Single Sign-On 5.0

Dec 11, 2015

À propos de

Oct 21, 2015

Single Sign-On 5.0 intègre Single Sign-On Plug-in à Citrix Receiver, simplifie l'expérience utilisateur, permet à Single Sign-On Plug-in d'être déployé à l'aide de Merchandising Server et prend désormais en charge le chinois simplifié avec Single Sign-On Plug-in.

- **Les utilisateurs accèdent à Single Sign-on Plug-in via l'icône de Citrix Receiver.** La ou les icônes de Single Sign-On Plug-in qui s'affichaient dans la zone de notification Windows sont maintenant remplacées par l'icône de Citrix Receiver. Seule une icône de Citrix Receiver s'affiche dans la zone de notification Windows, quel que soit le nombre de sessions Single Sign-On actives. Les utilisateurs gèrent les informations d'ouverture de session, peuvent mettre Single Sign-On en pause et le reprendre, déterminer si Single Sign-On est mis en pause et soumettre des mots de passe manuellement à l'aide des options de menu disponibles via l'icône de Citrix Receiver.
  Remarque : si des versions antérieures du plug-in sont installées, des icônes supplémentaires peuvent apparaître dans la zone de notification Windows. Consultez la section Installation de Single Sign-On Plug-in pour de plus amples informations.
- **Single Sign-On Plug-in est requis sur les machines utilisateur pour que l'utilisateur bénéficie de toutes les fonctionnalités.** Si Single Sign-On Plug-in n'est pas installé sur la machine utilisateur, il est possible que les utilisateurs ne puissent pas gérer les informations d'identification, mettre Single Sign-On en pause et le reprendre, déterminer si Single Sign-On est mis en pause ou soumettre des mots de passe manuellement. Consultez la section Scénarios de déploiement de Single Sign-On Plug-in pour de plus amples informations.
- **Les utilisateurs ferment Single Sign-On Plug-in en quittant Citrix Receiver**. Les utilisateurs quittent Single Sign-On en choisissant l'option Quitter dans le menu de l'icône Citrix Receiver. Cela ferme l'interface utilisateur de Citrix Receiver et tous les plug-ins auxquels vous avez accédé par le biais de Receiver.
- **Les utilisateurs gèrent les informations d'ouverture de session à l'aide la fenêtre Gérer les mots de passe.** Le Gestionnaire d'informations d'identification a été renommé Gérer les mots de passe et a été remanié pour simplifier l'expérience utilisateur :
  - Les utilisateurs accèdent à la fenêtre Gérer les mots de passe via une option de menu disponible via l'icône de Citrix Receiver. Cette fenêtre contient les informations d'ouverture de session des applications de toutes les sessions utilisateur.
  - Vous la configurez pour afficher les colonnes pour un ou plusieurs des attributs suivants : nom, description, groupe, date et heure de la dernière utilisation, date et heure de la dernière modification. Les utilisateurs peuvent trier les attributs.
  - La fenêtre Gérer les mots de passe ne dispose d'aucun menu déroulant. Les fonctionnalités auxquelles vous accédiez préalablement à l'aide des options de ces menus dans le Gestionnaire d'informations d'identification ont été supprimées ou sont accessibles comme suit :

Menu	Option	Qu'en est-il de cette fonctionnalité dans Single Sign-On 5.0 ?
Fichier	Nouvelles informations d'identification ou Nouvelles	Les utilisateurs stockent les informations d'identification manuellement à l'aide de l'option Envoyer disponible dans le menu de l'icône Citrix Receiver.

Menu	Option	Qu'en est-il de cette fonctionnalité dans Single Sign-On 5.0 ?
	informations d'identification > Configurer une application	
	Nouvelles informations d'identification > Configurer plusieurs applications	Les utilisateurs créent différents ensembles d'informations d'identification pour la même application en créant le premier ensemble d'informations d'identification, en le copiant et en modifiant la copie.
	Copier	Remplacé par le bouton Copier dans la fenêtre Gérer les mots de passe.
	Supprimer	Remplacé par le bouton Supprimer dans la fenêtre Gérer les mots de passe.
	Properties	Remplacé par le bouton Modifier dans la fenêtre Gérer les mots de passe.
	Sortir	Les utilisateurs quittent la fenêtre Gérer les mots de passe à l'aide du bouton Fermer de Windows.
View	Icône, liste et détail	Cette fonctionnalité a été supprimée pour simplifier l'expérience utilisateur.
	Organiser les icônes selon	Cette fonctionnalité n'est pas disponible, mais les utilisateurs peuvent trier les colonnes dans la fenêtre Gérer les mots de passe en cliquant sur l'en-tête de colonne.
	Actualiser	Remplacé par le lien Actualiser dans la fenêtre Gérer les mots de passe.
	Révéler les mots de passe	Les utilisateurs peuvent afficher un mot de passe à l'aide du bouton Révéler le mot de passe de la fenêtre Gérer les mots de passe. Ils ne peuvent révéler qu'un mot de passe à la fois.
Outils	Association de comptes	Les utilisateurs ne peuvent pas activer la fonction Association de comptes à l'aide de Single Sign-on Plug-in. Pour leur permettre d'activer cette fonction, donnez-leur accès à AccAssoc.exe en tant qu'application publiée.
	Enregistrement des questions de sécurité	Les utilisateurs ne peuvent pas réenregistrer leurs réponses aux questions de sécurité à l'aide de Single Sign-On Plug-in, à moins que vous ne les invitiez à le faire. Pour permettre aux utilisateurs de réenregistrer leurs réponses aux questions de sécurité

Menu	Option	Qu'en est-il de cette fonctionnalité dans Single Sign-On 5.0 ?
	Options > Confirmer la sortie	La confirmation de sortie est contrôlée via Citrix Receiver. Single Sign-On Plug-in n'affiche pas de message vous invitant à confirmer votre volonté de quitter.
Aide	Aide du Gestionnaire d'informations d'identification	Remplacé par le lien Aide dans la fenêtre Gérer les mots de passe.
	À propos de	Remplacé par le lien À propos de dans la fenêtre Gérer les mots de passe.

sans y être invités, donnez-leur accès à QBAEnroll.exe en tant qu'application publiée.

- La fenêtre Gérer les mots de passe ne dispose d'aucun menu contextuel. Les fonctionnalités auxquelles vous accédiez préalablement à l'aide de ce menu dans le Gestionnaire d'informations d'identification sont maintenant accessibles comme suit :

Option	Qu'en est-il de cette fonctionnalité dans Single Sign-On 5.0 ?
Copier	Remplacé par le bouton Copier dans la fenêtre Gérer les mots de passe.
Supprimer	Remplacé par le bouton Supprimer dans la fenêtre Gérer les mots de passe.
Properties	Remplacé par le bouton Modifier dans la fenêtre Gérer les mots de passe.

- **Les utilisateurs ne peuvent pas être invités à stocker leurs informations d'identification la première fois qu'ils utilisent Single Sign-On.** L'option de configuration initiale des informations d'identification a été supprimée.
- **Single Sign-On Plug-in peut être déployé et géré à l'aide de Merchandising Server.** Si Citrix Receiver Updater est installé sur les machines utilisateur, vous pouvez déployer et gérer Single-Sign-On Plug-in avec Merchandising Server.
- **Single Sign-On Plug-in peut être déployé en chinois simplifié.**

Consultez les Problèmes connus dans XenApp 6.5 pour Windows Server 2008 R2 pour les problèmes connus de Single Sign-on 5.0.

Mise en route

Oct 21, 2015

Composants principaux de Single Sign-On :

- magasin central ;
- composant Single Sign-On de Citrix AppCenter ;
- Single Sign-On Plug-in
- service Single Sign-On (facultatif).

Le magasin central est un stockage centralisé permettant à Single Sign-On de stocker et de gérer les données utilisateur et d'administration. Les données utilisateur comprennent notamment les informations d'identification, les réponses aux questions de sécurité et d'autres données relatives à l'utilisateur. Les données d'administration incluent les stratégies de mot de passe, les définitions d'application, les questions de sécurité et d'autres données de portée plus large. Lorsqu'un utilisateur ouvre une session, Single Sign-On compare ses informations d'identification à celles stockées dans le magasin central. Lorsque l'utilisateur ouvre des applications ou des pages Web protégées par mot de passe, les informations d'identification adéquates sont extraites du magasin central.

Le composant Single Sign-On de Citrix AppCenter est le centre de commande de Single Sign-On. Vous pouvez y configurer la façon dont fonctionne Single Sign-On, les fonctions à déployer, les mesures de sécurité à utiliser et d'autres paramètres importants liés aux mots de passe.

Le composant contient quatre éléments principaux, ou nœuds, dans le panneau de gauche. Lorsque vous sélectionnez un nœud, ses tâches spécifiques apparaissent. Ces nœuds sont les suivants.

- Les configurations utilisateur permettent d'ajuster certains paramètres des utilisateurs en fonction de leur emplacement géographique ou de leur rôle dans l'entreprise.
- Les définitions d'application offrent les informations nécessaires à Single Sign-On Plug-in pour l'authentification auprès des applications et pour la détection des erreurs. Utilisez les modèles de définition d'application fournis avec Single Sign-On pour accélérer le processus ou créer vos définitions personnalisées pour les applications qui ne peuvent pas utiliser ces modèles.
- Les stratégies de mot de passe contrôlent la longueur des mots de passe, le type et la variété des caractères des mots de passe définis par l'utilisateur et générés automatiquement. Elles vous permettent aussi de spécifier les caractères à exclure dans les mots de passe et la réutilisation des mots de passe précédents. La création de stratégies de mot de passe cohérentes avec les stratégies de sécurité de votre entreprise garantit une bonne gestion de la sécurité des mots de passe par Single Sign-On.
- La vérification d'identité vous permet de créer des questions de sécurité qui offrent une couche de sécurité supplémentaire à Single Sign-On Plug-in. Les questions de sécurité protègent contre l'usurpation d'identité, les modifications de mot de passe et les déverrouillages de compte non autorisés. Les utilisateurs qui s'inscrivent et qui répondent à vos questions de sécurité peuvent ensuite vérifier leur identité en fournissant les mêmes réponses aux questions. Une fois la vérification effectuée, les utilisateurs peuvent accomplir les tâches des fonctions autonomes sur leur compte, comme la réinitialisation de leur mot de passe principal ou le déverrouillage de leur compte utilisateur. Les questions de sécurité peuvent également servir à la récupération de clés.

Single Sign-On Plug-in soumet les informations d'identification appropriées aux applications exécutées sur la machine cliente de l'utilisateur, applique les stratégies de mot de passe, fournit la fonctionnalité des fonctions autonomes et permet aux utilisateurs de gérer leurs informations d'identification avec la fenêtre Gérer les mots de passe (anciennement Gestionnaire d'informations d'identification). En outre, le plug-in offre aux utilisateurs une grande variété de fonctions. Ces dernières dépendent des paramètres administratifs définis dans les configurations utilisateur.

Il est exécuté sur un serveur Web qui constitue la base des fonctionnalités optionnelles disponibles dans cette version. Installez le service Single Sign-On si vous envisagez de mettre en place au moins un des modules suivants :

- Fonctions autonomes de compte, qui permet la réinitialisation des mots de passe Windows et le déverrouillage des comptes Windows.
- Intégrité des données, qui protège les données lors de leur transfert du magasin central vers Single Sign-On Plug-in.
- Gestion des clés, qui permet aux utilisateurs de récupérer leurs informations d'identification secondaires lorsque leur mot de passe principal change, soit par récupération de clé automatique, soit après réponse aux questions de sécurité avec authentification avec questions.
- Habilitation, qui vous permet d'utiliser le composant Single Sign-On de Citrix AppCenter pour ajouter, supprimer ou mettre à jour les données utilisateur et les informations d'identification Single Sign-On.
- Synchronisation des informations d'identification, qui synchronise les informations d'identification sur les différents domaines utilisant un service Web.

Si vous ne mettez pas en place ces modules, n'installez pas le service Single Sign-On.

Évaluer

Oct 21, 2015

Si vous utilisez XenApp 6.5 pour Windows Server 2008 R2 pour publier des applications et que vous souhaitez utiliser Single Sign-On 5.0 pour offrir un accès protégé par mot de passe doublé d'une authentification unique, cette rubrique vous permet de déployer Single Sign-On rapidement. Le déploiement Single Sign-On décrit ici peut être utilisé pour évaluer Single Sign-On ou en tant que déploiement pilote auquel vous pouvez ajouter plus d'utilisateur et d'applications.

Remarque : pour simplifier le processus de déploiement, le déploiement décrit ici exclut certains composants, fonctionnalités et options qui sont disponibles lorsque vous utilisez Single Sign-On 5.0 avec XenApp 6.5.
Le déploiement décrit ici inclut les composants Single Sign-On suivants :

- **Magasin central.** Le magasin central est un stockage centralisé permettant à Single Sign-On de stocker et de gérer les données utilisateur et d'administration. Les données utilisateur comprennent notamment les informations d'identification, les réponses aux questions de sécurité et d'autres données relatives à l'utilisateur. Les données d'administration incluent les stratégies de mot de passe, les définitions d'application, les questions de sécurité et d'autres données de portée plus large. Lorsqu'un utilisateur ouvre une session, Single Sign-On compare ses informations d'identification à celles stockées dans le magasin central. Lorsque l'utilisateur ouvre des applications ou des pages Web protégées par mot de passe, les informations d'identification adéquates sont extraites du magasin central.
- **Composant Single Sign-On de Citrix AppCenter.** Pour ce déploiement, vous pouvez utiliser le déploiement Single Sign-On de Citrix AppCenter pour définir des stratégies de mot de passe, configurer Single Sign-On de manière à reconnaître les applications et créer des configurations utilisateur.
- **Outil de définition d'application** L'Outil de définition d'application dispose des mêmes fonctionnalités que la partie du composant Single Sign-On de Citrix AppCenter chargée de configurer Single Sign-On afin de reconnaître les applications.
- **Single Sign-on Plug-in.** Single Sign-On Plug-in est le composant de Single Sign-On avec lequel les utilisateurs interagissent. Il envoie les informations d'identification appropriées aux applications exécutées sur la machine cliente de l'utilisateur, applique les stratégies de mot de passe et permet aux utilisateurs de gérer leurs informations d'identification avec la fenêtre Gérer les mots de passe. Il est installé sur chaque machine utilisateur dans le cadre de ce déploiement.

Ce déploiement ne comprend pas le service Single Sign-On et aucune des fonctionnalités supplémentaires que ce dernier prend en charge :

- Fonctions autonomes de compte, qui permet la réinitialisation des mots de passe Windows et le déverrouillage des comptes Windows.
- Intégrité des données, qui protège les données lors de leur transfert du magasin central vers Single Sign-On Plug-in.
- Gestion des clés, qui permet aux utilisateurs de récupérer leurs informations d'identification secondaires lorsque leur mot de passe principal change, soit par récupération de clé automatique, soit après réponse aux questions de sécurité avec authentification avec questions.
- Habilitation, qui vous permet d'utiliser le composant Single Sign-On de Citrix AppCenter pour ajouter, supprimer ou mettre à jour les données utilisateur et les informations d'identification Single Sign-On.
- Synchronisation des informations d'identification, qui synchronise les informations d'identification sur les différents domaines utilisant un service Web.

Réalisez les tâches détaillées dans cette rubrique dans l'ordre dans lequel elles apparaissent.

- Vérifiez la configuration système requise pour le magasin central, le composant Single Sign-On d'AppCenter, l'Outil de

définition d'application et le plug-in : Configuration système requise.

- Vérifiez les exigences en termes de licences pour Single Sign-On et installez ou mettez à niveau des licences le cas échéant : Configuration système requise.
- Identifiez les applications que vous voulez inclure. Pour de déploiement, choisissez uniquement des applications Windows et Web publiées avec XenApp :
  - Pour les applications Windows, utilisez des applications Windows 32 bits (y compris les applications Java) telles que Microsoft Outlook, Lotus Notes, SAP ou toute application Windows protégée par mot de passe. Single Sign-On considère toute application lancée par un fichier portant l'extension .exe comme une application Windows.
  - Pour les applications Web, utilisez des applications Web (y compris les applets Java et SAP), accessibles via Microsoft Internet Explorer. En règle générale, Single Sign-On considère toute application exécutée dans un navigateur comme une application Web. Single Sign-On prend en charge les applications Web exécutées sur Internet Explorer versions 6.0, 7.0, 8.0 et 9.0.
- Identifiez les utilisateurs que vous voulez inclure. Assurez-vous que leurs machines utilisateur prennent en charge Single Sign-On Plug-in.
- Décidez où installer le magasin central. Le magasin central pour ce déploiement est un partage réseau NTFS.
- Décidez où installer le composant Single Sign-On de Citrix AppCenter. Vous pouvez utiliser un AppCenter déjà installé ou en installer un nouveau.
- Décidez si vous allez installer l'Outil de définition d'application et où l'installer le cas échéant. Si Citrix AppCenter n'est pas installé sur l'ordinateur exécutant une application que vous voulez inclure à votre déploiement, installez l'Outil de définition d'application sur cet ordinateur. Lorsque vous configurez Single Sign-On de manière à ce qu'il reconnaisse des applications, vous exécutez les applications et autorisez les assistants à capturer des informations sur les applications.
- Planifiez vos stratégies de mot de passe. Les stratégies de mot de passe sont des règles qui contrôlent la manière dont les mots de passe sont créés, envoyés et gérés ; vous pouvez appliquer des stratégies de mot de passe à tous les utilisateurs ou à des groupes spécifiques d'applications. Single Sign-On comporte deux stratégies de mot de passe standard intitulées Default et Domain. Si les valeurs par défaut de ces stratégies standard répondent à vos besoins dans le cadre de ce déploiement, vous pouvez les utiliser sans les modifier. Sinon, vous pouvez créer de nouvelles stratégies basées sur les stratégies standard et modifier ces valeurs.
  - Pour une présentation des stratégies de mot de passe, veuillez consulter la section Stratégies de mot de passe.
  - Pour obtenir des conseils sur la façon de sécuriser vos stratégies de mot de passe, consultez la section Stratégies de mot de passe.
  - Pour savoir comment Single Sign-On applique les stratégies de mot de passe, consultez la section Application des exigences de mot de passe.
  - Pour déterminer si les valeurs par défaut des règles de stratégie de mot de passe sont adaptées à vos applications et utilisateurs, passez en revue les valeurs par défaut de chaque paramètre dans la rubrique de référence Stratégies de mot de passe et toutes ses sous-rubriques. Valeurs par défaut des stratégies de mot de passe standard (par défaut et domaine).
- Planifiez vos configurations utilisateur. Une configuration utilisateur constitue une collection unique de réglages, stratégies de mot de passe et applications que vous appliquez à des utilisateurs associés à une hiérarchie Active Directory (unité organisationnelle ou utilisateur) ou à un groupe Active Directory. Une configuration utilisateur vous permet de contrôler le comportement et l'aspect du plug-in au niveau des utilisateurs.
  - Pour consulter une présentation des configurations utilisateur et vérifier les paramètres de configuration utilisateur utilisés dans ce déploiement et leurs valeurs par défaut, consultez Liste de référence des paramètres de Single Sign-On 5.0. Gardez à l'esprit que certaines des options et fonctionnalités abordées dans cette rubrique ne sont pas utilisées dans ce déploiement. Cette présentation traite des points suivants :
    - Interaction de base du plug-in
    - Interface utilisateur du plug-in

- Synchronisation
  Remarque : ne sélectionnez pas Permettre l'accès aux informations d'identification par le module de synchronisation des informations d'identification. Ce déploiement de configuration utilisateur ne comprend pas le module de synchronisation des informations d'identification.
- Prise en charge d'application
- Système de licences

- Pour protéger les informations d'identification de vos utilisateurs, consultez la section Méthode de protection des données.
  Remarque : utilisez les valeurs par défaut pour les paramètres de la protection secondaire des données. Les autres valeurs requièrent le module de gestion des clés, qui n'est pas inclus dans ce déploiement.
  Pour ce déploiement, vous pouvez utiliser les paramètres par défaut de la configuration utilisateur (à l'exception des paramètres du système de licences) dans la plupart des environnements. Si vos circonstances changent une fois le déploiement opérationnel, vous pouvez modifier les valeurs de la configuration utilisateur.

  Les paramètres des fonctionnalités qui ne sont pas utilisées dans ce déploiement sont désactivés par défaut.

Il existe deux types de magasin central Single Sign-On : Active Directory ou partage réseau NTFS. Dans le cadre de ce déploiement, vous créez un partage réseau NTFS car sa création requiert moins de permissions que la création d'un magasin central Active Directory. Pour passer en revue les avantages et considérations à prendre en compte lors de la création d'un magasin central sur un partage réseau NTFS, consultez la section Choix d'un point de partage réseau NTFS.

Au besoin, vous pouvez migrer des utilisateurs vers un magasin central Active Directory ultérieurement.

Pour créer un magasin central sur un partage réseau NTFS :

1. Chargez le support XenApp.
2. À partir du menu Autorun, sélectionnez Installer les composants manuellement > Composants serveur > Fonctionnalités supplémentaires > Single Sign-On.
3. Sélectionnez Magasin central.
4. Sélectionnez Partage réseau NTFS.

Le magasin central est crée sous %LecteurSystème%\CITRIXSYNC$.

AppCenter inclut par défaut le composant Single Sign-On lorsqu'il est installé.

Pour utiliser un AppCenter existant avec Single Sign-On, configurez et exécutez la découverte après la création du magasin central.

Pour installer un nouveau AppCenter à utiliser avec Single Sign-On, assurez-vous que les packs Microsoft Visual C++ Redistributable Packages et Microsoft Primary Interoperability Assemblies sont installés, comme décrit dans la section Configuration système requise.

Pour installer AppCenter :

1. Chargez le support XenApp sur l'ordinateur.
2. À partir du menu Autorun, sélectionnez Installer les composants manuellement > Composants courants > Console de gestion. Suivez les instructions.
3. Sélectionnez Configurer et exécuter la découverte et suivez les instructions.

Après la configuration, le composant Single Sign-On de AppCenter est connecté au magasin central et vous pouvez l'utiliser pour définir des stratégies de mot de passe, configurer Single Sign-On à reconnaître des applications et créer des configurations utilisateur.

Si Citrix AppCenter n'est pas installé sur l'ordinateur exécutant une application que vous voulez inclure à votre déploiement, installez l'Outil de définition d'application pour créer des définitions d'application pour l'application.

1. Chargez le support XenApp sur l'ordinateur.
2. Accédez au fichier ASC_PasswordManager dans le dossier Administration et exécutez-le.
3. Sélectionnez Outil de définition d'application. Suivez les instructions.

Si vous avez déterminé que les valeurs par défaut des stratégies de mot de passe standard répondaient à vos besoins pour ce déploiement, vous n'avez pas à définir de stratégies supplémentaires. Sinon, créez de nouvelles stratégies basées sur les stratégies standard.

Pour créer une nouvelle stratégie de mot de passe :

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Stratégies de mot de passe.
3. À partir du menu Action, cliquez sur Créer une nouvelle stratégie de mot de passe.
4. Suivez les instructions de l'Assistant de stratégie de mot de passe.

Single Sign-On reconnaît et répond aux applications selon des paramètres définis dans les définitions d'application. Les définitions d'application offrent les informations nécessaires à Single Sign-On Plug-in pour l'authentification auprès des applications et pour la détection des erreurs.

Les définitions d'application se composent de définitions de formulaire. Les définitions de formulaire permettent à Single Sign-On Plug-in d'analyser chaque application au moment de son lancement, de reconnaître certaines des caractéristiques qui l'identifient et de déterminer si elle requiert que le plug-in effectue des actions spécifiques, par exemple :

- soumettre des informations d'identification de l'utilisateur dans une invite d'authentification ;
- traiter une interface d'informations d'identification changeante ;
- traiter l'interface de confirmation des informations d'identification.

Bien que la plupart des applications et leurs définitions utilisent seulement deux formulaires pour gérer les informations d'identification des utilisateurs, vous pouvez définir autant de formulaires que nécessaire dans une définition d'application.

Vous pouvez créer les types de formulaires de gestion des informations d'identification utilisateur suivants :

- Formulaire d'authentification
  Identifie l'interface d'authentification d'une application et gère les actions requises pour accéder à l'application associée.

- Formulaire de modification de mot de passe
  Identifie l'interface de modification du mot de passe d'une application et gère les actions requises pour modifier le mot de passe utilisateur permettant d'accéder à l'application.

- Formulaire de modification de mot de passe réussie
  Identifie l'interface de modification du mot de passe d'une application et gère les actions requises pour confirmer la

réussite du changement du mot de passe permettant d'accéder à l'application.

- Formulaire d'échec de modification de mot de passe
  Identifie l'interface indiquant l'échec du changement du mot de passe et définit les actions à effectuer dans ces cas.

Vous créez des définitions d'application à l'aide des assistants disponibles dans AppCenter ou de l'Outil de définition d'application. Lorsque l'application que vous voulez définir est exécutée ou disponible dans une fenêtre de navigateur, ces assistants aident à capturer les informations dont vous avez besoin pour la définition de l'application. Pour pouvoir créer une définition d'application, vous devez avoir accès à l'application sur l'ordinateur sur lequel la définition d'application est créée.

Étant donné que certaines signatures d'applications varient considérablement selon le système d'exploitation sous-jacent, testez les définitions d'application sur tous les systèmes d'exploitation sur lesquels elles seront exécutées.

Des modèles d'application sont disponibles pour certaines applications. Ces modèles permettent de simplifier le processus d'ajout de définitions d'application à votre déploiement Single Sign-On en fournissant la plupart des informations requises pour créer une définition d'application. Pour plus d'informations sur les modèles d'application, consultez la section Modèles d'application.

Pour créer une définition d'application Windows

Pour créer des définitions d'application pour une application Windows, exécutez l'application sur un ordinateur sur lequel vous lancez l'assistant de définition d'application à partir de Citrix AppCenter ou de l'Outil de définition d'application. Accédez ensuite au formulaire au sein de l'application nécessitant un événement de gestion des informations d'identification utilisateur (ouverture de session utilisateur, modification du mot de passe, modification réussie du mot de passe ou échec de la modification de mot de passe) lors de l'exécution de l'assistant.

Pour obtenir un aperçu des aspects à considérer lors de la création de définitions d'applications Windows, consultez la section Définitions d'applications de type Windows.

1. Démarrer l'application.
2. Démarrez l'assistant de définition d'application :
   - À partir de AppCenter : cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter. Développez le nœud Single Sign-On et sélectionnez Définitions d'application.
   - À partir de l'Outil de définition d'application : à partir de AppCenter : cliquez sur Démarrer > Tous les programmes > Citrix > Single Sign-On > Outil de définition d'application.
3. Sélectionnez Créer une définition d'application.
4. Assurez-vous que les cases Windows et Créer une nouvelle définition sont sélectionnées et cliquez sur Démarrer l'assistant.
5. Entrez le nom de l'application tel que vous voulez qu'il apparaisse dans le magasin central. Éventuellement, entrez une description. Cliquez sur Suivant.
6. Cliquez sur Ajouter un formulaire. Cela lance l'assistant de définition de formulaire.
7. Si ce n'est pas encore fait, accédez au formulaire d'authentification, de modification de mot de passe, de modification de mot de passe réussie ou d'échec de modification de mot de passe.
8. Dans la page Identifier le formulaire de l'assistant de définition de formulaire, cliquez sur Sélectionner.
9. Dans le Sélecteur de fenêtre qui s'affiche, sélectionnez l'application pour laquelle vous créez la définition. L'application choisie est entourée d'une bordure clignotante.
10. Sur la page Nommer le formulaire, entrez un nom pour le formulaire et sélectionnez le type de formulaire. Cliquez sur Suivant.
11. Dans le Sélecteur de fenêtre, cliquez sur OK.

12. Sur la page Identifier le formulaire, cliquez sur Suivant.
13. Sur la page Définir les actions du formulaire, configurez les champs d'authentification et les boutons que vous voulez inclure au formulaire.
    1. Cliquez sur le lien hypertexte Définir/Modifier associé aux informations d'identification d'un utilisateur spécifique. Cette action ouvre la boîte de dialogue Configuration du texte de contrôle, qui permet d'identifier le contrôle qui doit recevoir les informations d'identification sélectionnées.
    2. Sélectionnez le type de contrôle qui doit recevoir les informations d'identification. À mesure que les différents candidats sont sélectionnés, le type de contrôle associé est mis en évidence sur l'application à l'aide d'une bordure clignotante.
    3. Répétez cette procédure pour toutes les informations d'identification requises pour le formulaire ainsi que pour le bouton utilisé pour soumettre le formulaire.
       Certains formulaires requièrent des domaines ou d'autres informations d'identification configurées par l'utilisateur, qui doivent être correctement soumises pour que le formulaire puisse être traité. Pour répondre à ces exigences, deux champs personnalisables sont disponibles. Utilisez ces champs pour définir des informations d'identification spéciales. Les noms associés à ces champs sont définis dans la page Nommer les champs personnalisés de l'assistant de définition d'application, une fois le formulaire défini.

       Remarque : toutes les informations d'identification identifiées au haut de la page Définir les actions du formulaire ne doivent pas obligatoirement être configurées.
14. Si votre application requiert des formulaires supplémentaires, utilisez les assistants pour les créer.

Pour créer une définition d'application Web

Pour créer des définitions d'application pour une application Web, exécutez l'application sur un ordinateur sur lequel vous lancez l'assistant de définition d'application à partir de Citrix AppCenter ou de l'Outil de définition d'application. Accédez ensuite au formulaire au sein de l'application nécessitant un événement de gestion des informations d'identification utilisateur (ouverture de session utilisateur, modification du mot de passe, modification réussie du mot de passe ou échec de la modification de mot de passe) lors de l'exécution de l'assistant.

1. Démarrer l'application.
2. Démarrez l'assistant de définition d'application :
   - À partir de AppCenter : cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter. Développez le nœud Single Sign-On et sélectionnez Définitions d'application.
   - À partir de l'Outil de définition d'application : à partir de AppCenter : cliquez sur Démarrer > Tous les programmes > Citrix > Single Sign-On > Outil de définition d'application.
3. Sélectionnez Créer une définition d'application.
4. Assurez-vous que les cases Web et Créer une nouvelle définition sont sélectionnées et cliquez sur Démarrer l'assistant.
5. Dans la page Identifier l'application qui s'affiche, entrez le nom de l'application tel que vous voulez qu'il apparaisse dans le magasin central. Éventuellement, entrez une description. Cliquez sur Suivant.
6. Cliquez sur Ajouter un formulaire. Cela lance l'assistant de définition de formulaire.
7. Sur la page Nommer le formulaire, cliquez sur Suivant.
   1. Entrez un nom pour le formulaire.
   2. Sélectionnez le type de formulaire.
   3. Assurez-vous que la case Aucune action spéciale est sélectionnée.
   4. Cliquez sur Suivant.
8. Si ce n'est pas encore fait, accédez au formulaire d'authentification, de modification de mot de passe, de modification de mot de passe réussie ou d'échec de modification de mot de passe.

9. Sur la page Identifier le formulaire, cliquez sur Sélectionner. Cela lance l'assistant de formulaire Web.
10. Sur la page Sélecteur de page Web qui s'affiche, sélectionnez l'application pour laquelle vous créez la définition. Cliquez sur OK. Une bordure clignotante entoure la page Web qui affiche le formulaire d'informations d'identification de l'application.
11. Entrez un nom pour le formulaire et sélectionnez le type de formulaire. Cliquez sur Suivant.
12. Sur la page Identifier le formulaire, deux cases à cocher vous permettent de contrôler la façon dont les URL identifiées doivent être interprétées. Sélectionnez les cases appropriées et cliquez sur Suivant.
    - Recherche d'URL stricte
      Cochez cette case pour reconnaître uniquement les événements de gestion des informations d'identification des applications Web qui sont lancées à partir des URL spécifiées. Certaines URL peuvent contenir des données dynamiques telles que des identificateurs de gestion de session, des paramètres d'application ou d'autres identificateurs qui peuvent varier pour chaque instance. Dans ces circonstances, l'utilisation de la correspondance stricte risque de ne pas permettre la reconnaissance de l'URL.

    - URL sensible à la casse
      Cochez cette case pour utiliser l'URL avec la casse exacte.

13. Sur la page Définir les actions du formulaire, configurez les champs d'authentification et les boutons que vous voulez inclure au formulaire.
    1. Cliquez sur le lien hypertexte Définir/Modifier associé aux informations d'identification d'un utilisateur spécifique. Cette action ouvre la boîte de dialogue Configurer le texte du champ, qui permet d'identifier le champ qui doit recevoir les informations d'identification sélectionnées. Si le formulaire est déjà ouvert, cette boîte de dialogue affiche tous les types de champ possibles pour les informations d'identification sélectionnées ou pour l'option de soumission.
    2. Si le formulaire d'informations d'identification de l'application n'est pas ouvert, lancez l'application et affichez le formulaire approprié. Puis sélectionnez Actualiser. Une fois que vous avez sélectionné le formulaire de l'application, cette boîte de dialogue affiche les types de contrôle de champ appropriés pour les informations d'identification sélectionnées.
    3. Sélectionnez le type de champ qui doit recevoir les informations d'identification. À mesure que vous sélectionnez différentes options, le type de champ correspondant est mis en surbrillance dans l'application pour permettre de mieux voir la façon dont les informations d'identification sélectionnées et le bouton de soumission seront affichées.
    4. Répétez cette procédure pour toutes les informations d'identification requises pour le formulaire ainsi que pour le bouton utilisé pour soumettre le formulaire.
       Certains formulaires requièrent des domaines ou d'autres informations d'identification configurées par l'utilisateur, qui doivent être correctement soumises pour que le formulaire puisse être traité. Pour répondre à ces exigences, deux champs personnalisables sont disponibles. Utilisez ces champs pour définir des informations d'identification spéciales. Les noms associés à ces champs sont définis dans la page Nommer les champs personnalisés de l'assistant de définition d'application, une fois le formulaire défini.

       Remarque : toutes les informations d'identification identifiées au haut de la page Définir les actions du formulaire ne doivent pas obligatoirement être configurées.
14. Si votre application requiert des formulaires supplémentaires, utilisez les assistants pour les créer.

Pour ajouter une définition d'application à l'aide d'un modèle disponible

L'assistant de définition d'application vous aide à localiser les modèles d'application et à les ajouter à votre déploiement.

1. Démarrez l'assistant de définition d'application :
    - À partir de AppCenter : cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.

Développez le nœud Single Sign-On et sélectionnez Définitions d'application.
- À partir de l'Outil de définition d'application : à partir de AppCenter : cliquez sur Démarrer > Tous les programmes > Citrix > Single Sign-On > Outil de définition d'application.

2. Sélectionnez Gérer les modèles.
3. Passez en revue la liste des modèles pour voir si votre application y figure. Vous pouvez également cliquer sur le lien pour télécharger davantage d'applications du Web et les importer dans la liste.
4. Sélectionnez le modèle d'application que vous voulez ajouter et cliquez sur Créer une définition d'application.
5. Utilisez l'assistant pour modifier les formulaires de l'application ou acceptez les valeurs par défaut.

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. Cliquez sur Ajouter une nouvelle configuration utilisateur.
4. Entrez le nom de l'application tel que vous voulez qu'il apparaisse dans le magasin central. Éventuellement, entrez une description.
5. Indiquez comment vous allez associer cette configuration utilisateur aux utilisateurs.
   Vous disposez de deux options d'association des utilisateurs : à une hiérarchie de domaine Active Directory (unité organisationnelle ou utilisateur) ou à un groupe Active Directory. Si nécessaire, vous pourrez associer la configuration utilisateur à une autre hiérarchie ou un autre groupe plus tard, en cliquant sur Déplacer la configuration utilisateur dans le menu Action.

   Important : le mode d'organisation de votre environnement Active Directory peut affecter le fonctionnement des configurations utilisateur. Si vous utilisez les deux (une hiérarchie et des groupes Active Directory) et qu'un utilisateur se trouve dans les deux conteneurs, la configuration utilisateur associée à la hiérarchie a priorité et sera celle utilisée. Ce schéma est appelé environnement mixte.
   En outre, si un utilisateur appartient à deux groupes Active Directory et que chaque groupe est associé à une configuration utilisateur, la configuration qui possède le plus haut niveau de priorité sera celle utilisée.

   L'association de configurations utilisateur à des groupes n'est prise en charge que dans des domaines Active Directory utilisant l'authentification Active Directory.

6. Dans la page Choisir les applications, ajoutez les applications de la configuration utilisateur. Lorsque vous cliquez sur le bouton Ajouter, une boîte de dialogue contenant les définitions d'applications que vous avez créées précédemment s'affiche.
7. Utilisez la page Configurer l'interaction de Single Sign-On Plug-in pour déterminer l'expérience de tous les utilisateurs du plug-in dans votre environnement.
8. Sélectionnez un serveur de licences et un modèle de licences sur la page Configurer le système de licences.
9. Utilisez la page Sélectionner les méthodes de protection des données pour sélectionner les méthodes de protection de données à utiliser pour protéger les informations d'identification des utilisateurs en fonction des différentes méthodes d'authentification autorisées pour vos utilisateurs.

Single Sign-On Plug-in s'exécute sur le serveur XenApp et fournit des informations d'identification ainsi que l'accès aux applications publiées. Le plug-in s'exécute également sur chaque machine utilisateur, où il soumet les informations d'identification aux applications et permet aux utilisateurs de gérer leurs informations d'identification.

Considérations relatives à l'installation :

- Après installation du plug-in sur un système d'exploitation pris en charge qui utilise le composant Windows GINA (Microsoft Graphical Identification and Authentication), vous devez redémarrer la machine. Cela comprend Windows XP, Microsoft Windows XP Embedded, Microsoft Windows Fundamentals for Legacy PCs, Microsoft Windows Server 2003 R2 et Microsoft Windows Server 2003 avec Service Pack 2.
  WinLogon utilise les commandes GINA pour contrôler la boîte de dialogue que les utilisateurs voient lorsqu'ils appuient sur les touches CTRL+ALT+SUPPR. Cette boîte collecte les données nécessaires à l'authentification. XenApp, Single Sign-On Plug-in et le client Novell NetWare interagissent avec la DLL GINA ou nécessitent son remplacement. Cela implique d'installer ou désinstaller les logiciels dans un ordre spécifique pour préserver la chaîne GINA correcte. En installant Single Sign-On Plug-in en dernier, vous garantissez que la GINA de Single Sign-On est appelée en premier par le processus Winlogon.
- Une fois l'installation terminée (et après avoir redémarré la machine, le cas échéant), l'icône de Citrix Receiver s'affiche dans la barre d'état système.
- Après avoir installé le plug-in, si vous configurez ou que vous modifiez les informations relatives au système de licences Citrix, redémarrez le plug-in pour que les modifications soient appliquées.

Pour installer Single Sign-On Plug-in sur une machine utilisateur ou un serveur sur lequel XenApp est installé :

1. Chargez le support XenApp sur l'ordinateur ou le serveur.
2. À partir du menu Autorun, sélectionnez Installer les composants manuellement > Composants serveur > Fonctionnalités supplémentaires > Single Sign-On > Single Sign-On Plug-in.
3. Suivez les instructions.

Avant de commencer à utiliser Single Sign-On, consultez l'aide de l'utilisateur via l'interface de Single Sign-On. Indiquez à vos utilisateurs comment Single Sign-On fonctionne et les fonctionnalités auxquelles ils auront accès dans ce déploiement.

Configuration système requise

Oct 21, 2015

Les ordinateurs présents dans votre environnement Single Sign-On requièrent les logiciels suivants :

Composant logiciel	Requis par	Emplacement
Microsoft Windows Installer 3.0 ou version supérieure (inclus automatiquement durant l'installation d'Autorun)	Tous	• Dossier Support du support d'installation de Single Sign-On • http://www.microsoft.com
Microsoft .NET Framework 3.5 Service Pack 1 (inclus automatiquement durant l'installation d'Autorun)	• Service Single Sign-On • Composant Single Sign-On de la console AppCenter • Outil de définition d'application	Dossier Support du support d'installation de Single Sign-On
Microsoft Internet Explorer Version 6.0, 7.0, 8.0 ou 9.0 (mode non protégé)	Utilisateurs qui accèdent aux applications Web activées pour Single Sign-On	http://www.microsoft.com
ASP.NET	Service Single Sign-On	http://www.asp.net/

• Pour les ordinateurs 32 bits : Microsoft Visual C++ 2005 Redistributable Package (x86) Service Pack 1
  • vc80_vcredist_x86.exe
• Pour les ordinateurs 64 bits : Microsoft Visual C++ 2005 Redistributable Package (x64) Service Pack 1
  • vc80_vcredist_x86.exe
  • vc80_vcredist_x64.exe
	Composant console Single Sign-On, service ou plug-in — lors de l'installation du composant console, service ou plug-in à partir d'une invite de commande sur un ordinateur Windows Vista, Windows Server 2008 ou Windows Server 2008 R2	Dossier Support du support d'installation de Single Sign-On

• Pour les ordinateurs 32 bits : Microsoft Visual C++ 2008 Redistributable Package (x86) Service Pack 1 • vc90_vcredist_x86.exe • Pour les ordinateurs 64 bits : Microsoft Visual C++ 2008 Redistributable Package (x86)	Composant console Single Sign-On, service ou plug-in — lors de l'installation du composant console, service ou plug-in à partir d'une invite de commande sur un ordinateur Windows Vista, Windows Server 2008 ou Windows Server 2008 R2	Dossier Support du support d'installation de Single Sign-On

Composant logiciel	Requis par	Emplacement
Service Pack 1 • vc90_vcredist_x86.exe • vc90_vcredist_x64.exe		
Microsoft Primary Interoperability Assemblies • vs90_piaredist.exe	Composant console Single Sign-On — lors de l'installation du composant console à partir d'une invite de commande sur un ordinateur Windows Vista, Windows Server 2008 ou Windows Server 2008 R2	Dossier Support du support d'installation de Single Sign-On
Configuration de sécurité renforcée d'Internet Explorer	Single Sign-On Plug-in — désactivez la configuration de sécurité renforcée d'Internet Explorer lorsque vous installez le plug-in sur un ordinateur Windows Server 2003, Windows Server 2008 ou Windows Server 2008 R2. Si elle est activée, le plug-in ne répond pas aux définitions d'application Web.	

Composant Single Sign-On	Environnement ou système d'exploitation Microsoft Windows pris en charge	Langues prises en charge	Configuration matérielle requise
Magasin central	• Active Directory • Partage de fichiers NTFS	• Anglais • Allemand • Français • Espagnol • Japonais	30 Ko d'espace disque par utilisateur
Composant Single Sign-On de la console AppCenter	• Microsoft Windows 7 Service Pack 1 — 32 bits et 64 bits • Microsoft Windows 7—32 bits et 64 bits • Microsoft Windows Vista Service Pack 2 (édition Professionnel, édition Intégrale, édition Entreprise) – 32 bits et 64 bits • Microsoft Windows Vista (édition Professionnel, édition Intégrale, édition Entreprise) – 32 bits et 64 bits • Windows XP Service Pack 3 — 32 bits	• Anglais • Allemand • Français • Espagnol • Japonais	• 64 Mo de mémoire vive • 60 Mo d'espace disque

Composant Single Sign-On	Environnement ou système d'exploitation Microsoft Windows pris en charge	Langues prises en charge	Configuration matérielle requise
	• Microsoft Windows XP Professionnel Service Pack 2, 32 bits • Microsoft Windows XP Professionnel, édition x64 – 64 bits • Windows Server 2008 R2 Service Pack 1 — 64 bits • Microsoft Windows Server 2008 R2 64 bits • Microsoft Windows Server 2008 (édition Standard, édition Enterprise, édition Datacenter) — 32 bits et 64 bits • Microsoft Windows Server 2003 R2 (édition Standard, édition Enterprise, édition Datacenter) — 32 bits et 64 bits • Microsoft Windows Server 2003 avec Service Pack 2 (édition Standard, édition Enterprise, édition Datacenter) — 32 bits et 64 bits		
Plug-in	• Microsoft Windows 7 Service Pack 1 — 32 bits et 64 bits • Microsoft Windows 7—32 bits et 64 bits • Microsoft Windows Vista Service Pack 2 (édition Professionnel, édition Intégrale, édition Entreprise) – 32 bits et 64 bits • Microsoft Windows Vista (édition Professionnel, édition Intégrale, édition Entreprise) – 32 bits et 64 bits • Windows XP Service Pack 3 — 32 bits • Microsoft Windows XP Professionnel Service Pack 2, 32 bits • Microsoft Windows XP Professionnel, édition x64 – 64 bits • Microsoft Windows XP Embedded • Windows Server 2008 R2 Service Pack 1 — 64 bits • Microsoft Windows Server 2008 R2 64 bits • Microsoft Windows Server 2008 (édition Standard, édition Enterprise, édition Datacenter) — 32 bits et 64 bits • Microsoft Windows Server 2003 R2 (édition Standard, édition Enterprise, édition Datacenter) — 32 bits et 64 bits • Microsoft Windows Server 2003 avec Service Pack 2 (édition Standard, édition Enterprise, édition Datacenter) — 32 bits et 64 bits	• Anglais • Allemand • Français • Espagnol • Japonais • Chinois simplifié	• 10 Mo de mémoire vive • 25 Mo d'espace disque (si les fonctionnalités optionnelles ne sont pas installées) • 35 Mo d'espace disque (si les fonctionnalités optionnelles sont installées)

Composant Single Sign-On	Environnement ou système d'exploitation Microsoft Windows pris en charge	Langues prises en charge	Configuration matérielle requise
Service	• Windows Server 2008 R2 Service Pack 1 — 64 bits • Microsoft Windows Server 2008 R2 64 bits • Microsoft Windows Server 2008 (édition Standard, édition Entreprise, édition Datacenter) — 32 bits • Microsoft Windows Server 2003 R2 (édition Standard, édition Entreprise, édition Datacenter) — 32 bits • Microsoft Windows Server 2003 avec Service Pack 2 (édition Standard, édition Enteprise, édition Datacenter) — 32 bits	• Anglais • Allemand • Français • Espagnol • Japonais	• 128 Mo de mémoire vive • 30 Mo d'espace disque
Outil de définition d'application	Identique au plug-in	• Anglais • Allemand • Français • Espagnol • Japonais	Identique au plug-in

Remarque : Single Sign-On n'est pas pris en charge sur Microsoft Windows XP Édition Familiale.
Le Bureau dynamique est uniquement pris en charge sur les systèmes d'exploitation suivants :

- Microsoft Windows XP Professionnel Service Pack 2, 32 bits
- Microsoft Windows XP Embedded

Il n'est pas pris en charge par les systèmes d'exploitation 64 bits ou tout système d'exploitation serveur.

Installez le serveur de licences et ajoutez les licences avant d'installer Single Sign-On.

Avant d'exécuter cette version, assurez-vous que la dernière version du serveur de licences est installée. Si vous exécutez une version antérieure du serveur de licences, vous devez le mettre à niveau.
Important : les instances de Single Sign-On Plug-in installées localement ne nécessitent pas de licence distincte pour les utilisateurs qui ont accès à des applications hébergées dans un environnement Citrix XenApp, édition Platinum.

Mode déconnecté

Si certains de vos utilisateurs sont amenés à être déconnectés du serveur de licences pour des périodes étendues (par exemple, utilisateurs itinérants travaillant sur des ordinateurs portables), vous devez spécifier une durée de mode déconnecté pour ces derniers. Cette durée est définie dans le cadre des réglages de licence de la configuration utilisateur de l'utilisateur. Elle détermine deux aspects du cycle de vie des licences :

- La durée pendant laquelle l'utilisateur peut être déconnecté du serveur de licences sans entrer dans la période de grâce de la licence. Au terme de la durée du mode déconnecté, les utilisateurs employant la configuration utilisateur associée entrent dans la période de grâce, qui dure 30 jours.
- La durée s'écoulant avant qu'une licence extraite, actuellement utilisée en mode déconnecté, soit réintégrée au pool des licences disponibles sur le serveur de licences, que le produit soit reconnecté ou non à ce dernier. Si une licence est extraite et que le mode déconnecté associé à celle-ci expire avant que la licence ait été réintégrée, le serveur de licences la réintègre automatiquement afin qu'elle soit à nouveau disponible. Par exemple, si un ordinateur portable exécutant Single Sign-On est perdu et n'est jamais reconnecté au réseau de votre entreprise, le serveur de licences réintègre

automatiquement la licence au terme de la durée du mode déconnecté.

En d'autres termes, lorsque vous définissez le mode déconnecté, vous spécifiez le temps devant s'écouler avant la réintégration de la licence au pool de licences disponibles.

Pensez à définir de longues durées de mode déconnecté pour les utilisateurs ne se connectant pas régulièrement au réseau de votre entreprise, comme le personnel commercial travaillant à distance. Cependant, n'oubliez pas qu'il n'est pas possible de récupérer de licences extraites pendant cette durée, même si ces dernières sont installées sur du matériel perdu ou dégradé.

Types de licences mixtes

Selon votre environnement Single Sign-On et les besoins de votre entreprise, il est possible que vous utilisiez des licences Single Sign-On autonomes achetées préalablement. Par exemple, vous pouvez créer des configurations utilisateur basées sur le modèle de licence Utilisateurs désignés pour des utilisateurs itinérants employant Single Sign-On Plug-in via un ordinateur de bureau et un ordinateur portable. Vous pouvez également créer des configurations utilisateur basées sur le modèle de licence Utilisateurs simultanés pour les utilisateurs du Bureau dynamique.

Dans certains cas, toutes vos licences Utilisateurs désignés peuvent être utilisées, ce qui empêche certains utilisateurs d'accéder à Single Sign-On. Dans ce cas, vous pouvez utiliser les licences Utilisateurs simultanés disponibles dans votre configuration utilisateur pour un usage en mode déconnecté.

Planifier

Oct 21, 2015

Vous devez planifier votre environnement avant d'installer Single Sign-On. Il convient donc de déterminer le type de magasin central à utiliser, les applications activées pour Single Sign-On dans votre entreprise, les fonctionnalités Single Sign-On à utiliser, et d'établir des stratégies de mot de passe.

Un environnement Single Sign-On peut inclure ce qui suit :

- dossiers réseau partagés ou Active Directory contenant le magasin central ;
- un ou plusieurs ordinateurs exécutant le composant Single Sign-On de Citrix AppCenter ;
- ordinateurs d'utilisateurs exécutant Single Sign-On Plug-in ;
- serveur dédié hébergeant le service Single Sign-On, avec un ou plusieurs modules de fonctionnalités installés ;
- environnement Citrix XenApp hébergeant Single Sign-On Plug-in ;
- dispositifs d'authentification tels que des cartes à puces ;
- fonctionnalités de Single Sign-On telles que le Bureau dynamique et la gestion des clés.

Type de magasin central

Oct 21, 2015

Single Sign-On utilise un référentiel appelé magasin central pour le stockage et la récupération d'informations sur vos utilisateurs et votre environnement. Single Sign-On s'appuie sur les données du magasin central pour exécuter toutes les fonctions d'authentification par défaut et celles que vous configurez. vous pouvez créer un magasin central de façon automatique lors du processus d'installation de Single Sign-On ou manuellement à l'aide des utilitaires de configuration de magasin central.

Le magasin central contient des données utilisateur et des données d'administration.

- Les données utilisateur du magasin central comprennent des informations d'identification secondaires des utilisateurs, des questions/réponses de sécurité, des données liées au service (par exemple, données habilitées, données de l'authentification avec questions, enregistrement de la récupération de clé, etc.) et des données utilisateur de registre Windows associées à Single Sign-On.
- Les données administratives du magasin central comprennent des définitions d'application, des stratégies de mot de passe, des questions de sécurité et autres réglages effectués par le biais de la console pour les fonctionnalités et composants de Single Sign-On.

Plus concrètement, le magasin central permet au plug-in exécuté sur un l'ordinateur d'un utilisateur ou sur un serveur Citrix XenApp de communiquer avec le magasin central et les services afin de fournir les informations d'identification aux applications auquel l'utilisateur a accès.

Le plug-in gère un magasin local sur l'ordinateur de l'utilisateur. Ce magasin local contient uniquement les informations d'identification secondaires de l'utilisateur, les données de récupération de clé et les questions/réponses de sécurité (le cas échéant). Il effectue une synchronisation avec le magasin central pour permettre aux utilisateurs de se déplacer dans l'entreprise tout en ayant en permanence accès aux informations d'identification enregistrées.

Les types de magasins centraux suivants sont disponibles.

- Active Directory
  Le magasin central utilise l'environnement et les objets Active Directory pour stocker et mettre à jour les données de Single Sign-On.

- Point de partage réseau NTFS
  Le magasin central utilise un partage de fichiers réseau Windows pour stocker les données de Single Sign-On.

Le cas échéant, vous pouvez effectuer la migration d'utilisateurs d'un type de magasin central à un autre.

En choisissant un magasin central de type Active Directory, vous pouvez tirer parti de vos structures d'authentification utilisateur et d'administration d'objets Active Directory existantes. Par exemple, vous pouvez appliquer des paramètres utilisateur à tout niveau dans un domaine (domaine, unité organisationnelle, groupe ou utilisateur).

Deux nouvelles classes et deux attributs ont été ajoutés au schéma Active Directory pour la création d'un magasin central Active Directory :

Class	Description
citrix-SSOConfig	Décrit l'objet contenant les données correspondant aux réglages du plug-in, à l'état de

Class	Description
	synchronisation, ainsi que les définitions d'application et le comportement des utilisateurs à la première utilisation du plug-in. Cette classe inclut les attributs suivants :citrix-SSOConfigData - contient les données actuelles et citrix-SSOConfigType - indique le type de données
citrix-SSOSecret	Décrit l'objet de données secrètes utilisé pour authentifier un utilisateur Single Sign-On. Cette classe inclut l'attribut suivant : citrix-SSOSecretData - contient des informations d'identification cryptées pour une application et les données du module de réinitialisation de mot de passe des fonctions autonomes du compte

Remarque : pour plus d'informations sur ces classes et attributs, veuillez consulter le fichier CitrixMPMSchema.xml, dans le dossier \Tools du support d'installation.
En règle générale, nous vous recommandons de choisir Active Directory comme type de magasin central dans les cas suivants :

- Vous avez la possibilité d'étendre votre schéma Active Directory sans affecter votre entreprise.
- Vous avez déjà mis en place des procédures de sauvegarde et de restauration Active Directory conformes aux recommandations de Microsoft (bien que cela ne soit pas obligatoire).
- Vous préférez que les données de votre magasin central bénéficient du haut niveau de disponibilité que confère Active Directory.

Avantages d'un magasin central Active Directory

L'utilisation d'un magasin central Active Directory présente les avantages suivants :

- Étant donné qu'Active Directory intègre des capacités de récupération et de redondance des données en cas de panne, des mesures supplémentaires de restauration d'urgence ne sont pas nécessaires.
- La réplication Active Directory contribue à répartir les données administratives et utilisateur du magasin central dans votre entreprise.
- L'utilisation d'un magasin central Active Directory ne nécessite aucun matériel supplémentaire.

Considérations sur le magasin central Active Directory

Tenez compte de ce qui suit avant d'utiliser un magasin central Active Directory :

- L'utilisation d'un magasin central Active Directory implique d'étendre votre schéma ; cette opération doit être planifiée et mise en œuvre avec précaution. L'extension du schéma affecte l'ensemble de la forêt.
- Il est conseillé d'étendre le schéma et de créer votre magasin central Active Directory en dehors des heures de bureau. Le temps de latence du cycle de réplication d'Active Directory influe sur la vitesse de copie de ces changements sur tous les contrôleurs de domaine de la forêt.
- Dans les grandes entreprises, la réplication intersite des données de magasin central au moyen de réseaux étendus (WAN) nécessite de configurer la réplication correctement afin de limiter le temps de latence. Notez que la réplication intrasite, en revanche, génère en principe un temps de latence moins élevé.

En choisissant un magasin central de type point de partage réseau NTFS, vous pouvez tirer parti de vos structures d'authentification utilisateur et arborescence Active Directory existantes sans avoir à étendre le schéma Active Directory. Par exemple, vous pouvez appliquer des paramètres utilisateur à tout niveau dans un domaine (domaine, unité organisationnelle, groupe ou utilisateur).

Important : dans ce cas, utilisez un partage caché pour le magasin central.
Single Sign-On crée un dossier partagé nommé CITRIXSYNC$ incluant deux sous-dossiers appelés People et CentralStoreRoot.

Le dossier People contient un sous-dossier par utilisateur et inclut les propriétés de droits d'accès en lecture et en écriture adéquates pour l'utilisateur. Le dossier CentralStoreRoot contient des données administratives.

Avantages d'un point de partage réseau NTFS

L'utilisation d'un partage réseau NTFS présente les avantages suivants :

- Vous pouvez émuler l'aspect et la commodité d'un magasin central Active Directory sans avoir à étendre votre schéma Active Directory, tout en tirant parti de votre hiérarchie ou de vos groupes Active Directory existants.
  Remarque : l'association de configurations utilisateur à des groupes n'est prise en charge que dans des domaines Active Directory utilisant l'authentification Active Directory.
- Les données utilisateur sont toujours à jour, étant donné qu'elles sont stockées dans un emplacement central. Les temps de latence associés à Active Directory sont également éliminés.
- Pour accroître le niveau de disponibilité, vous pouvez mettre en place un dispositif d'équilibrage de la charge de vos partages sur plusieurs ordinateurs pouvant chacun héberger un partage réseau NTFS.
- Le point de partage réseau NTFS permet de réduire la charge de travail associée aux tâches d'authentification de votre environnement Active Directory.
- Single Sign-On vous permet de migrer votre magasin central de type dossier partagé NTFS vers un magasin central de type Active Directory si vous décidez d'en mettre un en œuvre ultérieurement.

Considérations sur le point de partage réseau NTFS

Tenez compte de ce qui suit avant d'utiliser un partage réseau NTFS :

- L'hébergement du magasin central peut nécessiter du matériel supplémentaire.
- Vous devez sauvegarder les fichiers et dossiers du magasin central (y compris les autorisations associées) de façon régulière. Veillez également à gérer et mettre en place des plans de restauration d'urgence permettant la réplication des fichiers et dossiers pour la récupération du site.
- La topologie réseau de votre entreprise peut nécessiter que les utilisateurs (et Single Sign-On Plug-in) transfèrent les données utilisateur via une ou plusieurs liaisons WAN. Dans ce cas, il est judicieux de mettre en œuvre la technologie Système de fichiers distribués (DFS) intégrée à Microsoft Windows Server 2003 et 2008. Cette dernière est décrite en détail sur le site Web de Microsoft, à l'adresse http://support.microsoft.com.

Les administrateurs peuvent créer plusieurs magasins centraux dans des entreprises contenant plusieurs domaines. Il est en outre possible d'utiliser plusieurs types de magasins centraux dans ce type d'environnement. Par exemple, vous pouvez associer des configurations utilisateur avec un magasin central de type point de partage réseau NTFS dans un domaine et avec un magasin central de type Active Directory dans un autre domaine.

Étant donné que les sociétés gèrent parfois plusieurs domaines Windows, les utilisateurs peuvent alors disposer de plusieurs comptes Windows. Single Sign-On offre une fonction appelée Association de comptes. Celle-ci permet à un utilisateur d'ouvrir une session sur n'importe quelle application à partir d'un ou plusieurs comptes Windows. Dans la mesure où Single Sign-On lie généralement les informations d'identification d'utilisateur à un seul compte, ces informations ne sont pas automatiquement synchronisées entre les différents comptes que peut posséder un utilisateur.

Cependant, les administrateurs peuvent configurer la fonction Association de comptes pour synchroniser les informations d'identification de l'utilisateur à l'aide du module de synchronisation des informations d'identification. Les utilisateurs bénéficiant de la fonction Association de comptes peuvent accéder à toutes les applications à partir de n'importe lequel de leurs comptes dans leur environnement Single Sign-On. Lors de la modification, de l'ajout ou de la suppression d'informations d'identification dans un compte, elles sont automatiquement synchronisées avec chacun des comptes associés à l'utilisateur.

Sans la fonction Association de comptes, les utilisateurs possédant plusieurs comptes Windows doivent modifier manuellement leurs informations de connexion séparément dans chaque compte Windows.

Pour permettre aux utilisateurs de synchroniser les informations d'identification à l'aide de la fonction Association de comptes, donnez-leur accès à AccAssoc.exe en tant qu'application publiée.

- L'association de comptes permet d'accroître la productivité et de réduire le nombre de sollicitations du service d'assistance en synchronisant les informations d'identification des utilisateurs en vue de limiter les opérations de maintenance ou les échecs liés aux ouvertures de sessions.
- La synchronisation de comptes est possible sur différents types de magasins centraux. En d'autres termes, un compte utilisateur configuré pour utiliser Active Directory comme type de magasin central peut être synchronisé avec un compte utilisateur associé configuré pour utiliser un point de partage réseau NTFS.
- La synchronisation de comptes est également possible sur différentes associations de configurations utilisateur. Par exemple, une configuration utilisateur peut être associée à une hiérarchie Active Directory (unité organisationnelle ou utilisateur) dans un domaine et à un groupe Active Directory dans un autre domaine.
- La synchronisation de comptes est aussi possible sur différentes associations de configurations utilisateur au sein du même domaine et au sein du même magasin central.
- Il n'est pas nécessaire d'établir de relations de confiance entre les contrôleurs de domaine pour utiliser la fonction Association de comptes.

Tenez compte des éléments suivants pour la configuration de l'association de comptes.

- L'association de comptes n'est pas compatible avec les cartes à puces lorsque celles-ci sont utilisées comme mécanisme d'authentification principale pour ouvrir une session sous Windows.
  Remarque : la configuration utilisateur de chaque domaine peut inclure des stratégies de mot de passe différentes susceptibles d'empêcher l'accès à une ressource. Cela étant, l'association de comptes ne synchronise que les informations d'identification et non les stratégies des configurations utilisateur. Penchez-vous sur le mode d'élaboration des stratégies de mot de passe utilisées dans votre entreprise.
- Chaque compte de domaine associé doit utiliser Single Sign-On.
- Le nom des définitions d'application doit être le même dans chaque configuration utilisateur pour que la fonction Association de comptes puisse synchroniser les informations d'identification.
- Les informations d'identification sont partagées uniquement pour les applications spécifiées dans les définitions d'application créées par l'administrateur de Single Sign-On.
- Le module de synchronisation des informations d'identification, intégré au service Single Sign-On, est un service Web disponible via une connexion HTTP sécurisée. Il est donc accessible à partir de tous les ordinateurs de votre entreprise utilisant l'association de comptes.

Stratégies de mot de passe

Oct 21, 2015

Les stratégies de mot de passe sont des règles contrôlant la manière dont les mots de passe sont créés, soumis et gérés. L'installation de Single Sign-On comprend deux stratégies de mot de passe standard intitulées Default et Domain, qu'il n'est pas possible de supprimer. Vous pouvez copier et modifier ces stratégies pour les adapter aux stratégies et réglementations de votre entreprise.

Single Sign-On applique la stratégie par défaut aux applications protégées par mot de passe utilisées dans votre entreprise (sauf celles nécessitant des informations d'identification de domaine). Cette stratégie est appliquée à toute application non définie par un administrateur (à l'aide de la fonction de définition d'application de la Console) ou non intégrée dans un groupe d'applications.

Lorsqu'un utilisateur ajoute ses informations d'identification à la fenêtre Gérer les mots de passe (anciennement Gestionnaire d'informations d'identification) pour une application non associée à une définition d'application, Single Sign-On applique la stratégie par défaut pour gérer cette application.

En règle générale, un administrateur crée un groupe d'applications et sélectionne la stratégie de domaine à appliquer aux applications de ce groupe. Single Sign-On applique ensuite la stratégie de domaine aux applications dont l'accès est conditionné à l'entrée des informations d'identification de domaine de l'utilisateur. La stratégie de domaine peut être modifiée ou copiée pour refléter les stratégies de domaine NT ou Active Directory de votre entreprise liées aux comptes utilisateur.

Si vous souhaitez étendre le groupe de partage de mot de passe à un domaine, vous devez lui appliquer la stratégie Domain. un groupe d'applications est un ensemble d'applications définies associées à une ou plusieurs configurations utilisateur comprenant la stratégie de gestion des applications.

Vous pouvez créer des stratégies de mot de passe selon vos besoins : vous pouvez appliquer une stratégie pour votre groupe de partage de domaine, créer des stratégies individuelles à appliquer aux groupes individuels d'applications pour les sécuriser encore davantage, etc.

Lorsque vous créez une stratégie de mot de passe personnalisée ou que vous modifiez des stratégies existantes, assurez-vous que les exigences de votre entreprise ne divergent pas de celles de l'application. Par exemple, si vous créez une stratégie qui ne correspond pas au moins aux besoins d'une application, vos utilisateurs ne pourront pas s'authentifier auprès d'elle.

Les stratégies de mot de passe peuvent généralement imposer des restrictions semblables à celles énumérées ci-après.

- Nombre minimum et maximum de caractères pour un mot de passe
- Règle d'utilisation des caractères alphabétiques et numériques
- Nombre de répétitions d'un caractère autorisées
- Règle d'utilisation des caractères ou des caractères spéciaux (inclusion ou exclusion)
- Affichage des mots de passe stockés par les utilisateurs
- Nombre de tentatives de saisie du mot de passe par les utilisateurs

- Expiration de mot de passe
- Historique de mot de passe et exceptions

Tenez compte de ce qui suit avant d'établir des stratégies de mot de passe :

- Tenez compte du confort des utilisateurs lors de l'élaboration de vos stratégies de sécurité. Des mots de passe trop restrictifs risquent d'être difficiles à créer, à mettre en place ou à mémoriser pour les utilisateurs.
- Étant donné que Single Sign-On est sécurisé par nature, la stratégie de mot de passe par défaut définit le niveau minimum de sécurité recommandé par Citrix pour la sécurisation de la plupart des applications à authentification unique. Vous pouvez modifier ces paramètres selon les stratégies et réglementations de votre entreprise.
- Dans la mesure où le service Single Sign-On applique la stratégie de mot de passe Default aux applications ajoutées par les utilisateurs, assurez-vous de configurer cette stratégie de façon à être la plus large possible, afin d'accepter les mots de passe de toutes les applications pour lesquelles vous autorisez les utilisateurs à stocker des mots de passe.
- Lorsque les utilisateurs modifient leurs mots de passe, Single Sign-On peut être configuré, au moyen d'un paramètre de configuration utilisateur, pour comparer leur ancien mot de passe avec le nouveau. Cela empêche l'utilisation répétée d'un même mot de passe pour une application.
- Dans certains cas, les utilisateurs disposent d'un seul mot de passe pour plusieurs applications (dans une suite logicielle, par exemple). Cette situation est appelée partage de mot de passe : les applications utilisent la même autorité d'authentification.
  Même si les informations d'identification (nom d'utilisateur et champs personnalisés) sont différentes pour ces applications, le mot de passe reste identique. Dans ce cas, créez un groupe d'applications qui est également un groupe de partage de mot de passe pour garantir que le plug-in gère le mot de passe pour toutes les applications du groupe comme s'il s'agissait d'une seule. Lors d'une modification du mot de passe pour l'une d'entre elles, le plug-in s'assure que cette modification est répercutée pour toutes les applications du groupe.

- Les groupes de partage de mot de passe de domaine ont la particularité d'utiliser le mot de passe de domaine de l'utilisateur en tant que mot de passe principal pour le groupe d'applications. Lors d'une modification du mot de passe de domaine, le plug-in s'assure que cette modification est répercutée pour toutes les applications du groupe. Cependant, seul le mot de passe de domaine peut être modifié. Les utilisateurs ne peuvent pas modifier le mot de passe pour les autres applications du groupe, à moins que l'administrateur ne retire l'application du groupe de partage de mot de passe de domaine.

Définitions d'application

Oct 21, 2015

En tant qu'administrateur de Single Sign-On, vous pouvez créer une définition d'application ou modifier un modèle de définition d'application pour chaque application que Single Sign-On doit gérer pour vos utilisateurs. Pour créer des définitions d'application, utilisez la Console ou l'Outil de définition d'application autonome, qui peut être installé sur des stations de travail n'exécutant pas la Console.

Vous pouvez également permettre aux utilisateurs d'ajouter leurs informations d'identification dans Single Sign-On pour toutes leurs applications côté client qu'il détecte, selon les paramètres définis dans les configurations utilisateur. Le plug-in peut détecter et répondre aux modifications d'informations d'identification de la plupart des applications, notamment celles appartenant aux catégories suivantes :

Type d'application	Description
Windows	Applications Windows 32 bits (y compris les applications Java) telles que Microsoft Outlook, Lotus Notes, SAP ou toute application Windows protégée par mot de passe
Web	Applications Web (y compris les applets Java et SAP), accessibles via Microsoft Internet Explorer
Émulateur de terminal	Applications accessibles à partir d'un émulateur de terminal compatible HLLAPI (Single Sign-On ne prend pas en charge les logiciels d'émulation de terminal 64 bits.)

Le plug-in répond selon les définitions d'application créées de toute part ou copiées à partir de modèles existants. Une définition d'application :

- active le plug-in pour qu'il reconnaisse et réponde aux applications et aux formulaires utilisés par ces dernières pour traiter les informations d'identification des utilisateurs ;
- est composée d'un ensemble d'identificateurs établissant les paramètres requis pour effectuer la reconnaissance et la réponse.

Dans chaque définition, vous créez des formulaires d'ouverture de session et de mot de passe requis par l'application pour autoriser l'accès. L'assistant de définition d'application vous aide à créer une définition si vous ouvrez l'application ; il détecte les formulaires et champs de la plupart des applications à l'aide des fonctions de correspondance de fenêtre de Single Sign-On.

Conseil : Single Sign-On inclut des modèles de définition d'application par défaut pour diverses applications ou fonctionnalités applicatives Citrix. Pour obtenir d'autres modèles, consultez le site Web de l'assistance Citrix.

Cartes à puce

Oct 21, 2015

Citrix a testé des cartes à puce conformes à la norme ISO 7816 relative aux cartes avec contacts électriques (carte contact) qui communiquent avec un système informatique via un périphérique appelé lecteur de cartes à puce. Vous pouvez connecter le lecteur à l'ordinateur hôte via le port série, le port USB ou le port PC Card (PCMCIA) de ce dernier.

Citrix permet l'utilisation de cartes à puce cryptographiques PC/SC. Ces cartes prennent en charge des opérations cryptographiques telles que le cryptage et les signatures numériques. Les cartes cryptographiques permettent de sécuriser le stockage des clés privées comme celles utilisées dans les systèmes de sécurité à infrastructure à clé publique (ICP, aussi appelée PKI : Public Key Infrastructure).

Ces cartes assurent les fonctions cryptographiques sur la carte à puce proprement dite, ce qui signifie que la clé privée ne quitte jamais la carte. En outre, vous pouvez assurer une sécurité accrue en utilisant une authentification à deux facteurs : le numéro de la carte et le code secret de l'utilisateur. La combinaison de ces facteurs garantit que l'utilisateur est bien le détenteur autorisé de la carte.

Pour connaître le détail des configurations requises pour la mise en place d'un système recourant à des cartes à puce, veuillez contacter votre intégrateur ou distributeur de cartes à puce. Les composants suivants sont nécessaires sur le serveur ou le client :

- logiciel PC/SC ;
- logiciel CSP (Cryptographic Service Provider : fournisseur de services cryptographiques) ;
- pilotes logiciels du lecteur de cartes à puce.

Vos systèmes d'exploitation Windows clients et serveurs vous ont peut-être été fournis avec des logiciels PC/SC, des logiciels CSP ou des pilotes de lecteur de cartes à puce. Pour savoir si ces composants logiciels sont pris en charge ou s'ils doivent être remplacés par d'autres logiciels spécifiques, veuillez contacter votre distributeur de cartes à puce.

pour utiliser les cartes à puce dans un environnement Windows 2008 ou Windows Vista, vous devez créer ou mettre à niveau votre magasin central avec une console Single Sign-On 4.5 (anciennement Password Manager) ou ultérieure et API de protection des données de Microsoft (nécessite des profils itinérants) doit être sélectionné dans vos configurations utilisateur.

Vérification d'identité

Oct 21, 2015

Si les paramètres de configuration utilisateur l'exigent, les utilisateurs peuvent être amenés à vérifier leur identité dans les cas suivants.

- Les utilisateurs modifient leurs types d'authentification ; par exemple, un utilisateur passe d'une authentification à carte à puce à une authentification par mot de passe. Vous pouvez créer une configuration utilisateur qui n'exige de vérification initiale qu'en cas de changement du type d'authentification.
- Modification du mot de passe principal par un administrateur.
- Réinitialisation du mot de passe principal par un utilisateur à l'aide des fonctions autonomes de compte.
- Déverrouillage du compte de domaine à l'aide des fonctions autonomes de compte.
- Modification du mot de passe principal par un utilisateur sur une machine où le plug-in n'est pas installé, puis ouverture de session sur une machine où il est installé.

Single Sign-On peut être configuré pour vérifier l'identité de l'utilisateur afin de garantir que l'utilisateur est autorisé à utiliser Single Sign-On. Vous pouvez choisir l'une des deux méthodes de vérification suivantes.

Méthode	Description
Mot de passe précédent	Dans ce cas, les utilisateurs doivent vérifier leur identité en entrant leur mot de passe principal précédent.
Questions de sécurité (méthode également appelée authentification avec questions)	Dans ce cas, vous créez un questionnaire contenant autant de questions et de groupes de questions que vous souhaitez proposer aux utilisateurs. Vous pouvez utiliser les questions par défaut fournies par Single Sign-On ou créer vos propres questions.

Attention : lorsque le mot de passe précédent est la seule méthode de vérification d'identité disponible pour les utilisateurs, ceux qui l'oublient ne peuvent plus accéder au système. Un administrateur doit alors utiliser la tâche Réinitialiser les données utilisateur du composant Single Sign-On pour permettre aux utilisateurs de s'enregistrer à nouveau. Ce dernier devra peut-être également réinitialiser les mots de passe dans les applications de l'utilisateur.

Single Sign-On vous permet d'utiliser l'authentification avec questions pour vérifier l'identité des utilisateurs. Single Sign-On inclut quatre questions (en anglais, français, allemand, japonais, chinois simplifié et espagnol) utilisables avec cette méthode.

L'authentification avec questions s'utilise comme suit :

- lors de l'enregistrement des questions de sécurité de l'utilisateur au cours de son premier enregistrement sur le plug-in ;
- après l'enregistrement, si vous avez configuré les fonctions autonomes de compte pour permettre aux utilisateurs de modifier leurs informations d'identification principales ou de déverrouiller leur compte.

Lorsque les utilisateurs modifient leur mot de passe principal, vous pouvez confirmer leur identité en les invitant à répondre aux questions de sécurité dans le cadre d'un questionnaire que vous créez. Ce questionnaire apparaît à la première ouverture du plug-in. Les utilisateurs répondent à un nombre minimum de questions, puis peuvent être invités à entrer de nouveau ces informations lors d'événements de modification de mot de passe spécifiques.

Pour permettre aux utilisateurs de réenregistrer leurs réponses aux questions de sécurité sans y être invités, donnez-leur

accès à QBAEnroll.exe en tant qu'application publiée.

Si vous décidez de ne pas configurer les questions de sécurité, les utilisateurs sont invités à entrer leur mot de passe principal précédent à la première ouverture de session et lorsqu'ils changent leur mot de passe principal. Vous pouvez aussi permettre aux utilisateurs de choisir la méthode qu'ils préfèrent utiliser pour l'authentification (mots de passe précédents ou questions de sécurité).

Important : la gestion automatique des clés n'est pas aussi sûre que d'autre mécanisme de récupération de clé tels que les questions de sécurité et le mot de passe précédent.
Vous pouvez configurer Single Sign-On pour ne pas effectuer de vérification d'identité et pour récupérer automatiquement les informations d'identification (à savoir, les clés de cryptage associées aux données utilisateur) en utilisant le module de gestion des clés du service Single Sign-On.

La procédure de base pour utiliser la gestion automatique des clés est la suivante.

1. Installez le service Citrix Single Sign-On avec le module de gestion de clés.
2. Créez ou modifiez les configurations utilisateur et sélectionnez la méthode de récupération de clé permettant une gestion automatique des clés sans vérification d'identité. Cette option est incluse dans la propriété de protection secondaire des données de la configuration utilisateur.

Planification de vos configurations utilisateur Single Sign-On Plug-in

Oct 21, 2015

Une configuration utilisateur est un ensemble unique de paramètres, stratégies de mot de passe et applications appliqués aux utilisateurs associés à une hiérarchie Active Directory (unité organisationnelle ou utilisateur individuel) ou à un groupe Active Directory (hormis les groupes de distribution et les groupes locaux de domaine en mode Active Directory mixte, qui ne sont pas pris en charge). Une configuration utilisateur vous permet de contrôler le comportement et l'aspect du plug-in au niveau des utilisateurs.

Ces configurations définissent les informations utilisateurs, les définitions d'application, les stratégies de mot de passe et les méthodes de vérification d'identité. Vous devez également spécifier des informations de licence (serveur de licences et type de licence) dans chaque configuration utilisateur. C'est pourquoi les utilisateurs ne peuvent pas utiliser le plug-in tant que vous n'avez pas configuré les paramètres de leur configuration utilisateur.

Avant de créer vos configurations utilisateur, assurez-vous que vous avez déjà créé ou défini les éléments suivants :

- Magasin central
- Modules de service optionnels
- Définitions d'application
- Stratégies de mot de passe
- Questions de sécurité (facultatif)

Les configurations utilisateur comprennent les éléments suivants :

- Utilisateurs associés à une hiérarchie de domaine Active Directory (unité organisationnelle ou utilisateur individuel) ou à un groupe Active Directory.
- Méthodes de protection des données.
- Définitions d'application créées, que vous pouvez combiner dans un groupe d'applications lors de la création d'une configuration utilisateur.
- Stratégies de mot de passe associées à des groupes d'applications. (Lors de la création d'une configuration utilisateur, vous pouvez créer un ou plusieurs groupes d'applications à associer à une configuration utilisateur. Vous pouvez également ajouter un groupe d'applications à une configuration utilisateur après avoir créé la configuration utilisateur).
- Fonctions autonomes de compte (déverrouillage de compte et réinitialisation de mot de passe) et options de gestion de clés (utilisation des mots de passe précédents, questions de sécurité créées pour vos utilisateurs et gestion automatique des clés).
- Réglages des options telles que le Bureau dynamique, l'habilitation et la prise en charge d'applications.

L'association de configurations utilisateur à des groupes n'est prise en charge que dans des domaines Active Directory utilisant l'authentification Active Directory.

Tenez compte de ce qui suit lors de la planification de votre environnement utilisateur Single Sign-On :

- Si vous devez appliquer les mêmes paramètres de configuration utilisateur à un groupe différent d'utilisateurs, dupliquez la configuration utilisateur sur la Console et modifiez les réglages selon vos besoins.
- Le mode d'organisation de votre environnement Single Sign-On peut affecter le fonctionnement des configurations utilisateur. En d'autres termes, vous associez des configurations utilisateur de votre environnement Single Sign-On à une hiérarchie Active Directory (unité d'organisation ou utilisateurs) ou à un groupe Active Directory. Si vous utilisez les deux

(hiérarchie et groupe) et qu'un utilisateur se trouve dans les deux conteneurs, la configuration utilisateur associée à la hiérarchie a la priorité et sera celle utilisée. Ce schéma est appelé environnement mixte.

- Les informations de configuration utilisateur gérées dans le magasin central sont prioritaires par rapport à celles contenues dans le magasin local (à savoir, les données utilisateur stockées sur l'ordinateur d'un utilisateur). Les données utilisateur du magasin local sont principalement utilisées lorsque le magasin central n'est pas disponible ou qu'il est déconnecté.

Activation du partage de ressources ou d'une station de travail entre plusieurs utilisateurs (Bureau dynamique)

Oct 21, 2015

Le Bureau dynamique permet aux utilisateurs de partager leurs stations de travail de façon sûre et efficace. Avec le Bureau dynamique, Single Sign-On vous offre à la fois une rotation accélérée des utilisateurs et l'accès à l'authentification unique.

Toutefois, avant la mise en place de cette fonctionnalité, vous devez :

- créer des configurations utilisateur dédiées ;
- configurer un compte partagé de Bureau dynamique ;
- modifier les scripts qui définissent les applications à exécuter sur les machines en Bureau dynamique ainsi que leur comportement au démarrage et à l'arrêt.

Cette fonctionnalité n'est pas installée par défaut, vous pouvez la sélectionner pendant la phase initiale de l'installation du plug-in. Vous pouvez également l'ajouter lors d'une mise à niveau de vos déploiements.

Si vous déployez le Bureau dynamique dans un environnement dans lequel les utilisateurs se connectent à l'aide de cartes à puce et dans lequel votre source de clé de carte à puce est DPAPI avec profil, ne sélectionnez pas l'option Saisie du mot de passe précédent en tant que méthode de récupération de clé unique pour ces utilisateurs. Dans un tel environnement, les utilisateurs ne peuvent pas saisir le mot de passe précédent adéquat et ne peuvent donc définitivement plus accéder au système. Pour prévenir ce problème, sélectionnez l'option de gestion automatique des clés ou proposez une option d'authentification avec questions aux utilisateurs.

Ils peuvent s'authentifier rapidement à l'aide de leurs informations d'identification Windows ou d'une authentification renforcée avec carte à puce. En tant qu'administrateur, vous pouvez configurer le Bureau dynamique pour lancer des applications dans l'environnement Bureau dynamique afin que les utilisateurs n'aient pas à rechercher leurs applications et à ensuite patienter pendant leur chargement.

De même, vous pouvez configurer le Bureau dynamique de sorte que toutes les applications soient fermées correctement, laissant un environnement « propre » pour la prochaine session.

Lorsque le compte partagé effectue une ouverture de session, il place la machine en mode « rotation utilisateur rapide », ce qui entraîne l'affichage d'une boîte d'ouverture de session Windows standard. La session du compte partagé reste ouverte quelle que soit l'activité de l'utilisateur du Bureau partagé.

Lorsque les utilisateurs s'authentifient, ils n'ouvrent pas de session dans le Bureau dynamique de la façon habituelle. Le Bureau dynamique utilise leurs informations d'identification Windows pour démarrer une session Bureau dynamique. Les utilisateurs n'ouvrent pas véritablement de session, mais ils s'authentifient. Ainsi, les événements associés à l'ouverture de session, tels que l'application de la stratégie de groupe, l'initialisation des imprimantes, etc., et les délais qu'ils impliquent sont éliminés. Le Bureau dynamique offre une impression de permutation rapide des utilisateurs. Un utilisateur peut démarrer une session, effectuer des tâches liées à son poste et fermer la session afin que le prochain utilisateur puisse accéder au système et faire de même. Le passage d'un utilisateur à l'autre s'effectue de façon rapide et efficace.

Single Sign-On Plug-in est lancé lorsqu'une session du Bureau dynamique démarre. Une fois la session établie, le Bureau dynamique accède aux informations d'identification du compte Windows pour lancer les applications en utilisant l'interface shell standard. En général, ces applications clientes légères invitent les utilisateurs à entrer leurs informations d'identification, qui peuvent être fournies par le plug-in en fonction des paramètres associés à leur compte Windows.

Planification des fonctionnalités du service Single Sign-On

Oct 21, 2015

Le service Single Sign-On est un service Web qui utilise Secure Sockets Layers (SSL) pour crypter les données partagées par le service Single Sign-On, la console et le plug-in. Il utilise un serveur Web dédié pour héberger les fonctionnalités facultatives de Single Sign-On.

Installez le service Single Sign-On si vous envisagez de mettre en place un ou plusieurs des modules suivants :

- Module de gestion des clés
- Intégrité des données
- Habilitation
- Fonctions autonomes
- Synchronisation d'informations d'identification

Important : le serveur hébergeant le service Single Sign-On contient des informations utilisateur très sensibles. Citrix recommande d'utiliser un serveur dédié et de le placer dans un endroit protégé.

Ce module permet aux utilisateurs d'ouvrir une session sur le réseau et d'obtenir un accès immédiat aux applications gérées par Single Sign-On sans qu'il soit nécessaire de vérifier leur identité via l'authentification avec questions (également appelée gestion automatique des clés). Pour réduire le risque d'attaques de sécurité, la gestion automatique des clés utilise la scission de clé (division en deux d'une clé privée).

Toutefois, elle ne protège pas contre un accès par un utilisateur non autorisé ou par un administrateur empruntant l'identité d'un utilisateur car il n'existe aucun « secret de l'utilisateur » pour protéger le mot de passe réseau de celui-ci. Pour prévenir ce risque, mettez en place la gestion automatique des clés en combinaison avec les fonctions autonomes de compte et l'authentification avec questions.
Important : la politique de sécurité d'une organisation permet parfois aux administrateurs système d'avoir accès aux mots de passe des applications gérées par Single Sign-On. Consultez la politique de sécurité de votre société avant d'autoriser Single Sign-On à gérer les mots de passe dont les utilisateurs souhaitent maintenir le secret. La désélection des fonctions de gestion automatique des clés du paramètre Méthodes de protection des données de la configuration utilisateur peut également contribuer à empêcher les accès non autorisés.

Le module d'intégrité de données contient les fichiers de clé publique et privée utilisés pour signer les données. Il utilise un système de clé publique RSA pour garantir que le plug-in n'obtient les données de configuration que d'une source autorisée. le module d'intégrité des données ne distribue pas la clé privée.

Une fois les données signées par la Console, cette dernière envoie les données et la signature au magasin central. Le plug-in reçoit les données et la signature du magasin central pendant la synchronisation. Il contacte alors le service Single Sign-On pour obtenir une copie de la clé publique nécessaire à la vérification de la signature reçue du magasin central.

Installez ce module si vous souhaitez garantir que les données transmises entre les composants de Single Sign-On proviennent d'une source fiable et approuvée. Ce module facultatif est destiné aux utilisateurs disposant de réseaux non fiables.

Si le plug-in est configuré pour utiliser le module d'intégrité des données, il refuse toujours des données de configuration

pour lesquelles la vérification d'intégrité échoue. En cas d'échec, le plug-in journalise l'événement et affiche un message d'erreur invitant les utilisateurs à contacter leur administrateur. Le plug-in applique ensuite par défaut les configurations précédentes ou rétablit l'état déconnecté.

Si vous avez déjà mis en place une structure sécurisée pour protéger les données transmises, tel qu'IPsec (Internet Protocol Security) ou SMB (Server Message Block), il n'est pas nécessaire d'installer le module d'intégrité des données.

L'habilitation vous permet d'automatiser certains processus de gestion des informations d'identification. Vous pouvez :

- ajout, modification et suppression d'informations d'identification dans le magasin central ;
- réinitialisation d'informations d'identification ;
- suppression d'utilisateurs et de leurs informations d'identification d'application de Single Sign-On.

L'habilitation consiste à utiliser les informations de l'environnement pour créer un modèle permettant d'ajouter, de supprimer ou de modifier des informations d'identification dans le magasin central.

Vous pouvez configurer les fonctions autonomes de compte de Single Sign-On pour permettre à vos utilisateurs de réinitialiser leur mot de passe principal sans intervention de l'administrateur ou du personnel d'assistance technique. En fonction de vos besoins, vous pouvez mettre en œuvre l'une des fonctions autonomes de réinitialisation de mot de passe et de déverrouillage de compte (ou les deux) en toute sécurité dans votre environnement Single Sign-On.
Remarque : vous ne pouvez utiliser les fonctions autonomes de compte que dans un environnement Active Directory afin d'autoriser les utilisateurs à réinitialiser leur mot de passe principal ou à déverrouiller leur compte de domaine Windows.
Les fonctions autonomes de compte sont protégées par l'authentification avec questions, qui garantit l'autorisation des utilisateurs lorsqu'ils s'apprêtent à réinitialiser leur mot de passe ou à déverrouiller leur compte. Lorsque ces fonctions sont activées, les utilisateurs doivent suivre un processus d'inscription au cours duquel ils doivent répondre à des questions de sécurité que vous créez et sélectionnez. Ces questions de sécurité sont présentées aux utilisateurs lorsqu'ils doivent réinitialiser leur mot de passe ou déverrouiller leur compte. Après avoir répondu correctement, ils sont autorisés à réinitialiser leur mot de passe ou à déverrouiller leur compte.

La synchronisation d'informations d'identification (également appelée Association de comptes) permet à un utilisateur de se connecter à n'importe quelle application à l'aide d'un compte Windows ou plus. Dans la mesure où Single Sign-On lie généralement les informations d'identification d'utilisateur à un seul compte, ces informations ne sont pas automatiquement synchronisées entre les différents comptes que peut posséder un utilisateur. Toutefois, les administrateurs peuvent configurer la fonction Association de comptes de manière à synchroniser les informations d'identification des utilisateurs. Les utilisateurs bénéficiant de la fonction Association de comptes peuvent accéder à toutes les applications à partir de n'importe lequel de leurs comptes dans leur environnement Single Sign-On. Lors de la modification, de l'ajout ou de la suppression d'informations d'identification dans un compte, elles sont automatiquement synchronisées avec chacun des comptes associés à l'utilisateur.

Scénarios de déploiement de Single Sign-On Plug-in

Oct 21, 2015

Vous pouvez utiliser Single Sign-On dans des environnements comprenant des applications hébergées XenApp, des applications installées localement ou les deux.

Dans un déploiement XenApp, vous installez le logiciel Single Sign-on Plug-in sur chaque serveur de la batterie XenApp qui héberge des applications nécessitant l'authentification des informations d'identification. Les utilisateurs peuvent accéder à ces applications au moyen de connexions Citrix. Le plug-in sur le serveur détermine le type d'application (Windows, Web ou émulateur de terminal) et récupère les informations d'identification correspondantes à partir du magasin local d'informations d'identification du profil de l'utilisateur.

Vous pouvez également installer Single Sign-On Plug-in sur une machine utilisateur. Pour un déploiement XenApp, tenez compte des considérations décrites ci-dessous. Si les utilisateurs exécutent des applications qui sont installées localement sur leurs machines, Single Sign-On Plug-in doit être installé sur la machine utilisateur pour fournir les informations d'identification et l'accès aux applications locales.

Que Single Sign-On Plug-in soit installé ou non sur la machine utilisateur, les utilisateurs peuvent réenregistrer les réponses aux questions de sécurité sans y être invité, ou synchroniser les informations d'identification à l'aide de la fonction Association de comptes (vous pouvez leur donner accès à cette fonction en tant qu'application publiée après avoir installé le plug-in sur un serveur XenApp).

Single Sign-On peut être utilisé avec :

- Access Gateway édition Advanced (les applications sont disponibles à partir de XenApp via un navigateur Web)
- Fonctionnalités de Citrix XenApp :
  - Citrix Receiver pour Windows
  - Citrix Offline Plug-in
  - Interface Web

Dans un environnement XenApp, la décision d'installer ou de publier Single Sign-On Plug-in sur la machine utilisateur dépend de ce que vous voulez autoriser vos utilisateurs à effectuer. Quel que soit le scénario choisi, les informations d'identification sont envoyées aux applications publiées.

- Si vous n'installez pas Single Sign-On Plug-in sur la machine utilisateur, les utilisateurs peuvent :
  - enregistrer les réponses aux questions de sécurité lorsqu'ils y sont invités ;
  - stocker les informations d'identification automatiquement lorsqu'ils y sont invités par Single Sign-On ;
  - changer le mot de passe d'un programme ou site Web lorsqu'ils y sont invités par Single Sign-On ;
- Si vous publiez l'application Gérer les mots de passe (LogonManager.exe, installée dans le cadre de l'installation de Single Sign-On Plug-in), les utilisateurs peuvent :
  - enregistrer les réponses aux questions de sécurité lorsqu'ils y sont invités ;
  - stocker les informations d'identification automatiquement lorsqu'ils y sont invités par Single Sign-On ;
  - changer le mot de passe d'un programme ou site Web lorsqu'ils y sont invités par Single Sign-On ;
  - modifier, supprimer ou révéler les mots de passe stockés dans Single Sign-On ;
- Si vous installez Single Sign-On Plug-in sur la machine utilisateur, les utilisateurs peuvent réaliser toutes les tâches Single Sign-On disponibles :
  - enregistrer les réponses aux questions de sécurité lorsqu'ils y sont invités ;
  - stocker les informations d'identification automatiquement lorsqu'ils y sont invités par Single Sign-On ;

- changer le mot de passe d'un programme ou site Web lorsqu'ils y sont invités par Single Sign-On ;
- modifier, supprimer ou révéler les mots de passe stockés dans Single Sign-On ;
- envoyer les informations d'identification manuellement, lorsqu'ils n'y sont pas invités par Single Sign-On ;
- ajouter des mots de passe supplémentaires pour les programmes et sites Web déjà répertoriés dans Single Sign-On ;
- mettre en pause Single Sign-On, reprendre Single Sign-On, ou déterminer si Single Sign-On est mis en pause ;
- Utiliser les fonctions autonomes de compte

Planification d'authentification principale et de protection des informations d'identification multiples

Oct 21, 2015

Lors de la création ou de la modification d'une configuration utilisateur, vous pouvez sélectionner des méthodes de protection des informations d'identification selon les plans d'authentification en place dans votre entreprise.

Les pages de propriétés de configuration utilisateur ci-après vous permettent de régler le comportement de Single Sign-On Plug-in et la méthode de protection des informations d'identification utilisée lors de la mise en place par les utilisateurs d'une ou plusieurs méthodes d'authentification principale.

La page de propriétés de configuration utilisateur Méthodes de protection des données vous permet de sélectionner des méthodes de protection des données d'authentification principale simples ou multiples. En outre, vous pouvez également réglementer l'accès des administrateurs aux informations d'identification des utilisateurs afin de les empêcher d'emprunter l'identité d'un utilisateur et d'accéder sans autorisation aux informations de l'utilisateur.

Pour un meilleur niveau de sécurité en cas de modification de l'authentification principale par les utilisateurs (par exemple, modification de mot de passe de domaine ou remplacement de carte à puce), la page de propriétés de configuration utilisateur Protection secondaire des données vous permet d'obliger les utilisateurs à s'authentifier de nouveau et à vérifier leur identité avant de déverrouiller leurs informations d'identification d'application.

Les deux questions à se poser lors du choix des options sur ces deux pages de propriétés de configuration utilisateur sont les suivantes.

- Quels types d'authentification sont utilisés dans mon environnement pour les utilisateurs administrés dans cette configuration utilisateur ?
- Comment trouver un équilibre entre les besoins de sécurité de l'entreprise et le confort d'utilisation de l'ensemble des utilisateurs ?

Notez également que les choix suivants ne s'excluent pas mutuellement et que vous pouvez les combiner dans votre entreprise (on parle alors d'une authentification principale multiple). Votre choix repose sur l'équilibre entre vos besoins de sécurité et le confort des utilisateurs de votre entreprise.

Si vous souhaitez interdire l'accès des administrateurs aux informations d'identification des utilisateurs, Sélectionnez Oui pour l'option Devez-vous réglementer l'accès des administrateurs aux données utilisateurs ? . Les informations d'identification sont protégées contre toute tentative d'usurpation d'identité par des administrateurs en vue d'accéder aux informations des utilisateurs.

Oui est le réglage par défaut de la page Méthodes de protection des données. Avec cette configuration, l'administrateur de comptes ou autres ne peut pas accéder aux mots de passe ou aux données de l'utilisateur. Ce paramètre permet d'empêcher un administrateur de prendre l'identité d'un utilisateur. L'administrateur ne peut pas ouvrir de session sous le nom de l'utilisateur ni accéder aux données stockées dans le magasin d'informations d'identification local de l'utilisateur.

La valeur Oui désactive l'utilisation de l'option API de protection des données de Microsoft de cette page ainsi que l'option Aucune invite aux utilisateurs ; restauration automatique de la protection principale des données sur le réseau de la page Protection secondaire des données suivante. Les cartes à puce et les profils itinérants ne sont pas autorisés dans ce cas et les informations d'identification ne sont pas automatiquement restaurées en cas de changement de mot de passe sans authentification ni vérification.

Sélectionnez Non pour autoriser l'utilisation de l'ensemble des fonctions d'authentification multiple disponibles sur cette page et sur la page Protection secondaire des données (y compris la possibilité de restaurer les informations d'identification sans nouvelle authentification ni vérification d'identité).

La mise en place la plus simple correspond au réglage par défaut de la page Méthodes de protection des données : un environnement dont la sécurité repose uniquement sur le mot de passe. Ce réglage par défaut autorise vos utilisateurs à utiliser leur nom d'utilisateur et mot de passe tout en protégeant leurs informations d'identification contre tout accès non autorisé par des administrateurs.

Important : la sécurité procurée par ce choix dépend de la rigueur relative de votre stratégie de mot de passe de domaine. Plus les contraintes liées aux mots de passe sont fortes (et donc complexes), plus le niveau sécurité offert par ce choix est élevé.

Option	Description
Devez-vous réglementer l'accès des administrateurs aux données utilisateurs ?	Voir la section *— Usurpation d'identité* .
Données d'authentification des utilisateurs	Sélectionnée. Un secret utilisateur est utilisé pour accéder aux données utilisateur et ainsi protéger ces dernières. Dans ce cas, le secret utilisateur est un mot de passe. La sécurité du mot de passe peut être calculée à partir du mot de passe de domaine saisi par l'utilisateur ou d'un mot de passe ponctuel généré par des dispositifs à jetons, de proximité ou à reconnaissance biométrique.

Utilisez les options Certificat de carte à puce et Données d'authentification des utilisateurs si vous souhaitez combiner des cartes à puce avec certificats ou signatures numériques incorporés avec les données d'authentification des utilisateurs de votre entreprise. L'association de cartes à puce avec un nom d'utilisateur et un mot de passe pour l'authentification est la meilleure solution de protection des données d'authentification des utilisateurs.

sélectionnez l'option Certificat de carte à puce si vous utilisez des cartes à puce avec le Bureau dynamique.

pour utiliser les cartes à puce dans un environnement Windows 2008 ou Windows Vista, vous devez créer ou mettre à niveau votre magasin central avec une console Single Sign-On 4.5 (anciennement Password Manager) ou ultérieure et API de protection des données de Microsoft (nécessite des profils itinérants) doit être sélectionné dans vos configurations utilisateur.

Option	Description
Devez-vous réglementer l'accès des administrateurs aux données utilisateurs ?	Voir la section *— Usurpation d'identité* .
Données d'authentification des utilisateurs	Sélectionnée. Un secret utilisateur est utilisé pour accéder aux données utilisateur et ainsi protéger ces dernières. Dans ce cas, le secret utilisateur est un mot de passe. La sécurité du mot de passe peut être calculée à partir du mot de passe de domaine saisi par l'utilisateur ou d'un mot de passe ponctuel généré par des dispositifs à jetons, de proximité ou à reconnaissance biométrique.
Certificat de carte à puce	Sélectionnée. Dans ce cas, le secret utilisateur est protégé par cryptage et décryptage fournis par le certificat de sécurité de la carte.

Si vous utilisez des cartes à puce ne prenant pas en charge les certificats de sécurité en tant qu'authentification principale dans un domaine Windows ou que vous n'utilisez pas de profil itinérant, utilisez l'option Permettre le code secret de carte à puce. Lorsque vous sélectionnez cette option, les clés de cryptage utilisées pour protéger les informations d'identification secondaires sont calculées à partir du code secret de carte à puce.

Pensez à mettre en place une politique de code secret restrictif. Dans certaines sociétés, les codes secrets sont des numéros à quatre chiffres qui n'offrent pas un niveau de protection élevé (inférieur à un mot de passe à huit caractères, par exemple) et risquent d'être plus exposés aux attaques. N'utilisez cette option que si votre entreprise a mis en place une politique de code secret impliquant un mélange de lettres et de chiffres et une longueur minimum de huit caractères.

Option	Description
Devez-vous réglementer l'accès des administrateurs aux données utilisateurs ?	Voir la section *— Usurpation d'identité* .
Données d'authentification des utilisateurs	Sélectionnée. Un secret utilisateur est utilisé pour accéder aux données utilisateur et ainsi protéger ces dernières. Dans ce cas, le secret utilisateur est un code secret.
Permettre le code secret de carte à puce	Sélectionnée. Autoriser l'utilisation du code secret de carte à puce comme secret utilisateur pour assurer la protection. Utilisez cette option uniquement si votre entreprise a instauré une politique de code secret restrictif.

cette option est prise en charge par la version 4.1 de Single Sign-On (anciennement Password Manager) Plug-in si vous sélectionnez les options Utiliser la même protection des données qu'avec Single Sign-On 4.1 et versions précédentes et Code secret en tant que mot de passe, si vous envisagez d'utiliser des plug-ins d'ancienne génération.

Sélectionnez Non en réponse à la question Devez-vous réglementer l'accès des administrateurs aux données utilisateurs ? pour autoriser l'utilisation de profils itinérants et de l'API de protection des données de Microsoft dans votre environnement. Cette option est la mieux sécurisée après la méthode Cartes à puce avec certificats et données d'authentification des utilisateurs.

Sélectionnez cette option si vous utilisez des profils itinérants exploitant un protocole d'authentification de réseau Kerberos pour les utilisateurs. Cette option ne fonctionne que si des profils itinérants sont présents. Si vous stockez également des profils itinérants sur des stations de travail, vous devez la sélectionner.

Single Sign-On calcule les clés de cryptage protégeant les informations d'identification secondaires à partir du mot de passe principal de l'utilisateur. Néanmoins, si un utilisateur utilise une carte à puce pour l'authentification principale, il n'existe aucun mot de passe principal et cette opération alors est impossible. Dans ce cas, la meilleure solution pour le plug-in est l'option API de protection des données de Microsoft. Cette option utilise la DPAPI de Microsoft pour calculer les clés de cryptage et protéger les informations d'identification secondaires. Ce mécanisme de cryptage utilise les informations d'identification Windows ou de domaine de l'utilisateur pour calculer les clés de cryptage.

Si les utilisateurs saisissent des mots de passe pour accéder à leur PC et un protocole d'authentification réseau Kerberos pour accéder aux serveurs Citrix XenApp, sélectionnez les options suivantes :

- Non en réponse à la question Devez-vous réglementer l'accès des administrateurs aux données utilisateurs ?
- Données d'authentification des utilisateurs
- API de protection des données de Microsoft

Cette méthode admet également l'utilisation d'informations d'identification de l'utilisateur et de cartes à puce pour l'ouverture de session.

pour utiliser les cartes à puce dans un environnement Windows 2008 ou Windows Vista, vous devez créer ou mettre à niveau votre magasin central avec une console Single Sign-On 4.5 (anciennement Password Manager) ou ultérieure et API de protection des données de Microsoft (nécessite des profils itinérants) doit être sélectionné dans vos configurations utilisateur.

cette méthode est prise en charge par la version 4.1 de Single Sign-On Plug-in et supportée par les plates-formes Windows XP et Windows 2003 Server. Sélectionnez les options Utiliser la même protection des données qu'avec Single Sign-On 4.1 et versions précédentes et DPAPI avec profil si vous envisagez d'utiliser ces plug-ins d'ancienne génération.

L'utilisation d'un mot de passe vide doit rester exceptionnelle et doit être uniquement utilisée dans des environnements à faible niveau de sécurité nécessitant un confort d'utilisation optimal. Elle convient, par exemple, aux situations dans lesquelles une station de travail ou un ordinateur commun localisé dans une usine sert à de nombreux utilisateurs. Vous pouvez toujours utiliser Single Sign-On pour contrôler l'accès aux applications mais les informations d'identification utilisées pour accéder à la station de travail incluent un mot de passe vide.

Important : si vous ne sélectionnez pas cette option et qu'un mot de passe vide est autorisé dans votre environnement, le plug-in ne calcule aucun secret utilisateur et n'assure aucune protection des données avec le mot de passe vide.

Option	Description
Devez-vous réglementer l'accès des administrateurs aux données utilisateurs ?	Voir la section *— Usurpation d'identité* .
Données d'authentification des utilisateurs	Sélectionnée. Un secret utilisateur est utilisé pour accéder aux données utilisateur et ainsi protéger ces dernières. Dans ce cas, le secret utilisateur est un mot de passe.
Autoriser la protection des données à l'aide d'un mot de passe vide	Sélectionnée. Si vous sélectionnez cette option et que le plug-in détecte que l'utilisateur dispose d'un mot de passe vide, un secret utilisateur de protection des données est calculé à partir de l'ID de l'utilisateur.

Installation et mise à niveau

Oct 21, 2015

Il est recommandé d'installer Single Sign-On dans l'ordre suivant :

1. Créez le magasin central.
2. Installez Citrix AppCenter, qui comprend le composant de console Single Sign-On.
3. Installez le service Single Sign-On si vous souhaitez utiliser un ou plusieurs des modules suivants :
   - Gestion des clés
   - Fonctions autonomes
   - Habilitation
   - Synchronisation d'informations d'identification
   - Intégrité des données
     Si vous décidez d'installer le module d'intégrité des données ultérieurement ou après avoir installé Citrix AppCenter et Single Sign-On Plug-in, vous devez ajouter une signature numérique aux données existantes de votre magasin central à l'aide de l'outil de signature des données CtxSignData.exe (disponible une fois que vous avez installé le module d'intégrité des données). De la même manière, si vous désinstallez le module d'intégrité des données, vous devez retirer la signature des données de votre magasin central.
4. Installez l'Outil de définition d'application sur un ou plusieurs ordinateurs de votre environnement lorsque vous devez uniquement créer des définitions d'application. (Lorsque vous installez le rôle de serveur XenApp avec les composants par défaut, l'Outil de définition d'application est inclus.)
5. Installez Single Sign-On Plug-in sur chaque ordinateur utilisateur et sur le serveur XenApp.

Important : le ou les serveurs hébergeant le service Single Sign-On et le magasin central NTFS contiennent des informations très sensibles sur les utilisateurs. Veillez à utiliser un serveur dédié dans un endroit protégé.
Les installations suivantes ne sont pas recommandées et ne sont pas prises en charge :

- N'installez pas le service et le plug-in sur le même ordinateur.
- N'installez pas le service et le rôle de serveur XenApp sur le même serveur.
- N'installez pas Single Sign-On sur un contrôleur de domaine. L'installation sur un contrôleur de domaine du plug-in, du service, de la console ou du magasin central de type point de partage réseau NTFS n'est pas prise en charge.

Vous devez mettre votre environnement complet à niveau vers Single Sign-on version 5.0 ou utiliser une approche par étapes.

1. Bien que cela ne soit pas requis, Citrix vous recommande d'effectuer une mise à niveau vers la version précédente du serveur de licences et d'ajouter les licences requises avant d'effectuer la mise à niveau de Single Sign-on.
2. Si vous utilisez l'un des modules suivants, effectuez la mise à niveau du service Single Sign-On. À cette occasion, vous pouvez également installer d'autres modules.
   - Gestion des clés
   - Fonctions autonomes
   - Habilitation
   - Synchronisation d'informations d'identification

- Intégrité des données

  Remarque : si vous décidez d'installer le module d'intégrité des données ultérieurement ou après avoir installé le composant de console Single Sign-On de Citrix AppCenter et Single Sign-On Plug-in, vous devez ajouter une signature numérique aux données existantes de votre magasin central à l'aide de l'outil de signature des données CtxSignData.exe. (disponible une fois que vous avez installé le module d'intégrité des données). De la même manière, si vous désinstallez le module d'intégrité des données, vous devez retirer la signature des données de votre magasin central.

3. Mettez à niveau le composant de console Single Sign-On de Citrix AppCenter (anciennement appelé Delivery Services Console) sur un ou plusieurs ordinateurs de votre environnement.

   Remarque :

   - Citrix vous recommande d'utiliser le service Single Sign-on et le composant de console au même niveau de version.
   - La mise à niveau du composant de console à la version 5.0 réalise également une mise à niveau du magasin central Single Sign-on. Après avoir effectué la mise à niveau d'une console Single Sign-on 4.8 à la version 5.0, d'autres consoles version 4.8 ne peuvent pas effectuer de modifications dans le magasin central.
4. Si vous devez uniquement créer des définitions d'applications, mettez à niveau ou installer l'Outil de définition d'application sur un ou plusieurs ordinateurs dans votre environnement. (Lorsque vous installez le rôle de serveur XenApp avec les composants par défaut, l'Outil de définition d'application est inclus.)
5. Mettez à niveau le magasin central Single Sign-on.
   - Pour les magasins centraux basés sur des partages réseau NTFS :
     - Sauvegardez le dossier de partage réseau avant d'effectuer la mise à niveau du magasin central Single Sign-on.
     - Sélectionnez le nœud Single Sign-on et exécutez l'assistant Configurer et exécuter la découverte depuis Citrix AppCenter pour mettre à niveau automatiquement le magasin central Single Sign-on.
     - Dans l'assistant, spécifiez le chemin d'accès UNC à votre partage réseau NTFS, généralement \\NomServeur\CITRIXSYNC$, où NomServeur est le nom du serveur sur lequel vous avez créé votre magasin central.
   - Pour les magasins centraux basés sur Active Directory, sélectionnez le nœud Single Sign-on et exécutez l'assistant Configurer et exécuter la découverte depuis Citrix AppCenter pour mettre à niveau automatiquement le magasin central Single Sign-on.
   - Si vous procédez à une mise à niveau à partir d'une version de Citrix Password Manager qui prend en charge le dossier partagé Novell (par exemple, la version 4.6), vous devrez peut-être sauvegarder le partage et exporter/importer les données administratives pour pouvoir continuer à utiliser les paramètres configurés dans ce type de magasin central. Reportez-vous à la documentation relative à l'administration et à l'installation de Password Manager 4.6 pour obtenir des informations sur le déplacement de données de magasin central. La documentation est disponible dans le Centre de connaissances Citrix.
6. Après avoir configuré les fonctionnalités de Single Sign-On dans Citrix AppCenter, mettez à niveau ou installez Single Sign-On Plug-in sur chaque machine utilisateur de votre environnement.

1. Commencez par ajouter des machines utilisateur exécutant Single Sign-on 5.0 Plug-in dans votre environnement (Single Sign-on 4.8) existant.
2. Lorsque vous êtes prêt, mettez à niveau à la fois le service Single Sign-on et la console à la version 5.0.
3. Distribuez le déploiement de Single Sign-on 5.0 Plug-in au reste de vos machines utilisateur.

Configuration de la sécurité et de comptes préalablement à l'installation de Single Sign-On

Oct 21, 2015

Avant d'installer le service Single Sign-On, assurez-vous que les comptes et composants nécessaires à sa prise en charge sont disponibles. Par ailleurs, étant donné que le service utilise le mode HTTP sécurisé (HTTPS), il requiert un certificat d'authentification serveur pour ses communications avec la console et le plug-in à l'aide du protocole SSL (Secure Sockets Layer).

Obtenez, auprès d'une autorité de certification (CA), un certificat d'authentification serveur pour les transmissions à l'aide du protocole SSL ou, si vous disposez d'une infrastructure de clé publique (PKI), téléchargez votre propre certificat sur le serveur exécutant le service.

Il est nécessaire d'obtenir un certificat SSL pour assurer des communications sécurisées entre le service et le plug-in et la console, et pour garantir que la console et le plug-in communiquent avec le serveur de service approprié.

- Ce certificat est utilisé pour les transmissions à l'aide du protocole SSL. Son nom commun doit donc correspondre au nom de domaine complet du serveur de service (FQDN). Spécifiez une taille de clé minimale de 1024.
- Installez le certificat dans le magasin de certificats de votre ordinateur local et établissez la relation de confiance appropriée pour le composant Single Sign-On de Citrix AppCenter et le plug-in.
- Installez ce certificat sur les ordinateurs exécutant le composant Single Sign-On de Citrix AppCenter, le service Single Sign-On et le plug-in.
- Dans un environnement de service à équilibrage de charge ou en clusters, vous pouvez utiliser un certificat unique pour plusieurs serveurs de service si le nom commun du certificat SSL inclut un caractère générique (en général, un astérisque). Par exemple, vous pouvez utiliser un certificat SSL avec le nom commun Serveur*.MaSociété.com pour un environnement intégrant des serveurs nommés Serveur1.MaSociété.com, Serveur2.MaSociété.com et Serveur3.MaSociété.com. Il est également possible d'utiliser un certificat SSL avec le nom commun *.MaSociété.com lorsque ce dernier ne coïncide pas avec le FQDN du serveur.

Important : si vous obtenez votre certificat d'une autorité non approuvée par défaut (telle qu'une autorité de certification installée dans votre société), installez le certificat d'autorité racine dans le magasin de certificat « Autorités de certification racines de confiance » de votre ordinateur local pour établir une relation de confiance.
Les échecs de connexion SSL éventuellement rencontrés par les utilisateurs sont généralement liés à un certificat de serveur non approuvé. Pour obtenir des instructions sur l'extraction et le déploiement de certificats de CA racines, veuillez consulter le site Web de Microsoft.

Les certificats de signature et de validation créés durant l'installation de Single Sign-On sont indépendants du certificat SSL.

Le service Single Sign-On peut nécessiter jusqu'à trois types de compte pour la lecture et l'écriture de données lors de son exécution dans votre environnement. Le nombre et le type de comptes nécessaires dépendent des modules du service à utiliser. Le tableau ci-dessous présente les comptes requis par chaque module du service. Lorsque différents modules nécessitent le même type de compte, vous pouvez utiliser le même compte pour plusieurs modules ou spécifier des comptes personnalisés différents pour chaque module.

Module	Comptes requis		
	Service	Intermédiaire d'authentification	Fonctions autonomes
Intégrité des données	Yes	Non	Non
Module de gestion des clés	Yes	Yes	Non
Habilitation	Yes	Yes	Non
Fonctions autonomes	Yes	Yes	Yes
Synchronisation d'informations d'identification	Yes	Non	Non

Sur le serveur exécutant le service Single Sign-On, utilisez les comptes Service réseau ou Service local existants.

Vous ne pouvez pas spécifier un compte d'utilisateur local comme compte de service dans cette version de Single Sign-On. En revanche, cela est possible avec le compte Service local intégré.

si vous choisissez de créer un compte de domaine en tant que compte de service, vous devez enregistrer un nom principal de service pour ce compte de domaine et pour l'ordinateur de service dans Active Directory à l'aide de l'utilitaire setspn.exe. Si vous utilisez un compte utilisateur de domaine, le compte doit disposer des droits « Ouvrir une session en tant que service ». L'ordinateur exécutant le service doit être approuvé pour la délégation.

Pour plus d'informations sur les noms principaux de service, veuillez consulter le site Web de Microsoft.

Sur le serveur exécutant le service Single Sign-On, créez un compte d'administrateur de domaine doté des réglages suivants. Ce dernier sera utilisé pour les échanges entre l'intermédiaire d'authentification et le service.

Ce compte requiert des droits d'accès en lecture et en écriture au magasin central. Les exigences applicables au compte dépendent du type de magasin central mis en place.

Type de magasin central	Description du compte
Partage réseau NTFS	Caractéristiques du compte : • droits d'accès en lecture et en écriture au magasin central • membre du domaine Une fois le magasin central créé : • Accordez au compte les autorisations de partage Contrôle total sur le point de partage CITRIXSYNC$. • Accordez au compte les autorisations Contrôle total au dossier CITRIXSYNC et à ses sous-

Type de magasin central	Description du compte
	dossiers : le dossier CentralStoreRoot et le dossier People. • Accordez au compte les autorisations Contrôle total à tous les objets de fichiers du dossier CITRIXSYNC et ses sous-dossiers. • Assurez-vous que le groupe Utilisateurs authentifiés dispose des droits requis pour créer des dossiers au sein du dossier People.
Active Directory	Caractéristiques du compte : • droits d'accès en lecture et en écriture au magasin central • membre du groupe d'administrateurs de domaine

Si vous avez recours aux fonctions de réinitialisation de mot de passe ou de déverrouillage de compte du module de fonctions autonomes, utilisez un compte appartenant au groupe des administrateurs de domaine.

L'utilisateur installant le service Single Sign-On et exécutant l'assistant de configuration du service doit appartenir au domaine (utilisateur de domaine) et au groupe d'administrateurs locaux de l'ordinateur de service (ajoutez un compte utilisateur de domaine au groupe d'administrateurs locaux).

L'utilisateur installant le composant de console Single Sign-On, réalisant une opération de découverte et de configuration et utilisant celui-ci doit être un administrateur de domaine et appartenir au groupe d'administrateurs locaux de l'ordinateur de la console. Ce compte utilisateur requiert des droits d'accès en lecture et en écriture au magasin central. Il est possible d'accorder à un compte non administrateur des droits de gestion du composant de console et de ses fonctions associées via la délégation Active Directory ou la délégation contrainte.

L'utilisateur installant Single Sign-on Plug-in doit appartenir au domaine (utilisateur de domaine) et au groupe d'administrateurs locaux de la machine utilisateur. L'utilisateur installant le plug-in doit appartenir au domaine (utilisateur de domaine) et au groupe d'administrateurs locaux de la machine utilisateur. L'utilisateur exécutant le plug-in doit appartenir au domaine (utilisateur de domaine).

Installation de Java Runtime Environment

Oct 21, 2015

Single Sign-On prend en charge Java Runtime Environment (JRE), versions 1.4.x, 5 (1.5.x) et 6 (1.6.x). Téléchargez la version actuellement prise en charge depuis le site Web de Sun Microsystems (http://java.sun.com).

Si vous installez JRE ou en effectuez la mise à jour après installation du composant Single Sign-On de la console Delivery Services Console, de l'Outil de définition d'application ou du plug-in, associez la version actuelle de JRE au composant Single Sign-On.

1. Dans le Panneau de configuration, accédez à la zone Programmes et sélectionnez le composant Single Sign-On.
2. Cliquez sur Change.
3. Dans la boîte de dialogue de configuration, sélectionnez Réparer.

Le message d'erreur suivant peut apparaître lors de l'installation ou de la désinstallation du plug-in :

« Citrix Single Sign-On a détecté qu'au moins un programme ou fichier Java est actuellement en cours d'utilisation. Veuillez fermer tous les programmes et arrêter tous les services liés à Java avant de continuer. "

En général, cette erreur se produit lors de l'installation du plug-in sur un ordinateur exécutant également un service de serveur Web, tel qu'un serveur Apache Tomcat ou Apache HTTP. Elle peut aussi apparaître lors de l'installation du plug-in sur un serveur XenApp pour lequel la console License Management Console est installée.

Dans ce cas, effectuez l'une des opérations suivantes.

1. Arrêtez le service.
2. Installez ou désinstallez le plug-in.
3. Redémarrez le service.

Création d'un magasin central

Oct 21, 2015

1. Chargez le support XenApp.
2. À partir du menu Autorun, sélectionnez Installer les composants manuellement > Composants serveur > Fonctionnalités supplémentaires > Single Sign-On.
3. Sélectionnez Magasin central.
4. Sélectionnez un type de magasin central : partage réseau NTFS ou Active Directory.
   - Si vous sélectionnez Partage réseau NTFS, le magasin central est créé à l'emplacement suivant : %LecteurSystème%\CITRIXSYNC$.
   - Si vous sélectionnez Active Directory :
     1. Sélectionnez Étape 1 : étendre Active Directory. Le schéma Active Directory est étendu.
     2. Sélectionnez Étape 2 : créer un magasin central.
     3. Après creation du magasin central, redémarrez le serveur sur lequel la console Single Sign-on est installée. Vous devez effectuer ceci afin que le magasin central soit découvert.

     Important : assurez-vous que le serveur actuel fait partie du domaine Active Directory et que l'utilisateur actuel est membre du groupe d'administrateurs du schéma et du groupe d'administrateurs du domaine. vérifiez que le contrôleur du schéma Active Directory est configuré pour permettre les mises à jour. Si le serveur utilisé pour l'extension du schéma Active Directory n'est pas le contrôleur de domaine, veillez également à ce que l'utilitaire Microsoft Windows, Ldifde.exe est installé sur le serveur avant de procéder à cette étape. L'utilitaire est disponible sur le support d'installation Windows ou sur le site Web de Microsoft. Vous ne pourrez pas terminer ce processus si le fichier Ldifde.exe n'est pas installé.

Installation du composant console

Oct 21, 2015

Le composant de console Single Sign-On est inclus lorsque vous installez Citrix AppCenter

Important : vous devez créer votre magasin central Single Sign-On avant de pouvoir exécuter l'assistant Configurer et exécuter la découverte et d'utiliser Single Sign-On.

Pour installer AppCenter (et le composant de console Single Sign-On) lors de l'installation de XenApp

1. Suivez la procédure d'installation du rôle de serveur XenApp. AppCenter est inclus par défaut à l'installation.
2. Sélectionnez Configurer et exécuter la découverte et suivez les instructions.

Pour installer AppCenter (et le composant de console Single Sign-On) manuellement

Assurez-vous que les packs Microsoft Visual C++ Redistributable Packages et Microsoft Primary Interoperability Assemblies sont installés, comme décrit dans la section Configuration système requise.

1. Chargez le support XenApp sur l'ordinateur.
2. À partir du menu Autorun, sélectionnez Installer les composants manuellement > Composants courants > Console de gestion. Suivez les instructions.
3. Sélectionnez Configurer et exécuter la découverte et suivez les instructions.

Installation et configuration des modules du service

Oct 21, 2015

La procédure d'installation et de configuration comprend les étapes suivantes :

1. Obtenez et installez un certificat SSL sur les ordinateurs exécutant le service Single Sign-On, la console et le plug-in.
2. Créez le type de compte requis par les modules du service que vous allez installer.
3. Installez les modules du service.
4. Configurez les modules du service

Les procédures suivantes présupposent que le support d'installation de Single Sign-On est chargé sur l'ordinateur destiné à héberger les modules du service Single Sign-On et que l'écran du programme Autorun de XenApp est affiché.

Pour installer les modules du service

1. Chargez le support XenApp.
2. À partir du menu Autorun, sélectionnez Installer les composants manuellement > Composants serveur > Fonctionnalités supplémentaires > Single Sign-On > Single Sign-on Service.
3. Suivez les instructions.

Pour configurer les modules du service

L'assistant de configuration du service démarre lorsque l'installation des modules du service se termine. Vous pouvez démarrer l'assistant ultérieurement en cliquant sur Démarrer > Tous les programmes > Citrix > Password Manager > Configuration du service.

Suivez les instructions.

- Sur la page Configuration du service :

Paramètre de connexion	Indiquez le numéro de port pour la connexion au service. Le port par défaut est 443. Vous pouvez utiliser tout autre port disponible du serveur exécutant le service. Si vous installez un ou plusieurs modules de service ultérieurement, utilisez le numéro de port que vous avez spécifié lors de la première installation du service. Le service ne peut pas être exécuté sur plusieurs ports. Si vous spécifiez un numéro de port incorrect, Single Sign-On risque d'afficher ultérieurement des messages d'erreur du type « impossible de communiquer ou de se connecter au service Single Sign-On ». Spécifiez le numéro de port approprié lors de l'utilisation de l'Outil de signature de l'intégrité des données sur l'invite de commande.
Certificat SSL	Sélectionnez le certificat SSL installé sur l'ordinateur du service et à utiliser pour la communication avec les machines clientes. Sélectionnez la case à cocher Afficher le nom long pour afficher les informations du paramètre de connexion LDAP contenues dans le certificat.

Nom d'hôte virtuel	L'option Utiliser une valeur par défaut est sélectionnée par défaut si le nom du certificat SSL et le nom d'hôte virtuel correspondent. Le nom d'hôte virtuel doit correspondre au nom du certificat SSL. L'hôte virtuel est le nom de la machine visible par les utilisateurs lors de la création du certificat ; ce nom ne correspond pas nécessairement au nom réel de la machine. Par exemple, le nom du certificat peut inclure un caractère générique (astérisque) ou un nom de domaine en majuscules ou en minuscules ne correspondant pas à la casse du nom de domaine du certificat. Ce paramètre est utile dans les environnements de service à équilibrage de charge ou en clusters.
Informations d'identification du compte	Sélectionnez l'ordinateur local à utiliser pour le service. En général, vous pouvez sélectionner le compte Service réseau.

- Dans la page Configuration des domaines :
  1. Cochez la case correspondant à chaque domaine pour lequel vous souhaitez activer la prise en charge du service.
  2. Sélectionnez un domaine ou plus et cliquez sur Propriétés pour ouvrir la boîte de dialogue Modification de la configuration.
  3. Si vous avez créé un magasin central Active Directory, sélectionnez Contrôleur de domaine et sélectionnez le contrôleur de domaine correct à partir de la liste.
  4. Sélectionnez Compte de l'intermédiaire d'authentification et entrez le nom d'utilisateur, le mot de passe et le domaine du compte de l'intermédiaire d'authentification utilisé pour communiquer avec le magasin central.
  5. Si vous installez le module Fonctions autonomes, sélectionnez Compte des fonctions autonomes de compte et entrez les informations d'identification de cette fonction. Sélectionnez OK pour fermer la boîte de dialogue Modification de la configuration.
     Important : si le service est exécuté dans un environnement Windows Server 2008 ou Windows Server 2008 R2 avec un magasin central NTFS, vous devez utiliser le fichier CtxFileSyncPrep.exe pour ajouter le compte d'intermédiaire d'authentification en tant qu'administrateur au magasin central. Tapez :
     CtxFileSyncPrep [/Admin:nomcompte]

     Si le service est exécuté dans un environnement Windows Server 2008 ou Windows Server 2008 R2 avec un magasin central Active Directory, vous devez aussi ajouter le compte d'intermédiaire d'authentification en tant qu'administrateur au magasin central. Le site Web de Citrix contient des suggestions sur la manière de procéder, à l'adresse (http://support.citrix.com/article/ctx107690).

Configuration du service pour une utilisation multi-domaine

Le service Single Sign-On traite les demandes de service entre utilisateurs appartenant à des domaines approuvés différents. Un administrateur peut installer Citrix AppCenter avec le composant de console Single Sign-On sur des ordinateurs de domaines différents et créer une ou plusieurs configurations dans chacun des domaines.

Par exemple, en supposant un ordinateur équipé du service Single Sign-On et situé dans le domaine A, les utilisateurs configurés dans le domaine A peuvent utiliser les fonctions autonomes du compte pour déverrouiller leurs comptes. Les utilisateurs associés à une configuration utilisateur dans le domaine B peuvent également utiliser cette fonctionnalité, telle

qu'elle est fournie par l'ordinateur du service du domaine A. Dans ce cas, plusieurs configurations utilisateur existent dans des domaines multiples, elles utilisent un seul ordinateur du service pour cette fonction.

Configuration requise par la fonction du service multi-domaine

Avant de mettre en place la fonction de service multi-domaine, veillez à répondre aux critères de configuration requise suivants :

Composant	Configuration requise
Domaines	Chaque domaine partageant le service doit faire partie de la même forêt de domaine. Les domaines de cette forêt doivent avoir un accord de confiance transitif bidirectionnel.
Magasin central	Cette fonctionnalité est disponible pour les mises en place utilisant les magasins centraux Active Directory ou de points de partage réseau NTFS. Tous les utilisateurs partageant le même ordinateur de service doivent être mis en place à l'aide du même type de magasin central : Active Directory ou dossier partagé NTFS. Les types multiples de magasins centraux ne sont pas pris en charge. Un magasin central de type dossier partagé NTFS par domaine n'est pas pris en charge dans ce cas. Toutefois, vous pouvez utiliser un magasin central de type dossier partagé NTFS par forêt.
Fonction d'intégrité des données	La fonction Intégrité des données doit être utilisée uniformément pour tous les domaines. C'est-à-dire qu'elle est soit activée, soit désactivée, dans les configurations du service et de Single Sign-On Plug-in, et ce pour tous les domaines. Par exemple, vous pouvez activer cette fonction dans la configuration du service et la désactiver lors de l'installation de Single Sign-On Plug-in.
Composant de console Single Sign-On de Citrix AppCenter	Chaque console ne peut afficher qu'un seul magasin central et non des magasins centraux multiples. L'administrateur de Single Sign-On doit installer une console dans chaque domaine en utilisant un compte utilisateur disposant des droits d'administration pour ce domaine. L'administrateur peut également installer une console avec la possibilité d'accéder à d'autres domaines et, au besoin, de passer à ces domaines en ouvrant une session avec des informations d'identification spécifiques à ce domaine précis.
Comptes de l'intermédiaire d'authentification et de fonctions autonomes du compte	Vous pouvez configurer un compte de l'intermédiaire d'authentification et un compte de fonctions autonomes du compte disposant des droits en lecture et écriture au magasin central et de privilèges suffisants pour réinitialiser les mots

Composant	Configuration requise
	de passe des utilisateurs et déverrouiller les comptes utilisateurs. Vous pouvez aussi spécifier ces comptes pour chaque domaine dans l'Outil de configuration du service.

Pour configurer le service pour une utilisation multi-domaine

1. Ouvrez une session en tant qu'administrateur sur la machine sur laquelle le service est installé.
2. Démarrez l'Outil de configuration du service en cliquant sur Démarrer > Tous les programmes > Citrix > Password Manager > Configuration du service.
3. Lorsque l'Outil de configuration du service s'affiche, cliquez sur Configuration de domaine dans le panneau de gauche.
4. Cochez la case correspondant à chaque domaine pour activer la prise en charge du service sur ce domaine.
5. Sélectionnez un domaine ou plus et cliquez sur Propriétés pour ouvrir la boîte de dialogue Modification de la configuration.
6. Dans la boîte de dialogue Modification de la configuration :
    1. Si vous avez créé un magasin central Active Directory, cliquez sur Contrôleurs de domaine et, dans la liste, sélectionnez le contrôleur de domaine auquel vous voulez que Single Sign-On se lie pour l'écriture dans le magasin central ou sélectionnez Tout contrôleur de domaine autorisant l'écriture.
    2. Cliquez sur Compte de l'intermédiaire d'authentification et entrez le nom d'utilisateur, le mot de passe et le domaine du compte de l'intermédiaire d'authentification utilisé pour communiquer avec le magasin central.
    3. Si vous installez le module Fonctions autonomes, cliquez sur Compte des fonctions autonomes de compte et entrez les informations d'identification de cette fonction.

Installation de Single Sign-On Plug-in

Oct 21, 2015

Single Sign-On Plug-in s'exécute sur le serveur XenApp et fournit des informations d'identification ainsi que l'accès aux applications publiées. Le plug-in s'exécute également sur chaque machine utilisateur sur lesquelles il fournit des informations d'identification, l'accès aux applications exécutées localement sur la machine utilisateur et la possibilité de contrôler les opérations de Single Sign-On.

Remarque : lorsque vous utilisez cette version du plug-in sur XenApp pour publier des applications activées pour Single Sign-On, le plug-in doit déjà être installé sur les machines utilisateur. Si le plug-in n'est pas installé sur les machines utilisateur, Single Sign-On enverra automatiquement les informations d'identification aux applications publiées avec XenApp, mais l'utilisateur ne pourra pas modifier, supprimer, révéler de mot de passe, mettre en pause ou reprendre Single Sign-On, déterminer si Single Sign-On est mis en pause ou envoyer les mot de passe manuellement.
Considérations relatives à l'installation :

- L'installation de cette version de Single Sign-On Plug-in sur une machine utilisateur met à niveau une version 4.8.
- Après installation du plug-in sur un système d'exploitation pris en charge qui utilise le composant Windows GINA (Microsoft Graphical Identification and Authentication), vous devez redémarrer la machine. Cela comprend Windows XP, Microsoft Windows XP Embedded, Microsoft Windows Fundamentals for Legacy PCs, Microsoft Windows Server 2003 R2 et Microsoft Windows Server 2003 avec Service Pack 2.
  WinLogon utilise les commandes GINA pour contrôler la boîte de dialogue que les utilisateurs voient lorsqu'ils appuient sur les touches CTRL+ALT+SUPPR. Cette boîte collecte les données nécessaires à l'authentification. XenApp, Single Sign-On Plug-in et le client Novell NetWare interagissent avec la DLL GINA ou nécessitent son remplacement. Cela implique d'installer ou désinstaller les logiciels dans un ordre spécifique pour préserver la chaîne GINA correcte. En installant Single Sign-On Plug-in en dernier, vous garantissez que la GINA de Single Sign-On est appelée en premier par le processus Winlogon.
- Une fois l'installation terminée (et après avoir redémarré la machine, le cas échéant), l'icône de Citrix Receiver s'affiche dans la barre d'état système.
- Après avoir installé le plug-in, si vous configurez ou que vous modifiez les informations relatives au système de licences Citrix, redémarrez le plug-in pour que les modifications soient appliquées.

Pour installer Single Sign-On Plug-in sur un serveur lorsque vous installez XenApp (à l'aide de l'assistant)

1. Suivez les instructions fournies dans la section
   — Installation de XenApp à l'aide de l'assistant de Server Role Manager
   . À partir de la liste Composants facultatifs, sélectionnez Single Sign-On Plug-in.
2. Lors de la configuration de XenApp à l'aide de l'outil Server Configuration Tool, vous êtes invité à sélectionner le type de magasin central : Microsoft Active Directory (valeur par défaut) ou Partage réseau NTFS et son chemin d'accès.

Pour installer Single Sign-On Plug-in sur un serveur lorsque vous installez XenApp (à l'aide d'une ligne de commande)

1. Suivez les instructions fournies dans la section
   — Installation de XenApp à l'aide de la ligne de commande
   . Incluez l'option SSONAgentFeature (/install:XenApp,SSONAgentFeature).
2. Lors de la configuration de XenApp à partir d'une ligne de commande, vous pouvez inclure l'option /SSOPluginUncPath:chemin d'accès afin de spécifier le chemin d'accès UNC au magasin central du partage réseau NTFS. Si vous omettez cette option, Active Directory sera utilisé.

Pour installer Single Sign-On Plug-in sur une machine utilisateur ou un serveur sur lequel XenApp est installé

1. Chargez le support XenApp sur l'ordinateur ou le serveur.
2. À partir du menu Autorun, sélectionnez Installer les composants manuellement > Composants serveur > Fonctionnalités supplémentaires > Single Sign-On > Single Sign-On Plug-in.
3. Suivez les instructions. Vous êtes invité à sélectionner le type de magasin central ainsi que les composants à installer (tels que les packs de langue, les fonctions autonomes et l'intégrité des données).

Pour installer Single Sign-On Plug-in sur une machine utilisateur à l'aide de Merchandising Server

Suivez les procédures de téléchargement ou de mise à disposition de plug-ins dans la documentation de Merchandising Server.

Consolidation des icônes dans la zone de notification Microsoft Windows

Lors de l'utilisation de cette version de Single Sign-On Plug-in pour toutes les sessions XenApp et sur chaque machine utilisateur, la zone de notification Microsoft Windows de chaque machine utilisateur ne contient qu'une seule icône Receiver. Dans cette dernière figure un menu Single Sign-On intégré qui regroupe toutes les sessions.

Toutefois, si le serveur XenApp ou la machine utilisateur utilise une version antérieure d'un plug-in, la zone de notification Windows peut également contenir des icônes Single Sign-On. Le tableau suivant illustre plusieurs scénarios.

Machine utilisateur		**Serveur XenApp**		**Zone de notification Windows**	**Le menu des mots de passe est-il disponible depuis l'icône de Receiver ?**
Citrix Receiver	**Single Sign-On Plug-in**	**Citrix Receiver**	**Single Sign-On Plug-in**		
Actuel *	5.0	Actuel	5.0	Une icône Receiver	Oui
Actuel	-	Actuel	5.0	Une icône Receiver	Non
Actuel	5.0	-	4.8	Une icône Receiver et une icône Single Sign-On pour chaque session XenApp connectée. **	Oui
Actuel	4.8	Actuel	5.0	Une icône Receiver et une icône Single Sign-On	Non
Actuel	4.8	Actuel	4.8	Une icône Receiver et une icône Single Sign-On, plus une icône Single Sign-On pour chaque session XenApp connectée. **	Non
Online Plug-in antérieur	4.8	Actuel	5.0	Une icône Single Sign-On et une icône Online Plug-in	Non

* Actuel = Receiver pour Windows, qui contient Online Plug-in

Machine utilisateur		Serveur XenApp		Zone de notification Windows	Le menu des mots de passe est-il disponible depuis l'icône de Receiver ?
Citrix Receiver	Single Sign-On Plug-in	Citrix Receiver	Single Sign-On Plug-in		

** Si les serveurs XenApp exécutent une version antérieure de Single Sign-On Plug-in, et que le dernier logiciel Receiver est installé sur la machine utilisateur (que Single Sign-On Plug-in soit installé ou non sur la machine utilisateur), la zone de notification Windows de la machine utilisateur contient une icône Single Sign-On pour chacun des serveurs XenApp (exécutant la version antérieure du plug-in) auxquels elle est connectée.

Gérer

Oct 21, 2015

Vous pouvez utiliser des stratégies de mot de passe pour définir les règles contrôlant les caractéristiques des mots de passe stockés par les utilisateurs. Ces règles incluent des stratégies de mot de passe, applicables à tous les utilisateurs ou à des groupes spécifiques d'applications, selon les besoins de votre organisation.

Remarque : Citrix XenApp fournit des règles de stratégie permettant de configurer et de contrôler quels utilisateurs ont accès à Single Sign-On lorsqu'ils se connectent aux serveurs et aux applications publiées de la batterie. En dépit de noms similaires, il n'existe aucune relation entre ces deux types de stratégies.
Single Sign-On comporte deux stratégies de mot de passe standard intitulées Default et Domain. Vous pouvez utiliser ces stratégies telles quelles, les copier de manière à les adapter aux stratégies et aux normes de votre entreprise. Vous ne pouvez pas les supprimer.

Lorsqu'un utilisateur ajoute ses informations d'identification dans la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification) pour une application qui n'a pas été définie par l'administrateur, Single Sign-On applique la stratégie Default à cette application. Si vous souhaitez étendre le groupe de partage de mot de passe à un domaine, vous devez lui appliquer la stratégie Domain.

Dans la mesure où Single Sign-On applique la stratégie de mot de passe Default aux applications ajoutées par les utilisateurs, configurez cette stratégie de façon à être la plus large possible, afin d'accepter les mots de passe de toutes les applications pour lesquelles vous autorisez les utilisateurs à stocker des mots de passe.

Vous avez la possibilité de créer autant de mots de passe que nécessaire pour votre entreprise. Par exemple, vous pouvez appliquer une stratégie pour votre groupe de partage de domaine et créer des stratégies spécifiques à appliquer à des groupes individuels d'applications pour mieux cibler vos besoins. Une stratégie de mot de passe vous permet de :

- automatiser les modifications de mot de passe pour les applications ;
- mettre en place des plans de sécurité comprenant des mots de passe complexes et des mots de passe spécifiques aux applications invisibles pour les utilisateurs ;
- définir une date d'expiration des mots de passe d'application, même si l'application ne dispose pas d'une telle fonctionnalité ;
- empêcher l'utilisation répétée d'un même mot de passe pour une application.

Groupes de partage de mot de passe

Dans certains cas, les utilisateurs disposent d'un seul mot de passe pour plusieurs applications (dans une suite logicielle, par exemple). Cette situation est appelée partage de mot de passe : les applications utilisent la même autorité d'authentification.

Même si les informations d'identification (nom d'utilisateur et champs personnalisés) sont différentes pour ces applications, le mot de passe reste identique. Dans ce cas, créez un groupe d'applications qui est également un groupe de partage de mot de passe pour garantir que Single Sign-On Plug-in gère le mot de passe pour toutes les applications du groupe comme s'il s'agissait d'une seule. Lors d'une modification du mot de passe pour l'une d'entre elles, Single Sign-On Plug-in s'assure que cette modification est répercutée pour toutes les applications du groupe.

Groupes de partage de mot de passe de domaine

Les groupes de partage de mot de passe de domaine diffèrent des autres groupes de partage de mot de passe car le mot de passe de domaine de l'utilisateur est le mot de passe principal pour le groupe d'applications. Lors d'une modification du

mot de passe de domaine, Single Sign-On Plug-in s'assure que cette modification est répercutée pour toutes les applications du groupe. Cependant, seul le mot de passe de domaine peut être modifié. Les utilisateurs ne peuvent pas modifier le mot de passe pour les autres applications du groupe, à moins que l'administrateur ne retire l'application du groupe de partage de mot de passe de domaine.

Application de stratégies de mot de passe

Single Sign-On applique les stratégies de mot de passe, que le mot de passe soit défini par l'utilisateur ou généré automatiquement par Single Sign-On.

Une stratégie de mot de passe n'est pas appliquée dans les conditions suivantes :

- Un utilisateur s'enregistre auprès de Single Sign-On (lors de la première utilisation).
- Un utilisateur mots de passe à partir de la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification).
- Un administrateur crée une définition d'application.

Single Sign-On n'applique pas de stratégie de mot de passe sur les mots de passe existants (c'est-à-dire ceux créés avant la mise en œuvre de Single Sign-On dans l'entreprise) car les utilisateurs pourraient se voir refuser l'accès à des applications ou des ressources qu'ils utilisent déjà.

Configuration de Single Sign-On pour reconnaître les applications

Oct 21, 2015

Single Sign-On reconnaît et répond aux applications selon des paramètres définis dans les définitions d'application.

Les définitions d'application contiennent des formulaires qui permettent à Single Sign-On Plug-in d'analyser chaque application au moment de son lancement, de reconnaître certaines des caractéristiques qui l'identifient et de déterminer si elle requiert que le plug-in effectue des actions spécifiques, par exemple :

- soumettre des informations d'identification de l'utilisateur dans une invite d'authentification ;
- traiter une interface d'informations d'identification changeante ;
- traiter l'interface de confirmation des informations d'identification.

Les définitions d'application consistent en des ensembles de caractéristiques d'actions et de reconnaissance de formulaire d'informations d'identification appelés définitions de formulaires. Elles comprennent également un groupe d'options de configuration qui s'applique à tous les formulaires d'une même configuration.

Les paramètres de la définition de formulaire définissent les actions réalisées par Single Sign-on lorsqu'une application requiert des informations d'identification.

Une définition d'application contient tous les formulaires de gestion des informations d'identification associés à une même application.

Bien que la plupart des applications et leurs définitions utilisent seulement deux formulaires pour gérer les informations d'identification des utilisateurs, vous pouvez définir autant de formulaires que nécessaire dans une définition d'application.

Single Sign-On prend en charge un grand nombre d'applications, y compris des applications de type Windows, Web et émulateur de terminal. Il fonctionne avec des applications Java, des solutions SAP ainsi que des applications hébergées sur un ordinateur central (mainframe), un système AS/400 ou un serveur UNIX.

Utilisez les assistants fournis pour créer des définitions d'application pour les applications qui n'ont pas de modèles prédéfinis. L'assistant de définition d'application configure les caractéristiques de tous les formulaires inclus dans la définition. Il comprend également un assistant de définition de formulaire contenant des procédures détaillées pour vous permettre de définir la prise en charge des applications de type Windows, Web et d'émulateur de terminal.

Single Sign-On permet également la prise en charge de la découverte d'applications externes et du traitement d'actions correspondantes. Cette fonction permet aux implémenteurs tiers d'étendre les tâches de détection d'applications et de soumission des informations d'identification d'un formulaire en permettant d'accéder à des processus externes durant les phases de détection d'applications et de traitement des actions par Single Sign-On Plug-in.

La combinaison de toutes ces fonctions constitue un environnement de création de définitions d'application flexible et adaptable qui permet d'offrir à votre communauté d'utilisateurs un accès sécurisé et flexible aux applications critiques par Single Sign-on.

Attention : Single Sign-On dépend d'un fonctionnement sécurisé des ordinateurs hébergeant les composants du produit. Si la machine cliente devient infectée par un code malveillant, il existe un risque que ce code puisse nuire à la sécurité fournie par Single Sign-On. Pour réduire ce risque, observez les consignes de bonnes pratiques de sécurité standard de manière à maintenir la sécurité de l'infrastructure de votre organisation.

Modèles d'application

Les modèles d'application sont des fichiers XML qui permettent de partager les définitions d'application entre plusieurs environnements Single Sign-On. Les modèles d'application représentent un gain de temps car vous pouvez les convertir en définitions d'application moyennant une intervention ou une configuration réduite. Les modèles requièrent que vous fournissiez certaines informations pour compléter la définition d'application, telles qu'une adresse URL ou un nom de fichier exécutable, une date d'expiration du mot de passe et des paramètres de détection avancés.

Installez les modèles d'applications à l'aide du nœud Single Sign-On sur Citrix AppCenter ou l'Outil de définition d'application. Ces deux outils incluent des modèles pour les applications Windows et Web les plus courantes.

Important : pour permettre les écritures sur un magasin central Active Directory exécuté dans l'environnement Windows Server 2008, Windows Server 2008 R2, Windows Vista ou Windows 7, l'Outil de définition d'application doit être paramétré avec un niveau d'intégrité élevé. Pour démarrer l'outil sur l'ordinateur système, le compte que vous utilisez pour ouvrir une session doit être membre du groupe d'administrateurs locaux, ainsi que membre du groupe d'administrateurs de domaine ou disposer des droits en écriture sur les objets Active Directory du magasin central. Fournissez ces informations d'identification en exécutant l'outil, soit à l'invite Contrôle de compte d'utilisateur, soit lors de l'ouverture de session sur le système. L'outil est paramétré avec un niveau d'intégrité élevé et peut écrire sur le fichier Active Directory.
Lorsqu'un modèle d'application est introuvable, créez une définition d'application à l'aide du nœud Single Sign-On de Citrix AppCenter ou de l'Outil de définition d'application.

Identification des applications et des événements de gestion des informations d'identification par Single Sign-On Plug-in

Oct 21, 2015

L'interface utilisateur d'une application inclut différents formulaires qui permettent de gérer les événements d'informations d'identification associés à l'application.

Par exemple, un formulaire entre les informations d'identification d'ouverture de session, un second modifie le mot de passe de l'application et un troisième confirme une modification apportée aux informations d'identification de l'utilisateur.

Selon le type d'application définie (Windows, Web ou émulateur de terminal), Single Sign-On utilise un nombre varié d'identificateurs collectés dans les définitions d'application pour identifier et répondre aux formulaires. Ceux-ci incluent mais ne sont pas limités au type d'application, titre de fenêtre et au nom du fichier exécutable.

Une fois l'application et le formulaire identifiés, Single Sign-On Plug-in invite l'utilisateur à fournir ou à enregistrer ses informations d'identification, soumet les informations d'identification enregistrées ou invite l'utilisateur à mettre à jour ses informations d'identification, selon les paramètres définis.

Les définitions d'applications sont créées à l'aide de AppCenter ou de l'outil de définition d'application.

Une définition d'application prend en charge tous les événements de gestion des informations d'identification associés à une application spécifique, dont notamment :

- l'authentification de l'utilisateur ;
- la modification des informations d'identification de l'utilisateur ;
- la confirmation des modifications des informations d'identification.

Les définitions d'applications se divisent en trois catégories principales qui déterminent les informations collectées :

- applications Windows (y compris les applications Java et SAP LogonPad) ;
- applications Web (y compris les applets Java) ;
- applications d'émulateurs de terminal compatibles HLLAPI.

Une définition d'application se compose des éléments suivants.

- Caractéristiques de l'application qui s'appliquent à tous les formulaires inclus dans la définition. Celles-ci sont définies à l'aide de l'assistant de définition d'application.
- Données spécifiques au formulaire permettant de reconnaître chaque événement de gestion des informations d'identification associé à l'application. Définissez ces formulaires et événements à l'aide de l'assistant de définition de formulaire. Cet assistant est exécuté dans le cadre de l'assistant de définition d'application.

Les caractéristiques de l'application contiennent des informations de configuration similaires pour tous les types d'applications. Cependant, les données spécifiques au formulaire d'une définition d'application varient largement selon le type d'application définie.

Pour pouvoir créer une définition d'application, vous devez avoir accès à l'application sur l'ordinateur sur lequel la définition d'application est créée. Étant donné que certaines signatures d'applications varient considérablement selon le système d'exploitation sous-jacent, testez les définitions d'application dans tous les logiciels de système d'exploitation présents dans votre entreprise.

Testez les modifications ou mises à niveau apportées à une application après qu'une définition d'application a été déployée pour vérifier qu'il n'existe aucun changement de signature qui requière de modifier la définition de l'application.

Important : par mesure de sécurité, dans son état par défaut, Windows Server 2008, Windows Server 2008 R2, Windows Vista et Windows 7 s'exécutent avec la fonction Isolation des privilèges au niveau de l'interface graphique (UIPI) activée. La fonction UIPI empêche aux applications d'envoyer des messages vers d'autres applications avec un niveau d'intégrité supérieur. Par conséquent, Single Sign-On Plug-in, qui fonctionne à un niveau d'intégrité moyen, ne détecte ni ne soumet d'informations d'identification aux applications exécutées à un niveau d'intégrité supérieur. Pour conserver le niveau de sécurité escompté de ces systèmes d'exploitation et Single Sign-On, continuez d'utiliser ces paramètres par défaut.

Présentation de l'assistant de définition de formulaire et d'application

Oct 21, 2015

Toutes les définitions d'application sont initialement créées à l'aide de l'assistant de définition d'application et de l'assistant de définition de formulaire intégré.

L'assistant de définition de formulaire définit les caractéristiques associées à chaque formulaire de gestion des informations d'identification inclus dans une définition d'application.

Présentation de l'assistant de définition d'application

Pour démarrer l'assistant de définition d'application, sélectionnez le nœud Définitions d'application dans AppCenter, et, à partir du menu Action, sélectionnez Créer une définition d'application.

L'assistant de définition d'application recueille des informations sur chaque type d'application (Windows, Web et d'émulateur de terminal).

Données collectées	Windows	Web	Émulateur de terminal
Identification de l'application	X	X	X
Gestion des formulaires	X	X	X
Nom des champs personnalisés	X	X	X
Désignation de l'icône	X		
Configuration de la détection avancée	X	X	X
Configuration de l'expiration du mot de passe	X	X	X
Confirmation des réglages	X	X	X

Gestion des formulaires avec l'assistant de définition d'application

La plupart des applications ont des formulaires distincts pour l'authentification et la modification du mot de passe. Certaines applications disposent également de formulaires distincts destinés à notifier les utilisateurs de la réussite de la modification de leur mot de passe.

La page Gestion des formulaires permet d'ajouter des formulaires à la définition d'une application. Cette page permet également de modifier ou supprimer des formulaires.

La sélection de l'option Ajouter un formulaire lance l'assistant de définition de formulaire qui permet de collecter les données de formulaire. Utilisez l'assistant de définition de formulaire pour chaque formulaire ajouté à la définition d'application.

Affectation d'un nom aux champs personnalisés

Single Sign-On inclut des champs de nom d'utilisateur et de mot de passe correspondant aux informations requises pour tous les formulaires d'authentification. Certaines applications requièrent des informations supplémentaires telles que le nom de la base de données, du domaine ou du système pour authentifier l'utilisateur.

Vous pouvez ajouter jusqu'à deux champs personnalisés à l'aide de l'assistant de définition de formulaire. Si vous procédez de la sorte, une fois de retour sur l'assistant de définition d'application, utilisez la page Nom des champs personnalisés pour donner un nom à ces champs.

Pour créer une touche d'accès rapide dans le nom de champ personnalisé, placez une esperluette (&) immédiatement avant la lettre à utiliser comme touche d'accès rapide. Si aucune touche d'accès rapide n'est définie, Single Sign-On Plug-in associe dynamiquement une valeur numérique comme touche d'accès rapide à la commande. Celle-ci apparaît sous la forme (1) ou (2) sur le bouton, selon le nombre de champs personnalisés qui ont été définis.

Spécification d'une icône pour les applications Windows

Par défaut, Single Sign-on utilise une icône différente pour faire la différence entre applications Windows, Web et de terminaux basées sur des émulateurs dans la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification). Vous pouvez toutefois spécifier une icône personnalisée pour les applications Windows sur la page Désignation de l'icône afin de faciliter l'identification d'applications spécifiques. Si vous optez pour l'option d'icône personnalisée, stockez le fichier d'icône dans le même emplacement que l'application.

Empêcher les boucles liées aux informations d'identification

Utilisez les options de la page Configuration de la détection avancée pour limiter les boucles de soumission des informations d'identification et les boucles de changement de ces informations.

Les utilisateurs peuvent parfois se trouver sur un site Web en boucle de soumission des informations d'identification. Dans ces cas de figure, les utilisateurs se déconnectent d'une application et sont renvoyés sur l'écran d'ouverture de session. Single Sign-On Plug-in détecte l'écran d'ouverture de session et soumet les informations d'identification des utilisateurs, qui sont alors reconnectés automatiquement. Activez l'option Ne traiter que la première ouverture de session pour cette application pour empêcher la soumission automatique.

Lorsqu'une application prédéfinie est lancée pour la première fois et que cette option est sélectionnée, Single Sign-On Plug-in soumet les informations d'identification dans la première instance du formulaire d'authentification sans qu'aucune autre action de l'utilisateur ne soit requise. Lorsque les utilisateurs se déconnectent et retournent à l'écran d'ouverture de session, une fenêtre s'affiche et reste visible pendant environ 10 secondes. Trois options s'offrent aux utilisateurs :

- Fermer la fenêtre : aucune information d'identification n'est soumise.
- Fermer la fenêtre : aucune information d'identification n'est soumise.
- Cliquer sur le lien : les informations d'identification sont soumises.

La fermeture de l'application met fin à la session et Single Sign-On soumet les informations d'identification lors de l'ouverture suivante de l'application.

Pour éviter d'entrer dans une boucle de changement des informations d'identification, activez l'option Ne traiter que la première modification de mot de passe pour cette application. Si cette option est sélectionnée, et que les utilisateurs tentent de modifier leur mot de passe plusieurs fois lorsqu'ils tentent d'accéder à une application donnée, ils sont invités à vérifier les modifications de mot de passe suivantes.

Configuration de l'expiration du mot de passe

La page Configuration de l'expiration du mot de passe contient des options permettant les opérations suivantes :

- identifier un script à exécuter lorsque le mot de passe expire ;
- notification d'expiration de Single Sign-On.

Vous pouvez développer un script pour demander aux utilisateurs de modifier régulièrement leur mot de passe pour toutes les applications ou seulement certaines d'entre elles, modifier automatiquement une partie ou l'ensemble de leurs applications ou utiliser une combinaison de ces processus pour l'adapter à votre politique de sécurité. Pour exécuter un script lorsque la stratégie de mot de passe associée à la définition d'application expire (telle que définie dans la stratégie de mot de passe), activez l'option d'exécution du script et spécifiez le chemin d'accès absolu au script. Le chemin d'accès au script doit être accessible à tous les utilisateurs. N'utilisez pas un chemin UNC (Universal Naming Convention).

En général, le script appelle une application associée en utilisant une interface d'invite de commandes à l'aide d'un paramètre de modification du mot de passe.

Vous pouvez également activer la notification d'expiration de Single Sign-On. Lorsque vous activez cette option, une notification d'expiration du mot de passe Single Sign-On s'affiche lorsque la stratégie de mot de passe associée à l'application indique que le mot de passe a expiré. Cette action affiche un message récurrent indiquant que la période associée a expiré sans obliger l'utilisateur à changer son mot de passe.

Présentation de l'assistant de définition de formulaire

Utilisez l'assistant de définition de formulaire pour :

- définir un formulaire avec l'assistant de définition d'application ;
- modifier un formulaire existant ;
- ajouter un formulaire à une définition d'application existante.

Utilisez l'assistant de définition de formulaire pour définir plusieurs formulaires de gestion des informations d'identification standard :

- Formulaire d'authentification
  Identifie l'interface d'authentification d'une application et gère les actions requises pour accéder à l'application associée.
- Formulaire de modification de mot de passe
  Identifie l'interface de modification du mot de passe d'une application et gère les actions requises pour modifier le mot de passe utilisateur permettant d'accéder à l'application.
- Formulaire de modification de mot de passe réussie
  Identifie l'interface de modification du mot de passe d'une application et gère les actions requises pour confirmer la réussite du changement du mot de passe permettant d'accéder à l'application.
- Formulaire d'échec de modification de mot de passe
  Identifie l'interface indiquant l'échec du changement du mot de passe et définit les actions à effectuer dans ces cas.

Les versions 4.0 et 4.1 de l'Agent Password Manager ne prennent pas en charge les formulaires d'échec ou de réussite de modification des informations d'identification et ne répondent pas aux définitions d'application contenant ces formulaires.

Les données collectées pour chaque formulaire remplissent deux fonctions :

- Reconnaître à quel moment un formulaire spécifique à une application est lancé.
- Effectuer les actions de traitement des informations d'identification associées au formulaire.

Pour lancer l'assistant de définition de formulaire, sélectionnez l'option Ajouter un formulaire dans la page Gestion des formulaires de l'assistant de définition d'application.

Le tableau suivant indique les informations de formulaire qui sont requises pour chaque type d'application (Windows, Web et émulateur de terminal) lors de l'utilisation de l'assistant de définition de formulaire.

Données collectées	**Windows**	**Web**	**Émulateur de terminal**
Nom du formulaire	X	X	X
Identification du formulaire	X	X	X
Définition des actions de formulaire	X	X	
Définition des règles de détection de champ			X
Autres réglages	X	X	X
Confirmation des réglages	X	X	X

Définitions d'applications de type Windows

Oct 21, 2015

Utilisez les définitions d'applications de type Windows pour identifier les applications Windows et Java ainsi que les applications lancées à partir de SAP Logon Pad.

Dans le contexte des définitions d'application, considérez les applications lancées par un fichier doté d'une extension .exe comme des applications Windows.

Pour rassembler des informations requises pour les définitions d'applications Windows, lancez l'application et naviguez vers le formulaire ayant lancé l'événement de gestion des informations d'identification (authentification de l'utilisateur, changement du mot de passe, réussite du changement de mot de passe ou échec du changement de mot de passe) lors de l'exécution de l'assistant de définition de formulaire à partir de la console ou de l'outil de définition d'application. L'assistant fournit des instructions permettant de localiser et d'identifier les parties applicables de l'application.

Identification des formulaires

Lorsque vous créez des définitions pour des applications de type Windows, utilisez la page Identification du formulaire pour fournir les informations requises par Single Sign-On Plug-in pour reconnaître sans équivoque le formulaire défini.

Ces informations d'identification incluent le titre de la fenêtre et le nom du fichier exécutable. Lorsque Single Sign-On Plug-in détecte le nom du fichier exécutable, il surveille l'application pour rechercher les titres de fenêtres définis.

Lorsqu'il détecte un titre de fenêtre, Single Sign-On Plug-in effectue les actions définies pour le formulaire.

Pour identifier un formulaire

1. Si ce n'est pas encore fait, démarrez Windows et accédez au formulaire authentification de l'utilisateur, changement du mot de passe, modification de mot de passe réussie ou échec de la modification de mot de passe.
2. Dans la page Identifier le formulaire de l'assistant de définition de formulaire, cliquez sur Sélectionner.
3. Si le programme souhaité n'est pas en surbrillance, utilisez le Sélecteur de fenêtre pour choisir un des autres programmes disponibles.

Identification de titres de fenêtre dynamiques

Sur la page Identification du formulaire, vous pouvez modifier les titres dans Titres de fenêtre pour ce formulaire pour permettre traitement des données de titres de fenêtre dynamiques telles qu'une date ou un identificateur de session. Pour ce faire, utilisez des caractères génériques à la place des données dynamiques qui s'affichent dans le titre d'une fenêtre, comme suit :

Wildcard	Description
?	À n'utiliser que pour un seul caractère dynamique/changeant dans un titre de fenêtre Windows.
*	Utilisez cette valeur pour représenter un ou plusieurs caractères de données dynamiques dans un titre. Cette valeur est recommandée pour les titres vides. Utilisez NULL dans ces situations.
NULL	Utilisez cette valeur pour les titres Windows vides. Le mot « NULL » doit être en majuscules.

Identification de chemins d'accès sécurisés

La zone Noms et chemins d'accès des fichiers exécutables affiche le nom du fichier exécutable défini et toutes les informations de chemin sécurisé.

Les chemins sécurisés limitent la reconnaissance de l'application aux instances de programmes lancés à partir des chemins d'accès spécifiés. Si un ou plusieurs chemins sécurisés sont définis, Single Sign-On Plug-in soumet les informations d'identification uniquement lorsque le programme identifié est exécuté à partir du chemin d'accès défini et que tous les autres identificateurs du formulaire sont présents.

Vous pouvez définir un chemin d'accès sécurisé en cliquant sur Chemin d'accès exécutable complet dans le sélecteur de fenêtre.

Si aucune information de chemin n'est définie, Non fourni(e)(s) s'affiche et Single Sign-On Plug-in transmet les informations d'identification à tous les programmes correspondant aux autres identificateurs du formulaire.

Chemins d'accès multiples avec points virgule. Vous pouvez utiliser des chemins d'accès absolus ou des variables d'environnement pour définir le chemin d'accès.

Remarque : vous pouvez utiliser les définitions d'applications qui incluent des informations de chemin sécurisé pour créer un modèle de définition d'application. Cependant, le chemin d'accès n'est pas inclus dans le modèle.

Définition des actions de formulaire

La page Définition des actions du formulaire vous permet de définir les actions qui doivent être effectuées par Single Sign-On Plug-in pour soumettre les informations d'identification correspondantes pour le formulaire défini.

Le haut de la page affiche les informations d'identification associées au formulaire :

	Formulaire d'authentification	**Formulaire de modification de mot de passe**	**Formulaire de modification de mot de passe réussie**	**Formulaire d'échec de modification de mot de passe**
Nom d'utilisateur/ID	X	X	X	X
Mot de passe	X		X	X
Ancien mot de passe		X		
Nouveau mot de passe		X		
Confirmer le mot de passe		X		
Champ personnalisé 1	X		X	X
Champ personnalisé 2	X		X	X

OK	X Formulaire d'authentification	X Formulaire de modification de mot de passe	X Formulaire de modification de mot de passe réussie	X Formulaire d'échec de modification de mot de passe

La partie inférieure de la page indique la séquence d'actions définie.

Cette page a pour fonction de définir les actions que Single Sign-On Plug-in doit effectuer pour soumettre les informations d'identification requises au formulaire identifié.

Pour définir des actions du formulaire

La procédure suivante convient à la plupart des applications Windows :

1. Cliquez sur le lien hypertexte Définir/Modifier associé aux informations d'identification d'un utilisateur spécifique. Cette action ouvre la boîte de dialogue Configuration du texte de contrôle, qui permet d'identifier le contrôle qui doit recevoir les informations d'identification sélectionnées.
2. Sélectionnez le type de contrôle qui doit recevoir les informations d'identification. À mesure que vous sélectionnez différentes options, le type de contrôle correspondant est mis en surbrillance dans l'application pour permettre de mieux voir la façon dont les informations d'identification sélectionnées et le bouton de soumission seront affichées.
3. Répétez cette procédure pour toutes les informations d'identification requises pour le formulaire ainsi que pour le bouton utilisé pour soumettre le formulaire.
   Certains formulaires requièrent des domaines ou d'autres informations d'identification configurées par l'utilisateur, qui doivent être correctement soumises pour que le formulaire puisse être traité. Pour répondre à ces exigences, deux champs personnalisables sont disponibles. Utilisez ces champs pour définir des informations d'identification spéciales. Les noms associés à ces champs sont définis dans la page Nommer les champs personnalisés de l'assistant de définition d'application, une fois le formulaire défini.

   Remarque : toutes les informations d'identification identifiées au haut de la page Définir les actions du formulaire ne doivent pas obligatoirement être configurées.

Identificateur de fenêtre

Cette page permet de définir un ID de contrôle Windows qui identifie un formulaire lorsque plusieurs fenêtres peuvent être identifiées simplement à l'aide du titre Windows et du nom de fichier exécutable définis. Elle est uniquement utile si l'ID de contrôle Windows peut être utilisé pour distinguer entre les multiples formulaires qui peuvent être identifiés.

Cochez la case Activer la correspondance par identificateur de contrôle de fenêtre et indiquez l'ID de contrôle permettant de distinguer la fenêtre du formulaire défini de tous les autres formulaires possibles.

Extensions d'identification

Les extensions d'identification font partie des extensions de définitions d'application. Ces extensions permettent la prise en charge d'applications qui sont externes au plug-in pour reconnaître la présence d'un événement de traitement des informations d'identification et effectuer le processus de soumission de ces informations.

Bien que les administrateurs Single Sign-On puissent généralement créer des définitions d'applications à l'aide de la console Single Sign-On et de l'Outil de définition d'application, certaines applications ont des exigences spéciales qui requièrent un autre moyen de détecter l'application et de soumettre les informations d'identification de l'utilisateur ou d'effectuer des actions similaires.

Pour pouvoir prendre en charge ces applications, les administrateurs Single Sign-On peuvent utiliser des extensions de définitions d'application pour obtenir une abstraction des contrôles de l'application et des mécanismes de saisie des

données associées.

Les extensions d'identifications sont développées par des implémenteurs tiers et leur mise en œuvre est spécifique à l'application. Par conséquent, les procédures requises pour configurer leur utilisation sont spécifiques à l'application.

En général, les administrateurs Single Sign-On ne sont pas impliqués dans le développement de ces extensions. Les extensions sont créées par des implémenteurs tiers. Étant donné que la configuration de ces extensions est spécifique à chaque application, les instructions de configuration des extensions sont généralement livrées avec l'extension.

Définition des séquences d'action des formulaires Windows à l'aide de l'Éditeur d'action

Utilisez la page Définition des actions du formulaire pour définir les actions qui doivent être effectuées par le plug-in pour soumettre les informations d'identification correspondantes pour le formulaire de gestion des informations d'identification défini.

Pour la plupart des applications Windows, les informations de base recueillies dans l'assistant de définition de formulaire sont suffisantes pour définir le formulaire. Cependant, certains formulaires requièrent des informations, étapes, clés spéciales et autres actions supplémentaires pour compléter le processus de configuration des informations d'identification. Pour ce type de formulaire, cliquez sur Éditeur d'action sur la page Définition des actions du formulaire pour ouvrir la boîte de dialogue Éditeur d'action.

La boîte de dialogue Éditeur d'action se compose des éléments suivants :

- Sélection d'actions
  Cette option affiche toutes les actions possibles et leurs séquences :
- Configuration d'actions
  Cette option permet de définir les options spécifiques à l'action à inclure dans la séquence d'actions.
- Séquence d'actions
  Cette option affiche la séquence d'actions définies à effectuer pour traiter le formulaire de gestion des informations d'identification spécifique.

La partie inférieure de la boîte de dialogue Éditeur d'action comprend le bouton Paramètres avancés, qui permet d'accéder à la boîte de dialogue Paramètres avancés. La boîte de dialogue Paramètres avancés propose les deux commandes suivantes.

- Nombres ordinaux de contrôle
  Cochez cette case pour utiliser des nombres ordinaux de contrôle (souvent appelés ordre Z) à la place des numéros d'ID de contrôle. Les nombres ordinaux de contrôle sont énumérés indépendamment durant le processus de définition (et par le plug-in) pour identifier les contrôles indépendamment des numéros d'ID de contrôle définis par l'application.

  Envisagez de sélectionner cette fonction lorsque vous définissez des applications .NET qui génèrent dynamiquement des numéros d'ID de contrôle ou pour des applications qui ont des numéros d'ID de contrôle en double.
- Pause initiale
  Sélectionnez cette option et définissez la période de temps pendant laquelle le plug-in doit retarder le traitement avant de commencer la séquence d'actions. Une pause peut être configurée soit à l'aide de cette option, soit en lançant la séquence d'actions à l'aide de l'action Insertion d’une pause pour obtenir davantage d'informations.

  Contrairement à l'option Insertion d’une pause, accessible dans la zone Actions disponibles de la boîte de dialogue Éditeur d'action et définie comme une opération d'envoi de frappe clavier, l'option Pause initiale peut être utilisée pour éviter

d'avoir à créer une définition d'application uniquement prise en charge par les versions 4.5, 4.6, 4.6 avec Service Pack 1, 4.8 et 5.0 de Single Sign-On Plug-in.

Pour définir une extension d'action

1. Sélectionnez une action dans la liste Sélection d'actions.
2. Configurez l'action à l'aide des options Configuration d'actions. Lorsque vous êtes satisfait des paramètres de configuration, cliquez sur Insérer. L'action configurée apparaît dans Séquence d'actions.
3. Répétez les étapes 1 et 2 pour toutes les actions requises par le formulaire d'informations d'identification.
4. Sélectionnez les actions dans Séquence d'actions et cliquez sur Monter ou Descendre pour réorganiser les actions selon la séquence d'exécution correcte requise par le formulaire défini.
5. Lorsque vous êtes satisfait de la séquence d'actions, cliquez sur OK. Cette action vous renvoie à la page Définition des actions du formulaire qui contient maintenant la séquence d'actions définie dans la zone Séquence d'action.
6. Cliquez sur Suivant pour continuer le processus de définition du formulaire de la page Autres réglages. Si une combinaison d'actions de formulaire limite la séquence définie uniquement au plug-in/agent de Password Manager 4.5, Password Manager 4.6, Password Manager 4.6 avec Service Pack 1, Single Sign-On 4.8 et Single Sign-on 5.0, un message s'affiche pour vous permettre de continuer ou de revenir en arrière pour modifier votre configuration.

Considérations sur les définitions de type Windows

Lorsque vous définissez des définitions d'applications de type Windows, tenez compte des points suivants.

- Les modèles d'applications facilitent la création des définitions d'applications.
- Testez vos définitions d'application avec le plug-in avant de les mettre à la disposition de vos utilisateurs.
- La plupart des définitions d'application fonctionnent uniquement avec des informations de base. Si une définition d'application ne fonctionne pas comme prévu dans votre environnement de test, cela peut être dû à des fonctions uniques telles qu'un titre de fenêtre dynamique, des ID de contrôle dynamiques ou d'autres identificateurs ou actions spéciaux qui sont programmés dans l'application.
- Pour exporter des définitions d'application de votre environnement de test vers votre environnement de production, utilisez la tâche Exporter les informations d'administration du composant Single Sign-On de Citrix AppCenter.
- Les paramètres qui sont sélectionnés au niveau de la définition d'application s'appliquent à tous les formulaires contenus dans une définition d'application.
- Certains paramètres sélectionnés au niveau de la définition d'application peuvent être ignorés au niveau du formulaire. Par exemple, pour une application ayant trois formulaires définis, la soumission automatique peut être activée au niveau de la définition d'application. Chaque fois que le plug-in rencontre l'un de ces trois formulaires pour l'application, les informations d'identification sont soumises automatiquement. Toutefois, la soumission automatique peut être désactivée pour l'un des formulaires au niveau du formulaire et le plug-in ne soumet alors pas automatiquement ces informations. Dans ce cas, l'utilisateur doit cliquer sur Soumettre ou sur OK pour le formulaire sélectionné.
- Pour créer une touche d'accès rapide dans le nom de champ personnalisé, placez une esperluette (&) immédiatement avant la lettre à utiliser comme touche d'accès rapide.
  Si aucune touche d'accès rapide n'est définie, le plug-in associe dynamiquement une valeur numérique comme touche d'accès rapide à la commande. Celle-ci apparaît sous la forme (1) ou (2) sur le bouton, selon le nombre de champs personnalisés qui ont été définis.

  N'oubliez pas de tester le formulaire final pour vous assurer que le nom défini ne dépasse pas le nombre de caractères autorisé pour le champ personnalisé.

Redirection vers application Windows

Lorsque aucun formulaire n'est reconnu pour l'application Web dans l'assistant de formulaire Web, la définition du formulaire doit être redirigée vers une définition définie pour une application Windows.

Les formulaires ne sont pas reconnus lorsque l'application Web utilise des contrôles ActiveX, Flash, certains types de contrôles Ajax ou d'autres contrôles non HTML pour gérer les événements de gestion des informations d'identification.

Dans ce cas, assurez-vous que la case Redirection vers application Windows est cochée dans la page Nom du formulaire. Cliquez sur Suivant pour avancer dans les pages restantes de l'assistant de définition de formulaire, puis cliquez sur Terminer sur la page Confirmation des réglages.

Les caractéristiques de reconnaissance de formulaire et les actions d'informations d'identification doivent maintenant être définies à l'aide de définitions de type Windows et d'actions de type d'envoi de frappe clavier.

Identification des formulaires Windows avec la Correspondance avancée

Oct 21, 2015

La page Identification du formulaire de l'assistant de définition de formulaire fournit suffisamment de correspondance d'identification de formulaire pour la plupart des applications Windows. Certains formulaires de gestion des informations d'identification requièrent des identificateurs supplémentaires. Pour ces formulaires, Single Sign-On offre la Correspondance avancée. Vous pouvez accéder à cette fonctionnalité à partir de la page Identification du formulaire de l'assistant de définition de formulaire en cliquant sur Correspondance avancée.

Correspondance avancée offre cinq identificateurs avancés pour les applications Windows :

- Informations de la classe
- Recherche de correspondance du contrôle
- Informations de session SAP
- Identificateur de fenêtre
- Extensions d'identification

Ignorer les formulaires à l'aide des informations de classe

À l'aide de la page Information de la classe, vous pouvez identifier les formulaires à ignorer par Single Sign-On. Si vous entrez une classe de fenêtre dans le champ Ignorer cette classe de fenêtre, Single Sign-On Plug-in ne réagit pas lorsqu'un formulaire avec ces informations de classe s'affiche.

N'utilisez pas ce type de correspondance pour les applications .NET ou les applications qui utilisent la classe de fenêtres 32770 (classe par défaut).

Ce paramètre est utile lorsque la classe de la fenêtre est dynamique. Dans ce cas, utilisez des caractères génériques pour remplacer un identificateur de classe de fenêtre dynamique.

Wildcard	Description
?	À utiliser uniquement pour un seul caractère dynamique/changeant.
*	Utilisez cette valeur pour représenter un ou plusieurs caractères de données d'identificateur dynamiques. Cette valeur n'est pas recommandée pour les identificateurs de classe de fenêtre vides. Utilisez NULL dans ces situations.
NULL	Utilisez cette valeur pour les identificateurs de classe de fenêtre vides. Le mot « NULL » doit être en majuscules.

Utilisez des identificateurs de classe de fenêtre pour identifier une classe de fenêtre parmi de nombreuses cibles de classes de fenêtres potentielles. Les conditions suivantes s'appliquent.

- Le titre de fenêtre spécifié et le fichier exécutable associé sont inclus dans les résultats de correspondance multiples. Cette condition se produit généralement lorsque le titre de fenêtre contient des données dynamiques et que des caractères génériques sont spécifiés.
- Le formulaire cible doit être associé à un identificateur de classe de fenêtre unique et toutes les autres correspondances doivent utiliser des identificateurs de classe de fenêtre différents.

Pour identifier les informations de la classe

Démarrez cette procédure à partir de la page Identification du formulaire de l'assistant de définition de formulaire.

1. Cliquez sur Correspondance avancée, puis sélectionnez l'option Information de la classe.
2. Cliquez sur Sélectionner pour choisir l'application cible parmi les applications actuellement ouvertes sur votre ordinateur.
   Remarque : pour étendre les choix, cochez la case Afficher les fenêtres de programmes masquées ou la case Afficher les fenêtres enfants.

Définition de critères de correspondance avec la Correspondance avancée lorsque des identificateurs associés sont différents

Certaines applications affectent des informations dynamiques aux légendes des contrôles. Dans ces cas, le titre de la fenêtre, l'application exécutable associée et les identificateurs de contrôle peuvent être les mêmes pour plusieurs formulaires de gestion des informations d'identification tandis que les légendes ou autres propriétés du formulaire varient en fonction des événements spécifiques aux applications.

Pour ces types de formulaires, utilisez les options de configuration de correspondance de contrôle pour identifier un formulaire spécifique et l'action du plug-in associée en fonction des valeurs de classe, de style ou de texte associées à l'ID de contrôle (ou à plusieurs ID de contrôle si plusieurs définitions sont requises pour identifier le formulaire).

Pour définir des critères de correspondance

Démarrez cette procédure à partir de la page Identification du formulaire de l'assistant de définition de formulaire.

1. Cliquez sur Correspondance avancée, puis sélectionnez l'option Recherche de correspondance du contrôle.
2. Cliquez sur Ajouter une correspondance.
   Remarque : définissez uniquement un nombre suffisant de critères de correspondance pour permettre d'identifier le formulaire de traitement des informations d'identification défini.
3. À partir de la boîte de dialogue Définition des critères de correspondance, cliquez sur Sélectionner.
4. Cliquez avec le bouton droit de la souris sur une entrée d'identificateur de contrôle.
5. Sélectionnez Classe, Style ou Texte pour choisir une caractéristique à utiliser pour associer le formulaire à l'identificateur de contrôle sélectionné.
6. Répétez les étapes 4 et 5 pour chaque ID de contrôle qui doit être utilisé pour identifier le formulaire.

Identification de correspondances lors de l'utilisation de session SAP multiples

Les versions plus anciennes de SAP sont gérées à l'aide de définitions d'applications Windows et Web standard. Cependant, la boîte de dialogue Correspondance avancée offre une prise en charge des applications SAP lorsque plusieurs systèmes SAP sont configurés pour utiliser la même interface graphique d'authentification SAP (telle que SAP Logon Pad).

La prise en charge des informations de session SAP requiert que l'administrateur SAP active les scripts d'interface graphique sur le serveur. Ceci permet à la console et à Single Sign-On Plug-in d'interroger le SAP Logon Pad et de déterminer l'ID du système ou le nom du serveur (ou les deux) requis pour identifier le formulaire de traitement d'informations d'identification spécifique.

L'option Informations de session SAP définit que les informations de session peuvent être extraites d'une fenêtre SAP pour permettre d'identifier et de distinguer une fenêtre de session SAP d'une autre.

Pour définir les informations de session SAP manuellement

Les valeurs des champs ID système SAP et Nom du serveur peuvent être saisies manuellement. Ces deux champs acceptent des expressions rationnelles comme valeurs. Ceci est utile pour contrôler la capacité de recherche des serveurs multiples.

Vous pouvez également entrer manuellement les valeurs pour faire correspondre les noms DNS et NetBIOS d'un serveur.

Utilisez le format d'expression régulière pour prendre en charge les noms DNS et NetBIOS.

^NomServeur(\.domaine\.com)?$

Pour générer un message de script d'interface graphique SAP

Les messages de scripts d'interface graphique SAP peuvent être générés chaque fois qu'un programme tente d'établir une connexion au SAP LogonPad à l'aide de l'interface graphique SAP. Dans ce cas, il suffit de modifier un paramètre de registre pour éviter de recevoir ce message.

La clé de registre est HKEY_CURRENT_USER\Software\SAP\SAPGUI Front\SAP Frontend Server\Security\WarnOnAttach. Il s'agit d'une clé DWORD. Si cette valeur de clé est définie sur 0, aucun message ne s'affiche. La valeur par défaut est 1.

Définitions d'applications de type Web

Oct 21, 2015

Les définitions d'application de type Web sont utilisées pour identifier des applications Web, y compris les applets Java.

En général, toutes les applications qui sont exécutées dans un navigateur sont des applications Web dans le contexte des définitions d'application. Single Sign-On prend en charge les applications Web exécutées sur Internet Explorer versions 6.0, 7.0, 8.0 et 9.0.

Les définitions d'applications Web sont créées, en partie, en identifiant des parties de l'application à mesure qu'elle est exécutée. Pour rassembler des informations requises pour les définitions d'applications Web, lancez l'application et naviguez vers le formulaire ayant lancé l'événement de gestion des informations d'identification (authentification de l'utilisateur, changement du mot de passe, réussite du changement de mot de passe ou échec du changement de mot de passe) lors de l'exécution de l'assistant de définition de formulaire à partir de la console ou de l'outil de définition d'application. L'assistant affiche des instructions à l'écran pour permettre de localiser et d'identifier les parties applicables de l'application.

Nom du formulaire

Lorsque vous créez des définitions d'application pour des applications de type hôte, la page Nom du formulaire de l'assistant de définition de formulaire vous permet d'effectuer les opérations suivantes:

- affecter un nom défini par l'utilisateur au formulaire créé ;
- définir le type du formulaire créé.
- définir des actions spéciales éventuelles.

Notez que le nom attribué au formulaire s'affiche dans la page Gestion des formulaires de l'assistant de définition d'application. Choisissez un nom approprié pour le type de formulaire défini.

L'assistant de définition de formulaire permet de définir plusieurs types de formulaires de gestion des informations d'identification standard

- Formulaire d'authentification
  Il permet de définir l'interface d'authentification d'une application et de gérer les actions de soumission d'informations d'identification requises pour accéder à l'application associée.

- Formulaire de modification de mot de passe
  Il permet de définir l'interface de modification du mot de passe d'une application et de gérer les actions de soumission d'informations d'identification requises pour changer le mot de passe utilisateur permettant d'accéder à l'application.

- Formulaire de modification de mot de passe réussie
  Il permet de définir l'interface de modification du mot de passe d'une application et de gérer les actions de soumission d'informations d'identification requises pour confirmer la réussite du changement du mot de passe utilisateur permettant d'accéder à l'application.

- Formulaire d'échec de modification de mot de passe
  Il permet de définir l'interface indiquant l'échec du changement du mot de passe et de définir les actions à effectuer dans ces cas.

Les versions 4.0 et 4.1 de l'Agent Password Manager ne prennent pas en charge les formulaires d'échec ou de réussite de modification des informations d'identification et ne répondent pas aux définitions d'application contenant ces formulaires.

Utilisez la zone Actions spéciales pour identifier tout traitement spécial pour le formulaire défini :

- Aucune action spéciale
  Sélectionnez cette option pour effectuer un traitement de formulaire Web normal.
- Redirection vers application Windows
  Choisissez cette option lorsque aucun formulaire n'est reconnu pour l'application Web dans l'assistant de formulaire Web. Ceci se produit lorsque l'application Web utilise des contrôles ActiveX, Flash, certains types de contrôles Ajax ou d'autres contrôles non HTML pour gérer les événements de gestion des informations d'identification.
- Ignorez ce formulaire lorsqu'il est détecté par le plug-in.
  Sélectionnez cette option pour que le plug-in ignore le formulaire.

Identification du formulaire

Lorsque vous créez des définitions pour des applications de type Web, la page Identification du formulaire vous permet de fournir des informations requises pour que Single Sign-On Plug-in puisse reconnaître sans équivoque le formulaire défini.

Les applications Web sont identifiées à l'aide de l'adresse URL associée au formulaire de gestion des informations d'identification défini.

Cliquez sur Sélectionner pour ouvrir le sélecteur de page Web. Utilisez le sélecteur de page Web pour identifier la page Web que vous voulez associer au formulaire.

Après avoir complété le sélecteur de page Web, vous revenez à cette page. Deux cases à cocher sont disponibles pour contrôler la façon dont les URL identifiées doivent être interprétées :

- Recherche d'URL stricte
  Cochez cette case pour reconnaître uniquement les événements de gestion des informations d'identification des applications Web qui sont lancées à partir des URL spécifiées. Certaines URL peuvent contenir des données dynamiques telles que des identificateurs de gestion de session, des paramètres d'application ou d'autres identificateurs qui peuvent varier pour chaque instance. Dans ces circonstances, l'utilisation de la correspondance stricte risque de ne pas permettre la reconnaissance de l'URL.
- URL sensible à la casse
  Cochez cette case pour utiliser l'URL avec la casse exacte.

Définition des actions de formulaire

La page Définition des actions du formulaire vous permet de définir les actions qui doivent être effectuées par Single Sign-On Plug-in pour soumettre les informations d'identification correspondantes pour le formulaire défini.

Le haut de la page affiche les informations d'identification associées au formulaire :

	Formulaire d'authentification	**Formulaire de modification de mot de passe**	**Formulaire de modification de mot de passe réussie**	**Formulaire d'échec de modification de mot de passe**
Nom d'utilisateur/ID	X	X	X	X
Mot de passe	X		X	X

Ancien mot de passe	**Formulaire d'authentification**	X **Formulaire de modification de mot de passe**	**Formulaire de modification de mot de passe réussie**	**Formulaire d'échec de modification de mot de passe**
Nouveau mot de passe		X		
Confirmer le mot de passe		X		
Champ personnalisé 1	X		X	X
Champ personnalisé 2	X		X	X
OK	X	X	X	X

La partie inférieure de la page indique la séquence d'actions définie.

Cette page a pour fonction de définir les actions que le plug-in doit effectuer pour soumettre les informations d'identification requises au formulaire identifié.

Pour la plupart des applications Web, le processus suivant est le seul requis :

1. Cliquez sur le lien hypertexte Définir/Modifier associé aux informations d'identification d'un utilisateur spécifique. Cette action ouvre la boîte de dialogue Configurer le texte du champ, qui permet d'identifier le champ qui doit recevoir les informations d'identification sélectionnées. Si le formulaire est déjà ouvert, cette boîte de dialogue affiche tous les types de champ possibles pour les informations d'identification sélectionnées ou pour l'option de soumission.
   Si le formulaire d'informations d'identification de l'application n'est pas ouvert, lancez l'application et affichez le formulaire approprié. Puis sélectionnez Actualiser. Une fois que vous avez sélectionné le formulaire de l'application, cette boîte de dialogue affiche les types de contrôle de champ appropriés pour les informations d'identification sélectionnées.
2. Sélectionnez le type de champ qui doit recevoir les informations d'identification. À mesure que vous sélectionnez différentes options, le type de champ correspondant est mis en surbrillance dans l'application pour permettre de mieux voir la façon dont les informations d'identification sélectionnées et le bouton de soumission seront affichées.
3. Répétez cette procédure pour toutes les informations d'identification requises pour le formulaire ainsi que pour le bouton utilisé pour soumettre le formulaire.
   Certains formulaires requièrent des domaines ou d'autres informations d'identification configurées par l'utilisateur, qui doivent être correctement soumises pour que le formulaire puisse être traité. Pour répondre à ces exigences, deux champs personnalisables sont disponibles. Utilisez ces champs pour définir des informations d'identification spéciales. Les noms associés à ces champs sont définis dans la page Nommer les champs personnalisés de l'assistant de définition d'application, une fois le formulaire défini.

   Remarque : toutes les informations d'identification identifiées au haut de la page Définir les actions du formulaire ne doivent pas obligatoirement être configurées.

Pour la plupart des applications Web, une fois que vous avez défini les champs du formulaire qui doivent recevoir les informations d'identification sélectionnées et le bouton permettant de soumettre le formulaire, le processus de définition des actions de formulaire est terminé et vous pouvez passer à la page suivante de l'assistant.

Cependant, certains formulaires requièrent des informations, étapes, clés spéciales et autres actions supplémentaires pour compléter le processus de configuration des informations d'identification. Pour ces formulaires, cliquez sur Éditeur d'action pour ouvrir la boîte de dialogue Éditeur d'action.

Définition des séquences d'action des formulaires Web à l'aide de l'Éditeur d'action

Utilisez la page Définition des actions du formulaire pour définir les actions qui doivent être effectuées par le plug-in pour soumettre les informations d'identification correspondantes pour le formulaire de gestion des informations d'identification défini.

Pour la plupart des applications Web, les informations de base recueillies dans l'assistant de définition de formulaire sont suffisantes pour définir le formulaire. Cependant, certains formulaires requièrent des informations, étapes, clés spéciales et autres actions supplémentaires pour compléter le processus de configuration des informations d'identification. Pour ce type de formulaire, cliquez sur Éditeur d'action sur la page Définition des actions du formulaire pour ouvrir la boîte de dialogue Éditeur d'action.

La boîte de dialogue Éditeur d'action pour Web se compose des éléments suivants :

- Sélection d'actions
  Cette option affiche toutes les actions possibles et leurs séquences :
- Configuration d'actions
  Cette option permet de définir les options spécifiques à l'action à inclure dans la séquence d'actions.
- Séquence d'actions
  Cette option affiche la séquence d'actions définies à effectuer pour traiter le formulaire de gestion des informations d'identification spécifique.

Autres réglages

Pour les définitions Web, la page Autres réglages est utilisée pour spécifier si le bouton de soumission de la page Web est automatiquement activé par le plug-in ou si l'utilisateur doit sélectionner le bouton manuellement.

Sélectionnez l'option Soumettre ce formulaire automatiquement pour soumettre le formulaire automatiquement sans intervention de l'utilisateur.

Boîte de dialogue Paramètres avancés pour les applications Web

Oct 21, 2015

Certaines applications Web utilisent des URL dynamiques. Lorsque c'est le cas, des critères de définition de formulaire supplémentaires (appelés entrées de correspondance de détection) doivent être utilisés pour permettre d'identifier un formulaire de gestion d'informations d'identification spécifique.

Ces entrées de correspondance de détection sont définies à l'aide de la boîte de dialogue Détails des éléments de détection et s'affichent dans la boîte de dialogue Paramètres avancés. Pour accéder à la boîte de dialogue Détail des éléments de détection, cliquez sur Correspondance avancée dans la page Identification du formulaire pour accéder à la boîte de dialogue Paramètres avancés, puis cliquez sur Ajouter.

Utilisez les options et commandes de la boîte de dialogue Détails des éléments de détection pour définir les critères utilisés pour identifier un formulaire de gestion d'informations d'identification spécifique. Ces critères permettent de rechercher des valeurs spécifiques dans le contenu balisé du formulaire HTML destiné à traiter une action de gestion des informations d'identification spécifique. Vous devez uniquement définir un nombre suffisant de critères de correspondance pour permettre d'identifier le formulaire de gestion des informations d'identification défini.

Entrez l'élément Web pour lequel vous voulez trouver une correspondance dans la case Rechercher. Si l'élément n'est pas trouvé, développez la section Paramètres supplémentaires l'identifier manuellement.

La section Paramètres supplémentaires se compose des zones suivantes :

- Balise
  Ce champ indique la balise HTML à rechercher. Si vous connaissez l'instance spécifique de la balise, cochez la case Correspondance instance et spécifiez quelle instance utiliser dans le document. Si aucune instance spécifique n'est identifiée, toutes les instances du document sont évaluées. Seule la balise doit être spécifiée et non le délimiteur (par exemple, p plutôt que

). Pour ne pas vous tromper, sélectionnez la balise la plus proche du contenu recherché.

  Remarque : étant donné que l'option Correspondance instance peut varier d'un navigateur à l'autre, utilisez cette fonction uniquement lorsque c'est nécessaire et veillez à tester votre configuration.
- Type de données
  Cette zone permet de définir les critères de correspondance. Sélectionnez l'un des critères suivants.

Critères	Description
Text	Il peut s'agir de toute chaîne de texte incluse dans le code HTML.
HTML	Tout code spécifique inclus dans la balise spécifiée.
Attribut	Tout attribut du code HTML (par exemple, un attribut nom d'une balise formulaire).

- Valeur
  Ce champ zone permet d'entrer la valeur de recherche de correspondance. Cochez la case Valeur entière pour rechercher une correspondance exacte de la valeur (la présence de texte non spécifié dans la balise fait échouer la correspondance).

Incluez tous les délimiteurs et guillemets qui peuvent être inclus.

Remarque : cochez la case Valeur entière uniquement lorsqu'il existe plusieurs instances de critères de correspondance similaires.

- Opérateur
  Cette zone permet de définir la relation entre l'entrée courante et les autres entrées définies pour ce formulaire. Les opérateurs disponibles sont les suivants.

Options	Description
ET	Sélectionnez cette option lorsque l'entrée doit être associée à d'autres entrées pour permettre d'identifier le formulaire. Lorsque vous sélectionnez cette option, le résultat de la correspondance courante est comparé au résultat suivant. Si les deux résultats sont vrais, il y a correspondance.
SOIT	Sélectionnez cette option lorsqu'une entrée de correspondance seule permet d'identifier le formulaire. Lorsque vous sélectionnez cette option, le résultat de la correspondance courante est comparé au résultat suivant. Si l'un des deux résultats est vrai, il y a correspondance. Cette option est utilisée pour les définitions à correspondance unique.
NON	Sélectionnez cette opération pour appliquer une logique négative à l'opérateur. Cet opérateur est utilisé pour définir des critères de correspondance qui ne doivent pas apparaître sur la page pour qu'il y ait correspondance.

Définitions d'applications de type émulateur de terminal

Oct 21, 2015

Les définitions d'applications de type émulateur de terminal sont utilisées pour identifier des applications d'émulateur de terminal, y compris mainframe, AS/400, OS/390 ou UNIX. Single Sign-On propose la fonction de Single Sign-on pour les applications d'émulateur de terminal qui mettent en œuvre l'interface HLLAPI (High-Level Language Application Programming Interface) ou qui disposent d'un langage de script intégré pouvant afficher une boîte de dialogue.

Rassemblement des informations requises pour les définitions d'applications d'émulateur de terminal

En général, la meilleure façon (et la plus simple) de rassembler les informations requises pour les définitions d'applications d'émulateur de terminal (HLLAPI) consiste à lancer l'application.

Pour créer des définitions d'applications d'émulateur de terminal, utilisez l'assistant de définition de formulaire. Cet assistant permet de définir une ou plusieurs chaînes de texte qui doivent être présentes (ou absentes) sur les écrans d'un formulaire de gestion des informations d'identification de l'application d'émulateur de terminal (authentification, modification de mot de passe, modification de mot de passe réussie, échec de la modification de mot de passe).

À mesure que vous vous déplacez dans le formulaire de gestion des informations d'identification défini, enregistrez toutes les actions utilisateur requises pour accéder au formulaire. Ces actions doivent être fournies dans la définition de chaque formulaire lorsque vous exécutez l'assistant de définition de formulaire à partir de la console ou de l'outil de définition d'application.

Lorsque vous avez identifié le formulaire correct, les coordonnées des champs de saisie des données utilisés pour soumettre les informations d'identification appropriées à l'application sont définies. Celles-ci sont définies en spécifiant la séquence d'actions ou de touches requises pour se déplacer entre les champs ou les écrans et pour entrer du texte.

Processus de définition de formulaire

Oct 21, 2015

Pour les applications Windows, le processus de définition de formulaire consiste à rassembler des informations d'identification spécifiques au formulaire et des informations d'actions à l'aide des pages suivantes de l'assistant de définition de formulaire pour applications Web :

- Nom du formulaire
- Identification du formulaire
- Autres réglages
- Confirmation des réglages

Lorsque vous avez effectué les actions requises dans une page spécifique, cliquez sur Suivant pour passer à l'étape suivante de l'assistant. Le bouton Précédent est généralement disponible sur chaque page pour revenir à certaines options configurées précédemment. Toutefois, pour modifier certaines options que vous avez configurées précédemment, il peut être nécessaire de modifier d'autres paramètres.

Nom du formulaire

Lorsque vous créez des définitions d'application pour des applications de type émulateur de terminal (HLLAPI), la page Nom du formulaire de l'assistant de définition de formulaire vous permet d'effectuer les opérations suivantes :

- affecter un nom défini par l'utilisateur au formulaire créé ;
- définir le type du formulaire créé.

Notez que le nom attribué au formulaire s'affiche dans la page Gestion des formulaires de l'assistant de définition d'application. Choisissez un nom approprié pour le type de formulaire défini.

L'assistant de définition de formulaire permet de définir plusieurs types de formulaires de gestion des informations d'identification standard

- Formulaire d'authentification
  Il permet de définir l'interface d'authentification d'une application et de gérer les actions de soumission d'informations d'identification requises pour accéder à l'application associée.

- Formulaire de modification de mot de passe
  Il permet de définir l'interface de modification du mot de passe d'une application et de gérer les actions de soumission d'informations d'identification requises pour changer le mot de passe utilisateur permettant d'accéder à l'application.

- Formulaire de modification de mot de passe réussie
  Il permet de définir l'interface de modification du mot de passe d'une application et de gérer les actions de soumission d'informations d'identification requises pour confirmer la réussite du changement du mot de passe utilisateur permettant d'accéder à l'application.

- Formulaire d'échec de modification de mot de passe
  Il permet de définir l'interface indiquant l'échec du changement du mot de passe et de définir les actions à effectuer dans ces cas.

Les versions 4.0 et 4.1 de l'Agent Password Manager ne prennent pas en charge les formulaires d'échec ou de réussite de modification des informations d'identification et ne répondent pas aux définitions d'application contenant ces formulaires.

Si l'émulateur de terminal utilisé affiche plus d'une page d'ouverture de session ou de modification de mot de passe, vous

devez créer un formulaire pour chaque page.

Identification du formulaire

Lorsque vous créez des définitions pour des applications de type émulateur de terminal (HLLAPI), la page Identification du formulaire vous permet de fournir des informations requises pour que Single Sign-On Plug-in puisse reconnaître sans équivoque le formulaire défini.

Les applications d'émulateur sont identifiées en recherchant des chaînes de texte qui s'affichent sur des lignes et des colonnes spécifiées dans la page de l'application d'émulateur de terminal. Vous devez uniquement définir un nombre suffisant de correspondances de chaînes de texte pour permettre d'identifier l'hôte.

Pour ajouter une entrée de qualification de correspondance de texte

1. Assurez-vous que l'application d'émulateur de terminal est lancée et que vous avez déjà déterminé les chaînes de texte à utiliser pour identifier l'application cible.
2. Sur la page Identification du formulaire de l'assistant de définition de formulaire, cliquez sur Ajouter pour ajouter une nouvelle entrée de correspondance de texte à la liste des entrées utilisées pour identifier l'application. Cette action ouvre la boîte de dialogue Texte à rechercher.
3. Renseignez les champs suivants de la boîte de dialogue Texte à rechercher :
   - Chaîne de texte
     Entrez le texte exact qui doit être utilisé pour identifier l'application.
   - Ligne
     Entrez le numéro de ligne exact de la chaîne.
   - Colonne
     Entrez le numéro de colonne exact de la chaîne.

   Remarque : lorsque le plug-in analyse une application d'émulateur de terminal, il examine l'écran pour rechercher la chaîne de texte exacte à l'emplacement de ligne et de colonne défini. Si le texte situé aux coordonnées définies ne correspond pas au texte spécifié, l'écran est ignoré.
4. Cliquez sur OK. L'entrée Texte à rechercher définie s'affiche dans la page Identification du formulaire.

Il est souvent nécessaire de définir plusieurs chaînes de texte pour permettre d'identifier l'application hôte cible. Si des chaînes de texte à rechercher supplémentaires sont requises, répétez les étapes 2 à 4 pour chaque chaîne.

Définition des règles de détection de champ

La page Définition des règles de détection de champ permet d'indiquer l'emplacement et les actions clé requises pour gérer le formulaire d'informations d'identification défini.

L'objectif est de créer des entrées de champ qui indiquent les informations d'identification à traiter, l'emplacement où elles doivent être insérées à l'écran (coordonnées de lignes et de colonnes) et les touches requises pour faire avancer le curseur vers l'information suivante ou le bouton de soumission.

Pour ajouter une entrée de champ

1. Cliquez sur Ajouter pour ouvrir la boîte de dialogue Définition du champ.
2. Renseignez les champs suivants de la boîte de dialogue Définition du champ :
   - Fonction du champ
     Sélectionnez les informations d'identification à soumettre dans la zone de liste déroulante.

- Ligne
  Entrez le numéro de ligne exact de la chaîne.
- Colonne
  Entrez le numéro de colonne exact de la chaîne.
- Frappes après
  Entrez les codes de touches requis pour déplacer le curseur vers le champ d'informations d'identification suivant ou pour effectuer l'action de soumission des informations.

Remarque : sélectionnez le lien Code clavier virtuel pour accéder aux informations d'aide sur les codes clavier valides.

3. Cliquez sur OK. L'entrée de champ définie s'affiche sur la page Définition des règles de détection de champ.
4. Répétez les étapes 1 à 3 pour chaque champ requis pour le formulaire défini.
5. Les entrées de champ affichées dans la page Définition des règles de détection de champ sont traitées de haut en bas telles qu'elles apparaissent sur la page. Utilisez les flèches haut et bas pour organiser les entrées selon la séquence requise par le formulaire d'informations d'identification défini.

Autres réglages

La page Autres réglages vous permet d'accéder aux options de paramètres avancés pour le formulaire défini. Les paramètres avancés permettent de :

- définir une pause avant le traitement initial du formulaire ;
- définir les touches requises pour accéder au formulaire de gestion des informations d'identification défini ;
- définir les critères de correspondance de chaîne de texte indiquant au plug-in d'ignorer le traitement.

Si une configuration avancée supplémentaire est requise pour le formulaire défini, cliquez sur Avancé pour ouvrir la boîte de dialogue Paramètres avancés.

Paramètres avancés pour applications d'émulateur de terminal

Oct 21, 2015

Certaines applications d'émulateur de terminal requièrent une configuration supplémentaire pour faire en sorte que le formulaire d'informations d'identification correct soit identifié. Cette configuration peut définir :

- d'attendre un intervalle de temps défini que l'application d'émulateur de terminal soit lancée avant de tenter d'identifier l'application ;
- de traiter une série de touches pour naviguer vers la page d'authentification initiale ou la page de modification de mot de passe ;
- d'ignorer le traitement d'une page lorsqu'une chaîne de texte spécifique apparaît.

Si des paramètres de configuration avancés sont requis pour un formulaire de gestion des informations d'identification, cliquez sur Avancé dans la page Autres réglages de l'assistant de définition de formulaire pour ouvrir la boîte de dialogue Paramètres avancés.

La boîte de dialogue Paramètres avancés contient deux pages de configuration accessibles à partir du volet gauche de la page :

- Mettez en surbrillance l'option Paramètres supplémentaires des formulaires d'hôte pour accéder aux options Paramètres supplémentaires :
  - Retarder les entrées des champs (ms). Entrez la période de temps (en millisecondes) pendant laquelle le traitement du formulaire doit être retardé pendant que l'application est chargée.
  - Frappes préliminaires. Entrez les codes de touches virtuels qui doivent être entrés pour accéder au premier champ du formulaire de gestion des informations d'identification traité. Sélectionnez le lien Code clavier virtuel pour accéder aux informations d'aide sur les codes clavier valides.
- Mettez en surbrillance l'option Texte à ignorer pour accéder à l'option Texte bloquant la soumission des informations d'identification. Cette option permet de spécifier des chaînes de texte qui apparaissent dans la page de l'application pour les formulaires qui doivent être ignorés.

Considérations de définitions de type d'émulateur de terminal

Oct 21, 2015

Tenez compte des facteurs suivants lorsque vous définissez des définitions d'application de type émulateur de terminal (HLLAPI) :

- La prise en charge de l'émulation de terminal doit être activée pour chaque configuration utilisateur utilisant des applications d'émulateur de terminal.
- Vérifiez que votre programme d'émulateur de terminal est conforme à HLLAPI.
- Vérifiez que votre programme d'émulateur de terminal est défini dans le fichier mfrmlist.ini du plug-in.
- Vous pouvez gagner du temps en utilisant un émulateur de terminal qui indique les coordonnées de ligne et de colonne de la position du curseur. Ceci vous permet de déterminer plus facilement l'emplacement du texte et des champs utilisés pour identifier l'application hôte et ses formulaires d'authentification.
- Pour la détection HLLAPI, l'émulateur doit définir un nom court pour chaque session. Le plug-in ne peut pas détecter d'application sans le nom court de session de l'émulateur de terminal.
- La documentation relative à votre application d'émulateur de terminal peut inclure des identificateurs uniques, tels que des numéros d'écrans, pour les écrans utilisés pour soumettre les informations d'identification. Dans ce cas, utilisez le numéro d'écran comme identificateur unique pour faire en sorte que le plug-in puisse identifier et soumettre les informations d'identification au formulaire correct.

Prise en charge de l'émulation de terminal

Oct 21, 2015

Les émulateurs de terminal pris en charge sont inclus dans le fichier Mfrmlist.ini. Ce fichier représente tous les émulateurs de terminal qui ont été testés par Citrix.

Il est possible d'ajouter des émulateurs de terminal à cette liste. Cependant, il est recommandé de tester et de vérifier ces définitions avant de les introduire dans votre environnement de production. Un exemple d'une section de ce fichier figure ci-dessous.

```
[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=Re
```

Les entrées d'émulateur de terminal de la section [Emulators] du fichier Mfrmlist.ini doivent suivre une séquence numérique, de EMU1 à EMU99. Toute rupture de la séquence entraîne la fin du processus ssomho.exe avant la lecture de toutes les entrées.

La suppression ou l'ajout de marque de commentaire pour des émulateurs inutilisés permet parfois d'améliorer le démarrage. Ssomho.exe ne recherche pas l'emplacement de DLL HLLAPI inutilisées (économie de ressources et de temps).

Pour placer un commentaire devant une entrée, déplacez celle-ci vers le bas de la liste, faites-la précéder d'un point virgule, puis renumérotez les entrées EMU restantes pour éviter une rupture de la séquence.

Single Sign-On ne peut pas mettre à jour le fichier mfrmlist.ini. Vous devez le modifier manuellement après installation du plug-in. Pour les déploiements à grande échelle, pensez à utiliser des fichiers de traitement par lot ou des scripts exécutés lors de l'installation avec SMS (System Management Server), CA-Unicenter ou Active Directory.

Définition de champs dans mfrmlist.ini

Oct 21, 2015

Les émulateurs de terminal ajoutés au fichier Mfrmlist.ini fonctionnent uniquement s'ils sont conformes à la norme HLLAPI. Les définitions de champ du fichier mfrmlist.ini figurent ci-dessous. Si vous devez ajouter une définition d'émulateur de terminal, vérifiez auprès du fabricant de l'émulateur de terminal s'il prend en charge HLLAPI et obtenez les entrées de définition de champ correctes. Pour déterminer si un émulateur de terminal fonctionne avec Single Sign-On, testez-le en dehors de votre environnement de production.

Champ	**Définitions**
[EmulatorName]	La valeur de EmulatorName doit correspondre à la valeur de la ligne EMUnn=EmulatorName dans la section [Emulators].
GroupName	Utilisation interne seulement.
DisplayName	Nom affiché de l'émulateur de terminal. Il s'agit d'un des deux paramètres utilisés lors de la création d'un nouveau processus pour gérer la session. Il doit être unique dans le fichier mfrmlist.ini.
RegistryLoc	Cette clé de registre de HKEY_LOCAL_MACHINE\SOFTWARE pointe vers le chemin d'accès de stockage du fichier DLL HLLAPI. Si le programme ne stocke pas ces informations dans HKEY_LOCAL_MACHINE\SOFTWARE, utilisez le paramètre ExplicitPath au lieu de RegistryLoc. Si RegistryLoc et ExplicitPath sont définis, le paramètre ExplicitPath a préséance.
ExplicitPath	Le chemin d'accès absolu du fichier DLL HLLAPI utilisé par cet émulateur. Ce paramètre est utilisé au lieu du paramètre RegistryLoc lorsque l'émulateur ne stocke pas l'emplacement du fichier DLL HLLAPI dans le registre. Si RegistryLoc et ExplicitPath sont définis, le paramètre ExplicitPath a préséance.
ValueName	Nom de la valeur de la clé RegistryLoc contenant le chemin d'accès.
DLLFile	Nom du fichier DLL HLLAPI
StripFileName	Indique que la valeur stockée dans ValueName contient des barres obliques inverses (\) à supprimer lors de l'assemblage du chemin d'accès du fichier DLL HLLAPI à partir des entrées ValueName et DLL File.
IntSize	Définit la taille (entier) prise en charge par l'émulateur de terminal : 16 bits ou 32 bits.
WindowClass	Nom de la classe de fenêtre pour l'émulateur de terminal. Obtenu dans la console Single Sign-On ou l'Outil de définition d'application.
WindowTitle	Une partie du titre de fenêtre pouvant être utilisée par Single Sign-On pour assurer que cette fenêtre est associée à l'émulateur de terminal. Elle doit contenir au moins un mot qui sera toujours présent dans le nom de fenêtre. Des caractères

Champ	Définitions
	génériques sont placés automatiquement des deux côtés du texte.
UseSendKeys	Indique à Single Sign-On qu'il doit utiliser l'envoi de frappes clavier pour communiquer avec l'émulateur de terminal. Cette option n'est pas la même que celle utilisée pour les applications Windows.

Création de configurations utilisateur

Oct 21, 2015

Une configuration utilisateur vous permet de contrôler le comportement et l'aspect du plug-in au niveau des utilisateurs. La création d'une ou plusieurs configurations utilisateur est la dernière étape à suivre avant de distribuer Single Sign-On Plug-in auprès des utilisateurs de votre environnement. Notez que vous pouvez ajouter ou modifier à tout moment les configurations utilisateur existantes.

Une configuration utilisateur constitue une collection unique de réglages, stratégies de mot de passe et applications que vous appliquez à des utilisateurs associés à une hiérarchie Active Directory (une unité organisationnelle ou un utilisateur) ou à un groupe Active Directory.

Une configuration utilisateur comporte les éléments suivants :

- les utilisateurs associés à une hiérarchie de domaine Active Directory (unité organisationnelle ou utilisateur) ou à un groupe Active Directory ;
  Important : les groupes de distribution et les groupes locaux de domaine en mode Active Directory mixte ne sont pas pris en charge ;
- le type de licence et les paramètres concernés relatifs aux utilisateurs (modèle simultané ou de licences utilisateurs désignés) ;
- les méthodes de protection des données ;
- les définitions d'application créées, que vous pouvez combiner dans un groupe d'applications lors de la création d'une configuration utilisateur ;
- les stratégies de mot de passe associées à des groupes d'applications ;
- les fonctions autonomes (déverrouillage de compte et réinitialisation de mot de passe) et les options de gestion de clés (utilisation du mot de passe précédent, questions de sécurité et gestion automatique des clés) ;
- les paramètres des options tels que l'habilitation et la prise en charge d'applications.

Avant de créer vos configurations utilisateur, assurez-vous que vous avez déjà créé ou défini les éléments suivants :

- Magasin central
- Définitions d'application
- Stratégies de mot de passe
- Questions de sécurité

Vous devez créer des configurations utilisateur avant de déployer Single Sign-On Plug-in vers vos utilisateurs. Entre autres paramètres, une configuration utilisateur contient le serveur et les informations de licences requis pour le fonctionnement du plug-in.

Pour obtenir les détails des paramètres par défaut, consultez les rubriques situées sous
— Liste de référence des paramètres de Single Sign-On > Configurations de l'utilisateur
.

Pour spécifier un contrôleur de domaine pour une configuration utilisateur existante

Dans les environnements où vous utilisez un magasin central Active Directory avec plus d'un contrôleur de domaine, vous pouvez sélectionner le contrôleur de domaine auquel vous souhaitez lier les configurations utilisateur lors des écritures dans le magasin central.

Ce schéma de liaison permet de réduire les délais de synchronisation engendrés par la réplication Active Directory. Ce type de délais peut apparaître dans les environnements où les utilisateurs accèdent simultanément à Single Sign-On dans plusieurs sites Active Directory.

Au cours du processus de découverte offert par la console, Single Sign-On peut détecter tous les contrôleurs de votre domaine. Vous pouvez lier les configurations utilisateur que vous avez créées à un contrôleur de domaine spécifique en sélectionnant ce contrôleur lors de la création d'une configuration utilisateur.

Par exemple, vous pouvez demander la liaison des utilisateurs à un contrôleur de domaine dans leur réseau local. Une fois que vous avez spécifié un contrôleur de domaine, les utilisateurs y sont liés lors de leur prochaine connexion à Single Sign-On.

Par défaut, les utilisateurs sont liés à n'importe quel contrôleur de domaine autorisant l'écriture jusqu'à ce que vous ayez sélectionné un contrôleur de domaine auquel ils doivent être liés. Vous pouvez à tout moment modifier le paramètre de contrôleur de domaine en mettant à jour la configuration utilisateur selon vos besoins sans pour autant mettre en péril l'intégrité des données des utilisateurs.

Remarque : lorsque vous choisissez un contrôleur de domaine de liaison, vérifiez que les ressources disponibles sur le contrôleur de domaine peuvent accepter le trafic de communications généré par les utilisateurs lorsqu'ils se connectent au contrôleur de domaine en période d'utilisation intense.
Si le contrôleur de domaine spécifié est indisponible ou hors connexion, le plug-in utilise les données utilisateur du magasin local (c'est-à-dire les données utilisateur situées sur l'ordinateur de l'utilisateur). Si le contrôleur de domaine est hors connexion sur une longue période (selon vos paramètres), vous pouvez sélectionner la tâche Modifier la configuration utilisateur dans la console et choisir un autre contrôleur de domaine ou l'option Tout contrôleur de domaine autorisant l'écriture.

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. Sélectionnez une configuration utilisateur.
4. Dans le menu Action, sélectionnez Modifier la configuration utilisateur.
5. Sélectionnez Contrôleur de domaine dans la liste d'options sur le côté gauche de la page de l'assistant Modifier la configuration utilisateur.
6. Sélectionnez un contrôleur de domaine disponible ou Tout contrôleur de domaine autorisant l'écriture.

Pour créer une configuration utilisateur

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix Delivery Services Console.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. À partir du menu Action, cliquez sur Ajouter une nouvelle configuration utilisateur.

Définition d'un nom pour vos configurations utilisateur

La page Nom de la configuration utilisateur de l'assistant de configuration utilisateur vous permet de nommer votre configuration utilisateur et de choisir de quelle manière vous associerez la configuration utilisateur aux utilisateurs.

- Name
  Pensez à nommer la configuration utilisateur en fonction de la façon dont vous envisagez de regrouper vos utilisateurs et de les associer à des applications spécifiques. Par exemple, Utilisateurs Marketing, Utilisateurs Développement de logiciels, Utilisateurs France, etc.

- Association de configuration utilisateur
  Vous disposez de deux options d'association des utilisateurs : à une hiérarchie de domaine Active Directory (unité organisationnelle ou utilisateur) ou à un groupe Active Directory. Si nécessaire, vous pourrez associer la configuration utilisateur à une autre hiérarchie ou un autre groupe plus tard, en cliquant sur Déplacer la configuration utilisateur dans le menu Action.

  Important : le mode d'organisation de votre environnement Active Directory peut affecter le fonctionnement des configurations utilisateur. Si vous utilisez les deux (une hiérarchie et des groupes Active Directory) et qu'un utilisateur se trouve dans les deux conteneurs, la configuration utilisateur associée à la hiérarchie a priorité et sera celle utilisée. Ce schéma est appelé environnement mixte.
  En outre, si un utilisateur appartient à deux groupes Active Directory et que chaque groupe est associé à une configuration utilisateur, la configuration qui possède le plus haut niveau de priorité sera celle utilisée.

  L'association de configurations utilisateur à des groupes n'est prise en charge que dans des domaines Active Directory utilisant l'authentification Active Directory.

Spécification d'un contrôleur de domaine

Si vous utilisez un magasin central Active Directory, la page Définition du serveur de synchronisation de l'assistant de configuration utilisateur vous permet de sélectionner un contrôleur de domaine disponible ou de sélectionner Tout contrôleur de domaine autorisant l'écriture.

Choisir des applications et configurer des paramètres utilisateur

Oct 21, 2015

Dans la page Choix d'applications de l'assistant de configuration utilisateur, ajoutez les applications de la configuration utilisateur. Lorsque vous cliquez sur le bouton Ajouter, une boîte de dialogue contenant les définitions d'applications que vous avez créées précédemment s'affiche. Vous pouvez alors combiner ces définitions d'applications à un groupe d'applications. Un groupe d'applications peut contenir une ou plusieurs applications.

Vous pouvez également convertir le groupe d'applications en un groupe de partage de mot de passe pour automatiser et simplifier le processus de modification des mots de passe. En cas de modification du mot de passe d'une définition d'application appartenant à un groupe de partage de mot de passe, le plug-in s'assure que la modification de mot de passe est prise en compte dans les informations d'identification stockées pour toutes les applications du groupe.

Les groupes de partage de mot de passe permettent au plug-in de gérer plusieurs combinaisons d'informations d'identification pour des applications utilisant la même autorité d'authentification. Par exemple, si vous disposez de deux applications utilisant la même base de données Oracle pour l'authentification (telles qu'une application de gestion financière et une application de gestion des ressources humaines), vous pouvez les placer dans le même groupe de partage de mot de passe. Si vos utilisateurs modifient leur mot de passe pour l'une de ces applications, ceux de l'autre application sont automatiquement mis à jour.

Important : pour optimiser les résultats, assurez-vous que tous les mots de passe compris dans le groupe de partage sont gérés par une autorité d'authentification commune. Par exemple, vous mettez en œuvre un groupe de partage de mot de passe si les applications d'un groupe de partage utilisent une autorité d'authentification principale commune, telle qu'une base de données, où l'utilisateur soumet les mêmes informations d'identification à chaque application pour l'authentification à la base de données. Vous ne regroupez pas des applications non liées, telles qu'un programme de messagerie, une application Web et un Single Sign-on activé sur votre réseau Intranet, où un utilisateur peut éventuellement soumettre trois ensembles différents d'informations d'identification mais utilise seulement par hasard les mêmes informations d'identification pour les trois applications. Dans ce cas, si un utilisateur modifie des informations d'identification pour une application dans ce groupe de partage de mot de passe, elles ne seront pas obligatoirement valides pour les deux autres applications.

Configurer les réglages utilisateur

Utilisez les pages suivantes pour configurer les paramètres utilisateur. Pour obtenir les détails des paramètres, consultez les rubriques situées sous

— Liste de référence des paramètres de Single Sign-On > Configurations de l'utilisateur

.

- La page Configurer l'interaction de Single Sign-On Plug-in de l'assistant de configuration utilisateur vous permet de déterminer l'expérience de tous les utilisateurs du plug-in dans votre environnement.
- Sélectionnez un serveur de licence et un modèle de système de licences dans la page Configuration du système de licences de l'assistant de configuration utilisateur.
  Important : si vous modifiez ultérieurement la configuration utilisateur et que vous modifiez les éditions des produits, votre modèle de licences change. Par exemple, passer de l'édition Single Sign-On Enterprise à l'édition Single Sign-On Advanced entraîne le changement de votre modèle de licences du modèle Utilisateurs simultanés à Utilisateur désigné.
- La page Sélection des méthodes de protection des données de l'assistant de configuration utilisateur vous permet de sélectionner les méthodes de protection des informations d'identification des utilisateurs en fonction des différentes

méthodes d'authentification autorisées pour vos utilisateurs. Dans certains environnements, les utilisateurs peuvent appliquer plus d'une méthode.

- Lorsque les utilisateurs modifient leur méthode d'authentification principale (par exemple, modification de mot de passe de domaine ou remplacement de carte à puce), la page Sélection de la protection secondaire des données de l'assistant de configuration utilisateur vous permet d'obliger les utilisateurs à s'authentifier de nouveau et à vérifier leur identité avant de déverrouiller leurs informations d'identification d'application. Grâce à elle, vous pouvez également demander à vos utilisateurs de confirmer leur identité pour améliorer la sécurité. En outre, elle vous permet de spécifier la restauration automatique des informations d'identification en mettant en œuvre le module de gestion des clés.
- Les options disponibles dans la page Fonctions autonomes de compte de l'assistant de configuration utilisateur nécessitent l'installation du module de gestion des clés. Cette fonctionnalité ajoute un bouton Fonctions autonomes de compte aux boîtes de dialogue d'ouverture de session Windows et Déverrouillage de l'ordinateur et permet de réduire les coûts relatifs aux interventions des administrateurs ou de l'assistance technique dans votre entreprise.
- Les pages Module de gestion des clés et Module d'habilitation de l'assistant de configuration utilisateur nécessitent que vous indiquiez l'URL et le port du service de tout module de service installé.

Synchronisation des informations d'identification à l'aide de la fonction Association de comptes

Oct 21, 2015

Dans les entreprises pouvant maintenir plusieurs domaines Windows, les utilisateurs peuvent posséder plus d'un compte Windows. Single Sign-On comprend un service dénommé Synchronisation des informations d'identification pour autoriser l'Association de comptes.

La fonction Association de comptes permet à un utilisateur de se connecter à n'importe quelle application à l'aide d'un compte Windows ou plus. Dans la mesure où Single Sign-On lie généralement les informations d'identification d'utilisateur à un seul compte, ces informations ne sont pas automatiquement synchronisées entre les différents comptes que peut posséder un utilisateur. Toutefois, les administrateurs peuvent configurer la fonction Association de comptes de manière à synchroniser les informations d'identification des utilisateurs. Les utilisateurs bénéficiant de la fonction Association de comptes peuvent accéder à toutes les applications à partir de n'importe lequel de leurs comptes dans leur environnement Single Sign-On. Lors de la modification, de l'ajout ou de la suppression d'informations d'identification dans un compte, elles sont automatiquement synchronisées avec chacun des comptes associés à l'utilisateur.

Sans la fonction Association de comptes, une personne possédant plusieurs comptes Windows doit modifier manuellement ses informations de connexion séparément dans chaque compte Windows.

Pour configurer la fonction Association de comptes, les administrateurs du domaine Windows de l'entreprise doivent procéder aux opérations suivantes, selon cet ordre :

1. Choisir un domaine dans lequel installer et exécuter le module de synchronisation des informations d'identification, qui fait partie du service Single Sign-On.
2. Déployer le certificat racine de confiance sur tous les ordinateurs de l'entreprise qui doivent utiliser la fonction Association de comptes.
3. Synchroniser manuellement les définitions d'application entre les domaines.
4. Configurer les paramètres utilisateur de l'Association de compte dans les autres domaines, pour la connexion au module de synchronisation des informations d'identification.
5. Mettez l'outil Association de comptes à la disposition des utilisateursen tant qu'application publiée.

Chaque utilisateur doit activer la fonction Association de comptes dans Single Sign-on Plug-in.

Choix et configuration d'un domaine pour l'hébergement du module de synchronisation des informations d'identification

Choisissez le domaine qui contient les comptes de tous les utilisateurs de votre entreprise qui vont utiliser la fonction Association de comptes. Le module de synchronisation des informations d'identification fait office de concentrateur pour toutes les informations d'identification au sein de l'entreprise. Installez ce module dans ce domaine de la même manière qu'un autre service Single Sign-On.

Important : contactez votre administrateur réseau pour décider s'il est nécessaire d'apporter des modifications au pare-feu et si ces modifications sont compatibles avec les stratégies de votre entreprise.
Une fois le module de synchronisation des informations d'identification installé, créez ou modifiez les configurations utilisateur à partir de Citrix AppCenter de manière à autoriser les comptes des utilisateurs individuels à utiliser le module de synchronisation, comme suit.

Pour configurer les fonctions de synchronisation des informations d'identification dans le domaine hôte

Ouvrez la console à partir du domaine hébergeant le module de synchronisation des informations d'identification. Certains domaines peuvent accéder à plusieurs magasins centraux. Assurez-vous que la console que vous utilisez est configurée pour une connexion au même magasin central que le module de synchronisation des informations d'identification.

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. Sélectionnez une configuration utilisateur existante ou créez-en une nouvelle.
   - Si vous créez une nouvelle configuration utilisateur, vous pouvez accéder aux options suivantes à l'aide du bouton Paramètres avancés de la page Configurer l'interaction du plug-in de l'assistant de configuration utilisateur.
   - Si vous modifiez une configuration utilisateur existante, les options suivantes sont disponibles dans la page de propriétés Modification de la configuration utilisateur.
4. Cliquez sur Synchronisation et sélectionnez Permettre l'accès aux informations d'identification par le module de synchronisation des informations d'identification.
5. Cliquez sur OK et répétez les étapes 3 et 4 pour chaque configuration utilisateur (nouvelle et existante).

Pour synchroniser manuellement les définitions d'application entre les domaines

les comptes peuvent également être synchronisés entre différentes associations de configurations utilisateur. Par exemple, une configuration utilisateur peut être associée à une hiérarchie Active Directory (unité organisationnelle ou utilisateur) dans un domaine et à un groupe Active Directory dans un autre domaine. Tant que les noms de définition d'application sont identiques dans chaque configuration utilisateur, la fonction Association de comptes est en mesure de synchroniser les informations d'identification.

Les informations d'identification ne sont partagées que pour les applications définies par l'administrateur Single Sign-On. Les administrateurs doivent s'assurer que chaque définition d'application de chaque domaine porte le même nom dans chaque magasin central.

Par exemple, si la définition d'application de SAP est nommée Connexion SAP sur un domaine, SAP sur un autre, et Lancement SAP sur un troisième, les informations d'identification pour ces applications ne seront pas synchronisées sur les comptes de ces domaines.

Lorsque vous créez une nouvelle définition d'application sur des domaines, il est fortement recommandé d'exécuter les tâches Exporter les informations d'administration et Importer les informations d'administration dans la console. Elles vous permettront d'exporter les définitions d'application nouvellement créées à importer dans chaque magasin central. Vous devez également renommer manuellement les applications existantes, déjà définies.

Pour configurer les paramètres utilisateur de l'Association de compte dans les autres domaines

Installez et ouvrez la console à partir d'un poste de travail dans chaque domaine qui n'héberge pas le module de synchronisation des informations d'identification. Certains domaines possèdent plusieurs magasins centraux. N'oubliez donc pas de configurer chaque magasin central.

Tous les administrateurs de domaines doivent autoriser les utilisateurs à associer leurs comptes à leur compte de domaine hôte. Modifiez en conséquence la section Association de comptes des configurations utilisateur voulues dans la console.

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. Sélectionnez une configuration utilisateur existante ou créez-en une nouvelle.
   - Si vous créez une nouvelle configuration utilisateur, vous pouvez accéder aux options suivantes à l'aide du bouton Paramètres avancés de la page Configurer l'interaction du plug-in de l'assistant de configuration utilisateur.
   - Si vous modifiez une configuration utilisateur existante, les options suivantes sont disponibles dans la page de propriétés Modification de la configuration utilisateur.
4. Cliquez sur Association de comptes.
5. Sélectionnez Permettre aux utilisateurs d'associer des comptes.
   Les options suivantes ne sont pas obligatoires, mais elles contribuent à améliorer l'expérience des utilisateurs.
6. Sélectionnez Fournir une adresse du service par défaut et entrez l'adresse du service Single Sign-On et le port du domaine hébergeant le module de synchronisation des informations d'identification.
7. Désélectionnez l'option Permettre aux utilisateurs de modifier l'adresse du service.
8. Sélectionnez Fournir le domaine par défaut et tapez le nom du domaine hébergeant le module de synchronisation des informations d'identification. Si vous n'indiquez pas de domaine, les utilisateurs pourraient avoir des incertitudes quant aux informations d'identification de compte de domaine ils doivent fournir.
9. Désélectionnez l'option Permettre aux utilisateurs de modifier le domaine.
10. En fonction des stratégies de sécurité de votre entreprise, sélectionnez Permettre aux utilisateurs de garder le mot de passe en mémoire.
11. Cliquez sur OK et répétez l'opération pour chaque configuration utilisateur.

Publication de l'outil Association de comptes

Cette version de Single Sign-on Plug-in ne fournissant pas d'option de menu permettant aux utilisateurs d'activer l'Association de comptes, vous offrez un outil aux utilisateurs pour activer l'Association de comptes en tant qu'application publiée :

1. Installez Single Sign-on Plug-in sur un serveur XenApp.
2. Situez le fichier AccAssoc.exe sur le serveur XenApp.
3. Publiez le fichier AccAssoc.exe et mettez-le à la disposition des utilisateurs.
4. Informez les utilisateurs de la manière d'accéder à l'outil Association de comptes et de l'utiliser.

Remarque : les utilisateurs exécutant Single Sign-on Plug-in versions 4.8 et antérieures peuvent utiliser une option de menu de plug-in pour activer l'outil Association de comptes. Ces utilisateurs ne requièrent pas accès à l'outil Association de comptes en tant qu'application publiée.

Pour activer la fonction Association de comptes dans Single Sign-on Plug-in

Oct 21, 2015

Lors de leur connexion au domaine hébergeant le module de synchronisation des informations d'identification, les utilisateurs n'ont pas besoin d'intervenir pour que la fonction Association de comptes soit activée. Ces comptes tiennent le rôle de magasin central des informations d'identification des utilisateurs.

Lors de l'ouverture de session sur d'autres domaines, les utilisateurs peuvent activer l'Association de compte de deux manières différentes, selon la version de Single Sign-on Plug-in utilisée :

- Pour cette version de Single Sign-on Plug-in, les utilisateurs accèdent à l'outil Association de comptes en tant qu'application publiée. Vous publiez l'outil d'Association de compte et indiquez aux utilisateurs comment y accéder et l'utiliser.
- Pour Single Sign-on Plug-in versions 4.8 et antérieures, les utilisateurs désormais voient l'option Association de compte s'afficher sous le menu Outils dans le Gestionnaire d'informations d'identification du logiciel du plug-in. Les utilisateurs doivent sélectionner cette option pour configurer l'Association de comptes.

1. Suivant la version du plug-in utilisée, les utilisateurs accèdent à l'outil Association de comptes en tant qu'application publiée ou sélectionnent Outils > Association de comptes depuis le Gestionnaire d'informations d'identification. La boîte de dialogue Association de comptes s'affiche.
2. Les utilisateurs sélectionnent Activer l'association de comptes.
   Remarque : si vous n'avez pas indiqué l'adresse du service qui héberge le module de synchronisation des informations d'identification, les utilisateurs doivent l'indiquer dans la zone de texte. Si ce champ n'est pas disponible, cela signifie que vous avez déjà saisi cette adresse de service et que les utilisateurs ne peuvent pas entrer de données dans ce champ.
3. Les utilisateurs cliquent sur OK. La boîte de dialogue Authentification pour association de comptes s'affiche.
4. Les utilisateurs tapent le nom d'utilisateur et le mot de passe du compte Windows associé à l'utilisateur. Si le domaine d'installation du module de synchronisation des informations d'identification ne s'affiche pas, les utilisateurs le saisissent dans le champ Domaine.
   Remarque : si vous avez spécifié le nom de domaine, les utilisateurs ne peuvent pas entrer de texte dans ce champ.
5. Les utilisateurs cliquent sur OK. L'association de comptes est maintenant activée. Les informations d'identification sont synchronisées en même temps que le plug-in.

Gestion des configurations utilisateur

Oct 21, 2015

L'authentification unique (Single Sign-On) vous permet de gérer les configurations utilisateur. Vous pouvez :

- Réinitialiser les données utilisateur
- Supprimer les données utilisateur
- Inviter les utilisateurs à s'enregistrer de nouveau
- Définir la priorité de la configuration utilisateur
- Assigner la configuration utilisateur à d'autres utilisateurs
- Mettre à niveau la configuration d'utilisateurs existants

Pour réinitialiser les données utilisateur

L'opération Réinitialiser les données utilisateur nécessite préalablement l'installation et la configuration du module d'habilitation.

Réinitialiser les données utilisateur vous permet de réinitialiser les informations des utilisateurs dans votre magasin central, ce qui retourne l'utilisateur sélectionné à son état initial.

- Dans les magasins centraux Active Directory, les données des utilisateurs (informations d'identification, questions et réponse de sécurité, etc.) sont alors supprimées et l'utilisateur est signalé comme possédant des données réinitialisées.
- Dans les magasins centraux de partage réseau NTFS, les dossiers des utilisateur sont conservés, toutes les données utilisateur sont supprimées et l'utilisateur est signalé comme possédant des données réinitialisées.

Vous pouvez utiliser la fonction Réinitialiser les données utilisateur si des utilisateurs oublient les réponses à leurs questions de sécurité ou pour réinitialiser leurs informations d'identification en cas d'altération des données de l'utilisateur. Lorsque l'utilisateur contacte ultérieurement le magasin central à l'aide du plug-in, toutes les données du magasin local d'informations d'identification de l'utilisateur sont supprimées et il doit de nouveau s'enregistrer.

Cette opération est également utile lorsqu'un utilisateur ne peut pas se connecter au plug-in.

Important : l'historique du mot de passe est enregistré utilisateur par utilisateur. Si vous réinitialisez les données d'un utilisateur, son historique de mot de passe est supprimé et l'historique ne peut pas être appliqué pour les mots de passe supprimés.

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. À partir du menu Action, cliquez sur Autres tâches > Réinitialiser les données utilisateur. La boîte de dialogue Sélectionner Utilisateur s'affiche.
4. Tapez un nom d'utilisateur dans la zone de texte et cliquez sur Vérifier les noms.
5. Si vous obtenez un résultat, cliquez sur OK.
6. Sélectionnez un utilisateur dans votre magasin central et cliquez sur Réinitialiser.
7. Cliquez sur OK. Un message d'avertissement s'affiche.
8. Vérifiez que tous les utilisateurs susceptibles d'exécuter Single Sign-On en tant qu'application hébergée par Citrix XenApp sont déconnectés et cliquez sur Continuer pour signaler les données de l'utilisateur à réinitialiser.
   Remarque : s'ils n'ont pas fermé leur session, cliquez sur Annuler, réinitialisez leur session ICA et revenez à cette procédure.
9. Cliquez sur OK dans la boîte de dialogue Réinitialiser les données utilisateur une fois les informations des utilisateurs vérifiées et réinitialisées. Les données des utilisateurs sont réinitialisées lors de leur prochaine connexion à Single Sign-On à l'aide du plug-in.

Pour supprimer les données utilisateur

L'opération Supprimer les données utilisateur du magasin central permet d'effacer toutes les données et les informations utilisateur du magasin central. Vous pouvez l'utiliser lorsqu'un utilisateur quitte définitivement votre entreprise.

Le magasin local d'informations d'identification de l'ordinateur de l'utilisateur reste intact jusqu'à sa suppression par un administrateur ou un opérateur.

En cas d'exécution du plug-in par l'utilisateur désormais supprimé, le plug-in synchronise son magasin local d'informations d'identification avec le magasin central, sauf si le magasin local d'informations est expressément supprimé par un administrateur ou un opérateur. Pour éviter ce genre de situation, supprimez cet utilisateur de votre entreprise (par exemple, désactivez ou supprimez l'utilisateur dans Active Directory).

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. À partir du menu Action, cliquez sur Autres tâches > Supprimer les données utilisateur du magasin central. La boîte de dialogue Sélectionner Utilisateur s'affiche.
4. Tapez un nom d'utilisateur dans la zone de texte et cliquez sur Vérifier les noms.
5. Si vous obtenez un résultat, cliquez sur OK. Cliquez sur Oui pour confirmer votre choix. Un message de confirmation s'affiche.
6. Cliquez sur OK. L'utilisateur est maintenant supprimé du magasin central.

Pour inviter les utilisateurs à se réenregistrer

Vous pouvez demander à un utilisateur ou à tous les utilisateurs d'enregistrer de nouveau les questions de sécurité. Vous utilisez les fonctions suivantes à des fins de sécurité ou en cas d'altération de données d'utilisateurs :

- Effacer les questions de sécurité d'un utilisateur
  Sélectionnez cette option pour supprimer les données de questions de sécurité d'un utilisateur. L'utilisateur ne bénéficiera pas de l'authentification par question tant qu'il ne se sera pas réenregistré.

- Inviter à nouveau tous les utilisateurs à enregistrer leurs questions de sécurité
  Sélectionnez cette option pour demander à tous les utilisateurs de réenregistrer leurs questions et leurs réponses de sécurité lorsqu'ils démarrent le plug-in. Les données de questions de sécurité sont conservées et toutes les fonctions nécessitant une authentification par questions restent disponibles avec leurs réponses en cours. Les utilisateurs reçoivent des invites jusqu'à ce qu'ils se réenregistrent.

Si des utilisateurs choisissent de ne pas réenregistrer leurs réponses en annulant la boîte de dialogue Enregistrement Citrix Single Sign-On à l'invite, ils ne pourront pas utiliser les fonctions utilisant l'authentification par questions telles que les fonctions autonomes de compte jusqu'à ce qu'ils choisissent de réenregistrer leurs réponses.

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. À partir du menu Action, cliquez sur Autres tâches et l'une des options suivantes :
   - Effacer les questions de sécurité d'un utilisateur
     La boîte de dialogue Sélectionner Utilisateur s'affiche. Tapez ou sélectionnez un utilisateur. Confirmez que vous souhaitez révoquer l'enregistrement des questions de sécurité de cet utilisateur.

   - Inviter à nouveau tous les utilisateurs à enregistrer leurs questions de sécurité
     Cliquez sur Oui pour inviter tous les utilisateurs, puis sur OK.

Pour définir une stratégie de configuration utilisateur

Lorsque vous créez ou modifiez une configuration utilisateur, vous pouvez associer des utilisateurs de groupes Active Directory à des configurations utilisateur. Il est possible d'associer un utilisateur d'un groupe à plus d'une configuration utilisateur. Dans ce cas, vous pouvez définir la priorité de la configuration utilisateur.

Important : le mode d'organisation de votre environnement Single Sign-On peut affecter le fonctionnement des configurations utilisateur. En d'autres termes, vous associez des configurations utilisateur de votre environnement Single Sign-On à une hiérarchie Active Directory (unité d'organisation ou utilisateurs) ou à un groupe Active Directory. Si vous utilisez les deux (hiérarchie et groupe) et qu'un utilisateur se trouve dans les deux conteneurs, la configuration utilisateur associée à la hiérarchie a la priorité et sera celle utilisée. Ce schéma est appelé environnement mixte.

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. À partir du menu Actions, cliquez sur Autres tâches >Définir la priorité de configuration utilisateur. La boîte de dialogue Définition de la priorité de configuration utilisateur s'affiche.
4. Sélectionnez une configuration utilisateur et cliquez sur Monter ou Descendre, selon vos préférences.

Affectation d'une configuration utilisateur à différents utilisateurs

Lorsque vous modifiez une configuration utilisateur existante, notez que vous ne pouvez pas en modifier l'emplacement. Vous pouvez effectuer l'une des procédures suivantes :

- Application par copie d'une configuration utilisateur à un ensemble d'utilisateurs supplémentaire
- Application par déplacement d'une configuration utilisateur à un ensemble d'utilisateurs différent

Pour copier une configuration utilisateur

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. Sélectionnez la configuration utilisateur.
4. À partir du menu Action, cliquez sur Copier la configuration utilisateur.
5. Entrez le nom de la configuration en double.
6. Spécifiez l'unité d'organisation, l'utilisateur ou le groupe contenant les utilisateurs auxquels la configuration utilisateur doit s'appliquer.

Pour déplacer une configuration utilisateur vers différents utilisateurs

Vous ne pouvez pas déplacer une configuration utilisateur associée à un groupe Active Directory. Pour associer la configuration utilisateur à une hiérarchie Active Directory (unité d'organisation ou utilisateur), copiez-la et spécifiez l'association souhaitée.

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. Sélectionnez la configuration utilisateur.
4. À partir du menu Action, cliquez sur Déplacer la configuration utilisateur.
5. Spécifiez l'unité d'organisation, l'utilisateur ou le groupe contenant les utilisateurs auxquels la configuration utilisateur doit s'appliquer.

Mise à niveau des configurations utilisateur existantes

Dans les versions 4.0 et 4.1 de Password Manager, vous associiez des utilisateurs à une configuration utilisateur par le biais

d'une hiérarchie Active Directory (unité d'organisation ou utilisateur). Dans les versions 4.5 et 4.6 de Password Manager et 4.8 et 5.0 de Single Sign-On, vous pouvez choisir d'associer les utilisateurs par un groupe Active Directory.

- Si vous utilisez une configuration utilisateur existante organisée par hiérarchie et que vous créez maintenant des configurations utilisateur organisées par groupe, et qu'un utilisateur se trouve dans les deux conteneurs, la configuration utilisateur associée à la hiérarchie a la priorité et sera celle utilisée. Ce schéma est appelé environnement mixte. Dans ce cas, vos utilisateurs peuvent rencontrer des comportements non souhaités de la part du plug-in. Ils auront en effet accès aux ressources associées à la configuration utilisateur de la hiérarchie et non à celles associées à la configuration utilisateur de groupe.
- Si vous souhaitez conserver les paramètres de vos configurations utilisateur de hiérarchie existantes mais modifier leur association, déplacez la configuration utilisateur vers un autre utilisateur. Cette procédure est valide pour les configurations utilisateur de hiérarchie des versions 4.1, 4.5, 4.6, 4.8 et 5.0.

Tenez compte des éléments suivants si vous souhaitez mettre à niveau des configurations existantes dont les utilisateurs sont organisés par unité d'organisation ou par utilisateurs :

Si vous mettez à niveau le service et la console Single Sign-On mais pas le plug-in, celui-ci assurera ses fonctions de base auprès des utilisateurs dont les configurations sont liées à des hiérarchies Active Directory (unités d'organisation ou utilisateurs). Cependant, vos utilisateurs n'auront pas accès aux dernières fonctionnalités de Single Sign-On. Citrix recommande de mettre à niveau le plug-in dès que possible pour qu'il corresponde aux versions du service et de la console.

Authentification des utilisateurs et vérification d'identité

Oct 21, 2015

Single Sign-On offre deux types d'authentification :

- L'authentification principale, qui s'applique lorsque les utilisateurs utilisent leurs noms d'utilisateur principaux, leurs mots de passe et, éventuellement, le nom de domaine en ouvrant une session sur Microsoft Windows pour accéder au réseau de leur entreprise. Le sous-système de sécurité Windows existant prend en charge la gestion de l'authentification sur le réseau.
- L'authentification secondaire, qui s'applique lorsque vous configurez Single Sign-On de manière à soumettre les informations d'identification permettant aux utilisateurs d'accéder aux ressources d'authentification unique protégées. Ces ressources peuvent inclure une application d'entreprise, une application Web, un champ protégé au sein d'une application, une adresse IP, une URL, etc.

Après la réussite de l'authentification au réseau, Single Sign-On obtient le mot de passe principal de l'ouverture de session Windows et combine ces informations à d'autres variables pour créer la clé de cryptage qui protège les informations d'identification de l'utilisateur. Le plug-in utilise cette clé pour récupérer et décrypter les informations d'identification demandées par les applications ou les ressources.

Important : si le mot de passe d'un utilisateur est dévoilé, réinitialisez-le deux fois plutôt qu'une afin de garantir que le mot de passe en question est supprimé de la fonction utilisant le mot de passe précédent. Les utilisateurs doivent ouvrir une session avec chacun des nouveaux mots de passe afin que le plug-in puisse capturer les modifications.

Confirmation de l'identité des utilisateurs

Chaque fois que les utilisateurs ouvrent une session dans votre environnement, ils confirment leur identité en tapant leur nom d'utilisateur et mot de passe, ou à l'aide d'une carte à puce ou tout autre dispositif d'authentification les identifiant de façon unique.

Néanmoins, certains événements nécessitent un deuxième niveau d'authentification afin de vérifier que l'utilisateur à l'origine de la modification y est autorisé.

Événement	Description
Modification du mot de passe principal par un administrateur	Lorsque les administrateurs modifient les mots de passe principaux des utilisateurs, ceux-ci sont invités à confirmer leur identité pour garantir que l'utilisateur autorisé a ouvert la session.
Réinitialisation du mot de passe principal par un utilisateur à l'aide des fonctions autonomes de compte.	Lorsque les utilisateurs réinitialisent leur mot de passe principal à l'aide la fonction Fonctions autonomes de compte, ils doivent confirmer leur identité. N'utilisez pas l'option d'authentification Saisie du mot de passe précédent si vous activez les fonctionnalités de fonctions autonomes de compte.
Déverrouillage du compte de domaine à l'aide des fonctions autonomes de compte.	Lorsque les utilisateurs déverrouillent leur compte à l'aide de la fonctionnalité Fonctions autonomes de compte, ils sont invités à reconfirmer leur identité.

Evénement	Description
Modification des types d'authentification	Par exemple, lorsque les utilisateurs passent d'une authentification avec carte à puce vers une authentification avec mot de passe, ils sont invités à reconfirmer leur identité.
Modification de mot de passe sur une machine cliente exécutant Single Sign-On.	Les utilisateurs qui modifient leur mot de passe principal sur une machine cliente n'exécutant pas le plug-in sont invités à confirmer leur identité à la prochaine ouverture de session sur une machine cliente l'exécutant.

Vos utilisateurs peuvent confirmer leur identité en utilisant l'une des options, ou plus, que vous pouvez préciser pour répondre aux besoins de votre entreprise.

Présentation des méthodes de vérification d'identité

Single Sign-On comporte deux méthodes de vérification d'identité pour garantir que l'utilisateur est autorisé à utiliser Single Sign-On :

- Mot de passe précédent
- Questions de sécurité

Vous pouvez également choisir de contourner la vérification d'identité en utilisant la fonction de gestion automatique des clés :

vous pouvez autoriser les utilisateurs à choisir la méthode de vérification d'identité (mots de passe précédents ou questions de sécurité) qu'ils privilégient pour l'authentification. Cette option est disponible dans le cadre de la propriété Protection de données secondaire dans la configuration utilisateur.

Mot de passe précédent

Si vous sélectionnez cette méthode, les utilisateurs doivent confirmer leur identité en tapant leur mot de passe principal précédent.

Attention : lorsque le mot de passe précédent est la seule méthode disponible pour les utilisateurs, ceux qui l'oublient ne peuvent plus accéder au système. Leurs données doivent être supprimées du magasin central et de toutes les machines clientes où elles sont stockées. Ils doivent de nouveau entrer leurs informations d'identification pour toutes les applications.

Questions de sécurité

Lorsque les utilisateurs modifient leur mot de passe principal, vous pouvez confirmer leur identité en les invitant à répondre aux questions de sécurité dans le cadre d'un questionnaire que vous créez. Ce questionnaire apparaît à la première ouverture du plug-in. Les utilisateurs répondent à un nombre minimum de questions puis sont invités à entrer de nouveau ces informations lors d'événements de modification de mot de passe spécifiques.

Elles doivent être conçues de façon à ce que la réponse apportée par une personne ne soit connue que d'elle. Vous pouvez utiliser les questions par défaut fournies par Single Sign-On ou créer vos propres questions.

Contournement de la vérification d'identité

Important : la gestion automatique des clés n'est pas aussi sûre que d'autre mécanisme de récupération de clé tels que les questions de sécurité et le mot de passe précédent.
Si vous souhaitez que Single Sign-On contourne la vérification d'identité et récupère automatiquement les clés de cryptage

des utilisateurs, vous pouvez spécifier l'option Protection de données secondaire Ne pas interroger les utilisateurs, restaurer automatiquement la protection de données principale sur le réseau.

Cette méthode, appelée gestion automatique des clés, est disponible une fois que vous avez installé le module de gestion des clés et que vous avez créé une configuration utilisateur en sélectionnant cette option.

Cette méthode permet aux utilisateurs d'ouvrir une session sur le réseau et d'obtenir un accès immédiat aux applications gérées par Single Sign-On. Ils ne doivent répondre à aucune question. Lorsque les utilisateurs changent leur mot de passe réseau, le plug-in détecte la modification et récupère les clés de cryptage de l'utilisateur à l'aide du service Single Sign-On.

La gestion automatique des clés offre aux utilisateurs la méthode d'accès la plus simple et la plus rapide à leurs applications. Toutefois, elle ne protège pas contre un accès par un utilisateur non autorisé car il n'existe aucun secret de l'utilisateur pour protéger le mot de passe réseau de celui-ci. Pour prévenir ce risque, mettez en place le module de récupération de clé automatique en combinaison avec les fonctions autonomes. Ce module nécessite l'authentification avec questions pour autoriser vos utilisateurs à confirmer leur identité lorsqu'ils réinitialisent leur mot de passe principal ou déverrouillent leur compte de domaine.

Permutation entre plusieurs méthodes d'authentification principale

Dans Single Sign-On, les utilisateurs peuvent basculer entre plusieurs méthodes d'authentification principale. Single Sign-On protège les mots de passe des utilisateurs avec une copie unique de la clé de sécurité comme méthode de réauthentification pour déverrouiller efficacement les données de l'utilisateur chaque fois que l'utilisateur bascule entre des méthodes d'authentification, sans que l'utilisateur soit obligé de confirmer son identité.

L'option de sélection de plusieurs méthodes d'authentification est disponible sur la page Méthode de protection des données dans la configuration utilisateur.

Considérons le scénario suivant :

- Un superviseur du centre d'appels se connecte à un ordinateur à l'aide de ses informations d'identification principales (nom d'utilisateur et mot de passe Windows). Single Sign-On Plug-in est installé sur l'ordinateur et lui permet d'utiliser des applications Single Sign-on (SSO).
- Le superviseur utilise parfois une carte à puces avec code secret (PIN) pour ouvrir une session sur un ordinateur partagé à l'étage du centre d'appels et lance une autre application publiée par le biais de XenApp. Cet ordinateur utilise le Bureau dynamique pour activer la commutation rapide des utilisateurs entre les différents comptes.

Dans les versions 4.0 et 4.1 de Citrix Password Manager, le superviseur du centre d'appels devait confirmer son identité avant d'utiliser les applications d'authentification pour tout changement de méthode d'authentification principale. Dans ce scénario, le superviseur utilisait deux méthodes d'authentification principales : d'abord son nom d'utilisateur et son mot de passe, puis une carte à puce avec code secret. Les versions 4.0 et 4.1 de Password Manager traitent le changement de méthode d'authentification comme nécessitant la récupération des clés de sécurité et éventuellement la confirmation de l'identité du superviseur.

Les utilisateurs doivent s'enregistrer ou s'inscrire dans chaque nouvelle méthode d'authentification la première fois qu'ils utilisent la méthode ou basculent vers elle. Toutefois, les commutations ultérieures ne nécessitent pas d'enregistrement ou d'inscription (autrement dit, une récupération de clé n'est pas requise par la suite).

Gestion de l'authentification avec questions

Oct 21, 2015

L'authentification avec questions permet de fournir une authentification sécurisée aux utilisateurs qui modifient leur mot de passe principal (dans certaines circonstances), leur méthode d'authentification, ou dont le compte est verrouillé.

L'utilisation des questions de sécurité et de l'authentification avec questions peut offrir une protection contre des accès non autorisés en demandant des informations connues uniquement de chaque utilisateur. Les questions créées doivent demander des informations confidentielles difficiles à deviner pour un tiers (notamment, par une recherche aléatoire ou à l'aide d'un dictionnaire).

Important : si vous envisagez d'utiliser les fonctions autonomes de compte (réinitialisation de mot de passe ou déverrouillage de compte de domaine) du module de gestion des clés de Single Sign-On, vous devez employer l'authentification avec questions pour permettre à vos utilisateurs de confirmer leur identité lors du déverrouillage de leur compte de domaine ou de la réinitialisation de leur mot de passe principal.

Confirmation de l'identité d'un utilisateur à l'aide de l'authentification avec questions

Si vous mettez en œuvre les fonctions de réinitialisation de mot de passe ou de déverrouillage de compte de domaine (qui font partie des fonctions autonomes de compte) du module de gestion des clés de Single Sign-On, utilisez l'authentification avec questions pour la vérification de l'identité des utilisateurs. Cette méthode peut également servir de protection secondaire des données en cas de modification de l'authentification principale d'un utilisateur.

Si les paramètres de configuration utilisateur définis sur la Console l'exigent, les utilisateurs peuvent être amenés à vérifier leur identité dans les cas suivants :

- Modification du type d'authentification des utilisateurs (par exemple, basculement de l'utilisateur entre l'authentification avec carte à puce et l'authentification avec mot de passe).
- Modification du mot de passe principal par un administrateur.
- Réinitialisation du mot de passe principal par un utilisateur à l'aide des fonctions autonomes de compte.
- Déverrouillage du compte de domaine à l'aide des fonctions autonomes de compte.
- Modification du mot de passe principal par un utilisateur sur une machine où le plug-in n'est pas installé, puis ouverture de session sur une machine où il est installé.

Remarque : vous pouvez également créer une configuration utilisateur ne nécessitant aucune vérification après basculement entre les différents types d'authentification. Veuillez consulter la section *— Permutation entre plusieurs méthodes d'authentification principale* .

Si cette fonction est configurée, Single Sign-On Plug-in demande aux utilisateurs de répondre à des questions de sécurité lors de leur première utilisation. Lorsque des événements nécessitant la vérification d'identité surgissent, le plug-in lance le questionnaire que vous avez créé. Un questionnaire est une liste préconfigurée de questions que vous avez créées.

Chaque question du questionnaire apparaît sur une page différente. Par exemple, si cinq questions se trouvent dans votre questionnaire, les utilisateurs verront s'afficher cinq pages distinctes. Ils doivent répondre à toutes correctement. Si les paramètres de l'administrateur l'exigent, les réponses doivent être totalement identiques, notamment du point de vue de la casse et de la ponctuation, aux réponses fournies à la première utilisation de Single Sign-On.

La combinaison correcte des questions et réponses confirme leur identité. Après confirmation, le plug-in crypte à nouveau les clés à l'aide du nouveau mot de passe principal et stocke les informations d'identification secondaires de l'utilisateur.

Notions importantes

- Si vous élisez de ne pas configurer les réponses aux questions de sécurité comme une condition requise pour les utilisateurs, ceux-ci sont invités à fournir leur précédent mot de passe principal lorsqu'ils en changent et qu'ils tentent d'ouvrir une session avec le nouveau mot de passe. Vous pouvez permettre aux utilisateurs de choisir la méthode de vérification d'identité qu'ils préfèrent utiliser pour l'authentification. Cette option est incluse dans la propriété de protection secondaire des données de la configuration utilisateur.
- Pour prévenir le verrouillage des utilisateurs, ne combinez pas le module de réinitialisation de mot de passe avec l'option Saisie du mot de passe précédent. Les utilisateurs qui réinitialisent leur mot de passe risquent de ne pas se souvenir de leur mot de passe principal précédent et d'être alors incapables de récupérer leurs informations d'identification secondaires.
- Les questions multiples offrent la meilleure protection.
- Par défaut, l'authentification avec questions utilise quatre questions de sécurité. Bien qu'il soit possible de n'utiliser que ces quatre questions, pensez à ajouter vos propres questions de sécurité et groupes de questions.

Important : si les paramètres de l'administrateur l'exigent, la réponse de l'utilisateur aux questions de sécurité doit respecter la casse, la ponctuation et les espaces de la réponse enregistrée initialement.

Étapes de l'authentification avec questions

Créez et proposez les questions de sécurité avant de déployer le plug-in. Lorsqu'une question est sélectionnée par un utilisateur, elle doit toujours rester disponible. Si vous modifiez ou supprimez une question utilisée, les utilisateurs concernés ne peuvent plus utiliser les questions de sécurité pour récupérer leurs informations d'identification secondaires, jusqu'à ce que, et à moins que, vous les contraigniez à se réinscrire.

1. Créez vos questions de sécurité, en définissant la longueur minimum et l'utilisation de la casse. Ces questions peuvent être proposées dans n'importe quelle langue prise en charge par Single Sign-On.
2. Vous pouvez regrouper ces questions par groupes de questions de sécurité. Vous pouvez créer des questions parmi lesquelles choisiront vos utilisateurs, ce qui leur permet de sélectionner librement une question dont ils retiendront plus facilement la réponse. Cela permet de définir le nombre de questions de chaque groupe auxquelles les utilisateurs doivent répondre.
3. Ajoutez vos questions ou questions et groupes de questions au questionnaire.
4. Sélectionnez une ou deux questions à utiliser pour la récupération de clé. Ces questions permettent de crypter les données de la récupération de clé ; vos utilisateurs doivent toujours fournir les réponses aux questions enregistrées.
5. Si vous le souhaitez, vous pouvez activer le masquage des réponses aux questions de sécurité. Cette fonctionnalité vous donne l'option de masquer les réponses de l'utilisateur aux questions de sécurité de l'authentification avec questions. Si elles sont activées, les réponses des utilisateurs sont protégées pendant l'enregistrement des réponses et la vérification d'identité.
   Le masquage des réponses aux questions de sécurité est uniquement disponible sur la console et le plug-in exécutant Password Manager 4.6 et 4.6 avec Service Pack 1 et Single Sign-On 4.8 et 5.0.

Conception des questions de sécurité: compromis entre maintien de la sécurité et simplicité d'utilisation

Single Sign-On fournit quatre questions par défaut que vous pouvez utiliser pour l'inscription des utilisateurs. Ces questions sont disponibles dans toutes les langues prises en charge (anglais, français, allemand, japonais, chinois simplifié et espagnol). Citrix recommande de créer vos propres questions de sécurité et de les proposer dans toutes les langues de votre environnement.

Tout individu tentant d'accéder au mot de passe d'un utilisateur doit connaître la réponse à toutes ces questions. Cependant, trop de questions peuvent représenter un obstacle dans la confirmation d'identité de vos utilisateurs.

Les questions de sécurité doivent demander des informations confidentielles difficiles à deviner pour un tiers (notamment, par une recherche aléatoire ou à l'aide d'un dictionnaire). Le facteur clé pour déterminer la sécurité d'une question est le degré de difficulté pour en deviner la réponse.

Les questions bien conçues ont un niveau d'entropie élevé ; en d'autres termes, elles impliquent les points suivants :

- large éventail de réponses possibles ;
- probabilité de découverte très faible.

Pour des raisons pratiques, la réponse doit être facile à retenir pour l'utilisateur en question mais difficile à déchiffrer pour un tiers. Par exemple :

- Quel est le nom de votre professeur de lycée ou d'université préféré ?
- Où rêvez-vous de passer vos vacances ? (ville, pays)
- Quel est le nom de votre chanson et de votre chanteur favoris ?
- Quel est le nom de votre livre et de votre auteur favoris ?
- Quel est le nom de votre œuvre favorite, à qui la doit-on et où vous l'avez découverte ?

Néanmoins, les affinités culturelles peuvent conduire vers les mêmes réponses des utilisateurs d'une même population, même si ces utilisateurs ne partagent pas délibérément leurs réponses. Ce facteur accroît les risques d'une attaque interne.

Évitez de créer des questions présentant les caractéristiques suivantes :

- questions impliquant une réponse simple, comme « Quelle est votre couleur préférée ? » ;
- questions demandant des informations susceptibles d'être connues ou d'évoluer (par exemple: « Quelle est votre adresse ? »).

Autoriser les utilisateurs à modifier les réponses aux questions de sécurité

Single Sign-On permet aux utilisateurs de modifier leurs réponses aux questions de sécurité à tout moment et sans intervention de l'administrateur.

Si votre environnement inclut des questions de sécurité ou des fonctions autonomes de compte, les utilisateurs enregistrant des questions et réponses de sécurité peuvent utiliser le plug-in pour fournir de nouvelles réponses à leurs questions de sécurité existantes.

Une fois que les utilisateurs ont fourni leurs réponses et reçu la confirmation de l'enregistrement de leurs nouvelles réponses dans le magasin central, leurs anciennes réponses ne sont plus valides.

Les utilisateurs changent leurs réponses aux questions de sécurité an accédant à l'assistant d'enregistrement aux questions de sécurité.

Vous offrez aux utilisateurs un accès à l'assistant d'enregistrement aux questions de sécurité en tant qu'application publiée :

1. Installez Single Sign-on Plug-in sur un serveur XenApp.
2. Situez le fichier QBAEnroll.exe sur le serveur XenApp.
3. Publiez le fichier QBAEnroll.exe et mettez-le à la disposition des utilisateurs.
4. Informez les utilisateurs de la manière d'accéder à l'assistant d'enregistrement aux questions de sécurité et de l'utiliser.

Remarque : les utilisateurs exécutant Single Sign-on Plug-in Version 4.8 peuvent accéder à l'assistant d'enregistrement aux questions de sécurité en sélectionnant Outils > Enregistrement des questions de sécurité dans le Gestionnaire d'informations d'identification. Ces utilisateurs ne requièrent pas accès à l'assistant d'enregistrement aux questions de

sécurité en tant qu'application publiée. Les utilisateurs exécutant Single Sign-on Plug-in Version 4.6 Service Pack 1 ou version antérieure ne peuvent pas accéder à l'assistant d'enregistrement aux questions de sécurité en tant qu'application publiée.

Gestion de vos questions

Oct 21, 2015

Le nœud Authentification avec questions du composant Single Sign-On de Citrix AppCenter offre un emplacement central pour la gestion de toutes les questions de sécurité associées à la vérification d'identité, la réinitialisation de mot de passe et au déverrouillage de compte. Vous pouvez ajouter vos propres questions de sécurité à la liste de questions par défaut, créer des groupes de question et les destiner à des utilisateurs particuliers.

- Si vous modifiez les questions fournies par défaut après l'enregistrement des réponses des utilisateurs, tenez compte de la signification des questions modifiées. La modification d'une question ne force pas une réinscription. Toutefois, si la signification d'une question est changée, les utilisateurs qui ont répondu auparavant à cette question peuvent se retrouver incapables d'y apporter une réponse.
- L'ajout, la suppression et le remplacement de questions de sécurité après inscription des utilisateurs avec les anciennes questions entraînent l'impossibilité pour ces utilisateurs de s'authentifier et de réinitialiser leur mot de passe tant qu'ils ne sont pas réinscrits. Les utilisateurs doivent répondre à des nouvelles questions à la première ouverture du plug-in.
- Chaque question de sécurité peut appartenir à plusieurs groupes de questions de sécurité. Lorsque vous créez des groupes de questions de sécurité, toutes vos questions peuvent être utilisées dans n'importe quel groupe.

Utilisez ces étapes pour accéder aux paramètres référencés dans les procédures suivantes :

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On, développez Vérification d'identité et sélectionnez le nœud Authentification avec questions.
3. À partir du menu Action, cliquez sur Gérer les questions.

Pour créer de nouvelles questions de sécurité

Vous pouvez créer différentes questions et choisir une langue pour chacune d'entre elles. Vous pouvez aussi saisir plusieurs traductions d'une même question. Le plug-in présente à l'utilisateur le questionnaire dans la langue définie dans les paramètres de langue de son profil. Si la langue n'est pas disponible, Single Sign-On affiche les questions dans la langue par défaut.

Remarque : lorsque vous sélectionnez une langue pour une question de sécurité, la question est présentée aux utilisateurs dont les paramètres de système d'exploitation sont définis pour cette langue. Si les paramètres de système d'exploitation sélectionnés ne correspondent pas à ceux de certaines questions disponibles, la langue par défaut est utilisée.

1. Sélectionnez Questions de sécurité.
2. Sélectionnez une langue dans la liste déroulante Langue et cliquez sur Ajouter une question. La boîte de dialogue Question de sécurité s'affiche.
3. Ajoutez la nouvelle question dans la boîte de dialogue Question de sécurité.

Important : vous devez utiliser la commande Modifier pour ajouter le texte traduit des questions existantes. Si vous sélectionnez Ajouter une question, vous créez une nouvelle question qui n'est pas associée à l'original.

Pour configurer une langue par défaut

Dans la plupart des cas, les utilisateurs voient les questions de sécurité s'afficher dans la langue associée à leur profil utilisateur actuel. Si la langue n'est pas disponible, Single Sign-On affiche les questions dans la langue par défaut spécifiée.

1. Sélectionnez Authentification avec questions.
2. Dans la liste déroulante Langue par défaut, sélectionnez la langue par défaut de votre choix.

Remarque : l'option Vérification de la rétrocompatibilité garantit que les plug-ins associés à Password Manager 4.0 et Password Manager 4.1 peuvent continuer à présenter les questions de vérification d'identité.

Pour ajouter ou modifier le texte de questions existantes

L'ajout, la suppression et le remplacement de questions de sécurité après inscription des utilisateurs avec les anciennes questions entraînent l'impossibilité pour ces utilisateurs de s'authentifier et de réinitialiser leur mot de passe tant qu'ils ne sont pas réinscrits. Les utilisateurs doivent répondre à des nouvelles questions à la première ouverture du plug-in. La modification d'une question ne force pas une réinscription. Toutefois, si la signification d'une question est changée, les utilisateurs qui ont répondu auparavant à cette question peuvent se retrouver incapable d'y apporter une réponse.
Important : si vous modifiez une question existante, préservez-en le sens. Dans le cas contraire, il est possible que les réponses des utilisateurs ne correspondent pas lors des authentifications ultérieures. En d'autres termes, l'utilisateur risque de fournir une réponse ne correspondant pas à la réponse enregistrée.

1. Sélectionnez Questions de sécurité.
2. Sélectionnez une langue dans la liste déroulante Langue.
3. Sélectionnez la question et cliquez sur Modifier. La boîte de dialogue Question de sécurité s'affiche.
4. Modifiez la question dans la boîte de dialogue Question de sécurité.

Pour créer un groupe de questions de sécurité

Vous pouvez créer des questions de sécurité auxquelles répondent vos utilisateurs pour confirmer leur identité. Chaque question ajoutée au questionnaire doit recevoir une réponse des utilisateurs. Cependant, vous pouvez également rassembler ces questions dans un groupe de questions de sécurité.

Les groupes de questions permettent d'ajouter, par exemple, six questions à un questionnaire et de permettre aux utilisateurs de choisir de ne répondre qu'à trois d'entre elles. Ils bénéficient ainsi d'une plus grande souplesse dans la sélection des questions et la saisie des réponses de vérification d'identité.

1. Sélectionnez Questions de sécurité.
2. Cliquez sur Ajouter le groupe.
3. Dans la boîte de dialogue Groupe de questions de sécurité, donnez un nom au groupe, sélectionnez les questions et spécifiez le nombre de questions auquel l'utilisateur doit répondre.

Pour modifier un groupe de questions de sécurité

1. Sélectionnez Questions de sécurité.
2. Sélectionnez le groupe de questions de sécurité à modifier et cliquez sur Modifier. La boîte de dialogue Groupe de questions de sécurité présente une liste de questions de sécurité pouvant faire partie du groupe. Les questions du groupe sont signalées par une coche. Vous pouvez modifier le nom du groupe, ajouter des questions au groupe et sélectionner le nombre de questions nécessitant une réponse de l'utilisateur.

Pour sélectionner une ou plusieurs questions pour la récupération de clé

Vous devez sélectionner une ou deux questions nécessitant une réponse des utilisateurs afin de crypter les données de la récupération de clé. Vos utilisateurs doivent fournir des réponses à toutes les questions auxquelles ils avaient répondu lors de l'enregistrement mais les questions que vous avez sélectionnées permettent de fournir les données nécessaires au processus de cryptage et de récupération de clé.

1. Sélectionnez Récupération de clé.
2. Sélectionnez la case à côté de chaque question ou groupe de questions à utiliser pour la récupération de clé lors de la vérification d'identité.
3. Cliquez sur OK pour enregistrer votre question et vos réglages. Il est possible qu'un message d'activation du

réenregistrement forcé des réponses par les utilisateurs apparaisse. Cliquez sur Oui pour forcer le réenregistrement.

Pour activer le masquage des réponses de sécurité

Le masquage des réponses de sécurité est uniquement disponible avec les versions 4.6 et 4.6 avec Service Pack 1 de Password Manager et 4.8 et 5.0 de Single Sign-On.

Le masquage des réponses de sécurité apporte un niveau de sécurité supplémentaire à vos utilisateurs lorsqu'ils enregistrent leur réponses aux questions de sécurité ou qu'ils enregistrent leurs questions de sécurité ou qu'ils fournissent leurs réponses lors de la vérification d'identité. Lorsque cette fonctionnalité est activée, les réponses des utilisateurs exécutant Password Manager 4.6, Password Manager 4.6 avec Service Pack 1, Single Sign-On 4.8 ou Single Sign-On 5.0 sont masquées. Lors de l'enregistrement des réponses, ces utilisateurs sont invités à taper leurs réponses deux fois afin d'éviter les fautes de frappe ou d'orthographe. Les utilisateurs ne doivent taper leurs réponses qu'une seule fois lors de la validation d'identité, puisqu'ils sont invités à réessayer en cas d'erreur.

Remarque : les réponses aux questions de sécurité enregistrées dans l'Agent Password Manager 4.5 peuvent être masquées lorsque le logiciel est mis à niveau vers la version 5.0 de Single Sign-On. Les réponses aux questions de sécurité des utilisateurs de l'Agent Password Manager 4.5, 4.1 ou 4.0 demeurent invisibles quel que soit le réglage de la console.

1. Sélectionnez Masquage des réponses de sécurité.
2. Sélectionnez Masquer les réponses aux questions de sécurité.

Pour activer la rétrocompatibilité de votre questionnaire

Le mode de rétrocompatibilité permet au plug-in de continuer à offrir aux utilisateurs les questions de vérification d'identité utilisées dans Password Manager 4.0 et 4.1. Il permet également de continuer à utiliser la question par défaut « Quelle est votre formule de vérification d'identité? ». Si vous effectuez une mise à niveau à partir de la version 4.1, les questions de vérification d'identité et les questions utilisées pour la réinitialisation de mot de passe apparaissent sous forme de questionnaire dans la boîte de dialogue Gérer les questions.

Important : lors de la création et de la modification des configurations utilisateur, n'activez pas la rétrocompatibilité si vous disposez d'une nouvelle version installée de Single Sign-On car cela limite le plug-in aux versions 4.0 et 4.1 du produit. De même, ne désactivez pas le mode de rétrocompatibilité si l'Agent de la version 4.0 ou 4.1 est en cours d'exécution car cela empêche les utilisateurs d'effectuer une récupération de clé et les réinitialisations de mots de passe.
Si vous utilisez la gestion de clé automatique, n'activez pas la rétrocompatibilité. Celle-ci ne nécessite pas de réponses aux questions de vérification d'identité de la part des utilisateurs.

Pour la rétrocompatibilité avec les versions 4.0 et 4.1, le questionnaire doit inclure au moins une question de sécurité associée à la fonction autonome de réinitialisation de mot de passe.

Chaque question de sécurité doit inclure les réglages suivants :
- casse désactivée ;
- longueur minimum de 1 ;
- questions non activées pour la récupération de clé.

Pour vérifier la rétrocompatibilité

Vous pouvez vérifier la rétrocompatibilité si vous effectuez une mise à niveau à partir d'une version précédente de Single Sign-On/Password Manager :
1. Sélectionnez Authentification avec questions.
2. Sélectionnez Vérifier la rétrocompatibilité et cliquez sur OK.

Single Sign-On effectue la vérification de rétrocompatibilité et affiche les erreurs dans une boîte de dialogue.

Autorisation des utilisateurs à gérer leurs informations d'identification principales avec les fonctions autonomes de compte

Oct 21, 2015

Vous pouvez configurer les fonctions autonomes de compte de Single Sign-On pour permettre à vos utilisateurs de réinitialiser leur mot de passe principal sans intervention de l'administrateur ou du personnel d'assistance technique. En fonction de vos besoins, vous pouvez mettre en œuvre les fonctions autonomes de réinitialisation de mot de passe et de déverrouillage de compte en toute sécurité dans votre environnement Single Sign-On.

Remarque : pour mettre en place les fonctions autonomes du compte avec l'Interface Web Citrix, consultez *— l'Interface Web*

.

Les fonctions autonomes de compte sont protégées par l'authentification avec questions, qui garantit l'autorisation des utilisateurs lorsqu'ils s'apprêtent à réinitialiser leur mot de passe ou à déverrouiller leur compte. Lors de leur première utilisation de Single Sign-On Plug-in ou de la première utilisation suivant la configuration des fonctions autonomes de compte, les utilisateurs doivent enregistrer des réponses à des questions de sécurité, que vous créez et sélectionnez pendant la configuration de Single Sign-On.

Ces questions de sécurité sont présentées aux utilisateurs lorsqu'ils doivent réinitialiser leur mot de passe ou déverrouiller leur compte. Lorsqu'ils répondent aux questions correctement, les utilisateurs sont autorisés à réinitialiser leur mot de passe ou à déverrouiller leur compte, ce qui leur évite de faire appel au personnel d'assistance technique ou à l'administrateur.

Important : les fonctions autonomes de réinitialisation de mot de passe et de déverrouillage de compte nécessitent la mise en œuvre d'une authentification avec questions. Les utilisateurs doivent enregistrer des réponses à des questions de sécurité pour bénéficier de ces fonctions. Si vous choisissez de ne pas utiliser l'authentification avec questions dans votre environnement Single Sign-On, vos utilisateurs ne disposeront pas des fonctions autonomes de réinitialisation de mot de passe et de déverrouillage de compte.

Points à considérer :

- Vous pouvez mettre en œuvre le module de fonctions autonomes pour permettre à vos utilisateurs de réinitialiser leur mot de passe principal (compte de domaine) ou de déverrouiller leurs comptes de domaine Windows dans un environnement Active Directory uniquement.
- Lorsque les utilisateurs modifient leur mot de passe d'application à l'aide de Single Sign-On Plug-in ou leur mot de passe principal en utilisant la combinaison Ctrl+Alt+Suppr sur un ordinateur doté du plug-in, Single Sign-On prend automatiquement en compte le changement de mot de passe.
- Pour prévenir le verrouillage des utilisateurs, ne combinez pas le module de réinitialisation de mot de passe avec l'option Saisie du mot de passe précédent, qui permet de confirmer exclusivement l'identité des utilisateurs. lorsque le mot de passe précédent est la seule méthode disponible pour les utilisateurs, ceux qui l'oublient ne peuvent plus accéder au système. Leurs données doivent être réinitialisées ou supprimées du magasin central et de toutes les machines utilisateur où elles sont stockées. Ils doivent de nouveau entrer leurs informations d'identification pour toutes les applications.

Résumé des tâches d'implémentation des fonctions autonomes

Pour utiliser la fonctionnalité Fonctions autonomes de compte, procédez comme suit :

1. Installez le module de fonctions autonomes et le module de gestion des clés.
2. Configuration de l'authentification avec questions

3. Création d'une configuration utilisateur avec activation de l'une des fonctions autonomes de réinitialisation de mot de passe et de déverrouillage de compte (ou des deux)
4. Installation et configuration du plug-in

Utilisation de la gestion automatique de clés avec les fonctions autonomes

Combiner la gestion automatique de clés avec les fonctions autonomes confère davantage de convivialité aux utilisateurs qui ont besoin d'un accès à des applications protégées par mot de passe gérées par Single Sign-On Plug-in. Par exemple, si des utilisateurs réinitialisent leur mot de passe principal, ils n'ont pas besoin de répondre aux questions de sécurité après avoir réinitialisé leur mot de passe avec succès. (Toutefois, ils doivent répondre aux questions de sécurité pendant le processus de réinitialisation de mot de passe.)

Avec la gestion automatique de clés, les utilisateurs n'ont pas besoin de confirmer leur identité après avoir déverrouillé leur compte ou réinitialisé leur mot de passe de domaine.

Pour réinitialiser l'enregistrement des utilisateurs dans les fonctions autonomes

Si le compte Windows des utilisateurs est verrouillé et s'ils ne se souviennent pas des réponses à leurs questions de sécurité, vous devez utiliser le composant Single Sign-On de Citrix AppCenter pour réinitialiser l'enregistrement aux fonctions autonomes des utilisateurs. Après réinitialisation des utilisateurs, l'assistant d'enregistrement apparaît à leur prochaine ouverture du plug-in. Ils peuvent alors enregistrer leurs réponses aux questions de sécurité.

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On, développez le nœud Vérification d'identité et sélectionnez Authentification avec questions.
3. Dans le menu Action, cliquez sur Autres tâches >Effacer les questions de sécurité d'un utilisateur.
4. Dans la boîte de dialogue Sélectionnez un utilisateur, entrez le nom de l'utilisateur ou du groupe d'utilisateurs.

Expérience utilisateur

Une fois que le plug-in et le service sont installés et configurés, les fonctions autonomes modifient la boîte de dialogue d'ouverture de session de Windows de l'utilisateur et la boîte de dialogue Déverrouillage de l'ordinateur ou l'écran de bienvenue de Windows Vista, Windows 7, Windows Server 2008 et Windows Server 2008 R2, (disponible lorsque les utilisateurs verrouillent leur ordinateur avec la combinaison de touches CTRL-ALT-SUPPR) en y ajoutant un bouton Fonctions autonomes de compte.

Pour pouvoir accéder aux fonctions autonomes, les utilisateurs doivent se connecter à leur compte de domaine principal et enregistrer des réponses dans les fonctions de sécurité. Une fois qu'ils se sont enregistrés correctement, ils peuvent utiliser les fonctions autonomes de réinitialisation de mot de passe et de déverrouillage de compte.

Avec la gestion automatique de clés, les utilisateurs n'ont pas besoin de confirmer leur identité après avoir déverrouillé leur compte ou réinitialisé leur mot de passe de domaine.

Fonctions autonomes de compte

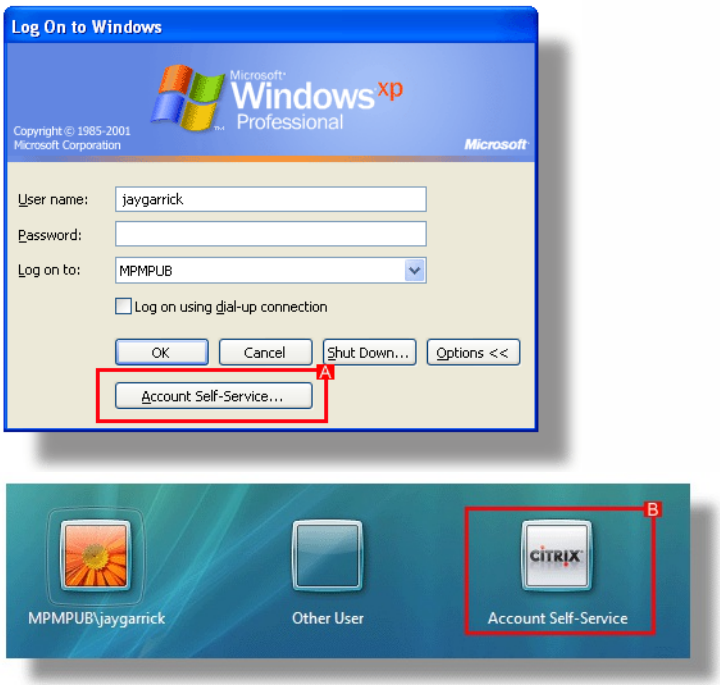
Oct 21, 2015

Les clients Single Sign-On ont la possibilité de déployer les fonctions autonomes de compte, soit Réinitialisation du mot de passe et Déverrouillage autonome du compte, sans qu'aucune autre fonctionnalité d'authentification unique ne soit disponible pour les utilisateurs.

Les fonctions autonomes de compte de Single Sign-On permettent de réduire le nombre d'appels reçus par votre service d'assistance informatique, ce qui permet à vos employés d'effectuer les opérations suivantes d'eux-mêmes :

- Modifier leur mot de passe sur le domaine Microsoft Windows.
- Déverrouiller leur compte de domaine Windows.

Les fonctions autonomes de compte vous permettent d'établir une série de questions de sécurité servant à la vérification d'identité. Après l'activation de l'authentification avec questions et après que les fonctions autonomes de compte sont mises à la disposition de vos utilisateurs, ces derniers s'inscrivent, ou s'enregistrent sur le service en répondant à la série de questions de sécurité. Une fois enregistrés, vos utilisateurs peuvent cliquer sur Fonctions autonomes de compte (A), situé dans la boîte de dialogue Ouverture de session Windows ou, pour les utilisateurs Microsoft Windows Vista, l'écran Bienvenue (B).



Les administrateurs peuvent requérir que les utilisateurs s'enregistrent à nouveau de la manière suivante :

- Par la révocation des données des questions d'un utilisateur.
- Par une invite de ré-enregistrement pour tous les utilisateurs.
- Par la modification du questionnaire existant.

Les utilisateurs inscrits peuvent aussi démarrer la procédure de ré-enregistrement à tout moment afin de modifier leurs réponses aux questions de sécurité.

Ce document décrit comment installer et configurer Single Sign-On afin de ne fournir aux utilisateurs que les fonctions

autonomes de compte.

Remarque : les fonctions autonomes de compte ne prennent pas en charge les ouvertures de session de nom d'utilisateur principal (UPN), tels que nomutilisateur@domaine.com.

Utilisation des licences

Une licence Single Sign-On est utilisée durant le processus de réinscription lorsque les utilisateurs soumettent de nouvelles réponses aux questions d'authentification. L'utilisation de licences Utilisateurs simultanés garantit une disponibilité des licences maximale au sein de votre organisation. Une licence Utilisateur simultané est renvoyée au regroupement de licences après que l'utilisateur ait terminé le processus de réinscription. Dans la même situation, l'utilisateur conserve une licence Utilisateur désigné, même si elle n'est pas utilisée, pendant deux jours minimum.

Des ratios sont utilisés pour fournir un plus grand nombre de licences Fonctions autonomes de compte par licence Single Sign-On. Les licences Utilisateurs simultanés utilisent un ratio de 10:1, 100 licences d'utilisateurs simultanés correspondent donc à 1 000 licences Fonctions autonomes de compte. Les licences Utilisateurs désignés utilisent un ratio de 5:1, 100 licences correspondent donc à 500 licences Fonctions autonomes de compte.

Pour utiliser des licences Utilisateurs simultanés disponibles en mode déconnecté

1. Créez une configuration utilisateur.
2. Sur la page Configuration du système de licences de l'assistant de configuration utilisateur, sélectionnez Licences Utilisateurs simultanés (éditions Enterprise et Platinum uniquement).
3. Sélectionnez Autoriser l'utilisation de la licence en mode déconnecté et définissez la durée pendant laquelle la licence peut être extraite du serveur de licences.
4. Terminez la définition de la configuration utilisateur.

Pour les utilisateurs associés à cette configuration utilisateur, le modèle de licence est identique à celui d'une licence Utilisateurs désignés : la licence peut être utilisée par des utilisateurs travaillant occasionnellement à distance et pouvant se trouver déconnectés sur de courtes périodes. L'utilisation des licences Utilisateurs simultanés est alors gérée utilisateur par utilisateur.

Important : les instances de Single Sign-On Plug-in installées localement ne nécessitent pas de licence distincte pour les utilisateurs qui ont accès à des applications hébergées dans un environnement Citrix XenApp, édition Platinum.

Pour créer une configuration utilisateur destinée uniquement aux fonctions autonomes de compte

Suivez les étapes suivantes pour créer une configuration utilisateur qui permette d'utiliser les fonctions autonomes de compte sans pour autant activer l'authentification unique.

Remarque : les définitions d'application ne sont pas incluses dans cette configuration utilisateur car cette fonction ne comprend pas la fonctionnalité d'authentification unique. Si les utilisateurs requièrent la fonctionnalité d'authentification unique, placez-les dans une configuration utilisateur qui ne comprenne pas les modifications apportées aux fonctions autonomes de compte.

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion et sélectionnez Citrix AppCenter.
2. Pour démarrer l'assistant, développez le nœud Single Sign-On et cliquez sur Configurations utilisateur. Dans la zone Actions, cliquez sur Ajouter une nouvelle configuration utilisateur pour ouvrir l'assistant de configuration utilisateur.
3. Sur la page Nommer la configuration utilisateur :
    1. dans le champ Nom, entrez le nom de la configuration utilisateur.
    2. Dans la zone Association de configuration utilisateur, choisissez comment la configuration utilisateur est associée aux utilisateurs en identifiant la hiérarchie Active Directory (Unité d'organisation ou utilisateur) ou le groupe Active Directory.

4. Sur la page Sélectionner l'édition du produit, sélectionnez Single Sign-On Enterprise.
5. Sur la page Choisir les applications, cliquez sur Suivant.
6. Sur la page Configurer l'interaction du plug-in, décochez les cases suivantes :
   - Détecter automatiquement les applications et inviter l'utilisateur à stocker les informations d'identification
   - Traiter automatiquement les formulaires définis lorsque Single Sign-On Plug-in les détecte

   Cliquez sur Paramètres avancés.
7. Dans Paramètres Single Sign-On Plug-in avancés :
   - Sélectionnez Prise en charge d'application et décochez la case Détecter les définitions d'application sur le client.

   Cliquez sur OK pour fermer Paramètres avancés et cliquez sur Suivant.
8. Sur la page Configurer le système de licences, dans la zone Adresse du serveur de licences, entrez le nom de votre serveur de licences et son numéro de port.
   Dans la zone Modèle de licences, sélectionnez Licences d'utilisateur désigné ou Licences Utilisateurs simultanés.

   Remarque : l'utilisation de licences Utilisateurs simultanés garantit une disponibilité des licences maximale au sein de votre organisation. Une licence Utilisateur simultané est renvoyée au regroupement de licences après que l'utilisateur ait terminé le processus de réinscription. Dans la même situation, l'utilisateur conserve une licence Utilisateur désigné, même si elle n'est pas utilisée, pendant deux jours minimum.
9. Sur la page Sélectionner les méthodes de protection des données, entrez les informations nécessaires.
10. Sur la page Sélectionner la protection secondaire des données, sélectionnez Sélection d'une méthode : mot de passe précédent ou questions de sécurité.
11. Sur la page Activer les fonctions autonomes de compte, sélectionnez l'une des options suivantes ou les deux :
    - Autoriser les utilisateurs à réinitialiser leur mot de passe de domaine principal
    - Autoriser les utilisateurs à déverrouiller leur compte de domaine
12. Sur la page Localiser les modules du service > Module de gestion des clés, entrez l'adresse du service.
13. Complétez l'assistant sans apporter de modifications supplémentaires.

Préparation de l'ordinateur exécutant le plug-in

Remarque : il peut s'avérer utile d'automatiser les procédures suivantes à l'aide de scripts pour optimiser l'efficience et la précision.
Une fois le logiciel Single Sign-On Plug-in installé sur les ordinateurs des utilisateurs, vous devez modifier le raccourci ssoShell.exe et le menu Démarrer pour permettre aux utilisateurs d'accéder uniquement aux fonctions autonomes de compte.

Durant l'installation de base du logiciel Single Sign-On Plug-in, le raccourci ssoShell.exe contient le commutateur de ligne de commande suivant :

/background

Remplacez-le par :

/qbaenroll /noforceqbaenroll

Cette modification entraîne, lors de l'ouverture de session de l'utilisateur, la synchronisation du logiciel Single Sign-On Plug-in sur l'ordinateur de l'utilisateur avec le magasin central et détermine l'état de l'enregistrement de l'authentification avec questions de l'utilisateur. Si le processus d'enregistrement a été complété, l'utilisateur n'est pas invité à s'enregistrer.
L'utilisateur est invité à s'enregistrer si l'une des conditions suivantes est découverte durant la synchronisation :

- L'utilisateur n'a pas complété le processus d'enregistrement de l'authentification avec questions.

- L'administrateur a réinitialisé les questions de l'authentification avec questions de l'utilisateur.
- L'administrateur a modifié le questionnaire de l'authentification avec questions.

Après avoir effectué la synchronisation et démarré le processus d'enregistrement (le cas échéant), ssoShell se ferme automatiquement.

Pour mettre à jour le raccourci ssoShell.exe Single Sign-On

Pour une installation sur un bureau :

1. Ordinateurs Windows Vista : à l'aide de l'explorateur Windows, accédez à %SystemDrive%\ProgramData\Microsoft\Windows\Menu Démarrer\Programmes\Démarrage.
   Ordinateurs autres que Windows Vista : à l'aide de l'explorateur Windows, accédez à %SystemDrive%\Documents and Settings\All Users\Menu Démarrer\Programmes\Démarrage.
2. À partir du dossier Démarrage, sélectionnez Single Sign-on Background Process et Fichier > Propriétés.
3. Dans la boîte de dialogue Propriétés Single Sign-on Background Process, cliquez dans le champ Cible, allez à la fin du texte dans ce champ et supprimez /background.
4. Dans le champ Cible, à la suite du texte restant, tapez /qbaenroll /noforceqbaenroll.

Pour une installation sur un serveur :
Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

1. Ouvrez le registre et accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\windows NT\CurrentVersion\Winlogon\AppSetup.
2. Dans cette sous-clé, double-cliquez sur l'entrée par défaut pour ouvrir la boîte de dialogue Modification de la chaîne.
3. Dans le champ Données de la valeur :
   Remplacez : %SystemDrive%\Citrix\Metaframe Password Manager\WTS\SSOlauncher.exe /no ssoshutdown

   par : %SystemDrive%\Citrix\Metaframe Password Manager\ssoshell.exe /qbaenroll /noforceqbaenroll.

Le fichier ssoShell.exe est modifié uniquement pour les fonctions autonomes de compte.

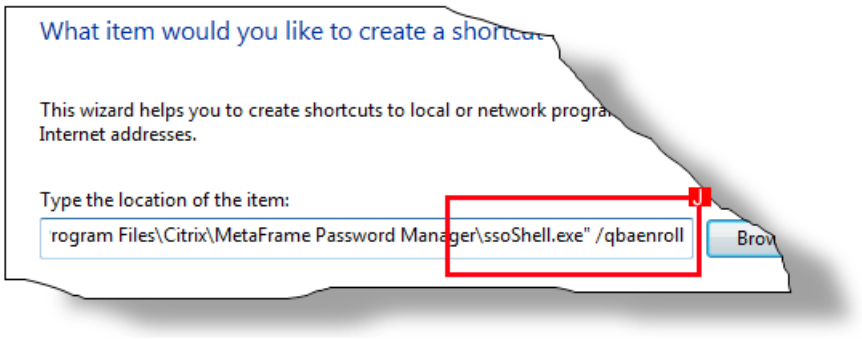
Pour ajouter un raccourci de l'enregistrement aux fonctions autonomes au menu Démarrer

Ajoutez un raccourci au menu Démarrer pour permettre aux utilisateurs de lancer le processus d'enregistrement par eux-mêmes. Cela permet d'éliminer les appels passés à l'assistance lorsque les utilisateurs ne fournissent pas de réponses durant l'ouverture de session ou qu'ils souhaitent modifier les réponses qu'ils ont définies préalablement.

1. Ordinateurs Windows Vista : à l'aide de l'explorateur Windows, accédez à %SystemDrive%\ProgramData\Microsoft\Windows\Menu Démarrer\Programmes\Citrix\.
   Ordinateurs autres que Windows Vista : à l'aide de l'explorateur Windows, accédez à %SystemDrive%\Documents and Settings\All Users\Menu Démarrer\Programmes\Citrix\.
2. Dans le menu Fichier, sélectionnez Nouveau > Raccourci. L'assistant Création d'un raccourci s'affiche.
3. Cliquez sur Parcourir.
4. Accédez à %InstallationDirectory%\Program Files\Citrix\Metaframe Password Manager\, sélectionnez ssoShell.exe et

cliquez sur OK. La boîte de dialogue Rechercher un dossier se ferme et le chemin d'accès vers ssoShell.exe s'affiche dans le champ Entrez l'emplacement de l'élément.

5. Dans le champ Entrez l'emplacement de l'élément, placez le point d'insertion après ssoShell.exe et tapez un espace suivi de /qbaenroll (J).



6. Cliquez sur Suivant.
7. Tapez Enregistrement aux fonctions autonomes de compte Citrix cliquez sur Terminer.

Le raccourci s'affiche dans Démarrer > Tous les programmes > Citrix.

Pour supprimer le raccourci Single Sign-On

Durant l'installation du logiciel Single Sign-On Plug-in, un raccourci est placé dans le menu Démarrer. Si un utilisateur configuré pour utiliser uniquement les fonctions autonomes de compte sélectionne cette commande, ssoShell.exe se lance et se ferme, à moins que des modifications aient été apportées à l'authentification avec questions de l'utilisateur. Cela peut prêter à confusion pour l'utilisateur et entraîner un accroissement des appels passés à l'assistance. Pour éviter ce problème, supprimez le raccourci du menu Démarrer.

1. Ordinateurs Windows Vista : à l'aide de l'explorateur Windows, accédez à %SystemDrive%\ProgramData\Microsoft\Windows\Menu Démarrer\Programmes\Citrix\.
   Ordinateurs autres que Windows Vista : à l'aide de l'explorateur Windows, accédez à %SystemDrive%\Documents and Settings\All Users\Menu Démarrer\Programmes\Citrix\.
2. Supprimez le raccourci Single Sign-On.

Le raccourci Single Sign-On est supprimé du menu Démarrer.

Pour supprimer le raccourci Single Sign-On Plug-in du dossier Démarrage

Supprimez le raccourci Single Sign-On Plug-in sur la machine utilisateur pour empêcher le plug-in de démarrer chaque fois que l'utilisateur ouvre une session sur l'ordinateur. Cette tâche permet d'éviter que l'utilisateur ne consomme une licence inutilement.

1. À l'aide de l'explorateur Windows, accédez à %SystemDrive%\Documents and Settings\All Users\Menu Démarrer\Programmes\Démarrage.
2. À partir du dossier Démarrage, supprimez Single sign-on plug-in Background Process.
   Remarque : si le plug-in est installé sur Citrix Presentation Server ou un environnement Terminal Server, la sous-clé de registre AppSetup, qui se trouve dans HKLM\SOFTWARE\microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup doit être modifiée pour supprimer la référence à Password Manager ou Single Sign-On.

Le raccourci Single Sign-On Plug-in ne se lance plus automatiquement lorsqu'un utilisateur ouvre une session.

Automatisation de la saisie des informations d'identification à l'aide de l'habilitation

Oct 21, 2015

Utilisez le module d'habilitation pour manipuler les informations d'identification associées aux applications définies dans une configuration utilisateur. L'habilitation vous permet d'automatiser ces procédures et de les appliquer à plusieurs utilisateurs. Si vous souhaitez mettre un nouveau logiciel à disposition de vos utilisateurs, vous pouvez simplement créer une définition pour l'application et utiliser l'habilitation pour ajouter les informations d'identification de tous les utilisateurs qui l'utiliseront.

Récapitulatif des tâches d'habilitation

Pour manipuler les informations d'identification de votre magasin central pour les applications SSO contenues dans des configurations utilisateur, vous devez effectuer les tâches suivantes.

1. Installer le module d'habilitation du service Single Sign-On.
2. Créer une configuration utilisateur impliquant le service d'habilitation.
3. Générer un modèle d'habilitation.
4. Remplir le modèle à l'aide d'informations d'identification et choisir une commande à exécuter.
5. Traiter les données d'habilitation.

Important : le fichier XML utilisé pour fournir les informations d'identification contient des informations utilisateur sensibles. Pensez à supprimer ce fichier ou à le transférer vers un emplacement sécurisé lorsque l'habilitation est terminée.
Après ajout, suppression ou modification des informations d'identification dans le magasin central, celles-ci sont prêtes à être utilisées dans votre environnement. À l'ouverture du plug-in, les informations d'identification sont mises à jour dans le plug-in et les applications sont mises à disposition des utilisateurs.

L'ajout, la modification ou la suppression des informations d'identification dans le magasin central peuvent requérir une grande quantité de ressources système. Lorsque cela est possible, procédez à l'habilitation durant les heures creuses.

Kit de développement logiciel (SDK) de l'habilitation

Si vous devez manipuler les informations d'identification d'un grand nombre d'utilisateurs, pensez à utiliser le kit de développement logiciel (SDK) de l'habilitation. Le kit de développement logiciel (SDK) fournit une description des API disponibles après installation du module d'habilitation du service Single Sign-On. Vous pouvez utiliser le SDK et les exemples de code inclus pour créer vos propres clients d'habilitation destinés à être utilisés avec Single Sign-On.

Génération d'un modèle d'habilitation

la procédure suivante implique que vous ayez créé une configuration utilisateur comprenant au moins l'un des éléments suivants : définition d'application, groupe d'applications, stratégie de mot de passe (incluant éventuellement un groupe optionnel de partage de mot de passe) et activation de l'habilitation dans la configuration utilisateur.

Un modèle d'habilitation est un document XML contenant des informations relatives aux applications incluses dans la configuration utilisateur sélectionnée.

- Groupe d'applications
- Nom et identificateur global unique de la définition d'application
- Informations utilisateur telles que le nom d'utilisateur et le mot de passe

Il inclut également des commandes d'ajout, de suppression et de modification à utiliser lors de l'emploi du modèle modifié dans la console Password Manager pour exécuter l'habilitation.

Le modèle obtenu inclut des exemples d'informations de commande et des informations spécifiques sur la configuration utilisateur sélectionnée.

Pour générer un modèle d'habilitation

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et sélectionnez Configurations utilisateur.
3. Sélectionnez une configuration utilisateur.
4. À partir du menu Action, cliquez sur Générer le modèle d'habilitation.
5. Dans la boîte de dialogue Générer le modèle d'habilitation, entrez un nom pour le modèle.

Pour traiter votre modèle d'habilitation

Utilisez le composant Single Sign-On de Citrix AppCenter pour effectuer les tâches de provisioning du fichier XML. Single Sign-On valide la syntaxe de chaque commande, exécute les commandes et ajoute ou modifie les données du magasin central.

Attention : ne fermez pas l'écran de l'habilitation tant que ce processus n'est pas terminé. Cela n'entraîne pas la fin du processus. Néanmoins, il devient alors impossible de recueillir quelque information que ce soit ou de suspendre le processus.

1. Cliquez sur Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter.
2. Développez le nœud Single Sign-On et développez Configurations utilisateur.
3. Sélectionnez une configuration utilisateur ou un groupe d'applications d'une configuration utilisateur.
4. À partir du menu Action, cliquez sur Exécuter l'habilitation. L'assistant d'habilitation s'affiche.
5. Cliquez sur Suivant.
6. Entrez le nom de votre fichier XML d'habilitation ou cliquez sur le bouton Parcourir pour le rechercher, puis cliquez sur Suivant. Single Sign-On valide le fichier XML.
   - Si aucune erreur de syntaxe n'est détectée, un récapitulatif des modifications possibles est présenté. Vous pouvez enregistrer ce récapitulatif.
   - Si des erreurs de syntaxe ou autres sont trouvées, un journal des erreurs s'affiche. Vous pouvez l'enregistrer, puis cliquer sur Annuler pour fermer l'assistant.
7. Si aucune erreur n'est trouvée, cliquez sur Suivant pour exécuter les commandes du fichier. Étant donné que les informations sont modifiées dans le magasin central, toute erreur résultant de l'habilitation est affichée. Pour arrêter l'habilitation en cours, cliquez sur Abandonner. Lorsque Single Sign-On atteint la fin de la section de données en cours de traitement (par défaut, les données sont traitées par groupes de 50 lignes de code), le provisioning se termine.

Une fois l'assistant terminé, vous pouvez enregistrer les résultats de l'habilitation.

Réglage manuel du traitement de l'habilitation

Attention : cette procédure nécessite que vous modifiiez le registre. Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Faites toujours une copie de sauvegarde du registre système avant de continuer.
Par défaut, si vous utilisez Single Sign-On pour le provisioning, vos informations sont traitées par lot de 50 commandes en respectant un temps d'arrêt de 100 000 milli-secondes. Vous pouvez modifier ces valeurs par défaut dans les clés de registre suivantes :

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Console\Provisioning\BatchSize

Type : DWORD

Valeur par défaut : 50

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Console\Provisioning\ServiceTimeout

Type : DWORD

Valeur par défaut en millisecondes : 100000

Modification du modèle d'habilitation

Oct 21, 2015

utilisez un éditeur de texte ou un éditeur de fichier XML pour modifier le modèle généré. Le modèle d'habilitation utilise le langage SPML (Service Provisioning Markup Language), qui est une norme XML conçue pour l'échange de données. Comme pour le langage XML, veillez que chaque balise ou élément SPML (par exemple, la balise) soit formé correctement et soit conforme aux règles syntaxiques XML. Par exemple, pour supprimer des caractères de commentaire tels que !-- et --, veillez à supprimer tout crochet supplémentaire (< ou >) afin d'éviter des erreurs lors du traitement du modèle d'habilitation. Pour obtenir des informations détaillées sur le langage XML, veuillez consulter le site Web de W3C à l'adresse http://www.w3.org/. Veillez à supprimer les caractères de commentaire (!-- et --), le cas échéant.

Exemple de fichier généré

Le modèle généré comprend les éléments suivants :

- informations relatives à l'utilisateur ayant généré le modèle ;
- commande pour le nom d'application inclus dans la configuration utilisateur ;
- commande accompagnée du nom de la définition d'application.

Vers la fin du fichier XML figurent des informations propres à la configuration utilisateur sélectionnée, que vous pouvez copier et utiliser dans votre modèle. Par exemple :

Par exemple, vous pouvez copier les informations utilisateur situées entre les balises et , en retirer les marques de commentaire, puis les modifier pour chaque utilisateur dont vous souhaitez ajouter les informations d'identification.

Remarque : dans l'exemple ci-dessus, représente le domaine et le nom de l'utilisateur ayant généré le modèle. Vous pouvez ajouter des commentaires à ces informations ou les supprimer si vous ne souhaitez pas les enregistrer dans le modèle.

La balise cpm-provision

Notez que vous devez inclure vos balises et commandes dans la balise d'habilitation (située vers la ligne 70 du fichier XML généré) :

insérer ici la balise et les commandes

La balise user

Utilisez la balise pour ajouter les informations de domaine et de nom de chaque utilisateur dont vous souhaitez fournir les informations d'identification d'application. Vous devez fournir une balise pour chaque utilisateur à habiliter. Chaque balise contient également les commandes à exécuter sur le compte de cet utilisateur.

La syntaxe de cette commande est la suivante.

votreDomaine\idUtilisateur"> <commande>
où :

votreDomaine	Indique le nom de domaine de l'utilisateur à ajouter.
IDUtilisateur	Indique le nom d'utilisateur à ajouter.
commande	Indique une ou plusieurs commandes à exécuter sur cet utilisateur : • • • • • •

La commande add

La commande vous permet d'ajouter un nom d'utilisateur et mot de passe requis pour les applications incluses dans la configuration utilisateur.

La syntaxe de cette commande est la suivante.

%NOMAPPLI%">%GUIDAPP% DescriptionLongue%NOMINFOIDENTIFICATION% DescriptionLongue %NOMAPPLI% description masquée ID utilisateur motdepasse %TEXTELÉGENDES%">champ
où :

	Obligatoire. L'élément et ses attributs sont en principe générés automatiquement à la génération d'un modèle. L'attribut name= est facultatif. • %NOMAPPLI% est le nom de la définition d'application incluse dans la configuration utilisateur sélectionnée. • %APPGUID% est l'identificateur global unique de l'application et doit concorder.
	Obligatoire. L'élément et ses attributs sont en principe générés automatiquement. • %NOMINFOIDENTIFICATION% est le nom de l'application incluse dans la définition d'application.
	Facultatif. Entrez un texte décrivant la configuration utilisateur.
	Facultatif. Entrez le texte de votre choix.
	Obligatoire. userid est le nom d'utilisateur de l'utilisateur à ajouter.

	Obligatoire. password est le mot de passe de l'utilisateur à ajouter.
	Obligatoire si un autre champ est requis pour l'authentification (par exemple, champ dans lequel l'utilisateur doit entrer le domaine). Utilisez autant de champs personnalisés que le requiert l'application.

La commande modify

La commande vous permet de modifier un nom d'utilisateur et mot de passe requis pour les applications incluses dans la configuration utilisateur.

Important : cette commande requiert les informations d'identification de l'utilisateur. Vous pouvez récupérer ces informations d'identification à l'aide de la commande avant d'utiliser la commande . Incluez uniquement les éléments à modifier.

- Pour laisser une valeur inchangée, supprimez la ligne correspondante. Par exemple, supprimez l'élément pour conserver le nom de l'application.
- Pour modifier une valeur, spécifiez la valeur dans le modèle. Par exemple, incluez l'élément pour spécifier un nouveau nom d'application.
- Une valeur est effacée en incluant l'élément sans insérer de valeur. Par exemple, utilisez pour supprimer la description actuelle.

La syntaxe de cette commande est la suivante.

%ID-INFOIDENTIFICATION% %NOMINFOIDENTIFICATION% DescriptionLongue %NOMAPPLI% description masquée ID utilisateur motdepasse %TEXTELÉGENDE%"> champ personnalisé 1 %TE

où :

	Obligatoire. La valeur de l'identificateur global unique des informations d'identification %ID-INFOIDENTIFICATION% de l'utilisateur doit correspondre à la valeur renvoyée par une commande .
	Facultatif. L'élément et ses attributs sont en principe générés automatiquement. • %NOMINFOIDENTIFICATION% est le nom de l'application incluse dans la définition d'application.
	Facultatif. Entrez un texte décrivant la configuration utilisateur.
	Facultatif. Entrez le texte de votre choix.
	Obligatoire. userid est le nom d'utilisateur de l'utilisateur à modifier.
	Obligatoire. password est le mot de passe de l'utilisateur à modifier.
	Obligatoire si un autre champ est requis pour l'authentification (par exemple, champ dans lequel l'utilisateur doit entrer le domaine). Utilisez autant de champs personnalisés que le requiert l'application.

La commande delete

La commande vous permet de supprimer les informations d'identification d'un utilisateur pour une application SSO particulière.

Important : cette commande requiert les informations d'identification de l'utilisateur. Vous pouvez récupérer ces informations d'identification à l'aide de la commande avant d'utiliser la commande . La syntaxe de cette commande est la suivante.

votreDomaine\IDUtilisateur"> %ID-INFOIDENTIFENTIFICATION%

où :

votreDomaine	Indique le nom de domaine de l'utilisateur.
IDUtilisateur	Indique le nom de l'utilisateur.
	Obligatoire. La valeur de l'identificateur global unique des informations d'identification %ID-INFOIDENTIFICATION% de l'utilisateur doit correspondre à la valeur renvoyée par une commande .

La commande remove

La commande vous permet de supprimer des données et informations utilisateur du magasin central. Utilisez cette commande lorsqu'un utilisateur quitte définitivement votre entreprise. Le magasin local d'informations d'identification de la machine utilisateur reste intact jusqu'à sa suppression par un administrateur ou un opérateur.

La syntaxe de cette commande est la suivante.

votreDomaine\IDUtilisateur">

où :

votreDomaine	Indique le nom de domaine de l'utilisateur.
IDUtilisateur	Indique le nom de l'utilisateur.

Remarque : cette commande est identique à la tâche Supprimer les données utilisateur du magasin central de Single Sign-On effectuée à partir de Citrix AppCenter.

La commande reset

La commande vous permet de réinitialiser les informations utilisateur de votre magasin central, ce qui a pour effet de renvoyer l'utilisateur sélectionné à son état initial. Dans le cas de magasins centraux autres que Active Directory, les dossiers de l'utilisateur sont conservés, mais toutes ses données (par exemple, informations d'identification, questions et réponses d'enregistrement) sont supprimées. Dans le cas de magasins centraux Active Directory, les données de l'utilisateur sont supprimées et l'utilisateur est marqué de l'indicateur de réinitialisation des données.

La syntaxe de cette commande est la suivante.

votreDomaine\IDUtilisateur">

où :

votreDomaine	Indique le nom de domaine de l'utilisateur.

IDUtilisateur	Indique le nom de l'utilisateur.

Remarque : cette commande est identique à la tâche Réinitialiser les données utilisateur de Single Sign-On effectuée à partir de Citrix AppCenter.

La commande list-credentials

La commande vous permet de récupérer les informations d'identification d'un utilisateur particulier pour chaque application de la configuration utilisateur associée. Les commandes et nécessitent d'utiliser l'identificateur global unique des informations d'identification récupérées comme valeur du paramètre %ID-INFOIDENTIFICATION%.

Le numéro d'identification récupéré par cette commande est un identificateur global unique d'informations d'identification (par exemple, 634EE015-10C2-4ed2-80F5-75CCA9AA5C11).

La syntaxe de cette commande est la suivante.

votreDomaine\IDUtilisateur">
où :

votreDomaine	Indique le nom de domaine de l'utilisateur.
IDUtilisateur	Indique le nom de l'utilisateur.

Le Bureau dynamique: un environnement de bureau partagé destiné aux utilisateurs

Oct 21, 2015

Le Bureau dynamique offre à la fois une rotation accélérée des utilisateurs et une sécurité supplémentaire grâce à l'accès à l'authentification unique de Single Sign-On. Cette fonctionnalité n'est pas installée par défaut, vous pouvez la sélectionner pendant l'installation de Single Sign-On Plug-in. Vous pouvez également mettre à niveau les déploiements Single Sign-On Plug-in existants afin d'utiliser le Bureau dynamique. Toutefois, avant de pouvoir implémenter le Bureau dynamique, vous devez le configurer selon les besoins de votre environnement et de votre entreprise.

Le Bureau dynamique est uniquement pris en charge sur les systèmes d'exploitation suivants :

- Microsoft Windows XP Professionnel Service Pack 2, 32 bits
- Microsoft Windows XP Embedded

Il n'est pas pris en charge par les systèmes d'exploitation 64 bits ou tout système d'exploitation serveur.

Le Bureau dynamique n'est pas disponible lorsque Single Sign-On est déployé via Citrix Receiver Updater.

La fonction Bureau dynamique de Single Sign-On permet aux utilisateurs de partager leur station de travail de façon sûre et efficace. Le Bureau dynamique étend l'environnement Windows standard en permettant aux utilisateurs de :

- s'authentifier rapidement auprès de Windows à l'aide de la boîte de dialogue d'ouverture de session interactive GINA ;
- exécuter des applications activées par authentification unique dans le shell interactif de l'utilisateur en utilisant ses informations d'identification Single Sign-On ;
- se déconnecter de la station de travail Bureau dynamique pour que d'autres utilisateurs puissent exécuter des applications.

Récapitulatif des tâches du Bureau dynamique

Avant la mise en place de cette fonctionnalité, vous devez :

- créer un compte Bureau dynamique partagé ;
- créer des configurations utilisateur avec des paramètres de Bureau dynamique spécifiques définissant l'expérience de l'utilisateur ;
- définir le comportement du Bureau dynamique au démarrage et à la fermeture, y compris :
  - Les applications qui doivent être lancées au démarrage et les applications qui doivent utiliser les informations d'identification et autorisations du compte utilisateur ou du compte Bureau dynamique partagé.
  - Les applications qui sont persistantes et qui doivent être exécutées même lorsque les utilisateurs se déconnectent (pour permettre la rotation accélérée des utilisateurs) et les applications qui doivent être fermées lorsque l'utilisateur se déconnecte, y compris les scripts et applications de nettoyage facultatifs qui suppriment les informations de l'utilisateur d'une session à une autre.

Pour configurer et activer le Bureau dynamique, effectuez les tâches suivantes :

1. Créez un compte Bureau dynamique partagé accessible à chaque station de travail ou machine cliente exécutant le Bureau dynamique.
2. Déterminez quelles applications activées par SSO doivent être exécutées dans l'environnement Bureau dynamique.

3. Déterminez quelles applications sont exécutées dans le Bureau dynamique et configurez l'environnement utilisateur du Bureau dynamique.
4. Créez ou modifiez une configuration utilisateur pour sélectionner des options Bureau dynamique.
5. Installez le plug-in en sélectionnant la fonction Bureau dynamique.
6. Désinstallez le Bureau dynamique si nécessaire.

Processus de démarrage et de fermeture du Bureau dynamique

Ce processus décrit les événements associés au démarrage et à la fermeture du Bureau dynamique. Lorsque la station de travail ou la machine cliente démarre, une session est automatiquement ouverte avec le compte partagé, ce qui permet une exécution en mode de bureau partagé.

Remarque : le compte partagé reste ouvert tout le temps. Les utilisateurs ne sont pas autorisés à le fermer.

1. Un utilisateur du Bureau dynamique ouvre une session sur la machine de travail et entre un nom d'utilisateur et un mot de passe ou utilise un système d'authentification renforcée, telle qu'une carte à puce.
2. Après authentification, la session du Bureau dynamique démarre.
3. Single Sign-On démarre. Le plug-in synchronise ses données avec celles du magasin central. Ainsi, l'utilisateur dispose des définitions d'application, des stratégies de mot de passe et autres réglages du plug-in les plus récents.
4. Le système lit le fichier session.xml et démarre les applications définies pour une exécution avec le compte partagé ou le compte d'utilisateur du Bureau dynamique. Il peut s'agir d'applications locales ou distantes publiées par XenApp. L'utilisateur accède aux applications pour effectuer les tâches liées à sa fonction.
5. L'utilisateur du Bureau dynamique ferme sa session.
   Remarque : lorsque la machine de travail n'est pas utilisée, le Bureau dynamique lance un compteur d'expiration. Dans la Console Access Management, vous pouvez spécifier un délai d'expiration pour une machine de travail inactive. Si ce délai est dépassé, le Bureau dynamique verrouille la machine de travail. Après un intervalle supplémentaire d'inactivité, le Bureau dynamique met fin à la session.
6. Le Bureau dynamique laisse les applications ouvertes ou les ferme selon les paramètres définis dans process.xml.
7. Single Sign-On se ferme.
8. Tous les scripts de fermeture spécifiés dans le fichier session.xml sont exécutés.
9. La session du Bureau dynamique est fermée.

Résolution des problèmes de démarrage utilisateur du Bureau dynamique

Lorsqu'un utilisateur se connecte à un ordinateur exécutant Single Sign-On configuré pour le Bureau dynamique, il est possible que les scripts de démarrage spécifiés dans le fichier session.xml soient exécutés avant que Single Sign-On Plug-in ne soit complètement lancé.

Au cours du démarrage, le Bureau dynamique attend 30 secondes que le plug-in démarre avant de lancer les scripts de démarrage. Au bout de 30 secondes, les scripts de démarrage sont exécutés, même si le lancement du plug-in n'est pas complètement terminé.

Cette situation est plus susceptible de se produire durant la connexion initiale de l'utilisateur (également appelé utilisateur initial), lorsque l'administrateur Single Sign-On a identifié une liste d'applications qui requièrent des informations d'identification ou des réponses à des questions de sécurité. Dans ce cas, la séquence d'événements est la suivante :

1. L'utilisateur se connecte à l'ordinateur ou à la machine cliente exécutant le plug-in et est invité à enregistrer ses informations d'identification pour les applications indiquées ou à entrer des réponses aux questions de sécurité.
2. Pendant que l'utilisateur effectue ces tâches, 30 secondes sont écoulées et les scripts de démarrage du Bureau dynamique sont exécutés. Il est possible qu'une série de fenêtres s'affichent et se ferment, selon les applications

spécifiées dans les scripts de démarrage du fichier session.xml.
3. Cette situation peut être frustrante pour l'utilisateur car l'ordinateur active constamment les fenêtres de scripts de démarrage.
4. Une fois que les scripts de démarrage sont terminés, un message d'erreur s'affiche. Ce message d'erreur est similaire à : « Une ou plusieurs erreurs se sont produites. Consultez le journal des événements pour plus d'informations ».

Bien que ce comportement soit frustrant pour l'utilisateur, il n'a aucun effet néfaste sur les données de l'utilisateur, l'environnement de travail ou Single Sign-On.

Conseillez aux utilisateurs de ne pas enregistrer leurs informations d'identification d'ouverture de session ni les réponses aux questions de sécurité tant que le message d'erreur ne s'affiche pas. Ils peuvent alors fermer le message d'erreur et procéder à l'enregistrement.

Après la fermeture du message d'erreur et l'enregistrement, si une application spécifiée dans session.xml ne s'ouvre pas, indiquez à l'utilisateur de se déconnecter, puis de se reconnecter au compte. Cette opération redémarre les scripts de démarrage du Bureau dynamique et les exécute sans interruption étant donné que l'enregistrement est à présent terminé et ne retarde pas le processus.

Création d'un compte partagé de Bureau dynamique

Vous devez créer un compte partagé de Bureau dynamique pour les machines clientes ou les stations de travail sur lesquelles sera exécutée cette fonctionnalité. Ce compte partagé peut être un compte de domaine ou un compte local sur la machine. Lorsque vous installez le Bureau dynamique sur la machine cliente, vous devez fournir des informations d'identification pour le compte partagé. Lorsque la station de travail ou la machine cliente démarre, une session est automatiquement ouverte avec le compte partagé, ce qui permet une exécution en mode de bureau partagé.

Les sessions utilisateur sont exécutées « par-dessus » la session Windows du compte partagé. Les utilisateurs ne peuvent pas modifier le compte partagé à moins que vous ne leur en donniez l'autorisation. Les utilisateurs démarrent une session du Bureau dynamique en entrant leurs informations d'identification de domaine Windows. Un compte d'utilisateur Windows est appelé utilisateur du Bureau dynamique dans l'environnement du Bureau dynamique.

Organisation des utilisateurs du Bureau dynamique

Si vous envisagez de déployer le Bureau dynamique, il peut être utile de configurer d'abord l'environnement utilisateur. Par exemple, vous pouvez grouper les utilisateurs du Bureau partagé dans une ou plusieurs unités organisationnelles ou groupes Active Directory. En outre, vous pouvez organiser les utilisateurs qui utilisent à la fois le Bureau dynamique et leur propre station de travail en plusieurs groupes (et définir leur priorité).

Cette méthode vous permet d'appliquer les paramètres, les définitions d'applications, les stratégies de mot de passe et d'autres informations de configuration du Bureau dynamique aux utilisateurs de ces unités organisationnelles.

Restrictions des droits des utilisateurs

Une machine du Bureau dynamique est partagée par tous les utilisateurs du Bureau dynamique. Il peut donc être nécessaire de restreindre les autorisations au strict minimum requis pour utiliser les applications spécifiées. Par exemple, les utilisateurs du Bureau dynamique ne doivent pas être en mesure d'arrêter la machine. Ce privilège doit être réservé au groupe des administrateurs.

Bureau dynamique, cartes à puce et récupération de clé

Remarque : sélectionnez l'option de protection des données de configurations de l'utilisateur Certificat de carte à puce si les utilisateurs utilisent des cartes à puce dans l'environnement du Bureau dynamique.
Si vous déployez le Bureau dynamique dans un environnement où les utilisateurs se connectent à l'aide de cartes à puce, ne sélectionnez pas l'option Saisie du mot de passe précédent comme seule méthode de récupération de clé et de protection des données pour ces utilisateurs. Les utilisateurs utilisant ce type d'environnement ne peuvent pas entrer l'ancien mot de passe correct et risquent d'être verrouillés hors du système. Pour éviter ce problème, sélectionnez l'option de récupération de clé pour la gestion de clés automatique ou autorisez également l'authentification basée sur des questions.

Instructions sur la création du compte partagé de Bureau dynamique

Suivez les instructions suivantes pour créer le compte partagé.

- Vérifiez que le compte n'appartient pas au groupe Administrateurs du domaine ou local.
- Ce compte partagé peut être un compte local ou de domaine. Tous les privilèges disponibles pour le compte partagé sont uniquement accessibles aux utilisateurs du Bureau dynamique pour les applications que vous spécifiez. En d'autres termes, vous pouvez déterminer quelles applications sont lancées avec les informations d'identification du compte partagé du Bureau dynamique et quelles applications sont lancées avec les informations d'identification de domaine Windows de l'utilisateur.
- L'installation du Bureau dynamique entraîne la vérification du nom d'utilisateur et du domaine du compte partagé. Lorsque vous créez ce compte, assurez-vous que vous sélectionnez l'option Le mot de passe n'expire pas. N'utilisez pas des informations d'identification expirées.
- Vérifiez que le compte dispose de droits d'accès limités. Limiter les permissions à l'utilisation du Bureau dynamique seulement.
- Indiquez le nom du domaine auquel appartient la machine, au format NetBIOS et non sous forme de nom de domaine complet (FQDN). Si vous utilisez un compte local, indiquez le nom d'hôte de la machine.
- En règle générale, il est préférable de nommer le compte partagé « Bureau dynamique ». Ainsi, les utilisateurs voient s'afficher un message de fermeture de session au Bureau dynamique lorsqu'ils ferment leur session. Si vous utilisez un nom obscur, les utilisateurs le voient s'afficher lors de la fermeture de session et peuvent ne pas comprendre. Si vous disposez de plusieurs groupes d'utilisateurs du Bureau dynamique, vous pouvez nommer chaque compte partagé en conséquence, par exemple : « Bureau partagé Marketing », « Bureau partagé Comptabilité », etc.

Conditions requises pour les applications utilisées dans le Bureau dynamique

Les applications utilisées dans l'environnement Bureau dynamique doivent répondre aux critères suivants.

- Les applications nécessitant des informations d'identification utilisateur doivent être définies en vue d'une utilisation avec Single Sign-On dans les définitions d'applications et les configurations utilisateur.
- Les applications lancées à l'aide du compte partagé doivent pouvoir être exécutées dans l'environnement interactif Windows. Dans cette situation, les applications (et les utilisateurs du Bureau dynamique) doivent avoir accès aux profils utilisateur, aux partages réseau et aux autres ressources associées au compte partagé.
- Les applications doivent s'arrêter normalement lorsqu'elles en reçoivent la demande. Le Bureau dynamique met fin aux applications selon des procédures similaires à une fermeture de session interactive Windows. Cette fermeture normale est particulièrement importante dans l'environnement Bureau dynamique car l'application peut être utilisée plusieurs fois avant l'arrêt de la station de travail ou machine cliente.
- Toute application qui doit enregistrer des données sensibles dans le profil utilisateur ou qui doit accéder au profil utilisateur pour des réglages doit être exécutée avec le compte d'utilisateur du Bureau dynamique. Les applications pouvant partager des informations de configuration peuvent être exécutées avec le compte partagé. Les administrateurs peuvent utiliser un script d'arrêt de session spécifié dans le fichier session.xml pour s'assurer que les fichiers propres aux utilisateurs sont supprimés à la fin de chaque session.

Important : si vous souhaitez que Single Sign-On soumette des informations d'identification dans un environnement de Bureau dynamique pour les émulateurs de terminal qui stockent des informations dans la clé HKEY_CURRENT_USER, vous devez exécuter ces applications avec le compte d'utilisateur du Bureau dynamique. Indiquez les émulateurs de terminal à exécuter avec le compte d'utilisateur du Bureau dynamique dans la section ShellExecute du fichier process.xml. Pour exécuter un émulateur de terminal au démarrage de session, désignez-le dans la section de script de démarrage du fichier session.xml. Les émulateurs de terminal doivent être exécutés avec le compte d'utilisateur du Bureau dynamique dans le script de démarrage.

Définition du comportement des applications pour les utilisateurs du Bureau dynamique

Single Sign-On fournit deux fichiers permettant de définir le comportement des applications dans un environnement Bureau dynamique : session.xml et process.xml.

Important : vous ne pouvez pas indiquer à la fois qu'un processus doit être exécuté comme un compte partagé du Bureau dynamique dans le fichier session.xml et qu'il doit être exécuté en tant qu'utilisateur de Bureau dynamique (HDU) dans le fichier process.xml. Les entrées du fichier session.xml remplacent celles de l'élément du fichier process.xml.
Avant de commencer :

- Pour vous connecter à la station de travail ou à la machine utilisateur pour des besoins d'administration (par exemple, pour modifier le fichier process.xml), maintenez la touche MAJ enfoncée durant le processus de démarrage de Windows. Pour plus d'informations sur le contournement de l'ouverture de session Windows automatique, veuillez consulter le site Web Microsoft.
- Les variables d'environnement suivantes ne sont pas prises en charge lors de l'exécution des scripts du fichier session.xml, des scripts d'expiration du mot de passe ou de tout autre script, fichier exécutable ou fichier de traitement par lots depuis une session utilisateur du Bureau dynamique : APPDATA, HOMEDRIVE, HOMEPATH, HOMESHARE et LOGONSERVER. Si l'une des variables non prises en charge est utilisée, le script, l'application ou le fichier exécutable risque de ne pas être exécuté. Pour éviter ce problème, il est préférable que les applications n'accèdent pas aux variables d'environnement non prises en charge pendant la durée d'une session utilisateur du Bureau dynamique.
- Vous devez expliquer aux utilisateurs qu'ils doivent fermer les applications désignées comme étant des processus persistants. Par exemple, si un utilisateur lance un processus persistant, crée un fichier puis laisse le fichier ouvert lorsqu'il ferme sa session du Bureau dynamique, le prochain utilisateur qui ouvre une session peut accéder au contenu du fichier.
  Important : indiquez aux utilisateurs de veiller à toujours fermer les applications dont le contenu est sensible et qui sont définies comme des processus persistants, avant de mettre fin à leur session du Bureau dynamique.
  Lorsque vous définissez une application comme un processus persistant dans process.xml et comme script de démarrage dans session.xml, le nombre d'instances de l'application risque d'augmenter si les utilisateurs ne ferment pas les nouvelles instances d'une session du Bureau dynamique. Pour éviter cela, limitez le nombre d'instances en créant un script ou une application générale qui lance l'application. Vous pouvez également modifier l'application elle-même pour garantir qu'une seule instance est exécutée à tout moment.

- Les applications lancées à partir d'une invite de commande sont exécutées avec le compte partagé même si elles sont spécifiées avec le compte d'utilisateur du Bureau dynamique. Pour exécuter des applications à partir de l'invite de commande avec le compte d'utilisateur du Bureau dynamique, vous devez spécifier l'invite de commande dans la section du fichier process.xml. De même, si l'invite de commande est exécutée avec le compte partagé, si l'association de type de fichier (par exemple, *.txt) est définie dans la section du fichier process.xml et si l'utilisateur exécute un fichier ayant l'extension .txt, l'application est exécutée avec le compte d'utilisateur du Bureau dynamique.
- Les applications persistantes utilisant le format de fichier 8.3 doivent utiliser ce format dans le chemin d'accès de l'exécutable spécifié dans le fichier process.xml.
- Les balises XML et la mise en forme du fichier process.xml prennent en compte la casse, contrairement aux chemins d'accès et aux noms d'exécutable.

- Si vos utilisateurs exécutent SAP Logon for Windows (saplogon.exe), ce fichier doit être exécuté en tant qu'utilisateur du Bureau dynamique. Dans le fichier process.xml, spécifiez saplogon.exe dans la balise .

Paramètres de configuration utilisateur du Bureau dynamique

Oct 21, 2015

Les paramètres de configuration utilisateur vous permettent de contrôler l'expérience utilisateur du Bureau dynamique.

Attention : certaines procédures nécessitent que vous modifiiez le registre. Toute utilisation incorrecte de l'Éditeur du Registre peut générer des problèmes sérieux, pouvant vous obliger à réinstaller le système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Faites toujours une copie de sauvegarde du registre système avant de continuer.

Chemin d'accès du fichier de paramètres de scripts de session

Localisez les paramètres du Bureau dynamique dans une configuration utilisateur :

- Lorsque vous créez une nouvelle configuration utilisateur, ces paramètres sont disponibles dans la zone Paramètres avancés de la boîte de dialogue Configuration de l'interaction du plug-in.
- Lorsque vous modifiez une configuration utilisateur existante, ces paramètres s'affichent dans le volet Bureau dynamique de la boîte de dialogue Modification de la configuration utilisateur.
  Pour obtenir les détails des paramètres, consultez la rubrique du Bureau dynamique située sous
  — Liste de référence des paramètres de Single Sign-On > Configurations de l'utilisateur
  .

Pour configurer le chemin d'accès au fichier de paramètres de scripts de session

1. Dans la page Bureau dynamique de la boîte de dialogue Modification de la configuration utilisateur, dans la zone de texte Chemin d'accès du fichier de paramètres de scripts de session, tapez l'emplacement du fichier session.xml. Cet emplacement peut être un dossier de réseau partagé. Par exemple, si vous placez votre fichier session.xml sur un point de partage réseau tel que \\Citrix\MPM\Share\, tapez ce chemin d'accès ici.
2. Redémarrez la station de travail Bureau dynamique une fois que vous avez enregistré la configuration utilisateur et installé le fichier session.xml.

Interaction avec la récupération de clé automatique

dans un environnement Single Sign-On utilisant la récupération de clé automatique en combinaison avec le Bureau dynamique, les modifications de mot de passe réalisées par l'administrateur ne sont pas communiquées au plug-in des utilisateurs concernés possédant une session du Bureau dynamique active. Si ces utilisateurs verrouillent puis déverrouillent leur session, ils peuvent être invités à fournir leur mot de passe précédent. Les utilisateurs doivent alors fermer la boîte de dialogue affichée, puis clore et redémarrer la session du Bureau dynamique pour continuer à utiliser le plug-in.

Économiseur d'écran du Bureau dynamique

Pour permettre aux utilisateurs d'identifier facilement les stations de travail exécutant le Bureau dynamique, un économiseur d'écran est inclus avec l'installation du Bureau dynamique. Celui-ci n'est lancé qu'après dix minutes d'inactivité de la machine.

Remarque : une session verrouillée est considérée comme étant active. L'économiseur d'écran est lancé après 10 minutes d'inactivité et après la fermeture de toutes les sessions utilisateur sur la machine.

Pour installer le Bureau dynamique

Le Bureau dynamique peut être installé avec une nouvelle installation ou une installation existante de Single Sign-On Plug-in.

1. Ouvrez une session sur la machine utilisateur en tant qu'administrateur local.
2. Dans le Panneau de configuration, sélectionnez Ajout/Suppression de programmes.
3. Sélectionnez Single Sign-On Plug-in et cliquez sur Modifier.
4. Sélectionnez Modifier et cliquez sur Suivant.
5. Sélectionnez Bureau dynamique et cliquez sur Suivant.
6. Cliquez sur Oui sur le message de confirmation pour désactiver les services Terminal Server et le Bureau à distance.
7. Spécifiez l'emplacement du magasin central, puis cliquez sur Suivant.
8. Indiquez l'adresse du serveur de service, puis cliquez sur Suivant.
9. Entrez les informations d'identification pour le compte partagé du Bureau dynamique et cliquez sur le bouton Suivant. Indiquez le nom du domaine auquel appartient la machine, au format NetBIOS et non sous forme de nom de domaine complet (FQDN).
10. Cliquez sur Installer. Accédez au support d'installation pour que le processus d'installation puisse localiser le fichier Single Sign-on Plug-in .msi.

Une fois l'installation terminée, redémarrez la machine utilisateur.

Pour désinstaller le Bureau dynamique

Pour supprimer la fonction Bureau dynamique d'une station de travail, Il se peut que vous deviez également effectuer les procédures suivantes une fois la fonction Bureau dynamique désinstallée :

- Restaurer les services Terminal Server après désinstallation du Bureau dynamique
- Activer les sessions multiples après désinstallation du Bureau dynamique

1. Pour vous connecter à la station de travail ou machine cliente partagée afin d'effectuer des tâches d'administration, maintenez la touche MAJ enfoncée pendant le démarrage de Windows.
   Ceci évite que le compte Bureau dynamique partagé ne soit déconnecté et que l'environnement du Bureau dynamique ne soit démarré. Pour plus d'informations sur le contournement de l'ouverture de session Windows automatique, veuillez consulter le site Web Microsoft.

   Ouvrez une session en tant qu'administrateur.

2. Ouvrez le Panneau de configuration et sélectionnez Ajout/Suppression de programmes.
3. Sélectionnez Single Sign-On Plug-in.
4. Cliquez sur Modifier pour ne supprimer que la fonctionnalité Bureau dynamique.
5. Dans la page Maintenance de l'application, sélectionnez Modifier.
6. Dans la page Sélection de composants, sélectionnez Bureau dynamique et rendez cette fonctionnalité non disponible.
7. Suivez les invites pour sélectionner votre type de magasin central et pour confirmer les changements apportés au plug-in.
8. Redémarrez la station de travail.

Le Bureau dynamique n'est pas complètement supprimé tant que la station de travail n'a pas redémarré.
Important : lors de la désinstallation du logiciel potentiellement responsable de la rupture de la chaîne GINA, il est important de désinstallez le logiciel dans l'ordre inverse de son installation sur la machine cliente. Autrement, l'ordinateur risque de se trouver dans un état non valide. Ne modifiez pas le registre.

Pour activer les services Terminal Server après désinstallation du Bureau dynamique

L'installation du Bureau dynamique entraîne la désactivation des services Terminal Server. Procédez comme suit pour activer les services Terminal Server.

1. Ouvrez une session en tant qu'administrateur sur la station de travail.
2. Cliquez sur Démarrer > Exécuter et tapez regedit.
3. Définissez la valeur de la clé de registre sur 1 comme suit : [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]TSEnabled=dword:00000001

Pour activer des sessions multiples

Lors de l'installation du Bureau dynamique, le programme d'installation réinitialise la valeur de la clé de registre à 0. Procédez comme suit pour activer des sessions multiples.

1. Ouvrez une session en tant qu'administrateur sur la station de travail.
2. Cliquez sur Démarrer > Exécuter et tapez regedit.
3. Changez la valeur de la clé de registre sur 1 comme suit : [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon] AllowMultipleSessions =dword:00000001

Pour afficher les profils du Bureau dynamique

Dans un environnement de Bureau dynamique, le shell (explorer.exe) est exécuté avec le compte partagé du Bureau dynamique. Par conséquent, il ne dispose pas des droits d'accès lui permettant de naviguer vers le dossier de profil de l'utilisateur du Bureau dynamique.

1. Dans le fichier process.xml, sous la section , incluez Internet Explorer (iexplore.exe) afin qu'il soit exécuté avec le compte d'utilisateur du Bureau dynamique.
2. Ouvrez une session en tant qu'utilisateur du Bureau dynamique et lancez Internet Explorer.
3. Pour afficher les profils, entrez le chemin d'accès complet du répertoire des profils d'utilisateur du Bureau dynamique dans la barre d'adresse. Par exemple : C:\Documents and Settings\All Users\Application Data\Citrix\MetaFrame Password Manager

Pour désactiver la prise en charge de la fonction AutoAdminLogon

Certaines systèmes d'authentification tiers peuvent ne pas fonctionner si la fonction AutoAdminLogon est activée. Certaines applications tierces désactivent ou suppriment cette fonction pendant l'installation. Si tel est le cas, vous devez désactiver la fonction AutoAdminLogon du Bureau dynamique.

1. Redémarrez la station de travail ou machine utilisateur partagée, en maintenant la touche MAJ enfoncée durant le processus de démarrage. Ceci évite que le compte Bureau dynamique partagé ne soit déconnecté et que l'environnement du Bureau dynamique ne soit démarré. Pour plus d'informations sur le contournement de l'ouverture de session Windows automatique, veuillez consulter le site Web Microsoft.
2. Ouvrez une session en tant qu'administrateur.
3. Modifiez le registre en définissant les valeurs suivantes pour la clé HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\HotDesktop.

Nom de la valeur	Type	Valeur
AutoAdminLogon	REG_SZ	0 pour désactiver

4. Après définition des valeurs, redémarrez la station de travail et ouvrez manuellement une session à l'aide du compte partagé. La page d'ouverture de session du Bureau dynamique apparaît et permet aux utilisateurs d'utiliser un système

d'authentification tiers.

Pour modifier le mot de passe du compte partagé de Bureau dynamique

À un certain stade, il peut être nécessaire de modifier le mot de passe du compte Bureau dynamique partagé. Vous avez entré pour la première fois les informations d'identification du compte durant l'installation du plug-in. Pour modifier le mot de passe, procédez comme suit.

1. Ouvrez une session sur une station de travail sur laquelle le Bureau dynamique est installé.
   Important : n'utilisez pas un compte administrateur ou les informations d'identification du compte Bureau partagé dans l'étape 1.
2. Appuyez sur la combinaison de touches CTRL+ALT+SUPPR. La boîte de dialogue Sécurité de Windows s'affiche.
3. Cliquez sur Modifier le mot de passe.
4. Tapez ou sélectionnez les informations suivantes :
   - nom d'utilisateur du compte Bureau dynamique partagé ;
   - nom du domaine ou de l'ordinateur local ;
   - ancien mot de passe ;
   - nouveau mot de passe.
5. Cliquez sur OK.
6. Dans la boîte de dialogue Sécurité de Windows, cliquez sur Arrêter le système, puis sur Redémarrer pour redémarrer l'ordinateur.

Pour fermer une station de travail du Bureau dynamique

Les administrateurs étant les seuls autorisés à fermer les stations de travail Bureau dynamique, l'option Arrêter le système n'est pas disponible dans le menu Démarrer de ces stations.

Pour fermer une station de travail Bureau dynamique en vue d'une utilisation administrative, cliquez sur CTRL+ALT+SUPPR. Lorsque la boîte de dialogue Sécurité de Windows s'affiche, cliquez sur Arrêter le système.

Interaction avec les autres produits Citrix

Single Sign-On prend en charge l'utilisation de plug-ins Citrix avec le Bureau dynamique. Utilisez ces points à prendre en considération si vous envisagez d'utiliser le Bureau dynamique avec ces plug-ins et l'Interface Web :

- Modifiez le fichier process.xml pour garantir que Citrix Receiver et Citrix Offline Plug-in sont des processus transitoires (au cas où le plug-in est paramétré pour un lancement par le programme de démarrage de Windows et qu'il est exécuté après le démarrage de la première session du Bureau dynamique).
- Si vous utilisez l'interface SSPI (Security Service Provider Interface), vous devez exécuter le plug-in avec le compte d'utilisateur du Bureau dynamique. Vous pouvez également exécuter le plug-in avec le compte d'utilisateur du Bureau dynamique par souci de sécurité. Les fichiers ICA (Independent Computing Architecture) sont stockés dans le profil.
  - Modifiez la section du fichier process.xml pour garantir que Citrix Receiver et Citrix Offline Plug-in sont exécutés avec le compte d'utilisateur du Bureau dynamique lors de leur lancement à partir du shell Windows.
  - Modifiez le fichier session.xml en spécifiant un script de démarrage ou un exécutable pour lancer Citrix Receiver et Citrix Offline Plug-in lors de l'ouverture de la première session du Bureau dynamique.

Citrix Receiver

Vous pouvez configurer Citrix Receiver afin qu'il utilise l'interface SSPI (Security Support Provider Interface). SSPI permet au Receiver de s'authentifier auprès du serveur XenApp avec les informations d'identification de l'utilisateur du Bureau

dynamique. Vous devez vous assurer qu'une relation de confiance existe entre XenApp et l'autorité de sécurité Windows utilisée pour authentifier l'utilisateur du Bureau dynamique. Pour plus d'informations sur la configuration de SSPI pour Receiver, consultez les rubriques relatives à

— l'administration de XenApp

.

Interface Web

Le plug-in du Bureau dynamique peut soumettre des informations d'identification via l'Interface Web à un serveur XenApp. Pour de plus amples informations, consultez les rubriques

— Interface Web

relatives à la configuration.

Fichier Session.xml

Oct 21, 2015

Utilisez le fichier session.xml pour définir les applications à lancer lors du démarrage d'une session de Bureau dynamique (script de démarrage) et la suppression des fichiers ou autres informations résultant d'une session utilisateur (script d'arrêt). Après avoir modifié ce fichier selon vos besoins, placez-le sur un point de partage réseau ou un autre emplacement central pour que les stations de travail Bureau dynamique puissent y accéder. Spécifiez cet emplacement du fichier session.xml dans la configuration utilisateur.

Vous devez inclure les balises souhaitées à l'intérieur des balises et du fichier.

Remarque : un exemple de fichier session.xml est disponible dans le dossier \Support du support d'installation.

Exemple : nettoyage d'une session à l'aide d'un script

Utilisez un script de fermeture Visual Basic pour nettoyer les données utilisateur restantes à la fin d'une session. Le script session_cleanup.vbs est lancé en tant que compte partagé (appelé HDSA) et se situe dans C:\.

Exemple : lancement d'Internet Explorer

Lancez Internet Explorer avec l'URL de votre Intranet MaSociété.com. Dans ce cas, Internet Explorer est exécuté comme processus associé à l'utilisateur du Bureau dynamique.

Notez que vous devez inclure les balises souhaitées à l'intérieur des balises et du fichier.

startup_scripts

Cette section du fichier est utilisée pour spécifier les applications à lancer avec le compte partagé du Bureau dynamique et le compte Windows associé à l'utilisateur du Bureau dynamique.

où :

compte	correspond au compte sous lequel l'application est exécutée. Vous pouvez choisir entre le nom d'utilisateur HDU ou le nom d'utilisateur du compte partagé du Bureau dynamique.
répertoire_travail	Indique le répertoire de travail de l'application.
options_chemin	Indique le chemin d'accès complet du fichier exécutable de l'application ou du script sur l'ordinateur local, ainsi que toutes les options à exécuter avec l'application. Par exemple : c:\program files\Internet Explorer\iexplore.exe http://www.yahoo.com

shutdown_scripts

Modifiez les applications d'arrêt du fichier session.xml pour supprimer toutes les données résultant d'une session utilisateur fermée. En général, ces applications suppriment les fichiers de configuration qui pourraient empêcher le prochain utilisateur

de travailler, les fichiers contenant des informations sensibles tels que les fichiers journaux et les documents stockés sur le système. Ces applications garantissent que l'environnement du Bureau dynamique est nettoyé en vue de la prochaine session utilisateur. Cette partie du fichier est particulièrement utile pour la sécurité des données.

Remarque : si besoin est, vous pouvez lancer des programmes administrateur ou des scripts pour nettoyer l'environnement utilisateur lors de la fermeture. Par exemple, vous pouvez écrire un script en Visual Basic qui utilise une application tierce pour supprimer les fichiers .ini de chaque utilisateur.

où :

compte	Correspond au compte sous lequel l'application de fermeture est exécutée. Vous pouvez choisir entre le nom d'utilisateurHDU et le nom d'utilisateur du compte partagé du Bureau dynamique.
répertoire_travail	Indique le répertoire de travail de l'application.
options_chemin	Indique le chemin d'accès complet du fichier exécutable de l'application ou du script sur l'ordinateur local, ainsi que toutes les options à exécuter avec l'application. Par exemple : c:\cleanup.vbs

Lancement d'applications à l'aide de Session.xml

Tenez compte des considérations suivantes :

- Les applications désignées dans le fichier session.xml doivent déjà être installées sur la station de travail.
- Le Bureau dynamique est un composant du logiciel Single Sign-On Plug-in. Par conséquent, le plug-in démarre automatiquement et n'a pas besoin d'être désigné dans ce fichier.

D'autres applications spécifiées dans le fichier session.xml peuvent être lancées à partir du shell du compte partagé du Bureau dynamique, invitant les utilisateurs à entrer leurs informations d'identification. Le plug-in se comporte alors selon les paramètres définis dans les configurations utilisateur.

Important : enregistrez le fichier session.xml au format UTF-8. Le codage ANSI est accepté si tous les caractères sont compris dans la plage de caractères 0 à 127 (jeu de caractères anglais standard). Si le fichier session.xml contient des caractères spéciaux ou étrangers, tels que des caractères asiatiques, vous devez l'enregistrer au format UTF-8.

Fichier process.xml

Oct 21, 2015

Remarque : le fichier process.xml est créé sur chaque station de travail ou machine sur laquelle le Bureau dynamique est installé et se situe dans le dossier C:\Program Files\Citrix\MetaFrame Password Manager\HotDesktop. un exemple de fichier process.xml est également disponible dans le dossier \Support du support d'installation. Par conséquent, tous les changements que vous souhaitez apporter à ce fichier doivent être effectués individuellement sur chaque machine. Toutefois, consultez l'article du support Citrix http://support.citrix.com/article/CTX110394 pour savoir comment remplacer chaque fichier process.xml utilisateur à l'aide d'une stratégie de groupe de machines dans Active Directory.
Utilisez le fichier process.xml pour spécifier quelles applications doivent continuer à être exécutées lorsqu'un utilisateur du Bureau dynamique se déconnecte. Ces applications sont appeléesapplications persistantes ou processus persistants.

Vous pouvez également utiliser le fichier process.xml pour spécifier les applications qui doivent s'arrêter lorsqu'un utilisateur du Bureau dynamique se déconnecte. Ces applications sont appeléesapplications transitoires ou processus transitoires.

Notez que vous devez inclure les balises souhaitées à l'intérieur des balises et du fichier.

Important : enregistrez le fichier process.xml au format UTF-8. Le codage ANSI est accepté si tous les caractères sont compris dans la plage de caractères 0 à 127 (jeu de caractères anglais standard). Si le fichier process.xml contient des caractères spéciaux ou étrangers, tels que des caractères asiatiques, vous devez l'enregistrer au format UTF-8.

shellexecute_processes

Utilisez cette section du fichier pour spécifier les types d'applications ou de fichiers qui doivent être exécutés en tant qu'utilisateur du Bureau dynamique. Ce paramètre permet de garantir la sécurité des applications à exécuter à l'aide d'informations d'identification des utilisateurs déjà connectés.

Remarque : après l'installation, le logiciel du plug-in spécifie automatiquement une application shell exécutable appelée ssoshell.exe (logiciel Single Sign-On Plug-in) dans le fichier process.xml. Par défaut, elle est définie comme un processus à exécuter en tant qu'utilisateur du Bureau dynamique.
Alors que le script de démarrage du fichier session.xml spécifie les applications à lancer lors de l'ouverture d'une session du Bureau dynamique, indique les applications qui peuvent être lancées par les utilisateurs ayant déjà ouvert une session du Bureau dynamique.

NomApp
où :

NomApp	Indique le nom de l'application ou du processus à exécuter. Le chemin complet n'est pas requis. Par exemple : pnagent.exe.

Remarque : process.xml autorise l'utilisation du caractère générique (*) dans les noms de fichiers statiques tels que Notepad.exe. Ces caractères peuvent être utilisés seuls ou en combinaison avec des noms de fichiers. Par exemple, *.txt, pnagent.exe, et *.doc sont des noms d'application valides.

persistent_processes

Utilisez cette section du fichier pour indiquer quelles applications doivent continuer à être exécutées une fois qu'un utilisateur du Bureau dynamique a fermé la session. Les applications spécifiées restent alors ouvertes lors de la fermeture (ou déconnexion) des sessions Bureau dynamique, même si celles-ci ont été lancées durant la session. Indiquez le chemin

d'accès complet du processus persistant pour garantir que seuls les processus appropriés restent ouverts à la fin de chaque session.

options_chemin

où :

options_chemin	Indique le chemin d'accès complet du fichier exécutable de l'application ou du script sur l'ordinateur local, ainsi que toutes les options à exécuter avec l'application. Par exemple : c:\program files\Internet Explorer\iexplore.exe http://www.yahoo.com

Remarque : après l'installation, le plug-in crée automatiquement une entrée pour une application persistante appelée activator.exe dans le fichier process.xml. L'application activator.exe fournit aux utilisateurs leur indicateur de session Bureau dynamique. Il s'agit une fenêtre transparente et déplaçable que les utilisateurs voient lorsqu'ils ouvrent une session. Elle contient des informations à propos des utilisateurs et de leurs sessions telles qu'elles sont définies par l'administrateur. Par défaut, activator.exe est définie en tant que processus persistant afin d'éviter son redémarrage à chaque ouverture et fermeture de session du Bureau dynamique.

transient_processes

Utlisez cette section du fichier pour indiquer quelles applications doivent être arrêtées une fois qu'un utilisateur du Bureau dynamique a fermé la session.

Remarque : après l'installation, le plug-in spécifie automatiquement une application transitoire appelée shellexecute.exe dans le fichier process.xml. Par défaut, elle est définie en tant que processus transitoire afin d'éviter qu'elle ne se ferme à chaque fin de session du Bureau dynamique.

NomApp

où :

NomApp	Indique le nom de l'application ou du processus qui doit s'arrêter. Le chemin complet n'est pas requis. Par exemple : pnagent.exe.

Références

Oct 21, 2015

Cette liste répertorie les paramètres et les conditions par défaut des paramètres du nœud Single Sign-On de Citrix AppCenter, regroupés en fonction de leur emplacement dans la console.

Configurations utilisateur

Cette section décrit les paramètres et les commandes des configurations utilisateur. Toutes les aides à la navigation fournies dans cette section sont relatives à une configuration utilisateur existante pendant l'exécution d'une fonction d'édition. Pour accéder à la boîte de dialogue Modifier la configuration utilisateur, cliquez sur les éléments suivants :

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On> Configurations utilisateur > [configuration] > Modifier la configuration utilisateur

Interaction de base du plug-in

Ces commandes permettent de personnaliser le fonctionnement de Single Sign-On Plug-in pour la configuration utilisateur en question. C'est là que vous définissez l'interface utilisateur.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On> Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Interaction de base du plug-in

Permettez aux utilisateurs de révéler leurs mots de passe.

Ce paramètre détermine si les utilisateurs peuvent révéler les mots de passe dans la fenêtre Gérer les mots de passe. Lorsque ce paramètre est désactivé, le bouton Révéler le mot de passe l'est aussi. Pour limiter la révélation du mot de passe à certaines applications, activez ce paramètre puis utilisez la stratégie de mot de passe correspondante pour autoriser ou non les utilisateurs à révéler les mots de passe pour les applications gérées par cette stratégie.

Valeur par défaut : sélectionné

Forcer la re-authentification avant de révéler les mots de passe utilisateur

Ce paramètre permet d'obliger les utilisateurs à s'authentifier à nouveau auprès de Single Sign-On avant de révéler un mot de passe.

Valeur par défaut : sélectionné

Détecter automatiquement les applications et proposer le stockage des informations d'identification

Ce paramètre permet d'activer l'affichage par le plug-in d'une invite demandant à l'utilisateur s'il souhaite ajouter les informations d'identification pour toute nouvelle application nouvellement détectée par le logiciel du plug-in.

Désélectionnez cette option pour désactiver la capacité de Single Sign-On Plug-in à détecter des applications qui ne sont pas associées à cette configuration utilisateur. Si cette option n'est pas activée, les utilisateurs doivent soumettre manuellement les informations d'identification auprès de ces applications. Utilisez ce paramètre pour empêcher les utilisateurs d'ajouter à leur ensemble d'applications d'authentification unique des applications qui ne font actuellement pas

partie de la configuration utilisateur qui leur est affectée.

Si elle est désélectionnée, cette option remplace Autoriser les utilisateurs à annuler le stockage des informations d'identification lorsqu'une nouvelle application est détectée disponible dans la page Paramètres avancés > Interactions côté client. En outre, si vous envisagez d'utiliser l'habilitation, la désélection de cette option évitera que les utilisateurs ne soient invités à entrer leurs informations d'identification.

Valeur par défaut : sélectionné

Traiter automatiquement les formulaires définis lorsque Single Sign-On Plug-in les détecte

Sélectionnez cette option pour permettre au plug-in de soumettre automatiquement les informations d'identification mémorisées sans que l'utilisateur n'ait à intervenir. Les champs d'informations d'identification dans l'application sont renseignés automatiquement si vous avez activé le paramètre Soumettre ce formulaire automatiquement correspondant dans la définition d'application associée à cette configuration utilisateur.

Valeur par défaut : sélectionné

Durée séparant les requêtes de nouvelle authentification

Ce paramètre spécifie la durée séparant les requêtes de nouvelle authentification du plug-in. Lorsque l'intervalle spécifié expire, la machine utilisateur est verrouillée et l'utilisateur doit à nouveau s'authentifier à l'aide de ses informations d'identification principales. La valeur minimale autorisée est d'une minute.

Valeur par défaut : 8 heures

Interface utilisateur du plug-in

Ces commandes sont utilisées pour définir le délay d'envoi des informations d'identification et les colonnes de la fenêtre Gérer les mots de passe.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On> Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Interface utilisateur du plug-in

Pause du plug-in avant soumission des informations d'identification

Sélectionnez ce paramètre pour spécifier le délai de soumission d'informations d'identification du plug-in après détection d'une application autorisée. Dans ce cas, spécifiez la durée (en secondes) de délai de soumission des informations d'identification. Ce paramètre permet de s'assurer que l'application est prête à recevoir les informations d'identification. Pendant cet intervalle, le plug-in affiche un indicateur de progression, signalant le traitement en cours.

Valeur par défaut : non sélectionné (0 secondes)

Définir les colonnes par défaut et leur ordre dans le Gestionnaire d'informations d'identification

Ce paramètre détermine les colonnes affichées dans la vue de détails de la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification). Vous pouvez également contrôler l'ordre de présentation des colonnes.

Paramètres par défaut :

- Nom de l'application
- Description
- Groupe
- Dernière utilisation
- Modification

Interaction côté client

Ces paramètres permettent de configurer la journalisation d'événements du logiciel du plug-in, la conservation de clés de Registre à la fermeture et le stockage d'informations d'identification sur les applications nouvellement détectées.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On> Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Interaction côté client

Journaliser les événements Single Sign-on Plug-in utilisant la journalisation d'événements Windows

Sélectionnez cette commande pour suivre les événements d'informations du logiciel du plug-in dans le journal d'événements de Windows local. Les avertissements et les erreurs sont toujours journalisés, quelque soit ce paramètre.

Valeur par défaut : non sélectionné

Supprimer le dossier de données et les clés de registre de l'utilisateur à l'arrêt de Single Sign-On Plug-in

Sélectionnez cette commande pour supprimer le dossier de données (y compris les informations d'identification cryptées) et les clés de registre de l'utilisateur lors de l'arrêt du plug-in.

Valeur par défaut : non sélectionné

Autoriser les utilisateurs à annuler le stockage des informations d'identification lorsqu'une nouvelle application est détectée

Ce paramètre permet d'activer l'invite demandant aux utilisateurs s'ils souhaitent stocker leurs informations d'identification chaque fois que le plug-in reconnaît une application pour laquelle aucune information n'est stockée. S'il est sélectionné, les utilisateurs peuvent stocker leurs informations d'identification dans la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification) tout de suite, ultérieurement ou jamais. Si le paramètre Détecter automatiquement les applications et inviter l'utilisateur à stocker les informations d'identification de la page Configurer l'interaction du plug-in est désactivé, le plug-in n'invite pas les utilisateurs à stocker leurs informations d'identification.

Valeur par défaut : sélectionné

Limiter le nombre de jours de suivi des informations d'identification supprimées

Ces commandes permettent de spécifier la durée pendant laquelle le magasin central effectue le suivi des informations d'identification supprimées de la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification) . Si elles sont stockées sur plusieurs machines clientes, le plug-in supprime les informations d'identification

lors de la synchronisation avec le magasin central dans le délai imparti. Si elles sont encore stockées sur la machine cliente lorsque le délai expire, elles sont restaurées à la synchronisation.

Valeur par défaut : sélectionné / 180 jours

Synchronisation

Ces commandes permettent d'autoriser les utilisateurs à actualiser les réglages de Single Sign-On Plug-in, de synchroniser la configuration utilisateur, de permettre au plug-in de continuer de fonctionner s'il ne peut pas se connecter au magasin central et de spécifier les intervalles de synchronisation automatique.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On> Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Synchronisation

Autoriser les utilisateurs à actualiser les réglages de Single Sign-On Plug-in

Sélectionnez ce paramètre pour permettre aux utilisateurs d'actualiser les réglages du plug-in dans la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification). Lorsque ce paramètre est désactivé, le bouton Actualiser de la fenêtre Gérer les mots de passe l'est aussi.

Valeur par défaut : sélectionné

Synchroniser à chaque lancement d'applications reconnues ou du Gestionnaire d'informations d'identification par l'utilisateur

Sélectionnez ce paramètre pour que le plug-in synchronise les informations de configuration utilisateur dès que l'utilisateur lance une application reconnue ou la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification). Une synchronisation fréquente peut entraîner une dégradation des performances sur le client et le serveur, ainsi qu'un accroissement du trafic réseau.

Valeur par défaut : non sélectionné

Permettre à Single Sign-On Plug-in de fonctionner même s'il ne peut pas se reconnecter au magasin central

Ce paramètre détermine si Single Sign-On continue à fonctionner lorsqu'il ne peut pas se connecter au magasin central pour la synchronisation. Lorsque cette option est activée, une instance de Single Sign-On Plug-in disposant d'une licence continue à fonctionner même en l'absence de connexion. Dans le cas contraire, le plug-in ne fonctionne qu'avec une connexion au magasin central.

Valeur par défaut : sélectionné

Délai entre les demandes de synchronisation automatique

Cette commande permet de spécifier la durée (en minutes) entre les tentatives de synchronisation automatique. La synchronisation automatique ne dépend pas de l'activité utilisateur et s'ajoute à la synchronisation provoquée par certains événements.

Valeur par défaut : non sélectionné / 0 minutes

Permettre l'accès aux informations d'identification par le module de synchronisation des informations d'identification

Sélectionnez ce paramètre pour autoriser les clients distants à accéder aux informations d'identification via ce service. Cette option est utilisée par la fonction Association de comptes, qui autorise un utilisateur du plug-in à se connecter à n'importe quelle application à l'aide d'au moins un compte Windows.

Valeur par défaut : non sélectionné

Association de comptes

Dans la mesure où les entreprises peuvent utiliser plusieurs domaines Windows, les utilisateurs peuvent également posséder plus d'un compte Windows. Les options d'association de comptes permettent à un utilisateur de se connecter à n'importe quelle application à l'aide d'un ou plusieurs comptes Windows. Ces commandes permettent aux utilisateurs d'associer leurs informations d'identification dans plusieurs comptes Windows.

Démarrer > Tous les programmes > Consoles de gestion > Citrix AppCenter > Single Sign-On > Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Association de comptes

Permettre aux utilisateurs d'associer des comptes

Sélectionnez ce paramètre pour permettre aux utilisateurs d'associer plusieurs comptes Windows et de spécifier l'adresse URL et le port d'installation du module de synchronisation des informations d'identification. Cette option ne peut pas être définie lors de la configuration initiale d'une Configuration utilisateur. Ce n'est possible qu'en modifiant une configuration existante.

Valeur par défaut : non sélectionné

Fournir une adresse du service par défaut

Sélectionnez ce paramètre pour définir l'adresse du service par défaut et le port du service dans le module de synchronisation des informations d'identification. Après avoir défini les paramètres, vous pouvez sélectionner l'option Valider pour confirmer l'adresse et le port du service.

Valeur par défaut : /MPMService/

Port du service : 443

Permettre aux utilisateurs de modifier l'adresse du service

Si une adresse de service est définie, sélectionnez ce paramètre pour permettre à l'utilisateur de modifier les réglages dans l'interface du plug-in. Sélectionnez cette option si la synchronisation des informations d'identification est exécutée sur différents ordinateurs et que les utilisateurs doivent pouvoir changer de poste de travail.

Valeur par défaut : non sélectionné

Fournir le domaine par défaut

Sélectionnez ce paramètre pour spécifier le domaine par défaut d'authentification lorsque le plug-in se synchronise au compte Windows qui lui est associé. Si vous le sélectionnez, entrez le nom de domaine par défaut dans l'espace fourni. Si

vous n'indiquez pas de domaine, les utilisateurs pourraient avoir des doutes quant aux informations d'identification qu'ils doivent fournir.

Valeur par défaut : non sélectionné

Permettre aux utilisateurs de modifier le domaine

Sélectionnez ce paramètre pour permettre à l'utilisateur de modifier le domaine par défaut d'authentification lorsque le plug-in se synchronise au compte Windows qui lui est associé.

Valeur par défaut : non sélectionné

Permettre aux utilisateurs de garder le mot de passe en mémoire

Sélectionnez ce paramètre pour autoriser les utilisateurs à mémoriser leur mot de passe de compte Windows associé dans le plug-in.

Valeur par défaut : non sélectionné

Prise en charge d'application

Ces commandes permettent au plug-in de détecter les définitions d'application côté client, d'activer la prise en charge de l'émulateur de terminal et de spécifier le nombre minimum de niveaux de nom de domaine à vérifier pour les applications Web.

Démarrer > Tous les programmes > Consoles de gestion > Citrix AppCenter > Single Sign-On > Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Prise en charge d'application

Détecter les définitions d'application sur le client

Sélectionnez ce paramètre pour permettre à Single Sign-On de détecter les applications de l'une des manières suivantes.

- Toutes les applications
  Détecte les applications (et y répond) définies par un administrateur ou un utilisateur (dans la fenêtre Gérer les mots de passe anciennement appelée Gestionnaire d'informations d'identification) et définies dans les paramètres par défaut lors de l'installation.
- Applications définies par les utilisateurs dans le Gestionnaire d'informations d'identification
  Détecte les applications (et y répond) définies par un administrateur ou un utilisateur dans la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification). Le plug-in ne reconnaît pas celles définies dans les paramètres par défaut à l'installation.
- Applications incluses dans Single Sign-On Plug-in uniquement
  Détecte les applications (et y répond) définies par un administrateur et définies dans les paramètres par défaut lors de l'installation. Les utilisateurs ne peuvent pas créer leurs propres définitions d'application à partir de la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification).

Valeur par défaut : toutes les applications

Activer la prise en charge des émulateurs de terminal

Ce paramètre permet d'activer la prise en charge des émulateurs de terminal. Lorsque ce paramètre est activé, le plug-in exécute un processus qui détecte les émulateurs de terminal et les applications d'émulateur de terminal.

Valeur par défaut : non sélectionné

Fréquence de surveillance par le plug-in des modifications dans l'émulateur

Ce paramètre spécifie le délai à respecter (en milli-secondes) avant que le plug-in vérifie la présence de changements dans l'affichage de l'émulateur de terminal. Des valeurs plus faibles peuvent requérir plus de temps d'UC sur le client et augmentent le trafic réseau.

Valeur par défaut : 3000 millisecondes

Nombre de niveaux de nom de domaine de correspondance

Ce paramètre spécifie le nombre minimum de niveaux de nom de domaine de correspondance pour les applications Web autorisées. Une valeur inférieure ou égale à 2 correspond à *.domaine1.domainedepremierniveau, une valeur 3 à *.domaine2.domaine1.domainedepremierniveau. Les niveaux de nom de domaine supérieurs au nombre spécifié ne sont pas pris en compte. Pour contrôler de façon stricte la correspondance d'adresse URL pour les applications Web, définissez une recherche plus contraignante dans vos définitions d'application.

Valeur par défaut : 99

Bureau dynamique

Ces commandes permettent de spécifier la manière dont les sessions du Bureau dynamique sont gérées.

Démarrer > Tous les programmes > Consoles de gestion > Citrix AppCenter > Single Sign-On > Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Bureau dynamique

Chemin d'accès du fichier de paramètres de scripts de session

Cette commande spécifie le chemin d'accès du fichier de paramètres de session définissant les scripts à exécuter au début et à la fin d'une session de Bureau dynamique. Le script de démarrage permet de démarrer des applications. Le script d'arrêt permet d'effectuer des tâches de nettoyage telles que la suppression de fichiers. Le fichier utilisé doit être accessible par tous les utilisateurs.

Valeur par défaut : [vide]

Délai d'expiration du verrouillage

Cette commande spécifie en minutes la durée pendant laquelle une session de Bureau dynamique reste active lorsque le poste de travail est inactif. Si ce délai est dépassé, le bureau est verrouillé.

Valeur par défaut : 10 minutes

Délai d'expiration de session

Cette commande spécifie en minutes la durée pendant laquelle une session de Bureau dynamique s'exécute alors que le poste de travail est verrouillé. Si ce délai est dépassé, il est mis fin à la session et une nouvelle session s'ouvre lorsque le bureau est déverrouillé.

Valeur par défaut : 5 minutes

Activer l'indicateur de session

Ce paramètre permet de sélectionner une fenêtre identifiant que la session de Bureau dynamique est activée. Lorsqu'il est sélectionné, une fenêtre transparente (qu'il est possible de déplacer) est affichée sur le bureau pendant les sessions de Bureau dynamique. Cette fenêtre indique le nom de l'utilisateur et le temps écoulé dans la session active.

Valeur par défaut : sélectionné

Activer le graphique

Cette commande spécifie le chemin du fichier graphique affiché dans l'Indicateur de session de Bureau dynamique. Le fichier utilisé doit être accessible à tous les utilisateurs et enregistré au format bitmap (.bmp) de Windows.

Une image bitmap par défaut, appelée Citrix.bmp, est disponible dans le dossier %ProgramFiles%\Citrix\MetaFrame Password Manager\Hot Desktop sur chaque station de travail du Bureau dynamique.

Valeur par défaut : [aucune]

Système de licences

Ces commandes sont utilisées pour identifier le serveur de licences et le modèle de licences.

Démarrer > Tous les programmes > Consoles de gestion > Citrix AppCenter > Single Sign-On > Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Systèmes de licences

Important : les instances de Single Sign-On Plug-in installées localement ne nécessitent pas de licence distincte pour les utilisateurs qui ont accès à des applications hébergées dans un environnement Citrix XenApp, édition Platinum.

Serveur de licences

Le nom de domaine complet (nomhôte.domaine.tld) associé au serveur de licences doit être identifié.

Valeur par défaut : [vide]

Port par défaut (pour le numéro de port du serveur de licences)

Sélectionnez ce paramètre pour utiliser le port d'accès par défaut du serveur de licences. Si le serveur de licences écoute sur un autre port que son port par défaut, désactivez ce paramètre et tapez le port d'accès dans le champ fourni.

Valeur par défaut : sélectionné

Port par défaut : 27000

Licences d'utilisateur désigné

Cette option est activée si vous sélectionnez Single Sign-On Advanced pour l'édition du produit. Vous pouvez également l'activer si vous sélectionnez Single Sign-On Enterprise pour l'édition du produit. Avec ce type de licences, Single Sign-On ne peut être utilisé que par des utilisateurs spécifiques, désignés. Si cette option est sélectionnée, vous devez spécifier la durée (en jours, heures et minutes) d'affectation de la licence à l'utilisateur désigné avant son expiration et la reconnexion du plug-in au serveur de licences. L'utilisateur garde le contrôle de la licence pendant la durée spécifiée même si son ordinateur

s'arrête.

Valeur par défaut : sélectionné si l'édition est Single Sign-On Advanced ; indisponible si l'édition est XenApp Platinum.

Valeur de déconnexion par défaut : 21 jours

Licences Utilisateurs simultanés (éditions Enterprise et Platinum uniquement)

Cette option est activée automatiquement si vous sélectionnez les éditions Single Sign-On Enterprise ou XenApp Platinum pour l'édition du produit. Elle n'est pas disponible si vous sélectionnez l'édition Advanced pour le produit.
Remarque : ce modèle de licences est activé si vous avez effectué une mise à niveau à partir de Password Manager version 4.1. Citrix Systems considère que cette version précédente est équivalente à l'édition Enterprise de Single Sign-On 5.0 pour ce qui est des licences lors de la mise à niveau.
Ce type de licence permet de partager une seule licence Single Sign-On entre différents utilisateurs (mais pas en même temps ; ce type de licence est parfois aussi appelé licence flottante).

Valeur par défaut : sélectionnée si l'édition est Single Sign-On Enterprise ou XenApp Platinum ; indisponible si l'édition est Single Sign-On édition Advanced.

Valeur de déconnexion par défaut : 1 heure, 30 minutes si l'option Autoriser l'utilisation de la licence en mode déconnecté n'est pas sélectionnée ; 21 jours si cette même option est sélectionnée.

Autoriser l'utilisation de la licence en mode déconnecté

Cette option n'est disponible que si le paramètre Licences Utilisateurs simultanés est sélectionné. Sélectionnez-la pour spécifier la durée pendant laquelle l'utilisateur peut être déconnecté (hors connexion) avant l'expiration de la licence et son retour dans l'ensemble de licences disponibles. L'utilisateur garde alors le contrôle de la licence pendant la durée spécifiée même si son ordinateur s'arrête. La durée par défaut est de 1 heure 30 minutes ; la valeur recommandée est comprise entre 2 et 365 jours.

Valeur par défaut : non sélectionné

Continuer sans valider les informations de licence

Ce réglage permet de modifier le processus d'édition sans requérir de nom de serveur de licence et de port d'accès valides.

Valeur par défaut : non sélectionné

Méthodes de protection des données

Oct 21, 2015

Ces paramètres permettent de sélectionner les méthodes de protection principale des informations d'identification de vos utilisateurs. Dans certains environnements, les utilisateurs peuvent appliquer plus d'une méthode.

Démarrer > Tous les programmes > Consoles de gestion > Citrix AppCenter > Single Sign-On > Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Méthodes de protection des données

Devez-vous réglementer l'accès des administrateurs de comptes aux données utilisateur ?

Sélectionnez Oui pour interdire l'accès des administrateurs aux informations d'identification des utilisateurs. La sélection de cette option entraîne la désactivation des options API de protection des données de Microsoft (y compris le DPAPI avec profil dans le menu déroulant de source de carte à puce) et de l'option Ne pas interroger les utilisateurs, restaurer automatiquement la protection de données principale sur le réseau dans les paramètres de protection secondaire des données. Avec cette configuration, l'administrateur de comptes ou autres ne peut pas accéder aux mots de passe ou aux données de l'utilisateur. Ce paramètre permet d'empêcher un administrateur de prendre l'identité d'un utilisateur. L'administrateur ne peut pas se connecter sous l'identité de l'utilisateur avec le paramètre par défaut et éventuellement accéder aux données situées dans le magasin central local de l'utilisateur.

Sélectionnez Non pour autoriser l'utilisation de toutes les fonctions d'authentification multiple ici et des méthodes de protection secondaire des données dans les paramètres de configuration Protection secondaire des données.

Valeur par défaut : oui

Pour améliorer le processus d'ouverture de session des utilisateurs, sélectionnez toutes les méthodes de protection des données qui s'appliquent

Sélectionnez cette option pour utiliser les fonctions d'authentification principale accessibles dans les paramètres décrits dans le tableau suivant.

Valeur par défaut : sélectionné

Utiliser la même protection des données qu'avec Password Manager 4.1 et versions précédentes

Contrôle	Description
Données d'authentification des utilisateurs	Un secret de l'utilisateur permet d'accéder aux données de l'utilisateur et de les protéger. Le secret d'authentification peut être un mot de passe de l'utilisateur ou un périphérique de saisie de code confidentiel installé dans votre environnement. Valeur par défaut : sélectionné Pour améliorer encore la protection des données des utilisateurs, vous pouvez également sélectionner les options suivantes : Permettre le code secret de carte à puce Cette option vous permet d'utiliser le code secret d'une carte à puce en guise de secret de l'utilisateur pour protéger les données. Elle n'est recommandée que si

Contrôle	Description
	votre entreprise ou votre environnement possède une stratégie forte en matière de codes secrets. Valeur par défaut : non sélectionné Autoriser la protection des données à l'aide d'un mot de passe vide Ne sélectionnez cette option que si les besoins de sécurité de votre domaine sont faibles et admettent des mots de passe de domaine vides. Si vous le faites et que le plug-in détecte que le mot de passe de l'utilisateur est vide, un secret de l'utilisateur est calculé à partir de l'ID de l'utilisateur. Si vous ne sélectionnez pas cette option, le plug-in ne calcule pas de secret de l'utilisateur ou n'assure pas de protection des données à l'aide du mot de passe vide. Si vous sélectionnez Données d'authentification des utilisateurs mais pas Permettre le code secret de carte à puce ni Autoriser la protection des données à l'aide d'un mot de passe vide, un message d'erreur s'affiche lorsque l'utilisateur tente d'ouvrir une session pour procéder à l'inscription et à l'enregistrement initiaux et le plug-in est désactivé. Valeur par défaut : non sélectionné
API de protection des données de Microsoft	Sélectionnez cette option si vous utilisez des profils itinérants exploitant un protocole d'authentification de réseau Kerberos pour les utilisateurs. Cette option ne fonctionne que si des profils itinérants sont présents. Par exemple, sélectionnez Données d'authentification des utilisateurs ainsi que cette option si vos utilisateurs se servent de mots de passe pour accéder à leurs ordinateurs et d'un protocole d'authentification de réseau Kerberos pour accéder à une batterie de serveurs Citrix XenApp. Cette méthode admet également l'utilisation d'informations d'identification de l'utilisateur et de cartes à puce pour l'ouverture de session. Valeur par défaut : non sélectionné
Certificat de carte à puce	Cette option permet d'utiliser des cartes cryptographiques autorisant le cryptage et le décryptage des données d'authentification. Citrix vous conseille de sélectionner cette option, dans la mesure du possible, si vous utilisez Bureau dynamique dans votre environnement. Valeur par défaut : non sélectionné

Sélectionnez cette option ainsi qu'une méthode dans le menu déroulant de source de clé de carte à puce pour autoriser l'utilisation d'une seule méthode d'authentification principale et/ou si vous utilisez la version 4.0 de Password Manager ou 4.1 de l'Agent/du plug-in. En outre, si vous avez mis à niveau votre magasin central de la version 4.1 vers la version 5.0, cette option est sélectionnée automatiquement.

Cette option n'est disponible que lorsque la méthode de cryptage Triple DES est utilisée.

Les choix de source de clé de carte à puce sont les suivants :

- Code secret en tant que mot de passe
- Protection des données par carte à puce
- DPAPI avec profil (non disponible si l'option Non est sélectionnée pour la question Devez-vous réglementer l'accès des administrateurs de comptes aux données utilisateurs ?

Valeur par défaut : non sélectionné

Protection secondaire des données

Ces options vous permettent de spécifier des fonctions de protection secondaire des informations d'identification à utiliser avant de déverrouiller les informations d'identification lorsque les utilisateurs modifient leur authentification principale (par exemple, en cas de modification de mot de passe de domaine ou de remplacement d'une carte à puce). En outre, elle vous permet de spécifier la restauration automatique des informations d'identification en mettant en œuvre le module de gestion des clés.

Démarrer > Tous les programmes > Consoles de gestion > Citrix AppCenter > Single Sign-On > Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Protection secondaire des données

Demande de vérification d'identité des utilisateurs

Valeur par défaut : sélectionné

Choisissez ce bouton radio pour sélectionner l'une des méthodes de réauthentification suivantes :

Contrôle	Description
Saisie du mot de passe précédent	Si vous sélectionnez cette option, n'oubliez pas que les utilisateurs qui oublient leur mot de passe précédent seront exclus du système et devront réenregistrer leurs informations d'identification des applications. Ne sélectionnez pas cette option si vos utilisateurs se servent de cartes à puce pour leur authentification principale. Valeur par défaut : sélectionné
Sélection d'une méthode : mot de passe précédent ou questions de sécurité	Grâce à cette option, les utilisateurs reçoivent une invite en fonction de la méthode de vérification qu'ils ont choisie. Elle comporte cette sous-option : Utiliser la question de vérification d'identité comme dans les versions précédentes de Password Manager. Sélectionnez cette option en cas de mise à niveau de la version 4.0 ou 4.1 de Password Manager et de l'activation de l'authentification avec questions ou des questions de vérification d'identité. Les versions 4.0 et 4.1 du plug-in n'ont pas besoin d'accéder au service dans ce cas. Valeur par défaut : non sélectionné

Contrôle	Description

Aucune invite aux utilisateurs ; restauration automatique de la protection principale des données sur le réseau

Sélectionnez cette option lorsque vous mettez en œuvre le module de gestion des clés pour contourner la vérification d'identité et déverrouiller automatiquement les informations d'identification des utilisateurs. Cette méthode est moins sure que les autres méthodes de protection de données mais elle est plus pratique pour vos utilisateurs, dans la mesure où les informations d'identification sont récupérées automatiquement.

Valeur par défaut : non sélectionné

Fonctionnalités Self-Service

Les options disponibles dans cette section nécessitent l'installation du module de gestion des clés. Celui-ci ajoute un bouton à la boîte de dialogue d'ouverture de session Windows qui permet la réinitialisation des mots passe par les utilisateurs.

Démarrer > Tous les programmes > Consoles de gestion > Citrix AppCenter > Single Sign-On > Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Fonctions autonomes

Autoriser les utilisateurs à réinitialiser leur mot de passe de domaine principal

Sélectionnez ce paramètre pour autoriser les utilisateurs à réinitialiser leur mot de passe principal de domaine sans demander l'intervention de l'administrateur.

Valeur par défaut : non sélectionné

Autoriser les utilisateurs à déverrouiller leur compte de domaine

Sélectionnez ce paramètre pour permettre aux utilisateurs de déverrouiller leur compte de domaine.

Valeur par défaut : non sélectionné

Module de gestion des clés

Ces commandes identifient l'emplacement et le port de service du module de gestion des clés.

Démarrer > Tous les programmes > Consoles de gestion > Citrix Delivery Services Console > Single Sign-On > Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Module de gestion des clés

Emplacement du service (Module de gestion des clés)

Ce paramètre permet d'identifier l'adresse et le port du module de gestion des clés. Utilisez le bouton Valider pour vous assurer de la validité des réglages.

Valeur par défaut : [vide]

Port du service : 443

Module d'habilitation

Le module d'habilitation permet d'importer, de modifier et de supprimer les informations d'identification associées à des

utilisateurs dans cette configuration utilisateur. Cette page impose la spécification de l'emplacement et du port de service du module d'habilitation.

Démarrer > Tous les programmes > Consoles de gestion > Citrix AppCenter > Single Sign-On > Configurations utilisateur > [configuration] > Modifier la configuration utilisateur > Module d'habilitation

Exécuter l'habilitation

Sélectionnez ce paramètre pour utiliser l'habilitation.

Valeur par défaut : non sélectionné

Emplacement du service (Module d'habilitation)

Ce paramètre permet d'identifier l'adresse et le port du module d'habilitation. Utilisez le bouton Valider pour vous assurer de la validité des réglages.

Valeur par défaut : [vide]

Port du service : 443

Définitions d'application

Oct 21, 2015

Cette rubrique décrit les paramètres et les commandes de définition d'application. Toutes les aides à la navigation fournies dans cette rubrique sont relatives à une définition d'application pendant une fonction d'édition.

Formulaires d'application

Ces commandes définissent les règles relatives à la longueur des mots de passe et à la répétition de caractères.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Définitions d'application > [définition] > Modifier la définition d'application > Formulaires d'application > [formulaire défini] > Modifier > Autres paramètres

Soumettre ce formulaire automatiquement

Ce paramètre permet de spécifier si le bouton Soumettre est automatiquement activé par le plug-in ou si l'utilisateur doit le faire manuellement. Cochez la case Soumettre ce formulaire automatiquement pour soumettre le formulaire automatiquement, sans intervention de l'utilisateur.

Valeur par défaut : sélectionné

Icône d'application

Cette commande permet d'identifier l'icône affichée en regard de l'application dans la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification).

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Définitions d'application > [définition] > Modifier la définition d'application > Icône d'application

Icône de l'application

Ce paramètre détermine l'icône d'application affichée en regard du nom de l'application dans la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification). Deux options sont disponibles :

- Utiliser une icône par défaut
- Utiliser une icône personnalisée (entrez son chemin d'accès)

Si vous souhaitez utiliser une icône personnalisée, utilisez la fonction de navigation pour indiquer le chemin d'accès de son fichier. Le système identifie n'importe quel fichier d'icône Windows standard. Les variables d'environnement Microsoft Windows sont prises en charge.

Valeur par défaut : utiliser une icône par défaut

Détection avancée

Ces commandes permettent au plug-in d'ignorer les formulaires de modification d'informations d'identification ou de mot de passe suivants au cours d'une session d'application lorsque ce type de modification a déjà été exécuté.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Définitions d'application > [définition] > Modifier la définition d'application > Identification de l'application

Ne traiter que la première ouverture de session pour cette application

Sélectionnez cette commande pour ne traiter que la première ouverture de session pour cette application et ignorer les demandes d'identification suivantes.

Valeur par défaut : non sélectionné

Ne traiter que la première modification de mot de passe pour cette application

Sélectionnez cette commande pour ne traiter que la première modification de mot de passe pour cette application et ignorer les demandes de modification suivantes.

Valeur par défaut : non sélectionné

Expiration du mot de passe

Ces commandes permettent de spécifier les paramètres de cette application en cas d'expiration du mot de passe. La stratégie d'expiration de Single Sign-On n'est appliquée que si elle est sélectionnée dans la stratégie de mot de passe associée à cette application.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Définitions d'application > [définition] > Modifier la définition d'application > Expiration du mot de passe

Exécuter le script à l'expiration du mot de passe

Sélectionnez ce paramètre et spécifiez le script (et son chemin d'accès absolu) à exécuter lorsque le mot de passe expire. N'utilisez pas un chemin UNC (Universal Naming Convention).

Valeur par défaut : non sélectionné

Utiliser la notification d'expiration de Citrix Single Sign-On

Sélectionnez ce paramètre pour utiliser la notification d'expiration de Single Sign-On en cas d'expiration du mot de passe.

Valeur par défaut : non sélectionné

Stratégies de mot de passe

Oct 21, 2015

Cette section décrit les paramètres et les commandes de stratégie de mot de passe. Toutes les aides à la navigation fournies dans cette section sont relatives à une stratégie de mot de passe existante pendant l'exécution d'une fonction d'édition. Pour accéder à la boîte de dialogue Modifier la stratégie de mot de passe, cliquez sur les éléments suivants :

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Stratégies de mot de passe > [stratégie] > Modifier la stratégie de mot de passe > Test de la stratégie de mot de passe

Règles de mot de passe de base

Ces commandes définissent les règles relatives à la longueur des mots de passe et à la répétition de caractères.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Stratégies de mot de passe > [stratégie] > Modifier la stratégie de mot de passe > Règles de mot de passe de base

Longueur de mot de passe minimale

Spécifie le nombre minimum de caractères requis dans un mot de passe. Minimum autorisé = 0. Maximum autorisé = 128.

Valeur par défaut : 8

Longueur de mot de passe maximale

Spécifie le nombre maximum de caractères autorisés dans un mot de passe. Minimum autorisé = 1. Maximum autorisé = 128.

Valeur par défaut : 20

Nombre de répétitions possibles d'un caractère

Spécifie le nombre maximum de répétitions possibles d'un caractère dans un mot de passe. Minimum autorisé = 1. Maximum autorisé = 128.

Valeur par défaut : 6

Nombre de répétitions successives possibles d'un caractère

Spécifie le nombre de répétitions successives possibles d'un caractère. Minimum autorisé = 1. Maximum autorisé = 128.

Valeur par défaut : 4

Règles des caractères alphabétiques

Ces commandes définissent les règles relatives à l'utilisation des lettres dans les mots de passe.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Stratégies de mot de passe > [stratégie] > Modifier la stratégie de mot de passe > Règles des caractères alphabétiques

Autoriser les minuscules

Ce réglage détermine si les mots de passe peuvent contenir des lettres minuscules.

Valeur par défaut : autoriser les minuscules

Le mot de passe peut débuter avec une minuscule

Ce réglage détermine si les mots de passe peuvent commencer par une minuscule.

Valeur par défaut : le mot de passe peut débuter avec une minuscule

Le mot de passe peut se terminer par une minuscule

Ce réglage détermine si les mots de passe peuvent se terminer par une minuscule.

Valeur par défaut : le mot de passe peut se terminer par une minuscule

Nombre minimum de minuscules requis

Spécifie le nombre minimum de minuscules requis dans un mot de passe. Minimum autorisé = 0. Maximum autorisé = 128.

Valeur par défaut : 0

Autoriser les majuscules

Ce réglage détermine si les mots de passe peuvent contenir des lettres majuscules.

Valeur par défaut : autoriser les majuscules

Le mot de passe peut débuter avec une majuscule

Ce réglage détermine si les mots de passe peuvent commencer par une majuscule.

Valeur par défaut : le mot de passe peut débuter avec une majuscule

Le mot de passe peut se terminer avec une majuscule

Ce réglage détermine si les mots de passe peuvent se terminer par une majuscule.

Valeur par défaut : le mot de passe peut se terminer par une majuscule

Nombre minimum de majuscules requis

Spécifie le nombre minimum de majuscules requis dans un mot de passe. Minimum autorisé = 0. Maximum autorisé = 128.

Valeur par défaut : 0

Règles de caractère numérique

Ces commandes définissent les règles relatives à l'utilisation des chiffres (0-9) dans les mots de passe.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Stratégies de mot de passe > [stratégie] > Modifier la stratégie de mot de passe > Règle de caractère numérique

Autoriser les caractères numériques

Ce réglage détermine si les mots de passe peuvent contenir des caractères numériques.

Valeur par défaut : autoriser les caractères numériques

Le mot de passe peut débuter avec un caractère numérique

Ce réglage détermine si les mots de passe peuvent commencer par un caractère numérique.

Valeur par défaut : le mot de passe peut débuter avec un caractère numérique

Le mot de passe peut se terminer par un caractère numérique

Ce réglage détermine si les mots de passe peuvent se terminer par un caractère numérique.

Valeur par défaut : le mot de passe peut débuter avec un caractère numérique

Nombre minimum de caractères numériques requis

Spécifie le nombre minimum de caractères numériques requis dans un mot de passe. Minimum autorisé = 0. Maximum autorisé = 128.

Valeur par défaut : 0

Nombre maximum de caractères numériques autorisé

Spécifie le nombre maximum de caractères numériques autorisé dans un mot de passe. Minimum autorisé = 1. Maximum autorisé = 128.

Valeur par défaut : 20

Règles des caractères spéciaux

Ces commandes définissent les règles relatives à l'utilisation des caractères spéciaux (ni alphabétiques, ni numériques) dans les mots de passe.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Stratégies de mot de passe > [stratégie] > Modifier la stratégie de mot de passe > Règles des caractères spéciaux

Autoriser les caractères spéciaux

Permet d'autoriser les caractères spéciaux (ni alphabétiques, ni numériques) dans les mots de passe.

Valeur par défaut : autoriser les caractères numériques

Le mot de passe peut débuter avec un caractère spécial

Ce réglage détermine si les mots de passe peuvent commencer par un caractère spécial.

Valeur par défaut : le mot de passe peut débuter avec un caractère spécial

Le mot de passe peut se terminer par un caractère spécial

Ce réglage détermine si les mots de passe peuvent se terminer par un caractère spécial.

Valeur par défaut : le mot de passe peut se terminer avec un caractère spécial

Nombre minimum de caractères spéciaux requis

Spécifie le nombre minimum de caractères spéciaux requis dans un mot de passe. Minimum autorisé = 0, maximum autorisé = 128.

Valeur par défaut : 0

Nombre maximum de caractères spéciaux autorisé

Spécifie le nombre maximum de caractères spéciaux autorisé dans un mot de passe. Minimum autorisé = 0, maximum autorisé = 128.

Valeur par défaut : 20

Liste de caractères spéciaux autorisés

Spécifie les caractères spéciaux autorisés dans un mot de passe.

Valeur par défaut : !@#$^&*()_-+=[]\|,?

Règles d'exclusion

Ces commandes spécifient les caractères et les chaînes de caractères qui ne sont pas autorisés dans les mots de passe.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Stratégies de mot de passe > [stratégie] > Modifier la stratégie de mot de passe > Règles d'exclusion

Exclure des mots de passe les caractères ou groupes de caractères de cette liste

Sélectionnez l'option Modifier la liste pour ouvrir la boîte de dialogue Modifier la liste d'exclusion qui permet de spécifier jusqu'à 256 caractères ou groupes de caractères non autorisés dans les mots de passe. Tapez un caractère ou groupe de caractères par ligne. Chaque groupe peut contenir jusqu'à 32 caractères. Les caractères ou groupes de caractères ne sont pas sensibles à la casse.

Valeur par défaut : [vide]

Ne pas autoriser le nom d'utilisateur de l'application dans le mot de passe

Ce réglage détermine si l'utilisation du nom d'utilisateur de l'application est autorisée dans le mot de passe. Dans l'affirmative, activez cette case à cocher.

Valeur par défaut : non sélectionné

Ne pas autoriser les portions de nom d'utilisateur d'application dans le mot de passe

Ce réglage détermine si l'utilisation de certaines parties du nom d'utilisateur de l'application est autorisée dans le mot de passe. Cela comprend tous les groupes de caractères possibles issus du nom de l'utilisateur. Ce paramètre est étroitement lié au paramètre Nombre de caractères des portions. Par exemple, lorsque ce paramètre est sélectionné et que le paramètre Nombre de caractères des portions est réglé sur la valeur 4, un mot de passe comprenant un groupe de caractères « citr », « itri » ou « trix » ne serait pas autorisé si le nom d'utilisateur Windows est « citrix ».

Valeur par défaut : non sélectionné

Ne pas autoriser le nom d'utilisateur Windows dans le mot de passe

Ce réglage détermine si l'utilisation du nom d'utilisateur Windows est autorisée dans le mot de passe. S'il n'est pas sélectionné, le nom d'utilisateur Windows est autorisé dans le mot de passe. Ce paramètre est étroitement lié au paramètre Nombre de caractères des portions. Par exemple, lorsque ce paramètre est sélectionné et que le paramètre Nombre de caractères des portions est réglé sur la valeur 4, un mot de passe comprenant un groupe de caractères « citr », « itri » ou « trix » ne serait pas autorisé si le nom d'utilisateur Windows est « citrix ».

Valeur par défaut : non sélectionné

Historique et expiration des mots de passe

Ces commandes spécifient si un nouveau mot de passe peut être une répétition d'un mot de passe précédent, ainsi que le paramètre d'expiration de mot de passe.

l'historique du mot de passe est enregistré utilisateur par utilisateur. Si vous réinitialisez les données d'un utilisateur, son historique de mot de passe est supprimé et l'historique ne peut pas être appliqué pour les mots de passe supprimés.

L'option d'expiration de mot de passe envoie une notification aux utilisateurs indiquant uniquement qu'un mot de passe est parvenu ou va parvenir à expiration. Vos utilisateurs peuvent se servir d'informations expirées, mais voient s'afficher des rappels ou des demandes de modification de mot de passe jusqu'au changement effectif dans la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification).

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Stratégies de mot de passe > [stratégie] > Modifier la stratégie de mot de passe > Historique et expiration des mots de passe

Le nouveau mot de passe doit être différent des précédents

Ce réglage indique si le nouveau mot de passe peut être identique à un mot de passe précédent. Les mots de passe précédents sont conservés dans un historique des mots de passe.

Valeur par défaut : le nouveau mot de passe peut être identique au précédent (case à cocher non activée)

Nombre de mots de passe précédents retenus

Spécifie le nombre de mots de passe précédents conservés dans l'historique des mots de passe. Minimum autorisé = 1. Maximum autorisé = 24.

Valeur par défaut : 1

Utiliser les paramètres d'expiration de mot de passe associés aux définitions d'application

Lorsque cette option est sélectionnée, les paramètres (Délai d'expiration du mot de passe (jours) et Nombre de jours pour la notification avant expiration du mot de passe) spécifiés ici sont appliqués aux définitions d'application associées à cette stratégie. La stratégie de Single Sign-On fonctionne indépendamment de la stratégie d'expiration de mot de passe existante intégrée à l'application.

Valeur par défaut : expiration de mot de passe non spécifiée (case à cocher non activée)

Délai d'expiration du mot de passe (jours)

Spécifie le nombre de jours maximum pendant lequel un mot de passe peut rester inchangé. Minimum autorisé = 1. Maximum autorisé = 99999.

Valeur par défaut : 42

Nombre de jours pour la notification avant expiration du mot de passe

Spécifie le nombre de jours précédant l'expiration d'un mot de passe avant que l'utilisateur ne commence à recevoir des avertissements d'expiration de mot de passe. Minimum autorisé = 0. Maximum autorisé = 99998.

Valeur par défaut : 14

Test de la stratégie de mot de passe

Ces commandes permettent de tester un mot de passe généré manuellement afin de vérifier sa conformité à la stratégie définie, de créer automatiquement un mot de passe conforme et de vérifier que les contraintes définies n'empêchent pas la création d'un nombre suffisant de mots de passe pour votre organisation.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Stratégies de mot de passe > [stratégie] > Modifier la stratégie de mot de passe > Test de la stratégie de mot de passe

Tester la conformité d'un mot de passe créé manuellement

Ce champ permet de tester la conformité d'un mot de passe créé manuellement. Entrez votre mot de passe et cliquez sur Tester. Le mot de passe saisi est comparé aux critères établis.

Valeur par défaut : aucune

Générer un mot de passe aléatoire conforme à la stratégie

Cette commande permet de générer un mot de passe conforme aux critères de mot de passe actuellement en vigueur. Cliquez sur Générer afin de créer un mot de passe conforme, qui pourra être copié à partir de ce champ (Ctrl-C).

Valeur par défaut : aucune

Générer et tester des mots de passe uniques conformes à la stratégie

Il est également possible de définir un ensemble de contraintes sur les mots de passe pour accepter un nombre limité de mots de passe possibles. Cette commande permet de générer un nombre personnalisé de mots de passe conformes afin de déterminer si la stratégie définie est assez flexible pour répondre aux besoins de mots de passe de l'organisation. Cliquez sur Générer plusieurs mots de passe pour ouvrir une boîte de dialogue de création d'un certain nombre de mots de passe définis par l'utilisateur.

Valeur par défaut : aucune

Préférences d'authentification

Ces commandes permettent de définir si l'option Révéler est disponible pour les définitions d'application utilisant cette stratégie, de demander une nouvelle authentification de l'utilisateur avant la soumission des informations d'identification d'application, de définir le nombre de nouvelles tentatives de connexion et de définir le délai dont dispose l'utilisateur pour s'authentifier après l'échec d'une tentative d'authentification.

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Stratégies de mot de passe > [stratégie] > Modifier la stratégie de mot de passe > Préférences d'authentification

Autoriser l'utilisateur à révéler le mot de passe pour les applications

Cette commande permet de déterminer si le bouton Révéler de la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification). est disponible pour les applications gérées par cette stratégie. Lorsqu'un utilisateur sélectionne ce bouton Révéler dans la fenêtre Gérer les mots de passe, son mot de passe est affiché en clair. Si ce paramètre n'est pas sélectionné, les utilisateurs ne peuvent pas révéler leur mot de passe.

Valeur par défaut : le bouton Révéler n'apparaît pas (case à cocher non activée)

Demander authentification avant soumission des infos d'identification d'une application

Cette commande permet de demander aux utilisateurs d'entrer leurs informations d'identification principales avant soumission par le plug-in de celles destinées à l'application. Lorsque ce paramètre est sélectionné, Single Sign-On Plug-in verrouille immédiatement la station de travail dès qu'il reconnaît une application gérée par ce paramètre. Les utilisateurs doivent entrer leurs informations d'identification principales pour déverrouiller la station de travail. Le plug-in transmet ensuite les informations d'identifications à l'application. Ce paramètre est utile pour les applications permettant l'accès à des informations confidentielles ou sensibles car il oblige les utilisateurs à confirmer leur identité avant soumission de leurs informations d'identification par le plug-in à l'application.

Valeur par défaut : l'utilisateur n'est pas obligé de s'authentifier de nouveau (case à cocher non activée)

Nombre de tentatives d'ouverture de session

Cette commande permet de définir le nombre de nouvelles soumissions autorisé des informations d'identification à une même application dans le délai spécifié. Lorsque vous optez pour la valeur minimum de 0, les utilisateurs reçoivent immédiatement un message d'erreur à la seconde tentative d'authentification dans l'application.

Valeur par défaut : 0

Délai limite pour les tentatives

Cette commande permet de spécifier le délai (en secondes) octroyé à l'utilisateur pour soumettre ses informations d'identification à la même application après l'échec de la première tentative.

Valeur par défaut : 30 secondes

Assistant de modification de mot de passe

Cette commande permet de déterminer la façon dont l'assistant de modification de mot de passe répond au formulaire de modification de mot de passe. Vous devez configurer l'une des quatre options possibles :

- Permettre aux utilisateurs de choisir un mot de passe généré par le système ou de créer leur propre mot de passe
- Autoriser les utilisateurs à créer leur propre mot de passe seulement
- Autoriser les utilisateurs à choisir un mot de passe généré par le système seulement
- Générer un mot de passe et le soumettre à l'application sans afficher l'assistant de modification de mot de passe

Démarrer > Tous les programmes > Citrix > Consoles de gestion > Citrix AppCenter > Single Sign-On > Stratégies de mot de passe > [stratégie] > Modifier la stratégie de mot de passe > Assistant de modification de mot de passe

Généré par le système ou créé par les utilisateurs eux-mêmes

Sélectionnez cette option pour que l'assistant de modification de mot de passe autorise les utilisateurs à choisir un mot de passe généré par le système ou à créer leur propre mot de passe.

Valeur par défaut : sélectionné

Utilisateurs uniquement autorisés à créer leur propre mot de passe

Sélectionnez cette option pour que l'assistant de modification de mot de passe empêche les utilisateurs de choisir un mot de passe généré par le système et les oblige à créer leur propre mot de passe.

Valeur par défaut : non sélectionné

Utilisateurs uniquement autorisés à choisir un mot de passe généré par le système

Sélectionnez cette option pour que l'assistant de modification de mot de passe utilise automatiquement un mot de passe généré par le système sans autoriser les utilisateurs à créer leur propre mot de passe.

Valeur par défaut : non sélectionné

Généré et soumis à l'application sans affichage de l'assistant de modification de mot de passe

Sélectionnez cette option pour que Single Sign-On Plug-in soumette automatiquement un mot de passe généré par le système, sans afficher l'assistant de modification de mot de passe à l'utilisateur. L'utilisateur peut voir les champs de l'écran de modification de mot de passe renseignés et le message de l'application indiquant si le mot de passe a été modifié avec succès ou non.

Valeur par défaut : non sélectionné

Opérations

Oct 21, 2015

Single Sign-On peut journaliser des événements du plug-in ou générés par l'utilisateur dans le journal des applications d'événements de Windows. Ils sont classés selon les catégories informations, avertissements et erreurs. Les avertissements et les erreurs sont toujours journalisés. La journalisation des événements d'information est désactivée par défaut mais vous pouvez l'activer dans la console après création de la configuration utilisateur.

Single Sign-on journalise les événements de fonctionnalités telles que le Bureau dynamique, les cartes à puce, les licences et le service Single Sign-on. Des événements relatifs à la sécurité nécessitant parfois un suivi afin de respecter les réglementations en vigueur sont interceptés et vérifiés. Les capacités de journalisation d'événements de Single Sign-On permettent également d'améliorer la sécurité de votre réseau.

Si vous utilisez Single Sign-On dans un environnement XenApp, le journal d'événements identifie les informations des utilisateurs et des sessions. Toute tentative infructueuse d'ouverture de session est journalisée.

Pour activer la journalisation des événements d'informations :

1. Dans la console, localisez votre configuration utilisateur et, à partir du menu Action, sélectionnez Modifier la configuration utilisateur.
2. Dans les propriétés de cette configuration, sélectionnez Interaction côté client.
3. Cliquez sur Journaliser les événements Single Sign-on Plug-in utilisant la journalisation d'événements Windows.

Le tableau ci-dessous contient certains événements standard journalisés par Single Sign-On :

Types d'événements standard
Tentative infructueuse d'ouverture de session (authentification du plug-in)
Journalisé lors d'une authentification infructueuse d'un utilisateur auprès de Single Sign-On. Échec d'ouverture du magasin d'informations d'identification.
Tentative réussie d'ouverture de session (authentification du plug-in)
Journalisé lors d'une authentification d'un utilisateur et d'une ouverture du magasin central réussies.
Tentative d'ouverture de session (soumission d'informations d'identification)
Journalisé lors de tentatives de soumission d'informations d'identification à une application externe.
Opérations avec des informations d'identification
Journalisé lors d'opérations sur des informations d'identification, notamment la modification, la révélation et la vérification d'identité.
Échec de synchronisation (communication)
Journalisé lors d'échec de synchronisation avec le magasin central en raison de problèmes de communication.
Échec de synchronisation (autorisations)

Types d'événements standard
Journalisé lors d'échec de synchronisation avec le magasin central en raison d'informations d'identification incorrectes.
Échec de cryptage/décryptage - Protection des données par carte à puce
Journalisé lors d'un échec général associé au cryptage ou au décryptage des données de carte à puce.
Échec de cryptage/décryptage - Protection des données par carte à puce (carte manquante)
Journalisé lorsque la carte à puce n'est pas disponible.
Démarrage et fermeture du plug-in
Journalisé lorsque la carte à puce n'est pas disponible.
Fichiers .dll manquant ou altérés
Journalisé lorsqu'un fichier .dll ne peut pas être chargé correctement.

Le tableau ci-dessous contient certains événements du Bureau dynamique journalisés par Single Sign-On.

Types d'événements du Bureau dynamique
Échec d'ouverture de session du Bureau dynamique
Journalisé seulement en présence d'une erreur fatale au démarrage de la session.
Ouverture de session du Bureau dynamique réussie
Journalisé lors de l'ouverture d'une session du Bureau dynamique après une authentification d'utilisateur réussie.
Échec de fermeture de session du Bureau dynamique
Journalisé seulement en présence d'une erreur fatale à la fermeture de session.
Fermeture de session du Bureau dynamique réussie
Journalisé lors d'une fermeture de session réussie après intervention de l'utilisateur ou expiration du délai d'inactivité d'une session.

Fichier Mfrmlist.ini

Oct 21, 2015

Le fichier Mfrmlist.ini contient une liste d'émulateurs de terminal et les emplacements des fichiers HLLAPI.dll que Single Sign-On Plug-in surveille. Son emplacement est le suivant :

%ProgramFiles%\Citrix\MetaFrame Password Manager\Helper\MFEmu

Single Sign-On Plug-in ne soumet pas les informations d'identification

Oct 21, 2015

Parfois, Single Sign-On Plug-in ne soumet pas les informations d'identification à une application configurée. Plusieurs raisons peuvent être à l'origine du problème, parmi lesquelles :

- Modifications apportées à l'application Web, ce qui rend la définition d'application obsolète.
- Paramètre configuré involontairement lors de la création de la définition d'application.

Commencez par effectuer les tâches suivantes pour déterminer la raison de l'échec de la soumission d'informations d'identification.

- Vérifiez tous les paramètres pour identifier les éventuels conflits.
- Vérifiez que le plug-in est configuré pour la détection d'applications.
- Comparez les définitions du plug-in et de la console Single Sign-On.
- Supprimez les champs de critères de correspondance et de soumission un à un jusqu'à ce que le plug-in recommence à soumettre les informations d'identification.

Important : Single Sign-On met à votre disposition un large éventail de paramètres destinés à faciliter la création de définitions d'application, de stratégies de mot de passe, de configurations utilisateur et de méthodes de vérification d'identité. Certains réglages impliquent parfois des paramètres conflictuels, ce qui peut notamment conduire à des échecs de soumission d'informations d'identification aux applications.
Si Single Sign-On Plug-in ne parvient toujours pas à soumettre les informations d'identification de l'utilisateur, essayez les techniques de résolution de problèmes suivantes pour les applications Web et les applications d'émulation de terminal.

Applications Web

- Contrôlez que l'option de recherche d'URL stricte est utilisée correctement.
  1. Dans le composant Single Sign-On de AppCenter, sélectionnez l'application Web à afficher.
  2. À partir du menu Action, cliquez sur Modifier la définition d'application.
  3. Cliquez sur Formulaires d'application, sélectionnez un formulaire d'application, puis cliquez sur Modifier.
  4. Cliquez sur Identité du formulaire. À ce niveau, vous pouvez activer la recherche d'adresse URL stricte ainsi que la prise en compte de la casse de l'adresse URL.
  5. Assurez-vous que les pages utilisent des types de champs HTML. Les définitions d'application Web requièrent ces types de champs. Les types de champ défini par l'utilisateur et indéfini ne sont pas détectés.

- Lorsque vous utilisez la navigation InPrivate dans Internet Explorer 8, assurez-vous que l'option Désactiver les barres d'outils et les extensions lors du démarrage de la navigation InPrivate n'est pas sélectionnée. Pour obtenir des informations sur les fonctionnalités de confidentialité d'Internet Explorer, visitez le site Web de Microsoft.

Applications d'émulateur de terminal

Créez des définitions d'application d'émulation de terminal à l'aide de l'assistant de définition d'application et de l'assistant de définition de formulaire. Lors de l'ajout de la définition d'application à une configuration utilisateur, veillez à activer la prise en charge des émulateurs de terminal.

- Assurez-vous que l'émulateur de terminal est configuré dans le fichier Mfrmlist.ini.
  Le processus Ssomho.exe, qui contrôle l'interaction de Single Sign-On avec les émulateurs de terminal, ne reconnaît que les émulateurs définis dans le fichier Mfrmlist.ini. Si l'émulateur de terminal n'y est pas défini, le processus Ssomho.exe

n'essaie pas de communiquer avec l'émulateur de terminal.

- Assurez-vous qu'un nom court de session est spécifié.
  Le processus Ssomho.exe utilise le nom de session court pour communiquer avec HLLAPI dll. Sans ce nom court, Ssomho.exe est chargé mais ne peut pas surveiller l'activité à l'écran. Le nom de session court doit être configuré dans l'émulateur de terminal de la machine cliente.

- Assurez-vous que le processus ssomho.exe est en cours d'exécution.
  Suivez les instructions ci-dessous pour cette vérification :
  1. Sur l'ordinateur exécutant Single Sign-On Plug-in, ouvrez le Gestionnaire de tâches et sélectionnez l'onglet Processus.
  2. Cliquez sur l'en-tête Image Name pour trier les processus par nom d'image.
  3. Vérifiez la présence de Ssomho.exe dans la liste.

  S'il ne s'y trouve pas, il est possible qu'il ne soit pas en mesure de trouver un fichier HLLAPI.dll qu'il soit fermé prématurément en raison de problèmes liés à des émulateurs de terminal tiers.

  Remarque : même si le processus ssomho.exe apparaît, ses communications avec HLLAPI.dll peuvent être infructueuses. Vérifiez le nom de session court avant de rechercher d'autres solutions.
- Testez chaque émulateur de terminal.
  Si vous avez installé plusieurs émulateurs pris en charge sur un même système, ssomho.exe tente de communiquer avec tous. Parfois, un des fichiers HLLAPI.dll peut provoquer une instabilité de ssomho.exe. Testez chaque émulateur de terminal en supprimant les autres ou en plaçant des marques de commentaire devant les entrées du fichier mfrmlist.ini et en modifiant leur séquence.

  Cette étape permet de s'assurer que le processus ssomho ne se connecte pas par erreur à un autre émulateur que celui faisant l'objet de votre test.

Prise en charge des émulateurs de terminal

Oct 21, 2015

Pour activer la prise en charge HLLAPI pour tout émulateur de terminal dans Single Sign-On, vous devez activer la prise en charge des émulateurs de terminal dans la console.

Lorsque la prise en charge des émulateurs de terminal est activée, SSOShell démarre le processus ssomho.exe. Ce processus lit d'abord le fichier Mfrmlist.ini situé à l'emplacement %Program Files%\Citrix\MetaFrame Password Manager\Helper\MFEmu, puis recherche tous les émulateurs configurés et tente de charger le fichier DLL HLLAPI affecté à ce fichier.

Le fichier mfrmlist.ini peut être étendu pour s'adapter à des émulateurs HLLAPI supplémentaires.

Le processus ssomho.exe recherche dans la clé de registre HKEY_LOCAL_MACHINE\SOFTWARE l'emplacement du fichier DLL HLLAPI sauf instruction contraire du fichier mfrmlist.ini.

Certains émulateurs de terminal situent l'emplacement dans la clé HKEY_CURRENT_USER. Pour ces émulateurs, spécifiez manuellement l'emplacement du fichier DLL en utilisant un chemin d'accès absolu dans le fichier Mfrmlist.ini.

La configuration de Single Sign-On pour qu'il fonctionne avec les émulateurs testés est un processus en plusieurs étapes. Ce processus nécessite l'installation de l'émulateur, la création d'une session d'émulateur à utiliser avec Single Sign-On et la configuration dans Single Sign-On d'une définition d'application d'émulateur de terminal qui utilise la correspondance de texte afin de reconnaître une session d'émulateur particulière.

1. Installez l'émulateur de terminal et redémarrez l'ordinateur.
2. Démarrez l'émulateur de terminal et créez une nouvelle session, en définissant l'affichage et la connexion.
3. Définissez le nom de session court.
4. Activez la prise en charge de HLLAPI.
   Remarque : une définition d'application d'émulateur de terminal séparée est nécessaire pour chaque session qui utilise Single Sign-On. Le plug-in détecte les sessions en faisant correspondre le texte dans l'écran de l'application d'émulateur de terminal avec le texte de la ligne et de la colonne spécifiées de la définition d'application. Single Sign-On soumet les informations d'identification en fonction des données de ligne et de colonne fournies dans la définition d'application. Par conséquent, chaque session nécessite sa propre définition d'application.
5. Enregistrez puis fermez votre session.
6. Quittez l'émulateur de terminal.
7. Créez une définition d'application pour l'application d'hôte.
8. Ouvrez la Console et vérifiez si la prise en charge est activée dans les configurations utilisateurs concernées.
9. Exécutez l'émulateur et ouvrez une session.
10. Démarrez ou actualisez Single Sign-On Plug-in.

Ce dernier reconnaît alors l'écran de connexion et affiche un formulaire pour la saisie et l'enregistrement des informations d'identification.

Single Sign-On Plug-in ne démarre pas

Oct 21, 2015

Single Sign-On Plug-in doit être le dernier logiciel modifiant le composant GINA installé sur vos machines autres que Windows Server 2008, Windows Server 2008 R2, Windows Vista ou Windows 7. Si Single Sign-On Plug-in est installé mais qu'il ne démarre pas comme prévu, il est possible que la chaîne GINA soit rompue. Cette situation se produit lorsqu'un logiciel installé ou mis à niveau après Single Sign-On Plug-in modifie la chaîne GINA Windows. Les packs logiciels prenant en charge l'authentification par carte à puce, Symantec et XenApp modifient la chaîne GINA de Windows.

Si vous avez déjà installé Single Sign-On et que vous envisagez d'installer ou de mettre à niveau un logiciel qui modifie la chaîne GINA de Windows, désinstallez d'abord Single Sign-On Plug-in. Après cette désinstallation, installez le nouveau logiciel (ou effectuez la mise à niveau) puis réinstallez Single Sign-On Plug-in. Ainsi, le fichier .dll correct est installé et enregistré en vue d'une utilisation avec Single Sign-On.

1. Désinstallez tout logiciel tiers modifiant la chaîne GINA.
2. Désinstallez le plug-in.
3. Installez le logiciel tiers.
4. Installez le plug-in.

Si vous avez récemment mis à niveau ou installé un logiciel tiers et que vous soupçonnez une modification de la chaîne GINA de Windows, vérifiez l'entrée de registre Windows et la machine cliente pour vous assurer de la présence et de l'emplacement des fichiers .dll de la chaîne GINA propres à votre installation. Si les fichiers sont absents de la machine, désinstallez et réinstallez Single Sign-On Plug-in.

Important : lors de la désinstallation du logiciel potentiellement responsable de la rupture de la chaîne GINA, il est important de désinstaller le logiciel dans l'ordre inverse de son installation sur la machine utilisateur. Autrement, l'ordinateur risque de se trouver dans un état non valide. Ne modifiez pas le registre.

Création d'un certificat de signature

Oct 21, 2015

Le service Single Sign-On génère des alertes dans le journal d'événements avant et après l'expiration du certificat de signature. Créez un certificat pour mettre fin aux alertes. CtxCreateSigningCert.exe est un outil permettant la création de ces certificats. Utilisez l'outil de signature (ctxsigndata) pour signer à nouveau les données du magasin central (à l'aide des clés du nouveau certificat).

Il n'est pas nécessaire de créer un certificat de signature après avoir configuré le service Single Sign-On sauf dans l'une des situations suivantes :

- Votre certificat de signature va parvenir ou est parvenu à expiration.
- Vous avez des soupçons quant à l'intégrité de votre certificat de signature.

Pour créer un certificat, vous devez exécuter l'outil CtxCreateSigningCert.exe, disponible dans le dossier %ProgramFiles%\Citrix\MetaFrame Single sign-on\Service. À l'invite de commande de l'ordinateur exécutant le service Single Sign-On, entrez CtxCreateSigningCert.exe.

Entrez le nom de la clé publique, celui de la clé privée et le délai d'expiration, en mois, du certificat de signature. Le certificat est créé.

CtxCreateSigningCert	
Syntaxe :	CtxCreateSigningCert
Dans cette formule :	= nom de fichier à utiliser pour le certificat public = nom de fichier à utiliser pour le certificat privé = nombre de mois avant l'expiration du certificat
Exemple :	ctxcreatesigningcert "C:\PublicKeyCert.cert" "C:\PrivateKeyCert.cert" "12"

Signature, retrait de signature, renouvellement de signature et vérification des données

Oct 21, 2015

Utilisez l'outil de signature (CtxSignData.exe) pour signer les données du magasin central, renouveler ou retirer leur signature et pour les vérifier. Cet outil est également disponible en ligne de commande, dans le répertoire \Service du support d'installation. CtxSignData.exe est également installé sur le serveur hébergeant le service : %ProgramFiles%\Citrix\MetaFrame Password Manager\Service\SigningTool\CtxSignData.exe.

Remarque : l'outil de signature est installé avec le module d'intégrité des données du service Single Sign-On. Ce module peut être installé ultérieurement s'il n'a pas été inclus dans l'installation initiale de Single Sign-On.
Entrez CtxSignData.exe à l'invite de commande de l'ordinateur exécutant le service Single Sign-On. Vous pouvez utiliser les paramètres suivants : -s, -r, -u, -v.

Le paramètre de signature permet d'activer l'intégrité des données dans un environnement contenant des données non signées.

Remarque : si vous disposez d'un environnement Single Sign-On sans l'intégrité des données et que vous décidez par la suite d'activer le module d'intégrité des données, vous devez utiliser l'outil de signature des données pour signer les données du magasin central.
Fournissez le nom de fichier du certificat de signature, l'URI (Uniform Resource Identifier) du service Single Sign-On, l'emplacement du magasin central et le type du magasin central (partage réseau NTFS ou Active Directory). Toutes les données sont lues et signées à l'aide du nouveau certificat de signature.

La syntaxe de la commande CtxSignData avec le paramètre -s est la suivante :

```
CtxSignData [-s chemin_service fichier_certificat emplacement_magasincentral NTFS|AD]
```

où :

-s	signe les fichiers de données dans le magasin central
chemin_service	chemin d'accès du service Single Sign-On au format URI
fichier_certificat	nom de fichier du certificat à utiliser pour la signature ou le renouvellement de signature des données
emplacement_magasincentral	chemin d'accès UNC (Universal Naming Convention) du partage de fichier ou du DNS (Domain Name System) du contrôleur de domaine Active Directory
NTFS | AD	NTFS | AD = type de service d'annuaire du magasin central, où • NTFS = partage de fichier Microsoft NTFS • AD = Microsoft Active Directory

Ci-dessous figurent des exemples de la commande CtxSignData avec le paramètre -s.

```
ctxsigndata -s "mpmserver.masociete.com/MPMService" "C:\priv12mos.cert" "\\MPMCentralServer\citrixsync$" NTFS
ctxsigndata -s mpmserver.masociete.com/MPMService "C:\priv12mos.cert" DC1.masociete.com AD
```

Utilisez le paramètre de renouvellement de signature de la ligne de commande lorsque le certificat de signature existant approche de la date d'expiration, a déjà expiré ou lorsque son intégrité est compromise. Fournissez le nom de fichier du certificat de signature, l'URI (Uniform Resource Identifier) du service Single Sign-On, l'emplacement du magasin central et le type du magasin central (partage réseau NTFS ou Active Directory). Toutes les données sont lues, vérifiées et signées à l'aide du nouveau certificat de signature. Aucune modification de paramètre n'est nécessaire dans la console ou dans le plug-in car l'intégrité des données est déjà activée.

Suivez les étapes suivantes pour renouveler la signature de données altérées :

1. Ouvrez le composant Single Sign-On de Citrix AppCenter et recherchez la configuration utilisateur affectée.
2. Ouvrez cette configuration pour vérifier si les données peuvent être lues à partir du magasin central.
3. Fermez la configuration utilisateur pour enregistrer les données non altérées dans le magasin central.
4. Utilisez l'outil de signature (ctxsigndata) pour signer à nouveau les données du magasin central.

Remarque : si l'altération des données semble être causée par un problème de sécurité, effectuez cette procédure pour toutes les configurations utilisateur avant de signer à nouveau les données afin d'éviter de signer par erreur des données non protégées.
La syntaxe de la commande CtxSignData avec le paramètre -s est la suivante :

```
CtxSignData [-r chemin_service fichier_certificat emplacement_magasincentral NTFS|AD]
```

où :

-r	renouvelle la signature des fichiers de données dans le magasin central (contient le paramètre -v)
chemin_service	chemin d'accès du service Single Sign-On au format URI
fichier_certificat	nom de fichier du certificat à utiliser pour la signature ou le renouvellement de signature des données
emplacement_magasincentral	chemin d'accès UNC (Universal Naming Convention) du partage de fichier ou du DNS (Domain Name System) du contrôleur de domaine Active Directory
NTFS | AD	NTFS | AD = type de service d'annuaire du magasin central, où • NTFS = partage de fichier Microsoft NTFS • AD = Microsoft Active Directory

Ci-dessous figurent des exemples de la commande CtxSignData avec le paramètre -r :

```
ctxsigndata -r "mpmserver.masociete.com/MPMService" "C:\priv12mos.cert" "\\MPMCentralServer\citrixsync$" NTFS
ctxsigndata -r mpmserver.masociete.com/MPMService "C:\priv3mos.cert" DC1.masociete.com AD
```

Utilisez le paramètre de retrait signature de la ligne de commande lorsque vous désactivez le module d'intégrité des données. Fournissez le nom de fichier du certificat de signature, l'URI du service Single Sign-On, l'emplacement du magasin central et le type du magasin central (partage réseau NTFS ou Active Directory). Toutes les données sont lues sans vérification et les signatures sont supprimées.

La syntaxe de la commande CtxSignData avec le paramètre -s est la suivante :

```
CtxSignData [-u emplacement_magasincentral NTFSAD]
```

où :

-u	retire la signature des fichiers de données dans le magasin central
emplacement_magasincentral	chemin d'accès UNC (Universal Naming Convention) du partage de fichier ou du DNS (Domain Name System) du contrôleur de domaine Active Directory
NTFS | AD	NTFS | AD = type de service d'annuaire du magasin central, où • NTFS = partage de fichier Microsoft NTFS • AD = Microsoft Active Directory

Ci-dessous figurent des exemples de la commande CtxSignData avec le paramètre -u :

```
ctxsigndata -u “\\MPMCentralServer\citrixsync$” NTFS
ctxsigndata -u DC1.masociete.com AD
```

Utilisez le paramètre de ligne de commande pour vérifier que toutes les données du magasin central ont été signées et vérifiées. Fournissez le nom de fichier du certificat de signature, l'URI du service Single Sign-On, l'emplacement du magasin central et le type du magasin central (partage réseau NTFS ou Active Directory). Toutes les données sont lues, vérifiées et signées.

La syntaxe de la commande CtxSignData avec le paramètre -v est la suivante :

```
CtxSignData [-v chemin_service emplacement_magasincentral NTFSAD]
```

Dans cette formule :

-v	vérifie les signatures des fichiers de données dans le magasin central
chemin_service	chemin d'accès du service Single Sign-On au format URI
emplacement_magasincentral	chemin d'accès UNC (Universal Naming Convention) du partage de fichier ou du DNS (Domain Name System) du contrôleur de domaine Active Directory
NTFS | AD	NTFS | AD = type de service d'annuaire du magasin central, où • NTFS = partage de fichier Microsoft NTFS • AD = Microsoft Active Directory

Ci-dessous figurent des exemples de la commande CtxSignData avec le paramètre -v :

```
ctxsigndata -v "mpmserver.masociete.com/MPMService" "\\MPMCentralServer\citrixsync$" NTFS
ctxsigndata -v mpmserver.masociete.com/MPMService "https://mpmserver.masociete.com/MPMService" DC1.masociete.com AD
```

Utilisez le paramètre de la ligne de commande d'aide pour afficher l'aide correspondant à la commande CtxSignData.

La syntaxe de la commande CtxSignData avec le paramètre -h est la suivante :

```
CtxSignData [-h]
```

Dans cette formule :

-h	affiche l'aide

Ci-dessous figure un exemple de la commande CtxSignData avec le paramètre -h :

```
ctxsigndata -h
```

Activation et désactivation du service d'intégrité des données dans Single Sign-On Plug-in

Oct 21, 2015

La clé de registre suivante peut être modifiée afin d'activer ou de désactiver le service d'intégrité des données pour Single Sign-On Plug-in.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\PerformIntegrityCheck

Type : DWORD

Valeurs :

0=validation de l'intégrité des données désactivée

1=validation de l'intégrité des données activée

Déplacement des données vers un autre magasin central

Oct 21, 2015

Plusieurs raisons peuvent vous conduire à effectuer la migration de vos stratégies de mot de passe, modèles d'application, définitions d'application, questions de sécurité et autres types de données administratives de Single Sign-On.

- déplacement de l'utilisateur vers un nouveau domaine ;
- ajout d'un nouveau serveur dans l'environnement Single Sign-On ;
- ajout d'un nouveau domaine pour permettre aux utilisateurs d'activer la fonction d'association de comptes de Single Sign-On ;
- utilisation de l'association de comptes sur des domaines existants ;
- déplacement de Single Sign-On d'un environnement de test vers un environnement de production.

La migration est un processus constitué de deux étapes réalisées via le composant Single Sign-On de Citrix AppCenter : étape 1. Exportez les données administratives existantes ; étape 2. Exportez les données administratives dans le nouvel environnement. Généralement, vous devez rediriger les utilisateurs vers le nouveau magasin central.

Le tableau ci-dessous contient les données faisant l'objet ou non d'une migration lorsque vous utilisez la commande Exporter.

Migration	Pas de migration
Stratégies de mot de passe (sauf pour les stratégies par défaut et de domaine)	Configurations utilisateur
Modèles d'application	Dossiers People
Définitions d'application	Groupes d'applications
Questions de sécurité et groupes de questions de sécurité utilisés dans le cadre de l'authentification avec questions	Informations d'identification
	Questionnaires
	Données du service Single Sign-On

Le service Single Sign-On n'est pas migré d'un magasin central vers un autre. Pour garantir le bon déroulement de la migration si vous utilisez un service, vous devez installer le service Single Sign-On dans un nouvel emplacement et faire en sorte que le service existant et le nouveau service soient tous les deux disponibles (temporairement) après la migration.

Attention : afin de garantir la réussite de la migration, vous devez effectuer des étapes supplémentaires si les modules des services Fonctions autonomes ou Intégrité des données sont installés ou si l'option Supprimer le dossier de données et les clés de registre à l'arrêt de Single Sign-On Plug-in est activée dans une configuration utilisateur.
Les configurations utilisateur ne subissent pas automatiquement de migration d'un magasin central vers l'autre. Généralement, vous devez recréer les configurations utilisateur et rediriger les utilisateurs vers le nouveau magasin central. Lorsque Single Sign-On Plug-in synchronise ses données avec celles du magasin central d'origine, il détecte la modification des valeurs et copie alors les informations d'identification vers le nouveau magasin central.

L'Assistant d'exportation des données d'administration vous permet d'exporter des définitions d'application, des modèles d'application, des stratégies de mot de passe et des questions de sécurité et groupes dans le magasin central. Vous pouvez choisir d'exporter ou d'ignorer des types entiers de données, mais cet assistant ne vous autorise pas à agir sur un sous-ensemble de données : par exemple, vous devez exporter toutes les stratégies de mot de passe ou les laisser dans l'ancien magasin central.

À la différence des autres types de données d'administration, vous pouvez choisir quelles définitions d'application exporter à l'aide de la commande de définition d'application Export.

Attention : afin de garantir la réussite de la migration, vous devez effectuer des étapes manuelles si les modules des services Fonctions autonomes ou Intégrité des données sont installés ou si l'option Supprimer le dossier de données et les clés de registre à l'arrêt de Single Sign-On Plug-in est activée dans une configuration utilisateur.

1. Dans Citrix AppCenter, tout en étant connecté au magasin central d'origine, cliquez sur le nœud Single Sign-On, et à partir du menu Action, cliquez sur Exporter les informations d'administration.
2. Suivez les instructions de l'assistant d'exportation des données d'administration.

1. Sur la nouvelle machine, installez et démarrez le composant de console Single Sign-on, et terminez le processus Configurer et exécuter la découverte.
   Remarque : le processus Configurer et exécuter la découverte permet d'identifier le magasin central auquel vous voulez vous connecter.

2. Dans Citrix AppCenter, tout en étant connecté au nouveau magasin central, cliquez sur le nœud Single Sign-On, et à partir du menu Action, cliquez sur Importer les informations d'administration.
3. Suivez les instructions de l'assistant d'importation des données d'administration.
4. Créez de nouvelles configurations utilisateur.
5. Dans Citrix AppCenter, tout en étant connecté au magasin central d'origine, sélectionnez une configuration utilisateur migrée, et à partir du menu Action, sélectionnez Rediriger les utilisateurs et identifiez l'emplacement du nouveau magasin central. Répétez l'opération autant de fois que nécessaire.
6. Assurez-vous que tous les utilisateurs se connectent à Single Sign-On au moins une fois. Vous pouvez maintenant arrêter le magasin central d'origine et le service en toute sécurité.

Si votre entreprise active l'option Supprimer le dossier de données et les clés de registre à l'arrêt de Single Sign-On Plug-in dans des configurations utilisateur, suivez les étapes suivantes pour migrer les données d'administration de vos utilisateurs vers un nouveau magasin central. Si vous ne procédez pas de la sorte, les utilisateurs migrés sont obligés de s'enregistrer à nouveau, par le biais de l'authentification avec questions ou de la récupération de clé automatique chaque fois qu'ils ouvrent une session sur leur ordinateur. Ceci est dû au fait que les données d'administration des utilisateurs sont supprimées chaque fois qu'ils ferment une session ou qu'ils ferment Single Sign-On Plug-in.

1. Migrez les données administratives dans le nouveau magasin central.
2. Dans Citrix AppCenter, tout en étant connecté au nouveau magasin central, créez de nouvelles configurations utilisateur. N'activez pas l'option Supprimer le dossier de données et les clés de registre à l'arrêt de Single Sign-On Plug-in.
3. Dans Citrix AppCenter, tout en étant connecté au magasin central d'origine, sélectionnez une configuration utilisateur migrée, et à partir du menu Action, sélectionnez Rediriger les utilisateurs et identifiez l'emplacement du nouveau magasin central. Répétez l'opération autant de fois que nécessaire.
4. Assurez-vous que tous les utilisateurs se connectent à Single Sign-On au moins une fois.
5. Rédigez un script et exécutez-le pour mettre à jour le type et l'emplacement du magasin central dans le registre des ordinateurs des utilisateurs. Le tableau suivant dresse la liste des paramètres de registre en fonction du type de magasin central

Type de magasin central	Anciens paramètres	Nouveaux paramètres
NTFS vers 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 vers 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 cers 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 =

Avertissement : la modification incorrecte du Registre peut entraîner des problèmes graves pouvant nécessiter la réinstallation de votre système d'exploitation. Citrix ne peut garantir la possibilité de résoudre les problèmes provenant d'une mauvaise utilisation de l'Éditeur du Registre. Utilisez l'Éditeur du Registre à vos risques. Effectuez une copie de sauvegarde de votre registre avant de le modifier.

6. Dans Citrix AppCenter, tout en étant connecté au nouveau magasin central, sélectionnez les nouvelles configurations utilisateur et activez l'option Supprimer le dossier de données et les clés de registre à l'arrêt de Single Sign-On Plug-in. Vous pouvez maintenant arrêter le magasin central d'origine et le service en toute sécurité.

Vous pouvez exporter des définitions d'une seule application ou un nombre illimité de définitions d'applications vers un fichier .xml.

Pour exporter une seule définition d'application

1. Dans Citrix AppCenter, tout en étant connecté au magasin central d'origine, développez le nœud Single Sign-On et développez Définitions d'application.
2. Sélectionnez la définition d'application à exporter et, à partir du menu Action, cliquez sur Exporter la définition d'application.
3. Dans la boîte de dialogue Exporter la définition d'application, enregistrez la définition d'application dans un emplacement accessible depuis l'ordinateur de la nouvelle console.

Pour exporter des définitions d'applications multiples

1. Dans Citrix AppCenter, tout en étant connecté au magasin central d'origine, développez le nœud Single Sign-On et cliquez sur Définitions d'application.
2. À partir du menu Action, cliquez sur Exporter les définitions d'application.
3. Suivez les instructions de l'assistant d'exportation de définitions d'applications.

Lorsque vous sauvegardez des fichiers importants, veillez à inclure le magasin central et son contenu, les certificats et les clés personnelles et privées dans les procédures standard de sauvegarde de votre société.

Important : vous devez modifier les autorisations d'accès à ces fichiers dans Windows si votre magasin central se trouve sur un point de partage réseau NTFS afin que votre programme de sauvegarde puisse y accéder.

1. Prenez toujours note des réglages que vous effectuez lors de l'exécution de l'Outil de configuration du service.
2. Exportez les données du service vers un point de partage sécurisé ou un disque à l'aide du processus CtxMoveServiceData.exe.
    1. Ouvrez une invite de commande et accédez au dossier %ProgramFiles%\Citrix\Metaframe Password Manager\Service\Tools.
    2. EntrezCtxMoveServiceData.exe –export \\server\share\backupfile.
       Remarque : vous ne devez pas insérer de variables d'environnement dans le chemin d'accès.
    3. Entrez un mot de passe à l'invite correspondante. Prenez soin de noter ce dernier.
       Important : les données du service enregistrées dans le fichier de sauvegarde seront cryptées à l'aide de ce mot de passe. Veillez à ne pas perdre le perdre.
    4. À l'invite de confirmation, entrez de nouveau votre mot de passe.
    5. Vérifiez que le fichier de sauvegarde a bien été créé.

1. Installez le service à partir du support d'installation.
2. Configurez le service à l'aide des paramètres appropriés, en vous reportant aux notes que vous avez prises avant la sauvegarde.
   Remarque : si vous utilisez l'intégrité de données, veillez à configurer l'emplacement du serveur d'intégrité des données correctement, que cet emplacement ait été modifié ou non.
3. Terminez la configuration et attendez que le service démarre. Une fois le service démarré, vous pouvez immédiatement l'arrêter si vous le souhaitez.
4. Importez les données du service à partir d'un point de partage sécurisé ou d'un disque à l'aide du processus CtxMoveServiceData.exe.
    1. Ouvrez une invite de commande et accédez au dossier %Program Files%\Citrix\Metaframe Password Manager\Service\tools.
    2. EntrezCtxMoveServiceData.exe –import <\\server\share\backupfile>.
    3. Entrez le mot de passe approprié à l'invite correspondante.
    4. Répondez Oui à l'invite d'écrasement du fichier AKR.DAT.
5. Redémarrez le service. Le service peut désormais être utilisé.

Utilisez l'outil CtxFileSyncClean pour supprimer les fichiers de données de configuration orphelins des magasins centraux des points de partage réseau. Ces fichiers sont devenus orphelins lorsque les objets vers lesquels ils pointaient ont été supprimés. L'outil CtxFileSyncClean ne supprime pas les fichiers de données utilisateur, même si l'utilisateur en question a été supprimé. Exécutez le fichier CtxFileSyncClean.exe à partir du répertoire \Tools du support d'installation.

Extensions des définitions d'application

Jul 20, 2016

Bien que les administrateurs de Single Sign-On puissent généralement créer des définitions d'applications à l'aide du composant Single Sign-On de Citrix AppCenter et de l'Outil de définition d'application, certaines applications requièrent des considérations spéciales ou un processus externe pour déterminer si une application a démarré ou pour soumettre les informations d'identification de l'utilisateur à l'aide de Single Sign-On Plug-in.

Pour prendre en charge les applications ayant ce type d'exigences, les implémenteurs tiers qui créent les processus devant répondre à ces exigences de traitement externe peuvent utiliser les extensions de définition d'application du composant Single Sign-On de Citrix AppCenter ainsi que l'Outil de définition d'application pour définir de quelle façon et à quel moment ces processus doivent être lancés.

Il existe deux types différents d'extensions de définitions d'applications :

- Extensions d'identification
  Celles-ci utilisent des processus externes pour déterminer si l'application est un formulaire qui requiert des actions de gestion des informations d'identification de l'utilisateur. Vous pouvez utiliser ces processus externes à la place de ou conjointement à d'autres algorithmes de détection de fenêtres définis dans la définition du formulaire.
- Extensions d'actions
  Celles-ci utilisent des processus externes pour effectuer les actions de gestion des informations d'identification requises. Vous pouvez utiliser ces processus externes à la place de ou conjointement à d'autres algorithmes de détection de fenêtres définis dans la définition du formulaire.

Il est possible de configurer une définition de formulaire unique de façon à ce qu'elle utilise les extensions de définitions d'applications pour effectuer l'une de ces opérations ou les deux.

Single Sign-On Plug-in utilise un système de détection pour identifier les événements sur le bureau (tels que l'instanciation d'applications, le chargement d'URL, les avis de fin de chargement de page HTML ou autres événements similaires).

À mesure que ces événements se produisent, le plug-in détermine si l'application cible requiert une action de gestion des informations d'identification (par exemple, ignorer, ouvrir une session, modifier le mot de passe, etc.). Pour cela, il compare les caractéristiques que présente l'application par rapport aux caractéristiques définies pour identifier un formulaire de façon unique. Ces caractéristiques incluent, au minimum, le titre Windows et le nom du fichier exécutable et, le cas échéant, d'autres caractéristiques de correspondance avancée telles que l'utilisation d'un processus externe pour identifier le formulaire (extension d'identification).

Lorsqu'un processus d'identification externe est requis, celui-ci est identifié dans la définition du formulaire. La définition du formulaire inclut des informations sur l'extension d'identification et tous les paramètres associés. Ces informations sont directement associées à un paramètre de registre.

Une fois que le plug-in a terminé le traitement des algorithmes à correspondance minimale et avancée, les extensions d'identification utilisant un processus externe sont évaluées.

Lorsque plusieurs extensions d'identification sont définies pour évaluer un formulaire, elles sont exécutées dans l'ordre dans

lequel elles apparaissent dans la page des extensions d'identification (de haut en bas).

Pour chaque extension d'identification, le plug-in attend pendant l'intervalle de temps défini (dans le paramètre de registre) que le processus externe se termine avant d'analyser le code de sortie du processus.

Si les processus à correspondance minimale, avancée et externe se terminent en renvoyant le code zéro, l'application cible est considérée comme correspondante. Si l'un des processus correspondants renvoie une autre valeur, le processus d'évaluation est arrêté et l'application est considérée comme non correspondante.

Si un processus renvoie une valeur négative, une erreur est consignée dans l'Observateur d'événements Windows. Les valeurs positives sont consignées dans un fichier journal, si celui-ci est activé.

Vous pouvez effectuer l'action de gestion des informations d'identification suivante en utilisant une combinaison quelconque d'actions de formulaire, de séquences d'actions ou d'extensions d'actions Windows standard.

Pour définir une extension d'identification

Configurez les extensions d'identification à l'aide de l'assistant de définition de formulaire pendant le processus de développement de définitions d'application.

1. À partir de AppCenter, développez le nœud Single Sign-On, sélectionnez Définitions d'application, et à partir du menu Action, cliquez sur Créer une définition d'application.
2. Dans l'assistant de définition d'application, accédez à la page Gérer les formulaires et sélectionnez Ajouter un formulaire pour démarrer l'assistant de définition de formulaire.
3. Avancez dans le processus de définition jusqu'à ce que la page Identifier le formulaire s'affiche.
4. Dans la page Identification du formulaire, cliquez sur Correspondance avancée. La page Correspondance avancée s'affiche.
5. Dans la boîte de dialogue Correspondance avancée, cliquez sur Extensions d'identification.
6. Sur la page Extensions d'identification, cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajout d'extension d'identification. Utilisez la boîte de dialogue Ajout d’extension d’identification pour définir les éléments suivants :

Identificateur d'extension	L'identificateur d'extension identifie le paramètre NomExtension à rechercher dans les paramètres du registre.
Description	Description définie par l'utilisateur de l'extension d'identification.
Paramètres	Toute paire nom/valeur (nom de paramètre/valeur de paramètre) utilisée pour transmettre les paramètres définis par l'implémenteur au processus externe lancé par cette extension.

NomExtension identifie le nom de la clé de registre. Ce nom de clé et les valeurs de clé associées définissent l'exécutable du processus d'identification externe et ses caractéristiques d'utilisation. Le nom de clé de registre et les clés associées se situent à l'emplacement suivant :

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extension\{NomExtension}]

où la valeur NomExtension est identifiée par la valeur Identificateur d'extension définie dans la boîte de dialogue Ajout d’extension d’identification.

Sur les plates-formes 64 bits, le nom de clé de registre et les clés associées se situent à l'emplacement suivant :

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\MetaFrame Password Manager\Extension\

{NomExtension}]

Le tableau suivant définit les caractéristiques des valeurs de clé.

Clé	Type	Valeur
Type	REG_SZ	Doit être EXECUTABLE
Timeout	REG_DWORD	0 indique d'attendre que l'application se termine. Toute autre valeur indique la période d'attente en millisecondes.
TerminateProcess	BOOL implémenté en tant que REG_DWORD	Au terme du délai d'expiration, terminer le processus (facultatif). TRUE : (valeur par défaut) terminer le processus. FALSE : (0) ne pas terminer le processus.
Exécutable	REG_EXPAND_SZ	Processus exécutable et son chemin d'accès complet.
Arguments	REG_SZ	Paramètres de l'exécutable.

La valeur Executable représente le chemin d'accès du fichier exécutable. Les variables d'environnement sont permises. Si l'extension est implémentée en tant que script, vous devez utiliser l'interpréteur de script pour l'exécutable et le nom du script comme partie des arguments. Pour développer des processus externes, vous pouvez utiliser un éditeur/langage ou un environnement de développement intégré de votre choix.

La valeur Arguments prend en charge les paramètres que le plug-in peut remplacer par des paramètres d'exécution ou les paires nom/valeur de paramètre spécifiées dans la boîte de dialogue Ajout d'extension d'identification. Chaque paramètre à remplacer doit contenir un délimiteur$ (signe dollar) en préfixe et suffixe. Par exemple, les arguments de ligne de commande :

/h $_HANDLE$ /s $SAPSERVER$ /t $SAPTYPE$
s'affichent comme suit pour l'exécutable :

/h 1275366 /s “Houston, TX” /t 43
Le descripteur Microsoft Windows associé à l'application est un paramètre interne pris en charge défini comme $_HANDLE$.

Tous les paramètres internes utilisent $_ comme préfixe afin d’éviter les conflits de nom. Les paramètres d’implémenteur ne permettent pas d’utiliser des traites de soulignement dans les noms de clés.

La priorité de remplacement est définie pour conserver les valeurs de paramètre après qu'ils ont été écrits. La priorité est définie comme suit : paramètres internes (ex. $_HANDLE$), suivis des paramètres d'implémenteur, puis des variables d'environnement.

Tous les paramètres d'implémenteur autorisent l'utilisation de lettres minuscules et majuscules et de chiffres dans les noms de clés. La casse n'est pas prise en compte dans les noms de clés.

Si l'exécutable d'identification d'extension requiert que les paramètres soient présentés selon une séquence spécifique, la valeur Argument doit prendre en charge la séquence requise. Les paires nom/valeur du paramètre définies dans la boîte de

dialogue Ajout d’extension d’identification peuvent suivre n'importe quelle séquence.

Les extensions d'actions utilisent un processus externe pour gérer les actions de gestion des informations d'identification de l'utilisateur. Le processus de définition d'extension est capable de transmettre les informations d'identification de l'utilisateur à l'application externe.

Une fois qu'un formulaire de gestion des informations d'identification a été identifié (voir *— Extensions d'identification*), vous pouvez effectuer l'action de gestion des informations d'identification suivante en utilisant une combinaison quelconque d'actions de formulaires, de séquences d'actions ou d'extensions d'actions Windows standard.

Single Sign-On Plug-in prend en charge les mêmes fonctions que celles précédemment décrites dans la section *— Extensions d'identification*.

Le plug-in exécute le processus externe et attend pendant l'intervalle de temps spécifié que le processus se termine (si WaitForCompletion est défini sur TRUE), puis analyse son code de sortie. Si le processus se termine en renvoyant la valeur zéro, l'extension a été correctement exécutée. Toute valeur autre que zéro indique une erreur.

Si un processus renvoie une valeur négative, l'erreur est consignée dans l'Observateur d'événements Windows. Les valeurs positives sont consignées dans un fichier journal, si celui-ci est activé (pour plus d'informations, veuillez consulter la section *— Activation de la journalisation*).

Pour définir une extension d'action

Configurez les extensions d'actions à l'aide de l'assistant de définition de formulaire pendant le processus de développement de définitions d'application.

1. À partir de Citrix AppCenter, développez le nœud Single Sign-On, sélectionnez Définitions d'application, et à partir du menu Action, cliquez sur Créer une définition d'application.
2. Dans l'assistant de définition d'application, accédez à la page Gérer les formulaires et sélectionnez Ajouter un formulaire pour démarrer l'assistant de définition de formulaire.
3. Avancez dans le processus de définition jusqu'à ce que la page Définir les actions du formulaire s'affiche.
4. Dans la page Définition des actions du formulaire, cliquez sur Éditeur d'action.
5. Dans la boîte de dialogue Éditeur d'action, sélectionnez Lancement de l'extension de l'action. Le volet Configuration d'actions s'affiche. Ce volet permet d'afficher, de modifier ou d'ajouter des entrées Lancement de l'extension de l'action à la séquence d'actions.
6. Pour ajouter une extension d'action à la séquence d'actions, entrez les informations suivantes, puis cliquez sur Insérer :

ID	L'identificateur identifie le paramètre NomExtension à rechercher dans les paramètres du registre.
Description	Description définie par l'utilisateur de l'extension d'action.
Paramètres	Toute paire nom/valeur (nom de paramètre/valeur de paramètre) utilisée pour transmettre les paramètres définis par l'implémenteur au processus externe lancé par cette extension.

Comme c'est le cas pour les extensions d'identification, NomExtension identifie le nom de la clé de registre. Ce nom de clé et les valeurs de clé associées définissent l'exécutable de traitement de l'action externe et ses caractéristiques d'utilisation. Le nom de clé de registre et les clés associées se situent à l'emplacement suivant :

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extension\{NomExtension}]

où la valeur NomExtension est identifiée par la valeur d'ID définie dans le volet Configuration d'actions.

Sur les plates-formes 64 bits, le nom de clé de registre et les clés associées se situent à l'emplacement suivant :

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\MetaFrame Password Manager\Extension\{NomExtension}]

Le tableau suivant définit les caractéristiques des valeurs de clé.

Clé	Type	Valeur
Type	REG_SZ	Doit être EXECUTABLE
Timeout	REG_DWORD	0 indique d'attendre que l'application se termine. Toute autre valeur indique la période d'attente en millisecondes.
TerminateProcess	BOOL implémenté en tant que REG_DWORD	Au terme du délai d'expiration, terminer le processus (facultatif). TRUE : (valeur par défaut) terminer le processus. FALSE : (0) ne pas terminer le processus.
WaitForCompletion	BOOL implémenté en tant que REG_DWORD	Le plug-in attend que le processus se termine (facultatif). TRUE : (valeur par défaut) attendre FALSE : (0) ne pas attendre.
Exécutable	REG_EXPAND_SZ	Processus exécutable et son chemin d'accès complet.
Arguments	REG_SZ	Paramètres de l'exécutable.

La valeur Executable suit les mêmes conventions que pour les extensions d'identification.

La valeur Arguments prend en charge les paramètres que le plug-in peut remplacer par des paramètres d'exécution ou les paires nom/valeur de paramètre spécifiées dans la vue Lancement de l'extension de l'action de l'Éditeur d'action. Chaque paramètre à remplacer doit contenir un délimiteur$ (signe dollar) en préfixe et suffixe. Par exemple, les arguments de ligne de commande :

/h $_HANDLE$ /s $SAPSERVER$ /t $SAPTYPE$
s'affichent comme suit pour l'exécutable :

/h 1275366 /s “Houston, TX” /t 43
Le descripteur Microsoft Windows associé à l'application est un paramètre interne pris en charge défini comme $_HANDLE$.

Tous les paramètres internes utilisent $_ comme préfixe afin d’éviter les conflits de nom. Les paramètres d’implémenteur ne permettent pas d’utiliser des traites de soulignement dans les noms de clés.

Outre le descripteur Windows, les paramètres internes suivants sont également pris en charge pour la gestion des informations d'identification de l'utilisateur :

- Nom d'utilisateur ($_USERNAME$)
- Mot de passe ($_PASSWORD$)
- Personnalisé1 ($_CUSTOM1$)
- Personnalisé2 ($_CUSTOM2$)
- Ancien mot de passe ($_OLDPASSWORD$)

La priorité de remplacement est définie pour conserver les valeurs de paramètre après qu'ils ont été écrits. La priorité est définie comme suit : paramètres internes, suivis des paramètres d'implémenteur, puis des variables d'environnement.

Tous les paramètres d'implémenteur autorisent l'utilisation de lettres minuscules et majuscules et de chiffres dans les noms de clés. La casse n'est pas prise en compte dans les noms de clés.

Si l'exécutable d'identification d'extension requiert que les paramètres soient présentés selon une séquence spécifique, la valeur Argument doit prendre en charge la séquence requise. La séquence dans laquelle les paires nom/valeur de paramètre sont définies dans la boîte de dialogue Configuration d'actions peut être un ordre quelconque.

Les processus externes utilisés pour effectuer des actions de correspondance avancées ou de gestion des informations d'identification sont définis comme des processus ou des applications qui peuvent être lancés à partir d'une interface de ligne de commande. Tous les arguments obligatoires ou facultatifs des extensions d'identification ou d'action doivent également pouvoir être spécifiés en ligne à l'aide d'une interface de ligne de commande.

Pour les extensions d'action, l’implémenteur doit prendre en charge les mêmes fonctions que la détection Windows décrite ci-dessus. Il doit en effet être en mesure de transmettre les informations d’identification Nom d'utilisateur, Mot de passe, Personnalisation1, Personnalisation2 et Ancien mot de passe à l'exécutable.

Pour les extensions d'identification et d'action, l'implémenteur est chargé des opérations suivantes :

- déploiement de tous les exécutables, modules de support et fichiers permettant de prendre en charge l'extension sur Single Sign-On Plug-in ;
- gestion de tous les modules déployés ;
- ajout de toutes les entrées de registre spécifiées sur le plug-in ;
- maintien du caractère unique des noms d'extension dans leurs domaines.

Le schéma de nom d'extension recommandé est un schéma de nom de domaine inverse (ex. com.citrix.cpm.ext4).

Pour activer le suivi de débogage de Single Sign-On Plug-in, vous devez effectuer une modification du registre.

Le nom de clé de registre et les clés associées se situent à l'emplacement suivant :

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Log]

Le tableau suivant définit les caractéristiques des valeurs de clé.

Clé	Type	Valeur
Activé	REG_DWORD	La valeur par défaut est 0. 0 : désactivé. 1 : activé.
Filtre	REG_DWORD	Masque de bit déterminant ce qui doit être consigné. 0x00000001 : indicateur d'application Windows utilisé pour consigner les erreurs d'extensions d'identification. 0x00000004 : mot de passe Windows utilisé pour consigner les erreurs d'extensions d'actions.
MaxSizeInBytes	REG_DWORD	Taille maximum du fichier journal, en octets. La valeur maximum théorique peut être de 4 Go (2^32). Valeur par défaut : 819200

Les données du fichier journal sont consignées dans un fichier sso_.log situé dans :

```
%LocalAppData%\Citrix\MetaFrame Password Manager
```

Code clavier virtuel pour les applications Windows, Web et d'émulateur de terminal

Oct 21, 2015

Single Sign-On prend en charge le code clavier virtuel pour les applications Windows, Web et d'émulateur de terminal. Ces codes permettent l'envoi de frappes clavier à des formulaires d'ouverture de session ou de modification de mot de passe.

Utilisez les identifiants suivants pour créer une séquence de codes clavier pour pour les applications Windows et Web.

Code	Description
'DELAY=N'	N est la valeur en milli-secondes de la pause.
'VKEY=N'	N est le code clavier virtuel à transmettre.

Par exemple, pour envoyer les frappes Tab, Fin, Espace, puis une pause de 1,5 secondes, la chaîne Nom d'utilisateur, la touche Espace, le nom d'utilisateur/ID, la touche Début, une pause de 0,35 seconde, la touche Tab puis le mot de passe, utilisez la ligne suivante.

VTabKey1= 'VKEY=9''VKEY=35' 'DELAY=1500 'Logon username'VKEY=32' VTabKey2='VKEY=36''DELAY=350''VKEY=9'

Clé	Code	Clé	Code	Clé	Code	Clé	Code
Pause	3	5	53	V	86	F5	116
Retour en arrière	8	6	54	W	87	F6	117
Onglets	9	7	55	X	88	F7	118
Suppr	12	8	56	O	89	F8	119
Entrée	13	9	57	Z	90	F9	120
Majuscule	16	A	65	Gauche (fenêtre)	91	F10	121
Ctrl	17	B	66	Droite (fenêtre)	92	F11	122
Alt	18	C	67	0 (du pavé numérique)	96	F12	123
Verr. Maj.	20	D	68	1 (du pavé numérique)	97	F13	124
Échap.	27	E	69	2 (du pavé numérique)	98	F14	125

Clé	Code	Clé	Code	Clé	Code	Clé	Code
Barre espace	32	F	70	3 (du pavé numérique)	99	F15	126
Page haut	33	G	71	4 (du pavé numérique)	100	F16	127
Page suivante	34	H	72	5 (du pavé numérique)	101	F17	128
Fin	35	I	73	6 (du pavé numérique)	102	F18	129
Home	36	J	74	7 (du pavé numérique)	103	F19	130
Gauche	37	K	75	8 (du pavé numérique)	104	F20	131
Haut	38	L	76	9 (du pavé numérique)	105	F21	132
Droit	39	M	77	Astérisque (*)	106	F22	133
Bas	40	N	78	Plus (+)	107	F23	134
Impression écran	44	O	79	Moins (-)	109	F24	135
Aide	47	P	80	Point (.)	110	Verr. Num.	144
0	48	Q	81	Barre oblique (/)	111	Arrêt défil.	145
1	49	R	82	F1	112	MAJ gauche	160
2	50	S	83	F2	113	MAJ droit	161
3	51	T	84	F3	114	Ctrl gauche	162
4	52	U	85	F4	115	Crtl droit	163

Caractère/commande	Code	Caractère/commande	Code	Caractère/commande	Code
Alt curseur	@$	Impression locale	@P	PF12/F12	@c
Retour en arrière	@<	Reset	@R	PF13/F13	@d
@	@@	Majuscule	@S	PF14/F14	@e
Alt	@A	Copier	@S@x	PF15/F15	@f
Champ -	@A@-	Marque champ	@S@y	PF16/F16	@g

Caractère/commande	Code	Caractère/commande	Code	Caractère/commande	Code
Champ +	@A@+	TAB droit	@I	PF17/F17	@h
Sortie champ	@A@E	Haut	@U	PF18/F18	@i
Alt curseur	@$	Bas	@V	PF19F19	@j
Effacer saisie	@A@F	Gauche	@L	PF20/F20	@k
Demande système	@A@H	Droite	@Z	PF21/F21	@l
Insérer basculement	@A@I	Page haut	@u	PF22/F22	@m
Sélection curseur	@A@J	Page suivante	@v	PF23/F23	@n
Attention	@A@Q	Fin	@q	PF24/F24	@o
Impression écran	@A@T	Home	@0	PA1	@x
Héxadecimal	@A@X	PF1/F1	@1	PA2	@y
Touche commande/fonction	@A@Y	PF2/F2	@2	PA3	@z
Impression (PC)	@A@t	PF3/F3	@3	PA4	@+
Tabulation gauche/retour	@B	PF4/F4	@4	PA5	@%
Suppr	@C	PF5/F5	@5	PA6	@&
Supprimer	@D	PF6/F6	@6	PA7	@’
Entrée	@E	PF7/F7	@7	PA8	@(
Effacer fin du fichier	@F	PF8/F8	@8	PA9	@)
Aide	@H	PF9/F9	@9	PA10	@*
Insérer	@I	PF10/F10	@a		
Nouvelle ligne	@N	PF11/F11	@b		

Kit de développement de logiciel (SDK - Software Development Kit) de l'habilitation Single Sign-On (en anglais)

Oct 21, 2015

Le kit de développement de logiciel de l'habilitation Single Sign-On vous permet de gérer entièrement les informations d'identification secondaires des utilisateurs. Les informations d'identification secondaires, qui sont spécifiques à certaines applications, sont celles que Single Sign-On soumet au nom de l'utilisateur, après que l'authentification principale sur le domaine a eu lieu.

L'habilitation des informations d'identification vous permet d'automatiser de nombreuses tâches associées à la gestion des informations d'identification des utilisateurs. Lors d'une nouvelle installation de Single Sign-On, de l'ajout de nouveaux utilisateurs, de l'ajout de nouvelles applications ou de la suppression d'informations inutiles, l'habilitation apporte les outils permettant d'accomplir ces tâches avec plus de rapidité et d'efficacité.

Cette aide en ligne décrit les grandes lignes du concept de la fonctionnalité d'habilitation des informations d'identification de Single Sign-On et offre un résumé des fonctions API que vous pouvez utiliser pour définir les actions dans le fichier XML d'habilitation.

Le module de provisioning fait partie de Single Sign-on Service et est un service Web standard qui expose un protocole Simple Object Access Protocol et une interface Service Provisioning Markup Language (SOAP/SPML) pour recevoir des commandes de provisioning. Toutes les communications entre le client et le module de provisioning se produisent via un canal Transport Layer Security (TLS).

Lors de l'envoi des commandes de provisioning à une file d'attente, assurez-vous que les données sont stockées de manière sécurisée et ne sont pas transmises via une connexion réseau non sécurisée.

Le module de provisioning doit posséder un accès en lecture et en écriture au magasin central Single Sign-on pour pouvoir mettre en file d'attente les commandes de provisioning entrantes jusqu'à ce que Single Sign-on Plug-in exécute les commandes.

Les commandes envoyées au module de provisioning ne peuvent être rappelées. Une fois envoyées, les commandes restent en file d'attente jusqu'à ce qu'elles soient exécutées par Single Sign-in Plug-in. Si vous devez supprimer une commande de la file d'attente, envoyez la commande opposée pour chaque utilisateur, application et objet credential devant être supprimé de la file d'attente.

Remarque : le module de provisioning utilise une interface qui se conforme à SPML 2.0. Seules les opérations de noyau requises pour conformité sont prises en charge.

Modèle SPML 2.0

Le fichier XML de provisioning et tout composant tiers qui délivrent des requêtes SPML sont appelés autorités de requête (RA).

Le module de provisioning est un fournisseur de service de provisioning (PSP). Ce PSP prend en charge une cible de service de provisioning unique (PST) qui réalise une mise en file d'attente par utilisateur des commandes de provisioning de single sign-

on.

Lors de l'exécution du provisioning, les utilisateurs se voient offrir des informations d'identification secondaires. Cela signifie que les utilisateurs finals et les informations d'identification secondaires sont les objets de service de provisioning (PSO) de la cible de service de provisioning. L'identificateur unique (PSO-ID) de chaque utilisateur final est un nom de domaine complet (FQDN). L'identificateur unique (PSO-ID) de chaque information d'identification secondaire est le GUID attribué à l'information d'identification lorsqu'elle est créée. Puisque les informations d'identification secondaires sont associées à un utilisateur particulier, l'utilisateur PSO agit en tant que conteneur pour les PSO des informations d'identification. Ceci est représenté par l'élément containerID dans une requête SPML.

Proprement dit, le single sign-on n'ajoute, ne modifie ou ne supprime pas d'utilisateurs ; cependant, le single sign-on n'ajoute, ne modifie ou ne supprime pas de données associées à un utilisateur.

Single Sign-on Plug-in étant responsable de la protection des informations d'identification secondaires d'un utilisateur avec des clés de cryptage spécifiques à cet utilisateur, l'exécution des opérations de provisioning est un processus à deux étapes. Vous devez tout d'abord soumettre la commande de provisioning sur un module de provisioning. Puis, au nom de son utilisateur courant, Single Sign-on Plug-in applique toute commande de provisioning en file d'attente au magasin d'informations d'identification secondaire de l'utilisateur.

Single Sign-on Plug-in détecte la présence des opérations de provisioning en file d'attente lors de son processus de synchronisation régulier, qui se produit au démarrage. Le plug-in exécute les commandes de provisioning en file d'attente avant de reprendre une activité normale. Ceci assure que dans le scénario de première utilisation, le plug-in réalise tout d'abord les actions de provisioning, réduisant ainsi les actions de configuration de première utilisation de l'utilisateur final.

Toutes les communications entre Single Sign-on Plug-in et le module de provisioning se produisent via une connexion sécurisée TLS.

L'application de provisioning client doit définir le mappage entre les applications répertoriées comme disponibles pour le provisioning et la représentation côté client de l'application.

Les informations d'identification secondaires sont associées à une définition d'application spécifique créée à l'aide du composant Single Sign-on de AppCenter ; ainsi, l'opération addRequest doit inclure des données qui lient les détails de l'utilisateur dans la requête pour une définition d'application spécifique. Ceci signifie que l'autorité de requête doit déterminer la liste des applications disponibles pour le provisioning par utilisateur, et fournissent un ID de la définition d'application faisant partie de l'opération addRequest. Ceci alourdit l'autorité de requête en déterminant l'association entre les définitions d'application de Single sign-on et votre identification externe (comme le nom de l'application) des applications auxquelles vous appliquez le provisioning.

Puisque la personne qui administre le single sign-on et la personne qui réalise les tâches de provisioning ne doivent pas être la même, cela peut prêter à confusion. Par exemple, un administrateur single sign-on peut définir l'application « Microsoft Outlook », tandis qu'un administrateur de provisioning crée des comptes « Microsoft Exchange ». Le single sign-on permet les informations d'identification secondaires multiples pour une définition d'application donnée. Par exemple, un utilisateur pourrait posséder plusieurs comptes MSN Hotmail pour lesquels le single sign-on a stocké des informations d'identification. Cette capacité signifie qu'il est valide pour un administrateur de délivrer plusieurs addRequests avec des paramètres identiques. Dans ce cas, plusieurs informations d'identification secondaires sont créées. De même, il se peut que l'administrateur souhaite provisionner plusieurs informations d'identification différentes pour la même application ;

cependant, les secrets de l'information d'identification (champs user ID, password et custom) sont cryptés par Single Sign-on Plug-in et ne sont pas récupérables par le module de provisioning pour aider l'autorité de requête en distinguant les informations d'identification à une date ultérieure.

Pour vous aider à adresser ces problèmes, un champ de données privée d'autorité de requête facultative, provision description est disponible dans les opérations addRequest et modifyRequest. Ceci offre à l'autorité de requête la possibilité d'ajouter un ID ou des données descriptives afin de l'aider à distinguer les informations d'identification. Ce champ n'est pas modifié ou affiché par Single Sign-on Plug-in ou le module de provisioning. Il est conservé et retourné à l'autorité de requête lorsqu'une liste d'informations d'identification est requise au travers d'une lookupRequest.

Single Sign-on Plug-in possède un accès/modification complet de toutes les informations d'identification secondaires. Ceci comprend des actions telles que la duplication, la suppression et la modification des informations d'identification. Ceci signifie que les utilisateurs peuvent modifier leurs données afin qu'elles ne correspondent plus à l'état créé par les opérations de provisioning.

De même, les utilisateurs peuvent définir des applications à volonté, ce qui signifie qu'ils peuvent ajouter des informations d'identification aux applications non définies dans la console Single sign-on. Cette capacité peut amener à des problèmes de propriété tels que si un administrateur peut supprimer ou modifier ou non une information d'identification secondaire ou si ces informations d'identification devraient être répertoriées dans une lookupResponse. Cette version de Single sign-on ne prend en charge aucune restriction de propriété ; toutes les informations d'identification peuvent être modifiées soit par l'administrateur soit par l'utilisateur final.

Single Sign-on vous permet de grouper des applications. Un attribut de ce groupement est qu'il peut ou non utiliser le même mot de passe pour toutes les informations d'identification définies pour les applications du groupe. Chaque fois qu'un utilisateur modifie une information d'identification associée à un groupe, la modification est appliquée à toutes les informations d'identification de toutes les applications du groupe.

Ce comportement persiste lorsque des modifications sont effectuées au travers de l'API de provisioning. De manière plus spécifique, si une information d'identification est ajoutée à un groupe d'applications, le nouveau mot de passe fourni en tant que paramètre à la commande add devient le nouveau mot de passe de chaque application du groupe. Ainsi, la commande add possède l'effet net d'une commande add et de plusieurs commandes modify. De manière similaire, une commande modify modifie toutes les applications d'un groupe et ainsi possède l'effet net de plusieurs commandes modify.

Code	Description
101	Un ou plusieurs champs d'informations d'identification requis sont manquant dans la requête de provisioning
102	Nom d'utilisateur non valide spécifié ; le nom d'utilisateur est soit manquant soit le format n'est pas correct
103	Utilisateur spécifié introuvable
104	Définition d'application non valide ; soit la définition d'application est manquante soit elle a une structure non valide
105	L'identificateur d'information d'identification n'est pas à un format valide.

Code	Description
106	Information d'identification spécifiée introuvable.
107	Jeton de sécurité d'autorisation non valide.
108	Jeton d'accès non autorisé. Jeton spécifié non autorisé à réaliser l'opération requise.
109	Le mécanisme de stockage est accédé par un autre processus. Veuillez réessayer plus tard.
110	Une erreur s'est produite lors de la consommation des commandes de provisioning.
111	L'utilisateur n'est pas autorisé à accéder à la file d'attente des commandes de provision d'accès.
112	Une erreur s'est produite lors de l'obtention de la clé secrète de provisioning.
113	Impossible d'attribuer de la mémoire pour le cryptage.
114	Impossible d'allouer le tampon de données de l'entropie.
115	Échec du cryptage.
116	Impossible d'attribuer le tampon cipherText.
117	Échec du décryptage.
118	Échec de formatage du code d'erreur Windows en message d'erreur.
119	l'ID du Pso est soit manquant soit ne se trouve pas au format approprié.
120	L'application référencée est introuvable.
121	La configuration utilisateur de l'utilisateur requis est introuvable.
122	L'attribut « join » est manquant pour l'information d'identification du groupe de partage de mot de passe.
123	L'attribut « use-new-password » est manquant pour l'information d'identification du groupe de partage de mot de passe.
124	Le mot de passe est manquant pour l'information d'identification du groupe de partage de mot de passe.
125	Le nom d'information d'identification est non valide ou manquant. Veuillez spécifier un nom d'information d'identification valide.
126	ID d'application spécifié non valide.
127	L'information d'identification ne peut rejoindre le groupe de partage de mot de passe.
128	Le provisioning n'est pas activé pour le compte d'utilisateur spécifié.

Résumé des fonctions API

Oct 21, 2015

Les fonctions API offrent une méthode que vous pouvez utiliser pour définir des actions dans le fichier XML de provisioning. En plus du code exemple dans ces rubriques, du code exemple supplémentaire est disponible sur le support d'installation de votre produit.

Tous les éléments spécifiques et attributs introduits de single sign-on possèdent le préfixe d'indicateur de namespace « ctxs ». Le fragment XML de chaque zone de texte répertorie à la fois une requête et une réponse qui lui correspond.

Seul le mode d'exécution synchrone est pris en charge. Toute requête d'utilisation de l'exécution asynchrone provoque des erreurs unsupportedExecutionMode.

Par souci de concision, les substituts descriptifs suivants sont utilisés à la place des valeurs d'exemple :

Texte de substituts	Interprétation
Nom de domaine complet	Nom de domaine complet de l'utilisateur
application-GUID	GUID attribué à une définition d'application lorsqu'elle est créée à l'aide du composant Single Sign-on de Citrix AppCenter.
credential-GUID	GUID attribué à l'information d'identification secondaire provisionnée par le service de provisioning jusqu'à la fin d'une addRequest.
RA-generated-ID	ID unique de requête créée par l'autorité de requête. Utilisé dans l'attribut facultatif requestID des éléments de requête. Ceci est uniquement pertinent si la prise en charge de l'exécution asynchrone est ajoutée.
AuthToken	L'élément authentication-token est obligatoire, mais n'est pas utilisé en ce moment.

Provisioning d'une application unique - addRequest

Oct 21, 2015

Utilisez l'opération addRequest pour ajouter des informations d'identification à une application pour un utilisateur.

Une opération addRequest requiert l'ajout d'un nouvel objet (l'information d'identification) à l'objet de conteneur spécifié (magasin de données de l'utilisateur). Un containerID (nom de domaine complet de l'utilisateur (FQDN)) doit être spécifié et le psoID (identificateur global unique des informations d'identification) de l'objet nouvellement créé est retourné. Les données de la requête sont les données spécifiques de l'information d'identification devant être créée.

Si la définition d'application attribuée à la nouvelle information d'identification est membre d'un groupe de partage de mot de passe, alors, les informations d'identification associées aux membres de ce groupe sont mises à jour et utilisent le nouveau mot de passe.

AuthToken Credential name Admin Text Credential description appdefGuid Domain salima pass123 domain database

requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à cette requête.
targetID (obligatoire)	C'est l'ID du Module de provisioning, identifié par targetID 'CPM Provisioning 1.0.'
returnData (obligatoire)	data : détails d'une information d'identification secondaire identifier : liste d'informations d'identification d'un utilisateur name : non pris en charge dans Single Sign-On everything : définitions d'application disponible pour l'utilisateur spécifié
executionMode (obligatoire)	Single sign-on prend en charge le mode d'exécution synchrone.
authentication-token (obligatoire)	L'élément authentication-token est obligatoire, mais n'est pas utilisé en ce moment. .
containerID (obligatoire)	containerID fournit le FQDN de l'utilisateur qui possède l'information d'identification.
data (obligatoire)	Data est la description des données en cours de modification. Ceci est l'élément credential et peut comprendre tout élément enfant des éléments credential et application.
ctxs:credential (obligatoire)	L'élément credential est utilisé pour décrire une seule information d'identification secondaire unique. Le nom et la description enfant de l'élément credential sont facultatifs. S'ils ne sont pas fournis, le plug-in utilise le nom et la description de la définition d'application.

ctxs:application (obligatoire)	L'élément application est utilisé à la fois pour décrire une définition d'application et pour décrire les détails d'une information d'identification. L'élément application doit correspondre à un élément précédemment obtenu à partir d'une opération lookupApplicationsRequest.

status (obligatoire)	Valeurs possibles : Success, Failure, Pending
requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à la requête associée.
pso (obligatoire)	Les données du pso sont des informations d'identification comme décrit dans ctxs:credential.
psoID (obligatoire)	Le psoID est un identifiant unique pour chaque utilisateur final ; PSOID est la valeur de l'identificateur global unique des informations d'identification retournée par lookupResponse.
containerID (obligatoire)	containerID fournit le FQDN de l'utilisateur qui possède l'information d'identification.
data (obligatoire)	Data est la description des données en cours de modification. Ceci est l'élément credential et peut comprendre tout élément enfant des éléments credential et application.

Les attributs join et use-new-password de l'élément de groupe contrôle la manière dont les nouvelles informations d'identification affectent les membres existants du groupe. Si le groupe d'applications n'a pas été configuré pour partager des mots de passe, l'élément group est ignoré.

Valeur Join	Valeur Use-new-password	Effet
False	False	La nouvelle information d'identification est dissociée des informations d'identification existantes du groupe. Il n'existe aucun effet sur le groupe existant.
False	True	La nouvelle information d'identification est dissociée des informations d'identification existantes du groupe. Il n'existe aucun effet sur le groupe existant.
True	False	La nouvelle information d'identification est jointe au groupe existant. Le mot de passe de la nouvelle information d'identification est défini sur le mot de passe partagé par les membres existants du groupe. S'il n'existe aucun membres existants dans le groupe, la valeur password est utilisée.
True	True	La nouvelle information d'identification est jointe au groupe existant. Le mot de passe inclus dans la commande est utilisé pour la nouvelle information d'identification et également

Valeur Join	Valeur Use-new-password	Effet
		attribuée à tous les autres membres existants du groupe.

L'identificateur global unique des informations d'identification retournées en tant que psoID dans la réponse est le même que celui qui sera répertorié dans l'opération lookupResponse et qui peut aussi être utilisé pour identifier cette information d'identification secondaire dans une opération modifyRequest ou deleteRequest.

batchRequest - Exécution de traitements par lots

Oct 21, 2015

L'opération batchRequest agit en tant que conteneur pour une liste contenant d'autres opérations (requestnameRequest). Single Sign-On prend en charge le mode de traitement séquentiel uniquement. batchRequest qui spécifie un traitement parallèle ne résulte pas en une erreur, mais est traité de manière séquentielle.

AuthToken Credential name appdefGuid janed pwd123 AuthToken Credential name appdefGuid2 salima pass123

processing (obligatoire)	Ceci est un mode de traitement. Les valeurs valides sont « séquentielles » et « parallèles » ; cependant, Single Sign-On ne prend en charge que le mode séquentiel. Lorsque le mode de traitement parallèle est spécifié, Single Sign-On traite la requête de manière séquentielle.
onError	Ceci est l'action que vous souhaitez voir Single Sign-On prendre lorsqu'une erreur se produit lors du traitement. Les valeurs valides sont « resume » et « exit ».
requestnameRequest (obligatoire, variable)	Répertorie chaque requête que vous souhaitez procéder dans ce lot, à l'aide de la syntaxe et des paramètres spécifiés pour cette requête.

requestnameResponse (variable)	Le nom de chaque requête spécifiée pour traitement dans cette requête de traitement de lots. Pour la syntaxe des valeurs retournées liée à chaque requête, référez-vous à la documentation de cette requête.

Suppression d'une information d'identification - deleteRequest

Oct 21, 2015

Utilisez l'opération deleteRequest pour supprimer une seule information d'identification. L'identificateur global unique des informations d'identification spécifie l'information d'identification devant être supprimée.

AuthToken

requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à cette requête.
executionMode (obligatoire)	Single sign-on prend en charge le mode d'exécution synchrone.
authentication-token (obligatoire)	L'élément auth-token est obligatoire, mais n'est pas utilisé en ce moment.
psoID (obligatoire)	Le psoID est un identifiant unique pour chaque utilisateur final ; PSOID est la valeur de l'identificateur global unique des informations d'identification retournée par lookupResponse.
containerID (obligatoire)	containerID fournit le FQDN de l'utilisateur qui possède l'information d'identification.

status (obligatoire)	Valeurs possibles : Success, Failure, Pending
requestID	C'est un identificateur généré par le client qui associe les valeurs de retour à la requête associée.

Suppression d'un utilisateur - deleteRequest

Oct 21, 2015

Utilisez l'opération deleteRequest pour supprimer toute donnée associée avec un utilisateur d'un magasin central.

AuthToken

requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à cette requête.
executionMode	Single sign-on prend en charge le mode d'exécution synchrone.
authentication-token	L'élément authentication-token est obligatoire, mais n'est pas utilisé en ce moment.
psoID (obligatoire)	Le psoID est un identifiant unique pour chaque utilisateur final ; PSOID est la valeur de l'identificateur global unique des informations d'identification retournée par lookupResponse.

status (obligatoire)	Valeurs possibles : Success, Failure, Pending
requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à la requête associée.

Vous pouvez choisir de complètement supprimer des données associées à des utilisateurs spécifiques lorsqu'ils quittent l'entreprise. De même, si les utilisateurs oublient leurs informations critiques et ne peuvent accéder à leurs informations d'identification, vous pouvez choisir de réinitialiser leur état Single Sign-On afin qu'ils puissent recommencer (voir resetRequest).

Ces deux scénarios, suppression complète des données et réinitialisation des données, doivent être différenciés car Single Sign-On Plug-in se comporte différemment dans chaque cas. Selon les paramètres administrateur, il se peut qu'il existe une copie locale des données Single Single Sign-On de l'utilisateur dans le profil de l'utilisateur. Si aucune donnée utilisateur n'existe dans le magasin central, le plug-in exécute un assistant d'enregistrement et copie les données locales de l'utilisateur dans le magasin central.

Lors du scénario de réinitialisation utilisateur, le logiciel du plug-in élimine les données locales puis exécute l'assistant d'enregistrement.

Interrogation des cibles - listTargetsRequest

Oct 21, 2015

L'opération listTargetsRequest interroge les cibles configurées sur le système. Le service Single Single Sign-On prend en charge une seule cible unique, le module de provisioning, identifié par targetID 'CPM Provisioning 1.0.'

AuthToken

requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à cette requête.
executionMode (obligatoire)	Single sign-on prend en charge le mode d'exécution synchrone.
authentication-token (obligatoire)	L'élément authentication-token est obligatoire, mais n'est pas utilisé en ce moment.

requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à la requête associée.
status (obligatoire)	Valeurs possibles : Success, Failure, Pending
targetID (obligatoire)	C'est l'ID du Module de provisioning : targetID='CPM Provisioning 1.0'.
schema (obligatoire)	La réponse de cette opération contient un ID unique du module et un schéma décrivant les objets dont le module de provisioning effectue la gestion, tels que les utilisateurs et leurs informations d'identification secondaires.

Obtention d'une liste d'applications disponibles pour un utilisateur - lookupApplicationRequest

Oct 21, 2015

Utilisez l'opération lookupApplicationRequest pour obtenir la liste des applications (y compris leur ID d'application) disponibles pour un utilisateur spécifique. Dans Single Sign-On, l'ensemble des définitions d'application disponibles pour un utilisateur est déterminé par la configuration utilisateur associée à l'utilisateur dans la console. Ces définitions d'application ne sont pas en possession de l'utilisateur et ne peuvent pas être modifiées en dehors de la console.

AuthToken

requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à cette requête.
authentication-token (obligatoire)	L'élément authentication-token est obligatoire, mais n'est pas utilisé en ce moment.
psoID (obligatoire)	Le psoID est un identifiant unique pour chaque utilisateur final ; PSOID est le nom complet de l'utilisateur.

app-GUID1 Outlook Outlook 2003 Domain app-GUID2 Vantive Bug Database SAP

status (obligatoire)	Valeurs possibles : Success, Failure, Pending
requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à la requête associée.
psoID (obligatoire)	Le psoID est un identifiant unique pour chaque utilisateur final ; PSOID est le nom complet de l'utilisateur.
data (obligatoire)	Data est la description des données en cours de modification. Ceci est l'élément credential et peut comprendre tout élément enfant des éléments credential et application.
ctxs:application (obligatoire)	L'élément application est utilisé à la fois pour décrire une définition d'application et pour décrire les détails d'une information d'identification. L'élément application doit correspondre à un élément précédemment obtenu à partir d'une opération lookupApplicationRequest. Il existe exactement un seul élément application pour chaque élément application pour chaque définition d'application disponible dans la configuration utilisateur. Voir ctxs:application pour plus d'informations.

Une recherche pour ce types de données est une anomalie non couverte dans les sémantiques SPML standards. Une capacité personnalisée est utilisée pour obtenir la liste des définitions d'application disponibles pour un utilisateur.

Obtention d'une liste d'applications pour lesquelles les informations d'identification sont stockées - lookupRequest

Oct 21, 2015

Utilisez l'opération lookupRequest pour obtenir la liste des applications pour lesquelles un utilisateur a stocké les informations d'identification. La valeur de l'attribut returnData détermine le niveau de détails retourné.

AuthToken

requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à cette requête.
returnData (obligatoire)	data : détails d'une information d'identification secondaire identifier : liste d'informations d'identification d'un utilisateur name : non pris en charge dans Single Sign-On everything : définitions d'application disponible pour l'utilisateur spécifié
executionMode (obligatoire)	Single sign-on prend en charge le mode d'exécution synchrone.
authentication-token (obligatoire)	L'élément authentication-token est obligatoire, mais n'est pas utilisé en ce moment.
psoID (obligatoire)	Le psoID est un identifiant unique pour chaque utilisateur final ; PSOID est la valeur de l'identificateur global unique des informations d'identification retournée par lookupResponse.

credential-GUID1 Aviva Aviva 5250 Demo Aviva 5250 app-GUID1 Aviva 5250 Demo AppGroup credential-GUID2 Dynamic App1

status (obligatoire)	Valeurs possibles : Success, Failure, Pending
requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à la requête associée.
pso (obligatoire)	Les données du pso sont des informations d'identification comme décrit dans ctxs:credential.
psoID (obligatoire)	Le psoID est un identifiant unique pour chaque utilisateur final ; PSOID est le nom complet de l'utilisateur. Selon le modèle SPML de Single Sign-On, les données du pso sont des informations d'identification comme décrit dans ctxs:credential. Cela serait inclus si l'attribut returnData était défini sur data ou everything. Il y a exactement un seul élément pso sur chaque information d'identification secondaire. L'attribut ID du psoID fournit l'identificateur global unique des informations d'identification.
data (obligatoire)	Data est la description des données recherchées. Ceci est l'élément credential et peut comprendre tout élément enfant des éléments credential et application.

ctxs:credential (obligatoire)	L'élément credential est utilisé pour décrire une seule information d'identification secondaire unique. Le nom et la description enfant de l'élément credential sont facultatifs. S'ils ne sont pas fournis, le plug-in utilise le nom et la description de la définition d'application. Voir ctxs:credential pour plus d'informations.
ctxs:application (obligatoire)	L'élément application est utilisé à la fois pour décrire une définition d'application et pour décrire les détails d'une information d'identification. L'élément application doit correspondre à un élément précédemment obtenu à partir d'une opération lookupApplicationRequest. Il existe exactement un seul élément application pour chaque définition d'application dans la configuration utilisateur de l'utilisateur. Voir ctxs:application pour plus d'informations.

Lorsqu'une opération lookupRequest spécifie une information d'identification, la réponse contient les détails de l'information d'identification. En règle générale, les secrets de chaque information d'identification sont cryptés par le logiciel du plug-in et ne peuvent être accédés par le module de provisioning. Ce qui signifie que les données du caractère des éléments de champs spécifiques sont vides pour les informations d'identification déjà gérées par le logiciel du plug-in.

Le provisioning est un processus en deux étapes. Tous d'abord, le module de provisioning met en file d'attente les commandes de provisioning. Ensuite, le logiciel du plug-in exécute les commandes mises en file d'attente. Pour vous permettre de vérifier une action que vous venez juste de réaliser, la liste des informations d'identification retournée doit tenir compte des commandes mises en file d'attente. Puisque les commandes mises en file d'attente sont protégées par le module de provisioning et non le logiciel du plug-in, le module de provisioning est capable de décrypter les paramètres de commande. Les informations d'identification qui ont placé en file d'attente des commandes add ou modify ont également répertoriés les paramètres des commandes accessibles lors de l'opération lookupResponse. Notez que les paramètres de commande peuvent inclure les valeurs userID, password et custom-field.

Récupération d'informations d'identification secondaire - lookupRequest

Oct 21, 2015

Utilisez cette opération pour récupérer les détails d'une information d'identification secondaire.

AuthToken

requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à cette requête.
returnData (obligatoire)	data : détails d'une information d'identification secondaire identifier : liste d'informations d'identification d'un utilisateur name : non pris en charge dans Single Sign-On everything : définitions d'application disponible pour l'utilisateur spécifié
executionMode (obligatoire)	Seul le mode d'exécution synchrone est pris en charge. Toute requête d'utilisation de l'exécution asynchrone provoque des erreurs unsupportedExecutionMode.
authentication-token (obligatoire)	L'élément authentication-token est obligatoire, mais n'est pas utilisé en ce moment.
psoID (obligatoire)	Le psoID est un identifiant unique pour chaque utilisateur final ; PSOID est le nom complet de l'utilisateur.
containerID (obligatoire)	containerID fournit le FQDN de l'utilisateur qui possède l'information d'identification.

Credential-name Admin text Credential description app-GUID Outlook description from app-def Domain

status (obligatoire)	Valeurs possibles : Success, Failure, Pending
requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à la requête associée.
psoID (obligatoire)	Le psoID est un identifiant unique pour chaque utilisateur final ; PSOID est le nom complet de l'utilisateur. Selon le modèle SPML de Single Sign-On, le données du pso sont une information d'identification comme décrit dans ctxs:credential Element. Cela serait inclus si l'attribut returnData

	était défini sur data ou everything. Il y a exactement un seul élément pso sur chaque information d'identification secondaire. L'attribut ID du psoID fournit l'identificateur global unique des informations d'identification.
containerID (obligatoire)	containerID fournit le FQDN de l'utilisateur qui possède l'information d'identification.
data (obligatoire)	Data est la description des données recherchées. Ceci est l'élément credential et peut comprendre tout élément enfant des éléments credential et application.
ctxs:credential (obligatoire)	L'élément credential est utilisé pour décrire une seule information d'identification secondaire unique. Le nom et la description enfant de l'élément credential sont facultatifs. S'ils ne sont pas fournis, Single Sign-on Plug-in utilise le nom et la description de la définition d'application. Voir ctxs:credential Element pour plus d'informations.
ctxs:application (obligatoire)	L'élément application est utilisé à la fois pour décrire une définition d'application et pour décrire les détails d'une information d'identification. L'élément application doit correspondre à un élément précédemment obtenu à partir d'une opération lookupApplicationRequest. Il existe exactement un seul élément application pour chaque définition d'application dans la configuration utilisateur de l'utilisateur. Voir ctxs:credential Element pour plus d'informations.

Modification d'une information d'identification - modifyRequest

Oct 21, 2015

Utilisez l'opération modifyRequest pour modifier une information d'identification précédemment provisionnée. Si la définition d'application associée à l'information d'identification modifiée est membre d'un groupe de partage de mot de passe, alors, toutes les informations d'identification associées aux membres de ce groupe sont mises à jour pour utiliser le nouveau mot de passe.

AuthToken New Credential Name username

requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à cette requête.
ctxs:authentication-token	L'élément authentication-token est obligatoire, mais n'est pas utilisé en ce moment.
psoID (obligatoire)	L'identificateur credential est un GUID (créé par le système Single Sign-On et stocké dans votre magasin central). Il doit correspondre à la valeur retournée par lookupRequest et est utilisé pour situer l'information d'identification en cours de modification.
containerID (obligatoire)	containerID fournit le FQDN de l'utilisateur qui possède l'information d'identification.
modification (obligatoire)	modificationMode (facultatif) add: pour ajouter des informations d'identification. Ceci produit le même résultat que addRequest. Si modificationMode est add, les restrictions du psoID et des éléments data sont les mêmes que pour addRequest. psoID doit uniquement spécifier un conteneur (comme dans deleteRequest) et les données doivent contenir un élément credential (comme dans addRequest). replace: pour remplacer une valeur field, placez la nouvelle valeur dans une balise. delete: pour effacer une valeur field. Le contenu de l'élément data est ignoré.
data (obligatoire)	Data est la description des données en cours de modification. Ceci est l'élément credential et peut comprendre tout élément enfant des éléments credential et application.
credential (obligatoire)	L'élément credential est utilisé pour décrire une seule information d'identification secondaire unique. Le nom et la description enfant de l'élément credential sont facultatifs. S'ils ne sont pas fournis, le plug-in utilise le nom et la description de la définition d'application. Voir ctx:credential pour plus d'informations.
name	name est le nom de la définition d'application comme il s'affiche dans votre composant Single

	Sign-on de AppCenter.
application (obligatoire)	L'élément application est utilisé à la fois pour décrire une définition d'application et pour décrire les détails d'une information d'identification. L'élément application doit correspondre à un élément précédemment obtenu à partir d'une opération lookupApplicationsRequest. Voir ctxs:application pour plus d'informations. Si le ID enfant d'une application est fourni, il doit correspondre à la valeur stockée dans l'information d'identification.
group	Les valeurs par défaut sont fournies si l'élément group ne fait pas partie de la requête add. Cet élément décrit la relation entre la nouvelle information d'identification et les informations d'identification existantes associées au groupe. Consultez les informations sur les attributs des éléments de groupe.
fields (obligatoire)	Chaque élément enfant de champs répertoriés dans l'opération doit être compris dans l'opération lookupResponse sinon une erreur est retournée.
userID (obligatoire)	userID offre cette information d'identification au compte de l'utilisateur.
password (obligatoire)	Password offre au compte de l'utilisateur le mot de passe associé à cette information d'identification.
custom-field	Custom-fields offre les valeurs personnalisées à cette information d'identification. Single Sign-On prend en charge deux champs personnalisés en plus des champs du nom d'utilisateur et du mot de passe.
psoID (obligatoire)	Le psoID est un identifiant unique pour chaque utilisateur final ; PSOID est le nom de domaine complet de l'utilisateur et il est utilisé pour spécifier le conteneur des informations d'identification en cours de modification.

status (obligatoire)	Valeurs possibles : Success, Failure, Pending
requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à la requête associée.

modifyRequest peut être utilisée pour effectuer une requête pour qu'une information d'identification dissociée rejoigne le groupe en définissant l'attribut join='true' (voir addRequest). L'élément group est sujet aux mêmes contraintes et a le même effet que décrit sous addRequest.

Notez que tout sous-élément ctxs:fields défini pour l'application peut être inclus dans une modifyRequest. Les champs disponibles sont répertoriés dans

— lookupResponse

.

Valeur Join	Valeur Use-new-password	Effet
False	True	La nouvelle information d'identification est dissociée des informations d'identification existantes du groupe. Il n'existe aucun effet sur le groupe existant.
True	False	La nouvelle information d'identification est jointe au groupe existant. Le mot de passe de la nouvelle information d'identification est défini sur le mot de passe partagé par les membres existants du groupe. S'il n'existe aucun membres existants dans le groupe, la valeur password est utilisée.
True	True	La nouvelle information d'identification est jointe au groupe existant. Le mot de passe inclus dans la commande est utilisé pour la nouvelle information d'identification et également attribuée à tous les autres membres existants du groupe.

L'identificateur global unique des informations d'identification retournées en tant que psoID dans la réponse est le même que celui qui sera répertorié dans l'opération lookupResponse et qui peut aussi être utilisé pour identifier cette information d'identification secondaire dans une opération modifyRequest ou deleteRequest.

Réinitialisation d'un utilisateur - resetRequest

Oct 21, 2015

Utilisez l'opération resetRequest pour réinitialiser l'état Single Sign-On des utilisateurs lorsqu'ils sont incapables d'accéder à leurs informations d'identification.

AuthToken

requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à cette requête.
executionMode	Single sign-on prend en charge le mode d'exécution synchrone.
authentication-token	L'élément authentication-token est obligatoire, mais n'est pas utilisé en ce moment.
psoID (obligatoire)	Le psoID est un identifiant unique pour chaque utilisateur final ; PSOID est le nom complet de l'utilisateur.

status (obligatoire)	Valeurs possibles : Success, Failure, Pending
requestID (obligatoire)	C'est un identificateur généré par le client qui associe les valeurs de retour à la requête associée.

Éléments namespace

Oct 21, 2015

Tous les éléments personnalisés Single Sign-on utilisés dans les commandes SPML sont membres du namespace http://citrix.com/Provision. Ce namespace est également appelé ctxs prefix. Il existe trois éléments de niveau supérieur dans ce namespace qui se produisent dans les commandes SPML : authentication-token, application et credential.

Élément de jeton d'authentification : ctxs:authentication-token

L'élément authentication-token est utilisé en tant que conteneur pour le jeton d'authentification (AuthToken). Cet élément est obligatoire, mais n'est pas utilisé. Il n'existe aucun élément enfant de l'élément authentication-token.

Syntaxe

```
AuthToken
```

Élément de l'application : ctxs:application

L'élément application peut se produire en tant qu'élément de niveau supérieur ou en tant qu'enfant de l'élément d'informations d'identification.

L'élément application est à la fois utilisé pour décrire une définition d'application (consultez lookupApplicationRequest) et pour décrire les détails d'une information d'identification (consultez addRequest).

Syntaxe

```
app-GUID Outlook description from app-def  Domain
```

Remarque : aucun des enfants de l'élément fields ne contient de données de caractères dans cet exemple.

Paramètres

ctxsID (obligatoire)	Le GUID attribué à la définition d'application lorsqu'il est créé dans la console
name	Le nom défini par l'administrateur pour la définition d'application
description	La description définie par l'administrateur pour la définition d'application
group (obligatoire si le partage de mot de passe est utilisé)	Le groupe d'application auquel cette définition est attribuée dans la console. L'attribut de partage de mot de passe est une valeur booléenne utilisée pour indiquer si ce groupe a été configuré pour partager des mots de passe. Pour plus d'informations, veuillez consulter addRequest.
fields (obligatoire)	Répertorie les champs de données devant être configurés pour les informations d'identification utilisant cette définition d'application. Tout sous-ensemble de champs répertoriés peut être défini pour toute définition d'application particulière. Enfant de l'élément des champs : • userID correspond à l'ID utilisateur • password correspond au mot de passe de l'utilisateur • custom-field correspond aux champs personnalisés qui peuvent être inclus dans une définition ;

	l'attribut d'index indique le champ particulier (soit '1' soit '2') et l'attribut d'étiquette contient le texte d'étiquette facultatif.

Consultez ctxs:credential pour un exemple de l'élément application en tant qu'enfant d'un élément credential.

Élément credential : ctxs:credential

L'élément credential est utilisé pour décrire une seule information d'identification secondaire unique. La plupart des informations d'identification sont associées à une définition d'application particulière ; elles sont exprimées par un élément d'application enfant. Les informations d'identification que les utilisateurs entrent manuellement ne contiennent aucun élément d'application.

Syntaxe

```
Credential Name user visible description  optional-RA provided-description   appdefGuid  johnd pass123 mydomain
```

Paramètres

status (obligatoire)	L'attribut status de l'élément credential indique l'état de cette information d'identification du point de vue du Single Sign-on Plug-in. L'état est soit actif soit en file d'attente. Une valeur active signifie que l'information d'identification est actuellement disponible pour utilisation par the Single Sign-on Plug-in. Une valeur de en file d'attente signifie qu'une commande destinée à ajouter l'information d'identification a été mise en file d'attente mais Single Sign-on Plug-in n'a pas encore traité cette commande.
pendingAction	L'attribut pendingAction de l'élément credential indique que n'importe quelle commande affecte cette information d'identification. Les valeurs de pendingAction sont add, modify et delete. Une valeur de delete indique qu'une commande delete a été mise en file d'attente pour cette information d'identification. Une valeur de delete indique qu'une commande delete a été mise en file d'attente pour cette information d'identification. Cet attribut est facultatif et est omis si aucune commande n'est mise en file d'attente pour l'information d'identification.
name	Cet attribut de nom de l'élément d'informations d'identification est la valeur affichée par Single Sign-On Plug-in dans la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification). Cette valeur peut être modifiée par l'utilisateur à l'aide de la page de propriétés de l'information d'identification.
description	La valeur de description de l'élément d'informations d'identification est la valeur affichée par Single Sign-On Plug-in dans la fenêtre Gérer les mots de passe (anciennement appelée Gestionnaire d'informations d'identification). Cette valeur peut être modifiée par l'utilisateur à l'aide de la page de propriétés de l'information d'identification.
provision-description	provision-description sont des données administratives qui ne peuvent pas être affichées ou modifiées par Single Sign-on Plug-in. Ceci est uniquement fourni pour le bénéfice de l'administrateur de provisioning.
application	L'élément application indique que l'ID de la définition d'application et les données de caractère des éléments userID, password et custom-field fournit les détails de l'utilisateur pour cette information d'identification.