

Comment vérifier si la connexion de votre client ODBC/JDBC à CIS est chiffré ?

Contenu

[Introduction](#)

[Comment vérifier si la connexion de votre client ODBC/JDBC à CIS est chiffré ?](#)

Introduction

Ce document décrit comment vérifier si la connexion de votre ODBC/Java de base de données client de la Connectivité (JDBC) au serveur d'informations de Cisco (CIS) est chiffrée ?

Comment vérifier si la connexion de votre client ODBC/JDBC à CIS est chiffré ?

Si vous avez choisi de placer votre DSN ou URL JDBC avec un mode de chiffrement pour votre outil de client, vous pouvez facilement vérifier la connexion cryptée.

Au moment du mode de chiffrement, la connexion utilise le port SSL ODBC/JDBC (port de base +3 de HTTP) et additionne +2 au port d'auditeur du par défaut ODBC/JDBC (base +1).

Il n'y a aucun besoin de spécifier (base+3) le port SSL vous-même dans le DSN ou l'URL.

Vérifiez l'utilisation du port SSL :

1. Désactivez temporairement le mode de libellé cette activation de contrôles du port décrypté (port de base +1).
 - a. Dans l'interface utilisateur de la configuration du studio (UI), naviguez vers ce chemin : **Serveur > pilotes client > transmissions > libellé activé** (sur la reprise de serveur)
 - b. Changez ceci à « faux » et redémarrez le serveur pour lui pour le prendre effet.
2. Connectez à CIS à une connexion décryptée. Il devrait échouer maintenant puisque l'auditeur non-SSL est inactif maintenant.
3. Connectez à CIS à votre connexion cryptée et si réussi, puis vous êtes connecté au-dessus du port SSL (port de base +3).