보안 및 모니터링

로그아웃 비활동 타이머

클라이언트			
Windows	**Mac**	**iPhone 및 iPad**	**Android**
예	예	예	예

배포			
온프레미스	**Webex Messenger**	팀 메시징 모드	**VDI용 Softphone**
예	예	예	예

로그아웃 비활성 타이머를 사용하면 지정된 시간 동안 사용하지 않을 경우 클라이언트에서 사용자를 자동으로 로그아웃할 수 있습니다.

모바일 클라이언트의 비활성은 다음을 포함합니다.

- 클라이언트가 백그라운드로 이동합니다.
- 음성 통화에 사용자가 개입할 필요가 없습니다.

ForceLogoutTimerMobile 매개 변수를 사용하여 모바일 클라이언트에서 이 기능을 구성합니다.

데스크톱 클라이언트의 비활성은 다음을 포함합니다.

- 키보드 또는 마우스 활동이 없습니다.
- 전화를 걸고 받기 위해 연결된 액세서리에 대한 사용자 상호 작용이 없습니다.

ForceLogoutTimerDesktop 매개 변수를 사용하여 데스크톱 클라이언트에서 이 기능을 구성합니다.

매개 변수를 설정하지 않은 경우 클라이언트는 자동으로 로그아웃되지 않습니다.

문제 보고

클라이언트			
Windows	**Mac**	**iPhone** 및 **iPad**	**Android**
예	—	—	—

배포			
온프레미스	**Webex Messenger**	팀 메시징 모드	**VDI**용 **Softphone**
예	예	예	예

문제 보고 기능을 설정하면 클라이언트에서 발생하는 문제에 대한 요약을 사용자에게 보낼 수 있습니다. 문제 보고서를 제출하는 방법은 다음과 같이 두 가지가 있습니다.

- 사용자가 클라이언트 인터페이스를 통해 문제 보고서를 직접 제출합니다.
- 사용자가 문제 보고서를 로컬로 저장한 다음 나중에 업로드합니다.

클라이언트는 HTTP POST 메서드를 사용하여 문제 보고서를 제출합니다. POST 요청을 수락 하는 사용자 정의 스크립트를 만들고 구성 매개 변수로 HTTP 서버에서 스크립트의 URL을 지정합니다. 사용자는 문제 보고서를 로컬로 저장할 수 있으므로 사용자가 문제 보고서를 업로드하는 데 사용할 수 있는 양식이 포함된 HTML 페이지를 생성해야 합니다.

시작하기 전에

환경을 준비하려면 다음 단계를 완료하십시오.

1. HTTP 서버를 설치하고 구성합니다.
2. HTTP POST 요청을 수락하는 사용자 정의 스크립트를 만듭니다.
3. 사용자가 로컬에 저장된 문제 보고서를 업로드하는 데 사용할 수 있는 HTML 페이지를 만듭니다. HTML 페이지는 `.ZIP` 아카이브로 저장된 문제 보고서를 수락 하는 양식을 포함하고 사용자 정의 스크립트를 사용하여 문제 보고서를 게시하는 작업을 포함해야 합니다.

다음은 문제 보고서를 수락하는 예제 양식입니다.

```
<form name="uploadPrt" action="http://server_name.com/scripts/UploadPrt.php" method="post"
 enctype="multipart/form-data">
 <input type="file" name="zipFileName" id="zipFileName" /><br />
 <input type="submit" name="submitBtn" id="submitBtn" value="Upload File" />
</form>
```

단계 **1** HTTP 서버에서 사용자 정의 스크립트를 호스팅합니다.

단계 **2** 구성 파일의 PrtLogServerUrl 매개 변수 값으로 스크립트의 URL을 지정합니다.

문제 보고서 암호 해독

문제 보고서를 해독하는 명령줄 도구 `CiscoJabberPrtDecrypter.exe`는 Windows 시스템에서만 사용할 수 있고 설치 관리자에 포함되어 있습니다. 이 도구에는 다음과 같은 인수가 있습니다.

- `--help` - 도움말 메시지를 표시합니다.
- `--privatekey` - 개인 키 파일을 지정합니다. 이는 프라이버시 고급 메일(.pem) 또는 개인 정보 교환 PKCS #12(.pfx) 형식입니다.
- `--password` - 입력 개인 키 파일이 암호로 보호되는 경우 선택 사항입니다.
- `--encryptionkey` - 암호화 비밀 키 파일(예: `file.zip.esk`)을 지정합니다.
- `--encryptedfile` - 암호화된 파일(예: `file.zip.enc`)을 지정합니다.
- `--outputfile` - 출력 파일(예: `decryptedfile .zip`)을 지정합니다.

시작하기 전에

문제 보고서를 해독하려면 다음이 필요합니다.

- 암호화를 사용하여 문제 보고서를 생성할 때 생성되는 zip 파일의 두 파일:
  - *file.zip.esk* - 암호화 된 대칭 키입니다.
  - *file.zip.enc* - AES256를 사용하여 암호화된 원래 데이터입니다.
- 데이터를 암호화 하는 데 사용되는 인증서에 대한 개인 키입니다.

단계 **1** Windows에서 명령 프롬프트를 엽니다.

단계 **2** `C:\Program Files(x86)\Cisco Systems\CUCILync\` 디렉터리로 이동합니다.

단계 **3** 명령과 매개 변수를 입력합니다.

데스크톱 클라이언트의 예: `CiscoJabberPrtDecrypter.exe --privatekey C:\PRT\PrivateKey.pfx --password 12345 --encryptedfile C:\PRT\file.zip.enc --encryptionkey C:\PRT\file.zip.esk --outputfile C:\PRT\decryptedfile.zip`

암호 해독에 성공하면 출력 파일이 생성됩니다. 잘못 된 매개 변수가 있는 경우 암호 해독이 실패하고 명령줄에 오류가 표시됩니다.

PRT 로그를 원격으로 수집

사용자가 PRT 로그를 업로드하는 것을 기다리지 않고, **Unified CM** 관리에서 로그를 원격으로 생성할 수 있습니다.

시작하기 전에

이 기능을 사용 하려면 구축에 Unified CM 릴리스 12.5.1 SU 1 이상이 필요합니다. RemotePRTServer 매개 변수는 PRT 로그를 서버에 업로드하는 스크립트를 지정합니다.

단계 **1** 장치 > 전화기를 선택합니다.

단계 **2** 로그가 필요한 장치를 선택합니다.

단계 **3** 선택 항목에 대한 **PRT** 생성을 클릭합니다.

스크립트에서 PRT 로그를 서버에 업로드합니다.

참고 Cisco Sunkist 헤드셋에서 로그를 수집하려면 펌웨어 버전 1.3 이상이 필요합니다.

원격 PRT 로그 수집에 대한 설정

PRT 로그를 원격으로 수집하려면 먼저 **Unified CM** 관리에서 로그를 업로드하는 스크립트를 지정해야 합니다.

단계 **1** 사용자 관리 > 사용자 설정 > **UC** 서비스를 선택합니다.

단계 **2** **UC** 서비스 유형 이 **Jabber** 클라이언트 구성**(jabber-config.xml)**인 UC 서비스를 추가합니다.

단계 **3** 다음 값을 사용하여 **Jabber** 구성 매개 변수를 추가합니다.

- 섹션 - 정책
- 매개 변수 - **RemotePRTServer**
- 값 - 업로드 스크립트의 URL.

장치 **PIN** 설정

클라이언트			
Windows	**Mac**	**iPhone** 및 **iPad**	**Android**
—	—	예	예

배포			
온프레미스	**Webex Messenger**	팀 메시징 모드	**VDI**용 **Softphone**
예	예	예	—

보안 장치에서만 Jabber를 사용하는 것이 좋습니다. 장치가 안전한지 확인하려면 ForceDevicePin 매개 변수를 **`true`**로 구성합니다.

예:

```
<ForceDevicePin>true</ForceDevicePin>
```

장치가 보안되어 있지 않은 경우:

- 그러면 Jabber가 PIN 설정 알림을 표시합니다. 이 알림은 사용자가 13초 내에 **SET PIN**을 누르지 않으면 Jabber에서 로그아웃 됩니다.

  사용자가 **SET PIN** 옵션을 누른 후에는 사용자가 장치 설정으로 이동하여 PIN 또는 지문 인증을 사용하여 장치를 보호해야 합니다.

- 사용자가 Jabber에 로그인한 다음 즉시 백그라운드에 배치하는 경우 Jabber는 사용자가 장치를 보호하는지 여부를 확인합니다. 장치에 보안이 설정되지 않은 경우 사용자는 Jabber에서 로그아웃 됩니다.

모바일 클라이언트의 생체 인증

클라이언트			
Windows	**Mac**	**iPhone** 및 **iPad**	**Android**
—	—	예	예

배포			
온프레미스	**Webex Messenger**	팀 메시징 모드	**VDI**용 **Softphone**
예	예	예	—

Cisco Jabber는 사용자가 안전하게 로그인할 수 있도록 지문 또는 얼굴 인식 지문, 터치 ID 또는 얼굴 ID 인증을 지원합니다. 이러한 인증 방법을 사용하여 사용자가 모바일 장치에서 Cisco Jabber에 빠르고 안전하게 로그인하도록 할 수 있습니다.

다음 시나리오에서는 지문 또는 얼굴 인식 이 사용됩니다.

- Android용 Cisco Jabber 사용자가 수동으로 로그아웃하거나 자동 로그아웃한 후 Jabber에 로그인할 때 지문 또는 얼굴 인식에 의한 인증을 사용할 수 있습니다.
- iPhone 및 iPad용 Cisco Jabber 사용자가 수동으로 로그아웃하거나 자동 로그아웃 후에 Cisco Jabber에 로그인할 때 터치 ID 또는 얼굴 ID 인증을 사용하여 Cisco Jabber에 로그인해야 합니다.

매개 변수 LocalAuthenticationWithBiometrics를 구성하여 Cisco Jabber 사용자가 이 인증을 사용하여 로그인하도록 활성화할 수 있습니다.

이 매개 변수는 다음 값을 사용하여 구성할 수 있습니다.

- AdminEnabled - Cisco Jabber가 사용자에게 지문 또는 얼굴 인식. 사용자는 생체 인증을 사용하여 Cisco Jabber에 로그인해야 합니다. 그러나 사용자의 장치에서 생체 인식 기능을 지원하지 않는 경우에는 사용자가 암호를 사용하여 로그인해야 합니다.
- UserDecision(기본값) - Cisco Jabber가 사용자에게 지문 또는 얼굴 인식. 사용자는 생체 인증을 사용하여 Cisco Jabber에 로그인할 것인지 여부를 결정할 수 있습니다.
- AdminDisabled - Cisco Jabber가 지문 또는 얼굴 인식. 사용자에게 메시지가 표시되지 않습니다.

인증이 실패하면 Cisco Jabber에서 사용자에게 로그인할 때마다 자격 증명을 입력하라는 메시지를 표시합니다.

예: `<LocalAuthenticationWithBiometrics>AdminDisabled</LocalAuthenticationWithBiometrics>`

생체 인식 인증을 위한 장치 요구 사항

이 기능은 운영 체제에서 생체 인식 인증을 지원하는 장치에서만 사용할 수 있습니다.

무성 모니터링 및 녹음

클라이언트			
Windows	**Mac**	**iPhone 및 iPad**	**Android**
예	예	예	예

배포			
온프레미스	**Webex Messenger**	팀 메시징 모드	**VDI용 Softphone**
예	예	예	예

무성 통화 모니터링은 Cisco Unified Communications Manager 기능입니다. 이 기능을 사용하면 감독자가 두 통화 참가자를 모두 들을 수 있지만 통화 참가자 중 어느 누구도 감독자가 하는 말을 들을 수 없습니다.

통화 녹음은 녹음 서버가 상담원 대화를 보관할 수 있도록 하는 Unified CM 기능입니다.

- Jabber는 무성 모니터링 또는 통화 녹음을 시작하기 위한 인터페이스를 제공하지 않습니다. 적절한 소프트웨어를 사용하여 통화를 자동으로 모니터링하거나 녹음합니다.
- Jabber는 현재 모니터링 알림 신호음을 지원하지 않습니다.
- 무성 모니터링 및 통화 녹음 기능만 사용할 수 있습니다. Jabber는 참여 또는 위 스퍼 코칭 등의 다른 기능을 지원하지 않습니다.

서버 요구 사항:

- 온프레미스 구축에 대해서만 무성 모니터링 및 통화 녹음을 지원합니다.
- Windows용 Cisco Jabber 및 Mac용 Cisco Jabber에 Cisco Unified Communications Manager 9.x 이상이 필요합니다.
- iPhone 및 iPad용 Cisco Jabber 및 Android용 Cisco Jabber에 Cisco Unified Communications Manager 11.0 이상이 필요합니다.

일부 Unified CM 릴리스에서는 모니터링 및 녹음 기능을 활성화하기 위해 장치 패키지가 필요합니다. 장치에 대해 전화기 구성 창에서 내장 브리지 필드를 사용할 수 있는지 확인합니다. 이 필드를 사용할 수 없는 경우 최신 장치 패키지를 다운로드하여 적용합니다.

무성 모니터링 또는 통화 녹음을 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 기능 구성 설명서를 참조하십시오.

요청 시 녹음

클라이언트			
Windows	**Mac**	**iPhone 및 iPad**	**Android**
예	예	—	—

배포			
온프레미스	**Webex Messenger**	팀 메시징 모드	**VDI용 Softphone**
예	예	예	예

모든 통화를 녹음하는 대신 사용자에게 녹음을 원하는 시기를 선택할 수 있는 유연성을 제공할 수 있습니다.

Unified Communications Manager 릴리스 12.5(1) 이상을 구축하는 경우 Jabber는 Jabber의 빌트인 브리지(BiB)를 사용하여 통합 CM의 주문형 녹음을 지원할 수 있습니다. Cisco Unified CM 관리에서 장치 >

전화기 > 녹음 옵션을 선택적 통화 녹음 활성화로 설정하여 기능을 활성화합니다. 클러스터 전체 또는 개별 전화기에서도 BiB를 활성화합니다.

이 기능을 활성화하면 통화 제어 메뉴에 사용자가 언제든지 녹음을 시작하고 중지할 수 있는 녹음 옵션이 포함됩니다.

사용 가능한 레코더 간 환경설정

기본적으로 사용자가 통화를 녹음하는 외부 브리지가 설정된 전화회의 통화에 참가하는 경우 Jabber는 녹음을 위해 해당 외부 브리지를 사용합니다. 그러나 일부 조직에서는 규정 준수를 위해 Jabber BiB를 사용하는 모든 녹음을 선호할 수 있습니다. 이러한 경우에는 Prefer_BIB_recorder 매개 변수를 사용하여 Jabber BIB에서 녹음을 시행합니다.

Cisco Jabber 분석을 통한 원격 분석

클라이언트			
Windows	**Mac**	**iPhone** 및 **iPad**	**Android**
예	예	예	예

구축			
온프레미스	**Webex Messenger**	팀 메시징 모드	**VDI**용 **Softphone**
예	예	예	예

경험 및 제품 성능을 개선하기 위해 Cisco Jabber는 비 개인 식별 가능 사용량 및 성능 데이터를 수집하여 Cisco로 전송할 수 있습니다. 집계된 데이터는 Cisco가 Jabber 클라이언트의 사용 방법 추세와 성능을 확인하는 데 사용합니다.

텔레메트리 기능을 사용하려면 `GoDaddy Class 2 인증 기관 루트 인증서`를 설치해야 합니다. 텔레메트리 서버 인증서 이름은 "metrics-a.wbx2.com"입니다. 이 인증서 이름에 대한 경고를 해결하려면 필요한 GoDaddy 인증서를 설치합니다. 인증서에 대한 자세한 정보는 계획 설명서를 참조하십시오.

기본적으로 텔레메트리 데이터는 설정되어 있습니다. 다음과 같은 텔레메트리 매개 변수를 구성할 수 있습니다.

- Telemetry_Enabled - 분석 데이터 수집 여부를 지정합니다. 기본값은 True입니다.
- TelemetryEnabledOverCellularData - 셀룰러 데이터와 Wi-Fi(true) 또는 Wi-Fi 전용(false)을 통해 분석 데이터를 전송할 것인지 여부를 지정합니다. 기본값은 True입니다.
- TelemetryCustomerID - 이 선택적 매개 변수는 분석 정보의 소스를 지정합니다. 이 ID는 개별 고객을 명시적으로 식별하는 문자열이거나, 고객을 식별하지 않고 일반 소스를 식별하는 문자열일 수 있습니다. 36자 고유 식별자를 만들거나 역방향 도메인 이름을 사용하려면 전역 고유 식별자(GUID)를 생성하는 도구를 사용하는 것이 좋습니다.

참고 Jabber 팀 메시징 모드 사용자는 텔레메트리를 비활성화하는 옵션을 사용할 수 없습니다.

이러한 매개 변수에 대한 자세한 내용은 매개 변수 참조 설명서를 참조하십시오.

https://www.cisco.com/c/en/us/about/legal/privacy-full.html에서 Cisco가 분석 데이터를 처리하는 방법에 대한 세부 정보를 확인할 수 있습니다.

Webex Control Hub의 Jabber 분석

클라이언트			
Windows	**Mac**	**iPhone 및 iPad**	**Android**
예	예	예	예

배포			
온프레미스	**Webex Messenger**	팀 메시징 모드	**VDI용 Softphone**
예	예	—	—

이제 Webex Control Hub를 통해 Jabber 분석에 액세스할 수 있습니다. 데이터는 분석 페이지의 **Jabber** 탭에서 사용할 수 있습니다. Jabber 분석은 다음과 같이 추세를 제공하는 핵심 성과 지표를 제공합니다.

- Active users
- 메시지가 전송되었음
- Jabber에서 발신 또는 수신된 통화
- Jabber의 화면 공유

Jabber 분석에 액세스하려면 Webex Control Hub가 설정되어 있어야 합니다. `jabber-config.xml`에서 이러한 매개 변수를 설정합니다.

- TelemetryEnabled - true
- TelemetryEnabledOverCellularData - true
- TelemetryCustomerID를 제어 허브의 OrgID

이 기능은 다음 구축 모드에서 사용할 수 있습니다.

- 전체 UC가 있는 온프레미스
- 온프레미스 IM 전용
- 온프레미스 전화기 전용

- Webex Messenger를 사용 하는 Jabber

참고 이 기능은 Jabber 구축에 영향을 주는 Webex Control Hub의 새로운 기능입니다. Jabber의 모든 릴리스에서 이 기능에 액세스할 수 있습니다.

무선 위치 모니터링 서비스

적용 대상: 모든 클라이언트

클라이언트			
Windows	**Mac**	**iPhone** 및 **iPad**	**Android**
예	예	예	예

구축			
온프레미스	**Webex Messenger**	팀 메시징 모드	**VDI**용 **Softphone**
예	예	예	예

무선 위치 모니터링 서비스를 사용하면 Cisco Jabber 사용자가 회사 네트워크에 연결하는 실제 위치를 확인할 수 있습니다. 이 정보는 Cisco Unified Communications Manager에 저장됩니다.

in Cisco Unified Communications Manager 11.5 이상에서 무선 위치 모니터링 서비스를 구성할 수 있습니다. 자세한 내용은 Cisco Unified Communications Manager 시스템 구성 설명서를 참조하십시오.

Cisco Jabber는 사용자의 위치를 모니터링하고 SSID(서비스 세트 ID) 및 BSSID (기본 서비스 세트 ID) 정보를 수집한 후, 다음을 수행하여 이 정보를 24시간마다 또는 다음과 같은 경우가 있을 때마다 Unified CM에 전달합니다.

- 현재 액세스 포인트가 변경됩니다.
- Cisco Jabber에 로그인합니다.
- 온프레미스와 모바일 및 Remote Access용 Expressway 네트워크 사이를 전환합니다.
- Cisco Jabber가 절전 모드에서 다시 시작되거나 활성 상태가 됩니다.

온프레미스 구축의 경우 값이 *true*인 EnableE911OnPremLocationPolicy 매개 변수를 사용하여 무선 위치 모니터링을 구성합니다.

모바일 및 Remote Access용 Expressway의 경우 값이 *true*인 EnableE911EdgeLocationPolicy 및 세미콜론으로 구분하여 최대 30개의 SSID 목록이 있는 E911EdgeLocationWhiteList를 사용하여 무선 위치 모니터링을 구성할 수 있습니다.

이러한 매개 변수에 대한 자세한 내용은 최신 *Cisco Jabber*용 매개 변수 참조 설명서를 참조하십시오.

인스턴트 메시지용 보안 레이블

클라이언트			
Windows	**Mac**	**iPhone** 및 **iPad**	**Android**
예	—	—	—

배포			
온프레미스	**Webex Messenger**	팀 메시징 모드	**VDI**용 **Softphone**
예	—	—	예

고객은 종종 데이터를 볼 수 있는 사람을 제한하는 데이터 처리 규칙을 가지고 있습니다. 구축에서 컴플라이언스 서버를 사용하여 인스턴트 메시지를 필터링할 수 있습니다. 릴리스 12.7에서 Jabber는 이러한 필터링을 활성화하기 위해 *XEP-0258: XMPP*의 보안 레이블 표준에 대한 지원을 포함합니다.

InstantMessageLabels 매개 변수를 사용하여 보안 레이블 카탈로그를 정의할 수 있습니다. 카탈로그가 채팅 입력 필드 위에 선택 목록을 채웁니다.

보안 레이블을 구현할 때 IM을 전송하는 일반적인 워크 플로우는 다음과 같습니다.

1. 사용자가 IM을 보낼 수 있으려면 먼저 보안 레이블을 선택해야 합니다.
2. Jabber에서 XMPP 보안 레이블을 IM에 추가합니다.
3. IM이 컴플라이언스 서버로 이동합니다.
4. 컴플라이언스 서버는 수신자가 해당 분류의 IM을 볼 수 있도록 허용하는 라우팅 규칙을 확인합니다.
   - 허용하면 컴플라이언스 서버에서 IM을 허용합니다.
   - 허용하지 않으면 컴플라이언스 서버에서 IM을 거부합니다.
5. Jabber가 채팅 창에 IM을 표시하면 텍스트 위에 보안 레이블이 표시됩니다.

InstantMessageLabels 매개 변수 사용에 대한 자세한 내용은 *Cisco Jabber*용 매개 변수 참조 설명서를 참조하십시오. 이 설정은 통합 CM 관리 또는 `jabber-config.xml` 구성 파일에서 구성할 수 있습니다.

다음 예제에서는 보안 레이블 태그의 <label> 요소를 사용하는 방법을 보여줍니다.

```
<InstantMessageLabels>
  <item selector="Classified|SECRET">
    <securitylabel xmlns='urn:xmpp: sec-label:0'>
     <displaymarking fgcolor='black' bgcolor='red'>SECRET </displaymarking>
      <label>
       <edhAttrs xmlns="https://www.surevine.com/protocol/xmpp/edh">
       <specification>2.0.2</specification>
       <version>XXXX:1.0.0</version>
       <policyRef></policyRef>
```

```
        <originator>Acme</originator>
        <custodian>Acme</custodian>
        <classification>A</classification>
        <nationalities>Acme</nationalities>
        <organisations>Acme</organisations>
        </edhAttrs>
      </label>
    </securitylabel>
  </item>
<item…> … </item>
</InstantMessageLabels>
```

이 매개 변수를 설정하면 Jabber가 구성 변경을 감지하고 사용자에게 Jabber에 다시 로그인하도록 요청합니다. 보안 레이블을 지원하지 않는 Jabber 버전을 실행 중인 장치의 경우, IM은 보안 레이블 없이 메시지의 내용을 표시합니다.