Cisco Unified Communications Manager 및 IM and Presence 서비스용 관리 가이드, 릴리스 12.0(1)

초판: 2017년 08월 23일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이센스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이센스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 University of Berkeley(UCB)에서 개발된 프로그램을 적용하여 구현합니다. 모든 권리는 저작권자의 소유입니다. Copyright © 1981, Regents of the University of California.

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급업체의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에서 언급한 공급자는 상품성, 특정 목적에의 적합성 및 비침해에 대한 보증을 포함하되 이에 제한되지 않으며 거래 과정, 사용 또는 거래 관행으로부터 발생되는 모든 명시적이거나 묵시적인 보증을 부인합니다.

CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco 및/또는 해당 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 보려면 다음 URL을 방문하십시오. http://www.cisco.com/go/trademarks 여기에 언급된 타사 상표는 해당 소유권자의 자산입니다. 파트너라는 용어의 사용이 Cisco와 다른 업체 사이의 제휴 관계를 의미하는 것은 아닙니다. (1110R)

목 차

부

관리 개요

1 장

관리 개요

Cisco Unified CM 관리 개요

웹 기반 애플리케이션인 Cisco Unified CM 관리는 Cisco Unified Communications Manager의 기본 관리 및 구성 인터페이스입니다. 일반 시스템 구성 요소, 기능, 서버 설정, 통화 라우팅 규칙, 전화기, 최종 사용자 및 미디어 리소스를 포함하여 시스템에 대한 광범위한 항목을 구성하는 데 Cisco Unified CM 관리를 사용할 수 있습니다.

구성 메뉴

Cisco Unified CM 관리의 [구성] 창은 다음 메뉴로 구성되어 있습니다.

- 시스템—이 메뉴의 구성 창을 사용하여 서버 정보, NTP 설정, 날짜 및 시간 그룹, 지역, DHCP, LDAP 통합 및 엔터프라이즈 매개 변수 등 일반 시스템 설정을 구성합니다.
- 통화 라우팅—이 탭의 구성 창을 사용하여 경로 패턴, 경로 그룹, 헌트 파일럿, 다이얼 규칙, 파티션, 발신 검색 공간, 디렉터리 번호 및 변환 패턴을 포함하여 Cisco Unified Communications Manager가 통화를 전송하는 방식과 관련된 항목을 구성합니다.
- 미디어 리소스—이 탭의 구성 창을 사용하여 미디어 리소스 그룹, 컨퍼런스 브리지, 알림 장치 및 트랜스코더와 같은 항목을 구성합니다.
- 고급 기능—이 탭의 구성 창을 사용하여 음성 메일 파일럿, 메시지 대기 및 통화 제어 에이전트 프로파일 같은 기능을 구성합니다.

- 장치—이 탭의 구성 창을 사용하여 전화기, IP 전화 서비스, 트렁크, 게이트웨이, 소프트키 템플릿 및 SIP 프로파일 등의 장치를 설정합니다.
- 애플리케이션—이 탭의 구성 창을 사용하여 Cisco Unified JTAPI, Cisco Unified TAPI 및 Cisco Unified Real-Time Monitoring Tool 같은 플러그인을 다운로드하고 설치합니다.
- 사용자 관리—사용자 관리 탭의 구성 창을 사용하여 시스템의 최종 사용자와 시스템 애플리케이션 사용자를 구성합니다.
- 벌크 관리—벌크 관리 도구를 사용하여 한 번에 많은 수의 최종 사용자 또는 장치를 가져오고 구성합니다.
- 도움말—이 메뉴를 클릭하여 온라인 도움말 시스템에 액세스합니다. 온라인 도움말 시스템에는 사용자 시스템에서 다양한 구성 창에 대한 설정을 구성하는 데 도움이 되는 설명서가 포함되어 있습니다.

운영 체제 관리 개요

Cisco Unified Communications 운영 체제 관리를 사용하여 운영 체제를 구성 및 관리하고 다음 관리 작업을 수행합니다.

- 소프트웨어 및 하드웨어 상태 확인
- IP 주소 확인 및 업데이트
- 다른 네트워크 장치 Ping
- NTP 서버 관리
- 시스템 소프트웨어 및 옵션 업그레이드
- IPsec 및 인증서를 포함하여 노드 보안 관리
- 원격 지원 계정 관리
- 시스템 다시 시작

운영 체제 상태

다음을 포함한 다양한 운영 체제 구성 요소의 상태를 확인할 수 있습니다.

- 클러스터 및 노드
- 하드웨어
- 네트워크
- 시스템
- 설치된 소프트웨어 및 옵션

운영 체제 설정

다음과 같은 운영 체제 설정을 보고 업데이트할 수 있습니다.

- IP—애플리케이션을 설치할 때 입력한 IP 주소와 DHCP 클라이언트 설정을 업데이트합니다.
- NTP 서버 설정—외부 NTP 서버의 IP 주소를 구성하고 NTP 서버를 추가합니다.
- SMTP 설정—이메일 알림을 보내기 위해 운영 체제가 사용할 SMTP(Simple Mail Transfer Protocol) 호스트를 구성합니다.

운영 체제 보안 구성

보안 인증서와 IPsec 설정을 관리할 수 있습니다. 보안 메뉴에서 다음 보안 옵션을 선택할 수 있습니다.

- 인증서 관리—인증서와 인증서 서명 요청(CSR)을 관리합니다. 인증서를 표시, 업로드, 다운로드, 삭제 및 다시 생성할 수 있습니다. 인증서 관리를 통해 노드에서 인증서의 만료 날짜를 모니터링할 수도 있습니다.
- IPsec 관리—기존 IPsec 정책을 표시하거나 업데이트하고 새 IPsec 정책 및 연결을 설정합니다.

소프트웨어 업그레이드

운영 체제를 실행 중인 소프트웨어 버전을 업그레이드하거나 또는 Cisco Unified Communications 운영 체제 로캘 설치 프로그램, 다이얼 플랜 및 TFTP 서버 파일을 포함한 특정 소프트웨어 옵션을 설치할 수 있습니다.

설치/업그레이드 메뉴 옵션에서 로컬 디스크 또는 원격 서버에서 시스템 소프트웨어를 업그레이드할 수 있습니다. 업그레이드된 소프트웨어가 비활성 파티션에 설치되고 시스템을 다시 시작하고 파티션을 전환할 수 있으므로 시스템은 최신 소프트웨어 버전에서 실행을 시작합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html에서 *Cisco Unified Communications Manager* 업그레이드 가이드를 참조하십시오.

참고 Cisco Unified Communications Operating System 인터페이스 및 CLI에 포함된 소프트웨어 업그레이드 기능을 통해 모든 소프트웨어 설치와 업그레이드를 수행해야 합니다. 시스템은 Cisco Systems가 승인한 소프트웨어만 업로드 및 처리할 수 있습니다. 승인되지 않은 타사 또는 Windows 기반 소프트웨어 애플리케이션을 설치하거나 사용할 수는 없습니다.

서비스

애플리케이션은 다음과 같은 운영 체제 유틸리티를 제공합니다.

- Ping—다른 네트워크 장치와의 연결을 확인합니다.
- 원격 지원—Cisco 기술 지원 담당자가 시스템에 액세스하는 데 사용할 수 있는 계정을 설정합니다. 이 계정은 사용자가 지정한 일수가 지나면 자동으로 만료됩니다.

CLI

CLI는 운영 체제에서 또는 서버에 대한 보안 셸 연결을 통해 액세스할 수 있습니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

인증 네트워크 시간 프로토콜 지원

이 릴리스에서는 Cisco Unified Communications Manager를 위한 인증된 NTP(Network Time Protocol) 기능이 지원됩니다. 이 지원은 Cisco Unified Communications Manager에 대한 보안 NTP 서버 연결에 추가됩니다. 이전 릴리스에서 NTP 서버에 대한 Cisco Unified Communications Manager 연결은 보호되지 않았습니다.

이 기능은 대칭 키 기반 인증을 기반으로 하며 NTPv3 및 NTPv4 서버에 의해 지원됩니다. Cisco Unified Communications Manager는 SHA1 기반 암호화만 지원합니다. SHA1 기반 대칭 키 지원은 NTP 버전 4.2.6 이상에서 사용할 수 있습니다.

- 대칭 키
- 인증 없음

Cisco Unified OS 관리 애플리케이션의 관리 CLI 또는 **NTP** 서버 목록 페이지를 통해 NTP 서버의 인증 상태를 확인할 수 있습니다.

Cisco Unified Serviceability 개요

Cisco Unified Serviceability는 다양한 서비스, 알림 및 관리자의 시스템 관리에 도움이 되는 도구를 제공하는 웹 기반 문제 해결 도구입니다. Cisco Unified Serviceability가 관리자에게 제공하는 기능은 다음과 같습니다.

- 시작 및 중지 서비스--관리자가 시스템을 관리하는 데 도움이 되는 서비스를 설정할 수 있습니다. 예를 들어, 관리자가 실시간 모니터링 도구를 사용하여 시스템의 상태를 모니터링할 수 있도록 Cisco CallManager Serviceability RTMT 서비스를 시작할 수 있습니다.
- SNMP—SNMP를 사용하면 노드, 라우터 등과 같은 네트워크 장치 간에 관리 정보를 교환하기 쉽습니다. TCP/IP 프로토콜의 일부로 SNMP를 사용하면 관리자가 네트워크 성능을 원격 관리하고 네트워크 문제를 찾아 해결하며 네트워크 확장을 계획할 수 있습니다.
- 알람—시스템과 관련된 문제를 해결할 수 있도록 알람은 런타임 상태 및 시스템 상태 정보를 제공합니다.
- 추적—추적 도구는 음성 애플리케이션으로 문제를 해결하는 데 도움이 됩니다.
- Cisco Serviceability Reporter—Cisco Serviceability Reporter는 Cisco Unified Serviceability에서 일별 보고서를 생성합니다.
- SNMP—SNMP를 사용하면 노드, 라우터 등과 같은 네트워크 장치 간에 관리 정보를 교환하기 쉽습니다. TCP/IP 프로토콜의 일부로 SNMP를 사용하면 관리자가 네트워크 성능을 원격 관리하고 네트워크 문제를 찾아 해결하며 네트워크 확장을 계획할 수 있습니다.

- CallHome—Cisco Unified Communications Manager가 진단 경고, 재고 및 기타 메시지를 Smart Call Home 백엔드 서버와 통신하고 전송할 수 있도록 Cisco Unified Communications Manager Call Home 기능을 구성합니다.

추가 관리 인터페이스

Cisco Unified Serviceability를 사용하여 다음과 같은 추가 관리 인터페이스를 사용할 수 있는 서비스를 시작할 수 있습니다.

- 실시간 모니터링 도구—실시간 모니터링 도구는 시스템의 상태를 모니터링할 수 있는 웹 기반 인터페이스입니다. RTMT를 사용하여 시스템의 상태에 대한 자세한 정보를 포함하는 알람, 카운터 및 보고서를 볼 수 있습니다.
- Dialed Number Analyzer—Dialed Number Analyzer는 관리자가 다이얼 플랜 문제를 해결하는 데 도움이 되는 웹 기반 인터페이스입니다.
- Cisco Unified CDR Analysis and Reporting-CDR Analysis and Reporting은 시스템에서 건 통화의 세부 정보를 보여주는 통화 상세 내역 레코드를 수집합니다.

Cisco Unified Serviceability를 사용하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Serviceability* 관리 설명서를 참조하십시오.

Cisco Unified Reporting 개요

Cisco Unified Communications Manager 및 Cisco Unified Communications Manager IM and Presence Service 콘솔에 액세스할 수 있는 Cisco Unified Reporting 웹 애플리케이션은 클러스터 데이터 문제 해결 또는 검사를 위해 통합된 보고서를 생성합니다.

이 도구는 클러스터 데이터의 스냅샷을 얻는 간단한 방법을 제공합니다. 이 도구는 기존 소스에서 데이터를 수집하고 데이터를 비교하며 불규칙성을 보고합니다. Cisco Unified Reporting에서 보고서를 생성하면 보고서는 하나 이상의 서버에 있는 하나 이상의 소스의 데이터를 하나의 출력 보기로 결합합니다. 예를 들어, 시스템을 관리하는 데 도움이 되는 다음 보고서를 볼 수 있습니다.

- Unified CM 클러스터 개요—이 보고서를 보고 Cisco Unified Communications Manager 및 IM and Presence 서비스 버전, 서버 호스트 이름 및 하드웨어 세부 사항을 포함하여 클러스터의 스냅샷을 얻을 수 있습니다.
- 전화기 기능 목록—기능을 구성하는 경우 이 보고서를 봅니다. 이 보고서는 전화기가 어느 Cisco Unified Communications Manager 기능을 지원하는지 보여주는 목록을 제공합니다.
- 회선 없는 Unified CM 전화기—클러스터에 있는 전화기에 전화기 회선이 없는지 보려면 이 보고서를 봅니다.

Cisco Unified Reporting을 통해 제공되는 보고서의 전체 목록과 애플리케이션을 사용하는 방법에 대한 지침은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에 있는 *Cisco Unified Reporting* 관리 설명서를 참조하십시오.

재난 복구 시스템 개요

Cisco Unified Communications Manager 관리에서 호출할 수 있는 재난 복구 시스템(DRS)은 전체 데이터 백업 및 복원 기능을 제공합니다. 재난 복구 시스템을 사용하면 정기적으로 예약된 자동 또는 사용자가 호출한 데이터 백업을 수행할 수 있습니다.

DRS은 플랫폼 백업/복원의 일환으로 자체 설정(백업 장치 설정 및 예약 설정)을 복원합니다. DRS는 `drfDevice.xml` 및 `drfSchedule.xml` 파일을 백업 및 복원합니다. 이러한 파일로 서버가 복원되면 DRS 백업 장치 및 일정을 다시 구성할 필요가 없습니다.

재난 복구 시스템에는 다음과 같은 기능이 포함됩니다.

- 백업 및 복원 작업을 수행하기 위한 사용자 인터페이스.
- 백업 및 복원 기능을 수행하기 위해 분산된 시스템 아키텍처.
- 예약된 백업.
- 실제 테이프 드라이브 또는 원격 SFTP 서버에 백업을 보관합니다.

벌크 관리 도구 개요

Cisco Unified CM 관리에서 [벌크 관리] 메뉴와 하위 메뉴 옵션을 사용하면 Bulk Administration Tool 사용을 통해 Cisco Unified Communications Manager의 항목을 구성할 수 있습니다.

Cisco Unified Communications Manager BAT(Bulk Administration Tool)는 웹 기반 애플리케이션으로, 관리자가 Cisco Unified Communications Manager 데이터베이스에 대한 벌크 트랜잭션을 수행할 수 있도록 합니다. BAT에서는 다수의 유사한 전화기, 사용자 또는 포트를 동시에 추가, 업데이트 또는 삭제할 수 있습니다. Cisco Unified CM 관리를 사용하는 경우 데이터베이스 트랜잭션마다 개별 수동 작업이 필요한 반면, BAT에서는 프로세스가 자동화되어 추가, 업데이트 및 삭제 작업을 더 빨리 수행할 수 있습니다.

BAT를 사용하여 다음과 같은 유형의 장치 및 레코드 작업을 수행할 수 있습니다.

- Cisco Unified IP Phone, 게이트웨이, 전화기, CTI(컴퓨터 텔레포니 인터페이스) 포트 및 H.323 클라이언트 추가, 업데이트 및 삭제
- 사용자, 사용자 자치 프로파일, Cisco Unified Communications Manager Assistant 관리자 및 보조자 추가, 업데이트 및 삭제
- 강제 인증 코드(Forced Authorization Code) 및 클라이언트 매터 코드(Client Matter Code) 추가 또는 삭제
- 통화 당겨받기 그룹 추가 또는 삭제
- 지역 매트릭스 채우기/채우기 취소
- 액세스 목록 삽입, 삭제 또는 내보내기
- 원격 대상/원격 대상 프로파일 삽입, 삭제 또는 내보내기
- 인프라 장치 추가

벌크 관리 도구를 사용하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.

2 장

시작하기

관리 인터페이스에 로그인

이 절차를 수행하여 시스템의 관리 인터페이스 중 하나에 로그인합니다.

절차

단계 **1** 웹 브라우저에서 Unified Communications Manager 인터페이스를 엽니다.
단계 **2** 탐색 드롭다운 목록에서 관리 인터페이스를 선택합니다.
단계 **3** 이동을 클릭합니다.
단계 **4** 사용자 이름과 암호를 입력합니다.
단계 **5** 로그인을 클릭합니다.

관리자 또는 보안 암호 재설정

관리자 암호를 잊어버려 시스템에 액세스할 수 없는 경우 다음 절차를 수행하여 암호를 다시 설정할 수 있습니다.

시작하기 전에

- 이 절차를 수행하는 노드에 실제로 액세스해야 합니다.

- 언제든지, CD 또는 DVD 미디어를 삽입할 것을 요청하면 VMWare 서버용 vSphere Client를 통해 ISO 파일을 마운트해야 합니다. 안내서는 여기에 있는 "가상 머신에 DVD 또는 CD 드라이브 추가"를 참조하십시오.
- 클러스터의 모든 노드에서 보안 암호가 일치해야 합니다. 모든 시스템의 보안 암호를 변경하십시오. 그렇지 않으면 클러스터 노드가 통신되지 않습니다.

절차

단계 **1** 다음과 같은 사용자 이름과 암호로 게시자 노드의 CLI에 로그인합니다.

a) 사용자 이름: pwrecovery

b) 암호: pwreset

단계 **2** 아무 키나 눌러 계속합니다.

단계 **3** 디스크 드라이브에 올바른 CD/DVD가 있거나 ISO 파일을 마운트했으면 VMWare 클라이언트에서 제거합니다.

단계 **4** 아무 키나 눌러 계속합니다.

단계 **5** 드라이브에 유효한 CD 또는 DVD를 삽입하거나 ISO 파일을 마운트합니다.

참고 이 테스트에는 데이터일 뿐인 ISO 파일이나 디스크를 사용해야 합니다.

단계 **6** 시스템이 마지막 단계를 확인하고 나면 다음 옵션 중 한 가지를 입력하여 계속 진행하라는 메시지가 표시됩니다.

- 관리자 암호를 재설정하려면 **a**를 입력합니다.
- 보안 암호를 재설정하려면 **s**를 입력합니다.

  참고 보안 암호를 변경한 후 클러스터에서 각 노드를 재설정해야 합니다. 노드를 재부팅하지 못하면 시스템 서비스 문제 및 가입자 노드의 관리 창에서 문제가 발생합니다.

단계 **7** 새 암호를 입력한 다음 다시 암호를 입력하여 확인합니다.

관리자 자격 증명은 반드시 영문자로 시작해야 하며 최소 여섯 글자 이상이어야 하고 영숫자, 하이픈과 밑줄을 포함할 수 있습니다.

단계 **8** 시스템이 새 암호의 강도를 확인하면 암호가 재설정되고 아무 키나 눌러 암호 재설정 유틸리티를 종료하라는 메시지가 표시됩니다.

다른 관리자 암호를 설정하려면 **set password** CLI 명령을 사용합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

시스템 종료 또는 다시 시작

예를 들어, 구성 변경 사항을 작성한 후, 시스템을 종료하거나 다시 시작해야 할 경우 이 절차를 따르십시오.

시작하기 전에

가상 머신에서 서버를 종료하고 다시 시작해야 하는 경우에는 파일 시스템이 손상된 것일 수 있습니다. 강제 종료를 피합니다. 대신, 이 절차 후 또는 CLI에서 **utils system shutdown**을 실행한 후 서버가 적절하게 종료되기를 기다립니다.

절차

단계 **1** Cisco Unified OS 관리에서설정 > 버전을 선택합니다.

단계 **2** 다음 작업 중 하나를 수행합니다.

- 모든 프로세스를 중지하고 시스템을 종료하려면 종료를 클릭합니다.
- 모든 프로세스를 중지하고 시스템을 다시 시작하려면 다시 시작을 클릭합니다.

II 부

사용자 관리

3 장

사용자 액세스 관리

사용자 액세스 개요

최종 사용자에게 다음 항목을 할당하여 Cisco Unified Communications Manager에 대한 사용자 액세스를 관리할 수 있습니다.

- 역할
- 액세스 제어 그룹
- 사용자 순위

역할, 액세스 제어 그룹 및 사용자 정의 순위 컨트롤은 Cisco Unified Communications Manager에 여러 보안 수준을 제공합니다. 각 역할은 Cisco Unified Communications Manager 내의 특정 리소스에 대한 권한 집합을 정의합니다. 액세스 제어 그룹에 역할을 할당한 다음 해당 액세스 제어 그룹에 최종 사용자를 할당하면 이러한 최종 사용자에게 역할에 의해 정의된 모든 액세스 권한을 부여합니다.

사용자 순위 프레임워크는 역할 및 액세스 제어 그룹 프레임워크를 오버레이하고 최종 사용자가 어떤 그룹을 사용할 수 있는지 제어합니다. 최종 사용자 및 애플리케이션 사용자는 사용자 순위가 허용하는 액세스 제어 그룹에만 할당할 수 있습니다.

역할 개요

최종 사용자를 프로비저닝할 때 사용자에게 할당하는 역할을 결정해야 합니다. 최종 사용자, 애플리케이션 사용자 또는 액세스 제어 그룹에 역할을 할당할 수 있습니다. 단일 사용자에 여러 역할을 할당할 수 있습니다.

각 역할에는 특정 리소스 또는 애플리케이션에 연결된 권한 집합이 포함됩니다. 예를 들어, 표준 CCM 최종 사용자 역할은 해당 역할이 할당된 사용자에게 Cisco Unified Communications 셀프 케어 포털에 대한 액세스 권한을 제공합니다. 또한 Cisco Unified Communications Manager 관리, Cisco CDR Analysis and Reporting, Dialed Number Analyzer 및 CTI 인터페이스 같은 리소스에 대한 액세스 권한을 제공하는 역할도 할당할 수 있습니다. 특정 구성 창 같이 그래픽 사용자 인터페이스가 있는 대부분의 리소스의 경우 역할에 연결된 권한을 사용하면 해당 창 또는 관련된 창의 그룹에서 데이터를 보거나 업데이트할 수 있습니다.

역할 구성 및 할당

사용자에게 표준 역할을 할당하거나 사용자 정의 역할을 작성할지 여부를 결정해야 합니다.

- 표준 역할—표준 역할은 Cisco Unified Communications Manager에 설치된 미리 정의된 기본 역할입니다. 어떤 식으로든 권한을 편집하거나 역할을 수정할 수 없습니다.
- 사용자 정의 역할—사용자가 만든 사용자 정의 역할입니다. 사용자에게 할당하려는 권한이 포함된 표준 역할이 없는 경우 사용자 정의 역할을 만들 수 있습니다. 예를 들어, 표준 역할을 할당하고 싶지만, 권한 중 하나를 수정하려는 경우 표준 역할의 권한을 사용자 정의 역할에 복사한 다음 해당 사용자 정의 역할에서 권한을 편집할 수 있습니다.

권한 유형

각 역할에는 특정 리소스에 연결된 권한 집합이 포함됩니다. 리소스를 할당할 수 있는 권한은 두 가지 유형이 있습니다.

- 읽기—읽기 권한을 사용하면 사용자가 해당 리소스에 대한 설정을 볼 수 있지만 사용자 구성은 업데이트할 수 없습니다. 예를 들어, 권한을 사용하면 특정 구성 창에 대한 설정을 볼 수 있지만 해당 응용 프로그램에 대한 구성 창에는 업데이트 단추 또는 아이콘이 표시되지 않습니다.
- 업데이트—업데이트 권한을 사용하면 해당 리소스에 대한 설정을 수정할 수 있습니다. 예를 들어, 권한을 사용하여 특정 구성 창에서 업데이트할 수 있습니다.

최종 사용자 및 관리자 역할

표준 CCM 최종 사용자 역할은 최종 사용자에게 Cisco Unified Communications 셀프 케어 포털에 대한 액세스 권한을 제공합니다. CTI 액세스 같은 추가 권한이 필요한 경우 표준 CTI 활성화됨 역할 같은 추가 역할을 할당해야 합니다.

표준 CCM 관리 사용자 역할은 모든 관리 작업에 대한 기본 역할이며 인증 역할로 사용됩니다. 이 역할은 Cisco Unified Communications Manager 관리 사용자 인터페이스에 대한 관리 액세스를 제공합니다. Cisco Unified Communications Manager 관리는 Cisco Unified Communications Manager 관리에 로그인하는 데 필요한 역할로 이 역할을 정의합니다.

관련 항목

표준 역할 및 액세스 제어 그룹, 31 페이지

액세스 제어 그룹 개요

비슷한 액세스 요구 사항을 가진 그룹에 네트워크 액세스 권한을 빠르게 할당하기 위해 역할과 함께 액세스 제어 그룹을 사용할 수 있습니다.

액세스 제어 그룹은 최종 사용자 및 애플리케이션 사용자의 목록입니다. 필요한 역할과 권한을 포함하는 액세스 제어 그룹에 대한 액세스 요구 사항이 비슷한 최종 사용자 또는 애플리케이션 사용자를 할당할 수 있습니다. 액세스 제어 그룹에 할당할 최종 사용자 또는 애플리케이션 사용자의 경우 사용자는 해당 액세스 제어 그룹에 대한 최소 순위 요구 사항을 충족해야 합니다. 예를 들어, 사용자 순위가 4인 최종 사용자는 최소 순위 요구 사항이 4-10 사이인 액세스 제어 그룹에만 할당할 수 있습니다.

시스템은 미리 정의된 표준 액세스 제어 그룹의 집합을 포함하고 있습니다. 각 표준 액세스 제어 그룹에는 기본적으로 할당된 역할 집합이 있습니다. 이 액세스 제어 그룹에 사용자를 할당하면 해당 역할도 이 최종 사용자에게 할당됩니다.

표준 액세스 제어 그룹에 할당된 역할은 편집할 수 없습니다. 하지만, 사용자 정의된 액세스 제어 그룹을 만들고 사용자 정의된 액세스 제어 그룹에 사용자가 선택하는 역할을 할당할 수 있습니다.

관련 항목

표준 역할 및 액세스 제어 그룹, 31 페이지

사용자 순위 개요

사용자 순위 액세스 제어는 최종 사용자 또는 애플리케이션 사용자에게 관리자가 제공할 수 있는 액세스 수준에 대한 제어 집합을 제공합니다. 사용자 순위 매개 변수의 범위는 1-10의 정수이며 1이 가장 높은 순위입니다. 사용자 순위는 사용자 및 액세스 제어 그룹에 할당되므로 특정 액세스 제어 그룹에 할당할 수 있는 사용자를 관리하는 순위 계층을 만듭니다.

최종 사용자 또는 애플리케이션 사용자를 프로비저닝할 때 관리자는 각 사용자에 대한 사용자 순위를 할당해야 합니다. 또한 관리자는 각 액세스 제어 그룹에 사용자 순위를 할당해야 합니다. 관리자는 사용자에게 동일한 순위 또는 낮은 순위를 갖는 액세스 제어 그룹만 할당할 수 있습니다. 예를 들어, 최종 사용자의 사용자 순위가 3인 경우 사용자 순위가 3-10 사이인 액세스 제어 그룹에 할당할 수 있습니다. 해당 사용자는 사용자 순위가 1이어야 하는 액세스 제어 그룹에는 할당할 수 없습니다.

관리자는 사용자 순위 구성 창 내에서 사용자 순위 계층 구조를 사용자 정의한 다음 이러한 순위를 최종 사용자, 애플리케이션 사용자 및 액세스 제어 그룹에 할당할 수 있습니다.

사용자 액세스 필수 구성 요소

새 역할 또는 액세스 제어 그룹을 만들기 전에 시스템에 미리 설치된 표준 역할 및 액세스 제어 그룹을 검토하여 기존 액세스 제어 그룹에 사용자가 필요한 역할 및 권한이 포함되어 있는지 확인합니다.

자세한 내용은 표준 역할 및 액세스 제어 그룹, 31 페이지를 참조하십시오.

사용자 액세스 구성 작업 흐름

사용자 액세스를 구성하려면 다음 작업을 수행합니다.

절차

	명령 또는 동작	목적
단계 **1**	사용자 정의 사용자 순위 만들기, 21 페이지	사용자 정의 사용자 순위를 생성하여 사용자 순위 계층 구조를 설정합니다.
단계 **2**	다음 방법 중 하나를 사용하여 새 역할을 만듭니다. • 사용자 지정 역할 만들기, 21 페이지 • 역할 복사, 22 페이지	'만들기' 절차를 사용하여 처음부터 새 역할을 만들고 구성합니다. 새 역할에 표준 역할과 유사한 설정이 있는 경우 '복사' 명령을 사용합니다. 기존의 표준 역할에서 새 역할로 권한 설정을 복사할 수 있습니다. 그런 다음 새 역할에서 설정을 편집할 수 있습니다.
단계 **3**	다음 방법 중 하나를 사용하여 액세스 제어 그룹을 만듭니다. • 액세스 제어 그룹 만들기, 23 페이지 • 액세스 제어 그룹 복사, 23 페이지	'만들기' 절차를 사용하여 새 액세스 제어 그룹을 만들고 구성합니다. 새 액세스 제어 그룹이 기본 그룹 중 하나와 매우 비슷한 경우 '복사' 명령을 사용할 수 있습니다. 기존 그룹에서 새 그룹으로 역할 할당을 복사한 다음 편집할 수 있습니다.
단계 **4**	액세스 제어 그룹에 역할 할당, 24 페이지	역할을 추가 또는 삭제하여 액세스 제어 그룹에 할당된 역할을 업데이트합니다.
단계 **5**	액세스 제어 그룹에 사용자 할당, 25 페이지	그룹에서 사용자를 추가 또는 삭제하여 액세스 제어 그룹의 사용자 목록을 업데이트합니다. 그룹에 할당된 모든 사용자는 그룹에 할당된 역할에 구성된 권한을 사용합니다.
단계 **6**	사용자 권한 보고서 보기, 26 페이지	(선택 사항) 사용자에 대해 할당된 액세스 권한을 검토해야 하는 경우 해당 사용자의 권한 보고서를 보십시오.
단계 **7**	액세스 제어 그룹에 대한 권한 정책 중복 구성, 26 페이지	(선택 사항) Cisco Unified Communications Manager가 액세스 제어 그룹 할당에서 발생할 수 있는 중복 사용자 권한을 처리하는 방법을 구성합니다. 여기에서는 각각 역할 및 권한 설정이 충돌하는 상태에서 최종 사용자가 여러 액세스 제어 그룹에 할당된 상황을 처리합니다.
단계 **8**	사용자 지정 지원 센터 역할 작업 흐름 만들기, 27 페이지	(선택 사항) 일부 회사에서는 지원 센터 직원이 특정 관리 작업을 수행할 수 있도록 권한을 부여하기를 원합니다. 전화기를 추가하고 최종 사용자를 추가하는 등의 작

	명령 또는 동작	목적
		업을 수행할 수 있는 지원 센터 팀원을 위한 역할 및 액세스 제어 그룹을 구성합니다.
단계 **9**	액세스 제어 그룹 삭제, 30 페이지	(선택 사항) 시스템에서 액세스 제어 그룹을 삭제하는 경우 이 절차를 사용합니다.

사용자 정의 사용자 순위 만들기

순위 계층 구조에 대한 사용자 정의 사용자 순위를 만들려면 이 절차를 사용합니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 사용자 순위를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 사용자 순위 드롭다운 메뉴에서 1-10 사이의 순위 설정을 선택합니다. 가장 높은 순위는 1입니다.

단계 **4** 순위 이름 및 설명을 입력합니다.

단계 **5** 저장을 클릭합니다.

사용자 지정 역할 만들기

사용자 지정 역할을 만들고 해당 역할에 대한 권한을 구성하려면 이 절차를 수행합니다. 사용자에게 할당하려는 권한과 일치하는 시스템 정의 표준 역할이 없는 경우 사용자 정의 역할을 만들 수 있습니다.

절차

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자 설정 > 역할을 클릭합니다.

단계 **2** 애플리케이션 드롭다운 목록 상자에서 이 역할과 연결된 애플리케이션을 선택합니다.
역할 구성 창이 표시됩니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 이름 텍스트 상자에 역할의 이름을 입력합니다.
이름은 최대 128자로 구성될 수 있습니다. 올바른 문자에는 글자, 숫자, 대시, 점(마침표), 공백 및 밑줄이 포함됩니다.

단계 **5** 설명 텍스트 상자에 역할에 대한 설명을 입력합니다.
설명에는 최대 128자가 포함될 수 있습니다.

단계 **6** 새 역할의 각 리소스에 대해 다음과 같이 권한을 편집합니다.

- 역할에서 해당 리소스를 볼 수 있도록 하려면 읽기 확인란을 클릭합니다.
- 역할에서 해당 리소스를 편집할 수 있도록 하려면 업데이트 확인란을 클릭합니다.
- 역할에서 해당 리소스를 보고 편집할 수 있도록 하려면 읽기 및 업데이트 확인란을 모두 선택합니다.
- 역할에서 해당 리소스에 액세스하지 못하도록 하려면 두 확인란을 선택 취소합니다.

단계 **7** 모두에게 액세스 부여{ 또는 모두에게 액세스 거부 단추를 클릭하여 이 역할에 대해 페이지에 표시되는 모든 리소스에 대한 권한을 부여 또는 제거합니다.

참고 리소스 목록이 두 페이지 이상 표시되는 경우 이 단추는 현재 페이지에 표시되는 리소스에만 적용됩니다. 기타 페이지에 나열된 리소스의 액세스를 변경하려면 해당 페이지를 표시하고 해당 페이지에 있는 단추를 사용해야 합니다.

단계 **8** 저장을 클릭합니다.

다음에 할 작업

새 액세스 제어 그룹을 설정하려면 다음 절차 중 하나를 수행합니다.

- 액세스 제어 그룹 만들기, 23 페이지
- 액세스 제어 그룹 복사, 23 페이지

역할 복사

표준 역할의 설정을 새 역할에 복사하여 새 역할을 생성하려면 다음 절차를 수행합니다. Cisco Unified Communications Manager는 표준 역할의 권한을 편집할 수 없지만 사용자가 생성한 역할에서는 권한을 편집할 수 있습니다.

절차

단계 **1** Cisco Unified Communications Manager 관리에서 사용자 관리 > 사용자 설정 > 역할을 클릭합니다.

단계 **2** 찾기를 클릭하고 리소스와 권한을 복사할 역할을 선택합니다.

단계 **3** 복사를 클릭합니다.

단계 **4** 새 역할의 이름을 입력하고 확인을 클릭합니다.
역할 구성 창이 새 역할의 설정을 표시합니다. 새 역할에 대한 권한은 복사한 역할에 대한 권한과 동일합니다.

단계 **5** 새 역할의 모든 리소스에 대해 다음과 같이 권한을 편집합니다.

- 읽기 확인란을 선택하여 사용자가 리소스를 볼 수 있도록 허용합니다.
- 업데이트 확인란을 선택하여 사용자가 리소스를 편집할 수 있도록 허용합니다.

- 리소스에 대한 액세스를 제한하려면 두 확인란을 선택하지 않은 상태로 둡니다.

단계 **6** 저장을 클릭합니다.

다음에 할 작업

사용자에게 역할을 지정하려면 새 액세스 제어 그룹을 만들고 해당 그룹에 역할을 할당합니다. 새 액세스 제어 그룹을 만들려면 다음 절차 중 하나를 수행합니다.

- 액세스 제어 그룹 만들기, 23 페이지
- 액세스 제어 그룹 복사, 23 페이지

액세스 제어 그룹 만들기

새 액세스 제어 그룹을 만들려면 이 절차를 사용합니다.

시작하기 전에

액세스 제어 그룹에 기존 그룹과 유사한 설정이 있는 경우 복사 명령을 사용하여 기존 그룹의 설정을 사용자가 만든 새 그룹에 복사할 수 있습니다.

액세스 제어 그룹 복사, 23 페이지

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 액세스 제어 그룹의 이름을 입력합니다.

단계 **4** 사용자 순위가 있는 사용자에 사용 가능 드롭다운에서 이 그룹에 할당할 사용자의 최소 사용자 순위를 선택합니다. 기본 사용자 순위는 1입니다.

단계 **5** 저장을 클릭합니다.

다음에 할 작업

액세스 제어 그룹에 역할 할당, 24 페이지

액세스 제어 그룹 복사

기존 액세스 제어 그룹에서 편집할 수 있는 새 그룹으로 역할 설정을 복사하여 새 액세스 제어 그룹을 생성하려면 다음 작업을 수행합니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

단계 **2** 찾기를 클릭하고 설정을 복사할 액세스 제어 그룹을 선택합니다.

단계 **3** 복사를 클릭합니다.

단계 **4** 새 액세스 제어 그룹의 이름을 입력하고 확인을 클릭합니다.

단계 **5** 사용자 순위가 있는 사용자에 사용 가능 드롭다운에서 이 그룹에 할당할 사용자의 최소 사용자 순위를 선택합니다.

단계 **6** 저장을 클릭합니다.

다음에 할 작업

액세스 제어 그룹에 할당된 역할을 검토하고 편집해야 하는 경우:

액세스 제어 그룹에 역할 할당, 24 페이지

액세스 제어 그룹에 역할 할당

이 절차를 사용하여 액세스 제어 그룹에 역할을 할당합니다. 기존 그룹에서 액세스 제어 그룹 설정을 복사한 경우 역할을 삭제해야 할 수도 있습니다.

관리자 같이 모든 액세스 권한을 가진 사용자는 액세스 제어 그룹에 대해 역할을 할당하거나 역할을 삭제할 수 있습니다. 역할을 할당받은 액세스 제어 그룹은 역할을 구성하는 모든 리소스에 액세스할 수 있습니다.

참고 액세스 제어 그룹에 역할을 할당할 때는 표준 Unified CM 관리 사용자 역할을 액세스 제어 그룹에 할당해야 합니다. 이 역할을 사용하여 사용자가 Unified CM 관리에 로그인할 수 있습니다.

시작하기 전에

새 액세스 제어 그룹을 만들어야 하는 경우 다음 작업 중 하나를 수행합니다.

- 액세스 제어 그룹 복사, 23 페이지
- 액세스 제어 그룹 만들기, 23 페이지

절차

단계 **1** 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.
액세스 제어 그룹 찾기 및 나열 창이 나타납니다.

단계 **2** 찾기를 클릭하고 역할을 할당할 액세스 제어 그룹의 이름을 선택합니다.

액세스 제어 그룹 구성 창이 표시됩니다.

단계 **3** 관련 링크 드롭다운 목록에서 액세스 제어 그룹에 역할 할당을 선택한 다음 이동을 클릭합니다.
역할 할당 창이 표시됩니다.

단계 **4** 새 역할을 액세스 제어 그룹에 추가하려면 다음을 수행합니다.

a) 그룹에 역할 할당을 클릭합니다.
b) 찾기를 클릭하여 역할 목록을 검색합니다.
c) 이 액세스 제어 그룹에 추가하려는 역할을 선택합니다.
d) 선택한 항목 추가를 클릭합니다.
새 역할이 역할 목록 상자에 표시됩니다.

단계 **5** 액세스 제어 그룹에서 할당된 역할을 삭제하려면 다음을 수행합니다.

a) 역할 목록 상자에서 삭제하려는 역할을 강조 표시합니다.
b) 역할 할당 삭제를 클릭합니다.

단계 **6** 저장을 클릭합니다.
역할 할당이 데이터베이스의 액세스 제어 그룹에 추가됩니다.

다음에 할 작업

액세스 제어 그룹에 사용자 할당, 25 페이지

액세스 제어 그룹에 사용자 할당

새 사용자를 할당하거나 기존 사용자를 삭제하여 액세스 제어 그룹에 있는 최종 사용자 또는 애플리케이션 사용자의 목록을 업데이트하려면 이 작업을 완료합니다.

참고 사용자 순위가 액세스 제어 그룹에 대한 최소 사용자 순위와 같거나 더 높은 사용자만 추가할 수 있습니다.

시작하기 전에

액세스 제어 그룹에 역할 할당, 24 페이지

절차

단계 **1** 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.
액세스 제어 그룹 찾기 및 나열 창이 나타납니다.

단계 **2** 찾기를 클릭하고 사용자 목록을 업데이트할 액세스 제어 그룹의 이름을 선택합니다.

단계 **3** 찾기를 클릭하여 사용자 목록을 표시합니다.

단계 **4** 액세스 제어 그룹에 최종 사용자 또는 애플리케이션 사용자를 추가하려면 다음을 수행합니다.

a) 액세스 제어 그룹에 최종 사용자 추가 또는 액세스 제어 그룹에 애플리케이션 사용자 추가를 클릭합니다.
b) 추가하려는 사용자를 선택합니다.
c) 선택한 항목 추가를 클릭합니다.

단계 **5** 액세스 제어 그룹에서 사용자를 삭제하려면:

a) 삭제하려는 사용자를 선택합니다.
b) 선택한 항목 삭제를 클릭합니다.

단계 **6** 저장을 클릭합니다.

다음에 할 작업

(선택 사항) 특정한 최종 사용자 또는 애플리케이션 사용자에 대한 사용자 권한 보고서를 확인해야 할 경우 다음을 참조하십시오.

• 사용자 권한 보고서 보기, 26 페이지

사용자 권한 보고서 보기

기존 최종 사용자 또는 기존 애플리케이션 사용자에 대한 사용자 권한 보고서를 보려면 다음 절차를 수행합니다. 사용자 권한 보고서는 최종 사용자 또는 애플리케이션 사용자에 할당된 액세스 제어 그룹, 역할 및 액세스 권한을 표시합니다.

절차

단계 **1** Cisco Unified CM 관리에서 다음 단계 중 하나를 수행합니다.

- 최종 사용자의 경우 사용자 관리 > 최종 사용자를 선택합니다.
- 애플리케이션 사용자의 경우 사용자 관리 > 애플리케이션 사용자를 선택합니다.

단계 **2** 찾기를 클릭하고 액세스 권한을 보려는 사용자를 선택합니다.

단계 **3** 관련 링크 드롭다운 목록에서 사용자 권한 보고서를 선택한 다음 이동을 클릭합니다.
사용자 권한 창이 표시됩니다.

액세스 제어 그룹에 대한 권한 정책 중복 구성

Cisco Unified Communications Manager가 액세스 제어 그룹 할당에서 발생할 수 있는 중복 사용자 권한을 처리하는 방법을 구성합니다. 여기에서는 각각 역할 및 권한 설정이 충돌하는 상태에서 최종 사용자가 여러 액세스 제어 그룹에 할당된 상황을 처리합니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 사용자 관리 매개 변수에서 다음과 같이 사용자 그룹 및 역할을 중복하는 유효 액세스 권한에 대해 다음 값 중 하나를 구성합니다.

- 최대—유효 권한은 모든 중첩 액세스 제어 그룹의 최대 권한을 나타냅니다. 이것이 기본 옵션입니다.
- 최소—유효 권한은 모든 중첩 액세스 제어 그룹의 최소 권한을 나타냅니다.

단계 **3** 저장을 클릭합니다.

사용자 지정 지원 센터 역할 작업 흐름 만들기

일부 회사에서는 지원 센터 직원이 특정 관리 작업을 수행할 수 있도록 권한을 부여하기를 원합니다. 전화기를 추가하고 최종 사용자를 추가하는 등의 작업을 수행할 수 있는 지원 센터 팀원을 위한 역할 및 액세스 제어 그룹을 구성하려면 이 작업 흐름의 단계를 수행합니다.

절차

	명령 또는 동작	목적
단계 **1**	사용자 지정 지원 센터 역할 만들기, 27 페이지	지원 센터 팀 구성원을 위한 사용자 정의 역할을 만들고 새 전화기 추가 및 새 사용자 추가 같은 항목에 대한 권한을 할당합니다.
단계 **2**	사용자 지정 지원 센터 액세스 제어 그룹 만들기, 28 페이지	지원 센터 역할에 대해 새 액세스 제어 그룹을 만듭니다.
단계 **3**	액세스 제어 그룹에 지원 센터 역할 할당, 28 페이지	지원 센터 액세스 제어 그룹에 지원 센터 역할을 할당합니다. 이 액세스 제어 그룹에 할당된 모든 사용자는 지원 센터 역할의 권한이 할당됩니다.
단계 **4**	액세스 제어 그룹에 지원 센터 구성원 할당, 29 페이지	사용자 정의 지원 데스크 역할의 권한을 사용하여 지원 센터 팀 구성원 할당합니다.

사용자 지정 지원 센터 역할 만들기

조직 내의 지원 센터 구성원에 할당할 수 있는 사용자 지정 지원 센터 역할을 만들려면 이 절차를 수행합니다.

절차

단계 **1** Cisco Unified Communications Manager 관리에서 사용자 관리 > 사용자 설정 > 역할을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 애플리케이션 드롭다운 목록에서 이 역할에 할당하려는 애플리케이션을 선택합니다. 예를 들어, **Cisco CallManager** 관리를 선택합니다.

단계 **4** 다음을 클릭합니다.

단계 **5** 새 역할의 이름을 입력합니다. 예를 들어 지원 센터를 입력합니다.

단계 **6** 권한 읽기 및 업데이트에서 지원 센터 사용자에 할당하려는 권한을 선택합니다. 예를 들어, 지원 센터 구성원이 사용자와 전화기를 추가할 수 있도록 하려면 사용자 웹 페이지와 전화기 웹 페이지에 대해 읽기 및 업데이트 확인란을 선택합니다.

단계 **7** 저장을 클릭합니다.

다음에 할 작업

사용자 지정 지원 센터 액세스 제어 그룹 만들기, 28 페이지

사용자 지정 지원 센터 액세스 제어 그룹 만들기

시작하기 전에

사용자 지정 지원 센터 역할 만들기, 27 페이지

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 액세스 제어 그룹의 이름을 입력합니다. 예를 들어 지원 센터를 입력합니다.

단계 **4** 저장을 클릭합니다.

다음에 할 작업

액세스 제어 그룹에 지원 센터 역할 할당, 28 페이지

액세스 제어 그룹에 지원 센터 역할 할당

지원 센터 역할에서 권한이 있는 지원 센터 액세스 제어 그룹을 구성하려면 다음 단계를 수행합니다.

시작하기 전에

사용자 지정 지원 센터 액세스 제어 그룹 만들기, 28 페이지

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

단계 **2** 찾기를 클릭하고 지원 센터를 위해 사용자가 만든 액세스 제어 그룹을 선택합니다.
액세스 제어 그룹 구성 창이 표시됩니다.

단계 **3** 관련 링크 드롭다운 목록 상자에서 액세스 제어 그룹에 역할 할당 옵션을 선택하고 이동을 클릭합니다.
역할 찾기 및 나열 팝업이 표시됩니다.

단계 **4** 그룹에 역할 할당 단추를 클릭합니다.

단계 **5** 찾기를 클릭하고 지원 센터 역할을 선택합니다.

단계 **6** 선택한 항목 추가를 클릭합니다.

단계 **7** 저장을 클릭합니다.

다음에 할 작업

액세스 제어 그룹에 지원 센터 구성원 할당, 29 페이지

액세스 제어 그룹에 지원 센터 구성원 할당

시작하기 전에

액세스 제어 그룹에 지원 센터 역할 할당, 28 페이지

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

단계 **2** 찾기를 클릭하고 사용자가 만든 사용자 정의 지원 센터 액세스 제어 그룹을 선택합니다.

단계 **3** 다음 단계 중 하나를 수행합니다.

- 지원 센터 팀 구성원이 최종 사용자로 구성된 경우 그룹에 최종 사용자 추가를 클릭합니다.
- 지원 센터 팀 구성원이 애플리케이션 사용자로 구성된 경우 그룹에 앱 사용자 추가를 클릭합니다.

단계 **4** 찾기를 클릭하고 지원 센터 사용자를 선택합니다.

단계 **5** 선택한 항목 추가를 클릭합니다.

단계 **6** 저장을 클릭합니다.
Cisco Unified Communications Manager는 사용자가 만든 사용자 정의 지원 센터 역할의 권한을 사용하여 지원 센터 팀 구성원을 할당합니다.

액세스 제어 그룹 삭제

다음 절차를 사용하여 액세스 제어 그룹을 완전히 삭제합니다.

시작하기 전에

액세스 제어 그룹을 삭제하면 Cisco Unified Communications Manager가 데이터베이스에서 모든 액세스 제어 그룹 데이터를 제거합니다. 어떤 역할이 액세스 제어 그룹을 사용 중인지 확인 합니다.

절차

단계 **1** 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.
액세스 제어 그룹 찾기 및 나열 창이 나타납니다.

단계 **2** 삭제할 액세스 제어 그룹을 찾습니다.

단계 **3** 삭제할 액세스 제어 그룹의 이름을 클릭합니다.
선택한 액세스 제어 그룹이 나타납니다. 이 액세스 제어 그룹에 속하는 사용자가 알파벳 순으로 목록에 표시됩니다.

단계 **4** 액세스 제어 그룹을 완전히 삭제하려면 삭제를 클릭합니다.
대화 상자에 액세스 제어 그룹 삭제를 취소할 수 없다는 경고가 표시됩니다.

단계 **5** 액세스 제어 그룹을 삭제하려면 확인을 클릭하거나 작업을 취소하려면 취소를 클릭합니다. 확인을 클릭하는 경우 Cisco Unified Communications Manager가 데이터베이스에서 액세스 제어 그룹을 제거합니다.

기존 **OAuth** 새로 고침 토큰 해지

AXL API를 사용하여 기존 OAuth 새로 고침 토큰을 해지합니다. 예를 들어, 한 직원이 회사를 퇴사하는 경우 이 API를 사용하여 새 액세스 토큰을 받을 수 없고 더 이상 회사 계정에 로그인 할 수 없도록 해당 직원의 현재 새로 고침 토큰을 해지할 수 있습니다. API는 AXL 인증서에 의해 보호되는 REST 기반 API입니다. API를 호출하려면 명령줄 도구를 사용할 수 있습니다. 다음 명령은 새로 고침 토큰을 해지하는 데 사용할 수 있는 cURL 명령의 예를 제공합니다.

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

여기서:

- `admin:password`는 Cisco Unified Communications Manager 관리자 계정의 로그인 ID와 암호입니다.
- `UCMaddress`는 Cisco Unified Communications Manger 게시자 노드의 FQDN 또는 IP 주소입니다.
- `end_user`는 새로 고침 토큰을 해지하려는 사용자의 사용자 ID입니다.

원격 계정 설정

Cisco 지원이 일시적으로 문제 해결을 위해 시스템에 액세스할 수 있도록 원격 계정을 구성합니다.

절차

단계 **1** Cisco Unified Operating System 관리에서 서비스 > 원격 지원을 선택합니다.

단계 **2** 계정 이름 필드에 원격 계정의 이름을 입력합니다.

단계 **3** 계정 기간 필드에 계정 기간(일)을 입력합니다.

단계 **4** 저장을 클릭합니다.
원격 지원 계정에 대한 정보를 표시하는 필드가 나타납니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **5** Cisco 지원에 연락하여 원격 지원 계정 이름 및 암호를 제공하십시오.

표준 역할 및 액세스 제어 그룹

다음 표는 Cisco Unified Communications Manager에 미리 구성된 표준 역할 및 액세스 제어 그룹을 요약합니다. 표준 역할에 대한 권한은 기본적으로 구성됩니다. 뿐만 아니라 표준 역할에 연결된 액세스 제어 그룹은 기본적으로도 구성됩니다.

표준 역할 및 연결된 액세스 제어 그룹 모두에 대해 권한 또는 역할 할당을 편집할 수 없습니다.

표 ***1:*** 표준 역할**,** 권한 및 액세스 제어 그룹

표준 역할	역할에 대한 권한**/**리소스	연결된 표준 액세스 제어 그룹
표준 AXL API 액세스	AXL 데이터베이스 API에 대한 액세스 허용	표준 CCM 수퍼 사용자
표준 AXL API 사용자	AXL API를 실행할 로그인 권한을 부여합니다.	
표준 AXL 읽기 전용 API 액세스	기본적으로 AXL 읽기 전용 API(list APIs, get APIs, executeSQLQuery API)를 실행할 수 있습니다.	
표준 관리 보고 도구 관리	Cisco Unified Communications Manager CDR Analysis and Reporting(CAR)을 보고 구성할 수 있습니다.	표준 CAR 관리 사용자, 표준 CCM 수퍼 사용자

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 감사 로그 관리	감사 로깅 기능에 대한 다음 작업을 수행할 수 있습니다. • Cisco Unified Serviceability의 감사 로그 구성 창에서 감사 로깅 보기 및 구성 • Cisco Unified Serviceability에서 추적 보기 및 구성과 실시간 모니터링 도구에서 감사 로그 기능에 대한 추적 수집 • Cisco Unified Serviceability에서 Cisco 감사 이벤트 서비스 보기 및 시작/중지 • RTMT에 연결된 경고 보기 및 업데이트	표준 감사 사용자
표준 CCM 관리 사용자	Cisco Unified Communications Manager 관리에 로그인 권한을 부여합니다.	표준 CCM 관리 사용자, 표준 CCM 게이트웨이 관리, 표준 CCM 전화 관리, 표준 CCM 읽기 전용, 표준 CCM 서버 모니터링, 표준 CCM 수퍼 사용자, 표준 CCM 서버 유지 보수, 표준 패킷 스니퍼 사용자
표준 CCM 최종 사용자	Cisco Unified Communications 셀프 케어 포털에 최종 사용자 로그인 권한을 부여합니다	표준 CCM 최종 사용자

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 CCM 기능 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다. • 벌크 관리 도구를 사용하여 다음 항목을 보고, 삭제하고, 삽입합니다. ◦ 클라이언트 매터 코드 및 강제 인증 코드 ◦ 통화 당겨받기 그룹 • Cisco Unified Communications Manager 관리에서 다음 항목을 보고 구성합니다. ◦ 클라이언트 매터 코드 및 강제 인증 코드 ◦ 통화 보류 ◦ 통화 당겨받기 ◦ 강제 인증 코드 번호/패턴 ◦ 메시지 대기 중 ◦ Cisco Unified IP Phone 서비스 ◦ 음성 메일 파일럿, 음성 메일 포트 마법사, 음성 메일 포트 및 음성 메일 프로파일	표준 CCM 서버 유지 관리
표준 CCM 게이트웨이 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다. • 벌크 관리 도구에서 게이트웨이 템플릿 보기 및 구성 • 게이트키퍼, 게이트웨이 및 트렁크 보기 및 구성	표준 CCM 게이트웨이 관리

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 CCM 전화 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다. • 벌크 관리 도구에서 전화기 보기 및 내보내기 • 벌크 관리 도구에서 사용자 장치 프로파일 보기 및 삽입 • Cisco Unified Communications Manager 관리에서 다음 항목을 보고 구성합니다. ◦ BLF 단축 다이얼 ◦ CTI 경로 포인트 ◦ 기본 장치 프로파일 또는 기본 프로파일 ◦ 디렉터리 번호 및 회선 표시 ◦ 펌웨어 로드 정보 ◦ 전화기 단추 템플릿 또는 소프트키 템플릿 ◦ 전화기 ◦ [전화기 구성] 창에서 [단추 항목 수정] 단추를 클릭하여 특정 전화기에 대한 전화기 단추 정보 순서 바꾸기	표준 CCM 전화 관리
표준 CCM 경로 플랜 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다. • 애플리케이션 다이얼 규칙 보기 및 구성 • 발신 검색 공간 및 파티션 보기 및 구성 • 다이얼 규칙 패턴을 포함하는 다이얼 규칙 보기 및 구성 • 헌트 목록, 헌트 파일럿 및 회선 그룹 보기 및 구성 • 경로 필터, 경로 그룹, 경로 헌트 목록, 경로 목록, 경로 패턴 및 경로 플랜 보고서 보기 및 구성 • 시간 기간 및 시간 일정 보기 및 구성 • 변환 패턴 보기 및 구성	

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 CCM 서비스 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다. • 다음 항목을 보고 구성합니다. ◦ 알림 장치, 컨퍼런스 브리지 및 트랜스코더 ◦ 오디오 소스 및 MOH 서버 ◦ 미디어 리소스 그룹 및 미디어 리소스 그룹 목록 ◦ 미디어 종료 지점 ◦ Cisco Unified Communications Manager Assistant 마법사 • 벌크 관리 도구에서 관리자 삭제, 관리자/보조자 삭제 및 관리자/보조자 삽입 창 보기 및 구성	표준 CCM 서버 유지 관리

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 CCM 시스템 관리	Cisco Unified Communications Manager 관리에서 다음 작업을 수행할 수 있습니다. • 다음 항목을 보고 구성합니다. ◦ AAR(Automate Alternate Routing) 그룹 ◦ Cisco Unified Communications Manager(Cisco Unified CM) 및 Cisco Unified Communications Manager 그룹 ◦ 날짜 및 시간 그룹 ◦ 장치 기본값 ◦ 장치 풀 ◦ 엔터프라이즈 매개 변수 ◦ 엔터프라이즈 전화 구성 ◦ 위치 ◦ NTP(Network Time Protocol) 서버 ◦ 플러그인 ◦ SCCP(Skinny Call Control Protocol) 또는 SIP(Session Initiation Protocol)를 실행하는 전화기의 보안 프로파일, SIP 트렁크의 보안 프로파일 ◦ SRST(Survivable Remote Site Telephony) 참조 ◦ 서버 • 벌크 관리 도구에서 작업 스케줄러 창 보기 및 구성	표준 CCM 서버 유지 관리
표준 CCM 사용자 권한 관리	Cisco Unified Communications Manager 관리에서 애플리케이션 사용자를 보고 구성할 수 있습니다.	
표준 CCMADMIN 관리	CCMAdmin 시스템의 모든 기능에 액세스할 수 있습니다.	
표준 CCMADMIN 관리	Cisco Unified Communications Manager 관리 및 벌크 관리 도구에서 모든 항목을 보고 구성할 수 있습니다.	표준 CCM 수퍼 사용자
표준 CCMADMIN 관리	Dialed Number Analyzer에서 정보를 보고 구성할 수 있습니다.	

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 CCMADMIN 읽기 전용	모든 CCMAdmin 리소스에 읽기 액세스할 수 있습니다.	
표준 CCMADMIN 읽기 전용	Cisco Unified Communications Manager 관리 및 벌크 관리 도구에서 구성을 볼 수 있습니다.	표준 CCM 게이트웨이 관리, 표준 CCM 전화 관리, 표준 CCM 읽기 전용, 표준 CCM 서버 유지 관리, 표준 CCM 서버 모니터링
표준 CCMADMIN 읽기 전용	Dialed Number Analyzer에서 라우팅 구성을 분석할 수 있습니다.	
표준 CCMUSER 관리	Cisco Unified Communications 셀프 케어 포털에 액세스할 수 있습니다.	표준 CCM 최종 사용자
표준 CTI 통화 모니터링 허용	CTI 애플리케이션/장치에서 통화를 모니터링할 수 있습니다.	표준 CTI 통화 모니터링 허용
표준 CTI 통화 지정보류 모니터링 허용	CTI 애플리케이션/장치에서 통화 지정보류를 사용할 수 있습니다.	표준 CTI 통화 지정보류 모니터링 허용
표준 CTI 통화 녹음 허용	CTI 애플리케이션/장치에서 통화를 녹음할 수 있습니다.	표준 CTI 통화 녹음 허용
표준 CTI 발신 번호 수정 허용	CTI 애플리케이션에서 통화 중 발신자 번호를 변환할 수 있습니다.	표준 CTI 발신 번호 수정 허용
표준 CTI 모든 장치 제어 허용	모든 CTI 제어 가능 장치 제어 허용	표준 CTI 모든 장치 제어 허용
연결된 Xfer 및 conf를 지원하는 전화의 표준 CTI 컨트롤 허용	호전환 연결 및 전화회의를 지원하는 모든 CTI 장치 제어 허용	연결된 Xfer 및 conf를 지원하는 전화의 표준 CTI 컨트롤 허용
표준 CTI 롤오버 모드를 지원하는 전화의 컨트롤 허용	롤오버 모드를 지원하는 모든 CTI 장치 컨트롤 허용	표준 CTI 롤오버 모드를 지원하는 전화의 컨트롤 허용
표준 CTI SRTP 키 자료 수신 허용	CTI 애플리케이션에서 SRTP 키 자료에 액세스하고 배포하도록 허용	표준 CTI SRTP 키 자료 수신 허용
표준 CTI 활성화	CTI 애플리케이션 컨트롤 활성화	표준 CTI 활성화
표준 CTI 보안 연결	Cisco Unified Communications Manager에 대한 보안 CTI 연결 활성화	표준 CTI 보안 연결

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 CUReporting	애플리케이션 사용자가 다양한 소스에서 보고서를 생성하도록 허용	
표준 CUReporting	Cisco Unified Reporting에서 보고서 보기, 다운로드, 생성 및 업로드 허용	표준 CCM 관리 사용자, 표준 CCM 수퍼 사용자
표준 EM 인증 프록시 권한	애플리케이션용 Cisco Extension Mobility(EM) 인증 권한 관리, Cisco Extension Mobility와 상호 작용하는 모든 애플리케이션 필요(예: Cisco Unified Communications Manager Assistant 및 Cisco Web Dialer)	표준 CCM 수퍼 사용자, 표준 EM 인증 프록시 권한
표준 패킷 스니핑	Cisco Unified Communications Manager 관리에 액세스하여 패킷 스니핑(캡처)을 활성화할 수 있습니다.	표준 패킷 스니퍼 사용자
표준 RealtimeAndTraceCollection	Cisco Unified Serviceability 및 실시간 모니터링 도구에 액세스하여 다음 항목을 보고 사용할 수 있습니다. • SOAP(Simple Object Access Protocol) 서비스 가용성 AXL API • SOAP 호출 레코드 API • SOAP 진단 포털(Analysis Manager) 데이터베이스 서비스 • 감사 로그 기능에 대한 추적 구성 • 추적 수집을 포함하여 실시간 모니터링 도구 구성	표준 RealtimeAndTraceCollection

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 서비스 가용성	Cisco Unified Serviceability 또는 실시간 모니터링 도구에서 다음 창을 보고 구성할 수 있습니다. • 알람 구성 및 알람 정의(Cisco Unified Serviceability) • 감사 추적(읽기/보기 전용으로 표시됨) • SNMP 관련 창(Cisco Unified Serviceability) • 추적 구성 및 추적 구성 문제 해결(Cisco Unified Serviceability) • 로그 파티션 모니터링 • 경고 구성(RTMT), 프로파일 구성(RTMT) 및 추적 수집(RTMT) SOAP 서비스 가용성 AXL API, SOAP 통화 레코드 API 및 SOAP 진단 포털(Analysis Manager) 데이터베이스 서비스를 보고 사용할 수 있습니다. SOAP 통화 레코드 API의 경우 RTMT Analysis Manager 통화 레코드 권한은 이 리소스를 통해 제어됩니다. SOAP 진단 포털 데이터베이스 서비스의 경우 RTMT Analysis Manager 호스팅 데이터베이스 액세스는 이 리소스를 통해 제어됩니다.	표준 CCM 서버 모니터링, 표준 CCM 수퍼 사용자
표준 SERVICEABILITY 관리	서비스 가용성 관리자는 Cisco Unified Communications Manager 관리에서 플러그인 창에 액세스하여 이 창에서 플러그인을 다운로드할 수 있습니다.	
표준 SERVICEABILITY 관리	Dialed Number Analyzer에 대한 서비스 가용성의 모든 기능을 관리할 수 있습니다.	
표준 SERVICEABILITY 관리	Cisco Unified Serviceability 또는 실시간 모니터링 도구에서 모든 창을 보고 구성할 수 있습니다. (감사 추적은 보기만 지원). 모든 SOAP 서비스 가용성 AXL API를 보고 사용할 수 있습니다.	
표준 서비스 가용성 읽기 전용	Dialed Number Analyzer에 있는 구성 요소에 대한 모든 서비스 가용성 관련 데이터를 볼 수 있습니다.	표준 CCM 읽기 전용

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 서비스 가용성 읽기 전용	Cisco Unified Serviceability 또는 실시간 모니터링 도구에서 구성을 볼 수 있습니다. (표준 감사 로그 관리 역할로 표시되는 감사 구성 창은 제외) 모든 SOAP 서비스 가용성 AXL API, SOAP 통화 레코드 API 및 SOAP 진단 포털(Analysis Manager) 데이터베이스 서비스를 볼 수 있습니다.	
표준 시스템 서비스 관리	Cisco Unified Serviceability에서 서비스를 보고 활성화하고 시작하고 중지할 수 있습니다.	
표준 SSO 구성 관리	SAML SSO 구성의 모든 기능을 관리할 수 있습니다.	
표준 기밀 액세스 수준 사용자	모든 기밀 액세스 수준 페이지에 액세스할 수 있습니다.	표준 Cisco Call Manager 관리
표준 CCMADMIN 관리	CCMAdmin 시스템의 모든 기능을 관리할 수 있습니다.	표준 Cisco Unified CM IM and Presence 관리
표준 CCMADMIN 읽기 전용	모든 CCMAdmin 리소스에 읽기 액세스할 수 있습니다.	표준 Cisco Unified CM IM and Presence 관리
표준 CUReporting	애플리케이션 사용자가 다양한 소스에서 보고서를 생성하도록 허용	표준 Cisco Unified CM IM and Presence 보고

4 장

최종 사용자 관리

최종 사용자 개요

실행 중인 시스템을 관리할 때 시스템에 구성된 최종 사용자의 목록을 업데이트해야 할 수 있습니다. 여기에는 다음 항목이 포함됩니다.

- 새 사용자 설정
- 새 최종 사용자를 위해 전화기 설정
- 최종 사용자에 대한 암호 또는 PIN 변경
- IM and Presence 서비스에 대해 최종 사용자 활성화

관리자는 Cisco Unified CM 관리의 최종 사용자 구성 창을 사용하여 Unified CM 최종 사용자에 대한 정보를 추가, 검색, 표시 및 유지 관리할 수 있습니다. 빠른 사용자/전화기 추가 창을 사용하여 새 최종 사용자를 신속하게 구성하고 해당 최종 사용자에 대해 새 전화기를 구성할 수도 있습니다.

최종 사용자 관리 작업

절차

	명령 또는 동작	목적
단계 **1**	사용자 템플릿 구성, 42 페이지	사용자 프로파일 또는 범용 회선과 장치 템플릿을 포함하는 기능 그룹 템플릿으로 시스템을 구성하지 않은 경우 다음 작업을 수행하여 설정합니다. 새 사용자 및 전화기를 신속하게 구성하려면 모든 새 최종 사용자에 이러한 템플릿을 적용할 수 있습니다.

	명령 또는 동작	목적
단계 **2**	다음 방법 중 하나를 사용하여 새 최종 사용자 추가 • LDAP에서 최종 사용자 가져오기, 46 페이지 • 최종 사용자를 수동으로 추가, 46 페이지	시스템이 회사 LDAP 디렉터리와 동기화된 경우 LDAP 디렉터리에서 새 최종 사용자를 직접 가져올 수 있습니다. 구성한 경우 그렇지 않으면, 최종 사용자를 수동으로 추가 및 구성할 수 있습니다.
단계 **3**	다음 작업 중 하나를 수행하여 전화기를 새 사용자 또는 기존의 최종 사용자에게 할당합니다. • 최종 사용자를 위한 새 전화기 추가, 48 페이지 • 최종 사용자에게 기존 전화기 이동, 48 페이지	범용 장치 템플릿의 설정을 사용하여 최종 사용자에 대한 새 전화기를 구성하기 위해 '새 전화기 추가' 절차를 사용할 수 있습니다. 또한 이미 구성된 기존 전화기를 할당하려면 '이동' 절차를 사용할 수 있습니다.
단계 **4**	최종 사용자 PIN 변경, 49 페이지	(선택 사항) Cisco Unified Communications Manager 관리에서 최종 사용자에 대한 PIN을 변경합니다.
단계 **5**	최종 사용자 암호 변경, 49 페이지	(선택 사항) Cisco Unified Communications Manager 관리에서 최종 사용자에 대한 암호를 변경합니다.
단계 **6**	Cisco Unity Connection 음성 사서함 생성, 50 페이지	(선택 사항) Cisco Unified Communications Manager 관리에서 개별 Cisco Unity Connection 음성 사서함을 생성합니다.

사용자 템플릿 구성

사용자 프로파일 및 기능 그룹 템플릿을 설정하려면 다음 작업을 수행합니다. 새 최종 사용자를 추가할 때 회선 및 장치 설정을 사용하여 신속하게 최종 사용자에 대한 전화기를 구성할 수 있습니다.

절차

	명령 또는 동작	목적
단계 **1**	범용 회선 템플릿 구성, 43 페이지	일반적으로 디렉터리 번호에 적용되는 공통 설정을 사용하여 범용 회선 템플릿을 구성합니다.

	명령 또는 동작	목적
단계 **2**	범용 장치 템플릿 구성, 43 페이지	일반적으로 전화기에 적용되는 공통 설정을 사용하여 범용 장치 템플릿을 구성합니다.
단계 **3**	사용자 프로파일 구성, 44 페이지	사용자 프로파일에 범용 회선 및 범용 장치 템플릿을 할당합니다. 셀프 프로비저닝 기능이 구성된 경우 이 프로파일을 사용하는 사용자에 대해 셀프 프로비저닝을 활성화할 수 있습니다.
단계 **4**	기능 그룹 템플릿 구성, 45 페이지	사용자 프로파일을 기능 그룹 템플릿에 할당합니다. LDAP 동기화된 사용자의 경우 기능 그룹 템플릿은 사용자 프로파일을 최종 사용자에게 연결합니다.

범용 회선 템플릿 구성

일반적으로 디렉터리 번호에 적용되는 공통 설정을 사용하여 범용 회선 템플릿을 구성합니다. 조직 내에서는 물론 사용자 프로파일을 통해 대부분 일반 디렉터리 번호 구성을 반영하는 설정 모음을 만들기 위해 하나 이상의 범용 장치 템플릿을 만들 수 있으며 최종 사용자에게 프로비저닝하는 새 디렉터리 번호에 이러한 설정을 적용할 수 있습니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 범용 회선 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 범용 회선 템플릿 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

다음에 할 작업

범용 장치 템플릿 구성, 43 페이지

범용 장치 템플릿 구성

범용 장치 템플릿을 구성합니다. 범용 장치 템플릿에는 전화기, 원격 대상 프로파일 또는 내선 이동 프로파일에 일반적으로 적용되는 공통의 설정 집합이 포함되어 있습니다. 조직 내에서는 물론 사용자 프로파일을 통해 대부분 일반 장치 구성을 반영하는 하나 이상의 범용 장치 템플릿을 만들 수 있으며 최종 사용자에게 프로비저닝하는 새 장치에 이러한 설정을 적용할 수 있습니다.

시작하기 전에

범용 회선 템플릿 구성, 43 페이지

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 범용 장치 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 범용 장치 템플릿 구성 창에서 필드를 완성합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

다음에 할 작업

사용자 프로파일 구성, 44 페이지

사용자 프로파일 구성

해당 프로파일을 사용하는 사용자에게 할당하려는 범용 회선 템플릿 및 범용 장치 템플릿을 포함하는 사용자 프로파일을 구성합니다. 이 서비스 프로파일을 사용하는 사용자에 대한 셀프 프로비저닝을 활성화할 수도 있습니다.

시작하기 전에

범용 장치 템플릿 구성, 43 페이지

절차

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자 설정 > 사용자 프로파일을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 사용자 프로파일의 이름 및 설명을 입력합니다.

단계 **4** 사용자의 사무실 전화기, 모바일 및 데스크톱 장치 및 원격 대상/장치 프로파일에 적용할 범용 장치 템플릿을 할당합니다.

단계 **5** 이 사용자 프로파일의 사용자에 대한 전화 회선에 적용할 범용 회선 템플릿을 할당합니다.

단계 **6** 이 사용자 프로파일의 사용자가 자신의 전화기를 프로비저닝하는 데 셀프 프로비저닝 기능을 사용할 있도록 하려면 다음을 수행합니다.

a) 최종 사용자에게 자신의 전화기 프로비저닝 허용 확인란을 선택합니다.

b) 최종 사용자가 이렇게 많은 전화기를 가지고 있으면 프로비저닝 제한 필드에 사용자가 프로비저닝하도록 허용되는 전화기의 최대 수를 입력합니다. 최대값은 20입니다.

단계 **7** 이 사용자 프로파일과 연결된 Cisco Jabber 사용자가 모바일 및 원격 액세스(MRA) 기능을 사용할 수 있도록 하려면 모바일 및 원격 액세스 활성화 확인란을 선택합니다.

참고 기본적으로 이 확인란은 선택되어 있습니다. 이 확인란을 선택 취소하면 **Jabber** 정책 섹션이 비활성화되고 기본적으로 서비스 클라이언트 없음 정책 옵션이 선택됩니다.

참고 이 설정은 Cisco Jabber 사용자의 경우에만 필수입니다. 비 Jabber 사용자는 이 설정이 없어도 MRA를 사용할 수 있습니다. MRA 기능은 Jabber MRA 사용자에 대해서만 적용되며 다른 엔드포인트 또는 클라이언트에는 적용되지 않습니다.

단계 **8** 이 사용자 프로파일에 대해 Jabber 정책을 할당합니다. **Jabber** 데스크톱 클라이언트 정책 및 **Jabber** 모바일 클라이언트 정책 드롭다운 목록 상자에서 다음 옵션 중 하나를 선택합니다.

- 서비스 없음—이 정책은 모든 Jabber 서비스에 대한 액세스를 비활성화합니다.
- IM & 프레즌스만 해당—이 정책은 인스턴트 메시징 및 프레즌스 기능을 활성화합니다.
- IM & 프레즌스, 음성 및 영상 통화—이 정책은 음성 또는 영상 장치가 있는 모든 사용자에 대해 인스턴트 메시징, 프레즌스, 음성 메일 및 전화 회의 기능을 활성화합니다. 이것이 기본 옵션입니다.

참고 Jabber 데스크톱 클라이언트는 Cisco Jabber for Windows 사용자와 Cisco Jabber for Mac 사용자를 포함합니다. Jabber 모바일 클라이언트는 Cisco Jabber for iPad 및 iPhone 사용자와 Cisco Jabber Android 사용를 포함합니다.

단계 **9** 저장을 클릭합니다.

다음에 할 작업

기능 그룹 템플릿 구성, 45 페이지

기능 그룹 템플릿 구성

기능 그룹 템플릿에는 일반 회선, 장치 및 기능 설정 집합이 포함되어 있습니다. 새 사용자에게 기능 그룹 템플릿을 적용하면 이러한 회선, 장치 및 기능 설정이 사용자 전화기 및 전화 회선에 적용됩니다. 기능 그룹 템플릿은 프로비저닝된 사용자를 위해 전화기, 회선 및 기능을 매우 신속하게 구성하도록 도와 시스템 배포를 지원합니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 기능 그룹 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 이 템플릿을 사용하는 모든 사용자에 대해 로컬 클러스터를 홈 클러스터로 사용하려는 경우 홈 클러스터 확인란을 선택합니다.

단계 **4** 이 템플릿을 사용하는 사용자가 인스턴트 메시징을 위해 IM and Presence 서비스를 사용하도록 활성화려는 경우 **Unified CM IM and Presence**에 대해 사용자 활성화 확인란을 선택합니다.

단계 **5** 드롭다운 메뉴에서 서비스 프로파일 및 사용자 프로파일을 선택합니다.

단계 **6** 기능 그룹 템플릿 구성 창에서 나머지 필드를 완성합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

다음에 할 작업

새 최종 사용자를 추가합니다. 시스템이 회사 LDAP 디렉터리와 통합된 경우 LDAP 디렉터리에서 사용자를 직접 가져올 수 있습니다. 그렇지 않으면 수동으로 최종 사용자를 만듭니다.

- LDAP에서 최종 사용자 가져오기, 46 페이지
- 최종 사용자를 수동으로 추가, 46 페이지

LDAP에서 최종 사용자 가져오기

새 최종 사용자를 회사 LDAP 디렉터리에서 수동으로 가져오려면 다음 절차를 수행합니다. LDAP 동기화 구성에 범용 회선 템플릿 및 장치 템플릿은 물론 DN 풀을 포함하는 기능 그룹 템플릿이 포함된 경우 가져오기 프로세스는 최종 사용자 및 기본 내선 번호를 자동으로 구성합니다.

시작하기 전에

이 절차에서는 Cisco Unified Communications Manager가 회사 LDAP 디렉터리와 이미 동기화되었다고 가정합니다. LDAP 동기화는 범용 회선 템플릿 및 장치 템플릿이 있는 기능 그룹 템플릿을 포함해야 합니다.

절차

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **2** 찾기를 클릭하고 사용자가 추가한 LDAP 디렉터리를 선택합니다.

단계 **3** 전체 동기화 수행을 클릭합니다.
Cisco Unified Communications Manager는 외부 LDAP 디렉터리와 동기화합니다. LDAP 디렉터리에 있는 새 최종 사용자를 Cisco Unified Communications Manager 데이터베이스로 가져옵니다.

다음에 할 작업

셀프 프로비저닝을 위해 사용자가 활성화된 경우 최종 사용자는 셀프 프로비저닝 대화형 음성 응답(IVR)을 사용하여 새 전화기를 프로비저닝할 수 있습니다. 그렇지 않으면 다음 작업 중 하나를 수행하여 전화기를 최종 사용자에게 할당합니다.

- 최종 사용자를 위한 새 전화기 추가, 48 페이지
- 최종 사용자에게 기존 전화기 이동, 48 페이지

최종 사용자를 수동으로 추가

새 최종 사용자를 추가하고 액세스 제어 그룹 및 기본 회선 내선 번호로 해당 최종 사용자를 구성하려면 다음 절차를 수행합니다.

시작하기 전에

범용 회선 템플릿이 포함되어 있는 사용자 프로파일이 구성되었는지 확인합니다. 새 내선 번호를 구성해야 하는 경우 Cisco Unified Communications Manager는 범용 회선 템플릿의 설정을 사용하여 기본 내선 번호를 구성합니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 빠른 사용자/전화기 추가를 선택합니다.

단계 **2** 사용자의 사용자 **ID** 및 성을 입력합니다.

단계 **3** 기능 그룹 템플릿 드롭다운 목록에서 기능 그룹 템플릿을 선택합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** 사용자 프로파일 드롭다운 목록에서 선택한 사용자 프로파일에 범용 회선 템플릿이 포함되어 있는지 확인합니다.

단계 **6** 액세스 제어 그룹 구성원 섹션에서 + 아이콘을 클릭합니다.

단계 **7** 사용자는 다음의 구성원입니다**.** 드롭다운 목록에서 액세스 제어 그룹을 선택합니다.

단계 **8** 기본 내선 번호 아래에서 + 아이콘을 클릭합니다.

단계 **9** 내선 번호 드롭다운 목록에서 **(**사용 가능**)**으로 표시되는 디렉터리 번호를 선택합니다.

단계 **10** 모든 회선 내선 번호가 **(**사용됨**)**으로 표시되는 경우 다음 단계를 수행합니다.

a) 새로 만들기**...** 단추를 클릭합니다.
새 내선 번호 추가 팝업이 표시됩니다.
b) 디렉터리 번호 필드에 새 회선 내선 번호를 입력합니다.
c) 회선 템플릿 드롭다운 목록 상자에서 범용 회선 템플릿을 선택합니다.
d) 확인을 클릭합니다.
Cisco Unified Communications Manager는 범용 장치 템플릿의 설정을 사용하여 전화기를 구성합니다.

단계 **11** (선택 사항) 빠른 사용자/전화기 추가 구성 창에서 추가 필드를 완료합니다.

단계 **12** 저장을 클릭합니다.

다음에 할 작업

다음 절차 중 하나를 수행하여 전화기를 이 최종 사용자에게 할당합니다.

- 최종 사용자를 위한 새 전화기 추가, 48 페이지
- 최종 사용자에게 기존 전화기 이동, 48 페이지

최종 사용자를 위한 새 전화기 추가

신규 또는 기존 최종 사용자에 대해 새 전화기를 추가하려면 다음 절차를 수행합니다. 이 절차에서는 최종 사용자에 대한 사용자 프로파일에 범용 장치 템플릿이 포함되어 있다고 가정합니다. Cisco Unified Communications Manager는 범용 장치 템플릿의 설정을 사용하여 전화기를 구성합니다.

시작하기 전에

최종 사용자를 추가하려면 다음 절차 중 하나를 수행합니다.

- 최종 사용자를 수동으로 추가, 46 페이지
- LDAP에서 최종 사용자 가져오기, 46 페이지

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 빠른/사용자 전화기 추가를 선택합니다.

단계 **2** 찾기를 클릭하고 새 전화기를 추가하려는 최종 사용자를 선택합니다.

단계 **3** 장치 관리 단추를 클릭합니다.
[장치 관리] 창이 나타납니다.

단계 **4** 새 전화기 추가를 클릭합니다.
[사용자에게 전화기 추가] 팝업이 표시됩니다.

단계 **5** 제품 유형 드롭다운 목록에서 전화기 모델을 선택합니다.

단계 **6** 장치 프로토콜 드롭다운에서 프로토콜로 SIP 또는 SCCP를 선택합니다.

단계 **7** 장치 이름 텍스트 상자에 장치 MAC 주소를 입력합니다.

단계 **8** 범용 장치 템플릿 드롭다운 목록에서 범용 장치 템플릿을 선택합니다.

단계 **9** 전화기가 확장 모듈을 지원하는 경우 배포하려는 확장 모듈 수를 입력합니다.

단계 **10** 내선 이동을 사용하여 전화에 액세스하려면 내선 이동에서 확인란을 선택합니다.

단계 **11** 전화기 추가를 클릭합니다.
[새 전화기 추가] 팝업이 닫힙니다. Cisco Unified Communications Manager는 사용자에게 전화기를 추가하고 범용 장치 템플릿을 사용하여 전화기를 구성합니다.

단계 **12** 전화기 구성을 추가 편집하려면 해당 연필 아이콘을 클릭하여 [전화기 구성] 창에서 전화기를 엽니다.

다음에 할 작업

최종 사용자에게 기존 전화기 이동, 48 페이지

최종 사용자에게 기존 전화기 이동

기존 전화기를 새 사용자 또는 기존 최종 사용자에게 이동하려면 이 절차를 수행합니다.

시작하기 전에

최종 사용자를 위한 새 전화기 추가, 48 페이지

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 빠른/사용자 전화기 추가를 선택합니다.

단계 **2** 찾기를 클릭하고 기존 전화기를 이동할 사용자를 선택합니다.

단계 **3** 장치 관리 단추를 클릭합니다.

단계 **4** 이 사용자로 이동할 전화기 찾기 단추를 클릭합니다.

단계 **5** 이 사용자로 이동하려는 전화기를 선택합니다.

단계 **6** 선택 항목 이동을 클릭합니다.

최종 사용자 **PIN** 변경

절차

단계 **1** Cisco Unified Communications Manager 관리에서 사용자 관리 > 최종 사용자를 선택합니다.
사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.
최종 사용자 구성 창이 표시됩니다.

단계 **3** **PIN** 필드에서 암호화된 기존의 PIN을 두 번 클릭하고 새 PIN을 입력합니다. 할당된 자격 증명 정책에 지정된 최소 문자 수(1~127자) 이상을 입력해야 합니다.

단계 **4** **PIN** 확인 필드에서 기존의 암호화된 PIN을 두 번 클릭하고 새 PIN을 다시 입력합니다.

단계 **5** 저장을 클릭합니다.

참고 Cisco Unity Connection의 애플리케이션 서버 구성 창에서 최종 사용자 **PIN** 동기화 확인란이 활성화된 경우 내선 이동, 지금 전화회의, 모바일 연결 및 Cisco Unity Connection 음성 메일에 동일한 최종 사용자 PIN을 사용하여 로그인할 수 있습니다. 최종 사용자는 동일한 PIN을 사용하여 내선 이동에 로그인하고 음성 메일에 액세스할 수 있습니다.

최종 사용자 암호 변경

LDAP 인증이 활성화된 경우에는 최종 사용자 암호를 변경할 수 없습니다.

절차

단계 **1** Cisco Unified Communications Manager 관리에서 사용자 관리 > 최종 사용자를 선택합니다.
사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.
최종 사용자 구성 창이 표시됩니다.

단계 **3** 암호 필드에서 암호화되어 있는 기존 암호를 두 번 클릭하고 새 암호를 입력합니다. 할당된 자격 증명 정책에 지정된 최소 문자 수(1~127자) 이상을 입력해야 합니다.

단계 **4** 암호 확인 필드에서 암호화되어 있는 기존 암호를 두 번 클릭하고 새 암호를 다시 입력합니다.

단계 **5** 저장을 클릭합니다.

Cisco Unity Connection 음성 사서함 생성

시작하기 전에

- 음성 메시징을 위해 Cisco Unified Communications Manager를 구성해야 합니다. Cisco Unity Connection을 사용하도록 Cisco Unified Communications Manager를 구성하는 자세한 내용은 다음 위치에서 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

- 장치 및 기본 내선 번호를 최종 사용자와 연결해야 합니다.
- 이 섹션에 설명된 절차를 수행하는 대신에 Cisco Unity Connection에 제공되는 가져오기 기능을 사용할 수 있습니다. 가져오기 기능을 사용하는 방법에 대한 자세한 내용은 *Cisco Unity Connection* 관련 사용자 이동, 추가 및 변경 설명서를 참조하십시오.

절차

단계 **1** Cisco Unified Communications Manager 관리에서 사용자 관리 > 최종 사용자를 선택합니다.
사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.
최종 사용자 구성 창이 표시됩니다.

단계 **3** 기본 내선 번호가 이 사용자와 연결되어 있는지 확인합니다.
참고 기본 내선을 정의해야 합니다. 그렇지 않으면 [Cisco Unity 사용자 생성] 링크가 관련 링크 드롭다운 목록 상자에 표시되지 않습니다.

단계 **4** 관련 링크 드롭다운 목록에서 [Cisco Unity 애플리케이션 사용자 생성] 링크를 선택하고 이동을 클릭합니다.

[Cisco Unity 사용자 추가] 대화 상자가 표시됩니다.

단계 **5** **Application Server** 드롭다운 목록 상자에서 Cisco Unity Connection 사용자를 생성할 Cisco Unity Connection 서버를 선택하고 다음을 클릭합니다.

단계 **6** 가입자 템플릿 드롭다운 목록 상자에서 사용할 가입자 템플릿을 선택합니다.

단계 **7** 저장을 클릭합니다.
사서함이 생성됩니다. 최종 사용자 구성 창의 관련 링크 드롭다운 목록 상자에 있는 링크가 [Cisco Unity 사용자 편집]으로 변경됩니다. 이제 Cisco Unity Connection 관리에서 생성한 사용자를 볼 수 있습니다.

참고 Cisco Unity Connection 사용자를 Cisco Unified Communications Manager 최종 사용자와 통합한 후에는 Cisco Unity Connection 관리에서 [별칭](Cisco Unified CM 관리에서는 [사용자 ID]), [이름], [성] 및 [내선](Cisco Unified CM 관리에서는 [기본 내선]) 같은 필드를 편집할 수 없습니다. 이러한 필드는 Cisco Unified CM 관리에서만 업데이트할 수 있습니다.

5 장

애플리케이션 사용자 관리

애플리케이션 사용자 개요

관리자는 Cisco Unified CM 관리의 애플리케이션 사용자 구성 창에서 Cisco Unified Communications Manager 애플리케이션 사용자에 대한 정보를 추가, 검색, 표시 및 유지 관리할 수 있습니다.

Cisco Unified CM 관리에는 기본적으로 다음 애플리케이션 사용자가 포함됩니다.

- CCMAdministrator
- CCMSysUser
- CCMQRTSecureSysUser
- CCMQRTSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService

참고 표준 CCM 수퍼 사용자 그룹의 관리자 사용자는 애플리케이션 중 하나에 대해 SSO(Single Sign-On)를 사용하여 Cisco Unified Communications Manager Administration, Cisco Unified Serviceability 및 Cisco Unified Reporting에 액세스할 수 있습니다.

애플리케이션 사용자 작업 흐름

절차

	명령 또는 동작	목적
단계 **1**	새 애플리케이션 사용자 추가, 54 페이지	새 애플리케이션 사용자 추가
단계 **2**	애플리케이션 사용자와 장치 연결, 55 페이지	애플리케이션 사용자와 연결할 장치를 할당합니다.
단계 **3**	Cisco Unity 또는 Cisco Unity Connection에 관리자 사용자 추가, 55 페이지	Cisco Unity 또는 Cisco Unity Connection에 관리자 사용자로 사용자를 추가합니다. Cisco Unified CM 관리에서 애플리케이션 사용자를 구성하고 나서 Cisco Unity 또는 Cisco Unity Connection 관리에서 사용자에 대한 추가 설정을 구성할 수 있습니다.
단계 **4**	애플리케이션 사용자 암호 변경, 56 페이지	애플리케이션 사용자 암호를 변경합니다.
단계 **5**	애플리케이션 사용자 암호 인증서 정보 관리, 57 페이지	인증서 정보(예: 연관된 인증 규칙, 연관된 인증 정책 또는 애플리케이션 사용자가 마지막으로 암호를 변경한 시간)를 변경하거나 확인합니다.

새 애플리케이션 사용자 추가

절차

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 애플리케이션 사용자 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

다음에 할 작업

애플리케이션 사용자와 장치 연결, 55 페이지

애플리케이션 사용자와 장치 연결

절차

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 선택합니다.
사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.

단계 **3** 사용 가능한 장치 목록에서 애플리케이션 사용자와 연결할 장치를 선택하고 목록 아래의 아래쪽 화살표를 클릭합니다. 선택한 장치가 제어된 장치 목록으로 이동합니다.

참고 사용 가능한 장치 목록을 제한하려면 다음과 같이 추가 전화기 찾기 또는 추가 경로 포인트 찾기 단추를 클릭합니다.

단계 **4** 추가 전화기 찾기 단추를 클릭하면 전화기 찾기 및 나열 창이 표시됩니다. 검색을 수행하여 이 애플리케이션 사용자와 연결할 전화기를 찾습니다.
애플리케이션 사용자에게 할당할 각 장치에 대해 위 단계를 반복합니다.

단계 **5** 추가 경로 포인트 찾기 단추를 클릭하면 **CTI** 경로 포인트 찾기 및 나열 창이 표시됩니다. 검색을 수행하여 이 애플리케이션 사용자와 연결할 CTI 경로 포인트를 찾습니다.
애플리케이션 사용자에게 할당할 각 장치에 대해 위 단계를 반복합니다.

단계 **6** 저장을 클릭합니다.

Cisco Unity 또는 Cisco Unity Connection에 관리자 사용자 추가

Cisco Unified Communications Manager를 Cisco Unity Connection 7.x 이상에 통합하려는 경우 이 섹션에 설명된 절차를 수행하는 대신에 Cisco Unity Connection 7.x 이상에 제공되는 가져오기 기능을 사용할 수 있습니다. 가져오기 기능을 사용하는 방법에 대한 자세한 내용은 다음 위치에서 Cisco Unity Connection 7.x 이상 관련 사용자 이동, 추가 및 변경 설명서를 참조하십시오.

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.

Cisco Unity 또는 Cisco Unity Connection 사용자를 Cisco Unified CM 애플리케이션 사용자와 통합할 때 필드를 편집할 수 없습니다. 이러한 필드는 Cisco Unified Communications Manager 관리에서만 업데이트할 수 있습니다.

Cisco Unity 및 Cisco Unity Connection은 Cisco Unified Communications Manager 데이터의 동기화를 모니터링합니다. Cisco Unity 관리 또는 Cisco Unity Connection 관리의 [도구] 메뉴에서 동기화 시간을 구성할 수 있습니다.

시작하기 전에

Cisco Unity 또는 Cisco Unity Connection에 추가할 사용자에게 적합한 템플릿을 정의했는지 확인합니다.

해당하는 Cisco Unity 또는 Cisco Unity Connection 소프트웨어를 설치하고 구성하는 경우에만 **Create Cisco** 사용자 생성 링크가 표시됩니다. 다음 위치에서 해당되는 Cisco Unity 관련 *Cisco Unified Communications Manager* 통합 설명서 또는 해당되는 Cisco Unity Connection 관련 *Cisco Unified Communications Manager SCCP* 통합 설명서를 참조하십시오.

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html.

절차

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 선택합니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.

단계 **3** 관련 링크 드롭다운 목록에서 **Cisco Unity** 애플리케이션 사용자 생성 링크를 선택하고 이동을 클릭합니다.
Cisco Unity 사용자 추가 대화 상자가 표시됩니다.

단계 **4** 애플리케이션 서버 드롭다운 목록에서 Cisco Unity 또는 Cisco Unity Connection 사용자를 생성할 Cisco Unity 또는 Cisco Unity Connection 서버를 선택하고 다음을 클릭합니다.

단계 **5** 애플리케이션 사용자 템플릿 드롭다운 목록에서 사용할 템플릿을 선택합니다.

단계 **6** 저장을 클릭합니다.
Cisco Unity 또는 Cisco Unity Connection에 관리자 계정이 생성됩니다. 애플리케이션 사용자 구성 창에서 [관련 링크]의 링크가 **Edit Cisco** 사용자 편집으로 변경됩니다. 이제 Cisco Unity 관리 또는 Cisco Unity Connection 관리에서 생성한 사용자를 볼 수 있습니다.

애플리케이션 사용자 암호 변경

절차

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 선택합니다.
사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.
애플리케이션 사용자 구성 창에 선택한 애플리케이션 사용자에 대한 정보가 표시됩니다.

단계 **3** 암호 필드에서 기존의 암호화된 암호를 두 번 클릭하고 새 암호를 입력합니다.

단계 **4** 암호 확인 필드에서 암호화되어 있는 기존 암호를 두 번 클릭하고 새 암호를 다시 입력합니다.

단계 **5** 저장을 클릭합니다.

애플리케이션 사용자 암호 인증서 정보 관리

애플리케이션 사용자 암호에 대한 인증서 정보를 관리하려면 다음 절차를 수행합니다. 암호 잠금, 암호에 인증 정책 적용 또는 마지막으로 실패한 로그인 시도 시간과 같은 정보 보기 등의 관리 작업을 수행할 수 있습니다.

절차

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 선택합니다.
사용자 찾기 및 나열 창이 표시됩니다.

단계 **2** 기존 사용자를 선택하려면 사용자 찾기 위치 필드에 적절한 필터를 지정하고 찾기를 선택하여 사용자 목록을 가져온 다음 목록에서 사용자를 선택합니다.
애플리케이션 사용자 구성 창에 선택한 애플리케이션 사용자에 대한 정보가 표시됩니다.

단계 **3** 암호 정보를 변경 또는 확인하려면 암호 필드 옆에 있는 인증서 편집 단추를 클릭합니다.
사용자 인증서 구성 창이 표시됩니다.

단계 **4** 인증서 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **5** 설정을 변경한 경우 저장을 클릭합니다.

III 부

장치 관리

6 장

전화기 관리

전화기 관리 개요

이 장에서는 네트워크의 전화기를 관리하는 방법을 설명합니다. 새 전화기 추가, 다른 사용자에게 기존 전화기 이동, 전화기 잠금 및 전화기 재설정 등의 작업 항목을 설명합니다.

전화기 관리 작업

절차

	명령 또는 동작	목적
단계 **1**	장치 템플릿을 사용하여 새 전화기 추가, 62 페이지	최종 사용자에 대해 새 전화기를 추가하고 범용 장치 템플릿을 할당합니다.
단계 **2**	기존 전화기 이동, 63 페이지	구성된 전화기를 다른 최종 사용자로 이동합니다.
단계 **3**	적극적으로 로그인한 장치 찾기, 63 페이지	특정 장치 또는 사용자가 실제 로그인한 모든 장치를 검색합니다.
단계 **4**	원격으로 로그인된 장치 찾기, 64 페이지	특정 장치 또는 사용자가 원격으로 로그인한 모든 장치를 검색합니다.
단계 **5**	원격으로 전화기 잠금, 65 페이지	일부 전화기는 원격으로 잠글 수 있습니다. 전화기를 원격으로 잠그면 잠금이 해제될 때까지 전화기를 사용할 수 없습니다.

	명령 또는 동작	목적
단계 **6**	전화기를 초기 기본값으로 재설정, 65 페이지	전화기를 초기 설정으로 재설정합니다.
단계 **7**	잠겨 있거나 재설정된 장치 검색, 66 페이지	원격으로 잠그고 원격으로 초기 기본 설정으로 재설정된 장치를 검색합니다.
단계 **8**	전화기의 LSC 상태 보기 및 CAPF 보고서 생성, 67 페이지	전화기에서 LSC 만료 상태를 검색하고 CAPF 보고서도 생성합니다.

장치 템플릿을 사용하여 새 전화기 추가

최종 사용자에 대해 새 전화기를 추가하려면 다음 절차를 수행합니다.

시작하기 전에

전화기를 추가하는 최종 사용자에게 장치 템플릿을 포함하는 사용자 프로파일이 설정되었습니다. Cisco Unified Communications Manager는 범용 장치 템플릿의 설정을 사용하여 전화기를 구성합니다.

- 최종 사용자 관리 작업, 41 페이지

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 빠른/사용자 전화기 추가를 선택합니다.

단계 **2** 찾기를 클릭하고 새 전화기를 추가하려는 최종 사용자를 선택합니다.

단계 **3** 장치 관리 단추를 클릭합니다.
[장치 관리] 창이 나타납니다.

단계 **4** 새 전화기 추가를 클릭합니다.
[사용자에게 전화기 추가] 팝업이 표시됩니다.

단계 **5** 제품 유형 드롭다운 목록에서 전화기 모델을 선택합니다.

단계 **6** 장치 프로토콜 드롭다운에서 프로토콜로 SIP 또는 SCCP를 선택합니다.

단계 **7** 장치 이름 텍스트 상자에 장치 MAC 주소를 입력합니다.

단계 **8** 범용 장치 템플릿 드롭다운 목록에서 범용 장치 템플릿을 선택합니다.

단계 **9** 전화기가 확장 모듈을 지원하는 경우 배포하려는 확장 모듈 수를 입력합니다.

단계 **10** 내선 이동을 사용하여 전화에 액세스하려면 내선 이동에서 확인란을 선택합니다.

단계 **11** 전화기 추가를 클릭합니다.

[새 전화기 추가] 팝업이 닫힙니다. Cisco Unified Communications Manager는 사용자에게 전화기를 추가하고 범용 장치 템플릿을 사용하여 전화기를 구성합니다.

단계 **12** 전화기 구성을 추가 편집하려면 해당 연필 아이콘을 클릭하여 [전화기 구성] 창에서 전화기를 엽니다.

기존 전화기 이동

최종 사용자에게 구성된 전화기를 이동하려면 다음 절차를 수행합니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 빠른/사용자 전화기 추가를 선택합니다.

단계 **2** 찾기를 클릭하고 기존 전화기를 이동할 사용자를 선택합니다.

단계 **3** 장치 관리 단추를 클릭합니다.

단계 **4** 이 사용자로 이동할 전화기 찾기 단추를 클릭합니다.

단계 **5** 이 사용자로 이동하려는 전화기를 선택합니다.

단계 **6** 선택 항목 이동을 클릭합니다.

적극적으로 로그인한 장치 찾기

Cisco Extension Mobility 및 Cisco Extension Mobility Cross Cluster 기능에서는 사용자가 활성 로그인한 장치에 대한 레코드를 유지합니다. Cisco Extension Mobility 기능의 활성 로그인한 장치 보고서에서는 로컬 사용자가 활성 로그인한 로컬 전화기를 추적하고, Cisco Extension Mobility Cross Cluster 기능의 활성 로그인한 장치 보고서에서는 원격 사용자가 활성 로그인한 로컬 전화기를 추적합니다.

Cisco Unified Communications Manager에서는 사용자가 로그인한 장치를 검색하는 특정 검색 창을 제공합니다. 다음 단계에 따라 특정 장치를 검색하거나 사용자가 활성 로그인한 모든 장치를 나열합니다.

절차

단계 **1** 장치 > 전화기를 선택합니다.

단계 **2** 오른쪽 상단의 관련 링크 드롭다운 목록 상자에서 적극적으로 로그인한 장치 보고서를 선택하고 이동을 클릭합니다.

단계 **3** 데이터베이스에서 적극적으로 로그인한 장치 레코드를 모두 찾으려면 대화 상자가 비어 있는지 확인하고 4단계로 이동합니다.
레코드를 필터링하거나 검색하려면 다음을 수행합니다.

a) 첫 번째 드롭다운 목록 상자에서 검색 매개 변수를 선택합니다.
b) 두 번째 드롭다운 목록 상자에서 검색 패턴을 선택합니다.
c) 적절한 검색 텍스트를 지정합니다(해당하는 경우).
참고 다른 검색 기준을 추가하려면 + 단추를 클릭합니다. 기준을 추가하면 시스템에서 지정한 모든 기준과 일치하는 레코드를 검색합니다. 기준을 제거하려면 – 단추를 클릭하여 마지막으로 추가된 기준을 제거하거나 [필터 지우기] 단추를 클릭하여 추가된 검색 기준을 모두 제거합니다.

단계 **4** 찾기를 클릭합니다.
일치하는 레코드가 모두 표시됩니다. [행/페이지] 드롭다운 목록 상자에서 다른 값을 선택하여 각 페이지에 표시할 항목 수를 변경할 수 있습니다.

단계 **5** 표시되는 레코드 목록에서 보려는 레코드의 링크를 클릭합니다.
참고 정렬 순서를 역순으로 변경하려면 목록 헤더에서 위쪽 또는 아래쪽 화살표를 클릭합니다(사용 가능한 경우).
창에 선택한 항목이 표시됩니다.

원격으로 로그인된 장치 찾기

Cisco Extension Mobility Cross Cluster 기능에서는 사용자가 원격으로 로그인한 장치에 대한 레코드를 유지합니다. [원격으로 로그인된 장치] 보고서에서는 다른 클러스터에서 소유하지만 EMCC 기능을 사용 중인 로컬 사용자가 현재 로그인한 전화기를 추적합니다.

Cisco Unified Communications Manager에서는 사용자가 원격으로 로그인한 장치를 검색하기 위한 특정 검색 창을 제공합니다. 다음 단계에 따라 사용자가 원격으로 로그인한 특정 장치를 검색하거나 모든 장치를 나열합니다.

절차

단계 **1** 장치 > 전화기를 선택합니다.
단계 **2** 오른쪽 상단의 관련 링크 드롭다운 목록 상자에서 원격으로 로그인된 장치를 선택하고 이동을 클릭합니다.
단계 **3** 데이터베이스에서 원격으로 로그인된 장치 레코드를 모두 찾으려면 대화 상자가 비어 있는지 확인하고 4단계로 이동합니다.
레코드를 필터링하거나 검색하려면 다음을 수행합니다.
a) 첫 번째 드롭다운 목록 상자에서 검색 매개 변수를 선택합니다.
b) 두 번째 드롭다운 목록 상자에서 검색 패턴을 선택합니다.
c) 적절한 검색 텍스트를 지정합니다(해당하는 경우).
참고 다른 검색 기준을 추가하려면 + 단추를 클릭합니다. 기준을 추가하면 시스템에서 지정한 모든 기준과 일치하는 레코드를 검색합니다. 기준을 제거하려면 – 단추를 클릭하여 마지막으로 추가된 기준을 제거하거나 [필터 지우기] 단추를 클릭하여 추가된 검색 기준을 모두 제거합니다.

단계 **4** [찾기]를 클릭합니다.
일치하는 레코드가 모두 표시됩니다. [행/페이지] 드롭다운 목록 상자에서 다른 값을 선택하여 각 페이지에 표시할 항목 수를 변경할 수 있습니다.

단계 **5** 표시되는 레코드 목록에서 보려는 레코드의 링크를 클릭합니다.
참고 정렬 순서를 역순으로 변경하려면 목록 헤더에서 위쪽 또는 아래쪽 화살표를 클릭합니다(사용 가능한 경우).
창에 선택한 항목이 표시됩니다.

원격으로 전화기 잠금

일부 전화기는 원격으로 잠글 수 있습니다. 전화기를 원격으로 잠그면 잠금이 해제될 때까지 전화기를 사용할 수 없습니다.

전화기에서 원격 잠금 기능이 지원되면 오른쪽 상단 모서리에 잠금 단추가 표시됩니다.

절차

단계 **1** 장치 > 전화기를 선택합니다.

단계 **2** 전화기 찾기 및 나열 창에서 전화기 검색 기준을 입력하고 찾기를 클릭하여 특정 전화기를 찾습니다.
검색 조건과 일치하는 전화기 목록이 표시됩니다.

단계 **3** 원격 잠금을 수행할 전화기를 선택합니다.

단계 **4** 전화기 구성 창에서 잠금을 클릭합니다.
전화기가 등록되어 있지 않은 경우 전화기를 등록한 다음 잠글 수 있음을 알리는 팝업 창이 표시됩니다. 잠금을 클릭합니다.장치 잠금/삭제 상태 섹션에 최신 요청, 대기 중인지 여부 및 최신 확인에 대한 정보가 표시됩니다.

전화기를 초기 기본값으로 재설정

일부 전화기는 원격 삭제 기능을 지원합니다. 전화기에 원격 삭제를 수행하면 해당 작업으로 전화기가 출고시 설정으로 재설정됩니다. 이전에 전화기에 저장한 모든 내용이 삭제됩니다.

전화기에서 원격 삭제 기능이 지원되면 오른쪽 상단 모서리에 삭제단추가 표시됩니다.

⚠

주의 이 작업은 실행 취소할 수 없습니다. 전화기를 출고시 설정으로 재설정해야 할 때만 이 작업을 수행해야 합니다.

절차

단계 **1** 장치 > 전화기를 선택합니다.

단계 **2** 전화기 찾기 및 나열 창에서 전화기 검색 기준을 입력하고 찾기를 클릭하여 특정 전화기를 찾습니다. 검색 조건과 일치하는 전화기 목록이 표시됩니다.

단계 **3** 원격 삭제를 수행할 전화기를 선택합니다.

단계 **4** 전화기 구성 창에서 삭제를 클릭합니다.
전화기가 등록되어 있지 않은 경우 전화기를 등록한 다음 삭제할 수 있음을 알리는 팝업 창이 표시됩니다. 삭제를 클릭합니다.장치 잠금/삭제 상태 섹션에 최신 요청, 대기 중인지 여부 및 최신 확인에 대한 정보가 표시됩니다.

잠겨 있거나 재설정된 장치 검색

원격으로 잠그고 원격으로 초기 기본 설정으로 재설정된 장치를 검색할 수 있습니다. 다음 단계에 따라 원격으로 잠겼거나 원격으로 삭제된 장치 중 특정 장치를 검색하거나 장치를 모두 나열합니다.

절차

단계 **1** 장치 > 전화기를 선택합니다.
[전화기 찾기 및 나열] 창이 표시됩니다. 활성(이전) 쿼리의 레코드가 창에 표시될 수도 있습니다.

단계 **2** 창의 오른쪽 위에 있는 관련 링크 드롭다운 목록 상자에서 전화기 잠금/삭제 보고서를 선택하고 이동을 클릭합니다.

단계 **3** 데이터베이스에서 원격으로 잠기거나 원격으로 삭제된 장치를 모두 찾으려면 텍스트 상자가 비어 있는지 확인하고 4단계로 이동합니다.
특정 장치에 대한 레코드를 필터링하거나 검색하려면:

a) 첫 번째 드롭다운 목록 상자에서 검색할 장치 작업 유형을 선택합니다.
b) 두 번째 드롭다운 목록 상자에서 검색 매개 변수를 선택합니다.
c) 세 번째 드롭다운 목록 상자에서 검색 패턴을 선택합니다.
d) 적절한 검색 텍스트를 지정합니다(해당하는 경우).

참고 다른 검색 기준을 추가하려면 + 단추를 클릭합니다. 기준을 추가하면 시스템에서 지정한 모든 기준과 일치하는 레코드를 검색합니다. 기준을 제거하려면 – 단추를 클릭하여 마지막으로 추가된 기준을 제거하거나 [필터 지우기] 단추를 클릭하여 추가된 검색 기준을 모두 제거합니다.

단계 **4** 찾기를 클릭합니다.
일치하는 레코드가 모두 표시됩니다. [행/페이지] 드롭다운 목록 상자에서 다른 값을 선택하여 각 페이지에 표시할 항목 수를 변경할 수 있습니다.

단계 **5** 표시되는 레코드 목록에서 보려는 레코드의 링크를 클릭합니다.

참고 정렬 순서를 역순으로 변경하려면 목록 헤더에서 위쪽 또는 아래쪽 화살표를 클릭합니다(사용 가능한 경우).

창에 선택한 항목이 표시됩니다.

전화기의 **LSC** 상태 보기 및 **CAPF** 보고서 생성

Cisco Unified Communications Manager 인터페이스 내에서 LSC(Locally Significant Certificate) 만료 정보를 모니터링하려면 이 절차를 사용합니다. 다음 검색 필터는 LSC 정보를 표시합니다.

- LSC 만료일—전화기에 LSC 만료 날짜를 표시합니다.
- LSC 발급자—CAPF 또는 타사의 발급자 이름을 표시합니다.
- LSC 발급자 만료일—발급자의 만료 날짜를 표시합니다.

참고 새 장치에서 발행된 LSC가 없는 경우, **LSC** 만료 및 **LSC** 발급자 만료일 필드의 상태는 "NA"로 설정됩니다.

Cisco Unified Communications Manager 11.5(1)로 업그레이드하기 전에 LSC가 장치로 발행되는 경우, **LSC** 만료 및 **LSC** 발급자 만료일 필드의 상태는 "알 수 없음"으로 설정됩니다.

절차

단계 **1** 장치 > 전화기를 선택합니다.

단계 **2** 첫 번째 전화기 찾기 위치 드롭다운 목록에서 다음 기준 중 하나를 선택합니다.

- LSC 만료일
- LSC 발급자
- LSC 발급자 만료일

두 번째 전화기 찾기 위치 드롭다운 목록에서 다음 기준 중 하나를 선택합니다.

- 이전
- 정확하게 일치
- 이후
- 시작 단어
- 포함
- 끝 단어

- 정확하게 일치
- 비어 있음
- 비어 있지 않음

단계 **3** 찾기를 클릭합니다.
검색된 전화기 목록이 표시됩니다.

단계 **4** 관련 링크 드롭다운 목록에서 파일의 **CAPF** 보고서를 선택하고 이동을 클릭합니다.
보고서가 다운로드됩니다.

7장

장치 펌웨어 관리

장치 펌웨어 업데이트 개요

장치 로드는 IP 전화기, TelePresence 시스템 및 Cisco Unified Communications Manager에 프로비저닝되고 등록된 시스템 같은 장치용 소프트웨어 및 펌웨어입니다. 설치 또는 업그레이드 동안 Cisco Unified Communications Manager는 Cisco Unified Communications Manager의 버전이 릴리스된 시기를 기반으로 사용할 수 있는 최신 로드를 포함합니다. Cisco는 새 기능과 소프트웨어 수정 프로그램을 소개하기 위해 정기적으로 업데이트된 펌웨어를 릴리스하며 해당 로드를 포함하는 Cisco Unified Communications 업그레이드를 기다리지 않고 최신 로드로 전화기를 업데이트할 수 있습니다.

엔드포인트를 소프트웨어의 새 버전으로 업그레이드하기 전에 새 로드에 필요한 파일을 엔드포인트가 액세스할 수 있는 위치로 다운로드할 수 있어야 합니다. 가장 일반적인 위치는 "TFTP 서버"라고 하는 Cisco TFTP 서비스가 활성화된 Cisco UCM 노드입니다. 또한 일부 전화기는 "로드 서버"라고 하는 대체 다운로드 위치를 사용하여 지원됩니다.

서버에 있는 tftp 디렉터리에 이미 있는 파일을 나열하거나, 보거나, 다운로드하려는 경우 CLI 명령 file list tftp를 사용하여 TFTP 디렉터리에 있는 파일을 확인하고 file view tftp를 사용하여 파일을 보고 file get tftp를 사용하여 TFTP 디렉터리에 있는 파일을 복사합니다. 자세한 내용은 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오. 또한 웹 브라우저를 사용하여 URL "http://<tftp_server>:6970/<filename>"으로 이동하여 TFTP 파일을 다운로드할 수도 있습니다.

팁 시스템 차원의 기본값으로 구성하기 전에 단일 장치에 새 로드를 적용할 수 있습니다. 이 방법은 테스트 목적으로 유용합니다. 그러나 해당 유형의 다른 모든 장치가 새로운 로드로 시스템 차원의 기본값을 업데이트할 때까지 기존 로드를 사용합니다.

장치 팩 또는 개별 장치 펌웨어 설치

장치 패키지를 설치하여 새 전화기 유형을 소개하고 여러 전화기 모델에 대한 펌웨어를 업그레이드합니다. 기존 장치에 대한 개별 펌웨어는 다음 옵션을 사용하여 설치 또는 업그레이드할 수 있습니다.

- Cisco 옵션 패키지(COP) 파일—COP 파일에는 게시자에 설치했을 때 펌웨어 파일 설치와 별도로 기본 펌웨어를 업데이트하도록 펌웨어 파일과 데이터베이스 업데이트가 포함되어 있습니다.
- 펌웨어 파일만—zip 파일로 제공되고, 개별 장치 펌웨어 파일이 포함되어 있으며 수동으로 압축을 풀어 TFTP 서버의 해당 디렉터리로 업로드해야 합니다.

참고 COP 또는 펌웨어 파일 패키지의 설치 절차는 README 파일을 참조하십시오.

게시자 서버와 TFTP 서버부터 시작하여 모든 Cisco Unified Communications Manager 서버에 장치 패키지를 적용합니다. 시스템은 Cisco가 승인한 소프트웨어만 업로드 및 처리할 수 있습니다. Cisco Unified Communications Manager의 이전 버전에서 사용한 타사 또는 Windows 기반 소프트웨어 애플리케이션은 설치 또는 사용할 수 없습니다.

시작하기 전에

참고 게시자 노드를 재부팅하고 TFTP 서비스와 Tomcat 서비스가 실행되고 있는 모든 노드에서 이러한 서비스를 다시 시작합니다.

절차

단계 **1** Cisco Unified OS 관리에서 소프트웨어 업그레이드 > 설치/업그레이드를 선택합니다.

단계 **2** [소프트웨어 위치] 섹션에서 해당 값을 입력하고 다음을 클릭합니다.

단계 **3** 사용 가능한 소프트웨어 드롭다운 목록에서 장치 패키지 파일을 선택하고 다음을 클릭합니다.

단계 **4** MD5 값이 올바른지 확인하고 다음을 클릭합니다.

단계 **5** 경고 상자에서 올바른 펌웨어를 선택했는지 확인한 다음 설치를 클릭합니다.

단계 **6** 성공 메시지가 수신되었는지 확인합니다.

참고 클러스터를 재부팅하는 경우 8단계로 건너뛰니다.

단계 **7** TFTP 서버를 중지하고 다시 시작합니다.

단계 **8** 영향을 받는 장치를 재설정하여 장치를 새 로드로 업그레이드합니다.

단계 **9** Cisco Unified CM 관리에서 장치 > 장치 설정 > 장치 기본값을 선택하고 로드 파일(특정 장치)의 이름을 새 로드로 수동으로 변경합니다.

단계 **10** 저장을 클릭한 다음, 장치를 재설정합니다.

시스템에서 사용하지 않는 펌웨어 제거

장치 로드 관리 창을 사용하면 시스템에서 사용하지 않는 펌웨어(장치 로드) 및 관련 파일을 삭제하여 디스크 공간을 늘릴 수 있습니다. 예를 들어, 업그레이드하기 전에 사용하지 않는 로드를 삭제하여 디스크 공간 부족으로 인한 업그레이드 오류를 방지할 수 있습니다. 일부 펌웨어 파일에는 장치 로드 관리 창에 나열되지 않는 종속성 파일이 있을 수 있습니다. 펌웨어를 삭제하면 종속 파일도 삭제됩니다. 그러나 추가 펌웨어와 연결된 경우 종속 파일이 삭제되지 않습니다.

참고 클러스터의 각 서버에 대해 사용하지 않는 펌웨어를 개별적으로 삭제해야 합니다.

시작하기 전에

주의 사용하지 않는 펌웨어를 삭제하기 전에 올바른 로드를 삭제하고 있는지 확인합니다. 전체 클러스터의 DRS 복원을 수행하지 않고는 삭제된 로드를 복원할 수 없습니다. 펌웨어를 삭제하기 전에 백업을 수행하는 것이 좋습니다.

절차

단계 **1** Cisco Unified OS 관리에서 소프트웨어 업그레이드 > 장치 로드 관리를 선택합니다.

단계 **2** 검색 기준을 지정하고 찾기를 클릭합니다.

단계 **3** 삭제할 장치 로드를 선택합니다. 필요한 경우 여러 로드를 선택할 수 있습니다.

단계 **4** 선택한 로드 삭제를 클릭합니다.

단계 **5** 확인을 클릭합니다.

전화기 모델에 대한 기본 펌웨어 설정

이 절차를 사용하여 특정 전화기 모델에 대한 기본 펌웨어 로드를 설정합니다. 새 전화기를 등록하면 Cisco Unified Communications Manager는 전화기 구성이 전화기 구성 창에 지정된 펌웨어 로드를 제정의하지 않는 경우 전화기에 기본 펌웨어를 전송하려고 시도합니다.

참고 개별 전화기의 경우 전화기 구성 창에서 전화기 로드 이름 필드의 설정은 해당 특정 전화기에 대한 기본 펌웨어 로드를 재정의합니다.

시작하기 전에

TFTP 서버에 펌웨어가 로드되었는지 확인합니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 장치 > 장치 설정 > 장치 기본값을 선택합니다.
Cisco Unified Communications Manager가 지원하는 다양한 전화기 모델에 대한 기본 펌웨어 로드를 표시하는 장치 기본값 구성 창이 나타납니다. 펌웨어는 로드 정보 열에 나타납니다.

단계 **2** 장치 유형 아래에서 기본 펌웨어를 할당하려는 전화기 모델을 찾습니다.

단계 **3** 관련 로드 정보 필드에 펌웨어 로드를 입력합니다.

단계 **4** (선택 사항) 해당 전화기 모델에 대한 기본 장치 풀 및 기본 전화기 템플릿을 입력합니다.

단계 **5** 저장을 클릭합니다.

전화기에 대한 펌웨어 로드 설정

특정 전화기에 대한 펌웨어 로드를 할당하려면 이 절차를 사용합니다. 장치 기본값 구성 창에 지정된 기본값 이외의 다른 펌웨어 로드를 사용하려면 이 작업을 수행할 수 있습니다.

참고 여러 전화기에 대해 버전을 지정하려는 경우 Bulk Administration Tool을 사용하여 CSV 파일 또는 쿼리를 사용하는 전화기 로드 이름 필드를 구성할 수 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.

절차

단계 **1** Cisco Unified CM 관리에서 장치 > 전화기를 선택합니다.

단계 **2** 찾기를 클릭하고 개별 전화기를 선택합니다.

단계 **3** 전화기 로드 이름 필드에 펌웨어 이름을 입력합니다. 이 전화기에 대해 여기에 지정된 펌웨어 로드는 장치 기본값 구성 창에 지정된 기본 펌웨어 로드를 재정의합니다.

단계 **4** 전화기 구성 창의 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

단계 **6** 구성 적용을 클릭하여 변경된 필드를 전화기에 적용할 수 있습니다.

로드 서버 사용

전화기에서 TFTP 서버가 아닌 서버에서 펌웨어 업데이트를 다운로드하도록 하려면 전화기의 전화기 구성 페이지에 "로드 서버"를 구성할 수 있습니다. 로드 서버는 다른 Cisco Unified Communications Manager 또는 타사 서버일 수 있습니다. 타사 서버는 TCP 포트 6970(기본 설정)의 HTTP 또는 UDP 기반 TFTP 프로토콜을 통해 전화기가 요청하는 파일을 제공할 수 있어야 합니다. DX 제품군 Cisco TelePresence 장치와 같은 일부 전화기 모델만 펌웨어 업데이트를 위해 HTTP를 지원합니다.

참고 여러 전화기에 대해 로드 서버를 지정하려는 경우 Bulk Administration Tool을 사용하여 CSV 파일 또는 쿼리를 사용하는 로드 서버 필드를 구성할 수 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.

절차

단계 **1** Cisco Unified CM 관리에서 장치 > 전화기를 선택합니다.

단계 **2** 찾기를 클릭하고 개별 전화기를 선택합니다.

단계 **3** 로드 서버 필드에 대체 서버의 IP 주소 또는 호스트 이름을 입력합니다.

단계 **4** 전화기 구성 창의 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

단계 **6** 구성 적용을 클릭하여 변경된 필드를 전화기에 적용할 수 있습니다.

8 장

인프라 장치 관리

인프라 관리 개요

이 장에서는 위치 인식 기능의 일부로 스위치 및 무선 액세스 지점과 같은 네트워크 인프라 장치를 관리하는 작업에 대해 설명합니다. 위치 인식이 활성화되면 Cisco Unified Communications Manager 데이터베이스는 현재 각 스위치 또는 액세스 지점에 연결하는 엔드포인트의 목록을 포함하여 네트워크의 스위치 및 액세스 지점에 대한 상태 정보를 저장합니다.

엔드포인트와 인프라 장치 매핑을 사용하면 Cisco Unified Communications Manager 및 Cisco Emergency Responder에서 발신자의 물리적 위치를 확인할 수 있습니다. 예를 들어, 로밍 상황에 있는 동안 모바일 클라이언트에서 비상 통화를 하는 경우 Cisco Emergency Responder는 매핑을 사용하여 비상 서비스를 전송할 위치를 결정합니다.

데이터베이스에 저장된 인프라 정보도 인프라 사용량을 모니터링하는 데 도움이 됩니다. Cisco Unified Communications Manager 인터페이스에서 스위치 및 무선 액세스 지점 같은 네트워크 인프라 장치를 볼 수 있습니다. 또한 현재 특정 액세스 지점 또는 스위치에 연결하는 엔드포인트의 목록을 볼 수도 있습니다. 인프라 장치를 사용하지 않는 경우 인프라 장치의 추적을 비활성화할 수 있습니다.

인프라 필수 구성 요소 관리

Cisco Unified Communications Manager 인터페이스 내에서 무선 인프라를 관리하기 전에 위치 인식 기능을 구성해야 합니다. 유선 인프라의 경우 기능이 기본적으로 활성화됩니다. 구성 세부 사항은 다음 장을 참조하십시오.

Cisco Unified Communications Manager 시스템 구성 설명서의 "위치 인식".

네트워크 인프라도 설치해야 합니다. 자세한 내용은 무선 LAN 컨트롤러, 액세스 지점 및 스위치 같은 인프라 장치와 함께 제공되는 하드웨어 설명서를 참조하십시오.

인프라 작업 흐름 관리

네트워크 인프라 장치를 모니터링하고 관리하려면 다음 작업을 수행합니다.

절차

	명령 또는 동작	목적
단계 **1**	인프라 장치에 대한 상태 보기, 76 페이지	무선 액세스 지점 또는 이더넷 스위치(관련 엔드포인트 목록 포함)의 현재 상태를 가져옵니다.
단계 **2**	인프라 장치에 대한 추적 비활성화, 76 페이지	사용되지 않는 스위치 또는 액세스 지점이 있는 경우 장치를 비활성으로 표시합니다. 시스템은 인프라 장치에 대한 상태 또는 연결된 엔드포인트의 목록을 업데이트하는 것을 중지합니다.
단계 **3**	비활성화된 인프라 장치에 대한 추적 활성화, 77 페이지	비활성 인프라 장치에 대한 추적을 시작합니다. Cisco Unified Communications Manager는 인프라 장치에 대한 상태 및 연결된 엔드포인트의 목록으로 데이터베이스 업데이트를 시작합니다.

인프라 장치에 대한 상태 보기

무선 액세스 지점 또는 이더넷 스위치 같은 인프라 장치의 현재 상태를 가져오려면 이 절차를 사용합니다. Cisco Unified Communications Manager 인터페이스 내에서 액세스 지점이나 스위치에 대한 상태를 보고 연결된 엔드포인트의 현재 목록을 볼 수 있습니다.

절차

단계 **1** Cisco Unified CM 관리에서 고급 기능 > 장치 위치 추적 서비스 > 스위치 및 액세스 지점을 선택합니다.

단계 **2** 찾기를 클릭합니다.

단계 **3** 상태를 원하는 스위치 또는 액세스 지점을 클릭합니다.
스위치 및 액세스 지점 구성 창에는 현재 액세스 지점 또는 스위치에 연결하는 엔드포인트의 목록을 포함한 현재 상태가 표시됩니다.

인프라 장치에 대한 추적 비활성화

스위치 또는 액세스 지점 같은 특정 인프라 장치에 대한 추적을 제거하려면 이 절차를 사용합니다. 사용되지 않는 스위치 또는 액세스 지점에 대해 이 작업을 수행할 수 있습니다.

참고 인프라 장치에 대한 추적을 제거하는 경우 장치는 데이터베이스에 남지만 비활성화됩니다. Cisco Unified Communications Manager는 인프라 장치에 연결된 엔드포인트의 목록을 포함하여 장치의 상태를 더 이상 업데이트하지 않습니다. 스위치 및 액세스 지점 창의 관련 링크 드롭다운에서 비활성 스위치와 액세스 포인트를 볼 수 있습니다.

절차

단계 **1** Cisco Unified CM 관리에서 고급 기능 > 장치 위치 추적 서비스 > 스위치 및 액세스 지점을 선택합니다.

단계 **2** 찾기를 클릭하고 추적을 중지하려는 스위치 또는 액세스 지점을 선택합니다.

단계 **3** 선택한 항목 비활성화를 클릭합니다.

비활성화된 인프라 장치에 대한 추적 활성화

비활성화된 비활성 인프라 장치에 대한 추적을 시작하려면 이 절차를 사용합니다. 스위치 또는 액세스 지점이 활성화되면 Cisco Unified Communications Manager는 스위치 또는 액세스 지점에 연결하는 엔드포인트의 목록을 포함하여 상태를 동적으로 추적하기 시작합니다.

시작하기 전에

위치 인식을 구성해야 합니다. 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "위치 인식" 장을 참조하십시오.

절차

단계 **1** Cisco Unified CM 관리에서 고급 기능 > 장치 위치 추적 서비스 > 스위치 및 액세스 지점을 선택합니다.

단계 **2** 관련 링크에서 비활성 스위치 및 액세스 지점을 선택하고 이동을 클릭합니다.
비활성 스위치 및 액세스 지점 찾기 및 나열 창에 추적되지 않는 인프라 장치가 표시됩니다.

단계 **3** 추적을 시작하려는 스위치 또는 액세스 지점을 선택합니다.

단계 **4** 선택한 항목 재활성화를 클릭합니다.

IV 부

시스템 관리

9 장

시스템 상태 모니터링

클러스터 노드 상태 보기

클러스터의 노드에 대한 정보를 표시하려면 이 절차를 사용합니다.

절차

단계 **1** Cisco Unified Operating System 관리에서 표시 > 클러스터를 선택합니다.

단계 **2** 클러스터 창에서 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

하드웨어 상태 보기

이 절차를 사용하여 시스템의 하드웨어 상태 및 하드웨어 리소스에 대한 정보를 표시합니다.

절차

단계 **1** Cisco Unified Operating System 관리에서 표시 > 하드웨어를 선택합니다.

단계 **2** 하드웨어 상태 창에서 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

네트워크 상태 보기

이더넷 및 DNS 정보 같은 시스템의 네트워크 상태를 표시하려면 이 절차를 사용합니다.

표시되는 네트워크 상태 정보는 네트워크 장애 허용 오차가 활성화되었는지 여부에 따라 다릅니다.

- 네트워크 장애 허용 오차가 활성화된 경우 이더넷 포트 0이 실패하면 이더넷 포트 1이 자동으로 통신 네트워크를 관리합니다.
- 네트워크 장애 허용 오차가 활성화된 경우 이더넷 0, 이더넷 1 Bond 0에 대한 네트워크 상태 정보가 표시됩니다.
- 네트워크 장애 허용 오차가 활성화되지 않은 경우 이더넷 0에 대한 상태 정보만 표시됩니다.

절차

단계 **1** Cisco Unified Operating System 관리에서 표시 > 네트워크를 선택합니다.

단계 **2** 네트워크 구성 창에서 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

설치된 소프트웨어 보기

소프트웨어 버전 및 설치된 소프트웨어 패키지에 대한 정보를 보려면 이 절차를 사용합니다.

절차

단계 **1** Cisco Unified Operating System 관리에서 표시 > 소프트웨어를 선택합니다.

단계 **2** 소프트웨어 패키지 창에서 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

시스템 상태 보기

로캘, 가동 시간, CPU 사용 및 메모리 사용에 대한 정보 같이 전체 시스템 상태를 표시하려면 이 절차를 사용합니다.

절차

단계 **1** Cisco Unified Operating System 관리에서 표시 > 시스템을 선택합니다.

단계 **2** 시스템 상태 창에서 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

IP 환경 설정 보기

이 절차를 사용하여 시스템에 사용할 수 있는 등록된 포트 목록을 표시합니다.

절차

단계 **1** Cisco Unified Operating System 관리에서 표시 > **IP** 환경 설정을 선택합니다.

단계 **2** (선택 사항) 레코드를 필터링하거나 검색하려면 다음 작업 중 하나를 수행합니다.

- 첫 번째 목록에서 검색 매개 변수를 선택합니다.
- 두 번째 목록에서 검색 패턴을 선택합니다.
- 적절한 검색 텍스트를 지정합니다(해당하는 경우).

단계 **3** 찾기를 클릭합니다.

단계 **4** 시스템 상태 창에 나타나는 필드를 검토합니다. 필드에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

마지막 로그인 세부 정보 보기

최종 사용자(로컬 및 LDAP 인증서) 및 관리자가 Cisco Unified Communications Manager 또는 IM and Presence Service용 웹 애플리케이션에 로그인하면 메인 애플리케이션 창에 최근 성공/실패한 로그인 세부 정보가 표시됩니다.

SAML SSO 기능을 사용하여 로그인하는 사용자는 마지막 성공적인 시스템 로그인 정보만 볼 수 있습니다. 사용자는 IdP(ID 공급자) 애플리케이션을 참조하여 실패한 SAML SSO 로그인 정보를 추적할 수 있습니다.

다음 웹 애플리케이션은 로그인 시도 정보를 표시합니다.

- Cisco Unified Communications Manager:
  - Cisco Unified CM 관리
  - Cisco Unified Reporting
  - Cisco Unified Serviceability
- IM and Presence 서비스
  - Cisco Unified CM IM and Presence 관리
  - Cisco Unified IM and Presence 보고
  - Cisco Unified IM and Presence 서비스 가용성

관리자만 로그인하여 Cisco Unified Communications Manager의 다음 웹 애플리케이션에 대한 마지막 로그인 세부 정보를 볼 수 있습니다.

- 재해 복구 시스템
- Cisco Unified OS Administration

노드 Ping

네트워크의 다른 노드를 Ping하려면 Ping 유틸리티를 사용합니다. 그 결과는 장치 연결을 확인하거나 문제 해결에 도움이 될 수 있습니다.

절차

단계 **1** Cisco Unified Operating System 관리에서 서비스 > **Ping**을 선택합니다.

단계 **2** **Ping** 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **3** **Ping**을 선택합니다.
Ping 결과가 표시됩니다.

서비스 매개 변수 표시

클러스터의 모든 서버에서 특정 서비스에 속한 모든 서비스 매개 변수를 비교해야 할 수 있습니다. 또한 동기화되지 않은 매개 변수(즉, 값이 서버 간에 다른 서비스 매개 변수)나 제안 값에서 수정된 매개 변수만 표시해야 할 수도 있습니다.

다음 절차에 따라 클러스터의 모든 서버에서 특정 서비스의 서비스 매개 변수를 표시합니다.

절차

단계 **1** 시스템 > 서비스 매개 변수를 선택합니다.

단계 **2** [서버] 드롭다운 목록 상자에서 서버를 선택합니다.

단계 **3** [서비스] 드롭다운 목록 상자에서 클러스터의 모든 서버에서 서비스 매개 변수를 표시할 서비스를 선택합니다.

참고 [서비스 매개 변수 구성] 창에 서비스(활성 또는 비활성)가 모두 표시됩니다.

단계 **4** 표시되는 [서비스 매개 변수 구성] 창의 [관련 링크] 드롭다운 목록 상자에서 [모든 서버에 대한 매개 변수]를 선택한 다음 [이동]을 클릭합니다.

[모든 서버에 대한 매개 변수] 창이 표시됩니다. 목록에 현재 서비스에 대한 모든 매개 변수가 사전순으로 표시됩니다. 각 매개 변수마다 매개 변수 이름 옆에 제안 값이 표시됩니다. 각 매개 변수 이름 아래에 이 매개 변수를 포함하는 서버의 목록이 표시됩니다. 각 서버 이름 옆에는 현재 서버의 이 매개 변수에 대한 현재 값이 표시됩니다.

지정된 매개 변수에 대해 서버 이름이나 현재 매개 변수 값을 클릭하여 해당 서비스 매개 변수 창에 연결하여 값을 변경합니다. [모든 서버에 대한 매개 변수] 창 사이를 이동하려면 [이전] 및 [다음]을 클릭합니다.

단계 **5** 동기화되지 않은 매개 변수를 표시해야 하는 경우 [관련 링크] 드롭다운 목록 상자에서 [모든 서버에 대한 동기화되지 않은 매개 변수]를 선택한 다음 [이동]을 클릭합니다.

[모든 서버에 대한 동기화되지 않은 매개 변수] 창이 표시됩니다. 현재 서비스에 대해 서버 간에 값이 다른 서비스 매개 변수가 사전순으로 표시됩니다. 각 매개 변수마다 매개 변수 이름 옆에 제안 값이 표시됩니다. 각 매개 변수 이름 아래에 이 매개 변수를 포함하는 서버의 목록이 표시됩니다. 각 서버 이름 옆에는 현재 서버의 이 매개 변수에 대한 현재 값이 표시됩니다.

지정된 매개 변수에 대해 서버 이름이나 현재 매개 변수 값을 클릭하여 해당 서비스 매개 변수 창에 연결하여 값을 변경합니다. [모든 서버에 대한 동기화되지 않은 매개 변수] 창 사이를 이동하려면 [이전] 및 [다음]을 클릭합니다.

단계 **6** 제안 값에서 수정된 서비스 매개 변수를 표시해야 하는 경우 [관련 링크] 드롭다운 목록 상자에서 [모든 서버에 대한 수정된 매개 변수]를 선택한 다음 [이동]을 클릭합니다.

[모든 서버에 대한 수정된 매개 변수] 창이 표시됩니다. 현재 서비스에 대해 값이 제안 값과 다른 서비스 매개 변수가 사전순으로 표시됩니다. 각 매개 변수마다 매개 변수 이름 옆에 제안 값이 표시됩니다. 각 매개 변수 이름 아래에 값이 제안 값과 다른 서버의 목록이 표시됩니다. 각 서버 이름 옆에는 현재 서버의 이 매개 변수에 대한 현재 값이 표시됩니다.

지정된 매개 변수에 대해 서버 이름이나 현재 매개 변수 값을 클릭하여 해당 서비스 매개 변수 창에 연결하여 값을 변경합니다. [모든 서버에 대한 수정된 매개 변수] 창 사이를 이동하려면 [이전] 및 [다음]을 클릭합니다.

10 장

사용 레코드 보기

사용 레코드 개요

Cisco Unified Communications Manager는 구성된 항목이 시스템에서 사용되는 방식을 확인할 수 있는 레코드를 제공합니다. 구성된 항목은 장치 풀, 날짜 및 시간 그룹, 경로 플랜 같은 시스템 수준 설정 및 장치를 포함합니다.

종속성 레코드

다음 목적으로 종속성 레코드를 사용합니다.

- 서버, 장치 풀, 날짜 및 시간 그룹 등의 시스템 수준 설정에 대한 정보를 찾습니다.
- 다른 레코드를 사용하는 데이터베이스의 레코드를 확인합니다. 예를 들어 특정 발신 검색 공간을 사용하는 장치(예: CTI 경로 포인트 또는 전화기)를 확인할 수 있습니다.
- 레코드를 삭제하기 전에 레코드 간의 종속성을 표시합니다. 예를 들어, 파티션을 삭제하기 전에 종속성 레코드를 사용하여 어떤 발신 검색 공간(CSS) 및 장치가 연결되어 있는지 확인합니다. 그런 다음 설정을 재구성하여 종속성을 제거할 수 있습니다.

경로 플랜 보고서

경로 플랜 보고서를 사용하면 시스템에 구성된 숫자, 경로 및 패턴의 일부 또는 전체 목록을 볼 수 있습니다. 보고서를 생성하면 보고서의 패턴/디렉터리 번호, 파티션 또는 경로 세부 정보 열에서 항목을 클릭하여 각 항목에 대한 구성 창에 액세스할 수 있습니다.

또한 경로 플랜 보고서를 사용하면 보고서 데이터를 .CSV 파일로 저장하여 다른 애플리케이션으로 가져올 수 있습니다. 이 .CSV 파일에는 전화기의 디렉터리 번호, 경로 패턴, 패턴 사용, 장치 이름 및 장치 설명을 비롯하여 웹 페이지보다 더 자세한 정보가 포함됩니다.

Cisco Unified Communications Manager 는 경로 플랜을 사용하여 내부 통화와 외부 PSTN(Public Switched Telephone Network) 통화를 모두 라우팅합니다. 네트워크에 레코드가 여러 개 있을 수 있으므로 Cisco Unified Communications Manager 관리에서는 특정 기준을 기준으로 특정 경로 플랜 레코드를 찾을 수 있습니다.

사용 보고서 작업

절차

	명령 또는 동작	목적
단계 **1**	경로 플랜 레코드를 보고 이를 사용하여 할당되지 않은 디렉터리 번호를 관리하려면 다음 절차를 참조하십시오. • 경로 플랜 레코드 보기, 89 페이지 • 경로 플랜 보고서 저장, 89 페이지 • 할당되지 않은 디렉터리 번호 삭제, 90 페이지 • 할당되지 않은 디렉터리 번호 업데이트, 90 페이지	이 절차를 사용하여 특정 경로 플랜 레코드를 찾고 CSV 파일에 레코드를 저장하고 할당되지 않은 디렉터리 번호를 관리합니다.
단계 **2**	종속성 레코드를 사용하려면 다음 절차를 참조하십시오. • • 종속성 레코드 보기, 92 페이지	이 절차를 사용하여 시스템 수준 설정에 대한 정보를 찾고 데이터베이스에 있는 레코드 사이의 종속성을 표시합니다.

경로 플랜 보고서 작업 흐름

절차

	명령 또는 동작	목적
단계 **1**	경로 플랜 레코드 보기, 89 페이지.	경로 플랜 레코드를 확인하고 사용자 정의된 경로 플랜 보고서를 생성합니다.
단계 **2**	경로 플랜 보고서 저장, 89 페이지.	.csv 파일 형식으로 경로 플랜 보고서를 봅니다.

	명령 또는 동작	목적
단계 **3**	할당되지 않은 디렉터리 번호 삭제, 90 페이지.	경로 플랜 보고서에서 할당되지 않은 디렉터리 번호를 삭제합니다.
단계 **4**	할당되지 않은 디렉터리 번호 업데이트, 90 페이지.	경로 플랜 보고서에서 할당되지 않은 디렉터리 번호 설정을 업데이트합니다.

경로 플랜 레코드 보기

이 섹션에서는 경로 플랜 레코드를 보는 방법을 설명합니다. 네트워크에 레코드가 여러 개 있을 수 있으므로 Cisco Unified Communications Manager 관리에서는 특정 기준을 기준으로 특정 경로 플랜 레코드를 찾을 수 있습니다. 다음 절차를 사용하여 사용자 정의된 경로 플랜 보고서를 생성합니다.

절차

단계 **1** 통화 라우팅 > 경로 플랜 보고서를 선택합니다.

단계 **2** 데이터베이스에서 모든 레코드를 찾으려면 대화 상자가 비어 있는지 확인하고 3단계로 이동합니다. 레코드를 필터링하거나 검색하려면 다음을 수행합니다.

a) 첫 번째 드롭다운 목록 상자에서 검색 매개 변수를 선택합니다.
b) 두 번째 드롭다운 목록 상자에서 검색 패턴을 선택합니다.
c) 적절한 검색 텍스트를 지정합니다(해당하는 경우).

단계 **3** 찾기를 클릭합니다.
모든 또는 일치하는 레코드가 표시됩니다. [행/페이지] 드롭다운 목록 상자에서 다른 값을 선택하여 각 페이지에 표시할 항목 수를 변경할 수 있습니다.

단계 **4** 표시되는 레코드 목록에서 보려는 레코드의 링크를 클릭합니다.
창에 선택한 항목이 표시됩니다.

경로 플랜 보고서 저장

이 섹션에는 경로 플랜 보고서를 .csv 파일로 보는 방법에 대한 내용이 있습니다.

절차

단계 **1** 통화 라우팅 > 경로 플랜 보고서를 선택합니다.

단계 **2** 경로 플랜 보고서 창의 관련 링크 드롭다운 목록에서 파일로 보기를 선택한 다음 이동을 클릭합니다.
나타나는 대화 상자에서 파일을 저장하거나 다른 애플리케이션으로 가져올 수 있습니다.

단계 **3** 저장을 클릭합니다.
선택한 위치에 이 파일을 저장할 수 있는 다른 창이 표시됩니다.

참고 또한 파일을 다른 파일 이름으로 저장할 수 있으며, 파일 이름에 .CSV 확장자가 포함되어야 합니다.

단계 **4** 파일을 저장할 위치를 선택하고 저장을 클릭합니다. 이 작업은 지정한 위치에 파일을 저장해야 합니다.

단계 **5** 방금 저장한 .CSV 파일을 찾아 해당 아이콘을 두 번 클릭하여 파일을 확인합니다.

할당되지 않은 디렉터리 번호 삭제

이 섹션에서는 경로 플랜 보고서에서 할당되지 않은 디렉터리 번호를 삭제하는 방법을 설명합니다. 디렉터리 번호는 Cisco Unified Communications Manager 관리의 [디렉터리 번호 구성] 창에서 구성 및 제거됩니다. 장치에서 디렉터리 번호를 제거하거나 전화기를 삭제해도 디렉터리 번호는 Cisco Unified Communications Manager 데이터베이스에서 계속 유지됩니다. 데이터베이스에서 디렉터리 번호를 삭제하려면 [경로 플랜 보고서] 창을 사용합니다.

절차

단계 **1** 통화 라우팅 > 경로 플랜 보고서를 선택합니다.

단계 **2** [경로 플랜 보고서] 창에서 3개의 드롭다운 목록을 사용하여 할당되지 않은 모든 DN을 나열하는 경로 플랜 보고서를 지정합니다.

단계 **3** 다음과 같이 세 가지 방법으로 디렉터리 번호를 삭제할 수 있습니다.

a) 삭제할 디렉터리 번호를 클릭합니다. [디렉터리 번호 구성] 창이 표시되면 [삭제]를 클릭합니다.
b) 삭제할 디렉터리 번호 옆의 확인란을 선택합니다. 선택한 항목 삭제를 클릭합니다.
c) 할당되지 않은 것으로 확인된 디렉터리 번호를 모두 삭제하려면 [찾은 항목 모두 삭제]를 클릭합니다.
경고 메시지가 표시되고 디렉터리 번호를 삭제할 것인지 확인합니다.

단계 **4** 디렉터리 번호를 삭제하려면 [확인]을 클릭합니다. 삭제 요청을 취소하려면 [취소]를 클릭합니다.

할당되지 않은 디렉터리 번호 업데이트

이 섹션에서는 경로 플랜 보고서에서 할당되지 않은 디렉터리 번호의 설정을 업데이트하는 방법을 설명합니다. 디렉터리 번호는 Cisco Unified Communications Manager 관리의 [디렉터리 번호 구성] 창에서 구성 및 제거됩니다. 장치에서 디렉터리 번호를 제거해도 Cisco Unified Communications Manager 데이터베이스에서 디렉터리 번호가 계속 유지됩니다. 디렉터리 번호 설정을 업데이트하려면 [경로 플랜 보고서] 창을 사용합니다.

절차

단계 **1** 통화 라우팅 > 경로 플랜 보고서를 선택합니다.

단계 **2** 경로 플랜 보고서 창에서 3개의 드롭다운 목록을 사용하여 할당되지 않은 모든 DN을 나열하는 경로 플랜 보고서를 지정합니다.

단계 **3** 업데이트할 디렉터리 번호를 클릭합니다.

참고 디렉터리 번호 및 파티션을 제외한 디렉터리 번호의 모든 설정을 업데이트할 수 있습니다.

단계 **4** 발신 검색 공간 또는 착신 전환 옵션과 같이 필요한 업데이트를 수행합니다.

단계 **5** 저장을 클릭합니다.

[디렉터리 번호 구성] 창이 다시 표시되고 [디렉터리 번호] 필드가 비어 있습니다.

종속성 레코드 작업 흐름

절차

	명령 또는 동작	목적
단계 **1**	종속성 레코드 구성, 91 페이지.	종속성 레코드를 활성화하거나 비활성화하려면 이 절차를 사용합니다. 다이얼 플랜 크기와 복잡성, CPU 속도 및 기타 애플리케이션의 CPU 요구 사항으로 인해, 이 절차가 일반 우선 순위보다 낮은 우선 순위로 실행되고 완료하는 데 시간이 오래 걸릴 수 있습니다.
단계 **2**	종속성 레코드 보기, 92 페이지.	종속성 레코드를 활성화한 후 인터페이스의 [구성] 창에서 액세스할 수 있습니다.

종속성 레코드 구성

Cisco Unified Communications Manager 데이터베이스에서 레코드 간의 관계를 보려면 종속성 레코드를 사용합니다. 예를 들어, 파티션을 삭제하기 전에 종속성 레코드를 사용하여 어떤 발신 검색 공간(CSS) 및 장치가 연결되어 있는지 확인합니다.

주의 종속성 레코드로 인해 CPU 사용량이 많아집니다. 다이얼 플랜 크기와 복잡성, CPU 속도 및 기타 애플리케이션의 CPU 요구 사항으로 인해, 이 절차가 일반 우선 순위보다 낮은 우선 순위로 실행되고 완료하는 데 시간이 오래 걸릴 수 있습니다.

종속성 레코드가 활성화되어 있는 상태에서 시스템에 CPU 사용량 문제가 발생하는 경우 종속성 레코드를 비활성화할 수 있습니다.

절차

단계 **1** Cisco Unified CM 관리에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** **CCMAdmin** 매개 변수 섹션으로 스크롤하고 종속성 레코드 활성화 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **True**—종속성 레코드를 활성화합니다.
- **False**—종속성 레코드를 비활성화합니다.

선택하는 옵션에 따라 종속성 레코드의 활성화 또는 비활성화 결과에 대한 메시지가 있는 대화 상자가 표시됩니다. 메시지를 읽은 후에 이 대화 상자에서 확인을 클릭합니다.

단계 **3** 확인을 클릭합니다.

단계 **4** 저장을 클릭합니다.
변경을 확인하는 업데이트 성공 메시지가 표시됩니다.

종속성 레코드 보기

종속성 레코드를 활성화한 후 인터페이스의 [구성] 창에서 액세스할 수 있습니다.

시작하기 전에

종속성 레코드 구성, 91 페이지

절차

단계 **1** Cisco Unified CM 관리에서 보려는 레코드에 대한 구성 창으로 이동합니다.

예제**:**
장치 풀에 대한 종속성 레코드를 보려면 시스템 > 장치 풀을 선택합니다.
참고 장치 기본값 및 엔터프라이즈 매개 변수 구성 창에서는 종속성 레코드를 볼 수 없습니다.

단계 **2** 찾기를 클릭합니다.

단계 **3** 레코드 중 하나를 클릭합니다.
[구성] 창이 나타납니다.

단계 **4** 관련 링크 목록 상자에서 종속성 레코드를 선택하고 이동을 클릭합니다.
참고 종속성 레코드를 활성화하지 않은 경우 종속성 레코드 요약 창에 레코드에 대한 정보가 없이 메시지가 나타납니다.

데이터베이스의 다른 레코드에서 사용하는 레코드를 보여주는 종속성 레코드 요약 창이 나타납니다.

단계 **5** 이 창에서 다음 종속성 레코드 단추 중 하나를 선택합니다.

- 새로 고침—최신 정보로 창을 업데이트합니다.
- 닫기— [종속성 레코드] 링크를 클릭했던 [구성] 창으로 돌아가지 않고 창을 닫습니다.
- 닫은 후 뒤로— 창을 닫고 [종속성 레코드] 링크를 클릭했던 [구성] 창으로 돌아갑니다.

11 장

시스템 백업

백업 개요

일반 백업을 수행하는 것이 좋습니다. 재난 복구 시스템(DRS)을 사용하여 클러스터의 모든 서버에 대해 전체 데이터 백업을 수행할 수 있습니다. 언제든지 자동 백업을 설정하거나 백업을 호출할 수 있습니다.

재난 복구 시스템은 클러스터 수준 백업을 수행하며 중앙 위치로 Cisco Unified Communications Manager 클러스터의 모든 서버에 대한 백업을 수집하고 백업 데이터를 물리적 저장 장치에 보관합니다. 백업 파일은 암호화되고 시스템 소프트웨어에서만 열 수 있습니다.

DRS은 플랫폼 백업/복원의 일환으로 자체 설정(백업 장치 설정 및 예약 설정)을 복원합니다. DRS는 drfDevice.xml 및 drfSchedule.xml 파일을 백업 및 복원합니다. 이러한 파일로 서버가 복원되면 DRS 백업 장치 및 일정을 다시 구성할 필요가 없습니다.

시스템 데이터 복원을 수행하면 복원할 클러스터의 노드를 선택할 수 있습니다.

재난 복구 시스템에는 다음과 같은 기능이 포함됩니다.

- 백업 및 복원 작업을 수행하기 위한 사용자 인터페이스.
- 백업 기능을 수행하기 위해 분산된 시스템 아키텍처.
- 예약된 백업 또는 (사용자가 호출한) 수동 백업.
- 원격 sftp 서버에 백업을 보관합니다.

필수 구성 요소 백업

- 버전 요구 사항을 충족하는지 확인하십시오.
  - 모든 Cisco Unified Communications Manager 클러스터 노드는 동일한 버전의 Cisco Unified Communications Manager 애플리케이션을 실행하고 있어야 합니다.
  - 모든 IM and Presence 서비스 클러스터 노드는 동일한 버전의 IM and Presence 애플리케이션을 실행하고 있어야 합니다.
  - 백업 파일에 저장된 소프트웨어 버전은 클러스터 노드에서 실행되는 버전과 일치해야 합니다.

  전체 버전 문자열이 일치해야 합니다. 예를 들어, IM and Presence 데이타베이스 게시자 노드의 버전이 11.5.1.10000-1인 경우 모든 IM and Presence는 11.5.1.10000-1이어야 하며 백업 파일도 11.5.1.10000-1이어야 합니다. 현재 버전과 일치하지 않는 백업 파일에서 시스템을 복원하려고 하면 복원이 실패합니다. 백업 파일에 저장된 버전이 클러스터 노드에서 실행되는 버전과 일치하도록 소프트웨어 버전을 업그레이드할 때마다 시스템을 백업해야 합니다.
- DRS 암호화는 클러스터 보안 암호에 따라 달라집니다. 백업을 실행할 때 DRS은 암호화를 위해 임의의 암호를 생성한 다음, 임의의 암호를 클러스터 보안 암호로 암호화합니다. 백업하고 복원하는 사이에 클러스터 보안 암호가 변경된 경우 시스템을 복원하기 위해 해당 백업 파일을 사용하려면 백업 당시의 암호가 무엇인지 알고 있거나 보안 암호를 변경/재설정한 후 즉시 백업해야 합니다.
- 원격 장치로 백업하려는 경우 SFTP 서버를 설정했는지 확인하십시오. 사용 가능한 SFTP 서버에 관한 자세한 내용은 다음을 참조하십시오. 원격 백업용 SFTP 서버, 102 페이지

백업 작업 흐름

백업을 구성하고 실행하려면 이러한 작업을 수행합니다. 백업이 실행되는 동안에는 OS 관리 작업을 수행하지 마십시오. 그 이유는 재난 복구 시스템이 플랫폼 API를 잠가 모든 OS 관리 요청을 차단하기 때문입니다. 그러나 CLI 기반 업그레이드 명령만 플랫폼 API 잠금 패키지를 사용 하기 때문에 재난 복구 시스템은 대부분의 CLI 명령을 차단하지 않습니다.

절차

	명령 또는 동작	목적
단계 **1**	백업 장치 구성, 97 페이지	데이터를 백업할 장치를 지정합니다.
단계 **2**	백업 파일의 크기를 계산합니다., 98 페이지	SFTP 장치에 만들어지는 백업 파일의 크기를 예상합니다.
단계 **3**	다음 옵션 중 하나를 선택합니다. • 예약 백업 구성, 98 페이지	일정에 따라 데이터를 백업하는 백업 일정을 만듭니다. 필요한 경우 수동 백업을 실행합니다.

	명령 또는 동작	목적
	• 수동 백업 시작, 100 페이지	
단계 **4**	현재 백업 상태 보기, 101 페이지	(선택 사항) 백업의 상태를 확인합니다. 백업이 실행되는 동안 현재 백업 작업의 상태를 확인할 수 있습니다.
단계 **5**	백업 기록 보기, 101 페이지	(선택 사항) 백업 기록 보기

백업 장치 구성

최대 10개의 백업 장치를 구성할 수 있습니다. 백업 파일을 저장할 위치를 구성하려면 다음 단계를 수행합니다.

시작하기 전에

- 백업 파일을 저장할 SFTP 서버의 디렉터리 경로에 대한 쓰기 권한이 있는지 확인합니다.
- DRS 마스터 상담원이 백업 장치 구성의 유효성을 검사하므로 사용자 이름, 암호, 서버 이름 및 디렉터리 경로가 유효한지 확인합니다.

참고 네트워크 트래픽이 덜할 것으로 예상되는 기간 동안 백업을 예약합니다.

절차

단계 **1** 재난 복구 시스템에서 백업 > 백업 장치를 선택합니다.

단계 **2** 백업 장치 목록 창에서 다음 중 하나를 수행합니다.

- 새 장치를 구성하려면 새로 추가를 클릭합니다.
- 기존 백업 장치를 편집하려면 검색 조건을 입력하고 [찾기]를 클릭하고 선택한 항목 편집을 클릭합니다.
- 백업 장치를 삭제하려면 백업 장치 목록에서 장치를 선택하고 선택한 항목 삭제를 클릭합니다.

백업 일정에서 백업 장치로 구성된 백업 장치는 삭제할 수 없습니다.

단계 **3** 백업 장치 이름 필드에 백업 이름을 입력합니다.
백업 장치 이름은 영숫자, 공백( ), 대시(-) 및 밑줄(_)만 포함합니다. 다른 문자는 사용하지 마십시오.

단계 **4** 대상 선택 영역의 네트워크 디렉터리에서 다음을 수행합니다.

- 호스트 이름/**IP** 주소 필드에 네트워크 서버의 호스트 이름 또는 IP 주소를 입력합니다.

- 경로 이름 필드에 백업 파일을 저장하려는 디렉터리 경로를 입력합니다.
- 사용자 이름 필드에 유효한 사용자 이름을 입력합니다.
- 암호 필드에 유효한 암호를 입력합니다.
- 네트워크 디렉터리에 저장할 백업 수 드롭다운 목록에서 필요한 백업 수를 선택합니다.

단계 **5** 저장을 클릭합니다.

다음에 할 작업

백업 파일의 크기를 계산합니다., 98 페이지

백업 파일의 크기를 계산합니다.

하나 이상의 선택된 기능에 대한 백업 기록이 있는 경우에만 Cisco Unified Communications Manager는 백업 tar의 크기를 계산합니다.

계산된 크기는 정확한 값이 아니라 백업 tar의 예상 크기입니다. 크기는 이전의 성공적인 백업의 실제 백업 크기에 따라 계산되고, 마지막으로 백업한 이후 구성을 구성이 변경된 경우 다를 수 있습니다.

처음으로 시스템을 백업할 때가 아닌 및 이전 백업이 존재하는 경우에만 이 절차를 사용할 수 있습니다.

이 절차에 따라 SFTP 장치에 저장된 백업 tar의 크기를 예상합니다.

절차

단계 **1** 재난 복구 시스템에서 백업 > 수동 백업을 선택합니다.

단계 **2** 기능 선택 영역에서 백업할 기능을 선택합니다.

단계 **3** 예상 크기를 클릭하여 선택한 기능에 대한 백업의 예상 크기를 볼 수 있습니다.

다음에 할 작업

다음 절차 중 하나를 수행하여 시스템을 백업합니다.

- 예약 백업 구성, 98 페이지
- 수동 백업 시작, 100 페이지

예약 백업 구성

백업 예약을 최대 10개까지 만들 수 있습니다. 각 백업 일정에 자동 백업 일정, 백업할 기능 집합 및 저장 위치를 포함하여 자체 속성 집합이 있는 경우.

백업 .tar 파일이 임의로 생성되는 암호로 암호화되었는지 확인하십시오. 이 암호는 클러스터 보안 암호를 사용하여 암호화되고 백업 .tar 파일이 함께 저장됩니다. 이 보안 암호를 기억하고 있거나 보안 암호를 변경 또는 재설정한 후 즉시 백업을 수행해야 합니다.

주의 통화 처리 중단을 방지하고 서비스에 영향을 주지 않으려면 사용량이 적은 시간 동안 백업을 예약합니다.

시작하기 전에

백업 장치 구성, 97 페이지

절차

단계 **1** 재난 복구 시스템에서 백업스케줄러를 선택합니다.

단계 **2** 일정 목록 창에서 다음 단계 중 하나를 수행하여 새 일정을 추가하거나 기존 일정을 편집합니다.

- 새 일정을 만들려면 새로 추가를 클릭합니다.
- 기존 일정을 구성하려면 [일정 목록] 열에서 이름을 클릭합니다.

단계 **3** 스케줄러 창에서 일정 이름 필드에 일정 이름을 입력합니다.

참고 기본 일정의 이름은 변경할 수 없습니다.

단계 **4** 백업 장치 선택 영역에서 백업 장치를 선택합니다.

단계 **5** 기능 선택 영역에서 백업할 기능을 선택합니다. 하나 이상의 기능을 선택해야 합니다.

단계 **6** 백업 시작 영역에서 백업을 시작할 날짜 및 시간을 선택합니다.

단계 **7** 빈도 영역에서 백업이 발생하도록 하려는 빈도를 선택합니다. 빈도는 매일 한 번, 주별 및 월별로 설정할 수 있습니다. 주별을 선택하는 경우 백업이 발생할 요일을 선택할 수도 있습니다.

팁 백업 빈도를 화요일부터 토요일까지 발생하는 주별로 설정하려면 기본 설정을 클릭합니다.

단계 **8** 이러한 설정을 업데이트하려면 저장을 클릭합니다.

단계 **9** 다음 옵션 중 하나를 선택합니다.

- 선택한 일정을 활성화하려면 선택한 일정 활성화를 클릭합니다.
- 선택한 일정을 비활성화하려면 선택한 일정 비활성화를 클릭합니다.
- 선택한 일정을 삭제하려면 선택한 항목 삭제를 클릭합니다.

단계 **10** 일정을 활성화하려면 일정 활성화를 클릭합니다.
다음 백업은 설정한 시간에 자동으로 발생합니다.

참고 클러스터의 모든 서버에서 동일한 버전의 Cisco Unified Communications Manager 또는 Cisco IM and Presence 서비스를 실행 중이고 네트워크를 통해 연결할 수 있는지 확인합니다. 예약 백업 실행 시 연결할 수 없는 서버는 백업되지 않습니다.

다음에 할 작업

다음 절차를 수행합니다.

- 백업 파일의 크기를 계산합니다., 98 페이지
- (선택사항) 현재 백업 상태 보기, 101 페이지

수동 백업 시작

시작하기 전에

- 백업 파일에 대한 저장 위치로 네트워크 장치를 사용하는지 확인합니다. Unified Communications Manager의 가상화된 배포는 백업 파일을 저장할 테이프 드라이브 사용을 지원하지 않습니다.
- 모든 클러스터 노드에 동일한 버전의 Cisco Unified Communications Manager 또는 IM and Presence 서비스가 설치되었는지 확인하십시오.
- 백업 프로세스는 원격 서버의 사용 가능한 공간 부족 또는 네트워크 연결 중단으로 인해 실패할 수 있습니다. 백업이 실패한 원인이 되는 문제를 해결한 후 새로운 백업 시작해야 합니다.
- 네트워크 중단이 없는지 확인하십시오.
- 백업 장치 구성, 97 페이지
- 백업 파일의 크기를 계산합니다., 98 페이지
- 클러스터 보안 암호에 대한 기록이 있는지 확인합니다. 이 백업을 완료한 후 클러스터 보안 암호가 변경되는 경우 암호를 알고 있어야 합니다. 그렇지 않으면 백업 파일을 사용하여 시스템을 복원할 수 없습니다.

참고 백업이 실행되는 동안 재난 복구 시스템이 플랫폼 API를 잠가 모든 요청을 차단하기 때문에 Cisco Unified OS 관리 또는 Cisco Unified IM and Presence OS 관리에서 작업을 수행할 수 없습니다. 그러나 CLI 기반 업그레이드 명령만 플랫폼 API 잠금 패키지를 사용하기 때문에 재난 복구 시스템은 대부분의 CLI 명령을 차단하지 않습니다.

절차

단계 **1** 재난 복구 시스템에서 백업 > 수동 백업을 선택합니다.

단계 **2** 수동 백업 창의 백업 장치 이름 영역에서 백업 장치를 선택합니다.

단계 **3** 기능 선택 영역에서 기능을 선택합니다.

단계 **4** 백업 시작을 클릭합니다.

다음에 할 작업

(선택사항) 현재 백업 상태 보기, 101 페이지

현재 백업 상태 보기

현재 백업 작업의 상태를 확인하려면 다음 단계를 수행합니다.

주의 원격 서버에 대한 백업이 20시간 내에 완료되지 않을 경우 백업 세션 시간이 초과되고 새로 백업을 시작해야 합니다.

절차

단계 **1** 재난 복구 시스템에서 백업 > 현재 상태를 선택합니다.

단계 **2** 백업 로그 파일을 보려면 로그 파일 이름 링크를 클릭합니다.

단계 **3** 현재 백업을 취소하려면 백업 취소를 클릭합니다.

참고 현재 구성 요소가 백업 작업을 완료한 후에 백업을 취소합니다.

다음에 할 작업

백업 기록 보기, 101 페이지

백업 기록 보기

백업 기록을 보려면 다음 단계를 수행합니다.

절차

단계 **1** 재난 복구 시스템에서 백업 > 기록을 선택합니다.

단계 **2** 백업 기록 창에서 파일 이름, 백업 장치, 완료 날짜, 결과, 버전, 백업된 기능 및 실패한 기능을 포함하여 수행한 백업을 볼 수 있습니다.

참고 백업 기록 창에는 마지막 20개 백업 작업만 표시됩니다.

백업 상호 작용 및 제한 사항

백업 제한 사항

백업에 다음과 같은 제한 사항이 적용됩니다.

표 *2:* 백업 제한 사항

제한 사항	설명
클러스터 보안 암호	클러스터 보안 암호를 변경할 때마다 백업을 실행하는 것이 좋습니다. 백업 암호화는 클러스터 보안 암호를 사용하여 백업 파일의 데이터를 암호화합니다. 백업 파일을 만든 후 클러스터 보안 암호를 편집하는 경우 기존 암호가 기억나지 않으면 해당 백업 파일을 사용하여 데이터를 복원할 수 없습니다.
인증서 관리	재난 복구 시스템(DRS)은 Cisco Unified Communications Manager 클러스터 노드 사이에 인증 및 데이터 암호화를 위해 마스터 상담원과 로컬 상담원 간에 SSL 기반 통신을 사용합니다. DRS은 공개/개인 키 암호화를 위해 IPsec 인증서를 사용합니다. 인증서 관리 페이지에서 IPSEC truststore(hostname.pem) 파일을 삭제하는 경우 DRS는 예상대로 작동하지 않습니다. IPSEC-trust 파일을 수동으로 삭제하는 경우 IPSEC 인증서를 IPSEC-trust로 업로드해야 합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Manager* 보안 설명서의 "인증서 관리" 섹션을 참조하십시오.

원격 백업용 **SFTP** 서버

데이터를 네트워크의 원격 장치에 백업하려면 SFTP 서버를 구성해야 합니다. 모든 SFTP 서버 제품을 사용할 수 있지만 Cisco 기술 파트너의 인증을 받은 제품을 권장합니다. 사용 중인 Cisco Unified Communications Manager 버전으로 어느 공급업체가 해당 제품을 인증했는지 알아보려면 https://marketplace.cisco.com의 Cisco 개발자 네트워크에서 솔루션 카탈로그를 참조하십시오.

다음 표에 있는 정보를 사용하여 시스템에서 사용하는 SFTP 서버 솔루션을 확인합니다.

표 ***3: SFTP*** 서버 정보

SFTP 서버	정보
Cisco Prime Collaboration Deployment의 SFTP 서버	이 서버는 Cisco에서 제공하고 테스트했으면 Cisco TAC에서 지원됩니다. 버전 호환성은 Unified Communications Manager 및 Cisco Prime Collaboration Deployment 버전에 따라 달라집니다. 버전(SFTP) 또는 Unified Communications Manager를 업그레이드하기 전에 버전이 호환되는지 확인하기 위해 *Cisco Prime Collaboration Deployment* 관리 설명서를 참조하십시오.
기술 파트너의 SFTP 서버	이 서버는 타사에서 제공하고 타사에서 테스트하며 TAC 및 Cisco 공급업체에서 공동 지원합니다. 버전 호환성은 타사 테스트에 따라 다릅니다. SFTP 제품을 업그레이드하거나 Unified Communications Manager를 업그레이드할 경우 기술 파트너가 페이지에서 버전 호환성 여부를 참조하십시오. https://marketplace.cisco.com
다른 타사의 SFTP 서버	이러한 서버는 타사에서 제공하고 Cisco에서 제한적으로 테스트하며 Cisco TAC에서 공식 지원하지 않습니다. 버전 호환성은 SFTP 버전 및 Unified Communications Manager 버전의 호환성을 위해 최대한 노력합니다. SFTP 솔루션을 완벽하게 테스트하고 지원하기 위해 Cisco Prime Collaboration Deployment 또는 기술 파트너를 이용합니다.

Cisco는 내부 테스트를 위해 다음 서버를 사용합니다. 서버 중 하나를 사용할 수 있지만 지원은 공급업체에 문의해야 합니다.

- SSH 열기
- Titan

Cisco는 SFTP 제품 freeFTPd 사용을 지원하지 않습니다. 이 SFTP 제품은 파일 크기를 1GB로 제한하기 때문입니다.

타사 SFTP 제품을 설정하는 방법에 대한 자세한 내용은 타사 공급업체에 지원을 문의하십시오. Cisco 기술 개발자 프로그램 프로세스를 통해 인증되지 않은 타사 제품의 문제는 타사 공급업체에 지원을 문의하십시오. 지원되는 Cisco Unified Communications Manager 버전에서 GlobalSCAPE 사용에 대한 내용은 GlobalSCAPE에 문의하십시오.

참고 Unified Communications Manager를 업그레이드하거나, SFTP 서버를 업그레이드하거나, 다른 SFTP 서버로 전환한 후에 SFTP 서버에서 DRS을 다시 테스트하는 것이 좋습니다. 이 단계를 통해 이러한 구성 요소가 함께 올바르게 작동하는지 확인하십시오. 대기 또는 백업 서버에서 백업과 복원을 수행하는 것은 모범적인 사례입니다.

12 장

시스템 복원

복원 개요

재난 복구 시스템(DRS)은 시스템 복원 프로세스를 안내하는 마법사를 제공합니다.

백업 파일은 암호화되어 있으며 DRS 시스템만 데이터를 열어 복원할 수 있습니다. 재난 복구 시스템에는 다음과 같은 기능이 포함됩니다.

- 복원 작업을 수행하기 위한 사용자 인터페이스.
- 복원 기능을 수행하기 위해 분산된 시스템 아키텍처.

마스터 상담원

시스템이 클러스터의 각 노드에서 마스터 상담원 서비스를 자동으로 시작하지만 마스터 상담원은 게시자 노드에서만 작동합니다. 가입자 노드의 마스터 상담원은 모든 기능을 수행하지는 않습니다.

로컬 상담원

서버에 백업 및 복원 기능을 수행하는 로컬 상담원이 있습니다.

마스터 상담원이 포함된 노드를 포함하여 Cisco Unified Communications Manager 클러스터의 각 노드에 백업 및 복원 기능을 수행할 자체 로컬 상담원이 있어야 합니다.

참고 기본적으로 로컬 상담원이 IM and Presence 노드를 포함하여 클러스터의 각 노드에서 자동으로 시작됩니다.

필수 구성 요소 복원

- 버전 요구 사항을 충족하는지 확인하십시오.
  - 모든 Cisco Unified Communications Manager 클러스터 노드는 동일한 버전의 Cisco Unified Communications Manager 애플리케이션을 실행하고 있어야 합니다.
  - 모든 IM and Presence 서비스 클러스터 노드는 동일한 버전의 IM and Presence 애플리케이션을 실행하고 있어야 합니다.
  - 백업 파일에 저장된 버전은 클러스터 노드에서 실행되는 버전과 일치해야 합니다.

  전체 버전 문자열이 일치해야 합니다. 예를 들어, IM and Presence 데이타베이스 게시자 노드의 버전이 11.5.1.10000-1인 경우 모든 IM and Presence는 11.5.1.10000-1이어야 하며 백업 파일도 11.5.1.10000-1이어야 합니다. 현재 버전과 일치하지 않는 백업 파일에서 시스템을 복원하려고 하면 복원이 실패합니다.
- IP 주소, 호스트 이름, DNS 구성 및 서버의 배포 유형이 백업 파일에 저장된 IP 주소, 호스트 이름, DNS 구성 및 서버의 배포 유형과 일치하는지 확인하십시오.
- 백업을 실행한 후 클러스터 보안 암호를 변경한 경우 기존 암호에 대한 기록이 있어야 합니다. 그렇지 않으면 복원이 실패합니다.

작업 흐름 복원

복원 과정에서 Cisco Unified Communications Manager OS 관리 또는 Cisco Unified IM and Presence OS 관리를 사용하여 작업을 수행하지 마십시오.

절차

	명령 또는 동작	목적
단계 **1**	첫 번째 노드만 복원, 107 페이지	(선택 사항) 클러스터의 첫 번째 게시자 노드를 복원하는 경우에만 이 절차를 사용합니다.
단계 **2**	후속 클러스터 노드 복원, 109 페이지	(선택 사항) 클러스터의 가입자 노드를 복원하려면 이 절차를 사용합니다.

	명령 또는 동작	목적
단계 **3**	게시자를 다시 빌드한 후 한 번에 클러스터 복원, 110 페이지	(선택 사항) 게시자가 이미 다시 빌드된 경우 한 번에 전체 클러스터를 복원하려면 이 절차를 수행합니다.
단계 **4**	전체 클러스터 복원, 111 페이지	(선택 사항) 게시자 노드를 포함하여 클러스터의 모든 노드를 복원하는 경우 이 절차를 사용합니다. 주요 하드 드라이브 고장 또는 업그레이드 오류가 발생하거나 하드 드라이브를 마이그레이션하는 경우 클러스터의 모든 노드를 다시 빌드해야 할 수 있습니다.
단계 **5**	마지막으로 성공한 구성으로 노드 또는 클러스터 복원, 113 페이지	(선택 사항) 노드를 마지막으로 성공한 구성으로 복원하는 경우 이 절차를 사용합니다. 하드 드라이브 고장 또는 기타 하드웨어 고장이 발생한 후에는 이 절차를 사용하지 마십시오.
단계 **6**	노드 다시 시작, 113 페이지	노드를 다시 시작하려면 이 절차를 사용합니다.
단계 **7**	복원 작업 상태 확인, 114 페이지	(선택 사항) 복원 작업 상태를 확인하려면 이 절차를 사용합니다.
단계 **8**	복원 기록 보기, 114 페이지	(선택 사항) 복원 기록을 보려면 이 절차를 사용합니다.

첫 번째 노드만 복원

다시 빌드한 후에 첫 번째 노드에 복원하는 경우 백업 장치를 구성해야 합니다.

이 절차는 Cisco Unified Communications Manager 첫 번째 노드(게시자 노드라고도 함)에 적용됩니다. 다른 Cisco Unified Communications Manager 노드 및 모든 IM and Presence 서비스 노드는 보조 노드 또는 가입자로 간주됩니다.

시작하기 전에

클러스터에 IM and Presence 서비스 노드가 있는 경우 첫 번째 노드를 복원할 때 실행 중이고 액세스할 수 있는지 확인합니다. 이는 절차를 수행하는 동안 유효한 백업 파일을 찾을 수 있도록 하는데 필요합니다.

절차

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 복원 마법사 **1**단계 창의 백업 장치 선택 영역에서 복원할 적절한 백업 장치를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

참고 백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 다음을 클릭합니다.

단계 **7** 복원할 기능을 선택합니다.

참고 백업을 위해 선택한 기능이 표시됩니다.

단계 **8** 복원할 노드를 선택합니다.

단계 **9** 복원을 클릭하여 데이터를 복원합니다.

단계 **10** 다음을 클릭합니다.

단계 **11** 복원할 노드를 선택하라는 메시지가 표시되면 첫 번째 노드(게시자)만 선택합니다.

주의 복원 시도가 실패하므로 이 조건에서는 후속(가입자) 노드를 선택하지 마십시오.

단계 **12** (선택 사항) 서버 이름 선택 드롭다운 목록에서 게시자 데이터베이스를 복원하려는 가입자 노드를 선택합니다. 선택한 가입자 노드가 서비스 중이고 클러스터에 연결되었는지 확인합니다.

재난 복구 시스템은 백업 파일에서 모든 비 데이터베이스 정보를 복원하고 선택한 가입자 노드에서 최신 데이터베이스를 가져옵니다.

참고 이 옵션은 사용자가 선택한 백업 파일에 CCMDB database 구성 요소가 포함된 경우에 나타납니다. 처음에는 게시자 노드만 완전히 복원되지만 14단계를 수행하고 후속 클러스터 노드를 다시 시작하면 재난 복구 시스템은 데이터베이스 복제를 수행하고 모든 클러스터 노드 데이터베이스를 완벽하게 동기화합니다. 이렇게 하면 모든 클러스터 노드가 최신 데이터를 사용하게 됩니다.

단계 **13** 복원을 클릭합니다.

단계 **14** 데이터가 게시자 노드에 복원됩니다. 데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다.

참고 첫 번째 노드를 복원하면 전체 Cisco Unified Communications Manager 데이터베이스가 클러스터에 복원됩니다. 복원 중인 해당 데이터베이스의 노드 수와 크기에 따라 여러 시간이 걸릴 수 있습니다. 데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다.

단계 **15** 복원 상태 창의 완료 비율 필드가 100%를 표시하면 서버를 다시 시작합니다. 첫 번째 노드만 복원하는 경우 클러스터의 모든 노드를 다시 시작해야 합니다. 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 Cisco Unified Communications Manager 노드만 복원하는 경우 Cisco Unified Communications Manager 및 IM and Presence 서비스 클러스터를 다시 시작해야 합니다.

IM and Presence 서비스 게시자 노드만 복원하는 경우 IM and Presence 서비스 클러스터를 다시 시작해야 합니다.

다음에 할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 114 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 113 페이지

후속 클러스터 노드 복원

이 절차는 Cisco Unified Communications Manager 가입자(후속) 가입자 노드에 적용됩니다. 설치된 첫 번째 Cisco Unified Communications Manager 노드가 게시자 노드입니다. 다른 모든 Cisco Unified Communications Manager 노드 및 모든 IM and Presence 서비스 노드는 가입자 노드입니다.

클러스터에 있는 하나 이상의 Cisco Unified Communications Manager 가입자 노드를 복원하려면 이 절차를 수행합니다.

시작하기 전에

복원 작업을 수행하기 전에 복원의 호스트 이름, IP 주소, DNS 구성 및 배포 유형이 복원하려는 백업 파일의 호스트 이름, IP 주소, DNS 구성 및 배포 유형과 일치하는지 확인합니다. 재난 복구 시스템은 다른 호스트 이름, IP 주소, DNS 구성 및 배포 유형을 복원하지 않습니다.

서버에 설치된 소프트웨어 버전이 복원하려는 백업 파일의 버전과 일치하는지 확인하십시오. 재난 복구 시스템은 복원 작업의 경우 일치하는 소프트웨어 버전만 지원합니다. 다시 빌드한 이후 후속 노드를 복원하는 경우 백업 장치를 구성해야 합니다.

절차

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 복원 마법사 **1**단계 창의 백업 장치 선택 영역에서 복원을 시작할 백업 장치를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 복원하려는 기능을 선택합니다.

참고 사용자가 선택한 파일로 백업한 기능만 표시됩니다.

단계 **7** 다음을 클릭합니다. 복원 마법사 4단계 창이 표시됩니다.

단계 **8** 복원 마법사 **4**단계 창에서 복원할 노드를 선택하라는 메시지가 표시되면 후속 노드만 선택합니다.

단계 **9** 복원을 클릭합니다.

단계 **10** 데이터가 후속 노드에 복원됩니다. 복원 상태를 보는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 복원 과정에서 Cisco Unified Communications Manager 관리 또는 사용자 옵션을 사용하여 작업을 수행하지 마십시오.

단계 **11** 복원 상태 창의 완료 비율 필드가 100%를 표시하면 방금 복원한 보조 서버를 다시 시작합니다. 첫 번째 노드만 복원하는 경우 클러스터의 모든 노드를 다시 시작해야 합니다. 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 IM and Presence 서비스 첫 번째 노드가 복원된 경우. IM and Presence 서비스 후속 노드를 다시 시작하기 전에 IM and Presence 서비스 첫 번째 노드를 다시 시작해야 합니다.

다음에 할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 114 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 113 페이지

게시자를 다시 빌드한 후 한 번에 클러스터 복원

데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다. 게시자가 이미 다시 빌드되었거나 새로 설치한 경우 한 번에 전체 클러스터를 복원하려면 이 절차를 수행합니다.

절차

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 복원 마법사 **1**단계 창의 백업 장치 선택 영역에서 복원을 시작할 백업 장치를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.
백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

전체 클러스터를 복원하려는 클러스터의 백업 파일만 선택합니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 복원하려는 기능을 선택합니다.
화면에 백업 파일에 저장된 기능만 표시됩니다.

단계 **7** 다음을 클릭합니다.

단계 **8** 복원 마법사 **4**단계 창에서 **1** 단계 복원을 클릭합니다.
이 옵션은 복원을 위해 선택한 백업 파일이 클러스터의 백업 파일이고 복원을 위해 선택한 기능에 게시자 및 가입자 노드에 등록된 기능이 포함된 경우에만 복원 마법사 **4**단계 창에 나타납니다. 자세한 내용은 첫 번째 노드만 복원, 107 페이지 및 후속 클러스터 노드 복원, 109 페이지를 참조하십시오.

참고 상태 메시지에 게시자가 클러스터를 인식하는 데 실패했습니다. *1*단계 복원을 시작할 수 없습니다가 표시되는 경우, 게시자 노드를 복원한 다음, 가입자 노드를 복원해야 합니다. 자세한 내용은 관련 항목을 참조하십시오.

이 옵션을 사용하면 게시자가 클러스터를 인식할 수 있으며 이렇게 하는 데 5분 정도 걸립니다. 이 옵션을 클릭하면 "게시자가 클러스터를 인식할 때까지 5분간 기다리고 이 기간 동안에는 백업 또는 복원 활동을 시작하지 마십시오"라는 상태 메시지가 표시됩니다.

이 지연이 끝난 후 게시자가 클러스터를 인식하게 되면 "게시자가 클러스터를 인식했습니다. 서버를 선택하고 복원을 클릭하여 전체 클러스터의 복원을 시작하십시오."라는 상태 메시지가 표시됩니다.

이 지연이 끝난 후 게시자가 클러스터를 인식하지 못하는 경우 "게시자가 클러스터를 인식하는 데 실패했습니다. 1단계 복원을 시작할 수 없습니다. 계속해서 일반 2단계 복원을 수행하십시오."라는 상태 메시지가 표시됩니다. 2단계(게시자, 그런 다음 가입자)로 전체 클러스터를 복원하려면 첫 번째 노드만 복원, 107 페이지 및 후속 클러스터 노드 복원, 109 페이지에서 설명하는 단계를 수행합니다.

단계 **9** 복원하려면 노드를 선택하라는 메시지가 표시되면 클러스터의 모든 노드를 선택합니다.
재난 복구 시스템은 첫 번째 노드를 복원할 때 후속 노드에서 Cisco Unified Communications Manager 데이터베이스(CCMDB)를 자동으로 복원합니다. 복원 중인 해당 데이터베이스의 노드 수와 크기에 따라 여러 시간이 걸릴 수 있습니다.

단계 **10** 복원을 클릭합니다.
데이터는 클러스터의 모든 노드에 복원됩니다.

단계 **11** 복원 상태 창의 완료 비율 필드가 100%를 표시하면 서버를 다시 시작합니다. 첫 번째 노드만 복원하는 경우 클러스터의 모든 노드를 다시 시작해야 합니다. 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

다음에 할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 114 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 113 페이지

관련 항목

첫 번째 노드만 복원, 107 페이지
후속 클러스터 노드 복원, 109 페이지

전체 클러스터 복원

주요 하드 드라이브 고장 또는 업그레이드 오류가 발생하거나 하드 드라이브를 마이그레이션하는 경우 클러스터의 모든 노드를 다시 빌드해야 합니다. 전체 클러스터 복원하려면 다음 단계를 수행합니다.

네트워크 카드 바꾸거나 메모리를 추가하는 등 대부분의 다른 유형의 하드웨어 업그레이드를 수행하는 경우 이 절차를 수행할 필요가 없습니다.

절차

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 백업 장치 선택 영역에서 복원할 적절한 장치를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

참고 백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 다음을 클릭합니다.

단계 **7** 복원 마법사 **4**단계 창에서 복원 노드를 선택하라는 메시지가 표시될 때 모든 노드를 선택합니다.

단계 **8** 복원을 클릭하여 데이터를 복원합니다.

재난 복구 시스템은 첫 번째 노드를 복원할 때 후속 노드에서 Cisco Unified Communications Manager 데이터베이스(CCMDB)를 자동으로 복원합니다. 해당 데이터베이스의 노드 수와 크기에 따라 여러 시간이 걸릴 수 있습니다.

데이터가 모든 노드에서 복원됩니다.

참고 복원 과정에서 Cisco Unified Communications Manager 관리 또는 사용자 옵션을 사용하여 작업을 수행하지 마십시오.

데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다.

단계 **9** 복원 프로세스가 완료되면 서버를 다시 시작합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다.

첫 번째 노드가 다시 시작되고 Cisco Unified Communications Manager의 복원된 버전을 실행한 후에 후속 노드를 다시 시작합니다.

단계 **10** 클러스터를 재부팅하면 복제가 자동으로 설정됩니다. *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서에 설명된 대로 “utils dbreplication runtimestate” CLI 명령을 사용하여 모든 노드에서 복제 상태 값을 확인합니다. 각 노드의 값은 2가 되어야 합니다.

참고 후속 노드의 데이터베이스 복제는 클러스터의 크기에 따라 후속 노드를 다시 시작한 후 완료하는 데 많은 시간이 걸릴 수 있습니다.

팁 복제가 제대로 설정되지 않은 경우 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서에 설명된 대로 "utils dbreplication rebuild" CLI 명령을 사용합니다.

다음에 할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 114 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 113 페이지

마지막으로 성공한 구성으로 노드 또는 클러스터 복원

이 절차에 따라 마지막으로 성공한 구성으로 노드 또는 클러스터를 복원합니다.

시작하기 전에

- 복원 파일에 호스트 이름, IP 주소, DNS 구성 및 백업 파일에 구성된 배포 유형이 포함되어 있는지 확인하십시오.
- 서버에 설치된 Cisco Unified Communications Manager 버전이 복원하려는 백업 파일의 버전과 일치하는지 확인하십시오.
- 이 절차는 마지막으로 성공한 구성으로 노드를 복원하는 데만 사용해야 합니다.

절차

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 백업 장치 선택 영역에서 복원할 적절한 장치를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

참고 백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 다음을 클릭합니다.

단계 **7** 복원 노드를 선택하라는 메시지가 표시되면 해당 노드를 선택합니다.
데이터가 선택한 노드에서 복원됩니다.

단계 **8** 클러스터의 모든 노드를 다시 시작합니다. 첫 번째 Cisco Unified Communications Manager 노드를 다시 시작한 후에 이후의 Cisco Unified Communications Manager 노드를 다시 시작합니다. 클러스터에도 Cisco IM and Presence 노드가 있는 경우 첫 번째 Cisco IM and Presence 노드를 다시 시작한 후에 이후의 IM and Presence 노드를 다시 시작합니다. 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

노드 다시 시작

데이터 복원 후 노드를 다시 시작해야 합니다.

게시자 노드(첫 번째 노드)를 복원하는 경우 먼저 게시자 노드를 다시 시작해야 합니다. 게시자 노드를 다시 시작하고 및 소프트웨어의 복원된 버전을 성공적으로 실행한 후에만 가입자 노드를 다시 시작합니다.

⚠

주의 이 절차로 인해 시스템이 다시 시작되고 일시적으로 서비스를 사용할 수 없게 됩니다.

다시 시작해야 하는 클러스터의 모든 노드에서 이 절차를 수행합니다.

절차

단계 **1** Cisco Unified OS 관리에서 설정 > 버전을 선택합니다.

단계 **2** 노드를 다시 시작하려면 다시 시작을 클릭합니다.

단계 **3** 클러스터를 재부팅하면 복제가 자동으로 설정됩니다. **utils dbreplication runtimestate** CLI 명령을 사용하여 모든 노드에서 복제 상태 값을 확인합니다. 각 노드의 값은 2가 되어야 합니다. CLI 명령에 대한 정보를 찾으려면 아래의 관련 항목 섹션을 참조하십시오.
복제가 제대로 설정되지 않은 경우 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서에 설명된 대로 **utils dbreplication reset** CLI 명령을 사용합니다. CLI 명령에 대한 정보를 찾으려면 아래의 관련 항목 섹션을 참조하십시오.

참고 후속 노드의 데이터베이스 복제는 클러스터의 크기에 따라 후속 노드를 다시 시작한 후 완료하는 데 여러 시간이 걸릴 수 있습니다.

다음에 할 작업

(선택 사항) 복원 상태를 보려면 복원 작업 상태 확인, 114 페이지을 참조하십시오.

관련 항목

Cisco Unified Communications Manager (CallManager) 명령 참조

복원 작업 상태 확인

복원 작업 상태를 확인하려면 이 절차를 수행합니다.

절차

단계 **1** 재난 복구 시스템에서 복원 > 현재 상태를 선택합니다.

단계 **2** 복원 상태 창에서 복원 상태를 보려는 로그 파일 이름 링크를 클릭합니다.

복원 기록 보기

복원 기록을 보려면 다음 단계를 수행합니다.

절차

단계 **1** 재난 복구 시스템에서 복원 > 기록을 선택합니다.

단계 **2** 복원 기록 창에서 파일 이름, 백업 장치, 완료 날짜, 결과, 버전, 복원된 기능 및 실패한 기능을 포함하여 수행한 복원을 볼 수 있습니다.
복원 기록 창에는 마지막 20개 복원 작업만 표시됩니다.

데이터 인증

추적 파일

다음 추적 파일 위치는 문제를 해결하는 동안 또는 로그를 수집하는 동안 사용됩니다.

마스터 에이전트, GUI, 각 로컬 상담원 및 JSch 라이브러리에 대한 추적 파일은 다음 위치에 기록됩니다.

- 마스터 상담원의 경우 추적 파일 위치: platform/drf/trace/drfMA0*
- 각 로컬 상담원의 경우 추적 파일 위치: platform/drf/trace/drfLA0*
- GUI의 경우 추적 파일 위치: platform/drf/trace/drfConfLib0*
- JSch의 경우 추적 파일 위치: platform/drf/trace/drfJSch*

자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html에서 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

Command Line Interface

또한 재난 복구 시스템은 다음 표에 표시된 대로 백업 및 복원 기능의 하위 집합에 대한 명령줄 액세스를 제공합니다. 이러한 명령 및 이 명령줄 인터페이스 사용에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html에서 Cisco Unified Communications Solutions용 명령줄 인터페이스 설명서를 참조하십시오.

표 ***4:*** 재난 복구 시스템 명령줄 인터페이스

명령	설명
utils disaster_recovery estimate_tar_size	SFTP/로컬 장치에서 백업 tar의 예상 크기를 표시하고 기능 목록에 대해 하나의 매개 변수가 필요

명령	설명
utils disaster_recovery backup	재난 복구 시스템 인터페이스에 구성된 기능을 사용하여 수동 백업 시작
utils disaster_recovery jschLogs	JSch 라이브러리 로깅 활성화 또는 비활성화
utils disaster_recovery restore	복원을 시작하고 백업 위치, 파일 이름, 기능 및 복원할 노드에 대한 매개 변수가 필요
utils disaster_recovery status	진행 중인 백업 또는 복원 작업의 상태 표시
utils disaster_recovery show_backupfiles	기존 백업 파일 표시
utils disaster_recovery cancel_backup	진행 중인 백업 작업 취소
utils disaster_recovery show_registration	현재 구성된 등록 표시
utils disaster_recovery device add	네트워크 장치 추가
utils disaster_recovery device delete	장치 삭제
utils disaster_recovery device list	모든 장치 나열
utils disaster_recovery schedule add	일정 추가
utils disaster_recovery schedule delete	일정 삭제
utils disaster_recovery schedule disable	일정 비활성화
utils disaster_recovery schedule enable	일정 활성화
utils disaster_recovery schedule list	모든 일정 나열
utils disaster_recovery backup	재난 복구 시스템 인터페이스에 구성된 기능을 사용하여 수동 백업 시작
utils disaster_recovery restore	복원을 시작하고 백업 위치, 파일 이름, 기능 및 복원할 노드에 대한 매개 변수가 필요

명령	설명
utils disaster_recovery status	진행 중인 백업 또는 복원 작업의 상태 표시
utils disaster_recovery show_backupfiles	기존 백업 파일 표시
utils disaster_recovery cancel_backup	진행 중인 백업 작업 취소
utils disaster_recovery show_registration	현재 구성된 등록 표시

알람 및 메시지

알람 및 메시지

재난 복구 시스템 문제는 백업 또는 복원 절차 동안 발생할 수 있는 다양한 오류에 대해 알람을 제공합니다. 다음 표에서는 Cisco 재난 복구 시스템 알람 목록을 제공합니다.

표 ***5:*** 재난 복구 시스템 알람 및 메시지

알람 이름	설명	설명
DRFBackupDeviceError	DRF 백업 프로세스가 장치에 액세스하는 데 문제가 있습니다.	장치에 액세스하는 동안 DRS 백업 프로세스에 오류가 발생했습니다.
DRFBackupFailure	Cisco DRF 백업 프로세스가 실패했습니다.	DRS 백업 프로세스에 오류가 발생했습니다.
DRFBackupInProgress	다른 백업을 실행 중에는 새 백업을 시작할 수 없습니다.	다른 백업을 실행 중에는 DRS가 새 백업을 시작할 수 없습니다.
DRFInternalProcessFailure	DRF 내부 프로세스에 오류가 발생했습니다.	DRS 내부 프로세스에 오류가 발생했습니다.
DRFLA2MAFailure	DRF 로컬 상담원이 마스터 상담원에 연결할 수 없습니다.	DRS 로컬 상담원이 마스터 상담원에 연결할 수 없습니다.
DRFLocalAgentStartFailure	DRF 로컬 상담원이 시작되지 않습니다.	DRS 로컬 상담원이 종료될 수 있습니다.

알람 이름	설명	설명
DRFMA2LAFailure	DRF 마스터 상담원이 로컬 상담원에 연결할 수 없습니다.	DRS 마스터 상담원이 로컬 상담원에 연결할 수 없습니다.
DRFMABackupComponentFailure	DRF가 하나 이상의 구성 요소를 백업할 수 없습니다.	DRS가 데이터를 백업할 구성 요소를 요청했습니다. 하지만 백업 프로세스 동안 오류가 발생했으며 구성 요소가 백업되지 않았습니다.
DRFMABackupNodeDisconnect	백업 중인 노드가 완전히 백업되기 전에 마스터 상담원에서 연결이 끊어졌습니다.	DRS 마스터 상담원이 Cisco Unified Communications Manager 노드에서 백업 작업을 실행하는 동안 백업 작업이 완료되기 전에 노드 연결이 끊어졌습니다.
DRFMARestoreComponentFailure	DRF가 하나 이상의 구성 요소를 복원할 수 없습니다.	DRS가 데이터를 복원할 구성 요소를 요청했습니다. 하지만 복원 프로세스 동안 오류가 발생했으며 구성 요소가 복원되지 않았습니다.
DRFMARestoreNodeDisconnect	복원 중인 노드가 완전히 복원되기 전에 마스터 상담원에서 연결이 끊어졌습니다.	DRS 마스터 상담원이 Cisco Unified Communications Manager 노드에서 복원 작업을 실행하는 동안 복원 작업이 완료되기 전에 노드 연결이 끊어졌습니다.
DRFMasterAgentStartFailure	DRF 마스터 상담원이 시작되지 않았습니다.	DRS 마스터 상담원이 종료될 수 있습니다.
DRFNoRegisteredComponent	등록된 구성 요소를 사용할 수 없으므로 백업에 실패했습니다.	등록된 구성 요소를 사용할 수 없으므로 DRS 백업에 실패했습니다.
DRFNoRegisteredFeature	백업을 위한 기능을 선택하지 않았습니다.	백업을 위한 기능을 선택하지 않았습니다.
DRFRestoreDeviceError	DRF 복원 프로세스가 장치에 액세스하는 데 문제가 있습니다.	장치에서 DRS 복원 프로세스 읽을 수 없습니다.
DRFRestoreFailure	DRF 복원 프로세스가 실패했습니다.	DRS 복원 프로세스에 오류가 발생했습니다.

알람 이름	설명	설명
DRFSftpFailure	DRF SFTP 작업에 오류가 발생했습니다.	DRS SFTP 작업에서 오류가 발생했습니다.
DRFSecurityViolation	DRF 시스템이 보안 위반이 발생할 수 있는 악의적인 패턴을 발견했습니다.	DRF 네트워크 메시지에 코드 삽입 또는 디렉터리 통과 같은 보안 위반이 발생할 수 있는 악의적인 패턴이 포함되어 있습니다. DRF 네트워크 메시지가 차단되었습니다.
DRFTruststoreMissing	IPsec truststore가 노드에 누락되어 있습니다.	IPsec truststore가 노드에 누락되어 있습니다. DRF 로컬 상담원이 마스터 상담원에 연결할 수 없습니다.
DRFUnknownClient	Pub의 DRF 마스터 상담원이 클러스터 외부의 알 수 없는 서버로부터 클라이언트 연결 요청을 받았습니다. 요청이 거부되었습니다.	Pub의 DRF 마스터 상담원이 클러스터 외부의 알 수 없는 서버로부터 클라이언트 연결 요청을 받았습니다. 요청이 거부되었습니다.
DRFBackupCompleted	DRF 백업이 성공적으로 완료되었습니다.	DRF 백업이 성공적으로 완료되었습니다.
DRFRestoreCompleted	DRF 복원이 성공적으로 완료되었습니다.	DRF 복원이 성공적으로 완료되었습니다.
DRFNoBackupTaken	DRF가 현재 시스템의 유효한 백업을 찾지 못했습니다.	DRF가 업그레이드/마이그레이션 또는 새로 설치 후 현재 시스템의 유효한 백업을 찾지 못했습니다.
DRFComponentRegistered	DRF가 요청된 구성 요소를 성공적으로 등록했습니다.	DRF가 요청된 구성 요소를 성공적으로 등록했습니다.
DRFRegistrationFailure	DRF를 등록하지 못했습니다.	일부 내부 오류로 인해 구성 요소에 대한 DRF 등록 작업이 실패했습니다.
DRFComponentDeRegistered	DRF가 요청된 구성 요소를 성공적으로 등록 해제했습니다.	DRF가 요청된 구성 요소를 성공적으로 등록 해제했습니다.
DRFDeRegistrationFailure	구성 요소에 대한 DRF 등록 해제 요청이 실패했습니다.	구성 요소에 대한 DRF 등록 해제 요청이 실패했습니다.

알람 이름	설명	설명
DRFFailure	DRF 백업 또는 복원 프로세스가 실패했습니다.	DRF 백업 또는 복원 프로세스에 오류가 발생했습니다.
DRFRestoreInternalError	DRF 복원 작업에 오류가 발생했습니다. 복원이 내부적으로 취소되었습니다.	DRF 복원 작업에 오류가 발생했습니다. 복원이 내부적으로 취소되었습니다.
DRFLogDirAccessFailure	DRF가 로그 디렉터리에 액세스할 수 없습니다.	DRF가 로그 디렉터리에 액세스할 수 없습니다.
DRFDeRegisteredServer	DRF가 서버에 대한 모든 구성 요소를 자동으로 등록 해제했습니다.	서버가 Unified Communications Manager 클러스터에서 연결이 끊어졌습니다.
DRFSchedulerDisabled	백업에 사용할 수 있는 기능이 구성되지 않아 DRF 스케줄러가 비활성화되었습니다.	백업에 사용할 수 있는 기능이 구성되지 않아 DRF 스케줄러가 비활성화되었습니다.
DRFSchedulerUpdated	기능 등록 해제로 인해 DRF 일정 백업 구성이 자동으로 업데이트되었습니다.	기능 등록 해제로 인해 DRF 일정 백업 구성이 자동으로 업데이트되었습니다.

복원 상호 작용 및 제한 사항

복원 제한 사항

다음 제한 사항은 재난 복구 시스템을 사용하여 Cisco Unified Communications Manager 또는 IM and Presence 서비스를 복원하는 데 적용됩니다.

표 ***6:*** 복원 제한 사항

제한 사항	설명
내보내기 제한	제한된 버전에서 제한된 버전으로만 DRS 백업을 복원할 수 있으며 무제한 버전의 백업은 무제한 버전에만 복원할 수 있습니다. Cisco Unified Communications Manager의 미국 수출 무제한 버전으로 업그레이드하는 경우 나중에 이 소프트웨어의 미국 수출 제한 버전으로 업그레이드하거나 새로 설치를 수행할 수 없습니다.

제한 사항	설명
플랫폼 마이그레이션	재난 복구 시스템을 사용하여 플랫폼 간에 데이터를 마이그레이션할 수 없습니다(예를 들어, Windows에서 Linux로 또는 Linux에서 Windows로). 복원은 백업과 동일한 제품 버전에서 실행해야 합니다. Windows 기반 플랫폼에서 Linux 기반 플랫폼으로 데이터 마이그레이션에 대한 자세한 내용은 *Data Migration Assistant* 사용 설명서를 참조하십시오.
하드웨어 교체 및 마이그레이션	데이터를 새 서버로 마이그레이션하기 위해 DRS 복원을 수행할 때 이전 서버에서 사용한 것과 동일한 IP 주소 및 호스트 이름을 새 서버에 할당해야 합니다. 또한 백업을 수행할 때 DNS가 구성된 경우 복원을 수행하기 전에 동일한 DN 구성이 있어야 합니다. 서버를 교체하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 단일 서버 또는 클러스터 교체 설명서를 참조하십시오. 뿐만 아니라, 하드웨어 교체 후 인증서 신뢰 목록(CTL) 클라이언트를 실행해야 합니다. 후속 노드(가입자) 서버를 복원하지 않은 경우 CTL 클라이언트를 실행해야 합니다. 다른 경우에는 DRS가 필요한 인증서를 백업합니다. 자세한 내용은 *Cisco Unified Communications Manager* 보안 설명서에서 "CTL 클라이언트 설치" 및 "CTL 클라이언트 구성" 절차를 참조하십시오.
클러스터 간 내선 이동	백업에서 원격 클러스터에 로그인한 클러스터 간 내선 이동 사용자는 복구 후 로그인을 유지합니다.

참고

Cisco Unified Communications 서버 구성 요소를 성공적으로 복원한 후 Cisco Unified Communications Manager를 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성을 사용하여 등록합니다. 백업을 수행하기 전에 이미 제품이 등록된 경우 라이센스 정보를 업데이트하기 위해 제품을 다시 등록합니다.

Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성을 사용하여 제품을 등록하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서, 릴리스 12.0(1)(http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html)을 참조하십시오.

문제 해결

더 작은 가상 시스템으로 **DRS** 복원 실패

문제

IM and Presence 서비스 노드를 디스크 더 작은 VM으로 복원하는 경우 데이터베이스 복원이 실패할 수 있습니다.

원인

이 오류는 큰 디스크 크기에서 작은 디스크 크기로 마이그레이션하는 경우에 발생합니다.

해결 방법

2개의 가상 디스크가 있는 OVA 템플릿에서 복원을 위해 VM을 배포합니다.

13 장

엔터프라이즈 매개 변수 관리

엔터프라이즈 매개 변수 개요

엔터프라이즈 매개 변수는 전체 클러스터의 모든 장치 및 서비스에 적용되는 기본 설정을 제공합니다. 예를 들어, 시스템은 엔터프라이즈 매개 변수를 사용하여 관련 장치 기본값의 초기값을 설정합니다.

엔터프라이즈 매개 변수를 추가하거나 삭제할 수는 없지만 기존 엔터프라이즈 매개 변수를 업데이트할 수 있습니다. 구성 창은 범주 아래 엔터프라이즈 매개 변수 표시합니다(예: CCMAdmin 매개 변수, CCMUser 매개 변수 및 CDR 매개 변수).

엔터프라이즈 매개 변수 구성 창에서 엔터프라이즈 매개 변수에 대한 자세한 내용을 볼 수 있습니다.

주의 대부분의 엔터프라이즈 매개 변수는 변경할 필요가 없습니다. 변경하려는 기능을 완전히 이해했거나 Cisco TAC(기술 지원 센터)에서 변경을 조언한 경우가 아니면 엔터프라이즈 매개 변수를 변경하지 마십시오.

엔터프라이즈 매개 변수 정보 보기

엔터프라이즈 매개 변수 구성 창에 포함된 콘텐츠를 통해 엔터프라이즈 매개 변수에 대한 정보에 액세스합니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 다음 작업 중 하나를 수행합니다.

- 특정 엔터프라이즈 매개 변수에 대한 설명을 보려면 매개 변수 이름을 클릭합니다.

- 모든 엔터프라이즈 매개 변수에 대한 설명을 보려면 **?**를 클릭합니다.

엔터프라이즈 매개 변수 업데이트

엔터프라이즈 매개 변수 구성 창을 열고 시스템 수준의 설정을 구성하려면 이 절차를 사용합니다.

주의 대부분의 엔터프라이즈 매개 변수는 변경할 필요가 없습니다. 변경하려는 기능을 완전히 이해했거나 Cisco TAC(기술 지원 센터)에서 변경을 조언한 경우가 아니면 엔터프라이즈 매개 변수를 변경하지 마십시오.

절차

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 변경하려는 엔터프라이즈 매개 변수의 원하는 값을 선택합니다.

단계 **3** 저장을 클릭합니다.

다음에 할 작업

장치에 구성 적용, 124 페이지

장치에 구성 적용

사용자가 구성한 설정으로 클러스터에 있는 모든 영향을 받는 장치를 업데이트하려면 이 절차를 사용합니다.

시작하기 전에

엔터프라이즈 매개 변수 업데이트, 124 페이지

절차

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 변경 사항을 확인한 다음 저장을 클릭합니다.

단계 **3** 다음 옵션 중 하나를 선택합니다.

- 시스템이 재부팅할 장치를 결정하도록 하려면 구성 적용을 클릭합니다. 경우에 따라 장치를 재부팅할 필요가 없습니다. 장치 풀에 SIP 트렁크가 포함되어 있지 않으면 진행 중인 통화가 끊길 수 있지만 연결된 통화는 유지됩니다.

- 클러스터의 모든 장치를 재부팅하려면 재설정을 클릭합니다. 이 단계는 사용량이 적은 시간 동안 수행하는 것이 좋습니다.

단계 **4** 확인 대화 상자를 읽은 후 확인을 클릭합니다.

기본 엔터프라이즈 매개 변수 복원

엔터프라이즈 매개 변수를 기본 설정으로 재설정하려면 이 절차를 사용합니다. 일부 엔터프라이즈 매개 변수에 구성 창의 열에 표시된 대로 제안된 값이 포함되어 있습니다. 이 절차는 이러한 값을 기본 설정으로 사용합니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 기본값으로 설정을 클릭합니다.

단계 **3** 확인 프롬프트를 읽은 후 확인을 클릭합니다.

14 장

서버 관리

서버 관리 개요

이 장에서는 Cisco Unified Communications Manager 관리 노드의 속성을 관리하고 Presence 서버 상태를 보고 Unified Communications Manager 서버의 호스트 이름을 구성하는 방법을 설명합니다.

클러스터에서 노드 제거

IM and Presence 서비스 노드를 해당 프레즌스 중복 그룹에서 안전하게 제거해야 하는 경우 이 절차를 수행합니다.

⚠ 주의 노드를 제거하면 프레즌스 중복 그룹에 있는 나머지 노드의 사용자에 대한 서비스가 중단됩니다. 이 절차는 유지 보수 기간 동안에만 수행해야 합니다.

절차

단계 **1** **Cisco Unified CM** 관리 > 시스템 > 프레즌스 중복 그룹페이지에서 고가용성이 활성화되어 있는 경우 이를 비활성화합니다.

단계 **2** **Cisco Unified CM** 관리 > 사용자 관리 > **Presence** 사용자 할당 페이지에서 제거할 노드의 모든 사용자를 할당 해제하거나 이동합니다.

단계 **3** 해당 프레즌스 중복 그룹에서 노드를 제거하려면 프레즌스 중복 그룹의 [프레즌스 중복 그룹 구성] 창에 있는 [Presence 서버] 드롭다운 목록에서 선택하지 않음을 선택합니다. 경고 대화 상자에 노드 할당 해제로 인해 프레즌스 중복 그룹의 서비스가 다시 시작된다는 내용이 표시되면 확인을 선택합니다.

단계 **4** **Cisco Unified CM** 관리 > 시스템 > 서버 페이지에서 할당 해제된 노드를 삭제합니다. 경고 대화 상자에 이 작업을 실행 취소할 수 없다는 내용이 표시되면 확인을 선택합니다.

단계 **5** 할당 해제한 노드의 호스트 VM 또는 서버를 종료합니다.

삭제된 서버를 클러스터에 다시 추가

Cisco Unified Communications Manager 관리에서 후속 노드(가입자)를 삭제한 후 클러스터에 다시 추가하려면 다음 절차를 수행합니다.

절차

단계 **1** Cisco Unified Communications Manager 관리에서 시스템 > 서버를 선택하여 서버를 추가합니다.

단계 **2** Cisco Unified Communications Manager 관리에 후속 노드를 추가한 후 소프트웨어 키트에 제공된 디스크를 사용하여 서버에 설치합니다.

팁 예를 들어, 버전 8.5(1) 디스크가 있으면 노드에 8.5(1)를 설치합니다. 6.1(3) 호환 버전 디스크가 있는 경우에는 디스크를 사용하여 후속 노드에 Cisco Unified CM을 설치합니다. 설치하는 동안 설치 화면에 옵션이 표시되면 [설치 시 업그레이드] 옵션을 선택합니다.

후속 노드에 설치하는 버전이 클러스터의 첫 번째 노드(게시자)에 실행하는 버전과 일치해야 합니다.

클러스터의 첫 번째 노드에서 Cisco Unified Communications Manager 8.5(1) 버전 및 서비스 업데이트(또는 엔지니어링 전문)가 실행되는 경우 설치 화면에 설치 옵션이 표시되면 [설치 시 업그레이드] 옵션을 선택해야 합니다. 이 옵션은 DVD 또는 원격 서버의 서비스 업데이트(또는 엔지니어링 전문) 이미지에 액세스할 수 있어야 선택할 수 있습니다. 설치하는 방법에 대한 자세한 내용은 해당 Cisco Unified Communications Manager 버전을 지원하는 설치 설명서를 참조하십시오.

단계 **3** Cisco Unified CM을 설치한 후에는 해당 Cisco Unified CM 버전을 지원하는 설치 설명서에 설명된 대로 후속 노드를 구성합니다.

단계 **4** Cisco Unified Reporting, RTMT 또는 CLI에 액세스하여 기존 노드 사이에서 데이터베이스 복제가 발생하는지 확인합니다. 필요한 경우 노드 간 데이터베이스 복제를 복구합니다.

설치 전 클러스터에 노드 추가

노드 설치 전에 [Cisco Unified Communications Manager 관리]를 사용하여 클러스터에 새 노드를 추가합니다. 노드를 추가할 때 선택하는 서버 유형과 설치하는 서버 유형이 일치해야 합니다.

새 노드를 설치하기 전에 첫 번째 노드에서 [Cisco Unified Communications Manager 관리]를 사용하여 새 노드를 구성해야 합니다. 클러스터에 노드를 설치하려면 *Cisco Unified Communications Manager* 설치 설명서를 참조하십시오.

Cisco Unified Communications Manager 비디오/음성 서버의 경우 Cisco Unified Communications Manager 소프트웨어의 초기 설치 중 추가하는 첫 번째 서버가 게시자 노드로 지정됩니다. 이후 설치 또는 추가되는 서버는 모두 가입자 노드로 지정됩니다. 클러스터에 추가하는 첫 번째 Cisco Unified Communications Manager IM and Presence 노드는 IM and Presence 서비스 데이터베이스 게시자 노드로 지정됩니다.

참고 서버가 추가된 후에는 [Cisco Unified Communications Manager 관리]를 사용하여 서버 유형을 변경할 수 없습니다. 기존 서버 인스턴스를 삭제한 다음 새 서버를 다시 추가하고 서버 유형 설정을 올바로 선택해야 합니다.

절차

단계 **1** 시스템 > 서버를 선택합니다.
서버 찾기 및 나열 창이 표시됩니다.

단계 **2** 새로 추가를 클릭합니다.
서버 구성 - 서버 추가 창이 표시됩니다.

단계 **3** 서버 유형 드롭다운 목록 상자에서 추가할 서버를 선택한 후 다음을 클릭합니다.

- CUCM 비디오/음성
- CUCM IM and Presence

단계 **4** 서버 구성 창에서 서버 설정을 적절히 입력합니다.
서버 구성 필드에 대한 설명은 서버 설정을 참조하십시오.

단계 **5** 저장을 클릭합니다.

Presence 서버 상태 보기

Cisco Unified CM 관리를 사용하여 IM and Presence 서비스 노드의 중요 서비스 및 셀프 진단 테스트 결과에 대한 상태를 확인합니다.

절차

단계 **1** 시스템 > 서버를 선택합니다.
서버 찾기 및 나열 창이 나타납니다.

단계 **2** 서버 검색 매개 변수를 선택한 다음 찾기를 클릭합니다.
일치하는 레코드가 나타납니다.

단계 **3** 서버 찾기 및 나열 창에 나열되는 IM and Presence 서버를 선택합니다.
서버 구성 창이 나타납니다.

단계 **4** 서버 구성 창의 [IM and Presence 서버 정보] 섹션에서 [Presence 서버 상태] 링크를 클릭합니다.
서버에 대한 노드 세부 정보 창이 표시됩니다.

호스트 이름 구성

다음 표에서는 Unified Communications Manager 서버의 호스트 이름을 구성할 수 있는 위치, 호스트 이름에 대해 허용되는 문자 수 및 호스트 이름에 대해 권장되는 첫 번째와 마지막 문자 수를 나열합니다. 호스트 이름을 올바르게 구성하지 않을 경우 운영 체제, 데이터베이스 설치 등과 같은 Unified Communications Manager의 일부 구성 요소가 예상대로 작동하지 않을 수 있습니다.

주의 다음 표에 나열된 위치의 호스트 이름 또는 IP 주소를 변경하기 전에 *Cisco Unified Communications Manager*에 대한 *IP* 주소 및 호스트 이름 변경 문서를 참조하십시오. 구성한 후 호스트 이름 또는 IP 주소를 올바르게 업데이트하지 않으면 Unified Communications Manager에 문제가 발생할 수 있습니다.

표 *7: Cisco Unified Communications Manager*에서 호스트 이름 구성

호스트 이름 위치	허용되는 구성	허용되는 문자 수	호스트 이름에 권장되는 첫 번째 문자	호스트 이름에 권장되는 마지막 문자
호스트 이름/IP 주소 필드 Cisco Unified Communications Manager Administration의 시스템 > 서버	클러스터에서 서버의 호스트 이름을 추가 또는 변경할 수 있습니다.	2-63	영문자	영숫자
호스트 이름 필드 Cisco Unified Communications Manager 설치 마법사	클러스터에서 서버의 호스트 이름을 추가할 수 있습니다.	1-63	영문자	영숫자
호스트 이름 필드 Cisco Unified Communications 운영 체제의 설정 > **IP** > 이더넷	클러스터에서 서버의 호스트 이름을 변경할 수 있으며 추가할 수는 없습니다.	1-63	영문자	영숫자
set network hostname hostname Command Line Interface	클러스터에서 서버의 호스트 이름을 변경할 수 있으며 추가할 수는 없습니다.	1-63	영문자	영숫자

팁 호스트 이름은 ARPANET 호스트 이름에 대한 규칙을 따라야 합니다. 호스트 이름의 첫 번째 문자와 마지막 문자 사이에 영숫자와 하이픈을 입력할 수 있습니다.

모든 위치에서 호스트 이름을 구성하기 전에 다음 정보를 검토합니다.

- 장치-서버, 애플리케이션-서버 및 서버-서버 통신을 지원하는 서버 구성 창의 호스트 이름/IP 주소 필드를 사용하면 점으로 구분된 형식의 IPv4주소 또는 호스트 이름을 입력할 수 있습니다. Unified Communications Manager 게시자 노드를 설치한 후에 게시자의 호스트 이름이 이 필드에 자동으로 표시됩니다. Unified Communications Manager 가입자 노드를 설치하기 전에 Unified Communications Manager 게시자 노드에서 이 필드에 가입자 노드의 IP 주소 또는 호스트 이름을 입력합니다.

  이 필드에 Unified Communications Manager가 DNS 서버에 액세스하여 IP 주소에 대한 호스트 이름을 확인할 수 있는 경우에만 호스트 이름을 구성합니다. 반드시 DNS 서버에서 Cisco Unified Communications Manager 이름과 주소 정보를 구성해야 합니다.

팁 DNS 서버에서 Unified Communications Manager 정보를 구성하는 것 외에도 Cisco Unified Communications Manager를 설치하는 동안 DNS 정보를 입력합니다.

- Unified Communications Manager 게시자 노드를 설치하는 동안 정적 네트워킹을 사용하려는 경우 필수인 호스트 이름과 게시자 노드의 IP 주소를 입력하여 네트워크 정보를 구성합니다. Unified Communications Manager 가입자 노드를 설치하는 동안 Unified Communications Manager가 네트워크 연결 및 게시자-가입자를 확인할 수 있도록 Unified Communications Manager 게시자 노드의 호스트 이름과 IP 주소를 입력합니다. 뿐만 아니라, 가입자 노드에 대한 호스트 이름 및 IP 주소를 입력해야 합니다. Unified Communications Manager 설치 프로그램에서 가입자 서버의 호스트 이름을 묻는 메시지를 표시하는 경우 호스트 이름/IP 주소 필드에 가입자 서버의 호스트 이름을 구성했으면 Cisco Unified Communications Manager 관리의 서버 구성 창에 표시되는 값을 입력합니다.

V 부

보안 관리

15 장

SAML Single Sign-On 관리

SAML Single Sign-On 개요

SAML Single Sign-On(SSO)을 사용하여 이러한 애플리케이션 중 하나에 로그인한 후 Cisco 애플리케이션의 정의된 집합에서 액세스할 수 있습니다. SAML은 신뢰할 수 있는 비즈니스 파트너 간의 보안 관련 정보 교환에 대해 설명합니다. 이것은 사용자를 인증하기 위해 서비스 제공자(예: Cisco Unified Communications Manager)에서 사용하는 인증 프로토콜입니다. SAML을 사용하여 IdP(ID 공급자)와 서비스 공급자 간에 보안 인증 정보가 교환됩니다. 기능은 다양한 애플리케이션 간에 일반 인증서 및 관련 정보를 사용하는 보안 메커니즘을 제공합니다.

SAML SSO는 메타데이터 및 인증서를 프로비저닝 프로세스의 일부로 IdP와 서비스 제공자 간에 교환하여 CoT(Circle of Trust)를 설정합니다. 서비스 제공자는 IdP의 사용자 정보를 신뢰하여 다양한 서비스 또는 애플리케이션에 대한 액세스를 제공합니다.

클라이언트가 IdP를 인증하고 IdP는 클라이언트에 어설션을 부여합니다. 클라이언트는 서비스 제공자에 어설션을 제공합니다. CoT가 설정되었으므로 서비스 제공자는 어설션을 신뢰하고 클라이언트에 대한 액세스를 부여합니다.

iOS에서 Cisco Jabber용 인증서 기반 SSO 인증을 위한 옵트인 제어

Cisco Unified Communications Manager의 이 릴리스는 IdP(ID 공급자)를 사용하여 iOS SSO 로그인 동작에서 Cisco Jabber를 제어하기 위한 옵트인 구성 옵션을 소개합니다. 이 옵션을 사용하면 Cisco Jabber에서 제어되는 모바일 장치 관리(MDM) 배포에서 IdP를 사용하여 인증서 기반 인증을 수행할 수 있습니다.

Cisco Unified Communications Manager의 **iOS**용 **SSO** 로그인 동작 엔터프라이즈 매개 변수를 통해 옵트인 제어를 구성할 수 있습니다.

참고 이 매개 변수의 기본값을 변경하기 전에 http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html에서 Cisco Jabber 기능 지원 및 설명서를 참조하여 iOS의 Cisco Jabber가 SSO 로그인 동작 및 인증서 기반 인증을 지원하는지 확인하십시오.

이 기능을 활성화하려면 iOS에 Cisco Jabber용 SSO 로그인 동작 구성, 138 페이지 절차를 참조하십시오.

SAML Single Sign-On 필수 구성 요소

- Cisco Unified Communications Manager 클러스터를 위해 구성된 DNS
- IdP(ID 공급자) 서버
- IdP 서버에서 신뢰하고 시스템에서 지원하는 LDAP 서버

SAML 2.0을 사용하는 다음 IdP는 SAML SSO 기능에 대해 테스트됩니다.

- OpenAM 10.0.1
- Microsoft® Active Directory® 페더레이션 서비스 2.0(AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

타사 애플리케이션은 다음과 같은 구성 요구 사항을 충족해야 합니다.

- IdP에 필수 특성 "uid"를 구성해야 합니다. 이 특성은 Cisco Unified Communications Manager에서 LDAP 동기화된 사용자 ID로 사용되는 특성과 일치해야 합니다.

  참고 Cisco Unified Communications Manager는 현재 사용자 ID 설정에 대한 LDAP 특성으로 sAMAccountName 옵션만 지원 합니다.

  필수 특성 매핑을 구성하는 방법에 대한 내용은 IdP 제품 설명서를 참조하십시오.

- SAML SSO에 참여하는 모든 엔티티의 시계를 동기화해야 합니다. 시계를 동기화하는 방법에 대한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html의 *Cisco Unified Communications Manager* 시스템 구성 설명서에서 "NTP 설정"을 참조하십시오.

SAML Single Sign-On 관리

SAML Single Sign-On 활성화

참고 동기화 에이전트 테스트 확인에 성공하기 전까지는 SAML SSO를 활성화할 수 없습니다.

시작하기 전에

- 사용자 데이터가 Cisco Unified Communications Manager 데이터베이스에 동기화되었는지 확인합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.
- Cisco Unified CM IM and Presence 서비스 Cisco 동기화 에이전트 서비스에서 데이터 동기화를 성공적으로 완료했는지 확인합니다. **Cisco Unified CM IM and Presence** 관리 > 진단 > 시스템 문제 해결 도구를 선택하여 이 테스트의 상태를 확인합니다. “Sync Agent에서 관련 데이터(예: 장치, 사용자, 라이센싱 정보)를 동기화함” 테스트에서는 데이터 동기화가 성공적으로 완료된 경우 "테스트 통과" 결과를 표시합니다.
- 하나 이상의 LDAP 동기화된 사용자가 표준 CCM 수퍼 사용자 그룹에 추가되어 Cisco Unified CM 관리에 액세스할 수 있는지 확인합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.
- IdP와 서버 간 신뢰 관계를 구성하려면 먼저 IdP에서 신뢰 메타데이터 파일을 얻은 후 모든 서버로 가져와야 합니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 시스템 > **SAML Single Sign-On**을 선택합니다.
단계 **2** **SAML SSO** 활성화를 클릭합니다.
단계 **3** 모든 서버 연결이 다시 시작될 것임을 알려주는 경고 메시지가 표시되면 계속을 클릭합니다.
단계 **4** 찾아보기를 클릭하여 IdP 메타데이터를 찾고 업로드합니다.
단계 **5** **IdP** 메타데이터 가져오기를 클릭합니다.
단계 **6** 다음을 클릭합니다.
단계 **7** 신뢰 메타데이터 파일 집합 다운로드를 클릭하여 서버 메타데이터를 시스템으로 다운로드합니다.
단계 **8** IdP 서버에서 서버 메타데이터를 업로드합니다.
단계 **9** 다음을 클릭하여 작업을 계속합니다.
단계 **10** 유효한 관리자 ID 목록에서 관리자 권한이 있는 LDAP 동기화된 사용자를 선택합니다.
단계 **11** 테스트 실행을 클릭합니다.
단계 **12** 유효한 사용자 이름과 암호를 입력합니다.
단계 **13** 성공 메시지가 표시되면 브라우저 창을 닫습니다.
단계 **14** 완료를 클릭하고 웹 애플리케이션이 다시 시작될 때까지 1 ~ 2분 기다립니다.

iOS에 Cisco Jabber용 SSO 로그인 동작 구성

절차

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.
단계 **2** 옵트인 제어를 구성하려면 SSO 구성 섹션에서 **iOS**에 대한 **SSO** 로그인 동작 매개 변수에 대해 기본 브라우저 사용 옵션을 선택합니다.
참고 **iOS**에 대한 **SSO** 로그인 동작 매개 변수는 다음 옵션을 포함합니다.

- 포함된 브라우저 사용—이 옵션을 활성화하면 Cisco Jabber는 SSO 인증을 위해 포함된 브라우저를 사용합니다. 이 옵션을 사용하여 기본 Apple Safari 브라우저로 교차 실행하지 않고 버전 9 이전의 iOS 장치에서 SSO를 사용할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다.
- 기본 브라우저 사용—이 옵션을 활성화하면 Cisco Jabber는 iOS 장치의 Apple Safari 프레임워크를 사용하여 MDM 배포에서 IdP(Identity Provider)를 사용하여 인증서 기반 인증을 수행합니다.
  참고 기본 브라우저 사용은 포함된 브라우저 사용만큼 안전하지 않으므로 제어된 MDM 배포를 제외하고 이 옵션을 구성하는 것이 좋습니다.

단계 **3** 저장을 클릭합니다.

업그레이드한 후 WebDialer에서 SAML Single Sign-on 활성화

업그레이드 후에 Cisco WebDialer에서 SAML Single Sign-On을 다시 활성화하려면 이 작업을 수행합니다. SAML Single Sign-On을 활성화하기 전에 Cisco WebDialer가 활성화된 경우 Cisco WebDialer에서 기본적으로 SAML Single Sign-On이 활성화되지 않습니다.

절차

	명령 또는 동작	목적
단계 **1**	Cisco WebDialer 서비스 비활성화, 139 페이지	Cisco WebDialer 웹 서비스가 이미 활성화되어 있는 경우 비활성화합니다.
단계 **2**	SAML Single Sign-On 비활성화, 139 페이지	SAML Single Sign-on이 이미 활성화 되어 있는 경우 비활성화합니다.
단계 **3**	Cisco WebDialer 서비스 활성화, 140 페이지	
단계 **4**	SAML Single Sign-On 활성화, 137 페이지	

Cisco WebDialer 서비스 비활성화

Cisco WebDialer 웹 서비스가 이미 활성화되어 있는 경우 비활성화합니다.

절차

단계 **1** Cisco Unified Serviceability에서 도구 > 서비스 활성화를 선택합니다.
단계 **2** 서버 드롭다운 목록에서 나열된 Cisco Unified Communications Manager 서버를 선택합니다.
단계 **3** **CTI** 서비스에서 **Cisco WebDialer** 웹 서비스 확인란을 선택 취소합니다.
단계 **4** 저장을 클릭합니다.

다음에 할 작업

SAML Single Sign-On 비활성화, 139 페이지

SAML Single Sign-On 비활성화

SAML Single Sign-on이 이미 활성화 되어 있는 경우 비활성화합니다.

시작하기 전에

Cisco WebDialer 서비스 비활성화, 139 페이지

절차

CLI에서 명령 **utils sso disable**을 실행합니다.

다음에 할 작업

Cisco WebDialer 서비스 활성화, 140 페이지

Cisco WebDialer 서비스 활성화

시작하기 전에

SAML Single Sign-On 비활성화, 139 페이지

절차

단계 **1** Cisco Unified Serviceability에서 도구 > 서비스 활성화를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 나열된 Cisco Unified Communications Manager 서버를 선택합니다.

단계 **3** **CTI** 서비스에서 **Cisco WebDialer** 웹 서비스 확인란을 선택합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** Cisco Unified Serviceability에서 도구 > 제어 센터 - 기능 서비스를 선택하여 CTI 관리자 서비스가 활성 상태이며 시작 모드인지 확인합니다.
Webdialer가 제대로 작동하려면 CTI 관리자 서비스를 활성화하고 시작 모드에 있어야 합니다.

다음에 할 작업

SAML Single Sign-On 활성화, 137 페이지

복구 URL에 액세스

복구 URL을 사용하면 문제 해결을 위해 SAML Single Sign-On을 우회하여 Cisco Unified Communications Manager 관리 및 Cisco Unified CM IM and Presence 서비스 인터페이스에 로그인할 수 있습니다. 예를 들어, 서버의 도메인 또는 호스트 이름을 변경하기 전에 복구 URL을 활성화합니다. 복구 URL에 로그인하여 서버 메타데이터를 손쉽게 업데이트할 수 있습니다.

시작하기 전에

- 관리 권한이 있는 애플리케이션 사용자만 복구 URL에 액세스할 수 있습니다.
- SAML SSO가 활성화된 경우, 복구 URL은 기본적으로 활성화됩니다. CLI에서 복구 URL을 활성화하거나 비활성화할 수 있습니다. 복구 URL을 활성화 및 비활성화하기 위한 CLI 명령에 대한 자세한 내용은 *Command Line Interface Guide for Cisco Unified Communications Solutions*를 참조하십시오.

절차

브라우저에 https://hostname:8443/ssosp/local/login을 입력합니다.

도메인 또는 호스트 이름 변경 후 서버 메타데이터 업데이트

도메인 또는 호스트 이름을 변경한 후 이 절차를 수행할 때까지 SAML Single Sign-On이 작동하지 않습니다.

참고 이 절차를 수행한 후에도 **SAML Single Sign-On** 창에 액세스할 수 없는 경우에는 브라우저 캐시를 지우고 다시 로그인해 보십시오.

시작하기 전에

복구 URL이 비활성화된 경우 Single Sign-On 링크를 우회할 URL이 나타나지 않습니다. 복구 URL을 활성화하려면 CLI에 로그인하고 **utils sso recovery-url enable**명령을 실행합니다.

절차

단계 **1** 웹 브라우저의 주소 표시줄에 다음 URL을 입력합니다.
https://<Unified CM-server-name>

여기서 <Unified CM-server-name>은 서버의 IP 주소 또는 호스트 이름입니다.

단계 **2** **Single Sign On(SSO)**를 우회할 복구 **URL**을 클릭합니다.

단계 **3** 관리자 역할을 가진 애플리케이션 사용자의 자격 증명을 입력하고 로그인을 클릭합니다.

단계 **4** [Cisco Unified CM 관리]에서 시스템 > **SAML Single Sign-On**을 선택합니다.

단계 **5** 메타데이터 내보내기를 클릭하여 서버 메타데이터를 다운로드합니다.

단계 **6** 서버 메타데이터 파일을 IdP에 업로드합니다.

단계 **7** 테스트 실행을 클릭합니다.

단계 **8** 올바른 사용자 ID 및 암호를 입력합니다.

단계 **9** 성공 메시지가 표시되면 브라우저 창을 닫습니다.

서버 메타데이터 수동 프로비저닝

여러 개의 UC 애플리케이션에 대한 ID 공급자에서 단일 연결을 설정하려면 ID 공급자 및 서비스 공급업체 사이에 신뢰할 수 있는 범위를 구성하는 한편, 서버 메타데이터를 수동으로 설정해야 합니다. 신뢰할 수 있는 범위를 구성하는 방법에 대한 자세한 내용은 IdP 제품 설명서를 참조하십시오.

일반적인 URL 구문은 다음과 같습니다.

https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>

절차

서버 메타데이터를 수동으로 설정하려면 ACS(Assertion Customer Service) URL을 사용합니다.

예제:
샘플 ACS URL: <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"
index="0"/>

16 장

인증서 관리

인증서 개요

시스템은 자체 서명 인증서 및 타사 서명 인증서를 사용합니다. 인증서는 장치를 안전하게 인증하고 데이터를 암호화하고 데이터를 해싱하여 소스와 대상 간의 무결성을 보장하기 위해 시스템의 장치 간에 사용됩니다. 인증서를 사용하면 대역폭, 통신 및 작업을 안전하게 전송할 수 있습니다.

인증서의 가장 중요한 부분은 데이터를 암호화하고 대상 웹사이트, 전화 또는 FTP 서버와 같은 항목과 공유하는 방법을 숙지하고 정의하는 것입니다.

시스템이 인증서를 신뢰하는 경우 올바른 대상과 정보를 공유하는 것을 완벽하게 신뢰할 수 있도록 시스템에 인증서가 미리 설치되어 있음을 의미합니다. 그렇지 않으면, 이러한 지점 간 통신은 종료됩니다.

인증서를 신뢰하기 위해서는 타사 인증 기관(CA)과 미리 신뢰가 설정되어 있어야 합니다.

장치가 CA 및 중간 인증서를 먼저 신뢰할 수 있음을 알고 있어야 보안 소켓 레이어(SSL) 핸드셰이크라고 하는 메시지를 교환하여 제공되는 서버 인증서를 신뢰할 수 있습니다.

참고

Tomcat용 EC 기반 인증서가 지원됩니다. 이 새로운 인증서를 tomcat-ECDSA라고 합니다. 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence* 서비스 구성 및 관리의 IM and Presence 서비스 섹션에서 향상된 TLS 암호화를 참조하십시오.

Tomcat 인터페이스의 EC Ciphers는 기본적으로 비활성화됩니다. Cisco Unified Communications Manager 또는 IM and Presence 서비스에서 **HTTPS** 암호 엔터프라이즈 매개 변수를 사용하여 활성화할 수 있습니다. 이 매개 변수를 변경하는 경우 모든 노드에서 Cisco Tomcat 서비스를 다시 시작해야 합니다.

EC-기반 인증서에 대한 자세한 내용은 Cisco Unified Communications Manager 및 IM and Presence 서비스에서 릴리스 노트의 승인된 솔루션을 위한 일반 기준에 대한 ECDSA 지원을 참조하십시오.

타사 서명 인증서 또는 인증서 체인

애플리케이션 인증서를 서명한 인증 기관의 인증 기관 루트 인증서를 업로드합니다. 하위 인증 기관이 애플리케이션 인증서를 서명한 경우 하위 인증 기관의 인증 기관 루트 인증서를 업로드해야 합니다. 모든 인증 기관 인증서의 PKCS#7 형식 인증서 체인을 업로드할 수도 있습니다.

동일한 인증서 업로드 대화 상자를 사용하여 인증 기관 루트 인증서 및 애플리케이션 인증서를 업로드할 수 있습니다. 인증 기관 루트 인증서 또는 인증 기관 인증서만 포함된 인증서 체인을 업로드할 때는 형식 인증서 type-trust인 인증서 이름을 선택합니다. 애플리케이션 인증서 또는 애플리케이션 인증서와 인증 기관 인증서를 포함하는 인증서 체인을 업로드할 때는 인증서 유형만 포함하는 인증서 이름을 선택합니다.

예를 들어, Tomcat 인증 기관 인증서 또는 인증 기관 인증서 체인을 업로드할 때는 **tomcat-trust**를 선택하고 Tomcat 애플리케이션 인증서 또는 애플리케이션 인증서와 인증 기관 인증서를 포함하는 인증서 체인을 업로드할 때는 **tomcat** 또는 **tomcat ECDSA**를 선택합니다.

CAPF 인증 기관 루트 인증서를 업로드할 때 CallManager-trust 저장소로 복사되므로 하지 CallManager용 인증 기관 루트 인증서를 별도로 업로드할 필요가 없습니다.

참고

타사 인증 기관에서 서명한 인증서를 성공적으로 업로드하면 서명된 인증서를 가져오는 데 사용된 최근에 생성된 CSR을 삭제하고 타사에서 서명한 인증서(업로드한 경우)를 포함하여 기존 인증서를 덮어씁니다.

참고

시스템은 tomcat-trust, CallManager-trust 및 Phone-SAST-trust 인증서를 클러스터의 각 노드에 자동으로 복제합니다.

참고 디렉터리 신뢰 인증서를 tomcat-trust에 업로드할 수 있으며, 이는 DirSync 서비스가 보안 모드에서 작동하는 데 필요합니다.

타사 인증 기관 인증서

타사 인증 기관이 발행하는 애플리케이션 인증서를 사용하려면 인증 기관 또는 PKCS #7 인증서 체인에서 서명된 애플리케이션 인증서 및 인증 기관 루트 인증서를 모두 얻어야 합니다(구별된 인코딩 규칙 [DER]). 여기에는 애플리케이션 인증서와 인증 기관 인증서가 모두 포함됩니다. 인증 기관에서 이러한 인증서를 받는 방법에 대한 정보를 검색합니다. 프로세스는 인증 기관마다 다릅니다. 서명 알고리즘은 RSA 암호화를 사용해야 합니다.

Cisco Unified Communications 운영 체제는 프라이버시 향상 메일(PEM) 인코딩 형식으로 CSR을 생성합니다. 시스템은 DER 및 PEM 인코딩 형식의 인증서와 PEM 형식의 PKCS #7 인증서 체인을 사용할 수 있습니다. CAPF(인증 기관 프록시 기능)를 제외한 모든 인증서 유형의 경우 인증 기관 루트 인증서와 애플리케이션 인증서를 받아 각 노드에 업로드해야 합니다.

CAPF의 경우 인증 기관 루트 인증서와 애플리케이션 인증서를 받아 첫 번째 노드에만 업로드합니다. CAPF 및 Cisco Unified Communications ManagerCSR은 인증 기관으로부터 애플리케이션 인증서 요청 시 포함해야 하는 확장을 포함합니다. 인증 기관이 ExtensionRequest 메커니즘을 지원하지 않을 경우 다음과 같이 X.509 확장을 활성화해야 합니다.

- CAPF CSR은 다음 확장을 사용합니다.

```
X509v3 확장 키 사용:
TLS, 웹 서버 인증, IPSec 엔드 시스템
X509v3 키 사용:
디지털 서명, 인증서 서명
```

- Tomcat 및 Tomcat-ECDSA용 CSR은 다음과 같은 확장을 사용합니다.

참고 Tomcat 또는 Tomcat-ECDSA 는 키 계약 또는 IPsec 엔드 시스템 키 사용을 요구하지 않습니다.

```
X509v3 확장 키 사용: TLS 웹 서버 인증, TLS 웹 클라이언트 인증, IPSec 엔드 시스템 X509v3 키 사용: 디지털 서명, 키 암호화, 데이터 암호화, 키 계약
```

- IPsec용 CSR은 다음 확장을 사용합니다.

```
 X509v3 확장 키 사용:
TLS 웹 서버 인증, TLS 웹 클라이언트 인증, IPSec 엔드 시스템
X509v3 키 사용:
디지털 서명, 키 암호화, 데이터 암호화, 키 계약
```

- Cisco Unified Communications Manager용 CSR은 다음 확장을 사용합니다.

```
 X509v3 확장 키 사용:
TLS 웹 서버 인증, TLS 웹 클라이언트 인증
X509v3 키 사용:
디지털 서명, 키 암호화, 데이터 암호화, 키 계약
```

참고 인증서에 대한 CSR을 생성하고 SHA256 서명을 사용하여 타사 인증 기관이 서명하도록 할 수 있습니다. 그런 다음 이 서명된 인증서를 다시 Cisco Unified Communications Manager에 업로드하여, Tomcat 및 기타 인증서가 SHA256을 지원할 수 있습니다.

인증서 표시

사용자 시스템에 속하는 인증서 및 신뢰 저장소에 대한 세부 정보를 확인합니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** 찾기 제어를 사용하여 인증서 목록을 필터링합니다.

단계 **3** 인증서 또는 신뢰 저장소의 세부 정보를 보려면 인증서의 .PEM 또는 .DER 파일 이름을 클릭합니다.

단계 **4** 인증서 목록 창으로 돌아가려면 관련 링크 목록에서 찾기/나열로 돌아가기를 클릭한 다음, 이동을 클릭합니다.

인증서 다운로드

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** 검색 기준을 지정하고 찾기를 클릭합니다.

단계 **3** 인증서의 파일 이름 또는 인증서 신뢰 목록(CTL)을 선택합니다.

단계 **4** 다운로드를 클릭합니다.

중간 인증서 설치

중간 인증서를 설치하려면 먼저 루트 인증서를 설치하고 서명된 인증서를 업로드해야 합니다. 이 단계는 특정 체인에서 여러 인증서가 있는 서명된 인증서를 인증 기관에서 제공하는 경우에만 필요합니다.

팁 루트 인증서 이름은 루트 인증서를 업로드할 때 생성된 `.pem` 파일입니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 클릭합니다.

단계 **2** 인증서 업로드를 클릭합니다.

단계 **3** 인증서 용도 드롭다운 목록에서 **intelligenceCenter-srvr-trust**를 선택하여 루트 인증서를 설치합니다.

단계 **4** 찾아보기를 클릭하고 파일을 탐색한 다음 열기를 클릭합니다.

단계 **5** 파일 업로드를 클릭합니다.

단계 **6** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **7** 인증서 업로드를 클릭합니다.

단계 **8** 인증서 업로드 팝업 창의 인증서 이름 드롭다운 목록에서 **IntelligenceCenter-srvr**를 선택하고 루트 인증서 이름을 입력합니다.

단계 **9** 다음 단계 중 하나를 수행하여 업로드할 파일을 선택합니다.

- 파일 업로드 텍스트 상자에서 파일의 경로를 입력합니다.
- 찾아보기를 클릭하고 파일을 탐색한 다음 열기를 클릭합니다.

단계 **10** 파일 업로드를 클릭합니다.

단계 **11** 고객 인증서를 설치한 후 FQDN을 사용하여 Cisco Unified Intelligence Center URL에 액세스합니다. IP 주소를 사용하여 Cisco Unified Intelligence Center에 액세스하는 경우 사용자 정의 인증서를 성공적으로 설치한 후에도 "계속 하려면 여기를 클릭하십시오." 메시지가 표시됩니다.

참고 Tomcat 인증서가 업로드되면 TFTP 서비스를 비활성화하고 나중에 활성화해야 합니다. 그렇지 않으면 TFTP는 이전 캐시된 자체 서명 tomcat 인증서를 계속 제공하게 됩니다.

신뢰 인증서 삭제

신뢰할 수 있는 인증서는 삭제할 수 있는 유일한 인증서 유형입니다. 시스템에서 생성되는 자체 서명된 인증서는 삭제할 수 없습니다.

주의 인증서를 삭제하면 시스템 작동에 영향을 미칠 수 있습니다. 인증서를 삭제하면 인증서가 기존 체인의 일부인 경우 인증서 체인이 끊어질 수 있습니다. 인증서 목록 창에서 관련 인증서의 사용자 이름 및 제목 이름에서 이 관계를 확인할 수 있습니다. 이 작업은 취소할 수 없습니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** 찾기 제어를 사용하여 인증서 목록을 필터링합니다.

단계 **3** 인증서의 파일 이름을 선택합니다.

단계 **4** 삭제를 클릭합니다.

단계 **5** 확인을 클릭합니다.

참고 삭제하는 인증서가 유형 "tomcat-trust", "CallManager-trust" 또는 "Phone-SAST-trust"인 경우 클러스터의 모든 서버에서 인증서가 삭제됩니다.

인증서 다시 생성

만료된 경우 인증서를 다시 생성합니다. 전화기를 다시 시작하고 서비스를 다시 부팅해야 하기 때문에 업무 시간이 끝난 후 이 절차를 수행합니다. Cisco Unified OS 관리에서 유형이 "cert"로 나열되는 인증서만 재생성할 수 있습니다.

주의 인증서를 다시 생성하면 시스템 작동에 영향을 미칠 수 있습니다. 인증서를 다시 생성하면 업로드된 경우 타사 서명 인증서를 포함하여 기존 인증서를 덮어씁니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** 새 자체 서명 인증서 생성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **3** 생성을 클릭합니다.

단계 **4** 다시 생성된 인증서의 영향을 받는 모든 서비스를 다시 시작합니다. 인증서 이름 및 해당 설명에 대한 자세한 내용은 관련 항목 섹션을 참조하십시오.

단계 **5** CAPF 또는 CallManager 인증서를 다시 생성한 후에 CTL 클라이언트(구성된 경우)를 다시 실행합니다.

참고 Tomcat 인증서가 다시 생성되면 TFTP 서비스를 비활성화하고 나중에 활성화해야 합니다. 그렇지 않으면 TFTP는 이전 캐시된 자체 서명 tomcat 인증서를 계속 제공하게 됩니다.

다음에 할 작업

인증서를 다시 생성한 후 최신 백업이 다시 생성된 인증서를 포함하도록 시스템 백업을 수행해야 합니다. 백업에 다시 생성된 인증서가 포함되어 있지 않고 시스템 복원 작업을 수행하는 경우 전화기를 등록할 수 있도록 시스템에서 각 전화기를 수동으로 잠금 해제해야 합니다. 백업 작업 흐름, 96 페이지 참조

관련 항목

인증서 이름 및 설명, 149 페이지

인증서 이름 및 설명

다음 표에서는 다시 생성할 수 있는 시스템 보안 인증서 및 다시 시작해야 하는 관련 서비스에 대해 설명합니다. TFTP 인증서 다시 생성에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오.

표 *8:* 인증서 이름 및 설명

이름	설명	관련 서비스
tomcat tomcat-ECDSA	이 자체 서명 루트 인증서는 HTTPS 노드를 설치하는 동안 생성됩니다.	Tomcat 및 TFTP
ipsec	이 자체 서명 루트 인증서는 MGCP 및 H.323 게이트웨이와의 IPsec 연결을 설치하는 동안 생성됩니다.	Cisco 재난 복구 시스템(DRS) 로컬 및 Cisco DRF Master
CallManager	Cisco Unified Communications Manager를 설치하면 이 자체 서명 루트 인증서가 자동으로 설치됩니다. 이 인증서는 노드 이름과 전역 고유 ID(GUID)를 포함하여 노드 식별을 제공합니다.	CallManager, CAPF 및 CTI
CAPF	시스템은 Cisco 클라이언트 구성을 완료한 후 이 루트 인증서를 클러스터의 사용자 노드 또는 모든 노드에 복사합니다.	CallManager 및 CAPF
TVS	이것이 자체 서명 루트 인증서입니다.	TVS

OAuth 새로 고침 로그인을 위해 키 다시 생성

명령줄 인터페이스를 사용하여 암호화 키와 서명 키를 다시 생성하려면 이 절차를 사용합니다. Cisco Jabber가 Cisco Unified Communications Manager의 OAuth 인증을 위해 사용하는 암호화 키 또는 서명

키가 손상된 경우 이 작업을 완료합니다. 서명 키는 비대칭이고 RSA 기반인 반면 암호화 키는 대칭 키입니다.

참고

- 이 작업을 완료한 후 이러한 키를 사용하는 현재 액세스 및 새로 고침 토큰은 무효화됩니다.
- 최종 사용자에게 미치는 영향을 최소화하기 위해 근무 시간 이후에 이 작업을 수행하는 것이 좋습니다.
- 암호화 키는 아래의 CLI를 통해서만 다시 생성될 수 있지만 서명 키는 Cisco Unified OS 관리 GUI를 사용하여 다시 생성할 수도 있습니다. 보안 > 인증서 관리를 선택하고 **AUTHZ** 인증서를 선택한 다음, 다시 생성을 클릭합니다.

절차

단계 **1** Cisco Unified Communications Manager 노드에서 명령줄 인터페이스에 로그인합니다.

단계 **2** 암호화 키를 다시 생성하려면:

a) `set key regen authz encryption` 명령을 실행합니다.

b) `yes`를 입력합니다.

단계 **3** 서명 키를 다시 생성하려면:

a) `set key regen authz signing` 명령을 실행합니다.

b) `yes`를 입력합니다.

Cisco Unified Communications Manager 게시자 노드는 키를 다시 생성하고 새 키를 IM and Presence 서비스 노드를 포함한 모든 Cisco Unified Communications Manager 클러스터 노드에 복제합니다.

다음에 할 작업

모든 UC 클러스터에 새 키를 다시 생성하고 동기화해야 합니다.

- IM and Presence 중앙 클러스터—IM and Presence 중앙 집중식 배포가 있는 경우 IM and Presence 노드는 텔레포니의 개별 클러스터에서 실행됩니다. 이 경우 IM and Presence 서비스 중앙 클러스터의 Cisco Unified Communications Manager 게시자 노드에서 이 절차를 반복합니다.
- Cisco Expressway 또는 Cisco Unity Connection—이러한 클러스터에서도 키를 다시 생성합니다. 자세한 내용은 Cisco Expressway 및 Cisco Unity Connection 설명서를 참조하십시오.

인증서 또는 인증서 체인 업로드

시스템이 신뢰하도록 하려는 새 인증서 또는 인증서 체인을 업로드합니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.

단계 **3** 인증서 용도 드롭다운 목록에서 인증서 이름을 선택합니다.

단계 **4** 다음 단계 중 하나를 수행하여 업로드할 파일을 선택합니다.

- 파일 업로드 텍스트 상자에서 파일의 경로를 입력합니다.
- 찾아보기를 클릭하고 파일을 탐색한 다음 열기를 클릭합니다.

단계 **5** 서버에 파일을 업로드하려면 파일 업로드를 클릭합니다.

참고 인증서를 업로드 한 후 영향을 받는 서비스를 다시 시작합니다. 서버가 다시 켜지면 CCMAdmin 또는 CCMUser GUI에 액세스하여 새로 추가되어 사용 중인 인증서를 확인할 수 있습니다..

타사 인증 기관 인증서 관리

이 작업 흐름은 순서대로 각 단계를 참조하여 타사 인증 프로세스의 개요를 제공합니다. 이 시스템은 타사 인증 기관이 PKCS # 10 인증서 서명 요청(CSR)으로 발행하는 인증서를 지원합니다.

절차

	명령 또는 동작	목적
단계 **1**	인증서 서명 요청 생성, 152 페이지	공개 키, 조직 이름, 일반 이름, 지역 및 국가를 포함하여 인증서 애플리케이션 정보를 포함하는 암호화된 텍스트 블록인 인증서 서명 요청(CSR)을 생성합니다. 인증 기관은 이 CSR을 사용하여 시스템에 대한 신뢰할 수 있는 인증서를 생성합니다.
단계 **2**	CSR(Certificate Signing Request) 다운로드, 152 페이지	인증 기관에 제출할 준비가 되도록 컴퓨터로 CSR을 다운로드합니다.
단계 **3**	인증 기관 설명서를 참조하십시오.	인증 기관에서 애플리케이션 인증서를 가져옵니다.
단계 **4**	인증 기관 설명서를 참조하십시오.	인증 기관에서 루트 인증서를 가져옵니다.
단계 **5**	인증 기관 서명 CAPF 루트 인증서를 신뢰 저장소에 추가, 153 페이지	루트 인증서를 신뢰 저장소에 추가합니다. 인증 기관에서 서명한 CAPF 인증서를 사용할 때는 이 단계를 수행합니다.

	명령 또는 동작	목적
단계 **6**	인증서 또는 인증서 체인 업로드, 150 페이지	노드에 인증 기관 루트 인증서를 업로드합니다.
단계 **7**	CAPF 또는 Cisco Unified Communications Manager용 인증서를 업데이트한 경우 새 CTL 파일을 생성합니다.	http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오. 타사에서 서명한 CAPF 또는 CallManager 인증서를 업로드한 후에 CTL 클라이언트(구성된 경우)를 다시 실행합니다.
단계 **8**	서비스 다시 시작, 153 페이지	새 인증서의 영향을 받는 서비스를 다시 시작합니다. 모든 인증서 유형에 대해 해당 서비스를 다시 시작합니다(예를 들어, Tomcat 또는 Tomcat-ECDSA 인증서를 업데이트한 경우 Cisco Tomcat 서비스를 다시 시작).

인증서 서명 요청 생성

공개 키, 조직 이름, 일반 이름, 지역 및 국가를 포함하여 인증서 애플리케이션 정보를 포함하는 암호화된 텍스트 블록인 인증서 서명 요청(CSR)을 생성합니다. 인증 기관은 이 CSR을 사용하여 시스템에 대한 신뢰할 수 있는 인증서를 생성합니다.

참고 새 CSR을 생성하는 경우 기존 CSR을 덮어씁니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** **CSR** 생성을 클릭합니다.

단계 **3** 인증서 서명 요청 생성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** **CSR** 생성을 클릭합니다.

CSR(Certificate Signing Request) 다운로드

인증 기관에 제출할 준비가 되도록 컴퓨터로 CSR을 다운로드합니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** **CSR** 다운로드를 클릭합니다.

단계 **3** 인증서 용도 드롭다운 목록에서 인증서 이름을 선택합니다.

단계 **4** **CSR** 다운로드를 클릭합니다.

단계 **5** (선택 사항) 프롬프트가 표시되면 저장을 클릭합니다.

인증 기관 서명 **CAPF** 루트 인증서를 신뢰 저장소에 추가

인증 기관에서 서명한 CAPF 인증서를 사용할 때 CallManager 신뢰 저장소에 루트 인증서를 추가하려면 다음 단계를 수행합니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.

단계 **3** 인증서/인증서 체인 업로드 팝업 창의 인증서 용도 드롭다운 목록에서 **CallManager-trust**를 선택하고 인증 기관에서 서명한 CAPF 루트 인증서로 이동합니다.

단계 **4** 파일 업로드 필드에 인증서가 나타나면 업로드를 클릭합니다.

서비스 다시 시작

시스템이 클러스터의 특정 노드에서 기능 또는 네트워크 서비스를 다시 시작해야 하는 경우 이 절차를 사용합니다.

절차

단계 **1** 다시 시작하는 서비스 유형에 따라 다음 작업 중 하나를 수행합니다.

- 도구 > 제어 센터 **-** 기능 서비스를 선택합니다.
- 도구 > 제어 센터 **-** 네트워크 서비스를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 시스템 노드를 선택하고 이동을 클릭합니다.

단계 **3** 다시 시작할 서비스 옆의 라디오 버튼을 클릭하고 다시 시작을 클릭합니다.

단계 **4** 다시 시작하는 데 약간 시간이 걸린다는 메시지가 표시되면 확인을 클릭합니다.

인증서 만료 모니터링

인증서 만료 날짜가 다가오면 시스템이 이메일 메시지를 자동으로 전송하도록 구성하려면 이 절차를 사용합니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 모니터링을 선택합니다.

단계 **2** 알림 시작 시간에 숫자 값을 입력합니다. 이 값은 이메일을 통해 알림을 받기 전의 남은 일 수입니다.

단계 **3** 알림 빈도에 숫자 값을 입력하고 일 또는 시간을 선택합니다.

단계 **4** (선택 사항) 이메일 알림 활성화를 선택한 다음, 이메일 **ID** 필드에 이메일 주소를 입력합니다.

단계 **5** 저장을 클릭합니다.

참고 인증서 모니터 서비스는 기본적으로 12시간 마다 실행됩니다. 인증서 모니터 서비스를 다시 시작하면 서비스를 시작한 다음 12시간 후에만 실행되도록 다시 일정을 계산합니다. 간격은 인증서가 만료일 7일 전까지도 변경되지 않습니다. 인증서가 만료되었거나 만료 1일 전이 되면 1시간 마다 실행됩니다.

온라인 인증서 상태 프로토콜 구성

온라인 인증서 상태 프로토콜(OCSP)을 사용하여 인증서의 해지 상태를 얻습니다.

참고 인증서 해지 상태 확인은 인증서 또는 인증서 체인 업로드 중에만 수행됩니다. 인증서가 해지되는 경우 해당 알람이 발생합니다.

시작하기 전에

주의 OSCP를 활성화하기 전에 OCSP Responder 인증서를 tomcat-trust로 업로드해야 합니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 해지를 선택합니다.

단계 **2** **OCSP** 활성화 확인란을 선택하고 다음 작업 중 하나를 수행합니다.

- 외부 또는 구성된 URI를 OCSP Responder에 연락하는 데 사용되는 경우 구성된 **OCSP URI** 사용을 선택합니다. **OCSP** 구성된 **URI** 필드에 인증서 해지 상태가 확인되는 OCSP Responder의 URI를 입력합니다.
- 인증서가 OCSP Responder에 연락하는 데 사용될 OCSP URI로 구성된 경우 인증서에서 **OCSP URI** 사용을 선택합니다.

단계 **3** 해지 확인 활성화 확인란을 선택하여 해지 확인을 수행합니다.

참고 해지 및 만료 확인 엔터프라이즈 매개 변수가 활성화됨으로 설정되면 LDAP 및 IPsec에 대한 인증서 해지 서비스가 활성화됩니다.

단계 **4** 항상 확인 값을 입력하여 인증서 해지 상태 확인의 빈도를 구성합니다.

a) 시간 또는 일을 클릭하여 시간별 또는 일별 해지 상태를 확인합니다.

단계 **5** 저장을 클릭합니다.

인증서 오류 문제 해결

IM and Presence 서비스 노드의 Cisco Unified Communications Manager 서비스 또는 Cisco Unified Communications Manager 노드의 IM and Presence 서비스 기능에 액세스하려 할 때 오류가 발생하는 경우 문제의 원인은 tomcat-trust 인증서입니다. 오류 메시지 서버에 연결할 수 없습니다(원격 노드에 연결할 수 없음)이 다음 서비스 가용성 인터페이스 창에 나타납니다.

- 서비스 활성화
- 제어 센터 - 기능 서비스
- 제어 센터 - 네트워크 서비스

이 절차를 사용하여 인증서 오류를 해결합니다. 첫 단계부터 시작하고 필요한 경우 계속 진행합니다. 경우에 따라 첫 단계만 완료해도 오류를 해결할 수 있으며 기타의 경우 모든 단계를 완료해야 합니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택하여 필수 tomcat-trust 인증서가 있는지 확인합니다.
필수 인증서가 없는 경우 30분 기다렸다가 다시 확인합니다.

단계 **2** 해당 정보를 보려는 인증서를 선택합니다. 콘텐츠가 원격 노드에 있는 해당 인증서와 일치하는지 확인합니다.

단계 **3** CLI에서 Cisco 클러스터 간 동기화 에이전트 서비스를 다시 시작합니다. **utils service restart Cisco Intercluster Sync Agent**.

단계 **4** Cisco 클러스터 간 동기화 에이전트 서비스가 다시 시작되면 Cisco Tomcat 서비스를 다시 시작합니다. **utils service restart Cisco Tomcat**.

단계 **5** 30분이 소요됩니다. 이전 단계로 인증서 오류가 해결되지 않고 tomcat-trust 인증서가 있는 경우 인증서를 삭제합니다. 인증서를 삭제한 후 각 노드에 대한 Tomcat 및 Tomcat-ECDSA 인증서를 다운로드하고 피어에 tomcat-trust 인증서로 업로드하여 수동으로 교환해야 합니다.

단계 **6** 인증서 교환이 완료된 후 각 영향을 받는 서버에서 Cisco Tomcat을 다시 시작합니다. **utils service restart Cisco Tomcat**.

17 장

벌크 인증서 관리

벌크 인증서 관리

클러스터 간에 인증서 집합을 공유하는 경우 벌크 인증서 관리를 사용합니다. 이 단계는 클러스터 간 내선 이동 같이 클러스터 간에 신뢰를 설정해야 하는 시스템 기능에 필요합니다.

절차

	명령 또는 동작	목적
단계 **1**	인증서 내보내기, 157 페이지	이 절차에서는 클러스터의 모든 노드에 대한 인증서를 포함하는 PKCS12 파일을 만듭니다. 참고 • 모든 참여 클러스터는 인증서를 동일한 SFTP 서버 및 SFTP 디렉터리로 내보내야 합니다. • Tomcat, Tomcat-ECDSA, TFTP 또는 CAPF 인증서가 클러스터 노드에서 다시 생성될 때마다 클러스터에서 인증서를 내보내야 합니다.
단계 **2**	인증서 가져오기, 158 페이지	홈 및 원격 (방문) 클러스터로 인증서를 다시 가져옵니다. 참고 업그레이드 후에도 이러한 인증서는 보존됩니다. 사용자가 인증서를 다시 가져오거나 다시 통합하지 않아도 됩니다.

인증서 내보내기

이 절차에서는 클러스터의 모든 노드에 대한 인증서를 포함하는 PKCS12 파일을 만듭니다.

참고

- 모든 참여 클러스터는 인증서를 동일한 SFTP 서버 및 SFTP 디렉터리로 내보내야 합니다.
- Tomcat, Tomcat-ECDSA, TFTP 또는 CAPF 인증서가 클러스터 노드에서 다시 생성될 때마다 클러스터에서 인증서를 내보내야 합니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 벌크 인증서 관리를 선택합니다.

단계 **2** 홈 및 원격 클러스터에서 연결할 수 있는 TFTP 서버에 대한 설정을 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 온라인 도움말을 참조하십시오.

단계 **3** 저장을 클릭합니다.

단계 **4** 내보내기를 클릭합니다.

단계 **5** 벌크 인증서 내보내기 창에서 인증서 종류 필드에 대해 모두를 선택합니다.

단계 **6** 내보내기를 클릭합니다.

단계 **7** 닫기를 클릭합니다.

인증서 가져오기

홈 및 원격 (방문) 클러스터로 인증서를 다시 가져옵니다.

참고 업그레이드 후에도 이러한 인증서는 보존됩니다. 사용자가 인증서를 다시 가져오거나 다시 통합하지 않아도 됩니다.

참고 벌크 인증서 관리를 사용하여 인증서를 가져오면 전화기가 재설정됩니다.

시작하기 전에

가져오기 단추가 표시되기 전에 다음과 같은 작업을 완료해야 합니다.

- 둘 이상의 클러스터에서 SFTP 서버로 인증서를 내보냅니다.
- 내보낸 인증서를 통합합니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > 벌크 인증서 관리 > 가져오기 > 벌크 인증서 가져오기를 선택합니다.

단계 **2** 인증서 유형 드롭다운 목록에서 모두를 선택합니다.

단계 **3** 가져오기를 선택합니다.

18 장

IPSec 정책 관리

IPsec 정책 개요

IPsec은 암호화 보안 서비스를 사용하여 IP 네트워크를 통해 개인 보안 통신을 보장하는 프레임워크입니다. IPsec 정책은 IPsec 보안 서비스를 구성하는 데 사용됩니다. 정책은 네트워크에서 대부분의 트래픽 유형을 위해 다양한 수준의 보호를 제공합니다. 컴퓨터, OU(조직 단위), 도메인, 사이트 또는 글로벌 엔터프라이즈의 보안 요구 사항을 충족하도록 IPsec 정책을 구성할 수 있습니다.

IPsec 정책 구성

참고

- 시스템 업그레이드 중 IPsec 정책에 적용되는 변경 사항은 손실되므로 업그레이드하는 동안 IPsec 정책을 수정 또는 생성하지 마십시오.
- IPsec은 양방향 프로비저닝 또는 각 호스트(또는 게이트웨이)에 대해 하나의 피어가 필요합니다.
- 한 IPsec 정책 프로토콜이 “ANY”로 설정되고 다른 두 IPsec 정책 프로토콜이 “UDP” 또는 “TCP”로 설정된 두 Cisco Unified Communications Manager 노드에서 IPsec 정책을 프로비저닝할 때 “ANY” 프로토콜을 사용하는 노드에서 실행할 경우 유효성 검사 결과는 거짓 부정이 될 수 있습니다.
- 특히 암호화를 사용하면 IPsec은 시스템 성능에 영향을 미칩니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > **IPSec** 구성을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** **IPSec** 정책 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

단계 **5** (선택 사항) IPsec를 확인하려면 서비스 > **Ping**을 선택하고 **IPsec** 확인 확인란을 선택한 다음 **Ping**을 클릭합니다.

IPsec 정책 관리

시스템 업그레이드 중 IPsec 정책에 적용되는 변경 사항은 손실되므로 업그레이드하는 동안 IPsec 정책을 수정 또는 생성하지 마십시오.

주의 인증서 이름, 도메인 또는 IP 주소 변경으로 인해 기존 IPsec 인증서가 변경되면 IPsec 정책을 삭제하고 다시 생성해야 합니다. 인증서 이름이 변경되지 않은 경우 원격 노드의 재생성된 인증서를 가져온 후 IPsec 정책을 비활성화하고 활성화해야 합니다.

절차

단계 **1** Cisco Unified OS 관리에서 보안 > **IPSEC** 구성을 선택합니다.

단계 **2** 정책을 표시, 활성화 또는 비활성화하려면 다음 단계를 수행합니다.

a) 정책 이름을 클릭합니다.

b) 정책을 활성화 또는 비활성화하려면 정책 활성화 확인란을 선택하거나 선택 취소합니다.

c) 저장을 클릭합니다.

단계 **3** 하나 이상의 정책을 삭제하려면 다음 단계를 수행합니다.

a) 삭제할 각 정책 옆의 확인란을 선택합니다.
모든 정책을 선택하려면 모두 선택을 클릭하고, 모든 확인란을 지우려면 모두 지우기를 클릭하면 됩니다.

b) 선택한 항목 삭제를 클릭합니다.

19 장

인증 정책 관리

인증 정책 및 인증

인증 기능은 사용자를 인증하고 인증서 정보를 업데이트하고 사용자 이벤트와 오류를 추적하고 기록하며 인증서 변경 내역을 기록하고 데이터 저장소에 대한 사용자 인증서를 암호화 또는 해독합니다.

시스템은 항상 Cisco Unified Communications Manager 데이터베이스에 대해 애플리케이션 사용자 암호 및 최종 사용자 PIN을 인증합니다. 시스템은 회사 디렉터리 또는 데이터베이스에 대해 최종 사용자 암호를 인증할 수 있습니다.

시스템이 회사 디렉터리와 동기화되는 경우 Cisco Unified Communications Manager 또는 LDAP(Lightweight Directory Access Protocol)의 인증 기능이 암호를 인증할 수 있습니다.

- LDAP 인증이 활성화된 경우 사용자 암호 및 인증 정책이 적용되지 않습니다. 이러한 기본값은 디렉터리 동기화(DirSync 서비스)로 생성된 사용자에게 적용됩니다.
- LDAP 인증이 비활성화되면 시스템이 데이터베이스에 대한 사용자 인증서를 인증합니다. 이 옵션을 사용하여 인증 정책을 할당하고 인증 이벤트를 관리하고 암호를 관리할 수 있습니다. 최종 사용자는 전화기 사용자 인터페이스를 통해 암호 및 PIN을 변경할 수 있습니다.

인증 정책은 운영 체제 사용자 또는 CLI 사용자에게 적용되지 않습니다. 이러한 관리자는 운영 체제에서 지원하는 표준 암호 확인 절차를 사용합니다.

사용자가 데이터베이스에 구성된 후 시스템은 데이터베이스에 사용자 인증서의 기록을 저장하여 사용자가 자신의 인증서를 변경하라는 메시지가 표시될 때 이전 정보를 입력하지 못하도록 합니다.

인증 정책에 대한 JTAPI 및 TAPI 지원

Cisco Unified Communications Manager Java 텔레포니 애플리케이션 프로그래밍 인터페이스(JTAPI) 및 텔레포니 애플리케이션 프로그래밍 인터페이스(TAPI)는 애플리케이션 사용자에게 할당된 인증 정책을 지원하므로 개발자는 인증 정책 시행을 위한 암호 만료, PIN 만료 및 인증 정책 반환 코드에 응답하는 애플리케이션을 만들어야 합니다.

애플리케이션은 애플리케이션이 사용하는 인증 모델에 관계 없이 API를 사용하여 데이터베이스 또는 회사 디렉터리를 인증합니다.

개발자를 위한 TAPI 및 JTAPI에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html의 개발자 설명서를 참조하십시오.

인증서 정책 구성

인증 정책은 애플리케이션 사용자 및 최종 사용자에 적용됩니다. 최종 사용자 및 애플리케이션 사용자에게 암호 정책을, 최종 사용자에게 PIN 정책을 할당합니다. 인증 정책 기본값 구성에는 이러한 그룹에 대한 정책 할당이 나열되어 있습니다. 새 사용자를 데이터베이스에 추가하면 기본 정책이 할당됩니다. 할당된 정책을 변경하고 사용자 인증 이벤트를 관리할 수 있습니다.

절차

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 인증서 정책을 선택합니다.

단계 **2** 다음 단계 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 인증서 정책을 선택합니다.
- 새로 추가를 클릭하여 새 인증서 정책을 생성합니다.

단계 **3** 인증서 정책 구성 창에서 필드를 완료합니다. 필드 및 해당 구성 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

인증 정책 기본값 구성

설치 시 Cisco Unified Communications Manager는 사용자 그룹에 정적 기본 인증 정책을 할당합니다. 기본 인증서를 제공하지는 않습니다. 시스템은 새 기본 정책을 할당하고 사용자에 대한 새 기본 인증서 및 인증서 요구 사항을 구성하는 옵션을 제공합니다.

절차

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 인증 정책 기본값을 선택합니다.

단계 **2** 인증 정책 드롭다운 목록 상자에서 이 그룹에 대한 인증 정책을 선택합니다.

단계 **3** 인증서 변경 및 인증서 확인 구성 창에 암호를 입력합니다.

단계 **4** 사용자가 이 인증서를 변경하는 것을 원하지 않을 경우 사용자가 변경할 수 없음 확인란을 선택합니다.

단계 **5** 최종 사용자가 다음에 로그인할 때 변경해야 하는 임시 인증서로 이 인증서를 사용하려는 경우 다음 로그인할 때 반드시 변경 확인란을 선택합니다.

단계 **6** 인증서가 만료되지 않도록 하려면 만료되지 않음 확인란을 선택합니다.

단계 **7** 저장을 클릭합니다.

인증 활동 모니터링

시스템은 마지막 hack 시도 시간 같은 최근 인증 결과를 표시하고 실패한 로그온 시도 횟수를 계산합니다.

시스템은 다음과 같은 인증 정책 이벤트에 대한 로그 파일 항목을 생성합니다.

- 인증 성공
- 인증 실패 (잘못된 암호 또는 알 수 없음)
- 다음 이유로 인증 실패
  - 관리 잠금
  - Hack 잠금(실패한 로그온 잠금)
  - 만료된 소프트 잠금(만료된 인증서)
  - 비활성 잠금(일정 시간 동안 인증서가 사용되지 않음)
  - 사용자를 변경해야 함(사용자에게 설정된 인증서를 변경해야 함)
  - LDAP 비활성(LDAP 인증으로 전환 및 LDAP가 비활성)
- 사용자 인증서 업데이트 성공
- 사용자 인증서 업데이트 실패

참고 최종 사용자 암호에 LDAP 인증을 사용할 경우 LDAP는 인증 성공 및 실패만 추적합니다.

모든 이벤트 메시지에는 문자열 “ims-auth” 및 인증을 시도하는 사용자 ID가 포함됩니다.

절차

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 최종 사용자를 선택합니다.

단계 **2** 검색 조건을 입력하고 찾기를 클릭한 다음, 결과 목록에서 사용자를 선택합니다.

단계 **3** 인증서 편집을 클릭하여 사용자의 인증 활동을 확인합니다.

다음에 할 작업

Cisco Unified Real-Time Monitoring Tool(Unified RTMT)로 로그 파일을 볼 수 있습니다. 또한 보고서에 캡처된 이벤트를 수집할 수 있습니다. Unified RTMT를 사용하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html의 *Cisco Unified Real-Time Monitoring Tool* 관리 설명서를 참조하십시오.

인증서 캐시 구성

인증서 캐싱을 활성화하여 시스템 효율성을 높입니다. 시스템은 모든 단일 로그인 요청에 대해 데이터베이스 조회를 수행하거나 저장된 프로시저를 호출할 필요가 없습니다. 관련된 인증 정책은 캐싱 기간이 만료될 때까지 적용되지 않습니다.

이 설정은 사용자 인증을 호출하는 모든 Java 애플리케이션에 적용됩니다.

절차

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 필요에 따라 다음 작업을 수행합니다.

- 캐싱 활성화 엔터프라이즈 매개 변수를 **True**로 설정합니다. 이 매개 변수를 활성화한 상태에서 Cisco Unified Communications Manager는 최대 2분 동안 캐시된 인증서를 사용합니다.
- 캐싱 활성화 엔터프라이즈 매개 변수를 **False**로 설정하여 캐싱을 비활성화하면 시스템이 캐시된 인증서를 인증에 사용하지 않습니다. 시스템은 LDAP 인증에서 이 설정을 무시합니다. 인증서 캐싱을 사용하려면 사용자당 최소 추가 메모리가 필요합니다.

단계 **3** 저장을 클릭합니다.