セキュリティおよびモニタリング

ログアウト非アクティビティ タイマー

Clients			
ウィンドウ	MAC	iPhone および iPad	Android
はい	はい	はい	はい

導入			
On-Premises	Webex Messenger	チームメッセージング モード	VDI 版ソフトフォン
はい	はい	はい	はい

サインアウト非アクティビティ タイマーにより、指定された時間にわたって非アクティブ状態のユーザをクライアントから自動的にサインアウトさせることができます。

モバイル クライアントでの「非アクティブ」には次の状態が含まれます。

- クライアントがバックグラウンド動作になる。
- 音声コールに関するユーザ操作がない。

この機能をモバイルクライアントでForceLogoutTimerMobileパラメータを使用して設定することができます。

デスクトップ クライアントでの「非アクティブ」には次の状態が含まれます。

- キーボードまたはマウスの操作がない。
- コール発信および応答のための接続済みアクセサリに関するユーザ操作がない。

この機能をモバイルクライアントでForceLogoutTimerMobileパラメータを使用して設定することができます。

このパラメータを設定していない場合、クライアントは自動的にサインアウトしません。

問題のレポート

Clients			
ウィンドウ	MAC	iPhone および iPad	Android
対応	—	—	—

導入			
On-Premises	Webex Messenger	チームメッセージング モード	VDI 版ソフトフォン
はい	はい	はい	はい

問題レポートをセットアップすると、クライアントの使用中に発生した問題の概要を送信できるようになります。次のように、問題レポートを送信する方法は 2 つあります。

- クライアント インターフェイスを介して問題レポートを直接送信する。
- 問題レポートをローカルに保存し、後でアップロードする。

クライアントは、HTTP POST メソッドを使用して問題レポートを送信します。POST 要求を受け入れるカスタム スクリプトを作成し、設定パラメータとして HTTP サーバ上のスクリプトの URL を指定します。ユーザは問題レポートをローカルに保存できるため、ユーザが問題レポートをアップロードできるようにするフォームを含む HTML ページを作成する必要もあります。

始める前に

環境の準備を行うには、次の手順を実行します。

1. HTTP サーバをインストールして設定します。
2. HTTP POST 要求を受け入れるカスタム スクリプトを作成します。

3. ユーザが、ローカルに保存されている問題レポートをアップロードできるHTMLページを作成します。HTML ページには、.ZIP アーカイブとして保存された問題レポートを受け入れ、カスタムスクリプトを使用して問題レポートを送信するアクションが含まれているフォームがあります。

次に、問題レポートを受け入れるフォームの例を示します。

```
<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>
```

手順

ステップ 1 HTTP サーバ上でカスタム スクリプトをホストします。

ステップ 2 設定ファイルの PrtLogServerUrl パラメータの値としてスクリプトの URL を指定します。

問題レポートの復号化

問題レポートの復号化用のコマンド ライン ツール `CiscoJabberPrtDecrypter.exe` は、インストーラに含まれており、Windowsマシンでのみ使用できます。このツールには次の引数があります。

- `--help`：ヘルプ メッセージを表示します。
- `--privatekey`：秘密キー ファイルを指定します。これはプライバシー強化メール（.pem）または個人情報交換 PKCS#12（.pfx）形式です。
- `--password`：入力された秘密キー ファイルがパスワードで保護されている場合のオプション。
- `--encryptionkey`：`file.zip.esk` など、暗号化秘密キー ファイルを指定します。
- `--encryptedfile`：`file.zip.enc` など、暗号化されたファイルを指定します。
- `--outputfile`：`decryptedfile.zip` など、出力ファイルを指定します。

始める前に

問題レポートを復号化するには、次のものが必要です。

- 暗号化を使用して問題レポートを生成したときに作成した zip ファイルに含まれる、次の 2 つのファイル
  - *file.zip.esk*：暗号化された対称キー
  - *file.zip.enc*：AES256 を使用して暗号化された元のデータ

- データの暗号化に使用した証明書の秘密キー

手順

ステップ 1 Windows でコマンド プロンプトを開きます。

ステップ 2 `C:\Program Files(x86)\Cisco Systems\CUCILync\` ディレクトリに移動します。

ステップ 3 コマンドとパラメータを入力します。

デスクトップ クライアントの例：`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`

復号化が成功すると出力ファイルが作成されます。無効なパラメータがあると復号化が失敗し、コマンド ラインにエラーが表示されます。

リモートでの PRT ログの収集

ユーザが PRT ログをアップロードするまで待機する代わりに、**Unified CM の管理**でリモートからログを生成することができます。

始める前に

この機能を使用するには、展開で Unified CM リリース 12.5.1 SU 1 以降が必要です。RemotePRTServer パラメータは、サーバに PRT ログをアップロードするためのスクリプトを指定します。

手順

ステップ 1 **[デバイス（Device）] > [電話（Phone）]** の順に選択します。

ステップ 2 ログが必要なデバイスを選択します。

ステップ 3 **選択された PRT の PRT の生成**をクリックします。

スクリプトは、PRT のログをサーバにアップロードします。

（注） Cisco Sunkist ヘッドセットからログを収集するには、ファームウェアバージョン 1.3 またはそれ以降が必要です。

リモート PRT ログコレクションのセットアップ

PRT ログをリモートで収集する前に、**Unified CM の管理**でログをアップロードするためのスクリプトを指定する必要があります。

手順

ステップ 1 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [UC サービス（UC Service）]** を選択します。

ステップ 2 **Jabber クライアント設定 (jabber-config)** の **UC サービスタイプ**で新しい UC サービスを追加します。

ステップ 3 次の値を含む **Jabber 設定パラメータ**を追加します。

- **セクション** : **ポリシー**
- **パラメータ** : **`RemotePRTServer`**
- **[値 (Value)**: アップロードスクリプトの URL。

デバイス PIN 設定

Clients			
ウィンドウ	MAC	iPhone および iPad	Android
—	—	はい	はい

導入			
On-Premises	Webex Messenger	チームメッセージングモード	VDI 版ソフトフォン
はい	はい	はい	—

Jabber はセキュアなデバイスのみに使用することを推奨します。デバイスがセキュアかどうかを確認するには、ForceDevicePin パラメータの値を **`true`**に設定します。

例：

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

デバイスがセキュアでない場合：

- Jabber は PIN を設定する通知を表示します。この通知には期限が設定されており、ユーザが 13 秒以内に [PIN 設定（SET PIN）] をタップしなかった場合は、そのユーザは Jabber からサインアウトされます。

PIN 設定オプションをタップした後、ユーザはデバイス設定に進んで、PIN または指紋認証でデバイスを保護する必要があります。

- ユーザが Jabber にサインインし、すぐに Jabber をバックグラウンドに移すと、Jabber はユーザがそのデバイスを保護したかどうかを確認します。デバイスが保護されていない場合、ユーザは Jabber からサインアウトされます。

モバイルクライアントでのバイオメトリック認証

Clients			
ウィンドウ	MAC	iPhone および iPad	Android
—	—	はい	はい

導入			
On-Premises	Webex Messenger	チームメッセージングモード	VDI 版ソフトフォン
はい	はい	はい	—

Cisco Jabber は、ユーザが安全にログインするための指紋または顔認識による認証をサポートしています。これらの認証方法を使用して、ユーザがモバイルデバイスの Cisco Jabber に迅速かつ安全にログインできることを確認してください。

指紋または顔認識による認証は、次のシナリオで使用されます。

- Android 版 Cisco Jabber ユーザが手動サインアウトや自動サインアウト後に Jabber にサインインする場合に、指紋または顔認識での認証ができます。
- iPhone および iPad 版 Cisco Jabber のユーザが手動でログアウトしたときや、その cisco jabber を使用したユーザが Cisco Jabber にログインしたときに、その Cisco Jabber にログインした場合、その Cisco Jabber にログインするには、Touch ID または顔 ID 認証を使用します。

パラメータ、localauthenticationwithbiometricsを設定することにより、Cisco Jabber のユーザがこの認証方法でサインインできるようにしてください。

このパラメータは、次のいずれかの値を使用して設定できます。

- AdminEnabled: Cisco Jabber は、指紋または顔認証を使用して、ユーザに認証するように促します。ユーザが Cisco Jabber にログインするには、バイオメトリック認証をを使用する必要があります。ただし、ユーザのデバイスがバイオメトリック機能をサポートしていない場合、ユーザはパスワードを使用してログインする必要があります。
- UserDecision (デフォルト): Cisco Jabber は、指紋または顔認識を使用して、ユーザに認証を促すメッセージを表示します。ユーザは、生体認証を使用して、Cisco Jabber にログインするかどうかを決定できます。

- AdminDisabled—Cisco Jabberは、 s 指紋や顔認識による認証を使用しません。ユーザにはプロンプトが表示されません。

認証に失敗すると、Cisco Jabberは、ユーザがログインするたびにログイン情報を入力するように求めるメッセージを表示します。

例: `<LocalAuthenticationWithBiometrics>AdminDisabled</LocalAuthenticationWithBiometrics>`

バイオメトリック認証のためのデバイス要件

この機能は、オペレーティングシステムがバイオメトリック認証をサポートしているデバイスでのみ使用できます。

サイレント モニタリングおよびコール録音

Clients			
ウィンドウ	MAC	iPhone および iPad	Android
はい	はい	はい	はい

導入			
On-Premises	Webex Messenger	チームメッセージングモード	VDI 版ソフトフォン
はい	はい	はい	はい

サイレントコール モニタリングは、Cisco Unified Communications Managerの機能です。サイレントコールモニタリングにより、スーパーバイザには通話参加者双方の声が聞こえますが、どちらの通話参加者にもスーパーバイザの声は聞こえません。

コール録音はUnified CMの機能の1つですが、これを利用すると録音サーバでエージェントの会話を記録できます。

- Cisco Jabberでは、サイレントモニタリングまたはコール録音を開始するインターフェイスを提供していません。コールをサイレントモニタリングまたは録音するための適切なソフトウェアを使用してください。
- Cisco Jabberは、現時点では、モニタリング通知トーンまたは録音通知トーンをサポートしていません。
- サイレントモニタリング機能およびコール録音機能のみ使用できます。Jabberは、割り込み、ウィスパー コーチングなど、その他の機能をサポートしていません。

サーバ要件:

- Ciscoでは、サイレントモニタリングおよび通話録音は、オンプレミス展開に対してのみサポートいたします。

- Windows 版 Cisco Jabber と Mac 版 Cisco Jabber には、Cisco Unified Communications Manager 9.x 以降のバージョンが必要です。
- iPhone、iPad および Android 版 Cisco Jabber では、Cisco Unified Communications Manager 11.0 以降が必要です。

Unified CM の一部のリリースでは、デバイスパッケージでモニタリングおよび録音機能を有効にする必要があります。**組み込みブリッジ**フィールドが、デバイスの**電話機の設定**ウィンドウで可用性があることを確認してください。このフィールドが使用できない場合は、最新のデバイスパッケージをダウンロードして適用してください。

サイレントモニタリングまたはコール録音の設定方法の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

オンデマンド レコーディング

Clients			
ウィンドウ	MAC	iPhone および iPad	Android
はい	はい	—	—

導入			
On-Premises	Webex Messenger	チームメッセージングモード	VDI 版ソフトフォン
はい	はい	はい	はい

すべての通話を記録するのではなく、ユーザに対して、いつ録音するのかを柔軟性に選択することができます。

ユニファイドコミュニケーション マネージャーリリース 12.5 (1) 以降の展開では、Jabber の組み込みブリッジを使用した統一 CM のオンデマンド録音をサポートしています (BiB)。Cisco Unified CM 管理で、**デバイス** > **電話機** > **録音オプション(選択的着信**] をオンにしてこの機能を有効にします。また、クラスタ全体または個々の電話機に対して、BiB を有効にします。

この機能を有効にすると、[コール制御 (call control)] メニューには、ユーザがいつでも録音を開始および停止するための**レコード**オプションが含まれます。

アクセスできるレコーダー間の優先順位

デフォルトでは、通話録音の外部ブリッジをセットアップした会議通話に参加すると、Jabber が外部ブリッジで録音を行うようになっています。ただし、一部の組織はコンプライアンス目的ですべての録音を希望して Jabber BiB を使用する場合があります。このような使用例では、Prefer_BIB_recorderパラメータを使用して Jabber BIB での録音をエンフォーサします。

Cisco Jabber 分析テレメトリ

Clients			
ウィンドウ	MAC	iPhone および iPad	Android
はい	はい	はい	はい

導入			
On-Premises	Webex Messenger	チームメッセージングモード	VDI 版ソフトフォン
はい	はい	はい	はい

ユーザ エクスペリエンスと製品パフォーマンスを向上させるために、Cisco Jabber は、個人識別が不可能な利用状況とパフォーマンスに関するデータを収集してシスコに送信する場合があります。収集されたデータは、シスコによって、Jabber クライアントがどのように使用され、どのように役立っているかに関する傾向を把握するために使用されます。

テレメトリ機能を使用するには、`GoDaddy Class 2 Certification Authority Root Certificate` という名前のルート証明書をインストールする必要があります。テレメトリ サーバ証明書名は "metrics-a.wbx2.com" です。この証明書名に関する警告を解決するには、必要な GoDaddy 証明書をインストールします。証明書の詳細については、『Planning Guide』を参照してください。

デフォルトで、テレメトリ データはオンになっています。次のテレメトリ パラメータを設定できます。

- Telemetry_Enabled：分析データを収集するかどうかを指定します。デフォルト値は true です。
- TelemetryEnabledOverCellularData：分析データを携帯データ ネットワークと Wi-Fi 経由で送信する（true）のか、WiFi 経由のみで送信する（false）のかを指定します。デフォルト値は true です。
- TelemetryCustomerID：このオプション パラメータは分析情報の送信元を指定します。この ID は、個別の顧客を明示的に識別する文字列にすることも、顧客を識別せずに共通の送信元を識別する文字列にすることもできます。*Global Unique Identifier*（GUID）を生成するツールを使用して 36 文字の一意の ID を作成するか、逆ドメイン名を使用することをお勧めします。

（注） テレメトリを無効にするオプションは、Jabber チームメッセージングモードのユーザは使用できません。

これらのパラメータの詳細については、『*Parameters Reference Guide*』を参照してください。

Cisco の分析データの処理方法については、https://www.cisco.com/c/en/us/about/legal/privacy-full.html を参照してください。

Webex Control Hub の Jabber 分析

Clients			
ウィンドウ	MAC	iPhone および iPad	Android
はい	はい	はい	はい

導入			
On-Premises	Webex Messenger	チームメッセージングモード	VDI 版ソフトフォン
はい	はい	—	—

Jabber 分析には、Webex Control Hub を介してアクセスできるようになりました。ユーザデータは、**分析**の**Jabber**タブからでクセスできます。Jabber 分析では、次のような、重要なパフォーマンス指標 (傾向含む) を提供します。

- アクティブ ユーザ
- メッセージが送信されました
- Jabber で作成または受信した通話
- Jabber のスクリーン共有

Jabber 分析にアクセスするには、Webex Control Hub をセットアップする必要があります。これらのパラメータを`jabber-config.xml`で設定します。

- TelemetryEnabled true
- TelemetryEnabledOverCellularData true へ
- 管理ハブから orgid への TelemetryCustomerID

この機能は、次の展開モードで使用できます。

- オンプレミスと完全な UC
- オンプレミスの IM のみ
- オンプレミスの電話専用
- Jabber と Webex Messenger

（注） これは、Jabber の展開に影響を与える Webex Control Hub の新機能です。この機能には、Jabber の任意のリリースでアクセスできます。

ワイヤレスロケーション モニタリングサービス

適用対象: すべてのクライアント

Clients			
ウィンドウ	MAC	iPhone および iPad	Android
はい	はい	はい	はい

導入			
On-Premises	Webex Messenger	チームメッセージングモード	VDI 版ソフトフォン
はい	はい	はい	はい

ワイヤレスロケーション モニタリングサービス: 社内ネットワークにアクセスしている Cisco Jabber ユーザの物理的な場所を判断できます。この情報は、Cisco Unified Communications Manager に格納されます。

Cisco Unified Communications Manager 11.5 以降のワイヤレスロケーション モニタリングサービスの設定については、『Cisco Unified Communications Manager 用システムコンフィギュレーション ガイド』を参照してください。

Cisco Jabber は、ユーザの位置情報をモニタリングし、サービスセット ID (SSID) と基本サービスセット ID (BSSID) の情報を収集して、この情報を少なくとも 24 時間ごとにまたは次の時間ごとに、Unified CM に送信します。

- その現在のアクセスポイントは変更されます。
- Cisco Jabber にサインインします。
- モバイルおよび Remote Access ネットワークのオンプレミスおよび Expressway 間で切り替えられます。
- Cisco Jabber はスリープ状態から再開するか、アクティブになります。

オンプレミスの展開の場合は、値*true*を使用するEnableE911OnPremLocationPolicyパラメータを使用してワイヤレスロケーション モニタリングを設定します。

モバイルおよび Remote Access 展開の Expressway の場合は、最大 30 SSID までのリストにある値*true*とE911EdgeLocationWhiteListでEnableE911EdgeLocationPolicyを使用して、セミコロンで区切られたワイヤレスロケーション モニタリングを設定します。

パラメータの詳細については、最新の『*Parameters Reference Guide for Cisco Jabber*』を参照してください。

インスタントメッセージ用のセキュリティラベル

Clients			
ウィンドウ	MAC	iPhone および iPad	Android
対応	—	—	—

導入			
On-Premises	Webex Messenger	チームメッセージングモード	VDI 版ソフトフォン
対応	—	—	あり

閲覧できるユーザやデータを制限するデータ処理ルールが顧客側に用意されていることはよくあります。展開する場合は、コンプライアンスサーバを使用してインスタントメッセージをフィルタリングしてください。リリース 12.7 では、Jabber は *XEP-0258: XMPP* のセキュリティラベル標準規格をサポートし、これらのフィルタリングが有効化されています。

InstantMessageLabelsパラメータを使用して、セキュリティラベルのカタログを定義してください。カタログが、チャット入力フィールド上の選択リストに入力します。

セキュリティラベルを実装する場合、IM 送信に関して一般的なワークフローは次のようになります。

1. IM を送信する前に、ユーザはセキュリティラベルを選択する必要があります。
2. Jabber は、IM に XMPP セキュリティラベルを付加します。
3. IM は、コンプライアンスサーバに送信されます。
4. コンプライアンスサーバは、そのルーティングルールによって受信者がその分類の IM を表示できるかどうかをチェックします。
   - [はい (yes)] の場合、コンプライアンスサーバは IM を許可します。
   - [いいえ (no)] の場合、コンプライアンスサーバは IM を拒否します。
5. Jabber でチャットウィンドウに IM が表示される場合、セキュリティラベルがテキストの上に表示されます。

InstandMessageLabels パラメータの使用方法の詳細については、 *Cisco Jabber* のパラメータリファレンス ガイドを参照してください。この設定は、Unified CM Administration または `jabber-config.xml`設定ファイルで構成できます。

次の例は、 <label>セキュリティラベルの要素の使用方法を示しています。

```
<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>
```

このパラメータを設定すると、Jabber は設定の変更を検出し、Jabber にもう一度サインインするようユーザに要求します。セキュリティラベルをサポートしていないバージョンの Jabber を実行しているデバイスの場合、IM はセキュリティラベルなしでメッセージの内容を表示します。