UCCX 솔루션 인증서 관리 가이드

목차

소개

이 문서에서는 자체 서명 및 서명된 인증서를 사용하도록 Cisco Unified Contact Center Express(UCCX)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 설명된 구성 단계를 진행하기 전에 다음 응용 프로그램에 대한 OS 관리 페이지에 액세스할 수 있는지 확인하십시오.

- UCCX
- 소셜 마이너
- 미디어센스

관리자는 에이전트 및 수퍼바이저 클라이언트 PC의 인증서 저장소에 액세스할 수 있어야 합니다.

FQDN, DNS 및 도메인

UCCX 컨피그레이션의 모든 서버는 DNS(Domain Name System) 서버 및 도메인 이름과 함께 설치해야 합니다. 또한 에이전트, 수퍼바이저 및 관리자가 FQDN(Fully Qualified Domain Name)을 통해 UCCX 구성 애플리케이션에 액세스해야 합니다.

UCCX 버전 10.0+를 사용하려면 설치 시 도메인 이름 및 DNS 서버를 채워야 합니다. UCCX 버전 10.0+ 설치 프로그램에서 생성되는 인증서에는 FQDN이 적절하게 포함되어 있습니다. UCCX 버전 10.0+로 업그레이드하기 전에 UCCX 클러스터에 DNS 서버와 도메인을 추가합니다.

도메인이 변경되거나 처음으로 채워지면 인증서가 재생성되어야 합니다. 서버 컨피그레이션에 도메인 이름을 추가한 후 Tomcat 인증서를 다른 애플리케이션, 클라이언트 브라우저 또는 서명을 위한 CSR(Certificate Signing Request) 생성 시 설치하기 전에 모든 Tomcat 인증서를 재생성합니다.

사용되는 구성 요소

이 문서에서 설명하는 정보는 다음 하드웨어 및 소프트웨어 구성 요소를 기반으로 합니다.

- UCCX 웹 서비스
- UCCX 알림 서비스
- UCCX 플랫폼 Tomcat
- Cisco Finesse Tomcat
- Cisco CUIC(Unified Intelligence Center) Tomcat
- 소셜마이너 톰캣
- MediaSense 웹 서비스

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

배경 정보

공동 상주 Finesse와 CUIC의 도입, 이메일 및 채팅을 위한 UCCX와 SocialMiner의 통합, Finesse를 통해 인증서를 기록, 파악 및 설치하기 위한 MediaSense의 사용으로 인해 이제 인증서 문제를 해결

할 수 있는 역량이 매우 중요해졌습니다.

이 문서에서는 UCCX 컨피그레이션 환경에서 자체 서명 인증서와 서명 인증서를 사용하는 방법에 대해 설명합니다.

- UCCX 알림 서비스
- UCCX 웹 서비스
- UCCX 스크립트
- 공동 상주 Finesse
- 공동 상주 CUIC(라이브 데이터 및 내역 보고)
- MediaSense(Finesse 기반 녹음 및 태깅)
- SocialMiner(채팅)

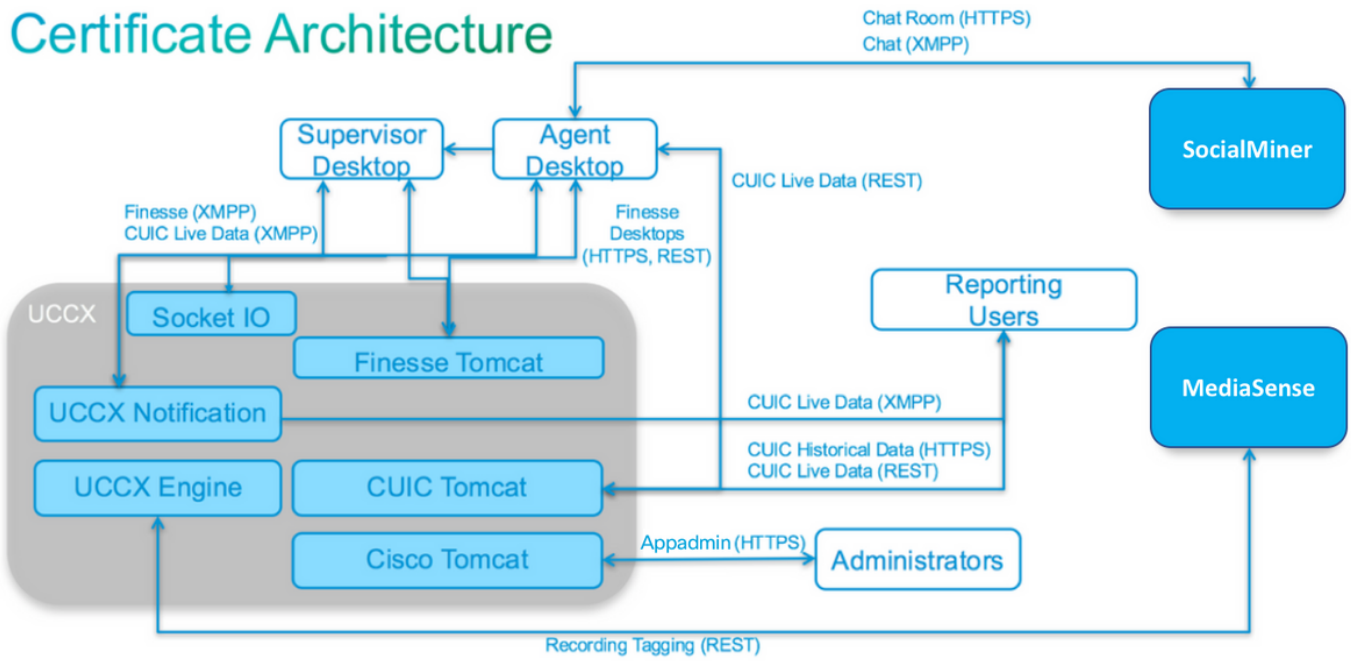
서명 또는 자체 서명된 인증서는 UCCX 구성의 애플리케이션(서버) 및 에이전트 및 수퍼바이저 클라이언트 데스크톱 모두에 설치해야 합니다.

UCOS(Unified Communications Operating System) 10.5에서는 클러스터의 각 노드에 대해 개별 인증서를 서명할 필요 없이 클러스터에 대해 단일 CSR을 생성할 수 있도록 다중 서버 인증서가 추가되었습니다. 이 인증서 유형은 UCCX, MediaSense 및 SocialMiner에서 명시적으로 지원되지 않습니다.

구성

이 섹션에서는 자체 서명 및 서명 인증서를 사용하도록 UCCX를 구성하는 방법에 대해 설명합니다.

구성 다이어그램



UCCX 솔루션 아키텍처는 UCCX 11.0부터 유효합니다. HTTPS 통신 다이어그램.

서명된 인증서

UCCX 컨피그레이션의 권장 인증서 관리 방법은 서명된 인증서를 활용하는 것입니다. 이러한 인증

서는 내부 CA(Certificate Authority) 또는 잘 알려진 서드파티 CA에서 서명할 수 있습니다.

Mozilla Firefox 및 Internet Explorer와 같은 주요 브라우저에서는 잘 알려진 서드파티 CA의 루트 인증서가 기본적으로 설치됩니다. 이러한 CA가 서명한 UCCX 컨피그레이션 애플리케이션의 인증서는 기본적으로 신뢰됩니다. 인증서 체인이 브라우저에 이미 설치된 루트 인증서로 끝나기 때문입니다.

내부 CA의 루트 인증서는 그룹 정책 또는 기타 현재 컨피그레이션을 통해 클라이언트 브라우저에 미리 설치될 수도 있습니다.

잘 알려진 서드파티 CA에서 서명한 UCCX 컨피그레이션 애플리케이션 인증서를 사용할지 또는 클라이언트 브라우저에서 CA에 대한 루트 인증서의 사용 가능 여부 및 사전 설치를 기반으로 내부 CA에서 서명한 인증서를 사용할지를 선택할 수 있습니다.

서명된 Tomcat 애플리케이션 인증서 설치

UCCX 게시자 및 가입자, SocialMiner, MediaSense 게시자 및 가입자 관리 애플리케이션의 각 노드에 대해 다음 단계를 완료합니다.

1. **OS Administration(OS 관리)** 페이지로 이동하고 **Security(보안) > Certificate Management(인증서 관리)를** 선택합니다.
2. Generate CSR(**CSR 생성)**을 클릭합니다.
3. Certificate **List** 드롭다운 **목록**에서 인증서 이름으로 **tomcat**을 선택하고 Generate CSR**을 클릭합니다**.
4. **Security(보안) > Certificate Management(인증서 관리)로** 이동하고 Download CSR(CSR **다운로드)을 선택합니다**.
5. 팝업 창의 드롭다운 목록에서 **tomcat**을 선택하고 **Download CSR**(CSR 다운로드)을 **클릭합니다**.

앞서 설명한 대로 새 CSR을 서드파티 CA에 보내거나 내부 CA로 서명합니다. 이 프로세스에서는 다음과 같은 서명된 인증서를 생성해야 합니다.

- CA의 루트 인증서
- UCCX 게시자 애플리케이션 인증서
- UCCX 가입자 애플리케이션 인증서
- SocialMiner 애플리케이션 인증서
- MediaSense 게시자 응용 프로그램 인증서
- MediaSense 구독자 응용 프로그램 인증서

참고: Distribution(**배포**) 필드를 서버의 FQDN으로 CSR에 둡니다.

참고: "다중 서버(SAN)" 인증서는 11.6 릴리스부터 UCCX에서 지원됩니다. 그러나 SAN에는 UCCX 노드-1 및 노드-2만 포함되어야 합니다. SocialMiner와 같은 다른 서버는 UCCX의 SAN에 포함되지 않아야 합니다.

참고: UCCX는 1024비트 및 2048비트의 인증서 키 길이만 지원합니다.

루트 인증서 및 애플리케이션 인증서를 노드에 업로드하려면 각 애플리케이션 서버에서 다음 단계를 완료합니다.

참고: 게시자(UCCX 또는 MediaSense)에 루트 및 중간 인증서를 업로드하는 경우 자동으로 가입자에게 복제되어야 합니다. 모든 애플리케이션 인증서가 동일한 인증서 체인을 통해 서명된 경우 컨피그레이션에서 루트 또는 중간 인증서를 게시자가 아닌 다른 서버에 업로드할 필요가 없습니다.

1. **OS Administration(OS 관리)** 페이지로 이동하고 **Security(보안) > Certificate Management(인증서 관리)를** 선택합니다.
2. Upload **Certificate(인증서 업로드)**를 클릭합니다.
3. 루트 인증서를 업로드하고 인증서 유형으로 **tomcat-**trust를 선택합니다.
4. Upload **File(파일 업로드)**을 클릭합니다.
5. Upload **Certificate(인증서 업로드)**를 클릭합니다.
6. 애플리케이션 인증서를 업로드하고 인증서 **유형**으로 tomcat을 선택합니다.
7. Upload **File(파일 업로드)**을 클릭합니다. **참고:** 하위 CA가 인증서에 서명하면 루트 인증서 대신 하위 CA의 루트 *인증서를* tomcat-*trust* 인증서로 업로드합니다. 중간 인증서가 발행된 경우 이 인증서를 애플리케이션 *인증서*와 함께 tomcat-*trust* 저장소에 업로드합니다.
8. 완료되면 다음 애플리케이션을 다시 시작합니다. Cisco MediaSense 게시자 및 가입자Cisco SocialMinerCisco UCCX 게시자 및 가입자

   참고: UCCX, MediaSense 및 SocialMiner 11.5 이상을 사용하는 경우 tomcat-ECDSA라는 새 인증서가 있습니다. 서명된 tomcat-ECDSA 인증서를 서버에 업로드하는 경우 애플리케이션 인증서를 tomcat 인증서가 아닌 tomcat-ECDSA 인증서로 업로드합니다. ECDSA에 대한 자세한 내용은 ECDSA 인증서를 이해하고 구성하는 링크에 대한 관련 정보 섹션을 참조하십시오.

자체 서명 인증서

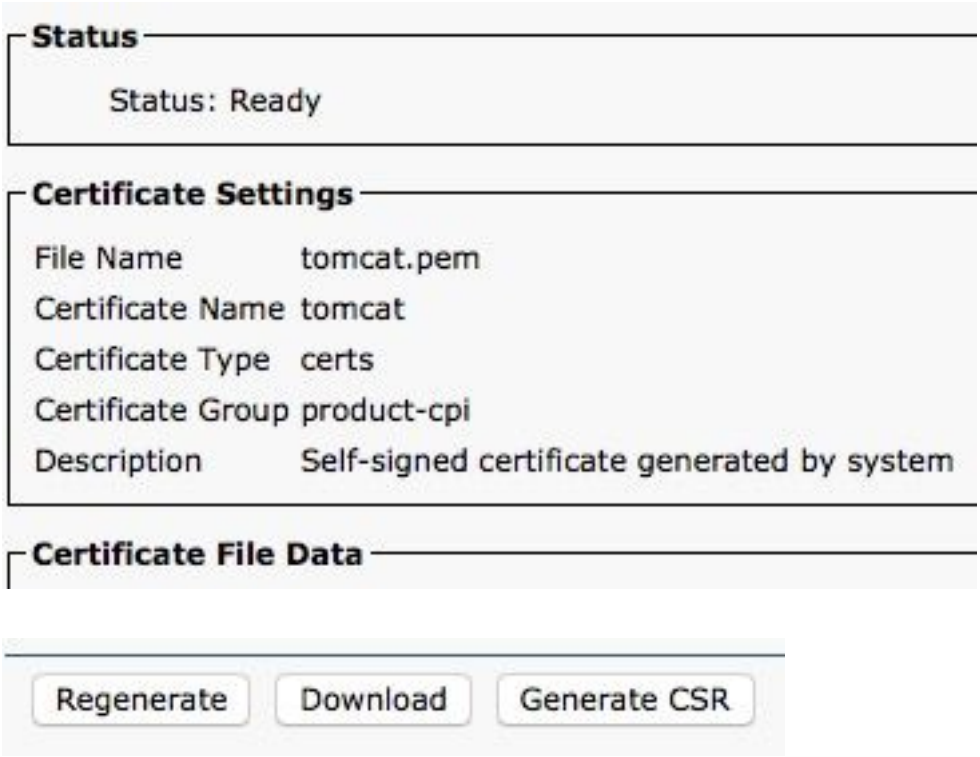
주변 장치 서버에 설치

UCCX 컨피그레이션에서 사용되는 모든 인증서는 컨피그레이션 애플리케이션에 사전 설치되어 자체 서명됩니다. 이러한 자체 서명 인증서는 클라이언트 브라우저 또는 다른 컨피그레이션 애플리케이션에 제공될 때 암시적으로 신뢰되지 않습니다. UCCX 컨피그레이션의 모든 인증서를 서명하는 것이 좋지만 사전 설치된 자체 서명 인증서를 사용할 수 있습니다.

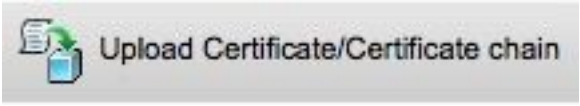
각 애플리케이션 관계에 대해 적절한 인증서를 다운로드하고 애플리케이션에 업로드해야 합니다. 인증서를 가져오고 업로드하려면 다음 단계를 완료합니다.

1. 애플리케이션 **OS 관리** 페이지**에 액세스** 하고 **보안 > 인증서 관리를 선택 합니다**.

2. 적절한 certificate**.pem** 파일을 클릭하고 Download(다운로드)를 **선택합니다**.



3. 적절한 애플리케이션에 인증서를 업로드하려면 **OS Administration(OS 관리)** 페이지로 이동하여 **Security(보안) > Certificate Management(인증서 관리)를** 선택합니다.
4. Upload **Certificate / Certificate Chain(인증서/인증서 체인 업로드)을 클릭합니다.**



5. 완료되면 다음 서버를 다시 시작합니다.

Cisco MediaSense 게시자 및 가입자Cisco SocialMinerCisco UCCX 게시자 및 가입자 클라이언트 컴퓨터에 자체 서명 인증서를 설치하려면 그룹 정책 또는 패키지 관리자를 사용하거나 각 에이전트 PC의 브라우저에서 개별적으로 설치하십시오.

Internet Explorer의 경우 클라이언트 측 자체 서명 인증서를 신뢰할 수 있는 루트 인증 기관 **저장소에** 설치합니다.

Mozilla Firefox의 경우 다음 단계를 완료합니다.

1. **도구 > 옵션**으로 **이동합니다**.
2. **Advanced(고급) 탭**을 클릭합니다.
3. View Certificates(**인증서 보기)를 클릭합니다**.
4. Servers(서버) **탭**으로 이동합니다.
5. Add Exception(**예외 추가)을 클릭합니다**.

자체 서명 인증서 재생성

자체 서명 인증서가 만료되는 경우 인증서를 다시 생성해야 하며 주변 장치 서버에 **설치**의 구성 단계**를** 다시 수행해야 합니다.

1. 애플리케이션 액세스 **OS 관리** 페이지 및 선택 **보안 > 인증서 관리**.

2. 적절한 인증서를 클릭하고 재생성을 **선택합니다**.
3. 인증서가 다시 생성된 서버를 다시 시작해야 합니다.
4. 각 애플리케이션 관계에 대해 적절한 인증서를 다운로드하고 주변 장치 서버에 설치의 컨피그레이션 단계에 따라 **애플리케이션에 업로드해야 합니다.**

통합 및 클라이언트 구성

UCCX-MediaSense

UCCX는 두 가지 목적으로 MediaSense 웹 서비스 REST API(Application Programming Interface)를 사용합니다.

- CUCM(Cisco Unified Communications Manager)에서 호출되는 새 녹음/녹화의 알림을 구독하려면 다음을 수행합니다.
- UCCX 상담원의 녹음 내용을 상담원 및 CSQ(연결 서비스 대기열) 정보와 태깅하려면

UCCX는 MediaSense 관리 노드에서 REST API를 사용합니다. MediaSense 클러스터에는 최대 2개가 있습니다. UCCX는 REST API를 통해 MediaSense 확장 노드에 연결되지 않습니다. 두 UCCX 노드 모두 MediaSense REST API를 사용해야 하므로 두 UCCX 노드에 두 MediaSense Tomcat 인증서를 설치합니다.

MediaSense 서버의 서명 또는 자체 서명 인증서 체인을 UCCX tomcat-*trust 키 저장소에* 업로드합니다.

MediaSense-to-Finesse

MediaSense는 Finesse에서 MediaSense Search and Play 가젯의 에이전트를 인증하기 위해 Finesse 웹 서비스 REST API를 사용합니다.

Search and Play 가젯용 Finesse XML 레이아웃에 구성된 MediaSense 서버는 Finesse REST API를 사용해야 하므로 해당 MediaSense 노드에 UCCX Tomcat 인증서 2개를 설치합니다.

UCCX 서버의 서명 또는 자체 서명 인증서 체인을 MediaSense tomcat-*trust 키 저장소에* 업로드합니다.

UCCX-소셜 마이너

UCCX는 이메일 연락처 및 컨피그레이션을 관리하기 위해 SocialMiner REST 및 Notification API를 사용합니다. 두 UCCX 노드 모두 SocialMiner REST API를 사용하고 SocialMiner 알림 서비스에서 알림을 받아야 하므로 두 UCCX 노드 모두에 SocialMiner Tomcat 인증서를 설치합니다.

SocialMiner 서버의 서명 또는 자체 서명 인증서 체인을 UCCX tomcat-*trust 키 저장소에* 업로드합니다.

UCCX AppAdmin 클라이언트 인증서

UCCX AppAdmin 클라이언트 인증서는 UCCX 시스템의 관리에 사용됩니다. UCCX 관리자용 UCCX AppAdmin 인증서를 설치하려면 클라이언트 PC에서 각 UCCX 노드의 https:// **<UCCX FQDN>/appadmin/main**으로 이동하여 브라우저를 통해 인증서를 설치합니다.

UCCX 플랫폼 클라이언트 인증서

UCCX 웹 서비스는 클라이언트 브라우저에 채팅 연락처를 전달하는 데 사용됩니다. UCCX 에이전트 및 수퍼바이저용 UCCX 플랫폼 인증서를 설치하려면 클라이언트 PC에서 각 UCCX 노드의 https:// **<UCCX FQDN>/appadmin/main**으로 이동하여 브라우저를 통해 인증서를 설치합니다.

알림 서비스 클라이언트 인증서

CCX 알림 서비스는 XMPP(Extensible Messaging and Presence Protocol)를 통해 클라이언트 데스크톱에 실시간 정보를 전송하기 위해 Finesse, UCCX 및 CUIC에서 사용합니다. 이는 실시간 Finesse 통신과 CUIC Live Data에 사용됩니다.

Live Data를 사용하는 에이전트 및 수퍼바이저 또는 보고 사용자의 PC에 Notification Service 클라이언트 인증서를 설치하려면 각 UCCX 노드에 대해 **https://<UCCX FQDN>:7443/**으로 이동하여 브라우저를 통해 인증서를 설치합니다.

Finesse 클라이언트 인증서

Finesse 클라이언트 인증서는 데스크톱과 공동 상주 Finesse 서버 간의 REST API 통신을 위해 Finesse Tomcat 인스턴스에 연결하기 위해 Finesse 데스크톱에서 사용됩니다.

에이전트 및 수퍼바이저용 Finesse 인증서를 설치하려면 클라이언트 PC에서 각 UCCX 노드에 대해 https://<UCCX FQDN**>:8445/**로 이동하고 브라우저 프롬프트를 통해 인증서를 설치합니다.

Finesse 관리자용 Finesse 인증서를 설치하려면 클라이언트 PC에서 각 UCCX 노드에 대한 https:// **<UCCX FQDN>:8445/cfadmin**으로 이동하여 브라우저 프롬프트를 통해 인증서를 설치합니다.

SocialMiner 클라이언트 인증서

SocialMiner Tomcat 인증서가 클라이언트 컴퓨터에 설치되어 있어야 합니다. 상담원이 채팅 요청을 수락하면 채팅 가젯이 채팅방을 나타내는 URL로 리디렉션됩니다. 이 채팅방은 SocialMiner 서버에서 호스팅하며 고객 또는 채팅 연락처를 포함합니다.

브라우저에 SocialMiner 인증서를 설치하려면 클라이언트 PC에서 https://**<SocialMiner FQDN>/로** 이동하고 브라우저 프롬프트를 통해 인증서를 설치합니다.

CUIC 클라이언트 인증서

CUIC Tomcat 인증서는 CUIC 웹 페이지 내 또는 데스크톱의 가젯 내에서 내역 보고서 또는 Live Data 보고서에 CUIC 웹 인터페이스를 사용하는 에이전트, 수퍼바이저 및 보고 사용자의 클라이언트 시스템에 설치해야 합니다.

브라우저에 CUIC Tomcat 인증서를 설치하려면 클라이언트 PC에서 https://<UCCX FQDN**>:8444/로** 이동하여 브라우저 프롬프트를 통해 인증서를 설치합니다.

CUIC Live Data 인증서(11.x 이후)

CUIC는 백엔드 라이브 데이터에 대해 Socket IO Service를 사용합니다. 이 인증서는 Live Data용 CUIC 웹 인터페이스를 사용하거나 Finesse 내에서 Live Data 가젯을 사용하는 에이전트, 수퍼바이저 및 보고 사용자의 클라이언트 시스템에 설치해야 합니다.

브라우저에 Socket IO 인증서를 설치하려면 클라이언트 PC에서 https://<UCCX FQDN**>:12015/로** 이동하고 브라우저 프롬프트를 통해 인증서를 설치합니다.

스크립트에서 액세스할 수 있는 타사 애플리케이션

서드파티 서버의 안전한 위치에 액세스하기 위해 UCCX 스크립트를 설계한 경우(예: HTTPS URL에 대한 *URL 문서 가져오기* 단계 또는 HTTPS REST URL에 대한 *Rest 호출* 만들기), 서드파티 서비스의 서명 또는 자체 서명 인증서 체인을 UCCX tomcat-*trust 키 저장소에* 업로드합니다. 이 인증서를 가져오려면 UCCX **OS Administration(**UCCX **OS 관리) 페이지**에 액세스하여 Upload Certificate(**인증서 업로드)를 선택합니다**.

UCCX 엔진은 타사 애플리케이션이 스크립트 단계를 통해 보안 위치에 액세스할 때 이러한 인증서가 제공된 경우 플랫폼 Tomcat 키 저장소에서 타사 인증서 체인을 검색하도록 구성됩니다.

Tomcat 키 저장소에는 기본적으로 루트 인증서가 없으므로 **OS 관리 페이지**를 통해 액세스할 수 있는 플랫폼 Tomcat 키 저장소에 전체 인증서 체인을 업로드해야 합니다.

이러한 작업을 완료한 후 Cisco UCCX 엔진을 다시 시작합니다.

다음을 확인합니다.

모든 인증서가 올바르게 설치되었는지 확인하려면 이 섹션에 설명된 기능을 테스트할 수 있습니다. 인증서 오류가 나타나지 않고 모든 기능이 제대로 작동하면 인증서가 올바르게 설치됩니다.

- 워크플로를 통해 에이전트를 자동으로 기록하도록 Finesse를 구성합니다. 상담원이 통화를 처리한 후 MediaSense Search and Play 애플리케이션을 사용하여 통화를 찾습니다. 통화에 MediaSense의 녹음 메타데이터에 연결된 에이전트, CSQ 및 팀 태그가 있는지 확인합니다.
- SocialMiner를 통해 에이전트 웹 채팅을 구성합니다. 웹 양식을 통해 채팅 연결을 삽입합니다. 상담원이 채팅 연결을 수락할 배너를 받았는지 확인하고 채팅 연결이 수락되면 채팅 양식이 제대로 로드되고 상담원이 채팅 메시지를 받고 보낼 수 있는지 확인합니다.
- Finesse를 통해 에이전트 로그인을 시도합니다. 인증서 경고가 표시되지 않고 웹 페이지에서 브라우저에 인증서를 설치하라는 메시지가 표시되지 않는지 확인합니다. 에이전트가 상태를 올바르게 변경할 수 있으며 UCCX에 대한 새 통화가 에이전트에 올바르게 표시되는지 확인합니다.
- 에이전트 및 수퍼바이저 Finesse 데스크톱 레이아웃에서 Live Data 가젯을 구성한 후 에이전트, 수퍼바이저 및 보고 사용자에게 로그인합니다. Live Data 가젯이 제대로 로드되고, 초기 데이터가 가젯에 채워지며, 기본 데이터가 변경되면 데이터가 새로 고쳐지는지 확인합니다.
- 브라우저에서 두 UCCX 노드의 AppAdmin URL로 연결을 시도합니다. 로그인 페이지를 표시하라는 메시지가 표시되면 인증서 경고가 표시되지 않는지 확인합니다.

문제 해결

문제 - 잘못된 사용자 ID/비밀번호

UCCX Finesse 에이전트가 "잘못된 **사용자 ID/비밀번호**" 오류로 로그인할 수 없습니다.

원인

Unified CCX는 예외 "SSLHandshakeException"을 throw하며 Unified CM과의 연결을 설정하지 못합니다.

솔루션

- Unified CM Tomcat 인증서가 만료되지 않았는지 확인합니다.
- Unified CM에서 업로드한 인증서에 다음 내선 번호 중 하나가 위험으로 표시되어 있는지 확인합니다.
  X509v3 키 사용(OID - 2.5.29.15)
  X509v3 기본 제약 조건(OID - 2.5.29.19)
  다른 확장을 중요로 표시하면 Unified CM 인증서 확인에 실패하여 Unified CCX와 Unified CM 간의 통신이 실패합니다.

문제 - CSR SAN과 인증서 SAN이 일치하지 않음

CA 서명 인증서의 업로드에는 "CSR SAN 및 인증서 SAN이 일치하지 않음" 오류가 표시됩니다.

원인

CA가 인증서 SAN(주체 대체 이름) 필드에 다른 부모 도메인을 추가했을 수 있습니다. 기본적으로 CSR에는 다음과 같은 SAN이 있습니다.

주체 대체 이름 [
  example.com(dNSName)
  hostname.example.com(dNSName)
]

CA는 다른 SAN이 인증서에 추가된 인증서를 반환할 수 있습니다. www.hostname.example.com 이 경우 인증서에는 추가 SAN이 있습니다.

주체 대체 이름 [
  example.com(dNSName)
  hostname.example.com(dNSName)

  www.hostname.example.com(dNSName)
]

이로 인해 SAN 불일치 오류가 발생합니다.

솔루션

UCCX 'Generate Certificate Signing Request'(인증서 서명 요청 생성) 페이지의 'Subject Alternate Name(SAN)' 섹션에서 빈 Parent Domain(상위 도메인) 필드를 사용하여 CSR을 생성합니다. 이렇게 하면 CSR이 SAN 특성으로 생성되지 않으며 CA가 SAN을 포맷할 수 있으며, UCCX에 인증서를 업로드할 때 SAN 특성이 일치하지 않습니다. Parent Domain(상위 도메인) 필드의 기본값은 UCCX 서버의 도메인이므로 CSR에 대한 설정을 구성하는 동안 값을 명시적으로 제거해야 합니다.

문제 - NET::ERR_CERT_COMMON_NAME_INVALID

UCCX, MediaSense 또는 SocialMiner 웹 페이지에 액세스하면 오류 메시지가 표시됩니다.

"귀하의 연결은 비공개가 아닙니다.

공격자가 <Server_FQDN>에서 사용자 정보(예: 암호, 메시지 또는 신용카드)를 훔치려고 시도할 수 있습니다. NET::ERR_CERT_COMMON_NAME_INVALID

이 서버는 <Server_FQDN>임을 확인할 수 없습니다. 보안 인증서는 [missing_subjectAltName]에서 가져온 것입니다. 이는 컨피그레이션 오류 또는 공격자가 연결을 가로채기 때문에 발생할 수 있습니다."

원인

크롬 버전 58은 웹사이트의 CN(Common Name)도 SAN으로 포함되지 않은 경우 웹사이트 인증서가 안전하지 않다고 보고하는 새로운 보안 기능을 도입했다.

솔루션

- **Advanced(고급) > <Server_FQDN> (unsafe)**로 **계속 진행하여 사이트**로 이동하여 인증서 오류를 승인할 수 있습니다.
- CA 서명 인증서와 함께 오류를 완전히 방지할 수 있습니다. CSR을 생성하면 서버의 FQDN이 SAN으로 포함됩니다. CA는 CSR에 서명할 수 있으며, 서명된 인증서를 다시 서버에 업로드하면 서버의 인증서는 SAN 필드에 FQDN을 갖게 되므로 오류가 표시되지 않습니다.

추가 정보

Chrome 58의 Deprecations and Removations에서 "인증서의 commonName 일치 지원 제거" 섹션을 참조하십시오.

인증서 결함

- Cisco 버그 ID CSCvb46250 - UCCX: Tomcat ECDSA 인증서가 Finesse Live Data에 미치는 영향
- Cisco 버그 ID CSCvb58580 - RSA CA에서 서명한 tomcat 및 tomcat-ECDSA를 모두 사용하여 SocialMiner에 로그인할 수 없음
- Cisco 버그 ID CSCvd56174 - UCCX: SSLHandshakeException으로 인한 Finesse 에이전트 로그인 실패
- Cisco 버그 ID CSCuv89545 - Finesse Logjam Vulnerability

관련 정보

- UCCX 솔루션의 ECDSA 인증서 이해
- UCCX에 대한 SHA 256 지원
- UCCX 서명 및 자체 서명 인증서 컨피그레이션 예
- 기술 지원 및 문서 – Cisco Systems

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.