



## 开始使用 ISE-PIC

---

- [管理员访问控制台，第 1 页](#)
- [初始设置和配置，第 2 页](#)
- [ISE-PIC 主页控制板，第 6 页](#)

### 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 **Login** 或按 **Enter**。

如果您登录不成功，请在登录窗口中单击[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 版本 88 及更低版本
- Mozilla Firefox ESR 版本 60.9 及更低版本
- Google Chrome 版本 90 及更低版本

[ISE 社区资源](#)

使用 Adblock Plus 时，ISE 页面无法完全加载

## 管理员由于登录尝试失败而锁定

如果在输入管理员用户 ID 的密码时错误次数足够多，则该帐户将在指定时间内暂停使用或被锁定（根据配置而定）。如果思科 ISE 被配置为将您锁定，则管理门户会将您锁定在系统之外。思科 ISE 会在“服务器管理员登录”(Server Administrator Logins)报告中添加一条日志，同时吊销该管理员 ID 的凭证。重置该管理员 ID 的密码，如《[思科身份服务引擎安装指南](#)》中的“重置因管理员锁定而禁用的密码”一节所述。禁用管理员帐户之前允许的失败登录尝试次数可按照《[思科身份服务引擎管理员指南](#)》中[对思科 ISE-PIC 进行管理访问](#)一节进行配置。管理员用户帐户被锁定后，思科 ISE 会向关联的用户（如已配置相关信息）发送电子邮件。

## 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[思科 ISE-PIC 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。有关详细信息，请参阅[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。

## 思科 ISE-PIC 许可

系统为思科 ISE-PIC 提供 90 天的评估期。要在 90 天评估许可证到期后继续使用思科 ISE-PIC，您必须在系统上获取并注册许可证。ISE-PIC 将提前 90、60 和 30 天通知您评估许可证到期。

每个永久许可证都会上传到单个 ISE-PIC 节点，如果部署中有两个节点，则第二个节点需要单独的许可证。完成安装后，为每个 UDI 生成单独的许可证，然后将许可证分别添加到每个节点。

### 许可安装和注册流程

1. 安装和注册 ISE-PIC 许可证。有关安装和注册 ISE-PIC 许可证的详细信息，请参阅[注册许可证，第 4 页](#)。您可以通过以下任一方式安装许可证：
  - 在安装 ISE-PIC 后立即安装。
  - 在 90 天评估期内随时安装。
2. 要轻松升级到基本 ISE 部署，请先安装思科 ISE-PIC 升级许可证，然后执行以下操作：
  - 安装 ISE 基础许可证，以便使用先前的 ISE-PIC 节点作为部署的主管理节点 (PAN)。
  - 将已升级的 PIC ISE-PIC 节点添加到现有 ISE 部署。
3. 安装任何其他相关许可证（Plus、Apex、TACACs+ 等），可轻松升级基本 ISE 部署并升级到智能许可。有关安装 ISE 许可证的详细信息，请参阅《思科身份服务引擎管理员指南》。

### 思科 ISE 许可证包

表 1: 所有思科 ISE 许可证包选项

ISE 许可证包	永久/订用（可用的期限）	涵盖的 ISE 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	此许可证允许以下选项： <ul style="list-style-type: none"> <li>• 启用其他（最多 300,000 个）并行会话。</li> <li>• 升级到完整 ISE 实例</li> </ul>	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。 安装此许可证后，已升级的节点即可加入现有 ISE 部署，或者在节点上安装基础许可证，以便用作 PAN。

Base	永久	<ul style="list-style-type: none"> <li>• 基本网络接入: AAA、IEEE-802.1X</li> <li>• 访客服务</li> <li>• 链路加密 (MACSec)</li> <li>• TrustSec</li> <li>• ISE 应用编程接口</li> </ul>	
Evaluation	临时 (90 天)	在 90 天内启用完整 ISE-PIC 功能。	

## 注册许可证

### 开始之前

安装 ISE-PIC 后，您有 90 天的评估期。您必须购买、注册和安装 ISE-PIC 许可证，以便继续顺利工作。如果您在到期之前尚未注册并安装许可证，则在到期后访问 ISE-PIC 时，所有 ISE-PIC 服务都处于禁用状态，并且系统会自动将您导航到导入许可证区域，从中可以完成该过程。有关 ISE-PIC 许可证的信息，请咨询思科合作伙伴/客户团队。

**步骤 1** 从思科网站上的订购系统（思科商务工作空间 - CCW）[www.cisco.com](http://www.cisco.com)，订购所需的许可证。对于部署中的每个节点（每个部署最多两个节点），您需要一个 ISE-PIC 许可证。

大约 1 小时后，系统会发送包含产品授权密钥 (PAK) 的确认邮件。

**步骤 2** 在思科 ISE-PIC 管理门户中，依次选择**管理 (Administration)** > **许可 (Licensing)**。在 **Licensing Details** 部分记录节点信息：产品标识 (PID)、版本标识 (VID) 和序列号 (SN)。

### 步骤 3

**步骤 4** 转至 [www.cisco.com/go/licensing](http://www.cisco.com/go/licensing)，在系统提示时，输入您所收到的许可证 PAK、节点信息以及关于您公司的一些详细信息。

一天之后，思科会向您发送许可文件。

**步骤 5** 请将此许可证文件保存至您的系统上的已知位置

**步骤 6** 在思科 ISE-PIC 管理门户中，依次选择**管理 (Administration)** > **许可 (Licensing)**。

**步骤 7** 在许可证部分中，点击**导入许可证**按钮。

**步骤 8** 点击 **Choose File**，然后选择您之前存储于系统上的许可文件。

**步骤 9** 点击 **Import**。

新许可证即已安装在您的系统上。

### 下一步做什么

依次选择“许可”控制面板中的**管理 > 许可**，然后验证新输入的许可证是否显示正确的详细信息。

## 删除许可证

### 开始之前

删除过期或不需要的许可证可以消除弹出提醒，并回收“许可”(Licensing)控制板上的空间。

**步骤 1** 依次选择 **管理 (Administration) > 许可 (Licensing)**

**步骤 2** 在 **License Files** 部分，点击相关文件名旁边的复选框，然后点击 **Delete License**。

**步骤 3** 点击确定。

## 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可能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。相比对称密钥加密，公共密钥加密更为安全。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** 选择 **设置 (Settings) > 系统时间 (System Time)**。

**步骤 2** 在 **NTP 服务器配置 (NTP Server Configuration)** 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** 选中 **仅允许已通过身份验证的 NTP 服务器 (Only allow authenticated NTP servers)** 复选框，以便限制思科 ISE 仅使用经过身份验证的 NTP 服务器保留系统和网络时间。

**步骤 4** （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，请单击 **NTP 身份验证密钥 (NTP Authentication Keys)** 选项卡并指定一个或多个身份验证密钥。执行以下步骤：

- a) 点击添加。
- b) 在 **密钥 ID (Key ID)** 和 **密钥值 (Key Value)** 字段中输入必要的值。通过选中或取消选中 **可信密钥 (Trusted Key)** 复选框来指定是否信任所述密钥，然后单击 **确定 (OK)**。**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。
- d) 返回 **NTP 服务器配置 (NTP Server Configuration)** 选项卡。

**步骤 5** （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 6** 点击保存。

## 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。

