开始使用 ISE-PIC

管理员访问控制台

以下步骤说明了如何登录管理门户。

开始之前

确保已正确安装（或升级）并配置思科ISE-PIC。有关思科ISE-PIC的安装、升级和配置的详细信息与帮助，请参阅《身份服务引擎被动身份连接器 *(ISE-PIC)* 安装和升级指南》。

步骤 1 在浏览器地址栏中输入思科 ISE-PIC URL（例如 https://<ise hostname or ip address>/admin/）。

步骤 2 输入在思科 ISE 初始设置过程中指定和配置的用户名及区分大小写的密码。

步骤 3 点击**登录 (Login)** 或按 **Enter**。

如果您登录不成功，请在登录窗口中点击**登录遇到问题？(Problem logging in?)** 链接并按照显示的说明操作。

管理员登录浏览器支持

思科 ISE 管理门户支持以下支持 HTTPS 的浏览器：

- Mozilla Firefox 107 和从版本 82 起的更早版本
- Mozilla Firefox ESR 102.4 及更低版本
- Google Chrome 107 和从版本 86 起的更早版本
- Microsoft Edge，最新版本和一个早于最新版本的版本

ISE 社区资源

使用 Adblock Plus 时，ISE 页面无法完全加载

使用 Diffie-Hellman 算法保护 SSH 密钥交换

将思科 ISE-PIC 配置为仅允许 Diffie-Hellman-Group14-SHA1 SSH 密钥交换。在思科 ISE-PIC CLI 配置模式下输入以下命令：

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

以下为输出示例：

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

初始设置和配置

要快速开始使用思科 ISE-PIC，请遵循以下流程：

1. 安装并注册许可证。有关详细信息，请参阅ISE-PIC 智能许可 ，第 2 页。
2. 确保您已正确配置 DNS 服务器，包括从思科 ISE-PIC 配置客户端机器的反向查找。有关详细信息，请参阅DNS 服务器 ，第 5 页。
3. 同步 NTP 服务器的时钟设置。
4. 使用 ISE-PIC设置来配置初始提供程序。有关详细信息，请参阅PassiveID 设置入门。
5. 配置单个或多个用户。

设置初始提供程序和用户后，可以轻松创建其他提供程序（请参阅提供程序）并从ISE-PIC（请参阅ISE-PIC 中的监控和故障排除服务）中的不同提供程序管理被动识别。

ISE-PIC 智能许可

ISE-PIC 3.1 和更高版本许可证完全通过名为思科智能软件管理器 (CSSM) 的集中式数据库进行管理。您可以通过单令牌注册轻松、高效地注册、激活和管理所有许可证。

ISE-PIC 3.1 和更高版本仅支持智能许可，不支持传统许可。如果您拥有传统 ISE-PIC 许可证，必须将其转换为智能许可证，才能在 ISE-PIC 3.1 和更高版本中启用许可证合规。

当您首次安装 ISE-PIC 时，默认情况下会启用评估许可证。评估许可证是 90 天的许可证，允许您访问所有 ISE-PIC 功能。在评估期间，许可证合规状态不会报告给 CSSM。

ISE-PIC 管理门户的右上角显示一条消息，其中包含评估模式下剩余的天数。您必须购买并激活所需的许可证，才能继续使用所需的 ISE-PIC 功能。

当智能许可证令牌处于活动状态并在 ISE-PIC 管理门户中注册时，CSSM 会监控 ISE-PIC 节点的许可证合规性状态。许可证合规性状态显示在 ISE-PIC 的**许可证 (Licenses)** 表中。要查看这些信息，请选择**管理 (Administration) > 系统 (System) > 许可 (Licensing)**。

自您向 CSSM 注册 ISE-PIC 以来，ISE-PIC 会每六小时向 CSSM 服务器报告一次许可证合规状态。ISE-PIC 通过存储 CSSM 证书的本地副本与 CSSM 服务器通信。在每日同步期间以及刷新**许可证 (Licenses)** 表时，系统会自动重新授权 CSSM 证书。通常，CSSM 证书有效期为六个月。

注册证书每六个月自动刷新一次。要手动刷新智能许可注册证书，请在**许可 (Licensing)** 窗口顶部点击**更新注册 (Renew Registration)**。

如果 ISE-PIC 与 CSSM 服务器同步时合规状态有变化，则**许可证 (Licenses)** 表的**最后授权 (Last Authorization)** 列会相应更新。此外，当权益不再合规时，**不合规天数 (Days Out of Compliance)** 列中会显示它们处于不合规状态地天数。

在以下情况下，您应更新许可协议：

- 试用期结束，而您尚未注册您的许可证。
- 您的许可证已过期。

启用 Essential 许可证可以将 ISE-PIC 节点升级为思科 ISE 节点。在启用基本许可证之前，您必须在 ISE-PIC 节点上购买并启用 ISE-PIC 和 ISE-PIC 升级许可证。在 CSSM 中注册许可证后，基本许可证会显示在**许可证 (Licenses)** 表中。应用服务会在升级期间重新启动。有关思科 ISE 许可证的信息，请参阅《思科身份服务引擎管理员指南》。

ISE-PIC 3.1 和更高版本支持 VM 通用许可证。此许可证替换在 3.1 之前版本中支持的 VM 小型、VM 中型和 VM 大型许可证。这个 VM 许可证涵盖内部部署和云部署中的 VM 节点。如果您有旧版 VM 许可证，则必须在升级到思科 ISE 3.1 和更高版本时将 VM 许可证迁移到 VM 通用许可证。要将旧版许可证转换为新的许可证类型，请通过支持案例管理器 (http://cs.co/scmswl) 或使用 http://cs.co/TAC-worldwide 中提供的联系信息在线提交支持案例。

有关许可状态的警报（例如许可证注册成功或失败、许可证不合规、评估许可证到期、智能许可通信故障）会显示在**警报 (Alarms)** dashlet 中。

ISE-PIC 许可证包

以下许可证包可用于 ISE-PIC：

许可证包	订用	涵盖的功能	注
ISE-PIC	永久	被动身份服务	每个节点一个许可证。每个许可证最多支持 3000 个并行会话。
ISE-PIC 升级	永久	• 启用其他（最多 300,000 个）并行会话 • 升级到完整 ISE 实例	每个节点一个许可证。每个许可证最多支持 300,000 个并行会话。

Essential	基于期限的许可证	• RADIUS 身份验证、授权和记账，包括 802.1X、MAC 身份验证绕过和轻松连接，以及 Web 身份验证 • MACsec • 基于单点登录 (SSO)、安全断言标记语言 (SAML) 和开放式数据库连接 (ODBC) 标准的身份验证 • 访客门户和发起人服务 • 用于监控目的的具象状态传输 (REST) API，以及用于 CRUD 操作的外部 RESTful 服务 API • 被动 ID 服务 • 安全有线和无线接入	—
Evaluation	临时（90 天）	在 90 天内启用完整 ISE-PIC 功能	—

注册并激活智能许可证

开始之前

- 如果您有传统的 ISE-PIC 许可证，必须将其转换为智能许可证。
- 在 CSSM 中注册新的智能许可证类型，以接收注册令牌。

步骤 1 在 ISE-PIC 中，点击**菜单**图标 (☰) 并选择**管理 (Administration)** > **系统 (System)** > **许可 (Licensing)**。

步骤 2 点击**注册详细信息 (Registration Details)**。

步骤 3 在**注册详细信息 (Registration Details)** 区域中，在**注册令牌 (Registration Token)** 字段中输入从 CSSM 收到的注册令牌。

步骤 4 从**连接方法 (Connection Method)** 下拉列表中选择连接方法：

- **直接 HTTPS (Direct HTTPS)**：如果已配置与互联网的直接连接，则可选择此选项。
- **HTTPS 代理 (HTTPS Proxy)**：如果没有与互联网的直接连接且需要使用代理服务器，则可选择此选项。如果在注册智能许可证后更改代理服务器配置，则必须在**许可 (Licensing)** 窗口中更新智能许可证配置。ISE-PIC 使用更新的代理服务器与 CSSM 建立连接，避免 ISE-PIC 服务中断。
- **传输网关 (Transport Gateway)**：这是推荐选项。如果已配置传输网关，则默认选择此连接。要选择其他连接方法，您必须删除传输网关配置。

- **SSM 本地部署服务器 (SSM On-Prem Server)**：要连接到配置的 SSM 本地服务器，则可选择此选项。

步骤 5 在**层 (Tier)** 和**虚拟设备 (Virtual Appliance)** 区域中，选中您需要启用的所有许可证的复选框。系统将激活所选许可证，并由 CSSM 跟踪其合规情况。

步骤 6 点击**注册 (Register)**。

注册许可证令牌后，如果您的 CSSM 帐户不包括特定授权，并且您没有在注册期间禁用它们，则 ISE-PIC 中将显示不合规通知。将这些授权添加到您的 CSSM 帐户，然后点击**许可证 (Licenses)** 表中的**刷新 (Refresh)** 以删除不合规通知。

要从您的智能帐户删除 ISE-PIC 注册，但是继续使用智能许可直到评估期结束，请在**思科智能许可 (Cisco Smart Licensing)** 区域的顶部点击 **取消注册 (Deregister)** 。如果您的评估期仍有剩余时间，则 ISE-PIC 仍处在智能许可中。如果评估即将过期，则在刷新浏览器时会显示通知。取消注册智能许可证后，您可以遵循注册流程以相同或不同的 UDI 再次注册。

特定许可证预留

特定许可证预留是一种智能许可方法，当您的组织的安全要求不允许 ISE-PIC 与 CSSM 之间存在持久连接时，可帮助您管理智能许可。特定许可证预留允许您在思科 ISE-PIC 节点上保留特定许可证授权。

您可以通过定义需要预留的许可证的类型和数量来创建特定许可证预留，然后在 ISE-PIC 节点上激活预留。然后，您在其上注册并启用预留的 ISE-PIC 节点会跟踪许可证使用情况，同时强制执行许可证使用合规性。

注释 使用特定许可证预留时，无法将 ISE-PIC 节点升级到思科 ISE 节点。为了升级，您必须首先返回特定许可证预留，启用智能许可注册，然后安装 ISE-PIC 升级和基本许可证。

DNS 服务器

在配置您的 DNS 服务器时，请确保注意以下事项：

- 您在思科 ISE 中配置的 DNS 服务器必须能够解析要使用的域的所有正向和反向 DNS 查询。
- 建议使用权威 DNS 服务器来解析 Active Directory 记录，因为 DNS 递归可能会导致延迟并对性能造成重大不利影响。
- 所有 DNS 服务器都必须能够对 DC、GC 和 KDC（无论它们是否具有额外的站点信息）的 SRV 查询作出应答。
- 思科建议向 SRV 响应添加服务器 IP 地址以提高性能。
- 避免使用查询公共互联网的DNS服务器。当必须解析未知名称时，这些服务器可能会泄漏有关网络的信息。

指定系统时间和网络时间协议服务器设置

思科 ISE-PIC 允许最多配置三个 NTP 服务器。使用 NTP 服务器维护正确时间和同步不同时区的时间。您还可以指定思科 ISE-PIC 是否必须只使用经过身份验证的 NTP 服务器，并为此目的输入一个或更多身份验证密钥。

我们建议将所有思科 ISE-PIC 节点均设置为协调世界时 (UTC) 时区。此程序可确保来自您的部署中各个节点的报告和日志的时间戳始终同步。

思科 ISE 支持 NTP 服务器的公共密钥身份验证。NTP 版本 4 使用对称密钥加密，但是也可根据公共密钥加密提供新的自动密钥安全模型。公共密钥加密比对称密钥加密更安全。这是因为安全性基于每个服务器生成并且从不会泄露的专用值。如果使用自动密钥安全模型，所有密钥分发和管理功能都将仅涉及公共值，可在很大程度上简化密钥分发和存储。

您可以在配置模式下从思科 ISE CLI 将 NTP 服务器配置为使用自动密钥安全模型。我们建议您使用敌我识别 (IFF) 系统，因为该系统使用最为广泛。

步骤 1 在思科 ISE GUI 中，点击**菜单**图标 (☰) 并选择 **设置 (Settings)** > **系统时间 (System Time)**。

步骤 2 在 **NTP 服务器配置** 区域中，输入 NTP 服务器的唯一 IP 地址（IPv4 或 IPv6 或完全限定域名 (FQDN) 值）。

步骤 3 （可选）要使用专用密钥对 NTP 服务器进行身份验证，并且您指定的服务器中有任意服务器要求通过身份验证密钥进行身份验证，请点击 **NTP 身份验证密钥** 选项卡并指定一个或更多身份验证密钥。执行以下步骤：

a) 点击**添加 (Add)**。

b) 在**密钥 ID (Key ID)** 和**密钥值 (Key Value)** 字段中输入必要的值。从 **HMAC** 下拉列表中选择所需的散列消息验证码 (HMAC) 值。**密钥 ID (Key ID)** 字段支持 1 至 65535 之间的数值，**密钥值 (Key Value)** 字段支持最多 15 个字母数字字符。

c) 点击**确定 (OK)**。

d) 返回**NTP 服务器配置 (NTP Server Configuration)** 选项卡。

步骤 4 （可选）要使用公共密钥身份验证对 NTP 服务器进行身份验证，请从 CLI 配置思科 ISE 上的自动密钥安全模型。请参阅对应于您的 ISE 版本的《思科身份识别服务引擎 CLI 参考指南》中的 **ntp server** 和 **crypto** 命令。

步骤 5 点击**保存 (Save)**。

注释 使用三台或更多台 NTP 服务器可确保网络中的时间同步，即使其中一台服务器发生故障或两台服务器不同步。请参阅https://insights.sei.cmu.edu/blog/best-practices-for-ntp-services。

ISE-PIC主页控制板

思科ISE-PIC主页控制板显示对于有效地进行监控和故障排除很重要的综合性相关摘要和统计数据，并实时更新。Dashlet 显示过去 24 小时的活动，另有说明的情况除外。

- **主要 (Main)** 视图具有线性指标控制板、饼形图 Dashlet 和列表 Dashlet。在 ISE-PIC 中，Dashlet 不可配置。将显示某些 Dashlet，这些 Dashlet 仅在 ISE 的完整版本中提供。例如，显示终端数据的 Dashlet。可用 Dashlet 包括：
  - **被动身份指标 (Passive Identity Metrics)**：显示当前跟踪的唯一实时会话总数、系统中配置的身份提供程序总数、主动提供身份数据的代理总数，以及当前配置的用户总数。
  - **提供程序 (Providers)**：提供程序向 ISE-PIC 提供用户身份信息。可以配置 ISE-PIC 探测器（从给定源收集数据的机制），并通过此探测器从提供程序源接收信息。例如，Active Directory (AD) 探测器和代理探测器均可帮助 ISE-PIC 从 AD 收集数据（每个采用不同的技术），而系统日志探测器可从读取系统日志消息的解析器收集数据。
  - **用户 (Subscribers)**：用户连接至 ISE-PIC 以检索用户身份信息。
  - **操作系统类型 (OS Types)**：可以显示的唯一操作系统类型为 Windows。Windows 类型按 Windows 版本显示。提供程序不报告操作系统类型，但 ISE-PIC 可查询 Active Directory 以获取此信息。Dashlet 中最多显示 1000 个条目。如果您的终端数量超过此最大数目，或者您希望显示除 Windows 以外的更多操作系统类型，可以升级至 ISE。
  - **警报 (Alarms)**：用户身份相关警报。
- **其他 (Additional)** 视图显示 PIC 上的活动会话，以及 PIC 系统的系统摘要。

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。