UCCX에 대한 SHA-256 지원

목차

소개

이 문서에서는 UCCX(Cisco Unified Contact Center Express)에 대한 SHA-256 지원에 대해 설명합니다. SHA-1 암호화는 곧 사용되지 않으며 UCCX에서 지원되는 모든 웹 브라우저는 SHA-1 암호화를 사용하는 인증서를 제공하는 서버에서 웹 페이지를 차단하기 시작합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco UCCX(Unified Contact Center Express)
- 인증서 관리

Microsoft 및 Mozilla의 발표 내용

SHA-1 감가상각 업데이트

계속해서 SHA-1 인증서를 단계적으로 제거합니다.

이러한 알림에서 브라우저 제조업체는 2016년 1월 1일 이후에 ValidFrom 날짜로 발행된 SHA-1 인

증서에 대해 우회할 수 있는 경고를 브라우저에 표시한다고 밝혔습니다.

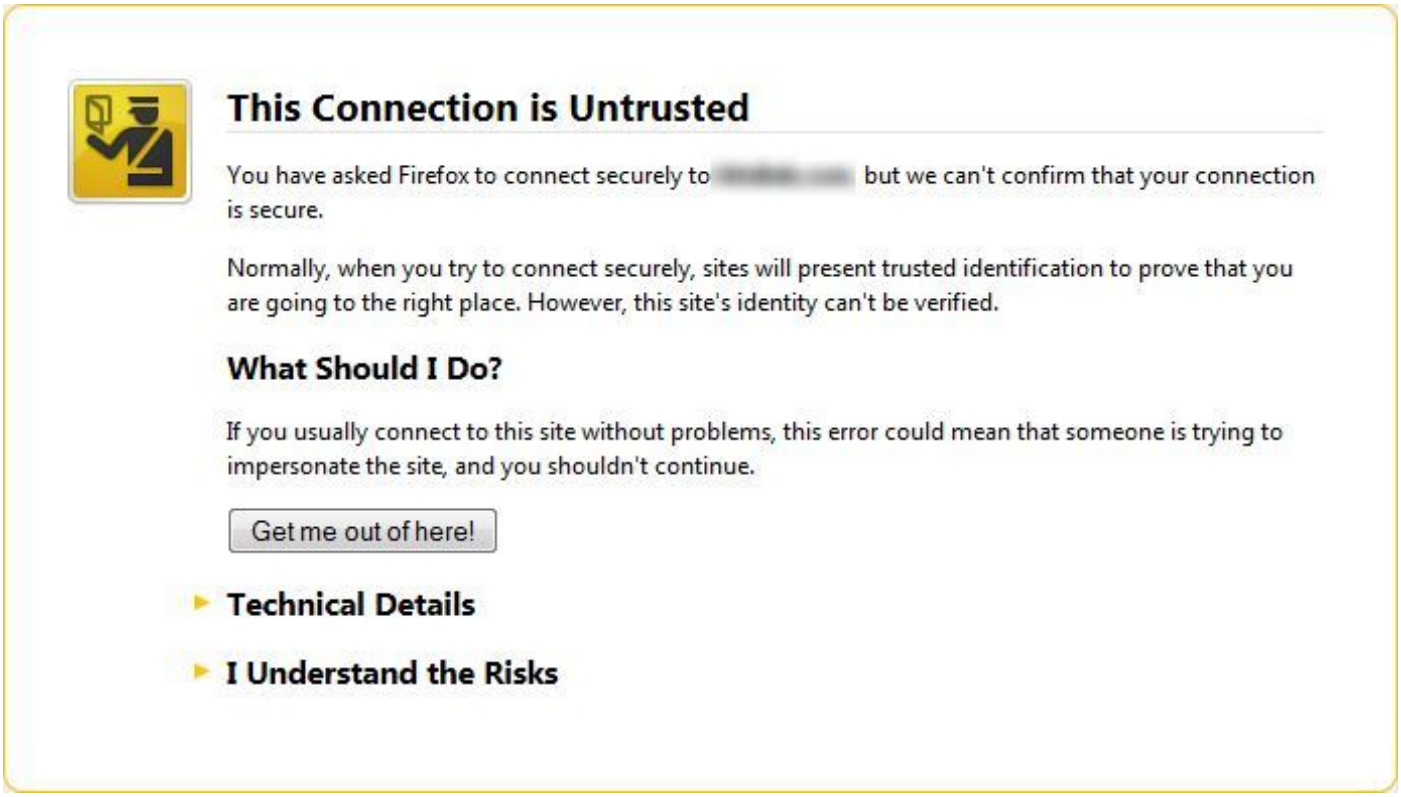
또한 현재 레코드 계획은 인증서의 ValidFrom 항목과 상관없이 2017년 1월 1일 이후에 SHA-1 인증서를 사용하는 웹 사이트를 차단하는 것입니다. 그러나 최근 SHA-1 인증서를 대상으로 한 공격의 경우 이러한 브라우저는 이 타임라인을 위로 이동하고 인증서 발급 날짜와 상관없이 2017년 1월 1일 이후에 SHA-1 인증서를 사용하는 웹 사이트를 차단할 수 있습니다.

Cisco는 고객에게 이 주제에 대한 Microsoft와 Mozilla의 추가 공지 사항을 자세히 읽고 최신 상태로 유지할 것을 권장합니다.

일부 버전의 UCCX는 SHA-1 인증서를 생성합니다. SHA-1 인증서로 보호되는 UCCX 웹 페이지에 액세스하는 경우, 이전에 설명한 날짜 및 규칙에 따라 경고가 생성되거나 차단될 수 있습니다.

사용자 환경

ValidFrom 날짜 및 이전에 나열된 규칙에 따라 SHA-1 인증서가 탐지되면 사용자에게 다음과 유사한 메시지가 표시될 수 있습니다.



사용자가 결정한 사항에 따라 이 경고를 우회할 수도 있고 우회하지 못할 수도 있습니다.

UCCX 고려 사항

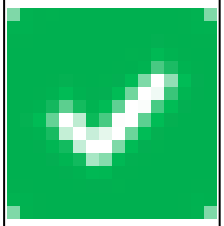
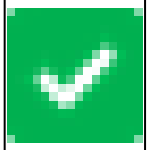
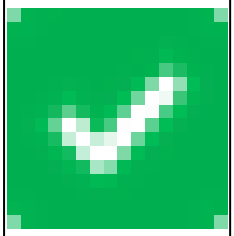
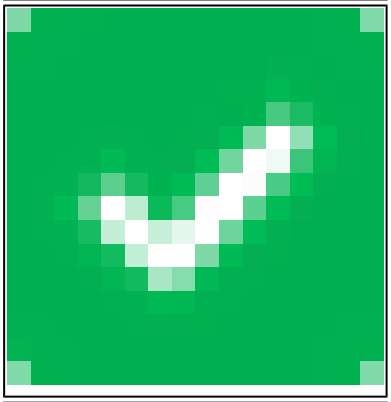
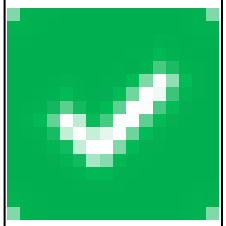
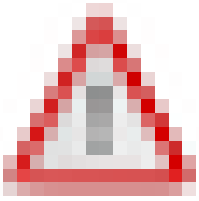
이 표에서는 현재 소프트웨어 유지 보수 중인 UCCX의 각 버전에 대한 SHA-1 인증서 영향 및 완화 전략에 대해 설명합니다.

이 문서에 사용된 표기법

표기법	설명

	이미 지원됩니다. 추가 작업이 필요하지 않습니다.
	지원도 가능하지만 인증서 재생성이 필요하다.
	지원을 사용할 수 없습니다.

UCCX 11.5

	UCCX 관리	CUIC 관리 라이브 데이터 번호	Finesse 관리 데스크톱 번호	상담원 전자메일 및 SocialMiner와의 채팅*	UCCX REST 스크립팅 단계	MediaSense* 11.5를 사용한 녹음
신규 설치						
이전 버전에서 업그레이드	 UCCX 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생	 UCCX Cisco CUIC(Unified Intelligence Center) 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생성된 경	 UCCX Finesse 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생성된 경	 SocialMiner 및 UCCX 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생성된 경우 자체 서명 인증서는 SHA-1 기반이므로 재생	 UCCX는 REST(Representational State Transfer) 통신의 일부로 SHA-1 인증서를 사용하는 원격 웹 서버를 거부하지 않습니다. REST 단계는 UCCX에서 인증서가 재생성된 후 작동합니	 MediaSense 및 UCCX 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생성된 경우 자체 서명 인증서는 SHA-1 기반이므로 재생

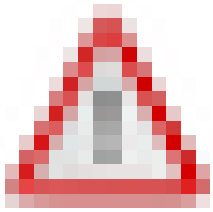
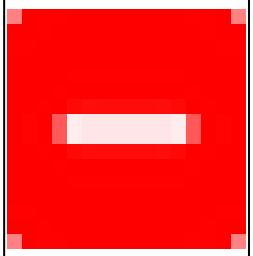
	성된 경우 자체 서명 인증서는 SHA-1 기반이므로 재생성해야 합니다.	우 자체 서명 인증서는 SHA-1 기반이므로 재생성해야 합니다.	우 자체 서명 인증서는 SHA-1 기반이므로 재생성해야 합니다.	성해야 합니다.	다.	성해야 합니다.

참고: *재생성된 MediaSense 및 SocialMiner 인증서를 UCCX로 다시 가져와야 합니다.

참고: Finesse와 CUIC에는 별도의 작업이 #No. 인증서는 UCCX 플랫폼 관리 페이지에서 한 번만 재생성됩니다.

UCCX 11.0(1)

	UCCX 관리	CUIC 관리 Live Data#	Finesse 관리 데스크톱 번호	상담원 이메일 및 SocialMiner와의 채팅**	UCCX REST 스크립팅 단계	MediaSense** 11.0* 및 10.5*를 사용한 녹음
신규 설치	기본적으로 모든 자체 서명 새 설치 인증서는 SHA-1 인증서이며 다시 생성해야 합니다.	기본적으로 모든 자체 서명 새 설치 인증서는 SHA-1 인증서이며 다시 생성해야 합니다.	기본적으로 모든 자체 서명 새 설치 인증서는 SHA-1 인증서이며 다시 생성해야 합니다.	기본적으로 모든 자체 서명 새 설치 인증서는 SHA-1 인증서이며 다시 생성해야 합니다.	UCCX는 SHA-1 인증서를 REST 통신의 일부로 사용하는 원격 웹 서버를 거부하지 않습니다. REST 단계는 UCCX에서 인증서가 재생성된 후 작동합니다.	기본 자체 서명 인증서는 SHA-1입니다. 재생성 인증서는 SHA-256에 대한 옵션을 제공하지 않습니다.

이전 버전에서 업그레이드	 UCCX 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생성된 경우 자체 서명 인증서는 SHA-1 기반이므로 재생성해야 합니다.	 UCCX CUIC 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생성된 경우 자체 서명 인증서는 SHA-1 기반이므로 재생성해야 합니다.	 UCCX Finesse 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생성된 경우 자체 서명 인증서는 SHA-1 기반이므로 재생성해야 합니다.	 SocialMiner 및 UCCX 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생성된 경우 자체 서명 인증서는 SHA-1 기반이므로 재생성해야 합니다.	 UCCX는 SHA-1 인증서를 REST 통신의 일부로 사용하는 원격 웹 서버를 거부하지 않습니다. REST 단계는 UCCX에서 인증서가 재생성된 후 작동합니다.	 기본 자체 서명 인증서는 SHA-1입니다. 재생성 인증서는 SHA-256에 대한 옵션을 제공하지 않습니다.

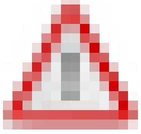
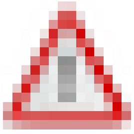
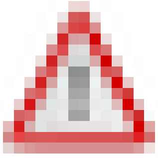
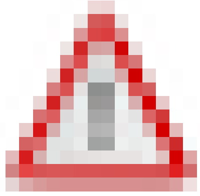
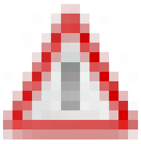
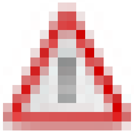
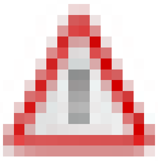
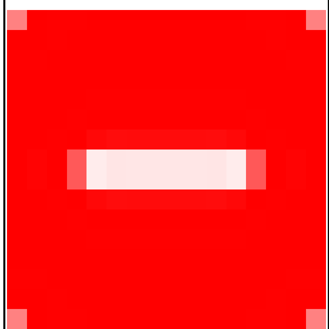
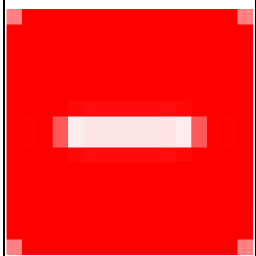
참고: *MediaSense 10.5 및 11.0에서 SHA-256 인증서를 생성하고 수락할 수 있도록 ES(Engineering Special)가 릴리스됩니다.

참고: **재생성된 MediaSense 및 SocialMiner 인증서를 UCCX로 다시 가져와야 합니다.

참고: Finesse와 CUIC에는 별도의 작업이 #No. 인증서는 UCCX 플랫폼 관리 페이지에서 한 번만 재생성됩니다.

UCCX 10.5 및 10.6

	UCCX 관리	CUIC 관리 Live Data#	Finesse 관리 데스크톱 번호	상담원 전자메일 및 SocialMiner와의 채팅*	UCCX REST 스크립팅 단계	MediaSense*** 10.0** / 10.5**를 사용한 녹음

신규 설치	 기본적으로 모든 자체 서명 새 설치 인증서는 SHA-1 인증서이며 다시 생성해야 합니다.	 기본적으로 모든 자체 서명 새 설치 인증서는 SHA-1 인증서이며 다시 생성해야 합니다.	 기본적으로 모든 자체 서명 새 설치 인증서는 SHA-1 인증서이며 다시 생성해야 합니다.	 에이전트 이메일 및 채팅에 대한 SHA-256 지원은 SM(SocialMiner) v11에서만 사용할 수 있으며 SM v11은 UCCX v10.x와 호환되지 않습니다.	 UCCX는 SHA-1 인증서를 REST 통신의 일부로 사용하는 원격 웹 서버를 거부하지 않습니다. REST 단계는 UCCX에서 인증서가 재생성된 후 작동합니다.	 기본 자체 서명 인증서는 SHA-1입니다. 재생성 인증서는 SHA-256에 대한 옵션을 제공하지 않습니다.
이전 버전에서 업그레이드	 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생성된 경우 자체 서명 인증서는 SHA-1 기반이므로 재생성해야 합니다.	 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생성된 경우 자체 서명 인증서는 SHA-1 기반이므로 재생성해야 합니다.	 인증서는 이전 릴리스의 알고리즘을 유지합니다. 이전 릴리스에서 SHA-11 키로 생성된 경우 자체 서명 인증서는 SHA-1 기반이므로 재생성해야 합니다.	 에이전트 이메일 및 채팅에 대한 SHA-256 지원은 SM v11에서만 사용할 수 있으며 SM v11은 UCCX v10.x와 호환되지 않습니다.	 UCCX는 SHA-1 인증서를 REST 통신의 일부로 사용하는 원격 웹 서버를 거부하지 않습니다. REST 단계는 UCCX에서 인증서가 재생성된 후 작동합니다.	 기본 자체 서명 인증서는 SHA-1입니다. 재생성 인증서는 SHA-256에 대한 옵션을 제공하지 않습니다.

참고: *Engineering Special은 SocialMiner 10.6에서 SHA-256 인증서를 생성하고 수락할 수 있도록 릴리스됩니다.

참고: **MediaSense 10.0 및 10.5에서 SHA-256 인증서를 생성하고 수락할 수 있도록 ES(Engineering Special)가 릴리스됩니다.

참고: ***재생성된 MediaSense 및 SocialMiner 인증서를 UCCX로 다시 가져와야 합니다.

참고: Finesse와 CUIC에는 별도의 작업이 #No. 인증서는 UCCX 플랫폼 관리 페이지에서 한 번만 재생성됩니다.

UCCX 10.0

	UCCX **	CUIC 관리 Live Data#	Finesse 관리 데스크톱 번호	SocialMiner와 상담원 채팅*	UCCX REST 스크립팅 단계	MediaSense*** 10.0**을 사용한 녹음
신규 설치	기본 자체 서명 인증서는 SHA-1입니다. 재생성 인증서는 SHA-256에 대한 옵션을 제공하지 않습니다.	기본 자체 서명 인증서는 SHA-1입니다. 재생성 인증서는 SHA-256에 대한 옵션을 제공하지 않습니다.	기본 자체 서명 인증서는 SHA-1입니다. 재생성 인증서는 SHA-256에 대한 옵션을 제공하지 않습니다.	에이전트 채팅에 대한 SHA-256 지원은 SM v11에서만 사용할 수 있으며 SM v11은 UCCX v10.x와 호환되지 않습니다.	UCCX는 SHA-1 인증서를 REST 통신의 일부로 사용하는 원격 웹 서버를 거부하지 않습니다. REST 단계는 UCCX에서 인증서가 재생성된 후 작동합니다.	기본 자체 서명 인증서는 SHA-1입니다. 재생성 인증서는 SHA-256에 대한 옵션을 제공하지 않습니다.
이전 버전에서 업그레이드	기본 자체 서명 인증서는 SHA-1입니다.	기본 자체 서명 인증서는 SHA-1입니다.	기본 자체 서명 인증서는 SHA-1입니다. 재생성 인	에이전트 채팅에 대한 SHA-256 지원은	UCCX는 SHA-1 인증서를 REST 통신의 일부로 사	기본 자체 서명 인증서는 SHA-1입니다.

	재생성 인증서는 SHA-256에 대한 옵션을 제공하지 않습니다.	재생성 인증서는 SHA-256에 대한 옵션을 제공하지 않습니다.	증서는 SHA-256에 대한 옵션을 제공하지 않습니다.	SM v11에서만 사용할 수 있으며 SM v11은 UCCX v10.x와 호환되지 않습니다.	용하는 원격 웹 서버를 거부하지 않습니다. REST 단계는 UCCX에서 인증서가 재생성된 후 작동합니다.	재생성 인증서는 SHA-256에 대한 옵션을 제공하지 않습니다.

참고: *Engineering Special은 SocialMiner 10.6에서 SHA-256 인증서를 생성하고 수락할 수 있도록 릴리스됩니다.

참고: **MediaSense 10.0에서 SHA-256 인증서를 생성하고 수락할 수 있도록 ES(Engineering Special)가 릴리스됩니다.

참고: ***재생성된 MediaSense 및 SocialMiner 인증서를 UCCX로 다시 가져와야 합니다.

참고: Finesse와 CUIC에는 별도의 작업이 #No. 인증서는 UCCX 플랫폼 관리 페이지에서 한 번만 재생성됩니다.

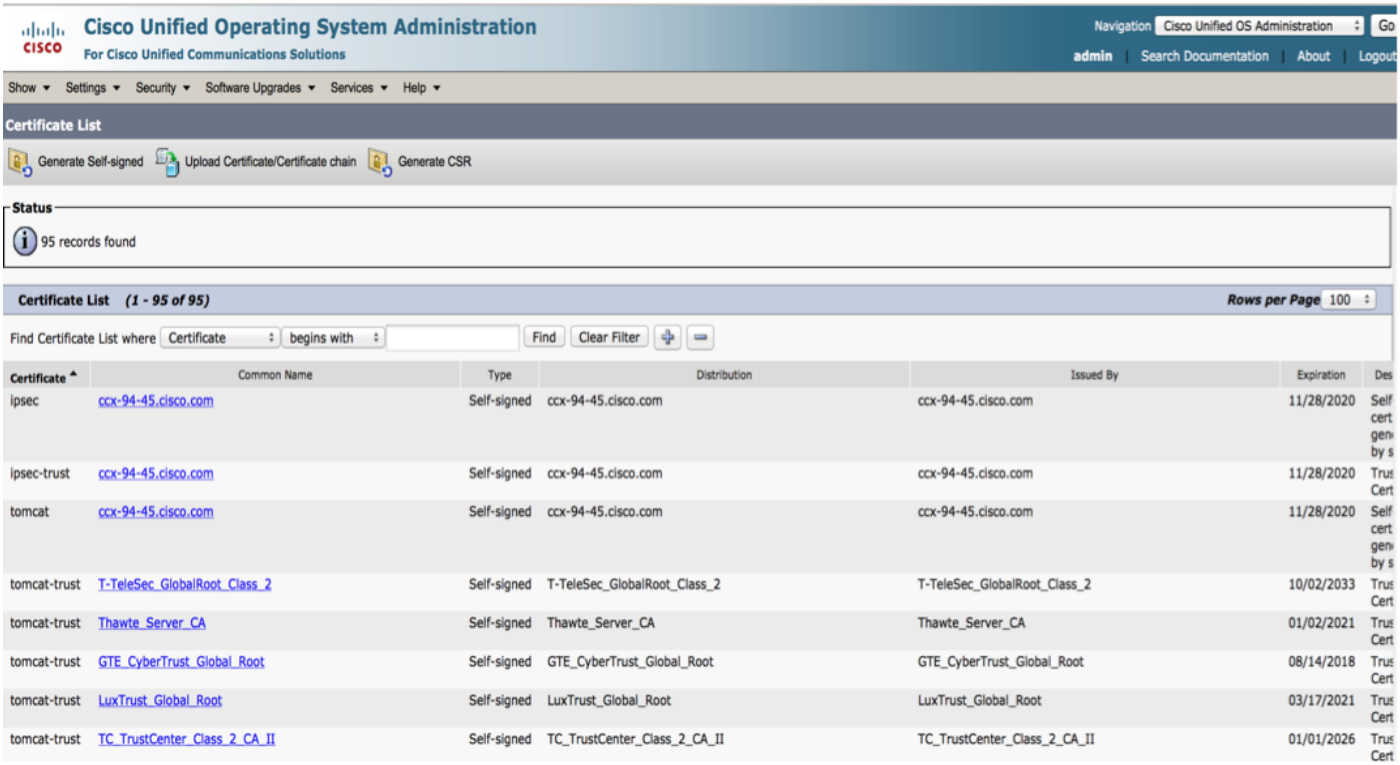
인증서 관리 지침

확인 및 재생성이 필요한 세 가지 유형의 인증서가 있습니다.

- 자체 서명 인증서
- 신뢰할 수 있는 루트 인증서
- 서드파티 서명 인증서

자체 서명 인증서

OS Administration(OS 관리) 페이지로 이동합니다. Security(보안) > Navigate Certificate management(인증서 관리)를 선택합니다. Find(찾기)를 클릭합니다.



4가지 인증서 범주를 확인합니다.

- ipsec
- ipsec 트러스트
- 수고양이
- tomcat-트러스트

tomcat 카테고리 아래의 인증서와 Self-signed 유형은 재생성이 필요한 인증서입니다. 이전 이미지에서 세 번째 인증서는 재생성이 필요한 인증서입니다.

인증서를 재생성하려면 다음 단계를 완료합니다.

1단계. 인증서의 Common Name(공용 이름)을 클릭합니다.

2단계. 팝업 창에서 재생성(Regenerate)을 클릭합니다.

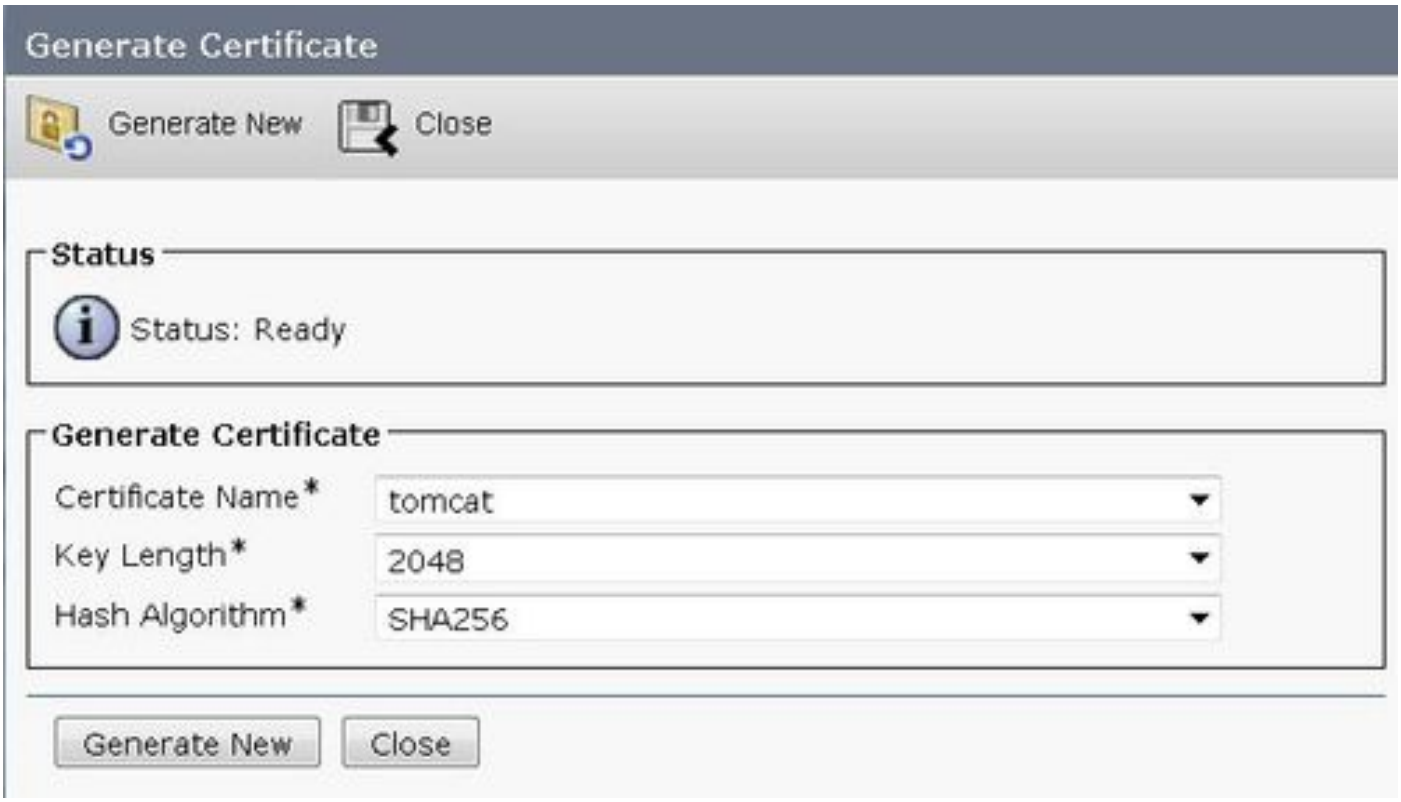
3단계. SHA-256의 암호화 알고리즘을 선택합니다.

UCCX 버전 10.6의 경우 인증서를 재생성하려면 다음 단계를 완료합니다.

1단계. Generate New(새로 생성)를 클릭합니다.

2단계. Certificate Name(인증서 이름)을 tomcat으로, Key Length(키 길이)를 2048으로, Hash Algorithm(해시 알고리즘)을 SHA256으로 선택합니다.

3단계. Generate New를 클릭합니다.



신뢰할 수 있는 루트 인증서

이는 플랫폼에서 제공하는 인증서입니다. 이러한 인증서의 SHA-1 기반 서명은 해시의 서명이 아니라 TLS(Transport Layer Security) 클라이언트에서 ID를 기반으로 신뢰하므로 문제가 되지 않습니다.

서드파티 서명 인증서

SHA-1 알고리즘으로 서드파티 Certificate Authority에서 서명한 인증서는 SHA-256 서명 인증서로 다시 가져와야 합니다. 인증서 체인의 모든 인증서는 SHA-256으로 종료해야 합니다.

추가 참고 사항

최신 Engineering Specials는 가능한 경우 cisco.com에 게시됩니다. Engineering Special 다운로드에 대한 해당 제품 페이지를 정기적으로 확인합니다.

- 인증서 재생성 또는 관련 문제에 대한 지원이 필요하면 Cisco TAC 케이스를 여십시오.
- UCCX 버전 8.x 또는 9.x에서 실행되는 고객은 Cisco 및 브라우저 지원을 유지하기 위해 지원되는 최신 릴리스로 업그레이드할 계획이어야 합니다.

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.