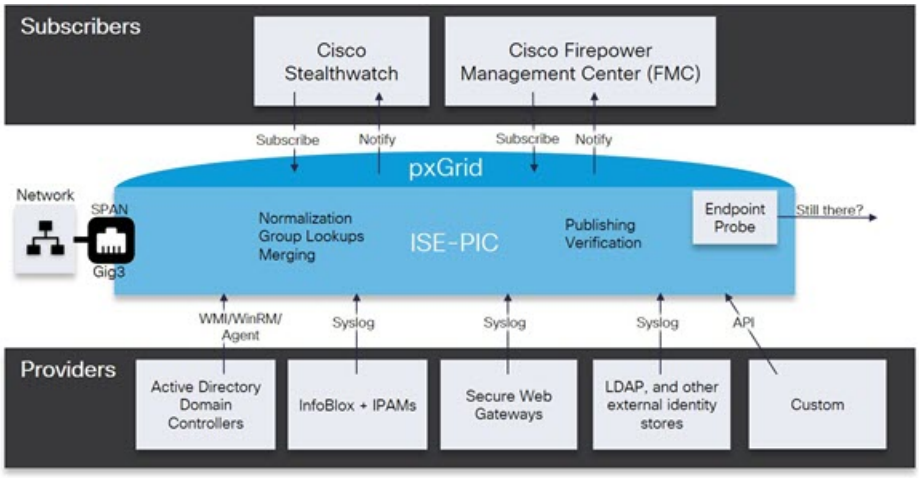
用户

ISE-PIC 使用 思科 pxGrid 服务，以便将从各种提供程序收集并由思科 ISE-PIC 会话目录存储的经过身份验证的用户身份传送到其他网络系统，例如思科 Stealthwatch 或思科 Firepower 管理中心 (FMC)。

在下图中，pxGrid 节点从外部提供程序收集用户身份。这些身份经过解析、映射和设置格式。pxGrid 获取这些设置格式的用户身份，并将其发送到 ISE-PIC 用户。

图 *1: ISE-PIC* 流



连接到思科 ISE-PIC 的用户必须注册才能使用 pxGrid 服务。用户可以使用唯一名称和基于证书的相互身份验证登录 pxGrid。一旦他们发送了有效证书，ISE-PIC 便会自动批准思科 pxGrid 用户。

用户可连接到已配置的 pxGrid 服务器主机名或 IP 地址。我们建议您使用主机名，以避免出现不必要的错误，尤其是为了确保 DNS 查询正常工作。功能是指在 pxGrid 上创建的供用户发布和订用的信息主题或通道。在思科 ISE-PIC 中，仅支持 SessionDirectory 和 IdentityGroup。功能信息可通过发布、定向查询或批量下载查询从发布者获取，并可导航至**功能 (Capabilities)** 选项卡中的**用户 (Subscribers)** 进行查看。

要使用户能够从 ISE-PIC 接收信息，必须执行以下操作：

1. 或者，从用户端生成证书。
2. ISE-PIC生成用户的 pxGrid 证书，第 2 页。

3. 启用用户，第 4 页。执行此步骤，或者自动启用批准，以便允许订户从 ISE-PIC 接收用户身份。请参阅 配置用户设置，第 4 页。

注释 您可能会在**用户 (Subscribers) > 摘要 (Summary)** 窗口中看到以下消息：

PxGrid 已禁用。为了导航到 pxGrid 服务页面，必须在 ISE 部署中的至少一个节点上启用 pxGrid 角色。请单击此链接以重定向到“部署”(Deployment) 页面。

单击此链接可能会显示以下消息：

页面不可访问。由于权限不足，您正在尝试加载的页面无法访问。

但是，**客户端管理 (Client Management)**、**诊断 (Diagnostics)**、**设置 (Settings)** 等所有其他窗口均可访问。有关详细信息，请参阅 CSCvz72069。

- 生成用户的 pxGrid 证书，第 2 页
- 启用用户，第 4 页
- 从实时日志查看用户事件，第 4 页
- 配置用户设置，第 4 页

生成用户的 pxGrid 证书

开始之前

注释 从思科 ISE 版本 3.1开始，所有 pxGrid 连接都必须基于 pxGrid 2.0。基于 pxGrid 1.0（基于 XMPP）的集成将从版本 3.1 开始在思科 ISE 上停止使用。

基于 WebSockets 的 pxGrid 版本 2.0 在思科 ISE 版本 2.4 中引入。我们建议将您的其他系统计划并升级到与 pxGrid 2.0 兼容的版本，以防止对集成造成可能的中断（如有）。

安装时，ISE-PIC 自动为由主 ISE-PIC 节点进行数字签名的 pxGrid 服务生成自签证书。此后，您可以生成 pxGrid 用户的证书，以便保证 pxGrid 和用户之间的相互信任，从而最终使用户身份能够从 ISE-PIC 传递到用户。

步骤 1 选择**用户 (Subscribers)**，然后转至**证书 (Certificates)** 选项卡。

步骤 2 从**我想 (I want to)** 下拉列表中选择以下选项之一：

- **“生成无证书签名请求的单个证书”(Generate a single certificate without a certificate signing request)**：如果选择此选项，则必须输入通用名称 (CN)。在“通用名称”字段中，输入包含 pxGrid 作为前缀的 pxGrid FQDN。例如，www.pxgrid-ise.ise.net。或者，使用通配符。例如，*.ise.net
- **“生成有证书签名请求的单个证书”(Generate a single certificate with a certificate signing request)**：如果选择此选项，则必须输入证书签名请求详细信息。

- **生成批量证书 (Generate bulk certificates)**：可以上传包含所需详细信息的 CSV 文件。
- **下载根证书链 (Download Root Certificate Chain)**：下载 ISE 公共根证书，以便将其添加到 pxGrid 客户端的受信任证书存储区。ISE pxGrid 节点仅信任新签名的 pxGrid 客户端证书，反之亦然，从而无需外部证书颁发机构。

步骤 3 （可选）您可以输入此证书的说明。

步骤 4 查看或编辑此证书所基于的 pxGrid 证书模板。证书模板包含证书颁发机构 (CA) 基于该模板颁发的所有证书通用的属性。证书模板定义了主题、主题备选名称 (SAN)、密钥类型、密钥大小、必须使用的 SCEP RA 配置文件、证书的有效期以及扩展密钥用法(EKU)（指定必须将证书用于客户端身份验证、服务器身份验证，还是用于两者）。内部思科 ISE CA (ISE CA) 使用证书模板颁发基于该模板的证书。对于 pxGrid，处理被动身份服务时只能使用 pxGrid证书模板，并且只能编辑此模板的主题信息。要编辑此模板，请选择**证书 (Certificates)** > **证书模板 (Certificate Templates)** **管理 (Administration)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **证书模板 (Certificate Templates)**。

步骤 5 指定使用者备选名称 (SAN)。可以添加多个 SAN。可提供以下选项：

- **FQDN**：输入 ISE 节点的完全限定域名。例如 www.isepic.ise.net。或者，使用通配符表示 FQDN。例如，*.ise.net

  可以为 FQDN 添加其中还可输入 pxGrid FQDN 的附加行。这应与您在“通用名称”(Common Name) 字段中使用的 FQDN 相同。
- **“IP 地址”(IP address)**：输入将与证书关联的 ISE 节点的 IP 地址。如果用户使用 IP 地址而不是 FQDN，则必须输入此信息。

注释 如果选定“生成批量证书”(Generate Bulk Certificate) 选项，则不会显示此字段。

步骤 6 从**证书下载格式 (Certificate Download Format)** 下拉列表中选择以下选项之一：

- **加强隐私电子邮件 (PEM) 格式的证书和 PKCS8 PEM 格式的密钥（包括证书链）(Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain))**：根证书、CA 中间证书和终端实体证书均采用 PEM 格式。PEM 格式的证书是采用 BASE64 编码的 ASCII 文件。每个证书的开头采用“-------证书开始 (BEGIN CERTIFICATE) -----”标签，结尾采用“-----证书结束 (END CERTIFICATE) ----”标签。终端实体的专用密钥使用 PKCS* PEM 存储。其开头采用“-----加密专用密钥开始 (BEGIN ENCRYPTED PRIVATE KEY) ----”标签，结尾采用“-----加密专用密钥结束 (END ENCRYPTED PRIVATE KEY) ----”标签。
- **PKCS12 格式（包括证书链；证书链和密钥的文件）(PKCS12 format [including certificate chain; one file for both the certificate chain and key])**：CA 根证书、CA 中间证书以及终端实体的证书和专用密钥存储在一个加密文件时，所采用的二进制格式。

步骤 7 输入证书密码。

步骤 8 单击**创建 (Create)**。

启用用户

必须执行此任务，或者自动启用审批，才能允许用户从思科 ISE ISE-PIC 接收用户身份。请参阅 配置用户设置，第 4 页。

步骤 1 选择**用户 (Subscribers)** 并确保查看的是**客户端 (Clients)**选项卡。

步骤 2 选中用户旁边的复选框，然后单击**审批 (Approve)**。

步骤 3 单击**刷新 (Refresh)** 查看最新的状态。

从实时日志查看用户事件

“实时日志”(Live Logs) 页面显示所有用户事件。事件信息包括用户和功能名称，以及事件类型和时间戳。

导航到**用户 (Subscribers)** 并选择**实时日志 (Live Log)** 选项卡以查看事件列表。您还可以清除日志并重新同步或刷新列表。

配置用户设置

步骤 1 选择**用户 (Subscribers)**，然后转至**设置 (Settings)**选项卡。

步骤 2 根据您的需求选择以下选项：

- **自动审批新账户 (Automatically Approve New Accounts)**：选中此复选框可自动审批来自新 pxGrid 客户端的连接请求。
- **允许创建基于密码的帐户 (Allow Password Based Account Creation)**：选中此复选框可为 pxGrid 客户端启用基于用户名/密码的身份验证。如果启用此选项，系统无法自动审批 pxGrid 客户端。

  pxGrid 客户端可以通过使用 REST API 发送用户名向 pxGrid 控制器注册。在客户端注册时，pxGrid 控制器为 pxGrid 客户端生成密码。管理员可以批准或拒绝连接请求。

步骤 3 单击**保存 (Save)**。