安全和监控

注销非活动计时器

客户端			
Windows	**Mac**	**iPhone 和 iPad**	**Android**
是	是	是	是

部署			
场内	**Webex Messenger**	**组消息模式**	**VDI 软终端**
是	是	是	是

注销非活动计时器允许您将处于非活动状态达到指定时长的用户自动从客户端注销。

移动客户端上的非活动状态包括：

- 客户端进入后台。
- 语音呼叫无用户交互。

您可以使用 ForceLogoutTimerMobile 参数在移动客户端上配置此功能。

桌面客户端上的非活动状态包括：

- 未使用键盘或鼠标。
- 没有用户在连接的配件上拨打和应答呼叫。

您可以使用 ForceLogoutTimerDesktop 参数在桌面客户端上配置此功能。

如果不设置此参数，客户端不会自动注销。

问题报告

客户端			
Windows	**Mac**	**iPhone 和 iPad**	**Android**
支持	—	—	—

部署			
场内	**Webex Messenger**	**组消息模式**	**VDI 软终端**
是	是	是	是

设置问题报告可让用户发送使用客户端时遇到的问题摘要。有以下两种提交问题报告的方法：

- 用户通过客户端界面直接提交问题报告。
- 用户在本地保存问题报告，然后稍后上传。

客户端使用 HTTP POST 方法提交问题报告。创建自定义脚本以接受 POST 请求，并在 HTTP 服务器上指定脚本的URL作为配置参数。因为用户只能在本地保存问题报告，所以您还应该使用表格创建 HTML 页面，以便让用户上传问题报告。

开始之前

完成以下步骤以准备环境：

1. 安装和配置 HTTP 服务器。
2. 创建自定义脚本以接受 HTTP POST 请求。
3. 创建 HTML 页面以使用户能够上传本地保存的问题报告。您的 HTML 页面应包含接受问题报告另存为 `.ZIP` 存档的表单，并包含使用自定义脚本发布问题报告的操作。

以下是接受问题报告的示例格式：

```
<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>
```

过程

步骤 1 在 HTTP 服务器上托管您的自定义脚本。

步骤 2 在配置文件中指定脚本的 URL 作为 PrtLogServerUrl 参数的值。

解密问题报告

用于解密问题报告的命令行工具 `CiscoJabberPrtDecrypter.exe` 仅在 Windows 计算机上可用并包含在安装程序中。该工具有以下参数：

- `--help` — 显示帮助消息。
- `--privatekey` — 指定私钥文件，此项为隐私增强型邮件 (.pem) 或个人信息交换 PKCS#12 (.pfx) 格式。
- `--password` —（可选）如果输入私钥文件受密码保护。
- `--encryptionkey`-指定加密密钥文件，例如`esk`。
- `--encryptedfile` — 指定加密文件，例如 `file.zip.enc`。
- `--outputfile` — 指定输出文件，例如 `decryptedfile.zip`。

开始之前

要解密问题报告，您需要以下各项：

- 当您使用加密生成问题报告时，来自所创建 zip 文件的两个文件：
  - *file.zip.esk* — 加密的对称密钥。
  - *file.zip.enc* — 使用 AES256 加密的原始数据。
- 用于加密数据的证书的私钥。

过程

步骤 1 在 Windows 中打开命令提示符。

步骤 2 导航到 `C:\Program Files(x86)\Cisco Systems\CUCILync\` 目录。

步骤 3 输入命令和您的参数。

桌面客户端的示例：`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`

如果解密成功，则会创建输出文件。如果存在无效的参数，则解密失败并在命令行中显示错误。

远程收集 PRT 日志

无需等待用户上传 PRT 日志，就可以在 **Unified CM 管理**中远程生成日志。

开始之前

要使用此功能，您的部署需要 Unified CM 版本 12.5.1 SU 1 或更高版本。RemotePRTServer 参数指定将 PRT 日志上传到服务器的脚本。

过程

步骤 1 选择**设备** > **电话**。

步骤 2 选择需要其日志的设备。

步骤 3 单击**生成所选项的 PRT**。

脚本会将 PRT 日志上传到您的服务器。

注释 要从 Cisco Sunkist 头戴式耳机收集日志，您需要 1.3 或更高版本的固件。

设置以远程收集 PRT 日志

必须先在 **Unified CM 管理**中指定上传日志的脚本，然后才能远程收集 PRT 日志。

过程

步骤 1 选择**用户管理** > **用户设置** > **UC 服务**。

步骤 2 添加新的 UC 服务，**UC 服务类型**为 **Jabber 客户端配置 (jabber-config.xml)**。

步骤 3 使用以下值添加 **Jabber 配置参数**：

- **部分**—**策略**
- **参数**—**RemotePRTServer**
- **值**—上传脚本的 URL。

设置设备个人识别码

客户端			
Windows	**Mac**	**iPhone 和 iPad**	**Android**
—	—	是	是

部署			
场内	**Webex Messenger**	组消息模式	**VDI 软终端**
是	是	是	—

我们建议您仅在安全设备上使用 Jabber。要检查设备是否安全，请将 ForceDevicePin 参数配置为值 **`true`**。

示例：

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

如果设备未受保护：

- 则 Jabber 会显示设置个人识别码的通知。这是一个时间限制通知，如果用户没有在 13 秒内点击**设置个人识别码**，则用户将从 Jabber 注销。

  用户点击**设置个人识别码**选项后，用户必须转到设备设置并使用个人识别码或指纹验证来保护设备安全。

- 如果用户登录 Jabber，然后立即将其置于后台，则 Jabber 会检查用户是否已对该设备进行保护。如果设备未受保护，则用户将从 Jabber 注销。

移动客户端上的生物特征验证

客户端			
Windows	**Mac**	**iPhone 和 iPad**	**Android**
—	—	是	是

部署			
场内	**Webex Messenger**	组消息模式	**VDI 软终端**
是	是	是	—

Cisco Jabber 支持 指纹或面部识别验证以使用户安全登录。您可以使用这些验证方法确保用户能够快速、安全地登录其移动设备上的 Cisco Jabber。

在以下情况下使用指纹或面部识别验证：

- 如果 Cisco Jabber Android 版本用户在手动或自动注销后登录 Jabber，可以使用指纹或面部识别验证。
- Cisco Jabber iPhone 和 iPad 版本用户在手动注销或自动注销后登录 Cisco Jabber 时，只能使用 Touch ID 或 Face ID 验证登录 Cisco Jabber。

通过配置参数 LocalAuthenticationWithBiometrics，您可使用此验证允许 Cisco Jabber 用户登录。

您可使用以下任何值配置此参数：

- AdminEnabled—Cisco Jabber 提示用户使用指纹或面部识别进行验证。用户必须使用生物识别验证来登录 Cisco Jabber。但是，如果用户的设备不支持生物识别功能，则用户必须使用其密码登录。
- UserDecision（默认值）— Cisco Jabber 提示用户使用指纹或面部识别进行验证。用户可以决定是否要使用生物识别身份验证来登录 Cisco Jabber。
- AdminDisabled — Cisco Jabber 不使用指纹或面部识别验证。不会向用户显示任何提示。

如果身份验证失败，Cisco Jabber 会在每次登录时提示用户输入其凭证。

示例：`<LocalAuthenticationWithBiometrics>AdminDisabled</LocalAuthenticationWithBiometrics>`

生物特征验证的设备要求

此功能仅在操作系统支持生物特征验证的设备上可用。

静默监听和呼叫录音

客户端			
Windows	**Mac**	**iPhone 和 iPad**	**Android**
是	是	是	是

部署			
场内	**Webex Messenger**	**组消息模式**	**VDI 软终端**
是	是	是	是

静默呼叫监控是 Cisco Unified Communications Manager 的一项功能。借助它，主管可以听到通话双方的声音，但他们都听不到主管的声音。

呼叫录音是一项 Unified CM 功能，让录音服务器能够存档座席对话。

- Jabber 不提供开始静默监听和呼叫录音的任何界面。使用适当的软件静默监听或对呼叫进行录音。
- Jabber 当前不支持监听通知音或录音通知音。
- 您只能使用静默监听和呼叫录音功能。Jabber 不支持其他功能，例如，插入或密谈指导。

服务器要求：

- 我们只对内部部署支持静默监听和呼叫录音。
- Cisco Jabber Windows 版本和 Cisco Jabber Mac 版本需要 Cisco Unified Communications Manager 9.x 或更高版本。
- Cisco Jabber iPhone 和 iPad 版本及 Cisco Jabber Android 版本需要 Cisco Unified Communications Manager 11.0 或更高版本。

某些版本的 Unified CM 需要设备包才能启用监听和录音功能。验证**内置桥**字段在设备的**电话配置**窗口中是否可用。如果该字段不可用，请下载并应用最新的设备包。

有关如何配置静默监听或呼叫录音的详细信息，请参阅《*Cisco Unified Communications Manager* 功能配置指南》。

按需录音

客户端			
Windows	**Mac**	**iPhone 和 iPad**	**Android**
是	是	—	—

部署			
场内	**Webex Messenger**	**组消息模式**	**VDI 软终端**
是	是	是	是

您无需记录每个呼叫，而可让用户在想要录音时选择灵活。

在使用 Unified Communications Manager 版本 12.5(1) 和更高版本的部署中，Jabber 可以使用 Jabber 的内置桥 (BiB) 支持 Unified CM 的按需录音。在 Cisco Unified CM 管理中，将**设备** > **电话** > **录音选项**设置为**启用选择性呼叫录音**以启用该功能。此外，还可以在群集范围内或单个电话上启用 BiB。

启用此功能后，呼叫控制菜单包括用户在任何时候开始和停止录音的**录制**选项。

可用记录器之间的首选项

默认情况下，如果用户加入具有设置为对呼叫进行录音的外部网桥的会议呼叫，Jabber 将使用该外部网桥进行录音。不过，出于合规性原因，有些组织可能希望使用 Jabber BiB 的所有录音。在这种情况下，使用 Prefer_BIB_recorder 参数在 Jabber BiB 上强制录音。

使用 Cisco Jabber Analytics 进行遥测

客户端			
Windows	**Mac**	**iPhone 和 iPad**	**Android**
是	是	是	是

部署			
场内	**Webex Messenger**	**组消息模式**	**VDI 软终端**
是	是	是	是

为改善您的体验和产品性能，Cisco Jabber 可能会收集非个人识别使用和性能数据并发送给 Cisco。Cisco 使用聚合数据了解 Jabber 客户端的使用方式及其执行方式的趋势。

您必须安装以下根证书以使用遥测功能：GoDaddy 2 类证书颁发机构根证书。遥测服务器证书名称为 "metrics-a.wbx2.com"。要解决关于此证书名称的任何警告，请安装所需的 GoDaddy 证书。有关证书的详细信息，请参阅规划指南。

默认情况下，遥测数据处于打开状态。您可以配置以下遥测参数：

- Telemetry_Enabled — 指定是否收集分析数据。默认值为 true。
- TelemetryEnabledOverCellularData — 指定分析数据是通过蜂窝数据和 Wi-Fi (true) 还是仅 Wi-Fi only (false) 发送。默认值为 true。
- TelemetryCustomerID — 此可选参数指定分析信息的来源。此 ID 可以是显式标识单个客户的字符串，也可以是标识通用来源而不标识客户的字符串。我们建议使用生成全局唯一标识符 (GUID) 的工具创建 36 个字符的唯一标识符，或者使用反向域名。

注释 用于禁用遥测的选项不适用于 Jabber 组消息模式用户。

有关这些参数的详细信息，请参阅《参数参考指南》。

您可以在以下网址找到有关 Cisco 如何处理分析数据的详细信息：https://www.cisco.com/c/en/us/about/legal/privacy-full.html。

Webex Control Hub 中的 Jabber 分析

客户端			
Windows	**Mac**	**iPhone 和 iPad**	**Android**
是	是	是	是

部署			
场内	Webex Messenger	组消息模式	VDI 软终端
是	是	—	—

您现在可以通过 Webex Control Hub 访问 Jabber 分析信息。您的数据将显示在**分析**页面的 **Jabber** 选项卡上。Jabber 分析提供趋势信息的关键绩效指标，例如：

- 活跃用户
- 发送的留言
- 从 Jabber 发出或接收的呼叫
- 来自 Jabber 的屏幕共享

要访问 Jabber 分析，必须设置好 Webex Control Hub。在 `jabber-config.xml` 中设置以下参数：

- 将 TelemetryEnabled 设置为 true
- 将 TelemetryEnabledOverCellularData 设置为 true
- 从 Control Hub 将 TelemetryCustomerID 设置为您的 OrgID

此功能适用于以下部署模式：

- 内部，完全 UC
- 内部，仅 IM
- 内部，仅电话
- 使用 Webex Messenger 的 Jabber

注释 这是 Webex Control Hub 中新增的功能，会影响 Jabber 部署。您可以访问任意版本的 Jabber 中的这项功能。

无线位置监控服务

适用于：所有客户端

客户端			
Windows	Mac	iPhone 和 iPad	Android
是	是	是	是

部署			
场内	Webex Messenger	组消息模式	VDI 软终端
是	是	是	是

无线位置监控服务可让您确定 Cisco Jabber 用户连接到公司网络的物理位置。此信息存储在 Cisco Unified Communications Manager 中。

您可以在 Cisco Unified Communications Manager 11.5 或更高版本中配置无线位置监控服务，有关详细信息，请参阅《Cisco Unified Communications Manager 系统配置指南》。

Cisco Jabber 监控用户的位置，收集服务集 ID (SSID) 和基本服务集 ID (BSSID) 信息，然后至少每隔 24 小时或在以下情况下将此信息发送给 Unified CM：

- 其当前接入点将发生变化时。
- 用户登录 Cisco Jabber 时。
- 用户在内部和 Expressway for Mobile and Remote Access 网络之间切换时。
- Cisco Jabber 从睡眠状态恢复或处于活动状态。

对于内部部署，使用 EnableE911OnPremLocationPolicy 参数及 *true* 值配置无线位置监控。

对于 Expressway for Mobile and Remote Access 部署，您可以使用 EnableE911EdgeLocationPolicy 及值 *true* 和 E911EdgeLocationWhiteList 及最多 30 个 SSID（用分号分隔）的列表配置无线位置监控。

有关这些参数的更多详细信息，请参阅最新的《*Cisco Jabber* 参数参考指南》。

即时消息的安全标签

客户端			
Windows	Mac	iPhone 和 iPad	Android
支持	—	—	—

部署			
场内	Webex Messenger	组消息模式	VDI 软终端
支持	—	—	是

客户通常有限制哪些用户可以查看哪些数据的数据处理规则。您的部署可以使用合规服务器过滤即时消息。从版本 12.7 起，Jabber 包括对 *XEP-0258*：*XMPP* 中的安全标签标准的支持以启用这类过滤。

您可以使用 InstantMessageLabels 参数定义安全标签的目录。该目录填充聊天输入字段上方的选择列表。

当您实施安全标签时，发送 IM 的常规工作流程如下：

1. 用户必须先选择安全标签，然后才能发送其 IM。
2. Jabber 会将 XMPP 安全标签附加到 IM。
3. IM 会转到合规服务器。
4. 合规服务器将检查其路由规则是否允许接收方查看具有该类别的 IM：
   - 如果是，则合规服务器允许 IM。
   - 如果不是，则合规服务器拒绝 IM。
5. 当 Jabber 在聊天窗口中显示 IM 时，安全标签将在文本上方显示。

有关使用 InstantMessageLabels 参数的详细信息，请参阅《*Cisco Jabber* 参数参考指南》。您可以在 Unified CM 管理或 `jabber-config.xml` 配置文件中配置此设置。

以下示例显示如何在安全标签标记中使用 <label>元素：

```
<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>
```

设置此参数后，Jabber 会检测配置更改，并要求用户重新登录 Jabber。对于在不支持安全标签的 Jabber 版本上运行的设备，IM 会显示不带安全标签的消息内容。