるようになります。

この方法では、ユーザーの同一性を検証するための認証処理が省かれ、アプリケーションに直ちにアクセスできるようにな

ます。ユーザーがプライマリパスワードを変更しても、Single Sign-On Plug-inによりその変更が自動的に認識され、ユーザーのログオン情報を暗号化しているキーがSingle Sign-Onサービスにより復元されます。

暗号キーの自動管理機能により、ユーザーはより簡単に、そして迅速に、アプリケーションにログオンできるようになります。ただし、質問ベースの認証機能のように、ユーザーだけが知っている「秘密の鍵」がないため、ユーザーの個人情報を不正なアクセスから保護することはできません。この潜在的な問題を避けるには、暗号キーの自動管理機能とアカウントセルフサービス機能を組み合わせて使用します。アカウントセルフサービス機能を有効にすると、ユーザーが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するときに、質問ベースの認証を使用して、ユーザーが自分の同一性を証明できます。

ユーザーによる認証方法の切り替え

Single Sign-Onでは、ユーザーが認証方法を切り替えることができます。再認証方法として固有のセキュリティキーでユーザーパスワードが保護されるため、ユーザーが認証方法を切り替えるたびに同一性の検証を行わずに、ユーザーデータのロックが効率よく解除されます。

ユーザー構成の［データの保護方法］ページで、複数の認証方法を選択できます。

次のユーザーシナリオについて考えてみます。

- コールセンターの監督者が、プライマリのログオン情報（Windowsのユーザー名とパスワード）を使用して自分のコンピューターにログオンします。このコンピューターにはSingle Sign-On Plug-inがインストールされており、パスワードが必要なアプリケーションに監督者がログオンできるようになっています。
- 監督者は、スマートカードとPINを使用してコールセンターの共有コンピューターにログオンし、XenAppサーバーの公開アプリケーションを起動します。このコンピューターではHot Desktopが有効に設定されていて、異なるアカウント間で高速ユーザースイッチを実行できます。

Single Sign-On（Password Manager）Version 4.0および4.1では、監督者がプライマリの認証方法を変更した後、Single Sign-Onを使用する前に自分の同一性を証明する必要がありました。この場合、監督者はユーザー名とパスワード、およびスマートカードとPINという2種類の認証方法を使用します。Single Sign-On（Password Manager）Version 4.0および4.1では、認証方法の変更はセキュリティキーの復元が必要な処理とみなされるため、監督者は自分の同一性を証明する必要がありました。

ユーザーが初めて認証方法を切り替えたときは、新しく使用する認証方法を登録する必要があります。ただし、2回目以降の切り替えでは登録は不要です。つまり、初回以降はキーの復元は必要ありません。

質問ベースの認証の管理

Sep 30, 2015

質問ベースの認証を使用すると、プライマリパスワードの変更、認証方法の切り替え、またはアカウントのロック解除を行ユーザーを安全に認証できるようになります。

質問ベースの認証では、本人だけが知っている情報を入力させることで、ほかのユーザーによる不正アクセスを防ぎます。ただし、質問を作成するときは、本人以外の人が簡単には推量できない回答をユーザーに入力させるように配慮する必要があります。他人が推量することが困難なほど、質問ベースの認証のセキュリティが高くなります。

重要：セルフサービスパスワードリセット機能またはアカウントのロック解除機能を有効にする場合は、ユーザーの同一性を検証する方法として、質問ベースの認証を使用する必要があります。

質問ベースの認証によるユーザーの同一性の検証

セルフサービスパスワードリセット機能またはアカウントのロック解除機能を有効にする場合は、ユーザーの同一性を検証する方法として、質問ベースの認証を使用する必要があります。質問ベースの認証は、ユーザーのプライマリパスワードが変更されたときの2次的なデータの保護方法として使用することもできます。

ユーザーの同一性の検証は、以下のイベントが発生したときに必要になります（管理者が作成するユーザー構成の内容により

- ユーザーが認証方法を変更した。たとえば、スマートカードではなくパスワードを使用するように変更した場合です。
- 管理者がユーザーのプライマリパスワードを変更した。
- アカウントセルフサービス機能を使用して、ユーザーがプライマリパスワードをリセットした。
- アカウントセルフサービス機能を使用して、ユーザーがアカウントのロックを解除した。
- ユーザーが、Single Sign-On Plug-inが動作していないワークステーション上でプライマリパスワードを変更した後、Single Sign-On Plug-inが動作するワークステーションにログオンした。

注：認証方法を変更しても同一性の検証を要求しないように設定することもできます。詳しくは、「*—ユーザーによる認証方法の切り替え*」を参照してください。

質問ベースの認証を管理者が有効に構成している場合、ユーザーはSingle Sign-On Plug-inを初めて起動するときに、セキュリティ用の質問に対する回答を登録する必要があります。ユーザーの同一性の検証が必要になると、ユーザーに質問リストが表示されます。質問リストは、管理者があらかじめ作成しておく質問のセットです。

質問リストに含まれる各質問は、ウィザードの各ページに表示されます。たとえば、5つの質問を含む質問リストを作成した場合は、それらの5つの質問がウィザードの各ページに表示されます。ユーザーは、提示された質問に対して、Single Sign-On Plug-inの初回起動時に登録した回答を正確に入力する必要があります。

ユーザーは、登録したすべての回答を正確に入力することで、本人であることを証明します。ユーザーの同一性が検証されると、Single Sign-On Plug-inが新しいプライマリパスワードを使って暗号キーを再暗号化し、ユーザーのログオン情報（セカンダリパスワード）を格納します。

注意事項

- セキュリティ用の質問を有効にしない場合、ユーザーがプライマリパスワードを変更し、新しいパスワードでログオンするときに、変更前のパスワードを入力するためのダイアログボックスが開きます。認証時に使用する同一性の検証方法をユーザーが選択できるようにすることもできます。このオプションは、ユーザー構成の［データの保護方法（セカンダリ）］ページで設定します。
- セルフサービスパスワードリセット機能を有効にする場合は、［変更前のパスワードを入力させる］オプションを唯一の

ユーザー識別処理方法として設定しないでください。パスワードをリセットするユーザーはパスワードを忘れていることが多いため、変更前のパスワードを入力することができないことがあるためです。この場合、ユーザーは登録済みのログオン情報にアクセスできなくなります。

- 複数の質問を組み合わせて、セキュリティを向上させることができます。
- 質問ベースの認証で使用される質問リストには、デフォルトで4つの質問が追加されています。これら4つの質問をそのまま使用することもできますが、独自の質問および質問グループを作成することをお勧めします。

重要：ユーザーが回答を入力する場合、アルファベットの大文字/小文字の区別（管理者が大文字/小文字の区別を無効にしている場合を除く）、および句読点やスペースの使用も含め、最初に登録した文字列に完全に合致する必要があります。

質問ベースの認証のワークフロー

セキュリティ用の質問は、Single Sign-On Plug-inソフトウェアを配布する前に作成し、有効にしておく必要があります。また、ユーザーがいったん選択した質問は、常に質問リストに表示されるようにする必要があります。ユーザーが選択した質問を管理者が後で変更したり削除したりすると、そのユーザーが同一性を証明できなくなり、自分のログオン情報にアクセスできなくなります。この場合は、ユーザーに回答を再登録させる必要があります。

1. セキュリティ用の質問を作成して、回答の最小文字数および大文字/小文字の区別を指定します。管理者はSingle Sign-Onがサポートするすべての言語用の質問を作成できます。
2. セキュリティ用の質問や質問グループを、質問リストに追加します。複数の質問をグループ化して、そのグループでユーザーが回答しなければならない質問の数を指定することもできます。ユーザーは、回答を登録するときに、自分が覚えやすい質問を選択できます。
3. キー復元用に使用される質問を選択します。
4. これらの質問は、キー復元用のデータを暗号化するために使用されます。ユーザーは、キー復元用の質問に対しても、登録時に入力したとおりに回答する必要があります。
5. 必要に応じて、［ユーザーの回答の文字列を表示しない］チェックボックスをオンにします。これにより、セキュリティ用の質問に対するユーザーの回答を保護できます。このチェックボックスをオンにすると、同一性を検証するときにユーザーが入力する回答の文字列が非表示になります。
   この機能は、Single Sign-On（Password Manager）のVersions 4.6、4.6 with Service Pack 1、4.8、および5.0でサポートされます。

セキュリティ用の質問の考案：安全性と使いやすさの両立

Single Sign-Onには、4つのセキュリティ用の質問があらかじめ設定されています。これらの質問は、Single Sign-Onがサポートするすべての言語（日本語、英語、ドイツ語、フランス語、簡体字中国語、およびスペイン語）で使用できます。ただし、独自の質問を作成して、必要に応じて翻訳しておくことをお勧めします。

他人のユーザーのアカウントを不正使用しようとするユーザーは、正規ユーザーの回答をすべて正確に入力しないと、アカウントにアクセスできません。ただし、過度に多くの質問をユーザーに提示すると、ユーザーが自分のアカウントにアクセスするときの手順が面倒になるという点にも配慮する必要があります。

セキュリティ用の質問を作成するときは、本人以外の人が簡単には推量できない回答、つまり、ブルートフォース攻撃（ツールを使用した総当り攻撃）や辞書攻撃が難しい回答をユーザーに入力させるように配慮する必要があります。他人が推量することが困難なほど、質問ベースの認証のセキュリティが高くなります。

次のような、回答の自由度が高いものほど、優れた質問です。

- ユーザーにより数多くの回答が考えられるような質問
- 他人が回答を推測することがとても困難な質問

使いやすさという観点から、本人にとって回答しやすく、他人が推量できない質問を作成します。次に例を示します。

- 高校時代または大学時代の恩師の名前は何ですか?
- いつかは行きたい夢のリゾートはどこですか?（国名と地名）
- 好きな歌のタイトルとアーティスト名は?
- 好きな本のタイトルと著者名は?
- 好きな絵画のタイトルとアーティスト名、およびそれを観賞した場所は?

これらの質問も、文化的な背景などの条件により、ユーザーの回答に一定の傾向が生じて、複数のユーザーが無意識的に同じ回答を選択する可能性があります。この場合、内部ユーザーによる攻撃の危険性が高くなります。

次の特徴のある質問は、セキュリティ用の質問として不適切です。

- 「何色が好きですか?」など、簡単に回答を推測できる質問
- 「住所はどこですか?」など、他人に知られている可能性、および回答が変わる可能性が高い質問

ユーザーによるセキュリティ用の回答の変更

管理者が介在しなくても、ユーザーは必要なときに自分でセキュリティ用の質問に対する回答を変更できます。

セキュリティ用の質問やアカウントセルフサービス機能が有効なSingle Sign-On環境では、ユーザーはSingle Sign-On Plug-inを使用して、新しい回答を登録できます。

新しい回答が中央ストアに保存されると、古い回答は無効になります。

セキュリティ用の回答を変更するには、セキュリティ用の質問の登録ウィザードを使用します。

管理者は、セキュリティ用の質問の登録ウィザードを公開アプリケーションとしてユーザーに提供できます。

1. XenAppサーバーにSingle Sign-On Plug-inをインストールします。
2. XenAppサーバー上で、QBAEnroll.exeファイルを見つけます。
3. このQBAEnroll.exeファイルをユーザーに公開します。
4. セキュリティ用の質問の登録ウィザードの起動方法および使用方法をユーザーに通知します。

注：Single Sign-On Plug-in Version 4.8を使用している場合は、ログオンマネージャーの [ツール] > [セキュリティ用の質問の登録] を選択してセキュリティ用の質問の登録ウィザードを起動します。この場合、このウィザードの公開アプリケーションを使用する必要はありません。Single Sign-On Plug-in Version 4.6 Service Pack 1およびそれ以前のバージョンのユーザーは、セキュリティ用の質問の登録ウィザードの公開アプリケーションにアクセスできません。

質問の管理

Sep 30, 2015

管理コンソールの［質問ベースの認証］ノードは、ユーザー識別処理、セルフサービスパスワードリセット、およびアカウントのロック解除機能に関連付ける、すべてのセキュリティ用の質問を集中管理するためのノードです。デフォルトの質問リストに独自の質問を追加したり、質問グループを作成して、それを特定のユーザーに割り当てたりすることができます。

- ユーザーがデフォルトの質問に対して回答を登録した後で、管理者が質問文を変更する場合は、その内容について考慮してください。質問の内容を変えずに質問文を編集した場合は、回答の再登録をユーザーに要求する必要はありません。ただし、編集後もユーザーが同じ回答を入力できるように配慮する必要があります。
- ユーザーがセキュリティ用の質問に対する回答を登録した後で、質問リストの質問を追加、削除、または編集すると、ユーザーが登録済みの回答を入力できなくなる場合があります。質問リストの質問を変更した場合は、ユーザーが新しい質問リストに回答を登録できるように、Single Sign-On Plug-inの初回起動時に登録ウィザードが起動するように設定できます。
- 同じ質問を複数の質問グループに追加することができます。質問グループに追加可能な質問の一覧には、既にほかのグループに追加されている質問も含め、すべての質問が表示されます。

以降で参照されている設定にアクセスするには、次の手順に従います。

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 AppCenter］の順に選択します。
2. コンソールツリーで［Single Sign-On］ノード、［ユーザー識別処理］ノードの順に開き、［質問ベースの認証］ノードを選択します。
3. ［操作］メニューから、［質問の管理］を選択します。

セキュリティ用の質問を作成するには

管理者は、異なる言語を使用して、複数の質問を作成できます。また、同じ質問に対して、各国語の翻訳を追加することもできます。Single Sign-On Plug-inでは、そのユーザーのプロファイルで設定されている言語に応じた質問が表示されます。プロファイルで設定されている言語の質問がない場合は、［質問ベースの認証］ページで設定するデフォルトの言語で表示されます。

注：管理者は、異なる言語を使用して、複数の質問を作成できます。また、同じ質問に対して、各国語の翻訳を追加することもできます。Single Sign-On Plug-inでは、そのユーザーのプロファイルで構成されている言語に応じた質問が表示されます。プロファイルで設定されている言語の質問がない場合は、［質問ベースの認証］ページで設定するデフォルトの言語で表示されます。

1. ダイアログボックス左側で［セキュリティ用の質問］をクリックします。
2. ［言語］ボックスの一覧で言語を選択し、［質問の追加］をクリックします。［セキュリティ用の質問］ダイアログボックスが開きます。
3. ［セキュリティ用の質問］ダイアログボックスで、質問を作成します。

重要：既存の質問に翻訳を追加する場合は、［質問の追加］ではなく［編集］をクリックすることに注意してください。［質問の追加］をクリックすると新しい質問が追加され、既存の質問とは関連付けられません。

デフォルトの言語を設定するには

通常、セキュリティ用の質問は、ユーザーが回答を登録したときのユーザープロファイルで設定されている言語で表示されます。プロファイルで設定されている言語の質問がない場合は、管理者が設定するデフォルトの言語で表示されます。

1. ダイアログボックス左側で［質問ベースの認証］をクリックします。
2. ［デフォルトの言語］ボックスの一覧でデフォルトの言語を選択します。

注：Single Sign-On（Password Manager）Versions 4.0および4.1のユーザーをサポートする質問リストを設定するには、［以前のバージョンとの互換性をチェックする］チェックボックスをオンにします。

既存の質問を編集したり翻訳を追加したりするには

ユーザーがセキュリティ用の質問に対する回答を登録した後で、質問リストの質問を追加、削除、または編集すると、ユーザーが登録済みの回答を入力できなくなる場合があります。質問リストの質問を変更した場合は、ユーザーが新しい質問リストに回答を登録できるように、Single Sign-On Plug-inの初回起動時に登録ウィザードが起動するように設定できます。質問の内容を変えずに質問文を編集した場合は、回答の再登録をユーザーに要求する必要はありません。ただし、編集後もユーザーが同じ回答を入力できるように配慮する必要があります。

重要：既存の質問を編集する場合は、質問の意味を変更しないように注意してください。質問の意味を変更すると、既存のユーザーが再認証を受けるときに正しい回答を入力できなくなる可能性があります。［編集］をクリックすると、これに対する注意を促すメッセージが表示されます。

1. ダイアログボックス左側で［セキュリティ用の質問］をクリックします。
2. ［言語］ボックスの一覧で編集する質問の言語を選択します。既存の質問に翻訳を追加する場合は、翻訳先の言語を選択します。
3. 編集または翻訳する質問を選択して、［編集］をクリックします。［セキュリティ用の質問］ダイアログボックスが開きます。
4. ［セキュリティ用の質問］ダイアログボックスで、質問を編集または翻訳します。

セキュリティ用の質問グループを作成するには

必要に応じて、多くのセキュリティ用の質問を作成して、ユーザーに回答させることができます。管理者が質問リストに追加したすべての質問に対して、ユーザーは回答を入力する必要があります。ただし、複数の質問をグループ化して、セキュリティ用の質問グループを作成すると、ユーザーがグループ内の質問を自由に選択して回答を登録できるようになります。この場合、ユーザーが回答しなければならない質問の数は、管理者が指定します。

たとえば、6つの質問で構成される質問グループを作成し、ユーザーが回答しなければならない質問の数を3に設定して、それを質問リストに追加します。ユーザーは、これら6つの質問から3つを自由に選択して、回答を登録します。以降、ユーザーの同一性の検証が必要な状況になると、ユーザーが選択した3つの質問が再提示されます。

1. ダイアログボックス左側で［セキュリティ用の質問］をクリックします。
2. ［グループの追加］をクリックします。
3. ［セキュリティ用の質問グループ］ダイアログボックスで、グループ名、使用する質問、およびユーザーが回答しなければならない質問の数を指定します。

セキュリティ用の質問グループを作成するには

1. ダイアログボックス左側で［セキュリティ用の質問］をクリックします。
2. ［言語］ボックスの一覧で編集する質問グループの言語を選択します。一覧から編集する質問グループを選択して、［編集］をクリックします。［セキュリティ用の質問グループ］ダイアログボックスが開き、グループに追加済みの質問、および追加可能な質問の一覧が表示されます。グループに追加済みの質問はチェックボックスがオンになっています。ここでは、グループ名を変更したり、グループに含まれる質問を追加または削除したり、ユーザーが回答しなければならない質問の数を変更したりできます。

キー復元用の質問を選択するには

質問リストに追加した質問のうち、一部またはすべての質問をキー復元用として選択する必要があります。質問リストが提示されたときに、ユーザーはすべての質問に対する回答を入力しますが、管理者が選択した特定の質問だけが、データの暗号化およびキー復元プロセスで使用されます。

1. ダイアログボックス左側で［キー復元］をクリックします。

2. ユーザーの同一性検証時にキー復元用に使用する質問のチェックボックスをオンにします。
3. ［OK］をクリックして質問および設定を保存します。ユーザーに強制的に回答を再登録させるかどうかを確認するメッセージが表示されます。再登録させる場合は［はい］をクリックします。

回答入力時のセキュリティを有効にするには

この機能は、Single Sign-On（Password Manager）のVersions 4.6、4.6 with Service Pack 1、4.8および5.0でサポートされます。

セキュリティ用の質問を使用したユーザー認証をより安全にするために、ユーザーがテキストボックスに入力する回答の文字列を、アスタリスク（*）で隠すことができます。これにより、ユーザーの回答が第三者に盗み見されることを防ぐことができます。この機能を有効にした場合、ユーザーがセキュリティ用の質問に対する回答を登録するときに、誤入力を避けるために同じ回答を2回入力する必要があります。ユーザーが同一性を証明するために再認証を受けるときは、回答を2回入力する必要はありません。入力した回答に誤りがある場合は、再入力を求めるメッセージが表示されます。

注：Single Sign-On 4.5のPlug-in（Password Managerエージェント）で回答を登録した場合でも、Version 4.8のPlug-inにアップグレードすればこの機能を使用できるようになります。管理者がこの機能を有効にしても、Password Managerエージェント4.5、4.1、および4.0のユーザーに対しては無効です。

1. ダイアログボックス左側で［回答入力時のセキュリティ］をクリックします。
2. ［ユーザーの回答の文字列を表示しない］チェックボックスをオンにします。

質問リストの下位互換性を維持するには

Single Sign-On（Password Manager）Versions 4.0および4.1で使用していたユーザー識別用の質問をサポートするには、Single Sign-Onを互換モードで使用します。また、このモードでは、以前のバージョンで使用していたデフォルトの質問「ユーザー識別用の語句は何ですか?」を継続使用できます。Version 4.0または4.1からアップグレードした場合は、ユーザー識別用の質問およびセルフサービスパスワードリセット用の質問が［質問の管理］ダイアログボックスに表示されます。

重要：Single Sign-Onを新規にインストールした環境では、ユーザー構成を作成したり編集したりするときに、互換モードを有効にしないでください。互換モードを有効にすると、Single Sign-On Plug-inの機能が以前のバージョンのレベルに限定されてしまいます。逆に、以前のバージョンのユーザーをサポートするには、互換モードを有効にしてください。互換モードを有効にしないと、暗号キーの復元やセルフサービスパスワードリセット機能を使用できなくなります。
暗号キーの自動管理機能を使用する場合は、互換モードを有効にしないでください。暗号キーの自動復元では、ユーザー識別用の質問が使用されません。

Version 4.0および4.1のアカウントセルフサービスパスワードリセット機能との互換性を維持するには、この機能で使用される質問が定義されている必要があります。

また、その質問が次のように設定されている必要があります。
- 回答の大文字/小文字を区別しない
- 回答の最小文字数は1
- キー復元に使用しない

下位互換性をチェックするには

質問ベースの認証機能が以前のバージョンのSingle Sign-On（Password Manager）との互換性をサポートしているかどうかをチェックするには、次の手順に従います。
1. ダイアログボックス左側で［質問ベースの認証］をクリックします。
2. ［以前のバージョンとの互換性をチェックする］チェックボックスをオンにして［OK］をクリックします。

現在の設定に対して互換性がチェックされ、問題がある場合はその内容がダイアログボックスに表示されます。

アカウントセルフサービス機能によるプライマリパスワードの管理

Sep 30, 2015

Single Sign-Onのアカウントセルフサービス機能を使用すると、管理者やヘルプデスクの手を煩わせずに、ユーザーが自分でプライマリパスワードをリセットしたり、Windowsドメイン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。組織のニーズに応じて、セルフサービスパスワードリセットとアカウントのロック解除の機能をSingle Sign-On環境に実装できます。

注：Citrix Web Interface環境にアカウントセルフサービス機能を実装する方法については、「*— Web Interface*」を参照してください。

アカウントセルフサービス機能のセキュリティは、質問ベースの認証により保護されます。つまり、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するユーザーは、セキュリティ用の質問に正しく回答できなければなりません。管理者は、Single Sign-Onをセットアップするときにセキュリティ用の質問を作成し選択します。ユーザーは、Single Sign-On Plug-inを初めて起動するとき、またはアカウントセルフサービス機能が設定された後で初めてSingle Sign-On Plug-inを起動するときに、それらの質問に対する回答を登録する必要があります。

ユーザーが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しようとすると、これらの質問がユーザーの画面に表示されます。ユーザーが事前に登録した回答を入力すると、パスワードをリセットしたりロックを解除したりできるようになるため、ヘルプデスクや管理者に問題解決を依頼する必要がなくなります。

重要：セルフサービスパスワードリセット機能とアカウントのロック解除機能を実装するには、質問ベースの認証を設定する必要があります。ユーザーがこれらの機能を使用するには、セキュリティ用の質問に対する回答を登録する必要があります。Single Sign-On環境に質問ベースの認証を設定しない場合、ユーザーはセルフサービスパスワードリセット機能とアカウントのロック解除機能を使用できません。

注意事項

- アカウントセルフサービスモジュールの機能を実装して、ユーザーがプライマリパスワードをリセットしたりWindowsアカウントのロックを解除したりできるように設定できるのは、Active Directory環境でSingle Sign-Onを使用する場合のみです。
- ユーザーがSingle Sign-On Plug-inを使用してアプリケーションのパスワードを変更したり、Single Sign-On Plug-inがインストールされているコンピューターでCtrl + Alt + Delキーを押してプライマリパスワードを変更したりすると、Single Sign-Onによってパスワード変更が自動的に認識されます。
- セルフサービスパスワードリセット機能を有効にする場合は、[変更前のパスワードを入力させる] オプションを唯一のユーザー識別処理方法として設定しないでください。変更前のパスワード入力を唯一の方法として設定した場合、変更前のパスワードを忘れたユーザーは、システムのロックを解除できなくなります。この場合、そのユーザーのデータを中央ストアおよびすべてのユーザーデバイスからリセットつまり削除して、ユーザーはアプリケーションへのログオン情報を再登録する必要があります。

アカウントセルフサービス機能の実装作業の概要

アカウントセルフサービス機能を使用するには、次の作業を行います。

1. セルフサービスモジュールとキー管理モジュールをインストールする。
2. 質問ベースの認証機能を構成する。
3. ユーザー構成を作成し、セルフサービスパスワードリセットまたはアカウントのロック解除のどちらかまたは両方を有効にする。
4. Single Sign-On Plug-inをインストールして構成する。

アカウントセルフサービス機能と暗号キーの自動管理機能の連動

アカウントセルフサービス機能と暗号キーの自動管理機能を組み合わせて使用すると、ユーザーはさらに簡単にSingle Sign-On Plug-inによるシングルサインオン機能を使用できるようになります。たとえば、暗号キーの自動管理機能を有効にすると、ユーザーがプライマリパスワードをリセットした後で、セキュリティ用の質問に回答する必要がありません。ただし、セルフサービスパスワードリセットのプロセスにおいてはセキュリティ用の質問に回答する必要があります。

暗号キーの自動管理機能を実装すると、ユーザーはアカウントのロックを解除したりドメインパスワードをリセットした後で、同一性を検証する必要がなくなります。

セキュリティ用の質問を初期化するには

Windowsアカウントがロックされたユーザーがセキュリティ用の質問の回答を覚えていない場合は、そのユーザーが登録した回答を管理コンソールで初期化する必要があります。これにより、ユーザーが次にSingle Sign-On Plug-inを起動したときに、アカウントセルフサービス機能への登録ウィザードが起動します。ユーザーは、このウィザードの手順に従って、セキュリティ用の質問に対する回答を再登録できます。

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 AppCenter］の順に選択します。
2. コンソールツリーで［Single Sign-On］ノード、［ユーザー識別処理］ノードの順に開き、［質問ベースの認証］ノードを選択します。
3. ［操作］メニューから、［そのほかのタスク］［ユーザーの回答を削除する］の順に選択します。
4. ［ユーザーの選択］ダイアログボックスにユーザーまたはユーザーグループの名前を入力します。

ユーザーエクスペリエンス

Single Sign-OnサービスとSingle Sign-On Plug-inをインストールおよび構成すると、アカウントセルフサービスモジュールによって、Windowsにログオンしたりコンピューターのロックを解除したりするためのダイアログボックスに［アカウントセルフサービス］ボタンが追加されます。

ユーザーがアカウントセルフサービス機能を使用するには、まずプライマリドメインアカウントでログオンし、セキュリティ用の質問に対する回答を登録する必要があります。登録が完了すると、セルフサービスパスワードリセット機能とアカウントのロック解除機能を使用できるようになります。

暗号キーの自動管理機能を実装すると、ユーザーはアカウントのロックを解除したりドメインパスワードをリセットした後で、同一性を検証する必要がなくなります。

アカウントセルフサービス

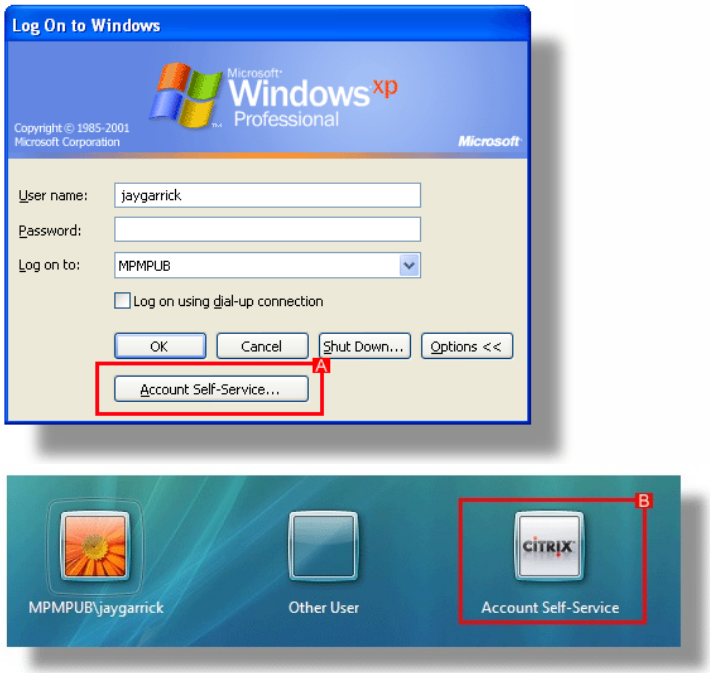
Sep 30, 2015

Single Sign-Onでは、ほかのシングルサインオン機能を無効にしたまま、アカウントセルフサービス機能（セルフサービスパスワードリセットおよびセルフサービスロック解除）だけを導入することもできます。

Single Sign-Onのアカウントセルフサービス機能を使用すると、ユーザーがアカウントに関する以下の問題を自分で解決できるようになるため、ヘルプデスクへの負担が軽減されます。

- Microsoft Windowsドメインのパスワードを変更する
- Windowsドメインアカウントのロックを解除する

アカウントセルフサービス機能では、ユーザーの同一性を検証するための質問事項（セキュリティ用の質問）を管理者が作成します。管理者が質問ベースの認証を有効にして、アカウントセルフサービス機能を設定したら、ユーザーはこれらの質問に対する回答を入力することで、サービスに登録します。この処理が完了すると、ユーザーの［Windowsへのログオン］ダイアログボックス（下図［A］）や、Microsoft Windows Vistaの場合は［ようこそ］画面（下図［B］）に［アカウントセルフサービス］ボタンが追加されます。



質問に対する回答をユーザーに再登録させるには、以下のいずれかを行います。

- 特定ユーザーの質問データを削除する。
- すべてのユーザーに回答を再登録させる。
- 既存の質問リストを変更する。

また、登録済みの回答を変更するために、ユーザーが再登録処理を開始することもできます。

以降のトピックでは、アカウントセルフサービス機能だけをユーザーに提供する場合のSingle Sign-Onのインストールおよび構成について説明します。

注：UPN（ユーザープリンシパル名。username@domain.comなど）を使用したログオン情報は、アカウントセルフサービス機能でサポートされません。

ライセンスを使用する

Single Sign-Onのライセンスは、質問ベースの認証に対してユーザーが回答を登録するときに消費されます。同時接続ユーザーライセンスを使用すると、組織内でのライセンス使用が効率化されます。同時接続ユーザーライセンスでは、ユーザーが再登録処理を完了すると、ライセンスがライセンスプールに返却されます。指定ユーザーライセンスでは、再登録処理の完了後、そのユーザーがライセンスを使用していなくても最低2日間はライセンスが返却されません。

1つのSingle Sign-Onライセンスで多くのユーザーがアカウントセルフサービス機能を使用できるように、アカウントセルフサービス機能のみを使用する環境ではライセンスに特定の比率が適用されます。同時接続ユーザーライセンスでの比率は10:1で、100ライセンスで1,000ユーザーがアカウントセルフサービス機能を使用できます。指定ユーザーライセンスでの比率は5で、100ライセンスで500ユーザーがアカウントセルフサービス機能を使用できます。

同時接続ユーザーライセンスをオフラインで使用できるようにするには

1. ユーザー構成の作成
2. ユーザー設定ウィザードの［ライセンスの設定］ページで、［同時接続ユーザーライセンス（Enterprise EditionとPlatinum Editionのみ）］を選択します。
3. ［オフラインでのライセンス使用を許可する］を選択し、ライセンスのチェックアウト期間を指定します。
4. ユーザー構成の作成を完了します。

同時接続ユーザーライセンスで非接続期間を有効にすると、そのユーザー構成が割り当てられたユーザーのライセンスは、指定ユーザーライセンスと同じように、各コンピューターではなく各ユーザーに割り当てられます。これにより、モバイルやオフラインで作業するユーザーがこのモデルのライセンスを使用できるようになります。

重要：ユーザーのコンピューター上にインストールされたSingle Sign-On Plug-inを使用してCitrix XenApp, Platinum Edition環境で公開されているアプリケーションにアクセスする場合、そのSingle Sign-On Plug-in用に個別のライセンスをインストールする必要はありません。

アカウントセルフサービス機能専用のユーザー構成を作成するには

アカウントセルフサービス機能のみを使用し、ほかのSingle Sign-On機能を使用しない場合は、以下の手順でユーザー構成を作成します。

注：シングルサインオン機能は使用しないため、アプリケーション定義はこの手順に含まれません。アプリケーションへのシングルサインオン機能が必要なユーザーを、ここで作成するユーザー構成に含めないでください。

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］ノードを選択します。操作ペインの［ユーザー設定の追加］をクリックします。ユーザー設定ウィザードが起動します。
3. ［ユーザー設定の名前］ページで、以下の操作を行います。
   1. ［名前］ボックスに、作成するユーザー構成の名前を入力します。
   2. ［ユーザー設定の割り当て］では、ユーザー構成を適用するActive Directory階層（組織単位または個々のユーザー）またはActive Directoryグループを指定します。
4. ［製品エディションの選択］ページでは、［Single Sign-on Enterprise］を選択します。
5. ［アプリケーションの選択］ページでは、そのまま［次へ］をクリックします。
6. ［Plug-inの動作の設定］ページでは、以下のチェックボックスをオフにします。
   - ログオン情報を登録するためのダイアログボックスをユーザーに表示する
   - 定義済みのフォームに対する自動処理を有効にする

   ［Advanced Settings］をクリックします。
7. ［Single Sign-On Plug-inの詳細設定］ダイアログボックスで、以下の操作を行います。

- ［アプリケーションのサポート］ページで、［クライアント側のアプリケーション定義を検出する］チェックボックスをオフにします。

［OK］をクリックして［Single Sign-On Plug-inの詳細設定］ダイアログボックスを閉じ、［次へ］をクリックします。

8. ［ライセンスの設定］ページの［ライセンスサーバーのアドレス］で、ライセンスサーバーの名前およびポート番号を指定します。
［ライセンスモデル］で、［指定ユーザーライセンス］または［同時接続ユーザーライセンス］をクリックします。

注：同時接続ユーザーライセンスを使用すると、組織内でのライセンス使用が効率化されます。同時接続ユーザーライセンスでは、ユーザーが再登録処理を完了すると、ライセンスがライセンスプールに返却されます。指定ユーザーライセンスでは、再登録処理の完了後、そのユーザーがライセンスを使用していなくても最低2日間はライセンスが返却されません。

9. データ保護方法の選択］ページでは、ユーザーのログオン情報を暗号化して保護するための方法について設定します。
10. ［もう1つのデータ保護方法（セカンダリ）の設定］ページでは、［同一性の検証方法（変更前のパスワードまたはセキュリティ用の質問）をユーザーに選択させる］をクリックします。
11. ［アカウントセルフサービス機能の設定］ページでは、必要に応じて以下のチェックボックスをオンにします。
    - プライマリパスワードのリセットを許可する
    - ロックされたアカウントの解除を許可する
12. ［サービスモジュールの指定］>［キー管理モジュール］ページでは、サービスのアドレスを指定します。
13. このまま追加の変更を行わずに、ウィザードを完了します。

Single Sign-On Plug-inを実行するコンピューターを準備する

注：ここでは、Single Sign-On Plug-inを実行するコンピューターを効率的かつ確実に準備できるように、スクリプトを使用する方法について説明します。
ユーザーのコンピューターにSingle Sign-On Plug-inをインストールしたら、管理者はssoShell.exeのショートカットおよび［スタート］メニューを変更して、ユーザーがアカウントセルフサービス機能にのみアクセスできるようにする必要があります。

Single Sign-On Plug-inをインストールすると、ssoShell.exeショートカットに以下のコマンドラインオプションが設定されます。

/background

このオプションを、以下のように変更する必要があります。

/qbaenroll /noforceqbaenroll

これにより、ユーザーがこのコンピューターにログオンしたときに、中央ストアとの同期処理が実行され、ユーザーの質問ベースの認証の登録状態がチェックされます。ユーザーの登録処理が完了している場合は、登録用のメッセージは表示されません。以下のいずれかの場合は、登録用のメッセージがユーザーに表示されます。

- ユーザーの登録処理が完了していない。
- ユーザーの回答が管理者により削除されている。
- 質問リストが管理者により変更されている。

中央ストアとの同期処理が完了し、必要に応じて登録処理が開始されると、ssoShell.exeが自動的に終了します。

Single Sign-onのssoShell.exeショートカットを更新するには

デスクトップの場合

1. Windows Vistaでは、Windowsエクスプローラーで%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Startupを開きます。

それ以外のWindowsでは、Windowsエクスプローラーで%SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Startupを開きます。

2. StartupフォルダーのSingle Sign-on Background Processを選択し、［ファイル」>［プロパティ］を選択します。
3. ［Single Sign-on Background Processのプロパティ］ダイアログボックスで、［リンク先］ボックスに入力されている/backgroundを削除します。
4. ［リンク先］ボックスに入力されている文字列の末尾に、「/qbaenroll /noforceqbaenroll」と入力します。

サーバーの場合
注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、Citrixでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。
1. レジストリエディターを起動して、HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\windows NT\CurrentVersion\Winlogon\AppSetupを開きます。
2. サブキーのデフォルトのエントリをダブルクリックして、[文字列の編集］ダイアログボックスを開きます。
3. ［値のデータ］ボックスで、
次の%SystemDrive%\Citrix\Metaframe Password Manager\WTS\SSOlauncher.exe /no ssoshutdown

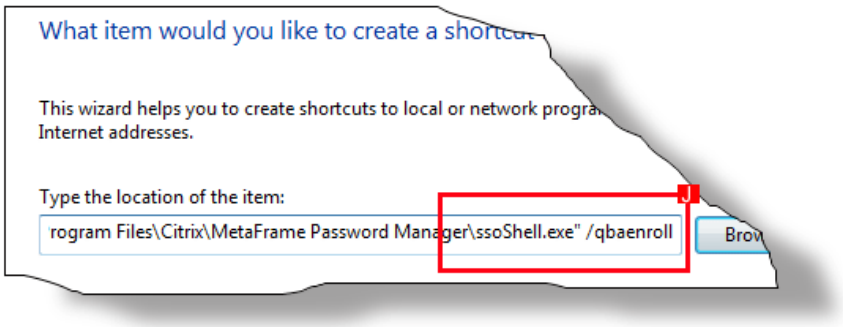
を%SystemDrive%\Citrix\Metaframe Password Manager\ssoshell.exe /qbaenroll /noforceqbaenrollに変更します。

これにより、ssoShell.exeがアカウントセルフサービス機能専用に変更されました。

アカウントセルフサービス機能への登録ショートカットを［スタート］メニューに追加するには

アカウントセルフサービス機能への登録処理を行うためのショートカットを[スタート］メニューに追加して、ユーザーが自分で登録処理を開始できるようにします。これにより、初回ログオン時の登録処理で回答を入力しなかったユーザーや、登録済みの回答を変更するユーザーが自分で登録処理を開始できるため、サービスデスクへの問い合わせが減ります。
1. Windows Vistaの場合：Windowsエクスプローラーで%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Citrixを開きます。
それ以外のWindowsの場合：Windowsエクスプローラーで%SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Citrixを開きます。

2. ［ファイル］メニューから、［新規作成］>［ショートカット］の順に選択します。ショートカットの作成ウィザードが起動します。
3. ［参照］をクリックします。
4. %InstallationDirectory%\Program Files\Citrix\Metaframe Password ManagerフォルダーのssoShell.exeを選択し、［OK］をクリックします。［ファイルまたはフォルダーの参照］ダイアログボックスが閉じ、ssoShell.exeのパスが［項目の場所を入力してください］ボックスに追加されます。
5. ［項目の場所を入力してください］ボックスで、「ssoShell.exe」の後に挿入ポイントを置き、スペースの後に「/qbaenroll」と入力します（下図［J］）。



6. ［次へ］をクリックします。
7. 「Citrix Account Self-Service Registration」と入力し、［完了］をクリックします。

［スタート］>［すべてのプログラム］>［Citrix］にショートカットが追加されます。

Single Sign-Onのショートカットを削除するには

Single Sign-On Plug-inをインストールすると、［スタート］メニューにショートカットが追加されます。アカウントセルフサービス機能のみを使用するユーザーがこのショートカットを選択すると、ssoShell.exeが起動し、質問ベースの認証に変更がない場合はそのまま終了します。これにより、ユーザーが混乱し、サポートデスクに問い合わせるかもしれません。これを避けるために、［スタート］メニューからこのショートカットを削除します。

1. Windows Vistaの場合：Windowsエクスプローラーで%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Citrixを開きます。
   それ以外のWindowsの場合：Windowsエクスプローラーで%SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Citrixを開きます。

2. Single Sign-onのショートカットを削除します。

これにより、ユーザーの［スタート］メニューからショートカットが削除されます。

Single Sign-On Plug-inのショートカットをスタートアップフォルダーから削除するには

ユーザーがコンピューターにログオンするたびにSingle Sign-On Plug-inが起動しないように、ショートカットを削除します。これにより、ライセンスが意図せず使用されることを回避できます。

1. Windowsエクスプローラで、%SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Startupを開きます。
2. Single Sign-on Plug-in Background Processを削除します。
   注：Citrix XenAppサーバーやターミナルサービス環境にSingle Sign-On Plug-inがインストールされている場合は、HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\Windows NT\CurrentVersion\Winlogon\AppSetupを編集して、Password ManagerまたはSingle Sign-onへの参照を削除する必要があります。

これにより、コンピューターへのログオン時にSingle Sign-On Plug-inが起動しなくなります。

プロビジョニングによるログオン情報入力の自動化

Sep 30, 2015

プロビジョニングモジュール（プロビジョニング）を使用すると、ユーザー構成に定義されるアプリケーションのログオン情報を一括操作できます。Single Sign-Onのプロビジョニング機能では、ユーザーデータの管理を自動化して、複数のユーザーに適用できます。管理者が新しいアプリケーションを環境に導入する場合、そのアプリケーションのアプリケーション定義を作成し、そのアプリケーションを使用するユーザー全員のログオン情報をプロビジョニング機能を使って追加できます。

プロビジョニングタスクの概要

中央ストアに格納されている、ユーザー構成に関連付けられたアプリケーションのログオン情報を操作するには、以下の作業を行う必要があります。

1. Single Sign-Onサービスのプロビジョニングモジュールをインストールする。
2. プロビジョニングサービスを使用するユーザー構成を作成する。
3. プロビジョニングテンプレートを作成する。
4. ユーザーのログオン情報データをテンプレートに入力し、実行するコマンドを選択する。
5. プロビジョニングコマンドを実行する。

重要：ログオン情報のプロビジョニングに使用するXMLファイルには、機密性の高いユーザー情報が記述されます。プロビジョニングが完了したら、このファイルを安全な場所に保管するか、削除することをお勧めします。
プロビジョニング機能で中央ストアのログオン情報を追加、削除、または変更したら、さらに必要な管理作業はありません。ユーザーがSingle Sign-On Plug-inを起動すると、ログオン情報の変更が自動的に認識されます。

中央ストアに格納されているログオン情報の追加、変更、または削除には、大量のシステムリソースが消費されることがあります。プロビジョニングは、サーバーの負荷が低い時間帯に行うことをお勧めします。

Provisioning SDK

ログオン情報の操作対象のユーザーが多い場合は、Provisioning Software Development Kit（SDK）を使用することをお勧めします。このSDKでは、Single Sign-Onサービスのプロビジョニングモジュールをインストールすると利用可能になるAPI（Application Programming Interface）の詳細が提供されます。Provisioning SDKのサンプルコードを参照しながら、独自のプロビジョニングスクリプトを作成できます。

プロビジョニングテンプレートの作成

以下の手順を実行するには、アプリケーション定義、アプリケーショングループ、パスワードポリシー（オプションのパスワード共有グループも含む）などを含むユーザー定義を作成して、プロビジョニングを有効にしておく必要があります。

プロビジョニングテンプレートは、選択したユーザー構成に関連付けられているアプリケーションの以下の情報を含むXML文書です。

- アプリケーショングループ
- アプリケーション定義名とGUID（Globally Unique Identifier：グローバル一意識別子）
- ユーザー名やパスワードなどのユーザー情報

このテンプレートには追加、削除、変更の各コマンドも含まれており、これらを編集して管理コンソールで使用できます。

このテンプレートには、コマンドのサンプルと選択したユーザー構成の特定の情報が含まれます。

プロビジョニングテンプレートを作成するには

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］ノードを選択します。
3. 既存のユーザー構成を選択します。
4. ［操作］メニューから、［プロビジョニングテンプレートの作成］をクリックします。
5. ［プロビジョニングテンプレートの作成］ダイアログボックスで、テンプレート名を入力します。

プロビジョニングを実行するには

Single Sign-On管理コンソールからプロビジョニングを実行すると、各コマンド構文の検証、コマンドの実行、中央ストアへのデータの追加または変更など、XMLファイルに定義されているプロビジョニングタスクが実行されます。

注意：プロビジョニング処理が完全に停止または完了するまで、実行画面を閉じないでください。この画面を閉じても、プロビジョニング処理は停止しません。この画面を閉じると、実行中の処理の情報を確認したり、処理を中止したりできなくなります。

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 AppCenter］の順に選択します。
2. ［Single Sign-On］ノードを開き、［ユーザー設定］を開きます。
3. ユーザー構成またはユーザー構成のアプリケーショングループを選択します。
4. ［操作］メニューから、［プロビジョニングの実行］を選択します。 プロビジョニングウィザードが起動します。
5. ［Next］をクリックします。
6. ファイル名を入力するか、［参照］をクリックしてプロビジョニングXMLファイルを指定し、［次へ］をクリックします。 Single Sign-OnによりXMLファイルが検証されます。
   - 構文エラーが検出されない場合は、実行されるプロビジョニングコマンドの内容が表示されます。この情報はファイルに保存できます。
   - 構文エラーなどのエラーが検出された場合は、エラーログが表示されます。この情報はファイルに保存できます。［キャンセル］をクリックして、プロビジョニングウィザードを閉じます。
7. エラーが検出されなかった場合は、［次へ］をクリックしてファイルのコマンドを実行します。 プロビジョニングにより中央ストアの情報が変更されます。エラーが発生すると、その内容が表示されます。プロビジョニング処理を中止するには、［中止］をクリックします。実行中のデータセクションの処理が終了した時点で、プロビジョニングが中止されます。デフォルトでは、データは50コード行単位で処理されます。

ウィザードを終了するときに、プロビジョニングの処理結果をファイルに保存することができます。

プロビジョニング処理の設定

注意：次の手順では、レジストリを変更する必要があります。レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの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。システムレジストリは、変更する前に必ずバックアップを作成してください。
ログオン情報のプロビジョニング機能には、デフォルトで、50コマンドずつのバッチ処理と100,000ミリ秒のタイムアウトが設定されています。これらのデフォルト設定を変更するには、以下のレジストリ値を変更します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Console\Provisioning\BatchSize

種類：REG_DWORD

この値を空白にした場合のデフォルト値：50

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Console\Provisioning\ServiceTimeout

種類：REG_DWORD

この値を空白にした場合のデフォルト値：100000

プロビジョニングテンプレートの編集

Sep 30, 2015

作成したテンプレートを編集するには、テキストエディターかXMLファイルエディターを使用します。このテンプレートは、プロビジョニング情報交換におけるXMLベースの標準であるSPML（Service Provisioning Markup Language）に基づいて作成されます。このため、各SPMLタグや要素（タグなど）がXML構文の規則に従って正しく記述されている必要があります。たとえば、コメント文字（!--や--）を削除するときに余分な山かっこ（<や>）を削除し忘れると、そのファイルによるプロビジョニング処理に問題が生じることがあります。XML構文について詳しくは、W3Cのwebサイト（http://www.w3.org/）を参照してください。必要に応じて、コメント文字（!--および--）を削除します。

テンプレートの出力例

作成されるテンプレートには、以下のタグとコマンドが含まれます。

- ：テンプレートを作成した管理者についての情報
- ：ユーザー構成にあるアプリケーションに対する追加コマンド
- ：ユーザー構成にあるアプリケーションに対する編集コマンド

XMLファイルの末尾近くには、選択したユーザー構成固有の情報が含まれており、これをコピーしてプロビジョニングに使用できます。次に例を示します。

たとえば、タグとタグの間のユーザー情報をコピーし、コメント文字を削除して、追加するログオン情報に応じて編集できます。

注：上記の例にあるは、テンプレートを作成したユーザーのドメインとユーザー名です。この情報はコメントアウトするか、テンプレートに残したくない場合は削除できます。

cpm-provisionタグ

使用するタグとコマンドは、タグ（XMLファイルの70行目あたり）の中に挿入する必要があります。

タグとコマンドをここに挿入します

userタグ

アプリケーションへのログオン情報をプロビジョニングする各ユーザーのドメインとユーザー名を追加するには、タグを使用します。プロビジョニング対象の各ユーザーにつき、タグを1つ使用する必要があります。また、各タグには、そのユーザーアカウントに対して実行するコマンドも含まれます。

コマンドの構文は、以下のとおりです。

yourDomain\usrid"> <command>
各項目の意味は次のとおりです。

yourDomain	対象ユーザーのドメイン名
userid	対象ユーザーのユーザー名
-command	このユーザーに対して実行するコマンド • • • • • •

addコマンド

コマンドを使用すると、ユーザー構成に関連付けられているアプリケーション用のログオン情報（ユーザー名やパスワードなど）を追加できます。

コマンドの構文は、以下のとおりです。

%APPNAME%">%APPGUID% longDescription%CREDENTIALNAME% longDescription %APPNAME% hidden description userid password %LABELTEXT%">custom-field1 %LABELTEXT%">custor
各項目の意味は次のとおりです。

	必須です。要素とその属性は、通常テンプレートを作成するときに自動的に生成されます。 name=属性は必須ではありません。 • %APPNAME%は、選択したユーザー構成にあるアプリケーション定義の名前です。 • %APPGUID%はアプリケーションのGUIDで、それと同じIDである必要があります。
	必須です。要素とその属性は、通常自動的に生成されます。 • %CREDENTIALNAME%は、アプリケーション定義にあるアプリケーションの名前です。
	オプションです。ユーザー構成の説明を入力します。
	オプションです。ここには任意の文字列を入力します。
	必須です。useridは追加するユーザーのユーザー名です。
	必須です。passwordは追加するユーザーのパスワードです。

	ユーザーがドメインを入力するフィールドなど、ログオン情報用の追加フィールドが必要な場合は必須です。アプリケーションに必要なカスタムフィールドを必要なだけ使用できます。

modifyコマンド

コマンドを使用すると、ユーザー構成に関連付けられているアプリケーション用のログオン情報（ユーザー名やパスワードなど）を変更できます。

重要：このコマンドを実行するには、ユーザーのログオン情報が必要です。コマンドを使用する前に、コマンドを使ってユーザーのログオン情報を取得できます。
コマンドのセクションには、変更対象の要素のみを記述します。
- 値を変更しない場合は、該当する行を削除します。たとえば、アプリケーション名をそのまま使用する場合は、要素の行を削除します。
- 値を変更する場合は、テンプレートに値を指定します。たとえば、アプリケーション名を変更する場合は、要素に新しいアプリケーション名を指定します。
- 値を指定せずに要素を指定すると、値は消去されます。たとえば、と記述すると、現在の説明が削除されます。

コマンドの構文は、以下のとおりです。

%CREDENTIAL-ID% %CREDENTIALNAME% longDescription %APPNAME% hidden description userid password %LABELTEXT%"> custom-field1 %LABELTEXT%">custom-field2
各項目の意味は次のとおりです。

	必須です。ユーザーのログオン情報のGUID値である%CREDENTIAL-ID%は、コマンドによって返される値と一致する必要があります。
	オプションです。要素とその属性は、通常自動的に生成されます。 ● %CREDENTIALNAME%は、アプリケーション定義にあるアプリケーションの名前です。
	オプションです。ユーザー構成の説明を入力します。
	オプションです。ここには任意の文字列を入力します。
	必須です。useridは変更するユーザーのユーザー名です。
	必須です。passwordは変更するユーザーのパスワードです。
	ユーザーがドメインを入力するフィールドなど、ログオン情報用の追加フィールドが必要な場合は必須です。アプリケーションに必要なカスタムフィールドを必要なだけ使用できます。

deleteコマンド

コマンドを使用すると、ユーザー構成に関連付けられているアプリケーション用のログオン情報（ユーザー名やパスワードなど）を削除できます。

重要：このコマンドを実行するには、ユーザーのログオン情報が必要です。コマンドを使用する前に、コマンドを使ってユーザーのログオン情報を取得できます。
コマンドの構文は、以下のとおりです。

yourDomain\userid"> %CREDENTIAL-ID%
各項目の意味は次のとおりです。

yourDomain	ユーザーのドメイン名。
userid	ユーザーのユーザー名。
	必須です。ユーザーのログオン情報のGUID値である%CREDENTIAL-ID%は、コマンドによって返される値と一致する必要があります。

removeコマンド

コマンドを使用すると、中央ストアからユーザーデータを削除できます。このコマンドは退職した社員のデータなど、現在の環境からそのユーザーのSingle Sign-On情報を削除する場合に使用します。ユーザーのコンピューター上にあるローカルのログオン情報ストアは、管理者またはオペレーターによって明示的に削除されるまで変更されません。

コマンドの構文は、以下のとおりです。

yourDomain\userid">
各項目の意味は次のとおりです。

yourDomain	ユーザーのドメイン名。
userid	ユーザーのユーザー名。

注：このコマンドは、Single Sign-On管理コンソールの [中央ストアからのユーザーデータの削除] タスクと同様に機能します。

resetコマンド

コマンドを使用すると、中央ストアのユーザー情報をリセットして、選択したユーザーを初期状態に戻すことができます。Active Directory用以外の中央ストアではユーザーフォルダーはそのまま残りますが、ユーザーデータ（ログオン情報、登録時の質問と回答など）はすべて削除されます。Active Directory用の中央ストアでは、ユーザーデータは削除され、データがリセットされたことを示すフラグがユーザーに付けられます。

コマンドの構文は、以下のとおりです。

yourDomain\userid">
各項目の意味は次のとおりです。

yourDomain	ユーザーのドメイン名。
userid	ユーザーのユーザー名。

注：このコマンドは、Single Sign-On管理コンソールの [ユーザーデータのリセット] タスクと同様に機能します。

list-credentialsコマンド

コマンドを使用すると、ユーザー構成に関連付けられている各アプリケーションへのログオン情報を取得して、ウィザードの画面で確認したりファイルに保存したりできます。コマンドとコマンドでは、%CREDENTIAL-ID%パラメーターの値として、取得したログオン情報のGUIDを使用する必要があります。

このコマンドが取得する識別番号は、634EE015-10C2-4ed2-80F5-75CCA9AA5C11などの、ログオン情報のGUIDです。

コマンドの構文は、以下のとおりです。

yourDomain\userid">
各項目の意味は次のとおりです。

yourDomain	ユーザーのドメイン名。
userid	ユーザーのユーザー名。

Hot Desktop：ユーザーのための共有デスクトップ環境

Sep 30, 2015

Hot Desktopを使用すると、Single Sign-Onによるシングルサインオン機能に加えて、ユーザーセッションを高速に切り替えることができるようになります。Hot Desktopは、デフォルトではインストールされません。Single Sign-On Plug-inのインストール時に選択してインストールする必要があります。また、インストール済みのSingle Sign-On Plug-inに、後からHot Desktop機能を追加することもできます。ただし、Hot Desktopを実装する前に、システム環境および業務上の要件に従って、Hot Desktopを構成する必要があります。

Hot Desktopは、以下のオペレーティングシステムのみをサポートしています。

- Microsoft Windows XP Professional Service Pack 2 - 32ビット
- Microsoft Windows XP Embedded

Hot Desktopは、64ビットのオペレーティングシステムでは使用できません。

Citrix Receiverを使用してSingle Sign-Onをインストールする場合は、Hot Desktop機能を使用できません。

Single Sign-OnのHot Desktop機能は、ユーザーが効率よく安全にワークステーションを共有できるようにするための機能です。Hot Desktopによって標準のWindows環境が拡張され、ユーザーは次の操作ができるようになります。

- 標準のGINA対話型ログオンダイアログボックスを使用して、すばやくWindowsにログオンする。
- ユーザーのSingle Sign-Onログオン情報を使用して、対話型ユーザーシェルでシングルサインオンが有効なアプリケーションを実行する。
- Hot Desktopワークステーションからログオフし、ほかのユーザーがアプリケーションを実行できるようにする。

Hot Desktopの設定に必要な作業

Hot Desktop機能を導入する前に、以下の作業を行う必要があります。

- Hot Desktop共有アカウントを作成する。
- ユーザー構成を作成し、Hot Desktopのユーザーエクスペリエンスに関するHot Desktop特有の設定を指定する。
- Hot Desktopの開始時および終了時の動作を定義する。次の項目を定義する必要があります。
  - 開始時に起動するアプリケーションと、Hot DesktopユーザーまたはHot Desktop共有アカウントのログオン情報とアクセス許可を使用するアプリケーションを決定する。
  - ユーザーがHot Desktopセッションからログオフしても永続的に実行されるアプリケーションと、ログオフすると終了するアプリケーションを決定する。後者については、クリーンアップ用のスクリプトまたはアプリケーションが実行されるように設定してセッションごとにユーザー情報を削除することもできます。

Hot Desktopを構成して有効にするには、次の作業を行います。

1. Hot Desktopを実行する各ワークステーションで使用できる、Hot Desktop共有アカウントを作成する。
2. Hot Desktop環境で実行する、シングルサインオン用のアプリケーションを決定する。
3. Hot Desktopでアプリケーションを実行する方法を決定し、Hot Desktopユーザー環境を構成する。
4. ユーザー構成を作成または変更し、Hot Desktopオプションを選択する。
5. Hot Desktop機能を有効にしてSingle Sign-On Plug-inをインストールする。
6. 必要な場合はHot Desktop機能をアンインストールする。

Hot Desktopの開始と終了プロセス

Hot Desktopセッションの開始時および終了時には、次のイベントが発生します。Hot Desktop機能では、ワークステーションが起動すると、自動的に共有アカウントでログオンして、共有デスクトップモードになります。

注：セッションが終了してもHot Desktop共有アカウントは常にアクティブになっていることに注意してください。ユーザーには、共有アカウントを終了できる権限はありません。

1. Hot Desktopのユーザーがワークステーションにログオンし、ユーザー名とパスワードを入力するか、スマートカードなどの認証システムを使って認証を受けます。
2. ユーザーが認証されると、Hot Desktopセッションが開始します。
3. Single Sign-On Plug-inが起動して、ローカルストアと中央ストアのデータを同期します。これにより、ユーザーが最新のアプリケーション定義、パスワードポリシー、およびSingle Sign-On設定を使用できるようになります。
4. session.xmlファイルが読み込まれ、指定されているアプリケーションがHot Desktop共有アカウントまたはHot Desktopユーザーアカウントで起動します。ローカルアプリケーションを起動したり、XenAppで公開されているリモートアプリケーションを起動したりできます。ユーザーがアプリケーションを使って必要な作業を行います。
5. Hot Desktopユーザーがログオフします。
   注：ワークステーションがアイドル状態になると、Hot Desktopセッションのタイムアウトが起算されます。セッションのタイムアウトを指定するには、管理コンソールを使用します。タイムアウトとして指定した時間が経過すると、まずワークステーションがロックされ、次にHot Desktopセッションが終了します。
6. Hot Desktopセッションの終了時には、process.xmlファイルの設定に従って、アプリケーションが実行状態のまま維持されたり、終了したりします。
7. Single Sign-On Plug-inが終了します。
8. session.xmlファイルに指定されている終了スクリプトが実行されます。
9. Hot Desktopセッションが終了します。

Hot Desktopの開始時のトラブルシューティング

Hot Desktopが有効なワークステーションにユーザーがログオンするとき、Single Sign-On Plug-inが完全に起動する前にprocess.xmlファイルに指定されている開始スクリプトが実行される場合があります。

Hot Desktopセッションでは、Single Sign-On Plug-inが起動するまで30秒間だけ待機し、その後で開始スクリプトが実行されます。30秒経過すると、Single Sign-On Plug-inが完全に起動していなくても開始スクリプトが実行されます。

このような状況は、ユーザーが初めてSingle Sign-OnPlug-inを起動して、ログオン情報の一括設定を行ったり、セキュリティ用の質問に対する回答を登録したりしなければならない場合に多く発生します。たとえば、次のような状況が考えられます。

1. Single Sign-On Plug-inを実行するワークステーションにユーザーがログオンします。
2. 一括設定リストに含まれるアプリケーションのログオン情報、またはセキュリティ用の質問に対する回答の登録を求めるメッセージがユーザーに表示されます。ユーザーがこれらの作業を行っている間に30秒が経過し、session.xmlファイルの開始スクリプトが実行されます。
3. 開始スクリプトによりウィンドウが開いたり閉じたりするために、入力フォーカスがユーザーの意図しないウィンドウに移動してしまう場合があります。
4. 開始スクリプトが終了したときに、「エラーが発生しました。詳しくはイベントログを参照してください」という内容のエラーメッセージが表示されます。

この動作によってユーザーが戸惑ったりいらだちを感じたりすることがありますが、ユーザーのデータ、作業環境、およびSingle Sign-On自体に問題が起きることはありません。

Hot Desktopセッションを初めて使用するユーザーには、このエラーメッセージが表示された後にログオン情報やセキュリティ用の質問の回答を登録するように指示してください。ユーザーは、エラーメッセージのダイアログボックスを閉じてか

ら、登録作業を完了できます。

メッセージのダイアログボックスを閉じて登録作業を完了した後で、session.xmlファイルに指定されているアプリケーション
が起動しない場合は、ユーザーにいったんログオフしてからログオンし直すように指示します。これにより、登録が完了した
状態になり、プロセスに遅延が発生しないため、Hot Desktopの開始スクリプトが中断なく再実行されます。

Hot Desktop共有アカウントの作成

Hot Desktopを実行するワークステーション用に、Hot Desktop共有アカウント（HDSA）を作成する必要があります。共有
アカウントには、ドメインアカウントまたはそのワークステーションのローカルアカウントを使用できます。Hot Desktopを
ワークステーションにインストールするときに、共有アカウントのログオン情報を指定します。ワークステーションが起動す
ると、自動的に共有アカウントでログオンして、Hot Desktopの共有デスクトップモードになります。

ユーザーは、共有アカウントのWindowsセッション上で実行されるHot Desktopセッションで作業することになります。そ
のため、ユーザーが共有アカウントの設定を変更することはできません（管理者がユーザーに変更を許可した場合を除く）。
ユーザーは、Windowsドメインの自分のログオン情報を入力して、Hot Desktopセッションを開始します。Hot Desktop環境
では、ユーザーのWindowsアカウントがHot Desktopユーザー（HDU）とみなされます。

Hot Desktopユーザーの編成

Hot Desktop機能を導入する場合は、まずユーザーの環境を設定します。たとえば、Active Directoryの組織単位やグループに
応じてHot Desktopユーザーをグループ化します。また、Hot Desktopワークステーションだけでなく個人用のワークステー
ションも使用するユーザーを複数のグループに分けて、これらのグループに優先順位を付けることもます。

これにより、Hot Desktop設定、アプリケーション定義、パスワードポリシー、そのほかのユーザー構成などを、これらの組
織単位に割り当てられた複数のHot Desktopユーザーに適用することができます。

ユーザーの権限の制限

Hot Desktopワークステーションは、すべてのHot Desktopユーザーで共有されるため、ユーザーに割り当てる権限を制限
し、割り当てられているアプリケーションを使用するために必要な最低限のアクセス許可を付与する必要があります。たとえ
ば、Hot Desktopユーザーにはワークステーションを終了する権限を与えずに、管理者だけが終了できるようにします。

Hot Desktop、スマートカード、およびキーの復元

注：Hot Desktop環境でユーザーがスマートカードを使用する場合は、ユーザー構成の［データの保護方法］ページで[ス
マートカード証明書］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用してログオンする環境でHot Desktopを有効にする場合は、そのユーザーのユーザー構成の
［データの保護方法（セカンダリ）］ページで、［変更前のパスワードを入力させる］をキーの復元とデータ保護の唯一の方
法として選択しないでください。このような環境では、ユーザーが変更前のパスワードを入力することが不可能なため、シス
テムのロックを解除することができません。この問題を解決するには、キー管理モジュールによる暗号キーの自動復元を有効
にするか、ユーザーが質問ベースの認証オプションを選択できるように設定してください。

Hot Desktop共有アカウントに関する注意事項

次に、Hot Desktop共有アカウントを作成する場合の注意事項を示します。

- 共有アカウントがローカルまたはドメインの管理者グループに属していないことを確認してください。
- ローカルアカウントまたはドメインアカウントを共有アカウントとして使用できます。共有アカウントに割り当てられて
  る権限は、管理者が指定するアプリケーションだけを対象に、Hot Desktopユーザーにも割り当てられます。つまり、Hot
  Desktop共有アカウントのログオン情報で起動するアプリケーションと、ユーザーのWindowsドメインのログオン情報で

起動するアプリケーションを指定できます。

- Hot Desktopのインストールプロセスにより、共有アカウントのユーザー名とドメインが確認されます。このアカウントを作成するときは、［パスワードを無期限にする］チェックボックスをオンにしてください。有効期限が切れたログオン情報を共有アカウントに使用しないでください。
- 共有アカウントには、必要最低限の権限を設定します。Hot Desktop環境で必要なアクセス許可だけを付与しておきます。
- ワークステーションが属するドメインの名前には、完全修飾ドメイン名（FQDN）ではなく、NetBIOS名を使います。ローカルアカウントを共有アカウントとして使用する場合は、ワークステーションのホスト名をドメインとして指定します。
- 共有アカウントには「Hot Desktop」という名前を付けることをお勧めします。これにより、ユーザーがWindowsからログオフするときに、Hot Desktopユーザーのログオフであることを示すメッセージが表示されます。ユーザーが知らない共有アカウント名を使用すると、ログオフ時にアカウント名が表示されたときに、ユーザーが混乱する場合があります。Hot Desktopのユーザーグループが複数ある場合は、「Hot Desktop Marketing」、「Hot Desktop Accounting」など、所属グループの名前を付け加えます。

Hot Desktopで使用するアプリケーションの条件

Hot Desktop環境でユーザーが使用するアプリケーションは、次の条件を満たしている必要があります。

- ログオンが必要なアプリケーションについては、Single Sign-Onでログオンできるようにアプリケーション定義とユーザー構成を作成しておきます。
- 共有アカウントで起動するアプリケーションは、Windowsの対話型環境で実行できるアプリケーションでなければなりません。この場合、アプリケーションおよびHot Desktopユーザーは、ユーザープロファイルやネットワーク上の共有フォルダーなど、Hot Desktop共有アカウントに関連付けられているすべてのリソースにアクセスできなければなりません。
- 終了操作を行ったときに、アプリケーションがプロセスを残さずに完全に終了する必要があります。Hot Desktopでは、セッションが終了するときに、Windowsの対話式セッションからログオフするときと同様の方法でアプリケーションが終了します。Hot Desktop環境では、ワークステーション自体をシャットダウンせずにアプリケーションの起動と終了を繰り返すことが多いため、正しく終了するアプリケーションであることが重要です。
- ユーザープロファイルにユーザーの個人情報を保存したり、ユーザープロファイルの設定を使用したりするアプリケーションは、Hot Desktopユーザーアカウントで実行する必要があります。共有の設定情報を使用するアプリケーションは、共有アカウントで実行できます。管理者は、session.xmlファイルに指定する終了スクリプトを使用して、セッション終了時にユーザー固有のファイルを削除できます。

重要：HKEY_CURRENT_USERレジストリハイブに情報を保存するターミナルエミュレーターへのログオンをSingle Sign-Onで処理する場合は、そのターミナルエミュレーターをHot Desktopユーザーアカウントで起動するアプリケーションとして登録する必要があります。これを行うには、process.xmlファイルのセクションに、そのターミナルエミュレーターを指定します。セッションの開始時にターミナルエミュレーターを起動するには、session.xmlファイルのセクションに、そのターミナルエミュレーターを指定します。つまり、開始スクリプトでHot Desktopユーザーアカウントのアプリケーションとしてターミナルエミュレーターを起動する必要があります。

Hot Desktopで実行するアプリケーションの動作制御

Hot Desktop環境で実行するアプリケーションの動作を制御するには、session.xmlとprocess.xmlという2つのファイルを使用します。

重要：同じアプリケーションを、session.xmlファイルでは共有アカウントで起動し、process.xmファイルではHot Desktopユーザーアカウントで起動するように指定することはできません。session.xmlファイルでの設定の方が、process.xmlのセクションの設定より優先されます。

はじめに

- process.xmlファイルを編集するなどの目的でHot Desktopワークステーションに管理者としてログオンするには、Windowsの起動画面が表示された直後にShiftキーを押したままにして、自動ログオンを一時的に無効にします。Windowsの自動ログオンを無効にする方法について詳しくは、Microsoft社のWebサイトを参照してください。

- Hot Desktopユーザーセッションでは、session.xmlファイル、パスワード期限切れスクリプトなどのスクリプト、実行可能ファイル、またはバッチファイルで、環境変数APPDATA、HOMEDRIVE、HOMEPATH、HOMESHARE、およびLOGONSERVERがサポートされません。サポートされない変数を使用すると、スクリプト、アプリケーション、または実行可能ファイルでエラーが発生する可能性があります。この問題を回避するため、アプリケーションをHot Desktopユーザーセッションで実行するときは、サポートされない環境変数を使用しないでください。
- アプリケーションを永続的なプロセスとして指定した場合は、ユーザーがそのアプリケーションのインスタンスを終了してからHot Desktopセッションを終了する必要があります。たとえば、ユーザーが永続的なプロセスのアプリケーションを起動してファイルを作成し、ファイルを開いたままHot Desktopセッションを終了すると、次にログオンしたユーザーにそのファイルの内容が表示されてしまいます。
  重要：永続的なプロセスとして指定したアプリケーションでユーザーが機密情報を扱う場合は、Hot Desktopセッションを終了する前に必ずアプリケーションを閉じるようにユーザーに指示してください。
  process.xmlファイルで永続的なプロセスとして指定したアプリケーションをsession.xmlファイルの開始スクリプトセクションに指定した場合、ユーザーがHot Desktopセッションでそのアプリケーションのインスタンスを閉じずにログオフすると、ログオンするたびに新しいインスタンスが起動してしまいます。これを防ぐには、起動するアプリケーションのインスタンス数を制限するスクリプトやラッパーアプリケーションを作成します。また、アプリケーション自体を変更して、同時に複数のインスタンスを実行できないようにします。

- ユーザーがコマンドプロンプトから起動したアプリケーションは、Hot Desktopユーザーアカウントで起動するように指定されていても、Hot Desktop共有アカウントで起動します。コマンドプロンプトからHot Desktopユーザーアカウントでアプリケーションを起動させるには、管理者がprocess.xmlファイルのセクションにコマンドプロンプト（cmd.exe）を指定しておく必要があります。また、コマンドプロンプトを共有アカウントで実行していても、process.xmlファイルのセクションでファイルタイプ（*.txtなど）を指定している場合は、ユーザーがコマンドプロンプトから関連付けられたファイルを開くと、アプリケーションがHot Desktopユーザーアカウントで起動します。
- 8.3ファイル形式を使用するアプリケーションをprocess.xmlファイルで指定する場合は、その実行可能ファイルのパスも8.3形式で入力する必要があります。
- process.xmlファイルでは、XMLタグの大文字/小文字が区別されますが、指定するパスや実行可能ファイル名の大文字/小文字は区別されません。
- SAP Logon for Windows（saplogon.exe）は、Hot Desktopユーザーアカウントで実行する必要があります。このため、process.xmlファイルのセクションに、saplogon.exeを指定します。

ユーザー構成のHot Desktopオプション

Sep 30, 2015

Hot Desktopのユーザーエクスペリエンスは、ユーザー構成設定の次のオプションで制御されます。

注意：このリリースのインストール後、一部のレジストリの変更が必要になる場合があります。レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windowsの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。システムレジストリは、変更する前に必ずバックアップを作成してください。

セッション設定のスクリプトのパス

ユーザー構成のHot Desktopオプションの設定場所

- 新しいユーザー構成を作成するときは、［Plug-inの動作の設定］ページの［詳細設定］をクリックして、Hot Desktop関連のオプションを設定できます。
- 既存のユーザー構成を編集するときは、［ユーザー設定の編集］ダイアログボックスの［Hot Desktop］ページでHot Desktop関連のオプションを設定できます。
  各オプションについて詳しくは、
  —「Single Sign-On設定リファレンス」の「ユーザー構成」の「Hot Desktop」
  を参照してください。

セッション設定のスクリプトのパスを構成するには

1. ［ユーザー設定の編集］ダイアログボックスの［Hot Desktop］ページにある［セッション設定のスクリプトのパス］ボックスに、session.xmlファイルの場所を入力します。 ネットワーク共有フォルダーを指定することもできます。たとえば、\\Citrix\MPM\Share\のようなネットワーク共有フォルダーにsession.xmlファイルを配置する場合は、ここにそのパスを入力します。
2. ユーザー構成を保存しsession.xmlファイルをインストールした後で、Hot Desktopワークステーションを再起動します。

暗号キーの自動復元の使用

暗号キーの自動復元を有効にしたSingle Sign-On環境では、アクティブなHot Desktopセッションのユーザーのパスワードを管理者が変更しても、そのユーザーのSingle Sign-On Plug-inに反映されません。このユーザーのセッションがロックされた場合、ユーザーがロックを解除しようとしたときに、変更前のパスワード入力が求められることがあります。ここでユーザーが以前のパスワードを入力できない場合は、パスワード入力用のダイアログボックスを閉じてログオフすることで、Hot Desktopセッションを起動し直す必要があります。

Hot Desktopのスクリーンセーバー

どのワークステーションでHot Desktopを実行しているかが簡単にわかるように、Hot Desktopにはカスタムスクリーンセーバーが用意されています。スクリーンセーバーは、ワークステーションがアイドル状態になって10分経過すると起動します。

注：ロックされているセッションは、アクティブと見なされます。スクリーンセーバーは、すべてのユーザーがログオフして、ワークステーションがアイドル状態になって10分経過すると起動します。

Hot Desktopをインストールするには

Hot Desktopは、Single Sign-On Plug-inと一緒にインストールしたり、インストール済みのSingle Sign-On Plug-inに追加したりできます。

1. ワークステーションにローカルの管理者としてログオンします。

2. コントロールパネルの [プログラムの追加と削除] を開きます。
3. ［Single Sign-On Plug-in］を選択し、［変更］をクリックします。
4. ［変更］をクリックし、［次へ］をクリックします。
5. ［Hot Desktop］をインストール項目として選択し、［次へ］をクリックします。
6. ターミナルサービスとリモートデスクトップを無効にすることを確認するダイアログボックスが開くので、[はい］をクリックします。
7. 中央ストアの場所を指定して［次へ］をクリックします。
8. サービスを実行するサーバーのアドレスを指定し、［次へ］をクリックします。
9. Hot Desktop共有アカウントのログオン情報を入力し、［次へ］をクリックします。 ワークステーションが属するドメインの名前には、完全修飾ドメイン名（FQDN）ではなく、NetBIOS名を使います。
10. ［インストール］をクリックします。 インストールメディアのCitrix Single Sign-On Plug-in.msiファイルにアクセスします。

インストールが完了したら、ワークステーションを再起動します。

Hot Desktopをアンインストールするには

ワークステーションからHot Desktop機能を削除する場合、Hot Desktop機能のアンインストール後に、必要に応じて以下の作業を行います。

- Hot Desktopアンインストール後にターミナルサービスを有効にする。
- Hot Desktopアンインストール後にマルチセッションを有効にする。

1. Shiftキーを押しながらWindowsを起動して、Hot Desktopワークステーションに管理者としてログオンします。
   これにより、Hot Desktop共有アカウントの自動ログオンが一時的に無効になり、Hot Desktop環境が開始されなくなります。Windowsの自動ログオンを無効にする方法について詳しくは、Microsoft社のWebサイトを参照してください。

   管理者としてログオンします。

2. コントロールパネルの [プログラムの追加と削除] を開きます。
3. ［Single Sign-On Plug-in］を選択します。
4. Hot Desktop機能だけを削除する場合は、［変更］をクリックします。
5. ［アプリケーションメンテナンス] ページで［変更］をクリックします。
6. ［機能の選択］ページで［Hot Desktop］をクリックして、この機能を無効にします。
7. 画面の指示に従って中央ストアの種類を選択し、Single Sign-On Plug-inへの変更を確認します。
8. ワークステーションを再起動します。

ワークステーションが再起動されるまで、Hot Desktopは完全にアンインストールされません。
重要：GINAチェーンを変更した複数のソフトウェアをアンインストールするときは、インストール時と逆の順番でアンインストールする必要があります。アンインストールする順番を間違えると、システムに問題が生じることがあります。また、WindowsレジストリのGINA設定は変更しないでください。

Hot Desktopをアンインストールした後でターミナルサービスを有効にするには

Hot Desktop機能をインストールすると、ワークステーションのターミナルサービスが無効になります。Hot Desktopをアンインストールした後でターミナルサービスを有効にするには、次の手順に従います。

1. ワークステーションに管理者としてログオンします。
2. レジストリエディターを起動します。
3. レジストリキーの値を次のように1に変更します：
   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]TSEnabled=dword:00000001

Hot Desktopをアンインストールした後でマルチセッションを有効にするには

Hot Desktop機能をインストールすると、ワークステーションのレジストリキーAllowMultipleSessionsの値が0にリセットされ、マルチセッションが無効になります。Hot Desktopをアンインストールした後でマルチセッションを有効にするには、次の手順に従います。

1. ワークステーションに管理者としてログオンします。
2. レジストリエディターを起動します。
3. レジストリキーの値を次のように1に変更します：[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon] AllowMultipleSessions =dword:00000001

Hot Desktopユーザーのプロファイルフォルダーを表示するには

Hot Desktop環境では、Hot Desktop共有アカウントでシェル（explorer.exe）が実行されます。このため、シェルでHot Desktopユーザーのプロファイルフォルダーにアクセスすることができません。Hot Desktopユーザーのプロファイルフォルダーを表示するには、次の手順に従います。

1. process.xmlファイルのセクションに、Internet Explorer（iexplore.exe）を追加します。これにより、Internet ExplorerがHot Desktopユーザーアカウントで実行されるようになります。
2. Hot Desktopセッションを開始して、Internet Explorerを起動します。
3. アドレスとして、Hot Desktopユーザーのプロファイルフォルダーの完全修飾パスを入力します。 例 :C:\Documents and Settings\All Users\Application Data\Citrix\MetaFrame Password Manager

AutoAdminLogon機能を無効にするには

Hot Desktopをインストールすると、WindowsのレジストリでAutoAdminLogonが有効になります。これにより、ワークステーションの起動時にHot Desktop共有アカウントで自動的にログオンされ、Hot Desktopの共有デスクトップモードが開始されます。ただし、この設定により一部のサードパーティ製認証システムが正しく動作しなくなる場合があります。このため、一部のサードパーティ製認証システムのインストール時に、レジストリのAutoAdminLogon値が削除されたり無効にされたりする場合があります。この問題を回避するには、Hot DesktopのAutoAdminLogon機能を無効にします。

1. ワークステーションを再起動し、Windowsの起動画面が表示された直後にShiftキーを押し、そのままWindowsを起動します。 これにより、Hot Desktop共有アカウントの自動ログオンが一時的に無効になり、Hot Desktop環境が開始されなくなります。Windowsの自動ログオンを無効にする方法について詳しくは、Microsoft社のWebサイトを参照してください。
2. 管理者としてログオンします。
3. サードパーティ製認証システムをサポートするためにAutoAdminLogonを無効にするには、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\HotDesktopのレジストリを次のように設定します。

値の名前	種類	値
AutoAdminLogon	REG_SZ	0

4. ワークステーションを再起動して、Hot Desktop共有アカウントで手動ログオンします。 すると、Hot Desktopのログオン画面が表示され、問題のあったサードパーティ製認証システムも使用可能になります。

Hot Desktop共有アカウントのパスワードを変更するには

Hot Desktop共有アカウントのパスワードを変更する必要が生じることがあります。このアカウントのログオン情報は、Single Sign-On Plug-inのインストール時に指定します。このアカウントのパスワードを後から変更するには、次の手順に従います。

1. Hot Desktopがインストールされているワークステーションにログオンします。
   重要：ここで管理者アカウントやHot Desktop共有アカウントのログオン情報を使用しないでください。
2. Ctrl + Alt + Delキーを押します。［Windowsのセキュリティ］ダイアログボックスが開きます。
3. ［パスワードの変更］をクリックします。
4. 次の項目を選択または入力します。
   - Hot Desktop共有アカウントのユーザー名
   - ドメイン名またはローカルコンピューター名
   - 現在のパスワード
   - 新規パスワード
5. ［OK］をクリックします。
6. ［Windowsのセキュリティ］ダイアログボックスで［シャットダウン］をクリックし、［再起動］を選択してワークステーションを再起動します。

Hot Desktopワークステーションをシャットダウンするには

Hot Desktopワークステーションは、管理者権限でのみシャットダウンできます。このため、Hot Desktopワークステーションの［スタート］メニューには、コンピューターをシャットダウンするためのコマンドが表示されません。

Hot Desktopワークステーションをシャットダウンする必要がある場合は、Ctrl + Alt + Delキーを押して［Windowsのセキュリティ］ダイアログボックスを開き、［シャットダウン］をクリックします。

Hot Desktop環境でのほかのCitrix製品の使用

Single Sign-OnのHot Desktop環境で、Citrix ReceiverやOffline Plug-inなどのプラグインソフトウェアを使用することもできます。ここでは、Hot Desktop環境でこれらのプラグインソフトウェアやWeb Interfaceを使用する場合の注意事項について説明します。

- 最初のHot Desktopセッション開始時にCitrix ReceiverやCitrix Offline Plug-inが自動的に起動するようにする場合（Windowsスタートアッププログラムとして起動する場合など）は、process.xmlファイルでこれらのプラグインソフトウェアを一時的なプロセスとして指定してください。
- SSPI（Security Support Provider Interface）を使用する場合は、プラグインソフトウェアをHot Desktopユーザーアカウントで実行する必要があります。プロファイルに保存されるICAファイルのセキュリティを保護する場合も、Hot Desktopユーザーアカウントでプラグインソフトウェアを実行します。
  - ユーザーがWindowsのシェルからCitrix ReceiverやCitrix Offline Plug-inを起動したときにHot Desktopユーザーアカウントが使用されるように、process.xmlファイルのセクションを編集します。
  - 最初のHot Desktopセッションを開始したときにCitrix ReceiverやCitrix Offline Plug-inが起動するように、session.xmlファイルの開始スクリプトを編集します。

Citrix Receiver

Citrix ReceiverでSSPIが使用されるように構成できます。これにより、XenAppのサーバーファームにHot Desktopユーザーアカウントでログオンできるようになります。ただし、Hot Desktopユーザーの認証に使用するWindowsの証明機関が、XenAppで信頼されている必要があります。Citrix ReceiverのSSPI構成について詳しくは、「
— XenAppの管理
」を参照してください。

Web Interface

Hot Desktop環境のSingle Sign-On Plug-inでは、Web Interface経由でXenAppサーバーにログオン情報を送信できます。構成について詳しくは、「

— *Web Interface*
」のトピックを参照してください。

session.xmlファイル

Sep 30, 2015

session.xmlファイルを使用して、Hot Desktopのセッション開始時に起動するアプリケーションやスクリプト（開始スクリプト）と、セッション終了時に起動するアプリケーションやスクリプト（終了スクリプト。通常はユーザーが残したファイルを削除するスクリプト）を指定します。サンプルファイルsample_session.xmlを編集して、Hot Desktopワークステーションからアクセスできるネットワークの共有フォルダーに保存します。ユーザー構成を作成するときに、session.xmlファイルの場所を指定する必要があります。

session.xmlファイルを編集するときは、との間に必要なセクションを定義します。

注：session.xmlファイルのサンプル（sample_session.xml）は、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。

例：スクリプトによるセッションのクリーンアップ

Visual Basicのスクリプトを使用して、Hot Desktopセッションの終了時に残っているユーザーデータをクリーンアップします。この例で、スクリプトsession_cleanup.vbsはHot Desktop共有アカウント（HDSA）で実行されます。スクリプトの場所はCドライブのルートです。

例：Internet Explorerの起動

Hot Desktopセッションの開始時にInternet Explorerを起動して、イントラネットサイトmycompany.comにアクセスします。この例では、Internet ExplorerがHot Desktopユーザーアカウントで実行されます。

との間に以下のセクションを定義します。

startup_scripts

このセクションには、Hot Desktopセッションの開始時に起動するアプリケーションと、そのアカウント（Hot Desktop共有アカウント、またはHot Desktopユーザーに関連付けられているWindowsアカウント）を指定します（開始スクリプト）。

各項目の意味は次のとおりです。

アカウント	アプリケーションを実行するアカウントです。HDUまたはHot Desktop共有アカウントのユーザー名を指定します。
wd	アプリケーションの作業ディレクトリです。
path_options	ローカルコンピューター上のアプリケーションの実行可能ファイルまたはスクリプトの完全修飾パスとオプションです。次に例を示します。 c:\program files\Internet Explorer\iexplore.exe http://www.yahoo.com

shutdown_scripts

このセクションには、Hot Desktopセッションの終了時に起動するアプリケーションやスクリプトを指定します（終了スク

リプト）。通常、次のユーザーセッションの妨げになる設定ファイルや、ログファイルなどの個人情報、および前のユーザーがシステムに保存したファイルなどを削除する目的で使用します。このように、終了スクリプトは、次にセッションを開始するユーザーのためにHot Desktop環境をクリーンアップします。このセクションは、データのセキュリティを維持する上で特に役立ちます。

注：必要であれば、管理用プログラムまたはスクリプトを起動して、ログオフ時にユーザー環境をクリーンアップできます。たとえば、サードパーティ製のアプリケーションを使ってユーザー固有のINIファイルを削除するVisual Basicスクリプトを作成できます。

各項目の意味は次のとおりです。

アカウント	アプリケーションを実行するアカウントです。次の選択肢があります。HDUおよびHot Desktop共有アカウントのユーザー名。
wd	アプリケーションの作業ディレクトリです。
path_options	ローカルコンピューター上のアプリケーションの実行可能ファイルまたはスクリプトの完全修飾パスとオプションです。次に例を示します。 c:\cleanup.vbs

session.xmlファイルによるアプリケーションの起動

次のように検討します。

- session.xmlファイルに指定するアプリケーションは、ワークステーションにインストール済みである必要があります。
- Hot DesktopはSingle Sign-On Plug-inの一部なので、セッションの開始時にSingle Sign-On Plug-inも自動的に起動します。このため、session.xmlファイルの開始スクリプトセクションにSingle Sign-On Plug-inを指定する必要はありません。

session.xmlファイルによりHot Desktop共有アカウントで起動したアプリケーションに対して、ログオン情報の入力が必要になる場合もあります。Single Sign-On Plug-inは、ユーザー構成に従ってこれらのアプリケーションのログオン情報を自動的に処理します。

重要：session.xmlファイルはUTF-8形式で保存します。ただし、すべての文字が0から127の文字コード範囲（標準的な英語の文字セット）にある場合はANSIでエンコードできます。session.xmlファイルに日本語や特殊文字を記述する場合は、必ずUTF-8形式で保存してください。

process.xmlファイル

Sep 30, 2015

注：process.xmlファイルは、各Hot Desktopワークステーションの%ProgramFiles%\Citrix\MetaFrame Password Manager\HotDesktopフォルダーにインストールされます。process.xmlファイルのサンプル（sample_process.xml）は、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。このファイルを変更する場合は、すべてのHot Desktopワークステーション上のprocess.xmlファイルを同様に変更する必要があります。各ワークステーション上のprocess.xmlファイルをActive Directoryのコンピューターグループポリシーを使用して置き換える方法については、Citrix Knowledge CenterのCTX112268（http://support.citrix.com/article/CTX112268）を参照してください。
process.xmlファイルを使用して、ユーザーがログオフした後も実行するアプリケーションを指定します。このようなアプリケーションを永続的なアプリケーションまたは永続的なプロセスと呼びます。

また、process.xmlファイルでは、ユーザーがログオフした後に終了するアプリケーションも指定できます。このようなアプリケーションを一時的なアプリケーションまたは一時的なプロセスと呼びます。

process.xmlファイルを編集するときは、との間に必要なセクションを定義します。

重要：process.xmlファイルはUTF-8形式で保存します。ただし、すべての文字が0から127の文字コード範囲（標準的な英語の文字セット）にある場合はANSIでエンコードできます。process.xmlファイルに日本語や特殊文字を記述する場合は、必ずUTF-8形式で保存してください。

shellexecute_processes

このセクションには、Hot Desktopユーザーアカウントで実行するアプリケーションまたはファイルタイプを指定します。これにより、ユーザーがHot Desktopセッション内で起動するアプリケーションが、確実にそのユーザーのアカウントで実行されるように設定できます。

注：Single Sign-On Plug-inをインストールすると、セクションにssoshell.exeという名前のエントリが自動的に追加されます。これはSingle Sign-On Plug-inの実行可能ファイルです。ssoshell.exeは、デフォルトでHot Desktopユーザーアカウントで実行するプロセスとして定義されます。
session.xmlファイルの開始スクリプトセクションでは、Hot Desktopセッションの開始時に起動するアプリケーションを指定するのに対し、process.xmlファイルのセクションでは、ユーザーがセッション中に起動できるアプリケーションを指定します。

appname
各項目の意味は次のとおりです。

appname	Hot Desktopユーザーアカウントで実行するプロセスまたはアプリケーションの名前です。完全修飾パスである必要はありません。次に例を示します。 pnagent.exe.

注：process.xmlファイルでは、実際のファイル名（Notepad.exeなど）だけでなく、ワイルドカード文字（*）を使ってアプリケーションを指定できます。ワイルドカードは、単独で使うことも、ファイル名と組み合わせて使うこともできます。たとえば、appnameの値として、*.txt、pnagent.exe、*.docなどを指定できます。

persistent_processes

このセクションには、ユーザーがログオフした後も実行するアプリケーションを指定します。ここで指定したアプリケーションは、Hot Desktopセッションの間に起動されたものであっても、セッションのシャットダウンまたはログオフ時に終了しません。永続的なプロセスの完全修飾パスを指定して、セッション後に適切なプロセスだけが実行状態で維持されるよ

うにします。

path_options

各項目の意味は次のとおりです。

path_options	ローカルコンピューター上のアプリケーションの実行可能ファイルまたはスクリプトの完全修飾パスとオプションです。次に例を示します。 c:\program files\Internet Explorer\iexplore.exe http://www.yahoo.com

注：Single Sign-On Plug-inをインストールすると、セクションにActivator.exeという名前のエントリが自動的に追加されます。Activator.exeは、Hot Desktopセッションインジケーターをユーザーに表示するアプリケーションです。このインジケーターは、ユーザーがログオンしたときに表示される透明で移動可能なウィンドウで、ユーザーとそのセッションについて管理者が定義した情報が表示されます。Activator.exeは、デフォルトで永続的なプロセスとして定義されるため、ユーザーがログオンしたりログオフしたりするたびに再起動されることはありません。

transient_processes

このセクションには、ユーザーがログオフした後に終了するアプリケーションを指定します。

注：Single Sign-On Plug-inをインストールすると、セクションにShellexecute.exeという名前のエントリが自動的に追加されます。Shellexecute.exeは、デフォルトで一時的なプロセスとして定義されるため、ユーザーがログオフするたびに終了します。

appname

各項目の意味は次のとおりです。

appname	ユーザーがログオフした後に終了するプロセスまたはアプリケーションの名前です。完全修飾パスである必要はありません。次に例を示します。 pnagent.exe.

リファレンス

Sep 30, 2015

このトピックでは、管理コンソール（Citrix AppCenterの［Single Sign-On］ノード）を使用して設定する各項目とそのデフォルト値を、表示場所ごとに分類して説明します。

ユーザー構成

ここでは、ユーザー構成とオプションについて説明します。ここに記載されている操作手順は、既存のユーザー構成を編集するときの操作です。［ユーザー設定の編集］ダイアログボックスを開くには、次の操作を行います。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］

Plug-inの基本動作

以下のオプションでは、このユーザー構成でのSingle Sign-On Plug-inの動作をカスタマイズします。ユーザーインターフェイスの設定をここで設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［Plug-inの基本動作］

パスワードの文字列をユーザーが表示することを許可する

［パスワード管理］ダイアログボックスでユーザーがパスワードの内容を表示できるようにするかどうかを指定します。このチェックボックスをオフにすると、［文字列の表示］ボタンが無効になります。特定のアプリケーションでだけパスワード文字列の表示機能を無効にするには、このチェックボックスをオンにして、そのアプリケーションのパスワードポリシーで［パスワードの文字列をユーザーが表示することを許可する］チェックボックスをオフにします。

デフォルト設定：オン

パスワードを表示するときにユーザーの再認証を行う

パスワードの内容を表示するときに、ユーザーの再認証処理を要求するかどうかを指定します。

デフォルト設定：オン

ログオン情報を登録するためのダイアログボックスをユーザーに表示する

ログオンが必要なアプリケーションがSingle Sign-On Plug-inにより認識されたときに、ログオン情報を登録するためのダイアログボックスを開くかどうかを指定します。

ユーザー構成に追加されていないアプリケーションをSingle Sign-On Plug-inが検出しないようにする場合は、このチェックボックスをオフにします。この場合、ユーザーはこれらのアプリケーションに手作業でログオン情報を入力してログオンする必要があります。ユーザー構成に定義されていないアプリケーションをユーザーがSingle Sign-Onに登録できないようにするには、このオプションを無効にします。

このオプションを無効にすると、［クライアント側の動作］ページにある［新しいアプリケーションに対するログオン情報の登録処理をユーザーがキャンセルできる］チェックボックスの設定は無視されます。また、プロビジョニング機能でユーザーのログオン情報を管理者が登録する場合は、このオプションを無効にして、ユーザーがログオン情報を登録しないようにできます。

デフォルト設定：オン

定義済みのフォームに対する自動処理を有効にする

このオプションを選択すると、ユーザー構成に追加されているアプリケーション定義のフォームがSingle Sign-On Plug-inにより自動的に検出され、ログオン情報が入力されるようになります。このユーザー構成に関連付けられているアプリケーション定義の［ログオン情報を自動送信する］オプションが有効な場合は、入力されたログオン情報が自動的にアプリケーションに送信されます。

デフォルト設定：オン

再認証要求の間隔

Single Sign-On Plug-inがユーザーの再認証を要求する間隔を指定します。ここで指定した時間が経過すると、ユーザーデバイスがロックされます。ユーザーは、プライマリパスワードを入力してロックを解除できます。最小値は1分です。

デフォルト設定：8時間

Plug-inのユーザーインターフェイス

以下のオプションでは、ログオン情報を送信するときの待機時間や、［パスワード管理］ダイアログボックスで表示する列項目について設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［Plug-inのユーザーインターフェイス］

ログオン情報を送信するまでの待機時間（秒）を指定する

Single Sign-On Plug-inがアプリケーションを検出してからログオン情報を送信するまでの待機時間を指定します。このチェックボックスをオンにする場合は、ログオン情報を送信するまでの待機時間を秒単位で指定します。このオプションは、アプリケーションがログオン情報を受信できるようになるまでに時間がかかる場合に使用します。Single Sign-On Plug-inが待機している間、ログオン情報の送信までの時間が示されます。

デフォルト設定：オフ。0秒

ログオンマネージャーにデフォルトで表示する情報の列見出しおよびその順序

［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）に表示する列項目、およびその順序を指定します。

デフォルトの設定は次の通りです：

- アプリケーション名
- 説明
- グループ
- 最終使用日
- 更新日時

クライアント側の動作

このページでは、ログ機能、終了時のレジストリキーの保持、および新しく検出されたアプリケーションに対するログオン情報の登録処理について設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［クライアント側の動作］

Citrix Single Sign-OnイベントをWindowsのイベントログに記録する

Single Sign-On Plug-inの情報イベントをWindowsのイベントログに記録するかどうかを指定します。警告イベントやエラーイベントは、このオプションの設定に関係なく常に記録されます。

デフォルト設定：オフ

Single Sign-On Plug-in終了時にユーザーのデータフォルダーとレジストリキーを削除する

Single Sign-On Plug-inの終了時に、レジストリキーと、暗号化された証明書を含むデータフォルダーを削除するかどうかを指定します。

デフォルト設定：オフ

新しいアプリケーションに対するログオン情報の登録処理をユーザーがキャンセルできる

ログオン情報の登録が必要なアプリケーションが検出されたときに、ログオン情報の登録をユーザーがキャンセルできるかどうかを指定します。このチェックボックスをオンにすると、アプリケーションが検出されたときにログオン情報の登録を確認するメッセージが表示され、ユーザーは［はい］、［今回はいいえ］、または［いいえ］を選択できます。［Plug-inの動作の設定］ページの［ログオン情報を登録するためのダイアログボックスをユーザーに表示する]チェックボックスがオフの場合、ログオン情報の登録用のダイアログボックスが開かなくなり、このオプションは無視されます。

デフォルト設定：オン

削除されたログオン情報を保持する日数を制限する

ユーザーがコンピューター上の［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）から削除したログオン情報を、中央ストアが追跡するかどうかと、追跡する場合はその日数を指定します。たとえば、ユーザーが2台のクライアントコンピューター（AとB）を使用する場合に、コンピューターA上で削除したログオン情報は、コンピューターB上のSingle Sign-On Plug-inが中央ストアと同期したときに、新しい情報として中央ストアに再登録されることがあります。ここで特定の期間を指定すると、その間は中央ストアで削除済みとして保持されるため、コンピューターBで同期しても再登録されなくなります。

デフォルト設定：オン。180日

同期

以下のオプションでは、Single Sign-On Plug-in設定の更新許可、ユーザー構成情報の同期、中央ストアに接続できない場合のSingle Sign-On Plug-inの使用許可、および自動的な同期処理間隔の指定について設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［同期処理］

ユーザーがSingle Sign-On Plug-in設定を更新することを許可する

［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）でユーザーがSingle Sign-On設定を更新できるよ

うにするかどうかを指定します。このチェックボックスをオフにすると、［パスワード管理］ダイアログボックスの［更新］コマンドが無効になります。

デフォルト設定：オン

定義済みアプリケーションまたはログオンマネージャーの起動時に同期処理を実行する

ユーザーが［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）を開いたり定義済みアプリケーションを起動したりしたときに、Single Sign-On Plug-inがユーザー構成情報を中央ストアと同期するかどうかを指定します。過度に頻繁な同期処理は、ネットワークの負担となるだけでなく、クライアントおよびサーバーのパフォーマンスを低下させる原因となります。

デフォルト設定：オフ

中央ストアに接続できない場合でもSingle Sign-On Plug-inの使用を許可する

中央ストアに接続して同期できない場合に、Single Sign-Onを使用できるようにするかどうかを指定します。このチェックボックスをオンにすると、中央ストアとの接続に失敗しても、正規にライセンスされた製品であれば、ユーザーは継続してSingle Sign-On Plug-in使用できます。このチェックボックスをオフにすると、中央ストアに接続している間だけSingle Sign-On Plug-inが動作するようになります。

デフォルト設定：オン

同期処理の要求間隔を指定する

自動同期処理の間隔を設定するかどうかと、設定する場合はその間隔を分単位で指定します。この設定による同期処理は、同期処理を起動するそのほかのユーザーイベントに関係なく、定期的に開始されます。

デフォルト設定：オフ。0分

ログオン情報の同期モジュールがユーザーのログオン情報にアクセスすることを許可する

ユーザーのログオン情報へのリモートからのアクセスを許可します。このオプションは、Single Sign-On Plug-inのユーザーが複数のWindowsアカウントを使用してアプリケーションにログオンできるようにする、アカウントの関連付け機能と組み合わせて使用します。

デフォルト設定：オフ

アカウントの関連付け

複数のWindowsドメインを運用している企業では、ユーザーも複数のWindowsアカウントを持っていることがあります。アカウントの関連付け機能のオプションでは、Single Sign-On Plug-inのユーザーが複数のWindowsアカウントを使用してアプリケーションにログオンできるようにするかどうかを指定します。以下のオプションを有効にすると、ユーザーが複数のWindowsアカウントのログオン情報を関連付けて管理できるようになります。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［アカウントの関連付け］

アカウントの関連付けをユーザーに許可する

ユーザーが複数のWindowsアカウントのログオン情報を関連付けて管理できるようにするかどうかを指定します。このチェックボックスをオンにすると、ログオン情報の同期モジュールがインストールされているサーバーのURLとポートを指定できます。ユーザー構成を作成するときにはこのオプションは設定できません。既存の設定を編集するときにだけ設定できます。

デフォルト設定：オフ

デフォルトのサービスアドレスを指定する

ログオン情報の同期モジュールがインストールされているサーバーのアドレスとサービスポートをデフォルトでユーザーに提供するかどうかを指定します。指定した後で［確認］をクリックして、アドレスとポートが有効かどうか確認できます。

デフォルト設定： /MPMService/

サービスポート：443

サービスアドレスの変更をユーザーに許可する

サーバーのアドレスとサービスポートをデフォルトでユーザーに提供する場合は、このチェックボックスをオンにして、ユーザーが設定を編集できるようにするかどうかを指定できます。ログオン情報の同期サービスが複数のコンピューターで動作していて、ユーザーがサービスを切り替えられるようにする必要がある場合は、このチェックボックスをオンにします。

デフォルト設定：オフ

デフォルトのドメインを指定する

Single Sign-On Plug-inがドメイン間でログオン情報を同期するときの認証先ドメインをデフォルトでユーザーに提供するかどうかを指定します。このチェックボックスをオンにする場合は、［ドメイン］ボックスにデフォルトのドメインを指定します。ここでデフォルトのドメインを指定しない場合、ユーザーがどのドメイン用のログオン情報を入力すべきか迷ってしまう可能性があります。

デフォルト設定：オフ

ドメインの変更をユーザーに許可する

ログオン情報を同期するときの認証先ドメインをデフォルトでユーザーに提供する場合は、そのデフォルト設定のユーザーによる編集を許可するかどうかを指定できます。

デフォルト設定：オフ

パスワードの保存をユーザーに許可する

関連付けられたWindowsアカウントのパスワードを、ユーザーがSingle Sign-On Plug-inで保存できるようにするかどうかを設定します。

デフォルト設定：オフ

アプリケーションのサポート

以下のオプションでは、クライアント側のアプリケーション定義の検出、ターミナルエミュレーターのサポート、Webアプリケーションのマッチするドメイン名のレベル数について設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユー

ザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［アプリケーションのサポート］

クライアント側のアプリケーション定義を検出する

次のアプリケーションからのログオン要求をSingle Sign-Onが検出できるようにするかどうかを指定します。

- すべてのアプリケーション
  管理者が作成したアプリケーション定義、ユーザーの［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）での設定、およびSingle Sign-Onのインストール時のデフォルト設定（applist.ini）に基づいてアプリケーションを検出して、ログオン処理を行います。
- ユーザーがログオンマネージャーに登録したアプリケーションのみ
  管理者が作成したアプリケーション定義、およびユーザーの［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）での設定に基づいてアプリケーションを検出して、ログオン処理を行います。Single Sign-Onのインストール時のデフォルト設定（applist.ini）で定義されているアプリケーションは検出されません。
- applist.iniに定義されているアプリケーションのみ
  管理者が作成したアプリケーション定義、およびSingle Sign-Onのインストール時のデフォルト設定（applist.ini）に基づいてアプリケーションを検出して、ログオン処理を行います。［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）でユーザーが自分でアプリケーション定義を作成することはできません。

デフォルト設定：すべてのアプリケーション

ターミナルエミュレーターのサポートを有効にする

ターミナルエミュレーションプログラムのサポート機能を有効にするかどうかを指定します。このチェックボックスをオンにすると、Single Sign-On Plug-inでターミナルエミュレーターベースのアプリケーションを検出するためのプロセスが実行されます。

デフォルト設定：オフ

ターミナルエミュレーターの更新をチェックする間隔

Single Sign-On Plug-inでターミナルエミュレーションプログラム画面の更新をチェックする間隔をミリ秒単位で指定します。過度に小さい値を設定すると、クライアントコンピューターのCPUとネットワークに負担がかかります。

デフォルト設定：3000ミリ秒

マッチするドメイン名のレベル数

定義済みのWebアプリケーションとして認識させるURLのレベルを指定します。たとえば、2を指定した場合、上位2ドメイン（「*.ドメイン.最上位ドメイン」）が定義済みURLと一致すると、そのWebアプリケーションとして認識されます。同様に、を指定した場合、上位3ドメイン（「*.サブドメイン.ドメイン.最上位ドメイン」）が一致すると、定義済みWebアプリケーションとして認識されます。指定したレベルを超えるドメイン名は、ワイルドカードとして処理されます。WebアプリケーションのURLを厳密にマッチさせるには、アプリケーション定義に定義されているフォームで［URLの完全マッチ］チェックボックスをオンにします。

デフォルト設定：99

Hot Desktop

以下のオプションでは、Hot Desktopセッションでの動作について設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［Hot Desktop］

セッション設定のスクリプトのパス

セッション設定ファイルのパスを指定します。起動時のスクリプトでは特定のアプリケーションを起動して、終了時のスクリプトではファイルの削除などのクリーンアップ処理を実行できます。ここで指定するファイルには、すべてのユーザーがアクセスできる必要があります。

デフォルト設定：なし

ロックのタイムアウト

ワークステーションがアイドル状態になってから、Hot Desktopセッションをアクティブなまま保持する時間を分単位で指定します。ここで指定した時間が経過すると、デスクトップがロックされます。

デフォルト設定：10分

セッションのタイムアウト

デスクトップがロックされている間、Hot Desktopセッションを保持する時間を分単位で指定します。ここで指定した時間が経過すると、Hot Desktopセッションが終了し、デスクトップのロックが解除されたときに新しいHot Desktopセッションが起動します。

デフォルト設定：5分

セッションインジケーターを有効にする

Hot Desktopセッションが実行されていることを示すウィンドウを表示するかどうかを指定します。このチェックボックスをオンにすると、半透明な可動ウィンドウがデスクトップに表示され、Hot Desktopセッションが実行中であることが示されます。このウィンドウには、アクティブなセッションのユーザー名と経過時間が表示されます。

デフォルト設定：オン

グラフィックを表示する

Hot Desktopセッションインジケーターとしてグラフィックを表示するかどうかと、表示する場合はグラフィックファイルのパスを指定します。このファイルは、すべてのユーザーがアクセスできるWindowsビットマップ（BMP）ファイルである必要があります。

デフォルトのCitrix.bmpファイルは、Hot Desktopワークステーションの%ProgramFiles%\Citrix\MetaFrame Password Manager\Hot Desktopフォルダーにインストールされます。

デフォルト設定：なし

ライセンス管理

以下のオプションでは、ライセンスサーバーとライセンスモデルについて設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［ライセンス］

重要：ユーザーのコンピューター上にインストールされたSingle Sign-On Plug-inを使用してCitrix XenApp, Platinum Edition環境で公開されているアプリケーションにアクセスする場合、そのSingle Sign-On Plug-in用に個別のライセンスをインストールする必要はありません。

ライセンスサーバー名

ライセンスサーバーを特定するために使用する、完全修飾ドメイン名（hostname.subdomain.domain形式）です。

デフォルト設定：なし

デフォルト値を使用する

ライセンスサーバーのデフォルトのアクセスポートを使用するかどうかを指定します。デフォルト以外のポートがライセンスサーバーで使用されている場合は、このチェックボックスをオフにして［ポート番号］ボックスにアクセスポートを入力します。

デフォルト設定：オン

デフォルトポート：27000

指定ユーザーライセンス

製品エディションがAdvanced Editionの場合はこのオプションが選択されます。製品エディションがEnterprise Editionの場合は、必要に応じてこのオプションを選択できます。このライセンスモデルでは、ライセンスが特定のユーザーに関連付けられるため、そのユーザーがSingle Sign-Onを使用しているときは、ほかのユーザーがそのライセンスを使用することはできません。このオプションを選択する場合は、指定ユーザーにライセンスを割り当てる期間を、日、時間、分の単位で指定する必要があります。この期間が過ぎるとライセンスが失効し、再度有効にするにはSingle Sign-On Plug-inがライセンスサーバーに再接続する必要があります。ユーザーは自分のコンピューターをシャットダウンしても、この期間の間はライセンスを使用できます。

デフォルト設定：オン（Single Sign-On Advanced Editionの場合。XenApp Platinum Editionでは選択不可）

許可される非接続期間：21日

同時接続ユーザーライセンス（Enterprise EditionとPlatinum Editionのみ）

このオプションは、製品エディションとしてXenApp PlatinumまたはSingle Sign-On Enterpriseを選択した場合に選択可能になります。製品エディションとしてAdvanced Editionを選択した場合、このオプションは選択不可になります。
注：このライセンスモデルは、Single Sign-On（Password Manager）Version 4.1からアップグレードした場合に有効になります。つまり、ライセンスに関してSingle Sign-On 5.0 Enterprise Editionと同等になります。
このライセンスモデルでは、1つのSingle Sign-Onライセンスを複数のユーザーで共有することができます（同時使用はできません）。このようなライセンスをフローティングライセンスと呼ぶこともあります。

デフォルト設定：オン（Single Sign-On EnterpriseまたはXenApp Platinum Editionの場合。Single Sign-On Advanced Editionでは選択不可）

許可される非接続期間：［オフラインでのライセンス使用を許可する］がオフの場合は1時間30分。［オフラインでのライセンス使用を許可する］がオンの場合は21日

オフラインでのライセンス使用を許可する

［同時接続ユーザーライセンス］が選択されている場合にだけ、このチェックボックスを使用できます。このオプションで

は、ライセンスが失効しライセンスプールに戻されるまで、ユーザーが接続していない、つまりオフラインの状態でいられる期間を設定するかどうかを指定します。このチェックボックスをオンにすると、ユーザーは自分のコンピューターをシャットダウンしても、指定されている期間はライセンスを使用できます。デフォルト設定は1時間30分ですが、2～365日に設定することをお勧めします。

デフォルト設定：オフ

ライセンス情報を確認しないで続行する

このチェックボックスをオンにすると、有効なライセンスサーバーの名前やポート番号を入力しなくても、管理コンソールでの作業を続行できる用になります。

デフォルト設定：オフ

データの保護方法

Sep 30, 2015

以下の設定では、ユーザーのログオン情報を保護するために使用する、プライマリのデータ保護方法を指定します。一部の環境では、ユーザーが複数の認証方法を使用することがあります。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［データの保護方法］

アカウント管理者がユーザーデータにアクセスすることを制限しますか?

管理者がユーザーのログオン情報にアクセスできないようにするには[はい］をクリックします。このオプションを選択すると、Microsoft Data Protection APIが無効になり、［スマートカードのキーリソース］ボックスの一覧で［DPAPIとプロファイル］を選択できなくなります。また、［データの保護方法（セカンダリ）］ページの［同一性を検証せずにネットワーク経由でプライマリのデータ保護方法を自動的に復元する］をクリックできなくなります。この設定では、アカウントの管理者などがユーザーのパスワードやデータにアクセスできません。これにより、管理者がユーザーを偽装することを防ぐことができます。管理者はデフォルト設定でユーザーとしてログオンできず、ユーザーのローカルのログオン情報ストアに格納されているデータにアクセスできません。

このページの複数の認証機能と、［データの保護方法（セカンダリ）］ページのセカンダリのデータの保護方法を使用できるようにするには、［いいえ］をクリックします。

デフォルト設定：はい

使用するデータ保護方法を選択する

ここで選択できるプライマリの認証機能を使用するかどうかを指定します。

デフォルト設定：オン

Password Manager 4.1以前で使用したデータ保護方法を使用する

コントロール	説明
ユーザーの認証データ	ユーザーのログオン情報が、ユーザーのプライマリパスワードに基づいて暗号化されます。プライマリパスワードとは、ユーザーがWindowsにログオンするときのドメインパスワード、トークンからのワンタイムパスワード、認証デバイスで使用されるPINなどです。 デフォルト設定：オン ユーザーデータの保護をさらに強化するために、以下のオプションも選択できます。 スマートカードのPINを許可する ユーザーのログオン情報が、スマートカードのPINに基づいて暗号化されます。このオプションを使用する場合は、より強力なPINを使用することをお勧めします。 デフォルト設定：オフ 空白のパスワードを許可する

コントロール	説明
	このオプションは、セキュリティ上の要件が低く、ログオンしやすいことが重視される環境でのみ許可してください。このオプションを選択すると、ユーザーが空白のプライマリパスワードを使用する場合に、ユーザーのログオン情報がユーザーIDに基づいて暗号化されます。 このオプションを選択しない場合、ユーザーが空白のプライマリパスワードを使用すると、Single Sign-On Plug-inでは暗号キーの生成やデータの保護が行われません。 ［ユーザーの認証データ］を選択し、［スマートカードのPINを許可する］と［空白のパスワードを許可する］を選択すると、ユーザーが空白のパスワードでログオンしようとした場合にエラーメッセージが表示され、Single Sign-On Plug-inが使用できなくなります。 デフォルト設定：オフ
Microsoft Data Protection API	移動プロファイルを使ってユーザーにKerberosネットワーク認証プロトコルを提供している環境では、このオプションを選択します。このオプションは、移動プロファイルが使用できる場合にだけ機能します。 たとえば、ユーザーがパスワードを使用して自分のコンピューターにログオンし、Kerberosネットワーク認証プロトコルを使用してCitrix XenAppのサーバーファームにアクセスしている場合は、［ユーザーの認証データ］チェックボックスとこのチェックボックスをオンにします。この場合、ユーザーはプライマリパスワードとスマートカードを使用してログオンすることもできます。 デフォルト設定：オフ
スマートカード証明書	認証データの暗号化と複合化ができる暗号化カードの使用を許可する場合に選択します。Hot Desktopを使用する場合には、このオプションの使用をお勧めします。 デフォルト設定：オフ

単純なプライマリ認証方法をユーザーが使用できるようにする場合、またはSingle Sign-On Plug-in（Password Managerエージェント）4.0や4.1をサポートする場合は、このオプションをクリックして［スマートカードのキーソース］ボックスの一覧から方法を選択します。Single Sign-Onの中央ストアのバージョンを4.1からアップグレードした場合は、このオプションが自動的に選択されます。

このオプションは、暗号化方式として3DESが選択されている場合のみ使用可能です。

スマートカードのキーソースとして、以下のオプションを選択できます。

- PINパスワード
- スマートカードによるデータ保護
- DPAPIとプロファイル（［アカウント管理者がユーザーデータにアクセスすることを制限しますか?]が［いいえ］の場合は選択不可）

デフォルト設定：オフ

データの保護方法（セカンダリ）

以下のオプションでは、ユーザーが自分のプライマリな認証方法を変更した場合（たとえば、ドメインパスワードやスマートカードを変更した場合）に、ユーザーのログオン情報のロックを解除するときに使用する、ログオン情報データのセカンダリの保護方法を指定します。キー管理モジュールを実装する場合は、ログオン情報が自動的に復元されるように指定することもできます。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［データの保護方法（セカンダリ）］

ユーザーの同一性を検証する

デフォルト設定：オン

このオプションを選択すると、次のいずれかのユーザー再認証方法を選択できます。

コントロール	説明
変更前のパスワードを入力させる	このオプションを選択する場合、変更前のパスワードを忘れたユーザーは、システムのロックを解除できなくなるため、ログオン情報を再登録しなければならなくなります。ユーザーがプライマリの認証方法としてスマートカードを使用している場合は、このオプションを選択しないでください。 デフォルト設定：オン
同一性の検証方法（変更前のパスワードまたはセキュリティ用の質問）をユーザーに選択させる	このオプションを選択すると、ユーザーが選択した再認証方法に応じて画面が表示されます。このオプションには、次のサブオプションがあります。 以前のバージョンのユーザー識別方法を使用する 質問ベースの認証またはユーザー識別用の質問を使用していたSingle Sign-On（Password Manager）4.0または4.1環境をアップグレード場合に、このオプションを選択します。この機能では、Single Sign-Onサービスは使用されません。 デフォルト設定：オフ

同一性を検証せずにネットワーク経由でプライマリのデータ保護方法を自動的に復元する

キー管理モジュールを実装して、同一性の検証を行わずユーザーのログオン情報のロックを自動的に解除する場合は、このオプションをクリックします。この方法はほかのデータ保護方法より安全度が低くなりますが、ログオン情報が自動的に取得されるためユーザーにとっては使いやすくなります。

デフォルト設定：オフ

Self-Serviceの機能

以下のオプションを使用するには、キー管理モジュールをインストールする必要があります。このモジュールによって、Windowsのログオン画面にボタンが追加され、ユーザーがパスワードをリセットできるようになります。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［アカウントセルフサービス機能］

プライマリパスワードのリセットを許可する

管理者の介在なしにユーザーがプライマリパスワードをリセットできるようにするかどうかを指定します。

デフォルト設定：オフ

ロックされたアカウントの解除を許可する

ユーザーがロックされたアカウントを解除できるようにするかどうかを指定します。

デフォルト設定：オフ

キー管理モジュール

以下のオプションでは、キー管理モジュールのサービスの場所とポートを指定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［キー管理モジュール］

サービスの場所（キー管理モジュール）

キー管理モジュールのサービスの場所とポートを指定します。設定内容が正しいかどうかを確認するには、［確認］をクリックします。

デフォルト設定：なし

サービスポート：443

プロビジョニングモジュール

プロビジョニングモジュールを使用すると、このユーザー構成に含まれるユーザーに関連付けられているログオン情報を、インポート、変更、および削除できます。これらの作業を行うには、プロビジョニングモジュールの場所とポートを指定する必要があります。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［ユーザー設定］>（既存のユーザー構成）>［ユーザー設定の編集］>［プロビジョニングモジュール］

プロビジョニングを使用する

プロビジョニングを使用するかどうかを指定します。

デフォルト設定：オフ

サービスの場所（プロビジョニングモジュール）

プロビジョニングモジュールのサービスの場所とポートを指定します。設定内容が正しいかどうかを確認するには、［確認］をクリックします。

デフォルト設定：なし

サービスポート：443

アプリケーション定義

Sep 30, 2015

ここでは、アプリケーション定義とオプションについて説明します。ここに記載されている操作手順は、既存のアプリケーション定義を編集するときの操作です。

アプリケーションフォーム

このページを開くには、［アプリケーション定義の編集］ダイアログボックス左側で［アプリケーションフォーム］をクリックします。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［アプリケーション定義］>（既存のアプリケーション定義）>［アプリケーション定義の編集］>［アプリケーションフォーム］>（既存のフォーム定義）>［編集］>［そのほかの設定］

ログオン情報を自動送信する

Single Sign-On Plug-inがログオン情報を入力した後で、［OK］（またはそれに相当するボタン）が自動的にクリックされ、ログオン情報が送信されるようにするか、ユーザーが手動でボタンをクリックするかを指定します。フォームを自動的に送信する場合は、［ログオン情報を自動送信する］チェックボックスをオンにします。

デフォルト設定：オン

アプリケーションのアイコン

［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）のアプリケーションの隣に表示されるアイコンを指定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［アプリケーション定義］>（既存のアプリケーション定義）>［アプリケーション定義の編集］>［アプリケーションのアイコン］

アプリケーションのアイコン

［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）のアプリケーションの隣に表示されるアイコンを指定します。次の2つのオプションがあります。

- デフォルトアイコンを使用する
- カスタムアイコンを使用する（アイコンのパスを入力）

カスタムアイコンを使用する場合は、［参照］をクリックしてアイコンファイルへのパスを指定します。標準のWindowsアイコンファイルを指定できます。Microsoft Windowsの環境変数がサポートされます。

デフォルト設定：デフォルトアイコンを使用する

詳細な検出設定

以下のオプションでは、1回のセッション内で、このアプリケーションの2回目以降のログオンフォームやパスワード変更フォームをSingle Sign-On Plug-inが無視するかどうかを設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［アプリケーション定義］>（既存のアプリケーション定義）>［アプリケーション定義の編集］>［詳細な検出設定］

初回のログオンのみを自動処理する

このアプリケーションへの初回のログオンだけを自動処理して、2回目以降のログオン要求を無視するかどうかを指定します。

デフォルト設定：オフ

初回のパスワード変更のみを自動処理する

このアプリケーションへの初回のパスワード変更要求だけを自動処理して、2回目以降のパスワード変更を無視するかどうかを指定します。

デフォルト設定：オフ

パスワードの有効期限

以下のオプションでは、パスワードの有効期限が切れたときにこのアプリケーションで実行する処理について設定します。Single Sign-Onの有効期限のポリシーは、このアプリケーションに関連付けられているパスワードポリシーで選択されている場合にだけ適用されます。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［アプリケーション定義］>（既存のアプリケーション定義）>［アプリケーション定義の編集］>［パスワードの有効期限］

パスワードの有効期限が切れたときにスクリプトを実行する

パスワードの有効期限が切れたときにスクリプトを実行するかどうかを指定します。実行する場合は、スクリプトファイルの絶対パスを入力します。UNC（Universal Naming Convention）パスは使用できません。

デフォルト設定：オフ

Citrix Single Sign-Onの有効期限警告機能を使用する

パスワードの有効期限が切れたときにCitrix Single Sign-Onの有効期限警告機能を使用するかどうかを指定します。

デフォルト設定：オフ

パスワードポリシー

Sep 30, 2015

ここでは、パスワードポリシーとオプションについて説明します。ここに記載されている操作手順は、既存のパスワードポリシーを編集するときの操作です。［パスワードポリシーの編集］ダイアログボックスを開くには、次の操作を行います。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［パスワードポリシー］>（既存のポリシー）>［パスワードポリシーの編集］

パスワードの基本規則

このページを開くには、［アプリケーション定義の編集］ダイアログボックス左側で［アプリケーションフォーム］をクリックします。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［パスワードポリシー］>（既存のポリシー）>［パスワードポリシーの編集］>［パスワードの基本規則］

パスワードの最小文字数

パスワードに必要な最小文字数を、0～128の数値で指定します。

デフォルト設定：8

パスワードの最大文字数

パスワードに使用できる最大文字数を、1～128の数値で指定します。

デフォルト設定：20

同一文字の最大使用数

パスワードに同一文字を使用できる回数を、1～128の数値で指定します。

デフォルト設定：6

同一文字の最大連続使用数

パスワードに同一文字を連続使用できる回数を、1～128の数値で指定します。

デフォルト設定：4

アルファベット文字の使用規則

以下のオプションでは、パスワードでのアルファベット文字の使用についての規則を設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［パスワードポリシー］>（既存のポリシー）>［パスワードポリシーの編集］>［アルファベット文字の使用規則］

小文字の使用を許可する

パスワードにアルファベットの小文字の使用を許可するかどうかを指定します。

デフォルト設定：オン

パスワードの最初の文字に小文字の使用を許可する

パスワードの最初の文字として小文字の使用を許可するかどうかを指定します。

デフォルト設定：オン

パスワードの最後の文字に小文字の使用を許可する

パスワードの最後の文字として小文字の使用を許可するかどうかを指定します。

デフォルト設定：オン

小文字の最小使用数

パスワードに必要な小文字の最小使用数を、0～128の数値で指定します。

デフォルト設定：0

大文字の使用を許可する

パスワードにアルファベットの大文字の使用を許可するかどうかを指定します。

デフォルト設定：オン

パスワードの最初の文字に大文字の使用を許可する

パスワードの最初の文字として大文字の使用を許可するかどうかを指定します。

デフォルト設定：オン

パスワードの最後の文字に大文字の使用を許可する

パスワードの最後の文字として大文字の使用を許可するかどうかを指定します。

デフォルト設定：オン

大文字の最小使用数

パスワードに必要な大文字の最小使用数を、0～128の数値で指定します。

デフォルト設定：0

数字の使用規則

以下のオプションでは、パスワードでの数字（0～9）の使用についての規則を設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［パスワードポリシー］>（既存のポリシー）>［パスワードポリシーの編集］>［数字の使用規則］

パスワードに数字の使用を許可する

パスワードに数字の使用を許可するかどうかを指定します。

デフォルト設定：オン

パスワードの最初の文字に数字の使用を許可する

パスワードの最初の文字として数字の使用を許可するかどうかを指定します。

デフォルト設定：オン

パスワードの最後の文字に数字の使用を許可する

パスワードの最後の文字として数字の使用を許可するかどうかを指定します。

デフォルト設定：オン

数字の最小使用数

パスワードに必要な数字の最小使用数を、0～128の数値で指定します。

デフォルト設定：0

数字の最大使用数

パスワードで許可される数字の最大使用数を、1～128の数値で指定します。

デフォルト設定：20

特殊文字の使用規則

以下のオプションでは、パスワードでの特殊文字（記号などの非英数字）の使用についての規則を設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［パスワードポリシー］>（既存のポリシー）>［パスワードポリシーの編集］>［特殊文字の使用規則］

パスワードに特殊文字の使用を許可する

パスワードに特殊文字（!、@、#など）の使用を許可するかどうかを指定します。

デフォルト設定：オン

パスワードの最初の文字に特殊文字の使用を許可する

パスワードの最初の文字として特殊文字の使用を許可するかどうかを指定します。

デフォルト設定：オン

パスワードの最後の文字に特殊文字の使用を許可する

パスワードの最後の文字として特殊文字の使用を許可するかどうかを指定します。

デフォルト設定：オン

特殊文字の最小使用数

パスワードに必要な特殊文字の最小使用数を、0～128の数値で指定します。

デフォルト設定：0

特殊文字の最大使用数

パスワードで許可される特殊文字の最大使用数を、0～128の数値で指定します。

デフォルト設定：20

使用を許可する特殊文字

パスワードに使用できる特殊文字を指定します。

デフォルト設定：!@#$^&*()_-+=[]\|,?

禁止文字列

以下のオプションでは、パスワードとしての使用を禁止する文字および文字列について設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［パスワードポリシー］>（既存のポリシー）>［パスワードポリシーの編集］>［禁止文字列］

パスワードに含めることを禁止する文字列

［一覧の編集］をクリックすると、［禁止文字列一覧の編集］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には、パスワードに含めることを禁止する、個々の文字または文字列を256個まで指定できます。文字または文字列は1行ごとに入力します。文字列の長さは最長で32文字です。個々の文字または文字列では、大文字と小文字が区別されません。

デフォルト設定：なし

アプリケーション用のユーザー名をパスワードとして使用することを禁止する

アプリケーションにログオンするときに使用するユーザー名を、パスワードとして使用できるようにするかどうかを指定します。アプリケーション用のユーザー名をパスワードとして使用できないようにするには、このチェックボックスをオンにします。

デフォルト設定：オフ

ユーザー名の一部を使用することも禁止する（アプリケーション用のユーザー名を含むパスワード）

アプリケーションにログオンするときに使用するユーザー名の一部を、パスワードとして使用できるようにするかどうかを指定します。ユーザー名の一部とは、ユーザー名から選び出せる任意の文字列のことです。この設定は、［禁止する文字数］ボックスの設定とも連動します。たとえば、このチェックボックスがオンで［禁止する文字数］ボックスの値が4のとき、ユーザー「citrix」は、「citr」、「itri」、「trix」を含む文字列をパスワードに使用できません。

デフォルト設定：オフ

Windows用のユーザー名をパスワードとして使用することを禁止する

Windowsにログオンするときに使用するユーザー名を、パスワードとして使用できるようにするかどうかを指定します。このチェックボックスがオフの場合は、Windows用のユーザー名をパスワードとして使用できます。この設定は、［禁止する文字数］ボックスの設定とも連動します。たとえば、このチェックボックスがオンで[禁止する文字数］ボックスの値が4のとき、ユーザー「citrix」は、「citr」、「itri」、「trix」を含む文字列をパスワードに使用できません。

デフォルト設定：オフ

パスワードの履歴と有効期限

以下のオプションでは、以前のパスワードを新しいパスワードとして設定できるようにするかどうかと、パスワードの有効期限について設定します。

パスワードの履歴情報は、ユーザーごとに保持されます。ユーザーのパスワードデータをリセットすると、そのユーザーのパスワード履歴も削除されます。

Single Sign-Onのパスワード有効期限オプションでは、有効期限に関する警告メッセージが表示されるだけで、ユーザーは有効期限が切れたパスワードを引き続き使用することができます（アプリケーション側で有効期限が設定されていない場合）。ただし、ユーザーがパスワードを変更するまで、この警告メッセージが表示されます。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［パスワードポリシー］>（既存のポリシー）>［パスワードポリシーの編集］>［パスワードの履歴と有効期限］

以前のパスワードを新しいパスワードとして設定できない

以前のパスワードを新しいパスワードとして設定できるようにするかどうかを指定します。以前のパスワードはパスワード履歴に保持されます。

デフォルト設定：オフ

禁止するパスワード履歴数

パスワード履歴に保持するパスワードの数を、1～24の数値で指定します。

デフォルト設定：1

アプリケーション定義に設定されているパスワードの有効期限を使用する

このチェックボックスがオンの場合は、ここで設定する［パスワードの有効期限が切れるまでの日数］ボックスと［パスワードの有効期限が切れる前にユーザーに警告する日数］ボックスの値が、このポリシーに関連付けられているアプリケーション定義に適用されます。Single Sign-Onのポリシーは、アプリケーション自体に組み込まれている既存のパスワード有効期限設定とは連動しません。

デフォルト設定：オフ

パスワードの有効期限が切れるまでの日数

同じパスワードを継続使用できる最大日数を、1～99999の数値で指定します。

デフォルト設定：42

パスワードの有効期限が切れる前にユーザーに警告する日数

パスワードの有効期限が切れる前にユーザーに警告する日数を、0～99998の数値で指定します。

デフォルト設定：14

パスワードポリシーのテスト

以下のオプションでは、手動で作成したパスワードが定義済みのポリシーに準拠しているかどうかを検証するためのテスト、準拠するパスワードの自動生成、および定義した条件下で十分な数のパスワードを生成できるかどうかの検証を行います。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［パスワードポリシー］>（既存のポリシー）>［パスワードポリシーの編集］>［パスワードポリシーのテスト］

パスワードを入力して準拠性を検証する

［パスワード］ボックスを使用して、手動で作成したパスワードがポリシーに準拠しているかどうかをテストします。手動で作成したパスワードを入力して［検証］をクリックします。入力されたパスワードが定義済みのすべての条件を満たしているかどうかがテストされます。

デフォルト設定：なし

ポリシーに準拠するパスワードをランダムに生成する

このオプションを使用して、現在定義されているパスワード条件を満たすパスワードを生成します。[生成］をクリックすると、ポリシーに準拠するパスワードが生成されます。このパスワードは、Ctrl＋Cキーを押してコピーできます。

デフォルト設定：なし

ポリシーに準拠するパスワードをカウントする

パスワード条件のセットを設定することにより、条件を満たすパスワードの数が制限されることがあります。定義したポリシーに、パスワードに関する組織のニーズを満たすための柔軟性が備わっているかどうかを確認するために、このオプションを使用して、ポリシーに準拠するパスワードを管理者が定義する数だけ生成します。［固有なパスワードのカウント］をクリックすると、管理者が定義する数のパスワードを生成するためのダイアログボックスが開きます。

デフォルト設定：なし

ログオンの設定

以下のオプションを使用して、このポリシーの対象となるアプリケーション定義でパスワードの文字列をユーザーが表示できるようにするかどうか、アプリケーションへのログオン情報の送信前にユーザーの再認証を行うかどうか、ログオンの最大再試行回数、および認証に失敗してからログオン情報を再送信するまでの、ログオンの再試行とみなされる間隔について設定します。

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［パスワードポリシー］>（既存のポリシー）>［パスワードポリシーの編集］>［ログオンの設定］

パスワードの文字列をユーザーが表示することを許可する

このポリシーの対象となるアプリケーションについて、［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）の［文字列の表示］ボタンを有効にするかどうかを指定します。ユーザーがこの[文字列の表示］ボタンを使用す

ると、パスワードの内容を確認することができます。このチェックボックスがオフの場合は、ユーザーはパスワードの内容を表示できません。

デフォルト設定：オフ

アプリケーションへのログオン情報を送信するときにユーザーの再認証を行う

Single Sign-On Plug-inがログオン情報をアプリケーションに送信するときに、ユーザーのプライマリパスワードの入力を要求するかどうかを指定します。このチェックボックスをオンにすると、このポリシーの対象となるアプリケーションが開いたときにワークステーションがロックされます。ユーザーは、プライマリパスワードを入力してロックを解除できます。正しいプライマリパスワードによりワークステーションのロックが解除されると、ログオン情報がアプリケーションに送信されます。重要な機密データにアクセスするアプリケーションに対してこの設定を有効にすると、同一性を確認できないユーザーによるアクセスを防ぐことができます。

デフォルト設定：オフ

ログオンの最大再試行回数

特定の時間内に同一アプリケーションにログオン情報を再送信できる回数を指定します。ここで最小値0を指定すると、初回のログオンに失敗した後でログオン情報を再送信したときにエラーが表示されます。

デフォルト設定：0

ログオン情報の送信を再試行とする時間

ログオン情報の最初の送信に失敗した後で、ここで指定した時間（秒）内に再度ログオン情報を送信すると、再試行として認識されます。

デフォルト設定：30秒

パスワード変更ウィザード

以下のオプションで、パスワード変更用の画面に対するパスワード変更ウィザードの動作について設定します。以下のいずれかのオプションをクリックする必要があります。

- ユーザーがパスワードの作成方法を選択する
- ユーザーがパスワードを作成する
- システムがパスワードを作成し、ユーザーに通知する
- ウィザードを起動せずに自動的にパスワードを作成してアプリケーションに送信する

［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix AppCenter］>［Single Sign-On］>［パスワードポリシー］>（既存のポリシー）>［パスワードポリシーの編集］>［パスワード変更ウィザード］

ユーザーがパスワードの作成方法を選択する

ユーザーに、パスワードの作成方法としてシステムに生成させるか自分で作成するかを選択させる場合は、このオプションをクリックします。

デフォルト設定：オン

ユーザーがパスワードを作成する

ユーザーに、システム生成のパスワードを使用させず、自分で作成させる場合は、このオプションをクリックします。

デフォルト設定：オフ

システムがパスワードを作成し、ユーザーに通知する

ユーザーに、システム生成のパスワードを使用させ、自分で作成することを許可しない場合は、このオプションをクリックします。

デフォルト設定：オフ

ウィザードを起動せずに自動的にパスワードを作成してアプリケーションに送信する

パスワード変更ウィザードをユーザーに表示せず、システム生成のパスワードが自動的に送信されるようにするには、このオプションをクリックします。ユーザーに、パスワード変更画面のフィールドにパスワードが入力されるところが表示され、アプリケーションによってパスワードが正常に変更されたかどうかを示すメッセージが表示される可能性があります。

デフォルト設定：オフ

運用

Sep 30, 2015

Single Sign-Onでは、Single Sign-On Plug-inまたはユーザーによるイベントを、ローカルコンピューター上のWindowsアプリケーションログに記録することができます。これらのイベントは、情報、警告、またはエラーとして分類されます。警告イベントおよびエラーイベントは、常に記録されます。情報イベントに対するログ機能を有効にするには、ユーザー構成を作成した後で、管理コンソールを使用します。

Single Sign-Onでは、Hot Desktop、スマートカード、ライセンス、およびSingle Sign-Onサービスに関するイベントが記録されます。イベントログには、FIPS（Federal Information Processing Standard）やHIPAA（Health Insurance Portability and Accountability Act of 1996）に準拠するために定期的に監視すべきセキュリティ関連のイベントが記録されます。また、これらの情報を参照して、Single Sign-On環境のセキュリティを向上させることもできます。

XenApp環境でSingle Sign-Onを使用している場合は、ユーザーやセッションを特定するための情報（失敗したログオン試行など）もイベントログに記録されます。このログ機能は、デフォルトで無効になっています。

情報イベントログを有効にするには

1. コンソールツリーで既存のユーザー構成を選択し、［操作］メニューから［ユーザー設定の編集］を選択します。［ユーザー設定の編集］ダイアログボックスが開きます。
2. ［クライアント側の動作］ページを開きます。
3. ［Citrix Single Sign-Onイベントを Windowsのイベントログに記録する］チェックボックスをオンにします。

次の表は、Single Sign-Onで記録される標準的なイベントの一覧です。

イベント
ログオン試行の失敗（Single Sign-Onの認証）
Single Sign-Onへのユーザー認証が失敗して、中央ストアへのアクセスが拒否されると記録されます。
ログオン試行の成功（Single Sign-Onの認証）
Single Sign-Onへのユーザー認証が成功して、中央ストアにアクセスできると記録されます。
ログオン試行（ログオン情報の送信）
外部アプリケーションへのログオン情報の送信イベントが記録されます。
ログオン情報の操作
パスワードの変更、パスワード文字列の表示、ユーザー識別処理など、パスワード関連のイベントが記録されます。
同期処理の失敗（通信）
通信の問題により中央ストアとの同期処理に失敗すると記録されます。
同期処理の失敗（権限）
アクセス権の問題（不正なアカウントなど）により中央ストアとの同期処理に失敗すると記録されます。

スマートカードのDataProtect暗号化/復号化エラーイベント
スマートカードデータの暗号化/復号化処理に関連した一般的な失敗イベントが記録されます。
スマートカードのDataProtect暗号化/復号化エラー（カード未検出）
スマートカードにアクセスできないと記録されます。
Single Sign-On Plug-inの起動と終了
スマートカードにアクセスできないと記録されます。
破損または損失したDLLファイル
DLLファイルを正しく読み込めないと記録されます。

次の表は、Single Sign-Onで記録されるHot Desktopイベントの一覧です。

Hot Desktopイベント
Hot Desktopセッションへのログオン失敗
セッションの開始時に重大なエラーが発生した場合にのみ記録されます。
Hot Desktopセッションへのログオン成功
ユーザー認証に成功してHot Desktopセッションが開始されると記録されます。
Hot Desktopセッションへのログオフ失敗
セッションの停止時に重大なエラーが発生した場合にのみ記録されます。
Hot Desktopログオフ成功
ユーザーまたはタイムアウトによりHot Desktopセッションが停止されると記録されます。

mfrmlist.iniファイル

Sep 30, 2015

mfrmlist.iniファイルには、ターミナルエミュレーターと、Single Sign-Onで監視するHLLAPI DLLの場所の一覧が含まれています。このファイルは、次のフォルダーにインストールされます。

%APPDATA%\Citrix\MetaFrame Password Manager\Helper\MFEmu

Single Sign-On Plug-inがアプリケーションを認識しない

Sep 30, 2015

登録済みのログオン情報が、Single Sign-Onでアプリケーションに正しく入力されないことがあります。この問題は、以下の原因などにより発生します。

- Webアプリケーションが変更され、既存のアプリケーション定義が正しく動作しなくなった。
- アプリケーション定義が正しく構成されていない。

ログオン情報が送信されない原因を特定するために、まず次の作業を行います。

- すべての設定について競合が起きていないか確認する。
- Single Sign-On Plug-inがアプリケーションを検出するように構成されていることを検証する。
- Single Sign-On Plug-inと管理コンソール側のアプリケーション定義を比較する。
- ログオン情報が正しく送信されるまで、アプリケーション定義からマッチ条件や送信フィールドの定義を1つずつ削除する。

重要：Single Sign-Onには、アプリケーション定義、パスワードポリシー、ユーザー構成、およびユーザー識別の方法を定義するための、さまざまな設定が用意されています。矛盾する設定を作成すると、アプリケーションにログオン情報が送信されないなどの問題が発生する場合があります。
これらの作業を行っても問題が解決されない場合は、次の「Webアプリケーション」、および「ホストベースのアプリケーション」を参照してください。

Webアプリケーション

- ［URLの完全マッチ］オプションの設定の検証
  1. AppCenterの［Single Sign-On］ノードで、既存のWebアプリケーション定義を選択します。
  2. ［操作］メニューから、［アプリケーション定義の編集］を選択します。
  3. ［アプリケーション定義の編集］ダイアログボックス左側で［アプリケーションフォーム］をクリックし、［定義済みのフォーム］ボックスの一覧からアプリケーションフォームを選択して［編集］をクリックします。
  4. ［アプリケーションフォームの編集］ダイアログボックス左側で［フォームID］をクリックします。このページで、［URLの完全マッチ］チェックボックスと［URLの大文字/小文字を区別する］チェックボックスの設定を確認できます。
  5. HTML準拠のフィールドタイプが使用されていることを確認します。Webアプリケーションを正しく認識するには、そのWebページでHTML準拠のフィールドタイプが使用されている必要があります。未定義のフィールドタイプまたはユーザーが独自に定義したフィールドタイプは、Single Sign-Onで認識されません。

- Internet Explorer 8のInPrivateブラウズ機能を使用する場合は、［InPrivateブラウズを開始したら、ツールバーと拡張機能を無効にする］チェックボックスがオフであることを確認してください。詳しくは、Microsoft社のWebサイトで、Internet Explorerのプライバシー機能について確認してください。

ターミナルエミュレーターベースのアプリケーション

ターミナルエミュレーターベースのアプリケーションのアプリケーション定義は、アプリケーション定義ウィザードとフォーム定義ウィザードを使用して作成します。ユーザー構成にアプリケーション定義を追加するときに、必ずターミナルエミュレーターのサポートを有効にしてください。

- mfrmlist.iniファイルにターミナルエミュレーターが定義されていることを確認する
  Single Sign-Onとターミナルエミュレーターとの連動を制御するssomho.exeプロセスは、mfrmlist.iniファイルに定義されているエミュレーターのみを認識します。ssomho.exeプロセスは、このINIファイルに定義されていないターミナルエミュ

レーターとの通信を行いません。

- 短いセッション名が指定されていることを確認する
  ssomho.exeプロセスは、短いセッション名を使ってHLLAPI DLLと通信を行います。短いセッション名がなくてもssomho.exeは読み込まれますが、画面のアクティビティは監視されません。短いセッション名は、クライアントコンピューター上のターミナルエミュレーターで構成します。

- ssomho.exeプロセスが実行されていることを確認する
  ssomho.exeが実行されていることを確認するには、次の手順に従います。
  1. Single Sign-On Plug-inが動作するコンピューター上でタスクマネージャーを開き、［プロセス］タブをクリックします。
  2. ［イメージ名］列をクリックして、一覧をイメージ名順に並べ替えます。
  3. 一覧にssomho.exeがあることを確認します。

  ssomho.exeプロセスが一覧に表示されない場合は、ssomho.exeプロセスがHLLAPI DLLを検索できないか、サードパーティ製のターミナルエミュレーターに関する問題によってssomho.exeプロセスが中止された可能性があります。

  注：タスクマネージャーの一覧にssomho.exeプロセスが表示される場合でも、このプロセスがHLLAPI DLLと通信していないことがあります。その場合は、短いセッション名が指定されていることを確認してください。
- 各エミュレーターを個別にテストする
  同一のコンピューター上に、複数のHLLAPI準拠のエミュレーターがインストールされている場合、ssomho.exeはすべてのエミュレーターと通信しようとします。いずれかのHLLAPI DLLに問題があると、ssomho.exeプロセスが不安定になることがあります。この場合、個々のターミナルエミュレーターをテストして、問題があるエミュレーターを特定します。

  個々のエミュレーターをテストするには、テストするエミュレーター以外のものを削除するか、mfrmlist.iniファイルでコメントアウトします。

ターミナルエミュレーターのサポート

Sep 30, 2015

Single Sign-Onで、ターミナルエミュレーターのHLLAPIサポート機能を有効にするには、管理コンソールでユーザー構成を開き、ターミナルエミュレーターのサポートを有効にする必要があります。

ターミナルエミュレーターのサポート機能を有効にすると、SSOShellがssomho.exeプロセスを開始します。このプロセスでは、最初に%ProgramFiles%\Citrix\MetaFrame Password Manager\Helper\MFEmuにあるMfrmlist.iniファイルが読み取られた後、そのファイルに定義されているすべてのエミュレーターが検出され、HLLAPI準拠のDLLファイルがロードされます。

mfrmlist.iniに、HLLAPI準拠のエミュレーターの定義を追加することもできます。

ssomho.exeプロセスは、mfrmlist.iniファイルで変更されていない限り、HKEY_LOCAL_MACHINEɪSOFTWAREハイブからHLLAPI準拠のDLLファイルの場所を取得します。

一部のターミナルエミュレーターでは、DLLファイルの場所がHKEY_CURRENT_USERハイブに格納されます。この場合、mfrmlist.iniファイルでパスを指定する必要があります。

エミュレーターのサポート機能を構成するには

テスト済みのエミュレータープログラムとSingle Sign-Onが連動するように設定するには、エミュレーターソフトウェアをインストールしてからエミュレーターセッションを作成し、そのエミュレーターセッションを検出するためのアプリケーションの定義を作成します。

1. ターミナルエミュレーターソフトウェアをインストールして、コンピューターを再起動します。
2. ターミナルエミュレーターソフトウェアを起動して、画面（ディスプレイ）と接続を定義した新しいセッションを作成します。
3. 短いセッション名を設定します。
4. HLLAPIサポートを有効にします。
   注：Impotant使用するセッションごとに、個別のアプリケーション定義が必要です。Single Sign-On Plug-inは、アプリケーション定義の行と列に指定されている文字列とホストベースのアプリケーション画面の文字列を照合してセッションを検出し、アプリケーション定義の行と列に含まれている情報に基づいて、ログオン情報を送信します。そのため、セッションごとに、個別のホストベースアプリケーション定義を設定する必要があります。
5. セッションを保存して終了します。
6. ターミナルエミュレーターを終了します。
7. アプリケーション定義を作成します。
8. 管理コンソールを開き、ユーザー構成の［ターミナルエミュレーターのサポートを有効にする］チェックボックスがオンになっていることを確認します。
9. エミュレーターを実行し、セッションを開きます。
10. Single Sign-On Plug-inを起動または更新します。

接続画面が認識され、ユーザーがログオン情報を登録できる画面が表示されます。

Single Sign-On Plug-inが起動しない

Sep 30, 2015

Single Sign-On Plug-inは、クライアントコンピューター（Windows Server 2008、Windows Server 2008 R2、Windows Vista、またはWindows 7が動作する場合を除く）に最後にインストールするGINA変更ソフトウェアである必要があります。インストールされているSingle Sign-On Plug-inが正しく起動しない場合は、GINAチェーンの設定が正しくない可能性があります。Single Sign-On Plug-inをインストールした後で、ほかのGINA変更ソフトウェアをインストールまたはアップグレードすると、Windows GINAチェーンが変更されてしまうことがあります。たとえば、スマートカード認証対応のソフトウェア、Symantec、XenAppなどのソフトウェアをインストールまたはアップグレードすると、Windows GINAチェーンが変更されることがあります。

Single Sign-On Plug-inをインストールした後でほかのGINA変更ソフトウェアをインストールまたはアップグレードする場合は、まずSingle Sign-On Plug-inをアンインストールしてください。ほかのソフトウェアのインストールやアップグレードが完了したら、Single Sign-On Plug-inを再インストールします。これにより、Single Sign-On Plug-inが使用する正しいDLLファイルがインストールされ、Windowsレジストリに登録されます。

推奨される再インストール手順

1. GINAチェーンを変更するサードパーティ製ソフトウェアをアンインストールします。
2. Single Sign-On Plug-inをアンインストールします。
3. サードパーティ製ソフトウェアをインストールします。
4. Single Sign-On Plug-inを再インストールします。

インストールまたはアップグレードしたサードパーティ製のソフトウェアによりWindows GINAチェーンが変更された可能性がある場合は、レジストリでGINA.dllエントリをチェックしてください。コンピューター上にGINAチェーンのDLLファイルがあり、適切な場所にインストールされていることを確認してください。コンピューターにGINAチェーンのDLLファイルがインストールされていない場合は、いったんSingle Sign-On Plug-inをアンインストールしてから再インストールします。その場合、Windowsレジストリは編集しないでください。

重要：GINAチェーンを変更した複数のソフトウェアをアンインストールするときは、インストール時と逆の順番でアンインストールする必要があります。アンインストールする順番を間違えると、システムに問題が生じることがあります。また、WindowsレジストリのGINA設定は変更しないでください。

新しい署名証明書の作成

Sep 30, 2015

署名証明書の期限が切れる直前と切れた時点に、イベントログアラートが生成されます。このアラートが表示されないようにするには、CtxCreateSigningCert.exeを実行して、新しい証明書を作成します。新しい証明書のキーを使って、中央ストアのデータに署名を追加するには、データ署名ツール（CtxSignData.exe）を使用します。

Single Sign-Onサービスを構成した後は、次の場合を除き、新しい署名証明書を作成する必要はありません。

- 署名証明書の期限がもうすぐ切れるか、既に切れている。
- 署名証明書が改ざんされている可能性がある。

新しい証明書を作成するには、コマンドプロンプトを開き、%ProgramFiles%\Citrix\MetaFrame Password Manager\Service フォルダーからSingle Sign-on Serviceを実行しているコンピューターのコマンドプロンプトで「CtxCreateSigningCert.exe」と入力します。

公開キーと秘密キーの証明書ファイルの名前を入力し、署名証明書の有効期限を月単位で入力します。新しい証明書が作成されます。

CtxCreateSigningCertコマンドの構文は、次のとおりです。	
構文	CtxCreateSigningCert public_cert private_cert expiration_period
各オプションの意味は次のとおりです。	public_cert = 公開キーの証明書ファイルの名前 private_cert = 秘密キーの証明書ファイルの名前 expiration_period = 証明書の有効期限（月単位）
例：	ctxcreatesigningcert C:\PublicKeyCert.cert C:\PrivateKeyCert.cert 12

データの署名/署名の削除/再署名/検証

Sep 30, 2015

中央ストアのデータの署名、署名の削除、再署名、および検証を行うには、データ署名ツール（CtxSignData.exe）を使用します。このコマンドラインツールはインストールメディアのServiceフォルダーに収録されています。また、Single Sign-Onサービスのホストサーバーの%ProgramFiles%\Citrix\MetaFrame Password Manager\Service\SigningToolにもインストールされます。

注：データ署名ツールは、Single Sign-Onサービスのデータの整合性チェックモジュールと一緒にインストールされます。Single Sign-Onを初めてインストールしたときにこのモジュールをインストールしなかった場合は、後でインストールすることができます。
データ署名ツールを開始するには、Single Sign-Onサービスのホストサーバーでコマンドプロンプトを開き、「CtxSignData.exe」を入力して適切なコマンドラインパラメーター（-s、-r、-u、-v）を使用します。

データの署名（-sオプション）

環境に未署名のデータがある場合に、データの整合性チェックを有効にするには、-sオプションを指定してCtxSignDataコマンドを実行します。

注：データの整合性チェックを実装せずにSingle Sign-On環境の運用を開始し、後で整合性チェックを実装する場合は、データ署名ツールを使って、中央ストア内の既存のデータに署名を追加しなければなりません。
このオプションには、パラメーターとして署名証明書のファイル名、Single Sign-OnサービスのURI（Uniform Resource Identifier）、中央ストアの場所と種類（NTFSネットワーク共有またはActive Directory）を指定します。このコマンドを実行すると、中央ストアにあるすべてのデータが読み取られ、新しい証明書を使って署名されます。

CtxSignDataコマンドに-sオプションを指定する場合の構文は以下のとおりです。

CtxSignData [-s service_path certificate_file centralstore_location NTFS|AD]
各項目の意味は次のとおりです。

-s	中央ストアにあるデータファイルに署名します。
service_path	Single Sign-OnサービスのURI形式のパス。
certificate_file	データの署名または再署名に使用する証明書ファイルの名前。
centralstore_location	中央ストアのUNC（Universal Naming Convention）パス、またはActive Directoryのドメインコントローラーの DNS（Domain Name System）。
NTFS|AD	中央ストアの種類。次のいずれかを指定します。 ● NTFS = Microsoft NTFSネットワーク共有 ● AD = Microsoft Active Directory

たとえば、以下のように使用します。

ctxsigndata -s “mpmserver.mycompany.com/MPMService” “C:\priv12mos.cert” “\\MPMCentralServer\citrixsync$” NTFS
ctxsigndata -s mpmserver.mycompany.com/MPMService “C:\priv12mos.cert” DC1.mycompany.com AD

データの再署名（-rオプション）

既存の署名証明書の期限切れが迫っているか、既に切れている、または証明書が改ざんされている可能性があり、データに署名し直す必要がある場合は、-rオプションを指定してCtxSignDataコマンドを実行します。このオプションには、パラメーターとして署名証明書のファイル名、Single Sign-OnサービスのURI、中央ストアの場所と種類（NTFSネットワーク共有またはActive Directory）を指定します。このコマンドを実行すると、中央ストアにあるすべてのデータが読み取られて検証され、新しい証明書を使って署名さ

れます。この場合は、既にデータの整合性チェックが有効になっているので、管理コンソールやSingle Sign-On Plug-inで設定を変更する必要はありません。

破損したデータを再署名するには、以下の手順に従います。

1. Citrix AppCenterを開き、問題のユーザー構成を選択します。
2. 操作ペインの［ユーザー設定の編集］をクリックして［ユーザー設定の編集］ダイアログボックスを開き、中央ストアの設定データが表示されるかどうかを確認します。
3. ［ユーザー設定の編集］ダイアログボックスを閉じて、破損していない新しいデータを中央ストアに格納します。
4. 署名ツール（CtxSignDataコマンド）を使用して、中央ストア内のデータを再署名します。

注：不正行為によりデータが破損したと判断される場合は、上記の手順をすべてのユーザー構成に対して行うことをお勧めします。これにより、信頼できないデータに署名することを避けることができます。
CtxSignDataコマンドに-rオプションを指定する場合の構文は以下のとおりです。

CtxSignData [-r service_path certificate_file centralstore_location NTFS|AD]
各項目の意味は次のとおりです。

-r	中央ストアにあるデータファイルに再署名します（-vオプションの動作も行います）。
service_path	Single Sign-OnサービスのURI形式のパス。
certificate_file	データの署名または再署名に使用する証明書ファイルの名前。
centralstore_location	中央ストアのUNC（Universal Naming Convention）パス、またはActive Directoryのドメインコントローラーの DNS（Domain Name System）。
NTFS|AD	中央ストアの種類。次のいずれかを指定します。 ● NTFS = Microsoft NTFSネットワーク共有 ● AD = Microsoft Active Directory

たとえば、以下のように使用します。

ctxsigndata -r “mpmserver.mycompany.com/MPMService” “C:\priv12mos.cert” “\\MPMCentralServer\citrixsync$” NTFS
ctxsigndata -r mpmserver.mycompany.com/MPMService “C:\priv3mos.cert” DC1.mycompany.com AD

データの署名の削除（-uオプション）

データの整合性チェックを無効にするには、-uオプションを指定してCtxSignDataコマンドを実行します。このオプションには、パラメーターとして署名証明書のファイル名、Single Sign-OnサービスのURI、中央ストアの場所と種類（NTFSネットワーク共有またはActive Directory）を指定します。このコマンドを実行すると、中央ストアにあるすべてのデータが検証なしで読み取られ、署名が削除されます。

CtxSignDataコマンドに-uオプションを指定する場合の構文は以下のとおりです。

CtxSignData [-u centralstore_location NTFS|AD]
各項目の意味は次のとおりです。

-u	中央ストアにあるすべてのデータファイルの署名を削除します。
centralstore_location	中央ストアのUNC（Universal Naming Convention）パス、またはActive Directoryのドメインコントローラーの DNS（Domain Name System）。
NTFS|AD	中央ストアの種類。次のいずれかを指定します。

	• NTFS = Microsoft NTFSネットワーク共有 • AD = Microsoft Active Directory

たとえば、以下のように使用します。

ctxsigndata -u “\\MPMCentralServer\citrixsync$” NTFS
ctxsigndata -u DC1.mycompany.com AD

データの検証（-vオプション）

中央ストアにあるすべてのデータの署名を検証するには、-vオプションを指定してCtxSignDataコマンドを実行します。このオプションには、パラメーターとして署名証明書のファイル名、Single Sign-OnサービスのURI、中央ストアの場所と種類（NTFSネットワーク共有またはActive Directory）を指定します。このコマンドを実行すると、中央ストアにあるすべてのデータが読み取られて検証され、署名されます。

CtxSignDataコマンドに-vオプションを指定する場合の構文は以下のとおりです。

CtxSignData [-v service_path centralstore_location NTFS|AD]
各オプションの意味は次のとおりです。

-v	中央ストアにあるデータファイルの署名を検証します。
service_path	Single Sign-OnサービスのURI形式のパス。
centralstore_location	中央ストアのUNC（Universal Naming Convention）パス、またはActive Directoryのドメインコントローラーの DNS（Domain Name System）。
NTFS|AD	中央ストアの種類。次のいずれかを指定します。 • NTFS = Microsoft NTFSネットワーク共有 • AD = Microsoft Active Directory

たとえば、以下のように使用します。

ctxsigndata -v “mpmserver.mycompany.com/MPMService” “\\MPMCentralServer\citrixsync$” NTFS
ctxsigndata -v mpmserver.mycompany.com/MPMService “https://mpmserver.mycompany.com/MPMService” DC1.mycompany.com AD

ヘルプの表示（-hオプション）

CtxSignDataコマンドのヘプルを表示するには、-hオプションを使用します。

CtxSignDataコマンドに-hオプションを指定する場合の構文は以下のとおりです。

CtxSignData [-h]
各オプションの意味は次のとおりです。

-h	ヘルプを表示します。

たとえば、以下のように使用します。

ctxsigndata -h

Single Sign-On Plug-inでデータの整合性チェック機能を有効/無効にする

Sep 30, 2015

Single Sign-Onでデータの整合性チェック機能を有効にしたり無効にしたりするには、次のレジストリ値を変更します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\PerformIntegrityCheck

種類：REG_DWORD

値のデータ：

0（データの整合性チェック機能を無効にする）

1（データの整合性チェック機能を有効にする）

ほかの中央ストアへのデータの移動

Sep 30, 2015

パスワードポリシー、アプリケーションテンプレート、アプリケーション定義、セキュリティ用の質問などのSingle Sign-Onの管理データを移行しなければならないことがあります。次のような状況で、データの移行が必要です。

- ユーザーが新しいドメインに移動する。
- Single Sign-On環境に新しいサーバーを追加する。
- 新しいドメインが追加されたため、Single Sign-Onのアカウントの関連付け機能の使用を開始する。
- 既存のドメイン間でアカウントの関連付け機能の使用を開始する。
- テスト環境で使用していたSingle Sign-Onを実稼働環境に移行する。

管理データを移行するには、Citrix AppCenterで2段階の操作を行います。まず管理コンソールで既存の管理データをエクスポートして、次にそのデータを新しい環境にインポートします。また、ほとんどの場合、ユーザーを新しい中央ストアにリダイレクトする必要があります。

次の表に、［管理データのエクスポート］オプションで移行できるデータと、移行できないデータを示します。

移行される	移行されない
パスワードポリシー（デフォルトのポリシーとドメインポリシーを除く）	ユーザー構成
アプリケーションテンプレート	Peopleフォルダー
アプリケーション定義	アプリケーショングループ
セキュリティ用の質問と質問グループ	ユーザーのログオン情報
	質問リスト
	Single Sign-Onサービスデータ

Single Sign-Onサービスをほかの中央ストアに移行することはできません。Single Sign-Onサービスを使用している場合は、新しい中央ストアでSingle Sign-Onサービスをインストールして、ほかのデータの移行後に一時的に新旧の中央ストアでサービスを実行する必要があります。

注意：セルフサービス機能やデータの整合性チェック機能がインストールされている場合、またはユーザー構成の[Single Sign-On Plug-in終了時にユーザーのデータフォルダーとレジストリキーを削除する］オプションが有効な場合は、データの移行時に追加操作が必要になります。
現在の中央ストアにあるユーザー構成を、自動的に別の中央ストアに移行することはできません。ユーザー構成を作成し直し、新しい中央ストアにユーザーをリダイレクトする必要があります。これにより、Single Sign-On Plug-inが元の中央ストアと同期するときに、値が変更されていることが認識され、ユーザーのログオン情報が新しい中央ストアにコピーされます。

新しい中央ストアへのデータの移行

管理データのエクスポートウィザードを使用すると、中央ストアに格納されているすべてのアプリケーション定義、アプリケーションテンプレート、パスワードポリシー、セキュリティ用の質問、および質問グループをエクスポートできます。このウィザードでは、エクスポートするデータの種類を指定できますが、個々のサブセットを指定することはできません。たとえば、古い中央ストアからパスワードポリシーをエクスポートする場合、すべてのポリシーがエクスポート対象になり、個々のポリシーを対象から除外することはできません。

ただし、［アプリケーション定義のエクスポート］コマンドでは、アプリケーション定義を個別にエクスポートできます。

注意：セルフサービス機能やデータの整合性チェック機能がインストールされている場合、またはユーザー構成の[Single Sign-On Plug-in終了時にユーザーのデータフォルダーとレジストリキーを削除する］オプションが有効な場合は、データの移行時に手作業による操作が必要になります。

管理データをエクスポートするには

1. Citrix AppCenterで、移行元の中央ストアに接続している状態で［Single Sign-On］ノードをクリックし、［操作］メニューの［管理データのエクスポート］を選択します。
2. 管理データのエクスポートウィザードの指示に従って操作します。

管理データをインポートするには

1. 新しいマシン上にSingle Sign-on管理コンソールをインストールして起動し、［検出の設定と実行］をクリックします。
   注：検出の設定と実行ウィザードの指示に従って、データの移行先の中央ストアを指定します。
2. Citrix AppCenterで移行先の中央ストアに接続し、［Single Sign-On］ノードをクリックして［操作］メニューの［管理データのインポート］を選択します。
3. 管理データのインポートウィザードの指示に従って操作します。
4. 新しいユーザー構成を作成します。
5. Citrix AppCenterで、移行元の中央ストアに接続している状態で移行済みのユーザー構成を選択し、［操作］メニューの［ユーザーのリダイレクト］を選択します。［ユーザーのリダイレクト］ダイアログボックスで、移行先の中央ストアを指定します。 必要に応じて、この手順を繰り返します。
6. すべてのユーザーが少なくても1回ログオンしたことを確認します。 すべてのユーザーがログオン済みであることを確認したら、移行元の中央ストアおよびサー

スを停止できます。

[Single Sign-On Plug-in終了時にユーザーのデータフォルダーとレジストリキーを削除する]オプションが有効な場合に中央ストアを移行するには

ユーザー構成の［Single Sign-On Plug-in終了時にユーザーのデータフォルダーとレジストリキーを削除する］オプションを有効にしている環境では、以下の手順でユーザーの管理データを新しい中央ストアに移行します。この手順に従わないと、ユーザーがコンピューターにログオンするたびに、質問ベースの認証または暗号キーの自動復元による再登録が必要になります。これは、Single Sign-On Plug-in終了時にユーザーの管理データが削除されるためです。

1. 新しい中央ストアに管理データを移行します。
2. Citrix AppCenterで移行先の中央ストアに接続し、新しいユーザー構成を作成します。 このとき、［Single Sign-On Plug-in終了時にユーザーのデータフォルダーとレジストリキーを削除する］チェックボックスをオフにしておきます。
3. Citrix AppCenterで、移行元の中央ストアに接続している状態で移行済みのユーザー構成を選択し、［操作］メニューの［ユーザーのリダイレクト］を選択します。［ユーザーのリダイレクト］ダイアログボックスで、移行先の中央ストアを指定します。 必要に応じて、この手順を繰り返します。
4. すべてのユーザーが少なくても1回ログオンしたことを確認します。
5. ユーザーのコンピューターのレジストリを変更するスクリプトを作成して、新しい中央ストアの種類および場所を設定します。 次の表は、中央ストアの種類に応て使用されるレジストリ設定の一覧です。

中央ストアの種類	変更前	変更後
NTFSからNTFS	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =
NTFSからActive Directory	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = ADSyncPath
Active DirectoryからNTFS	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = ADSyncPath	HKEY_Local_Machine\SOFTWARE\Citrix\Metaframe Password Manager\Extensions\SyncManager\Syncs\DefaultSync\SSOSyncType = FileSyncPath HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\Syncs\DefaultSync\Servers\Server1 =

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

6. Citrix AppCenterで移行先の中央ストアに接続し、新しいユーザー構成の［Single Sign-On Plug-in終了時にユーザーのデータフォルダーとレジストリキーを削除する］チェックボックスをオンにします。 すべてのユーザーがログオン済みであることを確認したら、移行元の中央ストアおよびサービスを停止できます。

アプリケーション定義をエクスポートする

単一または複数のアプリケーション定義をXMLファイルにエクスポートすることができます。

単一のアプリケーション定義をエクスポートするには

1. Citrix AppCenterで、移行元の中央ストアに接続している状態で［Single Sign-On］ノードの［アプリケーション定義］ノードを開きます。
2. エクスポートするアプリケーション定義を選択し、［操作］メニューから［アプリケーション定義のエクスポート］を選択します。
3. アプリケーション定義のエクスポートウィザードの指示に従って操作し、アプリケーション定義をエクスポートします。エクスポートしたデータを後でインポートする場合は、インポートするコンピューターからアクセス可能な場所にエクスポートします。

複数のアプリケーション定義をエクスポートするには

1. Citrix AppCenterで、移行元の中央ストアに接続している状態で［Single Sign-On］ノードの［アプリケーション定義］ノードを開きます。
2. ［操作］メニューから、［アプリケーション定義のエクスポート］を選択します。
3. ウィザードの指示に従って操作し、目的のアプリケーション定義をすべて選択してエクスポートします。

サービスデータをバックアップするには

組織で定期的にバックアップを行っている場合は、Single Sign-Onの中央ストアとそのデータ、証明書、公開キーファイル、および秘密キーファイルが自動的にバックアップされるように設定してください。

重要：中央ストアがNTFSネットワーク共有に格納されている場合は、バックアッププログラムからアクセスできるように、これらのファイルのWindowsのアクセス許可を変更する必要があります。

1. サービスの設定ツールを実行してサービスを設定したときに行った設定を書き留めます。
2. CtxMoveServiceData.exeを使用して、サービスのデータを安全なファイル共有またはディスクにエクスポートします。
   1. コマンドプロンプトで、%ProgramFiles%\Citrix\Metaframe Password Manager\Service\Toolsに移動します。
   2. 「CtxMoveServiceData.exe –export \\server\share\backupfile」と入力します。
      注：パスに環境変数を使用しないでください。
   3. パスワードの入力を求めるメッセージが表示されるので、任意のパスワードを入力し、 このパスワードを書き留めておきます。
      重要：バックアップファイルに保存したサービスのデータはこのパスワードで暗号化されます。パスワードを紛失しないように注意してください。
   4. パスワードの確認入力を求めるメッセージが表示されるので、パスワードを再度入力します。
   5. バックアップファイルが作成されたことを確認します。

サービスデータを復元するには

1. インストールメディアを使用してサービスをインストールします。
2. バックアップを行う前に書き留めた情報を使用して、サービスを適切に構成します。
   注：データの整合性チェック機能を使用する場合は、データの整合性チェックモジュールがインストールされているサーバーの場所が変更されていないか確認し、適切に構成します。
3. 設定を完了し、サービスを起動します。 サービスが起動した後は、必要に応じて直ちにサービスを停止できます。
4. CtxMoveServiceData.exeを使用して、サービスのデータを安全なファイル共有またはディスクからインポートします。
   1. コマンドプロンプトで、%ProgramFiles%\Citrix\Metaframe Password Manager\Service\Toolsに移動します。
   2. 「CtxMoveServiceData.exe –import <\\server\share\backupfile>」と入力します。
   3. パスワードの入力を求めるメッセージが表示されるので、バックアップ時に作成したパスワードを入力します。
   4. AKR.DATを上書きするかどうかを確認するメッセージが表示されるので、[Yes] を選択します。
5. サービスを再起動します。 これで、サービスを使用することができます。

中央ストアから削除されたオブジェクトを参照しているオブジェクトを削除する

CtxFileSyncCleanコマンドを実行すると、NTFSネットワーク共有の中央ストアで、削除済みのオブジェクトを参照している設定データファイルを削除できます。このコマンドでは、削除されたユーザーのユーザーデータファイルは削除されません。CtxFileSyncCleanコマンドは、インストールメディアのToolsフォルダーから実行できます。

アプリケーション定義拡張機能

Jul 22, 2016

通常は、Citrix AppCenterとアプリケーション定義ツールを使用してアプリケーション定義を作成できますが、一部のアプリケーションではアプリケーションの検出、ログオン情報の送信などを行うために別の方法が必要な場合があります。

このようなアプリケーションをサポートするための外部プロセスを作成する開発者は、Citrix AppCenterのアプリケーション定義拡張機能とアプリケーション定義ツールを使用して、その外部プロセスを起動する条件と方法を構成できます。

Single Sign-On Plug-inでの操作

アプリケーション定義拡張機能には、以下の2種類があります。

- フォーム識別拡張機能
  そのアプリケーションが、ユーザーのログオン情報についての管理アクションを必要とするフォームかどうか外部プロセスを使用して判断します。これらの外部プロセスは、フォーム定義のほかのウィンドウ検出アルゴリズムの代わりに使用したり、組み合わせて使用したりできます。

- アクション拡張機能
  ユーザーのログオン情報についての管理アクションを外部プロセスを使用して実行します。これらの外部プロセスは、フォーム定義のほかのウィンドウ検出アルゴリズムの代わりに使用したり、組み合わせて使用したりできます。

単一のフォーム定義に対して、フォーム識別拡張機能とアクション拡張機能のどちらかまたは両方を構成できます。

フォーム識別拡張機能

Single Sign-On Plug-inでは、アプリケーションのインスタンス化、URLのロード、HTMLページドキュメントの取得完了通知などのデスクトップイベントがリスナーフックにより検出されます。

これらのイベントが発生すると、無視、ログオン、パスワードの変更など、ユーザーのログオン情報についての管理アクションが必要かどうか判断されます。この判断は、アプリケーションによって提示される特性と、フォームを一意に特定する定義済みの特性を比較することによって行われます。これらの特性にはWindowsタイトルと実行可能ファイル名が含まれ、必要な場合はそのほかの条件も詳細マッチ特性として定義できます。フォームを識別するために外部プロセスを使用する場合は、詳細マッチ特性としてフォーム識別拡張機能を定義します。

フォームを識別するために外部プロセスが必要な場合は、フォーム定義でそのプロセスを指定します。フォーム定義には、フォーム識別拡張機能および関連するパラメーターの情報が含まれます。これらの情報はレジストリ設定に直接関連付けられます。

Single Sign-On Plug-inによって基本および詳細のマッチアルゴリズムが処理された後で、外部プロセスを使用するフォーム識別拡張機能が評価されます。

単一のフォームを評価するために複数のフォーム識別拡張機能が定義されているときは、［フォーム識別拡張機能］ページに表示されている順に各拡張機能が実行されます。

Single Sign-On Plug-inは、各拡張機能について、外部プロセスの終了をレジストリに設定されている時間だけ待機し、その後でプロセスの終了コードを分析します。

基本、詳細、および外部のマッチ特性の評価処理が戻り値0で終了した場合、アプリケーションがフォーム定義の条件に一致したことを示します。アプリケーションがフォーム定義の条件に一致しなかった場合は、0以外の値が返され、評価処理が停止します。

マイナスの値が返された場合は、Windowsのイベントビューアーにエラーが記録されます。ログ機能が有効な場合は、プラスの値がログファイルに記録されます。

評価処理の後に続く、ユーザーのログオン情報についての管理アクションは、標準のWindowsフォームアクション、アクションシーケンス、およびアクション拡張機能を組み合わせて実行できます。

フォーム識別拡張機能を定義するには

フォーム識別拡張機能は、アプリケーション定義を作成するときにフォーム定義ウィザードを使用して構成します。

1. Citrix AppCenterの［Single Sign-On］ノードを開き、［アプリケーション定義］ノードを選択して、［操作］メニューの［アプリケーション定義の作成］を選択します。
2. アプリケーション定義ウィザードに従って操作し、［フォームの管理］ページで［追加］をクリックしてフォーム定義ウィザードを起動します。
3. ［フォームの識別］ページが表示されるまでウィザードを進めます。
4. ［フォームの識別］ページで［詳細マッチ設定］をクリックします。［詳細マッチ設定］ダイアログボックスが開きます。
5. ［詳細マッチ設定］ダイアログボックスで、［フォーム識別拡張機能］をクリックします。
6. ［フォーム識別拡張機能］ページで［追加］をクリックします。［フォーム識別拡張機能の追加］ダイアログボックスが開きます。［フォーム識別拡張機能の追加］ダイアログボックスを使用して、以下の項目を定義します。

拡張機能ID	レジストリに書き込まれるキーの名前。ここでは、ExtensionNameとします。
説明	そのフォーム識別拡張機能の説明。
パラメーター	この拡張機能によって起動される外部プロセスに渡すパラメーターの名前と値。

ExtensionNameはレジストリキーの名前です。このキー名および関連するキーの値によって、起動する外部プロセスの実行可能ファイルと処理の内容が定義されます。レジストリキーの名前および関連するキーの値は以下の場所に存在します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extension\ExtensionName

ここでExtensionNameは、［フォーム識別拡張機能の追加］ダイアログボックスの［拡張機能ID］ボックスで定義する値です。

64ビットプラットフォームでは、レジストリキーの名前および関連するキーの値は以下の場所に存在します。

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\MetaFrame Password Manager\Extension\ExtensionName

各キーに設定可能な値は、以下の表のとおりです。

キー	種類	値
種類	REG_SZ	EXECUTABLEである必要があります。
Timeout	REG_DWORD	0はプロセスが終了するまで待機することを示します。ほかの値は、ミリ秒単位の待機時間を示します。
TerminateProcess	REG_DWORDとして定義されたブール値	タイムアウトが発生した場合に処理を終了するかどうかを示します（オプション）。

キー	種類	値
		TRUE（デフォルト）：処理を終了します。 FALSE（0）：処理を終了しません。
実行可能ファイル	REG_EXPAND_SZ	実行可能ファイルとその完全修飾パスです。
Arguments	REG_SZ	実行可能ファイルのパラメーターです。

Executableの値は実行可能ファイルのフルパスです。環境変数を使用してパスを指定することもできます。拡張機能をスクリプトとして実装する場合は、スクリプトのインタープリターをExecutableとして定義し、スクリプト名をArgumentsの一部として定義します。外部プロセスは、任意のエディター、言語またはIDEを使用して開発できます。

Argumentsの値は、Single Sign-On Plug-inによって置換される実行時パラメーター、または［アクションエディター］ダイアログボックスで指定するパラメーターの名前と値の組み合わせをサポートします。置換が必要なパラメーターは、ドル記号（$）で囲みます。たとえば、以下のコマンドライン引数をArgumentsに指定できます。

/h $_HANDLE$ /s $SAPSERVER$ /t $SAPTYPE$
この場合、実行可能ファイルによって以下のように解釈されます。

/h 1275366 /s "Houston, TX" /t 43
アプリケーションに関連付けられているMicrosoft Windowsハンドルは、内部パラメーターとしてサポートされ、$_HANDLE$として定義されます。

すべての内部パラメーターには接頭文字$_が使用されます。開発者が定義するパラメーター名にはアンダースコア（_）を使用できないため、名前の競合が防止されます。

パラメーター値が書き込まれた後に値を保持するために、置換の優先順位が定義されています。優先順位は、内部パラメーター（例：$_HANDLE$）、開発者が定義するパラメーター、環境変数の順です。

開発者が定義するパラメーター名には、小文字、大文字、および数字を使用できます。大文字と小文字は区別されません。

実行可能ファイルに特定の順序でパラメーターを指定する必要がある場合は、Argumentにもその順序で指定する必要があります。［フォーム識別拡張機能の追加］ダイアログボックスでは、パラメーターの名前と値の組み合わせを任意の順序で指定できます。

アクション拡張機能

アクション拡張機能では、外部プロセスを使用してユーザーのログオンやパスワード変更が管理されます。拡張機能で外部プロセスを定義して、目的のアプリケーションにユーザーのログオン情報を渡します。

ログオンまたはパスワード変更用のフォームが識別（「
— フォーム識別拡張機能
」を参照）された後のユーザー側のアクション（ログオンやパスワード変更など）は、標準のWindowsフォームアクション、アクションシーケンス、およびアクション拡張機能を組み合わせて実行できます。

Single Sign-On Plug-inでは、フォーム識別拡張機能（「
— フォーム識別拡張機能
」参照）と同様にアクション拡張機能を実行できます。

この機能では、外部プロセスを実行して、その処理が終了するまで待機し（WaitForCompletionが真に設定されている場合）、最後にプロセスの終了コードを分析します。プロセスが0を返して終了した場合は、拡張機能が正常に実行されたこと

を示します。エラーが発生した場合は、0以外の値が返されます。

マイナスの値が返された場合は、Windowsのイベントビューアーにエラーが記録されます。ログ機能が有効な場合は、プラスの値がログファイルに記録されます。ログ機能について詳しくは、「
— ログの有効化
」を参照してください。

アクション拡張機能を定義するには

アクション拡張機能は、アプリケーション定義を作成するときにフォーム定義ウィザードを使用して構成します。

1. Citrix AppCenterの［Single Sign-On］ノードを開き、［アプリケーション定義］ノードを選択して、［操作］メニューの［アプリケーション定義の作成］を選択します。
2. アプリケーション定義ウィザードに従って操作し、［フォームの管理］ページで［追加］をクリックしてフォーム定義ウィザードを起動します。
3. ［フォームアクションの定義］ページが表示されるまでウィザードを進めます。
4. ［フォームアクションの定義］ページで［アクションエディター］をクリックします。
5. ［アクションエディター］ダイアログボックス左上で［アクション拡張機能の起動］をクリックします。［アクションの設定］ペインが開きます。このペインを使用して、アクション拡張機能の各エントリを表示または編集したり､アクションシーケンスに追加したりします。
6. アクション拡張機能をアクションシーケンスに追加するには、以下の情報を入力して［挿入］をクリックします。

ID	レジストリに書き込まれるキーの名前。ここでは、ExtensionNameとします。
説明	そのアクション拡張機能の説明。
パラメーター	この拡張機能によって起動される外部プロセスに渡すパラメーターの名前と値。

フォーム識別拡張機能と同様に、ExtensionNameはレジストリキーの名前です。このキー名および関連するキーの値によって、アクションを処理する実行可能ファイルと処理の内容が定義されます。レジストリキーの名前および関連するキーの値は以下の場所に存在します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extension\ExtensionName

ここでExtensionNameは、［アクションの設定］ペインの［ID］ボックスで定義する値です。

64ビットプラットフォームでは、レジストリキーの名前および関連するキーの値は以下の場所に存在します。

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\MetaFrame Password Manager\Extension\ExtensionName

各キーに設定可能な値は、以下の表のとおりです。

キー	**種類**	**値**
種類	REG_SZ	EXECUTABLEである必要があります。
Timeout	REG_DWORD	0はプロセスが終了するまで待機することを示します。ほかの値は、ミリ秒単位の待機時間を示します。
TerminateProcess	REG_DWORDとして定義されたブール値	タイムアウトが発生した場合に処理を終了するかどうかを示します（オプション）。

キー	種類	値
		TRUE（デフォルト）：処理を終了します。 FALSE（0）：処理を終了しません。
WaitForCompletion	REG_DWORDとして定義されたブール値	Single Sign-On Plug-inが処理の終了を待機するかどうかを示します（オプション）。 TRUE（デフォルト）：待機します。 FALSE（0）：待機しません。
実行可能ファイル	REG_EXPAND_SZ	実行可能ファイルとその完全修飾パスです。
Arguments	REG_SZ	実行可能ファイルのパラメーターです。

Executableの値はフォーム識別拡張機能の場合と同様の規則に従います。

Argumentsの値は、Single Sign-On Plug-inによって置換される実行時パラメーター、または [アクションエディター] ダイアログボックスで指定するパラメーターの名前と値の組み合わせをサポートします。置換が必要なパラメーターは、ドル記号（$）で囲みます。たとえば、以下のコマンドライン引数をArgumentsに指定できます。

/h $_HANDLE$ /s $SAPSERVER$ /t $SAPTYPE$
この場合、実行可能ファイルによって以下のように解釈されます。

/h 1275366 /s "Houston, TX" /t 43
アプリケーションに関連付けられているMicrosoft Windowsハンドルは、内部パラメーターとしてサポートされ、$_HANDLE$として定義されます。

すべての内部パラメーターには接頭文字$_が使用されます。開発者が定義するパラメーター名にはアンダースコア（_）を使用できないため、名前の競合が防止されます。

Windowsハンドル以外にも、ユーザーのログオン情報を管理するための、以下の内部パラメーターがサポートされます。
- Username（$_USERNAME$）
- Password（$_PASSWORD$）
- Custom1（$_CUSTOM1$）
- Custom2（$_CUSTOM2$）
- Old Password（$_OLDPASSWORD$）

パラメーター値が書き込まれた後に値を保持するために、置換の優先順位が定義されています。優先順位は、内部パラメーター、開発者が定義するパラメーター、環境変数の順です。

開発者が定義するパラメーター名には、小文字、大文字、および数字を使用できます。大文字と小文字は区別されません。

実行可能ファイルに特定の順序でパラメーターを指定する必要がある場合は、Argumentにもその順序で指定する必要があります。［アクションの設定］ペインで、パラメーターの名前と値の組み合わせを任意の順序で指定できます。

開発者の満たすべき要件

フォーム識別拡張機能やアクション拡張機能で使用する外部プロセスは、コマンドラインインターフェイスを使用して起動できるプロセスまたはアプリケーションである必要があります。これらの拡張機能の必須またはオプションの引数も、コマン

ラインインターフェイスを使用してインラインで指定できるものでなければなりません。

開発者は、フォーム識別拡張機能とアクション拡張機能の両方について、ここで説明する要件を満たす必要があります。アクション拡張機能の場合は、実行可能ファイルに、Username、Password、Custom1、Custom2、およびOld Passwordを渡すことができます。

フォーム識別拡張機能やアクション拡張機能で使用する外部プロセスを開発する場合、以下の作業も必要になります。

- Single Sign-On Plug-inで拡張機能をサポートするための、すべての実行可能ファイル、サポートモジュール、およびファイルを実装する。
- 実装したすべてのモジュールを保守する。
- Single Sign-On Plug-inが動作するコンピューターに、すべての指定されたレジストリエントリを追加する。
- ドメイン内で拡張機能の名前を一意に保つ。

拡張機能の命名スキーマには、リバースドメイン命名スキーマ（com.citrix.cpm.ext4など）を使用することをお勧めします。

ログの有効化

Single Sign-On Plug-inのデバッグトレースを有効にするには、レジストリの変更が必要です。

レジストリキーの名前および関連するキーの値は以下の場所に存在します。

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Log

各キーに設定可能な値は、以下の表のとおりです。

キー	公開キー基盤（PKI）の各証明書に同じパスワードを使用する場合は「	値
有効	REG_DWORD	デフォルト値は0です。 0：無効 1：有効
フィルター	REG_DWORD	ログの対象を指定するビットマスクです。 0x00000001：フォーム識別拡張機能のエラーをログに記録するためのWindowsアプリケーションフラグ。 0x00000004：アクション拡張機能のエラーをログに記録するためのWindowsパスワード入力フラグ。
MaxSizeInBytes	REG_DWORD	ログファイルのサイズの上限（バイト単位）で、 論理的な上限値は4GB（2の32乗）です。 デフォルト値は819200です。

ログは以下のパスにあるsso_.logファイルに記録されます。

%LocalAppData%\Citrix\MetaFrame Password Manager

Windows、Web、およびターミナルエミュレーターベースのアプリケーション用の仮想キーコード

Sep 30, 2015

Single Sign-Onでは、Windowsアプリケーション、Webアプリケーション、およびターミナルエミュレーターベースのアプリケーションで仮想キーコードを使用できます。これらのコードは、ログオンまたはパスワード変更時に特定のキーストロークを送信するために使用されます。

VTabKeyN（WindowsおよびWeb）

以下の識別子を使用して、WindowsアプリケーションおよびWebアプリケーション用のキーコードシーケンスを作成します。

code	説明
'DELAY=N'	Nは、待機時間をミリ秒単位で示します。
'VKEY=N'	Nは、送信するキーコードを示します。

たとえば、Tab、End、Space、1.5秒の待機、Logon username、Space、ユーザー名/ID、Home、0.35秒の待機、Tab、さらにパスワードの順に送信するには、以下のコードを使用します。

VTabKey1= 'VKEY=9''VKEY=35' 'DELAY=1500 'Logon username'VKEY=32' VTabKey2='VKEY=36''DELAY=350''VKEY=9'

VirtualKeyCodeおよびVKEY（WindowsおよびWeb）

キー	code	キー	code	キー	code	キー	code
Break	3	5	53	V	86	F5	116
BackSpace	8	6	54	W	87	F6	117
ページ	9	7	55	○	88	F7	118
Clear	12	8	56	○	89	F8	119
Enter	13	9	57	Z	90	F9	120
Shift	16	A	65	左Windows	91	F10	121
Ctrl	17	B	66	右Windows	92	F11	122
Alt	18	C	67	数字キーパッドの0	96	F12	123
CapsLock	20	D	68	数字キーパッドの1	97	F13	124
Esc	27	E	69	数字キーパッドの2	98	F14	125
Space	32	F	70	数字キーパッドの3	99	F15	126

Page Up キー	33 code	G キー	71 code	数字キーパッドの4 キー	100 code	F16 キー	127 code
Page Down	34	H	72	数字キーパッドの5	101	F17	128
End	35	I	73	数字キーパッドの6	102	F18	129
Home	36	J	74	数字キーパッドの7	103	F19	130
左	37	K	75	数字キーパッドの8	104	F20	131
↑	38	L	76	数字キーパッドの9	105	F21	132
Right	39	M	77	アスタリスク（*）	106	F22	133
↓	40	未サポート	78	プラス記号（+）	107	F23	134
PrintScreen	44	O	79	マイナス記号（-）	109	F24	135
ヘルプ	47	P	80	ピリオド（.）	110	NumLock	144
0	48	Q	81	スラッシュ（/）	111	ScrollLock	145
1	49	R	82	F1	112	左Shift	160
2	50	S	83	F2	113	右Shift	161
3	51	T	84	F3	114	左Ctrl	162
4	52	U	85	F4	115	右Ctrl	163

HLLAPI準拠のターミナルエミュレータベースアプリケーション用仮想キーコード

文字/コマンド	code	文字/コマンド	code	文字/コマンド	code
Altカーソル	@$	Local Print	@P	PF12/F12	@c
BackSpace	@<	リセット	@R	PF13/F13	@d
@	@@	Shift	@S	PF14/F14	@e
Alt	@A	Dup	@S@x	PF15/F15	@f
Field -	@A@-	Field Mark	@S@y	PF16/F16	@g
Field +	@A@+	右Tab	@T	PF17/F17	@h
Field Exit	@A@E	カーソルを上に	@U	PF18/F18	@i
Altカーソル	@$	カーソルを下に	@V	PF19/F19	@j

文字/コマンド	code	文字/コマンド	code	文字/コマンド	code
Erase Input	@A@F	カーソルを左に	@L	PF20/F20	@k
Sys Request	@A@H	カーソルを右に	@Z	PF21/F21	@l
Insert Toggle	@A@I	Page Up	@u	PF22/F22	@m
カーソル選択	@A@J	Page Down	@v	PF23/F23	@n
Attention	@A@Q	End	@q	PF24/F24	@o
PrintScreen	@A@T	Home	@0	PA1	@x
16進	@A@X	PF1/F1	@1	PA2	@y
コマンド/ファンクションキー	@A@Y	PF2/F2	@2	PA3	@z
Print（PC）	@A@t	PF3/F3	@3	PA4	@+
Back/左Tab	@B	PF4/F4	@4	PA5	@%
Clear	@C	PF5/F5	@5	PA6	@&
削除	@D	PF6/F6	@6	PA7	@’
Enter	@E	PF7/F7	@7	PA8	@(
Erase EOF	@F	PF8/F8	@8	PA9	@)
ヘルプ	@H	PF9/F9	@9	PA10	@*
Ins	@I	PF10/F10	@a		
New Line	@N	PF11/F11	@b		

Single Sign-Onプロビジョニングソフトウェア開発キット（SDK）

Sep 30, 2015

Citrix Single Sign-Onプロビジョニングソフトウェア開発キット（SDK）を使用して、ユーザーのログオン情報を完全に管理できます。Single Sign-Onでは、ユーザーがドメインへのログオン（プライマリ認証）に成功すると、そのユーザーのアプリケーション固有のログオン情報が自動的に送信されます。

Single Sign-Onのプロビジョニング機能では、管理者がユーザーのログオン情報を管理するときの多くのタスクを自動化できます。この機能では、環境内にSingle Sign-Onの新しいバージョンを展開したり、多数のユーザーやアプリケーションを追加したり、不要な情報を整理したりするような作業を、短時間で効率的に完了するためのツールが提供されます。

このドキュメントでは、Single Sign-Onのプロビジョニング機能の設計について概説し、XMLファイルのプロビジョニングを定義するためのAPIの概要について説明します。

プロビジョニングモジュール

プロビジョニングモジュールはSingle Sign-Onサービスの1つで、プロビジョニングコマンドを受信するためのSOAP/SPML（Simple Object Access Protocol and Service Provisioning Markup Language）インターフェイスを提供する標準的なWebサービスです。クライアントとプロビジョニングモジュールとの間で通信されるすべてのデータは、TLS（Transport Layer Security）チャネルで保護されます。

プロビジョニングコマンドをキューに送るときに、データが安全に格納され、保護されたネットワークが使用されることを確認してください。

Single Sign-On Plug-inで実行するプロビジョニングコマンドをキューに送るには、プロビジョニングモジュールでSingle Sign-Onの中央ストアに対する読み取りと書き込みアクセスが必要です。

プロビジョニングモジュールに送信されたコマンドは、取り消しできません。コマンドがプロビジョニングモジュールに送信されると、Single Sign-On Plug-inで実行されるまでキューに入れられます。キューからコマンドを削除する必要がある場合は、対象となるユーザー、アプリケーション、およびログオン情報のオブジェクトごとに逆の効果を得るコマンドを送信してください。

注：プロビジョニングモジュールでは、SPML 2.0に準拠したインターフェイスが使用されます。この標準への準拠が必要な主要オペレーションのみがサポートされています。

SPML 2.0モデル

プロビジョニングXMLファイル、およびSPML要求を発行するサードパーティ製コンポーネントは、Requesting Authorities（RA）と呼ばれます。

プロビジョニングモジュールは、PSP（Provisioning Service Provider）に相当します。このPSPでは、Single Sign-Onプロビジョニングコマンドのユーザー単位でのキュー入れを行う単一のターゲット（PST：Provisioning Service Target）がサポートされます。

プロビジョニングにより、アプリケーションへのログオン情報がユーザーに提供され、Single Sign-Onで使用できるように準備されます。エンドユーザーとログオン情報は、プロビジョニングサービスターゲットのプロビジョニングサービスオブジェクト（Provisioning Service Object：PSO）です。各ユーザーに固有の識別子（PSO-ID）には、完全修飾ドメイン名（FQDN）が使用されます。同様に、各ログオン情報に固有の識別子（PSO-ID）には、そのログオン情報が作成されたときに割り当てられたGUIDが使用されます。ログオン情報は特定のユーザーに関連付けられているため、ユーザーのPSOがログオン情報の

PSOのコンテナーになります。このコンテナーは、SPML要求のcontainerIDエレメントで定義されます。

厳密には、Single Sign-Onが追加、変更、または削除するのはユーザーではなく、そのユーザーに関連付けられているデータです。

プロビジョニングとSingle Sign-On Plug-in

ユーザーが登録したログオン情報を暗号キーで保護するのはSingle Sign-On Plug-inであるため、プロビジョニングは以下の2つの段階により処理されます。まず、管理者がプロビジョニングモジュールにプロビジョニングコマンドを実行します。次に、Single Sign-On Plug-inがそのユーザーのログオン情報ストアにプロビジョニングコマンドを適用します。

Single Sign-On Plug-inは、起動時の通常の同期処理でプロビジョニングコマンドのキューを検出すると、それらのコマンドを実行してから通常の動作モードに戻ります。これにより、Single Sign-On Plug-inの初回起動時にプロビジョニングが実行されるため、ユーザーによる初期設定操作を最小限にすることができます。

Single Sign-On Plug-inとプロビジョニングモジュール間の通信は、すべてTLSで保護されます。

クライアントプロビジョニングアプリケーションでは、プロビジョニング対象のアプリケーションとクライアント側のアプリケーション間でマッピングを正しく定義する必要があります。

ログオン情報をプロビジョニングする

Single Sign-Onで処理するユーザーの資格情報（Secondary Credential。ここでは「ログオン情報」と訳します）は、AppCenterの［Single Sign-On］ノード（Single Sign-On管理コンソール）で作成したアプリケーション定義に関連付けられています。このため、addRequestオペレーションには、対象ユーザーの詳細を特定のアプリケーション定義にバインドするためのデータを含める必要があります。つまり、RAでは、プロビジョニング可能なアプリケーションのリストをユーザーごとに特定し、addRequestオペレーションでアプリケーション定義のIDを提供する必要があります。RAは、Single Sign-Onのアプリケーション定義と、プロビジョニング対象のアプリケーションの外的な識別情報（アプリケーション名など）との関連付けを特定しなければなりません。

Single Sign-Onの管理者とプロビジョニングを担当する管理者が常に同一であるとは限らないため、人為的な混乱が生じることがあります。たとえば、Single Sign-On管理者が「Microsoft Outlook」というアプリケーション定義を作成し、プロビジョニング管理者が「Microsoft Exchange」というアカウントを作成する場合などです。また、Single Sign-Onでは単一のアプリケーション定義に複数のログオン情報を関連付けることができます。たとえば、Single Sign-Onに複数のMSN Hotmailアカウントのログオン情報を登録することができます。管理者は、同一のパラメーターを指定した複数のaddRequestsオペレーションを発行して、複数のログオン情報を作成できます。同様に、同一アプリケーションに対して複数の異なるログオン情報をプロビジョニングしたいと思うかもしれません。しかし、Single Sign-On Plug-inにより暗号化されたシークレット（ユーザーID、パスワード、およびカスタムフィールド）をプロビジョニングモジュールで解読できないため、後からRAでログオン情報を識別できなくなるという問題も生じます。

これらの問題を解決するため、addRequestおよびmodifyRequestオペレーションには、RAのオプションのプライベートデータフィールドprovision-descriptionを使用できます。これにより、RAでログオン情報を識別するためのIDまたは説明データを追加できるようになります。このフィールドは、Single Sign-On Plug-inやプロビジョニングモジュールで表示したり変更したりすることはできません。このフィールドは保持され、lookupRequestでログオン情報のリストを要求すると、RAにその内容が返されます。

Single Sign-On Plug-inは、すべてのログオン情報に対する完全な編集アクセスを持ちます。これには、ログオン情報の複製、削除、および変更などが含まれます。このことはつまり、プロビジョニングにより作成されたデータをユーザーが変更できるということを意味します。

また、ユーザーはアプリケーションを定義することもできます。Single Sign-On管理コンソールで作成されていないアプリケーション定義を、ユーザーが必要に応じて作成することができます。ただし、この機能により、管理者がログオン情報の削

除や変更を行えるかどうか、またlookupResponseでログオン情報のリストを取得できるかどうかというオーナーシップの問題が発生します。このバージョンのSingle Sign-Onでは、オーナーシップに関する制限はサポートされません。つまり、すべてのログオン情報は、管理者またはユーザーによる変更の対象になります。

アプリケーショングループ

Single Sign-Onでは、アプリケーションをグループ化することができます。このアプリケーショングループの属性として、そのグループに属するすべてのアプリケーションで共通のパスワードを使用するかどうかというものがあります。アプリケーショングループのパスワードをユーザーが変更すると、そのグループ内のすべてのアプリケーションのパスワードが変更されます。

この動作は、プロビジョニングAPIを使用する場合にも当てはまります。たとえば、アプリケーショングループに新しいログオン情報を追加する場合、addコマンドのパラメーターとして指定された新しいパスワードが、そのグループ内のすべてのアプリケーションのパスワードになります。この場合のaddコマンドでは、addだけでなく、いくつかのmodifyコマンドの処理が行われます。同様に、1つのmodifyコマンドでグループ内のすべてのアプリケーションを変更できるため、いくつかのmodifyコマンドの処理が行われると理解することもできます。

エラーコード

code	説明
101	必要なログオン情報フィールドがプロビジョニング要求に指定されていません。
102	無効なユーザー名が指定されています。ユーザー名がないか、書式が不正です。
103	指定されたユーザーが見つかりません。
104	無効なアプリケーション定義です。アプリケーション定義がないか、構造が無効です。
105	ログオン情報の識別子の書式が無効です。
106	指定されたログオン情報が見つかりません。
107	無効な認証セキュリティトークンです。
108	認証されていないアクセストークンです。指定されたトークンでは、このオペレーションの実行が許可されません。
109	ストレージにほかのプロセスがアクセスしています。後で再試行してください。
110	プロビジョニングコマンドの使用時にエラーが発生しました。
111	このユーザーには、プロビジョニングコマンドのキューにアクセスする権限がありません。
112	プロビジョニングの秘密キーの取得時にエラーが発生しました。
113	暗号化用のメモリを割り当てることができません。
114	エントロピーデータバッファーを割り当てることができません。
115	暗号化に失敗しました。

code	説明
116	cipherTextバッファーを割り当てることができません。
117	暗号の解読に失敗しました。
118	エラーメッセージ用のWindowsエラーコードの書式設定に失敗しました。
119	Pso IDが指定されていないか、形式が不適切です。
120	参照されているアプリケーションが見つかりません。
121	要求されたユーザーのユーザー構成が見つかりません。
122	パスワード共有グループのcredentialエレメントでjoin属性が指定されていません。
123	パスワード共有グループのcredentialエレメントでuse-new-password属性が指定されていません。
124	パスワード共有グループのcredentialエレメントでパスワードが指定されていません。
125	ログオン情報名が無効または未指定です。正しいログオン情報名を指定してください。
126	無効なアプリケーションIDが指定されました。
127	共有グループにログオン情報を再追加できません。
128	指定されたユーザーアカウントのプロビジョニングが有効になっていません。

API関数の概要

Sep 30, 2015

API関数により、プロビジョニングXMLファイルで操作を定義するためのメソッドが提供されます。ここで説明するサンプルコードに加えて、製品インストールメディアにも多くのサンプルコードが収録されています。

Single Sign-On独自のすべてのエレメントや属性には、名前空間識別子である「ctxs」プレフィックスが使用されます。各テキストボックスのXMLスニペットには、要求およびそれに対する戻り値がリストされます。

同期実行モード（synchronous）のみがサポートされます。非同期実行モード（asynchronous）を指定すると、unsupportedExecutionModeエラーが発生します。

次の表は、サンプルコード内で実際に指定する値の代わりに使用するプレースホルダーの一覧です。

プレースホルダー	説明
FQDN	ユーザーの完全修飾ドメイン名（Fully Qualified Domain Name）です。
application-GUID	アプリケーション定義のGUIDです。AppCenterの［Single Sign-On］ノード（Single Sign-On管理コンソール）で作成したときに割り当てられます。
credential-GUID	ログオン情報のGUIDです。addRequestの実行時にプロビジョニングサービスにより割り当てられます。
RA-generated-ID	RAにより生成される要求のIDです。要求エレメントのrequestIDオプション属性で使用されます。非同期実行のサポートを追加する場合のみ意味を持ちます。
AuthToken	authentication-tokenエレメントは必須ですが、現在使用されていません。

単一アプリケーションをプロビジョニングする - addRequest

Sep 30, 2015

単一のアプリケーションにユーザーのログオン情報を追加するには、addRequestオペレーションを使用します。

addRequestオペレーションは、指定されたコンテナーオブジェクト（ユーザーのデータストア）への新規オブジェクト（ログオン情報）の追加を要求します。1つのcontainerID（ユーザーのFQDN）を指定して、作成されたオブジェクトのpsoID（ログオン情報のGUID）が返されます。作成するログオン情報の詳細を、dataエレメントで提供します。

作成されるログオン情報に関連付けられているアプリケーション定義がパスワード共有グループに含まれている場合は、そのグループのパスワードが新しいログオン情報のもので更新されます。

構文

AuthToken Credential name Admin Text Credential description appdefGuid Domain salima pass123 domain database

パラメーター

requestID（必須）	クライアント生成のIDで、これにより戻り値とこの要求が関連付けられます。
targetID（必須）	プロビジョニングモジュールのIDで、「CPM Provisioning 1.0」です。
returnData（必須）	data：ログオン情報の詳細を返します。 identifier：ユーザーのログオン情報のリストを返します。 name：Single Sign-Onではサポートされていません。 everything：指定されたユーザーのアプリケーション定義を返します。
executionMode（必須）	Single Sign-Onでは、同期実行モード（synchronous）がサポートされます。
authentication-token（必須）	authentication-tokenエレメントは必須ですが、現在使用されていません。.
containerID（必須）	そのログオン情報のユーザーのFQDNを提供します。
data（必須）	変更するデータの内容です。credentialエレメントでログオン情報の内容を定義し、子エレメントやapplicationエレメントが含まれる場合があります。
ctxs:credential（必須）	credentialエレメントでログオン情報の内容を定義します。子エレメントnameおよびdescriptionはオプションです。これらの子エレメントを指定しない場合、アプリケーション定義の名前および説明が使用されます。
ctxs:application（必須）	アプリケーション定義やログオン情報の詳細を記述します。applicationエレメントは、lookupApplicationsRequestオペレーションで取得した情報と一致している必要があります。

戻り値の構文（addResponse）

戻り値のパラメーター（addResponse）

status（必須）	値：success、failure、pending
requestID（必須）	クライアント生成のIDで、これにより戻り値と要求が関連付けられます。
pso（必須）	ctxs:credentialで説明されているように、psoエレメントのデータはログオン情報です。
psoID（必須）	各ユーザーに固有の識別子です。 PSOIDは、lookupResponseにより返されるログオン情報のGUIDです。
containerID（必須）	そのログオン情報のユーザーのFQDNを提供します。
data（必須）	変更するデータの内容です。credentialエレメントでログオン情報の内容を定義し、子エレメントやapplicationエレメントが含まれる場合があります。

groupエレメントの属性

groupエレメントのjoinおよびuse-new-password属性は、新しいログオン情報が既存のアプリケーショングループにどのよ
に反映されるかを制御します。パスワード共有が構成されていないアプリケーショングループでは、groupエレメントは無
されます。

join属性の値	**use-new-password属性の値**	**影響**
False	False	新しいログオン情報は、既存のアプリケーショングループに関連付けられません。既存のアプリケーショングループは影響を受けません。
False	true	新しいログオン情報は、既存のアプリケーショングループに関連付けられません。既存のアプリケーショングループは影響を受けません。
true	False	新しいログオン情報は、既存のアプリケーショングループに追加されます。新しいログオン情報のパスワードには、そのグループで共有されているものが設定されます。既存のグループメンバーがない場合は、passwordエレメントで指定した値が設定されます。
true	true	新しいログオン情報は、既存のアプリケーショングループに追加されます。新しいログオン情報のパスワードにはpasswordエレメントで指定した値が設定され、この新しいパスワードがグループ内で共有されます。

戻り値でpsoIDとして返されるログオン情報のGUID（credential-GUID）はlookupResponseオペレーションでリストされるも
のと同じものであり、modifyRequestオペレーションやdeleteRequestオペレーションでこのログオン情報を指定するときに
使用できます。

バッチ処理を実行する - batchRequest

Sep 30, 2015

batchRequestオペレーションは、ほかのオペレーション（<要求名>Request）のリストを含むコンテナーとして動作します。Single Sign-Onでは、順次処理モードのみがサポートされます。batchRequestで並列処理を実行しても、エラーは発生せず、順次処理が行われます。

構文

```
AuthToken  Credential name  appdefGuid  janed pwd123  AuthToken  Credential name  appdefGuid2  salima pass123
```

パラメーター

processing（必須）	処理モードを指定します。指定可能な値はsequentialおよびparallelですが、Single Sign-Onでは順次処理モード（sequential）のみがサポートされます。並列処理モード（parallel）を指定しても、Single Sign-Onでは順次処理が行われます。
onError	実行時にエラーが発生した場合のSingle Sign-Onの動作を指定します。指定可能な値は、resume（再開）とexit（終了）です。
<要求名>Request（必須）	バッチ処理に含める要求のリストです。各要求の構文およびパラメーターに従って指定します。

戻り値の構文（batchResponse）

戻り値のパラメーター（batchResponse）

<要求名>Request	バッチ処理に含まれている各要求の名前です。戻り値の構文については、各要求のトピックを参照してください。

ログオン情報を削除する - deleteRequest

Sep 30, 2015

単一のログオン情報を削除するには、deleteRequestオペレーションを使用します。削除するログオン情報は、そのGUIDで指定します。

構文

AuthToken

パラメーター

requestID（必須）	クライアント生成のIDで、これにより戻り値とこの要求が関連付けられます。
executionMode（必須）	Single Sign-Onでは、同期実行モード（synchronous）がサポートされます。
authentication-token（必須）	authentication-tokenエレメントは必須ですが、現在使用されていません。
psoID（必須）	各ユーザーに固有の識別子です。 PSOIDは、lookupResponseにより返されるログオン情報のGUIDです。
containerID（必須）	そのログオン情報のユーザーのFQDNを提供します。

戻り値の構文

戻り値のパラメーター

status（必須）	値：success、failure、pending
requestID	クライアント生成のIDで、これにより戻り値と要求が関連付けられます。

ユーザーを削除する - deleteRequest

Sep 30, 2015

特定のユーザーに関連付けられたすべてのデータをログオン情報ストアから削除するには、deleteRequestオペレーションを使用します。

構文

AuthToken

パラメーター

requestID（必須）	クライアント生成のIDで、これにより戻り値とこの要求が関連付けられます。
executionMode	Single Sign-Onでは、同期実行モード（synchronous）がサポートされます。
authentication-token	authentication-tokenエレメントは必須ですが、現在使用されていません。
psoID（必須）	各ユーザーに固有の識別子です。 PSOIDは、lookupResponseにより返されるログオン情報のGUIDです。

戻り値の構文（deleteResponse）

戻り値のパラメーター

status（必須）	値：success、failure、pending
requestID（必須）	クライアント生成のIDで、これにより戻り値と要求が関連付けられます。

備考

ユーザーが退職した場合などは、そのユーザーに関するすべてのデータを完全に削除できます。必要な情報をユーザーが忘れたために自分のログオン情報にアクセスできなくなった場合は、そのユーザーのデータを削除する代わりにSingle Sign-Onの状態をリセットして、ユーザーが最初からやり直せるようにします（「resetRequest」を参照）。

データを完全に削除する場合とデータをリセットする場合とでは、Single Sign-On Plug-inの動作が異なるため、適切なオペレーションを使い分ける必要があります。管理者による設定によっては、ユーザーのSingle Sign-Onデータのローカルコピーがそのユーザーのプロファイル内に存在する場合があります。中央ストア内にそのユーザーのデータが存在しない場合は、登録ウィザードが起動して、ユーザーのローカルデータが中央ストアにコピーされます。

ユーザーデーターをリセットする場合は、ローカルデータが削除され、その後で登録ウィザードが起動します。

ターゲットを照会する - listTargetsRequest

Sep 30, 2015

システム上で構成されているターゲットを照会するには、listTargetsRequestオペレーションを使用します。Single Sign-Onサービスでは、単一の固有なターゲットであるプロビジョニングモジュールがサポートされます。このプロビジョニングモジュールは、targetID「CPM Provisioning 1.0」で識別されます。

構文

AuthToken

パラメーター

requestID（必須）	クライアント生成のIDで、これにより戻り値とこの要求が関連付けられます。
executionMode（必須）	Single Sign-Onでは、同期実行モード（synchronous）がサポートされます。
authentication-token（必須）	authentication-tokenエレメントは必須ですが、現在使用されていません。

戻り値の構文

戻り値のパラメーター

requestID（必須）	クライアント生成のIDで、これにより戻り値と要求が関連付けられます。
status（必須）	値：success、failure、pending
targetID（必須）	プロビジョニングモジュールのIDで、「CPM Provisioning 1.0」です。
schema（必須）	このオペレーションの戻り値には、プロビジョニングモジュールの固有のIDが含まれ、このモジュールにより管理されるオブジェクト（ユーザーやそのログオン情報など）がschemaエレメントに記述されます。

ユーザーが使用可能なアプリケーションのリストを取得する - lookupApplicationRequest

Sep 30, 2015

特定のユーザーが使用可能なアプリケーション（アプリケーションのIDを含む）のリストを取得するには、lookupApplicationRequestオペレーションを使用します。特定のユーザーが使用可能なアプリケーション定義は、コンソールでそのユーザーに関連付けられているユーザー構成により決定されます。これらのアプリケーション定義はユーザーが所有するものではなく、コンソール以外で編集することはできません。

構文

AuthToken

パラメーター

requestID（必須）	クライアント生成のIDで、これにより戻り値とこの要求が関連付けられます。
authentication-token（必須）	authentication-tokenエレメントは必須ですが、現在使用されていません。
psoID（必須）	各ユーザーに固有の識別子で、ユーザーのFQDNです。

戻り値の構文 - lookupApplicationResponse

app-GUID1 Outlook Outlook 2003 Domain app-GUID2 Vantive Bug Database SAP

戻り値のパラメーター

status（必須）	値：success、failure、pending
requestID（必須）	クライアント生成のIDで、これにより戻り値と要求が関連付けられます。
psoID（必須）	各ユーザーに固有の識別子で、ユーザーのFQDNです。
data（必須）	変更するデータの内容です。credentialエレメントでログオン情報の内容を定義し、子エレメントやapplicationエレメントが含まれる場合があります。
ctxs:application（必須）	アプリケーション定義やログオン情報の詳細を記述します。applicationエレメントは、lookupApplicationRequestオペレーションで取得した情報と一致している必要があります。ユーザー構成の各アプリケーション定義について1つのapplicationエレメントがあります。詳しくは、「ctxs:application」を参照してください。

備考

この種類のデータを取得することは、標準的なSPML動作に含まれていません。カスタムの機能により、ユーザーが使用可能なアプリケーションのリストを取得しています。

登録されたログオン情報のアプリケーションリストを取得する - lookupRequest

Sep 30, 2015

ユーザーが登録したログオン情報のアプリケーションのリストを取得するには、lookupRequestオペレーションを使用します。returnData属性の値により、戻り値の詳細レベルが指定されます。

構文

AuthToken

パラメーター

requestID（必須）	クライアント生成のIDで、これにより戻り値とこの要求が関連付けられます。
returnData（必須）	data：ログオン情報の詳細を返します。 identifier：ユーザーのログオン情報のリストを返します。 name：Single Sign-Onではサポートされていません。 everything：指定されたユーザーのアプリケーション定義を返します。
executionMode（必須）	Single Sign-Onでは、同期実行モード（synchronous）がサポートされます。
authentication-token（必須）	authentication-tokenエレメントは必須ですが、現在使用されていません。
psoID（必須）	各ユーザーに固有の識別子です。 PSOIDは、lookupResponseにより返されるログオン情報のGUIDです。

戻り値の構文 - lookupResponse

credential-GUID1 Aviva Aviva 5250 Demo Aviva 5250 app-GUID1 Aviva 5250 Demo AppGroup credential-GUID2 Dynamic App1

戻り値のパラメーター

status（必須）	値：success、failure、pending
requestID（必須）	クライアント生成のIDで、これにより戻り値と要求が関連付けられます。
pso（必須）	ctxs:credentialで説明されているように、psoエレメントのデータはログオン情報です。
psoID（必須）	各ユーザーに固有の識別子で、ユーザーのFQDNです。Single Sign-OnのSPMLモデルにより、psoのデータは、ctxs:credentialで説明されているように、ログオン情報です。returnData属性がdataまたはeverythingの場合に、この情報が返されます。各ログオン情報について1つのpsoエレメントがあります。psoIDのID属性は、ログオン情報のGUIDを提供します。
data（必須）	取得するデータの内容です。credentialエレメントでログオン情報の内容を定義し、子エレメントやapplicationエレメントが含まれる場合があります。
ctxs:credential（必須）	credentialエレメントでログオン情報の内容を定義します。子エレメントnameおよびdescriptionはオプションです。これらの子エレメントを指定しない場合、アプリケーション定義の名前および説明が使用されます。詳しくは、「ctxs:credential」を参照してください。
ctxs:application（必須）	アプリケーション定義やログオン情報の詳細を記述します。applicationエレメントは、lookupApplicationRequestオペレーションで取得した情報と一致している必要があります。ユーザー構成の

	各アプリケーション定義について1つのapplicationエレメントがあります。詳しくは、「ctxs:application」を参照してください。

備考

lookupRequestオペレーションでログオン情報を指定すると、そのログオン情報の詳細が戻り値として返されます。一般に、各ログオン情報のシークレットはプラグインソフトウェアにより暗号化され、プロビジョニングモジュールからはアクセスできません。つまり、プラグインソフトウェアにより管理されているログオン情報のfieldエレメントの文字データは、空になります。

プロビジョニングは、以下の2つの段階により処理されます。まず、プロビジョニングモジュールがプロビジョニングコマンドをキューに入れます。次に、プラグインソフトウェアがキュー内のコマンドを実行します。実行した操作を検証できるようにするには、返されたログオン情報のリストでキュー内のコマンドを特定できる必要があります。キュー内のコマンドは、プラグインソフトウェアではなくプロビジョニングモジュールにより保護されるため、プラグインモジュールを使用してコマンドのパラメーターを解読できます。また、addまたはmodifyコマンドがキューに入れられたログオン情報には、lookupResponseオペレーションでリストされる、アクセス可能なコマンドパラメーターもあります。このコマンドパラメーターには、userID、password、およびcustom-fieldの値が含まれる場合があることに注意してください。

ログオン情報を取得する - lookupRequest

Sep 30, 2015

このオペレーションを使用して、ログオン情報の詳細を取得します。

構文

AuthToken

パラメーター

requestID（必須）	クライアント生成のIDで、これにより戻り値とこの要求が関連付けられます。
returnData（必須）	data：ログオン情報の詳細を返します。 identifier：ユーザーのログオン情報のリストを返します。 name：Single Sign-Onではサポートされていません。 everything：指定されたユーザーのアプリケーション定義を返します。
executionMode（必須）	同期実行モード（synchronous）のみがサポートされます。非同期実行モード（asynchronous）を指定すると、unsupportedExecutionModeエラーが発生します。
authentication-token（必須）	authentication-tokenエレメントは必須ですが、現在使用されていません。
psoID（必須）	各ユーザーに固有の識別子で、ユーザーのFQDNです。
containerID（必須）	そのログオン情報のユーザーのFQDNを提供します。

戻り値の構文 - lookupResponse

Credential-name Admin text Credential description app-GUID Outlook description from app-def Domain

戻り値のパラメーター

status（必須）	値：success、failure、pending
requestID（必須）	クライアント生成のIDで、これにより戻り値と要求が関連付けられます。
psoID（必須）	各ユーザーに固有の識別子で、ユーザーのFQDNです。Single Sign-OnのSPMLモデルにより、psoのデータは、「ctxs:credential Element」で説明されているように、ログオン情報です。returnData属性がdataまたはeverythingの場合に、この情報が返されます。各ログオン情報について1つのpsoエレメントがあります。psoIDのID属性は、ログオン情報のGUIDを提供します。
containerID（必須）	そのログオン情報のユーザーのFQDNを提供します。
data（必須）	取得するデータの内容です。credentialエレメントでログオン情報の内容を定義し、子エレメント

	やapplicationエレメントが含まれる場合があります。
ctxs:credential（必須）	credentialエレメントでログオン情報の内容を定義します。子エレメントnameおよびdescriptionはオプションです。これらの子エレメントを指定しない場合、アプリケーション定義の名前および説明が使用されます。詳しくは、「ctxs:credential Element」を参照してください。
ctxs:application（必須）	アプリケーション定義やログオン情報の詳細を記述します。applicationエレメントは、lookupApplicationRequestオペレーションで取得した情報と一致している必要があります。ユーザー構成の各アプリケーション定義について1つのapplicationエレメントがあります。詳しくは、「ctxs:credential Element」を参照してください。

ログオン情報を変更する - modifyRequest

Sep 30, 2015

プロビジョニング済みのログオン情報を変更するには、modifyRequestオペレーションを使用します。変更されるログオン情報に関連付けられているアプリケーション定義がパスワード共有グループに含まれている場合は、そのグループのパスワードが変更後のログオン情報のもので更新されます。

構文

```
AuthToken      New Credential Name   username
```

パラメーター

requestID（必須）	クライアント生成のIDで、これにより戻り値とこの要求が関連付けられます。
ctxs:authentication-token	authentication-tokenエレメントは必須ですが、現在使用されていません。
psoID（必須）	ログオン情報のIDはGUID（Single Sign-Onシステムにより生成され、中央ストアに格納されます）です。lookupRequestにより返された値と一致している必要があり、これにより変更対象のログオン情報が特定されます。
containerID（必須）	そのログオン情報のユーザーのFQDNを提供します。
modification（必須）	modificationMode（必須） add：ログオン情報を追加します。addRequestと同じ処理が行われます。modificationModeにaddを指定する場合、psoIDエレメントとdataエレメントにはaddRequestと同じ制限が適用されます。psoIDでは単一コンテナーを指定し（deleteRequestの場合と同様）、dataでは単一のcredentialエレメントを指定します（addRequestの場合と同様）。 replace：フィールドの値を変更します。タグ内に新しい値を指定します。 delete：フィールドの値を削除します。dataエレメントの内容は無視されます。
data（必須）	変更するデータの内容です。credentialエレメントでログオン情報の内容を定義し、子エレメントやapplicationエレメントが含まれる場合があります。
credential（必須）	credentialエレメントでログオン情報の内容を定義します。子エレメントnameおよびdescriptionはオプションです。これらの子エレメントを指定しない場合、アプリケーション定義の名前および説明が使用されます。詳しくは、「ctx:credential」を参照してください。
name	AppCenterのSingle Sign-Onコンソールに表示されるアプリケーション定義名です。
application（必須）	アプリケーション定義やログオン情報の詳細を記述します。applicationエレメントは、lookupApplicationsRequestオペレーションで取得した情報と一致している必要があります。詳しくは、「ctxs:application」を参照してください。applicationエレメントの子IDエレメントの値は、そのログオン情報に格納されている値と一致している必要があります。
グループ	add要求にgroupエレメントが含まれていない場合は、デフォルトの値が提供されます。groupエ

	レメントのjoinおよびuse-new-password属性は、新しいログオン情報が既存のアプリケーショングループにどのように反映されるかを制御します。下記「groupエレメントの属性」を参照してください。
fields（必須）	lookupResponseオペレーションのfieldsエレメントの各子エレメントは、addRequestオペレーションに含まれている必要があります。含まれていない場合はエラーが返されます。
userID（必須）	このログオン情報のユーザーアカウントです。
password（必須）	このログオン情報のパスワードです。
custom-field	このログオン情報のカスタムの値を提供するカスタムフィールドです。Single Sign-Onでは、ユーザー名やパスワード用のフィールドに加えて、2つのカスタムフィールドがサポートされます。
psoID（必須）	各ユーザーに固有の識別子です。PSOIDはユーザーのFQDNで、変更対象のログオン情報のコンテナーを特定するために使用されます。

戻り値の構文 - modifyResponse

戻り値のパラメーター

status（必須）	値：success、failure、pending
requestID（必須）	クライアント生成のIDで、これにより戻り値と要求が関連付けられます。

備考

modifyRequestでgroupエレメントのjoin属性にtrueを指定すると、パスワード共有グループから除外されたログオン情報をグループに追加することができます（addRequestを参照）。このオペレーションのgroupエレメントにはaddRequestの場合と同じ制限が適用され、同じ効果が提供されます。

modifyRequestオペレーションのapplicationエレメントで、ctxs:fields子エレメントを指定できることに注意してください。指定可能なフィールドのリストは、
— lookupResponse
で取得できます。

groupエレメントの属性

join属性の値	**use-new-password属性の値**	**影響**
False	true	新しいログオン情報は、既存のアプリケーショングループに関連付けられません。既存のアプリケーショングループは影響を受けません。
true	False	新しいログオン情報は、既存のアプリケーショングループに追加されます。新しいログオン情報のパスワードには、そのグループで共有されているものが設定されます。既存のグループメンバーがない場合は、passwordエレメントで指定した値が設定されます。
true	true	新しいログオン情報は、既存のアプリケーショングループに追加されます。新しいログオン情報の

join 属性の値	**use-new-password 属性の値**	パスワードにはpasswordエレメントで指定した値が設定され、この新しいパスワードがグループ内影響で共有されます。

戻り値でpsoIDとして返されるログオン情報のGUID（credential-GUID）はlookupResponseオペレーションでリストされるものと同じものであり、modifyRequestオペレーションやdeleteRequestオペレーションでこのログオン情報を指定するときに使用できます。

ユーザーをリセットする - resetRequest

Sep 30, 2015

ユーザーが自分のログオン情報にアクセスできなくなった場合は、resetRequestオペレーションを使用してユーザーのSingle Sign-Onデータをリセットします。

構文

```
AuthToken
```

パラメーター

requestID（必須）	クライアント生成のIDで、これにより戻り値とこの要求が関連付けられます。
executionMode	Single Sign-Onでは、同期実行モード（synchronous）がサポートされます。
authentication-token	authentication-tokenエレメントは必須ですが、現在使用されていません。
psoID（必須）	各ユーザーに固有の識別子で、ユーザーのFQDNです。

戻り値の構文 - resetResponse

戻り値のパラメーター

status（必須）	値：success、failure、pending
requestID（必須）	クライアント生成のIDで、これにより戻り値と要求が関連付けられます。

名前空間エレメント

Sep 30, 2015

SPMLコマンドで使用されるSingle Sign-Onのカスタムエレメントは、http://citrix.com/Provision名前空間に属しています。この名前空間は、プレフィックスctxsで示されます。この名前空間には、3つの最上位エレメントがあります。authentication-token、application、およびcredentialです。

authentication-tokenエレメント - ctxs:authentication-token

authentication-tokenエレメントは、認証トークン（AuthToken）のコンテナーとして使用されます。このエレメントは必須ですが、使用されません。また、authentication-tokenエレメントには子エレメントがありません。

構文

```
AuthToken
```

applicationエレメント - ctxs:application

applicationエレメントは、最上位エレメントである場合とcredentialエレメントの子エレメントである場合があります。

このエレメントでは、アプリケーション定義（「lookupApplicationRequest」を参照）やログオン情報の詳細（「addRequest」を参照）を記述します。

構文

```
app-GUID Outlook description from app-def  Domain
```

注：この例では、fieldsエレメントの子エレメントで文字データが定義されていません。

パラメーター

id（必須）	アプリケーション定義のGUIDで、コンソールでそのアプリケーション定義を作成したときに割り当てられたものです。
name	管理者が定義した、アプリケーション定義の名前です。
description	管理者が定義した、アプリケーション定義の説明です。
group（パスワードを共有する場合は必須）	コンソールでこのアプリケーション定義に割り当てられているアプリケーショングループです。password-sharing属性はブール値で、このグループに共有パスワードが構成されているかどうかを指定します。詳しくは、「addRequest」を参照してください。
fields（必須）	このアプリケーション定義を使ってログオン情報に構成する、データフィールドのリストです。これらのフィールドのサブセットを使用して、アプリケーション定義を作成します。 fieldsエレメントには、以下の子エレメントがあります。 • userIDは、ユーザーIDに対応します。 • passwordは、ユーザーのパスワードに対応します。 • custom-fieldは、アプリケーション定義に含めるカスタムフィールドに対応します。index属性（1または2）で個々のフィールドを指定し、label属性でオプションのラベル文字列を指定します。

credentialエレメントの子エレメントとしてのapplicationエレメントの例については、「ctxs:credential」を参照してください。

credentialエレメント - ctxs:credential

credentialエレメントでログオン情報の内容を定義します。多くの場合、各ログオン情報は特定のアプリケーション定義に関連付けられます。ログオン情報を関連付けるアプリケーション定義は、子エレメントであるapplicationエレメントで指定します。ユーザーが手入力するログオン情報には、applicationエレメントが含まれません。

構文

```
Credential Name user visible description  optional-RA provided-description   appdefGuid  johnd pass123 mydomain
```

パラメーター

status（必須）	credentialエレメントのstatus属性は、そのログオン情報の状態を示します。属性値は、activeまたはqueuedです。activeはそのログオン情報がSingle Sign-On Plug-inで使用可能であることを示し、queuedはそのログオン情報の追加コマンドがSingle Sign-On Plug-inで処理待ち状態であることを示します。
pendingAction	credentialエレメントのpendingAction属性は、そのログオン情報に対する処理待ちのコマンドを示します。属性値はadd、modify、またはdeleteです。deleteはそのログオン情報を削除するコマンドが処理待ちであることを示し、modifyはそのログオン情報を変更するコマンドが処理待ちであることを示します。この属性はオプションであり、処理待ちのコマンドがない場合は省略されます。
name	credentialエレメントのname属性は、Single Sign-On Plug-inの［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）に表示される名前を示します。ユーザーは、ログオン情報のプロパティを編集してこの値を変更することができます。
description	credentialエレメントのdescription属性は、Single Sign-On Plug-inの［パスワード管理］ダイアログボックス（旧称「ログオンマネージャー」）に表示される説明を示します。ユーザーは、ログオン情報のプロパティを編集してこの値を変更することができます。
provision-description	provision-descriptionは管理者用データで、Single Sign-On Plug-inで表示したり編集したりすることはできません。プロビジョニング管理者専用の情報です。
application	applicationエレメントはアプリケーション定義のGUIDを示し、userID、password、およびcustom-fieldエレメントの文字データはこのログオン情報の詳細を示します。