보안 설정 구성

보안 개요

이 장에는 IM and Presence 서비스의 보안 설정을 구성하는 절차가 포함되어 있습니다. IM and Presence 서비스에서 보안 TLS 연결을 구성하고 FIPS 모드와 같은 향상된 보안 설정을 활성화할 수 있습니다.

IM and Presence 서비스는 Cisco Unified Communications Manager와 플랫폼을 공유합니다. Cisco Unified Communications Manager에서 보안을 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오.

보안 설정 구성 작업 흐름

IM and Presence 서비스로 보안을 설정하려면 이 선택적 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	로그인 배너 만들기, 2 페이지	IM and Presence 서비스 인터페이스에 로그인할 때 사용자가 확인해야 하는 로그인 배너를 만듭니다.
단계 **2**	보안 XMPP 연결 구성 , 2 페이지	XMPP 보안을 구성하려면 이 작업을 완료하십시오.
단계 **3**	TLS 피어 주체 구성, 3 페이지	TLS 피어를 설정하려면 이 작업을 구성하십시오.
단계 **4**	TLS 컨텍스트 구성, 4 페이지	TLS 피어에 대한 TLS 컨텍스트 및 TLS 암호를 구성합니다.

	명령 또는 동작	목적
단계 **5**	FIPS 모드, 5 페이지	구축이 FIPS와 호환되도록 하려면 FIPS 모드를 활성화할 수 있습니다. 보안을 강화하기 위해 향상된 보안 모드 및 일반 준수 모드를 활성화할 수도 있습니다.

로그인 배너 만들기

사용자가 IM and Presence 서비스 인터페이스에 로그인할 때 표시되는 배너를 만들 수 있습니다. 텍스트 편집기를 사용하여 .txt 파일을 만들고, 사용자에게 전달할 중요한 알림을 포함하고, Cisco Unified IM and Presence OS 관리 페이지에 업로드하면 됩니다.

이 배너는 모든 IM and Presence 서비스 인터페이스에 표시되어, 사용자가 로그인하기 전에 법적 고지 사항을 비롯한 중요한 정보를 알립니다. 사용자가 로그인하기 전에 Cisco Unified CM IM and Presence 관리, Cisco Unified IM and Presence Operating System 관리, Cisco Unified IM and Presence 서비스 가용성, Cisco Unified IM and Presence 보고, IM and Presence 재해 복구 시스템 등의 인터페이스에 이 배너가 표시됩니다.

프로시저

단계 **1** .txt 파일을 만들고 배너에 표시할 내용을 작성합니다.

단계 **2** Cisco Unified IM and Presence Operating System 관리에 로그인합니다.

단계 **3** 소프트웨어 업그레이드 > 사용자 정의 로그온 메시지를 선택합니다.

단계 **4** 찾아보기를 클릭하여 .txt 파일을 찾습니다.

단계 **5** 파일 업로드를 클릭합니다.

대부분의 IM and Presence 서비스 인터페이스에서 로그인 전후에 배너가 나타납니다.

참고 각 IM and Presence 서비스 노드에 .txt 파일을 별도로 업로드해야 합니다.

보안 **XMPP** 연결 구성

이 절차를 사용하여 TLS를 사용하여 보안 XMPP 연결을 활성화하십시오.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 시스템 > 보안 > 설정을 선택합니다.

단계 **2** 다음 XMPP 보안 설정을 활성화하려면 해당 확인란을 선택하십시오.

표 *1: IM and Presence* 서비스에 대한 *XMPP* 보안 설정

설정	설명
IM/P 서비스 보안 모드에 대해 XMPP 클라이언트 활성화	이 기능을 활성화하면 IM and Presence 서비스가 클러스터의 XMPP 클라이언트 애플리케이션과의 보안 TLS 연결을 설정합니다. 이 설정은 기본적으로 활성화됩니다. XMPP 클라이언트 애플리케이션이 비보안 모드에서 클라이언트 로그인 자격 증명을 보호할 수 없다면 이 보안 모드를 해제하지 않는 것이 좋습니다. 보안 모드를 해제하는 경우 다른 방식으로 XMPP 클라이언트-노드 통신을 보호할 수 있는지 확인하십시오.
XMPP 라우터 대 라우터 보안 모드 활성화	이 설정을 활성화하면 IM and Presence 서비스는 동일한 클러스터 또는 다른 클러스터의 XMPP 라우터 간에 TLS 보안 연결을 설정합니다. IM and Presence 서비스는 클러스터 내부와 클러스터 간에 XMPP 인증서를 XMPP 신뢰 인증서로서 자동 복제합니다. XMPP 라우터는 동일한 클러스터 또는 다른 클러스터에 있으며 TLS 연결 설정이 가능한 다른 XMPP 라우터와 TLS 연결을 설정하려고 시도합니다.
IM/P 서비스 보안 모드에 대해 웹 클라이언트 활성화	이 설정을 활성화하면 IM and Presence 서비스는 IM and Presence 서비스 노드와 XMPP 기반 API 클라이언트 애플리케이션 간에 TLS 보안 연결을 설정합니다. 이 설정을 사용하는 경우 IM and Presence 서비스의 cup-xmpp-trust 저장소에 웹 클라이언트용 인증서 또는 서명 인증서를 업로드하십시오.

단계 **3** 저장을 클릭합니다.

다음에 수행할 작업

IM/P 서비스 보안 모드에 대해 **XMPP** 클라이언트 활성화 설정을 업데이트한 경우 Cisco XCP Connection Manager를 다시 시작합니다.

IM and Presence 서비스에서 SIP 보안 설정 구성

TLS 피어 주체 구성

IM and Presence 서비스 인증서 가져오기가 완료되면 IM and Presence 서비스는 자동으로 TLS 피어 주체를 TLS 피어 주체 목록 및 TLS 컨텍스트 목록에 추가하려고 시도합니다. TLS 피어 주체 및 TLS 컨텍스트 구성이 요구 사항에 맞게 설정되었는지 확인하십시오.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 시스템 > 보안 > **TLS** 피어 주체를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 피어 주체 이름에 대해 다음 작업 중 하나를 수행합니다.

a) 노드가 제공하는 인증서의 주체 CN을 입력합니다.

b) 인증서를 열고 CN을 찾아 여기에 붙여 넣습니다.

단계 **4** 설명 필드에 노드의 이름을 입력합니다.

단계 **5** 저장을 클릭합니다.

다음에 수행할 작업

계속 진행하여 TLS 컨텍스트를 구성합니다.

TLS 컨텍스트 구성

이 절차를 사용하여 TLS 컨텍스트와 TLS 암호를 TLS 피어 주체에 할당합니다.

참고 IM and Presence 서비스 인증서 가져오기가 완료되면 IM and Presence 서비스는 자동으로 TLS 피어 주체를 TLS 피어 주체 목록 및 TLS 컨텍스트 목록에 추가하려고 시도합니다.

시작하기 전에

TLS 피어 주체 구성, 3 페이지

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 시스템 > 보안 > **TLS** 컨텍스트 구성을 선택합니다.

단계 **2** 찾기를 클릭합니다.

단계 **3** **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**를 선택합니다.

단계 **4** 사용 가능한 TLS 피어 주체의 목록에서 자신이 구성한 TLS 피어 주체를 선택합니다.

단계 **5** > 화살표를 사용하여 이 TLS 피어 주체를 선택한 **TLS** 피어 주체로 이동합니다.

단계 **6** **TLS** 암호화 매핑 옵션을 구성합니다.

a) 사용 가능한 **TLS** 암호 및 선택한 **TLS** 암호 상자에서 사용할 수 있는 TLS 암호화 목록을 검토합니다.

b) 현재 선택되지 않은 TLS 암호를 활성화하려면 > 화살표를 사용하여 암호를 선택한 **TLS** 암호로 이동합니다.

단계 **7** 저장을 클릭합니다.

단계 **8** Cisco SIP Proxy 서비스를 다시 시작합니다.

a) Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

b) 서버 드롭다운 목록 상자에서 IM and Presence 서비스 클러스터 노드를 선택하고 이동을 클릭합니다.

c) **Cisco SIP Proxy** 서비스를 선택하고 다시 시작을 클릭합니다.

FIPS 모드

IM and Presence 서비스에는 시스템이 암호화, 데이터와 신호 암호화 및 감사 로깅과 같은 항목과 관련된 보다 엄격한 보안 지침 및 위험 관리 제어에서 작동할 수 있도록 하는 향상된 시스템 보안 모드 세트가 포함되어 있습니다

- FIPS 모드 - IM and Presence 서비스는 FIPS 모드에서 작동하도록 구성할 수 있습니다. FIPS 모드는 미국 및 캐나다 정부의 암호화 모듈 표준인 FIPS 또는 연방 정보 처리 표준을 준수합니다.
- 향상된 보안 모드 - 향상된 보안 모드는 FIPS 지원 시스템에서 실행되며 데이터 암호화 요구 사항, 엄격한 자격 증명 정책, 연락처 검색에 대한 사용자 인증 및 보다 엄격한 감사 로깅 요구 사항과 같은 추가 위험 관리 제어 기능을 제공합니다.
- 공통 기준 모드 - 공통 기준 모드는 시스템이 TLS 및 X.509 v3 인증서 사용과 같은 공통 기준 지침을 준수할 수 있도록 하는 추가 제어 기능을 제공하는 FIPS 지원 시스템에서도 실행됩니다.

참고 외부 데이터베이스가 MSSQL인 경우 메시지 아카이버, 텍스트 전화 회의 관리자 및 파일 전송 관리자와 같은 서비스가 일반 기준 모드에서 작동하려면 다음을 수행해야 합니다.

1. TLS 1.1 이상을 지원하도록 MSSQL 데이터베이스를 호스팅하는 서버를 구성합니다.
2. IM and Presence 서비스에 데이터베이스 인증서를 다시 업로드합니다.
3. 외부 데이터베이스 구성 페이지에서 **SSL** 활성화 확인란을 선택합니다. **Cisco Unified CM IM and Presence** 관리 > 메시징 > 외부 서버 설정 > 외부 데이터베이스를 선택하여 외부 데이터베이스를 구성합니다.

Cisco Unified Communicatiosn Manager 및 IM and Presence 서비스에서 FIPS 모드, 보안 강화 모드 및 공통 기준 모드를 활성화하는 방법에 대한 자세한 내용은 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html 에서 *Cisco Unified Communications Manager* 보안 설명서의 "FIPS 모드 설정" 장을 참조하십시오.

Microsoft Outlook 일정 통합용 FIPS

IM and Cisco Presence 서비스 서버에서 FIPS 모드가 활성화된 경우 Exchange 웹 서비스 정보를 가져올 수 있도록 NTLMv2만 지원됩니다. FIPS 모드가 비활성화된 경우 NTLMv1과 NTLMv2 모두 기존 동작에 따라 지원됩니다. 기본 인증은 FIPS 모드를 활성화 또는 비활성화하는 것과 관계 없이 두 경우 모두 지원됩니다.

Microsoft Outlook 일정 통합 기능을 통해 Exchange Server와의 연결을 설정하기 위해 프레즌스 엔진에서 사용하는 인증 유형을 확인하기 위해 **FIPS** 모드 **Exchange Server** 인증이라는 프레즌스 엔진 서비스에 대한 새 서비스 매개 변수가 도입되었습니다.

FIPS 모드 **Exchange Server** 인증 서비스 매개 변수를 자동 또는 기본 전용으로 설정할 수 있습니다.

자동으로 설정된 서비스 매개 변수: 프레즌스 엔진이 NTLMv2를 먼저 협상하고 NTLMv2 협상이 실패할 경우에만 "기본 인증"으로 대체합니다. NTLMv1는 FIPS 모드에서 협상되지 않습니다.

기본 전용으로 설정된 서비스 매개 변수: Exchange Server가 NTLM 및 기본 인증을 모두 허용하도록 구성되어 있더라도 프레즌스 엔진은 강제로 "기본 인증"을 사용합니다.

참고 서비스 매개 변수 설정을 변경하면 Cisco 프레즌스 엔진을 다시 시작해야 합니다.