

ADOBE® CONNECT™ ENTERPRISE SERVER 6

SSL 配置指南



© 2006 Adobe Systems Incorporated。保留所有权利。

适用于 Windows® 的 Adobe® Connect™ Enterprise Server 6 SSL 配置指南

如果本指南是与包含最终用户许可协议的软件一起分发，则本指南以及其中所说明的软件受许可协议的约束，只能在符合许可协议中所述的条件下才可使用和复制。除了许可协议中所允许的范围外，未经 Adobe Systems Incorporated 事先书面同意，不得将本指南的任何部分进行复制、存储在检索系统中、或以任何形式或手段（电子、机械、录制等等）传送。请注意本指南的内容受版权法的保护，即使其不是与包含最终用户许可协议的软件一起分发。

本指南的内容仅供参考，以后若有更改，恕不另行通知，不应将此理解为 Adobe Systems Incorporated 的责任。Adobe Systems Incorporated 不需对可能出现在本文档包含的信息内容中的错误承担任何责任或义务。

请记住，您准备纳入您项目中的现存的插图或图像可能受版权法保护。未经授权将这些材料合并到您的新工作中可能将侵犯版权所有者的权益。请确保已从版权所有处获取了所需的许可。

样本模板中对任何公司名称的提及只是为了进行演示，而并非指代任何实际的组织。

Adobe、Adobe 标志、Acrobat、Adobe Connect、Adobe Press、Breeze、Flash Media Server、Flash Player 和 JRun 是 Adobe Systems Incorporated 在美国和 / 或其他国家（地区）的注册商标或商标。

IBM 是 International Business Machines Corporation 在美国和 / 或其他国家（地区）的商标。Linux 是 Linus Torvalds 在美国和其他国家（地区）的注册商标。Macintosh 是 Apple Computer, Inc. 在美国和其他国家（地区）注册的商标。Microsoft、Windows 和 Windows Server 是 Microsoft Corporation 在美国和 / 或其他国家（地区）的注册商标或商标。Solaris 和 Sun 是 Sun Microsystems, Inc. 在美国和其他国家（地区）的商标或注册商标。UNIX 是 The Open Group 在美国和其他国家（地区）的注册商标。所有其他商标均为其各自所有者拥有。

美国政府最终用户请注意 本软件和文档都是 48 C.F.R. §2.101 所定义的“商品”，由 48 C.F.R. §12.212 或 48 C.F.R. §227.7202（以适用者为准）定义的“商品计算机软件”和“商品计算机软件文档”构成。与 48 C.F.R. 12.212 或 48 C.F.R.227.7202-1 至 227.7202-4 一致（凡适用），这个商用计算机软件和商用计算机文档许可给美国政府最终用户：(A) 只作为商用品 (B) 所授予的权利与遵守这个软件的 Adobe 标准商业协议中所述条款和条件的所有其它最终用户的权利相同。根据美国版权法保留未发表权利。Adobe 同意遵守所有适用的有关机会均等的法律，包括（如果适当）修订的 Executive Order 11246，1974 年 Vietnam Era Veterans Readjustment Assistance Act (38 USC 4212) 第 402 款和修订的 1973 年 Rehabilitation Act 第 503 款的规定，以及 41 CFR 的第 60-1 至 60-60、60-250 和 60-741 各节的规定。前一句中提到的确认性行动条款和规章可以引用至本协议中合并使用。

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

目录

第 1 章 :SSL 配置指南

SSL 配置准备工作	1
为 Connect Enterprise Server 配置 SSL	2
SSL 配置参考	7

第 1 章 : SSL 配置指南

您可以对 SSL 进行配置，以便为 Adobe® Connect™ Enterprise Server 和 Adobe Connect Edge Server 建立客户端与服务端之间的安全连接。

SSL 配置准备工作

关于 SSL 支持

Connect Enterprise Server 6 由两台服务器组成: Adobe 的 Macromedia® Flash® Media Server 和 Connect Enterprise 应用程序服务器。Flash Media Server 也称为会议服务器，因为它负责处理客户端与 Adobe® Acrobat® Connect™ Professional 会议之间的实时 RTMP 连接。Connect Enterprise 应用程序服务器负责处理客户端与 Connect Enterprise 应用程序逻辑之间的 HTTP 连接。默认情况下，Connect Enterprise Server 使用 443 端口进行加密通信。

您可以为应用程序服务器和 / 或会议服务器配置 SSL:

基于硬件的解决方案 使用 SSL 加速器以获得可靠的 SSL 配置。

您必须单独购买 SSL 加速器。Adobe 确认 Connect Enterprise Server 支持以下 SSL 硬件加速器: F5 Big-IP 1000、Cisco Catalyst 6590 Switch 和 Radware T100。

基于软件的解决方案 利用 Connect Enterprise Server 本身对 SSL 的支持。

注: Microsoft® Windows® 98 不支持 SSL。

Connect Enterprise Server 使用 HTTP CONNECT 方法来请求 SSL 连接。为确保 Acrobat Connect 会议能与客户端建立安全连接，而且 RTMP 不会越过 HTTP/HTTPS 进行连接，请确保代理服务器允许客户端使用 CONNECT 方法。

要获取 SSL 配置方面的帮助，请访问 Adobe 支持网站，网址为 www.adobe.com/go/connect_licensed_programs_cn。

使用证书

SSL 证书的作用是验证服务器对客户端的身份。

为保护会议服务器连接 (RTMP) 和应用程序服务器连接 (HTTP)，您必须有两个 SSL 证书，每个服务器分别有一个证书。若要为承载 Connect Enterprise Server 的计算机集群配置 SSL，则每台会议服务器都必须有一个 SSL 证书，但所有应用程序服务器可以共用一个证书。

例如，若要在同一台服务器上同时保护会议服务器连接和应用程序服务器连接，则需要两个 SSL 证书。若要在由三台服务器组成的计算机集群上同时保护会议服务器连接和应用程序服务器连接，则需要四个 SSL 证书 — 一个用于应用程序服务器，三个用于会议服务器。

获取证书

❖ 请联系证书颁发机构，即确认申请者身份的可信任的第三方机构。(Connect Enterprise 不支持自签名证书。)

证书颁发机构会要求您生成 SSL 证书签名请求 (CSR) 文件。CSR 是一个数字文件，您需要将此文件发送给证书颁发机构，以将其签署到 SSL 证书中。此文件中包含您的单位的相关信息，以及与 SSL 证书相关的 FQDN (完全限定的域名)。有关生成 CSR 的说明，请与证书颁发机构联系。

重要说明: 请将 SSL 证书的口令存放在安全且方便访问的位置。

安装证书

❖ 请将 PEM 格式的 SSL 证书安装在 Connect Enterprise Server 的根文件夹 (默认位置为 c:\breeze)。

如果从证书颁发机构收到的是 CRT 文件，您可以重命名该文件，将其文件扩展名改为 .pem。

注: 您必须有一个公钥 / 私钥文件。

为 Connect Enterprise Server 配置 SSL

配置基于软件的 SSL

通过配置基于软件的 SSL，您可以保护应用程序服务器 (HTTP) 和 / 或会议服务器 (RTMP)。您必须配置 DNS 服务器。在完成配置后，最好对配置进行测试。

配置 DNS 服务器

❖ 为要保护的服务器创建 DNS 条目。

因为 SSL 证书与名称相关，而与 IP 地址无关，所以需要为要保护的每台服务器定义 FQDN（例如 application.example.com 和 meeting1.example.com）。

注：计算机集群中的所有应用程序服务器可以共用一个 SSL 证书，但每台会议服务器必须有单独的 SSL 证书。

保护会议服务器和应用程序服务器

1 打开位于 [root_install_dir]\comserv\win32\conf_defaultRoot_ 的 Adaptor.xml 文件，并在其他位置保存一个备份副本。

2 在 Adaptor.xml 原始文件的 <Adaptor></Adaptor> 标签内插入以下代码（将斜体代码替换为您自己的相应值）：

```
<SSL>
  <Edge name="meetingserver">
    <SSLServerCtx>
      <SSLCertificateFile>[root_install_dir]\sslMeetingServer.pem</SSLCertificateFile>
      <SSLCertificateKeyFile type="PEM">[root_install_dir]\sslMeetingServer.pem</SSLCertificateKeyFile>
      <SSLPassPhrase>my passphrase</SSLPassPhrase>
      <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
      <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
  </Edge>
  <Edge name="applicationserver">
    <SSLServerCtx>
      <SSLCertificateFile>[root_install_dir]\sslAppServer.pem</SSLCertificateFile>
      <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslAppServer.pem</SSLCertificateKeyFile>
      <SSLPassPhrase>my passphrase</SSLPassPhrase>
      <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
      <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
  </Edge>
</SSL>
```

3 找到 Adaptor.xml 文件中的以下代码行：

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 将步骤 3 中的代码替换为以下代码：

```
<HostPort name="meetingserver" ctl_channel=":19350">meetingServerIP:-443</HostPort>
<HostPort name="applicationserver" ctl_channel=":19351">appServerIP:-443</HostPort>
```

5 保存 Adaptor.xml 文件。

6（可选）在网络浏览器中打开 Adaptor.xml 文件以验证语法。

如果浏览器报错，请更正错误，然后在网络浏览器中重新打开此文件。重复此步骤，直至文件有效。

7 打开位于安装根目录（默认位置为 c:\breeze）中的 custom.ini 文件，并在其他位置保存一个备份副本。

8 在 custom.ini 文件中插入以下代码，但不要替换或删除任何现有文本：

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

9 保存 `custom.ini` 文件。

10 打开位于 `[root_install_dir]\comserv\win32\conf_defaultRoot_defaultVHost_` 的 `VHost.xml` 文件，并在其他位置保存一个备份副本。

11 找到 `VHost.xml` 文件中的以下代码行：

```
<RouteEntry></RouteEntry>
```

12 将步骤 11 中的代码行替换为以下代码：

```
<RouteEntry protocol="rtmp">*:*:*:${ORIGIN_PORT}</RouteEntry>
```

13 保存 `VHost.xml` 文件。

14 (可选) 在网络浏览器中打开 `VHost.xml` 文件以验证语法。

15 重新启动 Adobe Connect Enterprise Server：

a 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“停止 Adobe Connect Enterprise Server”。

b 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“停止 Adobe Connect Meeting Server”。

c 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“启动 Adobe Connect Meeting Server”。

d 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“启动 Adobe Connect Enterprise Server”。

16 打开应用程序管理控制台 (打开网址 `http://localhost:8510/console`, 或选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“配置 Adobe Connect Enterprise Server”)。

17 在“应用程序设置”屏幕上，选择“服务器设置”，并执行以下任一操作：

a 在“Connect Enterprise 主机”框中输入 Connect Enterprise 帐户的 FQDN。

b 在“主机映射外部名称”框中输入 Connect Enterprise 会议服务器的 FQDN。

只保护应用程序服务器

1 打开位于 `[root_install_dir]\comserv\win32\conf_defaultRoot_` 的 `Adaptor.xml` 文件，并在其他位置保存一个备份副本。

2 在 `Adaptor.xml` 原始文件的 `<Adaptor></Adaptor>` 标签内插入以下代码 (将斜体代码替换为您自己的相应值)：

```
<SSL>
  <Edge name="applicationserver">
    <SSLServerCtx>
      <SSLCertificateFile>[root_install_dir]\sslAppServer.pem</SSLCertificateFile>
      <SSLCertificateKeyFile
type="PEM">[root_install_dir]\sslAppServer.pem</SSLCertificateKeyFile>
      <SSLPassPhrase>mypassphrase</SSLPassPhrase>
      <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
      <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
  </Edge>
</SSL>
```

3 找到 `Adaptor.xml` 文件中的以下代码行：

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 在步骤 3 的代码行下面添加以下代码：

```
<HostPort name="applicationserver" ctl_channel=":19351">:-443</HostPort>
```

5 保存 `Adaptor.xml` 文件。

6 (可选) 在网络浏览器中打开 `Adaptor.xml` 文件以验证语法。

如果浏览器报错，请更正错误，然后在网络浏览器中重新打开此文件。重复此步骤，直至文件有效。

7 打开位于安装根目录 (默认位置为 `c:\breeze`) 中的 `custom.ini` 文件，并在其他位置保存一个备份副本。

8 在 `custom.ini` 文件中插入以下代码，但不要替换或删除任何现有文本：

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
```

9 保存 `custom.ini` 文件。

10 重新启动 Adobe Connect Enterprise Server:

- a 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“停止 Adobe Connect Enterprise Server”。
- b 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“停止 Adobe Connect Meeting Server”。
- c 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“启动 Adobe Connect Meeting Server”。
- d 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“启动 Adobe Connect Enterprise Server”。

只保护会议服务器

1 打开位于 `[root_install_dir]\comserv\win32\conf_defaultRoot_` 的 `Adaptor.xml` 文件，并在其他位置保存一个备份副本。

2 在 `Adaptor.xml` 原始文件的 `<Adaptor></Adaptor>` 标签内插入以下代码（将斜体代码替换为您自己的相应值）：

```
<SSL>
  <Edge name="meetingserver">
    <SSLServerCtx>
      <SSLCertificateFile>[root_install_dir]\sslMeetingServer.pem</SSLCertificateFile>
      <SSLCertificateKeyFile type="PEM">[root_install_dir]\sslMeetingServer.pem</SSLCertificateKeyFile>
      <SSLPassPhrase>mypassphrase</SSLPassPhrase>
      <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
      <SSLSessionTimeout>5</SSLSessionTimeout>
    </SSLServerCtx>
  </Edge>
</SSL>
```

3 找到 `Adaptor.xml` 文件中的以下代码行：

```
<HostPort name="edge1">${DEFAULT_FCS_HOSTPORT}</HostPort>
```

4 将步骤 3 中的代码替换为以下代码：

```
<HostPort name="meetingserver" ctl_channel=":19350">:-443</HostPort>
```

5 保存 `Adaptor.xml` 文件。

6（可选）在网络浏览器中打开 `Adaptor.xml` 文件以验证语法。

如果浏览器报错，请更正错误，然后在网络浏览器中重新打开此文件。重复此步骤，直至文件有效。

7 打开位于 `[root_install_dir]\comserv\win32\conf_defaultRoot_defaultVHost_` 的 `VHost.xml` 文件，并在其他位置保存一个备份副本。

8 找到 `VHost.xml` 文件中的以下代码行：

```
<RouteEntry></RouteEntry>
```

9 将步骤 8 中的代码行替换为以下代码：

```
<RouteEntry protocol="rtmp">*:*:*:${ORIGIN_PORT}</RouteEntry>
```

10 保存 `VHost.xml` 文件。

11（可选）在网络浏览器中打开 `VHost.xml` 文件以验证语法。

12 打开位于安装根目录（默认位置为 `c:\breeze`）中的 `custom.ini` 文件，并在其他位置保存一个备份副本。

13 在 `custom.ini` 文件中插入以下代码，但不要替换或删除任何现有文本：

```
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

14 保存 `custom.ini` 文件。

15 重新启动 Adobe Connect Enterprise Server:

- a 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“停止 Adobe Connect Enterprise Server”。

- b** 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“停止 Adobe Connect Meeting Server”。
- c** 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“启动 Adobe Connect Meeting Server”。
- d** 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“启动 Adobe Connect Enterprise Server”。

测试配置

- 1** 如果保护的是应用程序服务器，请登录 Enterprise Manager。浏览器中会显示锁定图标。
- 2** 如果保护的是会议服务器，请进入 Acrobat Connect Professional 会议室。连接指示灯上会显示锁定图标。

配置基于硬件的 SSL

通过配置基于硬件的 SSL，您可以保护应用程序服务器 (HTTP) 和 / 或会议服务器 (RTMP)。您必须配置 DNS 服务器。在完成配置后，最好对配置进行测试。

有关如何配置硬件加速器的详细说明，请参阅供应商的相关文档。

配置 DNS 服务器

❖ 为要保护的服务器创建 DNS 条目。

因为 SSL 证书与名称相关，而与 IP 地址无关，所以需要为要保护的每台服务器定义 FQDN（例如 application.example.com 和 meeting1.example.com）。

注：计算机集群中的所有应用程序服务器可以共用一个 SSL 证书，但每台会议服务器必须有单独的 SSL 证书。

为会议服务器和应用程序服务器配置 SSL

- 1** 对硬件设备进行如下配置：
 - a** 将 application.example.com 设为在 443 端口进行外部监听。
 - b** 将未加密的数据转发至位于 8443 端口的应用程序服务器。
 - c** 将 meeting1.example.com 设为在 443 端口进行外部监听。
 - d** 将未加密的数据转发至位于 1935 端口的会议服务器。
 - e**（可选）将 application.example.com 设为在 80 端口进行外部监听，并将未加密的数据转发至位于 80 端口的应用程序服务器。应用程序服务器会将用户重定向至 443 端口。
- 2** 对防火墙进行如下配置：
 - a** 允许和 443 端口（如果执行了步骤 1e，则为 80 端口）上的应用程序服务器进行通信。
 - b** 允许和 443 端口上的会议服务器进行通信。
- 3** 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“配置 Adobe Connect Enterprise Server”以打开应用程序管理控制台。在“应用程序设置”屏幕上，选择“服务器设置”，并执行以下任一操作：
 - a** 在“Connect Enterprise 主机”框中输入应用程序服务器的 FQDN（例如 application.example.com）。
 - b** 在“主机映射外部名称”框中输入会议服务器的 FQDN（例如 meeting1.example.com）。
- 4** 打开位于安装根目录（默认位置为 c:\breeze）中的 custom.ini 文件，并在其他位置保存一个备份副本。
- 5** 在 custom.ini 文件中插入以下代码，但不要替换或删除任何现有文本：

```
ADMIN_PROTOCOL=https://
SSL_ONLY=yes
HTTPS_PORT=8443
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```
- 6** 保存 custom.ini 文件。
- 7** 重新启动 Adobe Connect Enterprise Server：
 - a** 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“停止 Adobe Connect Enterprise Server”。
 - b** 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“启动 Adobe Connect Enterprise Server”。

只为会议服务器配置 SSL

1 对硬件设备进行如下配置:

- a 将 `meeting1.example.com` 设为在 443 端口进行外部监听。
 - b 将未加密的数据转发至位于 1935 端口的会议服务器。
- 2 对防火墙进行配置, 允许与 443 端口上的会议服务器进行通信。
- 3 打开位于安装根目录 (默认位置为 `c:\breeze`) 中的 `custom.ini` 文件, 并在其他位置保存一个备份副本。
- 4 在 `custom.ini` 文件中插入以下代码, 但不要替换或删除任何现有文本:

```
RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
```

5 保存 `custom.ini` 文件。

只为应用程序服务器配置 SSL

1 对硬件设备进行如下配置:

- a 将 `application.example.com` 设为在 443 端口进行外部监听。
- b 将未加密的数据转发至位于 8443 端口的应用程序服务器。
- c (可选) 将 `application.example.com` 设为在 80 端口进行外部监听, 并将未加密的数据转发至位于 80 端口的应用程序服务器。应用程序服务器会将用户重定向至 443 端口。

2 对防火墙进行配置, 允许和 443 端口 (如果执行了步骤 1c, 则为 80 端口) 上的应用程序服务器进行通信。

3 在 Connect Enterprise Server 上, 在安装根文件夹 (默认位置为 `c:\breeze`) 下的 `custom.ini` 文件中添加以下代码:

```
ADMIN_PROTOCOL=https://  
SSL_ONLY=yes  
HTTPS_PORT=8443
```

4 重新启动 Adobe Connect Enterprise Server:

- a 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“停止 Adobe Connect Enterprise Server”。
- b 选择“开始”>“所有程序”>“Adobe Connect Enterprise Server”>“启动 Adobe Connect Enterprise Server”。

测试配置

- 1 如果保护的是应用程序服务器, 请登录 Enterprise Manager。浏览器中会显示锁定图标。
- 2 如果保护的是会议服务器, 请进入 Acrobat Connect Professional 会议室。连接指示灯上会显示锁定图标。

SSL 配置参考

XML 标签

标签	默认值	说明
SSLCertificateFile	无默认值。	发送至客户端的证书文件的位置。如果不指定绝对路径，则假定证书使用相对于 Adaptor 目录的位置。
SSLCertificateKeyFile	无默认值。	证书的私钥文件的位置。如果不指定绝对路径，则假定私钥文件使用相对于 Adaptor 目录的位置。如果私钥文件经过加密，则必须在 SSLPassPhrase 标签内指定口令短语。 type 属性指定证书密钥文件使用的编码类型。编码类型可以是 PEM 或 ASN1 。
SSLCipherSuite	请参阅说明。	算法。由冒号分隔的元素组成，可包括密钥交换算法、身份验证方法、加密方法、摘要类型或用于分组的选定数量的别名中的某一个。要获取算法元素的列表，请参阅 Flash Media Server 文档。 此标签的默认设置如下： <code>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</code> 若要更改默认设置，请与 Adobe 技术支持联系。
SSLPassPhrase	无默认值。	用于解密私钥文件的口令短语。如果私钥文件未经加密，请将此标签保留为空。
SSLSessionTimeout	5	启用了 SSL 的会话的有效时间，以分钟为单位。

配置参数

参数	默认值	说明
ADMIN_PROTOCOL	http://	应用程序服务器所用的协议。如果设置为 https:// ，则可配置 SSL。
DEFAULT_FCS_HOSTPORT	:1935	Flash Media Server 使用 RTMP 协议进行通信时使用的端口。如果设置为 :-443,1935 ，则可配置 SSL。
HTTPS_PORT	无默认值。	应用程序服务器监听 HTTPS 请求时使用的端口。此参数通常设置为 443 或 8443 ，以便配置 SSL。
SSL_ONLY	no	如果服务器仅支持安全连接，请将值设为 yes 。此设置会强制所有 Connect Enterprise URL 使用 HTTPS。
RTMP_SEQUENCE	无默认值。	连接 Flash Media Server （会议服务器）所用的源服务器、边缘服务器和端口。

