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 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 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.

프로시저

단계 **1** Cisco Unified CM 관리에서사용자 관리 > 사용자 설정 > 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.

프로시저

단계 **1** Cisco Unified CM 관리에서사용자 관리 > 사용자 설정 > 인증서 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.

참고 이 확인란을 선택하면 사용자가 개인 디렉터리 서비스를 사용하여 PIN을 변경할 수 없다는 점에 유의하십시오.

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.

프로시저

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 수행할 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.

프로시저

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.

세션 종료 관리

관리자는 이 절차를 사용하여 각 노드에 대한 사용자의 활성 로그인 세션을 종료할 수 있습니다.

참고

- 권한 수준이 4인 관리자만 세션을 종료할 수 있습니다.
- 세션 관리는 특정 노드에서 활성 로그인 세션을 종료합니다. 관리자가 서로 다른 노드에서 모든 사용자 세션을 종료하고자 하는 경우 관리자는 각 노드에 로그인하고 세션을 종료해야 합니다.

이 기능은 다음 인터페이스에 적용됩니다.

- Cisco Unified CM 관리
- Cisco 통합 서비스 가용성
- Cisco Unified Reporting
- Cisco Unified Communications 자가 관리 포털
- Cisco Unified CM IM and Presence 관리
- Cisco Unified IM and Presence Service 가용성
- Cisco Unified IM and Presence 보고

프로시저

단계 **1** Cisco 통합 OS 관리 또는 Cisco Unified IM and Presence OS 관리에서 보안 > 세션 관리를 선택합니다. 세션 관리 창이 표시됩니다.

단계 **2** 활성 로그인한 사용자의 사용자 ID를 사용자 **ID** 필드에 입력합니다.

단계 **3** 세션 종료를 클릭합니다.

단계 **4** 확인을 클릭합니다.

종료된 사용자가 로그인된 인터페이스 페이지를 새로 고치면 사용자가 로그아웃됩니다. 감사 로그에 항목이 생성되고 종료된 `userID`가 표시됩니다.