



pxGrid

- [pxGrid 和思科 ISE](#)，第 1 页

pxGrid 和思科 ISE



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）。

Cisco pxGrid 是一个开放且可扩展的安全产品集成框架，允许任意合作伙伴平台双向集成。

pxGrid 2.0 使用 REST 和 WebSocket 接口。客户端使用 REST 处理控制消息、查询和应用数据，并使用 WebSocket 推送事件。有关 pxGrid 2.0 的详细信息，请参阅[欢迎学习思科平台交换网格\(pxGrid\)](#)。

Cisco pxGrid 可以：

- 与其他网络系统（例如 ISE 生态系统合作伙伴系统）和其他思科平台共享思科 ISE 会话目录中的情景相关信息。
- 让第三方系统能调用自适应网络控制操作隔离用户和设备以应对网络或安全事件。标签定义、值和说明等 TrustSec 信息通过 TrustSec 主题从思科 ISE 传输到其他网络。
- 通过终端配置文件元主题，将具有完全限定名称 (FQN) 的终端配置文件从思科 ISE 发送到其他网络。
- 批量下载标签和终端配置文件。
- 通过 pxGrid 发布和订用 SXP 绑定（IP-SGT 映射）。有关 SXP 绑定的详细信息，请参阅《[思科 ISE 管理员指南](#)》中“分段”一章中的安全组标签交换协议部分。
- Cisco pxGrid Context-in 使生态系统合作伙伴能够将主题信息发布到思科 ISE。因此思科 ISE 能够根据生态系统中识别的资产采取行动。有关 Cisco pxGrid Context-in 的详细信息，请参阅[pxGrid Context-In](#)。

pxGrid 概述

pxGrid 具有以下组件：

- 控制器：处理发现、身份验证和授权。
- 提供程序：返回查询结果或发布。
- Pubsub：为提供程序和使用者提供 pxGrid 服务。
- 用户：获得授权后，用户会从订阅的主题获取情景信息和警报。

pxGrid 提供以下功能：

- 发现：根据服务名称发现服务属性。当提供程序要求向 pxGrid 控制器“注册服务”时，流程开始。注册后，消费者使用“查找服务”发现提供商的位置。
- 身份验证：pxGrid 控制器验证 pxGrid 客户端是否有权限访问服务。凭证为用户名和密码或证书（首选）。
- 授权：当 pxGrid 收到操作请求时，它会与 pxGrid 控制器协商以授权请求。pxGrid 将客户端分配到预定义的组。

pxGrid 2.0 的高可用性

pxGrid 2.0 节点在主动/主动配置下运行。为实现高可用性，部署中应至少有两个 pxGrid 节点。大型部署最多可以有四个节点，以增加规模和冗余。我们建议您为所有节点配置 IP 地址，以便在一个节点关闭时，该节点的客户端连接到工作节点。当 PAN 关闭时，pxGrid 服务器会停止处理激活。手动升级 PAN 才能激活 pxGrid 服务器。有关 pxGrid 部署的详细信息，请参阅 [ISE 性能和扩展](#)。

所有 pxGrid 服务提供商客户端会在 7.5 分钟内定期向 pxGrid 控制器重新注册。如果客户端未重新注册，PAN 节点会认定它处于非活动状态，并删除该客户端。如果 PAN 节点关闭超过 7.5 分钟，当它恢复正常运行时，它将删除时间戳值早于 7.5 分钟的所有客户端。所有这些客户端都必须再次向 pxGrid 控制器注册。

pxGrid 2.0 客户端使用 WebSocket 和基于 REST 的 API 进行发布/订阅和查询。这些 API 由端口 8910 上的 ISE 应用服务器提供。通过 `show logging application pxgrid` 显示的 pxGrid 进程不适用于 pxGrid 2.0。



注释 GUI 和 CLI 中对 pxGrid 1.0 进程的所有引用均已删除。

丢失检测

在思科 ISE 3.0 中，我们向 pxGrid 主题添加了序列 ID。如果传输中断，用户可以通过检查 ID 序列中的缺口来识别这种情况。用户注意到主题序列 ID 发生变化，根据最后一个序列号的日期请求数据。如果发布者关闭，则当它恢复时，主题序列从 0 开始。当用户看到序列 0 时，必须清除缓存并开始批量下载。如果用户关闭，发布者会继续分配顺序 ID。当用户重新连接后发现序列 ID 出现缺口时，用户会从最后一个序列号的时间开始请求数据。丢失检测配合 Session Directory 和 TrustSec 配置运行。对于 Session Directory，当客户端检测到丢失时，必须清除缓存并开始批量下载。

如果您现有的应用不使用序列 ID，则不必使用它们。但是，使用它们有助于检测丢失情况并从丢失中恢复。

Session Directory 会话是批处理的，在每个通知间隔内由 MnT 异步发布到 `/topic/com.cisco.ise.session`。

TrustSec Security Group 的更改将发布到 `/topic/com.cisco.ise.config.trustsec.security.group`。

丢失检测仅受 pxGrid 2.0 支持，默认情况下处于启用状态。

要查看使用丢失检测的代码示例，请参阅<https://github.com/cisco-pxgrid/pxgrid-rest-ws/tree/master/java/src/main/java/com/cisco/pxgrid/samples/ise>。

监控和调试

以下日志可用于 pxGrid:

- `pxgrid-server.log`: pxGrid 2.0 活动和错误

日志 (**Log**) 页面显示所有 pxGrid 2.0 管理事件。事件信息包括客户端和功能名称，以及事件类型和时间戳。选择 **管理 > pxGrid 服务 > 诊断 > 日志** 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。

pxGrid 摘要页面

“pxGrid 摘要”页面显示当前 pxGrid 2.0 环境的统计信息。

- 当前连接 (Current Connections): 列出与控制器的连接
- 控制消息 (Control Messages): 身份验证、授权和服务发现
- REST API: 使用 WebSocket 或 XMPP 连接的客户端数量
- Pubsub 吞吐量 (Pubsub Throughput): 发布到客户端的数据量
- 客户端 (Clients): 通过 REST 或 WebSocket 连接的客户端
- 错误数 (Errors): 导致客户端请求重新启动数据传输的传输错误数

pxGrid 客户端管理

客户端必须注册并获得账户批准才能在思科 ISE 中使用 pxGrid 服务。客户端通过 pxGrid SDK 使用 pxGrid 客户端库进行注册。思科 ISE 同时支持自动和手动注册。

- **客户端**: 选择 **管理 > pxGrid 服务 > 客户端管理 > 客户端** 以查看此窗口。列出 pxGrid 2.0 的外部客户端账户。
- **pxGrid 策略**: 选择 **管理 > pxGrid 服务 > 客户端管理 > pxGrid 策略** 以查看此窗口。列出客户端可以订阅的可用服务。您可以编辑策略以更改哪些组可以访问该策略。您还可以为尚无策略的服务创建新策略。

- **组**：选择 **管理 > pxGrid 服务 > 客户端管理 > 组** 以查看此窗口。默认组为 EPS 或 ANC。您可以添加更多组，并使用它们限制对服务的访问。

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。

- **证书**：选择 **管理 > pxGrid 服务 > 客户端管理 > 证书** 以查看此窗口。您可以生成新证书以使用思科 ISE 内部证书颁发机构。

有关为 pxGrid 创建证书的信息，请参阅：

- [随思科 pxGrid 部署证书 - 使用自签证书和思科 ISE 2.0/2.1/2.2 更新](#)
- [随思科 pxGrid 部署证书 - 使用外部 CA 和思科 ISE 2.0/2.1/2.2 更新](#)

控制 pxGrid 策略

您可以创建 pxGrid 授权策略来控制对 pxGrid 客户端可访问服务的访问。这些策略控制哪些服务可供 pxGrid 客户端使用。

您可以创建不同类型的组，并将 pxGrid 客户端的可用服务映射到这些组。使用 **客户端管理 > 组 (Client Management > Groups)** 窗口中的 **管理组 (Manage Groups)** 选项添加新组。您可以在“策略” (Policies) 窗口中查看使用预定义组（例如 EPS 和 ANC）的预定义授权策略。

要为 pxGrid 客户端创建授权策略，请执行以下操作：

步骤 1 选择 **Administration > pxGrid Services > Client Management > Policy**，然后点击 **Add**。

步骤 2 从 **服务 (Service)** 下拉列表中，选择以下选项之一：

- com.cisco.ise.radius
- come.cisco.ise.sxp
- com.cisco.ise.trustsec
- com.cisco.ise.session
- com.cisco.ise.system
- com.cisco.ise.mdm
- com.cisco.ise.config.trustsec
- com.cisco.ise.config.profiler
- com.cisco.ise.pxgrid.admin
- com.cisco.ise.config.deployment.node
- com.cisco.ise.endpoint
- com.cisco.ise.config.anc

- com.cisco.ise.dnac
- com.cisco.ise.config.upn
- com.cisco.ise.pubsub

步骤 3 从操作 (**Operation**) 下拉列表中，选择以下选项之一：

- <ANY>
- 发布
- publish /topic/com.cisco.ise.session
- publish /topic/com.cisco.ise.session.group
- publish /topic/com.cisco.ise.anc
- <CUSTOM> - 如果选择此选项，可以指定自定义操作。

步骤 4 从组 (**Groups**) 下拉列表中，选择要映射到此服务的组。

预定义组（例如 EPS 和 ANC）和手动添加的组列在此下拉列表中。

注释 只有属于策略中的组的客户端才能订阅该策略中指定的服务。

步骤 5 点击提交。

启用 pxGrid 服务

开始之前

- 至少在一个节点上启用 pxGrid 角色，以查看思科 pxGrid 客户端发送的请求。

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **管理 (Administration) > pxGrid 服务 (pxGrid Services)**。

步骤 2 选中该客户端旁边的复选框，然后点击**通过 (Approve)**。

步骤 3 点击**刷新 (Refresh)** 查看最新的状态。

步骤 4 选择要启用的功能，并点击**启用 (Enable)**。

步骤 5 单击**刷新 (Refresh)** 查看最新的状态。

pxGrid 诊断

- **Websocket: Administration > pxGrid Services > Diagnostics > Websocket** 页面列出了外部和内部 pxGrid 2.0 客户端。它还列出了可用 pxGrid 2.0 主题，以及发布或订阅每个主题的客户端。

- 日志： **Administration > pxGrid Services > Diagnostics > Live Logs** 页面列出了管理事件。
- 测试： 选择 **Administration > pxGrid Services > Diagnostics > Tests > Health Monitoring test** 并点击 **开始测试** 验证客户端是否可以访问会话目录服务。测试完成后，您可以查看测试活动的日志。

pxGrid 设置

在 **管理 > pxGrid 服务 > 设置** 窗口中选择以下选项之一：

- **自动批准新的基于证书的账户**：默认情况下，此选项处于禁用状态。它使您可以控制与 pxGrid 服务器的连接。仅当您信任环境中的所有客户端时，才选中此选项。
- **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，系统不会自动批准 pxGrid 客户端。

生成思科 pxGrid 证书

开始之前

- 某些版本的思科 ISE 具有使用 NetscapeCertType 的思科 pxGrid 证书。建议您生成新证书。
- 要执行以下任务，您必须是超级管理员或系统管理员。
- 必须从主 PAN 生成思科 pxGrid 证书。
- 如果思科 pxGrid 证书使用了使用者替代名称 (SAN) 扩展名，请确保将使用者身份的 FQDN 包含为 DNS 名称条目。
- 创建使用数字签名用法的证书模板，并使用该模板生成新的思科 pxGrid 证书。

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **管理 (Administration) > pxGrid 服务 (pxGrid Services) > 客户端管理 (Client Management) > 证书 (Certificates)**。

步骤 2 从 **我想要** 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)。
- **生成单个证书（带证书签名请求） 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。

步骤 3 （可选）输入此证书的说明。

步骤 4 点击 **pxGrid_Certificate_Template** 链接，根据您的要求下载和编辑证书模板。

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

- **IP 地址 (IP address)**：输入要与证书关联的思科 pxGrid 客户端的 IP 地址。


- **FQDN**: 输入 pxGrid 客户端的 FQDN。

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私钥存储在一个加密文件时, 所采用的二进制格式。

步骤 7 输入证书的密码。

步骤 8 点击创建。

您创建的证书可以在**已颁发证书 (Issued Certificates)** 窗口中查看。要查看此处窗口, 请单击**菜单** 图标 () , 然后选择 **管理 > 系统 > 证书 > 证书颁发机构 > 已颁发的证书**。

注释 从思科 ISE 2.4 补丁 13 开始, pxGrid 服务的证书要求变得更加严格。如果您使用思科 ISE 默认自签名证书作为 pxGrid 证书, 则思科 ISE 可能会在应用思科 ISE 2.4 补丁 13 或更高版本后拒绝此证书。这是因为此证书的旧版本具有指定为 **SSL 服务器 (SSL Server) 的 Netscape 证书类型 (Netscape Cert Type)** 扩展, 此扩展现在会失败 (现在还需要客户端证书)。

任何具有不合规证书的客户端都无法与思科 ISE 集成。使用内部 CA 颁发的证书或生成具有正确使用扩展名的新证书:

- 证书中的**密钥用法 (Key Usage)** 扩展名必须包含**数字签名 (Digital Signature)** 和**密钥加密 (Key Encipherment)** 字段。
- 证书中的**扩展密钥用法 (Extended Key Usage)** 扩展必须包含**客户端身份验证 (Client Authentication)** 和**服务器身份验证 (Server Authentication)** 字段。
- 不需要 **Netscape 证书类型 (Netscape Certificate Type)** 扩展。如果要包含此扩展, 则必须在扩展中同时添加 **SSL 客户端 (SSL Client)** 和 **SSL 服务器 (SSL Server)**。
- 如果使用的是自签名证书, 则**基本约束 CA (Basic Constraints CA)** 字段必须设置为 **True**, 并且**密钥用法 (Key Usage)** 扩展必须包含**密钥证书签名 (Key Cert Sign)** 字段。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。