사용자 액세스 관리

사용자 액세스 개요

다음 항목을 구성하여 Cisco Unified Communications Manager에 대한 사용자 액세스를 관리합니다.

- 액세스 제어 그룹
- 역할
- 사용자 순위

액세스 제어 그룹 개요

액세스 제어 그룹은 사용자 및 해당 사용자에게 할당된 역할의 목록입니다. 최종 사용자, 애플리케이션 사용자 또는 관리자 사용자를 액세스 제어 그룹에 할당할 때 사용자는 해당 그룹에 연결된 역할의 액세스 권한을 얻게 됩니다. 필요한 역할과 권한만 있는 액세스 제어 그룹에 비슷한 액세스 요구 사항을 가진 사용자를 할당하여 시스템 액세스를 관리할 수 있습니다.

액세스 제어 그룹에는 다음 두 가지 유형이 있습니다.

- 표준 액세스 제어 그룹 - 일반 배포 요구 사항을 충족하는 역할 할당을 사용하는 미리 정의된 기본 그룹입니다. 표준 그룹에서는 역할 할당을 편집할 수 없습니다. 그러나 사용자를 추가하고 삭제하는 것은 물론 사용자 순위 요구 사항도 편집할 수 있습니다 . 표준 액세스 제어 그룹 목록과 관련 역할에 대한 자세한 내용은 표준 역할 및 액세스 제어 그룹, 16 페이지의 내용을 참조하십시오.

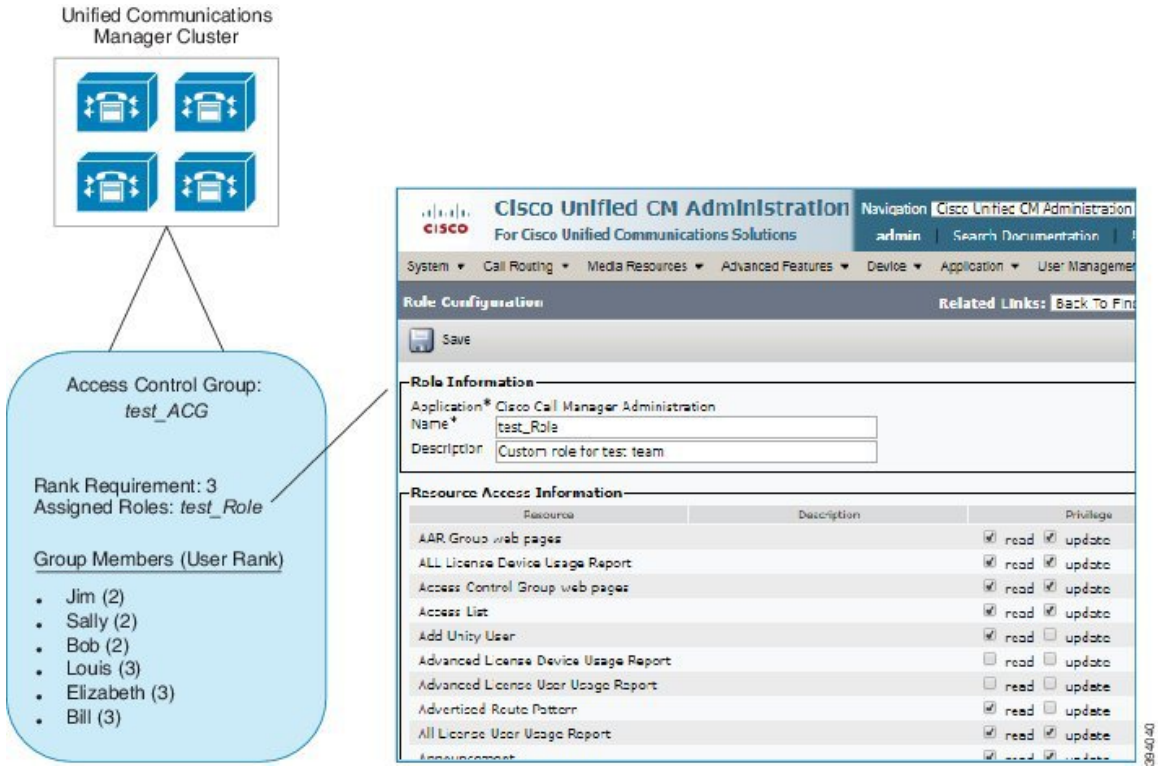
- 사용자 정의 액세스 제어 그룹 - 사용자의 요구에 맞는 역할 권한을 포함하는 표준 그룹이 없는 경우 고유한 액세스 제어 그룹을 생성합니다.

사용자 순위 프레임워크는 사용자에 게 할당할 수 있는 액세스 제어 그룹에 대한 제어 세트를 제공합니다. 액세스 제어 그룹에 할당하려면 사용자가 해당 그룹의 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. 최소 순위가 1인 그룹에는 할당할 수 없습니다.

예 - 액세스 제어 그룹을 포함한 역할 권한

다음 예는 테스트 팀의 구성원이 액세스 제어 그룹 **test_ACG**에 할당된 클러스터를 보여줍니다. 오른쪽의 화면 캡처에는 액세스 제어 그룹에 연결된 역할인 test_Role의 액세스 설정이 표시됩니다. 또한 액세스 제어 그룹의 최소 순위 요구 사항은 3입니다. 그룹에 참가할 수 있으려면 모든 그룹 구성원이 1-3 사이의 순위를 가져야 합니다.

그림 ***1:*** 액세스 제어 그룹을 포함한 역할 권한



역할 개요

사용자는 사용자가 구성원인 액세스 제어 그룹에 연결된 역할을 통해 시스템 액세스 권한을 얻습니다. 각 역할에는 특정 리소스나 애플리케이션(예: Cisco Unified CM 관리 또는 CDR 분석 및 보고)에 연결 된 권한 집합이 포함되어 있습니다. Cisco Unified CM 관리 같은 애플리케이션에의 경우 할에는 애플리케이션의 특정 GUI 페이지를 보거나 편집할 수 있는 권한이 포함될 수 있습니다. 리소스 또는 애플리케이션에 할당할 수 있는 권한 수준에는 다음 세 가지가 있습니다.

- 읽기 - 사용자가 리소스에 대한 설정을 볼 수 있습니다.
- 업데이트 — 사용자가 리소스에 대한 설정을 편집할 수 있습니다.
- 액세스 없음 - 사용자가 읽기 또는 업데이트 액세스 권한이 없는 경우에는 사용자가 지정된 리소스에 대한 설정을 보거나 편집할 수 없습니다.

역할 유형

사용자를 프로비저닝하는 경우 적용할 역할을 결정한 다음, 역할을 포함하는 액세스 제어 그룹에 사용자를 할당해야 합니다. Cisco Unified Communications Manager에는 두 가지 기본 역할 유형이 있습니다.

- 표준 역할 — 일반 배포의 요구 사항을 충족하도록 설계된 사전 설치된 기본 역할입니다. 표준 역할에 대한 권한은 편집할 수 없습니다.
- 사용자 정의 역할 — 표준 역할에 필요한 권한이 없을 때 사용자 정의 역할을 만듭니다. 또한 보다 세부적인 수준의 액세스 제어가 필요한 경우에는 고급 설정을 적용하여 관리자가 키 사용자 설정을 편집하는 기능을 제어할 수 있습니다. (자세한 내용은 아래 섹션을 참조하십시오.)

고급 역할 설정

사용자 정의 역할을 생성할 때 애플리케이션 사용자 구성 및 최종 사용자 구성 창에서 선택한 필드에 상세 제어 수준을 추가할 수 있습니다.

고급 역할 구성 창에서는 다음과 같은 작업에 대한 액세스를 제한하면서 Cisco Unified CM 관리에 대한 액세스를 구성할 수 있습니다.

- 사용자 추가
- 암호 편집
- 사용자 순위 편집
- 액세스 제어 그룹 편집

다음 표에는 이 구성으로 적용 할 수 있는 추가 컨트롤이 자세히 나와 있습니다.

표 *1:* 고급 리소스 액세스 정보

고급 리소스	액세스 제어
권한 정보	액세스 제어 그룹 추가 또는 편집 기능 제어: • 보기 - 사용자는 액세스 제어 그룹을 볼 수는 있지만 액세스 제어 그룹을 추가, 편집 또는 삭제할 수는 없습니다. • 업데이트 - 사용자는 액세스 제어 그룹을 추가, 편집 또는 삭제할 수 있습니다. 참고 두 값을 모두 선택하지 않으면 권한 정보섹션을 사용할 수 없습니다. 참고 보기를 선택하면 사용자가 자신의 사용자에 대한 권한 정보를 업데이트할 수 있음 필드가 아니요로 설정되고 비활성화됩니다. 이 필드를 편집할 수 있게 하려면 권한 정보 필드를 업데이트로 설정해야 합니다.
사용자는 자신의 사용자에 대한 권한 정보를 업데이트할 수 있음	사용자가 자신의 액세스 권한을 편집하는 기능을 제어: • 예 - 사용자가 자신의 권한 정보를 업데이트할 수 있습니다. • 아니요 - 사용자가 자신의 권한 정보를 업데이트할 수 없습니다. 그러나 사용자는 동일하거나 더 낮은 사용자에 대한 권한 정보를 보거나 수정할 수 있습니다. 참고 권한 정보 업데이트 확인란을 선택하지 않은 경우 사용자가 자신의 사용자에 대한 권한 정보를 업데이트할 수 있음 필드는 아니요로 설정되고 비활성화됩니다.
사용자 순위	사용자 순위를 변경하는 기능을 제어합니다. • 보기 - 사용자는 사용자 등급을 볼 수는 있지만 사용자 등급은 변경할 수 없습니다. • 업데이트 - 사용자는 사용자 순위를 변경할 수 있습니다. 참고 두 값을 모두 선택하지 않으면 사용자 순위 섹션을 사용할 수 없습니다. 참고 보기를 선택하면 사용자가 자신의 사용자에 대한 사용자 순위를 업데이트할 수 있음 필드가 아니요로 설정되고 비활성화됩니다. 이 필드를 편집할 수 있게 하려면 사용자 순위 필드를 업데이트로 설정해야 합니다.

고급 리소스	액세스 제어
사용자가 자신의 사용자에 대한 사용자 순위를 업데이트할 수 있음	사용자가 자신의 사용자 순위를 편집하는 기능을 제어: • 예 - 사용자가 자신의 사용자 순위를 업데이트할 수 있습니다. • 아니요 - 사용자가 자신의 사용자 순위를 업데이트할 수 없습니다. 그러나 사용자는 동일하거나 더 낮은 사용자에 대한 사용자 순위를 보거나 수정할 수 있습니다. 참고 사용자 순위 업데이트 확인란을 선택하지 않은 경우 사용자가 자신의 사용자에 대한 사용자 순위를 업데이트할 수 있음 필드는 아니요로 설정되고 비활성화됩니다.
새 사용자 추가	새 사용자를 추가하는 기능을 제어합니다. • 예 - 새 사용자를 추가할 수 있습니다. • 아니요 - 새로 추가 버튼을 사용할 수 없습니다.
암호	암호를 변경하는 기능을 제어합니다. • 예 - 애플리케이션 사용자 정보 섹션 아래에서 사용자 암호를 변경할 수 있습니다. • 아니요 - 애플리케이션 사용자 정보 섹션 아래에서 암호 및 암호 확인을 사용할 수 없습니다.

사용자 순위 개요

사용자 순위 계층은 최종 사용자 또는 애플리케이션 사용자에게 관리자가 할당할 수 있는 제어 그룹에 액세스하는 제어 집합을 제공합니다.

최종 사용자 또는 애플리케이션 사용자를 프로비저닝할 때 관리자는 사용자에 대한 사용자 순위를 할당할 수 있습니다. 또한 관리자는 각 액세스 제어 그룹에 사용자 순위 요구 사항을 할당할 수 있습니다. 사용자를 추가하여 제어 그룹에 액세스하는 경우 관리자는 사용자의 사용자 순위가 그룹의 순위 요구 사항을 충족하는 그룹에만 사용자를 할당할 수 있습니다. 예를 들어, 관리자는 사용자 순위가 3인 사용자를 사용자 순위 요구 사항이 3에서 10 사이인 액세스 제어 그룹에 할당할 수 있습니다. 그러나 관리자는 사용자 순위 요구 사항이 1 또는 2인 액세스 제어 그룹에 해당 사용자를 할당할 수 없습니다.

관리자는 사용자 순위 구성 창 내에서 고유한 사용자 순위 계층 구조를 생성할 수 있으며 사용자 및 액세스 제어 그룹을 프로비저닝할 때 해당 계층 구조를 사용할 수 있습니다. 사용자 순위 계층 구조를 구성하지 않거나 사용자 또는 액세스 제어 그룹을 프로비저닝할 때 사용자 순위 설정을 지정하지 않을 경우 모든 사용자 및 액세스 제어 그룹에는 기본 사용자 순위 1(가능한 가장 높은 순위)이 할당됩니다.

사용자 액세스 필수 구성 요소

사용자의 요구 사항을 검토하여 사용자에 게 필요한 액세스 수준을 확인하십시오. 사용자에게 필요한 액세스 권한을 가지는 역할을 할당하려고 하지만 액세스할 수 없는 시스템의 경우 액세스를 제공하지 않습니다.

새 역할 및 액세스 제어 그룹을 생성하기 전에 표준 역할 및 액세스 제어 그룹 목록을 검토하여 기존 액세스 제어 그룹에 필요한 역할 및 액세스 권한이 있는지 확인합니다. 자세한 내용은 표준 역할 및 액세스 제어 그룹, 16 페이지를 참조하십시오.

사용자 액세스 구성 작업 흐름

사용자 액세스를 구성하려면 다음 작업을 완료합니다.

시작하기 전에

기본 역할 및 액세스 제어 그룹을 사용하려는 경우 사용자 정의된 역할 및 액세스 제어 그룹을 만들기 위한 작업을 건너뛸 수 있습니다. 사용자를 기존 기본 액세스 제어 그룹에 할당할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	사용자 순위 계층 구조 구성, 7 페이지	사용자 순위 계층을 설정합니다. 이 작업을 건너뛰는 경우 모든 사용자 및 액세스 제어 그룹에 기본 사용자 순위인 1(최고 순위)이 할당됩니다.
단계 **2**	사용자 지정 역할 만들기, 7 페이지	기본 역할에 필요한 액세스 권한이 없는 경우 사용자 정의 역할을 만듭니다.
단계 **3**	관리자를 위한 고급 역할 구성, 8 페이지	(선택 사항) 사용자 정의 역할에서 고급 권한을 사용하면 관리자가 키 사용자 설정을 편집할 수 있는 기능을 제어할 수 있습니다.
단계 **4**	액세스 제어 그룹 만들기, 9 페이지	기본 그룹에 필요한 역할 할당이 없는 경우 사용자 정의 액세스 제어 그룹을 만듭니다.
단계 **5**	액세스 제어 그룹에 사용자 할당, 9 페이지	표준 또는 사용자 정의 액세스 제어 그룹에서 사용자를 추가하거나 삭제합니다.
단계 **6**	액세스 제어 그룹에 대한 권한 정책 중복 구성, 10 페이지	(선택 사항) 이 설정은 충돌하는 권한이 있는 여러 액세스 제어 그룹에 사용자가 할당된 경우에 사용됩니다.

사용자 순위 계층 구조 구성

이 절차를 사용하여 사용자 정의 사용자 순위 계층 구조를 만듭니다.

참고 사용자 순위 계층 구조를 구성하지 않으면 기본적으로 모든 사용자 및 액세스 제어 그룹에 사용자 순위 1(가능한 가장 높은 순위)이 할당됩니다.

프로시저

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.

단계 **6** 이 절차를 반복하여 추가 사용자 순위를 추가합니다.
사용자 순위를 사용자 및 액세스 제어 그룹에 할당하여 사용자에게 할당할 수 있는 그룹을 제어할 수 있습니다.

사용자 지정 역할 만들기

이 절차를 사용하여 사용자 정의된 권한이 있는 새 역할을 만듭니다. 정확히 필요한 권한이 있는 표준 역할이 없는 경우 이 작업을 수행할 수 있습니다. 역할을 만드는 방법은 두 가지가 있습니다.

- 새로 추가 버튼을 사용하여 처음부터 새 역할을 만들고 구성합니다.
- 기존 역할이 필요한 권한과 비슷한 액세스 권한을 가지는 경우 복사 버튼을 사용합니다. 기존 역할의 권한을 편집 가능한 새 역할에 복사할 수 있습니다.

프로시저

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

단계 **2** 다음 중 하나를 수행합니다.

- 새 역할을 만들려면 새로 추가를 클릭합니다. 이 역할이 연결되는 애플리케이션을 선택하고 다음을 클릭합니다 .
- 기존 역할에서 설정을 복사하려면 찾기를 클릭하고 기존 역할을 엽니다. 복사를 클릭하고 새 역할의 이름을 입력합니다. 확인을 클릭합니다.

단계 **3** 역할에 대한 이름 및 설명을 입력합니다.

단계 **4** 각 리소스에 대해 다음을 적용하는 상자를 선택합니다.

- 사용자가 리소스에 대한 설정을 볼 수 있게 하려면 읽기 확인란을 선택합니다.
- 사용자가 리소스의 설정을 편집할 수 있게 하려면 업데이트 확인란을 선택합니다.
- 리소스에 대한 액세스를 제공하지 않으려면 두 확인란을 선택하지 않은 상태로 둡니다.

단계 **5** 모두에게 액세스 부여**{** 또는 모두에게 액세스 거부 버튼을 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 버튼을 사용해야 합니다.

단계 **6** 저장을 클릭합니다.

관리자를 위한 고급 역할 구성

고급 역할 구성을 사용하면 보다 세분화된 수준에서 사용자 지정 역할에 대한 권한을 편집할 수 있습니다. 최종 사용자 구성 및 애플리케이션 사용자 구성 창에서 다음 키 설정을 편집하는 관리자의 기능을 제어할 수 있습니다.

- 사용자 순위 편집
- 액세스 제어 그룹 할당 편집
- 신규 사용자 추가
- 사용자 암호 편집

프로시저

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

단계 **2** 찾기를 클릭하고 사용자 지정 역할을 선택합니다.

단계 **3** 관련 링크에서 고급 역할 구성을 선택하고 이동을 클릭합니다.

단계 **4** 리소스 웹 페이지에서 애플리케이션 사용자 웹 페이지 또는 사용자 웹 페이지를 선택합니다.

단계 **5** 설정을 편집합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

액세스 제어 그룹 만들기

새 액세스 제어 그룹을 생성해야 하는 경우 이 절차를 사용하십시오. 필요한 역할 및 액세스 권한을 가진 표준 그룹이 없는 경우 이 작업을 수행할 수 있습니다. 사용자 정의 그룹을 만드는 방법은 두 가지가 있습니다.

- 새로 추가 버튼을 사용하여 처음부터 새 액세스 제어 그룹을 만들고 구성합니다.
- 기존 그룹이 필요한 그룹과 비슷한 역할 할당을 가지는 경우 복사 버튼을 사용합니다. 기존 그룹의 설정을 새 그룹 및 편집 가능한 그룹으로 복사할 수 있습니다.

프로시저

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

단계 **2** 다음 중 하나를 수행합니다.

- 처음부터 새 그룹을 만들려면 새로 추가를 클릭합니다.
- 기존 그룹의 설정을 복사하려면 찾기를 클릭하고 기존 액세스 제어 그룹을 엽니다. 복사를 클릭하고 새 그룹의 이름을 입력합니다. 확인을 클릭합니다.

단계 **3** 액세스 제어 그룹의 이름을 입력합니다.

단계 **4** 사용자 순위가 다음과 같은 사용자에 사용 가능 드롭다운에서 이 그룹에 할당하기 위해 사용자가 충족해야 하는 최소 사용자 순위를 선택합니다. 기본 사용자 순위는 1입니다.

단계 **5** 저장을 클릭합니다.

단계 **6** 액세스 제어 그룹에 역할을 할당합니다. 선택하는 역할은 그룹 구성원에게 할당됩니다.

a) 관련 링크에서 액세스 제어 그룹에 역할 할당을 선택하고 이동을 클릭합니다.
b) 찾기를 클릭하여 기존 역할을 검색합니다.
c) 추가할 역할을 선택하고 선택한 항목 추가를 클릭합니다.
d) 저장을 클릭합니다.

다음에 수행할 작업

액세스 제어 그룹에 사용자 할당, 9 페이지

액세스 제어 그룹에 사용자 할당

표준 또는 사용자 정의 액세스 제어 그룹에서 사용자를 추가하거나 삭제합니다. .

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

참고 회사 LDAP 디렉터리에서 새 사용자를 동기화하는 중이거나 적절한 권한으로 순위 계층 및 액세스 제어 그룹이 생성되는 경우 LDAP 동기화의 일부로 해당 그룹을 동기화된 사용자에게 할당할 수 있습니다. LDAP 디렉터리 동기화를 설정하는 방법에 대한 추가 정보는 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.

프로시저

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** 사용자 순위가 다음과 같은 사용자에 사용 가능 드롭다운에서 이 그룹에 할당하기 위해 사용자가 충족해야 하는 순위 요구 사항을 선택합니다.

단계 **4** 사용자 섹션에서 찾기를 클릭하여 사용자 목록을 표시합니다.

단계 **5** 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 **6** 액세스 제어 그룹에서 사용자를 삭제하려면:

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

단계 **7** 저장을 클릭합니다.

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.

프로시저

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 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.

프로시저

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.

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.

프로시저

	명령 또는 동작	목적
단계 **1**	사용자 지정 지원 센터 역할 만들기, 12 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, 12 페이지	지원 센터 역할에 대해 새 액세스 제어 그룹을 만듭니다.
단계 **3**	액세스 제어 그룹에 지원 센터 역할 할당, 13 페이지	지원 센터 액세스 제어 그룹에 지원 센터 역할을 할당합니다. 이 액세스 제어 그룹에 할당된

	명령 또는 동작	목적
		모든 사용자는 지원 센터 역할의 권한이 할당됩니다.
단계 **4**	액세스 제어 그룹에 지원 센터 구성원 할당, 13 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.

프로시저

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 수행할 작업

사용자 지정 지원 센터 액세스 제어 그룹 만들기, 12 페이지

사용자 지정 지원 센터 액세스 제어 그룹 만들기

시작하기 전에

사용자 지정 지원 센터 역할 만들기, 12 페이지

프로시저

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 수행할 작업

액세스 제어 그룹에 지원 센터 역할 할당, 13 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, 12 페이지

프로시저

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 버튼을 클릭합니다.

단계 **5** 찾기를 클릭하고 지원 센터 역할을 선택합니다.

단계 **6** 선택한 항목 추가를 클릭합니다.

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

액세스 제어 그룹에 지원 센터 구성원 할당, 13 페이지

액세스 제어 그룹에 지원 센터 구성원 할당

시작하기 전에

액세스 제어 그룹에 지원 센터 역할 할당, 13 페이지

프로시저

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 확인합니다.

프로시저

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.

비활성 사용자 계정 비활성화

다음 절차를 사용하여 Cisco Database Layer Monitor 서비스를 사용하여 비활성 사용자 계정을 비활성화합니다.

지정된 일 수 내에 Cisco Unified Communications Manager에 로그인하지 않은 경우 Cisco Database Layer Monitor는 예약된 유지 보수 작업 중에 사용자 계정 상태를 비활성으로 변경합니다. 비활성화된 사용자는 후속 감사 로그에서 자동으로 감사됩니다.

시작하기 전에

Cisco Database Layer Monitor 서비스(시스템 > 서비스 매개 변수)에서 선택한 서버의 유지 보수 시간을 입력합니다.

프로시저

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

단계 **2** 서버 드롭다운 목록 상자에서 서버를 선택합니다.

단계 **3** 서비스 드롭다운 목록 상자에서 **Cisco Database Layer Monitor** 매개 변수를 선택합니다.

단계 **4** 고급을 클릭합니다.

단계 **5** 용자 계정 비활성화 미사용 기간**(**일**)** 필드에 일 수를 입력합니다. 예를 들면 90을 입력합니다. 시스템은 입력된 값을 임계값으로 사용하여 계정 상태를 비활성으로 선언합니다. 자동 비활성화를 해제하려면 값을 0으로 입력합니다.

참고 이것은 필수 필드입니다. 기본값 및 최소값은 0이고 단위는 일입니다.

단계 **6** 저장을 클릭합니다.

구성된 일 수 내에 비활성 상태로 남아 있는 경우(예: 90일) 사용자가 비활성화됩니다. 감사 로그에 항목이 생성되고 "< userID > 사용자가 비활성으로 표시됨"이라는 메시지가 표시됩니다.

원격 계정 설정

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

프로시저

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.
시스템에서 암호화된 암호구를 생성합니다.

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 *2:* 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 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
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 감사 로그 관리	감사 로깅 기능에 대한 다음 작업을 수행할 수 있습니다. • Cisco 통합 서비스 가용성의 감사 로그 구성 창에서 감사 로깅 보기 및 구성 • Cisco 통합 서비스 가용성에서 추적 보기 및 구성과 실시간 모니터링 도구에서 감사 로그 기능에 대한 추적 수집 • Cisco 통합 서비스 가용성에서 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] 버튼을 클릭하여 특정 전화기에 대한 전화기 단추 정보 순서 바꾸기
		표준 CCM 전화 관리

표준 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
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 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 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
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 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 지정 보류를 사용할 수 있습니다. 중요 열려 있는 회선 및 지정 보류 회선의 최대 수는 65000을 초과해서는 안 됩니다. 합계가 65000을 초과하는 경우 애플리케이션 사용자에서 표준 CTI 허용 통화 지정 보류 모니터링 역할을 제거하거나 구성된 지정 보류 회선 수를 줄이십시오.	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 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
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 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 통합 서비스 가용성 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 통합 서비스 가용성 또는 실시간 모니터링 도구에서 다음 창을 보고 구성할 수 있습니다. • 알람 구성 및 알람 정의(Cisco 통합 서비스 가용성) • 감사 추적(읽기/보기 전용으로 표시됨) • SNMP 관련 창(Cisco 통합 서비스 가용성) • 추적 구성 및 추적 구성 문제 해결(Cisco 통합 서비스 가용성) • 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 역할	역할에 대한 권한/리소스	연결된 표준 액세스 제어 그룹
표준 SERVICEABILITY 관리	Cisco 통합 서비스 가용성 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 서비스 가용성 읽기 전용	Cisco 통합 서비스 가용성 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 통합 서비스 가용성에서 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