深圳市潮流网络技术有限公司.

GRP26XX 系列

安全手册

目录

图片目录

总览

本文档总结导致安全问题因素和配置，建议用户在配置和部署我们的 GRP 系列 IP 电话时要考虑这些措施。

注意：我们建议使用最新的固件。

本文档涵盖以下各节：

- **Web UI/SSH 访问**

  Web UI 访问受用户名/密码和登录超时保护。三级用户管理是可配置的。支持 SSH 访问（主要用于故障排除），建议在正常使用时将其禁用。

- **SIP 帐户和呼叫的安全性**

  SIP 帐户将特定端口用于信令和媒体流传输。 它还提供可配置的选项来阻止匿名呼叫和未经请求的呼叫。

- **GRP 服务的安全性**

  GRP 支持 HTTP / HTTPS / TFTP / FTP / FTPS 和 TR-069 等服务来进行设置。为了获得更好的安全性，我们建议将 HTTPS / FTPS 与用户名/密码一起使用，并使用受密码保护的 XML 文件。如果不使用 TR-069，建议您将其禁用（默认情况下禁用），以避免潜在的端口暴露。

- **GRP 部署指南**

  本节介绍了 GRP 上使用的协议和端口以及路由器/防火墙设置的建议。

本文如有更改，恕不另行通知。

WEB UI/SSH 访问

Web UI 访问

GRP 嵌入式 Web 服务器响应 HTTP / HTTPS GET / POST 请求。 嵌入式 HTML 页面允许用户通过 Web 浏览器（例如 Microsoft IE，Mozilla Firefox，Google Chrome 等）配置设备。管理员可以使用此页面访问和配置所有可用的 GRP 信息和设置。将 IP 电话放置在公共网络上时涉及的安全风险很大，建议不要这样做。

Web UI 访问协议

支持 HTTP 和 HTTPS 访问 GRP 的 Web UI，可以在 Web UI→维护→安全设置→安全下进行配置。

为了保护使用并防止未经授权的访问，强烈建议您:

1. 使用 HTTPS 代替 HTTP。
2. 避免使用默认的端口号，例如 80 和 443。

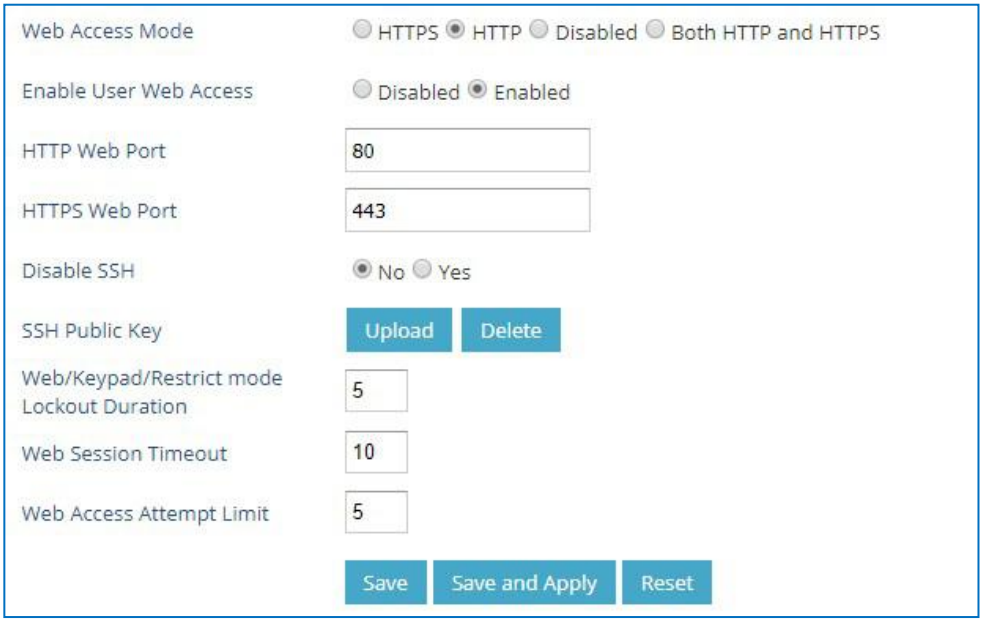

图 1 ：Web UI 访问设置

3. GRP 话机允许通过 SSH 访问以进行复杂的故障排除。除非管理员或潮流技术支持需要进行故障排除，否则不需要这样做。 默认情况下，使用端口 22 启用设备上的 SSH 访问，建议您将其禁用以用于日常正常使用。如果需要启用 SSH 访问，将端口更改为默认的端口 22 以外的其他端口是一个好习惯。

管理员登录

需要用户名和密码才能登录 GRP 的网络用户界面。

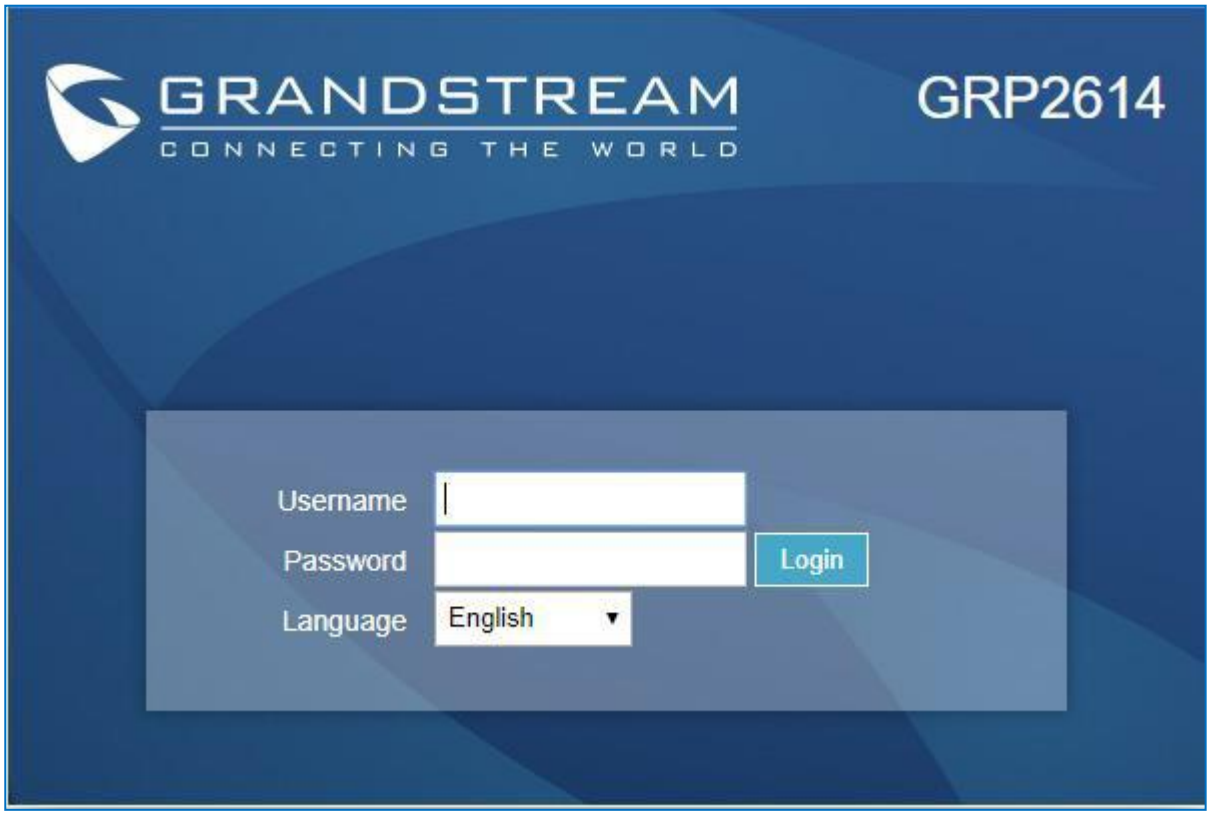

图 2：Web UI 登录

管理员级别的出厂默认用户名是“ admin”，默认密码是随机密码，位于设备背面的标签上。强烈建议您在首次登录时更改默认密码。

首次或在恢复出厂设置后访问 GRP 电话时，将要求用户在访问 GRP Web 界面之前更改默认管理员密码。

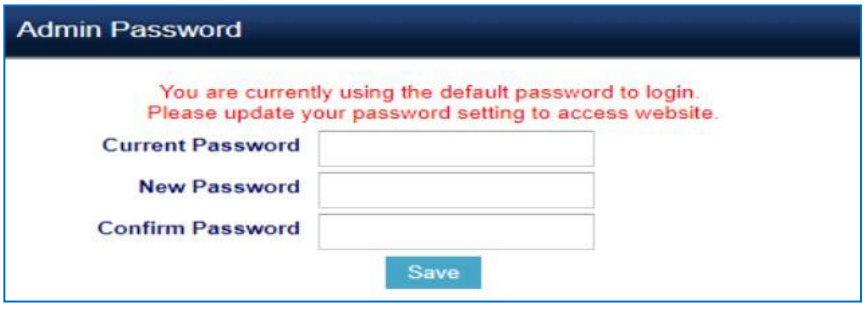

图 3：第一次登录修改管理员密码

要更改默认用户“ admin”的密码，请导航至 Web GUI→维护→Web 访问。

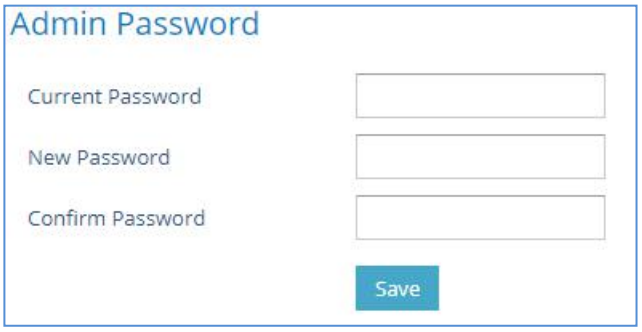

图 4：修改管理员密码

密码长度必须在 6 到 25 个字符之间。为了安全起见，建议始终使用由数字，大写字母，小写字母和特殊字符组成的强密码。

用户管理级别

当前支持两个用户权限级别：

- Admin
- User

用户级别	用户名	密码	Web 页面权限
用户级别	user	123	仅状态和基本设置
管理员级别	admin	随机密码，可以在设备背部贴纸上找的	所有页面

注意：

➢ 建议仅让管理员保留管理员登录名。如果需要访问 Web UI，则应该仅向用户提供用户级别的登录名。

➢ 遵循以下步骤，在首次登录时更改用户级别密码：

1. 通过在浏览器中输入其 IP 地址来访问您的 GRP Web UI。
2. 输入管理员密码。
3. 转到基本设置→新用户密码，然后输入新密码。
4. 确认新密码。
5. 按页面底部的“保存”以保存新设置。

图 5：修改用户密码

SIP 帐户和话机的安全性

协议和端口

默认情况下，恢复出厂设置后，所有帐户均处于激活状态。 知道默认的本地 SIP 端口（Account1：5060; Account2：5062…）的用户可以进行直接 IP 呼叫，即使这些帐户未注册到任何 PBX。 因此，建议禁用未使用的端口。 在 Web GUI 下→帐户→帐户 X→常规设置→帐户有效：“否”，”

➢ 用户还可以在“设置”→“呼叫特征功能”下，在所有端口上禁用直接 IP 呼叫：将“禁用直接 IP 呼叫：”设置为“是”。

- **SIP 传输协议：**

  GRP 支持 3 中 SIP 传输协议“ UDP”，“ TCP”和“ TLS”。默认情况下，它设置为“ UDP”。 建议使用“ TLS”，以便对 SIP 信令进行加密。 可以配置 SIP 传输协议 Web UI 下的每个帐户→帐户→帐户 X→SIP 设置→基本设置。 当“ TLS”使用，我们建议对 SIP URI 方案使用“ sips”而不是“ sip”，以确保整个 SIP 交互均得到保护，而不是“尽力而为”。

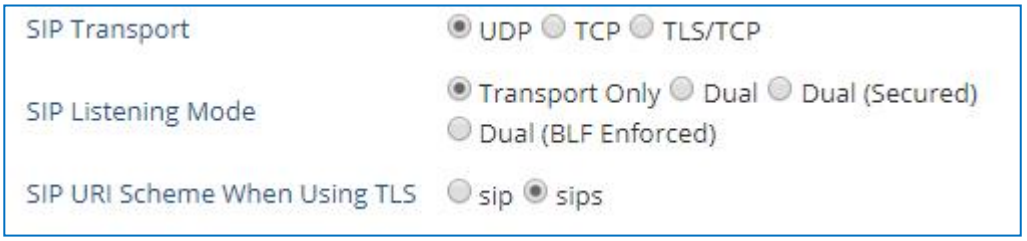

图 6：将 SIP 传输配置为 TLS

可以在维护→安全设置下配置 SIP TLS 证书，私钥和密码→安全页面：

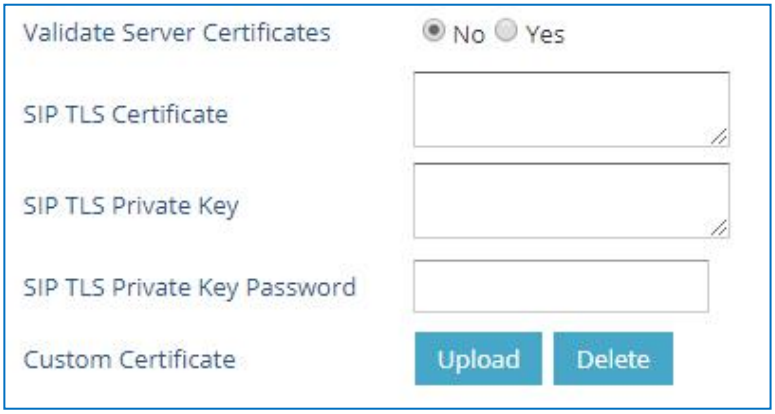

图 7 ： SIP TLS 设置

使用 SIP TLS 时，GRP 还提供其他配置：

- **验证服务器证书**：

此功能使用户可以使用我们受信任的 TLS 连接列表来验证服务器证书。

- **受信任的 CA 证书**：使用证书进行身份验证。

图 8 ：其他 SIP TLS 设置

- **使用 UDP / TCP 时的本地 SIP 端口：**
  从帐户 1 的 5060 开始，每个帐户的端口号增加 2。 例如，5062 是帐户 2 的默认本地 SIP 端口。

- **使用 TLS 时的本地 SIP 端口：**
  SIP TLS 端口是 UDP SIP 端口加 1。例如，如果帐户 1 SIP 端口是 5060，则其 TLS 端口将是 5061。

匿名/主动呼叫保护

如果用户希望阻止匿名呼叫，请转到 GRP 的 Web GUI→帐户 X→呼叫设置，并将“匿名呼叫拒绝”设置为“是”：然后，GRP 将通过发送一个匿名呼叫者 ID 拒绝所有来电。 “ 486 Busy here”消息。

图 9：拒接匿名呼叫

- **其他 SIP 安全设置:**

在 Web GUI 下→帐户 X→SIP 设置→安全设置:

- **仅允许来自 sip 服务器的 SIP 请求:**

设置为“是”以强制 GRP 检查传入 SIP 消息中请求 URI 的 SIP 地址；如果与帐户的 SIP 服务器地址不匹配，则呼叫将被拒绝。

此外，GRP 具有内置机制，可检测并阻止其他 SIP 呼叫使电话响铃。 请参阅下面的设置。

- **验证入局 sip 消息:**

设置“是”以通过检查呼叫者 ID 和 CSeq 标头来验证传入消息。 如果消息不包含标题，它将被拒绝。

- **来电 invite 时验证 sip 用户 ID:**

设置为“是”以启用验证入局 INVITE 的请求 URI 中的 SIP 用户 ID；如果与 GRP SIP 用户 ID 不匹配，则该呼叫将被拒绝。 如果选中，直接 IP 呼叫也将被禁用。

- **验证来电 INVITE:**

设置为“是”以通过“ SIP / 401 未经授权”消息来验证传入的邀请以进行身份验证。

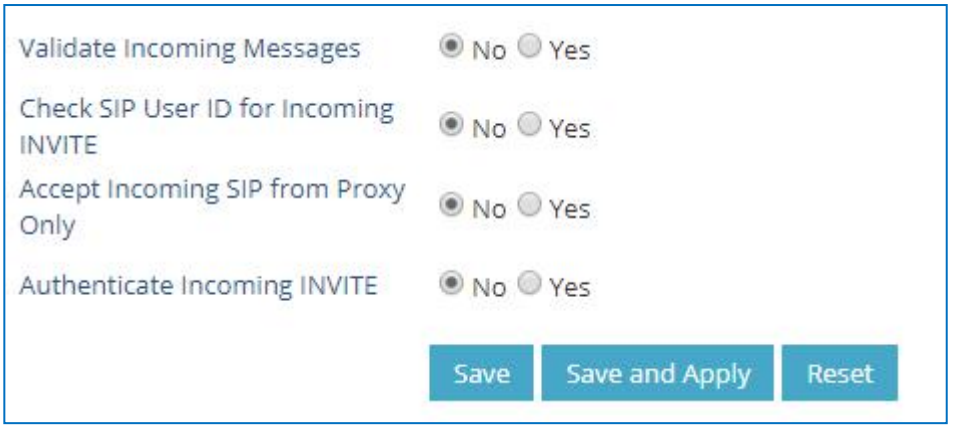

图 10 ： 阻止匿名呼叫的设置

SRTP

为了防止语音通信被窃听，GRP 支持 SRTP，用于使用 AES 的媒体流量 128 和 256。 如果 SIP 服务器（或服务提供商）支持 SRTP，则建议使用 SRTP。 可以在 Web GUI→帐户 X→语音设置下配置 SRTP。

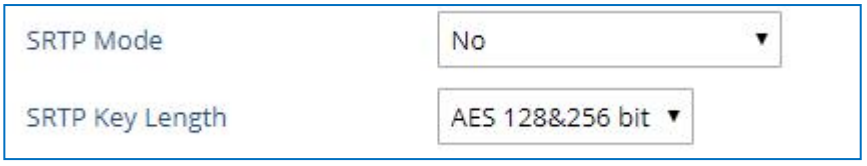

图 11 ： SRTP 设置

选择 SRTP 模式以进行选择（“否”，“使用但不是强制”，“强制并使用”或“可选”）。 默认值为否。它使用 SDP 安全说明交换密钥.

SNMP

SNMP 协议用于网络管理。 如果不使用它，我们建议禁用它。 用户可以通过 GRP 的 Web GUI 在“网络”→“ SNMP 设置”页面下执行此操作:

- 设置“**启用 SNMP** 为否”

图 12: SNMP 设置

GRP 服务的安全性

固件升级和配置

GRP IP 电话支持通过 TFTP，HTTP / HTTPS，FTP / FTPS 下载配置文件。下图显示了 Web GUI→维护→升级和配置下的相关选项：

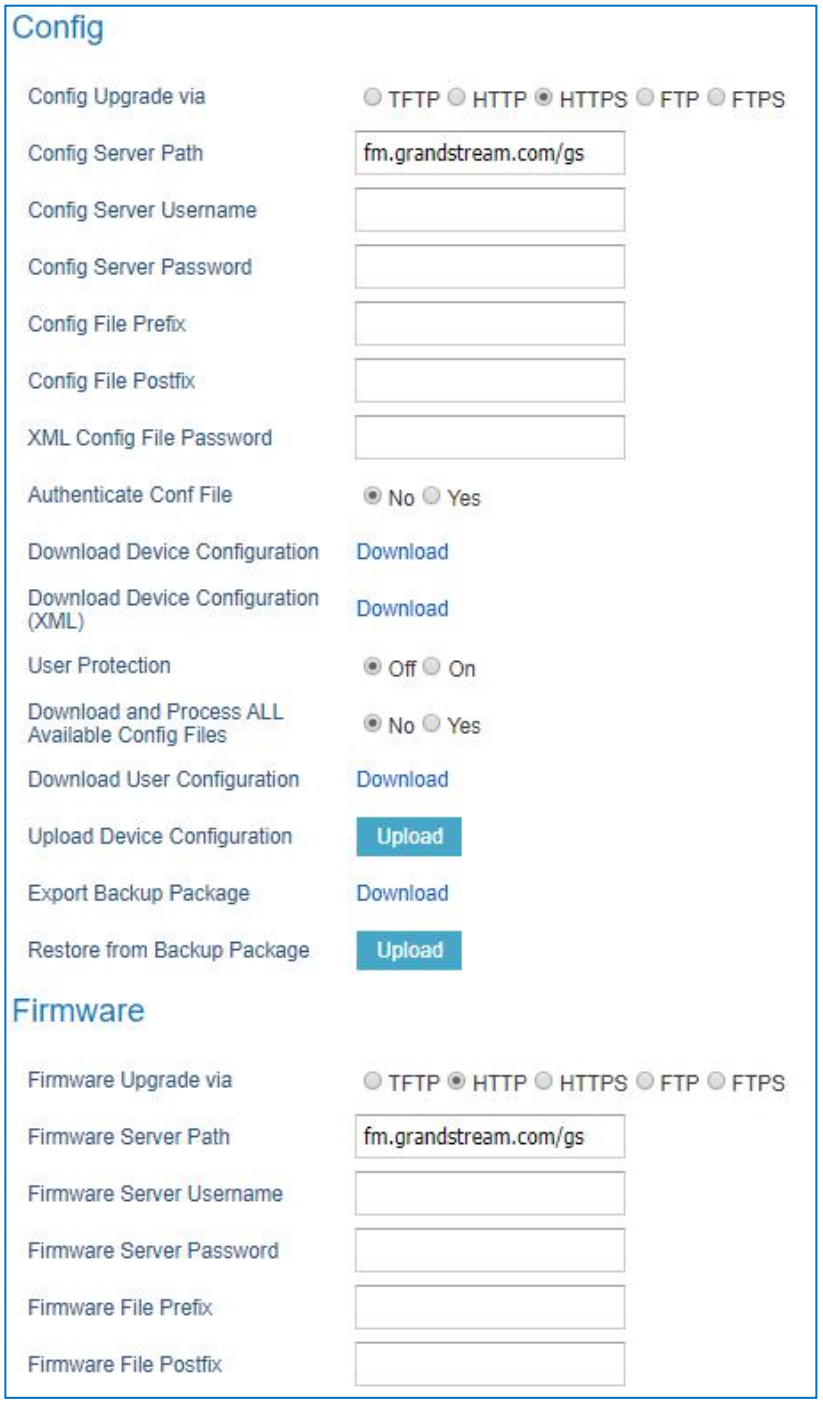

图 13：下载配置文件

我们建议用户在部署带有预配置的 GRP 时考虑以下选项以增强安全性。

- **升级方式：HTTPS：**
  默认情况下，选择 HTTPS。 建议这样做，以便在通过网络传播时对数据进行加密。

- **HTTP/HTTPS/FTP/FTPS 用户名和密码：**
  使用 HTTP / HTTPS / FTP / FTPS 时，可以在配置服务器上根据需要进行设置。仅当 GRP 配置了正确的用户名和密码后，才能由升级/配置服务器进行身份验证，并且可以下载配置文件。

- **验证配置文件：**
  这会将使 GRP 设置在应用配置文件之前先对其进行身份验证。设置为“是”时，配置文件必须包含 P 值 P1 和 GRP 话机的管理密码。如果丢失或与密码不匹配，则 GRP 不会应用配置文件。

- **XML 配置文件密码：**
  可以使用 OpenSSL 加密 GRP XML 配置文件。加密后，GRP 必须在此字段中提供正确的密码，以便下载后可以解密 XML 配置文件。然后可以应用该配置。请注意，XML 配置文件支持而二进制配置文件不支持此功能。因此，建议使用 XML 配置文件格式并使用此功能对其进行加密。

- **验证服务器证书：** （在维护下→安全性设置→安全性）
  这配置了在下载固件/配置文件时是否验证服务器证书。如果设置为“是”，则 GRP 将仅从合法服务器下载固件/配置文件。

TR-069

TR-069 默认情况下处于禁用状态，如果不使用，建议将其禁用。

当在维护→TR-069 下启用 TR-069 并使用该服务时，用户可以设置以下内容：

- **ACS URL**：指定 TR-069 自动配置服务器的 URL。
- **ACS 用户名/密码**：输入用户名/密码以认证 ACS。
- **开启定时连接**:发送定时连接的数据包到 ACS。
- **定时连接间隔**：设置将定时数据包发送到 ACS 的频率。
- **连接请求用户名/密码**：输入用户名/密码以使 ACS 连接到 GRP。

- **CPE SSL 证书**：填写话机通过 SSL 连接 ACS 时需要使用的证书文件。
- **CPE SSL 私钥**：填写话机通过 SSL 连接 ACS 时需要使用的证书密码。

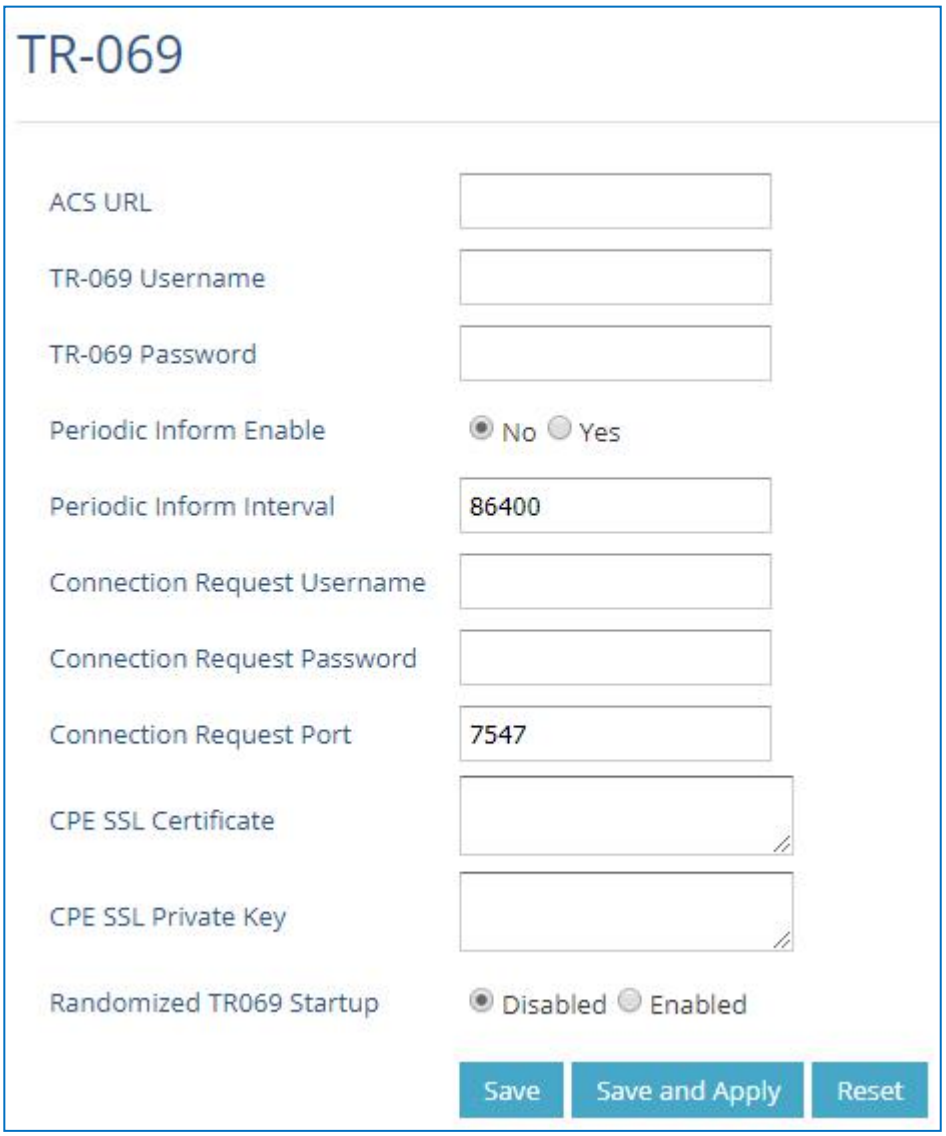

图 14 ：TR-069 连接设置

系统日志

GRP 支持将 Syslog 发送到远程 Syslog 服务器。默认情况下，它是通过 UDP 发送的，我们建议将其更改为“ SSL / TLS”，这样包含设备信息的系统日志消息将通过 TLS 连接安全地发送。

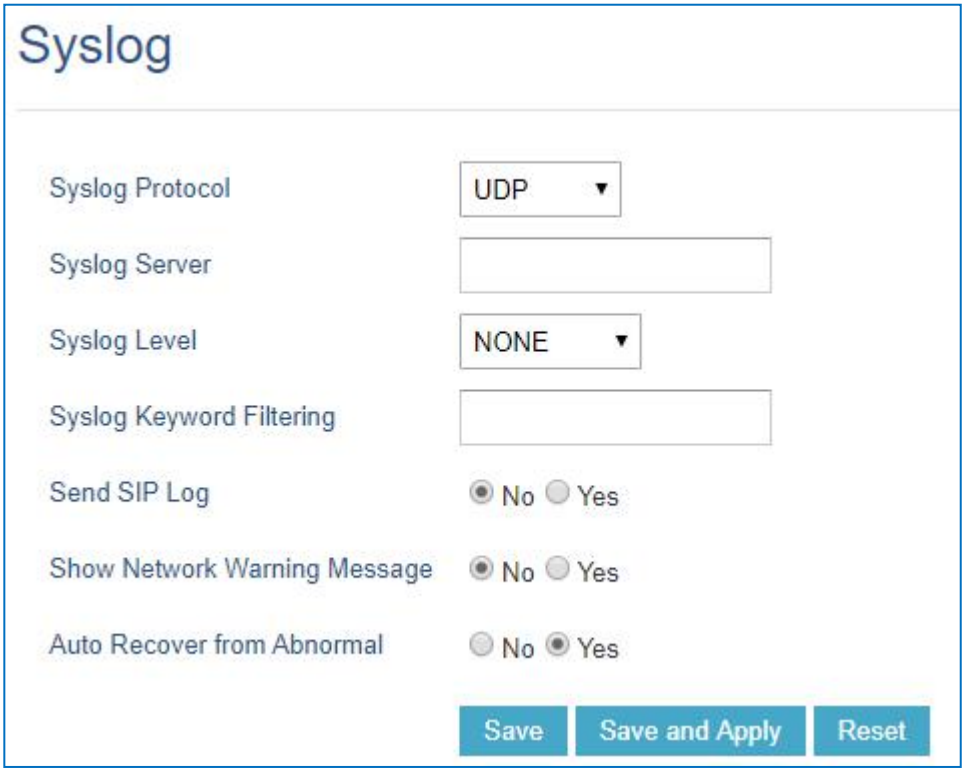

图 15 ： 系统日志协议

GRP 部署的安全准则

通常，GRP 部署在 NAT 之后。网络管理员可以考虑遵循以下安全准则，以使 GRP 正常且安全地工作。

- **在路由器上关闭 SIP ALG 功能**

  建议在客户的路由器上关闭 SIP ALG（应用层网关）。SIP ALG 在许多旨在通过检查 VoIP 数据包并在必要时进行修改以防止路由器防火墙引起的问题的路由器中很常见。即使 SIP ALG 旨在防止 VoIP 设备出现问题，也可能会实施不完善而引起问题，尤其是在某些情况下，SIP ALG 修改 SIP 数据包的方式可能不正确，这可能会导致 VoIP 设备无法注册或建立呼叫。

- **使用 TLS 和 SRTP 进行 SIP 呼叫**

  在 GRP 上，建议将 TLS 用于 SIP 传输，并将 SIP URL 方案中的“ sip”用于 SIP 信令加密，并使用 SRTP 进行媒体加密。

  如果网络管理员需要创建防火墙规则，则在 GRP 上使用的 SIP 端口和 RTP 端口以外创建。

  ➢ 在 web UI → **账号 x → SIP 设置 → 基本设置,** “本地端口”
  定义用于侦听和传输的本地 SIP 端口。使用 SIP 传输协议 UDP / TCP 时，默认值对于帐户 1 是 5060，对于帐户 2 是 5062，对于帐户 3 是 5064，对于帐户 4 是 5066…当使用 TLS 作为 SIP 传输协议时，对于帐户 1，默认值为 5061， 帐户 2 是 5063，帐户 3 是 5065，…有效范围是 1 到 65535。

  ➢ 在 web UI → **设置 → 基本设置**, “本地 RTP 端口” 定义了本地 RTP 用于监听和传输的端口。
  本地 RTP 端口范围是 1024 到 65400，并且必须是偶数。它是通道 0 的基本 RTP 端口。配置后，通道 0 将对 RTP 使用此 port_value，对于 RTCP 使用 port_value + 1。通道 1 将使用 port_value + 2 进行 RTP，以此类推，直到达到限制，然后将其重置为第一个 port_value。 RTP 的默认值为 5004，RTCP 的默认值为 5005。

  对于 GRP26XX 话机，可以为本地 RTP 端口选择一个范围，从 48 到 10000。默认设置为 200。

  注意: 在客户的防火墙上，建议确保为 GRP 上的 SIP 帐户打开 SIP 端口。无需在防火墙上使用默认端口 5060/5062 /…。 相反，出于安全目的，网络管理员可以考虑将防火墙上的其他端口映射到 GRP SIP 端口 5060。

- **使用 HTTPS 进行 Web UI 访问**

  除了使用 HTTPS，GRP Web UI 访问还应配备强密码。另外，请勿将 GRP Web 用户界面访问权限公开暴露于公共网络中。

- **使用 HTTPS 进行固件下载和配置文件下载**

  使用 HTTPS 进行固件下载和配置。除此之外，为 HTTP / HTTPS 服务器设置用户名和密码以要求身份验证。还建议您打开“验证服务器证书”，以便 GRP 在下载固件或配置文件时会验证服务器证书。