思科 ISE 端口参考

思科 ISE 所有角色节点端口

表 *1:* 所有节点使用的端口

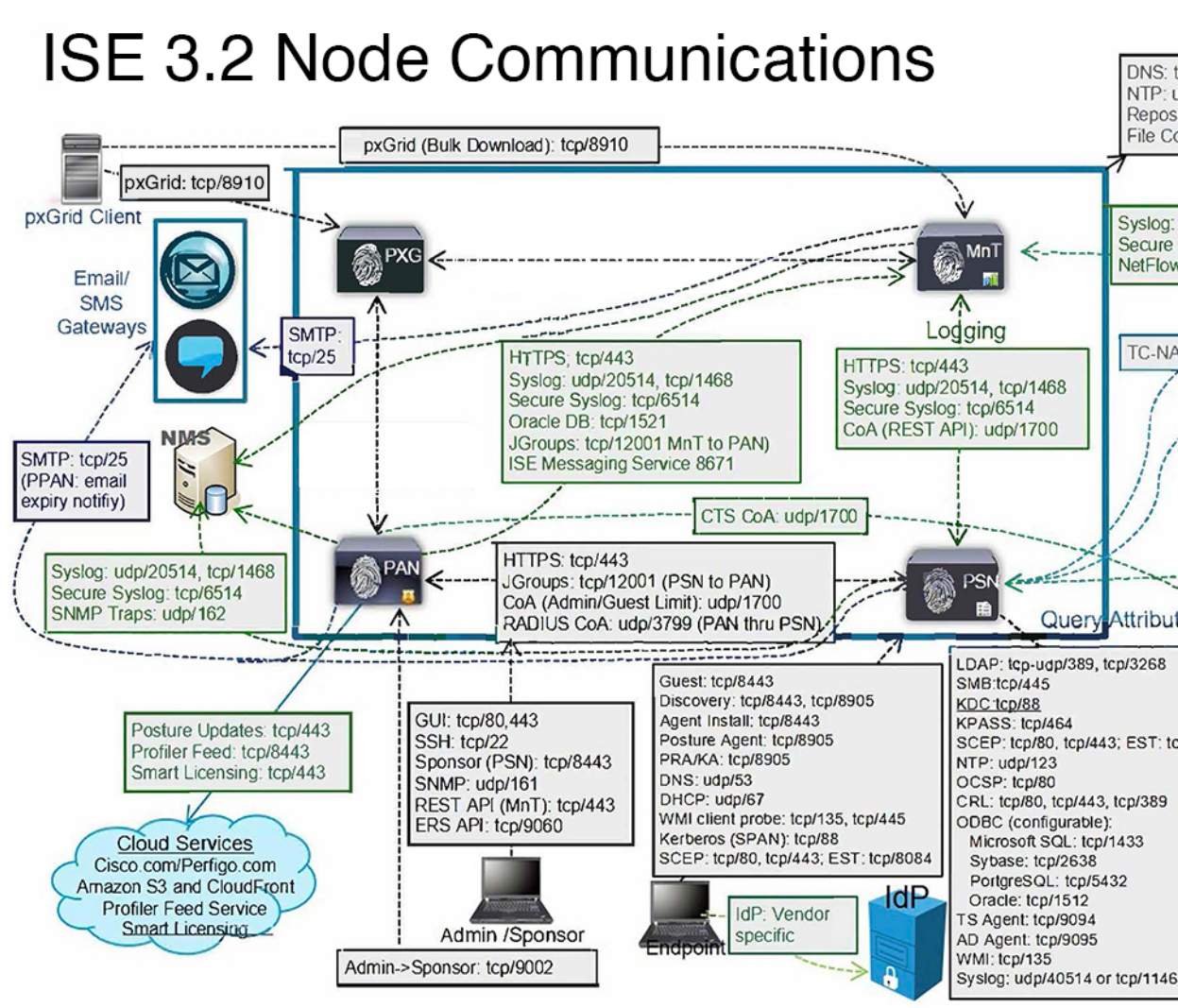
思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）上的端口
复制和同步	• HTTPS (SOAP)：TCP/443 • 数据同步/复制 (JGroups)：TCP/12001（全局） • ISE 消息服务：SSL：TCP/8671 • 分析器终端所有权同步/复制：TCP/6379	—

思科 ISE 基础设施

本附录列出思科 ISE 用于与外部应用和设备进行网络内通信的 TCP 和用户数据报协议 UDP 端口。此附录中列出的思科 ISE 端口在对应的防火墙上必须处于打开状态。

在思科 ISE 网络上配置服务时，请记住以下信息：

- 端口将基于您的部署中启用的服务而启用。除了由ISE中运行的服务打开的端口之外，思科ISE将拒绝访问所有其他端口。
- 思科 ISE 管理只限于千兆以太网 0。
- RADIUS 在所有网络接口卡 (NIC) 上进行侦听。
- 思科 ISE 服务器接口不支持 VLAN 标记。如果在硬件设备上安装，请确保在用于连接到思科 ISE 节点的交换端口上禁用 VLAN 中继，并将这些端口配置为接入层端口。
- 临时端口范围为 10000 到 65500。这在思科 ISE 版本 2.1 及更高版本中保持不变。
- 站点间 VPN 网络配置支持 VMware 云。因此，必须建立从网络访问设备和客户端到思科 ISE 的 IP 地址或端口可访问性，而无需进行 NAT 或端口过滤。
- 所有 NIC 都可以配置有 IP 地址。
- 策略信息点表示外部信息传达给策略服务角色所在的点。例如，外部信息可以是轻量级目录访问协议 (LDAP) 属性。



相关概念

分布式部署中的节点类型和角色

注释 ISE 上的 TCP 保持连接时间为 60 分钟。如果 ISE 节点之间存在防火墙，请在防火墙上相应调整 TCP 超时值。

思科 ISE 管理节点端口

下表列出了管理节点使用的端口：

表 *2:* 管理节点使用的端口

思科 **ISE** 服务	千兆以太网 **0** 或绑定 **0** 上的端口	其他以太网接口（千兆以太网 **1** 至 **5** 或绑定 **1** 和绑定 **2**）上的端口
管理		-

思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）上的端口
	• HTTP：TCP/80 和 HTTPS：TCP/443（TCP/80 重定向到 TCP/443；不可配置） • SSH 服务器：TCP/22 • CoA • 外部 RESTful 服务 (ERS) REST API：TCP/9060 注释 ERS 和 OpenAPI 服务是仅通过端口 443 运行的 HTTPS REST API。目前，ERS API 也通过端口 9060 运行。但是，在更高版本的思科 ISE 中，ERS API 可能不支持端口 9060。我们建议您仅将端口 443 用于 ERS API。 • 适用于 DNAC 集成模式的外部 RESTful 服务 (ERS) REST API 基于证书的身份验证：TCP/9062 • 从管理员 GUI 管理访客帐户：TCP/9002 • ElasticSearch（情景可视性；将数据从主管理节点复制到辅助管理节点）：TCP/9300 注释 端口 80 和 443 支持管理员 Web 应用，并且默认情况下处于启用状态。 对思科 ISE 的 HTTPS 和 SSH 访问只限于千	

思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）上的端口
	兆以太网 0。 TCP/9300 必须在主管理节点和辅助管理节点上对传入流量开放。 注释 对于 SAML 管理员登录，应从管理员尝试执行 SAML 登录的设备访问 PSN 的端口 8443。	
监控	• SNMP 查询：UDP/161 注释 此端口因路由表而异。 • ICMP	
日志记录（出站）	• 系统日志：UDP/20514 和 TCP/1468 • 安全系统日志：TCP/6514 注释 默认端口可配置用于外部日志记录。 • SNMP 陷阱：UDP/162	

思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）上的端口
外部身份源和资源（出站）	• 管理员用户界面和终端身份验证： • LDAP：TCP/389，3268，UDP/389 • SMB：TCP/445 • KDC：TCP/88 • KPASS：TCP/464 • WMI：TCP/135 • ODBC： 注释 ODBC 端口可在第三方数据库服务器上配置。 • Microsoft SQL：TCP/1433 • Sybase：TCP/2638 • PortgreSQL：TCP/5432 • Oracle：TCP/1521、TCPS/2484 • NTP：UDP/123 • DNS：UDP/53 和 TCP/53 注释 对于只能通过除千兆以太网 0 以外的接口访问的外部身份源和服务，请相应地配置静态路由。	
邮件	访客帐户和用户密码到期电子邮件通知：SMTP：TCP/25	
智能许可	通过 TCP/443 连接至思科云 通过 TCP/443 和 ICMP 连接到 SSM 本地服务器	

思科 ISE 监控节点端口

下表列出了监控节点使用的端口：

表 *3:* 监控节点使用的端口

思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）上的端口
管理	• HTTP：TCP/80 和 HTTPS：TCP/443 • SSH 服务器：TCP/22	-
监控	简单网络管理协议 [SNMP]：UDP/161 **注释** 此端口因路由表而异。 • ICMP	
日志记录	• 系统日志：UDP/20514 和 TCP/1468 • 安全系统日志：TCP/6514 **注释** 默认端口可配置用于外部日志记录。 • SMTP：TCP/25 用于警报电子邮件 • SNMP 陷阱：UDP/162	

思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）上的端口
外部身份源和资源（出站）	• 管理员用户界面和终端身份验证： • LDAP：TCP/389，3268，UDP/389 • SMB：TCP/445 • KDC：TCP/88 和 UDP/88 • KPASS：TCP/464 • WMI：TCP/135 • ODBC： 注释 ODBC 端口可在第三方数据库服务器上配置。 • Microsoft SQL：TCP/1433 • Sybase：TCP/2638 • PortgreSQL：TCP/5432 • Oracle：TCP/1521，15723，16820 • NTP：UDP/123 • DNS：UDP/53 和 TCP/53 注释 对于只能通过除千兆以太网 0 以外的接口访问的外部身份源和服务，请相应地配置静态路由。	
用于入站通信的端口	• 源自启用了 ISE API 网关以路由 MnT REST API 的 ISE 节点的 MnT 入站通信：TCP/9443 • TCP/1521：必须为 MnT 节点启用端口 1521。来自 PAN 的入站通信需要端口 1521。如果未为 MnT 节点启用此端口，则 MnT 节点故障切换可能会导致日志或报告丢失。 注释 无论是现场还是云，这些端口在所有类型的部署中均为必需。	
pxGrid 批量下载	SSL：TCP/8910	

思科 ISE 策略服务节点端口

思科 ISE 支持 HTTP 严格传输安全 (HSTS) 以提高安全性。思科 ISE 发送 HTTPS 响应，以向浏览器指示只能使用 HTTPS 访问 ISE。如果用户随后尝试使用 HTTP 而不是 HTTPS 访问 ISE，则浏览器会在生成任何网络流量之前将连接更改为 HTTPS。此功能可防止浏览器使用未加密的 HTTP 向思科 ISE 发送请求，避免服务器重定向这些请求。

下表列出了策略服务节点使用的端口：

表 *4:* 策略服务节点使用的端口

思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口上或绑定 1 和绑定 2 上的端口
管理	• HTTP：TCP/80 和 HTTPS：TCP/443 • SSH 服务器：TCP/22 • OCSP：TCP/2560	思科 ISE 管理只限于千兆以太网 0。
集群（节点组）	节点组/JGroups：TCP/7800	—
SCEP	TCP/9090	-
IPSec/ISAKMP	UDP/500	-
设备管理	TACACS+：TCP/49 **注释** 此端口可在版本 2.1 及更高版本中配置。	
TrustSec	使用 HTTP 和思科 ISE REST API 通过端口 9063 将 TrustSec 数据传输到网络设备。	
SXP	• PSN（SXP 节点）到 NAD：TCP/64999 • PSN 到 SXP（节点间通信）： TCP/9644	
TC-NAC	TCP/443	
监控	简单网络管理协议 [SNMP]：UDP/161 **注释** 此端口因路由表而异。	

思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口上或绑定 1 和绑定 2 上的端口
日志记录（出站）	• 系统日志：UDP/20514 和 TCP/1468 • 安全系统日志：TCP/6514 注释 默认端口可配置用于外部日志记录。 • SNMP 陷阱：UDP/162	
会话	• RADIUS 身份验证：UDP/1645 和 1812 • RADIUS 记帐：UDP/1646 和 1813 • RADIUS DTLS 身份验证/记帐：UDP/2083 • RADIUS 授权变更 (CoA) 发送：UDP/1700 • RADIUS 授权变更 (CoA) 侦听/中继：UDP/1700 和 3799 注释 UDP 端口 3799 不可配置。	

思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口上或绑定 1 和绑定 2 上的端口

外部身份源和资源（出站）	• 管理员用户界面和终端身份验证：
	  • LDAP：TCP/389 和 3268
	  • SMB：TCP/445
	  • KDC：TCP/88
	  • KPASS：TCP/464
	• WMI：TCP/135
	• ODBC：
	注释 ODBC 端口可在第三方数据库服务器上配置。
	  • Microsoft SQL：TCP/1433
	  • Sybase：TCP/2638
	  • PortgreSQL：TCP/5432
	  • Oracle：TCP/1521
	• NTP：UDP/123
	• DNS：UDP/53 和 TCP/53
	注释 对于只能通过除千兆以太网 0 以外的接口访问的外部身份源和服务，请相应地配置静态路由。	

被动 ID（入站）	• TS 代理：tcp/9094 • AD 代理：tcp/9095 • 系统日志：UDP/40514 和 TCP/11468	
Web 门户服务： - 访客/Web 身份验证 - 访客发起人门户 - 我的设备门户 - 客户端调配 - 证书调配 - 阻止列表门户	HTTPS（必须为思科 ISE 中的服务启用接口）： • 阻止列表门户：TCP/8000-8999（默认端口为 TCP/8444） • 访客门户和客户端调配：TCP/8000-8999（默认端口为 TCP/8443） • 证书调配门户：TCP/8000-8999（默认端口为 TCP/8443） • 我的设备门户：TCP/8000-8999（默认端口为 TCP/8443） • 发起人门户：TCP/8000-8999（默认端口为 TCP/8445） • 来自访客和发起人门户的 SMTP 访客通知：TCP/25	

思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口上或绑定 1 和绑定 2 上的端口
状态 - 发现 - 调配 - 评估/心跳	• 发现（客户端）：TCP/80 (HTTP) 和 TCP/8905 (HTTPS) 注释 默认情况下，TCP/80 重定向到 TCP/8443。请参阅“Web 门户服务：访客门户和客户端调配”。 思科 ISE 在 TCP 端口 8905 上提供安全评估和客户端调配管理证书。 思科 ISE 在 TCP 端口 8443（或者您为使用门户而配置的端口）上提供门户证书。 从思科 ISE 3.1开始，非策略服务节点上已默认禁用端口 8905。要启用此端口，请在**常规设置 (General Settings)** 窗口（**管理 (Administration) > 系统 (System) > 设置 (Settings) > 安全评估 (Posture) > 一般设置 (General Settings)**）中选中**在非政策服务节点上为安全评估服务启用 8905 端口 (Enable Port 8905 on non-Policy Service Nodes for Posture Services)** 复选框。 • 发现（策略服务节点端）：TCP/8443 和 8905 (HTTPS) 从思科 ISE 版本 2.2 或更高版本以及 AnyConnect 版本 4.4 或更高版本开始，此端口可配置。 • 评估 - 状态协商和代理报告：TCP/8905 (HTTPS) • 双向安全评估流程 - TCP/8000-8999（默认端口为 TCP/8449）	
自带设备 (BYOD)/网络服务协议 (NSP) - 重定向 - 调配 - SCEP	• 调配 - URL 重定向：请参阅“Web 门户服务：访客门户和客户端调配”。 • 对于使用 EST 身份验证的 Android 设备：TCP/8084。对于 Android 设备，端口 8084 必须添加到重定向 ACL。 • 调配 - Active-X 和 Java Applet 安装（包括启动向导安装）：请参阅“Web 门户服务：访客门户和客户端调配” • 调配 - 从思科 ISE（Windows 和 Mac 操作系统）执行向导安装：TCP/8443 • 调配 - 从 Google Play (Android) 执行向导安装：TCP/443 • 调配 - 请求方调配过程：TCP/8905 • SCEP 代理至 CA：TCP/80 或 TCP/443（基于 SCEP RA URL 配置）	

思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口上或绑定 1 和绑定 2 上的端口
移动设备管理 (MDM) API 集成	• URL 重定向：请参阅“Web 门户服务：访客门户和客户端调配” • API：供应商专用 • 代理安装和设备注册：供应商专用	
分析	• NetFlow：UDP/9996 注释 此端口是可配置的。 • DHCP：UDP/67 注释 此端口是可配置的。 • DHCP SPAN 探测：UDP/68 • HTTP：TCP/80 和 8080 • DNS：UDP/53（查找） 注释 此端口因路由表而异。 • SNMP 查询：UDP/161 注释 此端口因路由表而异。 • SNMP 陷阱：UDP/162 注释 此端口是可配置的。	

思科 ISE pxGrid 服务端口

注释 从思科 ISE 版本 3.1开始，所有 pxGrid 连接都必须基于 pxGrid 版本 2.0。基于 pxGrid 版本 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）。

下表列出了 pxGrid 服务节点使用的端口：

表 *5: pxGrid* 服务节点使用的端口

思科 ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）上的端口
pxGrid 用户	TCP/8910	

OCSP 和 CRL 服务端口

尽管思科 ISE 服务和端口参考分别列出了在思科 ISE 管理节点、策略服务节点监控节点中所用的基本端口，但对于在线证书状态协议服务 (OCSP) 和证书撤销列表 (CRL)，端口取决于 CA 服务器或托管 OCSP/CRL 的服务。

对于 OCSP，可以使用的默认端口是 TCP 80/TCP 443。思科 ISE 管理员门户希望对 OCSP 服务使用基于 http 的 URL，因此默认值为 TCP 80。您还可以使用非默认端口。

对于 CRL，默认协议包括 HTTP、HTTPS 和 LDAP，默认端口分别为 80、443 和 389。实际端口取决于 CRL 服务器。

思科 ISE 进程

下表列出了思科 ISE 进程及其服务影响：

进程名称	说明	服务影响
数据库侦听程序	Oracle 企业数据库侦听程序	必须处于运行状态，所有服务才能正常工作
数据库服务器	Oracle 企业数据库服务器。存储配置数据与操作数据。	必须处于运行状态，所有服务才能正常工作
应用服务器	ISE 的主 Tomcat 服务器	必须处于运行状态，所有服务才能正常工作
分析器数据库	用于 ISE 分析服务的 Redis 数据库	必须处于运行状态，ISE 分析服务才能正常工作
AD 连接器	Active Directory 运行时	必须处于运行状态，ISE 才能执行 Active Directory 身份验证
MnT 会话数据库	用于 MnT 服务的 Oracle TimesTen 数据库	必须处于运行状态，所有服务才能正常工作
MnT 日志收集器	用于 MnT 服务的日志收集器	必须处于运行状态才能获取 MnT 操作数据
MnT 日志处理器	用于 MnT 服务的日志处理器	必须处于运行状态才能获取 MnT 操作数据
证书颁发机构服务	ISE 内部 CA 服务	如果已启用 ISE 内部 CA，则必须处于运行状态

所需互联网 URL

下表列出了会使用某些 URL 的功能。配置网络防火墙或代理服务器，这样 IP 流量才能在思科 ISE 和这些资源之间传输。如果无法访问下表中列出的任何 URL，则表明相关功能可能已损坏或无法运行。

表 *6:* 所需 *URL* 访问权限

特性	URL
安全评估更新	https://www.cisco.com/ https://iseservice.cisco.com
分析源服务	https://ise.cisco.com
智能许可	https://tools.cisco.com

交互式帮助功能需要使用思科 ISE 才能使用管理门户浏览器连接到以下 URL：

- * .walkme.com
- * .walkmeusercontent.com

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。