CVP Call Studio 웹 서비스에 대해 TLS 1.2 지원을 활성화하는 절차

목차

소개

이 문서에서는 Cisco CVP(Customer Voice Portal) Call Studio 웹 서비스에 대해 TLS 1.2 지원을 활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- CVP 서버 11.5
- CVP Call Studio 11.5

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제 요약

Call Studio 웹 서비스 요소에서 TLS 1.0은 웹 서비스 서버에서 TLS1.2를 지원하는 경우에도 협상됩니다.

가능한 원인

JRE 7은 기본적으로 TLS1.0을 사용합니다.

권장 조치

Unified CVP 릴리스 10.5, 11.0 및 11.5용 패치 CVP 10.5 - ES24(더 이상 사용되지 않음) 및 ES26, CVP 11.0 - ES23, CVP 11.5 - ES7을 각각 설치합니다.

이 패치는 Java가 TLS 1.2에 대한 컨텍스트를 설정하도록 강제하므로 CVP의 모든 발신 https 요청은 TLS 1.2를 사용합니다.

참고: 이 결함 CSCvc39129는 이슈를 위해 열렸습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.