

Procedura per abilitare il supporto TLS 1.2 per i servizi Web CVP Call Studio

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Riepilogo del problema](#)

[Possibili cause](#)

[Azione consigliata](#)

Introduzione

Questo documento descrive come abilitare il supporto TLS 1.2 per i servizi Web Cisco Customer Voice Portal (CVP) Call Studio.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CVP Call Studio
- TLS (Transport Layer Security)
- Java Runtime Environment (JRE)

Le informazioni di questo documento si basano sulle seguenti versioni software:

- CVP Server 11.5
- CVP Call Studio 11.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Riepilogo del problema

In Call Studio Web Service Element, TLS 1.0 viene negoziato anche se il server del servizio Web supporta TLS1.2.

Possibili cause

JRE 7 utilizza TLS1.0 per impostazione predefinita.

Azione consigliata

Installare la patch CVP 10.5 - ES24 (deprecata) e ES26, CVP 11.0 - ES23, CVP 11.5 - ES7 per Unified CVP release 10.5, 11.0 e 11.5 rispettivamente.

Questa patch forza Java a impostare il contesto per TLS 1.2, quindi tutte le richieste https in uscita da CVP utilizzeranno TLS 1.2.

Nota: Il difetto [CSCvc39129](#) è stato aperto per il problema.