

Como verificar se a conexão do seu cliente ODBC/JDBC aos CI é cifrado?

Índice

[Introdução](#)

[Como verificar se a conexão do seu cliente ODBC/JDBC aos CI é cifrado?](#)

Introdução

Este documento descreve como verificar se a conexão do seu cliente da conectividade de base de dados ODBC/Java (JDBC) ao server de informação de Cisco (CI) está cifrada?

Como verificar se a conexão do seu cliente ODBC/JDBC aos CI é cifrado?

Se você optou para ajustar seu DSN ou JDBC URL com um modo de criptografia para sua ferramenta do cliente, você pode facilmente verificar a conexão criptografada.

Na altura do modo de criptografia, a conexão usa a porta ODBC/JDBC SSL (porta baixa +3 HTTP) e adiciona +2 à porta do ouvinte do padrão ODBC/JDBC (base +1).

Não há nenhuma necessidade de especificar (base+3) a porta você mesmo SSL no DSN ou na URL.

Verifique o uso da porta SSL:

1. Desabilite temporariamente o modo do texto não criptografado essa habilitação dos controles da porta UNencrypted (porta baixa +1).
 - a. Na interface do utilizador da configuração do estúdio (UI), navegue a este trajeto: **Server > driveres de cliente > comunicações > texto não criptografado permitido** (no reinício do server)
 - b. Mude isto a “falso” e reinicie o server para que tome o efeito.
2. Conecte aos CI com uma conexão UNencrypted. Deve falhar agora desde que o ouvinte NON-SSL é inativo agora.
3. Conecte aos CI com sua conexão criptografada e se bem sucedido, a seguir você é conectado sobre a porta SSL (porta baixa +3).