

# UCCX 솔루션에서 ECDSA 인증서 이해

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[절차](#)

[CA 서명 인증서 업그레이드 전](#)

[자체 서명 인증서 업그레이드 전](#)

[구성](#)

[UCCX 및 SocialMiner용 서명된 인증서](#)

[UCCX 및 SocialMiner용 자체 서명 인증서](#)

[FAQ\(자주 묻는 질문\)](#)

[관련 정보](#)

## 소개

이 문서에서는 ECDSA(Elliptical Curve Digital Signature Algorithm) 인증서를 사용하기 위해 Cisco UCCX(Unified Contact Center Express) 솔루션을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

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

- UCCX
- SocialMiner
- Cisco CUCM(Unified Communications Manager)
- UCCX 솔루션 인증서 컨피그레이션 - <http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html>

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

## 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

# 배경 정보

CC(Common Criteria) 인증의 일환으로 Cisco Unified Communications Manager는 버전 11.0에 ECDSA 인증서를 추가했습니다. 이 문제는 버전 11.5의 UCCX, SocialMiner, MediaSense 등 모든 VOS(Voice Operating System) 제품에 영향을 미칩니다.

Elliptic Curve Digital Signature Algorithm에 대한 자세한 내용은 여기에서 확인할 수 있습니다  
[.https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767](https://www.maximintegrated.com/en/app-notes/index.mvp/id/5767)

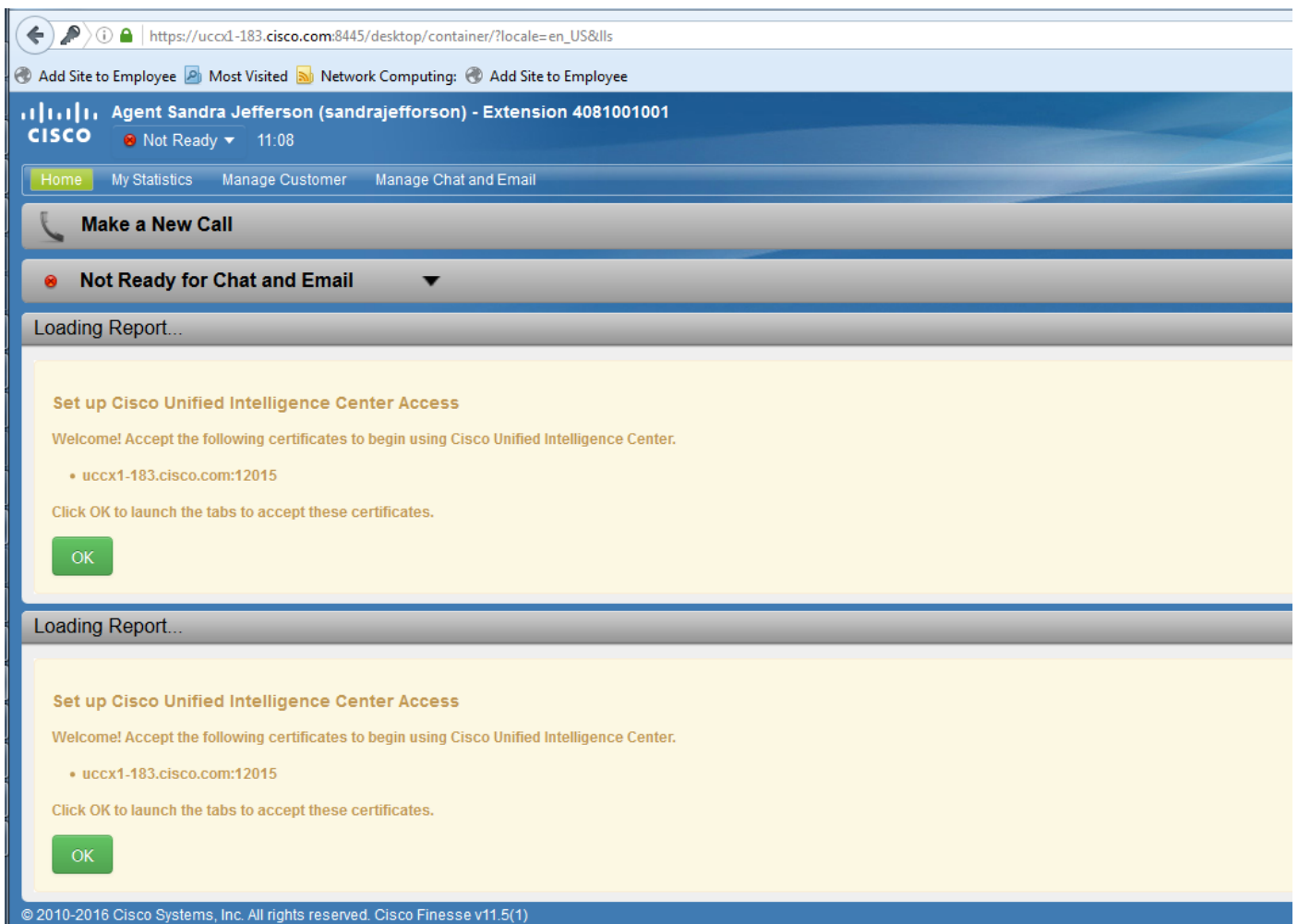
UCCX 솔루션과 관련하여 11.5로 업그레이드할 때 이전에 제공되지 않았던 추가 인증서가 제공됩니다.Tomcat-ECDSA 인증서입니다.

이 내용은 사전 출시 통신에도 설명되어 있습니다  
[.https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200651-UCCX-Version-11-5-Prerelease-Field-Commu.html?cachemode=refresh](https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200651-UCCX-Version-11-5-Prerelease-Field-Commu.html?cachemode=refresh)

## 상담원 경험

11.5로 업그레이드한 후, 에이전트가 인증서가 자체 서명되었는지 또는 CA(Certificate Authority)가 서명되었는지에 따라 Finesse 데스크톱에서 인증서를 승인하도록 요청할 수 있습니다.

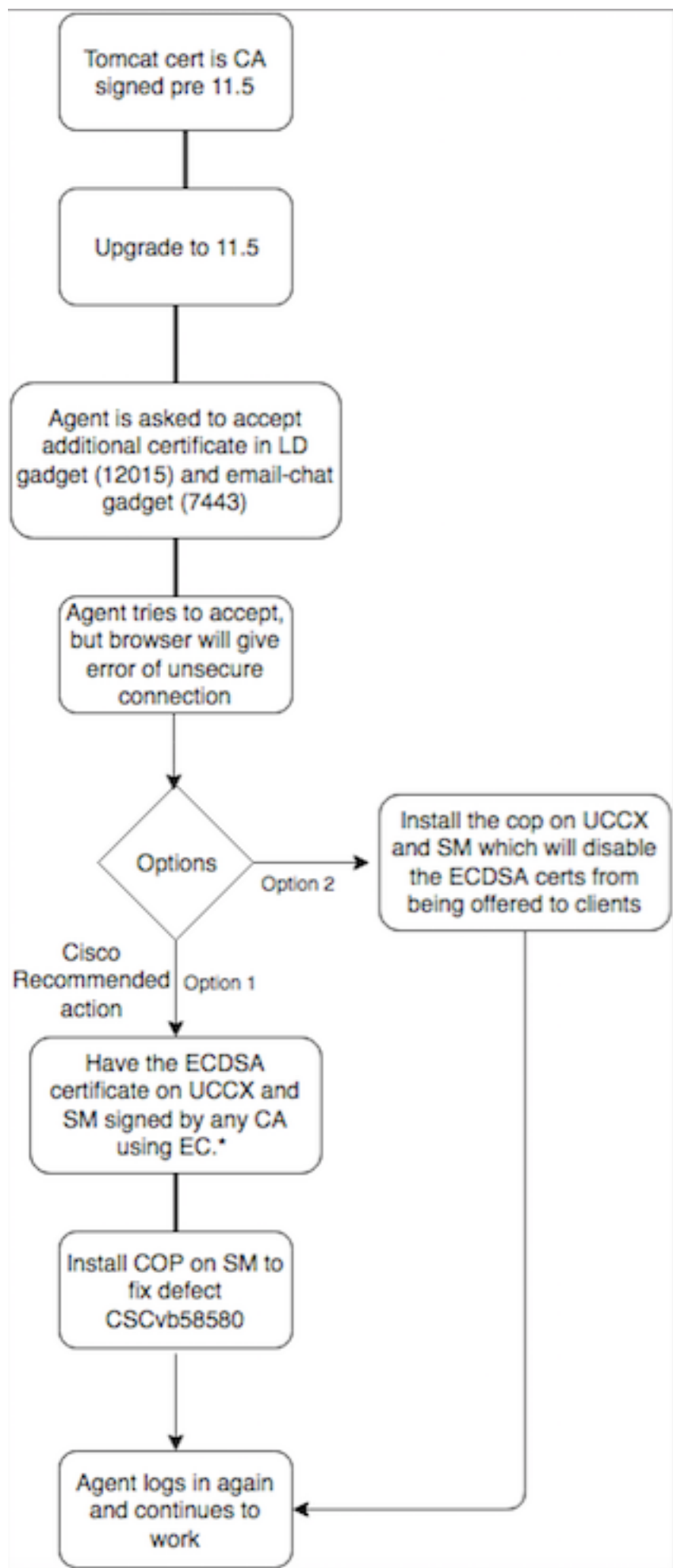
## 11.5로 업그레이드 후 사용자 환경



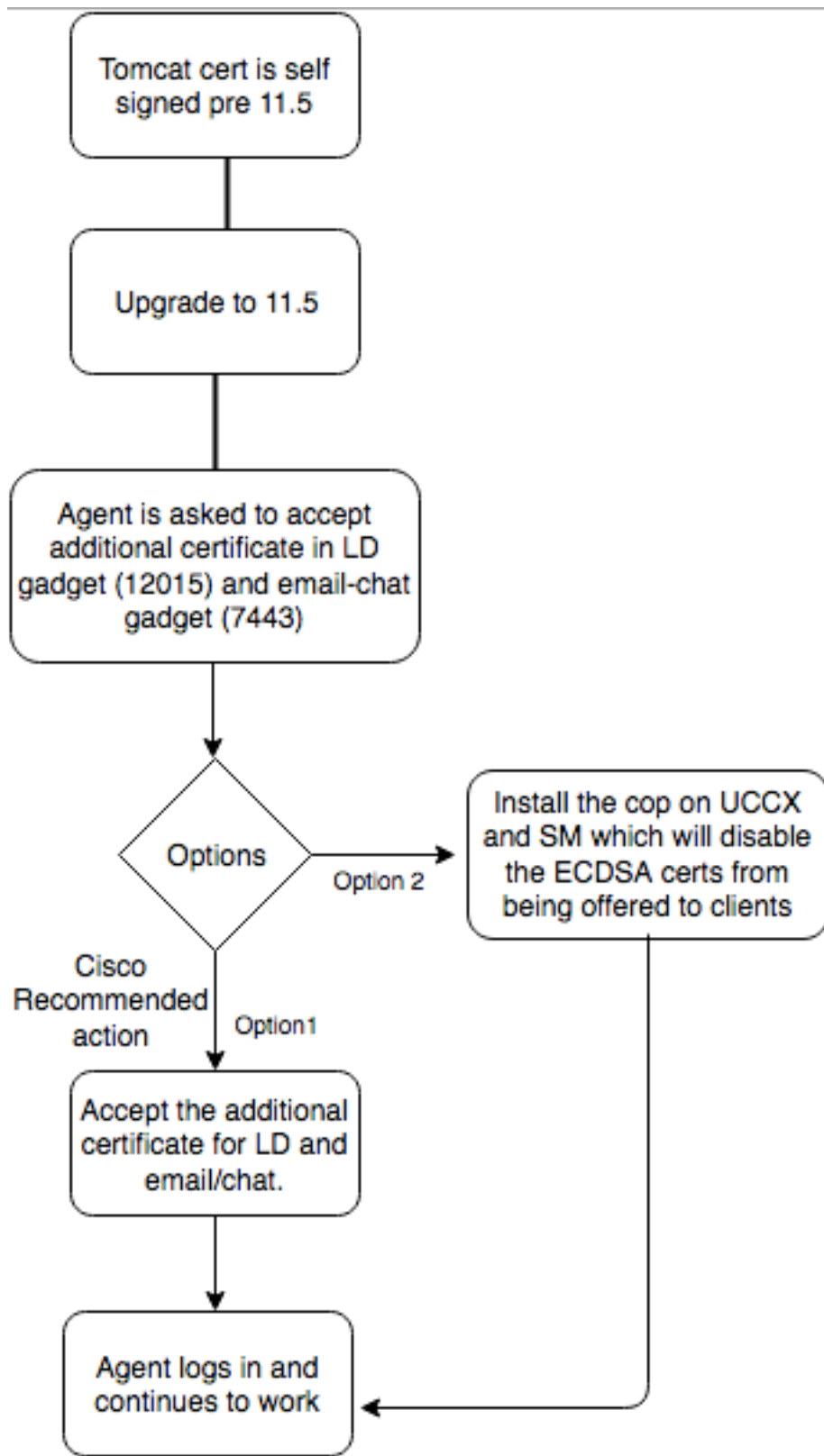
이는 Finesse 데스크톱이 이전에 제공되지 않았던 ECDSA 인증서를 제공받기 때문입니다.

## **절차**

**CA 서명 인증서 업그레이드 전**



## 자체 서명 인증서 업그레이드 전



## 구성

이 인증서에 권장되는 모범 사례

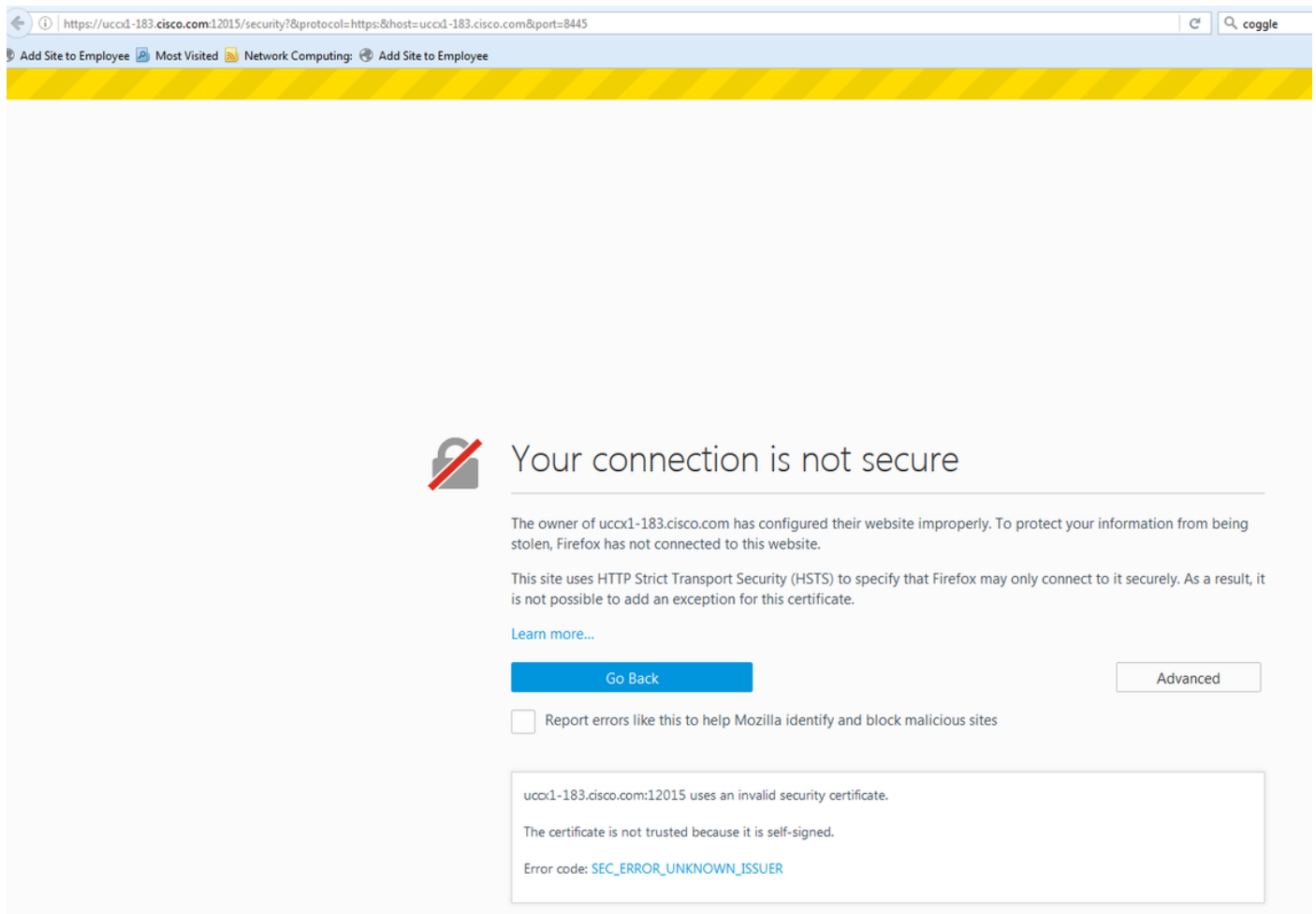
UCCX 및 SocialMiner용 서명된 인증서

CA 서명 인증서를 사용하는 경우 이 ECDSA 인증서는 다른 인증서와 함께 CA(Certificate Authority)에 의해 서명되어야 합니다

**참고:**CA가 이 ECDSA 인증서를 RSA에 서명하면 이 인증서가 클라이언트에 표시되지 않습니다.보안을 강화하기 위해 클라이언트에 제공되는 ECDSA 인증서가 권장 모범 사례입니다.

**참고:** SocialMiner의 ECDSA 인증서가 RSA를 사용하는 CA에 의해 서명된 경우 이메일 및 채팅 문제가 발생합니다.이는 결함 CSCvb58580에 문서화되며 cop 파일을 사용할 수 있습니다 .이 COP는 ECDSA 인증서가 클라이언트에 제공되지 않도록 합니다. RSA로만 ECDSA 인증서를 서명할 수 있는 CA가 있는 경우 이 인증서를 사용하지 마십시오.ECDSA 인증서가 제공되지 않고 RSA 전용 환경을 사용하도록 cop를 사용합니다.

CA 서명 인증서를 사용하고 업그레이드 후 ECDSA 인증서가 서명 및 업로드되지 않은 경우 에이전트는 추가 인증서를 수락하는 메시지를 경험합니다.OK(확인)를 클릭하면 웹 사이트로 리디렉션됩니다.그러나 ECDSA 인증서가 자체 서명되고 다른 웹 인증서가 CA에 서명되어 있으므로 브라우저 측에서 보안 시행 때문에 이 오류가 발생합니다.이러한 커뮤니케이션은 보안 위협으로 인식됩니다



버전 11.5에서 UCCX 및 SocialMiner로 업그레이드한 후 UCCX Publisher 및 Subscriber 및 SocialMiner의 각 노드에서 다음 단계를 완료합니다.

1. OS 관리 페이지로 이동하고 Security(보안) > Certificate Management(인증서 관리)를 선택합니다.

2. Generate CSR(CSR 생성)을 클릭합니다.

3. Certificate List 드롭다운 목록에서 인증서 이름으로 tomcat-ECDSA를 선택하고 Generate CSR을 클릭합니다.

4. Security(보안) > Certificate Management(인증서 관리)로 이동하고 Download CSR(CSR 다운로드)을 선택합니다.

5. 팝업 창의 드롭다운 목록에서 tomcat-ECDSA를 선택하고 Download CSR(CSR 다운로드)을 클릭합니다.

새 CSR을 서드파티 CA로 전송하거나 EC 인증서에 서명하는 내부 CA로 서명합니다.이렇게 하면 다음과 같은 서명된 인증서가 생성됩니다.

- CA용 루트 인증서(애플리케이션 인증서 및 EC 인증서에 동일한 CA를 사용하는 경우 이 단계를 건너뛸 수 있음)
- UCCX 게시자 ECDSA 서명 인증서
- UCCX 가입자 ECDSA 서명 인증서
- SocialMiner ECDSA 서명 인증서

**참고:** 게시자(UCCX)에 루트 및 중간 인증서를 업로드하면 자동으로 가입자에게 복제됩니다. 모든 응용 프로그램 인증서가 동일한 인증서 체인을 통해 서명된 경우 컨피그레이션의 게시자가 아닌 다른 서버에 루트 또는 중간 인증서를 업로드할 필요가 없습니다. 또한 동일한 CA가 EC 인증서에 서명하고 UCCX 애플리케이션 인증서를 구성할 때 이미 이 작업을 수행한 경우 루트 인증서의 업로드를 건너뛸 수 있습니다.

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

1. OS 관리 페이지로 이동하고 Security(보안) > Certificate Management(인증서 관리)를 선택합니다.

2. Upload Certificate를 클릭합니다.

3. 루트 인증서를 업로드하고 인증서 유형으로 tomcat-trust를 선택합니다.

4. Upload File을 클릭합니다.

5. Upload Certificate를 클릭합니다.

6. 애플리케이션 인증서를 업로드하고 인증서 유형으로 tomcat-ECDSA를 선택합니다.

7. Upload File을 클릭합니다.

**참고:** 하위 CA가 인증서에 서명하는 경우 루트 인증서 대신 하위 CA의 루트 인증서를 tomcat-trust 인증서로 업로드합니다. 중간 인증서가 발급되면 이 인증서를 애플리케이션 인증서 외에 tomcat-trust 저장소에 업로드합니다. 또한 동일한 CA가 EC 인증서에 서명하고 UCCX 애플리케이션 인증서를 구성할 때 이 작업을 이미 수행한 경우 루트 인증서의 업로드를 건너뛸 수 있습니다.

8. 완료되면 다음 애플리케이션을 다시 시작합니다.

## UCCX 및 SocialMiner용 자체 서명 인증서

UCCX 또는 SocialMiner가 자체 서명 인증서를 사용하는 경우 에이전트는 채팅 이메일 가젯과 Live Data 가젯에서 제공하는 인증서 경고를 수락하는 것이 좋습니다.

클라이언트 컴퓨터에 자체 서명 인증서를 설치하려면 그룹 정책 또는 패키지 관리자를 사용하거나 각 에이전트 PC의 브라우저에서 개별적으로 설치합니다.

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** 탭을 클릭합니다.
  3. **View Certificates**를 클릭합니다.
  4. Servers(서버) 탭으로 이동합니다.
  5. **Add Exception**을 클릭합니다.
1. **참고:**보안 예외를 추가하여 위의 프로세스와 동등한 인증서를 설치할 수도 있습니다.클라이언트에서 한 번 컨피그레이션입니다.

## FAQ(자주 묻는 질문)

CA 서명 인증서가 있으며 EC CA에서 서명해야 하는 ECDSA 인증서를 사용하고자 합니다.CA 서명 인증서를 사용할 수 있을 때까지 기다리는 동안 Live Data를 설정해야 합니다.어떻게 해야 합니까?

이 추가 인증서에 서명하거나 에이전트가 이 추가 인증서를 수락하도록 하지 않습니다.어떻게 해야 합니까?

브라우저에 ECDSA 인증서를 제공하는 것이 권장되지만 이를 비활성화하는 옵션이 있습니다 .UCCX 및 SocialMiner에 RSA 인증서만 클라이언트에 표시되도록 복사 파일을 설치할 수 있습니다 .ECDSA 인증서는 키 저장소에 남아 있지만 클라이언트에 제공되지는 않습니다.

클라이언트에 제공된 ECDSA 인증서를 비활성화하기 위해 이 복사본을 사용하는 경우 다시 활성화할 수 있습니까?

예, 롤백 경찰이 제공되었습니다.이 설정이 적용되면 이 인증서가 서명되어 서버에 업로드될 수 있습니다.



### 모든 인증서가 ECDSA로 설정됩니까?

현재는 아니지만 향후 VOS 플랫폼에 대한 추가 보안 업데이트

### UCCX COP는 언제 설치합니까?

- 자체 서명 인증서를 사용하고 에이전트가 추가 인증서를 수락하지 않도록 하는 경우
- CA에서 서명한 추가 인증서를 가져올 수 없는 경우

### SM COP는 언제 설치합니까?

- 자체 서명 인증서를 사용하고 에이전트가 추가 인증서를 수락하지 않도록 하는 경우
- CA에서 서명한 추가 인증서를 가져올 수 없는 경우
- RSA로만 ECDSA 인증서를 서명할 수 있는 CA가 있는 경우

기본적으로 다른 웹 서버 인스턴스에서 제공하는 인증서는 무엇입니까?

인증서 조합/웹 서버	11.5로 업그레이드 후 기본 에이전트 환경 (복사 없음)	UCCX Tomcat	UCCX Openfire(Cisco Unified CCX Notification Service)	UCCX 소켓IO	SocialMiner Tomcat	SocialMiner Openfire
자체 서명 Tomcat, 자체 서명 Tomcat-ECDSA	에이전트는 Live Data 가젯 및 채팅 이메일 가젯에서 인증서를 수락하도록 요청받습니다. 에이전트는 Finesse 및 Live Data를 사용할 수 있지만 이메일 채팅 가젯이 로드되지 않습니다.	자체 서명	자체 서명	자체 서명	자체 서명	자체 서명
RSA CA 서명 Tomcat, RSA CA 서명 Tomcat-ECDSA	에이전트는 Finesse 및 Live Data를 사용할 수 있지만 이메일 채팅 가젯이 로드되지 않습니다.*	RSA	RSA	RSA	RSA	RSA(cop 설치 필요 - <a href="https://www.cisco.com/c/enr/td/docs/conceptual/ucx/11.5/ucx_cop_installation.html">CSCvb58580</a> )
RSA CA 서명 Tomcat, EC CA 서명 Tomcat-ECDSA	에이전트는 라이브 데이터 및 채팅 이메일과 함께 Finesse를 사용할 수 있습니다.*	RSA	RSA	ECDSA	RSA	ECDSA
RSA CA 서명 Tomcat, 자체 서명 Tomcat-ECDSA	에이전트는 Live Data 및 이메일 채팅 가젯에서 추가 인증서를 수락하도록 요청받	RSA	RSA	자체 서명(상당원은 브라우저 강제 보안 조치로 인해 수락할 수 없습니다. 위의 스크린샷을	RSA	자체 서명

습니다.  
Live Data 가  
젯의 인증서를  
수락하지 못했  
습니다. 이메  
일 채팅 가젯  
의 인증서를  
수락합니다.\*

참조하십시오.  
클라이언트에  
제공된 ECDSA  
인증서를 비활  
성화하려면 EC  
CA에서 서명한  
인증서를 가져  
오거나  
UCCX에 사본  
을 설치해야 합  
니다.)

## 관련 정보

- UCCX ECDSA COP - [https://software.cisco.com/download/release.html?mdfid=286309734&softwareid=280840578&release=11.5\(1\)&flowid=80822](https://software.cisco.com/download/release.html?mdfid=286309734&softwareid=280840578&release=11.5(1)&flowid=80822)
- SocialMiner ECDSA COP - [https://software.cisco.com/download/release.html?mdfid=283613136&flowid=73189&release=11.5\(1\)&softwareid=283812550&sortparam=](https://software.cisco.com/download/release.html?mdfid=283613136&flowid=73189&release=11.5(1)&softwareid=283812550&sortparam=)
- UCCX 인증서 정보 - <http://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html>