# HP Universal CMDB 9.10 Configuration Manager

pour le système d'exploitation Windows

# Manuel de déploiement

Date de publication du document : Novembre 2010
Date de publication du logiciel : Novembre 2010

# Mentions légales

## Garantie

Les seules garanties applicables aux produits et services HP sont celles figurant dans les déclarations de garantie expresse accompagnant les dits produits et services. Aucun terme de ce document ne peut être interprété comme constituant une garantie supplémentaire. HP ne peut en aucun cas être tenu pour responsable des erreurs ou omissions techniques ou rédactionnelles du présent document.

Les informations contenues dans le présent document sont susceptibles d'être modifiées sans préavis.

## Légende de restriction des droits

Logiciel confidentiel. Licence HP valide requise pour la détention, l'utilisation ou la copie. En accord avec les articles FAR 12.211 et 12.212, les logiciels informatiques, la documentation des logiciels et les informations techniques commerciales sont concédés au gouvernement américain sous licence commerciale standard du fournisseur.

## Mentions relatives aux droits de reproduction

## Mises à jour de la documentation

La page de titre de ce document contient les informations d'identification suivantes :

- La date de publication du document est actualisée à chaque modification.
- La date de la version correspond à la date de disponibilité de cette version du logiciel.

Pour rechercher des mises à jour ou vérifier que vous disposez de l'édition la plus récente d'un document, visitez le site :

**http://h20230.www2.hp.com/selfsolve/manuals**

Pour accéder à ce site, vous devrez disposer d'un identificateur HP Passport. Le cas échéant, accédez à la page suivante pour demander un identificateur HP Passport :

**http://h20229.www2.hp.com/passport-registration.html**

Vous pouvez également cliquer sur le lien **New users - please register** (Nouveaux utilisateurs - Inscrivez-vous) de la page de connexion à HP.

Vous pouvez recevoir des mises à jour ou de nouvelles éditions de ce document si vous vous abonnez au service d'assistance approprié. Pour plus de détails, contactez votre représentant commercial HP.

# Support technique

Visitez le site d'assistance technique de HP Software à l'adresse :

**http://www.hp.com/go/hpsoftwaresupport**

Ce site Web indique les coordonnées des services et contient des informations sur les produits, les services et le support technique proposés par HP Software.

L'assistance technique en ligne offre aux utilisateurs des fonctions interactives pour résoudre des problèmes. De manière efficace et rapide, il vous donne un accès direct aux outils de support technique nécessaires à la gestion de vos opérations. En tant que client du support technique, vous pouvez réaliser les opérations suivantes sur ce site Web :

- rechercher des documents de connaissances présentant un réel intérêt ;
- soumettre et suivre des demandes de support et des demandes d'améliorations ;
- télécharger des correctifs logiciels ;
- gérer des contrats d'assistance ;
- rechercher des contacts HP spécialisés dans l'assistance ;
- consulter les informations sur les services disponibles ;
- participer à des discussions avec d'autres clients qui utilisent les logiciels ;
- rechercher des cours de formation sur les logiciels et vous y inscrire.

Pour accéder à la plupart des offres de support, vous devez vous inscrire en tant qu'utilisateur disposant d'un compte HP Passport et vous identifier comme tel. De nombreuses offres nécessitent en outre un contrat d'assistance.  Le cas échéant, accédez à la page suivante pour demander un identificateur HP Passport :

**http://h20229.www2.hp.com/passport-registration.html**

Les informations relatives aux niveaux d'accès sont détaillées à l'adresse suivante :

**http://h20230.www2.hp.com/new_access_levels.jsp**

# Sommaire

# 1

# Installation et configuration

Contenu de ce chapitre :

# Configuration Manager - Présentation

HP Universal CMDB Configuration Manager (Configuration Manager) permet d'analyser et de contrôler les données dans votre CMS. Il fournit un environnement de contrôle de l'infrastructure CMS, qui comprend de nombreuses sources de données et prend en charge une variété de produits et d'applications.

Le déploiement de Configuration Manager dans un environnement de réseau d'entreprise est un processus qui requiert la planification des ressources et la conception d'une architecture système. Avant d'installer Configuration Manager, passez en revue les informations de cette section, notamment la configuration système requise.

# Configuration Manager - Configuration requise

## Configuration système requise pour le serveur

Le tableau suivant décrit la configuration système requise pour le serveur Configuration Manager :

| | |
|---|---|
| **Processeur** | Intel Pentium 4, 4 cœurs au minimum |
| **Mémoire (RAM)** | 4 Go au minimum |
| **Plateforme** | x64 |
| **Système d'exploitation** | Les systèmes d'exploitation Windows 64 bits suivants sont pris en charge :<br>➤ Windows 2003 Enterprise SP2 et R2 SP2<br>➤ Windows 2008 Enterprise SP2 et R2 |

| | |
|---|---|
| **Base de données** | ➤ Microsoft SQL Server 2005 SP2 ; 2005 Compatibility Mode 80 ; (Enterprise Editions)<br>➤ Oracle 11.1.x |
| **HP Universal CMDB** | ➤ HP Universal CMDB version 9.03 (Installation CMDB standard)<br>Pour obtenir la liste complète de la configuration système de cette version, voir la documentation de HP Universal CMDB. |

## Configuration système requise pour le client

Le tableau suivant décrit la configuration système requise du client pour afficher Configuration Manager :

| | |
|---|---|
| **Navigateur** | ➤ Microsoft Internet Explorer 7.0, 8.0.<br>➤ Mozilla Firefox 3.x |
| **Plugin de navigateur Flash Player** | Flash Player 9 ou ultérieure |
| **Résolution d'écran** | ➤ 1 024 x 768 minimum<br>➤ 1 280 x 1 024 recommandée |
| **Qualité couleur** | 16 bits minimum |

## Instructions d'installation recommandées

Les instructions relatives aux options de configuration de Configuration Manager sont répertoriées dans le tableau ci-dessous.

| | |
|---|---|
| **LDAP** | Les environnements LDAP suivants sont pris en charge :<br>➤ Active Directory<br>➤ SunONE 6.x |
| **Taille minimale de schéma de base de données recommandée** | 2 Go |

## Configuration Manager - Limites de capacités

Les limites de capacité de Configuration Manager sont répertoriées dans le tableau ci-dessous.

| | |
|---|---|
| **Nombre maximal de vues recommandé** | 100 |
| **Nombre maximal de politiques recommandé** | 300 |
| **Nombre maximal de CI composites par vue recommandé** | 5000 |
| **Nombre maximal d'utilisateurs concurrents recommandé** | 50 |

# Configurer la base de données ou le schéma d'utilisateur

Pour utiliser Configuration Manager, vous devez indiquer un schéma de base de données. Configuration Manager prend en charge Microsoft SQL Server et le serveur de base de données Oracle. Cette tâche décrit comment configurer les propriétés de connexion de la base de données ou du schéma d'utilisateur Configuration Manager à l'aide de l'assistant d'installation.

---

**Remarque :** Pour connaître la configuration système Microsoft SQL Server et Oracle Server requise, voir "Configuration système requise pour le serveur", page 8.

---

**Pour configurer votre base de données :**

**1** Allouez une base de données Microsoft SQL Server ou un schéma d'utilisateur Oracle Server.

- Pour **Microsoft SQL Server 2005** : Activez la fonctionnalité d'isolement de capture d'instantané.

  Exécutez la commande suivante une fois la base de données créée :

  ```
  alter database <nom_basededonnées_ccm> set read_committed_snapshot on
  ```

  Pour plus d'informations sur la fonctionnalité d'isolement de capture d'instantané SQL Server, visitez le site http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx.

- Pour **Oracle** : Attribuez à l'utilisateur Oracle uniquement les rôles **Connect** et **Resource**.
  (L'octroi du privilège **Select any table** provoque l'échec de la procédure de remplissage du schéma.)

**2** Vérifiez les informations suivantes, nécessaires lors de ce processus de configuration :

| ✔ | **Informations requises** |
|---|---|
| | Nom d'hôte et port de la base de données |
| | Nom d'utilisateur et mot de passe de la base de données |
| | **Pour MS SQL** : Nom de la base de données |
| | **Pour Oracle** : SID |

**3** Exécutez l'assistant d'installation Configuration Manager. Pour plus d'informations, voir "Installer Configuration Manager", page 12.

## Installer Configuration Manager

Cette tâche décrit l'installation de Configuration Manager sur votre serveur, et la configuration de la connexion à la base de données et l'intégration d'UCMDB. Vous pouvez cliquer sur **Aide** sur les pages de l'assistant pour obtenir des informations sur l'installation. Pour la description détaillée des pages de l'assistant, voir "Assistant de configuration post-installation Configuration Manager", page 23.

**Pour installer Configuration Manager :**

**1** Dans le répertoire racine du DVD Configuration Manager, localisez le fichier : **install.bat**.

**2** Double-cliquez sur le fichier pour exécuter l'assistant d'installation de Configuration Manager.

**3** Cliquez sur **Next** pour ouvrir la page Contrat de Licence Utilisateur Final.

**4** Acceptez les termes de la licence et cliquez sur **Next** pour ouvrir la page Installation du produit.

**5** Sélectionnez les produits à installer (UCMDB et Configuration Manager) et spécifiez l'emplacement d'installation. Si vous disposez d'une licence UCMDB personnalisée, cochez la case. Cliquez sur **Next** pour démarrer l'installation d'UCMDB. Pour plus d'informations sur l'installation d'UCMDB, voir le PDF *HP Universal CMDB Deployment Guide*.

6. Lorsque l'installation et la post-installation d'UCMDB sont terminées, l'assistant de configuration de post-installation de Configuration Manager démarre automatiquement.
7. Cliquez sur **Next** sur la page de bienvenue pour ouvrir la page Configuration de la connexion à la base de données.
8. Sélectionnez le type de base de données (Oracle ou Microsoft SQL Server) et entrez le nom d'utilisateur et le mot de passe. Il est recommandé de tester la connectivité en cliquant sur le bouton **Test**. Si le test aboutit, cliquez sur **Next** pour ouvrir la page Configuration du serveur d'application.

---

**Remarque :** Vous pouvez configurer d'autres options avancées de connexion à la base de données lorsque l'Assistant est terminé. Pour plus d'informations, voir "Configuration des options avancées de connexion à la base de données", page 15.

---

9. Entrez le nom de l'hôte et cliquez sur **Next** pour ouvrir la page Configuration du service Windows.
10. Si vous souhaitez installer Configuration Manager comme service Windows, cochez la case. Cliquez sur **Next** pour ouvrir la page Informations d'identification de l'utilisateur.
11. Entrez le nom d'utilisateur et le mot de passe de l'utilisateur administratif et de l'intégration. Cliquez sur **Next** pour ouvrir la page Configuration de la connexion HP UCMDB.
12. Si UCMDB est déjà installé sur cet ordinateur ou sur un autre ordinateur, assurez-vous que le serveur UCMDB fonctionne avant de continuer.

    Si vous installez UCMDB sur un autre ordinateur, vérifiez que la case est cochée et entrez les paramètres appropriés. Il est recommandé de tester la connectivité en cliquant sur le bouton **Test**. Si le test de la connexion aboutit, cliquez sur **Next** pour ouvrir la page Récapitulatif des actions de post-installation.

**13** Vérifiez les informations de la page Récapitulatif des actions de post-installation. Si elles sont correctes, cliquez sur **Next** pour passer à la post-installation.

**14** Cliquez sur **Finish** dans la page Terminer pour mettre fin à la post-installation.

**15** S'il ne s'agit pas du premier démarrage d'UCMDB, vous devez modifier la taille de colonne dans UCMDB comme suit :

**a** Allez dans **Administration** > **Gestionnaire de paramètres d'infrastructure**. Localisez le paramètre **Racine de l'objet** et remplacez-le par **data**. Déconnectez-vous d'UCMDB et reconnectez-vous pour que la modification soit prise en compte.

**b** Allez dans **Modélisation** > **Gestionnaire des types de CI**. Sélectionnez le type de CI **data** dans l'arborescence et cliquez sur l'onglet Attributs. Modifiez l'attribut **Étiquette d'utilisateur** en remplaçant **Taille de valeur** par 900.

**c** Revenez dans le **Gestionnaire de paramètres d'infrastructure** et remplacez le paramètre **Racine de l'objet** par sa valeur originale. Déconnectez-vous et reconnectez-vous pour que la modification soit prise en compte.

**16** Si Gestion des flux de données a été exécuté dans UCMDB, les données de l'historique peuvent être altérées. Pour corriger ce problème, procédez comme suit :

**a** Lancez un navigateur Web et entrez l'adresse suivante : http://<adresse du serveur UCMDB>.<nom_domaine>:8080/jmx-console.

Entrez les informations d'identification pour l'authentification de la console JMX, qui sont par défaut :

- Nom de connexion = **sysadmin**
- Mot de passe = **sysadmin**

**b** Sous **UCMDB**, sélectionnez **Services DB de l'historique**.

**c** Sélectionnez la méthode **Fix902EndTimeRecords**.

**d** Pour le client à l'état Réel, entrez **1** pour l'ID client et cliquez sur **Appeler**.

**e** Si l'opération a réussi, un message indique "BD de l'historique mise à jour avec succès".

**f** Pour le client à l'état Autorisé, entrez **100001** pour l'ID client et cliquez sur **Appeler**.

**g** Si l'opération a réussi, un message indique "BD de l'historique mise à jour avec succès".

## Configuration des options avancées de connexion à la base de données

Si vous souhaitez utiliser plus de propriétés avancées de connexion à la base de données pour prendre en charge le déploiement de votre base de données, vous pouvez le faire après l'exécution de l'assistant Post-installation. Configuration Manager prend en charge toutes les options de connexion à la base de données reconnues par le pilote JDBC du fournisseur. Elles peuvent être configurées à l'aide de l'URL de connexion à la base de données. Pour configurer d'autres connexions avancées, modifiez la propriété **jdbc.url** dans **<répertoire d'installation Configuration Manager >\conf\database.properties**.

Voici des exemples d'options avancées Microsoft SQL Server :

- **Authentification Windows (NTLM).** Pour appliquer une authentification Windows, ajoutez la propriété du domaine à l'URL de connexion de votre JTDS dans le fichier database.properties. Spécifiez le domaine Windows à authentifier.

  Par exemple :

  ```
  jdbc:jtds:sqlserver://myServer:1433/myDatabase;sendStringParametersAsUnicode=false;domain=myDomain
  ```

- **SSL.** Pour plus d'informations sur la sécurisation de la connexion MS SQL Server à l'aide de SSL, visitez le site http://jtds.sourceforge.net/faq.html.

Voici des exemples d'options avancées Oracle Database Server :

- **URL Oracle.** Spécifiez l'URL de connexion du pilote natif Oracle. Spécifiez un nom de serveur Oracle et un SID valides. Si vous utilisez **Oracle RAC**, vous pouvez également spécifier les détails de la configuration Oracle RAC.

  ---

  **Remarque :** Pour plus de détails sur la configuration du format de l'URL JDBC Oracle native, visitez le site http://www.orafaq.com/wiki/JDBC#Thin_driver. Pour plus de détails sur la définition de l'URL pour Oracle RAC, visitez le site http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm.

  ---

- **SSL.** Pour plus d'informations sur la sécurisation de la connexion Oracle à l'aide de SSL, visitez les sites suivants :
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6

# Configuration de la base de données - Prise en charge de MLU (Multi-Lingual Unit)

Cette section décrit les paramètres de base de données requis pour la localisation du support.

## Paramètres Oracle Server

Les paramètres Oracle Server sont répertoriés dans le tableau ci-dessous :

| Option | Pris en charge | Recommandé | Remarques |
|---|---|---|---|
| Jeu de caractères | WE8ISO8859P1; UTF8,AL32UTF8 | AL32UTF8 | |

## Paramètres Microsoft SQL Server

Les paramètres Microsoft SQL Server sont répertoriés dans le tableau ci-dessous :

| Option | Pris en charge | Recommandé | Remarques |
|---|---|---|---|
| Collation (Classement) | Non-respect de la casse. Ne prend pas en charge l'ordre de tri binaire ni le respect de la casse. Seul l'ordre de non-respect de la casse avec une combinaison d'accent, kana ou paramètres de largeur est pris en charge. | Utilisez a boîte de dialogue Collation Settings (Paramètres de classement) pour sélectionner le classement. Ne cochez pas la case Binary (Binaire). La sensibilité à l'accent, kana et largeur doit être sélectionnée en fonction des besoins de la langue des données appropriée. La langue sélectionnée doit être identique à celle des paramètres régionaux du système d'exploitation Windows. | Limité aux définitions de paramètres régionaux Collation et English par défaut |
| Collation Database Property (Propriété de la base de données de classement) | Valeur par défaut Server (Serveur) | | |

**Remarque :**

Pour toutes les langues : **<Langue>_CI_AS** est l'option minimum requise. Par exemple, en japonais, si vous souhaitez sélectionner la sensibilité Kana et les options de sensibilité à la largeur, l'option recommandée est la suivante : **Japanese_CI_AS_KS_WS** ou **Japanese_90_CI_AS_KS_WS**. Cette recommandation indique que les caractères japonais sont sensibles à l'accent, à Kana et à la largeur.

- **Sensibilité à l'accent (_AS).** Distinction entre les caractères accentués et non accentués. Par exemple, **a** est différent de **á**. Si cette option n'est pas sélectionnée, Microsoft SQL Server considère les versions des lettres accentuées et non accentuées comme identiques pour le tri.
- **Sensibilité Kana (_KS).** Distinction entre les deux types de caractères Kana japonais : Hiragana et Katakana. Si cette option n'est pas sélectionnée, Microsoft SQL Server considère les caractères Hiragana et Katakana comme identiques pour le tri.
- **Sensibilité à la largeur (_WS).** Distinction entre un caractère codé sur un octet et le même caractère représenté sous la forme d'un caractère codé sur deux octets. Si cette option n'est pas sélectionnée, Microsoft SQL Server considère les caractères codés sur un octet et sur deux octets comme identiques pour le tri.

# Activer l'authentification LW-SSO (Lightweight Single Sign-On)

Certains utilisateurs de Configuration Manager sont également autorisés à se connecter à UCMDB. Pour plus de facilité, Configuration Manager fournit un lien direct à l'interface utilisateur UCMDB (sélectionnez **Administration** > **Ouvrir UCMDB**). Pour utiliser la connexion unique (qui exclut le besoin de se connecter à UCMDB après la connexion à Configuration Manager), vous devez activer LW-SSO pour Configuration Manager et UCMDB et vérifier qu'ils utilisent la même initString. Cette tâche décrit comment activer LW-SSO dans Configuration Manager et UCMDB.

**Pour activer LW-SSO :**

1. Ouvrez le fichier suivant dans le répertoire d'installation Configuration Manager : **\servers\server-0\webapps\cnc\WEB-INF\classes\cnclwssofmconf.xml**.

   ---

   **Remarque :** Ce fichier n'existe pas avant le démarrage de Configuration Manager.

   ---

2. Localisez la section suivante :

   ```
   enableLWSSO enableLWSSOFramework="true"
   ```

   et vérifiez que la valeur est **true**.

3. Localisez la section suivante :

   ```
   lwssoValidation  id="ID000001">
   <domaine> </domain>
   ```

   et entrez le domaine du serveur Configuration Manager après <**domaine**>.

**4** Localisez la section suivante :

```
<initString="Cette chaîne doit être remplacée"></crypto>
```

et remplacez "Cette chaîne doit être remplacée" par une chaîne partagée utilisée par toutes les applications approuvées s'intégrant dans LW-SSO.

**5** Localisez la section suivante :

```
<!--multiDomain>
<trustedHosts>
<DNSDomain>Cette valeur doit être remplacée par votre domaine
d'application</DNSDomain>
<DNSDomain>Cette valeur doit être remplacée par un domaine d'une autre
application</DNSDomain>
</trustedHosts>
</multiDomain-->
```

Supprimez le caractère de commentaire situé au début et entrez les domaines de serveur Configuration Manager dans les éléments DNSDomain (à la place de Cette valeur doit être remplacée par votre domaine d'application. La liste doit contenir le domaine de serveur entré à l'étape 3 à la page 19.

**6** Enregistrez vos modifications et redémarrez le serveur.

**7** Lancez un navigateur Web et entrez l'adresse suivante : http://<adresse du serveur UCMDB>.<nom_domaine>:8080/jmx-console.

Entrez les informations d'identification pour l'authentification de la console JMX, qui sont par défaut :

- Nom de connexion = **sysadmin**
- Mot de passe = **sysadmin**

**8** Sous **UCMDB-UI**, sélectionnez **Configuration LW-SSO** pour ouvrir la page Vue JMX MBEAN.

**9** Sélectionnez la méthode **setEnabledForUI**, définissez la valeur sur **true** et cliquez sur **Appeler**.

**10** Sélectionnez la méthode **setDomain**. Entrez le nom de domaine du serveur UCMDB et cliquez sur **Appeler**.

**11** Sélectionnez la méthode **setInitString**. Entrez la même initString que vous avez entrée pour Configuration Manager à l'étape 4 à la page 20 et cliquez sur **Appeler**.

**12** Si Configuration Manager et UCMDB se trouvent dans des domaines distincts, sélectionnez la méthode **addTrustedDomains** et entrez les noms de domaine des serveurs UCMDB et Configuration Manager. Cliquez sur **Appeler**.

**13** Pour afficher la configuration LW-SSO telle qu'elle a été sauvegardée dans le mécanisme des paramètres, sélectionnez la méthode **retrieveConfigurationFromSettings** et cliquez sur **Appeler**.

**14** Pour afficher la configuration actuelle LW-SSO chargée, sélectionnez la méthode **retrieveConfiguration** et cliquez sur **Appeler**.

## Prise en charge IPv6

Configuration Manager prend en charge les URL IPv6 pour les URL client uniquement.

**Pour travailler avec Configuration Manager en utilisant une adresse IPv6 :**

**1** Assurez-vous que votre système d'exploitation prend en charge IPv6. Pour plus d'informations, consultez la documentation du système d'exploitation.

**2** Ouvrez le fichier **client-config.properties**, situé dans le répertoire **conf** du <**répertoire d'installation Configuration Manager**>. Remplacez la valeur du paramètre **bsf.server.url** par l'adresse IPv6 entre crochets. Par exemple :

```
bsf.server.url=http://[2620:0:a17:e008:d840:5b0f:2040:519c]:8080/bsf
```

# 2

# Assistant de configuration post-installation Configuration Manager

Contenu de ce chapitre :

# Assistant de configuration post-installation Configuration Manager - Présentation

Ce chapitre contient des descriptions détaillées des pages de l'Assistant Post-installation Configuration Manager et des tâches de configuration associées. Il s'agit du contenu qui s'affiche lorsque vous cliquez sur **Aide** dans les pages de l'Assistant.

# Page Connexion à la base de données

Cette section inclut les rubriques suivantes :



## Général

Une connexion à la base de données doit être configurée et associée à une connexion URL standard. Si plusieurs fonctions avancées sont requises, telles que Oracle Real Application Cluster, configurez une connexion standard et modifiez manuellement le fichier **database.properties** pour configurer ces fonctions.

Configuration Manager utilise des pilotes natifs pour Oracle et Microsoft SQL Server. Cela signifie qu'en général, toutes les fonctions natives des pilotes sont prises en charge, à condition qu'elles puissent être configurées à l'aide de l'URL de base de données. L'URL se trouve dans le fichier **database.properties**.

---

**Remarque :** La configuration de fonctions avancées doit être réalisée lorsque la procédure de post-installation est terminée et qu'une configuration de travail a été établie.

---

## Paramètres

Pour configurer la connexion à la base de données, définissez les paramètres suivants :

| Paramètre | Valeur recommandée | Description |
|---|---|---|
| **Fournisseur** | <définie par l'utilisateur> | Fournisseur de base de données<br>Valeurs possibles : **Oracle** ou **Microsoft**<br>HP Universal CMDB peut être installé à l'aide du même programme d'installation que Configuration Manager—ou séparément.<br>Si Configuration Manager et UCMDB sont installés sur le même ordinateur à l'aide du même programme d'installation, la valeur par défaut de ce paramètre est le fournisseur de base de données sélectionné dans l'Assistant Post-installation UCMDB.<br>Les valeurs par défaut sont définies uniquement lors de l'installation des deux applications à l'aide des mêmes programmes d'installation. Si vous installez à l'aide de packages d'installation différents, même si UCMDB est installé sur le même ordinateur que Configuration Manager, les valeurs par défaut N'apparaissent PAS dans cet Assistant Post-installation. |
| **Nom d'hôte** | <définie par l'utilisateur> | Nom d'hôte du serveur de base de données<br>Si Configuration Manager et UCMDB sont installés sur le même ordinateur, la valeur par défaut de ce paramètre est le serveur de base de données sélectionné dans l'Assistant Post-installation UCMDB.<br>**Cette valeur est obligatoire.** |

| Paramètre | Valeur recommandée | Description |
|---|---|---|
| **Port** | <définie par l'utilisateur> | Port du programme d'écoute de la base de données<br>Si Configuration Manager et UCMDB sont installés sur le même ordinateur, la valeur par défaut de ce paramètre est le port de base de données sélectionné dans l'Assistant Post-installation UCMDB.<br>Pour Oracle, la valeur par défaut est **1521**.<br>Pour Microsoft SQL Server, la valeur par défaut est **1433**.<br>**Cette valeur est obligatoire.** |
| **SID/DB** | <définie par l'utilisateur> | Nom du SID Oracle ou nom de la base de données Microsoft SQL Server<br>Si Configuration Manager et UCMDB sont installés sur le même ordinateur, la valeur par défaut de ce paramètre est le sid/db de base de données sélectionné dans l'Assistant Post-installation UCMDB.<br>**Cette valeur est obligatoire.** |
| **Nom d'utilisateur** | <définie par l'utilisateur> | Nom d'utilisateur utilisé pour la connexion à la base de données.<br>**Cette valeur est obligatoire.** |
| **Mot de passe** | <définie par l'utilisateur> | Mot de passe utilisé pour la connexion à la base de données. |

## Options

Les options suivantes sont disponibles :

| Paramètre | Valeur recommandée | Description |
|---|---|---|
| **Chiffrer le mot de passe** | <définie par l'utilisateur> | Si elle est sélectionnée, cette option chiffre le mot de passe dans le fichier **database.properties**. Pour des raisons de sécurité, il est recommandé de chiffrer les mots de passe enregistrés dans des fichiers texte. |
| **Créer des objets de schéma** | <définie par l'utilisateur> | Si elle est sélectionnée, cette option crée les objets de schéma requis pour l'exécution de Configuration Manager. Désélectionnez cette option lorsque l'installation utilise un schéma existant préalablement créé et complété d'objets Configuration Manager. |

## Test

---

**Remarque :** Il est vivement recommandé de tester les propriétés de connexion avant de poursuivre.

---

Pour cela, cliquez sur **Test**. L'Assistant tente d'accéder à la base de données et de vérifier la connexion. Les résultats du test s'affichent à droite du bouton **Test**.

La base de données génère différents messages d'erreur. Pas besoin d'explications—concernent généralement l'entrée d'un nom d'utilisateur ou d'un mot de passe incorrect. L'erreur doit être corrigée, et le test doit être positif pour continuer.

# Page Serveur d'applications

Cette section inclut les rubriques suivantes :



## Général

Configurez le serveur d'applications Configuration Manager en utilisant les numéros de port par défaut indiqués ci-dessous.

## Paramètres

Pour configurer le serveur d'applications Configuration Manager, définissez les paramètres suivants :

| Paramètre | Valeur recommandée | Description |
|---|---|---|
| **Nom d'hôte** | <définie par l'utilisateur> | Nom externe du serveur d'applications<br>Par défaut, cette valeur est le nom d'hôte entièrement qualifié de l'ordinateur qui exécute l'Assistant (et Configuration Manager). Dans certains déploiements, ce nom doit être différent, par exemple lors du déploiement d'un serveur Web devant le serveur d'applications Configuration Manager. |
| **Personnaliser les ports** | <définie par l'utilisateur> | Par défaut, cette option n'est pas sélectionnée. Une fois sélectionnée, vous pouvez personnaliser les numéros de port par défaut du serveur d'applications. |

| Paramètre | Valeur recommandée | Description |
|---|---|---|
| **Port HTTP** | <définie par l'utilisateur> | Port HTTP du serveur d'applications Configuration Manager<br>Valeur par défaut : **8080**<br>Valeur par défaut une fois installé sur le même ordinateur HP Universal CMDB : **8180** |
| **Port HTTPS** | <définie par l'utilisateur> | Port HTTPS du serveur d'applications Configuration Manager<br>Valeur par défaut : **8443**<br>Valeur par défaut une fois installé sur le même ordinateur qu'UCMDB : **8143** |
| **Port Tomcat** | <définie par l'utilisateur> | Port de gestion du serveur d'applications Configuration Manager<br>Valeur par défaut : **8005** |
| **Port AJP** | <définie par l'utilisateur> | Port AJP (Apache Java Protocol) du serveur d'applications Configuration Manager<br>Valeur par défaut : **8009** |
| **Port HTTP JMX** | <définie par l'utilisateur> | Port HTTP JMX du serveur d'applications Configuration Manager<br>Valeur par défaut : **39900** |
| **Port à distance JMX** | <définie par l'utilisateur> | Port à distance JMX du serveur d'applications Configuration Manager<br>Valeur par défaut : **39600** |

# Page Configuration du service Windows

Indiquez s'il faut ou non installer Configuration Manager en tant que service Windows. Cette option n'est disponible que lors de l'installation sur un ordinateur Windows.

Le service Windows peut être configuré manuellement à l'aide de l'utilitaire **create-windows-service.bat** situé dans le répertoire **cnc-home/bin**.

# Page Informations d'identification de l'utilisateur

Cette section inclut les rubriques suivantes :

➤ "Général", page 30

## Général

Configurez les utilisateurs initiaux Configuration Manager suivants :

| Paramètre | Valeur recommandée | Description |
|---|---|---|
| **Utilisateur Admin** | <définie par l'utilisateur> | Utilisateur administratif de Configuration Manager—"super utilisateur" |
| **Utilisateur d'intégration** | <définie par l'utilisateur> | Utilisateur créé par Configuration Manager dans HP Universal CMDB pour les besoins d'intégration |

---

**Remarque :** Vous devez fournir un nom d'utilisateur et un mot de passe pour les utilisateurs administratif et d'intégration.

---

# Page Connexion HP Universal CMDB

Cette section inclut les rubriques suivantes :



## Général

La configuration de la connexion à HP Universal CMDB est facultative.

Lors de l'installation de Configuration Manager sur le même ordinateur qu'UCMDB dans une installation combinée, vous n'avez pas besoin de compléter cette page.

Si vous n'installez pas UCMDB dans une installation combinée, ou si vous installez UCMDB sur un autre ordinateur—même lors de la connexion à UCMDB sur localhost—ou lors de l'installation d'UCMDB avant Configuration Manager, UCMDB doit être activé et vous devez fournir ces propriétés de connexion.

---

**Remarque :** Lors de l'installation à l'aide d'une instance distante d'UCMDB, l'instance doit être activée et fonctionner. Lors de l'installation de Configuration Manager et d'UCMDB sur le même ordinateur, UCMDB doit être arrêté pendant l'exécution de cet Assistant.

---

## Paramètres

Pour configurer la connexion UCMDB, définissez les paramètres suivants :

| Paramètre | Valeur recommandée | Description |
|---|---|---|
| **Utiliser HP UCMDB sur un autre hôte** | <définie par l'utilisateur> | Sélectionnez cette option pour activer toutes les autres propriétés lors de l'installation de Configuration Manager et d'UCMDB sur des ordinateurs différents. |
| **Nom d'hôte** | <définie par l'utilisateur> | Nom d'hôte sur lequel UCMDB est installé |
| **Port** | <définie par l'utilisateur> | Port sur lequel UCMDB écoute |
| **Protocole** | <définie par l'utilisateur> | HTTP ou HTTPS |
| **Client** | <définie par l'utilisateur> | Client UCMDB |
| **Nom d'utilisateur administratif** | <définie par l'utilisateur> | Nom d'utilisateur sysadmin UCMDB |
| **Mot de passe administratif** | <définie par l'utilisateur> | Mot de passe sysadmin UCMDB |

## Test

---

**Remarque :** Il est vivement recommandé de tester les propriétés de connexion avant de poursuivre.

---

Pour cela, cliquez sur **Test**. L'Assistant tente d'accéder à UCMDB et de vérifier la connexion. Les résultats du test s'affichent à droite du bouton **Test**.

UCMDB génère différents messages d'erreur. Pas besoin d'explications— concernent généralement l'entrée d'un nom d'utilisateur ou d'un mot de passe incorrect. L'erreur doit être corrigée, et le test doit être positif pour continuer.

## Page Récapitulatif

Toutes les sélections effectuées dans les pages précédentes de l'Assistant sont affichées. Confirmez l'exactitude de toutes les sélections et effectuez les modifications appropriées. Lorsque tous les choix sont corrects, cliquez sur **Suivant**. L'Assistant exécute les tâches de configuration.

## Page Terminer

Il s'agit de la dernière page de l'Assistant Configuration de la post-installation Configuration Manager. Les tâches de configuration de la post-installation sont terminées. Cliquez sur **Terminer** pour fermer l'Assistant.

---

**Remarque :** Même si les tâches ont été exécutées avec succès, il est recommandé de vérifier les journaux situés dans **cnc-home/tmp/chp/app.log**.

---

# 3

# Configuration de LDAP

HP UCMDB Configuration Manager utilise LDAP pour gérer les utilisateurs, les rôles et les autorisations. Ce chapitre décrit les étapes de configuration et de résolution des problèmes LDAP.

Contenu de ce chapitre :



## LDAP - Présentation

Configuration Manager comporte un serveur LDAP interne (identifié dans l'interface utilisateur comme **Shared**) et peut également se connecter à un serveur LDAP organisationnel. Configuration Manager utilise ces serveurs pour localiser les utilisateurs, les groupes et les rôles, pour enregistrer les données de personnalisation et pour authentifier les utilisateurs. Vous pouvez choisir celui qui utilise le serveur LDAP organisationnel et le serveur LDAP interne.

Un déploiement type serait d'utiliser le serveur LDAP interne (Shared) pour enregistrer les rôles, et le serveur LDAP externe (organisation) pour les autres opérations.

### Choix des fournisseurs

1. Connectez-vous à **Configuration Manager** en tant qu'utilisateur administrateur.
2. Allez dans **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs**, et sélectionnez SHARED ou EXTERNAL pour chacun des attributs suivants en fonction de votre choix des fournisseurs (SHARED est l'option par défaut) :
   - ➤ Fournisseur d'authentification
   - ➤ Fournisseur de groupes
   - ➤ Fournisseur de personnalisation
   - ➤ Fournisseur de rôles
   - ➤ Fournisseur de relations de rôles
3. Enregistrez le jeu de configurations.

## Connexion à votre serveur LDAP organisationnel

HP UCMDB Configuration Manager est configuré à l'origine avec un serveur LDAP interne (Shared). Cette section décrit les étapes de connexion à votre serveur LDAP organisationnel.

Cette section inclut les rubriques suivantes :

## Configurer la connexion LDAP

Cette section explique comment connecter Configuration Manager à un serveur LDAP externe. Il s'agit du serveur LDAP organisationnel qui contient les utilisateurs d'organisation.

1. Connectez-vous à **Configuration Manager** en tant qu'utilisateur administrateur.
2. Allez dans **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs** > **Référentiel utilisateur externe**, et mettez à jour les attributs suivants en fonction des propriétés de votre LDAP organisationnel :

   **Connexion LDAP générale**

   **ldapHost** : <Nom d'hôte LDAP>

   **ldapPort** : <Numéro de port LDAP>

   **enableSSL** : <True/false—utiliser la connexion SSL à LDAP>

   **useAdministrator** : <True/false—utiliser l'utilisateur pour la connexion à LDAP>

   **ldapAdministrator** : <nom d'utilisateur LDAP (doit être défini si **useAdministrator=true)**>

   **ldapAdministratorPassword** : <mot de passe d'utilisateur LDAP (doit être défini si **useAdministrator=true**)>
3. Enregistrez le jeu de configurations.

## Configurer les fournisseurs de groupes et d'utilisateurs

Cette procédure définit le LDAP organisationnel (référentiel externe) comme fournisseur de groupes et d'utilisateurs. Ce LDAP interne (référentiel partagé) est toujours utilisé pour l'authentification, mais les utilisateurs et les groupes sont extraits du LDAP externe. Ce mode est utilisé pour tester la configuration du LDAP externe et octroyer des autorisations aux utilisateurs organisationnels.

**Pour définir les fournisseurs de groupes et d'utilisateurs :**

1. Si vous n'êtes pas déjà dans cette page, allez dans **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs** > **Référentiel utilisateur externe**. Assurez-vous d'utiliser le même jeu de configurations que vous avez enregistré dans la section "Configurer la connexion LDAP", page 37.
2. Mettez à jour les attributs suivants en fonction des propriétés de votre LDAP organisationnel :
   a. **Recherche d'utilisateurs**

      **usersBase** : <DN de base pour la recherche d'utilisateurs>

      **usersScope** : <Étendue de la recherche d'utilisateurs>

      **usersFilter** : <Filtre de la recherche d'utilisateurs>

   b. **Classe d'objets utilisateurs** (dépend du fournisseur LDAP)

      **usersObjectClass** : <Classe d'objets LDAP utilisateurs>

      **usersUniqueIDAttribute** : <Attribut ID LDAP unique utilisateurs>

      Les attributs suivants sont facultatifs :

      **usersDisplayNameAttribute** : <Attribut LDAP du nom d'affichage utilisateurs>

      **usersLoginNameAttribute** : <Attribut LDAP du nom de connexion utilisateurs>

      **usersFirstNameAttribute** : <Attribut LDAP du prénom utilisateurs>

      **usersLastNameAttribute** : <Attribut LDAP du nom utilisateurs>

      **usersEmailAttribute** : <Attribut LDAP de l'e-mail utilisateurs>

      **usersPreferredLanguageAttribute** : <Attribut LDAP de la langue privilégiée utilisateurs>

      **usersPreferredLocationAttribute** : <Attribut LDAP de l'emplacement privilégié utilisateurs>

      **usersTimeZoneAttribute** : <Attribut LDAP de fuseau horaire utilisateurs>

**usersDateFormatAttribute** : <Attribut LDAP de format de date utilisateurs>

**usersNumberFormatAttribute** : <Attribut LDAP de format numérique utilisateurs>

**usersWorkWeekAttribute** : <Attribut LDAP de semaine de travail utilisateurs>

**usersTenantIDAttribute** : <Attribut ID LDAP de clients utilisateurs>

**usersPasswordAttribute** : <Attribut LDAP de mot de passe utilisateurs>

**c** **Recherche de groupes**

**groupsBase** : <DN de base pour la recherche de groupes>

**groupsScope** : <Étendue LDAP pour la recherche de groupes>

**groupsFilter** : <Filtre de la recherche de groupes>

**rootGroupsBase** : <DN de base pour la recherche de groupes racine>

**rootGroupsScope** : <Étendue LDAP pour la recherche de groupes racine>

**rootGroupsFilter** : <Filtre de la recherche de groupes>

**d** **Classe d'objets de groupes** (dépend du fournisseur LDAP)

**groupsObjectClass** : <Classe d'objets LDAP de groupes>

**groupsMembersAttribute** : <Attribut LDAP de membres de groupes>

Les attributs suivants sont facultatifs :

**groupsNameAttribute** : <Attribut LDAP de nom unique de groupes>

**groupsDisplayNameAttribute** : <Attribut LDAP de nom d'affichage de groupes>

**groupsDescriptionAttribute** : <Attribut LDAP de description de groupes>

**enableDynamicGroups** : <Activer des groupes dynamiques>

**dynamicGroupsClass** : <Classe d'objets LDAP de groupes dynamiques>

**dynamicGroupsMemberAttribute** : <Attribut LDAP de membres de groupes dynamiques>

**dynamicGroupsNameAttribute** : <Attribut LDAP de nom unique de groupes dynamiques>

**dynamicGroupsDisplayNameAttribute** : <Attribut LDAP de nom unique d'affichage de groupes dynamiques>

**dynamicGroupsDescriptionAttribute** : <Attribut LDAP de description de groupes dynamiques>

**e** **Hiérarchie des groupes** (si votre LDAP organisationnel utilise la hiérarchie des groupes)

**enableNestedGroups** : <Activer la prise en charge des groupes imbriqués>

**maximalAllowedGroupsHierarchyDepth** : <Profondeur maximale autorisée pour la hiérarchie des groupes>

**f** **Configuration avancée**

**ldapVersion** : <Version LDAP>

**baseDistinguishNameDelimiter** : <Délimiteur de DN de base>

**scopeDelimiter** : <Délimiteur d'étendue>

**attributeValuesDelimiter** : <Délimiteur des valeurs d'attributs LDAP>

**3** Enregistrez le jeu de configurations.

## Activer le jeu de configurations

**1** Allez dans **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs**, et effectuez la mise à jour suivante :

**Source UUM externe :** True

**Fournisseur de groupes :** EXTERNAL

**Fournisseur d'utilisateurs :** EXTERNAL

**2** Enregistrez le jeu de configurations et activez-le.

**3** Déconnectez-vous et redémarrez le serveur **Configuration Manager**.

## Octroyer des autorisations aux utilisateurs

Cette procédure permet d'octroyer le rôle **Administrateur système** aux utilisateurs organisationnels. Un utilisateur ayant le rôle **Administrateur système** sera autorisé à octroyer les rôles appropriés aux autres utilisateurs organisationnels.

1. Connectez-vous à **Configuration Manager** en tant qu'utilisateur administrateur.
2. Ouvrez le module **Gestion des utilisateurs** (**Administration** > **Gestion des utilisateurs**).
3. Confirmez que les groupes et les utilisateurs de votre LDAP organisationnel sont visibles.
4. Allez dans **Gestion des utilisateurs** > **volet Recherche des utilisateurs** et recherchez les utilisateurs qui auront le rôle d'administrateur—exemple : Prénom = j*, Nom = Martin.
5. Ajoutez le rôle **Administrateur système** aux utilisateurs.

## Définir le fournisseur d'authentification comme LDAP externe

Cette procédure permet de définir le LDAP organisationnel externe comme fournisseur d'authentification, pour que les utilisateurs organisationnels soient utilisés pour l'authentification.

1. Allez dans **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs**, et effectuez la mise à jour suivante :

   **Fournisseur d'authentification** : EXTERNAL
2. Enregistrez le jeu de configurations et activez-le.
3. Déconnectez-vous et redémarrez le serveur **Configuration Manager**.
4. Connectez-vous avec l'un des utilisateurs organisationnels ayant le rôle **Administrateur système**.

### Importer le certificat LDAP

Si un certificat est requis pour la connexion à votre LDAP organisationnel, procédez comme suit :

1. Exportez le certificat dans un fichier.
2. Arrêtez le service Configuration Manager Windows.
3. Exécutez la commande suivante :

   <répertoire d'installation Configuration Manager >\java\windows\x86_64\bin\keytool.exe -import -trustcacerts -alias <alias de certificat> -keystore <répertoire d'installation Configuration Manager >\java\windows\x86_64\lib\security\cacerts -storepass changeit -file <chemin du fichier du certificat>

4. Démarrez le service Configuration Manager Windows.

## Configuration du LDAP interne (Shared)

### Modification du mot de passe du serveur LDAP (Shared) interne (facultatif)

Pour des raisons de sécurité, vous pouvez modifier le mot de passe du serveur LDAP (Shared) interne.

1. Connectez-vous à **HP Universal CMDB Configuration Manager**.
2. Ouvrez une ligne de commande et naviguez jusqu'au <**répertoire d'installation de Configuration Manager**>**ldap****serverRoot****bat**.
3. **ldappasswordmodify -h localhost -p <ldap port> -D "cn=Directory Manager" -w <mot de passe admin ldap> -c <mot de passe admin ldap> -n <nouveau mot de passe admin ldap>**.
   a. Le mot de passe admin ldap par défaut est **ldapadmin**.
   b. Le port par défaut est **2389**.
   c. Confirmez que la commande a été exécutée avec succès et poursuivez les étapes suivantes.

4. Dans **UCMDB Configuration Manager**, sélectionnez **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs** > **Référentiel utilisateur partagé**.
5. Mettez à jour le mot de passe dans l'attribut **ldapAdministratorPassword**.
6. Enregistrez le jeu de configurations et activez-le.
7. Déconnectez-vous d'**UCMDB Configuration Manager**.
8. Redémarrez le serveur **UCMDB Configuration Manager**.

## Configuration du port LDAP interne (Shared)

Le port par défaut, 2839, est peut-être utilisé par une autre application. Pour modifier ce port par défaut, procédez comme suit.

**Pour configurer le port LDAP interne :**

1. Ouvrez une ligne de commande et naviguez jusqu'au **<répertoire d'installation de Configuration Manager>\ldap\serverRoot\bat**.
2. Exécutez la commande suivante :
   dsconfig -h localhost -p 2444 -D "cn=directory manager" -w <mot de passe admin ldap> --trustAll -X -n set-connection-handler-prop --handler-name "LDAP Connection Handler" --set listen-port:<nouveau port>

   Le <mot de passe admin ldap> par défaut est **ldapadmin**.
3. Confirmez qu'aucun message d'erreur n'est affiché et poursuivez les étapes suivantes.
4. Connectez-vous à HP Universal CMDB Configuration Manager.
5. Dans UCMDB Configuration Manager, sélectionnez **Administration** > **Administration des serveurs** > **Gestion des utilisateurs**> **Configuration de la gestion des utilisateurs** > **Référentiel utilisateur partagé**, et mettez à jour le numéro de port dans l'attribut **ldapPort**.
6. Enregistrez le jeu de configurations et activez-le.
7. Déconnectez-vous d'UCMDB Configuration Manager.
8. Redémarrez le serveur UCMDB Configuration Manager.

# Résolution des problèmes LDAP

**Problème :** La communication avec le serveur LDAP ne peut pas être établie. Une exception de communication est enregistrée dans les journaux.

**Solution :** Vérifiez l'hôte LDAP, le port et les paramètres de mode SSL :

**a** Vérifiez que l'hôte et le port LDAP sont correctement configurés : Sélectionnez **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs** > **Référentiel utilisateur externe** et vérifiez les paramètres **ldapHost, ldapPort**.

**b** Vérifiez que le mode SSL est correctement configuré. Assurez-vous auprès de votre administrateur LDAP organisationnel que l'utilisateur administrateur est requis pour la connexion LDAP. Sélectionnez **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs** > **Référentiel utilisateur externe** et vérifiez le paramètre **enableSSL**.

**c** Assurez-vous que le certificat de serveur approprié est installé. Exécutez la commande suivante :

```
<répertoire d'installation Configuration Manager>\java\windows\x86_64\bin\keytool.exe -list -trustcacerts [-alias <alias de certificats>] -keystore <répertoire d'installation Configuration Manager>\java\windows\x86_64\lib\security\cacerts -storepass changeit
```

**d** Vérifiez auprès de votre administrateur LDAP organisationnel que l'administrateur est requis pour la connexion LDAP. Sélectionnez **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs** > **Référentiel utilisateur externe** et vérifiez les paramètres suivants : **useAdministrator, ldapAdministrator, ldapAdministratorPassword**

**Problème :** Aucun groupe n'est affiché sur l'écran de gestion des utilisateurs ou des groupes. Aucune exception n'est enregistrée dans les journaux.

**Solution :** Effectuez la vérification suivante :

**a** Vérifiez que les filtres de recherche d'utilisateurs et de groupes sont correctement configurés : Sélectionnez **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs** > **Référentiel utilisateur externe** et modifiez les propriétés suivantes : **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter.**

**b** Ouvrez le navigateur des clients LDAP et recherchez les utilisateurs sous le DNS de base.

**Problème :** L'interface utilisateur est trop lente.

**Solution :** Cela est généralement dû au fait qu'un trop grand nombre de groupes ou d'utilisateurs est configuré dans votre LDAP. Configurez le DNS de base et les filtres pour réduire le nombre de groupes dans le sous-ensemble approprié comme suit :

**a** Sélectionnez **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs** > **Référentiel utilisateur externe**

**b** Modifiez les paramètres suivants : **usersBase, usersScope, usersFilter, groupsBase, groupsScope, groupsFilter, rootGroupsBase, rootGroupsScope, rootGroupsFilter**

**Problème :** Des utilisateurs connus n'apparaissent pas sur l'écran de gestion des groupes ou des utilisateurs.

**Solution :** L'écran de gestion des utilisateurs ou des groupes n'affiche que les utilisateurs appartenant à un groupe. Placez les utilisateurs dans les groupes appropriés de LDAP pour qu'ils apparaissent sur l'écran principal.

**Problème :** La connexion est trop longue.

**Solution :** L'utilisateur appartient peut-être à trop de groupes. Vous pouvez personnaliser le temps de démarrage en modifiant le filtre de recherche des groupes pour qu'un nombre moindre de groupe soit renvoyé, comme suit :

**a** Sélectionnez **Administration** > **Administration des serveurs** > **Gestion des utilisateurs** > **Configuration de la gestion des utilisateurs** > **Référentiel utilisateur externe**

**b** Modifiez le paramètre **groupsFilter**.

# 4

# LW-SSO (Lightweight Single Sign-On Authentication) – Références générales

Contenu de ce chapitre :



## Authentification LW-SSO - Présentation

LW-SSO est une méthode de contrôle d'accès qui permet à un utilisateur d'établir une seule connexion aux ressources de plusieurs systèmes logiciels sans avoir à se reconnecter par la suite. Les applications figurant dans le groupe configuré de systèmes logiciels tiennent compte de cette authentification. Il n'est donc pas nécessaire de procéder à une autre authentification lorsque vous passez d'une application à une autre.

Les informations de cette section s'applique à LW-SSO versions 2.2 et 2.3.

Cette section contient les rubriques suivantes :

## Délai d'expiration du jeton LW-SSO

La valeur du délai d'expiration du jeton LW-SSO détermine la validité de la session de l'application. Par conséquent, la valeur de son délai d'expiration doit être au moins identique à celle de la session de l'application.

## Configuration recommandée pour le délai d'expiration du jeton LW-SSO

Chaque application qui utilise LW-SSO doit configurer le délai d'expiration du jeton. La valeur recommandée est 60 minutes. Pour une application ne requérant pas un haut niveau de sécurité, il est possible de configurer une valeur de 300 minutes.

## Heure GMT

Toutes les applications impliquées dans une intégration LW-SSO doivent utiliser la même heure GMT avec une différence maximum de 15 minutes.

## Fonctionnalité multi-domaines

La fonctionnalité multi-domaines requiert que toutes les applications qui participent à l'intégration LW-SSO configurent les paramètres trustedHosts (ou les paramètres **protectedDomains**, s'ils sont requis pour s'intégrer dans des applications de différents domaines DNS. De plus, ils doivent également ajouter le domaine approprié dans l'élément **lwsso** de la configuration.

## Obtenir SecurityToken pour la fonctionnalité URL

Pour recevoir des informations envoyées sous la forme d'un **SecurityToken pour URL** en provenance d'autres applications, l'application hôte doit configurer le domaine approprié dans l'élément **lwsso** de la configuration.

# Avertissements de sécurité LW-SSO

Cette section présente les avertissements de sécurité relatifs à la configuration LW-SSO :

➤ **Paramètre confidentiel InitString dans LW-SSO.** LW-SSO utilise une méthode de chiffrement symétrique (Symmetric Encryption) pour valider et créer un jeton LW-SSO. Le paramètre **initString** de la configuration sert à l'initialisation de la clé secrète. Une application crée un jeton et chaque application partageant le même paramètre initString valide le jeton.

---

**Attention :**

➤ Il n'est pas possible d'utiliser LW-SSO sans définir le paramètre **initString**.

➤ Le paramètre **initString** contient des informations confidentielles et doit être traité comme tel en termes de publication, de transport et de persistance.

➤ Le paramètre **initString** doit être partagé uniquement entre des applications mutuellement intégrées à l'aide de LW-SSO.

➤ Le paramètre **initString** doit contenir au minimum 12 caractères.

---

➤ **Activer LW-SSO uniquement en cas de besoin.** LW-SSO doit être désactivé sauf spécification contraire.

➤ **Niveau de sécurité d'authentification.** L'application qui utilise l'infrastructure d'authentification la plus faible et émet un jeton LW-SSO devant être approuvé par d'autres applications intégrées détermine le niveau de sécurité d'authentification de toutes les applications.

Seules les applications qui utilisent des infrastructures d'authentification fortes et sécurisées émettent un jeton LW-SSO.

- **Implications du chiffrement symétrique.** LW-SSO utilise le chiffrement symétrique pour émettre et valider des jetons LW-SSO. Par conséquent, toute application qui utilise LW-SSO peut émettre un jeton devant être approuvé par toutes les autres applications qui partagent le même paramètre **initString**. Ce risque potentiel est pertinent lorsqu'une application qui partage un paramètre initString, réside ou est accessible depuis un emplacement non approuvé.

- **Mappage des utilisateurs (Synchronisation).** L'infrastructure LW-SSO n'assure pas le mappage des utilisateurs entre les applications intégrées. Par conséquent, l'application intégrée doit contrôler le mappage des utilisateurs. Nous vous recommandons de partager le même registre utilisateur (comme LDAP/AD) entre toutes les applications intégrées.

  L'échec du mappage des utilisateurs peut provoquer des violations de sécurité et un comportement négatif des applications. Par exemple, le même nom d'utilisateur peut être attribué à différents utilisateurs réels dans les différentes applications.

  De plus, lorsqu'un utilisateur se connecte à une application (AppA) et accède ensuite à une seconde application (AppB) qui utilise l'authentification de conteneur ou d'application, l'échec du mappage de l'utilisateur peut forcer l'utilisateur à se connecter manuellement à AppB et à entrer un nom d'utilisateur. Si l'utilisateur entre un autre nom que celui utilisé pour la connexion à AppA, le comportement suivant peut se produire : si l'utilisateur accède ensuite à une troisième application (AppC) à partir d'AppA ou d'AppB, il va y accéder en utilisant les noms d'utilisateur spécifiés pour la connexion à AppA ou AppB respectivement.

- **Gestionnaire des identités**. Utilisé pour l'authentification, toutes les ressources non protégées du Gestionnaire des identités doivent être configurées à l'aide du paramètre **nonsecureURLs** du fichier de configuration LW-SSO.

# Résolution des problèmes et limitations

## Problèmes connus

Cette section décrit les problèmes connus en matière d'authentification LW-SSO.

- **Contexte de la sécurité.** Le contexte de la sécurité LW-SSO ne prend en charge qu'une valeur d'attribut par nom d'attribut.

  Par conséquent, lorsque le jeton SAML2 envoie plusieurs valeurs pour le même nom d'attribut, une seule valeur est acceptée par l'infrastructure LW-SSO.

  De même, si le jeton IdM est configuré pour envoyer plusieurs valeurs pour le même nom d'attribut, une seule valeur est acceptée par l'infrastructure LW-SSO.

- **Fonctionnalité de déconnexion multi-domaines dans Internet Explorer 7**. La fonctionnalité de déconnexion multi-domaines peut échouer dans les conditions suivantes :

  - Le navigateur utilisé est Internet Explorer 7 et l'application appelle plus de trois verbes de redirection HTTP 302 consécutifs dans la procédure de déconnexion.

  Dans ce cas, Internet Explorer 7 risque de ne pas interpréter correctement la réponse de redirection HTTP 302 et afficher une page d'erreur **Internet Explorer ne peut pas afficher la page Web**.

  Pour contourner le problème, il est recommandé, si possible, de réduire le nombre de commandes de redirection de l'application dans la séquence de déconnexion.

## Limitations

Notez les limitations suivantes lors de l'authentification LW-SSO :

- **Accès client à l'application**.

  **Si un domaine est défini dans la configuration LW-SSO** :

  - Les clients de l'application doivent accéder à l'application à l'aide d'un nom de domaine complet (FQDN) dans l'URL de connexion, par exemple, http://monserveur.**domaineentreprise**.com/AppWeb.
  - LW-SSO ne peut pas prendre en charge les URL contenant une adresse IP, par exemple, http://192.168.12.13/AppWeb.
  - LW-SSO ne peut pas prendre en charge les URL ne contenant pas de domaine, http://monserveur/AppWeb.

  **Si un domaine n'est pas défini dans la configuration LW-SSO** : Le client peut accéder à l'application sans FQDN dans l'URL de connexion. Dans ce cas, un cookie de session LW-SSO est créé spécifiquement pour un seul ordinateur sans informations de domaine. Par conséquent, le cookie n'est pas délégué par le navigateur à un autre navigateur, et ne transmet pas aux autres ordinateurs situés dans le même domaine DNS. Cela signifie que LW-SSO ne fonctionne pas dans le même domaine.

- **Intégration de l'infrastructure LW-SSO.** Les applications peuvent influencer et utiliser les fonctionnalités LW-SSO uniquement si elles sont pré-intégrées dans l'infrastructure LW-SSO.

- **Prise en charge multi-domaines**.

  - La fonctionnalité multi-domaines repose sur un point d'accès HTTP. Par conséquent, LW-SSO prend en charge les liens d'une application vers une autre et non pas la saisie d'une URL dans une fenêtre de navigateur, sauf si les applications partagent le même domaine.
  - Le premier lien croisé de domaine qui utilise **HTTP POST** n'est pas pris en charge.

    La fonctionnalité multi-domaines ne prend pas en charge la première demande **HTTP POST** d'une seconde application (seule la demande **HTTP GET** est prise en charge). Par exemple, si votre application comporte un lien HTTP vers une seconde application, une demande **HTTP GET** est prise en charge, mais une demande **HTTP FORM** ne l'est pas. Toutes les demandes émises après la première peuvent être **HTTP POST** ou **HTTP GET**.

- Taille du jeton LW-SSO :

  Le volume des informations que LW-SSO peut transférer d'une application d'un domaine vers une autre application d'un autre domaine est limité à 15 Groupes/Rôles/Attributs (notez que chaque élément peut contenir en moyenne 15 caractères).

- Liaison d'une page protégée (HTTPS) à une page non protégée (HTTP) dans une configuration multi-domaines :

  La fonctionnalité multi-domaines ne fonctionne pas pour la liaison d'une page protégée (HTTPS) à une page non protégée (HTTP). Il s'agit d'une limitation du navigateur où l'en-tête du point d'accès n'est pas envoyé lors de la liaison à partir d'une ressource protégée à une ressource non protégée. Pour un exemple, voir : http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP

- **Jeton SAML2**

  - La fonctionnalité de déconnexion n'est pas prise en charge lorsque le jeton SAML2 est utilisé.

    Par conséquent, si le jeton SAML2 est utilisé pour accéder à une seconde application, un utilisateur qui se déconnecte de la première application ne l'est pas de la seconde.

  - Le délai d'expiration du jeton SAML2 n'est pas reflété dans la gestion de session de l'application.

    Par conséquent, si le jeton SAML2 est utilisé pour accéder à une seconde application, chaque gestion de session d'application est traitée de manière indépendante.

- **Domaine JAAS.** Le domaine JAAS de Tomcat n'est pas pris en charge.

- **Utilisation d'espaces dans les répertoires Tomcat.** L'utilisation d'espaces dans les répertoires Tomcat n'est pas prise en charge.

  Il n'est pas possible d'utiliser LW-SSO lorsqu'un chemin d'installation Tomcat (dossiers) inclut des espaces (par exemple, Program Files) et que le fichier de configuration LW-SSO est situé dans le dossier Tomcat **common\classes**.

- **Configuration du processus d'équilibrage de la charge.** Un processus d'équilibrage de la charge déployé avec LW-SSO doit être configuré pour utiliser des sessions permanentes.

# 5

# Authentification du Gestionnaire des identités

Contenu de ce chapitre :



## Accepter l'authentification du Gestionnaire des identités

Si vous utilisez le Gestionnaire des identités et si vous prévoyez d'ajouter HP Universal CMDB Configuration Manager, vous devez exécuter cette tâche.

Celle-ci décrit comment configurer HP Universal CMDB Configuration Manager pour accepter l'authentification du Gestionnaire des identités.

Cette tâche inclut les étapes suivantes :



### Conditions préalables

Le serveur Tomcat Configuration Manager doit être connecté à votre serveur Web (IIS ou Apache) protégé par votre Gestionnaire des identités à l'aide d'un connecteur Tomcat Java (AJP13).

Pour les instructions d'utilisation d'un connecteur Tomcat Java (AJP13), voir la documentation Tomcat Java (AJP13).

## Configurer HP Universal CMDB Configuration Manager pour accepter le Gestionnaire des identités

**Pour configurer Tomcat Java (AJP13) à l'aide de IIS6 :**

1. Configurez le Gestionnaire des identités pour envoyer un en-tête / rappel de personnalisation contenant le nom de l'utilisateur, et demander le nom de l'en-tête.
2. Ouvrez le **<répertoire d'installation Configuration Manager>\conf\lwssofmconf.xml** et localisez la section commençant par **in-ui-identity-management**.

   Par exemple :

   ```
   <in-ui-identity-management enabled="false">
       <identity-management>
         <userNameHeaderName>sm-user</userNameHeaderName>
       </identity-management>
   </in-ui-identity-management>
   ```

   a. Activez la fonctionnalité en supprimant le caractère de commentaire.

   b. Remplacez **enabled="false"** par **enabled="true"**.

   c. Remplacez **sm-user** par le nom d'en-tête que vous avez demandé à l'étape 1.
3. Ouvrez le **<répertoire d'installation Configuration Manager>\conf\client-config.properties** et modifiez les propriétés suivantes :

   a. Modifiez **bsf.server.url** selon l'URL du Gestionnaire des identités et modifiez le port selon le port du Gestionnaire des identités :

   ```
   bsf.server.url=http://<URL du Gestionnaire des identités>:< Port du Gestionnaire des identités >/bsf
   ```

   b. Modifiez **bsf.server.services.url** selon le protocole HTTP et modifiez le port selon le port original Configuration Manager :

   ```
   bsf.server.services.url=http://<URL Configuration Manager>:< Port Configuration Manager>/bsf
   ```

# Exemple d'utilisation du connecteur Java pour configurer le Gestionnaire des identités pour Configuration Manager à l'aide de IIS6 sur un système d'exploitation Windows 2003

Cette tâche de l'exemple décrit comment installer et configurer le connecteur Java permettant de configurer le Gestionnaire des identités pour l'utiliser avec Configuration Manager à l'aide de IIS6 fonctionnant sur un système d'exploitation Windows 2003.

**Pour installer le connecteur Java et le configurer pour IIS6 sous Windows 2003 :**

1. Téléchargez la dernière version du connecteur Java (par exemple, **djk-1.2.21**) à partir du site Web Apache.
   a. Cliquez sur **http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/**.
   b. Sélectionnez la dernière version.
   c. Téléchargez le fichier **isapi_redirect.dll** à partir du répertoire **amd64**.
2. Enregistrez ce fichier sous **<répertoire d'installation Configuration Manager>\tomcat\bin\win32**.
3. Créez un nouveau fichier texte appelé **isapi_redirect.properties** dans le même répertoire contenant isapi_redirect.dll.

   Le contenu de ce fichier est le suivant :

   ```
   # Configuration file for the Jakarta ISAPI Redirector

   # The path to the ISAPI Redirector Extension, relative to the website

   # This must be in a virtual directory with execute privileges

   extension_uri=/jakarta/isapi_redirect.dll

   # Full path to the log file for the ISAPI Redirector

   log_file=<répertoire d'installation Configuration Manager>\servers\server-0\logs\isapi.log

   # Log level (debug, info, warn, error or trace)

   log_level=info
   ```

```
# Full path to the workers.properties file

worker_file==<répertoire d'installation Configuration Manager
>\tomcat\conf\workers.properties.minimal

# Full path to the uriworkermap.properties file

worker_mount_file==<répertoire d'installation Configuration
Manager>\tomcat\conf\uriworkermap.properties
```

**4** Créez un nouveau fichier texte appelé **workers.properties.minimal** dans <**répertoire d'installation Configuration Manager**>**tomcat****conf**.

Le contenu de ce fichier est le suivant :

```
# workers.properties.minimal -

#

# This file provides minimal jk configuration

# properties needed to

# connect to Tomcat.

#

# Defining a worker named ajp13w and of type ajp13

# Note that the name and the type do not have to

# match.

        worker.list=ajp13w

        worker.ajp13w.type=ajp13

        worker.ajp13w.host=localhost

        worker.ajp13w.port=8009

#END
```

**5** Créez un nouveau fichier texte appelé **uriworkermap.properties** dans <**répertoire d'installation Configuration Manager**>**tomcat****conf**.

Le contenu de ce fichier est le suivant :

```
# uriworkermap.properties - IIS

#
```

```
# This file provides sample mappings for example:
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]

/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

---

**Important :** Notez que Configuration Manager doit comporter deux règles. La nouvelle syntaxe leur permet de constituer une seule règle, telle que :

**/cnc|/*=ajp13w**

---

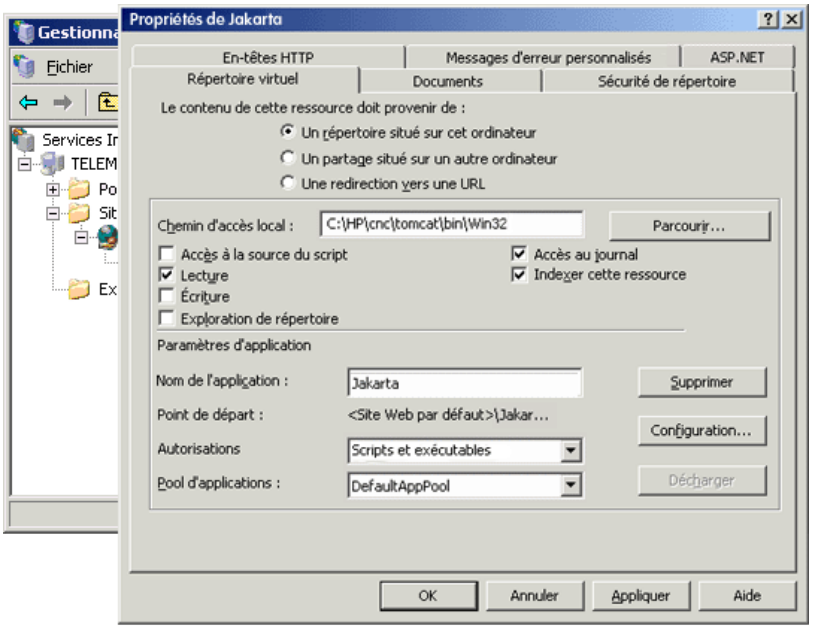
**6** Créez le répertoire virtuel dans l'objet Site Web correspondant de la configuration IIS.

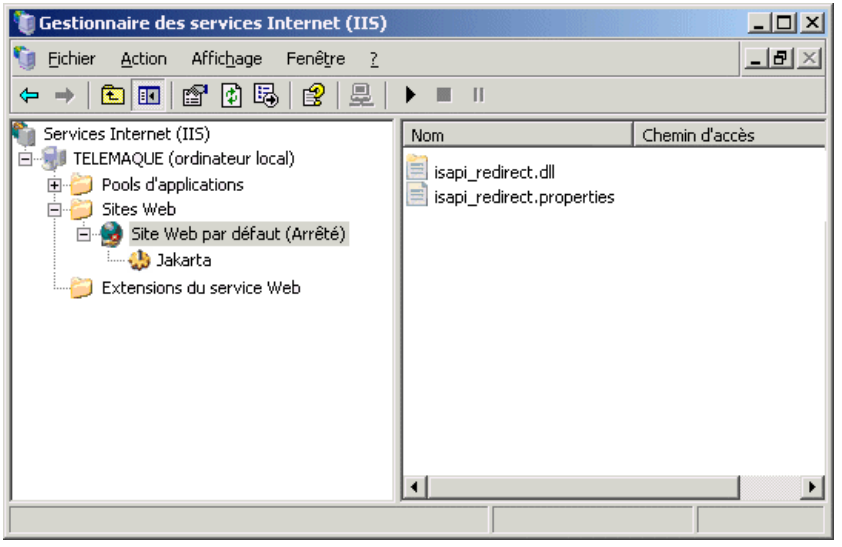
**a** Dans le menu Démarrer de Windows, ouvrez **Paramètres\Panneau de configuration\Outils d'administration\Gestionnaire Internet Information Services (IIS)**.

**b** Dans le volet de droite, cliquez avec le bouton droit sur le **<nom de l'ordinateur local>\Sites Web\<Le nom de votre site Web>** et sélectionnez **Nouveau\Répertoire virtuel**.

**c** Attribuez au répertoire le nom d'alias **Jakarta**, et définissez le chemin local jusqu'au répertoire contenant isapi_redirect.dll.

La fenêtre du Gestionnaire ressemble à la suivante :



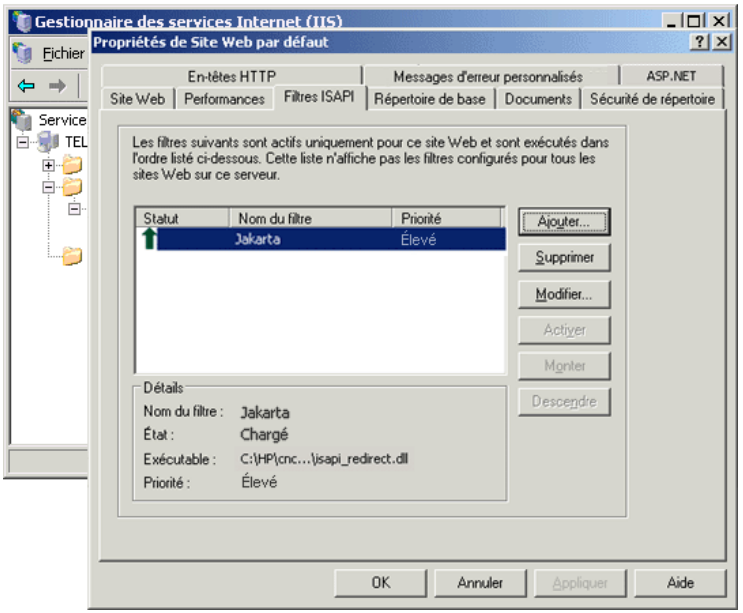
**7** Ajoutez **isapi_redirect.dll** comme filtre ISAPI.

**a** Cliquez avec le bouton droit sur le **<nom de votre site Web>** et sélectionnez **Propriétés**.

**b** Sélectionnez l'onglet **Filtres ISAPI**, et cliquez sur le bouton **Ajouter...**.

**c** Sélectionnez le nom du filtre **Jakarta**, et parcourez jusqu'à **isapi_redirect.dll**. Le filtre est ajouté, mais il n'est pas activé.

La fenêtre de configuration ressemble à la suivante :



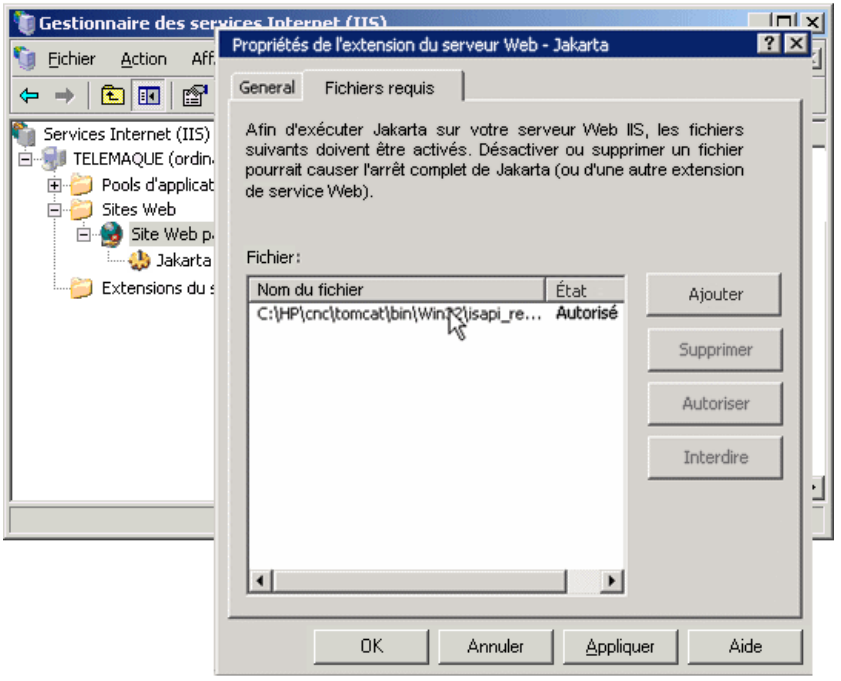

**d** Cliquez sur le bouton **Appliquer**.

**8** Définissez et autorisez la nouvelle extension du service Web.

**a** Cliquez avec le bouton droit sur le **<nom de l'ordinateur local >\entrée Extensions du service Web** et sélectionnez l'option de menu **Ajouter une nouvelle extension du service Web...**.

**b** Attribuez le nom **Jakarta** à la nouvelle extension du service Web, et parcourez jusqu'au fichier **isapi_redirect.dll**.

**Remarque :** Avant de cliquer sur le bouton **OK**, cochez la case **Définir l'état de l'extension à Autorisée**.




**9** Redémarrez le serveur Web IIS, et accédez à l'application par le biais du service Web.

# 6

# Connexion à Configuration Manager

Contenu de ce chapitre :



## Accès à Configuration Manager

Vous accédez à Configuration Manager à l'aide d'un navigateur Web pris en charge, à partir de n'importe quel ordinateur par le biais d'une connexion réseau (intranet ou Internet) sur le serveur Configuration Manager. Le niveau d'accès octroyé à l'utilisateur dépend de ses autorisations. Pour plus d'informations sur l'octroi d'autorisations utilisateur, consultez la section "Gestion des utilisateurs" du Guide de l'utilisateur *HP Universal CMDB Configuration Manager*.

Pour plus d'informations sur la configuration du navigateur Web, et la configuration minimale requise pour afficher Configuration Manager, voir "Configuration Manager - Configuration requise", page 8.

Pour plus d'informations sur l'accès en toute sécurité à Configuration Manager, voir "Sécurisation renforcée", page 73.

# Comment accéder à Configuration Manager

Dans le navigateur Web, entrez l'URL du serveur Configuration Manager, par exemple, **http://<nom du serveur ou adresse IP>.<nom de domaine>:<port>** où **<nom du serveur ou adresse IP>.<nom de domaine>** représente le nom de domaine qualifié (FQDN) du serveur Configuration Manager et **<port>** le port sélectionné au cours de l'installation.

## Se connecter à Configuration Manager

1. Entrez le nom d'utilisateur et le mot de passe que vous avez définis dans l'Assistant Post-installation Configuration Manager.
2. Cliquez sur **Connexion**. Une fois la connexion établie, le nom d'utilisateur s'affiche en haut à droite de l'écran.
3. (Recommandé) Connectez-vous au serveur LDAP organisationnel et attribuez des rôles administratifs aux utilisateurs LDAP pour que les administrateurs Configuration Manager puissent accéder au système. Pour plus d'informations sur l'attribution de rôles aux utilisateurs du système Configuration Manager, voir "Gestion des utilisateurs" dans le *Guide de l'utilisateur HP Universal CMDB Configuration Manager*.

## Se déconnecter

Lorsque vous avez terminé votre session, il est recommandé de vous déconnecter du site Web afin d'éviter toute entrée non autorisée.

**Pour vous déconnecter :**

Cliquez sur **Déconnexion** en haut de la page.

---

**Remarque :** Le temps d'expiration par défaut d'une session est de 30 minutes.

---

## Accès à la console JMX de Configuration Manager

Pour résoudre les problèmes ou modifier certaines configurations, il peut être nécessaire d'accéder à la console JMX.

**Pour accéder à la console JMX :**

1. Ouvrez la console JMX à l'adresse http://<nom de serveur ou adresse IP>:<port>/cnc/jmx-console. Il s'agit du port configuré au cours de l'installation de Configuration Manager.
2. Entrez les informations d'identification de l'utilisateur par défaut. Elles sont identiques à celles utilisées pour la connexion à Configuration Manager.

## Résolution des problèmes et limitations

**Problème**. Après avoir modifié le jeu de configurations dans Administration des serveurs, le serveur ne démarre pas.

**Solution**. Rétablissez le jeu de configurations précédent. Procédez comme suit :

1. Exécutez la commande suivante pour rechercher l'ID du dernier jeu de configurations activé :

   ```
   <HP Universal CMDB Configuration Manager>\bin\export-cs.bat
   <propriétés de la base de données> --history
   ```

   où les <**propriétés de la base de données**> peuvent être définies en pointant l'emplacement du <**répertoire d'installation Configuration Manager** >**\conf\database.properties** ou en spécifiant chaque propriété de base de données. Par exemple :

   ```
   cd <HP Universal CMDB Configuration Manager>\bin export-cs.bat -p
   ..\conf\database.properties --history
   ```

2. Exécutez la commande suivante pour exporter le dernier jeu de configurations :

   ```
   < HP Universal CMDB Configuration Manager>\bin\export-cs.bat
   <propriétés de la base de données> <ID jeu de configurations> <nom de
   fichier de vidage>
   ```

où <**ID jeu de configurations**> est l'ID du jeu de configurations de l'étape précédente et <**fichier de vidage**> le nom d'un fichier temporaire utilisé pour enregistrer le jeu de configurations. Par exemple, pour exporter un jeu de configurations à l'aide de l'ID **491520** dans le fichier **mydump.zip**, entrez la commande suivante :

```
cd <répertoire d'installation HP Universal CMDB Configuration>\bin export-cs.bat -p ..\conf\database.properties -i 491520 -f mydump.zip
```

3. Arrêtez le service HP Universal CMDB Configuration Manager.
4. Exécutez la commande suivante pour importer et activer le jeu de configurations précédent :

```
< HP Universal CMDB Configuration Manager>\bin\import-cs.bat <propriétés de base de données> <nom de fichier de vidage> --activate
```

**Problème**. La connexion UCMDB comporte une erreur.

**Solution**. La cause peut être l'une des suivantes :

- Le serveur UCMDB est arrêté. Redémarrez Configuration Manager une fois qu'UCMDB est entièrement activé (vérifiez que l'état du serveur UCMDB est **Activé**).
- Le serveur UCMDB est activé, mais les informations d'identification de la connexion à Configuration Manager ou l'URL sont erronées. Démarrez Configuration Manager. Allez dans Administration des serveurs, modifiez les paramètres de connexion d'UCMDB et enregistrez le nouveau jeu de configurations. Activez le jeu de configurations et redémarrez le serveur.

**Problème**. Les paramètres de connexion LDAP sont erronés.

**Solution**. Rétablissez le jeu de configurations précédent. Définissez les paramètres de connexion LDAP appropriés et activez le nouveau jeu de configurations.

**Problème**. Les modifications appliquées au modèle de classe UCMDB ne sont pas détectées dans Configuration Manager.

**Solution**. Redémarrez le serveur Configuration Manager.

**Problème**. Le journal Configuration Manager contient une erreur **UCMDB Délai d'exécution expiré**.

**Solution**. Cela se produit lorsque la base de données UCMDB est surchargée. Pour remédier à ce problème, augmentez le délai de connexion comme suit :

1. Créez un fichier jdbc.properties dans le dossier **UCMDBServer\conf**.
2. Entrez le texte suivant : QueryTimeout=<nombre de secondes>.
3. Redémarrez le serveur UCMDB.

**Problème**. Configuration Manager n'autorise pas l'ajout d'une vue à gérer.

**Solution**. Lorsqu'une vue est ajoutée pour être gérée, un nouveau TQL est créé dans UCMDB. Si la limite maximale des TQL actifs est atteinte, la vue ne peut pas être chargée. Augmentez la limite des TQL actifs dans UCMDB en modifiant les paramètres suivants dans le Gestionnaire des paramètres d'infrastructure :

- Nombre max de TQL actifs dans le serveur
- Nombre max d'objets dans les TQL actifs

**Problème**. Le certificat du serveur HTTPS n'est pas valide.

**Solution**. La cause peut être l'une des suivantes :

- La date de validation du certificat est obsolète. Vous devez obtenir un nouveau certificat.
- L'autorité de certification du certificat n'est pas une autorité approuvée. Ajoutez l'autorité de certification à votre liste Autorité de certification racine approuvée.

**Problème**. Lors de la connexion à partir de la page de connexion Configuration Manager, vous obtenez une erreur de connexion ou une page de refus d'accès.

**Solution**. La cause peut être l'une des suivantes :

- Le nom d'utilisateur n'est peut-être pas défini dans le fournisseur d'authentification (LDAP externe/partagé). Ajoutez l'utilisateur dans le système du fournisseur d'authentification.
- L'utilisateur est défini, mais ne dispose pas d'autorisation de connexion à Configuration Manager. Octroyez l'autorisation de connexion utilisateur. La meilleure pratique est d'attribuer une autorisation de connexion au groupe racine de tous les utilisateurs Configuration Manager.
- Ces solutions ne s'appliquent qu'en cas d'échec de la connexion provenant d'une connexion système IDM.

**Problème**. Le serveur Configuration Manager ne démarre pas en raison d'informations d'identification de base de données erronées.

**Solution**. Si vous modifiez les informations d'identification de base de données et que le serveur ne démarre pas, ces informations sont peut-être erronées. (**Remarque** : L'Assistant Post-Installation ne teste pas automatiquement les informations d'identification entrées. Vous devez cliquer sur le bouton **Test** de l'Assistant.) Vous devez chiffrer à nouveau le mot de passe de la base de données et entrer de nouvelles informations d'identification dans le fichier de configuration. Procédez comme suit :

1. Sur la ligne de commande, exécutez la commande suivante pour chiffrer le mot de passe de base de données mis à jour :

   <dossier d'installation Configuration Manager (CnC)>\bin\encrypt-password.bat –p <mot de passe>

   qui renvoie le mot de passe chiffré.

2. Copiez le mot de passe chiffré (notamment le préfixe {ENCRYPTED}), dans le paramètre **db.password** du <**dossier d'installation CnC**>**conf****database.properties**.

**Problème**. Si le DNS n'est pas correctement configuré, vous pouvez peut-être vous connecter à l'aide de l'adresse IP du serveur. Lors de la saisie de l'adresse IP, une seconde erreur DNS se produit.

**Solution**. Remplacez à nouveau le nom de l'ordinateur par l'adresse IP. Par exemple :

Si vous vous connectez à l'aide de l'adresse IP suivante :
http://16.55.245.240:8180/cnc/

et que vous obtenez une adresse contenant le nom de l'ordinateur indiquant une erreur DNS, telle que :
http://mon.exemple.com:8180/bsf/secure/authenicationPointURL.jsp...

remplacez-la par :
http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

et relancez l'application dans le navigateur.

**Problème**. Le serveur tomcat Configuration Manager ne démarre pas.

**Solution**. Essayez l'une des solutions suivantes :

- Exécutez l'Assistant Post-Installation et remplacez les ports du serveur Configuration Manager.
- Abandonnez l'autre procédure qui occupe les ports Configuration Manager.
- Modifiez manuellement les ports des fichiers de configuration Configuration Manager en éditant le fichier suivant : **<dossier d'installation CnC>\servers\server-0\conf\server.xml** et en mettant à jour les ports appropriés :
  - HTTP (8080) : ligne 69
  - HTTPS (8443) : lignes 71, 90

**Problème**. Le journal Configuration Manager contient une erreur d'insuffisance de données.

**Solution**. Augmentez la mémoire maximum Java selon les besoins.

Pour modifier la taille de mémoire dans le service Configuration Manager :

1. Allez dans le **<dossier d'installation CnC>\cnc\bin** et exécutez la commande suivante : edit-server-0.bat.
2. Sélectionnez l'onglet **Java**.

3 Mettez à jour les paramètres **Pool de mémoire initial** et **Pool de mémoire maximum**.

Pour modifier la taille de la mémoire dans le fichier de commandes :

1 Allez dans le **<dossier d'installation CnC>\cnc** et ouvrez le fichier **start-server-0.bat** pour le modifier.

2 Repérez la ligne commençant par **SET JAVA_OPTS=-Dcnc.home**.

3 Repérez les commandes **-Xms** et **-Xmx** et modifiez-les selon vos besoins :

```
-Xms<taille du pool de mémoire initial> -Xmx<taille du pool de mémoire maximum>
```

Par exemple : pour définir le pool de mémoire initial sur 100 Mo et le pool de mémoire maximum sur 800 Mo, entrez :

```
-Xms100m -Xmx800m
```

**Problème**. Il s'est déroulé un long délai pour que l'Assistant Post-installation réagisse après avoir cliqué **Terminer**.

**Solution**. Pour un système UCMDB non préconfiguré pour le mode consolidé, la consolidation du schéma peut être longue (dépend du volume de données). Attendez 15 minutes. Si aucune progression n'est détectée, abandonnez l'Assistant Post-Installation et relancez la procédure.

**Problème**. Les modifications apportées aux CI d'UCMDB ne sont pas reflétées dans Configuration Manager.

**Solution**. Configuration Manager exécute une procédure d'analyse asynchrone hors connexion. La procédure n'a peut-être pas encore traité les dernières modifications apportées à UCMDB. Pour résoudre ce problème, essayez l'une des solutions suivantes :

- Attendez quelques minutes. L'intervalle par défaut entre les exécutions de la procédure d'analyse est de 10 minutes. Il peut être configuré dans le module Administration des serveurs.
- Exécutez un appel JMX pour effectuer le calcul de l'analyse hors connexion sur la vue appropriée.

➤ Allez dans Administration des politiques. Cliquez sur le bouton **Recalculer l'analyse de la politique**. La procédure d'analyse hors connexion est appelée pour toutes les vues (peut prendre un certain temps). Vous pouvez également apporter une modification artificielle à une politique et la sauvegarder.

**Problème**. Lorsque vous cliquez sur **Administration** > **Ouvrir UCMDB**, la page de connexion UCMDB s'affiche.

**Solution**. Pour accéder à UCMDB sans vous reconnecter, vous devez activer la connexion unique. Pour plus d'informations, voir "Activer l'authentification LW-SSO (Lightweight Single Sign-On)", page 19. Par ailleurs, vérifiez que l'utilisateur Configuration Manager connecté est défini dans le système de gestion des utilisateurs UCMDB.

**Problème**. Lors de la configuration d'une connexion UCMDB dans l'Assistant Post-Installation vers une adresse IPv6, l'option de menu **Administration** > **Ouvrir UCMDB** ne fonctionne pas.

**Solution**. Procédez comme suit :

1. Allez dans **Administration** > **Administration des serveurs** > **Configuration Manager** > **Connexion UCMDB**.
2. Ajoutez des crochets à l'adresse IP dans l'URL d'accès UCMDB. L'URL doit avoir le format suivant : http://[x:x:x:x:x:x:x:x]:8080/.
3. Enregistrez le jeu de configurations et activez-le.
4. Redémarrez Configuration Manager.

Les limitations suivantes s'appliquent lorsque vous utilisez Configuration Manager :

➤ Chaque fois que l'heure est modifiée sur le serveur tomcat Configuration Manager, il doit être redémarré pour mettre à jour l'heure du serveur.

# 7

# Sécurisation renforcée

Contenu de ce chapitre :



## Sécurisation renforcée Configuration Manager

Cette section présente le concept d'une application de sécurisation Configuration Manager et décrit la planification et l'architecture requises pour implémenter la sécurité. Il est vivement recommandé de lire cette section avant de suivre la discussion sur la sécurisation renforcée dans les sections suivantes.

Configuration Manager a été conçu pour faire partie d'une architecture sécurisée, et peut par conséquent répondre au défi du traitement des menaces de sécurité auxquelles elle peut être exposée.

Les directives relatives à la sécurisation renforcée traitent la configuration requise pour implémenter une plus grande sécurité (renforcée) Configuration Manager.

Les informations relatives à la sécurisation renforcée fournies sont destinées principalement aux administrateurs Configuration Manager. Ceux-ci doivent se familiariser avec les paramètres et recommandations de sécurisation renforcée avant de commencer les procédures de sécurisation renforcée.

Voici les recommandations pour préparer la sécurisation renforcée de votre système :

- Évaluez le risque de sécurité/l'état de sécurité de l'ensemble de votre réseau, et basez-vous sur les conclusions pour effectuer le meilleur choix pour intégrer Configuration Manager dans votre réseau.
- Développez une bonne compréhension de l'infrastructure technique de Configuration Manager et des fonctionnalités de sécurité de Configuration Manager.
- Étudiez toutes les directives relatives à la sécurisation renforcée.
- Vérifiez que Configuration Manager est entièrement opérationnel avant de commencer les procédures de sécurisation renforcée.
- Suivez les procédures de sécurisation renforcée pas à pas, en suivant la chronologie de chaque section.

**Important :**

- Les procédures de sécurisation renforcée sont basées sur le fait que vous n'implémentez que les instructions fournies dans ces sections, et que vous n'exécutez pas d'autres étapes de sécurisation renforcée décrites ailleurs.
- Lorsque les procédures de sécurisation renforcées s'appliquent à une architecture distribuée spécifique, cela n'implique pas qu'il s'agit de la meilleure architecture qui réponde aux besoins de votre entreprise.
- Les procédures indiquées dans les sections suivantes doivent être exécutées sur des ordinateurs dédiés à Configuration Manager. L'utilisation de ces ordinateurs pour d'autres opérations en plus de Configuration Manager peut engendrer des résultats inattendus.
- Les informations de sécurisation renforcée fournies dans cette section ne doivent pas servir de guide pour évaluer les risques de sécurité de vos systèmes informatisés.

## Chiffrer le mot de passe de base de données

Le mot de passe de base de données est enregistré dans **<répertoire d'installation de Configuration Manager >\conf\database.properties**. Si vous souhaitez chiffrer le mot de passe, notre algorithme de chiffrement par défaut est compatible avec les normes FIPS 140-2. Pour chiffrer le mot de passe de base de données, cochez la case **Chiffrer le mot de passe** de la page Configuration de la base de données de l'assistant Post-installation de Configuration Manager.

Le chiffrement est réalisé à l'aide d'une clé, qui permet de chiffrer le mot de passe. La clé est ensuite chiffrée à l'aide d'une autre clé, appelée clé principale. Les deux clés sont chiffrées à l'aide du même algorithme. Pour plus d'informations sur les paramètres utilisés dans la procédure de chiffrement, voir "Paramètres de chiffrement", page 84.

---

**Attention :** Si vous modifiez l'algorithme de chiffrement, tous les mots de passe préalablement chiffrés ne sont plus utilisables.

---

**Pour modifier le chiffrement de votre mot de passe de base de données :**

1. Ouvrez <**Répertoire d'installation de Configuration Manager** >**conf****encryption.properties** et modifiez les fichiers suivants :
   - **engineName.** Entrez le nom de l'algorithme de chiffrement.
   - **keySize.** Entrez la taille de la clé principale de l'algorithme sélectionné.
2. Exécutez le script **generate-keys.bat**, qui crée le répertoire suivant : **cnc****security****encrypt_repository** et génère la clé de chiffrement.
3. Réexécutez l'Assistant Post-installation.

## Activer SSL sur l'ordinateur serveur à l'aide d'un certificat auto-signé

Ces sections expliquent comment configurer Configuration Manager pour prendre en charge l'authentification et le chiffrement à l'aide du canal SSL (Secure Sockets Layer).

Configuration Manager utilise Tomcat 6.0 comme serveur d'applications.

---

**Remarque :** Tous les emplacements de répertoire et de fichier dépendent de votre plate-forme, du système d'exploitation et de vos préférences d'installation.

---

### 1 Conditions préalables

Avant de lancer la procédure suivante, supprimez l'ancien fichier **tomcat.keystore** situé dans <**répertoire d'installation Configuration Manager** >**java****lib****security****tomcat.keystore**.

## 2 Générer un Keystore de serveur

Créez un keystore (type JKS) à l'aide d'un certificat auto-signé et d'une clé privée correspondante :

➤ À partir du répertoire bin de l'installation Java du <**répertoire d'installation de Configuration Manager** >, exécutez la commande suivante :

```
keytool -genkey -alias tomcat -keyalg RSA -keystore
..\lib\security\tomcat.keystore
```

La boîte de dialogue Console s'affiche.

➤ Entrez le mot de passe keystore. S'il a été modifié, changez-le manuellement dans le fichier.

➤ Répondez à la question, **Quels sont vos nom et prénom ?** Entrez le nom du serveur Web Configuration Manager. Entrez les autres paramètres inhérents à votre entreprise.

➤ Entrez le mot de passe de la clé. Il DOIT être identique au mot de passe keystore.

Un keystore JKS est créé sous le nom **tomcat.keystore** avec un certificat de serveur appelé **hpcert**.

## 3 Placer le certificat dans le magasin de données de confiance du client

Après la génération de **tomcat.keystore** et l'exportation du certificat du serveur, pour chaque client devant communiquer avec Configuration Manager par le biais de SSL à l'aide de ce certificat auto-signé, placez ce certificat dans les magasins de confiance du client.

---

**Limitation** : **tomcat.keystore** ne peut contenir qu'un seul certificat de serveur.

---

### 4 Vérifier les paramètres de configuration du client

Ouvrez le fichier **client-config.properties**, situé dans le répertoire **conf** du <**répertoire d'installation Configuration Manager**>. Définissez le protocole sur **https** et le port sur **8443**.

### 5 Modifier le fichier server.xml

Ouvrez le fichier **server.xml**, situé dans le répertoire **conf** du <**répertoire d'installation Configuration Manager** >. Localisez la section commençant par

Connector port="8443"

qui apparaît sous forme de commentaires. Activez le script en supprimant le caractère de commentaire et ajoutez les deux lignes suivantes :

keystoreFile="<tomcat.keystore file location>" (voir l'étape 2 à la page 77)

keystorePass="<password>"

### 6 Redémarrer le serveur

### 7 Vérifier la sécurité du serveur

Pour vérifier que le serveur Configuration Manager est sécurisé, entrez l'URL suivante dans le navigateur Web : **https://<Nom du serveur ou adresse IP Configuration Manager>:8443/cnc**.

---

**Conseil :** Si vous n'arrivez pas à vous connecter, utilisez un autre navigateur ou passez à une version plus récente du navigateur.

---

# Activer SSL sur l'ordinateur serveur à l'aide d'un certificat d'une autorité de certification

Pour utiliser un certificat émis pour une autorité de certification, keystore doit être au format Java. L'exemple suivant explique comment formater le keystore pour un ordinateur Windows.

## 1 Conditions préalables

Avant de lancer la procédure suivante, supprimez l'ancien fichier **tomcat.keystore** situé dans le **<répertoire d'installation Configuration Manager>\java\lib\security\tomcat.keystore**.

## 2 Générer un Keystore de serveur

**a** Générez un certificat signé par une autorité de certification et installez-le sous Windows.

**b** Exportez le certificat dans un fichier ***.pfx** (y compris les clés privées) à l'aide de Microsoft Management Console (**mmc.exe**).

➤ Entrez une chaîne comme mot de passe pour le fichier **pfx**. (Ce mot de passe vous est demandé lors de la conversion du type de keystore en un keystore JAVA.)
Le fichier **.pfx** contient un certificat public et une clé privée et il est protégé par un mot de passe.

**c** Copiez le fichier **.pfx** que vous avez créé dans le dossier suivant : **<Répertoire d'installation Configuration Manager>\java\lib\security**.

**d** Ouvrez l'invite de commande et remplacez le répertoire par le **<répertoire d'installation Configuration Manager>\bin\jre\bin**.

➤ Remplacez le type de keystore **PKCS12** par un keystore **JAVA** en exécutant la commande suivante :

```
keytool -importkeystore -srckeystore <répertoire d'installation Configuration Manager >\conf\security\<nom de fichier pfx> -srcstoretype PKCS12 -destkeystore tomcat.keystore
```

Le mot de passe du keystore source (**.pfx**) vous est demandé. Il s'agit du mot de passe que vous avez fourni lors de la création du fichier pfx à l'étape b.

### 3 Vérifier les paramètres de configuration du client

Ouvrez le fichier suivant : <**répertoire d'installation Configuration Manager**>**\cnc\conf\client-config.properties** et vérifiez que la propriété **bsf.server.url** est définie sur **https** et le port sur **8443**.

### 4 Modifier le fichier server.xml

Ouvrez le fichier suivant : <**Répertoire d'installation Configuration Manager**>**\conf\server.xml**. Localisez la section commençant par

```
Connector port="8443"
```

qui apparaît sous forme de commentaires. Activez le script en supprimant le caractère de commentaire et ajoutez les deux lignes suivantes :

```
keystoreFile="../../java/lib/security/tomcat.keystore"
keystorePass="password" />
```

### 5 Redémarrer le serveur

### 6 Vérifier la sécurité du serveur

Pour vérifier que le serveur Configuration Manager est sécurisé, entrez l'URL suivante dans le navigateur Web : **https://<Nom du serveur ou adresse IP Configuration Manager>:8443/cnc**.

---

**Limitation** : **tomcat.keystore** ne peut contenir qu'un seul certificat de serveur.

---

# Activer SSL à l'aide d'un certificat client

Si le certificat utilisé par le serveur Web de Configuration Manager est émis par une autorité de certification bien connue, il est fort probable que votre serveur Web valide le certificat sans action supplémentaire.

Si l'autorité de certification n'est pas approuvée par le magasin d'approbations du serveur, importez le certificat CA dans ce magasin.

L'exemple suivant démontre comment importer le certificat auto-signé **hpcert** dans le magasin d'approbations du serveur (cacerts).

**Pour importer un certificat dans le magasin d'approbations du serveur :**

1. Sur l'ordinateur client, localisez et renommez le certificat **hpcert** en **hpcert.cer**.

   Dans l'Explorateur Windows, l'icône indique que le fichier est un certificat de sécurité.

2. Double-cliquez sur **hpcert.cer** pour ouvrir la boîte de dialogue Certificat Internet Explorer et importer le fichier.

3. Sur l'ordinateur serveur, importez le certificat d'Autorité de certification dans le magasin d'approbations (cacerts) à l'aide de l'utilitaire keytool avec la commande suivante :

   ```
   keytool.exe -import -alias hp -file hp.cer -keystore ..\lib\security\cacerts
   ```

4. Modifiez le fichier.xml du serveur comme suit :

   a. Appliquez les modifications décrites à l'étape 5 à la page 78.

   b. Ensuite, ajoutez les lignes suivantes :

   ```
   truststoreFile="../../java/lib/security/cacerts"

   truststorePass="changeit" />
   ```

   c. Définissez clientAuth="true".

5. Vérifiez la sécurité du serveur comme indiqué à l'étape 7 à la page 78.

# Activer SSL pour l'authentification uniquement

Cette tâche décrit comment configurer Configuration Manager pour prendre en charge l'authentification uniquement. Il s'agit du niveau minimum de sécurité requis pour utiliser Configuration Manager.

**Pour activer SSL pour l'authentification :**

1. Suivez l'une des procédures d'activation de SSL sur l'ordinateur serveur comme indiqué dans "Activer SSL sur l'ordinateur serveur à l'aide d'un certificat auto-signé", page 76 jusqu'à l'étape 6 à la page 78 ou "Activer SSL sur l'ordinateur serveur à l'aide d'un certificat d'une autorité de certification", page 79 jusqu'à l'étape 5 à la page 80.
2. Entrez l'URL suivante dans le navigateur Web : **http://<Configuration Manager Nom du serveur ou adresse IP >:8080/cnc**.

# Activer l'authentification de certificat client

Cette tâche décrit comment configurer Configuration Manager pour accepter l'authentification de certificat côté client.

**Pour activer l'authentification de certificat client :**

1. Suivez la procédure pour activer SSL sur l'ordinateur serveur comme indiqué dans "Activer SSL sur l'ordinateur serveur à l'aide d'un certificat auto-signé", page 76.
2. Ouvrez le fichier suivant : **<Répertoire d'installation Configuration Manager >\conf\lwssofmconf.xml.** Localisez la section commençant par in-client certificate. Par exemple :

   ```
   <in-clientCertificate userIdentifierRetrieveField="SubjectDN"
   userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="e" />
   ```

   Activez la fonctionnalité de certificat client en supprimant le caractère de commentaire.
3. Extrayez le nom d'utilisateur du certificat en procédant comme suit :
   a. Le paramètre **userIdentifierRetrieveField** indique le champ de certificat qui contient le nom d'utilisateur. Les options sont les suivantes :
      - **SubjectDN**
      - **SubjectAlternativeName**

**b** Le paramètre **userIdentifierRetrieveMode** indique si le nom d'utilisateur correspond au contenu du champ approprié ou seulement une partie de ce champ. Les options sont les suivantes :

- **EntireField**
- **FieldPart**

**c** Si la valeur de **userIdentifierRetrieveMode** est **FieldPart**, le paramètre **userIdentifierRetrieveFieldPart** indique la partie du champ approprié correspondant au nom d'utilisateur. La valeur est une lettre de code basée sur la légende définie dans le certificat.

**4** Ouvrez le fichier suivant : **<Répertoire d'installation Configuration Manager>\conf\client-config.properties** et modifiez les propriétés suivantes :

- Modifiez **bsf.server.url** pour utiliser le protocole HTTPS et remplacez le port HTTPS par le port décrit dans "Activer SSL sur l'ordinateur serveur à l'aide d'un certificat auto-signé", page 76.
- Modifiez **bsf.server.services.url** pour utiliser le protocole HTTP et remplacez le port par le port HTTP original.

# Paramètres de chiffrement

Le tableau ci-dessous contient les paramètres inclus dans le fichier **encryption.properties** utilisé pour le chiffrement de mot de passe de base de données. Pour plus d'informations sur le chiffrement du mot de passe de base de données, voir "Chiffrer le mot de passe de base de données", page 75.

| Paramètre | Description |
|---|---|
| cryptoSource | Indiquer l'infrastructure d'implémentation de l'algorithme de chiffrement. Les options sont les suivantes :<br>➤ **lw.** Uses Bouncy Castle lightweight implementation (Option par défaut)<br>➤ **jce.** Java Cryptography Enhancement (infrastructure de chiffrement Java standard) |
| storageType | Indiquer le type de stockage de clé.<br>Actuellement, seul le **fichier binaire** est pris en charge. |
| binaryFileStorageName | Indiquer l'emplacement du fichier dans lequel la clé principale est stockée. |
| cipherType | Type de chiffrement. Actuellement, seul **symmetricBlockCipher** est pris en charge. |
| engineName | Nom de l'algorithme de chiffrement.<br>Les options suivantes sont disponibles :<br>➤ **AES.** American Encryption Standard. Ce chiffrement est compatible FIPS 140-2. (Option par défaut)<br>➤ **Blowfish**<br>➤ **DES**<br>➤ **3DES.** (Compatible FIPS 140-2)<br>➤ **Null**. Aucun chiffrement |

| Paramètre | Description |
|---|---|
| keySize | Taille de la clé principale. Elle est déterminée par l'algorithme :<br>➤ **AES.** 128, 192 ou 256 (Option par défaut 256)<br>➤ **Blowfish** 0-400<br>➤ **DES** 56<br>➤ **3DES.** 156 |
| encodingMode | Codage ASCII des résultats du chiffrement binaire.<br>Les options suivantes sont disponibles :<br>➤ **Base64** (Option par défaut)<br>➤ **Base64Url**<br>➤ **Hex** |
| algorithmModeName | Mode de l'algorithme. Actuellement, seul **CBC** est pris en charge. |
| algorithmPaddingName | Algorithme de remplissage utilisé.<br>Les options suivantes sont disponibles :<br>➤ **PKCS7Padding** (Option par défaut)<br>➤ **PKCS5Padding** |
| jceProviderName | Nom de l'algorithme de chiffrement JCE.<br>**Remarque :** Ne s'applique que si crytpSource est **jce**. Pour **lw**, engineName est utilisé. |