사용자 관리

Jabber ID

Cisco Jabber는 Jabber ID를 사용하여 연락처 소스에서 연락처 정보를 식별합니다.

기본 Jabber ID는 사용자 ID 및 프레즌스 도메인을 사용하여 생성됩니다.

예를 들어, Adam McKenzie의 사용자 ID가 `amckenzie`이고 해당 도메인이 `example.com`이며 Jabber ID가 `amckenzie@example.com`입니다.

Cisco Jabber 사용자 ID 또는 이메일 주소에서 다음 문자가 지원됩니다.

- 밑줄 문자(A ~ Z)
- 소문자(a ~ z)
- 숫자(0-9)
- 마침표(.)
- 하이픈(-)
- 밑줄(_)
- 물결표(~)
- 해시태그(#)

연락처 목록을 채울 때 클라이언트는 Jabber ID를 사용하여 연락처 소스를 검색하여 연락처를 확인하고 이름, 성 및 기타 연락처 정보를 표시합니다.

IM 주소 체계

Cisco Jabber 10.6 이상에서는 도메인이 동일한 프레즌스 아키텍처에 있는 경우(예: example-us.com 및 example-uk.com 사용자) 온프레미스 구축에 대한 다중 프레즌스 도메인 아키텍처 모델을 지원합니다. Cisco Jabber는 Cisco Unified Communications Manager IM and Presence 10.x 이상을 사용하여 유연한 IM 주소 체계를 지원합니다. IM 주소 체계는 Cisco Jabber 사용자를 식별하는 Jabber ID입니다.

다중 도메인 모델을 지원하려면 구축의 모든 구성 요소에 다음 버전이 필요합니다.

- Cisco Unified Communications IM and Presence 서버 노드 및 통화 제어 노드 버전 10.x 이상.
- Windows, Mac, IOS 및 Android 버전 10.6 이상을 실행 중인 모든 클라이언트.

다음과 같은 시나리오에서 여러 도메인 아키텍처를 사용하는 Cisco Jabber만 구축합니다.

- Cisco Jabber 10.6 이상 버전은 모든 플랫폼(Windows, Mac, IOS 및 Android(DX 시리즈와 같은 Android 기반 IP 전화기 포함))에서 조직의 모든 사용자에게 새 설치로 구축됩니다.
- 프레즌스 서버에서 도메인 또는 IM 주소를 변경하기 전에 Cisco Jabber는 모든 플랫폼(Windows, Mac, IOS 및 Android(DX 시리즈와 같은 Android 기반 IP 전화기 포함))에서 모든 사용자에 대해 버전 10.6 이상으로 업그레이드됩니다.

고급 프레즌스 설정에서 사용 가능한 IM 주소 체계는 다음과 같습니다.

- UserID@[기본 도메인]
- 디렉토리 URI

UserID@[기본 도메인**]**

사용자 ID 필드는 LDAP 필드에 매핑됩니다. 이는 기본 IM 주소 체계입니다.

예를 들어, 사용자 Anita Perez에 계정 이름 aperez가 있고 사용자 ID 필드는 sAMAccountName LDAP 필드에 매핑됩니다. 사용된 주소 체계는 aperez@example.com입니다.

디렉토리 **URI**

디렉터리 URI가 메일 또는 **msrtcsip-primaryuseraddress** LDAP 필드에 매핑됩니다. 이 옵션은 인증을 위해 사용자 ID와 관계 없는 체계를 제공합니다.

예를 들어, 사용자 Anita Perez에 계정 이름 aperez가 있고, 메일 필드가 Anita.Perez@domain.com이며 사용되는 주소 체계가 Anita.Perez@domain.com입니다.

Jabber ID를 사용한 서비스 검색

서비스 검색은 `[userid]@[domain.com]` 형식으로 입력한 Jabber ID를 사용하 고 기본적으로 Jabber ID의 `domain.com` 부분을 추출하여 사용 가능한 서비스를 검색합니다. 프레즌스 도메인이 서비스 검색 도메인과 동일하지 않은 구축의 경우, 다음과 같이 설치 중에 서비스 검색 도메인 정보를 포함할 수 있습니다.

- Windows용 Cisco Jabber에서는 이 작업이 `SERVICES_DOMAIN` 명령줄 인수를 사용하여 수행됩니다.
- Mac용 Cisco Jabber, Android용 Cisco Jabber 또는 iPhone 및 iPad용 Cisco Jabber의 경우 URL 구성에 사용된 `ServicesDomain` 매개 변수를 사용하여 서비스 검색 도메인을 설정할 수 있습니다.

.

SIP URI

SIP URI는 각 사용자와 연결됩니다. SIP URI는 이메일 주소, IMAddress 또는 UPN일 수 있습니다.

SIP URI는 Cisco Unified Communications Manager의 디렉터리 URI 필드를 사용하여 구성됩니다. 사용 가능한 옵션은 다음과 같습니다.

- mail
- msRTCSIP-primaryuseraddress

사용자는 SIP URI를 입력하여 연락처를 검색하고 연락처에 전화를 걸 수 있습니다.

LDAP 사용자 ID

디렉터리 소스에서 Cisco Unified Communications Manager로 동기화되면 디렉터리에 있는 속성에서 사용자 ID가 채워집니다. 사용자 ID를 보유하는 기본 속성은 `sAMAccountName`입니다.

페더레이션에 대한 사용자 ID 계획

페더레이션을 위해 Cisco Jabber는 연락처 검색 중에 각 사용자의 연락처 ID 또는 사용자 ID가 연락처를 확인하도록 요구합니다.

SipUri 매개 변수의 사용자 ID에 대한 속성을 설정합니다. 기본값은 `msRTCSIP-PrimaryUserAddress`입니다. 사용자 ID에서 제거할 접두사가 있는 경우 UriPrefix 매개 변수에 값을 설정할 수 있습니다. *Cisco Jabber*에 대한 매개 변수 참조 설명서의 최신 버전을 참조하십시오.

사용자 연락처 사진에 대한 프록시 주소

Cisco Jabber는 사진 서버에 액세스하여 연락처 사진을 검색합니다. 네트워크 구성에 웹 프록시가 포함되어 있는 경우에는 Cisco Jabber가 사진 서버에 액세스할 수 있는지 확인해야 합니다.

인증

Cisco Unified Communications Manager LDAP 인증

디렉터리 서버를 인증하도록 Cisco Unified Communications Manager에 LDAP 인증이 구성되어 있습니다.

사용자가 클라이언트에 로그인하면 프레즌스 서버가 해당 인증을 Cisco Unified Communications Manager로 라우팅합니다. 그런 다음 Cisco Unified Communications Manager는 디렉터리 서버에 대한 인증을 프록시합니다.

Webex Messenger 로그인 인증

Webex Messenger 인증은 Webex 관리 도구를 사용하여 구성됩니다.

사용자가 클라이언트에 로그인하면 정보가 Webex Messenger로 전송되고 인증 토큰이 클라이언트로 다시 전송됩니다.

SSO(Single Sign-On) 인증

단일 로그인 인증은 ID 제공자(IdP) 및 서비스를 사용하여 구성됩니다.

사용자가 클라이언트에 로그인하면 정보가 IdP로 전송되고 자격 증명이 승인되면 인증 토큰이 Cisco Jabber로 다시 전송됩니다.

iPhone 및 iPad용 Cisco Jabber에 대한 인증서 기반 인증

Cisco Jabber는 클라이언트 인증서를 통해 IdP 서버에서 인증합니다. 이 인증서 인증을 사용하면 사용자 자격 증명을 입력하지 않고도 서버에 로그인할 수 있습니다. 클라이언트는 Safari 프레임워크를 사용하여 이 기능을 구현합니다.

필요조건

- Cisco Unified Communications Manager 11.5, IM and Presence 서비스 11.5, Cisco Unity Connection 11.5 이상.
- 모바일 및 Remote Access용 Expressway 8.9 이상
- 통합 커뮤니케이션 인프라에 활성화된 SSO.

- 모든 서버 인증서는 Cisco Unified Communications Manager, IM and Presence 서비스, Cisco Unity Connection 및 IdP 서버를 포함하여 CA 서명됩니다. iOS 장치에서 OS의 신뢰할 수 있는 인증 기관을 사용하는 경우 Cisco Jabber 앱을 설치하기 전에 CA 인증서를 설치합니다.
- Cisco Unified Communications Manager의 SSO에 대한 기본 브라우저(임베디드 Safari)를 구성합니다. 자세한 내용은 *Cisco Jabber*의 온프레미스 구축에서 인증서 기반 SSO 인증에 대한 섹션을 참조하십시오.
- 모바일 및 Remote Access용 Expressway 서버의 SSO에 대한 기본 브라우저(임베디드 Safari)를 구성합니다. 자세한 내용은 https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html의 Cisco Expressway 설치 설명서를 참고하십시오.

EMM 솔루션을 통해 iOS 장치에 Cisco 인증서를 구축할 수 있습니다.

권장 사항 - Cisco는 iOS 장치에 인증서를 구축하는 데 EMM 솔루션을 사용할 것을 권장합니다.

Android용 Cisco Jabber에 대한 인증서 기반 인증

Cisco Jabber는 클라이언트 인증서를 사용하여 싱글 사인온 서버(Webex Messenger 및 온프레미스)에 로그인합니다.

요구 사항

- Android OS 5.0 이상
- SSO(Single Sign-On)가 활성화됨
- Jabber 클라이언트는 MRA(Mobile and Remote Access) 및 비 MRA 구축 모드를 통해 지원됩니다.
- Jabber는 Android 7.0 이상에서 잘못된 인증서에 대한 알림을 Android OS에 설치된 사용자 정의 CA 서명 인증서에 대해서만 표시합니다. Android 7.0을 대상으로 하는 앱은 시스템에서 제공하는 인증서만 신뢰하고 더 이상 사용자 추가 인증 기관을 신뢰하지 않습니다.

인증서 구축

Cisco는 Android 장치에 인증서를 구축하는 데 EMM 솔루션을 사용하는 것을 권장합니다.

음성 메일 인증

사용자가 Cisco Unity Connection에 있어야 합니다. Cisco Unity Connection은 다중 인증 유형을 지원합니다. Cisco Unified Communications Manager 및 Cisco Unity Connection이 동일한 인증을 사용하는 경우, 동일한 자격 증명을 사용하도록 Cisco Jabber를 구성하는 것이 좋습니다.

OAuth

Cisco Jabber에서 OAuth 프로토콜을 사용하여 서비스에 대한 사용자 액세스 권한을 인증하도록 설정할 수 있습니다. 사용자가 OAuth 사용 환경에 로그인하면 로그인할 때마다 자격 증명을 입력할 필요

가 없습니다. 그러나 서버가 OAuth를 지원하지 않는 경우 Jabber가 적절하게 작동하지 않을 수 있습니다.

Cisco Unified Communication Manager 12.5 이상을 사용하는 경우 SIP OAuth를 활성화할 수도 있습니다. Jabber가 SIP에 대한 권한을 부여하여 Jabber가 TLS를 통해 SIP 서비스에 연결할 수 있도록 합니다. 또한 Jabber에서 보안 연결(sRTP)을 통해 미디어를 전송할 수 있습니다. SIP OAuth는 보안 SIP 및 미디어를 활성화하는 데 CAPF 등록이 더 이상 필요하지 않음을 의미합니다.

필수 조건:

- 작동하도록 구축된 경우 이러한 모든 구성 요소에 대해 OAuth 새로 고침 토큰이 설정되어 있어야 합니다.
- Cisco Unified Communication Manager, Cisco Unified Communication Manager Instant Messaging and Presence 및 Cisco Unity Connection은 버전 11.5(SU3) 또는 12.0 이어야 합니다.
- 모바일 및 Remote Access용 Cisco Expressway 버전 X 8.10 이상
- SIP OAuth의 경우: Cisco Unified Communication Manager 12.5 이상, 모바일 및 Remote Access용 Cisco Expresswayversion X12.5 이상.

OAuth를 구성하기 전에 다음에 해당하는 구축 유형을 확인하십시오.

- 로컬 인증 구축을 사용하는 경우 IdP 서버가 필요하지 않으며 Cisco Unified Communication Manager가 인증을 담당합니다.
- OAuth를 구성하거나 구성하지 않은 상태로 OAuth를 설정할 수 있습니다. SSO를 사용하는 경우 모든 서비스에 대해 이 기능이 활성화되어 있는지 확인합니다. SSO가 활성화된 구축을 사용하는 경우 IdP 서버를 구축하고 IdP 서버가 인증을 담당합니다.

사용자를 위해 다음 서비스에서 OAuth를 활성화할 수 있습니다.

- Cisco Unified Communications Manager
- Cisco Expressway
- Cisco Unity Connection

이러한 서버에서 OAuth는 기본적으로 비활성화되어 있습니다. 이러한 서버에서 OAuth를 활성화하려면 다음을 수행합니다.

- Cisco Unified Communications Manager 및 Cisco Unity Connection 서버의 경우 엔터프라이즈 매개변수 구성 > 새로 고침 로그인 흐름을 사용한 **OAuth**로 이동합니다.
- Cisco Expressway-C의 경우 구성 통합 커뮤니케이션 > 구성 새로 고침을 사용하여 **OAuth** 토큰으로 인증으로 이동합니다.

이러한 서버에서 OAuth가 활성화 또는 비활성화되면 Jabber가 구성 다시 가져오기 간격 동안 이를 식별하고 사용자가 Jabber에서 로그아웃했다가 로그인하도록 합니다.

로그아웃하는 동안 Jabber는 캐시에 저장된 사용자 자격 증명을 삭제한 다음 사용자가 일반 로그인 흐름으로 로그인한 다음, Jabber가 모든 구성 정보를 먼저 가져온 다음 사용자가 Jabber 서비스에 액세스할 수 있도록 합니다.

Cisco Unified Communication Manager에서 OAuth를 구성하려면:

1. **Cisco Unified Communication Manager Admin** > 시스템 > 엔터프라이즈 매개 변수 > **SSO** 구성으로 이동합니다.
2. **O-Auth** 액세스 토큰 만료 타이머**(**분**)**를 원하는 값으로 설정합니다.
3. **O-Auth** 새로 고침 토큰 만료 타이머**(**일**)**를 원하는 값으로 설정합니다.
4. 저장 버튼을 클릭합니다.

Cisco Expressway에서 OAuth를 구성하려면:

1. 구성 > 통합 커뮤니케이션 > 구성 > **MRA** 액세스 제어로 이동합니다.
2. **O-Auth** 로컬 인증을 켜기로 설정합니다.

Cisco Unity에서 OAuth를 구성하려면:

1. **AuthZ** 서버로 이동하고 새로 추가를 선택합니다.
2. 모든 필드에 세부 정보를 입력하 고 인증서 오류 무시를 선택합니다.
3. 저장을 클릭합니다.

제한 사항

Jabber가 자동 침입 방지를 트리거합니다**.**

조건:

- 모바일 및 Remote Access용 Expressway 구축은 OAuth 토큰(새로 고침 토큰 포함 또는 제외)으로 인증되도록 구성됩니다.
- Jabber 사용자 액세스 토큰이 만료되었습니다.

Jabber는 다음 중 하나를 수행합니다.

- 데스크톱 최대 절전 모드에서 재시작
- 네트워크 연결 복구
- 몇 시간 동안 로그아웃한 후 빠른 로그인 시도

동작(Behavior):

- 일부 Jabber 모듈은 만료된 액세스 토큰을 사용하여 Expressway-E에서 인증을 시도합니다.
- Expressway-E는 (올바르게) 이러한 요청을 거부합니다.
- 특정 Jabber 클라이언트에서 이러한 요청이 6개 이상 있는 경우 Expressway-E는 10분(기본적으로) 동안 해당 IP 주소를 차단합니다.

증상:

영향을 받는 Jabber 클라이언트의 IP 주소는 HTTP 프록시 인증 실패 범주에 있는 Expressway-E의 차단된 주소 목록에 추가됩니다. 이 내용은 시스템 > 보호 > 자동 탐지 > 차단된 주소에서 확인할 수 있습니다.

대체 방법:

두 가지 방법으로 이 문제를 해결할 수 있습니다. 특정 범주에 대한 탐색 임계값을 늘리거나 영향을 받는 클라이언트에 대한 예외를 만들 수 있습니다. 여기서는 사용자 환경에서 예외가 실용적이 지 않을 수 있으므로 임계값 옵션에 대해 설명합니다.

1. 시스템 > 보호 > 자동 탐지 > 구성으로 이동합니다.
2. **HTTP** 프록시 인증 실패를 클릭합니다.
3. 트리거 수준을 5에서 10으로 변경합니다. 10은 만료된 토큰을 제공하는 Jabber 모듈을 허용하기에 충분해야 합니다.
4. 구성을 저장하여 즉시 적용합니다.
5. 영향을 받는 클라이언트의 차단을 해제합니다.

여러 리소스 로그인

모든 Cisco Jabber 클라이언트는 사용자가 시스템에 로그인할 때 다음 중앙 IM and Presence 서비스 노드 중 하나에 등록됩니다. 이 노드는 IM and Presence 서비스 환경의 가용성, 연락처 목록 및 기타 측면을 추적합니다.

- 온프레미스 구축: Cisco Unified Communications Manager IM and Presence Service
- 클라우드 구축: Webex.

이 IM and Presence 서비스 노드는 각 고유 네트워크 사용자와 연결된 등록된 모든 클라이언트를 다음 순서로 추적합니다.

1. 두 사용자 간에 새 IM 세션이 시작되면, 첫 번째 들어오는 메시지는 수신 사용자의 등록된 모든 클라이언트로 브로드 캐스팅됩니다.
2. 그런 다음 IM and Presence 서비스 노드는 등록된 클라이언트 중 하나의 첫 번째 응답을 기다립니다.
3. 응답하는 첫 번째 클라이언트는 사용자가 다른 등록된 클라이언트를 사용하여 응답을 시작할 때까지 나머지 수신 메시지를 수신합니다.
4. 그런 다음 노드는 후속 메시지를 이 새 클라이언트로 재 라우팅합니다.

참고 사용자가 여러 장치에 로그인되어 있을 때 활성 리소스가 없는 경우 우선 순위가 가장 높은 클라이언트에게 우선 순위가 부여됩니다. 모든 장치에서 프레즌스 상태 우선 순위가 동일하면 사용자가 로그인한 최신 클라이언트에게 우선 순위가 부여됩니다.