Procedure to Enable TLS 1.2 Support for CVP Call Studio Web Services

Contents

Introduction

This document describes how to to enable TLS 1.2 support for Cisco Customer Voice Portal (CVP) Call Studio Web Services.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

The information in this document is based on these software versions:

- CVP Server 11.5
- CVP Call Studio 11.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem Summary

In Call Studio Web Service Element, TLS 1.0 is negotiated even if Web Service Server supports TLS1.2.

Possible Causes

JRE 7 uses TLS1.0 by default.

Recomended Action

Install patch CVP 10.5 – ES24 (deprecated) and ES26, CVP 11.0 – ES23, CVP 11.5 – ES7 for Unified CVP Release 10.5, 11.0 and 11.5 respectively.

This patch forces Java to set the context for TLS 1.2, so all outgoing https requests from CVP will use TLS 1.2.

Note: This defect CSCvc39129was opened for the issue.