IBM Security Access Manager for Enterprise Single Sign-On
Version 8.2

Guide des widgets AccessProfile

SC11-7261-00

IBM Security Access Manager for Enterprise Single Sign-On
Version 8.2

Guide des widgets AccessProfile

SC11-7261-00

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 19.

Remarque

Certaines illustrations de ce manuel ne sont pas disponibles en français à la date d'édition.

Première édition - novembre 2012

Réf. US : SC27-4444-00

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Sommaire

Figures

Tableaux

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

A propos de cette publication

IBM Security Access Manager for Enterprise Single Sign-On - Guide des widgets AccessProfile fournit des informations sur la procédure à suivre pour créer et utiliser des widgets.

Accès aux publications et à la terminologie

Cette section contient :

- Une liste des publications dans «Bibliothèque IBM Security Access Manager for Enterprise Single Sign-On».
- Des liens vers «Des publications en ligne», à la page xiii.
- Un lien vers «Site Web de terminologie IBM», à la page xiii.

Bibliothèque IBM® Security Access Manager for Enterprise Single Sign-On

Les documents suivants sont disponibles dans la bibliothèque IBM Security Access Manager for Enterprise Single Sign-On :

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide de démarrage rapide*, CF38DML

  Ce guide décrit le démarrage rapide des principales tâches d'installation et de configuration pour le déploiement et l'utilisation d'IBM Security Access Manager for Enterprise Single Sign-On.
- *IBM Security Access Manager for Enterprise Single Sign-On - Guide de planification et de déploiement*, SC11-6553-02

  Lisez ce guide avant d'effectuer toute tâche d'installation ou de configuration. Il vous aide à planifier le déploiement et à préparer votre environnement. Il contient une présentation des fonctions et des composants du produit, de l'installation et de la configuration requises ainsi que les différents scénarios de déploiement. Il décrit également comment utiliser la haute disponibilité et la reprise après incident.
- *IBM Security Access Manager for Enterprise Single Sign-On - Guide d'installation*, GI11-7376-01

  Lisez ce guide pour connaître les procédures détaillées d'installation, de mise à niveau ou de désinstallation d'IBM Security Access Manager for Enterprise Single Sign-On.

  Ce guide vous aide à installer les différents composants du produit et leurs middleware obligatoires ; il contient également les configurations initiales requises pour effectuer le déploiement du produit. Il traite des procédures d'utilisation des dispositifs virtuels, des éditions de WebSphere Application Server Base et Network Deployement.
- *IBM Security Access Manager for Enterprise Single Sign-On - Guide de configuration*, GC11-6701-01

  Lisez ce guide si vous souhaitez configurer les paramètres d'IMS Server et l'interface utilisateur d'AccessAgent ainsi que son comportement.
- *IBM Security Access Manager for Enterprise Single Sign-On - Guide d'administration*, SC11-6552-02

Ce guide est destiné aux administrateurs. Il traite des différentes tâches d'administration. Il fournit des procédures pour créer et attribuer des modèles de règle, éditer des valeurs de règle, générer des journaux et des rapports et sauvegarder IMS Server et sa base de données. Utilisez ce guide en association avec IBM Security Access Manager for Enterprise Single Sign-On - Guide de définition des règles.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide du service d'assistance*, SC11-6554-02

  Ce guide est destiné aux représentants du service d'assistance. Il aide les représentants du service d'assistance à gérer des interrogations et des requêtes provenant d'utilisateurs généralement sur leurs facteurs d'authentification. Utilisez ce guide en association avec IBM Security Access Manager for Enterprise Single Sign-On - Guide de définition des règles.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide de définition des règles*, SC11-6703-01

  Ce guide contient des descriptions détaillées des différentes règles utilisateur, machine et système que les administrateurs peuvent configurer dans AccessAdmin. Utilisez-le en association avec IBM Security Access Manager for Enterprise Single Sign-On - Guide d'administration.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide de résolution des problèmes et de support*, GC11-6702-01

  Ce guide vous permet de résoudre les problèmes liés à l'installation, la mise à niveau et l'utilisation du produit. Il traite des problèmes connus et des limitations du produit. Il vous aide à déterminer les symptômes et la solution de contournement d'un problème. Vous y trouverez également des informations sur les correctifs, les bases de connaissances et le support technique.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide AccessStudio*, SC11-6557-02

  Ce guide explique comment créer et éditer des profils. Il fournit des procédures pour la création et l'édition de profils d'accès standard et avancés pour différents types d'application. Il contient également des informations sur la gestion des services d'authentification et des objets application ainsi que des informations sur d'autres fonctions et dispositifs d'AccessStudio.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide des widgets AccessProfile*, SC27444400

  Lisez ce guide si vous souhaitez créer et utiliser des widgets.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide d'intégration de l'application des accès*, SC11-6558-02

  Consultez ce guide pour des informations sur les différentes API Java et SOAP d'application des accès. Il couvre également les procédures d'installation et de configuration de l'agent Provisioning Agent.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide de l'API web de gestion des données d'identification*, SC11-7036-00

  Ce guide explique comment installer et configurer l'API Web pour la gestion des données d'identification.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide du SDK de mode AccessAgent léger sur Terminal Server*, SC11-7037-00

  Ce guide contient des informations détaillées sur le développement d'un connecteur de canal virtuel qui intègre AccessAgent à des applications Terminal Services.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide Serial ID SPI*, SC11-7035-00

IBM Security Access Manager for Enterprise Single Sign-On comporte une interface SPI (Service Provider Interface) pour les unités contenant des numéros de série, comme une carte RFID. Consultez ce guide pour savoir comment intégrer une unité avec des numéros de série et l'utiliser en tant que second facteur d'authentification avec AccessAgent.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide d'intégration de la gestion de contexte*, SC11-6555-02

  Ce guide explique comment installer et configurer la solution de gestion de contexte, Context Management.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide d'utilisation*, SC11-6551-02

  Ce guide est destiné aux utilisateurs finaux. Ce guide fournit des instructions pour l'utilisation d'AccessAgent et de Web Workplace.

- *IBM Security Access Manager for Enterprise Single Sign-On - Guide de référence des messages d'erreur*, GC11-7038-00

  Ce guide décrit tous les messages d'information, d'avertissement et d'erreur associés à IBM Security Access Manager for Enterprise Single Sign-On.

Des publications en ligne

IBM présente ses publications lors du lancement du produit et lorsque ces documents sont mis à jour aux emplacements suivants :

Centre de documentation IBM Security Access Manager for Enterprise Single Sign-On
Le site http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itamesso.doc/ic-homepage.html affiche la page d'accueil du centre de documentation pour ce produit.

Centre de documentation d'IBM Security
Le site http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp affiche une liste en ordre alphabétique ainsi que des informations générales sur toute la documentation du produit IBM Security.

IBM Publications Center
Le site http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss comporte des fonctions de recherche personnalisée pour vous permettre de trouver toutes les publications IBM dont vous avez besoin.

Site Web de terminologie IBM

Le site Web de terminologie IBM regroupe la terminologie des bibliothèques de logiciels en un seul emplacement. Le site de terminologie est accessible à l'adresse http://www.ibm.com/software/globalization/terminology.

Accessibilité

Les fonctions d'accessibilité permettent aux personnes souffrant d'un handicap physique (par exemple, une mobilité réduite ou une déficience visuelle) de pouvoir utiliser les logiciels. Ce produit permet d'utiliser des technologies d'assistance pour entendre et naviguer dans l'interface. Vous pouvez également vous servir du clavier au lieu de la souris pour utiliser toutes les fonctions de l'interface graphique.

Pour plus d'informations, consultez "Fonctions d'accessibilité" dans *IBM Security Access Manager for Enterprise Single Sign-On - Guide de planification et de déploiement*.

Formation technique

Pour des informations sur la formation technique, consultez le site Web IBM Education suivant : http://www.ibm.com/software/tivoli/education.

Informations relatives au support

Le support IBM vous offre une assistance dans la résolution de vos problèmes de codes, de routine, d'installation de courte durée et de vos questions liées à l'utilisation. Vous pouvez accéder directement au site de support logiciel IBM à l'adresse http://www.ibm.com/software/support/probsub.html.

IBM Security Access Manager for Enterprise Single Sign-On - Guide de résolution des problèmes et de support fournit des informations sur :

- Quelles informations collecter avant de contacter le support IBM.
- Les diverses méthodes pour contacter le supportIBM.
- Comment utiliser IBM Support Assistant.
- Instructions et ressources d'identification de problème pour isoler et résoudre le problème vous même.

Remarque : L'onglet **Community and Support** dans le centre de documentation peut fournir des ressources de support supplémentaires.

Chapitre 1. Présentation des widgets AccessProfile

Les widgets AccessProfile sont des profils d'accès comprenant des états pouvant être fixés, que vous pouvez utiliser pour créer un autre profil d'accès.

Avantages de l'utilisation des widgets AccessProfile

Création de profils d'accès à l'aide des widgets AccessProfile existants.

Le profil d'accès se compose d'éléments plus petits et plus focalisés d' états, de déclencheurs, et d'actions pouvant être ajoutés en tant que widgets dans d'autres profils d'accès.

Un Widget AccessProfile, tel un profil d'accès, se compose d'états, de déclencheurs et d'actions. Un Widget AccessProfile peut être appelé dans d'autresprofils d'accès.

Modulaire

Les widgets AccessProfile sont modulaires. Par exemple : Sur les clients grand système, les utilisateurs choisissent à partir d'une liste d'applications grand système disponibles. Actuellement, tous ces flux de travaux d'application doivent être incorporés dans un seul profil d'accès. Vous pouvez utiliser leswidgets AccessProfile pour diviser un seul profil d'accès en plusieurs widgets ; un pour chaque flux de travaux d'application.

Réutilisation

Vous pouvez transmettre des valeurs aux variables de paramètre des widgets AccessProfile , rendant les widgets AccessProfile plus applicable dans différents profils d'accès. Par exemple : Un widget qui obtient des données d'identification de différentes sources, tels le serveur Privileged Identity Manager, peut utiliser l'URL du serveur comme un paramètre.

Le même widget peut être imbriqué plusieurs fois dans un profil d'accès et dans des profils d'accès à quelques différences près, qui peuvent facilement être paramétrées.

D'autre exemples sont des flux de travaux d'une interface utilisateur commune qui peuvent survenir dans différents types d'application. Le profil d'accès pour une interface utilisateur qui s'affiche dans diverses applications peut être utilisé comme un widget. Il peut également être utilisé dans les profils d'accès de ces applications individuelles. L'invite de connexion Par exemple : Windows qui s'affiche lorsque vous utilisez le protocole RDP ou Windows Explorer Map Network Drive.

Conditions préalables

Pour utiliser la fonction widgets AccessProfile , vous devez installer IBM Security Access Manager for Enterprise Single Sign-On version 8.2.

Installez les composants suivants de IBM Security Access Manager for Enterprise Single Sign-On version 8.2. Voir le document *IBM Security Access Manager for Enterprise Single Sign-On - Guide d'installation*.

- IMS Server `ims-8.2.0.0.686`
- AccessAgent `aa-8.2.0.3001`

- AccessStudio `as-8.2.0.0505`

Les utilisateurs existants deIBM Security Access Manager for Enterprise Single Sign-On peuvent installer les groupes de correctifs suivants pour la mise à niveau.

- `8.2.0-ISS-SAMESSO-IMS-FP0003`
- `8.2.0-ISS-SAMESSO-AA-FP0011`

Restrictions

Les widgets AccessProfile ont des restrictions.

- Vous ne pouvez pas appeler un Widget AccessProfile dans un autre widget.
- Un profil d'accès peut être un profil autonome et un widget en même temps. Cependant, si leprofil d'accès est un widget, les propriétés du profil d'accès définies dans l'onglet des Propriétés générales dans AccessStudio sont ignorées lorsqu'elles sont utilisées en tant que widget.

Chapitre 2. Création et utilisation des widgets AccessProfile

Création d'un Widget AccessProfile, édition de ses propriétés, l'ajouter à un profil d'accès, et l'épingler à un état.

Voir les rubriques suivantes :

Création des widgets AccessProfile

Un Widget AccessProfile est un profil d'accès dont un ou plusieurs de ses états est déclaré comme *pouvant être fixé*. Utilisez un Widget AccessProfile pour créer des profils d'accès. Vous pouvez ajouter le Widget AccessProfile à un autre profil d'accès par l'intermédiaire de ses *états pouvant être fixés*.

Procédure

1. Il ouvre AccessStudio.
2. Sélectionnez le profil d'accès dans le panneau de types de données.
3. Cliquez sur l'onglet **Etats**.
4. Sélectionnez un état du profil d'accès.
5. Sélectionnez **Propriétés** > **Editeur de formulaires**.
6. Définissez **Can be pinned in another profil d'accès** sur**Yes**.
7. Répétez les étapes 4 à6 pour chaque état que vous souhaitez réutiliser.

Résultats

Les états sélectionnés sont fixés. Le profil d'accès devient un Widget AccessProfile.

Que faire ensuite

Ajoutez le Widget AccessProfile à un autre profil d'accès. Voir «Ajout de widgets».

Ajout de widgets

Utilisez la fonction **Ajouter un Widget** pour ajouter le Widget AccessProfile et ses états pouvant être fixés à un autre profil d'accès.

Pourquoi et quand exécuter cette tâche

Lorsque vous ajoutez plusieurs instances d'un widget à partir d'un profil d'accès unique, chaque instance du widget est automatiquement libellé au format suivant : *Widget_InstanceName (AccessProfile_WidgetName)*.

Par exemple :

- `Nouveau Widget1 (Profil2)`
- `Nouveau Widget2 (Profil2)`

Le `Nouveau Widget1` est le nom d'instance du widget. Le `Profil2` est le nom du profil d'accès du widget.

Lorsque vous ajoutez le widget au profil d'accès, il n'est pas automatiquement ajouté comme faisant parti du profil d'accès. Vous devez fixer le widget dans le profil d'accès état sélectionné. Voir «Fixation à un état», à la page 5.

Vous ne pouvez pas ajouter widgets à un Widget AccessProfile.

Procédure

1. Il ouvre AccessStudio.
2. Sélectionnez le profil d'accès dans le panneau de types de données.
3. Cliquez sur l'onglet **Etats**.
4. Cliquez sur **Ajouter un widget**.
5. Sélectionnez le nom du Widget AccessProfile que vous souhaitez ajouter.

Résultats

Le widget est ajouté au diagramme d'état.

Que faire ensuite

Fixez le widget et son état pouvant être fixé dans le profil d'accès état sélectionné. Voir «Fixation à un état», à la page 5.

Vous pouvez également personnaliser le nom du Widget AccessProfile avant de fixer le widget. Voir «Edition de widgets».

Edition de widgets

Vous pouvez modifier le nom du profil d'accès du widget, le nom d'instance du widget ou le nom de état pouvant être fixé. Editez les noms pour éviter toute confusion si vous utilisez plusieurs widgets AccessProfile .

Pourquoi et quand exécuter cette tâche

L'édition du nom duprofil d'accès du widget ou du nom de état pouvant être fixé reproduit les modification apportées à toutes les instances du Widget AccessProfile.

L'édition du nom d'instance du widget applique la modification uniquement à l'instance que vous avez modifié. Le nom de chaque instance du widget ajouté est spécifique à ce Widget AccessProfile.

Voir le *IBM Security Access Manager for Enterprise Single Sign-On - Guide AccessStudio* pour les concepts généraux sur les profil d'accès et pour les flux de travauxAccessStudio standard.

Procédure

- Pour modifier le nom du Widget AccessProfile :
  1. Sélectionnez le Widget AccessProfile dans le panneau de types de données.

2. Cliquez sur l'onglet **Propriétés générales**.
3. Modifiez l'**ID du AccessProfile**. Par exemple : `Profil2`.

- Pour modifier le nom d'instance du widget :
  1. Sélectionnez le profil d'accès dans le panneau de types de données.
  2. Cliquez sur l'onglet **Etats**.
  3. Cliquez sur le nom du **Widget** dans le diagramme d'état. Par exemple : `Nouveau Widget1 (Profil2)`.
  4. Sélectionnez le panneau des **Propriétés**.
  5. Sous l'onglet **Editeur de formulaires**, modifiez le **Nom du widget**.
  6. Cliquez en dehors de l'onglet **Editeur de formulaires** pour appliquer les modifications.

Que faire ensuite

Fixez le widget et son état pouvant être fixé dans le profil d'accès état sélectionné. Voir «Fixation à un état».

Fixation à un état

Lorsque vous ajoutez un widget au profil d'accès, il n'est pas automatiquement ajouté comme faisant parti du profil d'accès. Vous devez fixer le widget et son état pouvant être fixé dans le profil d'accès état sélectionné. La fixation del'état pouvant être fixé appelle le widget.

Pourquoi et quand exécuter cette tâche

Vous pouvez sélectionner l'instance du Widget AccessProfile et l'état pouvant être fixé que vous souhaitez fixer au profil d'accès état sélectionné.

Vous pouvez fixer les états pouvant être fixés d'un widget à un profil d'accès état. Il n'y a pas de limite quant au nombre d'états pouvant être fixés que vous pouvez fixer à un profil d'accès état. Vous pouvez fixer un ou plusieurs de ces états pouvant être fixés au même état.

Si vous fixez un état pouvant être fixé à une instance d'un Widget AccessProfile au profil d'accès principal, cet état n'est plus disponible pour la fixation.

La fixation à un profil d'accès état fusionne l'automate du widget fixé avec celui de la machine profil d'accès état. Lorsque la machine état actuelle atteint l'état avec d'autres états fixés, tous les déclencheurs de tous les états sont évalués. L'ordre de l'évaluation des déclencheurs dépend de l'ordre dans lequel les états sont fixés.

Procédure

1. Il ouvre AccessStudio.
2. Sélectionnez le profil d'accès dans le panneau de types de données.
3. Cliquez sur l'onglet **Etats**.
4. Cliquez avec le bouton droit de la souris sur le nom de l'état où vous souhaitez fixer le widget.
5. Sélectionnez **Pin State**.
6. Sélectionnez l'instance du widget et l'état pouvant être fixé spécifique que vous souhaitez fixer auprofil d'accès état. Le Widget AccessProfile et les noms d'état

sont affichés au format suivant :
`Widget_InstanceName::AccessProfile_WidgetName::Pinnable_state`.

Libération d'un état

Libérez un état si vous souhaitez supprimer la connexion d'une instance de widget et ses état pouvant être fixé de l'état sélectionné.

Pourquoi et quand exécuter cette tâche

Dans le panneau des propriétés du Widget AccessProfile, si vous remplacez le paramètre de l'état pouvant être fixé par **Cannot be pinned in another profil d'accès**, cet état est automatiquement libéré du profil d'accès état sélectionné.

Procédure

1. Il ouvre AccessStudio.
2. Sélectionnez le profil d'accès dans le panneau de types de données.
3. Cliquez sur l'onglet **Etats**.
4. Cliquez avec le bouton droit de la souris sur le nom duwidget fixé.
5. Sélectionnez **Unpin State**.

Développer et réduire les widgets

Développez ou réduisez le Widget AccessProfile pour visualiser ou masquer les détails concernant leétat.

Lorsque vous ajoutez le widget au profil d'accès profil d'accès :

- Le widget est réduit par défaut.
- Les états pouvant être fixés associés au widget sont visibles, bien que le widget soit réduit.
- Les états qui ne sont pas définis en tant que pouvant être fixé sont réduits.

Cliquez sur le signe plus à côté du nom de l'instance du widget pour développer ou réduire son contenu.

Suppression de widgets

Utilisez le options **Supprimer** si vous avez ajouté le mauvais widget au profil d'accès et que vous devez remplacer ou supprimer le widget.

Vous pouvez supprimer le widget qu'il soit fixé ou non à un état dans le profil d'accès. Si vous supprimez un Widget AccessProfile avec un fixé états, tous les fixé états de ce widget sont libérés et supprimés du profil d'accès dans lequel ils sont ajoutés et fixé.

Vous ne pouvez pas supprimer unétat fixé d'un widget à partir d'un profil d'accès qui l'utilise. En général, vous ne pouvez pas modifier un widget à partir d'un profil d'accès qui l'utilise.

Utilisez une des options suivantes pour supprimer le widget du profil d'accès diagramme d'état :

- Cliquez sur widget et appuyez sur la touche **Supprimer**.

- Cliquez avec le bouton droit de la souris sur lewidget et sélectionnez **Supprimer** du menu.

Téléchargement des profils d'accès et des widgets

Pour activer et utiliser le profil d'accès, téléchargez le profil d'accès et les widgets associés sur le serveur IMS Server.

Pourquoi et quand exécuter cette tâche

Lorsque vous téléchargez sur le serveur IMS Server, tous les widgets qui sont fixés au profil d'accès sont également téléchargés.

Procédure

1. Sélectionnez le profil d'accès du panneau Type de données.
2. Cliquez sur l'icône **Upload selected data to IMS** dans la barre d'outils.

   Ou alors, cliquez avec le bouton droit de la souris sur le profil d'accès sélectionné et sur les widgets associés et sélectionnez **Upload to IMS**.

Chapitre 3. Transmission de valeurs aux paramètres

Lorsque vous créez un Widget AccessProfile, vous déclarez les paramètres à travers lesquels le profil d'accès principal peut transférer des données auWidget AccessProfile.

Vous devez déclarer les variables de paramètre dans le Widget AccessProfile. Puis, définissez les variables de paramètre équivalentes dans le profil d'accès pour chaque paramètre Widget AccessProfile.

Vous pouvez définir les types de paramètres suivants :

- Sac de données de compte
- Elément de magasin de propriété

Les valeurs transmises à ces paramètres sont fournies en tant que valeurs directes ou sont dérivées de diverses sources pendant l'exécution du profil d'accès.

Ces valeurs peuvent être transmises auWidget AccessProfile via une des options suivantes :

- Par référence
- Par valeur
- Par valeur directe

Voir les rubriques suivantes :

La transmission par option de référence

Utilisez l'option de transmission par référence si vous souhaitez que la variable de paramètre Widget AccessProfile utilise et modifie la même valeur qui est affectée à la variable de paramètre dans le profil d'accès principal.

Lorsque les valeurs sont transmises par référence :

- Si la valeur qui est affectée à la variable de paramètre dans le profil d'accès principal est modifiée, la nouvelle valeur est reflétée sur la variable de paramètre désignée qui est déclarée dans le Widget AccessProfile.
- Si la valeur de la variable de paramètre qui est déclarée dans le Widget AccessProfile est modifiée, la nouvelle valeur est reflétée sur la variable de paramètre d'origine dans le profil d'accès principal. La variable de paramètre du Widget AccessProfile est définie à partir de la variable de paramètre d'origine dans le profil d'accès principal.

L'option de transmission par valeur

Utilisez l'option de transmission par valeur si vous souhaitez que le Widget AccessProfile copie et utilise la valeur actuelle de la variable dans le profil d'accès principal.

Lorsque les valeurs sont transmises par valeur :

- Si la valeur qui est affectée à la variable de paramètre dans le profil d'accès principal est modifiée, la nouvelle valeur n'est pas reflétée sur la variable de paramètre désignée qui est déclarée dans le Widget AccessProfile.
- Si la valeur de la variable de paramètre qui est déclarée dans le Widget AccessProfile est modifiée, la nouvelle valeur n'est *pas* reflétée sur la variable de paramètre d'origine dans le profil d'accès principal.

L'option de valeur directe

Utilisez l'option de valeur directe si vous souhaitez que le profil d'accès principal transmette la valeur codée en dur à un paramètre dans le Widget AccessProfile.

Grâce à cette option, la valeur attribuée à la variable de paramètre ne change pas au moment de l'exécution.

Transmission de valeurs aux paramètres

Vous pouvez transmettre des valeurs aux paramètres qui sont déclarés dans le Widget AccessProfile par référence, par valeur ou en indiquant la valeur directe. Définissez cette option dans le profil d'accès principal.

Procédure

1. Créez Widget AccessProfile.
   a. Ajoutez des états. Voir le document *IBM Security Access Manager for Enterprise Single Sign-On - Guide AccessStudio*.
   b. Sélectionnez l'état que vous souhaitez fixer dans un autre profil d'accès.
   c. Déclarez les paramètres que vous souhaitez que le profil d'accès principal transmette à l'état fixé.
      1) Sélectionnez le type de paramètre.
      2) Indiquez l'ID du paramètre et le nom d'affichage.

      Remarque : Il n'existe aucune limite quant au nombre de paramètres que vous pouvez ajouter. Répétez l'étape c jusqu'à ce que vous complétez tous les paramètres que vous souhaitez ajouter.
   d. Ajoutez des déclencheurs et desactions. Voir le document *IBM Security Access Manager for Enterprise Single Sign-On - Guide AccessStudio*.
2. Dans le profil d'accès principal :
   a. Ajoutez le Widget AccessProfile. Voir «Ajout de widgets», à la page 3.
   b. Fixez l'état pouvant être fixé à un état. Voir «Fixation à un état», à la page 5.
   c. Sélectionnez l'instance de l'état fixé pour modifier ses propriétés. Par exemple : `Widget_InstanceName::Pinnable_state.`
   d. Sous **Propriétés** > **Editeur de formulaires**, développez les détails des propriétés du paramètre. Par exemple : `Parameter_name[Type:Account Data Bag]`.

e. Sélectionnez le type de paramètre et l'option de transmission des paramètres, puis cliquez sur l'icône **Ajouter**.

Pour la transmission des paramètres par référence

- Sac de données de compte (par référence)
- Elément de magasin de propriétés (par référence)

Pour la transmission des paramètres par valeur

- Sac de données de compte (par valeur)
- Elément de magasin de propriétés (par valeur)

Pour la transmission des paramètres par valeur directe

1) Sélectionnez **Valeur directe** et l'icône **Ajouter**.
2) Indiquez la **String to transfer over**.

f. Enregistrez le profil d'accès.

Exemple : Transmission de valeurs aux paramètres

Cette rubrique fournit un exemple d'un Widget AccessProfile et un profil d'accès principal. Elle comprend une description de la méthode de transmission des valeurs de paramètre.

Exemple d'un Widget AccessProfile :

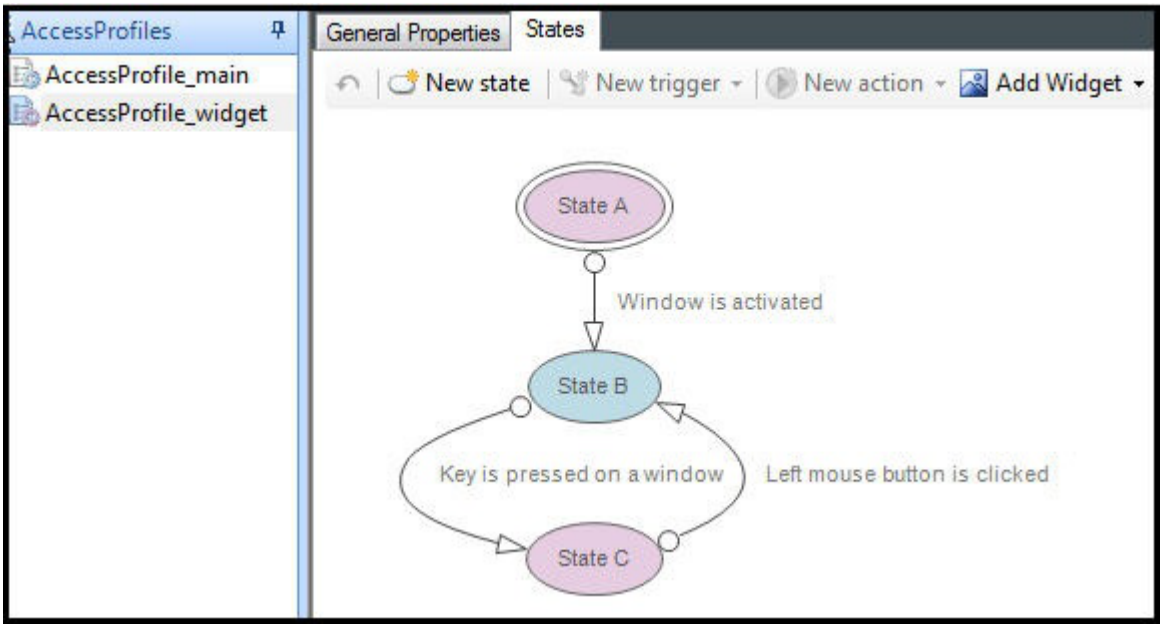

Figure 1. Exemple de widget AccessProfile

Ce Widget AccessProfile a les états suivants :

- L'*Etat A* est un état pouvant être fixé avec les types de paramètres et les variables de paramètres suivants :

Tableau 1. Détails des paramètres de l'Etat A

Variable de paramètre	Type de paramètre
param_adb1	Sac de données de compte
param_ps1	Elément de magasin de propriété

- L'*Etat B* ne peut être fixé.
- L*Etat C* est un état pouvant être fixé avec le type de paramètres et les variables de paramètres suivants :

Tableau 2. Détails des paramètres de l'Etat C

Variable de paramètre	Type de paramètre
param_ps2	Elément de magasin de propriété

Exemple d'un profil d'accès principal :

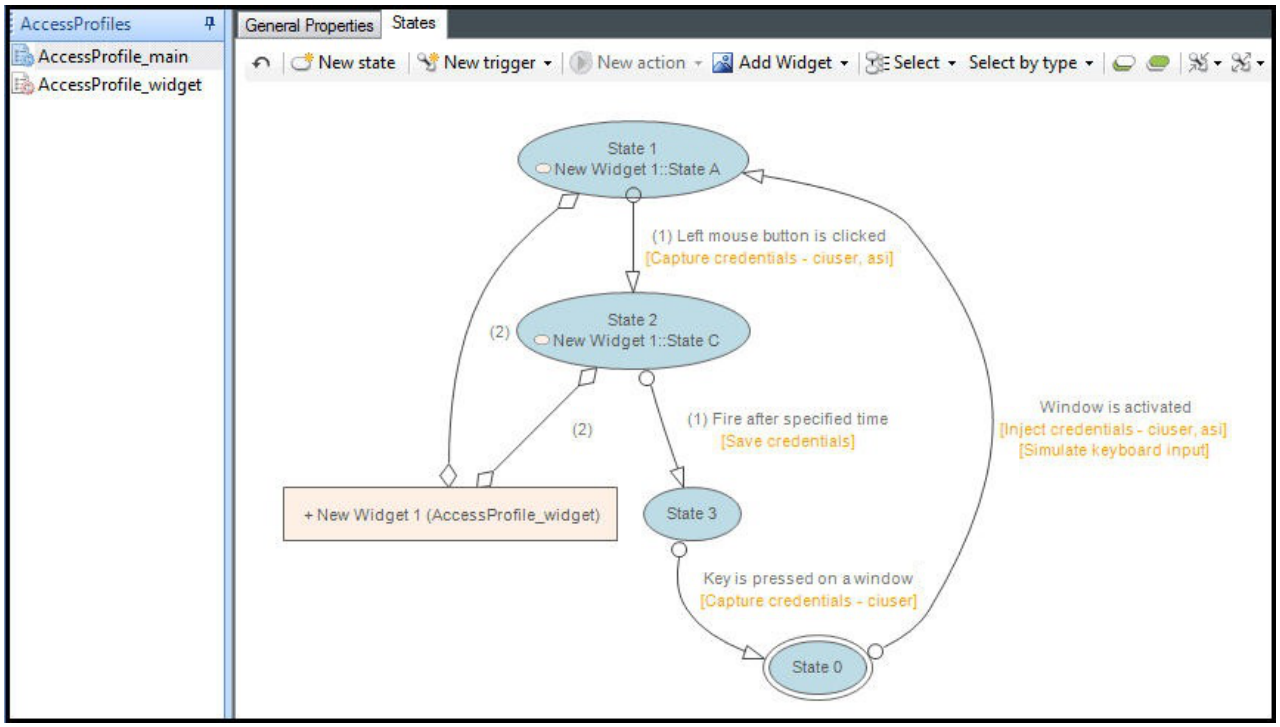

Figure 2. Exemple d'un profil d'accès principal qui démarre l'exemple de widget AccessProfile

Ce profil d'accès principal a les états suivants :

- *Etat 0*
- L'*Etat 1* possède les variables de paramètre et l'élément de transfert de données suivants :

Tableau 3. Détails des paramètres de l'Etat 1

Variable de paramètre	Elément de transfert de données
adb1	Sac de données de compte (par référence)
ps1	Elément de magasin de propriétés (par valeur)

- L'*Etat 2* possède les variables de paramètre et l'élément de transfert de données suivants :

Tableau 4. Détails des paramètres de l'Etat 2

Variable de paramètre	Elément de transfert de données
ps2	Elément de magasin de propriétés (par référence)

- *Etat 3*

Flux de travaux

Le tableau suivant décrit :

- La relation entre les états.
- Le flux de processus duprofil d'accès.
- Méthode de transmission des valeurs à partir des variables de paramètre du profil d'accès principal vers les variables de paramètre dans les états fixés du Widget AccessProfile.

Scénario	Sous-scénario	Résultat
• L'*Etat A* est fixé à l'*Etat 1* du *AccessProfile_main*. • L'*Etat 1* transmet les valeurs affectées à ses variables de paramètre aux variables de paramètre de l'*Etat A*. • L'*Etat C* est fixé à l'*Etat 2*. • L'*Etat 2* transmet les valeurs affectées à sa variable de paramètre à la variable de paramètre de l'*Etat C*.	*AccessProfile_main* passe de l'*Etat 0* à l'*Etat 1*.	• *param_adb1* est défini sur *adb1*. • *param_ps1* est défini sur *ps1*. • *param_ps2* demeure non initialisé dans une chaîne vide.
	AccessProfile_main passe de l'*Etat 1* à l'*Etat B* dans le *AccessProfile_widget*.	• *param_adb1* est toujours défini sur *adb1*. • *param_ps1* est toujours défini sur *ps1*. • *param_ps2* demeure non initialisé dans une chaîne vide. • Toute modification apportée à *param_adb1* est répercutée dans *adb1*, mais toute modification apportée à *param_ps1* n'est pas répercutée dans ps1.

Scénario	Sous-scénario	Résultat
	Le *AccessProfile_main* passe de l'*Etat B* à l'*Etat C* dans le *AccessProfile_widget*.	• *param_adb1* est toujours défini sur *adb1* et *param_ps1* est toujours défini sur ps1. • param_ps2 demeure non initialisé dans une chaîne vide. • Toute modification apporté à la valeur de *param_adb1* est copiée dans *adb1*. • Toute modification apportée à la valeur *param_ps1* n'est pas copiée dans *ps1*.
	AccessProfile_main passe de l'*Etat C* à l'*Etat 3*.	• La dernière valeur définie pour *param_adb1* est copiée dans *adb1* • La valeur de *ps2* reste inchangée.
	AccessProfile_main passe de l'*Etat 3* à l'*Etat 0*, puis à l'*Etat 1*.	• Les paramètres *param_adb1* et *param_ps1* sont réinitialisés avec les valeurs actuelles de *adb1* et *ps1*. • *param_ps2* demeure non initialisé dans une chaîne vide.
	AccessProfile_main passe de l'*Etat 1* à l'*Etat 2*.	• *param_adb1* demeure initialisé à la valeur récente de *adb1*. • *param_adb1* utilise toujours la valeur la plus récente de *adb1*. • Toute modification apportée à la valeur de *adb1* dans le profil est mise à la disposition de *param_adb1*. • *param_ps1* demeure initialisée sur la valeur de *ps1*. • Toute modification apportée à la valeur de *ps1* n'affecte pas la valeur de *param_ps1*. • *param_ps2* est initialisé avec la valeur la plus récente de *ps2*. • Toute modification apportée à la valeur de *param_ps2* dans le *AccessProfile_widget* est recopié dans *ps2*.

Scénario	Sous-scénario	Résultat
	AccessProfile_main passe de l'*Etat 2* à l'*Etat 3.*	• *param_adb1* demeure initialisé à la valeur la plus récente de *adb1*. • *param_ps1* demeure initialisée sur la dernière valeur définie de *ps1*. • *param_ps2* demeure initialisé à la valeur la plus récente de *ps2*.
• L'*Etat A* est fixé à l'*Etat 1* du *AccessProfile_main.* • L'*Etat 1* transmet les valeurs affectées à ses variables de paramètre aux variables de paramètre de l'*Etat A.* • L'*Etat C* du *AccessProfile_widget* reste en suspens.	*AccessProfile_main* passe à l'*Etat 1* de l'*Etat 0.*	• *param_adb1* est défini sur *adb1* et *param_ps1* est défini sur *ps1*. • *param_ps2* demeure non initialisé dans une chaîne vide.
	AccessProfile_main passe de l'*Etat 1* à l'*Etat B* dans le *AccessProfile_widget.*	• *param_adb1* est toujours défini sur *adb1* et *param_ps1* est toujours défini sur *ps1*. • *param_ps2* demeure non initialisé dans une chaîne vide. • Toute modification apportée à la valeur de *param_adb1* est copiée dans *adb1*, mais toute modification apportée à la valeur de *param_ps1* n'est pas copiée dans *ps1.*
	Le *AccessProfile_main* passe de l'*Etat B* à l'*Etat C* dans le *AccessProfile_widget.*	• *param_adb1* est toujours défini sur *adb1* et *param_ps1* est toujours défini sur *ps1*. • *param_ps2* demeure non initialisé dans une chaîne vide. • Toute modification apportée à la valeur de *param_adb1* est copiée dans *adb1*, mais toute modification apportée à la valeur de *param_ps1* n'est pas copiée dans *ps1.*

Annexe. Journaux d'exécution

Vérifiez les journaux d'exécution du profil d'accès principal ou le Widget AccessProfile associé en cas d'incident lors de l'utilisation du profil d'accès ou duwidget.

Vous pouvez visualiser les journaux d'exécution à partir du panneau AccessStudio **Messages**.

Exemple d'un journal d'exécution :

```
18:46:26.3437500   [State Machine Id - 0]
Action : Exécuter un VBScript ou JScript.
La ligne des propriétés est définie sur 'auth_ibm_intranet'.
```

Ce journal d'exécution inclut l'heure et l'action qui a été déclenchée.

Lorsque vous cliquez sur un nom état, un nom déclencheur ou un nom action dans le journal d'exécution, il affiche le profil d'accès qui contient le déclencheur et non le widget.

Les journaux d'exécution contiennent les informations suivantes :

- Lorsqu'un profil d'accès est chargé
- Lorsqu'un état est modifié
- Lorsqu'un déclencheur est mis en application
- Lorsqu'une action est exécutée
- Lorsqu'un widget est introuvable

Remarque : Les journaux d'exécution ne contiennent pas d'informations sur le changement d'état entre le *début* et la *fin* d'un état fixé.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Loi sur la propriété intellectuelle
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous serait pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 Etats-Unis

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le programme sous licence décrit dans le présent document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions du Livret Contractuel IBM, des Conditions internationales d'utilisation des Logiciels IBM ou de tout autre contrat équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les prix IBM affichés sont les prix de vente suggérés d'IBM et sont des prix actuels pouvant être changés sans avis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation IBM.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques déposées

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines aux Etats-Unis et/ou dans certains autres pays. Les autres noms de produits et de services peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web, "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript et toutes les marques incluant Adobe sont des marques ou des marques enregistrées d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

IT Infrastructure Library est une marque de The Central Computer and Telecommunications Agency qui fait désormais partie de The Office of Government Commerce.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

ITIL est une marque et une marque communautaire de The Office of Government Commerce et est enregistrée U.S. Patent and Trademark Office.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Cell Broadband Engine est une marque de Sony Computer Entertainment, Inc. aux Etats-Unis et/ou dans certains autres pays, utilisée sous licence.

Linear Tape-Open, LTO, le logo LTO, Ultrium et le logoUltrium sont des marques d'HP, IBM Corp. et Quantum aux Etats-Unis et dans d'autres pays.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Glossaire

Accès distant sécurisé (Secure Remote Access) : La solution qui permet une connexion unique basée sur le navigateur Web à toutes les applications de l'extérieure du pare-feu.

AccessAdmin : Console de gestion basée sur le Web, utilisée par les administrateurs et les représentants du service d'assistance pour l'administration d'IMS Server et la gestion des utilisateurs et des règles.

AccessAgent : Logiciel client qui gère l'identité de l'utilisateur et authentifie ce dernier, et automatise la connexion et la déconnexion uniques.

AccessAgent client : AccessAgent installé et en cours d'exécution sur la machine client.

AccessAgent serveur : AccessAgent déployé sur un serveur Microsoft Windows Terminal Server ou un serveur Citrix.

AccessAssistant : Interface basée sur le Web qui aide les utilisateurs à redéfinir leur mot de passe et à extraire leurs données d'identification d'application.

AccessProfile principal : Le AccessProfile qui contient un ou plusieurs widgets AccessProfile.

AccessStudio : Application utilisée par les administrateurs pour créer et gérer les profils d'accès.

Action : Dans le profilage, une opération qui peut être effectuée en réponse à un déclencheur. Par exemple, le remplissage automatique des informations relatives au nom d'utilisateur et au mot de passe dès qu'une fenêtre de connexion s'affiche.

ActiveCode : Codes d'authentification de courte durée, générés et contrôlés par IBM Security Access Manager for Enterprise Single Sign-On. Il existe deux types d'ActiveCode : Mobile ActiveCode et Predictive ActiveCode.

Les codes Mobile ActiveCode sont générés par IBM Security Access Manager for Enterprise Single Sign-On et diffusés sur le téléphone mobile ou le compte de messagerie électronique de l'utilisateur. Les codes Predictive ActiveCode, ou One Time Password, sont générés à partir de jetons OTP lorsqu'un utilisateur appuie sur le bouton correspondant.

Utilisé de concert avec d'autres unités ou d'autres canaux, les ActiveCodes permettent de réaliser une authentification effective à deux facteurs.

Active Directory (AD) : Service de répertoires hiérarchique qui permet une gestion centralisée et sécurisée de l'ensemble d'un réseau ; composant central de la plateforme Microsoft Windows.

Active RFID (ARFID) : ARFID est aussi bien un deuxième facteur d'authentification qu'un détecteur de présence. Il peut détecter la présence d'un utilisateur et AccessAgent peut être configuré pour exécuter des actions spécifiques. Dans les versions précédente, il s'appelle Active Proximity Badge.

Adaptateur Tivoli Identity Manager : Composant logiciel intermédiaire qui permet à IBM Security Access Manager for Enterprise Single Sign-On de communiquer avec Tivoli Identity Manager.

Administrateur : Personne chargée de tâches d'administration, par exemple la gestion de contenu ou des droits d'accès. Les administrateurs peuvent accorder différents niveaux de droits d'accès aux utilisateurs.

Adresse IP : Adresse unique d'un périphérique ou d'une unité logique sur un réseau qui utilise la norme IP (Internet Protocol).

Agent de noeud : Agent administratif gérant tous les serveurs d'application sur un noeud et représentant le noeud dans la cellule de gestion.

Annuaire : Fichier contenant les noms et les informations de contrôle des objets ou d'autres annuaires.

Annuaire d'entreprise : Annuaire de comptes utilisateur qui définissent les utilisateurs d'IBM Security Access Manager for Enterprise Single Sign-On. Il valide les données d'identification fournies par l'utilisateur au moment de la connexion si le mot de passe indiqué est identique à celui qu'il contient. Par exemple, Active Directory est un annuaire d'entreprise.

Annulation des accès de l'utilisateur : Suppression du compte utilisateur dans IBM Security Access Manager for Enterprise Single Sign-On.

Annuler les autorisations d'accès : Supprimer un service ou un composant. Par exemple, annuler l'accès sur un compte signifie supprimer ce compte d'une ressource.

API d'application d'accès : Interface qui permet à IBM Security Access Manager for Enterprise Single Sign-On d'effectuer l'intégration avec des systèmes d'application des accès côté utilisateur.

Application : Un ou plusieurs programmes d'ordinateur ou composants de logiciel qui fournissent une fonction de prise en charge directe de processus métier spécifiques. Dans AccessStudio, il s'agit du système qui fournit l'interface utilisateur pour la lecture ou la saisie des données d'authentification.

Application des accès des utilisateurs : Le processus d'enregistrement d'un utilisateur pour utiliser IBM Security Access Manager for Enterprise Single Sign-On.

Application PC : Application qui s'exécute sur un bureau électronique.

Application publiée : Application installée sur le serveur Citrix XenApp, accessible à partir de clients Citrix ICA.

Applications personnelles : Applications Windows et Web sur lesquelles AccessAgent peut stocker et entrer des données d'identification.

Des exemples d'applications personnelles sont les sites de courrier électronique basés sur le Web, tels les sites de courrier électronique des sociétés, les sites de banque électronique, les sites de magasinage en ligne, les programmes de messagerie instantanée et de discussion.

Assistant de configuration IMS : Les administrateurs utilisent l'assistant pour configurer IMS Server pendant l'installation.

Audit : Processus de journalisation des activités de l'utilisateur, de l'administrateur et du service d'assistance.

Authentification à deux facteurs : L'utilisation de deux facteurs pour authentifier un utilisateur. Par exemple, utilisation d'un mot de passe et d'une carte RFID pour se connecter à AccessAgent.

Authentication à partir d'un portable : Facteur d'authentification permettant à des utilisateurs de téléphone portable de se connecter en toute sécurité à leurs ressources d'entreprise à partir de n'importe quel endroit du réseau.

Authentification forte : Solution qui utilise des périphériques d'authentification multi-facteur afin d'empêcher un accès non autorisé aux données confidentielles et aux réseaux informatiques de l'entreprise, de son périmètre ou de l'extérieur.

autorité de certification (CA) : Organisation ou société de confiance qui émet des certificats numériques. L'autorité de certification vérifie généralement l'identité des personnes auxquelles le certificat unique est accordé.

Autorité de certification racine (CA) : Autorité de certification au sommet de la hiérarchie des autorités, qui vérifie l'identité du détenteur d'un certificat.

autorité de certification racine IMS : Autorité de certification racine qui signe les certificats pour la sécurisation du trafic entre AccessAgent et IMS Server.

Base de données IMS : Base de données relationnelle où IMS Server stocke toutes les données relatives au système ESSO, au poste de travail et aux utilisateurs ainsi que les journaux d'audit.

Biométriques : Identification d'un utilisateur en fonction de ses caractéristiques physiques (par exemple, empreinte digitale, couleur des yeux, visage, voix ou écriture).

Bureau partagé : Configuration bureau où plusieurs utilisateurs partagent un bureau Windows générique.

Bureau personnel : Le bureau n'est pas partagé avec d'autres utilisateurs.

Bureau privé : Sous ce schéma de bureau, les utilisateurs ont leurs propres bureaux Windows sur un poste de travail. Lorsqu'un utilisateur précédent revient au poste de travail et le déverrouille, AccessAgent passe à la session bureau de l'utilisateur précédent et reprend la dernière tâche.

Bureau publié : Fonction Citrix XenApp où les utilisateurs disposent d'un accès distant à un bureau Windows complet à partir de n'importe quel appareil, de n'importe où et à tout moment.

Capture automatique : Processus permettant à un système de collecter et de réutiliser des données d'identification de l'utilisateur pour différentes applications. Ces données d'identification sont capturées lorsque l'utilisateur saisit des informations pour la première fois, et sont ensuite enregistrées et sécurisées pour une utilisation ultérieure.

Carte à puce : Jeton intelligent intégré dans la puce d'un circuit intégré et qui fournit une capacité de mémoire et des fonctions informatiques.

Carte à puce hybride : Carte à puce conforme à la norme ISO-7816 qui contient une puce à chiffrement à clé publique et une puce RFID. La puce cryptographique est accessible via l'interface de contact. La puce RFID est accessible via l'interface sans contact (RF).

CCOW (Clinical Context Object Workgroup) : Norme indépendante du fournisseur, relative à l'échange d'informations entre applications médicales dans l'industrie médicale.

certificat IMS Server : Utilisé dans IBM Security Access Manager for Enterprise Single Sign-On. Le certificat IMS Server permet aux clients d'identifier et d'authentifier un serveur IMS.

Chaîne de service d'accréditation : Chaîne de modules opérant sous différents modes. Par exemple :

Chaîne de service d'accréditation de sécurité : Groupe d'instances de module configurées pour être utilisées simultanément. Chaque instance de module dans la

chaîne est appelée à tour de rôle pour effectuer une fonction spécifique, dans le cadre du processus général d'une requête.

Changement rapide d'utilisateur : Fonction permettant aux utilisateurs de passer d'un compte utilisateur à un autre sur un poste de travail unique sans quitter ni fermer les applications.

changement rapide d'utilisateur natif Windows : Fonction Windows XP qui permet aux utilisateurs de permuter rapidement d'un compte utilisateur à un autre.

Classification : Dans WebSphere Application Server, la mise en cluster consiste à regrouper des serveurs d'applications.

Clé privée : En sécurité informatique, partie secrète d'une paire de clés cryptographiques utilisées avec un algorithme de clé publique. La clé privée est uniquement connue de son propriétaire. Des clés privées sont généralement utilisées pour les données associées à une signature numérique et pour déchiffrer des données chiffrées à l'aide de la clé publique correspondante.

Client léger : Machine client contenant peu ou pas de logiciel. Elle a accès à des applications et des sessions de bureau qui s'exécutent sur des serveurs de réseau auxquels elle est connectée. Une machine client léger est une alternative à un client complet comme un poste de travail.

Clusters : Ensemble de serveurs d'applications qui collaborent pour l'équilibrage de la charge de travail et le basculement.

Code d'autorisation : Code alphanumérique généré pour des fonctions administratives, telles que la réinitialisation du mot de passe ou la non prise en compte de l'authentification à deux facteurs avec AccessAgent, AccessAssistant, et Web Workplace.

Code d'événement : Code représentant un événement particulier qui est contrôlé et consigné dans les tableaux du journal d'audit.

connecteur de canal virtuel : Connecteur utilisé dans un environnement de services de terminal. Le connecteur de canal virtuel établit un canal de communication virtuel pour gérer les sessions distantes entre le composant AccessAgent Client et le composant AccessAgent Serveur.

connecteur IMS : Module reliant IMS à des systèmes externes afin de diffuser un code actif mobile sur une passerelle de messagerie.

Connexion automatique : Technologie utilisant les interfaces utilisateur des applications pour automatiser le processus de connexion pour les utilisateurs.

Connexion automatique : Fonction permettant aux utilisateurs de se connecter au système d'automatisation de connexion et à ce système de connecter l'utilisateur à toutes les autres applications.

Connexion unique (SSO) : Processus d'authentification par lequel un utilisateur peut accéder à plusieurs systèmes ou applications en saisissant un seul ID utilisateur et mot de passe.

console d'administration WebSphere : Application cliente d'administration graphique Java qui effectue des appels de méthode vers les bean ressource dans le serveur d'administration afin d'accéder ou de modifier une ressource au sein du domaine.

Couche Secure Sockets Layer (SSL) : Protocole de sécurité fournissant une confidentialité des communications. SSL permet aux applications client/serveur de communiquer en toute confidentialité, sans risque de contrefaçon et de falsification des messages.

DB2 : Famille de programmes IBM sous licence pour la gestion des bases de données relationnelles.

Déploiement autonome : Déploiement dans lequel IMS Server est déployé dans un profil WebSphere Application Server indépendant.

Déploiement de réseau : Egalement dénommé déploiement en cluster. Type de déploiement où IMS Server est déployé sur un cluster WebSphere Application Server.

Détecteur de présence : Périphérique fixé à l'ordinateur qui détecte lorsqu'une personne s'en éloigne. Cela évite de verrouiller manuellement l'ordinateur lors d'une absence de courte durée.

Dispositif virtuel : Image de machine virtuelle avec un objet applicatif spécifique qui est déployée sur des plateformes de virtualisation.

DLL (Dynamic link library) : Fichier contenant du code exécutable et des données liés à un programme en phase de chargement ou d'exécution, plutôt qu'en phase de liaison. Le code et les données d'une bibliothèque DLL peuvent être partagés simultanément par plusieurs applications.

Données de compte : Informations de connexion requises pour vérifier un service d'authentification. Il peut s'agir du nom d'utilisateur, du mot de passe et du service d'authentification pour lesquels les informations de connexion sont stockées.

Données de connexion : Informations requises pour permettre aux utilisateurs d'accéder en toute sécurité à n'importe quelle application. Parmi ces données, il peut s'agir de noms d'utilisateurs, de mots de passe, d'informations sur le domaine et de certificats.

Données d'identification : Informations acquises lors de l'authentification et décrivant un utilisateur, des associations de groupe ou d'autres attributs d'identité relatifs à la sécurité et qui sont utilisées pour exécuter des services tels que l'autorisation, l'audit ou la délégation. Par exemple, l'ID utilisateur et le mot de passe sont des données d'identification qui permettent l'accès au réseau et aux ressources du système.

données d'identification d'Active Directory : Nom d'utilisateur et mot de passe Active Directory.

Données d'identification de l'utilisateur : Informations acquises lors de l'authentification et décrivant un utilisateur, des associations de groupe ou d'autres attributs d'identité relatifs à la sécurité et qui sont utilisées pour exécuter des services tels que l'autorisation, l'audit ou la délégation. Par exemple, l'ID utilisateur et le mot de passe sont des données d'identification qui permettent l'accès au réseau et aux ressources du système.

données d'identification ESSO : Nom d'utilisateur et mot de passe ISAM ESSO

écran d'accueil Windows, mode interface graphique Windows : Ecran sur lequel les utilisateurs entrent leur nom d'utilisateur et leur mot de passe pour se connecter au bureau Windows.

Elément de données de compte : Données d'identification permettant à l'utilisateur d'ouvrir une session.

Emulateur de terminal : Programme permettant à un périphérique tel qu'un micro-ordinateur ou un ordinateur personnel d'entrer et de recevoir des données à partir d'un système informatique comme s'il s'agissait d'un type de terminal relié particulier.

Enterprise Single Sign-On (ESSO) : Mécanisme permettant aux utilisateurs de se connecter à toutes les applications déployées dans l'entreprise en saisissant un ID utilisateur et d'autres données d'identification, par exemple un mot de passe.

environnement d'exécution Java (JRE) : Sous-ensemble d'un kit de développeur Java qui contient les programmes et fichiers exécutables de base constituant la plateforme Java standard. L'environnement d'exécution Java (JRE) inclut la machine virtuelle Java (JVM), les classes de base et les fichiers auxiliaires.

Equilibrage de charge : Surveillance des serveurs d'applications et gestion de la charge de travail sur les serveurs. Si un serveur dépasse sa charge de travail, les requêtes sont transmises à un autre serveur qui dispose de davantage de capacité.

ESSO GINA : Précédemment appelé Encentuate GINA (EnGINA). IBM Security Access Manager for Enterprise Single Sign-On GINA comporte une interface utilisateur intégrée aux facteurs d'authentification, qui fournit des options de réinitialisation de mots de passe et de non-prise en compte des facteurs secondaires.

Etat fixé : Un état pouvant être fixé qui est relié à un état dans le AccessProfile principal.

Etat pouvant être fixé : Etat du widget AccessProfile déclaré comme pouvant être fixé à un autre AccessProfile.

Facteur d'authentification : Il s'agit des différentes unités, biométries ou secrets requis en tant que donnée d'identification afin de valider des identités numériques. Les facteurs d'authentification sont par exemple les mots de passe, la carte à puce, la carte RFID, les biométries et les jetons de mots de passe à usage unique.

Facteur d'authentification principal : Mot de passe de IBM Security Access Manager for Enterprise Single Sign-On ou données d'identification du serveur d'annuaire.

Fichier de clés : En sécurité, fichier ou carte cryptographique matérielle où sont stockées les clés privées et les identités, à des fins d'authentification et de chiffrement. Certains fichiers de clés peuvent également contenir des clés sécurisées ou publiques.

Fichier de clés certifiées : Dans le domaine de la sécurité, objet d'archivage (fichier ou carte cryptographique matérielle) où sont stockées ses clés publiques sous forme de certificats sécurisés, à des fins d'authentification lors de transactions Internet. Dans certaines applications, ces certificats sécurisés sont déplacés dans le fichier de clés de l'application pour être stockés avec les clés privées.

FIPS (Federal Information Processing Standard) : Norme élaborée par le National Institute of Standards and Technology lorsqu'il n'existe aucune norme nationale ou internationale compatibles avec les exigences du gouvernement des Etats-Unis.

Fonctions en libre-service : Fonctions de IBM Security Access Manager for Enterprise Single Sign-On que les utilisateurs peuvent utiliser pour effectuer des tâches basiques telles que réinitialiser les mots de passe et les secrets avec une assistance minimale du centre d'assistance ou de votre Administrateur.

Forte identité numérique : Grâce à ce type d'identité et d'authentification d'une personne en ligne, il est très difficile de se faire passer pour elle car son profil est sécurisé par des clés privées sauvegardées sur une carte à puce.

fournisseur de données d'identification ESSO : Précédemment appelé Encentuate Credential Provider (EnCredentialProvider), c'est-à-dire IBM Security Access Manager for Enterprise Single Sign-On GINA for Windows Vista et Windows 7.

fournisseur de réseau ESSO : Précédemment appelé Encentuate Network Provider (EnNetworkProvider). Module AccessAgent qui capture les données d'identification du serveur Active Directory et utilise ces données pour connecter automatiquement les utilisateurs à leur portefeuille.

fournisseur de service cryptographique (CSP) : Une fonction du système d'exploitation i5/OS qui fournit des API. Le fournisseur CSP (Cryptographic Service Provider) CCA permet à un utilisateur d'exécuter des fonctions sur le coprocesseur 4758.

Gestion de la durée de validité des mots de passe : Fonction de sécurité par laquelle le superutilisateur peut indiquer à quelle fréquence les utilisateurs doivent changer leur mot de passe.

Gestion de sessions : Gestion de session utilisateur sur des bureaux électroniques privés et partagés.

Gestionnaire de bureaux : Gère simultanément des bureaux utilisateur sur un seul poste de travail.

Gestionnaire de déploiement : Serveur qui gère et configure des opérations pour un groupe logique ou une cellule d'autres serveurs.

GINA (Graphical Identification and Authentication) : Bibliothèque de liaison dynamique qui comporte une interface utilisateur étroitement intégrée aux facteurs d'authentification, qui fournit des options de réinitialisation de mots de passe et de non-prise en compte des facteurs secondaires.

Groupe de correctifs : Ensemble de correctifs cumulatifs disponibles entre les groupes de mises à jour planifiées, les mises à jour de fabrication ou les éditions. Permet aux clients de passer à un niveau de maintenance spécifique.

Haute disponibilité : Capacité du service informatique à résister à toutes les indisponibilités et à continuer à traiter les données, conformément à un niveau de service prédéfini. Les indisponibilités couvertes incluent les événements planifiés, par exemple la maintenance et les sauvegardes et les événements non planifiés, comme les pannes logicielles et matérielles, les coupures d'électricité et les sinistres.

IBM HTTP Server : Serveur Web IBM fournit un serveur Web appelé IBM HTTP Server qui accepte les demandes des clients et les expédie au serveur d'applications.

Identificateur URI : Chaînes de caractères compacte permettant l'identification d'une ressource abstraite ou physique.

IMS Server : Système de gestion intégré pour ISAM ESSO qui permet de gérer de façon centralisée les accès sécurisés d'une entreprise. Il active la gestion centralisée des identités des utilisateurs, les profils d'accès (AccessProfiles), les règles d'authentification. En outre, il fournit une gestion des pertes, une gestion des certificats et des audits de l'entreprise.

Interface de la ligne de commande : Une interface sur laquelle la commande d'entrée est une chaîne de caractère de texte.

Interface de programme d'application (API) : Une interface qui permet l'écriture d'un programme d'application dans un langage évolué afin d'utiliser des données ou des fonctions spécifiques du système d'exploitation ou d'un autre programme.

Interface de programme d'application cryptographique (CAPI) de Microsoft. : Spécification d'interface émise par Microsoft pour les modules qui fournissent une fonctionnalité cryptographique et qui permettent d'accéder aux cartes à puce.

Interface de programme d'application cryptographique (CAPI). : Une interface de programme d'application qui offre des services permettant aux développeurs de sécuriser des applications à l'aide de la cryptographie. Il s'agit d'un ensemble de bibliothèques reliées de façon dynamique qui fournit une couche abstraction qui isole les programmeurs du code utilisé pour chiffrer les données.

Interface SPI (Service Provider Interface) : Interface via laquelle des fournisseurs peuvent intégrer des périphériques dotés de numéros de série à IBM Security Access Manager for Enterprise Single Sign-On et les utiliser comme second facteur dans AccessAgent.

Interface SPI (Service Provider Interface) pour ID série : Interface de programmes conçue pour l'intégration de AccessAgent à des dispositifs Serial ID tiers, utilisés pour l'authentification à deux facteurs.

Java Management Extensions (JMX) : Méthode de gestion de la technologie Java et via cette technologie. JMX est une extension ouverte universelle du langage de programmation Java pour la gestion, qui peut être déployée pour tous les secteurs d'activités, dès lors que de la gestion est nécessaire.

jeton OTP : Un petit périphérique matériel portable que le propriétaire transporte pour autoriser l'accès aux systèmes numériques et aux actifs matériel.

journaux d'audit ESSO : Fichier journal contenant un enregistrement des événements système et des réponses. Les journaux d'audit ESSO sont stockés dans la base de données IMS.

Langue bidirectionnelle : Une langue qui utilise un script, tel que l'arabe ou l'hébreu, dont le flux général de texte va horizontalement de droite à gauche, mais les nombres, l'anglais et les autres textes de langue de gauche à droite sont écrits de gauche à droite.

Lightweight Directory Access Protocol (LDAP) : Protocole ouvert qui utilise TCP/IP pour fournir un accès à des répertoires qui prennent en charge un modèle X.500. Un protocole LDAP permet de localiser des individus, des organisations et d'autres ressources dans un annuaire Internet ou intranet.

Logiciel intermédiaire de carte à puce : Logiciel jouant le rôle d'interface entre des applications de carte à puce et du matériel de carte à puce. Généralement, ce logiciel est constitué de bibliothèques qui mettent en oeuvre la norme PKCS#11 et des interfaces CAPI sur des cartes à puce.

machine virtuelle Java (JVM) : Implémentation logicielle d'un processeur qui exécute du code Java compilé (applets et applications).

Message système : Boîte de dialogue système généralement utilisée pour afficher des messages importants. Lorsqu'un message modal système est affiché, vous ne pouvez rien sélectionner à l'écran tant que le message n'est pas fermé.

Mise à disposition : Fournir, déployer et suivre un service, un composant, une application ou une ressource.

Mise en cache de portefeuille : Lors d'une connexion unique pour une application, AccessAgent extrait les données d'identification de connexion du portefeuille de données d'identification de l'utilisateur. Le portefeuille de données d'identification de l'utilisateur est téléchargé sur la machine de l'utilisateur et est stocké de manière sécurisée sur le serveur IMS Server. Les utilisateurs peuvent alors accéder à leur portefeuille y compris lorsqu'ils se connectent ultérieurement à IBM Security Access Manager for Enterprise Single Sign-On à partir d'une machine différente.

Mobile ActiveCode (MAC) : Mot de passe à utilisation unique utilisé pour l'authentification à deux facteurs dans Web Workplace, AccessAssistant et d'autres applications. Ce mot de passe à utilisation unique est généré de façon aléatoire et expédié à l'utilisateur via SMS ou par e-mail.

Mode graphique interactif : Série de panneaux demandant des informations pour effectuer l'installation.

Modèle de données de compte : Un modèle qui définit le format des données de compte à stocker pour les données d'identification capturées à l'aide d'un profil d'accès spécifique.

Modèle d'élément de données de compte : Un modèle qui définit les propriétés d'un élément de données de compte.

Modèle de règle : Formulaire de règles prédéfini qui aide les utilisateurs à définir une règle en fournissant les éléments de la règle qui ne peuvent être modifiés et ceux qui peuvent l'être.

Mode léger : Mode AccessAgent serveur. Le fonctionnement en mode léger réduit l'encombrement mémoire d'AccessAgent sur serveur Citrix/Terminal et améliore le temps de démarrage de la connexion unique.

Mode silencieux : Méthode d'installation ou de désinstallation d'un composant de produit de la ligne de commande sans affichage de l'interface graphique. En mode silencieux, vous devez indiquer directement les données requises par le programme d'installation ou le programme de désinstallation sur la ligne de commande ou dans fichier (appelé fichier d'options ou fichier de réponses).

Mot de passe aléatoire : Mot de passe généré de manière arbitraire et utilisé pour augmenter la sécurité de l'authentification entre les clients et les serveurs.

Mot de passe du portefeuille : Mot de passe qui sécurise l'accès au portefeuille.

mot de passe ESSO : Mot de passe qui sécurise les accès au portefeuille de l'utilisateur.

Noeud géré : Noeud fédéré sur un gestionnaire de déploiement, qui contient un agent de noeud et pouvant inclure des serveurs gérés.

Noeuds : Un groupe logique de serveurs gérés.

Nom de domaine complet (FQDN) : En communications Internet, nom d'un système hôte qui comprend tous les sous-noms du nom de domaine. rchland.vnet.ibm.com est un exemple de nom de domaine complètement qualifié.

Nom d'hôte : Nom donné à un ordinateur dans la suite Internet de protocoles. Le nom d'hôte peut être un nom de domaine complet tel que `ordinateur.ville.entreprise.com` ou il peut être un sous-nom spécifique comme `ordinateur`.

Nom distinctif : Nom unique identifiant une entrée de répertoire. Un nom distinctif est constitué de paires de valeurs d'attributs, séparées par des virgules. Par exemple, CN=nom de personne et C=pays ou région.

Nom distinctif de base : Nom indiquant le point de départ des recherches dans le serveur d'annuaire.

Nom distinctif de liaison : Nom indiquant les données d'identification que le serveur d'applications doit utiliser pour se connecter à un service d'annuaire. Le nom distinctif identifie de manière unique une entrée dans un répertoire. Voir aussi *Nom distinctif*.

Nom d'utilisateur de l'entreprise : Nom d'utilisateur d'un compte utilisateur dans l'annuaire de l'entreprise.

normes PKCS : Ensemble de protocoles de norme industrielle utilisé pour sécuriser les échanges d'informations sur Internet. Les applications Domino Certificate Authority et Server Certificate Administration peuvent accepter des certificats au format PKCS.

Numéro de série : Numéro unique intégré dans les clés de IBM Security Access Manager for Enterprise Single Sign-On. Il y a un numéro par clé et celui-ci ne peut pas être modifié.

Numéro de série de la carte (CSN) : Elément de donnée unique qui identifie une carte à puce hybride. Il n'est aucunement lié aux certificats installés sur la carte à puce.

Numéro personnel d'identification (PIN) : Dans le support de chiffrement, numéro unique affecté par une organisation à un individu et utilisé comme preuve de son identité. Les codes confidentiels sont généralement attribués par les organismes financiers à leurs clients.

Objet de règles de groupe (GPO) : Ensemble de paramètres de règles de groupe. Les objets de règles de groupe sont des documents créés par le composant logiciel enfichable de règles de groupe. Les objets de règles de groupe sont stockés au niveau du domaine et affectent les utilisateurs et les ordinateurs contenus dans des sites, domaines et unités organisationnelles.

OTP (One-Time Password) : Mot de passe à utilisation unique généré pour un événement d'authentification, parfois transmis entre le client et le serveur via un canal sécurisé.

Outil Tivoli Common Reporting : Composant de génération de rapports que vous pouvez utiliser pour créer, personnaliser et gérer les rapports.

passerelle IMS : Module imbriqué dans des applications et des systèmes tiers pour l'appel d'API IMS pour l'application des accès et différentes autres fonctions.

Plug-in AccessAgent : Script écrit en VBscript ou Javascript, imbriqué dans un profil d'accès pour effectuer une vérification personnalisée des conditions ou pour exécuter des actions personnalisées. Permet d'étendre les capacités d'un profil d'accès au-delà des déclencheurs et des actions imbriqués.

Politiques d'application : Ensemble de règles et d'attributs régissant l'accès aux applications.

Pont d'application des accès : Processus de distribution des données d'identification IMS Server automatique avec des systèmes d'application des accès tiers qui utilise des bibliothèques API avec une connexion SOAP.

Portable : Dans WebSphere Application Server, une cellule est une unité virtuelle composée d'un gestionnaire de déploiement et d'un ou plusieurs noeuds.

Portail : Point d'accès unique et sécurisé à différentes informations, applications et personnes, qui peut être personnalisé et adapté.

Portée : Fait référence à l'applicabilité d'une règle, au niveau du système, de l'utilisateur ou de la machine.

Portefeuille : Un magasin de données sécurisées contenant des données d'identification d'accès d'un utilisateur et les informations associées, incluant les ID utilisateur, les mots de passe, les certificats et les clés de chiffrement.

Poste de travail client, poste client, ordinateurs client : Ordinateurs où est installé AccessAgent.

Poste de travail partagé : Poste de travail partagé par des utilisateurs.

profil de WebSphere Application Server : Nom d'utilisateur et profil de l'administrateur WebSphere Application Server. Définit l'environnement d'exécution.

profils d'accès (AccessProfiles) : AccessAgent utilise ces spécifications XML pour identifier des écrans d'application sur lesquels il peut exécuter la connexion unique et l'automatisation.

Profils de gestionnaire de déploiement : Environnement d'exécution WebSphere Application Server qui gère des opérations pour un groupe logique ou une cellule d'autres serveurs.

Protocole SMTP (Simple Mail Transfer Protocol) : Protocole d'application Internet pour transférer du courrier entre les utilisateurs d'Internet.

Question secrète : Question à laquelle seul l'utilisateur connaît la réponse. Une question secrète est utilisée comme fonction de sécurité pour vérifier l'identité d'un utilisateur.

Radio Frequency Identification (RFID) : Une technologie d'identification et de capture de données automatique qui identifie les éléments uniques et qui transmet des données par ondes radio.

RADIUS (Remote Authentication Dial-In User Service) : Système d'authentification et de statistiques qui utilise les serveurs d'accès pour offrir une gestion centralisée de l'accès aux grands réseaux.

Recherche utilisateur : Un utilisateur authentifié dans l'annuaire de l'entreprise et qui recherche d'autres utilisateurs. IBM Security Access Manager for Enterprise Single Sign-On se sert de l'utilisateur de recherche pour extraire les attributs utilisateur du référentiel d'entreprise Active Directory ou LDAP.

Référence auth-info directe : En profilage, auth-info directe est une référence directe à un service d'authentification existant.

Référence auth-info indirecte : En profilage, auth-info indirecte est une référence indirecte à un service d'authentification existant.

Registre : Référentiel contenant des informations d'accès et de configuration pour les utilisateurs, les systèmes et les logiciels.

Règle de complexité du mot de passe : Règle indiquant la longueur minimale et maximale du mot de passe, le nombre minimal de caractères numériques et alphabétiques, et s'il faut autoriser un mélange de minuscules et de majuscules.

Releveur de coordonnées du serveur : Une releveur de coordonnées qui regroupe un ensemble connexe d'applications Web nécessitant une authentification par le même service d'authentification. Dans AccessStudio, les modules de localisation de serveur identifient le service d'authentification auquel un écran d'application est associé.

Remote Desktop Protocol (RDP) : Protocole facilitant l'affichage et la saisie à distance sur des connexions réseau pour des applications serveur basées sur Windows. RDP prend en charge différentes topologies de réseau et de multiples connexions.

Reprise après incident : Opération automatique qui permet de basculer vers un système redondant ou de secours en cas d'indisponibilité d'un logiciel, d'un matériel ou d'un réseau.

Reprise après incident : Processus de restauration d'une base de données, d'un système ou de règles après la défaillance partielle ou totale d'un site provoqué par un événement catastrophique tel qu'un tremblement de terre ou un incendie. Généralement, la reprise après incident nécessite une sauvegarde totale à un emplacement différent.

Reproduction : Processus de gestion d'un jeu défini de données sur plusieurs emplacements. La réplication implique de copier les modifications indiquées apportées dans un emplacement (source) à un autre emplacement (cible) et de synchroniser les données dans ces deux emplacements.

réseau privé virtuel (VPN) SSL (Secure Sockets Layer) : Sorte de réseau virtuel privé pouvant être utilisé avec un navigateur Web standard.

Révoquer : Retirer un privilège ou un droit à un ID autorisation.

Ruche de registre : Dans les systèmes Windows, structure des données stockées dans le registre.

Sac de données de compte : Structure de données contenant en mémoire des données d'identification d'utilisateur pendant que la connexion unique est effectuée sur une application.

Security Token Service (STS) : Service Web utilisé pour émettre et échanger des jetons de sécurité.

Serveur autonome : Serveur pleinement opérationnel, géré indépendamment de tous les autres serveurs et utilisant sa propre console d'administration.

serveur de base de données (BD) : Logiciel qui utilise un gestionnaire de base de données pour fournir des services de base de données à des logiciels ou des ordinateurs.

Serveur de noms de domaine : Programme serveur qui fournit la conversion nom-adresse en mappant des noms de domaine sur des adresses IP.

Serveur IMS réparti : Les serveurs IMS sont déployés dans plusieurs emplacements géographiques.

serveur Web : Logiciel capable de satisfaire (servir) des demandes HTTP.

Service d'annuaire : Annuaire contenant les noms, les informations de profil et les adresses des ordinateurs de chaque utilisateur et ressource du réseau. Gère les comptes des utilisateurs et les autorisations en réseau. Lorsqu'un nom d'utilisateur est envoyé, il renvoie les attributs de cette personne et cela peut inclure un numéro de téléphone ou une adresse électronique. Les services de répertoire utilisent des bases de données hautement spécialisées qui sont généralement de type hiérarchique en matière de conception et offrent des fonctions de recherche rapide.

Service d'authentification : Dans IBM Security Access Manager for Enterprise Single Sign-On, service vérifiant la validité d'un compte par rapport à son magasin utilisateur ou à un annuaire d'entreprise. Identifie le service d'authentification associé à un écran. Les données de compte enregistrées sous un servie d'authentification particulier sont extraites et automatiquement renseignées pour l'écran de connexion défini. Les données de compte capturées à partir de l'écran de connexion sont sauvegardées dans le service d'authentification.

Service Web : Application modulaire intégrée explicite pouvant être publiée, reconnue et appelée sur un réseau utilisant des protocoles réseau standard. En général, le XML est utilisé pour baliser les données, le SOAP pour transférer les données, le WSDL pour décrire les services disponibles et l'UDDI pour répertorier les services disponibles.

Signature : En profilage, des données d'identification unique pour n'importe quelle application, fenêtre ou zone.

S'inscrire : Pour demander une ressource.

Site de reprise après incident : Un emplacement secondaire pour l'environnement de production en cas d'incident.

SOAP (Simple Object Access Protocol) : Protocole simple basé sur XML, permettant d'échanger des informations dans un environnement décentralisé et réparti. SOAP peut être utilisé pour interroger et renvoyer des informations ainsi que pour appeler des services via Internet.

Source de données : Moyen par lequel une application accède à des données à partir d'une base de données.

source de données IMS : Objet de configuration de WebSphere Application Server qui définit l'emplacement et les paramètres permettant d'accéder à la base de données IMS.

synchronisation du mot de passe Active Directory : Fonction IBM Security Access Manager for Enterprise Single Sign-On qui synchronise le mot de passe ISAM ESSO avec le mot de passe Active Directory.

Système d'application d'accès : Système offrant un service de gestion du cycle de vie des identités pour les utilisateurs d'applications dans les entreprises et gérant leurs données d'identification.

Téléscripteur (unité TTY) : Pilote de périphérique générique pour un affichage de texte. Une unité TTY effectue généralement des entrées et des sorties caractère par caractère.

Touche de raccourci : Séquence de touches utilisée pour changer d'opérations entre différentes applications ou entre différentes fonctions d'une application.

Trigger : En profilage, un événement qui provoque des transitions entre les états dans un moteur d'états, tel le chargement d'une page Web ou l'apparition d'une fenêtre sur le bureau.

utilitaire de configuration IMS : Utilitaire d'IMS Server permettant aux administrateurs de gérer les paramètres de configuration de bas niveau pour IMS Server.

Verrouillage d'écran transparent : Fonction qui, lorsqu'activée, permet aux utilisateurs de verrouiller leurs écrans tout en voyant tout de même le contenu du bureau.

Virtual Member Manager (VMM) : Composant WebSphere Application Server qui fournit des applications dont la fonction sécurisée permet d'accéder à des données d'entité organisationnelle de base telles que les individus, les comptes de connexion et les rôles de sécurité.

Virtual Private Network (VPN) : Extension d'un intranet d'une société par le biais de l'infrastructure préfabriquée existante d'un réseau public ou privé. Un VPN garantit la sécurisation des données envoyées entre les deux noeuds finaux de sa connexion.

Visual Basic (VB) : Langage de programmation piloté par événement et environnement de développement intégré (IDE) de Microsoft.

Wallet Manager : Le composant de l'interface graphique IBM Security Access Manager for Enterprise Single Sign-On que les utilisateurs peuvent utiliser pour gérer les donnée d'identification des applications dans le portefeuille d'identités personnelles.

WebSphere Application Server : Logiciel qui s'exécute sur un serveur Web et qui peut déployer, intégrer, exécuter et gérer des applications e-business.

Web Workplace : Interface basée sur le Web à laquelle les utilisateurs peuvent se connecter à des applications Web d'entrepris en cliquant sur des liens sans saisir les mots de passe pour les applications individuelles. Cette interface peut être intégrée avec le portail ou le réseau privé virtuel SSL existant du client.

Widget de profil d'accès/widget : Un profil d'accès indépendant qui comprend des états pouvant être fixé, pouvant être utilisés pour créer un autre profil d'accès.

Windows Terminal Services : Composant Microsoft Windows permettant aux utilisateurs d'accéder à des applications et des données sur un ordinateur distant, via un réseau.

WS-Trust : Spécification de sécurité de services Web qui définit un cadre pour que les modèles de confiance établissent une relation de confiance entre les services Web.

Index

SC11-7261-00