

CA Identity Manager™

User Console Design Guide (Manuel de conception de la console d'utilisateur)

12.6.4



La présente Documentation, qui inclut des systèmes d'aide et du matériel distribués électroniquement (ci-après nommés "Documentation"), vous est uniquement fournie à titre informatif et peut être à tout moment modifiée ou retirée par CA. La présente Documentation est la propriété exclusive de CA et ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA.

Si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer ou mettre à disposition un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser ou de mettre à disposition des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

DANS LES LIMITES PERMISES PAR LA LOI APPLICABLE, CA FOURNIT LA PRÉSENTE DOCUMENTATION "TELLE QUELLE", SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT CONCERNANT LA QUALITÉ MARCHANDE, L'ADÉQUATION À UN USAGE PARTICULIER, OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ÊTRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RÉSULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES OU DE CLIENTS, ET CE MÊME DANS L'HYPOTHÈSE OÙ CA AURAIT ÉTÉ EXPRESSÉMENT INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

Le présent Système étant édité par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2014 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Produits CA Technologies référencés

Ce document fait référence aux produits CA Technologies suivants :

- CA CloudMinder™ Identity Management
- Annuaire de listes CA
- CA Identity Manager™
- CA Identity Governance (anciennement CA GovernanceMinder)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder™

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse <http://www.ca.com/worldwide>.

Table des matières

Chapitre 1: Personnalisation de la console d'utilisateur	11
Console d'utilisateur par défaut.....	11
Tâches, onglets et fenêtres.....	13
Personnalisation de la console d'utilisateur.....	14
Chapitre 2: Navigation tâche	15
Navigation basée sur les tâches.....	15
Navigation basée sur les objets.....	17
Configuration de la navigation basée sur les objets.....	18
Catégories de tâches.....	20
Désactivation de l'annulation automatique des tâches.....	21
Flux de tâche.....	21
Configuration d'onglets de tâche indépendants.....	23
Configuration d'une tâche comme assistant.....	24
Configuration d'une séquence d'onglets.....	25
Chapitre 3: Configuration des onglets et fenêtres de profil	27
Onglets et fenêtres Profil.....	27
Personnalisation des fenêtres de profil.....	28
Modification d'une fenêtre Profil.....	29
Ajout ou suppression de champs.....	31
Propriétés de champs dans une fenêtre Profil.....	32
Styles des champs.....	39
Options du sélecteur de dates.....	41
Options du sélecteur d'objet.....	43
Affichage des attributs structurés.....	46
Remplissage des options de champs.....	50
Sélection d'une méthode de remplissage de champ.....	51
Utilisation de listes simples pour les options de champs.....	53
Données des boîtes de sélection.....	54
Utilisation du script Java pour les options de champs.....	66
Utilisation des gestionnaires d'attributs logiques pour les options de champs.....	68
Renseignement dynamique du champ Organisation.....	69
Modification dynamique des propriétés d'affichage des champs.....	70
Configuration des propriétés d'affichage du champ dynamique.....	71
Attributs logiques définis par fenêtre.....	72

Ajout d'attributs logiques définis par fenêtre	73
Attributs logiques définis par fenêtre dans l'onglet Afficher les tâches soumises	74
Composants supplémentaires d'une fenêtre de profil	74
Options de l'attribut Séparateur	75
Ajout d'un attribut binaire ou d'une image à une fenêtre Profil	76
Ajout de sections de pages	79
Ajout d'une tâche imbriquée	81
Ajout de texte d'aide aux fenêtres de profils.....	83
Ajout d'un champ Editeur d'historique	84
Ajout d'un champ Affichage de l'historique.....	85
Configuration de la validation de niveau tâche.....	86
Attributs personnalisés définis par l'utilisateur pour les rôles.....	87
Configuration des attributs personnalisés de l'onglet Profil pour les rôles	88
Ajout d'attributs personnalisés aux définitions de fenêtres de recherche	89

Chapitre 4: Configuration des onglets de compte 91

Onglet Comptes.....	91
Conditions préalables à l'utilisation de l'onglet Comptes	92
Champs de l'onglet Comptes.....	92
Autres fonctionnalités de l'onglet Comptes.....	93

Chapitre 5: Fenêtres de recherche et de liste 95

Configuration d'une fenêtre de recherche.....	95
Modification d'une fenêtre de recherche.....	95
Filtres de recherche	97
Champs et résultats de recherche	100
Aide sur les fenêtres de recherche définie par l'utilisateur	103
Types de fenêtres de recherche.....	103
Fenêtres de liste	106
Ajout d'une liste de tâches.....	108
Tâches supplémentaires dans les fenêtres de recherche et de liste.....	111
Ajout de tâches supplémentaires dans les fenêtres de recherche et de liste	112

Chapitre 6: Tâches d'auto-administration 115

Tâches d'auto-administration de CA Identity Manager	115
Configuration de tâches d'auto-administration	116
Configuration de la tâche d'auto-enregistrement.....	117
Configuration d'une organisation par défaut pour les utilisateurs auto-enregistrés	118
Ajout de questions et réponses de vérification	118
Configuration des tâches Réinitialisation du mot de passe oublié et ID d'utilisateur oublié.....	120

Tâche Réinitialisation du mot de passe oublié.....	120
Tâche ID d'utilisateur oublié	120
Configuration des tâches Réinitialisation du mot de passe oublié et ID d'utilisateur oublié	121
Collecte de paires de question/réponse pour la vérification de l'utilisateur	121
Configuration de la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié	122
Conception de fenêtres d'identification	123
Conception de fenêtres de vérification.....	124
Sélectionnez la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié.....	127
Déterminer comment les utilisateurs réinitialisent leurs mots de passe	129
Déterminer comment les utilisateurs récupèrent un ID d'utilisateur oublié.....	130
Pages de déconnexion.....	130
Configuration des pages de déconnexion.....	131

Chapitre 7: Personnalisation de la console d'utilisateur **133**

Apparences.....	133
Composants d'une apparence.....	134
Apparences de CA Identity Manager	135
Associations d'apparence.....	138
Création d'une apparence.....	138
Copie d'une apparence existante.....	139
Mise à jour des images d'apparence.....	140
Mise à jour des couleurs et des polices d'apparence	140
Modification du fichier .properties	140
Modification du fichier index.jsp	141
Recompilation des fichiers .jsp et redémarrage du serveur d'applications	142
Utilisation de plusieurs apparences	142
Priorité des apparences	143
Création d'une réponse d'apparence.....	144
Modification des pages de console	145
Modification de l'en-tête dans la console d'utilisateur CA Identity Manager	146
Modification et affichage du pied de page	147

Chapitre 8: Aide personnalisée **149**

Fonctionnement de l'aide personnalisée	149
Format de l'aide personnalisée.....	150
Expressions d'aide personnalisées	150
Utilisation de l'aide pour déterminer le lien à utiliser.....	151
Personnalisation de l'Aide.....	152
Exemples d'utilisation de l'Aide personnalisée	152
Exemple de personnalisation de l'Aide	153
Exemple de création d'Aide au format Wiki	153

Exemple de localisation de l'Aide.....	154
Exemple d'internationalisation de l'Aide	154

Chapitre 9: Localisation de CA Identity Manager **157**

Introduction	157
Groupes de ressources.....	157
Exemples d'environnements CA Identity Manager localisés	160
Restrictions sur l'utilisation de jeux de caractères internationaux.....	161
Configuration de la prise en charge de la localisation	162
Conditions requises pour la localisation	163
Configuration de l'agent Web CA SiteMinder	165
Modification du fichier server.xml de JBoss	166
Configuration de la variable PATH	166
Utilisation des exemples d'environnements localisés	167
Création de fichiers de localisation personnalisés	169
Traduction des modèles de courriel.....	170
Localisation des apparences personnalisées	170
Modification de la tâche Modifier mon compte	170
Localisation de code personnalisé	171
Affichage de CA Identity Manager dans différentes langues	171
Activation du changement de langue	172
Définition de l'en-tête HTTP imlanguage dans une réponse CA SiteMinder.....	172

Chapitre 10: Règles de validation **175**

Introduction aux règles de validation	175
A propos des règles de validation	175
Types de règles de validation.....	176
Ensembles de règles de validation.....	177
Notions de base de la définition de règle de validation.....	178
Utilisation de règles de validation par défaut	179
Validations de données par défaut	179
Règles de validation prédéfinies	181
Implémentation des règles de validation personnalisées.....	182
Implémentation à l'aide d'une expression régulière	182
Implémentation à l'aide de JavaScript	182
Implémentation à l'aide de Java	185
Exceptions	188
Configuration des règles de validation.....	190
Configuration d'une validation de niveau tâche	190
Configuration d'une validation de niveau annuaire.....	191
Initialisation de la validation	196

Exemples d'implémentation	197
Annexe A: Liste des onglets par défaut	199
Annexe B: Compilation des fichiers JSP de CA Identity Manager	205

Chapitre 1: Personnalisation de la console d'utilisateur

Ce chapitre traite des sujets suivants :

[Console d'utilisateur par défaut](#) (page 11)

[Personnalisation de la console d'utilisateur](#) (page 14)

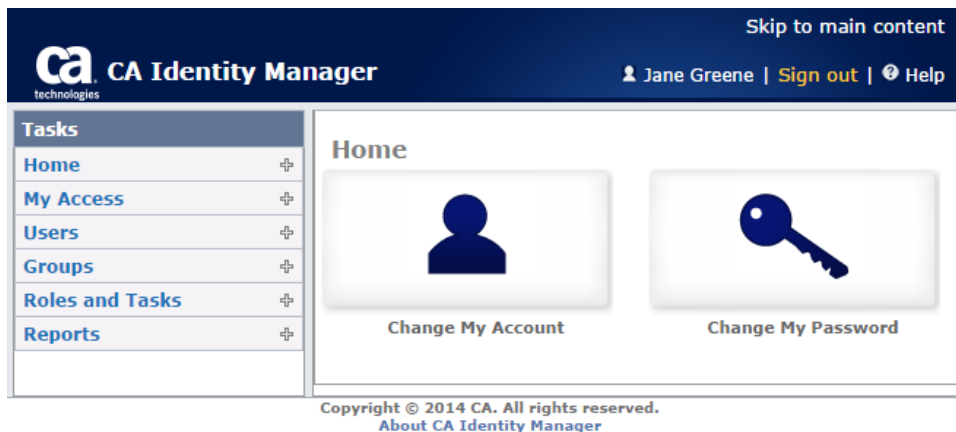
Console d'utilisateur par défaut

Lorsque vous créez un environnement, CA Identity Manager crée une console d'utilisateur par défaut que vous utilisez pour gérer l'environnement. La console d'utilisateur inclut un ensemble de tâches et de rôles par défaut.

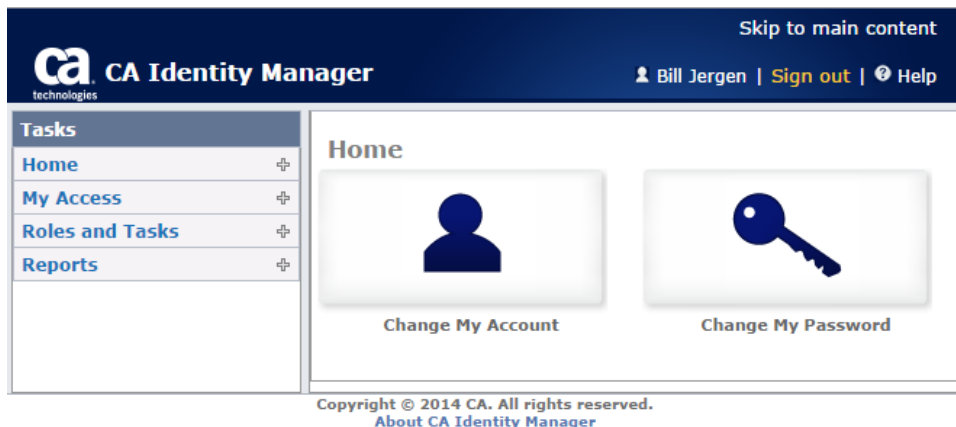
- Les tâches sont des actions exécutées par les utilisateurs CA Identity Manager. Il existe deux types de tâches.
 - Les tâches d'administration permettent de gérer les utilisateurs, les organisations, les groupes, les rôles et les tâches.
 - Les tâches externes exécutent des fonctions des applications métier, telles que le transfert des attributs d'utilisateur à une application de génération de rapports.
- Les rôles d'administration associent les utilisateurs et les droits à CA Identity Manager ou à d'autres applications. Les rôles sont composés de tâches. Un utilisateur ayant un rôle peut effectuer les tâches associées. Les utilisateurs peuvent posséder plusieurs rôles. Par exemple, un utilisateur peut disposer des rôles Comptable et Employé.

Les rôles d'administration sont composés de tâches d'administration.

Les tâches affichées lorsque vous ouvrez une session dans un environnement CA Identity Manager dépendent de vos rôles d'administration. Dans l'exemple suivant, l'utilisatrice Jane Green dispose du rôle Gestionnaire d'utilisateurs. Elle peut afficher les catégories des tâches d'administration disponibles pour les gestionnaires d'utilisateurs.



Dans cet exemple, Bill Jergen est associé au rôle Gestionnaire de rôles. Lorsqu'il se connecte à la console d'utilisateur, un ensemble de catégories différent s'affiche, comprenant les tâches qu'il peut utiliser.



Remarque : Pour plus d'informations sur les tâches et les rôles, reportez-vous au *manuel d'administration (en anglais)*.

Tâches, onglets et fenêtres

Une tâche d'administration est une fonction d'administration exécutée par les utilisateurs de CA Identity Manager. Elle est composée d'*onglets*, qui regroupent logiquement un ensemble de champs ou de fonctionnalités. Par exemple, la tâche Modifier l'utilisateur par défaut inclut les onglets suivants.

- Profil
- Rôles d'accès
- Rôles d'administration
- Rôles de provisionnement
- Groupes

Lorsque l'administrateur utilise cette tâche, il sélectionne l'onglet approprié pour entrer les informations de profil, gérer les rôles ou l'appartenance au groupe.

Un onglet peut être associé à plusieurs tâches.

L'exemple ci-après présente une tâche d'administration avec plusieurs onglets.

Modifier un utilisateur: liang

Profil	Rôles d'accès	Rôles d'administration	Rôles de provisionnement	Groupes
• = obligatoire				
Organisation	<input type="text" value="Dealer"/>			
ID de l'utilisateur	<input type="text" value="liang"/>			
Activé	<input checked="" type="checkbox"/>			
• Prénom	<input type="text" value="liang"/>			
• Nom	<input type="text" value="liang"/>			
• Nom complet	<input type="text" value="liang"/>			

Les onglets peuvent être associés à une *fenêtre* configurable qui détermine l'apparence et le contenu de l'onglet. Pour modifier un onglet par défaut, vous pouvez modifier la fenêtre associée ou créer une nouvelle fenêtre.

Une fenêtre peut être associée à plusieurs onglets.

Informations complémentaires :

[Liste des onglets par défaut](#) (page 199)

Personnalisation de la console d'utilisateur

Généralement, après avoir créé un environnement CA Identity Manager, un administrateur système effectue une première configuration pour s'assurer que l'environnement est conforme aux besoins métier. La personnalisation de la console d'utilisateur améliore son utilisation en créant les tâches qui correspondent aux flux de travaux de l'utilisateur, accroît la sécurité en s'assurant que les utilisateurs peuvent accéder uniquement aux champs dont ils ont besoin et améliore les performances.

Vous pouvez personnaliser les éléments suivants dans la console d'utilisateur.

- Navigation basée sur les tâches : détermine l'accès des administrateurs aux tâches et aux onglets associés.
- Onglets et fenêtres : contrôlent les champs qui apparaissent dans un onglet et leur affichage.

Les tâches d'administration de la console d'utilisateur par défaut sont créées selon les informations du fichier de configuration d'annuaire (directory.xml) qui définit les objets et les attributs que CA Identity Manager gère. Par exemple, l'onglet Profil de la tâche Créer un utilisateur par défaut inclut tous les attributs définis dans le fichier directory.xml pour l'objet d'utilisateur.

La plupart des utilisateurs doivent gérer uniquement un sous-ensemble d'attributs pour les objets.

- Tâches d'auto-administration : déterminent le fonctionnement des tâches d'auto-administration, telles que Mot de passe oublié ou ID d'utilisateur oublié.
- Marque : affiche les logos et les couleurs de l'entreprise dans la console d'utilisateur.
- Localisation : affiche la console d'utilisateur dans différentes langues.
- Aide en ligne personnalisée : offre une aide en ligne spécifique à une tâche ou à un onglet que vous personnalisez.

Chapitre 2: Navigation tâche

Ce chapitre traite des sujets suivants :

[Navigation basée sur les tâches](#) (page 15)

[Navigation basée sur les objets](#) (page 17)

[Catégories de tâches](#) (page 20)

[Flux de tâche](#) (page 21)

Navigation basée sur les tâches

Pour effectuer une action dans CA Identity Manager, sélectionnez une tâche et un objet sur lequel exécuter cette tâche. Par exemple, lorsque vous modifiez un profil d'utilisateur, la tâche est Modifier l'utilisateur et l'objet est le profil d'utilisateur que vous souhaitez modifier.

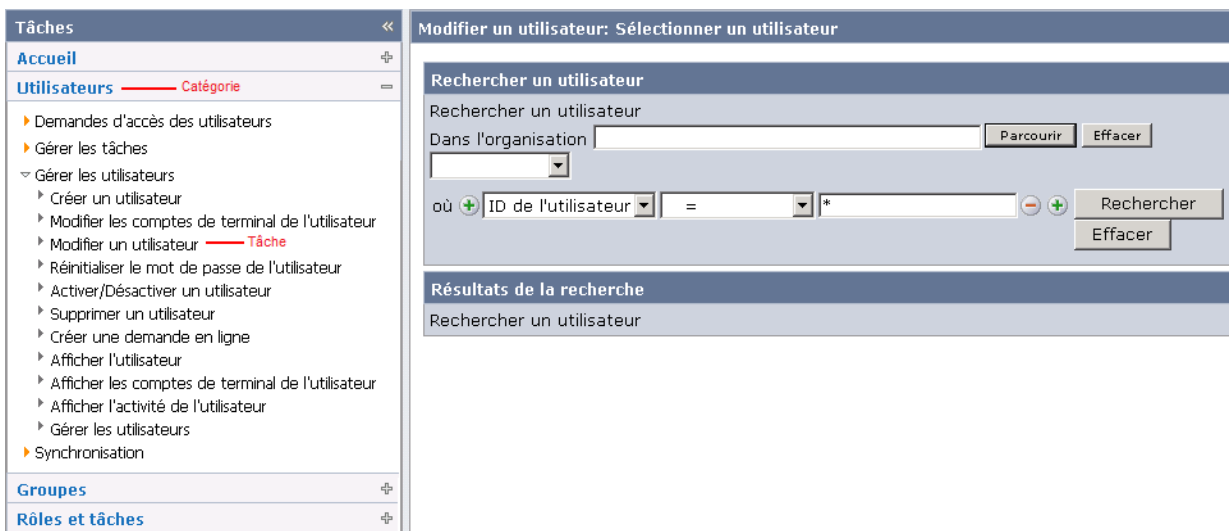
CA Identity Manager propose deux méthodes de sélection des tâches et des objets.

- Navigation basée sur les tâches
- Navigation basée sur les objets

Dans la navigation basée sur les objets, vous sélectionnez une catégorie et une tâche, puis recherchez l'objet auquel la tâche s'applique.

Par exemple, pour modifier un profil d'utilisateur, sélectionnez la catégorie Utilisateurs, puis la tâche Modifier l'utilisateur. Recherchez ensuite l'utilisateur à modifier.

L'exemple suivant présente les catégories et tâches dans la console d'utilisateur.



La navigation basée sur les tâches est la méthode de navigation par défaut. Utilisez la navigation basée sur les tâches lorsque les utilisateurs appliquent généralement une seule action à un objet.

Navigation basée sur les objets

La *navigation basée sur les objets* est une méthode qui permet à l'utilisateur de sélectionner un objet et d'afficher dans un menu déroulant toutes les tâches qu'il peut effectuer sur cet objet. Dans le menu, il peut sélectionner la tâche qu'il souhaite utiliser. Une fois la tâche terminée, il peut sélectionner une autre tâche dans le menu déroulant sans devoir rechercher à nouveau l'objet.

The screenshot illustrates the object-based navigation process. On the left, the navigation pane shows a tree structure where 'Utilisateurs' is the selected category and 'Gérer les tâches' is the selected task. The main content area displays search results for 'Gérer les utilisateurs: Rechercher des utilisateurs'. A context menu is open over a search result, listing various actions such as 'Gérer les demandes de renouvellement de l'utilisateur', 'Afficher l'historique des demandes d'accès des utilisateurs', 'Activer/Désactiver un utilisateur', 'Afficher l'activité de l'utilisateur', 'Afficher l'utilisateur', 'Afficher la liste de travail de l'utilisateur', 'Afficher les comptes de terminal de l'utilisateur', 'Créer une demande en ligne', 'Déléguer des tâches', 'Exécution de service', 'Gérer les demandes d'accès des utilisateurs', 'Gérer les tâches de l'utilisateur', 'Modifier les comptes de terminal de l'utilisateur', 'Modifier un utilisateur', 'Notification d'expiration de la demande d'accès', 'Renouvellement de service', 'Réinitialiser le mot de passe de l'utilisateur', 'Révocation du service', 'Supprimer un utilisateur', 'Synchroniser l'utilisateur', 'Synchroniser l'utilisateur avec des modèles de compte', 'Synchroniser l'utilisateur avec des rôles', 'Vérifier la synchronisation du modèle de compte', and 'Vérifier la synchronisation du rôle'. A red arrow points to the 'Liste de tâches' option in the context menu.

Par exemple, pour modifier un utilisateur à l'aide de cette méthode, sélectionnez la catégorie Utilisateurs, puis la tâche de gestion des utilisateurs. Recherchez et sélectionnez l'utilisateur que vous souhaitez gérer. Dans les résultats de recherche, cliquez sur une icône pour afficher la liste des tâches que vous pouvez utiliser pour gérer l'utilisateur sélectionné. Dans cette liste, vous pouvez sélectionner la tâche Modifier l'utilisateur ou une autre tâche appropriée.

L'exemple suivant illustre un menu contextuel de tâche.

Pensez à implémenter la navigation basée sur les objets lorsque des utilisateurs effectuent plusieurs actions sur un seul objet.

CA Identity Manager inclut les tâches d'administration par défaut suivantes configurées pour la navigation basée sur les objets.

- Gérer les utilisateurs
- Gérer les groupes

- Gérer les organisations
- Gérer les rôles d'administration/Gérer les tâches d'administration
- Gérer les rôles d'accès
- Manage Provisioning Roles (Gérer les rôles de provisionnement)

Vous pouvez également ajouter des menus contextuels de tâche à des fenêtres de liste et de résultats de recherche pour activer la navigation basée sur les objets dans des tâches existantes. Par exemple, vous pouvez ajouter la navigation basée sur les objets à la tâche Modifier les membres du rôle d'administration afin d'afficher un menu contextuel de tâche pour chaque membre du rôle. L'administrateur peut utiliser les menus de tâches pour gérer les membres de rôles sans devoir effectuer une nouvelle recherche pour chaque membre de rôle.

Configuration de la navigation basée sur les objets

Les tâches configurées pour la navigation basée sur les objets incluent une seule fenêtre de recherche. L'utilisateur recherche un objet à gérer, puis utilise les menus de tâches déroulants pour afficher toutes les tâches qu'il peut effectuer sur cet objet.

Lorsque vous configurez la navigation basée sur les objets, tenez compte de ce qui suit.

- Dans l'onglet Profil, l'action de la tâche d'administration doit être Rechercher.
- La tâche d'administration ne peut pas contenir d'onglets.
- Si vous voulez configurer toutes les tâches d'administration pour utiliser la navigation basée sur les objets, ajoutez des boutons Créer et Supprimer à la fenêtre de recherche pour pouvoir exécuter ces opérations. Les actions Créer et Supprimer ne sont pas prises en charge dans le menu contextuel de tâche.

Configuration de la navigation objet/tâche

1. Effectuez l'une des étapes suivantes :
 - Sélectionnez Modifier la tâche d'administration dans Rôles et tâches, puis Tâches d'administration. Recherchez et sélectionnez la tâche d'administration à modifier.
 - Sélectionnez Modifier la tâche d'administration dans Rôles et tâches, puis Tâches d'administration. Sélectionnez ensuite Créer une copie de tâche d'administration, puis recherchez une tâche à copier.

Remarque : Pour simplifier la configuration, pensez à créer une copie d'une tâche de gestion existante, telle que Gérer les utilisateurs. Les tâches de gestion par défaut incluent les paramètres de configuration nécessaires à la navigation objet/tâche.

CA Identity Manager affiche les onglets à configurer pour la tâche que vous avez sélectionnée.

2. Configurez les paramètres de l'onglet Profil selon les besoins. Définissez l'action de la tâche sur Rechercher.
3. Sélectionnez l'onglet Rechercher, puis cliquez sur Parcourir pour configurer la fenêtre de recherche pour la tâche.

CA Identity Manager affiche la liste de fenêtres de recherche que vous pouvez appliquer à cette tâche.

4. Sélectionnez la fenêtre de recherche dont vous avez besoin.

Remarque : Pour simplifier la configuration, pensez à créer une copie d'une définition existante de fenêtre de recherche sur la gestion portant le même type d'objet, telle que Recherche sur la gestion des utilisateurs. Les fenêtres de gestion de recherche par défaut sont configurées pour prendre en charge la navigation objet/tâche.

5. Remplissez les champs de la fenêtre de configuration de fenêtre de recherche selon les besoins.

Remarque : Si vous ne voulez pas inclure de tâches séparées dans les menus pour la création d'un objet ou la suppression de plusieurs objets, vous pouvez configurer la fenêtre de recherche afin de disposer de boutons pour le lancement de ces tâches. Vous pouvez ensuite masquer ces tâches dans les menus.

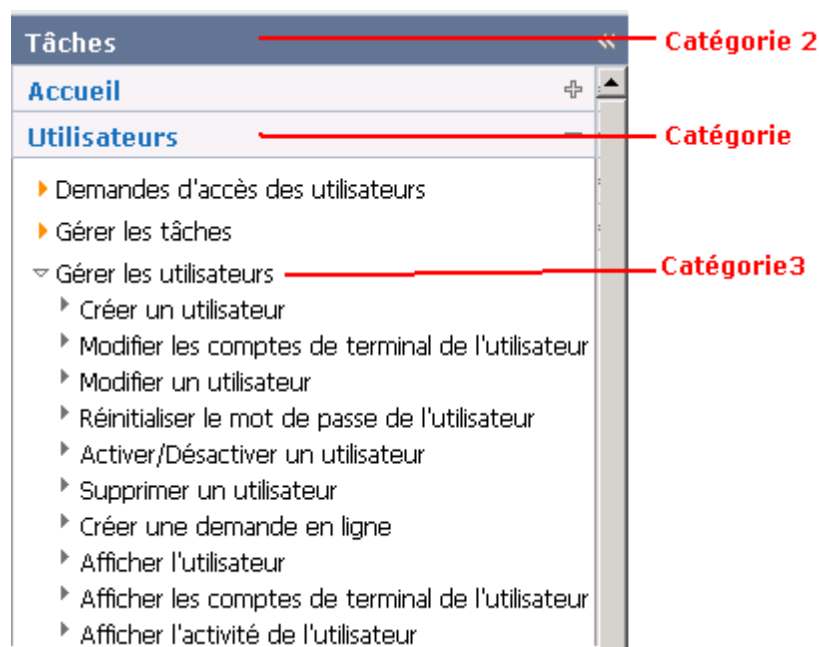
Catégories de tâches

Les catégories de tâches permettent d'organiser les tâches pour les rechercher et les localiser plus facilement dans la console d'utilisateur.

Vous pouvez spécifier trois catégories de tâches :

- La catégorie est la façon la plus commune de grouper des tâches. Généralement, le niveau de catégorie indique le type d'objet auquel la tâche s'applique, tel que le type Utilisateurs.
- La catégorie 2 détermine le nom de la catégorie de niveau supérieure. Par défaut, il s'agit de Tâches.
- La catégorie 3 fournit un niveau de groupement supplémentaire, si nécessaire. Par exemple, vous pouvez utiliser un nom de catégorie 3 pour grouper des tâches pour des sous-traitants.

Dans chaque catégorie, vous pouvez déterminer l'ordre dans lequel les éléments de la catégorie s'affichent en spécifiant un ordre de catégorie. Par exemple, dans l'illustration suivante, l'onglet Employé comporte un ordre de catégorie de 3.



Remarque : Lorsqu'une catégorie comporte plusieurs tâches, l'ordre de catégorie spécifié dans le profil de chaque tâche doit être le même. S'il est différent, plusieurs instances de cet onglet de catégorie apparaissent. Par exemple, la catégorie Employé contient deux tâches : Créer un employé et Modifier un employé. Si l'ordre de catégorie de la tâche Créer un employé est 3 et celui de la tâche Modifier un employé 6, la catégorie Employé apparaît sous la forme de deux onglets.

Désactivation de l'annulation automatique des tâches

Dans la console d'utilisateur, lorsqu'un utilisateur sélectionne un nouvel onglet de catégorie de tâche, CA Identity Manager annule la tâche active dans le volet des tâches. Si l'utilisateur a apporté des modifications à la tâche active, un message est affiché lui demandant de confirmer l'annulation. Par exemple, si un utilisateur apporte des modifications à l'aide de la tâche Modifier l'utilisateur, puis tente d'accéder à l'onglet Accueil avant d'envoyer les modifications Modifier l'utilisateur, CA Identity Manager informe l'utilisateur que la tâche est annulée et l'invite à confirmer.

Vous pouvez configurer CA Identity Manager pour permettre aux administrateurs de sélectionner un nouvel onglet de catégorie de tâche sans annuler la tâche active ni afficher de message de confirmation. Dans ce cas, la sélection du nouvel onglet de catégorie affiche le menu des tâches pour cette catégorie dans le volet de navigation gauche, mais conserve la tâche active dans le volet des tâches. Lorsque l'utilisateur sélectionne une nouvelle tâche, la tâche active est annulée sans notification.

Pour modifier le comportement par défaut afin que CA Identity Manager n'annule pas la tâche avant de basculer vers un nouvel onglet, ajoutez une propriété définie par l'utilisateur dans la console de gestion.

Pour modifier le comportement par défaut :

1. Ouvrez la console de gestion.
2. Sélectionnez Environnements, puis sélectionnez l'environnement que vous voulez modifier.

La page Propriétés de l'environnement s'ouvre.

3. Sélectionnez Paramètres avancés, Divers.
4. Entrez les valeurs suivantes et cliquez sur Ajouter.
 - Propriété : ConsoleDisableAutoTaskCancel
 - Valeur : true.
5. Cliquez sur Enregistrer.
6. Redémarrez l'environnement.

Flux de tâche

Dans CA Identity Manager, une tâche d'administration est composée d'un ou de plusieurs onglets qui représentent un groupement logique de fonctionnalités. Par exemple, la tâche Modifier l'utilisateur peut inclure les onglets Profil, Rôles d'administration et Groupes. *Le flux de tâche* détermine le déplacement des utilisateurs d'un onglet à l'autre à l'aide de la tâche d'administration.

CA Identity Manager offre trois options de flux de tâche.

- Onglets indépendants : les utilisateurs peuvent utiliser les onglets dans l'ordre souhaité.
- Assistants : les utilisateurs sont guidés parmi les onglets par un assistant.
- Séquences : les utilisateurs remplissent un onglet de la tâche, puis CA Identity Manager ouvre automatiquement l'onglet suivant.

L'option de flux d'onglet de séquence prend en charge les flux de pages dynamiques à l'aide d'une [logique personnalisée](#) (page 25).

Le flux de tâche est déterminé par le contrôleur d'onglets. Vous spécifiez le contrôleur d'onglets dans l'onglet Onglets lorsque vous créez ou modifiez une tâche d'administration.

Configuration d'onglets de tâche indépendants

Les onglets des tâches d'administration par défaut sont indépendants des autres onglets de la tâche. L'utilisateur peut utiliser les onglets de la tâche dans l'ordre de son choix. Il n'est pas nécessaire de compléter chaque onglet avant de soumettre la tâche.

Cette configuration d'onglet dans l'exemple suivant utilise le contrôleur d'onglets standard.

Create Contractor:

Profile | **Access Roles** | **Admin Roles**
Provisioning Roles | **Groups**

• = Required

• Organization

• User ID

Password

Confirm Password

Procédez comme suit:

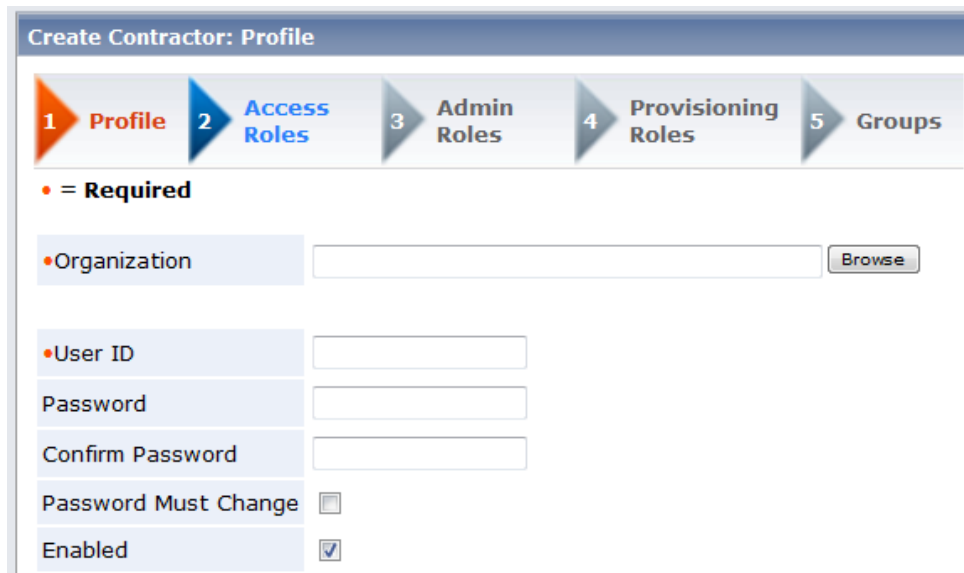
1. Dans la console d'utilisateur, sélectionnez l'une des options suivantes :
 - Rôles et tâches
 - Tâches, Rôles et tâches
2. Sélectionnez Tâches d'administration, Modifier la tâche d'administration.
3. Recherchez et sélectionnez la tâche d'administration à modifier.
CA Identity Manager affiche les onglets permettant de modifier une tâche d'administration.
4. Cliquez sur l'onglet Onglets.
5. Sélectionnez le contrôleur d'onglets standard dans la zone de liste.
6. Cliquez sur Soumettre.

CA Identity Manager enregistre les modifications apportées à la tâche.

Configuration d'une tâche comme assistant

L'assistant de contrôleur d'onglets permet de configurer une tâche comme assistant. Dans cette configuration d'onglets, les administrateurs utilisent chaque onglet dans un ordre précis. Lorsqu'un onglet est renseigné, ils cliquent sur le bouton Suivant pour accéder à l'onglet suivant dans la liste. Une zone en haut de l'assistant indique la progression et permet à l'administrateur de revenir aux fenêtres visitées précédemment.

L'exemple suivant affiche la tâche personnalisée Créer un sous-traitant affichée comme assistant.



Create Contractor: Profile

1 Profile 2 Access Roles 3 Admin Roles 4 Provisioning Roles 5 Groups

• = Required

• Organization

• User ID

Password

Confirm Password

Password Must Change

Enabled

Procédez comme suit:

1. Dans la console d'utilisateur, sélectionnez l'une des options suivantes :
 - Rôles et tâches
 - Tâches, Rôles et tâches
2. Sélectionnez Tâches d'administration, Modifier la tâche d'administration.
3. Recherchez et sélectionnez la tâche d'administration à modifier.
CA Identity Manager affiche les onglets à configurer pour la tâche que vous avez sélectionnée.
4. Cliquez sur l'onglet Onglets.
5. Sélectionnez l'assistant de contrôleur d'onglets dans la zone de liste.
6. Cliquez sur Soumettre.

CA Identity Manager enregistre les modifications apportées à la tâche.

Configuration d'une séquence d'onglets

Lorsqu'une tâche est configurée comme séquence d'onglets, CA Identity Manager affiche un onglet par page. L'utilisateur remplit un onglet, puis clique sur un bouton ou un lien personnalisé pour passer à l'onglet suivant.

La séquence d'onglets et les boutons/liens affichés sont déterminés par un script de programmation Java que vous enregistrez lorsque vous configurez le contrôleur d'onglets de séquence.

Dans le script Java personnalisé, vous pouvez spécifier l'apparence et l'ordre des onglets en fonction des entrées de l'utilisateur. Par exemple, si un utilisateur sélectionne une option dans le premier onglet, CA Identity Manager affiche une page. Si l'utilisateur sélectionne une autre option, une page différente s'affiche.

Pour configurer le contrôleur d'onglets de séquence :

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration.
2. Recherchez et sélectionnez la tâche d'administration à modifier.
CA Identity Manager affiche les onglets à configurer pour la tâche que vous avez sélectionnée.
3. Cliquez sur l'onglet Onglets.
4. Sélectionnez le contrôleur d'onglets de séquence dans la zone de liste.
5. Cliquez sur Soumettre.

CA Identity Manager enregistre les modifications apportées à la tâche.

Exemple de script Java pour contrôleurs d'onglets

CA Identity Manager inclut des exemples de fichiers JavaScript pour le script Java d'affichage des onglets et le script Java des onglets actifs.

Ces fichiers sont installés dans le répertoire `samples\WizardSequencerScripts` où résident les outils d'administration. Les outils d'administration sont installés aux emplacements par défaut ci-après.

- **Windows** : `<chemin_d'installation>\tools`
- **UNIX** : `<chemin_d'installation2>/tools`

Chapitre 3: Configuration des onglets et fenêtres de profil

Ce chapitre traite des sujets suivants :

[Onglets et fenêtres Profil](#) (page 27)

[Personnalisation des fenêtres de profil](#) (page 28)

[Modification d'une fenêtre Profil](#) (page 29)

[Ajout ou suppression de champs](#) (page 31)

[Propriétés de champs dans une fenêtre Profil](#) (page 32)

[Styles des champs](#) (page 39)

[Remplissage des options de champs](#) (page 50)

[Modification dynamique des propriétés d'affichage des champs](#) (page 70)

[Attributs logiques définis par fenêtre](#) (page 72)

[Composants supplémentaires d'une fenêtre de profil](#) (page 74)

[Configuration de la validation de niveau tâche](#) (page 86)

[Attributs personnalisés définis par l'utilisateur pour les rôles](#) (page 87)

Onglets et fenêtres Profil

Pour la plupart des tâches, vous incluez un onglet Profil, qui affiche les attributs de l'objet principal de la tâche. L'*objet principal* est l'objet devant être créé, affiché ou modifié par la tâche. Par exemple, dans la tâche de modification d'un utilisateur, l'objet principal est un utilisateur. L'onglet Profil inclut des attributs d'utilisateurs, tels qu'ID de l'utilisateur et Nom.

Lorsque vous configurez un onglet Profil, vous en définissez les caractéristiques de base et spécifiez une fenêtre Profil. La *fenêtre Profil* est la partie de l'onglet visible par l'utilisateur. Elle détermine quels attributs de l'objet principal s'affichent dans l'onglet, ainsi que les propriétés d'affichage de ces attributs.

Remarque : Vous pouvez utiliser la même fenêtre Profil dans l'onglet Profil de plusieurs tâches.

Lorsque vous créez une fenêtre Profil, vous sélectionnez les champs qui s'appliquent à celle-ci. Ces champs peuvent correspondre à des attributs de profils. Par exemple, la valeur entrée dans le champ ID de l'utilisateur de la tâche Créer un utilisateur est stockée dans un attribut de profil d'utilisateur.

Modifier la tâche d'administration: Modifier un utilisateur

Profil Rechercher Onglets Champs Événements

Utilisation du rôle

Configurer Profil

Sélectionner une définition de fenêtre

Configurer Fenêtre standard de profil

• = obligatoire

• Nom Profil de l'utilisateur par défaut

• Balise DefaultUserProfile

Utiliser 2 colonnes pour la mise en page

Organisation

(Espace)

ID de l'utilisateur

Personnalisation des fenêtres de profil

Une fenêtre de profil est composée de champs, qui collectent et affichent les valeurs des attributs. Par exemple, la fenêtre de profil des objets d'utilisateur contient les champs Prénom, Nom et Adresse électronique. Une fenêtre de profil peut également inclure les composants facultatifs suivants.

- Séparateurs de page
- Images
- Fichiers joints
- Champs d'historique
- Texte d'aide en ligne personnalisé
- Liens vers les tâches imbriquées

Lorsque vous créez un environnement CA Identity Manager, CA Identity Manager crée des fenêtres de profil par défaut qui contiennent les champs associés aux attributs spécifiés pour cet objet dans le fichier de configuration d'annuaire (directory.xml). Les administrateurs système doivent personnaliser les fenêtres de profil par défaut pour s'assurer qu'elles sont conformes aux exigences métier et permettent de tirer pleinement profit de CA Identity Manager.

Remarque : Pour plus d'informations sur les performances de CA Identity Manager, reportez-vous au *manuel d'implémentation (en anglais)*.

Les administrateurs système peuvent personnaliser les fenêtres de profil par défaut en procédant comme suit.

- Détermination des champs qui apparaissent dans une fenêtre de profil
- Spécification du style des champs
- Définition des valeurs de champ pour les zones de liste et les autres styles de champs
- Ajout de séparateurs de page pour simplifier l'affichage
- Ajout d'images
- Ajout de fichiers
- Ajout de liens pointant vers d'autres tâches
- Ajout de texte d'aide en ligne personnalisé

Modification d'une fenêtre Profil

Vous pouvez modifier une fenêtre de profil existante pour :

- Ajouter ou supprimer des champs
- Modifier la présentation des champs
- Modifier les propriétés des champs
- Ajouter du texte d'aide en créant des séparateurs de type HTML n'importe où dans la fenêtre Profil

Pour modifier une fenêtre de profil :

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration.
2. Recherchez et sélectionnez la tâche d'administration à modifier.
CA Identity Manager affiche les onglets à configurer pour la tâche que vous avez sélectionnée.
3. Sélectionnez l'onglet Onglets, puis l'onglet Profil.

4. Cliquez sur Parcourir en regard du champ Fenêtre.
CA Identity Manager affiche la liste des fenêtres de profil existantes.
5. Sélectionnez la fenêtre de profil à modifier ou à copier, puis cliquez sur l'un des boutons suivants.
 - **Sélectionner**
Ajoute la fenêtre sélectionnée à l'onglet en cours de configuration.
 - **Modifier**
Ouvre une nouvelle fenêtre dans laquelle vous pouvez modifier les paramètres (notamment les champs, les propriétés de champs et la présentation) de la fenêtre sélectionnée.
 - **Suppression**
Supprime la fenêtre sélectionnée.
 - **Nouveau**
Ouvre une nouvelle fenêtre dans laquelle vous pouvez créer une fenêtre. La nouvelle fenêtre n'inclut aucun champ par défaut.
 - **Copier**
Crée une fenêtre à l'aide des paramètres d'une fenêtre existante. Pour créer une fenêtre basée sur une fenêtre existante, ajoutez un nouveau nom et une nouvelle balise à la fenêtre, puis modifiez les paramètres selon les besoins.
 - **Annuler**
Réaffiche la fenêtre de configuration d'onglet.

Si vous avez sélectionné Modifier, Nouvelle ou Copier, CA Identity Manager ouvre une nouvelle fenêtre dans laquelle vous pouvez créer ou modifier une fenêtre de profil.

Ajout ou suppression de champs

Les fenêtres de profil par défaut incluent tous les attributs de l'objet dans l'ordre utilisé dans la configuration d'annuaire (directory.xml). Vous pouvez ajouter ou supprimer des champs, ou les réorganiser à l'aide des contrôles situés au bas de la liste d'attributs dans la définition de la fenêtre de profil.

The screenshot shows a configuration window for user profiles. At the top, there is a list of attributes with checkboxes and edit icons: 'User organization name', 'Disabled State', and 'Department'. Below this list are several control options, each with a dropdown menu set to '1' and a corresponding button:

- Ajouter 1 lignes pour 1 champs avant ou après chaque ligne sélectionnée (Ajouter)
- Ajouter 1 champs avant chaque ligne sélectionnée (Ajouter)
- Ajouter 1 champs après chaque ligne sélectionnée (Ajouter)
- Supprimer les lignes sélectionnées (Supprimer)
- Déplacer les lignes sélectionnées vers le haut de 1 lignes (Déplacer vers le haut)
- Déplacer les lignes sélectionnées vers le bas de 1 lignes (Déplacer vers le bas)
- Combiner les lignes adjacentes sélectionnées en une seule ligne (Combiner)
- Diviser chaque ligne sélectionnée en plusieurs lignes (Diviser)
- Aperçu (Aperçu)

Pour ajouter, supprimer ou réorganiser des champs :

1. [Modifiez une fenêtre de profil](#) (page 29).
2. Sélectionnez les champs à modifier, puis l'action à exécuter.

Remarque : Lorsque vous modifiez les propriétés de champs dans la fenêtre Profil, il peut être plus facile de manipuler des lignes contenant plusieurs champs comme suit :

 - a. Cliquez sur Diviser chaque ligne sélectionnée en plusieurs lignes pour placer les champs sur des lignes séparées.
 - b. Manipulez les champs sur des lignes distinctes.
 - c. Cliquez sur Combiner les lignes adjacentes sélectionnées en une seule ligne pour regrouper les champs sur une seule ligne.
3. Si vous sélectionnez une action nécessitant une valeur, sélectionnez cette dernière.

Par exemple, pour déplacer des lignes sélectionnées de trois niveaux vers le haut, sélectionnez 3 dans la zone de liste Déplacer les lignes sélectionnées vers le haut de.
4. Cliquez sur Aperçu pour afficher les modifications apportées.

CA Identity Manager ouvre une nouvelle fenêtre affichant les modifications que vous avez apportées.
5. Cliquez sur OK, puis sur Sélectionner pour revenir à la tâche Modifier la tâche d'administration.

Propriétés de champs dans une fenêtre Profil

Vous sélectionnez un champ pour en modifier les propriétés. Chaque style de champ comporte des propriétés distinctes, qui définissent l'affichage, les autorisations et les valeurs par défaut de cette propriété.

Remarque : L'option que vous sélectionnez dans le champ Style détermine les propriétés qui sont affichées dans la fenêtre Propriétés du champ. Il se peut que certaines propriétés décrites dans cette liste ne soient pas visibles.

Vous pouvez définir les propriétés suivantes (dans l'ordre alphabétique) pour un champ :

- **Nom de l'attribut**

Spécifie le nom de l'attribut de l'objet.

- **Etiquette des valeurs disponibles**

Définit le texte apparaissant au-dessus de la zone de liste qui contient les éléments pouvant être sélectionnés dans le sélecteur d'options.

- **Valeur sélectionnée**

Spécifie la valeur d'un champ lorsque sa case est sélectionnée. Par exemple, la valeur sélectionnée du champ Activé est True.

La valeur par défaut est True.

Remarque : Ce champ est visible lorsque le style Case à cocher est sélectionné.

- **Colonnes**

Spécifie la largeur en nombre de caractères pour la zone de texte.

Remarque : Ce champ n'est disponible que si vous sélectionnez le style Zone de texte.

- **Classe CSS**

Spécifie la classe de feuille de style en cascade qui contrôle la présentation de ce champ.

- **Style CSS**

Spécifie les règles de feuille de style en cascade qui contrôlent la présentation de ce champ.

Vous pouvez utiliser ce champ pour définir la largeur d'un champ. Par exemple, pour définir la largeur d'un champ avec le style Liste déroulante sur 300 pixels, spécifiez ce qui suit dans le champ Style CSS :

The screenshot shows a configuration interface for a dropdown list. It includes the following elements:

- Style CSS:** A text input field containing the CSS rule `{Width:300px}`, which is circled in red.
- Source des options de sélection:** A dropdown menu currently set to "Liste simple".
- Options de sélection:** A text area containing the list of options: "Boston", "New York City", "Portland", and "San Francisco".
- Instructions:** A note below the dropdown menu reads: "Entrez les options sur différentes lignes. Si les valeurs d'affichage et de stockage de l'option diffèrent, entrez-les sous la forme : valeur-stockage;valeur-affichage."

Remarque : Par défaut, la largeur des champs qui incluent une liste de valeurs (par exemple, une zone de liste déroulante ou multi-sélecteur) est définie sur auto (`{width:auto}`). Ce paramètre définit la taille du champ de sorte que le champ puisse recevoir la valeur la plus longue. Par exemple, si la valeur la plus longue dans le champ de sélection de ville est San Francisco, la liste d'options est dimensionnée pour afficher la valeur entière.

Vous pouvez également utiliser le champ Style CSS pour contrôler d'autres propriétés d'affichage, telles que la taille de texte et la couleur d'arrière-plan.

- **Etiquette des valeurs actuelles**

Définit le texte apparaissant au-dessus de la zone de liste qui contient des éléments sélectionnés dans le sélecteur d'objets.

- **Modèle d'affichage de date**

Détermine le format des dates affichées dans un champ et dans le contrôle Sélecteur de dates.

- **Modèle de stockage de date**

Détermine la façon dont CA Identity Manager stocke les dates dans les référentiels d'utilisateurs.

- **Par défaut**

Indique la valeur affichée par défaut, et qui est stockée dans le profil si aucune autre valeur n'est spécifiée.

Pour une case à cocher, entrez True pour que la valeur par défaut soit activée et False pour qu'elle soit désactivée.

Remarque : Les valeurs par défaut s'appliquent aux tâches Créer uniquement. Si vous définissez une valeur par défaut pour un champ qui est utilisé dans une tâche Modifier ou Afficher, la valeur par défaut ne s'affichera pas dans la fenêtre.

- **Script Java par défaut**

Permet d'utiliser JavaScript pour définir la valeur par défaut d'un champ. Avec JavaScript, vous pouvez définir la valeur de manière dynamique. Par exemple, vous pouvez définir une valeur par défaut en fonction d'autres attributs.

N'utilisez ce champ que pour les tâches de création.

- **Désactiver la saisie semi-automatique**

Désactive la saisie semi-automatique dans Internet Explorer. Si cette case à cocher est sélectionnée, Internet Explorer ne suggère aucune valeur de champ en fonction des entrées précédentes.

Pour plus d'informations sur la fonctionnalité de saisie semi-automatique, reportez-vous à la documentation d'Internet Explorer.

- **Script Java d'initialisation**

Permet d'utiliser JavaScript pour définir la valeur par défaut d'un champ. Utilisez ce champ pour n'importe quel type de tâche.

- **Remarque :** Le script Java figurant dans ce champ s'exécute après celui figurant dans le champ Script Java par défaut pour les tâches de création.

- **Etendue du champ**

Spécifie le nombre de colonnes que le champ englobe (étiquette non comprise)

- **Champ de correspondance**

Spécifie le champ dans lequel CA Identity Manager recherche une valeur correspondante. Cette fonctionnalité permet de vérifier que les valeurs de deux champs d'une fenêtre correspondent. Ce champ sert généralement à contrôler l'exactitude d'un mot de passe ou d'autres informations critiques. Par exemple, une fenêtre de profil peut comprendre des champs Mot de passe et Confirmer le mot de passe. Pour le champ Confirmer le mot de passe, la valeur de Champ de correspondance doit alors être Mot de passe.

Remarque : CA Identity Manager utilise un attribut logique défini par fenêtre pour vérifier que les valeurs des deux champs de la fenêtre coïncident. Pour que Champ de correspondance s'affiche, le champ Nom de l'attribut doit être défini sur (Fenêtre d'attributs logiques).

- **Etiquette droite**

Spécifie le texte qui s'affiche à droite du champ. Vous pouvez utiliser le champ Etiquette droite pour fournir un texte de description ou d'aide aux champs d'une fenêtre de profil.

- **Etendue de l'étiquette**

Spécifie le nombre de colonnes que l'étiquette englobe.

- **Longueur maximum**

Définit le nombre maximal de caractères que ce champ peut contenir.

- **nom**

Spécifie l'étiquette que vous souhaitez pour cet attribut dans la fenêtre.

- **Autorisation**

Détermine le niveau d'autorisation du champ.

Remarque : Si un champ est obligatoire, choisissez un paramètre Obligatoire. Les champs obligatoires sont signalés par un point dans la fenêtre.

- **Lire**

Un administrateur peut afficher le champ, mais pas le modifier.

- **Lecture/écriture**

Un administrateur peut voir la valeur actuelle du champ, le cas échéant, et entrer une valeur pour le champ.

- **Lecture/écriture requises**

Spécifie que le champ est obligatoire, mais fonctionne comme le paramètre Lecture/écriture.

- **Ecrire**

Un administrateur ne peut pas voir la valeur actuelle du champ, le cas échéant, mais peut entrer une valeur.

Par exemple, un administrateur peut changer le mot de passe d'un utilisateur, mais ne peut pas voir son mot de passe actuel.

- **Ecrire une fois**

Une valeur peut être entrée une seule fois et ne peut pas être modifiée.

Par exemple, un administrateur peut spécifier une organisation lors de la création d'un utilisateur, mais ne peut pas la modifier ultérieurement.

- **Ecriture requise**

Spécifie que le champ est obligatoire, mais fonctionne comme le paramètre Ecriture.

- **Conserver les options personnalisées**

Indique si CA Identity Manager conserve les valeurs existantes d'un attribut lorsque celles-ci ne sont pas valides. Par exemple, un champ Etat inclut les options Massachusetts et New York. En revanche, un utilisateur existant est californien. Si cette option est activée, CA Identity Manager affiche Californie comme s'il s'agissait d'une option valide pour cet utilisateur. Si cette option est désactivée, CA Identity Manager affiche la première option de la liste (Massachusetts). Si le champ n'est pas obligatoire, aucune valeur n'est affichée.

- **Par défaut**

- CA Identity Manager oblige l'utilisateur à sélectionner uniquement les options valides.

- **Lignes**

Spécifie le nombre de lignes qu'une zone de texte destinée à la saisie utilisateur doit inclure.

Par exemple, vous pouvez définir pour le champ Description une zone de texte permettant à l'utilisateur d'entrer quatre lignes de texte.

Remarque : Ce champ n'est disponible que si vous sélectionnez le style Zone de texte.

- **Afficher le sélecteur horaire**

Affiche un contrôle calendrier que les utilisateurs peuvent utiliser pour sélectionner une date et une heure.

- **Taille**

Spécifie la taille du champ. Entrez un nombre en fonction du style de champ. Pour les champs de texte et de mot de passe, entrez le nombre de caractères. Pour les champs déroulants, de sélection, de sélection multiple et multitexte, entrez le nombre de lignes.

- **Source des options de sélection**

Spécifie la manière dont un champ contenant plusieurs options est rempli.

- **Aucun**

- CA Identity Manager n'utilise pas de source externe pour les options de sélection.

- **Données des boîtes de sélection**

- Spécifie si CA Identity Manager ajoute les options dans le champ à l'aide des [données de boîtes de sélection](#) (page 54).

– **Liste simple**

Permet d'entrer une liste d'options dans une zone de texte. Si vous sélectionnez cette option, le champ suivant apparaît :

Options de sélection

Entrez les options sur des lignes séparées. Si les valeurs d'affichage et de stockage de l'option diffèrent, entrez-les sous la forme : "valeur-stockage;valeur-affichage".

– **Dépend de la valeur d'un autre champ**

Indique que CA Identity Manager remplit les options du champ en fonction des options d'un autre champ de la fenêtre de tâche. L'autre champ doit également être rempli à l'aide des données des boîtes de sélection ou dépend aussi de la valeur d'un autre champ.

La dépendance par rapport à un autre champ est définie dans la configuration des données des boîtes de sélection.

– **JavaScript**

Spécifie le script Java qui contient les options du champ. Si vous sélectionnez cette option, le champ suivant apparaît :

Options de sélection (JavaScript)

Ce script Java doit contenir une fonctionnalité avec la signature "fonction getOptions(FieldContext)," et renvoyer une chaîne d'options délimitée par des barres verticales Si les valeurs d'affichage et de stockage de l'option diffèrent, elles doivent être séparées par un point-virgule (;).

■ **Style**

Détermine la présentation du champ.

[Options de style](#) (page 39) répertorie les styles que vous pouvez sélectionner pour un champ.

■ **Texte de l'infobulle**

Spécifie le texte décrivant un champ. Le texte s'affiche dans la fenêtre à côté du champ auquel il s'applique.

- **Valeur non sélectionnée**

Spécifie la valeur d'un champ lorsque sa case à cocher est désélectionnée. Par exemple, la valeur non sélectionnée du champ Activé est False.

La valeur par défaut est false.

Remarque : Ce champ est visible lorsque le style Case à cocher est sélectionné.

- **Autoriser d'autres valeurs non sélectionnées**

Lorsque cette case est non sélectionnée, elle définit la valeur de l'attribut sur False dans le référentiel d'utilisateurs si l'attribut est vide. Lorsqu'elle est sélectionnée, CA Identity Manager autorise l'absence de valeur dans l'attribut.

Utilisez ce champ pour définir automatiquement les attributs vides sur False dans le magasin d'utilisateurs.

- **Expression de validation**

Contient une expression régulière qui effectue une validation de niveau tâche.

- **Classe Java de validation**

Contient le nom complet d'une classe Java qui effectue la validation. Par exemple :
com.mycompany.MyJavaValidator

CA Identity Manager recherchera le fichier de classe dans le répertoire racine spécifié pour les fichiers de classe Java personnalisés.

- **Script Java de validation**

contient le code JavaScript complet qui effectue la validation.

Ce champ permet également de spécifier un code JavaScript qui masque, affiche, active ou désactive de façon dynamique des champs particuliers en fonction des valeurs actuelles d'autres champs.

Remarque : Vous devez spécifier le code JavaScript dans ce champ. Avec la validation de niveau tâche, vous ne pouvez pas référencer un fichier contenant du code JavaScript.

Styles des champs

Le champ Style permet de spécifier la manière dont un champ est affiché dans une fenêtre Profil. Vous pouvez sélectionner les styles suivants :

Remarque : La liste des styles disponibles dans le champ Style dépend du type de champ que vous configurez. Il se peut que certaines de ces options n'apparaissent pas dans le champ Style pour le type de champ que vous définissez.

- **Case à cocher**

Ajoute en regard du nom du champ une case à cocher, qui active ou désactive un paramètre. Par exemple, utilisez une case à cocher pour le champ Activer un utilisateur. Si la case à cocher est sélectionnée, le compte d'utilisateur est activé. Si elle n'est pas sélectionnée, le compte d'utilisateur est désactivé.

- **Case à cocher : sélection multiple**

Ajoute une case à cocher en regard de chaque option d'un champ. L'utilisateur peut sélectionner plusieurs options dans la liste d'options.

Utilisez ce champ uniquement pour les attributs à valeurs multiples.

- **Sélecteur de dates** (page 41)

Affiche une icône de calendrier en regard d'un champ de date (par exemple, Date de début). L'administrateur clique sur l'icône de calendrier pour afficher un contrôle de calendrier lui permettant de sélectionner la date de leur choix.

- **Liste déroulante**

Permet de sélectionner une valeur pour le champ. Une seule valeur est visible. L'utilisateur clique sur une flèche pour afficher d'autres valeurs dans la liste.

L'utilisateur peut sélectionner une seule valeur dans la liste.

- **Liste modifiable déroulante**

Offre le même choix de valeurs affichées par un style Liste déroulante, mais ajoute une zone de texte dans laquelle l'utilisateur peut entrer une nouvelle valeur.

- **Sélecteur de groupes**

Affiche un contrôle permettant de sélectionner un groupe.

- **Masqué**

Extrait la valeur du champ de l'objet, mais l'étiquette et la valeur du champ ne sont pas affichées dans la fenêtre de tâche.

- **Sélection multiple**

Affiche une liste de valeurs pour un champ.

Dans une zone de sélection multiple, les valeurs possibles du champ apparaissent dans la zone de liste. L'utilisateur peut sélectionner plusieurs valeurs dans la liste.

Utilisez cette option uniquement avec les attributs à valeurs multiples.

- **Multitexte**

Permet d'entrer plusieurs valeurs dans une zone de texte.

Utilisez cette option uniquement avec les attributs à valeurs multiples.
- **Sélecteur d'objet**

Affiche un contrôle permettant de sélectionner un objet géré.

Ce style est généralement utilisé dans les fenêtres de gestion des comptes.

Utilisez cette option uniquement avec les attributs à valeurs multiples.
- **Sélecteur d'options**

Affiche deux zones de liste, qui affichent les valeurs disponibles et actuelles du champ. L'utilisateur clique sur des boutons pour ajouter ou supprimer des valeurs actuelles.

Utilisez cette option uniquement avec les attributs à valeurs multiples.
- **Sélecteur modifiable d'options**

Affiche les deux zones de liste utilisées pour un style Sélecteur d'options, ainsi qu'une zone de texte dans laquelle l'utilisateur peut entrer une nouvelle valeur.

Utilisez cette option uniquement avec les attributs à valeurs multiples.
- **Sélecteur d'organisations**

Affiche un contrôle permettant de sélectionner une organisation.
- **Mot de passe**

Affiche la valeur du champ sous la forme d'une série d'astérisques. Par exemple, le mot de passe secret est affiché sous la forme *****.
- **Sélection unique par bouton radio**

Affiche une liste de valeurs pour un champ. Un bouton radio apparaît en regard de chaque valeur.
- **Chaîne**

Affiche la valeur du champ en tant que valeur en lecture seule. S'il n'existe aucune valeur, le champ est vide.
- **Texte**

Affiche une zone dans laquelle l'utilisateur peut entrer une valeur pour le champ.

Si l'autorisation du champ est lecture seule, la valeur est affichée sous forme d'étiquette.

- **Zone de texte**

Affiche une zone dans laquelle l'utilisateur peut entrer des valeurs plus longues qu'un champ de texte. Par exemple, une description peut nécessiter une zone de texte.

- **Sélecteur d'utilisateurs**

Affiche un contrôle permettant de sélectionner un groupe.

Remarque : Vous pouvez spécifier des valeurs appelées *options* dans les menus déroulants, les zones de liste déroulante, les zones de sélection multiple, les sélecteurs d'options, les zones de sélecteur modifiable d'options et les zones de sélection unique. L'utilisateur peut activer une ou plusieurs options pour renseigner une valeur de champ. La section [Remplissage des options de champs](#) (page 50) fournit des informations sur les méthodes permettant de spécifier les options de champs.

Options du sélecteur de dates

Le style Sélecteur de dates permet d'ajouter une icône de calendrier à un champ de la fenêtre Profil. L'utilisateur peut cliquer sur l'icône pour ouvrir un calendrier lui permettant de sélectionner une date. La date sélectionnée est stockée dans l'attribut de profil associé au champ. Par exemple, vous pouvez ajouter le contrôle de calendrier à un champ Date de début de l'onglet Profil d'une tâche Créer un sous-traitant. Lorsqu'un administrateur sélectionne le premier jour du contrat, Identity Manager stocke cette date dans le profil de l'utilisateur.

Le style Sélecteur de dates comporte les paramètres de configuration ci-après.

■ **Modèle d'affichage de date (Facultatif)**

Détermine le format des dates affichées dans un champ et dans le contrôle Sélecteur de dates. Spécifie le modèle d'affichage de date à l'aide de conventions Java. Par exemple, l'expression Java ci-après s'affiche comme Oct 2011.

MMM aaaa

Le champ Modèle d'affichage de date apparaît uniquement si le style Sélecteur de dates est sélectionné.

Notez les informations suivantes lors de la spécification des modèles d'affichage de date :

- Le contrôle Sélecteur de dates prend en charge un *sous-ensemble* des formats de date Java.

La liste complète des formats de date Java s'affiche dans la documentation de la plate-forme Java™ 2 Standard Edition. Ed. v1.4.2 sur le site Web d'Oracle (<http://java.sun.com/j2se/1.4.2/docs>). Recherchez SimpleDateFormat.

Les formats suivants, qui sont pris en charge dans SimpleDateFormat, ne sont *pas* pris en charge par le contrôle Sélecteur de dates de CA Identity Manager :

Symbole	Signification	Type	Exemple
G	Epoque	Texte	"GG" -> "Après J.-C."
D	Jour de l'année (1-365 ou 1-364)	Nombre	"D" -> "65" "D" -> "065"
W	Semaine du mois (1-5)	Nombre	"W" -> "3"
k	Heure (1-24)	Nombre	"k" -> "3" "kk" -> "03"
K	Heure (0-23)	Nombre	"K" -> "15" "KK" -> "15"
S	Milliseconde (0-999)	Nombre	"SSS" -> "007"

Il est déconseillé de spécifier un modèle d'affichage de date si l'environnement prend en charge plusieurs paramètres régionaux. Si aucun modèle d'affichage n'est spécifié, la date est affichée dans un format qui correspond aux paramètres régionaux de l'utilisateur.

■ **Modèle de stockage de date**

Détermine la manière dont la date est stockée dans le magasin d'utilisateurs. Spécifie le modèle d'affichage de date à l'aide de conventions Java. Pour plus d'informations, reportez-vous à la description du champ Modèle d'affichage de date.

- **Texte de l'infobulle**

Spécifie le texte qui s'affiche à côté du sélecteur de dates dans la fenêtre de profil.

Vous pouvez utiliser ce champ pour fournir des informations supplémentaires sur le contrôle Sélecteur de dates.

- **Afficher le sélecteur horaire**

Permet aux utilisateurs de spécifier, outre la date, l'heure lors de l'utilisation d'un contrôle calendaire dans une fenêtre de profil. L'heure est stockée dans le magasin d'utilisateurs.

- **Masquer les secondes**

Masque l'affichage des secondes dans le contrôle Sélecteur horaire.

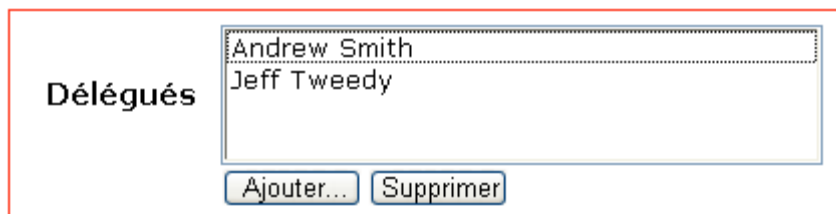
Remarque : Les champs Modèle de stockage de date, Afficher le sélecteur horaire et Format de sélecteur horaire s'affichent uniquement si l'attribut sélectionné ne comporte pas le type de valeur Date, ISODate ou UnicenterDate dans le fichier de configuration d'annuaire (directory.xml). Pour plus d'informations sur les types de valeurs, reportez-vous au *manuel de configuration (en anglais)*.

Options du sélecteur d'objet

Le style Sélecteur d'objet permet à l'administrateur d'ajouter la fonctionnalité de recherche à un champ d'une fenêtre de profil. Cette fonctionnalité permet à l'utilisateur de rechercher et de sélectionner un objet à associer à l'attribut décrit dans le profil. Par exemple, un administrateur peut ajouter un sélecteur d'objet au champ Gestionnaire pour permettre aux utilisateurs de rechercher le gestionnaire d'un nouvel utilisateur dans la tâche Créer un utilisateur. Lorsque l'utilisateur sélectionne un gestionnaire et soumet la tâche Créer un utilisateur, CA Identity Manager stocke les informations relatives à ce gestionnaire dans le profil du nouvel utilisateur.

Office	<input type="text"/>
Department	<input type="text"/>
Manager	<input type="text"/> <input type="button" value="Rechercher"/> <input type="button" value="Effacer"/>

Dans la plupart des cas, la recherche du sélecteur d'objet permet aux utilisateurs de sélectionner et de stocker une seule valeur. Toutefois, l'administrateur peut également configurer le sélecteur d'objet pour permettre aux utilisateurs de rechercher et de sélectionner plusieurs valeurs. Dans ce cas, les valeurs sélectionnées sont stockées dans un attribut à valeurs multiples.



Configuration d'un sélecteur d'objet

Le style Sélecteur d'objet ajoute un bouton Parcourir à un champ. Les utilisateurs peuvent cliquer sur le bouton pour rechercher et sélectionner un objet pour renseigner le champ.

Le sélecteur d'objet peut être appliqué aux champs d'attributs à valeurs multiples ou à valeur unique.

Pour configurer un sélecteur d'objet :

1. [Modifiez une définition de fenêtre de profil](#) (page 29).
2. Ajoutez un champ à la fenêtre de profil à l'aide des contrôles situés au bas de la liste de champs.
3. Cliquez sur l'icône représentant une flèche vers la droite pour ouvrir la boîte de dialogue Propriétés du champ pour l'attribut que vous ajoutez.
4. Spécifiez les valeurs des champs suivants :

Nom de l'attribut

Sélectionnez l'attribut associé au champ.

Par exemple, si vous configurez un champ spécifiant un gestionnaire d'utilisateurs, sélectionnez l'attribut dans le magasin d'utilisateurs qui stocke ces informations.

Remarque : Si vous configurez le champ d'un attribut qui stocke plusieurs valeurs, veillez à ce que l'attribut soit défini en tant qu'attribut à valeurs multiples dans le fichier de configuration d'annuaire (directory.xml). Pour plus d'informations, voir le *Manuel de configuration*.

Style

Sélectionnez le style Sélecteur d'objet.

Type d'objet

Spécifiez le type d'objet recherché par l'utilisateur. Par exemple, si vous configurez un sélecteur d'objet pour le champ Gestionnaire, sélectionnez le type d'objet Utilisateurs.

Restreindre à une valeur unique

Permet à l'administrateur de sélectionner une seule valeur lorsqu'il recherche un objet.

Remarque : Cette option est disponible uniquement lorsque vous spécifiez un attribut à valeurs multiples dans le champ Nom de l'attribut.

Attribut d'affichage

Sélectionnez l'attribut de l'objet sélectionné qui est affiché lorsque la valeur est sélectionnée.

Dans l'exemple du gestionnaire, sélectionnez Nom complet ou ID de l'utilisateur afin que les utilisateurs identifient facilement le gestionnaire.

Remarque : l'ID unique de l'objet est stocké dans l'attribut.

Fenêtre de recherche

Sélectionnez la fenêtre de recherche que les administrateurs utilisent pour rechercher l'objet.

Taille

Spécifie le nombre d'éléments à afficher dans la zone de liste.

Remarque : Ce champ est disponible uniquement lorsque vous spécifiez un attribut à valeurs multiples dans le champ Nom de l'attribut.

Par défaut

Sélectionnez l'objet par défaut que CA Identity Manager utilise lorsqu'aucun objet n'est sélectionné.

5. Cliquez sur Appliquer, puis sur OK pour revenir à la page Sélectionner une définition de fenêtre.

CA Identity Manager ajoute le sélecteur d'objet au champ que vous avez modifié.

6. Sélectionnez l'onglet que vous avez modifié, puis cliquez sur OK.

CA Identity Manager enregistre les modifications apportées à la fenêtre.

Affichage des attributs structurés

Un attribut structuré permet à une valeur d'attribut de stocker plusieurs valeurs associées : par exemple, la valeur d'un attribut structuré peut inclure le prénom, le nom et l'adresse de messagerie d'un utilisateur. Ces types d'attributs sont utilisés par certains types de terminaux mais peuvent être gérés dans CA Identity Manager.

Vous pouvez configurer CA Identity Manager de manière à afficher les valeurs d'un attribut structuré sous forme de tableau que les utilisateurs peuvent modifier. Dans ce cas, les modifications apportées aux valeurs de l'attribut sont stockées dans le magasin d'utilisateurs et propagées vers le compte du terminal (si la synchronisation est activée).

Conditions préalables à la prise en charge de l'attribut structuré

Pour ajouter une prise en charge de l'attribut structuré dans la console d'utilisateur, la définition de l'attribut structuré dans le fichier de configuration d'annuaire (directory.xml) doit inclure les paramètres ci-après.

- `multivalued="true"`

L'attribut doit être un attribut à valeurs multiples standard dans le magasin d'utilisateurs.
- `displayhint="value1;value2;valueN"`

Le paramètre `displayhint` doit contenir une liste des champs disponibles dans la valeur d'attribut, séparés par un point-virgule (;).
- `valuetype="structured"`

Le paramètre `valuetype` doit être défini sur "structured" pour configurer un tableau d'affichage dans la console d'utilisateur. Si ce paramètre n'est pas défini correctement, les champs servant à configurer le tableau d'affichage n'apparaissent pas.

Une description complète de l'attribut structuré doit ressembler à ce qui suit.

```
<Attribute physicalname="emailaddress" required="false" searchable="false"
multivalued="true" displayhint="courriel;type;principal" valuetype="structured">
```

Remarque : Pour plus d'informations sur la configuration du fichier `directory.xml`, reportez-vous au *manuel de configuration (en anglais)*.

Configuration d'un affichage d'attribut structuré

Pour permettre à des utilisateurs d'ajouter ou de modifier les valeurs d'un attribut structuré, vous pouvez ajouter un affichage d'attribut structuré à une fenêtre de profil. Cet affichage est généralement utilisé dans les modèles de compte pour les types de terminaux prenant en charge les attributs structurés.

Pour configurer un affichage d'attribut structuré :

1. Définissez la [configuration requise](#) (page 46) pour la prise en charge de l'attribut structuré.
2. [Modifiez une fenêtre de profil](#) (page 29).
3. Ajoutez un champ à la fenêtre de profil à l'aide des contrôles situés au bas de la liste de champs.
4. Cliquez sur l'icône représentant une flèche vers la droite pour ouvrir la boîte de dialogue Propriétés du champ.
5. Sélectionnez un attribut structuré dans la liste présentée dans le champ Nom de l'attribut.

Remarque : L'attribut que vous sélectionnez doit avoir le type de valeur *structuré* dans le fichier de configuration d'annuaire (directory.xml).

6. Sélectionnez Imbriqué et structuré dans le champ Style.

Les champs figurant dans la fenêtre Propriétés du champ varient en fonction du style sélectionné.

7. Ajoutez des champs au tableau d'affichage en cliquant sur l'icône représentant une flèche vers la droite, puis en sélectionnant une valeur dans la zone de liste.

Les valeurs figurant dans cette liste sont celles disponibles dans l'attribut structuré, tel que défini dans le [fichier de configuration d'annuaire](#) (page 46) (directory.xml).

Lorsque vous sélectionnez une valeur, CA CA Identity Manager l'ajoute au tableau d'affichage, dans lequel vous pouvez en configurer les propriétés.

8. Spécifiez les champs suivants pour la valeur lors de la configuration du tableau d'affichage.

Nom

Indique l'étiquette du champ.

Style

Spécifie les propriétés d'affichage du champ. Vous pouvez sélectionner l'une des options de style suivantes.

■ Case à cocher

Ajoute en regard du nom du champ une case à cocher, qui active ou désactive un paramètre.

■ Date

Affiche une zone de texte dans laquelle les administrateurs peuvent entrer une date.

CA Identity Manager valide le format de date.

- **Liste déroulante**

Permet de sélectionner une valeur pour le champ. Une seule valeur est visible. L'utilisateur clique sur une flèche pour afficher d'autres valeurs dans la liste.

L'utilisateur peut sélectionner une seule valeur dans la liste.

- **Liste modifiable déroulante**

Offre le même choix de valeurs affichées par un style Liste déroulante, mais ajoute une zone de texte dans laquelle l'utilisateur peut entrer une nouvelle valeur.

- **Sélecteur d'objet**

Permet d'ajouter une fenêtre de recherche pour la sélection d'un objet géré.

- **Case d'option**

Affiche une liste de valeurs pour un champ. Un bouton radio apparaît en regard de chaque valeur. L'utilisateur peut sélectionner une seule valeur dans la liste.

- **Chaîne**

Affiche la valeur du champ en tant que valeur en lecture seule. S'il n'existe aucune valeur, le champ est vide.

- **Structuré**

Affiche un bouton Ajouter afin d'ajouter une nouvelle valeur à la table d'attributs composés imbriqués.

- **Texte**

Affiche une zone dans laquelle l'utilisateur peut entrer une valeur pour le champ.

Si l'autorisation du champ est lecture seule, la valeur est affichée sous forme d'étiquette.

Triable

Détermine si les utilisateurs peuvent trier le tableau d'affichage sur le champ sélectionné.

- Sélectionnez la case à cocher Autoriser le reclassement des valeurs pour permettre aux administrateurs de réorganiser la liste d'attributs structurés dans la fenêtre de profil.

La sélection de ce paramètre a pour effet d'ajouter des flèches vers le haut et vers le bas à la dernière colonne de l'affichage d'attribut structuré.

- Le cas échéant, [ajoutez une prise en charge de l'ajout d'informations à partir d'autres objets gérés](#) (page 49).

Remarque : La configuration de la prise en charge d'autres objets gérés a pour effet d'ajouter une fenêtre de recherche dans le tableau d'affichage d'attribut structuré, qui permet aux utilisateurs de rechercher et d'ajouter des informations stockées dans d'autres types d'objets gérés. Par exemple, vous pouvez autoriser des utilisateurs à sélectionner des rôles SAP à ajouter à un attribut structuré sur un profil d'utilisateur.

- Cliquez sur Appliquer, puis sur OK.

L'affichage d'attribut structuré est ajouté à la fenêtre de profil que vous avez modifiée.

Ajout d'autres objets gérés dans un affichage d'attribut structuré

Dans certains cas, vous pouvez ajouter d'autres objets gérés à un attribut structuré. Par exemple, un attribut structuré d'un profil d'utilisateur répertorie les rôles SAP, ainsi que des dates de début et de fin de l'utilisation de ces rôles.

Pour configurer la prise en charge de ce cas d'utilisation, ajoutez un tableau d'affichage d'attribut structuré comme décrit dans la section [Configuration d'un affichage d'attribut structuré](#) (page 46), puis configurez d'autres champs de recherche et de stockage d'informations sur un autre type d'objet géré dans l'attribut structuré.

Lorsque cette prise en charge est configurée, CA Identity Manager affiche une fenêtre de recherche qui permet aux utilisateurs de rechercher et de sélectionner des valeurs d'objet géré à ajouter à l'attribut structuré.

Pour ajouter des objets gérés à un affichage d'attribut structuré :

1. [Configurez un affichage d'attribut structuré](#) (page 46).
2. Remplissez les champs suivants en fonction de vos besoins.

Champ d'objet

Sélectionnez le champ contenant la référence à l'objet géré. Dans la plupart des cas, il s'agit de l'ID unique de l'objet géré.

Type d'objet

Sélectionnez le type d'objet contenant les valeurs à ajouter à l'attribut structuré.

Par exemple, pour ajouter des rôles SAP à un attribut structuré du profil d'utilisateur, sélectionnez l'objet Rôles SAP.

Attribut d'objet (facultatif)

Sélectionnez l'attribut de l'objet géré qui servira à renseigner le champ d'objet.

Cet attribut est nécessaire uniquement si le champ contenant la référence à l'objet géré n'est pas le nom unique de l'objet géré. Si ce champ n'est pas renseigné, le nom unique est utilisé.

Fenêtre de recherche

Spécifiez la fenêtre de recherche qui s'affiche lorsque l'utilisateur clique sur le bouton Ajouter pour ajouter d'autres valeurs à l'attribut structuré.

3. Cliquez sur Appliquer, puis sur OK.

Remplissage des options de champs

Plusieurs styles de champs offrent diverses options à l'utilisateur.

- Case à cocher à sélection multiple
- Liste déroulante
- Liste modifiable déroulante
- Sélection multiple
- Sélecteur d'options
- Sélecteur modifiable d'options

- Sélection unique avec bouton d'option
- Sélection unique

Par exemple, le champ Bureau peut contenir la liste de tous les bureaux d'une société. L'utilisateur peut sélectionner son propre bureau pour renseigner le champ.

CA Identity Manager offre les méthodes de remplissage des champs ci-après.

Liste simple

Permet d'entrer une liste d'options dans une zone de texte. CA Identity Manager utilise le texte que vous entrez comme option pour le champ.

Données des boîtes de sélection

Vous permet de configurer les options de champs à l'aide des données des boîtes de sélection.

JavaScript

Vous permet de spécifier le script Java qui fournit les options du champ.

Gestionnaires d'attributs logiques

Vous permet de spécifier un gestionnaire d'attributs logiques qui fournit les options du champ.

Informations complémentaires :

[Données des boîtes de sélection](#) (page 54)

Sélection d'une méthode de remplissage de champ

Dans CA Identity Manager, quatre méthodes permettent de remplir les options de champs.

- Listes simples
- Données des boîtes de sélection
- JavaScript
- Gestionnaire d'attributs logiques

Lorsque vous sélectionnez une méthode, songez aux critères suivants.

- Facilité d'implémentation
Certaines méthodes permettent de configurer des options de champs dans la boîte de dialogue Propriétés du champ lorsque vous configurez une fenêtre de profil. D'autres options nécessitent une configuration supplémentaire ou un code personnalisé.

- **Prise en charge des options dynamiques**
Certaines méthodes permettent de créer un code personnalisé pour remplir de façon dynamique les options de champs ou pour récupérer des options de champs d'une autre source telle qu'une base de données.
- **Prise en charge des champs dépendants**
Certaines méthodes permettent de configurer une dépendance entre deux champs dans une fenêtre de tâche. Par exemple, les options qui sont disponibles dans le champ Ville peuvent dépendre d'une option choisie par l'utilisateur dans le champ Etat.

Le tableau suivant récapitule les caractéristiques de chaque méthode de remplissage de champ.

Méthode	Description	Dynamique ?	Prise en charge de champs dépendants ?
Listes simples	Les administrateurs entrent des options statiques dans la boîte de dialogue Propriétés du champ.	Non	Non
Données des boîtes de sélection	Une liste statique d'options est importée dans une base de données à partir d'un fichier XML qui peut être généré de façon dynamique.	Oui. Les options disponibles dans les champs dépendants peuvent varier en fonction des valeurs sélectionnées.	Oui, mais uniquement pour les champs hiérarchiques.
JavaScript	Une fonction JavaScript fournit une liste dynamique d'options. Le script Java est configuré dans la boîte de dialogue Propriétés du champ. Ce script Java côté serveur peut accéder à toute API Java disponible sur le serveur d'applications hébergeant CA Identity Manager.	Oui	Non
Gestionnaire d'attributs logiques	Un gestionnaire d'attributs logiques Java personnalisé fournit une liste dynamique d'options. Un administrateur crée le gestionnaire d'attributs logiques à l'aide de l'API d'attribut logique CA Identity Manager, puis configure l'environnement CA Identity Manager pour l'utiliser. L'administrateur associe ensuite le champ à l'attribut logique.	Oui	Non

Utilisation de listes simples pour les options de champs

Vous pouvez spécifier une liste statique d'options pour les champs de la fenêtre de profil à l'aide du style Liste simple du Sélecteur d'options. Lorsque l'utilisateur sélectionne une ou plusieurs options (selon le style de champ), CA Identity Manager stocke cette valeur dans le magasin d'utilisateurs.

Pour utiliser une liste simple pour renseigner les options de champs :

1. [Modifiez une fenêtre de profil](#) (page 29).
2. Sélectionnez un champ à modifier ou ajoutez-en un.
3. Si vous ajoutez un champ, sélectionnez l'attribut qui lui est associé dans la zone de liste.
4. Sélectionnez l'un des styles suivants.
 - Case à cocher : sélection multiple
 - Liste déroulante
 - Liste modifiable déroulante
 - Sélection multiple
 - Sélecteur d'options
 - Sélecteur modifiable d'options
 - Sélection unique avec bouton d'option
 - Sélection unique

Les champs figurant dans la fenêtre Propriétés du champ varient en fonction du style sélectionné.

5. Sélectionnez Liste simple dans le champ Source des options de sélection.
Le champ Options de sélection apparaît.
6. Entrez les options du champ dans le champ Options de sélection.

Chaque option doit figurer sur une ligne distincte.

Pour que CA Identity Manager stocke une valeur dans un magasin d'utilisateurs différente de la valeur affichée dans la liste des options, spécifiez chaque option comme suit.

```
"storage-value;display-value"
```

7. Spécifiez l'une des valeurs suivantes dans le champ Conserver les options personnalisées.
 - Oui : les valeurs existantes qui ne correspondent pas à l'une des options valides sont conservées.
 - Non : l'utilisateur doit sélectionner une valeur dans la liste des options prédéfinies. Les valeurs qui ne correspondent pas à une valeur existante ne sont pas conservées.
8. Spécifiez des valeurs pour les autres champs obligatoires.
9. Cliquez sur Appliquer, puis sur OK.

CA Identity Manager enregistre les propriétés de champ actuelles.

Données des boîtes de sélection

Les administrateurs et les concepteurs de fenêtres qui peuvent modifier des fenêtres de tâches peuvent spécifier les options qui s'affichent dans les champs de tâches. Les utilisateurs sélectionnent une option pour remplir le champ. Les options de champ doivent permettre aux utilisateurs de fournir les données correctes et de limiter les réponses possibles.

Vous pouvez spécifier des options pour les types de champs suivants :

- Case à cocher à sélection multiple
- Liste déroulante
- Liste modifiable déroulante
- Sélection multiple
- Sélecteur d'options
- Sélecteur modifiable d'options
- Sélection unique avec bouton d'option
- Sélection unique

Vous pouvez spécifier des données personnalisées que vous souhaitez utiliser pour remplir des boîtes dans des fichiers XML. Par exemple, vous pouvez utiliser les fichiers XML de données de boîtes de sélection pour remplir des options dans une zone déroulante Ville ou Etat dans la tâche Créer un utilisateur.

Vous pouvez aussi utiliser les fichiers XML de données de boîtes de sélection pour configurer une dépendance entre les deux champs dans une fenêtre de tâche. Par exemple, les options qui sont disponibles dans le champ Ville peuvent dépendre d'une option choisie par l'utilisateur dans le champ Etat.

Remplissage de champs au moyen de données de boîtes de sélection

En tant qu'administrateur, vous pouvez utiliser les données de boîtes de sélection pour définir les données que vous voulez remplir dans les champs de tâche. Vous devez créer un fichier XML de données de boîtes de sélection qui contient les données que vous voulez remplir dans les champs de tâche et importer le fichier XML dans l'environnement CA Identity Manager. Les données importées sont utilisées comme source pour les champs de tâche pour lesquels vous voulez remplir des options. Lorsque vous modifiez une tâche d'utilisateur, configurez les propriétés du champ de tâche pour utiliser les données de boîtes de sélection pour remplir les options pour le champ de tâche sélectionné.

Remarque : Dans le fichier XML de données de boîtes de sélection, vous pouvez conserver les champs afin de remplir des données précises et de limiter les réponses possibles.

Vous pouvez configurer les champs de tâche suivants de sorte à utiliser les données de boîtes de sélection :

- Case à cocher à sélection multiple
- Liste déroulante
- Liste modifiable déroulante
- Sélection multiple
- Sélecteur d'options
- Sélecteur modifiable d'options

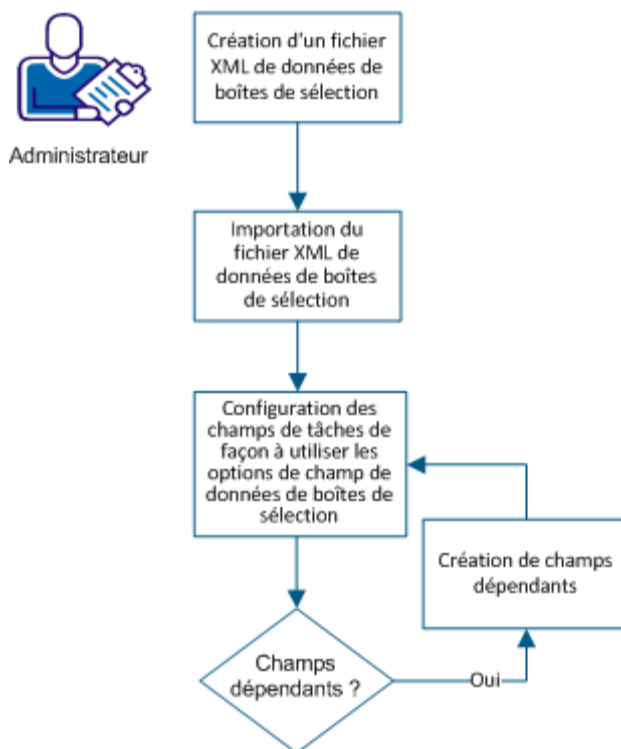
- Sélection unique avec bouton d'option
- Sélection unique

Vous pouvez spécifier des données personnalisées que vous souhaitez utiliser pour remplir des boîtes dans des fichiers XML. Par exemple, lorsque vous créez un utilisateur, vous pouvez utiliser des fichiers XML de données de boîtes de sélection pour remplir des options pour le menu déroulant Ville ou Etat.

Vous pouvez aussi utiliser les fichiers XML de données de boîtes de sélection pour configurer une dépendance entre les deux champs dans une fenêtre de tâche. Par exemple, les options qui sont disponibles dans le champ Ville peuvent dépendre d'une option choisie par l'utilisateur dans le champ Etat.

Le diagramme suivant représente le processus permettant de remplir les options des champs de tâche à l'aide de données de boîtes de sélection :

Procédure de remplissage des champs de tâches au moyen de données de boîtes de sélection



Procédez comme suit :

1. [Créez un fichier XML de données de boîtes de sélection.](#) (page 57)
2. [Importez le fichier XML de données de boîtes de sélection.](#) (page 60)

3. [Configurez les champs de tâche afin d'utiliser les données de boîtes de sélection](#) (page 64). S'il existe des champs dépendants, effectuez la tâche suivante :
 - [Créez des champs dépendants](#) (page 64).

Création d'un fichier XML de données de boîtes de sélection

Chaque fichier XML de données de boîtes de sélection contient des données que vous pouvez utiliser pour indiquer les options dans un contrôle de console d'utilisateur lors de la modification d'un profil. Vous pouvez remplir des options pour les champs de tâche dans une fenêtre de profil avec des éléments et des éléments enfants dans un fichier XML de données de boîtes de sélection.

Remarque : Les noms d'attribut doivent respecter la casse dans le fichier XML.

Procédez comme suit:

1. Créez un fichier texte avec une extension .xml à l'aide d'un éditeur XML ou de texte.
2. Ajoutez le code dans le fichier texte selon les options que vous voulez remplir dans le champ de tâche et enregistrez le fichier. Créez un fichier au format décrit ci-dessus.

Le fichier XML de données de boîtes de sélection est créé. Vous pouvez importer ce fichier XML dans l'environnement CA Identity Manager pour remplir les options des contrôles de la console d'utilisateur.

Exemple de création d'un fichier XML de données de boîtes de sélection

Cet exemple crée le fichier XML de données de boîtes de sélection qui remplit les noms d'états et les noms de villes lorsque le pays sélectionné est l'Australie ou le Royaume-Uni :

```
<nom lieux="places" displayName="places">
  <country name="AU" displayName="Australia">
    <state name="VIC" displayName="Victoria">
      <city name="MEL" displayName="Melbourne"/>
      <city name="GEEL" displayName="Geelong"/>
      <city name="BAL" displayName="Ballarat"/>
    </état>
    <state name="NSW" displayName="New South Wales">
      <city name="SYD" displayName="Sydney"/>
      <city name="NCL" displayName="Newcastle"/>
      <city name="WOD" displayName="Wodonga"/>
    </état>
    <state name="QLD" displayName="Queensland">
      <city name="BRIS" displayName="Brisbane"/>
      <city name="CNS" displayName="Cairns"/>
      <city name="TVL" displayName="Townsville"/>
    </état>
  </pays>
```

```
<country name="UK" displayName="UK">
  <state name="SU" displayName="Surrey">
    <city name="LON" displayName="London"/>
    <city name="READ" displayName="Reading"/>
  </état>
  <state name="WLS" displayName="Wales">
    <city name="CDF" displayName="Cardiff"/>
    <city name="SWN" displayName="Swansea"/>
  </état>
</pays>
</places>
```

Fichier XML de données de boîtes de sélection

Le fichier XML de données de boîtes de sélection est un ensemble en forme d'arborescence d'éléments et d'éléments enfants.

Le fichier XML de données de boîtes de sélection contient les éléments suivants :

Élément racine

Identifie le fichier XML de données de boîtes de sélection. Un fichier XML de données de boîtes de sélection inclut uniquement un élément racine. L'élément racine est un conteneur pour tous les éléments et les éléments enfants. Vous ne pouvez pas utiliser ces éléments pour remplir les champs.

Élément fournisseur

Spécifie les noeuds dans l'arborescence d'un fichier XML de données de boîtes de sélection. Ces éléments contiennent les options que vous pouvez utiliser de remplir les champs. L'élément de fournisseur ne contient pas d'élément parent. Par exemple, vous pouvez créer deux champs dépendants avec les options Melbourne et Victoria. Les éléments correspondants dans le fichier XML de données de boîtes de sélection doivent appartenir au même élément de fournisseur. Dans l'illustration ci-après, la ville Melbourne est dépendante de l'état Victoria. L'élément de fournisseur pour les deux options est Australie.

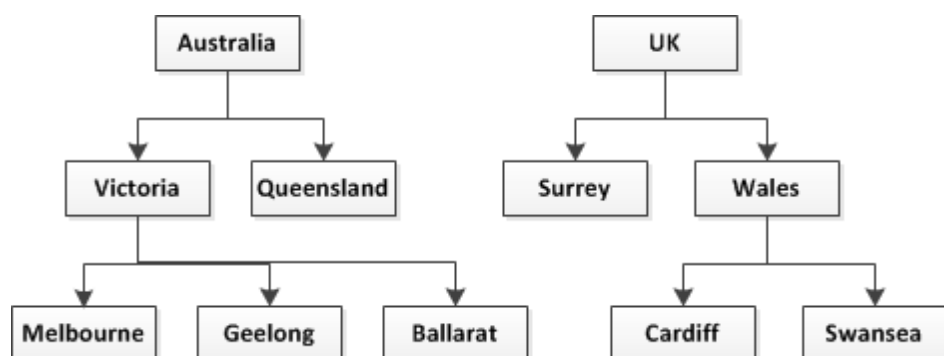
Éléments

Un élément XML dans le fichier XML de données de boîtes de sélection est identifié comme un élément. Un élément peut être un élément parent ou un élément enfant. Dans l'illustration suivante, Victoria est un élément parent de Melbourne. De même Victoria est un élément enfant d'Australie.

Éléments enfants

Tous les éléments XML qui sont contenus dans des éléments situés plus haut dans l'arborescence sont appelés des éléments enfants.

L'illustration suivante représente la structure de données de boîtes de sélection.



Chaque élément inclut les attributs suivants :

Nom d'affichage

Nom de l'élément qui est affiché dans la console d'utilisateur CA Identity Manager. Par exemple, Melbourne et Queensland sont les noms affichés.

Type

Identifie le type de ressource. Par exemple, le nom de l'état et le nom de la ville sont des éléments de type.

Importation du fichier XML de données de boîtes de sélection

Le fichier XML de données de boîtes de sélection inclut des données que CA Identity Manager utilise comme des options dans les champs de tâches sélectionnés dans les fenêtres de tâches. Vous devez importer le fichier XML de données de boîtes de sélection dans l'environnement CA Identity Manager pour les utiliser comme source pour les champs de tâches pour lesquels vous voulez spécifier des options.

Procédez comme suit:

1. Connectez-vous à la console d'utilisateur en tant qu'administrateur.
2. Sélectionnez une option :
 - Tâches, Système
 - Système
3. Sélectionnez Données des boîtes de sélection, Importer les données de boîtes de sélection.

La page Importer les données de boîtes de sélection apparaît.

4. Cliquez sur Créer un fournisseur.

La page Créer les données de boîtes de sélection apparaît.

5. Complétez les champs suivants :

nom

Nom unique du fichier XML de données des boîtes de sélection. CA Identity Manager valide l'unicité du nom identifiant.

Description

Description du fichier XML de données des boîtes de sélection.

Priorité

Indique la priorité du fichier XML de données de boîtes de sélection par rapport à d'autres fichiers XML de données de boîtes de sélection. La priorité devrait être numérique.

6. Cliquez sur Parcourir pour rechercher le fichier XML de données de boîtes de sélection, localisez-le, puis cliquez sur Créer.

Le fichier XML de données de boîtes de sélection est importé.

7. Cliquez sur Fermer.

Le fichier XML de données de boîtes de sélection récemment importé est affiché dans la fenêtre.

Configuration des champs de tâche afin d'utiliser les données de boîtes de sélection pour les options de champ

Vous devez configurer les champs (pour lesquels vous voulez remplir des options) dans la fenêtre de tâche, pour utiliser les données de boîtes de sélection en tant que source.

Procédez comme suit:

1. Dans la console d'utilisateur, sélectionnez l'une des options suivantes :
 - Rôles et tâches
 - Tâches, Rôles et tâches
2. Sélectionnez Tâches d'administration, Modifier la tâche d'administration.
3. Recherchez et sélectionnez la tâche d'administration à modifier.
CA Identity Manager affiche les onglets à configurer pour la tâche que vous avez sélectionnée.
4. Sélectionnez l'onglet Onglets, puis l'onglet Profil.
5. Cliquez sur Parcourir en regard du champ Fenêtre.
CA Identity Manager affiche la liste des fenêtres de profil existantes.
6. Sélectionnez la fenêtre de profil à modifier ou à copier, puis cliquez sur l'un des boutons suivants.
 - **Sélectionner**
Ajoute la fenêtre sélectionnée à l'onglet en cours de configuration.
 - **Modifier**
Ouvre une nouvelle fenêtre dans laquelle vous pouvez modifier les paramètres de la fenêtre sélectionnée, notamment les champs, les propriétés de champs et la présentation.
 - **Supprimer**
Supprime la fenêtre sélectionnée.
 - **Créer**
Ouvre une nouvelle fenêtre dans laquelle vous pouvez créer une fenêtre. La nouvelle fenêtre n'inclut aucun champ par défaut.
 - **Copier**
Crée une fenêtre à l'aide des paramètres d'une fenêtre existante. Pour créer une fenêtre basée sur une fenêtre existante, ajoutez un nouveau nom et une nouvelle balise à la fenêtre, puis modifiez les paramètres selon les besoins.
 - **Annuler**
Renvoie à la fenêtre de configuration Onglet.

Si vous avez sélectionné Modifier, Créer ou Copier, CA Identity Manager ouvre une nouvelle fenêtre dans laquelle vous pouvez créer ou modifier une fenêtre de profil.

7. Ajoutez ou sélectionnez un champ dans la fenêtre de profil, puis cliquez sur l'icône de flèche droite pour afficher les propriétés du champ.
8. Configurez les propriétés de champ de manière appropriée sur l'une des valeurs suivantes :
 - Case à cocher à sélection multiple
 - Liste déroulante
 - Liste modifiable déroulante
 - Sélection multiple
 - Sélecteur d'options
 - Sélecteur modifiable d'options
 - Sélection unique avec bouton d'option
 - Sélection unique

Le champ Source des options de sélection s'affiche.

9. Sélectionnez *l'une* des options suivantes :

Données des boîtes de sélection

Indique que les options pour le champ de tâche sont remplies à partir des données de boîtes de sélection. Si vous sélectionnez cette option, l'option Modifier s'affiche pour la fenêtre Options des boîtes de données de sélection.

La liste des éléments racines pour les données de boîtes de sélection s'affiche également.

- a. Cliquez sur Modifier.

La fenêtre Options de données de boîtes de sélection s'affiche. Elle vous permet de parcourir les données de boîtes de sélection importées.

- b. Cliquez sur un nom d'élément pour en afficher des informations sur les éléments enfants. Lorsque la liste d'éléments affichée représente la liste des options à utiliser pour le champ Profil, cliquez sur OK.

Les deux champs suivants permettent de filtrer les listes d'éléments étendues. Ces champs acceptent le caractère générique (*).

Filtre de nom enfant

Spécifie le nom de l'élément ou de l'élément enfant dans les données de boîtes de sélection.

Filtre de type enfant

Spécifie le type de l'élément ou de l'élément enfant dans un fichier XML de données de boîtes de sélection.

Remarque : Les valeurs que vous pouvez sélectionner dans ce champ sont remplies à partir du fichier XML de données de boîtes de sélection que vous avez importé dans CA Identity Manager.

- c. Cliquez sur Actualiser pour filtrer les résultats.

Dépend de la valeur d'un autre champ

Spécifie que le champ est rempli selon les valeurs sélectionnées dans un autre champ. Si vous avez sélectionné cette option, créez des champs dépendants.

10. Sélectionnez un champ existant sous la forme d'un champ Source d'options.
11. Sélectionnez une valeur dans le champ Conserver les options personnalisées.
12. Sélectionnez une valeur dans le champ Valider lors de la modification.
13. Cliquez sur Appliquer, puis OK pour enregistrer vos modifications.

Les champs configurés s'affichent dans l'onglet de profil de la tâche d'administration sélectionnée. Les contrôles basés sur la sélection, configurés pour utiliser les données de boîtes de sélection comme source, sont remplis avec les valeurs provenant du fichier XML de données de boîtes de sélection.

Création de champs dépendants

Lorsque chaque option dans un champ de tâche correspond à un élément ou à un élément enfant, créez une dépendance entre ces champs dans la fenêtre de tâche CA Identity Manager.

Procédez comme suit:

1. Créez un champ qui utilise le fichier XML de données de boîtes de sélection pour renseigner les options.

Par exemple, vous pouvez créer un champ appelé Etat qui utilise le style Liste déroulante et le fichier XML de données de boîtes de sélection pour les options. Chaque option du champ Etat correspond à un élément ou à un élément enfant dans le fichier XML de données de boîtes de sélection. Chaque élément du champ Etat dispose d'éléments enfants.

2. Créez un autre champ qui est renseigné en fonction de l'option sélectionnée à l'étape 1.

Par exemple, vous pouvez créer un champ appelé Ville, associé à un style Liste déroulante et dépendant du champ Etat.

Après avoir créé les champs dépendants, vous devez les configurer pour utiliser des données de boîtes de sélection. Les champs configurés s'affichent dans l'onglet de profil de la tâche d'administration sélectionnée. Les contrôles basés sur la sélection, configurés pour utiliser les données de boîtes de sélection comme source, sont remplis avec les valeurs provenant du fichier XML de données de boîtes de sélection.

Utilisation des données de boîtes de sélection pour les options de champs

Configurez des champs dans une fenêtre de tâche afin d'utiliser les données de boîtes de sélection comme source de sélection des champs d'options.

Pour configurer des champs afin d'utiliser les données de boîtes de sélection :

1. [Modifiez une fenêtre de profil](#) (page 29).
2. Ajoutez ou sélectionnez un champ dans la fenêtre de profil, puis cliquez sur l'icône flèche droite pour afficher les propriétés du champ.
3. Renseignez les propriétés du champ que vous avez ajouté. Définissez le Style sur l'une des valeurs ci-après.
 - Case à cocher à sélection multiple
 - Liste déroulante
 - Liste modifiable déroulante
 - Sélection multiple
 - Sélecteur d'options

- Sélecteur modifiable d'options
- Sélection unique avec bouton d'option
- Sélection unique

Le champ Source des options de sélection s'affiche.

4. Sélectionnez l'une des options suivantes pour le champ Source des options de sélection.

Données des boîtes de sélection

Spécifie que le champ est renseigné à l'aide des données de boîtes de sélection. Si vous sélectionnez cette option, Modifier pour les données de boîte de sélection pour les options s'affiche.

La liste des éléments racines pour les données de boîtes de sélection s'affiche également.

Cliquez sur Modifier pour afficher une page Options de données de boîtes de sélection qui vous permet de parcourir les données de boîtes de sélection importées. Cliquez sur un nom d'élément pour en afficher des informations sur les éléments enfants. Lorsque la liste d'éléments affichée représente la liste des options à utiliser pour le champ Profil, cliquez sur OK.

Les deux champs suivants permettent de filtrer les listes d'éléments volumineuses. Ces champs acceptent le caractère générique (*). Cliquez sur Actualiser pour filtrer les résultats.

Filtre de nom enfant

Identifie le nom de l'élément ou de l'élément enfant dans les données de boîtes de sélection.

Filtre de type enfant

Identifie le type de l'élément ou de l'élément enfant dans un fichier XML de données de boîtes de sélection.

Pour plus d'informations sur les noms et les types d'éléments, reportez-vous à la rubrique Fichier XML de données de boîtes de sélection.

Remarque : Les valeurs que vous pouvez sélectionner dans ce champ sont remplies à partir du fichier XML de données de boîtes de sélection que vous avez importé dans CA Identity Manager.

Dépend de la valeur d'un autre champ

Spécifie que le champ est rempli selon les valeurs sélectionnées dans un autre champ. Si vous avez sélectionné cette option, voir la section [Création de champs dépendants à l'aide de données de boîtes de sélection](#) (page 66).

Sélectionnez un champ existant sous la forme d'un champ Source d'options.

5. Sélectionnez l'une des valeurs pour le champ Conserver les options personnalisées.

6. Complétez les autres propriétés de champs nécessaires et cliquez sur Appliquer.
7. Cliquez sur OK pour enregistrer vos modifications.

Les champs que vous avez configurés apparaissent à l'utilisateur dans l'onglet Profil de la tâche d'administration sélectionnée. Les contrôles basés sur la sélection, configurés pour utiliser les données de boîtes de sélection comme source, sont remplis avec les valeurs provenant du fichier XML de données de boîtes de sélection.

Création de champs dépendants à l'aide de données des boîtes de sélection

Vous pouvez créer une dépendance entre deux champs sur une fenêtre de tâche CA Identity Manager. Pour créer une dépendance entre deux champs, respectez les étapes décrites par le processus suivant :

1. Créez un champ qui utilise des données de boîtes de sélection pour renseigner les options.

Par exemple, vous pouvez créer un champ appelé Etat qui utilise le style Liste déroulante et les données de boîtes de sélection pour les options. Chaque option du champ Etat correspond à un élément ou à un élément enfant dans les données de boîtes de sélection. Chaque élément du champ Etat dispose d'éléments enfants.
2. Créez un autre champ qui est renseigné en fonction de l'option sélectionnée à l'étape 1.

Par exemple, vous pouvez créer un champ appelé Ville, associé à un style Liste déroulante et dépendant du champ Etat.

Utilisation du script Java pour les options de champs

Pour spécifier les options qui s'affichent dans les champs d'une fenêtre de profil, générez un script Java personnalisé.

Pour utiliser le script Java pour renseigner les options de champs :

1. [Modifiez une fenêtre de profil](#) (page 29).
2. Sélectionnez un champ à modifier ou ajoutez-en un.
3. Si vous ajoutez un champ, sélectionnez l'attribut qui lui est associé dans la zone de liste.
4. Sélectionnez l'un des styles suivants.
 - Case à cocher : sélection multiple
 - Liste déroulante
 - Liste modifiable déroulante
 - Sélection multiple

- Sélecteur d'options
- Sélecteur modifiable d'options
- Sélection unique avec bouton d'option
- Sélection unique

Les champs figurant dans la fenêtre Propriétés du champ varient en fonction du style sélectionné.

5. Sélectionnez JavaScript dans le champ Source des options de sélection.

Le champ Options de sélection (JavaScript) apparaît.

6. Entrez un script Java pour fournir les options de champs dans le champ Options de sélection (JavaScript).

Ce script Java doit contenir une fonction avec la signature "fonction getOptions(FieldContext)" et renvoyer une chaîne d'options délimitées par des barres verticales. Si les valeurs d'affichage et de stockage de l'option diffèrent, entrez-les sous la forme : "valeur-stockage;valeur-affichage".

comme les exemples ci-dessous.

```
function getOptions(FieldContext) {  
    return "1;one|2;two|3;three|4;four";  
}
```

7. Spécifiez l'une des valeurs suivantes dans le champ Conserver les options personnalisées.
 - Oui : les valeurs existantes qui ne correspondent pas à l'une des options valides sont conservées.
 - Non : l'utilisateur doit sélectionner une valeur dans la liste des options prédéfinies. Les valeurs qui ne correspondent pas à une valeur existante ne sont pas conservées.

8. Spécifiez des valeurs pour les autres champs obligatoires.

Remarque : Pour plus d'informations sur les champs obligatoires, reportez-vous à l'Aide en ligne de la console d'utilisateur.

9. Cliquez sur Appliquer, puis sur OK.

CA Identity Manager enregistre les propriétés de champ actuelles.

Utilisation des gestionnaires d'attributs logiques pour les options de champs

Vous pouvez utiliser un attribut logique pour renseigner une liste d'options de champs. Les valeurs d'attributs logiques (dans ce cas, les options) ne sont pas directement associées au magasin d'utilisateurs, ni enregistrées dans celui-ci. Les valeurs d'attributs logiques sont présentées dans un champ Fenêtre de profil. Lorsqu'un utilisateur sélectionne une option et soumet une tâche, la valeur sélectionnée est traitée par le gestionnaire d'attributs logiques, qui la stocke dans l'attribut physique associé à l'attribut logique.

Remarque : CA Identity Manager inclut un exemple de gestionnaire d'attributs logiques appelé Sélecteur d'état qui permet de créer un gestionnaire d'attributs logiques qui renseigne les options de champs. Le dossier d'exemples StateSelector est installé sous `samples\LogicalAttributes` dans les outils d'administration. Les outils d'administration sont installés aux emplacements par défaut ci-après.

- **Windows** : `<chemin_d'installation>\tools`
- **UNIX** : `<chemin_d'installation2>/tools`

Pour plus d'informations sur les exemples, reportez-vous au fichier `readme.txt` du répertoire `StateSelector`.

Pour utiliser une liste simple pour renseigner les options de champs :

1. Créez un gestionnaire d'attributs logiques.

Remarque : l'API d'attribut logique permet d'enregistrer un gestionnaire d'attributs logiques. Pour plus d'informations, reportez-vous au *manuel de programmation Java (en anglais)*.

2. Dans la console d'utilisateur CA Identity Manager, [modifiez une fenêtre de profil](#) (page 29).
3. Ajoutez un nouveau champ.
4. Sélectionnez l'attribut logique associé au gestionnaire d'attributs logiques que vous avez créé.

Remarque : Les attributs logiques sont signalés par un caractère barre verticale (|) de début ou de fin.

5. Sélectionnez l'un des styles suivants.
 - Case à cocher : sélection multiple
 - Liste déroulante
 - Liste modifiable déroulante
 - Sélection multiple
 - Sélecteur d'options
 - Sélecteur modifiable d'options

- Sélection unique avec bouton d'option
- Sélection unique

Les champs figurant dans la fenêtre Propriétés du champ varient en fonction du style sélectionné.

6. Sélectionnez Aucun(e) dans le champ Source des options de sélection.
Le champ Options de sélection apparaît.
7. Spécifiez l'une des valeurs suivantes dans le champ Conserver les options personnalisées.
 - Oui : les valeurs existantes qui ne correspondent pas à l'une des options valides sont conservées.
 - Non : l'utilisateur doit sélectionner une valeur dans la liste des options prédéfinies. Les valeurs qui ne correspondent pas à une valeur existante ne sont pas conservées.
8. Spécifiez des valeurs pour les autres champs obligatoires.
Remarque : Pour plus d'informations sur les champs obligatoires, reportez-vous à l'Aide en ligne de la console d'utilisateur.
9. Cliquez sur Appliquer, puis sur OK.

CA Identity Manager enregistre les propriétés de champ actuelles.

Renseignement dynamique du champ Organisation

Si le magasin d'utilisateurs géré par Identity Manager inclut des organisations, la tâche Créer un utilisateur par défaut comporte un champ Organisation. Un administrateur doit rechercher et sélectionner l'organisation appropriée avant de créer un profil d'utilisateur.

Pour simplifier la tâche Créer un utilisateur, vous pouvez configurer Identity Manager afin de renseigner le champ Organisation de manière dynamique, en fonction de l'administrateur exécutant la tâche. Dans ce cas, l'administrateur n'a pas besoin de spécifier d'organisation. L'utilisateur est créé dans l'organisation où existe le profil de l'administrateur. Par exemple, si un administrateur, dont le profil existe dans l'organisation Employés, crée un profil d'utilisateur pour un nouvel employé, Identity Manager crée le nouveau profil dans l'organisation Employés. Si un administrateur dans l'organisation Fournisseurs utilise la même tâche Créer un utilisateur, le profil du nouvel utilisateur que le second administrateur crée existe dans l'organisation Fournisseurs.

Configuration d'un champ Organisation dynamique

Lorsque vous configurez un champ Organisation dynamique pour la tâche Créer un utilisateur, CA Identity Manager crée des utilisateurs dans l'organisation contenant le profil de l'administrateur qui les crée.

Configuration d'un champ Organisation dynamique

1. Dans la console d'utilisateur, sélectionnez Rôles et Tâches, Tâches d'administration, puis Modifier la tâche d'administration.
2. Recherchez et sélectionnez la tâche Créer un utilisateur.
3. Dans l'onglet Onglets, cliquez sur l'icône Modifier pour modifier l'onglet Profil.
4. Dans le champ Fenêtre, cliquez sur Parcourir pour afficher la liste des fenêtres à modifier.
5. Sélectionnez la fenêtre Créer un profil d'utilisateur et cliquez sur Modifier.
6. Localisez l'organisation et cliquez sur l'icône Modifier pour modifier les propriétés de l'organisation.
7. Définissez Style sur Masqué.
8. Dans le champ Script Java par défaut, entrez les éléments ci-après.

```
function defaultValue(FieldContext)
{
return FieldContext.getAdministrator().getOrg(null).getUniqueName();
}
```

9. Cliquez sur Appliquer.
10. Cliquez sur la flèche vers la gauche située en regard de Propriétés du champ pour revenir à la fenêtre.

Modification dynamique des propriétés d'affichage des champs

CA Identity Manager peut définir certaines propriétés d'affichage des champs selon la valeur des autres champs de la fenêtre de profil. Le script Java vous permet de masquer, d'afficher, d'activer ou de désactiver un champ. Par exemple, il permet d'afficher un champ Agence si le type d'employé est défini sur Temporaire. Si le type d'employé est défini sur Temps plein ou Temps partiel, le champ Agence est masqué.

Entrez le script Java dans les champs Script Java d'initialisation ou Script Java de validation dans la boîte de dialogue Propriétés du champ dans la définition de la fenêtre de profil. Les méthodes qui permettent de contrôler l'affichage d'un champ sont disponibles dans la classe FieldContext des méthodes init et validate.

Par exemple, pour contrôler l'affichage du champ Agence décrit ci-dessus, entrez le script Java suivant dans le champ Script Java de validation dans la boîte de dialogue Propriétés du champ du champ Type d'employé, car les modifications apportées à ce dernier contrôlent l'affichage du champ Agence :

```
function validate(FieldContext, attributeValue, changedValue, errorMessage) {  
    if (attributeValue == "Temporaire") {  
        FieldContext.showField("Agence");  
    }  
    else {  
        FieldContext.hideField("Agence");  
    }  
    return true;  
}
```

Pour vous assurer que le script Java est déclenché lorsque la valeur du champ change, définissez le champ Valider lors de la modification sur Oui.

Configuration des propriétés d'affichage du champ dynamique

Vous pouvez configurer CA Identity Manager de manière à masquer, afficher, activer ou désactiver un champ d'une fenêtre de profil en fonction de la valeur d'un autre champ de cette même fenêtre.

Pour configurer les propriétés d'affichage du champ dynamique :

1. [Modifiez la fenêtre de profil](#) (page 29).
CA Identity Manager affiche la liste des champs configurés pour la fenêtre.
2. Le cas échéant, ajoutez les champs pour lesquels vous configurez des propriétés de champ dynamique.
3. Cliquez sur l'icône Modifier située en regard du nom de champ pour modifier celui-ci.
CA Identity Manager affiche la boîte de dialogue Propriétés du champ.

- Entrez le code JavaScript dans le champ JavaScript de validation à l'aide de la méthode suivante.

```
function validate(FieldContext, attributeValue, changedValue, errorMessage) {
```

La classe FieldContext inclut les méthodes suivantes pour l'affichage, le masquage, l'activation et la désactivation d'un champ.

public void hide();

Masque le champ.

public void show();

Affiche le champ.

public void hideField(String attrName);

Masque le champ actuel.

public void showField(String attrName);

Affiche le champ actuel.

public void disable();

Désactive le champ actuel.

public void enable();

Active le champ actuel.

public void disableField(String attrName);

Désactive un champ pour un attribut spécifique.

public void enableField(String attrName);

Active un champ pour un attribut spécifique.

- Cliquez sur Appliquer, puis sur OK.

Attributs logiques définis par fenêtre

Les attributs logiques définis par fenêtre sont des champs d'un onglet Profil déterminés localement pour la tâche actuelle. Vous pouvez utiliser ces attributs logiques définis par fenêtre pour manipuler des objets dans une fenêtre de tâche ou *modifier* des attributs physiques stockés dans le référentiel d'utilisateurs.

Les attributs logiques définis par fenêtre sont définis, initialisés, validés, renseignés et implémentés à l'aide de JavaScript.

Par exemple, si vous disposez de 3 attributs physiques qui ont stocké une date (mois, jour, année), mais que vous voulez présenter à l'utilisateur un seul champ de saisie de date, vous pouvez configurer un attribut logique défini par fenêtre pour le champ Date. Lorsque l'utilisateur a entré une date, vous pouvez configurer le code JavaScript de validation pour décomposer la date en valeurs de mois, de jour et d'année et les définir en attributs physiques (qui seront probablement masqués à l'écran).

Remarque : Les attributs compris entre "|" sont identifiés comme attributs logiques définis par fenêtre.

Les attributs logiques définis par fenêtre sont utiles pour créer des tâches génériques qui ne sont liées à aucun objet principal. Dans ce cas, vous créez les champs dans l'onglet Profil en n'utilisant que des attributs logiques définis par fenêtre. Vous ne pouvez pas spécifier d'attributs logiques.

Ajout d'attributs logiques définis par fenêtre

N'importe quel champ d'une tâche de profil peut être défini comme attribut logique défini par fenêtre. Vous pouvez utiliser ces attributs logiques définis par fenêtre pour manipuler des objets localement selon la portée de cette fenêtre Profil ou modifier des attributs physiques dans le magasin d'objets. Par exemple, les attributs logiques définis par fenêtre permettent de capturer une note ou un avertissement d'une fenêtre de profil ou de traiter une valeur fournie par l'utilisateur avant son stockage dans l'attribut physique.

Pour définir des champs en tant qu'attributs logiques définis par fenêtre :

1. [Modifiez la fenêtre Profil](#) (page 29) pour ajouter ou modifier des champs afin d'utiliser des attributs logiques définis par fenêtre.
2. Créez ou mettez à jour des propriétés de champs avec les valeurs d'attributs logiques définis par fenêtre :

Nom de l'attribut

Sélectionnez (Attributs logiques de fenêtre) dans le champ Nom de l'attribut.

|Nom de l'attribut|

Identifie le nom d'attribut du champ. Il peut s'agir de toute valeur de votre choix.

Valeurs multiples

Indique que l'attribut logique défini par fenêtre comporte plusieurs valeurs.

Remarque : Par défaut, cette option est désactivée. Si ce champ est désactivé, l'attribut comporte une seule valeur.

Nom

Entrez le nom d'affichage de l'attribut logique défini par fenêtre.

Remarque : Si l'attribut logique défini par fenêtre porte le même nom qu'un gestionnaire d'attributs logiques, il a priorité par rapport au gestionnaire d'attributs logiques.

3. Spécifiez toutes les [propriétés de champs](#) (page 32) nécessaires.

Attributs logiques définis par fenêtre dans l'onglet Afficher les tâches soumises

Lorsque vous soumettez une tâche contenant des attributs logiques définis par fenêtre, les valeurs d'origine et mises à jour de ces attributs sont affichées dans la fenêtre Détails de la tâche de l'onglet Afficher les tâches soumises.

Composants supplémentaires d'une fenêtre de profil

Outre des champs, une fenêtre de profil peut inclure un ou plusieurs des composants suivants.

- Séparateurs de page
- Images
- Fichiers joints
- Affichage de l'historique
- Texte HTML personnalisé
- Liens ou boutons permettant de lancer des tâches

Options de l'attribut Séparateur

Lorsque vous sélectionnez Séparateur dans le champ Attribut de la boîte de dialogue Propriétés du champ, vous pouvez ajouter des composants supplémentaires à la fenêtre de profil. L'attribut Séparateur est associé aux options de style suivantes.

Binaire (pour les annuaires d'utilisateurs LDAP uniquement)

Permet d'ajouter un fichier binaire (par exemple, un certificat ou un autre document) à la fenêtre Profil de l'utilisateur.

HTML

Affiche du texte HTML dans une fenêtre Profil.

Affichage de l'historique

Affiche un tableau en lecture seule contenant des détails des entrées d'historique précédentes dans l'ordre chronologique.

Les entrées d'historique sont des annotations que vous pouvez ajouter à une tâche soumise. Vous pouvez les ajouter lorsque la tâche parcourt le flux de travaux et les afficher à l'aide de la tâche Afficher les tâches soumises.

Editeur d'historique

Affiche une zone de texte permettant de saisir de nouvelles entrées d'historique, ainsi qu'un bouton facultatif permettant de soumettre la nouvelle entrée.

Section de page

Permet de diviser la fenêtre Profil en plusieurs sections, qui peuvent ne pas présenter le même nombre de colonnes que les autres sections de page de la même fenêtre.

Par exemple, le style Section de page permet de créer une fenêtre Profil comportant une section de page à une seule colonne et une autre section de page à deux colonnes.

Binaire (pour les annuaires d'utilisateurs LDAP uniquement)

Permet d'ajouter une image à une fenêtre Profil de l'utilisateur.

Espace

Ajoute un espace vide à la fenêtre pour séparer visuellement un ensemble de champs.

Tâche

Ajoute un lien ou un bouton menant à une tâche différente dans l'onglet Profil.

Ajout d'un attribut binaire ou d'une image à une fenêtre Profil

Vous pouvez configurer CA Identity Manager pour inclure un fichier binaire ou afficher une image dans une fenêtre de profil d'utilisateur. Par exemple, vous pouvez configurer une fenêtre de profil d'utilisateur pour permettre aux utilisateurs d'attacher un document (par exemple, un certificat) à la fenêtre de profil ou d'afficher une photographie numérique de l'utilisateur géré.

Remarque : Cette fonctionnalité est disponible uniquement pour les fenêtres de profil d'utilisateur. Le magasin d'utilisateurs doit être un annuaire LDAP et l'attribut binaire ou l'image doit être stocké dans l'attribut défini dans le fichier de configuration d'annuaire (directory.xml).

Ajout d'un attribut binaire ou d'une image à une fenêtre Profil

1. [Modifiez la fenêtre de profil](#) (page 29).
2. Sélectionnez le champ situé sous la ligne où vous souhaitez ajouter l'image, puis cliquez sur le bouton Ajouter pour ajouter une ligne comportant un champ au-dessus de la ligne que vous avez sélectionnée.

CA Identity Manager ajoute un nouveau champ au-dessus du champ que vous avez sélectionné.
3. Cliquez sur l'icône Modifier pour modifier le nouveau champ.

La boîte de dialogue Propriétés du champ s'ouvre.
4. Sélectionnez l'attribut (Séparateur) dans le champ Nom de l'attribut.
5. Sélectionnez l'une des options suivantes dans le champ Style :
 - Binaire
 - ImageCA Identity Manager affiche de nouveaux champs de configuration dans la boîte de dialogue Propriétés du champ.

6. Remplissez les champs suivants selon les besoins :

■ **Nom**

L'étiquette que vous voulez pour ce champ dans la fenêtre de profil.

■ **Autorisation**

Niveau de droits du champ

Remarque : Si un champ est requis par le magasin d'utilisateurs, choisissez un paramètre Obligatoire. Les champs obligatoires sont signalés à l'écran par un point rouge.

– **Lire**

Un administrateur peut afficher le champ, mais pas le modifier.

– **Lecture/écriture**

Un administrateur peut voir la valeur actuelle du champ, le cas échéant, et entrer une valeur pour le champ.

– **Lecture/écriture requises**

Champ obligatoire, fonctionnant comme le paramètre Lecture/écriture.

– **Ecrire une fois**

Un administrateur ne peut pas voir la valeur actuelle du champ, le cas échéant, mais peut entrer une valeur.

Par exemple, un administrateur peut changer le mot de passe d'un utilisateur, mais ne peut pas voir le mot de passe actuel de l'utilisateur.

– **Ecriture requise**

Champ obligatoire, fonctionnant comme le paramètre Ecriture.

■ **Etendue de l'étiquette**

Nombre de colonnes que l'étiquette englobe.

■ **Etendue du champ**

Nombre de colonnes que le champ englobe (étiquette non comprise)

■ **Classe CSS**

Classe CSS (Cascading Style Sheet) qui contrôle la présentation de ce champ.

Remarque : Ce champ n'est disponible que pour les attributs d'images.

- **Style CSS**

Propriétés et style de champ définis à l'aide de règles CSS.

Vous pouvez utiliser ce champ pour définir la largeur d'un champ. Par exemple, pour définir la largeur du champ où l'image sera affichée à 300 pixels, spécifiez ce qui suit dans le champ Style CSS :

Style CSS

Remarque : Ce champ n'est disponible que pour les attributs d'images.

- **Nom de l'attribut binaire**

Spécifie le nom de l'attribut qui stocke l'image. Cet attribut doit exister dans le magasin d'utilisateurs, mais ne doit pas être défini dans le fichier de configuration d'annuaire (directory.xml).

- **Type de contenu**

Spécifie le type MIME d'image qui sera affiché. Par exemple, pour un fichier binaire, vous pouvez spécifier application/octet-stream. Pour une image, vous pouvez spécifier image/gif ou image/jpg.

- **Autre contenu**

Spécifie l'URI d'une autre image que CA CA Identity Manager affiche lorsqu'une image n'est pas disponible pour un certain utilisateur.

CA Identity Manager inclut une image par défaut affichée quand aucune autre image n'est disponible ; cependant, vous pouvez utiliser ce champ pour remplacer l'image par défaut.

L'image par défaut figure à l'emplacement

iam_im.ear\user_console.war\ui\images\user_photo_default.jpg

iam_im.ear correspond à l'emplacement déployé de CA CA Identity Manager sur le serveur d'applications.

Spécifiez le chemin d'une autre image, qui comporte le même type de contenu que l'attribut, par rapport à *user_console.war*.

Remarque : Ce champ n'est disponible que si vous sélectionnez le style Image.

7. Cliquez sur Appliquer, puis sur OK pour enregistrer vos modifications.

Ajout de sections de pages

Les sections de pages séparent visuellement les champs d'une fenêtre de profil en ajoutant un en-tête et en appliquant un nombre de colonnes différent à une partie d'une fenêtre de profil. La présentation de section de page s'applique jusqu'à la définition d'une autre section de page pour la fenêtre Profil.

L'exemple d'onglet Profil suivant présente deux sections de pages.

The screenshot shows a web interface for modifying a contractor's profile. The title is "Modify Contractor: jhansen". There are five tabs: "Profile", "Access Roles", "Admin Roles", "Provisioning Roles", and "Groups". The "Profile" tab is active. Below the tabs, there is a legend: "• = Required". The profile information is organized into two sections. The first section contains fields for Organization (Employee), User ID (jhansen), First Name (Julia), Last Name (Hansen), and Email. The second section, titled "Contractor Information", contains fields for Employee Number, Department, Employee Type, Manager, Office, and Start Date (6/1/2012).

Pour ajouter une section de page :

1. Modifiez la fenêtre de profil.
2. Sélectionnez le premier champ qui s'affiche dans la section de page que vous créez, puis ajoutez une ligne comportant un champ avant le champ sélectionné.
CA Identity Manager ajoute un nouveau champ au-dessus du champ que vous avez sélectionné. Ce champ indique l'endroit où commence la section de page.
3. Cliquez sur l'icône flèche droite pour modifier le nouveau champ.
La boîte de dialogue Propriétés du champ s'ouvre.
4. Sélectionnez l'attribut (Séparateur) dans le champ Nom de l'attribut.
5. Sélectionnez Section de page dans le champ Style.
CA Identity Manager ajoute d'autres champs à la boîte de dialogue Propriétés du champ.

6. Spécifiez les valeurs des champs suivants :

■ **Colonnes de mise en page**

Spécifie le nombre de colonnes que contient la section de page.

Une fois le nombre de colonnes spécifié, cliquez sur l'icône représentant une flèche vers la droite pour appliquer les modifications. Une fois les modifications appliquées, des champs supplémentaires apparaissent permettant de spécifier la largeur de chaque colonne.

Remarque : Chaque champ comprend deux colonnes : une colonne pour l'étiquette du champ et une autre pour les valeurs. Pour afficher deux champs sur une seule ligne, ajoutez quatre colonnes.

■ **En-tête du tableau**

Spécifie le texte qui apparaît au-dessus de la section de page en tant qu'en-tête.

■ **Texte de l'infobulle**

Spécifie le texte affiché sous le séparateur de page.

Vous pouvez utiliser ce champ pour indiquer une description sur la section de page ou pour fournir des instructions sur la façon dont les champs de la section de page doivent être renseignés.

■ **Activer les boutons Afficher/Masquer**

Détermine si l'utilisateur peut ou non masquer une section de page. Lorsque cette option est sélectionnée, CA Identity Manager ajoute une flèche dans l'en-tête de tableau qui permet d'afficher ou de masquer une section de page.

■ **Masquer par défaut**

Indique qu'une section de page est masquée par défaut.

Si l'utilisateur doit pouvoir utiliser la section de page, lorsque vous sélectionnez l'option Masquer par défaut, assurez-vous de sélectionner l'option Activer les boutons Afficher/Masquer pour que l'utilisateur puisse afficher la section de page.

■ **Spécifier la largeur des colonnes**

Détermine la largeur de chaque colonne dans la section de page. Chaque largeur de colonne est spécifiée en tant que pourcentage de la fenêtre Profil.

Par exemple, pour ajouter quatre colonnes de largeur égale, définissez chaque largeur de colonne sur 25 %.

Remarque : La largeur totale des colonnes doit être de 100 %.

7. Cliquez sur OK pour enregistrer les modifications apportées aux propriétés de champs.

8. Cliquez sur Sélectionner pour choisir la fenêtre que vous avez modifiée ou copiée.
9. Cliquez sur OK, puis sur Soumettre pour enregistrer les modifications apportées à la tâche.

Ajout d'une tâche imbriquée

Une tâche imbriquée est une tâche d'administration pouvant être ouverte à partir de l'onglet Profil d'une autre tâche. L'utilisateur de la première tâche ouvre la tâche imbriquée en cliquant sur un lien ou un bouton. Par exemple, vous pouvez ajouter un bouton Supprimer un utilisateur à la tâche Modifier l'utilisateur. Si le compte d'utilisateur n'est plus valide, un administrateur peut cliquer sur le bouton Supprimer un utilisateur pour supprimer le compte sans devoir retourner au volet de navigation pour sélectionner une nouvelle tâche.

Remarque : La tâche imbriquée n'apparaît pas si l'administrateur ne dispose pas des autorisations nécessaires pour y accéder.

Ajout d'une tâche imbriquée

1. [Modifiez la fenêtre de profil](#) (page 29).
2. Sélectionnez le champ situé sous la ligne où vous souhaitez ajouter l'image, puis cliquez sur le bouton Ajouter pour ajouter une ligne comportant un champ au-dessus de la ligne que vous avez sélectionnée.
Identity Manager ajoute un nouveau champ au-dessus du champ que vous avez sélectionné.
3. Cliquez sur l'icône Modifier pour modifier le nouveau champ.
La boîte de dialogue Propriétés du champ s'ouvre.
4. Sélectionnez l'attribut (Séparateur) dans le champ Nom de l'attribut.
5. Sélectionnez Tâche dans le champ Style.
Identity Manager affiche de nouveaux champs de configuration dans la boîte de dialogue Propriétés du champ.
6. Remplissez les champs suivants selon les besoins :
 - **Etendue du champ**
Nombre de colonnes que le champ englobe (étiquette non comprise)
 - **Tâche par défaut**
Spécifie la tâche ajoutée à la tâche existante.

- **Substituer le nom de la tâche**

Spécifie le nom du lien ou du bouton de tâche allant apparaître dans la fenêtre Profil de la tâche active.

- **Lien de tâche**

Détermine si la tâche imbriquée apparaît en tant que lien ou bouton.

- **Utiliser l'objet actuel comme sujet de la tâche**

Lorsque cette option est activée, CA Identity Manager utilise le sujet de la tâche active en tant que sujet de la tâche. Par exemple, supposons que la tâche Modifier un utilisateur inclue un lien vers la tâche Supprimer un utilisateur. Un administrateur utilise la tâche Modifier un utilisateur pour modifier le profil de John Smith. L'administrateur, ayant décidé que le profil de John Smith n'est plus nécessaire, utilise le lien Supprimer un utilisateur pour ouvrir la tâche Supprimer un utilisateur. Lorsque la tâche s'ouvre, Identity Manager demande à l'administrateur s'il souhaite supprimer le profil de John Smith. L'administrateur n'a pas besoin de rechercher le profil à supprimer.

- **Comportement de la tâche**

Détermine le mode d'ouverture de la tâche par Identity Manager.

- **Remplacer la tâche active**

Ouvre une nouvelle tâche avant que la tâche active soit accomplie. La nouvelle tâche remplace la tâche précédente. Lorsque la tâche imbriquée se termine, l'utilisateur n'est pas ramené à la tâche d'origine.

- **Imbriquer la tâche dans la tâche active**

Soumet la nouvelle tâche avant que la tâche active soit accomplie. Lorsque l'utilisateur termine la nouvelle tâche, il est ramené à la tâche d'origine.

- **Imbriquer la tâche dans la tâche active et l'exécuter uniquement une fois la tâche active terminée**

Soumet la nouvelle tâche une fois la tâche d'origine accomplie. Cette tâche est nommée post-tâche.

Ajout de texte d'aide aux fenêtres de profils

Vous pouvez ajouter du texte n'importe où dans une fenêtre de profil pour apporter aux utilisateurs des informations supplémentaires, comme du texte d'aide en ligne pour un champ.

Pour ajouter du texte d'aide à une fenêtre de profil, procédez comme suit.

1. [Modifiez la fenêtre de profil](#) (page 29).
2. Sélectionnez le champ situé sous la ligne où vous souhaitez ajouter le texte d'aide en ligne, puis cliquez sur Ajouter pour ajouter une ligne comportant un champ au-dessus de la ligne que vous avez sélectionnée.

CA Identity Manager ajoute un nouveau champ au-dessus du champ que vous avez sélectionné.
3. Cliquez sur l'icône Modifier pour modifier le nouveau champ.

La boîte de dialogue Propriétés du champ s'ouvre.
4. Sélectionnez l'attribut (Séparateur) dans le champ Nom de l'attribut.
5. Sélectionnez HTML dans le champ Style.

Le champ HTML s'affiche.
6. Saisissez le texte que vous souhaitez afficher dans les balises HTML, par exemple :

`<h1>Ajoutez votre texte d'aide en ligne ici</h1>`
7. Cliquez sur OK.

Remarque : Pour afficher du code HTML personnalisé dans une autre langue, spécifiez une clé de ressource au format suivant dans le champ HTML personnalisé :

`#{bundle=GroupeRessources:key=IDclé}`

GroupeRessources

Identifie le groupe de ressources incluant le mappage de chaînes de texte pour l'ID clé.

IDclé

Identifie l'ID clé mappé à la chaîne de texte à afficher. Le mappage doit exister dans un groupe de ressources.

Par exemple, le code HTML d'un champ localisé doit se présenter comme suit :

```
<p>  
#{bundle=MonGroupeRessources;key=MaCléRessources}  
</p>
```

Remarque : Pour plus d'informations sur les groupes de ressources, consultez le manuel *User Console Design Guide*.

Ajout d'un champ Editeur d'historique

L'éditeur d'historique est une zone de texte qui crée de nouvelles entrées d'historique, si elle contient du texte lorsque la tâche est soumise. L'éditeur d'historique peut inclure un bouton de soumission facultatif, qui permet de créer des entrées d'historique sans soumettre la tâche.

Pour ajouter un champ Editeur d'historique à une fenêtre de profil :

1. [Modifiez une fenêtre de profil](#) (page 29).
2. Sélectionnez un champ à modifier ou ajoutez-en un.
3. Sélectionnez (Séparateur) dans le champ Nom de l'attribut.
CA Identity Manager modifie les champs affichés.
4. Sélectionnez Editeur d'historique dans le champ Style.
5. Dans le champ Etiquette, entrez le nom du champ Editeur d'historique qui apparaît dans la fenêtre de profil.
6. Entrez le texte associé aux entrées du journal d'historique et qui décrit le rôle de l'utilisateur qui est l'auteur de l'entrée de journal dans le champ Intervenant.
Par exemple, la description suivante apparaîtrait dans la colonne Source d'un affichage d'historique d'un utilisateur associé à l'étiquette d'intervenant Approbateur.
Commentaire d'utilisateur du gestionnaire des ventes (John Doe) agissant en tant qu'approbateur
Il peut s'agir d'une chaîne ou d'une clé de localisation, spécifiée en fonction des règles de localisation de CA Identity Manager. Le type d'intervenant est vide par défaut et est facultatif.
7. Entrez le nombre de lignes et de colonnes de l'éditeur d'historique.
Remarque : Si vous ne spécifiez aucune valeur pour les lignes et les colonnes, l'éditeur d'historique ne s'affiche pas correctement dans la fenêtre de profil.
8. Sélectionnez l'une des options suivantes dans le champ Niveau d'historique.
 - Niveau tâche : pour les tâches d'approbation, il s'agit de la tâche appartenant à l'événement en cours d'approbation. Pour les tâches autres que les tâches d'approbation, il s'agit de la tâche actuelle.
 - Niveau événement : pour les tâches d'approbation, il s'agit de l'événement en cours d'approbation. Pour les tâches autres que les tâches d'approbation, ceci ne retourne aucun résultat.

9. Spécifiez le texte qui apparaît sur le bouton de soumission dans le champ Etiquette du bouton Ajouter.

Il peut s'agir d'une chaîne ou d'une clé de localisation, spécifiée en fonction des règles de localisation de CA Identity Manager. Si ce champ est vide (configuration par défaut), l'étiquette du bouton est Ajouter un événement d'historique.

10. Spécifiez la classe CSS à utiliser pour le bouton Ajouter dans le champ Ajouter un bouton Classe CSS.

Ces chaînes seront incluses dans l'élément <entrée> de la fenêtre Profil, en tant que contenu des éléments style et classe respectivement.

11. Spécifiez la classe CSS à utiliser pour le bouton Ajouter dans le champ Ajouter un bouton Style CSS.

Ces chaînes seront incluses dans l'élément <entrée> de la fenêtre Profil, en tant que contenu des éléments style et classe respectivement.

12. Spécifiez si l'éditeur d'historique inclut son propre bouton Ajouter indépendant en activant ou en désactivant le champ Activer le bouton Ajouter.

Lorsqu'il est activé, ce bouton soumet uniquement la nouvelle entrée d'historique et non la tâche entière.

Informations complémentaires :

[Ajout d'un champ Affichage de l'historique](#) (page 85)

Ajout d'un champ Affichage de l'historique

L'affichage d'historique est une liste d'entrées de texte créées à l'aide de l'éditeur d'historique. Il peut apparaître dans n'importe quelle fenêtre Profil, quel que soit le type de sujet. L'éditeur d'historique comporte les paramètres de propriétés de champs suivants :

Pour ajouter un champ Affichage de l'historique à une fenêtre de profil :

1. [Modifiez une fenêtre de profil](#) (page 29).
2. Sélectionnez un champ à modifier ou ajoutez-en un.
3. Sélectionnez (Séparateur) dans le champ Nom de l'attribut.
CA Identity Manager modifie les champs affichés.
4. Sélectionnez Affichage de l'historique dans le champ Style.
5. Dans le champ Etiquette, entrez le nom du champ Editeur d'historique qui apparaît dans la fenêtre de profil.

6. Dans le champ Niveau d'historique, sélectionnez l'une des options suivantes :
 - Niveau tâche : pour les tâches d'approbation, il s'agit de la tâche appartenant à l'événement en cours d'approbation. Pour les tâches autres que les tâches d'approbation, il s'agit de la tâche actuelle.
 - Niveau événement : pour les tâches d'approbation, il s'agit de l'événement en cours d'approbation. Pour les tâches autres que les tâches d'approbation, ceci ne retourne aucun résultat.
7. Dans le champ Afficher les types d'entrées, sélectionnez l'une des options suivantes :
 - Entrées créées par l'utilisateur uniquement : n'affiche que les entrées d'exécution créées à l'aide de l'éditeur d'historique.
 - Toutes les entrées : affiche toutes les entrées, y compris celles créées par le flux de travaux ou le contrôleur de tâches.

Configuration de la validation de niveau tâche

Vous configurez la validation de niveau tâche dans la console d'utilisateur lorsque vous définissez des propriétés de champs dans une fenêtre de tâche de profil.

Pour configurer la validation de niveau tâche :

1. Dans la fenêtre Profil, sélectionnez le champ à valider et cliquez sur Propriétés du champ.

Une fenêtre Profil se définit dans le cadre de la définition des onglets de la tâche.

2. Spécifiez une valeur dans l'un des champs suivants, selon la manière dont la règle de validation doit être implémentée :

- Expression de validation : contient une expression normale qui effectue la validation.
- Classe Java de validation : contient le nom complet d'une classe Java qui effectue la validation. Par exemple :

`com.mycompany.MyJavaValidator`

Identity Manager s'attend à ce que le fichier de classe soit situé dans le répertoire racine spécifié pour les fichiers de classe Java personnalisés. Pour obtenir des informations sur le déploiement de fichiers de classe Java, reportez-vous au *Manuel de programmation Java*.

- JavaScript de validation : contient le code JavaScript complet qui effectue la validation.

Le code JavaScript doit être spécifié dans ce champ. Avec la validation de niveau tâche, vous ne pouvez pas référencer un fichier contenant du code JavaScript.

3. (Facultatif) Activez la fonctionnalité Valider lors de la modification pour que le champ soit validé dès sa modification.
4. (Facultatif) Pour un utilisateur, un groupe ou une organisation, vous pouvez utiliser un bouton Valider dans l'onglet Profil. Par défaut, ce bouton est masqué. Pour l'afficher, désélectionnez l'option Masquer le bouton de validation lorsque vous configurez l'onglet Profil de la tâche.

Si l'option Valider lors de la modification est activée dans un champ et que la valeur de ce champ change, le bouton Valider met à jour les autres champs de la fenêtre.

Remarque : Le bouton Valider exécute également des gestionnaires d'attributs logiques incluant la méthode de validation. Pour plus d'informations sur les gestionnaires d'attributs logiques, reportez-vous au Manuel de programmation *Java*.

La validation de niveau annuaire valide les champs en fonction du contenu du fichier `directory.xml`.

Remarque : Pour plus d'informations sur la validation de niveau annuaire ou sur la validation par défaut incluse avec Identity Manager, reportez-vous au *manuel de configuration* (en anglais).

Attributs personnalisés définis par l'utilisateur pour les rôles

CA Identity Manager prend en charge les attributs personnalisés définis par l'utilisateur qui vous permettent de spécifier des informations complémentaires sur les rôles qui vous aident à filtrer les rôles de votre organisation. Par exemple, un environnement d'entreprise peut disposer de plus de mille rôles. Cette organisation peut spécifier des informations complémentaires, telles que l'unité commerciale ou la situation géographique, pour chaque rôle. L'administrateur peut alors utiliser ces informations pour faciliter les recherches de rôles.

Vous pouvez utiliser les attributs personnalisés dans les tâches Créer, Modifier et Afficher pour les rôles suivants.

- Rôles d'administration
- Rôles de provisionnement
- Rôles d'accès

Pour configurer des attributs personnalisés pour des rôles, procédez comme suit :

1. Ajoutez la prise en charge des attributs personnalisés à l'onglet Profil pour les tâches qui créent, modifient ou affichent des rôles d'administration, de provisionnement ou d'accès.
2. Configurez les fenêtres de recherche et de liste pour les rôles à inclure dans les attributs personnalisés.

Informations complémentaires :

[Configuration des attributs personnalisés de l'onglet Profil pour les rôles](#) (page 88)

[Ajout d'attributs personnalisés aux définitions de fenêtres de recherche](#) (page 89)

Configuration des attributs personnalisés de l'onglet Profil pour les rôles

CA Identity Manager permet de configurer un maximum de 10 attributs personnalisés dans l'onglet Profil des tâches qui permettent de créer, de modifier ou d'afficher des rôles.

Pour configurer des attributs personnalisés dans l'onglet Profil :

1. Cliquez sur l'une des options suivantes :
 - Tâches, Rôles et tâches.
 - Rôles et tâches
2. Cliquez sur Tâches d'administration, Modifier la tâche d'administration.
La page Sélectionner une tâche d'administration s'affiche.
3. Recherchez et sélectionnez la tâche d'administration que vous souhaitez modifier.
CA Identity Manager affiche les détails de la tâche d'administration sélectionnée.
4. Cliquez sur l'onglet Onglets.
Les onglets configurés pour être utilisés avec cette tâche d'administration apparaissent.
5. Cliquez sur l'icône représentant une flèche pour modifier l'onglet Profil.
La fenêtre Configurer le profil apparaît.
6. Activez la case à cocher en regard de chaque champ personnalisé à ajouter à l'onglet Profil, puis entrez une étiquette significative.
7. Cliquez sur OK.
Les attributs personnalisés sont disponibles dans l'onglet Profil de la tâche modifiée une fois la tâche soumise.

Remarque : Pour utiliser les attributs personnalisés dans les recherches de rôles, [configurez la fenêtre de recherche](#) (page 89) pour qu'elle affiche ces attributs personnalisés.

Ajout d'attributs personnalisés aux définitions de fenêtres de recherche

Pour filtrer des rôles dans CA Identity Manager, vous pouvez seulement utiliser les attributs disponibles dans la fenêtre de recherche. Pour filtrer les rôles en fonction des attributs personnalisés définis, vous devez ajouter ces derniers à la fenêtre de recherche des rôles.

Pour ajouter des attributs personnalisés à la fenêtre de recherche des rôles :

1. Cliquez sur l'une des options suivantes :
 - Tâches, Rôles et tâches.
 - Rôles et tâches
2. Cliquez sur Tâches d'administration, Modifier la tâche d'administration.
La page Sélectionner une tâche d'administration s'affiche.
3. Recherchez et sélectionnez la tâche d'administration que vous souhaitez modifier.
Pour ajouter des attributs personnalisés aux fenêtres de recherche, sélectionnez la tâche Modifier ou Afficher pour le type de rôle (administration, provisionnement ou accès) incluant les attributs personnalisés.
CA Identity Manager affiche les détails de la tâche d'administration sélectionnée.
4. Cliquez sur l'onglet Rechercher dans la fenêtre Modifier le rôle d'administration.
La fenêtre de détails de la recherche apparaît.
5. Cliquez sur Parcourir pour afficher la liste des définitions de fenêtres de recherche disponibles pour la tâche.
La page Sélectionner une définition de fenêtre s'ouvre.
6. Sélectionnez une définition de fenêtre de recherche à modifier ou créez une copie d'une définition existante.
La fenêtre Configure Standard search (Configurer la recherche standard) s'ouvre.
7. Ajoutez les attributs personnalisés aux tableaux suivants.
 - Sélectionner les champs de recherche
 - Sélectionner les champs des résultats de la recherche
8. Modifiez le nom de l'attribut personnalisé afin qu'il corresponde au nom que vous avez spécifié lorsque vous avez configuré l'onglet Profil.
9. Cliquez sur OK pour enregistrer les modifications apportées à la définition de fenêtre de recherche.
La page Sélectionner une définition de fenêtre s'ouvre.
10. Sélectionnez la fenêtre que vous avez créée ou modifiée, puis cliquez sur Sélectionner.

11. Sélectionnez Tous les rôles d'administration dans la liste Options de recherche.
12. Cliquez sur Soumettre.

La fenêtre de recherche inclut désormais les attributs personnalisés dans les options de recherche et affiche les attributs dans les résultats de la recherche.

Chapitre 4: Configuration des onglets de compte

Ce chapitre traite des sujets suivants :

[Onglet Comptes](#) (page 91)

[Conditions préalables à l'utilisation de l'onglet Comptes](#) (page 92)

[Champs de l'onglet Comptes](#) (page 92)


[Autres fonctionnalités de l'onglet Comptes](#) (page 93)

Onglet Comptes

L'onglet Comptes répertorie les comptes dans les terminaux gérés pour les utilisateurs disposant de rôles de provisionnement. En général, cet onglet est ajouté à des tâches permettant d'afficher ou de modifier un utilisateur.

Détails du compte

Pour effectuer une action, cliquez sur un nom de compte.

Sélectionner	Nom	Type de terminal	Terminal	Suspension	Verrouillé
<input checked="" type="checkbox"/>	 ken.david	Window NT	IM-terminal	Actif	Déverrouillé

Créer un compte

Actions pour les comptes sélectionnés

Actualiser les comptes	Suspendre	Reprendre	Déverrouiller
Modifier le mot de passe	Annuler l'affectation	Affecter	Supprimer

Lorsque l'onglet Comptes est ajouté à une tâche Modifier un utilisateur, l'administrateur peut effectuer d'autres actions sur les comptes de l'utilisateur. comme les exemples ci-dessous.

- Suspendre ou reprendre un compte
- Déverrouiller un compte ayant été automatiquement verrouillé suite à un accès incorrect ou inapproprié. Par exemple, un compte peut être verrouillé lorsqu'un utilisateur dépasse le nombre acceptable d'échecs de tentatives de connexion défini dans une stratégie de mot de passe d'Identity Manager.
- Changer le mot de passe de l'utilisateur dans un ou plusieurs comptes
- Affecter des comptes à un utilisateur ou annuler l'affectation de ses comptes

Pour obtenir des détails sur les autres options définissables dans l'onglet Comptes, voir l'aide de la console d'utilisateur concernant l'onglet Configuration des comptes.

Conditions préalables à l'utilisation de l'onglet Comptes

Pour utiliser l'onglet Comptes, Identity Manager doit être configuré avec une prise en charge de provisionnement et son environnement doit inclure un annuaire de provisionnement.

Remarque : Pour configurer une prise en charge de provisionnement pour un environnement, reportez-vous au *Manuel de configuration*.

Champs de l'onglet Comptes

L'onglet Comptes affiche des détails sur les comptes que l'utilisateur possède au niveau des terminaux.

Voici certains des champs les plus significatifs :

- Nom : nom de connexion, nom de courriel ou autre nom du compte.
- Type de terminal : type de terminal (par exemple, un annuaire LDAP) associé au compte.
- Terminal : terminal spécifique associé au compte.
- Suspendu : un des trois états.
 - Actif s'affiche si le compte est activé.
 - Suspendu s'affiche si le compte est désactivé.
 - Activation manuelle en attente s'affiche s'il n'est pas possible de le reprendre ou de le suspendre. Connectez-vous au terminal pour reprendre ou suspendre le compte.
 - Non disponible s'affiche si l'état ne peut pas être récupéré en raison de l'absence de communication avec le terminal.
- Verrouillé : indique si le compte est verrouillé. Le verrouillage se produit lorsqu'un utilisateur tente à plusieurs reprises de se connecter au compte avec un mot de passe incorrect. Non disponible s'affiche si l'état ne peut pas être récupéré en raison de l'absence de communication avec le terminal.

Autres fonctionnalités de l'onglet Comptes

Lorsque l'onglet Comptes est inclus dans une tâche qui modifie un utilisateur, l'administrateur peut utiliser cette tâche pour exécuter des fonctionnalités sur les comptes de l'utilisateur. Les fonctionnalités disponibles dépendent de la configuration de l'onglet.

Vous pouvez choisir quelles fonctionnalités sont disponibles en utilisant l'option Modifier la tâche d'administration sur une tâche contenant l'onglet Comptes. Modifiez l'onglet Comptes pour déterminer si des fonctionnalités telles que Affecter un compte et Annuler l'affectation du compte sont disponibles sous l'onglet.

Pour plus d'informations, reportez-vous à l'aide en ligne de l'onglet Configurer des comptes.

Chapitre 5: Fenêtres de recherche et de liste

Ce chapitre traite des sujets suivants :

[Configuration d'une fenêtre de recherche](#) (page 95)

[Fenêtres de liste](#) (page 106)

[Tâches supplémentaires dans les fenêtres de recherche et de liste](#) (page 111)

Configuration d'une fenêtre de recherche

Vous configurez une fenêtre de recherche pour limiter la portée de la tâche et contrôler les champs sur lesquels l'utilisateur peut effectuer une recherche. Les fenêtres de recherche s'appliquent à deux types d'objets :

- Un *objet principal* : l'objet que la tâche doit modifier ou afficher.
- Un *objet secondaire* : l'objet associé à l'objet principal.

Par exemple, si vous incluez un onglet de groupe dans une tâche Créer un utilisateur, l'utilisateur est l'objet principal et le groupe l'objet secondaire. L'onglet de groupe nécessite une fenêtre de recherche pour les groupes.

Remarque : Après avoir configuré une fenêtre de recherche, vous pouvez l'utiliser pour n'importe quelle tâche afin de rechercher un objet principal ou secondaire.

Modification d'une fenêtre de recherche

Vous pouvez modifier une fenêtre de recherche existante pour :

- Configurer des valeurs par défaut pour le filtre de recherche
- Modifier les champs des filtres de recherche
- Modifier les champs des résultats de recherche
- Ajouter un texte d'aide dans la fenêtre de recherche

Pour modifier une fenêtre de recherche :

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration.
2. Recherchez et sélectionnez la tâche d'administration à modifier.

CA Identity Manager affiche les onglets à configurer pour la tâche que vous avez sélectionnée.

3. Cliquez sur l'onglet Rechercher.
4. (Facultatif) Cochez la case Les objets modifiés doivent figurer dans la portée de l'administrateur.

Lorsque cette case est cochée, CA Identity Manager affiche une erreur si les modifications apportées à la tâche font que l'objet principal ne figure plus dans la portée de l'administrateur. Par exemple, un administrateur peut utiliser Modifier un utilisateur pour remplacer l'attribut Type d'employé d'un utilisateur par Gestionnaire. Cette modification peut placer l'utilisateur en dehors de la portée de l'administrateur.

Remarque : Cette option ne s'affiche pas pour les tâches de gestion des rôles.

5. Cliquez sur Parcourir en regard du champ Fenêtre.
CA Identity Manager affiche une liste de fenêtres applicables.
6. Sélectionnez la fenêtre de recherche à modifier ou à copier, puis cliquez sur l'un des boutons suivants.

- **Sélectionner**

Ajoute la fenêtre sélectionnée à la recherche en cours de configuration.

- **Modifier**

Ouvre une nouvelle fenêtre dans laquelle vous pouvez modifier les paramètres de la fenêtre sélectionnée, notamment les champs, les propriétés de champs et la présentation.

- **Supprimer**

Supprime la fenêtre sélectionnée.

- **Créer**

Ouvre une nouvelle fenêtre dans laquelle vous pouvez créer une fenêtre. La nouvelle fenêtre n'inclut aucun champ par défaut.

- **Copier**

Crée une fenêtre à l'aide des paramètres d'une fenêtre existante. Pour créer une fenêtre basée sur une fenêtre existante, ajoutez un nouveau nom et une nouvelle balise à la fenêtre, puis modifiez les paramètres selon les besoins.

- **Annuler**

Renvoie à la fenêtre de configuration de recherche.

Si vous avez sélectionné Modifier, Créer ou Copier, CA Identity Manager ouvre une nouvelle fenêtre dans laquelle vous pouvez créer ou modifier une fenêtre de recherche.

Filtres de recherche

Les filtres de recherche limitent les objets retournés par la recherche. Par exemple, si l'objet est Utilisateurs, vous pouvez limiter la recherche pour qu'elle ne trouve que des sous-traitants. Vous pouvez configurer un filtre pour rechercher les utilisateurs dont le type d'employé est Sous-traitant.

Vous pouvez configurer des recherches sur les champs ci-après.

Afficher uniquement les objets correspondant aux règles suivantes

Définit des critères supplémentaires à combiner avec le filtre défini par l'utilisateur pour affiner la recherche.

Prenez note des points suivants lors de l'utilisation de ce champ.

- En raison des limites dont les recherches de rôles de provisionnement font l'objet, ces critères écrasent les champs de filtre portant le même nom entré par l'utilisateur.
- Les attributs utilisés lorsque vous configurez ce champ ne doivent pas être ajoutés comme des champs de recherche disponibles dans la fenêtre de recherche.

Par exemple, si vous configurez l'écran de recherche pour n'afficher que les rôles lorsque l'attribut activé est Oui, supprimez l'attribut activé de la liste des attributs que les utilisateurs peuvent spécifier comme critère de recherche.

Sinon, le critère entré par l'utilisateur est ignoré.

Filtre de recherche par défaut

Définit un filtre qui s'affiche par défaut lorsqu'un administrateur utilise la fenêtre de recherche. Par exemple, si vous configurez une fenêtre de recherche pour la tâche Modifier un sous-traitant et savez que les administrateurs recherchent généralement les sous-traitants en fonction du nom de la société du contrat, vous pouvez définir le filtre par défaut sur Société du contrat = *. Les administrateurs peuvent remplacer le filtre par défaut en spécifiant des critères de recherche différents. Définir un filtre par défaut améliore les performances en limitant le nombre de résultats retournés si un administrateur ne spécifie pas de filtre avant de commencer une recherche.

Sélectionner automatiquement tous les résultats de recherche utilisés avec les tâches de multisélection

Indique que tous les résultats de recherche sont sélectionnés par défaut. Si vous activez cette case à cocher, tous les objets figurant dans la liste des résultats de recherche apparaissent accompagnés d'une case cochée.

Recherche automatique

Indique qu'un champ de recherche est affiché avec les résultats de recherche.

Définir automatiquement le sujet de la tâche pour les résultats de recherche unique

Définit automatiquement l'objet principal de la tâche lorsqu'un seul objet correspond au filtre de recherche.

Par exemple, supposons que cette option soit sélectionnée pour une fenêtre de recherche d'utilisateurs associée à la tâche Modifier l'utilisateur. Lorsqu'un administrateur ouvre la tâche Modifier l'utilisateur et entre un filtre de recherche qui ne retourne qu'un seul utilisateur, CA Identity Manager ouvre la tâche Modifier l'utilisateur pour cet utilisateur. L'administrateur n'a pas besoin de sélectionner l'utilisateur pour ouvrir cette tâche.

Remarque : Pour appliquer ce paramètre, la recherche automatique doit également être sélectionnée.

Enregistrer le filtre de recherche

Indique que le filtre de recherche de la tâche est enregistré pour l'utilisateur de la session actuelle. La prochaine fois qu'un utilisateur effectue une recherche dans la tâche, le filtre de recherche enregistré est affiché.

Remarque : CA Identity Manager enregistre le filtre de recherche pour la durée de la session de l'utilisateur. Le filtre de recherche est effacé lorsque l'utilisateur se déconnecte.

Rechercher dans l'organisation

Affiche un filtre d'organisation dans la fenêtre de recherche. Si cette case à cocher est activée, l'administrateur peut spécifier un filtre qui limite les organisations dans lesquelles CA Identity Manager recherche un objet. Vous pouvez spécifier des valeurs par défaut pour le filtre de recherche d'organisations en spécifiant une fenêtre de recherche dans le champ Recherche d'organisation.

Enregistrer l'organisation de recherche

Indique que l'organisation de la tâche est enregistrée si une organisation a été établie pour la recherche. La prochaine fois qu'un utilisateur effectue une recherche dans la tâche, l'organisation est affichée.

Recherche d'organisation

Spécifie la fenêtre de recherche que CA Identity Manager utilise pour permettre aux administrateurs de rechercher une organisation.

Portée de la recherche d'une organisation par défaut

Spécifie la portée de la recherche d'une organisation par défaut qui apparaît lorsqu'un administrateur utilise une fenêtre de recherche. La portée de la recherche détermine les niveaux d'une arborescence organisationnelle qui sont inclus dans la recherche. L'administrateur peut remplacer la portée de la recherche d'une organisation par défaut en spécifiant des critères de recherche différents dans la fenêtre de recherche.

Par exemple, si vous configurez une fenêtre de recherche pour une tâche Modifier un sous-traitant personnalisée dans un environnement qui enregistre les informations en relation avec les sous-traitants à divers niveaux de l'arborescence organisationnelle, vous pouvez définir la portée de la recherche d'une organisation par défaut sur Et moins que.

Rechercher une expression unique

Définit le type de filtre de recherche qui s'affiche dans la fenêtre de recherche. Si cette case est cochée, l'utilisateur peut spécifier un filtre de recherche unique, tel que <attribut><comparateur><valeur>. Si elle n'est pas cochée, l'utilisateur peut spécifier plusieurs filtres de recherche. Par exemple, <attribut1><comparateur><valeur1> AND <attribut2><comparateur> <valeur2>. Les objets remplissant les conditions définies par tous les filtres sont retournés dans les résultats de recherche. Dans l'exemple précédent, les objets incluant <valeur1> et <valeur2> sont retournés comme résultats de recherche.

Recherche en mode Est égal(e) à

Interdit aux administrateurs d'utiliser des opérateurs de recherche autres que l'opérateur Est égal(e) à.

Afficher le nombre de résultats

Affiche le nombre de résultats de recherche correspondant. Lorsque cette case à cocher est activée, toutes les recherches retournent le message "Il y a X résultats".

Ajouter un bouton de tâche pour <nom_de_la_tâche>

Ajoute un lien vers une autre tâche dans la fenêtre de recherche. Le lien est affiché sous forme de bouton.

Ce champ est généralement utilisé pour ajouter une tâche de création à une fenêtre de recherche configurée pour la navigation objet/tâche.

Etiquette facultative

Spécifie une étiquette pour la tâche sélectionnée dans le champ précédent. Cette étiquette s'affiche sur le bouton de la tâche.

Ajouter un bouton de suppression multiple pour <nom_de_la_tâche>

Ajoute à une tâche un lien qui permet à l'administrateur de sélectionner plusieurs objets à supprimer. Le lien est affiché sous forme de bouton. Ce champ est généralement utilisé avec la navigation objet/tâche.

Champs et résultats de recherche

Dans une autre partie de la fenêtre de recherche, vous sélectionnez les champs que l'administrateur peut utiliser dans une requête de recherche, ainsi que les champs à afficher dans les résultats de recherche.

Sélectionner les champs de recherche

Sélectionnez les champs que l'administrateur peut utiliser pour créer une requête de recherche.

Pour ajouter des champs supplémentaires, sélectionnez des champs dans la zone de liste en dessous du tableau des champs de recherche.

Une fois les champs sélectionnés, vous pouvez changer l'ordre dans lequel ils apparaissent à l'aide des icônes représentant une flèche vers le haut et vers le bas situées à droite du champ.

Remarque : Si vous ne spécifiez pas les champs que l'administrateur peut utiliser, CA Identity Manager démarre la recherche automatiquement.

Sélectionner les champs des résultats de la recherche

Sélectionnez les champs qu'CA Identity Manager affiche dans les résultats de recherche. Vous pouvez sélectionner des champs non disponibles dans la requête de recherche.

Pour ajouter des champs supplémentaires, sélectionnez des champs dans la zone de liste en dessous du tableau des champs de recherche.

Style

Lorsque vous sélectionnez un champ à afficher dans les résultats de recherche, vous pouvez sélectionner l'une des options de style suivantes :

■ Nom d'affichage booléen

Affiche le nom du champ pour tous les résultats qui sont vrais (True). Par exemple, si vous entrez Activé comme nom de l'attribut qui indique l'état de compte d'un utilisateur, Activé s'affiche dans les résultats de recherche pour tous les comptes d'utilisateurs actifs.

■ Coche

Affiche la valeur sous la forme d'une coche sélectionnée en fonction de la valeur de l'attribut. Par exemple, si vous sélectionnez le style Coche pour représenter l'état Activé/Désactivé de comptes d'utilisateurs, CA Identity Manager affiche une coche sélectionnée pour tous les comptes actifs.

- **Chaîne à valeurs multiples**

Affiche les valeurs d'un attribut à valeurs multiples sur des lignes séparées. Les valeurs sont répertoriées dans l'ordre alphabétique.

- **Case à cocher en lecture seule**

Affiche la valeur sous forme de case à cocher en lecture seule.

- **Chaîne**

Affiche la valeur sous forme de chaîne de texte.

- **Tâche**

Ajoute une liste de tâches à un champ. L'utilisateur clique sur une icône représentant une flèche pour afficher la liste des tâches qu'il peut effectuer sur l'objet associé au champ de recherche. Par exemple, si vous ajoutez une liste de tâches à un champ Nom dans les résultats de recherche, l'utilisateur peut cliquer sur l'icône flèche figurant dans ce champ pour afficher la liste des tâches qu'il peut effectuer sur l'utilisateur qu'il sélectionne.

Ce paramètre peut également être utilisé pour faire apparaître une valeur d'attribut comme un lien vers une tâche.

Si vous sélectionnez le style Tâche, une icône représentant une flèche vers la droite apparaît en regard de la colonne Style. Cliquez sur la flèche pour ouvrir la boîte de dialogue Propriétés du champ. Utilisez cette boîte de dialogue pour configurer une [liste de tâches](#) (page 108).

- **Liste des tâches**

Permet d'ajouter des tâches supplémentaires que les utilisateurs peuvent effectuer au niveau des objets dans les fenêtres de recherche et de liste. Par exemple, vous pouvez configurer la fenêtre de recherche dans la tâche Modifier un utilisateur de façon à permettre aux utilisateurs d'effectuer une tâche, comme désactiver un utilisateur de la liste d'utilisateurs renvoyés par la recherche.

Lorsque vous sélectionnez cette option, vous déterminez si les utilisateurs accèdent à la tâche en cliquant sur une icône ou sur un lien de texte.

- **Menu des tâches**

Permet d'ajouter des tâches supplémentaires (similaires au style Liste des tâches) en tant qu'éléments de menu contextuel.

Lorsque vous sélectionnez cette option, un bouton Action s'affiche à côté de chaque objet dans une fenêtre de recherche ou de liste. Les utilisateurs doivent cliquer sur le bouton Action pour voir la liste des tâches qu'ils sont autorisés à effectuer au niveau de cet objet.

Remarque : Pour voir les options des styles Liste des tâches et Menu des tâches, sélectionnez Séparateur lorsque vous ajoutez un champ à la table des résultats de la recherche. Pour plus d'informations sur l'ajout de tâches supplémentaires aux fenêtres de recherche et de liste, consultez le manuel *User Console Design Guide*.

Triable

Cochez cette case pour permettre à l'administrateur de trier les résultats de recherche en fonction d'un ou plusieurs champs.

Définir l'ordre de tri par défaut des résultats de la recherche

Détermine l'ordre dans lequel les résultats de recherche sont affichés. Les résultats de recherche sont d'abord triés en fonction du premier champ figurant dans la liste, puis en fonction de chacun des champs supplémentaires dans l'ordre dans lequel ils apparaissent. Cochez la case Décroissant pour trier les résultats dans l'ordre décroissant.

Sélectionner des objets contenant des champs *nom de champ* modifiés

Spécifie que les objets dans lesquels le champ spécifié a été modifié sont sélectionnés lorsque l'utilisateur clique sur le bouton Sélectionner.

Retourner *N* résultats par page

Sélectionnez le nombre de résultats à afficher par page. Si les résultats de recherche dépassent le nombre spécifié, CA Identity Manager affiche un lien vers chaque page de résultats.

Aide sur les fenêtres de recherche définie par l'utilisateur

Si vous souhaitez ajouter du texte personnalisé à votre fenêtre de recherche, vous pouvez définir votre texte dans la zone de texte HTML correspondante. Vous pouvez ajouter du texte dans les zones suivantes :

- Début ou fin de la page
- Avant ou après la création
- Avant ou après les résultats

Types de fenêtres de recherche

Identity Manager inclut les fenêtres de recherche préconfigurées suivantes.

Fenêtre de recherche de rôles d'accès

La fenêtre de recherche de rôles d'accès permet de configurer des filtres de recherche pour trouver des rôles d'accès correspondant à des critères spécifiques.

Fenêtre de recherche de tâche d'accès

La fenêtre de recherche de tâche d'accès permet de configurer des filtres de recherche pour trouver des tâches d'accès correspondant à des critères spécifiques. Cette fenêtre de recherche est utilisée pour trouver une tâche d'accès à afficher ou à modifier ou pour ajouter une tâche à un rôle d'accès.

Fenêtre de recherche de rôles d'administration

La fenêtre de recherche de rôles d'administration permet de configurer des filtres de recherche pour trouver des rôles d'administration correspondant à des critères spécifiques.

Fenêtre de recherche de tâches d'administration

La fenêtre de recherche de tâches d'administration permet de configurer des filtres de recherche pour trouver des tâches d'administration correspondant à des critères spécifiques. Cette fenêtre de recherche est utilisée pour trouver une tâche d'administration à afficher ou à modifier ou pour ajouter une tâche à un rôle d'administration.

Fenêtre de recherche d'approbations

La fenêtre de recherche d'approbations permet de configurer l'affichage qui apparaît en haut d'une tâche d'approbation.

Fenêtre de recherche d'un utilisateur du processus de certification initiale

La fenêtre de recherche d'un utilisateur du processus de certification initiale permet de configurer des filtres de recherche afin de trouver des utilisateurs pour lesquels définir l'état sur certification requise. L'état de certification des utilisateurs sélectionnés est défini sur *certification requise*.

Fenêtre de recherche d'utilisateurs à certifier

La fenêtre de recherche d'utilisateurs à certifier permet de configurer des filtres de recherche pour trouver les utilisateurs nécessitant une certification.

Fenêtre de recherche de délégations

La fenêtre de recherche de délégations permet de configurer des filtres de recherche pour trouver d'autres utilisateurs à ajouter en tant que délégués. Un délégué est un autre utilisateur que vous pouvez temporairement autoriser à afficher et à résoudre vos tâches de flux de travaux.

Fenêtre de recherche d'utilisateurs à activer/désactiver

La fenêtre de recherche d'utilisateurs à activer/désactiver permet de configurer des filtres de recherche pour activer/désactiver des utilisateurs correspondant à des critères spécifiques.

Fenêtre de recherche d'un utilisateur du processus de certification finale

La fenêtre de recherche d'un utilisateur du processus de certification finale permet de configurer des filtres de recherche pour identifier les utilisateurs dont le cycle de certification doit être terminé.

Fenêtre de recherche d'un contrat de licence de l'utilisateur final

La fenêtre de recherche d'un contrat de licence de l'utilisateur final permet de configurer la tâche Auto-enregistrement avec une page spécifique à votre application d'identités.

Fenêtre de recherche d'exploration et de corrélation

La fenêtre de recherche d'exploration et de corrélation permet de configurer des filtres de recherche pour des définitions d'exploration et de corrélation correspondant à des critères spécifiques.

Fenêtre de recherche de fichier de chargeur à télécharger

La fenêtre de recherche de fichier de chargeur à télécharger permet de rechercher le fichier de chargeur à télécharger. Un fichier de chargeur permet d'automatiser les actions répétitives effectuées sur un grand nombre d'objets gérés.

Fenêtre de recherche du mot de passe oublié/de l'ID d'utilisateur oublié

La fenêtre de recherche du mot de passe oublié permet de configurer la tâche Mot de passe oublié pour inviter l'utilisateur à entrer les informations prouvant son identité.

Fenêtre de recherche de groupes

La fenêtre de recherche de groupes permet de configurer des filtres de recherche pour des groupes, tels que des groupes situés dans l'organisation financière.

Fenêtre de recherche d'un ensemble de stratégies d'identité

La fenêtre de recherche d'un ensemble de stratégies d'identité permet de configurer des filtres de recherche pour trouver des ensembles de stratégies d'identité correspondant à des critères spécifiques.

Fenêtre de recherche d'un gestionnaire d'attributs logiques

La fenêtre de recherche d'un gestionnaire d'attributs logiques permet de configurer des filtres de recherche pour trouver des gestionnaires d'attributs logiques. Cette fenêtre de recherche est utilisée pour trouver un gestionnaire d'attributs logiques afin d'en afficher ou d'en modifier la configuration.

Fenêtre de recherche de gestion des rapports

La fenêtre de recherche de gestion des rapports permet de configurer des filtres de recherche pour trouver un rapport à afficher ou à supprimer.

Fenêtre de recherche d'un utilisateur non certifié

La fenêtre de recherche d'un utilisateur non certifié permet de configurer des filtres de recherche pour trouver les utilisateurs non certifiés à la fin de la période de certification.

Fenêtre de recherche d'organisations

La fenêtre de recherche d'organisations permet de configurer des filtres de recherche pour limiter le choix d'organisations à certaines sous-organisations.

Fenêtre de recherche de rôles de provisionnement

La fenêtre de recherche de rôles de provisionnement permet de configurer des filtres de recherche pour extraire des rôles de provisionnement.

Fenêtre de recherche de modèles de comptes

La fenêtre de recherche de modèles de comptes vous permet de configurer des filtres de recherche pour extraire des modèles de comptes.

Fenêtre de recherche d'une stratégie de mot de passe

La fenêtre de recherche d'une stratégie de mot de passe permet de configurer des filtres de recherche pour trouver des stratégies de mot de passe correspondant à des critères spécifiques.

Fenêtre de recherche de définition de cliché

La fenêtre de recherche de définition de cliché permet de configurer des filtres de recherche pour trouver une définition de cliché à afficher, à modifier ou à supprimer.

Fenêtre standard de recherche

La fenêtre standard de recherche permet de configurer des filtres pour trouver des objets gérés personnalisés.

Fenêtre de recherche d'utilisateurs

La fenêtre de recherche d'utilisateurs permet de configurer des filtres de recherche pour trouver des utilisateurs correspondant à des critères spécifiques. Par exemple, vous pouvez rechercher des utilisateurs qui sont des sous-traitants.

Une fois l'onglet Rechercher renseigné, choisissez les onglets de la tâche.

Fenêtres de liste

Lors de la configuration d'onglets, il est souvent nécessaire d'afficher une liste d'éléments (par exemple, une liste d'utilisateurs ou de rôles). La liste s'affiche dans l'onglet en cours de configuration. Dans ces cas, créez une fenêtre de liste pour contrôler les colonnes et le tri des objets figurant dans l'onglet.

Vous pouvez configurer les champs ci-après pour une fenêtre de liste.

nom

Définit le nom de la tâche.

Balise

Identifiant unique au sein de la tâche. La balise peut contenir des caractères ASCII (a-z, A-Z), des chiffres (0-9) ou des traits de soulignement, et commence par une lettre ou un trait de soulignement. La balise permet de définir les valeurs de données via des documents XML ou des paramètres HTTP.

Champ

Spécifie les attributs qui s'affichent en tant que champs dans les résultats de recherche.

nom

Spécifie l'étiquette du champ dans les résultats de recherche.

Style

Détermine le format du champ dans les résultats de recherche. Vous pouvez spécifier les options de style suivantes.

Nom d'affichage booléen

Affiche le nom du champ pour tous les résultats qui sont vrais (True). Par exemple, si vous entrez Activé comme nom de l'attribut qui indique l'état de compte d'un utilisateur, Activé s'affiche dans les résultats de recherche pour tous les comptes d'utilisateurs actifs.

Coche

Affiche la valeur sous la forme d'une coche sélectionnée ou désélectionnée en fonction de la valeur de l'attribut. Par exemple, si vous sélectionnez le style Coche pour représenter l'état Activé/Désactivé de comptes d'utilisateurs, CA Identity Manager affiche une coche sélectionnée pour tous les comptes actifs.

Chaîne à valeurs multiples

Affiche les valeurs d'un attribut à valeurs multiples sur des lignes séparées. Les valeurs sont répertoriées dans l'ordre alphabétique.

Case à cocher en lecture seule

Affiche la valeur sous forme de case à cocher en lecture seule.

Chaîne

Affiche la valeur sous forme de chaîne de texte.

Tâche

Ajoute une liste de tâches à un champ. L'utilisateur clique sur une icône flèche droite pour afficher la liste des tâches qu'il peut effectuer sur l'objet associé au champ de recherche. Par exemple, si vous ajoutez une liste de tâches à un champ Nom dans les résultats de recherche, l'utilisateur peut cliquer sur l'icône flèche figurant dans ce champ pour afficher la liste des tâches qu'il peut effectuer sur l'utilisateur qu'il sélectionne.

Triable

Détermine si l'utilisateur peut trier les résultats de recherche en fonction du champ sélectionné.

Décroissant

Détermine l'ordre dans lequel les résultats de recherche sont affichés. Lorsque la case Décroissant est cochée, les résultats de recherche sont triés alphabétiquement dans l'ordre décroissant. Les résultats sont triés dans l'ordre dans lequel ils s'affichent dans la liste.

Résultats par page

Indique le nombre de résultats de recherche à afficher dans les résultats de recherche.

Texte HTML apparaissant avant la liste

Spécifie le texte qui s'affiche au-dessus de la liste des résultats de recherche.

Texte HTML apparaissant après la liste

Spécifie le texte qui s'affiche en dessous de la liste des résultats de recherche.

Vous pouvez également ajouter du texte au-dessus et en dessous d'une fenêtre de liste.

Ajout d'une liste de tâches

Une liste de tâches est un menu de tâches auquel vous accédez à partir d'une liste d'objets (par exemple, une fenêtre de liste ou de résultats de recherche). Les listes de tâches permettent d'afficher et d'utiliser les tâches qui s'appliquent à un objet sans devoir rechercher ce dernier à chaque utilisation d'une nouvelle tâche. Par exemple, vous pouvez configurer CA Identity Manager afin d'afficher un menu de tâches pour chaque membre de rôle répertorié dans l'onglet Appartenance de la tâche Modifier les membres du rôle d'administration. L'administrateur peut utiliser les menus de tâches pour gérer les membres de rôles sans devoir effectuer une nouvelle recherche pour chaque membre de rôle.

Ajout d'une tâche imbriquée

1. Effectuez *l'une* des étapes suivantes :
 - Sélectionnez Modifier la tâche d'administration dans Rôles et tâches, puis Tâches d'administration. Recherchez et sélectionnez la tâche d'administration à modifier.
 - Sélectionnez Modifier la tâche d'administration dans Rôles et tâches, puis Tâches d'administration. Sélectionnez ensuite Créer une copie de tâche d'administration, puis recherchez une tâche à copier.

CA Identity Manager affiche les onglets à configurer pour la tâche que vous avez sélectionnée.

2. Sélectionnez l'onglet dans lequel vous souhaitez ajouter la liste de tâches.

En général, il s'agit d'un onglet incluant une fenêtre de recherche ou de liste, tel que l'onglet Appartenance.

3. Recherchez une liste ou une fenêtre de recherche à modifier en cliquant sur Parcourir.
4. Sélectionnez le champ pour la liste des tâches dans la liste de champs affichée dans les résultats de la recherche.
5. Sélectionnez Tâche dans le champ Style.

6. Cliquez sur l'icône représentant une flèche vers la droite pour ouvrir une section Propriétés du champ dans laquelle configurer la liste de tâches.
7. Remplissez les champs suivants selon les besoins :

- **Tâche par défaut**

Spécifie la tâche qui s'ouvre lorsqu'un utilisateur clique sur une valeur de ce champ. Lorsque vous configurez un champ pour prendre en charge les listes de tâches et spécifiez une tâche par défaut, la valeur du champ apparaît en bleu, ce qui indique qu'il s'agit d'un lien.

Par exemple, si vous configurez le champ Nom pour inclure une liste de tâches, un administrateur peut cliquer sur le nom d'un utilisateur pour ouvrir la tâche par défaut.

- **Autre tâche**

Spécifie la tâche qui s'ouvre lorsqu'un utilisateur clique sur la valeur du champ mais n'est pas autorisé à utiliser la tâche par défaut.

- **Activer le menu contextuel de tâche**

Affiche une icône représentant une flèche vers la droite en regard du champ. L'utilisateur clique sur cette icône pour afficher la liste des tâches qu'il peut effectuer sur cet objet dans ce champ.

Lorsque vous cochez cette case, les options suivantes apparaissent :

- **Inclure toutes les tâches que l'administrateur peut réaliser sur l'objet**
- **Inclure toutes les tâches que l'administrateur peut réaliser sur l'objet (à l'exception des tâches cachées dans les menus)**

- **Inclure uniquement les tâches spécifiées**

N'affiche que les tâches que vous sélectionnez dans le champ Tâche.

Remarque : L'utilisateur ne peut pas voir une tâche spécifiée s'il n'est pas autorisé à l'utiliser.

- **Exclure les tâches spécifiées**

Affiche les tâches qu'un administrateur peut effectuer sur l'objet, *sauf* celles répertoriées dans le champ Tâche.

– **Tâche**

Spécifie les tâches qui apparaissent ou n'apparaissent pas dans une liste de tâches, selon la sélection effectuée : Inclure uniquement les tâches spécifiées ou Exclure les tâches spécifiées.

■ **Imbriquer la tâche**

Lorsque cette option est activée, CA Identity Manager ouvre la tâche en tant que tâche imbriquée. Lorsque l'utilisateur termine la tâche imbriquée, il n'est pas ramené à la tâche d'origine.

Si cette option n'est pas sélectionnée, la nouvelle tâche remplace la tâche d'origine.

8. Cliquez sur OK.

Tâches supplémentaires dans les fenêtres de recherche et de liste

Vous pouvez configurer CA Identity Manager de façon à ajouter des actions supplémentaires que les utilisateurs peuvent effectuer dans les fenêtres de recherche et de liste. Par exemple, vous pouvez configurer la fenêtre de recherche dans la tâche Modifier un utilisateur de façon à permettre aux utilisateurs d'effectuer une tâche, comme désactiver un utilisateur de la liste d'utilisateurs renvoyés par la recherche.

L'ajout de tâches aux fenêtres de recherche et de liste réduit le nombre de clics requis pour effectuer une tâche et simplifie la console d'utilisateur.

Vous pouvez afficher les tâches des fenêtres de recherche et de liste de l'une des façons suivantes :

- Liens ou icônes de tâche

Ils affichent chaque tâche sous forme de lien ou d'icône dans les fenêtres de liste ou de résultat de recherche. Utilisez cette méthode pour afficher un petit nombre de tâches.

Modify Contractor: Select User

Search for a user

Search for a user
in organization

where User ID = *j*

Search Results

1-3 of 3

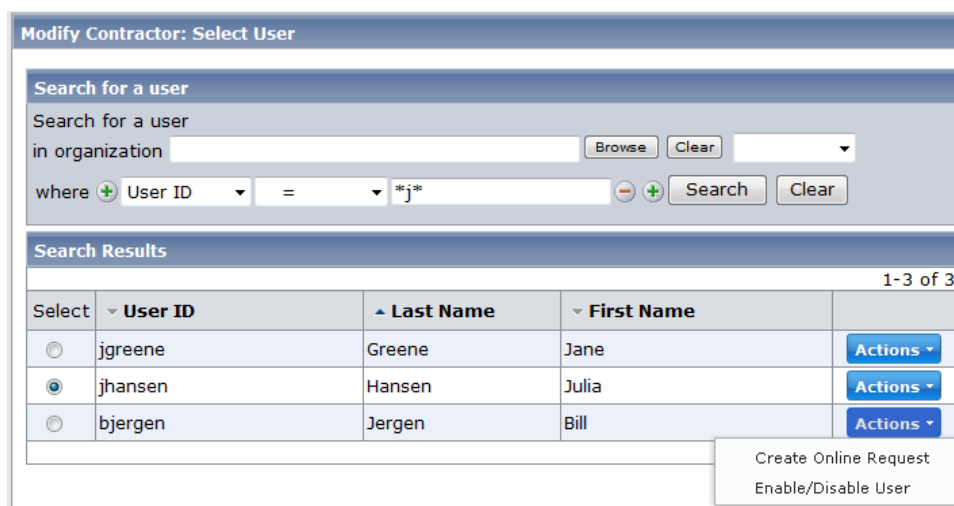
Select	User ID	Last Name	First Name	
<input type="radio"/>	jgreene	Greene	Jane	
<input checked="" type="radio"/>	jhansen	Hansen	Julia	
<input type="radio"/>	bjergen	Jergen	Bill	

1-3 of 3

- Menus des tâches

Ils affichent un bouton Action sur chaque ligne dans les fenêtres de liste ou de résultat de recherche. Les administrateurs cliquent sur le bouton Action pour voir la liste de tâches qu'ils peuvent effectuer pour cet utilisateur.

Utilisez cette méthode si les utilisateurs peuvent effectuer plus de deux ou trois tâches.



Ajout de tâches supplémentaires dans les fenêtres de recherche et de liste

Vous pouvez configurer l'exécution de tâches supplémentaires dans CA Identity Manager à partir des fenêtres de recherche ou de liste, afin de réduire le nombre d'étapes requises pour effectuer certaines tâches.

Pour ajouter des tâches supplémentaires dans les fenêtres de recherche et de liste :

1. Modifiez une fenêtre de recherche ou de liste.
La fenêtre Configure Standard Search Screen (Configurer la fenêtre de recherche standard) s'ouvre.
2. Ajoutez une nouvelle ligne dans la section de champs de résultats de la recherche comme suit :
 - a. Ajoutez une nouvelle ligne en cliquant sur le signe plus au-dessous de la table des résultats de la recherche.
 - b. Sélectionnez le style de séparateur.
 - Lien de tâche
Affiche les tâches supplémentaires sous la forme d'icônes ou de liens de texte.
 - Menu des tâches
Affiche le bouton Action qui permet aux utilisateurs d'afficher un menu des tâches qu'ils peuvent effectuer.

3. Si vous avez sélectionné Lien de tâche, procédez comme suit :
 - a. Spécifiez la tâche qui s'ouvre lorsque les utilisateurs cliquent sur l'icône ou le lien de tâche dans le champ Tâche par défaut.
 - b. Spécifiez une autre tâche qui s'ouvre si les utilisateurs ne disposent pas des droits pour ouvrir la tâche par défaut.
 - c. Déterminez l'option d'ouverture de la tâche en sélectionnant ou en effaçant le champ Tâche imbriquée.

Lorsque cette option est sélectionnée, la tâche s'ouvre comme une tâche imbriquée. Lorsqu'un utilisateur termine la tâche imbriquée, il est renvoyé à la fenêtre de recherche ou de liste.
 - d. Déterminez si les tâches supplémentaires seront affichées sous la forme d'icônes ou de lien de texte en sélectionnant ou en effaçant le champ Icône de tâche.

Si vous effacez cette option, CA Identity Manager affiche la tâche sous la forme d'un lien de texte.
4. Si vous avez sélectionné l'option Menu des tâches, procédez comme suit :
 - a. Sélectionnez le type de tâches affichées dans le menu des tâches.
 - b. Spécifiez les tâches à afficher *si* vous avez sélectionné l'option Inclure uniquement les tâches spécifiées ou Exclure les tâches spécifiées à l'étape a.
 - c. Déterminez si CA Identity Manager ouvre les tâches de menu comme des tâches imbriquées en sélectionnant ou en effaçant l'option Tâche imbriquée.

Lorsque vous sélectionnez l'option Tâche imbriquée, les utilisateurs sont renvoyés vers l'emplacement à partir duquel ils ont lancé la tâche lorsque celle-ci se termine.
5. Cliquez sur OK, puis sur Sélectionner.
6. Cliquez sur OK, puis sur Soumettre pour enregistrer les modifications apportées aux fenêtres.

Chapitre 6: Tâches d'auto-administration

Ce chapitre traite des sujets suivants :

[Tâches d'auto-administration de CA Identity Manager](#) (page 115)

[Configuration de tâches d'auto-administration](#) (page 116)

[Configuration de la tâche d'auto-enregistrement](#) (page 117)

[Configuration des tâches Réinitialisation du mot de passe oublié et ID d'utilisateur oublié](#) (page 120)

[Pages de déconnexion](#) (page 130)

Tâches d'auto-administration de CA Identity Manager

Les tâches d'auto-administration sont des tâches CA Identity Manager que l'utilisateur peut utiliser pour gérer ses propres profils. Ces tâches sont réparties dans deux types :

- Tâches publiques : tâches auxquelles l'utilisateur peut accéder sans fournir de données de connexion. Par exemple, il peut s'agir de tâches d'auto-enregistrement, de mot de passe oublié ou d'ID d'utilisateur oublié.
- Tâches protégées : tâches pour lesquelles l'utilisateur fournit des données de connexion valides. Par exemple, il peut s'agir de tâches de modification de mot de passe ou d'informations de profils. Pour accéder à ces tâches, l'utilisateur doit recevoir un rôle, tel que le rôle Auto-gestionnaire.

Le tableau suivant répertorie les tâches d'auto-administration par défaut, disponibles lorsque CA Identity Manager est installé.

Type de tâche	Tâches
Tâche publique	<ul style="list-style-type: none">■ Auto-enregistrement : permet à l'utilisateur de s'enregistrer sur un site Web d'entreprise.■ Réinitialisation du mot de passe oublié : permet à l'utilisateur de réinitialiser un mot de passe oublié.■ Mot de passe oublié : affiche un mot de passe provisoire qui permet à l'utilisateur de se connecter à CA Identity Manager. Lorsque l'utilisateur se connecte, il est invité à entrer un nouveau mot de passe.■ ID d'utilisateur oublié : extrait ou réinitialise un ID d'utilisateur oublié.

Type de tâche	Tâches
Tâche protégée	<ul style="list-style-type: none">■ Modifier mon mot de passe : permet à l'utilisateur de réinitialiser son mot de passe.■ Modifier mon profil : conserve les informations de profils, telles que les adresses et les numéros de téléphone.■ Modifier mes groupes : permet à l'utilisateur de s'inscrire à des groupes.■ Afficher mes rôles : affiche les rôles d'un utilisateur.■ Afficher mes tâches soumises : affiche les tâches CA Identity Manager lancées par l'utilisateur.

Configuration de tâches d'auto-administration

Le tableau suivant décrit les étapes de configuration des tâches d'auto-administration pour un environnement CA Identity Manager. Certaines de ces étapes sont facultatives.

Etape	Voir
1. Configurez un alias public dans la console de gestion pour permettre à l'utilisateur d'accéder à des tâches publiques, telles que les tâches d'auto-enregistrement, de réinitialisation de mot de passe oublié et d'ID d'utilisateur oublié.	<i>Manuel de configuration</i>
2. Configurez les tâches d'auto-administration qui s'appliquent à votre environnement.	<ul style="list-style-type: none">■ Configuration de la tâche d'auto-enregistrement (page 117)■ Configuration des tâches Réinitialisation du mot de passe oublié et ID d'utilisateur oublié (page 120)
3. Personnalisez les tâches d'auto-administration pour votre environnement.	Personnalisation de tâches d'auto-administration
4. Ajoutez des liens permettant d'accéder aux tâches d'auto-administration au site Web de votre entreprise.	Accès aux tâches d'auto-administration
5. Configurez le rôle Auto-gestionnaire. Si Par défaut, le rôle Auto-gestionnaire est affecté à tous les utilisateurs. N'effectuez cette étape que si vous souhaitez limiter les utilisateurs pouvant accéder au rôle.	<i>Manuel d'administration</i>

Configuration de la tâche d'auto-enregistrement

Pour que les utilisateurs puissent s'auto-enregistrer, vérifiez auparavant que vous disposez d'un alias pour les tâches publiques dans l'environnement CA Identity Manager. Reportez-vous au *Manuel de configuration*. Configuration de la tâche d'auto-enregistrement

Remarque : Pour éviter d'écraser la tâche d'auto-enregistrement par défaut, créez une copie de la tâche. Personnalisez la nouvelle tâche selon les besoins.

1. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration.
2. Configuration de la tâche d'auto-enregistrement
3. Dans l'onglet Rechercher, sélectionnez la fenêtre Contrat de licence de l'utilisateur final en cliquant sur Parcourir.

Modifiez la fenêtre afin qu'elle affiche un titre approprié et une URL de message.

Pour l'URL de message, utilisez une page que vous créez pour demander que les nouveaux utilisateurs acceptent les restrictions de licence de votre application.

4. Dans l'onglet Onglets, modifiez les onglets Profil et Groupes selon les besoins :
 - Si l'environnement CA Identity Manager prend en charge les organisations, [spécifiez une organisation par défaut où les profils des utilisateurs auto-enregistrés sont stockés](#). (page 118)
 - Si les tâches par défaut ne répondent pas à vos besoins métier, personnalisez les fenêtres de profil et de liste.
 - Si l'environnement CA Identity Manager prend en charge les mots de passe ou les ID d'utilisateurs oubliés, [ajoutez des champs de saisie de questions et réponses sur les mots de passe](#) (page 118).

Configuration d'une organisation par défaut pour les utilisateurs auto-enregistrés

Si votre environnement CA Identity Manager prend en charge les organisations, vous pouvez spécifier l'organisation dans laquelle CA Identity Manager crée les comptes des utilisateurs auto-enregistrés.

Remarque : Pour stocker des profils de différents types d'utilisateurs (par exemple, des clients et des fournisseurs) dans différents environnements, créez plusieurs tâches d'auto-enregistrement comportant différentes organisations par défaut. Par exemple, si des clients s'auto-enregistrent dans l'organisation des clients et des fournisseurs dans l'organisation des fournisseurs, créez deux tâches d'auto-enregistrement, telles qu'Enregistrement des clients et Enregistrement des fournisseurs. Dans chaque tâche, définissez l'organisation par défaut appropriée.

1. Si nécessaire, accédez à la fenêtre Configurer le profil de la tâche d'auto-enregistrement :
 - a. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration.
 - b. Configuration de la tâche d'auto-enregistrement
 - c. Cliquez sur l'onglet Onglets.
 - d. Cliquez sur la flèche vers la droite située en regard de l'onglet Profil.
2. Dans la fenêtre Configurer le profil, cliquez sur Parcourir en regard du champ Organisation par défaut.
3. Sélectionnez l'organisation dans laquelle de nouveaux utilisateurs doivent être créés.
4. Enregistrez vos modifications.

Ajout de questions et réponses de vérification

Pour permettre à l'utilisateur de spécifier des paires de question/réponse, qui permettent de récupérer un mot de passe ou un ID d'utilisateur oublié, ajoutez des champs de questions et de réponses à la fenêtre d'auto-enregistrement.

Remarque : Avant d'ajouter des champs Question et Réponse collectant les informations de vérification, vérifiez que les attributs logiques des paires question/réponse sont définis dans le gestionnaire d'attributs logiques des mots de passe oubliés. Les gestionnaires d'attributs logiques se définissent dans la console d'utilisateur ou de gestion. Pour plus d'informations, reportez-vous à l'aide en ligne de la console que vous utilisez.

Pour ajouter des questions et réponses de vérification :

1. Si nécessaire, accédez à la fenêtre Configurer le profil de la tâche d'auto-enregistrement :
 - a. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration.
 - b. Configuration de la tâche d'auto-enregistrement
 - c. Cliquez sur l'onglet Onglets.
 - d. Cliquez sur l'icône Modifier située en regard de l'onglet Profil.
2. Dans la fenêtre Configurer le profil standard, cliquez sur le bouton Parcourir en regard du champ Fenêtre.

La fenêtre Sélection d'une définition de fenêtre s'ouvre.
3. Sélectionnez le profil d'auto-enregistrement, puis cliquez sur le bouton Copier.
4. Spécifiez un nouveau nom et une nouvelle étiquette pour la fenêtre de profil d'auto-enregistrement personnalisée que vous créez.

La balise peut contenir des caractères ASCII (a-z, A-Z), des chiffres (0-9) ou des traits de soulignement, et commence par une lettre ou un trait de soulignement.
5. Ajoutez le nombre de lignes et de champs devant apparaître pour les questions et réponses de vérification.

Par exemple, si l'utilisateur doit fournir deux paires de question/réponse, ajoutez deux lignes et deux champs.
6. Dans les propriétés de champs de la première question, sélectionnez |Question 1| dans la liste des attributs disponibles. Configurez les propriétés de champs selon les besoins.

Remarque : Si le gestionnaire d'attributs logiques ForgottenPasswordHandler est configuré pour afficher une liste de questions que l'utilisateur peut sélectionner, spécifiez le style Sélecteur d'options.
7. Répétez l'étape 6 pour chacun des nouveaux champs que vous avez ajoutés.
8. Cliquez sur Appliquer.

La fenêtre Sélection d'une définition de fenêtre s'ouvre.
9. Vérifiez que la définition de fenêtre est sélectionnée, puis cliquez sur Sélectionner.

La fenêtre Configurer le profil apparaît.
10. Cliquez sur OK pour fermer la fenêtre Configurer le profil et retourner à l'onglet Onglets.

Configuration des tâches Réinitialisation du mot de passe oublié et ID d'utilisateur oublié

CA Identity Manager inclut des tâches par défaut qui sont inaccessibles si l'utilisateur ne peut pas accéder à son compte suite à un oubli de mot de passe ou d'ID.

- [Tâche Réinitialisation du mot de passe oublié](#) (page 120)
- [Tâche ID d'utilisateur oublié](#) (page 120)

Vous pouvez utiliser ces tâches telles qu'installées ou les personnaliser selon vos besoins.

Tâche Réinitialisation du mot de passe oublié

La tâche Réinitialisation du mot de passe oublié permet à l'utilisateur de réinitialiser un mot de passe après que CA Identity Manager a vérifié son identité. CA Identity Manager utilise deux types de questions pour vérifier l'identité d'un utilisateur.

- Des questions d'identification : déterminent l'identité de l'utilisateur. Il peut s'agir par exemple du nom complet, de l'ID ou de l'adresse électronique de l'utilisateur.
- Des questions de vérification : confirment l'identité de l'utilisateur. Selon la configuration de CA Identity Manager, l'utilisateur peut spécifier ses propres questions de vérification ou sélectionner des questions dans une liste prédéfinie.

Dans la tâche par défaut Réinitialisation du mot de passe oublié, l'utilisateur doit fournir un ID d'utilisateur et répondre à cinq questions de vérification. Chaque question de vérification, présentée dans une fenêtre séparée, est choisie de manière aléatoire dans une liste comportant cinq questions que l'utilisateur fournit pendant l'enregistrement.

Une fois que CA Identity Manager a vérifié l'identité d'un utilisateur, une fenêtre s'affiche dans laquelle l'utilisateur peut entrer un nouveau mot de passe.

Tâche ID d'utilisateur oublié

Dans la tâche ID d'utilisateur oublié par défaut, l'utilisateur doit spécifier une adresse électronique et répondre à une question de vérification pour afficher son ID d'utilisateur dans la console d'utilisateur. Chaque question de vérification, présentée dans une fenêtre séparée, est choisie de manière aléatoire dans une liste comportant cinq questions que l'utilisateur fournit pendant l'enregistrement.

Configuration des tâches Réinitialisation du mot de passe oublié et ID d'utilisateur oublié

Vous pouvez utiliser les tâches Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié telles qu'installées ou les personnaliser en fonction de votre environnement.

Vous pouvez :

- Spécifier le nombre de [questions](#) (page 121) auxquelles l'utilisateur doit répondre correctement pour que son identité soit vérifiée
- Déterminer si l'utilisateur fournit ses propres [questions de vérification](#) (page 121) ou s'il sélectionne des questions dans une liste prédéfinie
- [Définir la présentation](#) (page 124) des questions de vérification dans la fenêtre
- Demander à l'utilisateur de fournir des informations supplémentaires (par exemple, un numéro de sécurité sociale) pour [vérifier son identité](#) (page 126)
- Déterminer la manière dont l'utilisateur reçoit son [mot de passe](#) (page 129) ou son [ID d'utilisateur](#) (page 130)
- Spécifier des critères (par exemple, échouer à plus de trois tentatives de vérification) pour [verrouiller un utilisateur hors de la tâche](#) (page 127)

Collecte de paires de question/réponse pour la vérification de l'utilisateur

L'utilisateur doit fournir les paires de question/réponse utilisées pour vérifier son identité.

Vous pouvez autoriser l'utilisateur à spécifier ses propres questions ou lui demander de sélectionner des questions prédéfinies dans une liste.

Pour configurer CA Identity Manager afin de collecter les paires question/réponse, procédez comme suit :

- Ajoutez des champs de collecte de questions et de réponses aux [tâches](#) (page 117) Auto-enregistrement, Modifier mon profil et Modifier mon mot de passe.
- Configurez le gestionnaire ForgottenPasswordHandler dans la console d'utilisateur ou de gestion. Pour plus d'informations, reportez-vous à l'aide en ligne de la console que vous utilisez.

Configuration de la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié

La configuration des tâches Réinitialisation du mot de passe oublié et ID d'utilisateur oublié est similaire.

Pour configurer ces tâches :

1. Vérifiez que les éléments suivants sont configurés dans la console de gestion :
 - Alias public
Chaîne de texte que CA Identity Manager ajoute à l'URL pour l'accès aux tâches publiques, y compris les tâches Réinitialisation du mot de passe oublié et ID d'utilisateur oublié.
Remarque : Pour plus d'informations, reportez-vous au *manuel de configuration* (en anglais).
 - ForgottenPasswordHandler
Gestionnaire d'attributs logiques qui permet à l'utilisateur de créer une ou plusieurs questions de vérification ou d'en choisir dans une liste prédéfinie.
Pour plus d'informations, reportez-vous au *manuel de programmation Java* (en anglais).
Remarque : Vous pouvez également configurer l'attribut ForgottenPasswordHandler dans la console d'utilisateur. Pour plus d'informations, cliquez sur le bouton Aide de la console d'utilisateur.
2. Dans la console d'utilisateur, exécutez l'une des opérations suivantes.
 - Pour créer une copie de la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié (recommandé), choisissez Rôles et tâches, Tâches d'administration, puis Créer une tâche d'administration. Sélectionnez Créer une copie de tâche d'administration, puis recherchez la tâche à copier.
 - Pour modifier la tâche par défaut, sélectionnez Rôles et tâches, Tâches d'administration, puis Modifier la tâche d'administration. Recherchez la tâche à modifier.
CA Identity Manager affiche les tâches qui correspondent aux critères spécifiés.
3. Sélectionnez la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié.
4. Dans l'onglet Rechercher, cliquez sur Parcourir pour afficher la liste des fenêtres à modifier.
5. Sélectionnez l'une des fenêtres suivantes, puis cliquez sur Modifier :
 - Recherche du mot de passe oublié
 - Recherche de l'ID d'utilisateur oublié

6. Configurez les éléments suivants en fonction de vos besoins :
 - Fenêtre d'identification
Détermine l'identité de l'utilisateur. Il s'agit de la première fenêtre s'affichant lorsque l'utilisateur accède à la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié.
 - Fenêtres de vérification
Présente une ou plusieurs questions de vérification à l'utilisateur.
7. Spécifiez le nombre de questions auxquelles l'utilisateur doit répondre pour que son identité soit vérifiée.
Remarque : Si vous configurez CA Identity Manager pour afficher plusieurs questions de vérification dans une seule fenêtre, le nombre de questions est déterminé par le gestionnaire d'attributs logiques associé à la tâche. Le paramètre Nombre de questions ne s'applique pas.
8. Configurez les critères de verrouillage de la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié.
9. Soumettez la tâche.

Conception de fenêtres d'identification

La fenêtre d'identification est la première fenêtre qui s'affiche lorsque l'utilisateur accède à la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié.

La fenêtre d'identification par défaut invite l'utilisateur à spécifier un ID d'utilisateur. Vous pouvez ajouter des champs à la fenêtre d'identification ou en modifier les champs selon vos besoins.

Procédez comme suit:

1. Ouvrez la fenêtre de configuration de la recherche de mot de passe oublié ou de recherche d'ID d'utilisateur oublié dans la console d'utilisateur CA Identity Manager, si nécessaire :
 - a. Sélectionnez Rôles et tâches, Tâches d'administration, puis Modifier la tâche d'administration.
 - b. Sélectionnez la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié.
 - c. Dans l'onglet Rechercher, cliquez sur Parcourir pour afficher la liste des fenêtres à modifier.
 - d. Sélectionnez l'une des fenêtres suivantes, puis cliquez sur Modifier :
 - Recherche du mot de passe oublié
 - Recherche de l'ID d'utilisateur oublié

2. Entrez le texte allant apparaître au-dessus de la zone dans laquelle l'utilisateur fournit les informations de compte dans le champ Invite.
3. Sélectionnez la fenêtre appropriée dans la fenêtre Profil pour le champ Identification.
4. Modifiez la fenêtre pour inclure les attributs de votre choix que l'utilisateur doit entrer.

Conception de fenêtres de vérification

Une fois que l'utilisateur a correctement rempli la fenêtre d'identification, il est redirigé vers une fenêtre de vérification dans laquelle il doit fournir des informations afin que son identité soit vérifiée. Il peut être invité à répondre à une ou plusieurs questions ou à spécifier un attribut, tel qu'un numéro de sécurité sociale.

Si l'utilisateur doit répondre à plusieurs questions de vérification, CA Identity Manager peut afficher ces questions dans la même fenêtre ou dans des fenêtres distinctes.

Affichage simultané de plusieurs questions de vérification

Si l'utilisateur répond à plusieurs questions pour que son identité soit vérifiée, vous pouvez afficher ces questions dans une seule fenêtre.

Remarque : Si une seule fenêtre affiche plusieurs questions, le nombre de questions auxquelles l'utilisateur doit répondre est déterminé par le nombre de paires de question/réponse que vous ajoutez à la fenêtre Profil pour la première vérification, et non par le nombre de questions que vous configurez dans la fenêtre de recherche de la tâche.

Pour afficher plusieurs questions de vérification dans une seule fenêtre :

1. Configurez le gestionnaire d'attributs logiques de mot de passe oublié pour plusieurs paires de question/réponse.

Vous pouvez configurer le gestionnaire ForgottenPasswordHandler dans la console d'utilisateur ou de gestion. Pour obtenir des instructions, reportez-vous à l'aide en ligne de la console que vous utilisez.

Ajoutez des paires |VerifyQuestion1| , |VerifyAnswer1| selon le nombre de questions que vous souhaitez définir.

2. Accédez à la fenêtre Configuration de recherche du mot de passe oublié ou Configuration de recherche d'ID d'utilisateur oublié, si nécessaire.
3. Entrez le texte allant apparaître au-dessus de la zone dans laquelle l'utilisateur fournit les informations de vérification dans le champ Invite de la fenêtre de première vérification.

4. Dans le champ Fenêtre de profil pour la première vérification, sélectionnez une définition de fenêtre, telle que la fenêtre Vérification du mot de passe oublié.
5. Modifiez la définition de fenêtre pour inclure les attributs logiques de chacune des paires de question/réponse de vérification devant apparaître dans la fenêtre. Par exemple, ajoutez des champs comme suit :
`|VerifyQuestion1| - Read only.`
`|VerifyAnswer1| - Write Required.`
Remarque : Pour plus d'informations, reportez-vous à l'aide en ligne concernant le gestionnaire d'attributs `ForgottenPasswordLogical`.
6. Vérifiez que les champs Invite de la fenêtre de deuxième vérification et Fenêtre de profil de la deuxième vérification sont vides dans la fenêtre Configuration de recherche du mot de passe oublié ou Configuration de recherche d'ID d'utilisateur oublié.
7. Dans le champ Nombre de questions, entrez le nombre de questions auxquelles l'utilisateur doit répondre correctement.
8. Cliquez sur OK.

Affichage d'une seule question de vérification à la fois

Pour améliorer la sécurité, vous pouvez n'afficher qu'une seule question de vérification à la fois. Les questions suivantes ne s'affichent qu'une fois la réponse correcte fournie à la question actuelle.

Pour afficher chaque question de vérification dans une fenêtre séparée, définissez une fenêtre de première vérification et une fenêtre de deuxième vérification.

La fenêtre de première vérification s'affiche une fois que l'utilisateur a fourni une identification valide, telle qu'un ID d'utilisateur. Lorsque l'utilisateur répond correctement à une question dans la fenêtre de première vérification, CA Identity Manager affiche la fenêtre de deuxième vérification pour chaque question restante.

Pour configurer les fenêtres de première et de deuxième vérification :

1. Vérifiez que les attributs logiques `|VerifyQuestion|` et `|VerifyAnswer|` sont configurés dans le gestionnaire d'attributs logiques `ForgottenPasswordHandler`. Reportez-vous au *Manuel de programmation Java*.
2. Accédez à l'une des fenêtres suivantes, si nécessaire :
 - Fenêtre Configuration de recherche du mot de passe oublié
 - Fenêtre Configuration de recherche d'ID d'utilisateur oublié
3. Entrez le texte allant apparaître au-dessus de la zone dans laquelle l'utilisateur fournit les informations de vérification dans le champ Invite de la fenêtre de première vérification.

4. Dans le champ Fenêtre de profil pour la première vérification, sélectionnez une définition de fenêtre, telle que la fenêtre Vérification du mot de passe oublié.

Remarque : Modifiez la définition de fenêtre pour inclure les attributs logiques de chacune des paires de question/réponse devant apparaître dans la fenêtre.

5. Entrez le texte allant apparaître au-dessus de la zone dans laquelle l'utilisateur fournit les informations de vérification dans le champ Invite de la fenêtre de première vérification.

6. Sélectionnez la fenêtre Deuxième vérification du mot de passe oublié dans le champ Fenêtre de profil de la deuxième vérification.

Modifiez la fenêtre pour inclure les attributs logiques |VerifyQuestion| et |VerifyAnswer|.

Remarque : Pour utiliser une fenêtre de deuxième vérification, vous devez configurer une fenêtre de première vérification.

7. Dans le champ Nombre de questions, entrez le nombre de questions auxquelles l'utilisateur doit répondre correctement.
8. Cliquez sur OK.

Vérification d'un attribut d'utilisateur

CA Identity Manager peut vérifier l'identité d'un utilisateur en exigeant que celui-ci fournisse un ou plusieurs attributs de profil. Vous pouvez exiger ces attributs en plus des questions de vérification ou à la place.

Pour utiliser des attributs d'utilisateur dans le processus de vérification :

1. Configurez la fenêtre de vérification comme indiqué dans l'une des sections suivantes :
 - [Affichage simultané de plusieurs questions de vérification](#) (page 124)
 - [Affichage d'une seule question de vérification à la fois](#) (page 125)
2. Ajoutez un ou plusieurs champs pour collecter l'attribut d'utilisateur dans la fenêtre Vérification du mot de passe oublié ou dans une fenêtre de première vérification personnalisée si vous en avez conçue une.

Par exemple, pour collecter le matricule d'employé d'un utilisateur en plus de son ID, modifiez la fenêtre Identité de mot de passe oubliée. Ajoutez une ligne contenant un seul champ avant ou après le champ d'ID d'utilisateur. Cliquez sur la flèche vers la droite du nouveau champ pour définir les propriétés de ce champ.

Sélectionnez la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié.

Pour sécuriser la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié, vous pouvez limiter le nombre de tentatives de vérification échouées faites par l'utilisateur. Une fois que l'utilisateur dépasse le nombre maximum d'échecs de tentatives, la tâche se verrouille et il ne peut plus y accéder.

Vous pouvez déterminer ce que CA Identity Manager considère comme un échec de vérification. La définition d'une tentative échouée peut être très stricte (par exemple, fournir une réponse incorrecte à une question de vérification) ou plus indulgente pour autoriser plus d'erreurs (par exemple, une réponse mal tapée).

Remarque : Vous pouvez également configurer CA Identity Manager pour verrouiller la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié après un certain nombre de [tentatives de vérification abouties](#) (page 128). Ainsi, l'utilisateur ne peut pas utiliser la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié au lieu de mémoriser ses informations de connexion.

Configuration d'un nombre maximum d'échecs de tentatives

Pour configurer CA Identity Manager afin de verrouiller la tâche Réinitialisation du mot de passe oublié ou ID d'utilisateur oublié après des échecs de vérification :

1. Accédez à la fenêtre Configuration de recherche du mot de passe oublié, si nécessaire.
2. Configurez les critères de l'échec de vérification selon les besoins :
 - Nombre de réponses incorrectes acceptables : nombre de réponses incorrectes que l'utilisateur peut fournir avant que CA Identity Manager enregistre un échec de vérification.
 - Délai de la page de vérification : durée dont dispose l'utilisateur pour répondre à toutes les questions d'une page.

Nombre max. de tentatives pour la page de vérification : nombre de fois où l'utilisateur peut tenter de répondre aux questions d'une page.

Si une seule question apparaît par page, le nombre de tentatives pour la page de vérification correspond au nombre de tentatives de réponse d'un utilisateur à cette question.

Remarque : Spécifiez 0 pour les options qui ne s'appliquent pas.

Si l'utilisateur dépasse l'un des critères spécifiés, CA Identity Manager enregistre un échec de vérification.

3. Dans le champ Nombre maximum d'échecs de tentatives, entrez le nombre de fois consécutives où l'utilisateur peut échouer au processus de vérification avant que la tâche ne soit verrouillée.

CA Identity Manager verrouille l'accès de l'utilisateur à la tâche et peut désactiver son compte si l'utilisateur tente de vérifier son identité une fois le paramètre Nombre maximum d'échecs de tentatives atteint. Par exemple, si le nombre maximum d'échecs de tentatives est 4, l'utilisateur est bloqué et son compte est désactivé au bout du troisième échec.

4. Sélectionnez la case à cocher Désactiver l'utilisateur pour désactiver le compte de l'utilisateur en plus de verrouiller la tâche lorsque le nombre maximum d'échecs de tentatives est dépassé.
5. Dans le champ Longueur de verrouillage des échecs de tentatives, entrez le délai pendant lequel l'utilisateur est dans l'impossibilité d'utiliser la tâche s'il dépasse le nombre maximum d'échecs de tentatives.

Vous pouvez spécifier des minutes, des heures et des jours. Pour indiquer qu'aucune limite particulière ne s'applique pas, entrez 0.

Remarque : L'attribut spécifié doit être défini dans le fichier de configuration d'annuaires (directory.xml) pour l'environnement Identity Manager.

6. Dans le champ Attribut de suivi des tentatives, sélectionnez l'attribut que CA Identity Manager doit utiliser pour effectuer le suivi des tentatives de vérification.

Configuration d'un nombre maximum d'échecs de tentatives

La limitation du nombre de tentatives de vérification effectuées avec succès empêche les utilisateurs d'abuser de la tâche de réinitialisation du mot de passe ou de l'ID utilisateur. Par exemple, un utilisateur peut recourir à la tâche de réinitialisation du mot de passe oublié au lieu de s'en rappeler un conforme à une stratégie de mot de passe stricte.

Pour limiter le nombre maximum de tentatives réussies :

1. Accédez à la fenêtre Configuration de recherche du mot de passe oublié, si nécessaire.
2. Dans le champ Attribut de suivi des tentatives, sélectionnez l'attribut que CA Identity Manager doit utiliser pour effectuer le suivi des tentatives de vérification.
3. Dans le champ Nombre max. de tentatives ayant abouti, entrez le nombre de jours que l'utilisateur doit attendre avant d'utiliser la tâche.

Déterminer comment les utilisateurs réinitialisent leurs mots de passe

Une fois que CA Identity Manager a vérifié l'identité d'un utilisateur dans la tâche Mot de passe oublié, il effectue l'une des actions suivantes :

- Il redirige l'utilisateur vers une fenêtre dans laquelle il peut entrer un nouveau mot de passe (action par défaut).
- Il envoie par courriel ou affiche un mot de passe provisoire. L'utilisateur peut utiliser ce mot de passe provisoire pour se connecter à CA Identity Manager, où il est obligé de définir un nouveau mot de passe.

Pour configurer CA Identity Manager afin d'envoyer par courriel ou d'afficher un mot de passe provisoire, utilisez la tâche Mot de passe oublié à la place de la tâche Réinitialisation du mot de passe oublié.

La tâche Mot de passe oublié est associée à un gestionnaire de tâches métier, un objet Java qui forme une logique métier personnalisée, qui génère un mot de passe provisoire.

Par défaut, la tâche Mot de passe oublié affiche le mot de passe provisoire dans la console d'utilisateur.

Pour configurer la tâche Mot de passe oublié afin d'envoyer par courriel le mot de passe provisoire :

1. Dans la console de gestion, configurez des notifications électroniques pour l'environnement Identity Manager. Pour obtenir des instructions, reportez-vous au *Manuel de configuration*.
2. Dans la console d'utilisateur, sélectionnez Rôles et tâches, Tâches d'administration, Modifier la tâche d'administration.
3. Sélectionnez la tâche Mot de passe oublié.
4. Dans l'onglet Profil, cliquez sur Gestionnaires de tâches métier.
La fenêtre Gestionnaires de tâches métier apparaît. Le gestionnaire BLTHGenerateTemporaryPassword apparaît normalement dans la liste des gestionnaires.
5. Cliquez sur l'icône représentant une flèche vers la droite pour modifier les propriétés du gestionnaire.
6. Dans le champ Propriété, cliquez sur l'icône représentant un signe moins pour supprimer la propriété ShowPwdOnScreen.
7. Dans le champ Propriété, tapez de nouveau ShowPwdOnScreen.
8. Dans le champ Valeur, entrez :
false
9. Cliquez sur Ajouter.

Déterminer comment les utilisateurs récupèrent un ID d'utilisateur oublié

Après avoir vérifié l'identité d'un utilisateur, CA Identity Manager affiche l'ID de l'utilisateur.

Pour plus de sécurité, vous pouvez configurer CA Identity Manager afin d'envoyer par courriel l'ID de l'utilisateur.

Pour configurer CA Identity Manager afin d'envoyer par courriel un ID d'utilisateur :

1. Configurez l'environnement CA Identity Manager pour la prise en charge des notifications par courriel.
2. Sélectionnez Rôles et tâches, Tâches d'administration, puis Modifier la tâche d'administration.
3. Sélectionnez la tâche ID d'utilisateur oublié.
4. Dans l'onglet Profil, cliquez sur Gestionnaires de tâches métier.
La fenêtre Gestionnaires de tâches métier apparaît.
5. Cliquez sur l'icône Supprimer en regard du gestionnaire BLTHDisplayUserID pour le supprimer.

La suppression du gestionnaire BLTHDisplayUserID empêche CA Identity Manager d'afficher l'ID de l'utilisateur dans la console d'utilisateur. Pour que CA Identity Manager affiche l'ID de l'utilisateur dans la console d'utilisateur et l'envoie par courriel, ne supprimez pas le gestionnaire BLTHDisplayUserID.

Pages de déconnexion

Une page de déconnexion est une page vers laquelle un utilisateur est dirigé après avoir effectué une action dans certaines fenêtres de tâche CA Identity Manager. Par exemple, lorsque vous cliquez sur un lien Déconnexion dans la console d'utilisateur.

Pour les tâches d'auto-administration, comme les tâches de mot de passe oublié ou d'auto-enregistrement, les utilisateurs sont redirigés vers une page de déconnexion lorsqu'ils cliquent sur Annuler pour quitter la tâche ou lorsqu'ils cliquent sur OK dans un message de confirmation ou d'erreur.

Vous pouvez configurer une page de déconnexion personnalisée pour les fenêtres CA Identity Manager suivantes :

- Console d'utilisateur
- Tâches d'auto-enregistrement
- Tâches de mot de passe oublié

Important : Si CA Identity Manager est intégré à CA SiteMinder, configurez l'agent Web CA SiteMinder de manière à terminer la session dès que l'utilisateur se déconnecte de CA Identity Manager. Si vous ne configurez pas l'agent Web, CA SiteMinder peut rouvrir la session d'utilisateur.

Configuration des pages de déconnexion

Procédez comme suit:

1. Créez une ou plusieurs pages de déconnexion personnalisées.

Pour vous assurer qu'une page de déconnexion HTML est chargée à partir du serveur Web et non à partir du cache du navigateur, configurez la page de façon à rendre impossible sa mise en cache dans le navigateur. Par exemple, pour les pages HTML, vous pouvez ajouter les métabalisés suivantes à la page :

```
<META HTTP-EQUIV="Pragma" CONTENT="no-cache">  
<META HTTP-EQUIV="Expires" CONTENT="-1">
```

Important : Les métabalisés peuvent de pas toujours fonctionner avec Internet Explorer. Dans ce cas, utilisez un en-tête HTTP de contrôle de cache.

2. Dans la fenêtre d'environnements CA Identity Manager, cliquez sur le nom de l'environnement approprié.

La fenêtre Environment Properties (Propriétés de l'environnement) s'affiche.

3. Cliquez sur Advanced Settings (Paramètres avancés), puis sur Miscellaneous (Divers).

La fenêtre Miscellaneous Properties (Propriétés diverses) s'affiche.

4. Dans le champ Property (Propriété), saisissez l'une des propriétés suivantes :

- MainConsoleLogoutUrl : remplace l'URL de déconnexion par défaut dans la console principale.

Cette URL est également affichée pour les tâches d'auto-enregistrement et de mot de passe oublié si vous ne spécifiez pas les pages de déconnexion personnalisées à l'aide de la propriété *tasktagLogoutUrl*.

- `tasktagLogoutUrl` : spécifie une page de déconnexion pour une tâche publique.

Dans cette propriété, `tasktag` identifie la tâche pour laquelle vous configurez une page de déconnexion personnalisée.

Par exemple, pour configurer une page de déconnexion pour la tâche d'auto-enregistrement par défaut, entrez le suivant dans le champ Propriété :

`SelfRegistrationLogoutUrl`

Vous pouvez définir plusieurs propriétés `tasktagLogoutUrl` pour configurer des pages de déconnexion différentes pour des tâches différentes. Par exemple, lorsque vous avez des pages d'auto-enregistrement différentes pour les clients et les fournisseurs, vous pouvez définir une page de déconnexion différente pour chaque tâche.

Remarque : Vous spécifiez la balise de tâche lorsque vous configurez une tâche dans la console d'utilisateur. Pour plus d'informations, consultez le *Manuel d'administration*.

5. Dans le champ Valeur, saisissez l'URL vers laquelle les utilisateurs sont redirigés lors de la déconnexion.
6. Cliquez sur Enregistrer.

Chapitre 7: Personnalisation de la console d'utilisateur

Ce chapitre traite des sujets suivants :

[Apparences](#) (page 133)

[Composants d'une apparence](#) (page 134)

[Apparences de CA Identity Manager](#) (page 135)

[Associations d'apparence](#) (page 138)

[Création d'une apparence](#) (page 138)

[Recompilation des fichiers .jsp et redémarrage du serveur d'applications](#) (page 142)

[Utilisation de plusieurs apparences](#) (page 142)

[Modification des pages de console](#) (page 145)

Apparences

Les utilisateurs CA Identity Manager effectuent la plupart des tâches d'administration dans une console d'utilisateur. CA Identity Manager inclut les consoles d'utilisateur suivantes :

- ca12 : console d'utilisateur par défaut
- ui7 : console d'utilisateur conforme aux nouvelles normes de conception d'interface utilisateur de CA Technologies.
- imcss : console d'utilisateur alternative que vous pouvez personnaliser selon vos besoins métier.

Le nom de console est ajouté à l'URL pour chaque page de console. Par exemple, les URL suivantes correspondent à la tâche Créer un utilisateur dans les consoles ca12 et imcss, respectivement :

- <http://myserver.ca.com:8080/iam/im/neteauto/ca12/index.jsp?task.tag=CreateUser>
- <http://myserver.ca.com:8080/iam/im/neteauto/imcss/index.jsp?task.tag=CreateUser>

Remarque : CA Identity Manager génère ces URL automatiquement, une fois qu'un administrateur se connecte à la console d'utilisateur.

Vous pouvez changer une console à l'aide d'apparences. Une *apparence* est un ensemble de composants qui permettent de personnaliser l'apparence de l'interface utilisateur pour un public.

Vous pouvez modifier les aspects suivants :

- Images
- Couleurs et polices
- En-têtes et pieds de page

Dans l'environnement CA Identity Manager, vous pouvez définir plusieurs apparences et vous pouvez créer différentes apparences pour différents publics. Par exemple, les employés peuvent afficher une apparence et les partenaires peuvent en afficher une autre.

Composants d'une apparence

Les composants d'une apparence sont les suivants :

Feuille de style en cascade

Définit les fichiers CSS qui contiennent des définitions de couleur et de police.

Emplacement :

```
iam_im.ear/user_console_war/app/imcss/nom_apparence/nom_fichier.css *
```

Images

Définit un fichier graphique que vous pouvez afficher dans une page Web, comme un fichier .gif, .jpeg ou .png.

Emplacement :

```
iam_im.ear/user_console_war/app/imcss/nom_apparence/image/*
```

Fichier .properties

Définit le fichier texte qui définit les composants de l'apparence.

Emplacement :

```
iam_im.ear/user_console_war/app/imcss/nom_apparence/
```

```
iam_im.ear
```

Définit l'un des emplacements d'installation du répertoire iam_im.ear :

- WebLogic :

```
répertoire_installation_WebLogic\user_projects\domains\nom_domaine_Identity_Manager\applications\iam_im.ear\
```

- JBoss :

répertoire_installation_JBoss\jboss-
version\server\default\deploy\iam_im.ear\

- WebSphere :

was_im_tools_dir\WebSphere-ear\iam_im.ear\
was_im_tools_dir

Définit l'emplacement d'installation des outils CA Identity Manager pour WebSphere.

Remarque : Après avoir apporté des modifications au répertoire WebSphere-ear\iam_im.ear, effectuez la mise en package de ce répertoire dans un fichier Enterprise Archive (EAR), puis installez-le dans le serveur d'applications WebSphere. Pour plus d'informations, reportez-vous au *Manuel d'installation*.

Apparences de CA Identity Manager

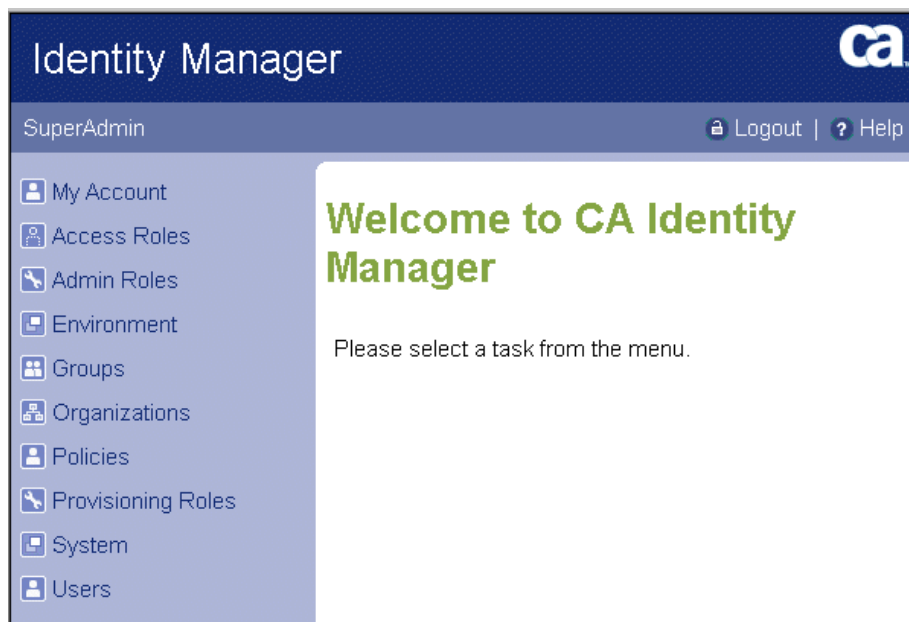
CA Identity Manager inclut les apparences suivantes :

- *idm* : définit les composants de la console d'utilisateur *idm* par défaut. Les composants qui ne sont pas définis par les apparences personnalisée prennent les valeurs des composants *idm*. Par exemple, si une apparence n'inclut aucun fichier CSS personnalisé, CA Identity Manager utilise le fichier CSS par défaut de l'apparence *idm*.

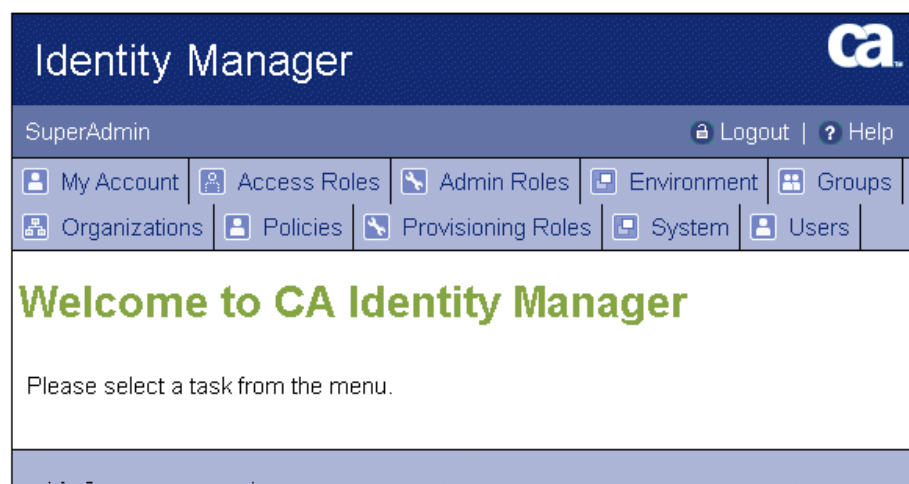
Cette apparence se trouve dans le dossier suivant :

`iam_im.ear/user_console_war/app/imcss/idm`

L'illustration suivante présente la console d'utilisateur idm :



- horizontal : définit les composants de la console d'utilisateur *horizontal*, comme dans l'illustration suivante :

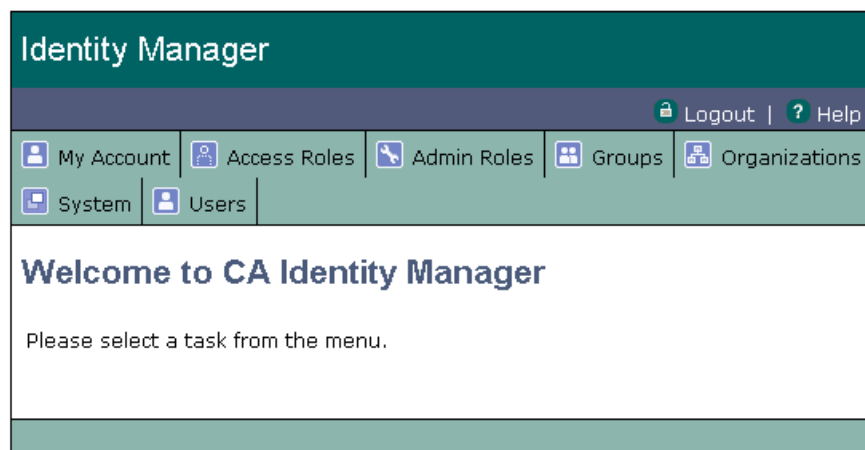


Cette interface est similaire à l'apparence *idm*, mais affiche des options de menu dans un format horizontal.

Cette apparence se trouve dans le dossier suivant :

`iam_im.ear/user_console_war/app/imcss/horizontal`

- `horizontal2` : définit les composants de la console d'utilisateur *horizontal2*, comme dans l'illustration suivante :

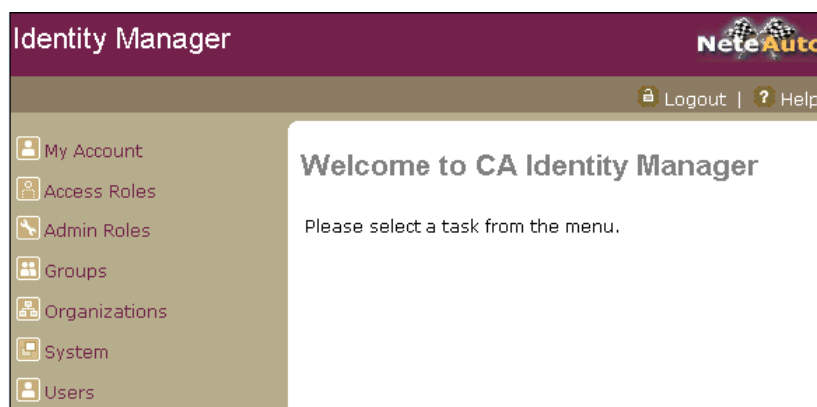


Cette interface est similaire à l'apparence *horizontale*, mais s'affiche en vert et en violet dans le même format horizontal.

Cette apparence se trouve dans le dossier suivant :

`iam_im.ear/user_console_war/app/imcss/horizontal2`

- `neteauto` : définit les composants de la console d'utilisateur *neteauto*, comme dans l'illustration suivante :



Cette interface a la même disposition que l'apparence *idm*, mais s'affiche en brun et en rouge, et affiche l'image NeteAuto.

Cette apparence se trouve dans le dossier suivant :

iam_im.ear/user_console_war/app/imcss/neteauto

Ce chapitre utilise l'apparence *neteauto* à des fins de démonstration.

Remarque : Les apparences dans les différentes illustrations s'appliquent à la console imcss.

Associations d'apparence

Une apparence peut hériter des propriétés d'une *apparence parente*. Par conséquent, vous pouvez définir un composant une fois et le réutiliser dans plusieurs apparences. Par exemple, un logo de société défini dans une apparence parente, peut se propager à toutes les apparences de la société.

Lorsqu'une console d'utilisateur est affichée, CA Identity Manager recherche l'apparence appropriée pour l'utilisateur. Lorsqu'une apparence parente est spécifiée, ses composants sont ajoutés.

Par exemple, supposez que l'apparence *corporate* inclut uniquement le logo de votre société. L'apparence *sales* inclut un JSP de pied de page personnalisé et pointe vers l'apparence parente *corporate*. Lorsque les vendeurs accèdent à CA Identity Manager, le pied de page défini dans l'apparence *sales* s'affiche, ainsi que le logo, les couleurs et les polices définis dans l'apparence *corporate*.

Création d'une apparence

Créer une apparence implique les étapes suivantes :

1. Copier une apparence existante
2. Mettre à jour les images de l'apparence
3. Mettre à jour les couleurs et les polices de l'apparence
4. Modifier le fichier `.properties`
5. Modifier le fichier `index.jsp`

Copie d'une apparence existante

Effectuez la procédure suivante pour copier une apparence existante.

Procédez comme suit:

1. Reportez-vous aux illustrations de la rubrique Apparences de CA Identity Manager et déterminez quelle apparence parmi les suivantes s'apparente le plus à celle que vous voulez créer pour votre société :

- Apparence *idm*
- Apparence *horizontal*
- Apparence *horizontal2*
- Apparence *neteauto*

A titre d'exemple, la section suivante suppose que vous avez choisi l'apparence *neteauto* et l'appelez *mon_apparence*. Le nom *mon_apparence* est le nom de l'apparence de votre société.

2. Copiez le fichier suivant :

iam_im.ear/user_console_war/app/imcss/neteauto

iam_im.ear/

Renommez-le comme suit :

iam_im.ear/user_console_war/app/imcss/mon_apparence

3. Dans le répertoire *mon_apparence*, renommez les fichiers du tableau suivant :

Nom actuel	Nouveau nom
<i>neteauto.css</i>	<i>mon_apparence.css</i>
<i>neteauto_task.css</i>	<i>mon_apparence_task.css</i>
<i>neteauto.properties</i>	<i>mon_apparence.properties</i>

Pour simplifier l'administration, le nom du fichier *.properties* et des fichiers *.css* doivent correspondre au nom de l'apparence.

Remarque : Les noms d'apparence doivent respecter la casse.

Mise à jour des images d'apparence

Procédez à la mise à jour de l'une des images .gif, .jpg ou .png dans les répertoires suivants avec les images qui correspondent à l'apparence de votre société :

- `iam_im.ear/user_console_war/app/imcss/mon_apparence/image`
- `iam_im.ear/user_console_war/app/imcss/mon_apparence/image/category`
- `iam_im.ear/user_console_war/app/imcss/mon_apparence/image/tab`
- `iam_im.ear/user_console_war/app/imcss/mon_apparence/image/tasks`

Par exemple, pour insérer le logo de votre société dans l'apparence *mon_apparence*, remplacez le fichier `logo.jpg` dans le répertoire d'images par le logo de votre société.

Il est recommandé d'utiliser les mêmes noms de fichier image, car la plupart des images sont déjà mappées avec les chemins d'accès appropriés dans le fichier `mon_apparence.properties`.

Mise à jour des couleurs et des polices d'apparence

Procédez à la mise à jour des feuilles de style en cascade de l'apparence *mon_apparence* avec les polices et le menu, l'arrière-plan, la marge et les couleurs de votre choix.

Les chemins d'accès aux feuilles de style sont les suivants :

- `iam_im.ear/user_console_war/app/imcss/mon_apparence/mon_apparence.css`
- `iam_im.ear/user_console_war/app/imcss/mon_apparence/mon_apparence_task.css`

Modification du fichier .properties

Effectuez la procédure suivante pour modifier le fichier `.properties`.

Procédez comme suit:

1. Dans le fichier `mon_apparence.properties`, remplacez toutes les références *neteauto* par *mon_apparence*.
2. Effectuez les modifications supplémentaires suivantes dans le fichier `mon_apparence.properties` :

- a. Si ce n'est pas déjà fait, spécifiez le suivant dans la section parente :

```
parent=/app/imcss/idm/im.properties
```

La section parente spécifie l'emplacement du fichier `.properties` de l'apparence parente. Dans cet exemple, l'apparence parente est *idm*.

- b. Définissez les feuilles de style en cascade comme suit :

```
stylesheet/skin.css=yourskin/mon_apparence.css
stylesheet/skin_task.css=yourskin/mon_apparence_task.css
```

- c. Poursuivez comme suit :

Si vous avez remplacé les images dans l'apparence sans les renommer, passez à l'étape d. Si vous avez renommé les images, procédez comme suit :

- Dans la section d'images d'en-tête, définissez le chemin d'accès aux images d'en-tête comme indiqué dans la section [Mise à jour des images d'apparence](#) (page 140).

Vous pouvez ajouter plusieurs entrées d'image au fichier .properties en ajoutant une entrée du type :

```
image/logo.gif=mon_apparence/image/logo.jpg
```

- Dans la section d'onglets standard, définissez le chemin d'accès aux images d'onglet comme indiqué dans la section [Mise à jour des images d'apparence](#) (page 140).
- Dans la section des boutons de corps de tâche, définissez le chemin d'accès aux images de bouton de corps de tâche comme indiqué dans la section [Mise à jour des images d'apparence](#) (page 140).

- d. Enregistrez le fichier.

Modification du fichier index.jsp

Effectuez la procédure suivante pour modifier le fichier index.jsp.

Procédez comme suit:

1. Ouvrez le fichier index.jsp dans un éditeur de texte. Ce fichier se trouve dans le dossier suivant :

```
<iam_im.ear>/user_console_war/app/imcss
```

2. Sous la section <skin:update>, ajoutez l'entrée suivante en premier :

```
<skin:skin name="mon_apparence"
filename="/app/imcss/mon_apparence/mon_apparence.properties" />
```

3. Enregistrez le fichier.

CA Identity Manager sélectionne l'apparence par défaut pour la console d'utilisateur CA Identity Manager selon la balise d'apparence répertoriée en premier dans la section <skin:update> du fichier index.jsp.

Comme noté dans la section <skin:update> suivante du fichier index.jsp, CA Identity Manager affichera la console d'utilisateur pour l'apparence *mon_apparence* :

```
<skin:update>
  <skin:skin name="mon_apparence"
    filename="/app/imcss/mon_apparence/mon_apparence.properties" />
  <skin:skin name="idm" filename="/app/imcss/idm/im.properties" />
  <skin:skin name="neteauto" filename="/app/imcss/neteauto/neteauto.properties"
    />
  <skin:skin name="horizontal"
    filename="/app/imcss/horizontal/horizontal.properties" />
  <skin:skin name="horizontal2"
    filename="/app/imcss/horizontal2/horizontal2.properties" />
</skin:update>
```

Lorsque vous voulez utiliser une apparence différente, vous devez changer l'ordre des balises d'apparence répertoriées.

Recompilation des fichiers .jsp et redémarrage du serveur d'applications

Si vous exécutez CA Identity Manager sur un serveur d'applications JBoss, vous devez recompiler les fichiers JSP et redémarrer le serveur d'applications après avoir créé une apparence, comme suit :

1. Configurez le serveur d'applications de manière à [recompiler tous les fichiers console.jsp](#) (page 205).
2. Redémarrez le serveur d'applications pour appliquer les modifications apportées à l'apparence *mon_apparence*.

Remarque : Si vous utilisez un serveur d'applications différent, n'effectuez pas cette opération.

Utilisation de plusieurs apparences

Vous pouvez vouloir définir différentes apparences pour différents ensembles d'utilisateurs. Par exemple, l'apparence des employés peut inclure le logo de la société et ses couleurs. L'apparence des fournisseurs peut inclure un logo et un schéma de couleurs différents, et afficher un pied de page spécifique à la société.

Remarque : L'intégration avec CA SiteMinder, un composant facultatif, est requise pour cette fonctionnalité.

Si CA Identity Manager est intégré à CA SiteMinder, vous pouvez utiliser une réponse CA SiteMinder pour associer l'apparence *mon_apparence* à un ensemble d'utilisateurs. La réponse est associée avec une règle dans une stratégie, qui est associée à un ensemble d'utilisateurs. Lorsque la règle se déclenche, une réponse contenant les informations sur l'apparence CA Identity Manager est envoyée pour permettre la création de la console d'utilisateur.

La procédure est la suivante :

1. Un utilisateur tente d'accéder à un environnement CA Identity Manager (protégé par CA SiteMinder).
2. CA SiteMinder authentifie et autorise l'utilisateur. La règle dans la stratégie se déclenche et envoie une réponse qui contient des informations sur l'apparence.
3. La réponse est transférée à CA Identity Manager via l'agent Web sous la forme d'une variable d'en-tête HTTP.
4. La console d'utilisateur est générée par CA Identity Manager en fonction de l'apparence.

Priorité des apparences

Plusieurs stratégies, et par conséquent plusieurs apparences, peuvent s'appliquer à un utilisateur unique. Pour vous assurer que l'apparence correcte est affichée pour l'utilisateur, affectez des priorités aux apparences.

Lorsque vous créez une réponse d'apparence, ajoutez le numéro de priorité au nom de variable d'en-tête. Ce numéro peut être compris entre 1 et 999, 1 étant la priorité la plus élevée.

Par exemple, le nom variable d'en-tête dans la réponse pour l'apparence *sales* est *skin3*. Pour l'apparence *management*, le nom de la variable d'en-tête est *skin2*. Lorsqu'un utilisateur se connecte à CA Identity Manager en tant que directeur commercial, l'apparence *management* s'affiche, car elle a une priorité plus élevée.

Création d'une réponse d'apparence

Effectuez la procédure suivante pour créer une réponse d'apparence.

Procédez comme suit:

1. Connectez-vous à l'une des interfaces suivantes en tant qu'administrateur avec des droits sur le domaine :
 - Pour CA SiteMinder Web Access Manager r12 ou version ultérieure, connectez-vous à l'interface d'administration.
 - Pour CA eTrust SiteMinder 6.0 SP5, connectez-vous à l'interface utilisateur du serveur de stratégies.

Remarque : Pour plus d'informations sur l'utilisation de ces interfaces, consultez la documentation de la version de CA SiteMinder que vous utilisez.

2. Identifiez le domaine de stratégie qui protège l'environnement CA Identity Manager. Le nom de domaine est au format suivant :

*nom_environnement*Domaine

nom_environnement

Définit le nom de l'environnement CA Identity Manager.

Par exemple, lorsque le nom de l'environnement CA Identity Manager est *employés*, le nom de domaine est *employés*Domaine.

Remarque : Le domaine de stratégie doit être associé à l'annuaire d'utilisateurs qui contient les utilisateurs CA Identity Manager qui utiliseront l'apparence.

3. Affichez les domaines du domaine.

Les domaines suivants sont affichés selon les fonctionnalités que vous avez configurées pour l'environnement :

- *nom_environnement_ims_realm* : protège l'environnement CA Identity Manager.
- *nom_environnement_pub_realm* : permet la prise en charge des tâches publiques, comme les tâches d'auto-enregistrement et de mot de passe oublié.

Ce domaine s'affiche uniquement si vous avez configuré un alias public.

4. Créez une règle dans chaque domaine. Spécifiez les valeurs ci-dessous.

- Ressource : /*
- Actions : GET, POST

Pour simplifier l'administration des apparences, incluez l'apparence dans le nom de la règle. Par exemple, lorsque le nom d'apparence est *mon_apparence*, créez une règle *mon_apparence*.

5. Créez une réponse pour le domaine avec les attributs de réponse suivants :
 - Attribut : WebAgent-HTTP-Header-Variable
Ajoute un nouvel en-tête HTTP à la réponse.
 - Type d'attribut : Statique
 - Nom de la variable : entrez un des noms de variables suivants :
 - skin : utilisez cette variable lorsque tous les utilisateurs CA Identity Manager affichent la même apparence.
 - skinx : utilisez cette variable si vous avez plusieurs apparences. Le **x** représente la priorité comprise entre 1 et 999, 1 étant la priorité la plus élevée.
 - Valeur de la variable : spécifiez le nom de l'apparence.
6. Créez une stratégie dans le domaine de stratégie avec les valeurs suivantes :
 - Utilisateurs : spécifiez les utilisateurs qui peuvent afficher l'apparence. Par exemple, si les membres de l'organisation des ventes peuvent afficher l'apparence, assurez-vous de spécifier ou=sales dans la stratégie.
 - Règles : ajoutez les règles que vous avez créées à l'étape 4. Associez chaque règle à la réponse que vous avez créée à l'étape 5.

Modification des pages de console

Pour modifier la disposition de la console d'utilisateur ou ajouter des liens aux en-têtes ou aux pieds de page, vous pouvez modifier les pages de console suivantes :

- [index.jsp](#) : (page 147) masque ou affiche les en-têtes et les pieds de page dans la console principale. Définit également les apparences CA Identity Manager disponibles.

Le fichier index.jsp se trouve sous `<iam_im.ear>`
`/user_console_war/app/imcss/`

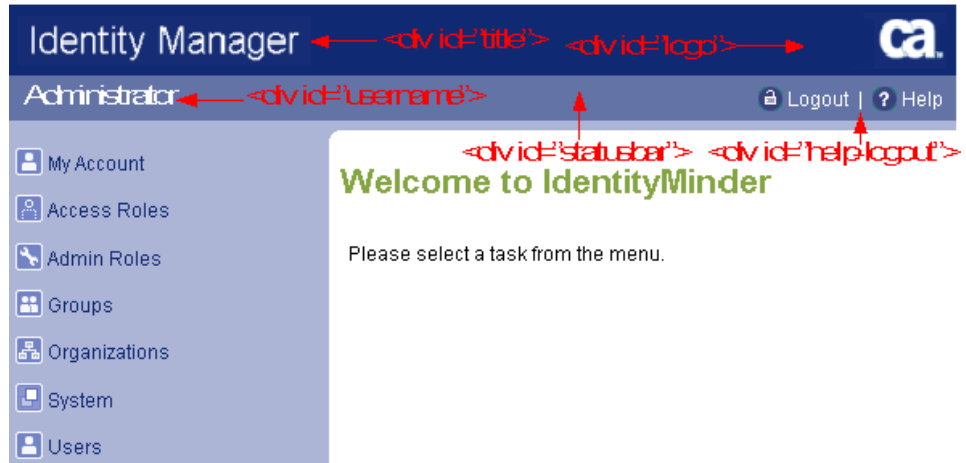
- [head.jsp](#) : (page 146) contient le code pour l'en-tête dans la page principale de la console d'utilisateur.
- `home.jsp` : contient le message de confirmation pour une tâche particulière.

Les fichiers head.jsp et home.jsp se trouvent sous `<iam_im.ear>`
`/user_console_war/app/imcss/component`

Remarque : Si CA Identity Manager est exécuté sur un serveur d'applications JBoss, vous devez manuellement [recompiler les fichiers JSP](#) (page 205) que vous modifiez avant que les modifications soient appliquées.

Modification de l'en-tête dans la console d'utilisateur CA Identity Manager

Utilisez le fichier `head.jsp`, qui se trouve sous `<iam_im.ear>/user_console_war/app/imcss/component`, pour modifier l'en-tête dans la console d'utilisateur. L'en-tête peut contenir des images, des liens, un titre, des couleurs et des polices. L'illustration suivante présente les marqueurs `<div id>` dans le fichier `head.jsp`, qui génèrent l'en-tête pour l'apparence `idm` :



Pour mettre à jour l'en-tête, modifiez le code pour les entrées suivantes dans le fichier `head.jsp` :

- `<div id="title">`
- `<div id="logo">`
- `<div id="statusbar">`
- `<div id="username">`
- `<div id="help-logout">`

Par exemple, pour changer le lien vers lequel les utilisateurs sont renvoyés lorsqu'ils cliquent sur l'image de logo qui s'affiche dans l'en-tête de la console d'utilisateur, remplacez l'URL dans le code suivant par l'URL de la page d'accueil de votre société.

```
<div id="logo">  
<a href="http://www.yourcompany.com/"><skin:img altKey="console.logo"  
titleKey="console.logo" src="logo.gif" width="93" height="33" border="0" /></a>  
</div>
```

Remarque : Après avoir modifié le fichier `head.jsp`, assurez-vous de [recompiler les fichiers .jsp](#) (page 142).

Modification et affichage du pied de page

Pour modifier et afficher le pied de page, procédez comme suit :

- Insérez le code HTML du pied de page dans le fichier `index.jsp` qui se trouve sous `iam_im.ear/user_console_war/app/imcss`.
- Modifiez le fichier CSS de l'une des apparences (*idm*, *horizontal*, *horizontal2* et *neteauto*) de manière que CA Identity Manager puisse afficher le pied de page.

Insertion du code HTML de pied de page dans le fichier `index.jsp`

Effectuez la procédure suivante pour insérer le code HTML du pied de page dans le fichier `index.jsp`.

Procédez comme suit:

1. Ouvrez le fichier `index.jsp` dans un éditeur de texte.
2. Sous la section `<div id="foot">` à la fin du fichier, ajoutez le code HTML pour le pied de page de l'apparence *mon_apparence* entre les marqueurs `<div>` et `</div>`.
3. Enregistrez le fichier.

Modification de la feuille de style en cascade pour l'affichage d'un pied de page

Utilisez le fichier de feuille de style en cascade de chaque apparence (*idm*, *horizontal*, *horizontal2* et *neteauto*) pour configurer l'affichage du pied de page. Ces fichiers CSS sont stockés dans le dossier suivant :

```
iam_im.ear/user_console_war/app/imcss/
```

Par défaut, le pied de page s'affiche dans les apparences *horizontal* et *horizontal2*, mais pas dans les apparences *idm* ou *neteauto*.

Actuellement, l'apparence *mon_apparence* n'affiche pas le pied de page, car il s'agit d'une copie de *neteauto*, qui utilise le fichier `idm.css` pour afficher les pieds de page. Les fichiers `neteauto.css` et `mon_apparence.css` contiennent des substitutions de couleur uniquement et importent le fichier `idm.css` pour gérer d'autres fonctions d'affichage comme l'affichage des pieds de page. Dans l'apparence *idm* affichée ci-après, la section `#foot` du fichier `idm.css` indique que le pied de page est désactivé :

```
#foot {  
    display: none;
```

Dans l'apparence horizontal affichée ci-après, la section #foot du fichier horizontal.css indique que le pied de page est activé :

```
#foot {  
    border: 1px solid black;  
    background-color: #AEB6D8;  
    padding: 4px;  
    display: block; /* to override parent */
```

La référence `display: block` indique que CA Identity Manager affiche le pied de page.

Pour que l'apparence *mon_apparence* affiche le pied de page :

- Ajoutez le code suivant dans `mon_apparence.css` :

```
/*CONSOLE FOOTER*/  
#foot {  
    display: block;  
}
```

Dans cette section, vous pouvez également modifier la bordure du pied de page, la couleur de l'arrière-plan et le remplissage.

Chapitre 8: Aide personnalisée

CA Identity Manager vous permet de créer une aide personnalisée pour les tâches et les onglets que vous avez personnalisés dans la console d'utilisateur. Pour implémenter l'aide personnalisée, vous pouvez créer un système d'aide contextuel avec des fichiers d'aide HTML personnalisés ou des pages Wikis et rediriger les liens d'aide dans la console d'utilisateur.

Cette fonctionnalité vous permet également de traduire une aide par défaut de l'anglais vers une autre langue.

Ce chapitre traite des sujets suivants :

[Fonctionnement de l'aide personnalisée](#) (page 149)

[Utilisation de l'aide pour déterminer le lien à utiliser](#) (page 151)

[Personnalisation de l'Aide](#) (page 152)

[Exemples d'utilisation de l'Aide personnalisée](#) (page 152)

Fonctionnement de l'aide personnalisée

CA Identity Manager utilise des groupes de ressources pour remplacer les fichiers d'aide par défaut et pour créer des liens vers l'aide contextuelle personnalisée.

A l'aide du format défini, vous pouvez créer un groupe de ressources et le placer dans le dossier iam_im.ear. Lorsqu'un utilisateur clique sur un lien d'aide, CA Identity Manager recherche dans tous les groupes de ressources applicables les correspondances d'aide personnalisée. S'il n'y a aucune correspondance d'aide personnalisée, CA Identity Manager fournit l'aide par défaut à l'utilisateur.

Si un utilisateur international clique sur un lien d'aide et un groupe de ressources spécifique à une langue a été créé, CA Identity Manager vérifie les paramètres régionaux de son navigateur et ouvre le lien d'aide correspondant à sa langue. S'il n'y a aucune correspondance dans le groupe de ressources spécifique à sa langue, l'utilisateur est dirigé vers l'aide en anglais par défaut.

Remarque : Le contenu des pages personnalisées n'est pas affiché lorsque vous effectuez des recherches dans l'aide par défaut ou affichez l'index de l'aide.

Format de l'aide personnalisée

Le groupe de ressources du lien d'aide utilise une paire clé-valeur pour déterminer la page d'aide vers laquelle diriger l'utilisateur. Pour l'aide personnalisée, les balises sont utilisées comme ID de clés et l'URL de la page Web personnalisée est la valeur. La syntaxe du groupe de ressources de lien d'aide peut être :

balise_tâche.balise_page=URL_aide

balise_tâche.@balise_définition_page=URL_aide

Une balise est l'identificateur unique d'une tâche, d'une fenêtre ou d'un onglet. Les paramètres pour la paire clé-valeur sont définis comme suit :

balise_tâche

Balise active de la tâche.

balise_page

Balise active de la recherche ou de l'onglet.

balise_définition_page

Balise de définition de la recherche active ou de l'onglet.

URL_aide

L'URL d'aide est une URL absolue (<http://www.neteauto.com>) ou une URL relative qui pointe vers le contenu sur le serveur CA Identity Manager (</iam/im/help/customhelp.html>).

Exemple :

`ModifyUser.Profile=/iam/im/userprofile.html`

Expressions d'aide personnalisées

Les expressions suivantes ont une signification particulière lorsque vous les utilisez dans des groupes de ressources d'aide personnalisés :

Expression	Signification
*	Utilisé pour la mise en correspondance avec une balise de tâche, une balise de page ou une balise de définition de page.
<code>\${task}</code>	Utilisé dans l'URL d'aide. Remplacé par la balise de tâche de la page active.
<code>\${page}</code>	Utilisé dans l'URL d'aide. Remplacé par la balise de page de la page active.
<code>\${pagedef}</code>	Utilisé dans l'URL d'aide. Remplacé par la balise de définition de page de la page active.

Exemple :

```
*.*=http://www.help.com/Wiki.jsp?page=${task}_${page}
```

Les expressions \$task et \$page sont remplacées par la balise de tâche et la balise de page pour la page Web actuelle à partir de laquelle l'utilisateur a cliqué sur le lien d'aide. Par exemple, si un utilisateur clique sur le lien d'aide à partir de l'onglet Profil de la tâche Créer un groupe, l'URL d'aide ouvre la page d'aide http://www.help.com/Wiki.jsp?page=CreateGroup_Profile.

Utilisation de l'aide pour déterminer le lien à utiliser

Lorsqu'un utilisateur clique sur un lien d'aide, CA Identity Manager effectue des vérifications pour déterminer l'URL d'aide à utiliser. Ces vérifications sont effectuées du cas le plus spécifique au plus général. Le groupe renvoyant la meilleure correspondance aux paramètres régionaux de l'utilisateur est utilisé.

L'ordre des vérifications pour un lien d'aide est le suivant :

1. [TaskTag].[PageTag]
2. [TaskTag].@[PageDefinitionTag]
3. *.*[PageTag]
4. *.*@[PageDefinitionTag]
5. [TaskTag].*
6. *.*

Exemple :

```
*.*=http://www.help.com/Wiki.jsp?page=${task}_${page}
```

Correspond à tous les éléments et inclut des balises de tâche et de page actives dans le lien d'aide généré.

Exemple :

```
ModifyUser.Profile=/iam/im/userprofile.html
```

Correspond à l'onglet Profil de la tâche Modifier un utilisateur et renvoie l'utilisateur à l'URL relative </iam/im/userprofile.html>.

Exemple :

```
*.@Profile=/iam/im/profile.html
```

Correspond à tous les onglets dérivés de la définition de l'onglet Profil sans correspondance spécifique, et renvoie les utilisateurs à l'URL relative </iam/im/profile.html>.

Personnalisation de l'Aide

L'Aide personnalisée vous permet de fournir des pages d'Aide ciblées à vos utilisateurs lorsqu'ils accèdent à des environnements CA Identity Manager personnalisés ou localisés.

Procédez comme suit:

1. Créez des pages d'Aide personnalisée et hébergez-les sur un site Web.
2. Créez un groupe de ressources avec des ID de clé mappés vers les pages d'Aide personnalisées. Nommez le groupe de ressources comme suit :
`help_NomEnvironnement_IdentificateurLangue.properties`

Remarque : L'identificateur de langue est une abréviation facultative de deux caractères décrivant une langue.

3. Placez le fichier `.properties` dans le répertoire
`iam_im.ear/config/com/netegrity/config`.

Remarque : Si vous localisez l'Aide dans plusieurs langues, créez un groupe de ressources pour chaque langue.

4. Redémarrez le serveur CA Identity Manager.

L'Aide personnalisée remplace désormais l'Aide par défaut lorsque vos utilisateurs cliquent sur les liens d'Aide de la console d'utilisateur CA Identity Manager.

Dans le cas des Aides internationalisées, les utilisateurs dont les préférences de paramètres régionaux du navigateur sont définies sur une autre langue seront dirigés vers l'Aide personnalisée appropriée.

Exemples d'utilisation de l'Aide personnalisée

Cette section fournit plusieurs exemples de situations dans lesquelles l'Aide personnalisée peut répondre aux besoins de votre entreprise liés à la localisation.

Exemple de personnalisation de l'Aide

Vous avez déployé un environnement CA Identity Manager avec des fenêtres personnalisées pour les utilisateurs, les groupes et les organisations. Le contenu de l'Aide est statique et concerne uniquement l'environnement par défaut. Vous voulez donc écrire votre propre contenu d'Aide pour refléter la personnalisation de l'environnement.

Procédez comme suit:

1. Ecrivez des pages d'Aide personnalisées pour chaque tâche et onglet personnalisé.
2. Hébergez les pages sur un site Web.
3. Créez un groupe de ressources et placez le fichier .properties dans le répertoire iam_im.ear/config/com/netegrity/config.
4. Redémarrez le serveur CA Identity Manager.

Par exemple, si le nom d'environnement est neteauto, créez le groupe de ressources help_neteauto.properties :

```
*.UserProfile=http://www.neteauto.com/imhelp/user.html
```

```
*.GroupProfile=http://www.neteauto.com/imhelp/group.html
```

```
*.OrgProfile=http://www.neteauto.com/imhelp/org.html
```

Les liens d'Aide pour l'environnement neteauto permettent d'accéder à l'Aide par défaut, sauf pour les onglets Profil des tâches Modifier un utilisateur, Modifier une organisation et Modifier un groupe.

Exemple de création d'Aide au format Wiki

Vous avez un environnement CA Identity Manager personnalisé et souhaitez accorder aux utilisateurs l'accès à un système d'Aide contextuel riche. Pour cela, vous créez un Wiki pour l'environnement que les utilisateurs peuvent consulter via les liens d'Aide.

Procédez comme suit:

1. Ecrivez le contenu du Wiki pour votre environnement personnalisé.
2. Créez un groupe de ressources et placez le fichier .properties dans le répertoire iam_im.ear/config/com/netegrity/config. Le groupe de ressources doit avoir une entrée unique :

```
*.*=http://www.neteauto.com/wiki.jsp?page=${task}-${page}
```

Les liens d'Aide lancent le Wiki avec une page spécifique pour la tâche et l'onglet.

3. (Facultatif) Si la page n'a pas encore été créée, l'utilisateur peut entrer les détails de la tâche et de l'onglet.
4. Redémarrez le serveur CA Identity Manager.

Exemple de localisation de l'Aide

Un client au Japon a acheté une version localisée de CA Identity Manager. Cependant, toute l'Aide est en anglais. Il veut donc écrire son Aide personnalisée en japonais et l'implémenter dans la console d'utilisateur.

Procédez comme suit:

1. Ecrivez des pages d'Aide personnalisées pour chaque tâche et onglet.
2. Hébergez les pages de l'Aide personnalisée sur un site Web.
3. Créez un groupe de ressources et placez le fichier .properties dans le répertoire iam_im.ear/config/com/netegrity/config.

Par exemple, si le nom d'environnement est neteauto, créez le groupe de ressources help_neteauto.properties :

```
ModifyUser.*=http://www.neteauto.jp/modifyuser.html
```

```
ModifyGroup.*=http://www.neteauto.jp/modifygroup.html
```

4. Redémarrez le serveur CA Identity Manager.

Les liens d'Aide dans la console d'utilisateur renvoient aux pages d'Aide personnalisées propres à une langue, qui sont hébergées sur le site Web www.neteauto.jp.

Exemple d'internationalisation de l'Aide

Une société internationale a acheté CA Identity Manager et doit prendre en charge des utilisateurs en anglais, en espagnol et en français. Les environnements CA Identity Manager peuvent être internationalisés, mais l'Aide est écrite en anglais. Vous voulez écrire une version de l'Aide dans chaque langue et la mettre à la disposition des utilisateurs en fonction de leur langue.

Procédez comme suit:

1. Ecrivez des pages d'Aide personnalisées pour chaque tâche et onglet, dans chaque langue.
2. Hébergez les pages de l'Aide personnalisée sur un site Web.

3. Créez deux groupes de ressources selon les paramètres régionaux définis et placez les fichiers .properties dans le répertoire iam_im.ear/config/com/netegrity/config.

Par exemple, si l'environnement est nommé neteauto, créez les groupes de ressources help_neteauto_es.properties pour l'espagnol et help_neteauto_fr.properties pour le français.

4. Redémarrez le serveur CA Identity Manager.

Les utilisateurs dont les préférences de paramètres régionaux du navigateur sont définies sur l'espagnol ou le français sont renvoyés vers l'Aide personnalisée appropriée à leur langue. Tous les autres utilisateurs sont renvoyés vers l'Aide en anglais par défaut.

Chapitre 9: Localisation de CA Identity Manager

Ce chapitre traite des sujets suivants :

[Introduction](#) (page 157)

[Groupes de ressources](#) (page 157)

[Exemples d'environnements CA Identity Manager localisés](#) (page 160)

[Restrictions sur l'utilisation de jeux de caractères internationaux](#) (page 161)

[Configuration de la prise en charge de la localisation](#) (page 162)

[Affichage de CA Identity Manager dans différentes langues](#) (page 171)

[Définition de l'en-tête HTTP imlanguage dans une réponse CA SiteMinder](#) (page 172)

Introduction

Vous pouvez localiser les éléments suivants dans la console d'utilisateur :

- Les invites, les boutons, le texte, les onglets et les titres affichés dans la console d'utilisateur
- Les messages de validation, de statut et d'erreur, ainsi que les instructions affichées pour les utilisateurs CA Identity Manager
- Les notifications par courriel
- Les graphiques
- Les fonctionnalités personnalisées créées avec les API CA Identity Manager

Remarque : Les rapports CA Identity Manager ne sont pas localisés.

Groupes de ressources

Un *groupe de ressources* est un fichier CA Identity Manager qui associe des éléments d'interface utilisateur à des chaînes de texte spécifiques aux paramètres régionaux. Dans ce fichier, un ID de clé est affecté à un élément d'interface utilisateur, qui est associé à une chaîne de texte spécifique aux paramètres régionaux.

Lorsque CA Identity Manager détecte un élément avec un ID de clé dans une fenêtre, telle qu'une fenêtre de profil de tâche d'administration, la valeur associée est affichée à partir du groupe de ressources.

Par exemple, l'entrée pour un bouton Soumettre dans un groupe de ressources CA Identity Manager est la suivante :

```
global.button.submit=Soumettre
```

L'ID de clé est `global.button.submit` et la valeur est `Soumettre`. Lorsque CA Identity Manager détecte l'ID de clé `global.button.submit` dans une définition de fenêtre d'interface utilisateur, le mot `Soumettre` s'affiche.

Tenez compte des informations suivantes concernant les ID de clés :

- Les éléments de la console d'utilisateur peuvent avoir uniquement un ID de clé, et les ID de clés doivent être uniques pour un groupe de ressources.

- Les ID de clés doivent respecter la casse et contenir uniquement des caractères US-ASCII sans espaces. Ils peuvent toutefois contenir plusieurs chaînes séparées par des points. Par exemple, l'ID de clé pour le nom de champ Service peut ressembler à l'ID suivant :

attribute.displayname.department

- CA Identity Manager prend en charge deux formats pour spécifier les ID de clés dans les fenêtres de tâche d'administration.

- Utilisation d'une syntaxe incluant le nom du groupe de ressources

Cette méthode vous permet de spécifier le nom d'un groupe de ressources personnalisé. Vous pouvez utiliser un groupe de ressources personnalisé pour séparer des mappages personnalisés du groupe de ressources par défaut.

La syntaxe est la suivante :

`#{bundle=groupe_ressources:key=ID_clé}`

Dans cet exemple :

bundle=groupe_ressources

Identifie le groupe de ressources qui inclut le mappage de chaîne de texte pour l'ID de clé, si vous utilisez un groupe de ressources personnalisé.

Remarque : Créez les groupes de ressources personnalisés dans `iam_im.ear/custom/resourceBundles`, puis référez-les comme `resourceBundles.MyResourceBundle`.

Les noms de groupe utilisent la syntaxe de localisation Java standard. Ils ne doivent pas inclure l'extension `.properties`, mais doivent être complet par rapport à `iam_im.ear/custom`.

Cette paire nom/valeur est facultative. Vous ne devez pas spécifier un groupe de ressources si l'ID de clé est défini dans le groupe de ressources de base `IMSResources.properties`. Dans ce cas, les ID de clés dans la fenêtre de tâche d'administration sont :

`#{key=ID_clé}`

key=ID_clé

Identifie l'ID clé mappé à la chaîne de texte à afficher. Le mappage doit exister dans un groupe de ressources.

Une entrée d'ID de clé complète ressemble à l'exemple suivant :

`#{bundle=resourceBundles.MyResourceBundle:key=attribute.displayname.department}`

- Utilisation du préfixe `imstask.label`

`imstask.label.nom_élément`

Exemple :

`imstask.label.attribute.displayname.department`

Lorsque vous utilisez cette méthode, `attribute.displayname.department` doit être affiché dans le groupe de ressources.

Remarque : Si vous [créez des fichiers de localisation personnalisés](#) (page 169), vous utilisez un outil de conversion pour changer la valeur mappée vers un ID de clé pour une langue différente. Par exemple, pour afficher le bouton Submit en français, l'outil de conversion remplace la valeur associée à l'ID de clé `global.button.submit` dans le groupe de ressources français comme suit :

`global.button.submit=Soumettre`

Exemples d'environnements CA Identity Manager localisés

CA Identity Manager inclut les fichiers permettant de créer des versions traduites de la console d'utilisateur. Vous pouvez utiliser ces exemples tels quels ou les utiliser comme modèle pour créer une console d'utilisateur traduite personnalisée. Les langues suivantes sont prises en charge :

- Français
- Allemand
- Italien
- Japonais
- Coréen
- Polonais
- Portugais
- Norvégien
- Chinois simplifié
- Espagnol

Les fichiers qui prennent en charge ces versions linguistiques se trouvent à l'emplacement suivant :

outils_admin\samples\Localization\langue

outils_admin

Spécifie l'emplacement d'installation des outils d'administration de CA Identity Manager.

Les outils d'administration sont situés aux emplacements par défaut ci-après.

Windows : <chemin_d'installation>\tools

UNIX : <chemin_d'installation2>/tools

langue

Spécifie la langue que vous souhaitez utiliser.

Restrictions sur l'utilisation de jeux de caractères internationaux

Les entrées suivantes doivent contenir des caractères ASCII uniquement :

- Noms d'environnement et alias
- Noms d'annuaires
- Balises de tâche
- Noms de classe utilisés dans les API suivantes :
 - API d'écouteur d'événements
 - API de règle de notification
 - API d'attribut logique
 - API de solveur d'organisation de flux de travaux
- Noms d'attribut logique et physique utilisés par l'attribut logique
- URL du contrat de licence d'utilisateur final affiché lors de l'auto-enregistrement des utilisateurs

Remarque : Le contrat de licence d'utilisateur final peut contenir des jeux de caractères internationalisés.

Configuration de la prise en charge de la localisation

Pour configurer l'utilisation d'une version traduite de CA Identity Manager, effectuez les opérations suivantes :

1. Vérifiez que le système hébergeant CA Identity Manager remplit les conditions définies dans la rubrique [Conditions requises pour la localisation](#) (page 163).
2. Si CA Identity Manager est intégré à CA SiteMinder, configurez l'agent Web CA SiteMinder pour la localisation.
3. Si CA Identity Manager est exécuté sur un serveur d'applications JBoss, [modifiez le fichier server.xml de Tomcat](#) (page 166).
4. Configurez la variable PATH.
5. Effectuez l'une des étapes suivantes :

- Si vous utilisez l'un des exemples d'environnements localisés, reportez-vous à la rubrique [Utilisation des exemples d'environnements localisés](#) (page 167).

CA Identity Manager installe les versions traduites de la console d'utilisateur et de l'Aide en ligne dans les langues suivantes :

- Français
- Allemand
- Italien
- Coréen
- Japonais
- Polonais
- Chinois simplifié
- Espagnol

Vous pouvez utiliser ces fichiers tels quels ou les utiliser comme modèle pour créer un environnement personnalisé dans l'une de ces langues.

- Si vous voulez traduire CA Identity Manager dans une langue pour laquelle un exemple n'est pas disponible ou si vous voulez traduire un environnement hautement personnalisé, reportez-vous à la rubrique [Création de fichiers de localisation personnalisés](#) (page 169).
6. Traduisez les composants supplémentaires suivants, si nécessaire :
 - [Modèles de courriel](#) (page 170)
 - [Apparences personnalisées](#) (page 170)
 - [Code personnalisé](#) (page 170)

Conditions requises pour la localisation

Avant de configurer CA Identity Manager pour la localisation, tenez compte des points suivants :

- CA Identity Manager doit être installé et configuré, et un ou plusieurs environnements doivent exister.

Remarque : Si vous utilisez CA SiteMinder et si votre environnement gère des utilisateurs avec des ID multioctets, ces derniers doivent s'authentifier avec un schéma d'authentification CA SiteMinder prenant en charge les caractères multioctets. Par exemple, ils peuvent utiliser l'authentification basée sur un formulaire HTML. Le schéma d'authentification de base ne prend pas en charge l'authentification multioctets. Pour plus d'informations sur la configuration d'un schéma d'authentification pour CA Identity Manager, consultez le chapitre sur la configuration des fonctionnalités CA SiteMinder pour CA Identity Manager dans le *Manuel de configuration*.

- Si vous utilisez CA SiteMinder, vérifiez qu'une version du serveur de stratégies CA SiteMinder prise en charge est installée et configurée.
- Vérifiez également que l'annuaire d'utilisateurs est configuré pour prendre en charge la localisation. Pour plus d'informations, consultez la documentation du référentiel d'utilisateurs que vous utilisez.

- Si vous utilisez un annuaire LDAP comme référentiel d'utilisateurs, vérifiez qu'il n'applique pas un contrôle de 7 bits à l'ID d'utilisateur, au mot de passe et à l'attribut de courriel. Pour plus d'informations, consultez la documentation de l'annuaire LDAP que vous utilisez.
- Si vous utilisez un référentiel d'objets de base de données Oracle, vérifiez que le composant de jeu de caractères du paramètre NLS_LANG et le codage de caractère de base de données sont définis sur AL32UTF8, un jeu de caractères multioctets.

CA Identity Manager utilise un codage de caractère multioctets (UTF-8). Si vous spécifiez une définition de caractère codé sur un octet, les caractères peuvent apparaître endommagés dû à un espace de caractère insuffisant.

Remarque : Pour obtenir des instructions sur la définition du paramètre NLS_LANG et sur le codage de caractère de base de données, consultez la documentation Oracle.

- CA Identity Manager inclut des outils que vous utilisez pour localiser un nouvel environnement. Pour que ces outils fonctionnent, les logiciels suivants sont requis :

Outil native2ascii du kit de développement logiciel Java

Cet outil permet de convertir les séquences d'échappement Unicode. La localisation impliquant principalement la conversion de fichiers .properties, les outils traitent tous les fichiers ASCII avec des séquences d'échappement Unicode.

Pour configurer les outils de localisation, installez un kit de développement Java comprenant l'outil native2ascii sur le système sur lequel les outils d'administration CA Identity Manager sont installés.

Pour plus d'informations sur l'outil native2ascii, accédez à la page du site Web Java :

<http://java.sun.com/j2se/1.5.0/docs/guide/intl/index.html>

ant 1.7 ou version ultérieure

Configuration de l'agent Web CA SiteMinder

Configurez le codage pour les valeurs d'en-tête HTTP que l'agent Web CA SiteMinder transfère à CA Identity Manager en définissant le paramètre `HTTPHeaderEncodingSpec` comme suit :

`HTTPHeaderEncodingSpec=spécification_codage, spécification_encapsulation`

où *spécification_codage* est une chaîne de texte qui représente le type de codage UTF-8 ou Shift-JIS, et *spécification_encapsulation* la spécification de l'encapsulation, qui doit être RFC-2047.

Exemple :

`HTTPHeaderEncodingSpec="Shift-JIS,RFC-2047"`

Remarque : Si aucune valeur n'est spécifiée dans le paramètre `HTTPHeaderEncodingSpec`, le codage est UTF-8 sans encapsulation.

Vous pouvez configurer le paramètre `HTTPHeaderEncodingSpec` de manière centralisée dans l'objet de configuration d'agent ou localement pour chaque agent Web, dans le fichier `WebAgent.conf`.

Remarque : Pour plus d'informations, consultez le Manuel *CA SiteMinder Web Access Manager Web Agent Configuration Guide*.

Modification du fichier server.xml de JBoss

Si CA Identity Manager est hébergé sur un serveur d'applications JBoss, la localisation de CA Identity Manager vers un jeu de caractères multioctets requiert une modification de la configuration. Le fichier server.xml de JBoss doit spécifier le codage UTF-8 pour l'URI.

Changez le codage dans l'élément Connector pour le connecteur HTTP/1.1 dans l'un des fichiers suivants :

- Pour JBoss 5.0.x :
répertoire_installation_jboss/server/default/deploy/jboss-web.deployer/server.xml
- Pour JBoss 5.1.x :
répertoire_installation_jboss/server/default/deploy/jbossweb.sar/server.xml

Spécifiez le codage UTF-8 pour l'URI comme suit :

```
<Server ...>
  <Service ...>
    <Connector port="8080" ... URIEncoding="UTF-8"/>
    ...
  </Connector>
</Service>
</Server>
```

Configuration de la variable PATH

CA Identity Manager inclut des versions traduites de la console d'utilisateur par défaut et l'Aide en ligne que vous pouvez utiliser dans des environnements localisés. Toutefois, si vous avez un environnement personnalisé que vous voulez traduire, CA Identity Manager fournit des outils de localisation que vous pouvez utiliser pour effectuer la traduction. Pour utiliser ces outils, vous devez installer ant 1.7 ou une version ultérieure, et Java JDK 1.5 ou une version ultérieure. Ces logiciels doivent être inclus dans la variable PATH. Vous pouvez les ajouter à l'aide des commandes suivantes :

Windows :

```
PATH %ANT_HOME%\bin;%PATH%
PATH %JAVA_HOME%\bin;%PATH%
```

UNIX :

```
PATH=%ANT_HOME%\bin:$PATH
export PATH
```

Utilisation des exemples d'environnements localisés

CA Identity Manager déploie les fichiers qui prennent en charge les exemples d'environnements localisés lors de l'installation.

Pour afficher des fenêtres et des tâches localisées dans la console d'utilisateur, procédez comme suit :

1. [Importez le fichier RoleDefinitions.xml](#) (page 167).
2. [Installez l'Aide en ligne.](#) (page 168)

Importation de l'exemple de fichier RoleDefinitions.xml

Le fichier RoleDefinitions.xml crée les tâches qui s'affichent initialement dans la console d'utilisateur.

Vous devez importer l'exemple de fichier RoleDefinitions.xml approprié à l'environnement CA Identity Manager requis.

Pour importer le fichier RoleDefinitions.xml :

1. Dans la console de gestion, cliquez sur CA Identity Manager environments (Environnements).
Une liste des environnements CA Identity Manager s'affiche.
2. Cliquez sur le nom d'un environnement CA Identity Manager.
La fenêtre de propriétés de cet environnement s'affiche.
3. Cliquez sur Role and Task Settings.
4. Cliquez sur Importer.

La console de gestion répertorie les fichiers RoleDefinition.xml qui peuvent être ajoutés à l'environnement.

5. Recherchez et sélectionnez le fichier RoleDefinitions.xml approprié pour la langue dont vous avez besoin.

Les fichiers RoleDefinitions.xml traduits se trouvent dans le dossier des outils d'administration :

outils_admin\samples\Localization\langue

outils_admin

Spécifie l'emplacement d'installation des outils d'administration de CA Identity Manager.

Les outils d'administration sont situés aux emplacements par défaut ci-après.

Windows : <chemin_d'installation>\tools

UNIX : <chemin_d'installation2>/tools

langue

Spécifie la langue que vous souhaitez utiliser.

Remarque : Pour obtenir une description du fichier RoleDefinitions.xml disponible, consultez le fichier readme.txt sous *outils_admin\samples\Localization*.

6. Cliquez sur Terminer.
Le statut est affiché dans la fenêtre Role Configuration Output (Résultat de la configuration de rôle).
7. Cliquez sur Continuer pour sortir.
8. Répétez les étapes 1 à 6 pour chaque fichier RoleDefinitions.xml pour chaque environnement.

Installation de l'Aide en ligne

CA Identity Manager inclut une Aide en ligne traduite pour chaque version traduite de la console d'utilisateur.

Procédez comme suit:

1. Téléchargez l'Aide en ligne traduite à partir du site de support de CA comme suit :
 - a. Accédez au [site du support de CA](#) dans une fenêtre de navigateur.
 - b. Cliquez sur Documentation.
 - c. Dans la section Find Other Product Documentation (Rechercher la documentation d'autres produits), entrez CA Identity Manager dans le champ Select a Product (Sélectionner un produit).
 - d. Sélectionnez la version et la langue appropriées, puis cliquez sur Go.

Le site de support affiche les documents traduits et l'Aide en ligne pour chaque Service Pack de la version sélectionnée.

- e. Cliquez sur le fichier ZIP de l'Aide en ligne pour le télécharger.

2. Copiez ce fichier comme suit :

```
copy nom_fichier.zip iam_im.ear\user_console.war\  
nom_fichier
```

Nom du fichier ZIP que vous avez téléchargé à l'étape 1.

```
iam_im.ear
```

Emplacement de déploiement de l'application CA Identity Manager sur le serveur d'applications.

Remarque : Créez une copie de sauvegarde de l'Aide en ligne par défaut avant de la remplacer par une version traduite. L'Aide en ligne par défaut est écrasée par la version traduite.

3. Décompressez le fichier im_help.zip dans le répertoire user_console.war.
La version traduite de l'Aide en ligne peut être utilisée.

Création de fichiers de localisation personnalisés

La localisation des groupes de ressources implique les opérations suivantes.

1. Exportez les rôles dans un fichier RoleDefinitions.xml et procédez comme suit :
 - Si vous localisez CA Identity Manager pour une langue unique, passez à l'étape suivante.
 - Si vous localisez CA Identity Manager pour plusieurs langues, marquez le fichier RoleDefinitions.xml.
Lorsque vous exécutez la commande pour créer un fichier RoleDefinitions.xml marqué, CA Identity Manager crée *RoleDefinitions_Tokenized.xml* et *RoleDefinitions_Tokenized.properties*.
2. Traduisez le fichier RoleDefinitions.xml.
3. Traduisez les groupes de ressources.
4. Installez les fichiers localisés.
5. Importez un fichier RoleDefinitions.xml marqué dans un nouvel environnement ou dans un environnement existant.

Remarque : Pour obtenir des instructions complètes, consultez le fichier Readme sous *outils_admin\samples\Localization*. Les outils d'administration sont situés aux emplacements par défaut ci-après.

- **Windows :** <chemin_d'installation>\tools
- **UNIX :** <chemin_d'installation2>/tools

Traduction des modèles de courriel

CA Identity Manager peut envoyer des notifications par courriel aux utilisateurs concernés lorsque certains événements se produisent, comme par exemple lorsqu'un administrateur approuve une demande ou lorsqu'une tâche se termine.

Vous créez et gérez les notifications par courriel à l'aide de stratégies de notification par courriel dans la console d'utilisateur.

Remarque : Si le courriel contient des caractères internationalisés, les utilisateurs doivent définir le codage de leur client de messagerie sur Unicode (UTF-8) pour afficher le message correctement. Pour plus d'informations sur la modification du codage des courriels, consultez la documentation incluse avec le client de messagerie.

Pour traduire des modèles de courriel :

1. Configurez la prise en charge des notifications par courriel, comme décrit dans le *Manuel d'administration*.
2. Effectuez les procédures permettant d'utiliser les notifications par courriel décrites dans le *Manuel d'administration*.

Lorsque vous personnalisez les notifications par courriel, traduisez le contenu dans la langue appropriée.

Localisation des apparences personnalisées

Les apparences personnalisées déterminent les graphiques, les couleurs et les polices d'un environnement CA Identity Manager. CA Identity Manager inclut une apparence par défaut et plusieurs exemples d'apparence que vous pouvez personnaliser pour une langue.

Modification de la tâche Modifier mon compte

Pour les environnements localisés, le processus de consultation par défaut comporte des noms de rôle en anglais dans la configuration qui entraîne l'échec de la tâche Modifier mon compte. Pour corriger cela, effectuez les tâches suivantes :

1. Dans la console d'utilisateur, modifiez la tâche Modifier mon compte.
2. Cliquez sur l'onglet Événements.
3. Dans la liste de rôles, sélectionnez les rôles User Manager (Gestionnaire d'utilisateurs) et User Approver (Approbateur d'utilisateur).
4. Enregistrez les modifications.

Localisation de code personnalisé

Lorsque vous créez un code personnalisé à l'aide des API CA Identity Manager, vous pouvez effectuer les tâches suivantes :

- Localisez les messages d'exception qui sont affichés dans les gestionnaires d'attributs logiques, dans les gestionnaires de tâches métier et dans les règles de validation.
- Localisez les noms d'affichage des attributs logiques.
- Spécifiez la langue utilisée pour toutes les communications entre CA Identity Manager et un client tiers lors de l'utilisation du service Web d'exécution des tâches.
- Utilisez la classe d'aide Localizer pour récupérer la version localisée d'une chaîne pour les paramètres régionaux. Par exemple, vous pouvez récupérer la version localisée d'une étiquette dans une fenêtre de tâche ou dans un nom de tâche.

Pour plus d'informations sur la localisation de code personnalisé, consultez les documents suivants :

- Les sections Localizer et IMSEException du chapitre Support Objects du manuel *Programming Guide for Java*.
- Les descriptions de classe des objets Localizer et IMSEException dans l'outil Javadoc.

Affichage de CA Identity Manager dans différentes langues

Lorsqu'un environnement prend en charge plusieurs langues, les utilisateurs peuvent sélectionner la langue qu'ils veulent afficher dans le champ Choisir la langue dans la fenêtre de connexion et dans la console d'utilisateur. Lorsqu'un utilisateur choisit une langue différente, CA Identity Manager affiche la fenêtre de connexion et les fenêtres de la console d'utilisateur dans la langue sélectionnée. L'utilisateur n'a pas besoin de se déconnecter de l'environnement pour que les changements s'appliquent.

La liste des langues du champ Choisir la langue dépend de la disponibilité des fichiers localisés pour l'environnement. La préférence de langue définie dans le navigateur de l'utilisateur détermine la langue par défaut.

Remarque : Pour afficher le champ Choisir la langue, effectuez les opérations de configuration suivantes dans CA Identity Manager :

- Configurez le champ Enable Language Switching (Activer le changement de langue) dans la console de gestion.
- Ajoutez la prise en charge de la langue dans l'environnement en important les fichiers RoleDefinitions traduits et en installant les fichiers d'Aide en ligne.

Remarque : Si vous créez des fichiers localisés personnalisés au lieu d'utiliser les exemples de fichier, des étapes de configuration supplémentaires sont requises.

Activation du changement de langue

Vous activez la prise en charge du changement des langues dans la fenêtre de connexion de CA Identity Manager et dans la console d'utilisateur de la console de gestion.

Pour activer le changement de langue :

1. Ouvrez la console de gestion à l'aide de l'URL suivante :

`http://nom_hôte:port/iam/immanage`

Remarque : Si vous utilisez un agent Web pour l'authentification avancée CA Identity Manager, tenez compte des points suivants :

- Vous ne devez pas spécifier le numéro de port.
 - Le champ Choisir la langue ne s'affichera pas dans la fenêtre de connexion.
2. Accédez à Environments (Environnements), *votre_environnement*, Advanced Settings (Paramètres avancés), User Console (Console d'utilisateur).
 3. Dans la section General Behavior (Comportement général), sélectionnez Enable Language Switching (Activer le changement de langue).
 4. Cliquez sur Enregistrer.
 5. Redémarrez l'environnement pour appliquer les modifications.

Définition de l'en-tête HTTP imlanguage dans une réponse CA SiteMinder

Lorsque CA Identity Manager est intégré à CA SiteMinder, vous pouvez définir la préférence des paramètres régionaux d'un utilisateur à l'aide d'un en-tête HTTP imlanguage. Dans CA SiteMinder, vous définissez cet en-tête dans une réponse CA SiteMinder et spécifiez un attribut d'utilisateur comme valeur de celui-ci. Cet en-tête imlanguage est défini comme la préférence de paramètres régionaux prioritaire pour un utilisateur.

Pour définir l'en-tête HTTP imlanguage dans une réponse CA SiteMinder :

1. Connectez-vous à l'une des interfaces suivantes en tant qu'administrateur avec des droits sur le domaine :
 - Pour CA SiteMinder Web Access Manager r12 ou version ultérieure, connectez-vous à l'interface d'administration.
 - Pour CA eTrust SiteMinder 6.0 SP5, connectez-vous à l'interface utilisateur du serveur de stratégies.

Remarque : Pour plus d'informations sur l'utilisation de ces interfaces, consultez la documentation de la version de CA SiteMinder que vous utilisez.

2. Recherchez la réponse CA SiteMinder pour l'environnement CA Identity Manager protégé :

*environnement_Identity_Manager*response_ims

3. Créez un éditeur d'attribut de réponse CA SiteMinder avec les valeurs suivantes :

- Attribut : WebAgent-HTTP-Header-Variable
Ajoute un nouvel en-tête HTTP à la réponse.
- Attribute Kind (Type d'attribut) : Attribut de l'utilisateur
- Nom de la variable : imlanguage
- Nom de l'attribut : entrez le nom de l'attribut physique à partir de l'annuaire d'utilisateurs qui contient les paramètres régionaux préférés, par exemple, employeetype.

Le contenu de l'attribut d'utilisateur dans l'annuaire d'utilisateurs doit contenir une préférence de langue consistant en un code de langue à deux lettres suivi par un code de pays à deux lettres facultatif, séparés par un trait d'union ou un trait de soulignement. Le paramètre de préférence de langue dans l'attribut d'utilisateur ne doit pas nécessairement respecter la casse, comme dans les exemples suivants :

- ja
- fr-FR
- en_uk

4. Enregistrez la réponse.

L'en-tête HTTP imlanguage est maintenant défini dans une réponse CA SiteMinder.

Chapitre 10: Règles de validation

Ce chapitre traite des sujets suivants :

[Introduction aux règles de validation](#) (page 175)

[A propos des règles de validation](#) (page 175)

[Utilisation de règles de validation par défaut](#) (page 179)

[Implémentation des règles de validation personnalisées](#) (page 182)

[Configuration des règles de validation](#) (page 190)

[Initialisation de la validation](#) (page 196)

[Exemples d'implémentation](#) (page 197)

Introduction aux règles de validation

Les valeurs des attributs du référentiel de données sont affectées via les champs de la fenêtre de tâche ou à l'aide d'un programme. Les règles de validation d'attribut permettent de vérifier que les valeurs saisies par les utilisateurs dans les champs de fenêtre de tâche ou fournies par un programme répondent à certaines conditions requises, comme dans les exemples suivants :

- Les conditions associées à l'annuaire d'utilisateurs, comme l'application d'un type de données ou la vérification du format approprié d'une entrée, telle qu'une date.
- L'intégrité des données : une entrée est-elle appropriée dans le contexte d'autres informations de la fenêtre de tâche ou selon les règles métier spécifiques du site ?

Vous pouvez associer directement une règle de validation à un champ de fenêtre de tâche ou indirectement au champ associé à un attribut d'objet géré qui est configuré pour le champ.

Toutes les règles de validation directement ou indirectement associées aux champs d'une fenêtre de tâche doivent être respectées pour que le traitement de la tâche puisse débuter. Lorsqu'une valeur fournie n'est pas valide, un message associé à la règle enfreinte est affiché. L'utilisateur peut alors la corriger et resoumettre la tâche.

A propos des règles de validation

Les règles de validation permettent d'appliquer les conditions requises, comme dans les exemples suivants :

- Un champ Quantité doit contenir uniquement des caractères numériques.
- Un champ Numéro de téléphone doit être spécifié selon le format nnn-xxx-nnnn.
- Un champ ID d'employé ne doit contenir aucune valeur supérieure à 9999.

- La valeur saisie dans un champ Code postal doit correspondre aux valeurs saisies dans les champs Ville et Etat.
- La valeur saisie dans un champ Titre offre-t-elle le niveau d'habilitation à l'utilisateur correspondant à la valeur saisie dans le champ Niveau de sécurité ?

Outre la vérification des entrées d'utilisateur, une règle de validation permet de *modifier* une entrée afin de la rendre conforme aux conditions requises de la règle, sans requérir l'intervention de l'utilisateur, comme dans les exemples suivants :

- Une règle de validation pour un champ Numéro de téléphone indique que les numéros de téléphone doivent être au format nnn-xxx-nnnn. Si un utilisateur saisit la valeur 9785551234, la règle de validation permet de modifier automatiquement l'entrée et de la rendre conforme au format approprié, 978-555-1234.
- Une règle de validation pour un champ Numéro de département requiert l'ajout d'un préfixe de trois caractères au numéro, représentant le nom saisi dans le champ Région. Lorsque le préfixe est manquant ou incorrect, la règle de validation fournit le préfixe correct.

Le processus de modification d'une entrée à l'aide d'une règle de validation est nommé *transformation*.

Types de règles de validation

Les types de règles de validation sont les suivants :

- **Validation de niveau tâche** : permet de valider une valeur d'attribut par rapport à d'autres attributs dans la tâche. Par exemple, vous pouvez vérifier que l'indicatif régional d'un numéro de téléphone fourni par l'utilisateur est approprié à la ville et à la région de l'utilisateur.

Pendant la configuration de la fenêtre de tâche, les règles de validation de niveau tâche sont directement associées aux champs de la fenêtre de tâche.

Vous pouvez utiliser ce type de validation pour renforcer l'intégrité des données.

- **Validation de niveau annuaire** : permet de valider la valeur de l'attribut lui-même, sans devoir recourir au contexte fourni par d'autres attributs dans la tâche. Par exemple, vous pouvez vérifier qu'un numéro de téléphone fourni par l'utilisateur corresponde au format nnn-xxx-nnnn utilisé dans l'annuaire.

Dans `directory.xml`, les règles de validation de niveau annuaire sont mappées vers un attribut d'objet géré via un ensemble de règles. Les règles de cet ensemble sont appliquées à un champ de fenêtre de tâche configuré avec l'attribut.

Vous pouvez utiliser ce type de validation pour appliquer les conditions requises liées à l'annuaire d'utilisateurs.

CA Identity Manager exécute les règles de validation de niveau tâche avant celles de niveau annuaire.

Exemple de comparaison de validation de niveau annuaire et de validation de niveau tâche

Dans cet exemple, un attribut de téléphone est mappé dans `directory.xml` vers une règle de validation de niveau annuaire spécifiant que les numéros de téléphone doivent être au format `nnn-xxx-nnnn`. Tous les champs configurés avec l'attribut de téléphone sont validés par rapport au format `nnn-xxx-nnnn`, que le champ s'affiche dans une fenêtre de tâche Créer un utilisateur, une fenêtre de tâche Créer un fournisseur ou une autre fenêtre de tâche.

Si un champ Numéro de téléphone s'affiche dans une fenêtre de tâche Créer un client, comme des champs de numéro de téléphone dans d'autres fenêtres de tâche, ce champ est configuré avec l'attribut de téléphone qui requiert le format `nnn-xxx-nnnn`. Cependant, certains clients de la société se trouvant dans d'autres états, le champ Numéro de téléphone de la fenêtre de tâche Créer un client est également associé à la logique de validation de niveau tâche suivante :

- Vérification de la valeur du champ Etat.
- Lorsque le client se trouve dans un autre état, vérifiez que l'indicatif régional du numéro de téléphone du client est approprié à cet état.

Ensembles de règles de validation

Avec la validation de niveau annuaire, une ou plusieurs règles de validation sont affectées à un ensemble de règles, et cet ensemble est associé à un attribut d'objet géré.

Les ensembles de règles vous permettent de définir et d'appliquer des règles d'une façon détaillée, comme dans les exemples suivants :

- Une règle peut être utilisée dans des ensembles de règles différents.
- Les règles peuvent être utilisées selon différentes combinaisons.

Lorsqu'un échec se produit pour une règle dans un ensemble de règles (par exemple, une règle Java ou JavaScript renvoie la valeur `False`), tous les messages d'exception associés à la règle sont affichés. Toutes les règles de validation associées à l'attribut doivent être respectées pour que celui-ci soit validé.

Ordre d'exécution

Les règles sont exécutées selon l'ordre dans lequel elles sont répertoriées dans l'ensemble de règles. CA Identity Manager exécute chaque règle d'un ensemble séparément et poursuit l'exécution des règles suivantes de façon transparente, sauf si un échec d'une règle se produit.

L'exécution des règles de validation selon un ordre préétabli vous permet d'implémenter des règles dont les actions sont dépendantes du résultat des règles précédentes, comme dans les exemples suivants :

- Le résultat d'une règle peut servir d'entrée pour la règle suivante.
- Lorsqu'une valeur de champ est modifiée lors de la validation, vous pouvez évaluer la nouvelle valeur dans les règles ultérieures.

Notions de base de la définition de règle de validation

Effectuez les opérations de base suivantes lorsque vous définissez des règles de validation personnalisées :

- **Implémentez une règle de validation.** Implémentez une règle de validation de l'une des façons suivantes :
 - Expression régulière
 - JavaScript
 - Classe Java
- **Intégrez une règle de validation à CA Identity Manager à l'aide d'une fenêtre de tâche ou de l'annuaire `directory.xml`.** Effectuez cette opération de manière intégrée, directement dans la fenêtre de tâche ou dans le fichier `directory.xml`, ou par référence d'un fichier source JavaScript ou d'un fichier de classe Java compilé, comme dans le tableau suivant :

	Intégrée	Par référence
Expression régulière	directory.xml ou fenêtre de tâche	—
JavaScript	directory.xml ou fenêtre de tâche	Fichier source référencé dans directory.xml
Java	—	Fichier de classe référencé dans directory.xml ou dans la fenêtre de tâche

- **Associez une ou plusieurs règles à un champ de fenêtre de tâche**, de l'une des façons suivantes :
 - Avec la validation de niveau tâche, vous affectez une règle de validation directement à un champ d'une fenêtre de tâche.

La validation de niveau tâche a une portée limitée à la tâche, c'est-à-dire que vous pouvez l'utiliser uniquement dans le contexte de la fenêtre de tâche appropriée.
 - Avec la validation de niveau annuaire, vous mappez un ensemble de règles vers un attribut d'objet géré dans `directory.xml`. Un champ de fenêtre de tâche est configuré avec l'attribut est validé selon les règles de l'ensemble de règles.

La validation de niveau annuaire a une portée globale. Cela veut dire que vous pouvez utiliser la validation de niveau annuaire sur un champ configuré avec l'attribut d'objet géré, indépendamment de la fenêtre de tâche qui contient ce champ et de l'environnement CA Identity Manager qui inclut cette fenêtre.

Utilisation de règles de validation par défaut

Les types de règles de validation suivants sont fournis par défaut avec CA Identity Manager :

- Validation des données des champs de fenêtre de tâche
- Règles de validation prédéfinies dans le fichier `directory.xml`

Validations de données par défaut

Par défaut, CA Identity Manager vérifie certaines données lorsqu'un administrateur soumet une tâche pour traitement. Lorsque les données ne sont pas valides, CA Identity Manager arrête le traitement de la tâche et affiche un message d'erreur. Les validations de données que CA Identity Manager effectue sont basées sur le type de tâche, comme illustré dans le tableau suivant :

Tâches	Validation
Toutes les tâches	Les champs obligatoires doivent avoir une valeur.
Créer un utilisateur	<p>Un administrateur ne peut pas créer un objet portant le même nom qu'un objet existant du même type. Par exemple, un administrateur ne peut pas créer deux rôles d'administration portant le même nom.</p> <p>Remarque : Pour les utilisateurs et les groupes, CA Identity Manager vérifie uniquement l'organisation actuelle.</p>
Créer un groupe	
Créer une organisation	
Créer un rôle d'accès	
Créer une tâche d'accès	
Créer un rôle d'administration	
Créer une tâche d'administration	

Tâches	Validation
Créer un utilisateur Créer un groupe Créer une organisation	<p>Un administrateur ne peut pas créer un utilisateur, un groupe ou une organisation avec un nom qui contient l'un des caractères suivants :</p> <ul style="list-style-type: none"> ■ Virgule (,) ■ Apostrophe simple (') ■ Guillemets (") ■ Astérisque (*) ■ Esperluette (&) ■ Barre oblique (/) ■ Barre oblique inversée (\) ■ Inférieur à (<) ■ Supérieur à (>) ■ Egal à (=) ■ Signe plus (+) ■ Point-virgule (;) ■ Dièse (#) ■ Espaces de début ou de fin <p>Remarque : Les noms d'organisation peuvent contenir une virgule (,) ou une esperluette (&).</p>
Toutes les tâches Créer et Modifier	<p>Les attributs avec des droits en lecture et en écriture (sauf les mots de passe) ne peuvent pas contenir les caractères suivants :</p> <ul style="list-style-type: none"> ■ Virgule (,) ■ Pourcentage (%) ■ Inférieur à (<) ■ Supérieur à (>) ■ Point-virgule (;) <p>Ces caractères sont vulnérables aux attaques par scripts de site à site.</p>
Créer un utilisateur Self-register (Auto-enregistrement) Modifier mon mot de passe Réinitialisation du mot de passe de l'utilisateur Toutes les tâches personnalisées qui collectent et stockent les mots de passe d'utilisateur.	<p>Si vous utilisez la fonctionnalité de services de mot de passe de CA SiteMinder pour appliquer des règles de mot de passe, comme la longueur minimum, les mots de passe d'utilisateur sont validés en fonction de ces règles.</p> <p>Si le mot de passe n'est pas conforme à la stratégie de mot de passe, il n'est pas accepté.</p> <p>Remarque : Pour plus d'informations, consultez le manuel <i>CA SiteMinder Web Access Manager Policy Server Configuration Guide</i>.</p>

Tâches	Validation
Modification d'un utilisateur	Les administrateurs ne peuvent pas s'attribuer un rôle ou la capacité d'affecter un rôle.
Mot de passe oublié	Si un profil d'utilisateur ne comporte aucun indice de mot de passe, ni la réponse correspondante, l'utilisateur ne peut pas utiliser la fonctionnalité de mot de passe oublié.
Supprimer un utilisateur Activer un utilisateur/Désactiver un utilisateur	Les administrateurs ne peuvent pas supprimer leur propre profil ou modifier le statut de leur compte.
Supprimer une organisation	Les administrateurs ne peuvent pas supprimer l'organisation à laquelle appartient le rôle qui leur est affecté et qui contient la tâche Supprimer une organisation. Considérez un administrateur auquel est affecté le rôle Organization Manager (Gestionnaire d'organisations) dans l'organisation Dealers (Grossistes). Le rôle Organization Manager lui permet de supprimer des organisations. Cet administrateur peut supprimer des sous-organisations de l'organisation Dealers, mais ne peut pas supprimer cette dernière.
Modifier une organisation	Les administrateurs ne peuvent pas modifier l'organisation à laquelle appartient le rôle qui leur est affecté et qui contient la tâche Modifier une organisation.

Règles de validation prédéfinies

CA Identity Manager inclut les règles de validation prédéfinies suivantes dans le fichier directory.xml. Les règles de validation prédéfinies sont utilisées pour la validation de niveau annuaire uniquement, comme illustré dans le tableau suivant :

Nom de règle prédéfinie	Description
Phone pattern	Applique le format suivant aux numéros de téléphone : +nn nnn-xxx-xxxx.
Set international	Ajoute le préfixe +1 à un numéro de téléphone international.
Valid User	Vérifie que l'objet d'utilisateur spécifié existe dans l'annuaire.
Valid Group	Vérifie que l'objet de groupe spécifié existe dans l'annuaire.
Valid Organization	Vérifie que l'objet d'organisation spécifié existe dans l'annuaire.

Les règles de validation prédéfinies et les règles de validation personnalisées peuvent s'afficher dans un même ensemble de règles.

Implémentation des règles de validation personnalisées

Vous pouvez implémenter une règle de validation selon les modalités suivantes :

- Expression régulière
- JavaScript
- Classe Java

Implémentation à l'aide d'une expression régulière

Une règle de validation peut être basée sur le modèle d'expression régulière correspondant. Vous pouvez, par exemple :

- Spécifier une liste de caractères ou de valeurs non valides pour un attribut
- Limiter les entrées de l'utilisateur à des constructions valides uniquement pour, par exemple, éviter un nom unique ou un numéro de téléphone au format incorrect.

L'exemple JavaScript suivant applique le format numérique de téléphone +nn nnn-
nnn-
nnnn :

```
phone=/\+\d{1,3} \d{3}-\d{3}-\d{4}/;
```

Encapsuler les expressions régulières définies en XML dans CDATA, comme dans l'exemple suivant :

```
<ValidationRule name="Phone pattern" description="+nn nnn-  
nnn-  
nnnn"  
messageid="4001">  
  <RegularExpression>  
    <![CDATA[ ((\+|\d)*+(\s*|\x2D))?\d\d\d-\d\d\d-\d\d\d\d]]>  
  </RegularExpression>  
</ValidationRule>
```

Les règles de validation basées sur des expressions régulières doivent respecter les conditions requises définies dans le package java.util.regex.

Implémentation à l'aide de JavaScript

Une règle de validation JavaScript doit implémenter l'interface pertinente, selon si la règle est utilisée pour la validation de niveau tâche ou de niveau annuaire.

Lors de la validation, CA Identity Manager appelle la fonction validate() et transfère la valeur à valider.

Interface JavaScript pour la validation de niveau tâche

La définition de l'interface JavaScript pour la validation de niveau tâche est la suivante :

Syntaxe

```
public boolean validate(  
    BLTHContext context,  
    String attributeValue,  
    StringRef changedValue,  
    StringRef errorMessage  
);
```

Paramètres

context

Paramètre d'entrée

Spécifie un objet qui contient des méthodes pour récupérer des informations dans la session de tâche actuelle.

attributeValue

Paramètre d'entrée

Spécifie la valeur de l'attribut en cours de validation.

changedValue

Paramètre de sortie

Fournit une valeur de transformation facultative qui remplace la valeur fournie par l'utilisateur en cours de validation. Si aucune transformation n'est nécessaire, la valeur renvoyée est nulle.

errorMessage

Paramètre de sortie

Si un échec de la validation se produit, un message s'affiche.

Le message est affiché via `AttributeValidationException`. Si la méthode renvoie la valeur `False`, CA Identity Manager génère une exception.

Commentaires

Les paramètres de sortie *changedValue* et *errorMessage* sont du type de données `StringRef`. `StringRef` est un type de données prédéfini qui contient la *référence* de champ à laquelle vous affectez une valeur, comme dans les exemples suivants :

- Ajout du préfixe 1 au numéro de téléphone correctement formaté :
`changedValue.reference="+1 " + phoneNumber;`
- Définition d'un message d'erreur pour un numéro formaté de façon incorrecte :
`errorMessage.reference="Phone number " + phoneNumber +
" Ne correspond pas au format nnn-xxx-nxxx.";`

Retour :

- True L'implémentation considère la valeur d'*attributeValue* valide ou renvoie une valeur transformée dans *changedValue*.
- False L'implémentation considère *attributeValue* comme non valide. CA Identity Manager génère une exception *AttributeValidationException* qui inclut *errorMessage*.

Interface JavaScript pour la validation de niveau annuaire

La définition de l'interface JavaScript pour la validation de niveau annuaire est la suivante :

Syntaxe

```
public boolean validate(  
    String attributeValue,  
    StringRef changedValue,  
    StringRef errorMessage  
);
```

Paramètres

attributeValue

Paramètre d'entrée

Spécifie la valeur de l'attribut en cours de validation.

changedValue

Paramètre de sortie

Fournit une valeur de transformation facultative qui remplace la valeur fournie par l'utilisateur en cours de validation. Si aucune transformation n'est nécessaire, la valeur renvoyée est nulle.

errorMessage

Paramètre de sortie

Si un échec de la validation se produit, un message s'affiche.

Le message est affiché via *AttributeValidationException*. Si la méthode renvoie la valeur False, CA Identity Manager génère une exception.

Commentaires

Les paramètres de sortie *changedValue* et *errorMessage* sont du type de données `StringRef`. `StringRef` est un type de données prédéfini qui contient la *référence* de champ à laquelle vous affectez une valeur, comme dans les exemples suivants :

- Ajout du préfixe 1 au numéro de téléphone correctement formaté :
`changedValue.reference="+1 " + phoneNumber;`
- Définition d'un message d'erreur pour un numéro formaté de façon incorrecte :
`errorMessage.reference="Phone number " + phoneNumber +
" Ne correspond pas au format nnn-xxx-xxxx.";`

Renvoi :

- `True` : l'implémentation considère la valeur d'*attributeValue* valide ou renvoie une valeur transformée dans *changedValue*.
- `False` : l'implémentation considère *attributeValue* comme non valide. CA Identity Manager génère une exception `AttributeValidationException` qui inclut *errorMessage*.

Implémentation à l'aide de Java

Une règle de validation Java doit implémenter l'interface pertinente, selon si la règle est utilisée pour la validation de niveau tâche ou de niveau annuel.

Lors de la validation, CA Identity Manager appelle la fonction `validate()` et transfère la valeur à valider.

Interface Java pour la validation de niveau tâche

La définition de l'interface Java pour la validation de niveau tâche est la suivante :

Syntaxe

```
public interface TaskValidator {
public class StringRef {
    public String reference = new String();
    public String toString(){return reference;}
public boolean validate(
    BLTHContext ctx,
    String attrValue,
    StringRef updatedValue,
    StringRef errorMessage
    ) throws AttributeValidationException;
}
```

Paramètres

ctx

Paramètre d'entrée

Spécifie un objet qui contient des méthodes pour récupérer des informations dans la session de tâche actuelle.

attrValue

Paramètre d'entrée

Spécifie la valeur de l'attribut en cours de validation.

updatedValue

Paramètre de sortie

Fournit une valeur de transformation facultative qui remplace la valeur fournie par l'utilisateur en cours de validation. Si aucune transformation n'est nécessaire, la valeur renvoyée est nulle.

errorMessage

Paramètre de sortie

Si un échec de la validation se produit, un message s'affiche.

Commentaires

Pour plus d'informations sur les règles de validation Java et sur les objets gérés, reportez-vous à l'outil Javadoc de CA Identity Manager.

Renvoi :

- True : l'implémentation considère la valeur d'*attributeValue* valide ou renvoie une valeur transformée dans *changedValue*.
- False : l'implémentation considère *attributeValue* comme non valide.

Renvoi :

AttributeValidationException

Interface Java pour la validation de niveau annuaire

La définition de l'interface Java pour la validation de niveau annuaire est la suivante :

Syntaxe

```
public interface IAttributeValidator {
    public class StringRef {
        public String reference = new String();
        public String toString(){return reference;}
    }
    public boolean validate(
        Object attributeValue,
        StringRef changedValue,
        StringRef errorMessage
    ) throws AttributeValidationException;
}
```

Paramètres

attributeValue

Paramètre d'entrée

Spécifie la valeur de l'attribut en cours de validation.

changedValue

Paramètre de sortie

Fournit une valeur de transformation facultative qui remplace la valeur fournie par l'utilisateur en cours de validation. Si aucune transformation n'est nécessaire, la valeur renvoyée est nulle.

errorMessage

Paramètre de sortie

Si un échec de la validation se produit, un message s'affiche.

Commentaires

Si l'opération de validation requiert des objets gérés de l'annuaire, utilisez AttributeValidator. Cette classe abstraite implémente l'interface IAttributeValidator et inclut une méthode pour récupérer les fournisseurs d'objet géré.

Retour :

- True : l'implémentation considère la valeur d'*attributeValue* valide ou renvoie une valeur transformée dans *changedValue*.
- False : l'implémentation considère *attributeValue* comme non valide.

Retour :

AttributeValidationException.

Exceptions

L'exception `AttributeValidationException` est renvoyée lorsqu'une règle de validation ne peut pas valider une valeur d'attribut fournie dans un champ de fenêtre de tâche ou à l'aide d'un programme. L'exception contient un ou plusieurs messages qui informent l'utilisateur et lui permettent de corriger l'entrée et de resoumettre la tâche.

Le renvoi de l'exception et l'affichage des messages d'erreur dépendent de si la règle est implémentée sous la forme d'un script JavaScript, d'une classe Java ou d'une expression régulière.

Exceptions lors de la validation de niveau tâche

Lorsque des erreurs de validation de niveau tâche se produisent, `AttributeValidationException` est renvoyé, comme illustré dans le tableau suivant :

Type de règle	Exception renvoyée	Source de message d'erreur
Expression régulière	Par CA Identity Manager si la validation d'expression régulière échoue.	CA Identity Manager utilise un message d'exception général.
JavaScript	Par CA Identity Manager si la méthode <code>validate()</code> renvoie <code>False</code> .	Le paramètre <code>errorMessage</code> de la méthode <code>validate()</code> .
Java	Par la règle de validation personnalisée ou par CA Identity Manager. CA Identity Manager renvoie l'exception lorsque la règle personnalisée n'est pas déclenchée et que la méthode <code>validate()</code> de la règle personnalisée renvoie <code>False</code> .	L'une des sources suivantes : <ul style="list-style-type: none"> ■ Le constructeur de l'exception, si la règle de validation personnalisée renvoie une exception. Le constructeur vous permet de spécifier l'ID d'un message dans un groupe de ressources et le texte d'un message supplémentaire. ■ Le paramètre <code>errorMessage</code> de la méthode <code>validate()</code>, si CA Identity Manager renvoie l'exception.

Si l'implémentation de la règle de validation ne fournit aucun message d'erreur, CA Identity Manager utilise un message d'erreur général.

Exceptions lors de la validation de niveau annuaire

Les messages d'exception pour les erreurs de validation de niveau annuaire proviennent de deux sources :

- Un groupe de ressources. Dans `directory.xml`, les définitions de tous les types de règles de validation (Java, JavaScript et expression régulière) incluent l'attribut `messageid`. Cet ID mappe vers un message d'exception personnalisé dans le groupe de ressources `IMSEExceptions.properties`. Lorsque l'exception `AttributeValidationException` est renvoyée, CA Identity Manager inclut le message mappé avec d'autres informations d'erreur qui peuvent être définies pour la règle de validation.
- Un code de règle de validation personnalisé. Les implémentations Java et JavaScript peuvent définir des messages d'exception supplémentaires pour la règle. Si une erreur de validation se produit dans la règle Java ou JavaScript, le message est affiché avec le message mappé vers la règle dans le groupe de ressources.

Les sources de ces messages d'exception Java et JavaScript sont définies dans le tableau précédent.

Cette fonctionnalité ne s'applique pas aux règles de validation de niveau annuaire implémentées à l'aide d'expressions régulières.

Remarque : Pour plus d'informations sur les messages d'exception dans les groupes de ressources, consultez la rubrique traitant de l'objet `AttributeValidationException` dans l'outil Javadoc de CA Identity Manager.

Construction de l'objet `AttributeValidationException`

Lorsque vous créez un objet `AttributeValidationException` pour une méthode `validate()` Java, utilisez la construction suivante :

Syntaxe

```
public AttributeValidationException(String attrName,  
    String attrValue,  
    String messageid,  
    String message);
```

Paramètres

attrName

Spécifie le nom de l'attribut d'objet géré en cours de validation.

attrValue

Spécifie la valeur à valider.

messageid

Si la valeur ne peut pas être validée, ce paramètre fournit l'ID associé au message à afficher. L'ID correspond à un message dans le groupe de ressources `IMSEExceptions.properties`.

message

Fournit un message supplémentaire qui peut être affiché. Ce paramètre vous permet d'afficher un message plus spécifique que celui du groupe de ressources ou qu'un message provenant d'un groupe de ressources personnalisé.

Remarque : Pour plus d'informations sur l'objet `AttributeValidationException`, consultez l'outil Javadoc de CA Identity Manager.

Configuration des règles de validation

Configurez une règle de validation en l'intégrant à CA Identity Manager et en l'associant directement ou indirectement à un champ de fenêtre de tâche.

La modalité de configuration d'une règle de validation détermine si la règle est appliquée à un champ dans une fenêtre de tâche (validation de niveau tâche) ou à un champ des fenêtres de tâche (validation de niveau annuaire), comme suit :

- La validation de niveau tâche vous permet d'associer directement la règle et un champ dans une fenêtre de tâche. La validation est effectuée dans le champ selon le contexte de la fenêtre de tâche uniquement.
- La validation de niveau annuaire vous permet d'associer la règle et le champ de fenêtre de tâche indirectement, comme suit :
 - Dans `directory.xml`, vous spécifiez la règle de validation, ajoutez la règle à un ensemble de règles et associez l'ensemble de règles à un attribut d'objet géré.
 - Dans la console d'utilisateur, un champ configuré avec l'attribut d'objet géré est validé selon l'ensemble de règles mappé vers l'attribut.

La validation est effectuée sur un champ configuré avec l'attribut, indépendamment de la fenêtre de tâche qui contient ce champ et de l'environnement CA Identity Manager qui contient cette fenêtre.

Configuration d'une validation de niveau tâche

Configurez la validation de niveau tâche dans la console d'utilisateur lorsque vous définissez des propriétés de champs dans une fenêtre de tâche de profil. La procédure standard est la suivante :

1. Accédez à la section de propriétés Champ de la fenêtre de configuration de profil contenant le champ à valider.

Remarque : Pour plus d'informations sur les propriétés de champ, consultez le *Manuel d'administration* et l'Aide en ligne de la console d'utilisateur.

2. Spécifiez une valeur dans l'un des champs suivants, selon la manière dont la règle de validation doit être implémentée :
 - Expression de validation : contient une expression régulière qui effectue la validation.
 - Classe Java de validation : contient le nom complet d'une classe Java qui effectue la validation. Par exemple :

```
com.mycompany.MyJavaValidator
```

CA Identity Manager recherchera le fichier de classe dans le répertoire racine spécifié pour les fichiers de classe Java personnalisés.
 - Script Java de validation : contient le code JavaScript complet qui effectue la validation.
Vous devez spécifier le code JavaScript dans ce champ. Avec la validation de niveau tâche, vous ne pouvez pas référencer un fichier contenant du code JavaScript.

Remarque : Pour plus d'informations sur la définition d'autres propriétés de champ dans une fenêtre de configuration de profil, cliquez sur Aide dans la fenêtre.

Configuration d'une validation de niveau annuaire

Vous configurez la validation de niveau annuaire dans le fichier `directory.xml` et dans une fenêtre de tâche. La procédure standard est la suivante :

- Dans le fichier `directory.xml`, procédez comme suit :
 - Spécifiez une règle de validation dans l'élément `ValidationRule`.
 - Spécifiez un ensemble de règles dans l'élément `ValidationRuleSet`. Un ensemble de règles contient une ou plusieurs règles prédéfinies, une ou plusieurs règles de validation personnalisées ou les deux.
 - Associez un ensemble de règles à un attribut d'objet géré dans l'élément `ImsManagedObjectAttr`.
- Dans une fenêtre de tâche, le champ à valider doit être configuré avec l'attribut mappé vers l'ensemble de règles.

Intégration de la validation de niveau annuaire avec CA Identity Manager

Définissez des règles de validation et des ensembles de règles dans CA Identity Manager à l'aide de l'élément `ImsManagedObjectAttrValidation` du fichier `directory.xml`.

Le schéma de l'élément `ImsManagedObjectAttrValidation` est le suivant :

```
<xs:element name="ImsManagedObjectAttrValidation" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="ValidationRule" minOccurs="0"
                  maxOccurs="unbounded">
        <xs:complexType>
          <xs:choice>
            <xs:element name="Java">
              <xs:complexType>
                <xs:attribute name="class" type="xs:string"
                              use="required"/>
              </xs:complexType>
            </xs:element>
            <xs:element name="JavaScript">
              <xs:complexType>
                <xs:simpleContent>
                  <xs:extension base="xs:string"/>
                </xs:simpleContent>
              </xs:complexType>
            </xs:element>
            <xs:element name="JavaScriptFile">
              <xs:complexType>
                <xs:attribute name="file" type="xs:string"
                              use="required"/>
              </xs:complexType>
            </xs:element>
            <xs:element name="RegularExpression">
              <xs:complexType>
                <xs:simpleContent>
                  <xs:extension base="xs:string"/>
                </xs:simpleContent>
              </xs:complexType>
            </xs:element>
          </xs:choice>
          <xs:attribute name="name" type="xs:string"
                        use="required"/>
          <xs:attribute name="description" type="xs:string"
                        use="optional"/>
          <xs:attribute name="messageid" type="xs:string"
                        use="required"/>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

```

<xs:element name="ValidationRuleSet" minOccurs="0"
              maxOccurs="unbounded">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="ValidationRule"
                  maxOccurs="unbounded">
        <xs:complexType>
          <xs:attribute name="name" type="xs:string"
                        use="required"/>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
    <xs:attribute name="name" type="xs:string"
                  use="required"/>
    <xs:attribute name="description" type="xs:string"
                  use="optional"/>
  </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>

```

Les éléments suivants sont définis :

ValidationRuleSet

Consiste en une ou plusieurs règles de validation personnalisées ou prédéfinies. Une règle de validation est spécifiée dans l'élément ValidationRule.

Les règles de validation prédéfinies et les règles de validation personnalisées peuvent s'afficher dans un même ensemble de règles. Un ensemble de règles peut également contenir une combinaison d'implémentations Java, JavaScript et d'expression régulière.

Les règles de validation sont exécutées dans l'ordre dans lequel elles s'affichent dans l'élément ValidationRuleSet. Cela permet d'effectuer une validation en cascade, c'est-à-dire d'utiliser le résultat d'une règle comme entrée pour la suivante.

ValidationRuleSet est associé à un attribut d'objet géré dans l'élément ImsManagedObjectAttr du fichier directory.xml.

ValidationRule

Spécifie une règle de validation à utiliser dans un ensemble ValidationRuleSet.

ValidationRule doit contenir uniquement l'un des sous-éléments suivants :

- Java : référence le fichier de classe Java qui implémente la règle.
- JavaScript : contient le code JavaScript intégré qui implémente la règle.
- JavaScriptFile : référence le fichier source JavaScript qui implémente la règle.
- RegularExpression : contient l'expression régulière intégrée qui implémente la règle. L'expression régulière doit être encapsulée dans CDATA.

Attributs clés

La plupart des attributs des éléments décrits au préalable sont explicites. Toutefois, les attributs suivants requièrent une explication :

- Classe d'attribut de l'élément <Java>
L'utilisation de règles de validation Java requiert le déploiement de la classe Java dans l'emplacement racine suivant sur le serveur d'applications :
`iam_im.ear\custom`
Les fichiers de classe à cet emplacement racine doivent être complets, sans avoir besoin d'autres informations de chemin d'accès. Par exemple :
`com.mycompany.MyJavaImpl.`
- Fichier d'attribut de l'élément <JavaScriptFile>
L'implémentation d'une règle de validation dans un fichier source JavaScript requiert le déploiement du fichier à l'emplacement racine suivant sur le serveur d'applications :
`iam_im.ear\custom\validationscripts`
Les fichiers sources JavaScript à cet emplacement racine sont référencés par leur nom uniquement. Par exemple : `MyJavaScriptImpl.js`.
- Attribut messageid de l'élément <ValidationRule>
L'ID de message spécifié dans cet attribut mappe vers un message d'erreur dans le groupe de ressources `IMSEExceptions.properties`.
Tous les types de règles de validation (JavaScriptFile, JavaScript, Java, et RegularExpression) contiennent un attribut messageid.

Exemple d'expression régulière intégrée

Les exemples suivants contiennent la règle de validation prédéfinie Phone pattern, incluse dans l'ensemble de règles Phone format. La règle est implémentée de manière intégrée sous la forme d'une expression régulière :

```
<ValidationRule name="Phone pattern" description="+nn nnn-xxx-xxxx"
                                     messageid="4001">
  <RegularExpression>
    <![CDATA[ ((\+|\d)*+(\s*|\x2D))?\d\d\d-\d\d\d-\d\d\d\d]]>
  </RegularExpression>
</ValidationRule>
<ValidationRuleSet name="Phone format" description=
  "Verify format +nn nnn-xxx-xxxx">
  <ValidationRule name="Phone pattern" />
</ValidationRuleSet>
```

Dans l'exemple précédent, messageid="4001" mappe vers la ligne suivante dans IMSExceptions.properties :

```
4001=Validation de l'attribut : la valeur {0} doit correspondre à une expression
régulière
                                     nnn-xxx-xxxx.
```

Exemple de référence au fichier JavaScript

L'exemple suivant spécifie la règle EndWithZ_js. Cette règle est implémentée en JavaScript et le script se trouve dans le fichier EndWithZ.js. L'ensemble de règles qui inclut la règle n'est pas affiché dans l'exemple :

```
<ValidationRule name="EndWithZ_js" messageid="custom-5001">
  <JavaScriptFile file="EndWithZ.js" />
</ValidationRule>
```

Dans cet exemple, le fichier JavaScript se trouve dans l'emplacement par défaut suivant :

```
iam_im.ear\custom\validationscripts
```

Association d'une définition de règle de validation avec un attribut d'objet géré

Associez un ensemble de règles à un attribut d'objet géré dans l'élément `ImsManagedObjectAttr` du fichier `directory.xml`.

Dans l'exemple suivant, l'ensemble de règles de validation `Phone format` est associé à l'attribut d'objet géré `telephonenumber` :

```
<ImsManagedObjectAttr physicalname="telephonenumber" displayname="Business Phone"
description="Business Phone" valuetype="String" required="false"
multivalued="false" maxlength="0" validationruleset="Phone format" />
```

Remarque : Lorsqu'un attribut d'objet géré est associé à une définition de règle de validation, le nom de l'ensemble de règles est affiché dans la fenêtre `Attribute Properties` (Propriétés d'attribut) de la console de gestion.

Association d'un ensemble de règles de validation avec un champ de fenêtre de tâche

La validation de niveau annuaire vous permet d'associer un ensemble de règles à un champ de fenêtre de tâche indirectement, comme suit :

1. Associez l'ensemble de règles à un attribut d'objet géré, comme décrit dans la section précédente.
2. Assurez-vous que le champ de fenêtre de tâche à valider est configuré avec l'attribut d'objet géré associé à l'ensemble de règles. Lors de l'exécution, une valeur de champ fournie par un utilisateur final est validée selon les règles de l'ensemble de règles.

En général, les champs de fenêtre de tâche sont déjà configurés avec des attributs. Toutefois, vous pouvez ajouter un champ à une fenêtre de tâche ou vous pouvez changer l'attribut affecté à un champ. Dans ce cas, si vous voulez que la valeur fournie dans le champ soit l'objet de la validation de niveau annuaire, configurez le champ avec un attribut mappé dans `directory.xml` vers l'ensemble de règles approprié.

Initialisation de la validation

Lors de l'exécution, la validation est initialisée de l'une des façons suivantes :

L'utilisateur soumet une tâche.

Permet de valider les champs de la fenêtre de tâche soumise qui sont associés à des règles de validation.

L'utilisateur accède à un onglet de fenêtre de tâche différent.

Permet de valider les champs de l'onglet libéré qui sont associés à des règles de validation.

L'utilisateur clique sur Valider dans un onglet.

Permet de valider les champs de l'onglet actuel qui sont associés à des règles de validation.

Le bouton Valider exécute également des gestionnaires d'attributs logiques incluant la méthode de validation.

L'utilisateur modifie une valeur dans un champ dont la propriété Valider lors de la modification est définie sur oui.

Permet de valider les champs de l'onglet actuel qui sont associés à des règles de validation.

Par exemple, si l'option Valider lors de la modification est activée pour un champ Type d'employé et que la valeur du champ Non-exempté est remplacée par Exempté, tous les champs de l'onglet qui sont associés à des règles de validation sont validés. Une règle peut requérir qu'un champ Salaire contienne une valeur et une autre règle peut automatiquement changer un champ Tarif horaire sur 0.

Le code personnalisé utilise une méthode setAttribute... dans l'élément AttributeCollection ou un gestionnaire d'onglets pour définir une valeur d'attribut d'objet géré.

Le champ est configuré avec l'attribut d'objet géré en cours de définition.

Exemples d'implémentation

Les exemples d'implémentation de règles de validation en JavaScript se trouvent dans le répertoire d'exemples suivant de CA Identity Manager :

Identity Manager\samples\validationscripts

Annexe A: Liste des onglets par défaut

Pour les tâches d'administration, CA Identity Manager inclut les onglets par défaut suivants.

Administrateurs du rôle d'accès

Permet d'ajouter, d'afficher ou de supprimer des administrateurs du rôle d'accès actuel.

Appartenance à un rôle d'accès

Permet d'ajouter, d'afficher ou de supprimer des membres du rôle d'accès actuel.

Profil du rôle d'accès

Définit le profil des rôles d'accès.

Tâches du rôle d'accès

Permet d'afficher les tâches d'accès d'un rôle ou d'ajouter ou de supprimer des tâches d'accès. Vous pouvez sélectionner les tâches d'accès de différentes applications.

Rôles d'accès

Permet d'ajouter, d'afficher ou de supprimer des rôles pour l'utilisateur sélectionné et de consulter ses droits.

Profil de tâche d'accès

Définit le profil des tâches d'accès.

Comptes

Répertorie les comptes dans les terminaux gérés pour les utilisateurs disposant de rôles de provisionnement. En général, cet onglet est ajouté à des tâches permettant d'afficher ou de modifier un utilisateur.

Modèles de compte

Permet d'ajouter, de supprimer ou d'afficher des modèles de compte associés à un rôle de provisionnement.

Administrateurs du rôle d'administration

Permet d'ajouter, d'afficher ou de supprimer des administrateurs du rôle d'administration actuel.

Appartenance à un rôle d'administration

Permet d'ajouter, d'afficher ou de supprimer des membres du rôle d'administration actuel.

Profil du rôle d'administration

Définit le profil des tâches d'administration.

Tâches du rôle d'administration

Permet d'afficher les tâches d'administration d'un rôle, d'ajouter ou de supprimer des tâches de ce type et d'en sélectionner dans différentes catégories.

Rôles d'administration

Permet d'ajouter, d'afficher ou de supprimer des rôles d'administration pour un utilisateur sélectionné et de consulter ses droits de membre et d'administrateur.

Profil de tâche d'administration

Définit l'onglet Profil des tâches d'administration.

Administrateurs

Permet d'ajouter, de modifier ou de supprimer des stratégies d'administration.

Approbateurs

Répertorie tous les participants pouvant approuver ou rejeter la tâche. Il permet également la réaffectation de la tâche.

Tâche d'approbation

Affiche des informations sur des tâches d'approbation particulières dans une liste de travail.

Approuver un événement

Affiche des informations sur des tâches d'approbation particulières dans une liste de travail.

Certifier un utilisateur

Permet de certifier ou de retirer les rôles d'un utilisateur.

Stratégies correspondantes/Stratégies déjà appliquées

Affiche l'état de synchronisation des utilisateurs.

Evénements

Permet de sélectionner et de configurer un processus de flux de travaux pour chaque événement que la tâche déclenche.

Exécuter la corrélation et l'exploration

Permet de sélectionner une définition d'exploration et de corrélation à exécuter.

Exécuter le profil de corrélation et d'exploration

Affiche les conteneurs dans un terminal que vous pouvez explorer ou corrérer.

Onglet externe (ExternalTab)

Affiche le contenu d'une URL dans l'onglet d'une tâche.

Champs

Permet d'afficher les champs contenus dans la tâche. Les champs sont les attributs définis dans la fenêtre de profil associée.

Administrateurs du groupe

Ajoute ou supprime des administrateurs pour le groupe actuel.

Appartenance à un groupe

Ajoute ou supprime des utilisateurs en tant que membres du groupe ou des groupes imbriqués à ce groupe.

Profil du groupe

Permet de définir ou d'afficher le profil du groupe.

Groupes

Permet d'ajouter, d'afficher ou de supprimer des groupes pour l'utilisateur sélectionné et de consulter les droits de ce dernier.

Propriétaires de l'ensemble de stratégies d'identité

Permet d'ajouter des règles de propriété, à savoir des règles déterminant qui peut modifier l'ensemble de stratégies d'identité.

Profil d'ensemble de stratégies d'identité

Définit le profil de l'ensemble de stratégies d'identité.

JSP

Affiche des informations personnalisées. Pour plus d'informations, contactez votre administrateur système.

Gestion de comptes système ou orphelins

Affecte un utilisateur global à un compte système ou orphelin.

Membres

Permet d'ajouter, de modifier ou de supprimer des stratégies de membre.

Profil d'une organisation

Permet de créer, de modifier ou d'afficher le profil d'une organisation.

Propriétaires

Permet d'ajouter, de modifier ou de supprimer des stratégies de propriétaire.

Stratégies

Crée ou modifie une stratégie d'identité.

Profil (AdminTaskProfile)

Permet de définir le profil de la tâche d'administration.

Profil (générique) (ObjectProfile)

Permet de définir le profil d'un objet géré.

Administrateurs du rôle de provisionnement

Permet d'ajouter, d'afficher ou de supprimer des administrateurs du rôle de provisionnement actuel.

Appartenance à un rôle de provisionnement

Permet d'ajouter, d'afficher ou de supprimer des membres du rôle de provisionnement actuel.

Profil du rôle de provisionnement

Définit le profil du rôle de provisionnement.

Onglet Réurrence

Permet de contrôler la planification de l'exécution de l'action d'exploration et de corrélation.

Portée (TaskScope)

Permet de limiter la portée d'une tâche. Si la tâche n'a pas d'objet principal ou s'il s'agit d'une action d'automodification, d'auto-affichage ou d'approbation, l'onglet Rechercher ne s'affiche pas.

Planification

Permet d'automatiser l'exécution d'une tâche à une date ultérieure.

Résumé de la synchronisation

Affiche l'état de synchronisation des utilisateurs.

Onglets (TaskTab)

Permet de sélectionner un contrôleur d'onglets, qui détermine le mode d'affichage des onglets d'une tâche, et de consulter, d'ajouter ou de supprimer les onglets inclus dans la tâche.

Historique de l'utilisateur

Affiche un historique de toutes les tâches lancées, approuvées, exécutées sur et effectuées par un utilisateur.

Liste de travail

Affiche une liste de tâches (d'approbation ou autres) qui s'affichent dans la console d'utilisateur Identity Manager du participant autorisé à approuver la tâche.

Profil de l'utilisateur

Définit ou affiche le profil d'un utilisateur.

Cet onglet inclut des fonctionnalités supplémentaires (par exemple, la génération d'événements distincts pour les changements de mots de passe) spécifiques aux objets Utilisateur.

Annexe B: Compilation des fichiers JSP de CA Identity Manager

Après avoir apporté des modifications aux fichiers JSP utilisés par CA Identity Manager pour générer la console d'utilisateur et la console de gestion sur un serveur d'applications JBoss, recompilez-les pour appliquer vos modifications.

Les fichiers JSP doivent être compilés à l'aide du script `compile_jsp.bat` ou `.sh`.

Le script `compile_jsp` crée une copie de sauvegarde des JSP, puis les recompile. Les copies de sauvegarde se trouvent dans les répertoires suivants:

- Pour la console d'utilisateur, le script `compile_jsp` crée le répertoire `iam/im_jsp_backup` à l'emplacement suivant :
`iam_im.ear\user_console.war`
- Pour la console de gestion, le script `compile_jsp` crée le répertoire `iam/im_jsp_backup` à l'emplacement suivant :
`iam_im.ear\management_console.war`

Pour recompiler les JSP dans un environnement JBoss :

1. Arrêtez le serveur d'applications JBoss, s'il est en cours d'exécution.
2. A partir d'une invite de commande, accédez à `répertoire_installation_jboss\bin`, où `répertoire_installation_jboss` est l'emplacement d'installation du serveur d'applications JBoss.
3. Exécutez l'un des scripts suivants :
 - **Windows** : `compile_jsp.bat`
 - **UNIX** : `compile_jsp.sh`
4. Démarrez le serveur d'applications JBoss.