



## 思科身份服务引擎被动身份连接器管理员指南，版本 3.1

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2021 Cisco Systems, Inc. 保留所有权利。



## 目录

---

### 第 1 章

#### 简介 ISE-PIC 1

- 思科 ISE-PIC 术语 1
- ISE-PIC 概述 2
- 思科 ISE-PIC 架构、部署和节点 3
- ISE-PIC 的优势 4
- 比较 ISE-PIC 与 ISE 和 CDA 5

---

### 第 2 章

#### 开始使用 ISE-PIC 9

- 管理员访问控制台 9
  - 管理员登录浏览器支持 9
  - 使用 Diffie-Hellman 算法保护 SSH 密钥交换 10
- 初始设置和配置 10
  - ISE-PIC 智能许可 10
    - ISE-PIC 许可证包 11
    - 注册并激活智能许可证 12
    - 特定许可证预留 13
  - DNS 服务器 13
  - 指定系统时间和网络时间协议服务器设置 14
- ISE-PIC 主页控制板 14

---

### 第 3 章

#### Active Directory 作为探测器和提供程序 17

- 使用 Active Directory 17
  - PassiveID 设置入门 18
  - 分步设置 Active Directory (WMI) 探测器 20

添加 Active Directory 加入点并将思科 ISE-PIC 节点加入到该加入点	20
添加域控制器	22
配置 Active Directory 用户组	22
对被动 ID 配置 WMI	23
管理 Active Directory 提供程序	23
对用户进行 Active Directory 组测试	24
查看节点的 Active Directory 加入	24
诊断 Active Directory 问题	25
退出 Active Directory 域	25
删除 Active Directory 配置	26
启用 Active Directory 调试日志	26
Active Directory 设置	27

---

**第 4 章****提供程序 31**

Active Directory 代理	33
自动安装并部署 Active Directory 代理	34
手动安装并部署 Active Directory 代理	35
卸载代理	36
Active Directory 代理设置	36
API 提供程序	37
为被动身份服务配置与 ISE-PIC REST 服务的桥接	38
将 API 调用发送到 ISE-PIC REST 服务	39
API 提供程序设置	39
API 调用	40
SPAN	42
使用 SPAN	42
SPAN 设置	43
系统日志提供程序	43
配置系统日志客户端	44
系统日志设置	45
自定义系统日志消息结构（模板）	48

自定义系统日志消息正文	49
自定义系统日志报头	50
系统日志自定义模板设置和示例	51
使用系统日志预定义消息模板	54
系统日志 ASA VPN 预定义模板	54
系统日志 Bluecat 预定义模板	56
系统日志 F5 VPN 预定义模板	57
系统日志 Infoblox 预定义模板	57
系统日志 Linux DHCPd3 预定义模板	58
系统日志 MS DHCP 预定义模板	59
系统日志 SafeConnect NAC 预定义模板	59
系统日志 Aerohive 预定义模板	60
系统日志 Blue Coat 预定义模板 - 主代理、代理 SG、Squid Web 代理	60
系统日志 ISE 和 ACS 预定义模板	62
系统日志 Lucent QIP 预定义模板	63
过滤被动身份服务	64
终端探测器	65
使用终端探测器	66

---

## 第 5 章

### 用户 67

生成用户的 pxGrid 证书	68
启用用户	70
从实时日志查看用户事件	70
配置用户设置	70

---

## 第 6 章

### 思科中的证书管理 ISE-PIC 71

思科 ISE-PIC 中的证书匹配	71
通配符证书	72
使用通配符证书的优势	73
使用通配符证书的缺点	73
通配符证书兼容性	74

证书层次结构ISE-PIC	74
系统证书	75
查看系统证书	75
导入系统证书	76
生成自签证书	77
编辑系统证书	77
删除系统证书	78
导出系统证书	79
受信任证书库	79
受信任证书命名限制	80
查看受信任的证书	81
更改受信任证书库中的证书状态	81
在受信任的证书库中添加证书	82
编辑受信任证书	82
删除受信任证书	83
从受信任证书库导出证书	83
将根证书导入受信任证书库	83
证书链导入	84
受信任证书导入设置	84
证书签名请求	85
创建证书签名请求并将其提交给证书颁发机构	86
将 CA 签名的证书绑定到证书签名请求	86
导出证书签名请求	87
证书签名请求设置	88
思科 ISE CA 服务	93
省略曲线加密证书支持	94
思科 ISE-PIC 证书颁发机构证书	94
编辑思科 ISE-PIC CA 证书	95
导出思科 ISE CA 证书	95
导入思科 ISE-PIC CA 证书	95
受信任证书设置	96

思科 ISE-PIC CA 证书和密钥的备份与恢复	98
导出思科 ISE CA 证书和密钥	99
导入思科 ISE-PIC CA 证书和密钥	99
生成根 CA 和从属 CA	100
将思科 ISE-PIC 根 CA 配置为外部 PKI 的辅助 CA	100
OCSP 服务	101
思科 ISE CA 服务在线证书状态协议响应器	101
OCSP 证书状态值	102
OCSP 高可用性	102
OCSP 故障	102
添加 OCSP 客户端配置文件	103
OCSP 统计计数器	103

---

**第 7 章**

<b>管理 ISE-PIC</b>	<b>105</b>
管理 ISE-PIC 节点	105
思科 ISE-PIC 部署设置	105
将数据从主 ISE-PIC 节点复制到辅助节点	105
在思科 ISE-PIC 中修改节点的影响	106
在部署中设置两个节点的指南	106
查看部署中的节点	106
注册辅助思科 ISE-PIC 节点	107
同步主要和辅助思科 ISE-PIC 节点	107
手动将辅助 PAN 升级为主 PAN	108
从部署中删除节点	108
更改思科 ISE-PIC 节点的主机名或 IP 地址	109
更换思科 ISE-PIC 设备硬件	109
管理 ISE-PIC 安装	110
安装软件补丁	110
思科 ISE-PIC 软件补丁	110
软件补丁安装指南	111
回滚软件补丁	111

软件补丁回滚指南	112	
备份和恢复数据	112	
备份和恢复存储库	112	
创建存储库	113	
存储库设置	114	
在 SFTP 存储库中启用 RSA 公共密钥身份验证	115	
按需备份和计划备份	116	
思科 ISE 恢复操作	119	
同步主节点和辅助节点	123	
恢复独立和两节点部署中断开的节点	124	
数据库清除	127	
将 ISE-PIC 升级到完整 ISE 安装	128	
通过注册许可证升级到 ISE	128	
管理设置 ISE-PIC	129	
基于角色的访问控制	129	
思科 ISE-PIC 管理员	130	
思科 ISE-PIC 管理员组	130	
CLI 管理员与基于 Web 管理员的权限对比	131	
创建新管理员	131	
对思科 ISE-PIC 进行管理访问	131	
管理员访问设置	132	
管理门户使用的端口	135	
配置 SMTP 服务器以支持通知	135	
从 GUI 启用外部 RESTful 服务 API - ERS 设置	135	
<b>第 8 章</b>	<b>ISE-PIC 中的监控和故障排除服务</b>	<b>137</b>
实时会话	137	
可用报告	140	
思科 ISE-PIC 警报	143	
警报设置	150	
添加自定义报警	151	



用于验证传入流量的 TCP Dump 实用工具	151
使用 TCP Dump 监控网络流量	151
保存 TCP Dump 文件	152
TCP Dump 设置	153
日志记录机制	154
思科 ISE-PIC 日志记录机制	154
配置系统日志清除设置	154
Active Directory 故障排除	154
将 Active Directory 与思科 ISE-PIC 集成的前提条件	154
执行各种操作所需的 Active Directory 帐户权限	155
必须开放用于通信的网络端口	156
支持 ISE-PIC 的 Active Directory 要求	156
获取其他故障排除信息	166
思科 ISE-PIC 支持捆绑包	166
支持捆绑包	167
下载思科 ISE-PIC 日志文件。	167
思科 ISE-PIC 调试日志	168
获取调试日志	168
思科 ISE-PIC 组件和相应的调试日志	168
下载调试日志	170





# 第 1 章

## 简介 ISE-PIC



### 注释

此产品的文档集力求使用无偏见语言。在本文档集中，无偏见定义为不暗示基于年龄、残障、性别、种族身份、族群身份、性取向、社会经济地位和交叉性的歧视的语言。由于产品软件的用户界面中使用的硬编码语言，基于 RFP 文档使用的语言或引用的第三方产品使用的语言，文档中可能存在例外情况。

用户身份必须经过身份验证，以保护网络免受未经授权的威胁。为此，需要在网络上实施安全产品。每个安全产品都有自己的检索必要身份验证的方法，通常用于识别授权的 IP 地址，而不是授权的用户。因此，这些产品指的是基于用户登录信息提供身份验证的不同外部服务器和方法，从而形成分散网络。思科身份识别服务引擎 (ISE) 被动身份连接器 (ISE-PIC) 提供集中的一站式安装和实施，让您轻松地各种来源收集用户的被动身份验证数据，并与安全产品用户共享这些用户身份。

- [思科 ISE-PIC 术语，第 1 页](#)
- [ISE-PIC 概述，第 2 页](#)
- [思科 ISE-PIC 架构、部署和节点，第 3 页](#)
- [ISE-PIC 的优势，第 4 页](#)
- [比较 ISE-PIC 与 ISE 和 CDA，第 5 页](#)

## 思科 ISE-PIC 术语

本指南在讨论 Cisco ISE-PIC 时使用以下术语：

术语	定义
GUI	图形用户界面。GUI 是指 ISE-PIC 软件安装中的任何屏幕和选项卡。
网卡	网络接口卡。
节点	单个物理或虚拟思科 ISE-PIC 设备。

术语	定义
PAN	ISE-PIC 部署中的主节点是主管理节点 (PAN)，您可以从此节点执行所有可用操作。在 ISE-PIC 中，最多可以安装两个节点。如果安装第二个节点，则此节点将称为辅助管理节点（辅助 PAN）。
解析器	接收系统日志消息，并将输入拆分为可管理、映射并发布到 ISE-PIC 的各部分的 ISE-PIC 后端组件。解析器将在系统日志消息到达时解析每行信息，查找关键信息。例如，如果解析器配置为查找“mac=”，则解析器会在查找此短语时解析每行信息。解析器设置为在找到已配置的关键短语后，将定义的信息传送到 ISE。
主节点	ISE-PIC 部署中的主节点是主管理节点 (PAN)，您可以从此节点执行所有可用操作。在 ISE-PIC 中，最多可以安装两个节点。如果安装第二个节点，则此节点将称为辅助管理节点（辅助 PAN）。
探测功能	探测器是从给定源收集数据的机制。探测器是一个说明任何机制的通用术语，但不具体描述如何收集数据或收集什么。例如，Active Directory (AD) 探测器有助于 ISE-PIC 从 AD 收集数据，而系统日志探测器则从读取系统日志消息的解析器收集数据。
提供程序	ISE-PIC 从中接收、映射和发布用户身份信息的客户端或源。
辅助节点	ISE-PIC 部署中的主节点是主管理节点 (PAN)，您可以从此节点执行所有可用操作。在 ISE-PIC 中，最多可以安装两个节点。如果安装第二个节点，则此节点将称为辅助管理节点（辅助 PAN）。
用户	订用 ISE-PIC 服务以接收用户身份信息的系统。

## ISE-PIC 概述

被动身份连接器 (ISE-PIC) 提供集中的一站式安装和实施，使您能够轻松简单地配置网络，以便接收用户身份信息并与各种不同的安全产品用户（例如思科 Firepower 管理中心 [FMC] 和 Stealthwatch）进行共享。作为用于被动识别的全面代理，ISE-PIC 从不同提供程序源（例如 Active Directory 域控制器 [AD DC]）收集用户身份，将用户登录信息映射到使用中的相关 IP 地址，然后将该映射信息与已配置的任何用户安全产品进行共享。

### 什么是被动身份？

思科身份服务引擎 (ISE) 之类的产品，用于提供身份验证、授权和记账 (AAA) 服务器，并利用 802.1X 或 Web 身份验证之类的技术，直接与用户或终端进行通信，从而请求访问网络，然后使用其登录凭证来确认其身份并主动进行身份验证。

被动身份服务不直接对用户进行身份验证，而是从 Active Directory 之类的外部身份验证服务器（称为提供程序）收集用户身份和 IP 地址，然后与用户共享该信息。ISE-PIC 首先从提供程序接收用户身份信息（通常根据用户登录名和密码），然后执行必要的检查和服务，以便将用户身份与相关 IP 地址进行匹配，从而向用户传送经过身份验证的 IP 地址。

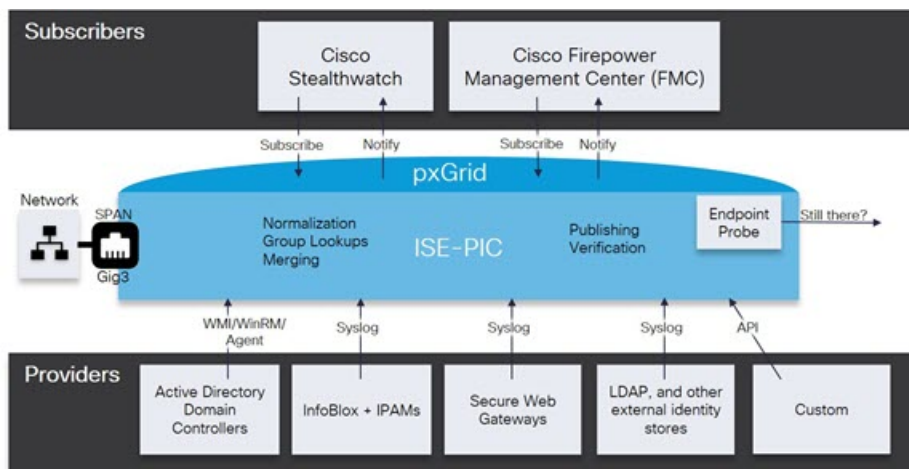
### 被动身份连接器 (ISE-PIC) 流程

ISE-PIC 的流程如下：

1. 提供程序对用户或终端执行身份验证。
2. 提供程序将经过身份验证的用户信息发送到思科 ISE-PIC。
3. ISE-PIC 将用户信息规范化，执行查找、合并、解析并将其映射到 IP 地址，然后将映射的详细信息发布到 pxGrid。
4. pxGrid 用户接收映射的用户详细信息。

下图说明了 ISE-PIC 提供的概要流程。

图 1: 概要流程



## 思科 ISE-PIC 架构、部署和节点

Cisco ISE-PIC 架构包括以下组件：

- 节点 - 在思科 ISE-PIC 部署中，最多可以配置两个节点，如下所述
- 网络资源
- 终端

具有单个 Cisco ISE-PIC 节点的部署称为独立部署。

具有两个思科 ISE-PIC 节点的部署称为高可用性部署，其中一个节点用作主要设备（主管理节点，即 PAN）。高可用性部署可提高服务可用性。

PAN 提供此网络模型所需的所有配置功能，并提供备份角色的辅助思科 ISE 节点（辅助 PAN）功能。辅助节点支持主节点，并在与主节点失去连接时恢复功能。

思科 ISE-PIC 会将位于主思科 ISE-PIC 节点上的所有内容与辅助思科 ISE-PIC 节点同步或进行复制，以确保您的辅助节点与主节点的状态一致（因此可用作备份）。

#### ISE 社区资源

有关部署和扩展的信息，请参阅[ISE 部署历程](#)。



**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）。

## ISE-PIC 的优势

ISE-PIC 为您提供：

- 与各种不同提供程序交互的单一身份解决方案。
- 支持简单配置、监控和故障排除的友好 GUI
- 简单安装和配置
- 轻松升级到 ISE 以进行主动身份验证。从 ISE-PIC 升级到完整 ISE 部署并使用 ISE-PIC 节点创建独立 ISE 部署时，或者将此节点作为主节点添加到现有部署时，ISE 将继续提供升级之前在 ISE-PIC 中可用的所有功能，并将保留您的现有配置。



**注释** 要升级到 ISE，请下载试用版，或联系您的思科代表以讨论许可选项。

将已升级 ISE-PIC 添加到现有 ISE 部署，但不将其用作主节点时，将覆盖之前的 ISE-PIC 配置。

有关升级流程的完整说明，请参阅[将 ISE-PIC 升级到完整 ISE 安装，第 128 页](#)。

## 比较 ISE-PIC 与 ISE 和 CDA

ISE-PIC 具备许多优势，包括能够平稳轻松地升级到 ISE。除 ISE-PIC 和 ISE 以外，思科还提供一种额外的安全机制，即 CDA。本节在下列表格中对这三种产品进行比较：

- [ISE-PIC 与 ISE 的详细比较，第 5 页](#)
- [ISE-PIC 与 ISE 和 CDA 的概括比较，第 6 页](#)

### ISE-PIC 与 ISE 的详细比较

ISE-PIC 设计为仅共享被动身份，并且不提供任何授权或身份验证服务，这两种服务均由 ISE 提供，ISE 可提供身份验证、授权和记账(AAA)服务器。下表中对这两种产品之间的差异进行了详细说明。

表 1: 比较 ISE-PIC 与 ISE

类别	特性	ISE-PIC	ISE
智能许可		-	√
身份验证和授权类型	授权策略	-	√
	TrustSec	-	√
	Active Directory 被动身份验证，包括 WMI	√	√
被动身份源		√	√
	Easy Connect	-	√
	系统日志源	√	√
	REST API 源	√	√
	SPAN	√	√
	安全组交换协议 (SXP)	-	√
	RADIUS，包括 RADIUS 代理	-	√
	自带设备	-	√
	访客	-	√
	安全评估	-	√
	设备管理 (TACACS+)	-	√

类别	特性	ISE-PIC	ISE
pxGrid	pxGrid 控制器	√ 仅适用于思科用户	√
	pxGrid 控制器冗余	√	√
	主题可扩展性	-	√
证书颁发机构 (CA)	pxGrid 证书模板	√	√
	终端 CA	-	√
	安全传输注册 (EST)	-	√
	其他证书模板	-	√
可视性与情景	Context Directory	-	√
	分析	-	√
报告		! 注释 ISE-PIC 提供报告，可用于监控系统运行状况并排除网络中的问题。但是，与 ISE 相比，ISE-PIC 提供一部分功能，因此在 ISE-PIC 中不提供某些 ISE 报告。	√

### ISE-PIC 与 ISE 和 CDA 的概括比较

CDA 是一种机制，用于将 IP 地址映射到用户名，以便允许安全网关了解哪个用户使用网络中的哪个 IP 地址，因此这些安全网关现在可根据这些用户（或用户所属的组）制定决策。但是，ISE-PIC 通过访问用户名、MAC 地址和端口等其他数据，可以更精确地收集用户身份。下表概括比较了 ISE-PIC、ISE 和 CDA。



表 2: 比较 ISE-PIC 与 ISE 和 CDA

被动身份验证详细信息	完整 ISE	ISE-PIC	CDA
域控制器数量	100	100	80
用户数	20	20	-
WMI（无代理）	是	是	是
Windows 服务器代理可用	是	是	—
需要 DCOM	无 (SPAN)	无 (SPAN)	是
Easy Connect	是	—	-
使用 SPAN 的 Kerberos 嗅探	是	是	—
绑定（IP 地址、MAC 地址和用户名）	300,000	300,000	64,000





## 第 2 章

# 开始使用 ISE-PIC

- [管理员访问控制台](#)，第 9 页
- [初始设置和配置](#)，第 10 页
- [ISE-PIC 主页控制板](#)，第 14 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** 单击 **登录 (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

## 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 10 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 13 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](#)，第 18 页。
5. 配置单个或多个用户。有关详细信息，请参阅[用户](#)，第 67 页。

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](#)，第 31 页）并从 ISE-PIC（请参阅 [ISE-PIC 中的监控和故障排除服务](#)，第 137 页）中的不同提供程序管理被动识别。

## ISE-PIC 智能许可

ISE-PIC 3.1 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 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 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**) 窗口顶部单击 **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 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 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	<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。

Essential	基于期限的许可证	<ul style="list-style-type: none"> <li>• 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</li> <li>• MACsec</li> <li>• 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</li> <li>• 访客门户和发起人服务</li> <li>• 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</li> <li>• 被动 ID 服务</li> <li>• 安全有线和无线接入</li> </ul>	—
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，单击菜单图标 (☰) 并选择**管理 (Administration) > 系统 (System) > 许可 (Licensing)**。

**步骤 2** 单击**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** 单击注册 (**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, 然后单击许可证 (**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**) 区域的顶部单击取消注册 (**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，单击菜单图标 (☰) 并选择 **设置 (Settings) > 系统时间 (System Time)**。

**步骤 2** 在 **NTP 服务器配置 (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** (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更多身份验证密钥。执行以下步骤：

- 单击 **添加 (Add)**。
- 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。
- 单击 **确定 (OK)**。
- 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** 单击 **保存 (Save)**。



**注释** 建议不要只使用两个 NTP 服务器。

## 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。





## 第 3 章

# Active Directory 作为探测器和提供程序

Active Directory (AD) 是一种高度安全且精确的源，可以从中接收用户身份信息，包括用户名、IP 地址和域名。

AD 探测器（被动身份服务）通过 WMI 技术从 AD 收集用户身份信息，而其他探测器则通过其他技术和方法将 AD 用作用户身份提供程序。有关 ISE-PIC 提供的其他探测器和提供程序类型的详细信息，请参阅[提供程序](#)，第 31 页。

通过配置 Active Directory 探测器，您还可以快速配置并启用以下其他探测器（它们也使用 Active Directory 作为源）：

- [Active Directory 代理](#)，第 33 页



**注** 释 仅在 Windows Server 2008 及更高版本上支持 Active Directory 代理。

- [SPAN](#)，第 42 页
- [终端探测器](#)，第 65 页

此外，配置 Active Directory 探测器，以便在收集用户信息时使用 AD 用户组。您可以对 AD、代理、SPAN 和系统日志探测使用 AD 用户组。有关 AD 组的详细信息，请参阅[配置 Active Directory 用户组](#)，第 22 页。

- [使用 Active Directory](#)，第 17 页
- [Active Directory 设置](#)，第 27 页

## 使用 Active Directory

在为被动身份服务配置 Active Directory 探测器之前，请确保：

- Microsoft Active Directory 服务器未驻留在网络地址转换器后，并且不具有网络地址转换 (NAT) 地址。
- 用于加入操作的 Microsoft Active Directory 帐户有效，且未配置为下次登录时修改密码。

- 确保您已正确配置 DNS 服务器，包括从 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 13 页](#)。
- 同步 NTP 服务器的时钟设置。有关详细信息，请参阅[指定系统时间和网络时间协议服务器设置，第 14 页](#)。



**注释** 如果您在思科 ISE-PIC 连接到 Active Directory 时发现操作问题，请查看[报告 \(Reports\)](#) 下的 AD 连接器操作报告。有关详细信息，请参阅[可用报告，第 140 页](#)。

## PassiveID 设置入门

ISE-PIC 提供向导，从中可以轻松快速地将 Active Directory 配置为第一个用户身份提供程序，以便从 Active Directory 接收用户身份。通过为 ISE-PIC 配置 Active Directory，还可以简化稍后配置其他提供程序类型的过程。一旦配置了 Active Directory，就必须配置用户（例如思科 Firepower 管理中心 (FMC) 或 Stealthwatch），以便定义将要接收用户数据的客户端。有关用户的详细信息，请参阅[用户，第 67 页](#)。

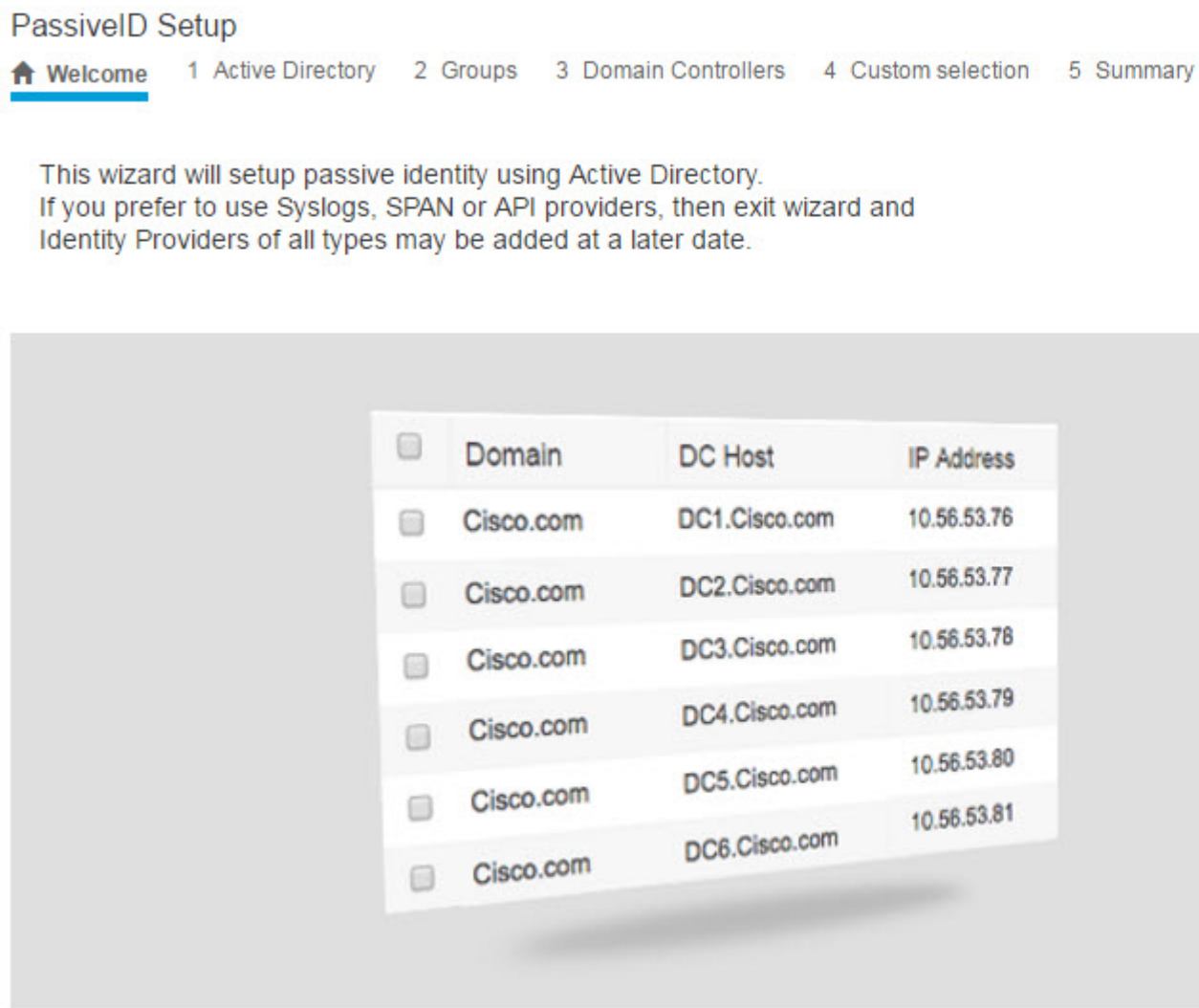
### 开始之前

- 确保 Microsoft Active Directory 服务器未驻留在网络地址转换器后，并且不具有网络地址转换 (NAT) 地址。
- 确保旨在用于加入操作的 Microsoft Active Directory 账户有效，并且未配置为下次登录时更改密码。
- 确保 ISE-PIC 在域名服务器 (DNS) 中具有条目。确保您已从 ISE-PIC 正确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 13 页](#)。

**步骤 1** 选择主页 (**Home**) > 简介 (**Introduction**)。从“被动身份连接器概述” (Passive Identity Connector Overview) 屏幕中，单击被动身份向导 (**Passive Identity Wizard**)。

系统将打开“PassiveID 设置” (PassiveID Setup):

图 2: PassiveID 设置



**步骤 2** 单击下一步 (Next) 以开始向导。

**步骤 3** 输入此 Active Directory 加入点的唯一名称。输入此节点连接的 Active Directory 域的域名，然后输入 Active Directory 管理员用户名和密码。有关 Active Directory 设置的详细信息，请参阅[#unique\\_32](#)。

您的管理员的用户名和密码，以便用于为监控配置的所有域控制器 (DC)。

**步骤 4** 单击下一步 (Next) 以定义 Active Directory 组并选中要包含和监控的任何用户组。  
Active Directory 用户组根据您在上一步中配置的 Active Directory 加入点自动显示。

**步骤 5** 单击下一步 (Next)。选择要监控的 DC。如果选择“自定义” (Custom)，则从下一个屏幕中选择用于监控的特定 DC。完成后，单击下一步 (Next)。

步骤 6 单击退出 (Exit) 以完成向导。

### 下一步做什么

完成将 Active Directory 配置为初始提供程序时，还可以轻松配置其他提供程序类型。有关详细信息，请参阅[提供程序](#)，第 31 页。此外，现在还可以配置指定要接收由任何已定义提供程序收集到的用户身份信息用户。有关详细信息，请参阅[用户](#)，第 67 页。

## 分步设置 Active Directory (WMI) 探测器

要为被动身份服务配置 Active Directory 和 WMI，请使用 [PassiveID 设置入门](#)，第 18 页或按照本章中的步骤操作，如下所示：

1. 配置 Active Directory 探测器。请参阅[添加 Active Directory 加入点并将思科 ISE-PIC 节点加入到该加入点](#)，第 20 页。
2. 为 WMI 配置的用于接收 AD 登录事件的一个或多个节点创建 Active Directory 域控制器列表。请参阅[#unique\\_35](#)。
3. 配置 Active Directory，以使其与 ISE-PIC 集成。请参阅[#unique\\_36](#)。
4. （可选）[管理 Active Directory 提供程序](#)，第 23 页。

## 添加 Active Directory 加入点并将思科 ISE-PIC 节点加入到该加入点

### 开始之前

确保思科 ISE-PIC 节点可以与 NTP 服务器、DNS 服务器、域控制器和全局日志服务器所在的网络通信。

必须创建加入点才能使用 Active Directory 以及使用的代理、系统日志、SPAN 和终端探测器。

在与 Active Directory 集成时，如果需要使用 IPv6，则必须确保已为相关 ISE-PIC 节点配置 IPv6 地址。

如果您使用 Google Chrome 浏览器并启用了广告拦截软件，则必须禁用广告拦截器。此任务包含受广告拦截器影响的思科 ISE GUI 元素。或者，您可以在 Google Chrome 隐身模式浏览器中执行此任务。

步骤 1 选择提供程序 (Providers) > Active Directory。

步骤 2 单击添加 (Add) 并从 Active Directory 加入点名称 (Active Directory Join Point Name) 设置中输入域名和身份存储库名称。有关详细信息，请参阅[#unique\\_32 unique\\_32\\_Connect\\_42\\_table\\_7E6BC3FF662C4DFC99017C0200D31BE9](#)。

步骤 3 单击提交 (Submit)。

此时将出现弹出窗口，询问您是否要将新创建的加入点加入到域中。如果要立即加入，请单击是 (Yes)。

如果已单击否 (No)，则保存配置将会全局保存 Active Directory 域配置，但不会将任何 ISE-PIC 节点加入到该域。

**步骤 4** 选中所创建的新 Active Directory 加入点旁边的复选框并单击**编辑 (Edit)**。系统将显示部署加入/退出表，其中包含所有思科 ISE-PIC 节点、节点角色及其状态。有关详细信息，请参阅[#unique\\_32 unique\\_32\\_Connect\\_42\\_table\\_v21\\_ffj\\_nx](#)。

**步骤 5** 如果加入点没有在步骤 3 中加入域，请选中相关思科 ISE-PIC 节点旁边的复选框，然后单击**加入 (Join)** 将思科 ISE-PIC 节点加入到 Active Directory 域。

您必须明确地执行此操作，即使已保存配置。要通过单个操作将多个思科 ISE-PIC 节点加入到域，所要使用的账户的用户名和密码必须对于所有加入操作都相同。如果需要不同的用户名和密码以加入每个思科 ISE-PIC 节点，则应对每个思科 ISE-PIC 节点分别执行加入操作。

**步骤 6** 在**加入域 (Join Domain)** 对话框中输入 Active Directory 用户名和密码。

您的管理员的用户名和密码，以便用于为监控配置的所有域控制器 (DC)。

用于加入操作的用户本身应存在于域中。如果该用户存在于其他域中或子域中，应使用 UPN 符号注解用户名，如 `jdooe@acme.com`。

**步骤 7** (可选) 选中**指定组织单位 (Specify Organizational Unit)** 复选框。

如果思科 ISE-PIC 节点机器帐户要位于除 `CN=Computers,DC=someDomain,DC=someTLD` 以外的特定组织单位中，应选中此复选框。思科 ISE-PIC 会在指定的组织单位下创建机器账户，如果该机器账户已存在，则会将该账户移至此位置。如果未指定组织单位，思科 ISE-PIC 将使用默认位置。应以完整可分辨名称 (DN) 格式指定值。语法必须符合 Microsoft 规范。特殊保留字符，例如 `/+,;=<>` 换行符、空格和回车符，必须用反斜线 (`\`) 转义。例如，`OU=Cisco ISE\US,OU=IT Servers,OU=Servers\和 Workstations,DC=someDomain,DC=someTLD`。如果计算机帐户已经创建，则您不需要选中此复选框。加入 Active Directory 域之后，您还可以更改计算机帐户的位置。

**步骤 8** 单击**确定 (OK)**。

您可以选择多个要加入 Active Directory 域的节点。

如果加入操作不成功，则系统会显示失败消息。单击每个节点的失败消息可查看该节点的详细日志。

**注释** 加入完成后，思科 ISE-PIC 将更新其 AD 组和对应的安全标识符 (SID)。思科 ISE-PIC 自动启动 SID 更新过程。您必须确保允许此过程完成。

**注释** 如果缺少 DNS 服务 (SRV) 记录，您可能无法将思科 ISE-PIC 加入 Active Directory 域 (域控制器不会对您尝试加入到的域公告其 SRV 记录)。请参阅以下 Microsoft Active Directory 文档，以获取故障排除信息：

- <http://support.microsoft.com/kb/816587>
- <http://technet.microsoft.com/en-us/library/bb727055.aspx>

**注释** 在 ISE 上最多只能添加 200 个域控制器。如果超出此限制，您将收到错误“创建 `<DC FQDN>` 时出错 - DC 数超出允许的最大值 200” (Error creating `<DC FQDN>` - Number of DCs Exceeds allowed maximum of 200)。

---

下一步做什么

[#unique\\_35](#)

[配置 Active Directory 用户组，第 22 页](#)

[#unique\\_36](#)

## 添加域控制器

**步骤 1** 选择提供程序 (Providers) > Active Directory。

**步骤 2** 选中所创建的 Active Directory 加入点旁边的复选框，然后单击编辑 (Edit)。系统将显示部署加入/退出表，其中包含所有思科 ISE-PIC 节点、节点角色及其状态。有关详细信息，请参阅[#unique\\_32 unique\\_32\\_Connect\\_42\\_table\\_v21\\_ffj\\_nx](#)。

**步骤 3** 注释 要为被动身份服务添加新域控制器 (DC)，您需要该 DC 的登录凭证。

转至 PassiveID 选项卡，然后单击添加 DC (Add DCs)。

**步骤 4** 选中要添加到加入点以进行监控的域控制器旁边的复选框，然后单击确定 (OK)。域控制器显示在 PassiveID 选项卡的“域控制器” (Domain Controllers) 列表中。

**步骤 5** 配置域控制器：

- 选中域控制器，然后单击编辑 (Edit)。系统将显示编辑项目 (Edit Item) 屏幕。
- 或者，编辑不同的域控制器字段。有关详细信息，请参阅[#unique\\_32](#)。
- 如果选择 WMI 协议，请单击配置 (Configure) 以自动配置 WMI，然后单击测试 (Test) 以测试连接。

DC 故障切换机制根据 DC 优先级列表进行管理，该列表确定在故障切换情况下选择 DC 的顺序。如果 DC 由于错误而离线或无法访问，则其优先级在优先级列表中会降低。当 DC 恢复在线时，其优先级会在优先级列表中相应地调整（提高）。



注释 思科 ISE 不支持将只读域控制器用于身份验证流程。

## 配置 Active Directory 用户组

配置 Active Directory 用户组，以使其可供在运用不同探测器从 Active Directory 收集用户身份信息时使用。在内部，思科 ISE 使用安全标识符 (SID) 帮助解决组名称不明确问题和增强组映射。SID 提供准确的组分配匹配。

**步骤 1** 选择提供程序 (Providers) > Active Directory。单击要为其添加组的加入点。

**步骤 2** 单击组 (Groups) 选项卡。

**步骤 3** 执行以下操作之一：

- 选择添加 (Add) > 从目录中选择组 (Select Groups From Directory) 以选择现有组。
- 选择添加 (Add) > 添加组 (Add Group) 以手动添加组。您可以同时提供组名称和 SID，也可以仅提供组名称并按获取 SID (Fetch SID)。

对于用户界面登录，请勿在组名称中使用双引号 (")。



**步骤 4** 如果您手动选择组，您可以使用过滤器进行搜索。例如，输入 **admin\*** 作为搜索条件，然后单击**检索组 (Retrieve Groups)**，即可查看以 **admin** 开头的用户组。您还可以输入星号 (\*) 通配符过滤结果。一次只能检索 500 个组。

**步骤 5** 选中想要可用于授权策略的组旁边的复选框，然后单击**确定 (OK)**。

**步骤 6** 如果您选择手动添加组，请为新组输入名称和 SID。

**步骤 7** 单击**确定 (OK)**。

**步骤 8** 单击**保存 (Save)**。

**注释** 如果删除某个组，然后创建一个与此组相同名称的新组，则必须单击**更新 SID 值 (Update SID Values)** 以向新创建的组分配新 SID。升级之后，SID 会在首次联接之后自动更新。

## 对被动 ID 配置 WMI

### 开始之前

确保您具有 Active Directory 域管理员凭证，这样才能对任何 AD 域配置进行更改。确保已在**管理 (Administration) > 系统 (System) > 部署 (Deployment)** 下对此节点启用被动 ID。

**步骤 1** 选择**提供程序 (Providers) > Active Directory**。

**步骤 2** 选中所创建的 Active Directory 加入点旁边的复选框，然后单击**编辑 (Edit)**。系统将显示部署加入/退出表，其中包含所有思科 ISE-PIC 节点、节点角色及其状态。有关详细信息，请参阅[#unique\\_32 unique\\_32\\_Connect\\_42\\_table\\_v21\\_ffj\\_nx](#)。

**步骤 3** 转至“被动 ID”选项卡，选中相关域控制器旁边的复选框，然后单击**配置 WMI (Config WMI)** 以使 ISE-PIC 能够自动配置所选的域控制器。

要手动配置 Active Directory 和域控制器或对任何配置问题进行故障排除，请参阅[将 Active Directory 与思科 ISE-PIC 集成的前提条件](#)，第 154 页。



**注释** 我们建议您在 Windows 请求者上禁用网络级别身份验证 (NLA)，以确保与被动 ID 正确映射。这是因为，当用户尝试使用备用帐户和远程桌面协议访问设备时，该备用用户帐户可能会映射到两台计算机，从而导致这些用户帐户的访问权限不正确。

## 管理 Active Directory 提供程序

创建并配置 Active Directory 加入点之后，通过以下任务继续管理 Active Directory 探测器：

- [对用户进行 Active Directory 组测试](#)，第 24 页
- [查看节点的 Active Directory 加入](#)，第 24 页
- [诊断 Active Directory 问题](#)，第 25 页

- 退出 Active Directory 域，第 25 页
- 删除 Active Directory 配置，第 26 页
- 启用 Active Directory 调试日志，第 26 页

## 对用户进行 Active Directory 组测试

“测试用户”工具可用于从 Active Directory 验证用户组。您可以对单个加入点或对范围运行测试。

**步骤 1** 选择提供程序 (Providers) > Active Directory。

**步骤 2** 选择以下选项之一：

- 要对所有加入点运行测试，请选择高级工具 (Advanced Tools) > 就所有加入点测试用户 (Test User for All Join Points)。
- 要对特定加入点运行测试，请选择该加入点并单击编辑 (Edit)。选择思科 ISE-PIC 节点并单击测试用户 (Test User)。

**步骤 3** 在 Active Directory 中输入用户（或主机）的用户名和密码。

**步骤 4** 选择身份验证类型。如果选择“查找” (Lookup) 选项，则无需步骤 3 中的密码输入。

**步骤 5** 如果您是对所有加入点运行此测试，请选择要对其运行此测试的思科 ISE-PIC 节点。

**步骤 6** 从 Active Directory 检索组，请选中“检索组” (Retrieve Groups) 和“检索属性” (Retrieve Attributes) 复选框。

**步骤 7** 单击测试 (Test)。

系统将显示测试操作的结果和步骤。这些步骤可帮助确定故障原因并进行故障排除。

您还可以查看 Active Directory 执行每个处理步骤所需的时间（以毫秒为单位）。如果操作所需的时间超过阈值，思科 ISE-PIC 将显示警告消息。

## 查看节点的 Active Directory 加入

您可以使用 Active Directory 页面上的节点视图 (Node View) 按钮查看给定思科 ISE-PIC 节点的所有 Active Directory 加入点的状态或所有思科 ISE-PIC 节点上的所有加入点列表。

**步骤 1** 选择提供程序 (Providers) > Active Directory。

**步骤 2** 单击节点视图 (Node View)。

**步骤 3** 从 ISE 节点 (ISE Node) 下拉列表中选择节点。

表格按节点列出 Active Directory 的状态。如果部署中有多个加入点和多个思科 ISE-PIC 节点，则更新此表可能需要几分钟时间。

**步骤 4** 单击加入点名称 (Name) 链接以转至该 Active Directory 加入点页面，然后执行其他特定操作。

**步骤 5** 单击诊断摘要 (Diagnostic Summary) 列中的链接以转至诊断工具 (Diagnostic Tools) 页面来对特定问题进行故障排除。诊断工具显示每个节点的每个加入点的最新诊断结果。

## 诊断 Active Directory 问题

诊断工具是在每个思科 ISE-PIC 节点上运行的服务。当思科 ISE-PIC 使用 Active Directory 时，通过该工具可自动测试和诊断 Active Directory 部署并执行一组测试，以检测可能导致功能或性能故障的问题。

思科 ISE-PIC 无法加入 Active Directory 或对其进行身份验证有多个原因。此工具帮助确保正确配置用于将思科 ISE-PIC 连接到 Active Directory 的前提条件。该工具有助于检测网络、防火墙配置、时钟同步、用户身份验证等问题。此工具以逐步操作指南的形式工作，并帮助您根据需要解决中间每层的问题。

---

**步骤 1** 选择提供程序 (Providers) > Active Directory。

**步骤 2** 单击高级工具 (Advanced Tools) 下拉列表，选择诊断工具 (Diagnostic Tools)。

**步骤 3** 选择要运行诊断的思科 ISE-PIC 节点。

如果未选择思科 ISE-PIC 节点，则在所有节点上运行测试。

**步骤 4** 选择特定的 Active Directory 加入点。

如果不选择 Active Directory 加入点，则在所有加入点上运行测试。

**步骤 5** 您可以按需或按计划运行诊断测试。

- 要立即运行测试，请选择立即运行测试 (Run Tests Now)。
- 要按计划间隔运行测试，请选中运行计划测试 (Run Scheduled Tests) 复选框并指定必须运行测试的开始时间和间隔（以小时、天或周为单位）。启用此选项后，将在所有节点和实例上运行所有诊断测试，并在主页控制面板上的警报 dashlet 中报告故障。

**步骤 6** 单击查看测试详情 (View Test Details) 查看具有警告或失败状态的测试的详细信息。

下表允许您重新运行特定测试、停止正在运行的测试和查看特定测试的报告。

---

## 退出 Active Directory 域

如果不再需要使用此 Active Directory 域或此加入点收集用户身份，则可以退出 Active Directory 域。

从命令行界面重置思科 ISE-PIC 应用配置或在备份或升级后恢复配置时，它将执行退出操作，从而将思科 ISE-PIC 节点与 Active Directory 域断开连接（如果已加入该节点）。但是，不会从 Active Directory 域中删除思科 ISE-PIC 节点账户。我们建议您使用 Active Directory 凭证从 Admin 门户执行退出操作，因为这也会从 Active Directory 域删除节点帐户。在更改思科 ISE-PIC 主机名时，也建议您如此操作。

---

**步骤 1** 选择提供程序 (Providers) > Active Directory。

**步骤 2** 选中所创建的 Active Directory 加入点旁边的复选框，然后单击编辑 (Edit)。系统将显示部署加入/退出表，其中包含所有思科 ISE-PIC 节点、节点角色及其状态。有关详细信息，请参阅[#unique\\_32 unique\\_32\\_Connect\\_42\\_table\\_v21\\_ffj\\_nx](#)。

**步骤 3** 选中思科 ISE-PIC 节点旁边的复选框，然后单击**退出 (Leave)**。

**步骤 4** 输入 Active Directory 用户名和密码，然后单击**确定 (OK)** 以退出该域并从思科 ISE-PIC 数据库中删除机器账户。

如果输入 Active Directory 凭证，则思科 ISE-PIC 节点将退出 Active Directory 域并从 Active Directory 数据库中删除思科 ISE-PIC 机器账户。

**注释** 要从 Active Directory 数据库中删除思科 ISE-PIC 机器账户，此处提供的 Active Directory 凭证必须具有从域中删除机器账户的权限。

**步骤 5** 如果您没有 Active Directory 凭证，请选中**无可用凭证 (No Credentials Available)** 复选框，然后单击**确定 (OK)**。

如果选中**退出没有凭证的域 (Leave domain without credentials)** 复选框，则主思科 ISE-PIC 节点将退出 Active Directory 域。Active Directory 管理员必须手动删除加入期间在 Active Directory 中创建的设备帐户。

---

## 删除 Active Directory 配置

如果您不会使用特定 Active Directory 配置作为探测器，则应删除 Active Directory 配置。如果您希望加入其他 Active Directory 域，则请勿删除该配置。您可以退出当前所加入的域并加入新的域。如果该配置是以下位置中的唯一配置，请勿将其删除： ISE-PIC

### 开始之前

确保您已退出 Active Directory 域。

---

**步骤 1** 选择**提供程序 (Providers) > Active Directory**。

**步骤 2** 选中已配置的 Active Directory 旁边的复选框。

**步骤 3** 检查并确保列出的本地节点状态为未加入。

**步骤 4** 单击**删除 (Delete)**。

您已从 Active Directory 数据库中移除该配置。如果希望以后再使用 Active Directory，您可以重新提交有效的 Active Directory 配置。

---

## 启用 Active Directory 调试日志

默认情况下，不会记录 Active Directory 调试日志。启用 Active Directory 调试日志可能会影响 ISE-PIC 性能。

---

**步骤 1** 选择**管理 (Administration) > 日志记录 (Logging) > 调试日志配置 (Debug Log Configuration)**。

**步骤 2** 单击要从中获取 Active Directory 调试信息的 Cisco ISE-PIC 节点旁边的单选按钮，然后单击**编辑 (Edit)**。

**步骤 3** 单击 **Active Directory** 单选按钮，然后单击**编辑 (Edit)**。

**步骤 4** 从 Active Directory 旁的下拉列表中选择 **DEBUG**。这将包括错误、警告和 verbose 日志。要获得完整日志，请选择 **TRACE**。

步骤 5 单击保存 (Save)。

## Active Directory 设置

Active Directory AD 是用于从中接收用户信息（包括用户名和 IP 地址）的高度安全且精确的源。

要通过创建和编辑加入点来创建和管理 Active Directory 探测器，请依次选择提供程序 (Providers) > Active Directory。

有关详细信息，请参阅[添加 Active Directory 加入点并将思科 ISE-PIC 节点加入到该加入点](#)，第 20 页。

依次选择提供程序 (Providers) > Active Directory，然后选中要编辑的加入点并单击编辑 (Edit)。对于“加入域” (Join Domain) 屏幕，请依次选择提供程序 (Providers) > Active Directory，选中要编辑的加入点并单击加入 (Join)。

表 3: Active Directory 加入点名称设置和加入域窗口

字段名称	说明
加入点名称	用于快速轻松地区分此已配置加入点的唯一名称。
Active Directory 域	此节点连接到的 Active Directory 域的域名。
域管理员	这是具有管理员权限的 Active Directory 用户的用户主体名称或用户账户名称。
密码	这是 Active Directory 中配置的域管理员的密码。
指定组织单位	输入管理员的组织单位信息
存储凭证	您的管理员的用户名和密码，以便用于为监控配置的所有域控制器 (DC)。 对于终端探测器，必须选择存储凭证 (Store credentials)。

选择提供程序 (Providers) > Active Directory。

表 4: Active Directory 加入/退出窗口

字段名称	说明
ISE 节点 (ISE Node)	安装中的特定节点的 URL。
ISE 节点角色	表示节点是安装中的主节点还是辅助节点。
状态	指示节点是否主动加入 Active Directory 域。

字段名称	说明
域控制器	对于加入 Active Directory 的节点，此列指示节点在 Active Directory 域中连接到的特定域控制器。
站点	仅对于完整 ISE 安装相关。有关详细信息，请参阅 <a href="#">将 ISE-PIC 升级到完整 ISE 安装，第 128 页</a> 。

表 5: 被动 ID 域控制器 (DC) 列表

字段	说明
域	域控制器所在的服务器的完全限定域名。
DC 主机	域控制器所在的主机。
站点	仅对于完整 ISE 安装相关。有关详细信息，请参阅 <a href="#">将 ISE-PIC 升级到完整 ISE 安装，第 128 页</a> 。
IP 地址	域控制器的 IP 地址。
监控方法	<p>通过以下方法之一监控 Active Directory 域控制器的用户身份信息：</p> <ul style="list-style-type: none"> <li>• WMI：使用 WMI 基础设施直接监控 Active Directory。</li> <li>• 代理名称：如果已定义代理来监控 Active Directory 的用户信息，请选择“代理” (Agent) 协议，并从下拉列表中选择要使用的代理。有关代理的详细信息，请参阅<a href="#">Active Directory 代理，第 33 页</a>。</li> </ul>

表 6: 被动 ID 域控制器 (DC) 编辑窗口

字段名称	说明
主机 FQDN	输入域控制器所在的服务器的完全限定域名。
说明	输入此域控制器的唯一说明，以便轻松标识此域控制器。
用户名	用于访问 Active Directory 的管理员的用户名。
密码	用于访问 Active Directory 的管理员的密码。

字段名称	说明
协议	<p>通过以下方法之一监控 Active Directory 域控制器的用户身份信息：</p> <ul style="list-style-type: none"> <li>• WMI：使用 WMI 基础设施直接监控 Active Directory。</li> <li>• 代理名称：如果已定义代理来监控 Active Directory 的用户信息，请选择“代理” (Agent) 协议，并从下拉列表中选择要使用的代理。有关代理的详细信息，请参阅 <a href="#">Active Directory 代理，第 33 页</a>。</li> </ul>

系统从 Active Directory 来定义和管理 Active Directory 组，并且可从此选项卡查看加入此节点的 Active Directory 的组。有关 Active Directory 的详细信息，请参阅 <https://msdn.microsoft.com/en-us/library/bb742437.aspx>。

依次选择提供程序 (Providers) > Active Directory > 高级设置 (Advanced Settings)。

表 7: Active Directory 高级设置

字段名称	说明
历史记录间隔	被动身份服务 读取已出现的用户登录信息的时间段。启动或重新启动 被动身份服务 以跟进在其不可用情况下生成的事件时需要此项。当终端探测器处于活动状态时，它将保持此间隔的频率。
用户会话老化时间	用户可以登录的时间量。被动身份服务 会识别 DC 中的新用户登录事件，但是 DC 在用户注销时不会进行报告。通过老化时间，ISE-PIC 可以确定用户登录的时间间隔。
NTLM 协议设置	您可以选择 NTLMv1 或 NTLMv2 作为 ISE-PIC 和 DC 之间的通信协议。NTLMv2 是建议默认值。







## 第 4 章

# 提供程序

---

为了使 ISE-PIC 能够向订用服务的使用者（用户）提供身份信息，您必须首先配置 ISE-PIC 探测器，它连接到身份提供程序。

下表提供了有关 ISE-PIC 中所有提供程序和探测类型的详细信息。有关 Active Directory 的详细信息，请参阅 [Active Directory 作为探测器和提供程序](#)，第 17 页。

您可以定义下列提供程序类型：

表 8: 提供程序类型

提供程序类型（探测器）	说明	源系统（提供程序）	技术	收集的用户身份信息	文档链接
Active Directory (AD)	<p>用于从中接收用户信息的高度安全而精确且最常用的源。</p> <p>作为探测器，AD 运用 WMI 技术传送经过身份验证的用户身份。</p> <p>此外，AD 本身而不是探测器，而是用作其他探测器从中检索用户数据的源系统（提供程序）。</p>	Active Directory 域控制器	WMI	<ul style="list-style-type: none"> <li>• 用户名</li> <li>• IP 地址</li> <li>• 域 (Domain)</li> </ul>	<a href="#">Active Directory 作为探测器和提供程序，第 17 页</a>
代理	Active Directory 域控制器或成员服务器上安装的本地 32 位应用。代理探测器是将 Active Directory 用于用户身份信息的一种快速高效的解决方案。		域控制器或成员服务器上安装的代理。	<ul style="list-style-type: none"> <li>• 用户名</li> <li>• IP 地址</li> <li>• 域 (Domain)</li> </ul>	<a href="#">Active Directory 代理，第 33 页</a>
终端	除其他已配置的探测器以外，始终在后台运行，以便验证用户是否仍然处于连接状态。		WMI	用户是否仍然处于连接状态	<a href="#">终端探测器，第 65 页</a>
SPAN	位于网络交换机上，以便侦听网络流量并根据 Active Directory 数据提取用户身份信息。		交换机上安装的 SPAN，以及 Kerberos 消息	<ul style="list-style-type: none"> <li>• 用户名</li> <li>• IP 地址</li> <li>• 域 (Domain)</li> </ul>	<a href="#">SPAN，第 42 页</a>

提供程序类型（探测器）	说明	源系统（提供程序）	技术	收集的用户身份信息	文档链接
API 提供程序	使用 ISE-PIC 提供的 RESTful API 服务从编程为与 RESTful API 客户端进行通信的任何系统收集用户身份信息。	编程为与 REST API 客户端进行通信的任何系统。	RESTful API。以 JSON 格式发送到用户的用户身份。	<ul style="list-style-type: none"> <li>• 用户名</li> <li>• IP 地址</li> <li>• 端口范围</li> <li>• 域</li> </ul>	<a href="#">API 提供程序，第 37 页</a>
系统日志	解析系统日志消息和检索用户身份，包括 MAC 地址。	<ul style="list-style-type: none"> <li>• 常规系统日志消息提供程序</li> <li>• DHCP 服务器</li> </ul>	系统日志消息	<ul style="list-style-type: none"> <li>• 用户名</li> <li>• IP 地址</li> <li>• MAC 地址</li> <li>• 域</li> </ul>	<a href="#">系统日志提供程序，第 43 页</a>



**注释** pxGrid 会每秒为会话主题发送 200 个事件，以避免客户端过载。如果发布方发送的事件超过 200 个，则额外的事件将排队并在下一批中发送。

如果 pxGrid 在很长一段时间内持续收到每秒超过 200 个事件，它可能会消耗比平时更多的内存来存储积压的事件。这可能会影响 pxGrid 的性能。

- [Active Directory 代理，第 33 页](#)
- [API 提供程序，第 37 页](#)
- [SPAN，第 42 页](#)
- [系统日志提供程序，第 43 页](#)
- [过滤被动身份服务，第 64 页](#)
- [终端探测器，第 65 页](#)

## Active Directory 代理

从 ISE-PIC，在 Active Directory (AD) 域控制器 (DC) 或成员服务器上的任意位置（根据配置）安装本地 32 位应用（即域控制器 (DC) 代理），以从 AD 检索用户身份信息，然后将这些身份发送给已配置的用户。代理探测器是将 Active Directory 用于用户身份信息的一种快速高效的解决方案。代理可安装在单独的域中，也可安装在 AD 域中，并且一旦安装，它们就会每分钟提供一次 ISE-PIC 的状态更新。

代理可由 ISE-PIC 自动安装和配置，您也可以手动对其进行安装。安装时，会发生以下情况：

- 代理及其关联文件安装在以下路径：**Program Files/Cisco/Cisco ISE PassiveID Agent**
- 系统将安装一个名为 **PICAgent.exe.config** 的配置文件，其中会指示代理的日志记录级别。您可以从该配置文件内手动更改日志记录级别。
- CiscoISEPICAgent.log 文件与所有日志记录消息一起存储。
- nodes.txt 文件包含部署中可与代理进行通信的所有节点的列表。代理会访问列表中的第一个节点。如果无法访问该节点，代理将根据列表中节点的顺序继续尝试通信。对于手动安装，必须打开文件并输入节点 IP 地址。（手动或自动）安装完成后，便只能通过手动更新该文件来对其进行更改。打开文件，然后根据需要添加、更改或删除节点 IP 地址。
- 思科 ISE PassiveID 代理服务在机器上运行，您可从“Windows 服务”对话框管理该机器。
- ISE-PIC 最多支持 100 个域控制器，而每个代理最多可以监控 10 个域控制器。要监控 100 个域控制器，必须配置 10 个代理。
- 仅在 Windows Server 2008 及更高版本上支持 Active Directory 代理。如果无法安装代理，则对被动身份服务使用 Active Directory 探测器。有关详细信息，请参阅[Active Directory 作为探测器和提供程序](#)，第 17 页。



**注释** 即使您在成员服务器上运行 AD 代理，它也仍会在 Active Directory 中查询登录请求。

## 自动安装并部署 Active Directory 代理

配置代理提供程序以监控域控制器的用户身份时，代理必须安装在成员服务器或域控制器上。代理可由 ISE-PIC 自动安装，也可以手动对其进行安装。自动或手动安装后，必须配置已安装的代理来监控指定域控制器，而非默认 WMI。以下流程说明了如何自动安装并配置代理以监控域控制器。

### 开始之前

- 从服务器端对相关 DNS 服务器配置反向查找。有关 ISE-PIC 的 DNS 服务器配置要求的详细信息，请参阅[DNS 服务器](#)，第 13 页
- 确保在指定用于代理的机器上更新 Microsoft .NET Framework，最低更新至版本 4.0。有关 .NET Framework 的详细信息，请参阅<https://www.microsoft.com/net/framework>。
- 创建 AD 加入点，并至少添加一个域控制器。有关创建加入点的详细信息，请参阅[Active Directory 作为探测器和提供程序](#)，第 17 页。

对 AD、代理、SPAN 和系统日志探测器使用 AD 用户组。有关 AD 组的详细信息，请参阅[配置 Active Directory 用户组](#)，第 22 页。

**步骤 1** 选择提供程序 (Providers) > 代理 (Agents)。

**步骤 2** 要添加新客户端，请从表的顶部单击添加 (Add)。

- 步骤 3 要创建新代理并将其自动安装到您在此配置中指示的主机上，请选择**部署新代理 (Deploy New Agent)**。
- 步骤 4 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅[Active Directory 代理设置](#)，第 36 页。
- 步骤 5 单击**部署 (Deploy)**。  
代理将根据您在配置中指示的域自动安装到主机上，并保存设置。代理现在显示在“Agents” (代理) 表格中，并可应用于监控指定域控制器，如以下步骤所述。
- 步骤 6 选择**提供程序 (Providers) > Active Directory** 以查看当前配置的所有接入点。
- 步骤 7 单击您要从中启用所创建代理的接入点的链接。
- 步骤 8 选择**被动 ID (Passive ID)** 选项卡以配置您作为前提条件的一部分而添加的域控制器。
- 步骤 9 选择您要通过所创建代理来监控的域控制器，然后单击**编辑 (Edit)**。
- 步骤 10 从**协议 (Protocol)** 下拉列表中，选择**代理 (Agent)**。
- 步骤 11 从**代理 (Agent)** 下拉列表中选择您创建的代理。输入您创建的代理的用户名和密码凭证（如果有），然后单击**保存 (Save)**。

## 手动安装并部署 Active Directory 代理

配置代理提供程序以监控域控制器的用户身份时，代理必须安装在成员服务器或域控制器上。代理可由 ISE-PIC 自动安装，也可以手动对其进行安装。自动或手动安装后，必须配置已安装的代理来监控指定域控制器，而非默认 WMI。以下流程说明了如何手动安装并配置代理以监控域控制器。

### 开始之前

- 从服务器端对相关 DNS 服务器配置反向查找。有关 ISE-PIC 的 DNS 服务器配置要求的详细信息，请参阅[DNS 服务器](#)，第 13 页
- 确保在指定用于代理的机器上更新 Microsoft .NET Framework，最低更新至版本 4.0。有关 .NET Framework 的详细信息，请参阅<https://www.microsoft.com/net/framework>。
- 创建 AD 加入点，并至少添加一个域控制器。有关创建加入点的详细信息，请参阅[Active Directory 作为探测器和提供程序](#)，第 17 页。

对 AD、代理、SPAN 和系统日志探测器使用 AD 用户组。有关 AD 组的详细信息，请参阅[配置 Active Directory 用户组](#)，第 22 页。

- 步骤 1 选择**提供程序 (Providers) > 代理 (Agents)**。
- 步骤 2 单击**下载代理 (Download Agent)** 以下载 `picagent-installer.zip` 文件进行手动安装。  
此文件将下载至标准 Windows 下载文件夹。
- 步骤 3 将此 zip 文件置于指定主机并运行安装。
- 步骤 4 从 ISE-PIC GUI 中，同样依次选择**提供程序 (Providers) > 代理 (Agents)**。
- 步骤 5 要配置新代理，请从表的顶部单击**添加 (Add)**。
- 步骤 6 要配置已在主机上安装的代理，请选择**注册现有代理 (Register Existing Agent)**。
- 步骤 7 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅[Active Directory 代理设置](#)，第 36 页。

- 步骤 8** 单击**保存 (Save)**。  
系统会保存代理设置。代理现在显示在“代理” (Agents) 表格中，并可应用于监控指定域控制器，如以下步骤所述。
- 步骤 9** 依次选择**提供程序 (Providers) > Active Directory** 以查看当前配置的所有接入点。
- 步骤 10** 单击您要从中启用所创建代理的接入点的链接。
- 步骤 11** 选择**被动 ID (Passive ID)** 选项卡以配置您作为前提条件的一部分而添加的域控制器。
- 步骤 12** 选择您要通过所创建代理来监控的域控制器，然后单击**编辑 (Edit)**。
- 步骤 13** 从**协议 (Protocol)** 下拉列表中，选择**代理 (Agent)**。
- 步骤 14** 从**代理 (Agent)** 下拉列表中选择您创建的代理。输入您创建的代理的用户名和密码凭证（如果有），然后单击**保存 (Save)**。

## 卸载代理

可以直接从 Windows 轻松（手动）卸载自动或手动安装的代理。

- 步骤 1** 在 Windows 对话框中，转至**程序和功能**。
- 步骤 2** 在已安装程序的列表中，查找并选择思科 ISE 被动 ID 代理。
- 步骤 3** 单击**卸载 (Uninstall)**。

## Active Directory 代理设置

允许 ISE-PIC 在网络中的指定主机上自动安装代理，以从不同的域控制器 (DC) 检索用户身份信息并向 ISE-PIC 订户提供此信息。

要创建和管理代理，请依次选择**提供程序 (Providers) > 代理 (Agents)**。请参阅[自动安装并部署 Active Directory 代理](#)，第 34 页。

表 9: “代理” (Agents) 窗口

字段名称	说明
名称	您配置的代理名称。
主机	安装代理的主机的完全限定域名。
监控	此为指定代理所监控的域控制器的逗号分隔列表。

表 10: 新建代理 (Agents New)

字段	说明
“部署新代理” (Deploy New Agent) 或 “注册现有代理” (Register Existing Agent)	<ul style="list-style-type: none"> <li>“部署新代理” (Deploy New Agent): 在指定主机上安装新代理。</li> <li>“注册现有代理” (Register Existing Agent): 在主机上手动安装代理, 然后从此屏幕为 ISE-PIC 配置此代理以启用服务。</li> </ul>
名称	输入可用于轻松识别代理的名称。
说明	输入可用于轻松识别代理的说明。
主机 FQDN	此为已安装代理 (注册现有代理) 或将要安装代理 (自动部署) 的主机的完全限定域名。
用户名	输入用户名以访问要安装代理的主机。ISE-PIC 将使用这些凭证为您安装代理。
密码	输入用户密码以访问要安装代理的主机。ISE-PIC 将使用这些凭证为您安装代理。

## API 提供程序

通过思科 ISE-PIC 中的“API 提供程序”功能, 可将用户身份信息从自定义程序或从终端服务器 (TS) 代理推送到内置的 ISE-PIC REST API 服务。通过此方式, 可以自定义网络中的可编程客户端, 以将从任何网络访问控制 (NAC) 系统收集到的用户身份发送到服务。此外, 通过思科 ISE-PIC API 提供程序, 还可与网络应用 (例如 Citrix 服务器上的 TS 代理, 其中所有用户都具有同一 IP 地址但分配有唯一端口) 接合。

例如, 在 Citrix 服务器上运行的用于为根据 Active Directory (AD) 服务器进行身份验证的用户提供身份映射的代理可向 ISE-PIC 发送 REST 请求, 请求只要有新用户登录或注销便添加或删除用户会话。然后, ISE-PIC 获取从客户端传送的用户身份信息 (包括 IP 地址和已分配的端口), 并将其发送到预配置用户, 例如思科 Firepower 管理中心 (FMC)。

ISE-PIC REST API 框架通过 HTTPS 协议实施 REST 服务 (无需客户端证书验证), 并以 JSON (JavaScript Object Notation) 格式传送用户身份信息。有关 JSON 的详细信息, 请参阅 <http://www.json.org/>。

ISE-PIC REST API 服务会解析用户身份, 此外还会将该信息映射到端口范围, 以便区分同时登录到一个系统的不同用户。每次将端口分配给用户时, API 都会向 ISE-PIC 发送一条消息。

### REST API 提供程序流程

配置了从 ISE-PIC 到自定义客户端的网桥后 (通过将该客户端声明为 ISE-PIC 的提供程序, 并使该特定自定义程序 (客户端) 能够发送 RESTful 请求), ISE-PIC REST 服务便通过以下方式进行工作:

1. 对于客户端身份验证，思科 ISE-PIC 需要身份验证令牌。客户端机器上的自定义程序在发起联系时发送身份验证令牌请求，然后 ISE-PIC 每次都会通知先前令牌已到期。系统会返回令牌以响应请求，从而启用客户端和 ISE-PIC 服务之间的持续通信。
2. 用户登录到网络中后，客户端便会检索用户身份信息，并使用 API 添加命令将该信息发布到 ISE-PIC REST 服务。
3. 思科 ISE-PIC 接收并映射用户身份信息。
4. 思科 ISE-PIC 向用户发送已映射的用户身份信息。
5. 只要有必要，自定义机器即可发送用于移除用户信息的请求，方法是发送“删除 API”调用并包含在发送“添加”调用后作为响应接收到的用户 ID。

### 在 ISE-PIC 中使用 REST API 提供程序

按照以下步骤激活 ISE-PIC 中的 REST 服务：

1. 配置客户端。有关详细信息，请参阅客户端用户文档。
2. 确保您已正确配置 DNS 服务器，包括从 ISE-PIC 配置客户端机器的反向查找。有关 ISE-PIC 的 DNS 服务器配置要求的详细信息，请参阅 [DNS 服务器，第 13 页](#)
3. 请参阅 [为被动身份服务配置与 ISE-PIC REST 服务的桥接，第 38 页](#)。



**注 释** 要将 API 提供程序配置为使用 TS 代理，请在创建从 ISE-PIC 到该代理的网桥时添加 TS 代理信息，然后参考 TS 代理文档以获取有关发送 API 调用的信息。

4. 生成身份验证令牌并向 API 服务发送添加和删除请求。

## 为被动身份服务配置与 ISE-PIC REST 服务的桥接

为了使 ISE-PIC REST API 服务能够从特定客户端接收信息，必须首先从 ISE-PIC 定义该特定客户端。您可以定义多个具有不同 IP 地址的 REST API 客户端。

### 开始之前

- 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。有关思科 ISE-PIC 的 DNS 服务器配置要求的详细信息，请参阅 [DNS 服务器，第 13 页](#)

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择提供程序 (Providers) > API 提供程序 (API Providers) 以查看当前配置的所有客户端、编辑和删除现有客户端，以及配置新客户端。

系统将显示“API 提供程序”表，包括每个现有客户端的状态信息。

**步骤 2** 要添加新客户端，请从表的顶部单击添加 (Add)。

**步骤 3** 填写所有必填字段，以便正确配置客户端。有关详细信息，请参阅 [API 提供程序设置，第 39 页](#)。



**步骤 4 单击提交 (Submit)。**

系统将保存客户端配置，并将其屏幕会显示更新后的“API提供程序”表。客户端现在可以将发布内容发送到 ISE-PIC REST 服务。

**下一步做什么**

设置自定义客户端，以将身份验证令牌和用户身份发布到 ISE-PIC REST 服务。请参阅[将 API 调用发送到 ISE-PIC REST 服务，第 39 页](#)。

## 将 API 调用发送到 ISE-PIC REST 服务

**开始之前**

为 [被动身份服务配置与 ISE-PIC REST 服务的桥接，第 38 页](#)

**步骤 1** 在浏览器的地址栏中输入思科 ISE URL（例如 `https://<ise hostname or ip address>/admin/`）

**步骤 2** 在以下位置中输入已从 **API 提供程序 (API Providers)** 窗口中指定并配置的用户名和密码。有关详细信息，请参阅[为被动身份服务配置与 ISE-PIC REST 服务的桥接，第 38 页](#)。

**步骤 3** 按 **Enter** 键。

**步骤 4** 在目标节点的“URL 地址” (URL Address) 字段中输入 API 调用。

**步骤 5** 单击发送 (**Send**) 以发出 API 调用。

**下一步做什么**

请参阅 [API 调用，第 40 页](#) 以获取有关不同 API 调用、其架构及其结果的更多信息和详细信息。

## API 提供程序设置

在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择提供程序 (**Providers**) > **API Providers (API 提供程序)** 以为 [被动身份服务](#) 配置新的 REST API 客户端。



**注释** 可以使用请求调用来检索完整的 API 定义和对象架构，如下所示：

- 对于完整 API 规范 (wadl) - `https://YOUR_ISE:9094/application.wadl`
- 对于 API 模型和对象架构 - `https://YOUR_ISE:9094/application.wadl/xsd0.xsd`

表 11: API 提供程序设置

字段	说明
名称	输入此客户端的用于快速轻松地将其与其他客户端进行区分的唯一名称。
说明	输入此客户端的明确说明。
状态	选择 <b>已启用 (Enabled)</b> 以使客户端能够在完成配置时立即与 REST 服务进行交互。
主机/IP	输入客户端主机的 IP 地址。确保您已正确配置 DNS 服务器，包括从 ISE-PIC 配置客户端机器的反向查找。
用户名	创建在发布到 REST 服务时要使用的唯一用户名。
密码	创建在发布到 REST 服务时要使用的唯一密码。

## API 调用

这些 API 调用用于通过思科 ISE-PIC 来管理 被动身份服务 的用户身份事件。

目的：生成身份验证令牌

- 请求

POST

`https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken`

请求应包含 BasicAuth 授权报头。提供先前从 ISE-PIC GUI 创建的 API 提供程序凭证。有关详细信息，请参阅 [API 提供程序设置](#)，第 39 页。

- 响应报头

该报头包含 X-auth-access-token。这是发布其他 REST 请求时要使用的令牌。

- 响应正文

HTTP 204 No Content

目的：添加用户

- 请求

POST

`https://<PIC IP address>:9094/api/identity/v1/identity/useridentity`

在发布请求标头中添加 X-auth-access-token，例如，标头：X-auth-access-token，值：  
f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- 响应报头

201 创建

- 响应正文

```
{
  "user": "<username>",
  "srcPatRange": {
    "userPatStart": <user PAT start value>,
    "userPatEnd": <user PAT end value>,
    "patRangeStart": <PAT range start value>
  },
  "srcIpAddress": "<src IP address>",
  "agentInfo": "<Agent name>",
  "timestamp": "<ISO_8601 format i.e. “YYYY-MM-DDTHH:MM:SSZ” >",
  "domain": "<domain>"
}
```

- 注

- 可在以上 JSON 中删除 srcPatRange 以创建单个 IP 用户绑定。
- 响应正文包含“ID”，这是所创建的用户会话绑定的唯一标识符。发送 DELETE 请求时使用此 ID，以指示应删除哪个用户。
- 此响应还包含自链接，这是此新创建的用户会话绑定的 URL。

### 目的：删除用户

- 请求

DELETE

https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>

在 <id> 中，输入从“添加”响应接收到的 ID。

在删除请求报头中添加 X-auth-access-token，例如，报头：X-auth-access-token，值：  
f3f25d81-3ac5-43ee-bbfb-20955643f6a7

- 响应报头

200 OK

- 响应正文

响应正文包含有关已删除的用户会话绑定的详细信息。

# SPAN

SPAN通过它可快速轻松地启用思科 ISE-PIC 以侦听网络和检索用户信息，而不必将 Active Directory 配置为直接使用思科 ISE-PIC。SPAN 嗅探网络流量（专门检查 Kerberos 消息），提取 Active Directory 也已存储的用户身份信息，并将该信息发送到 ISE-PIC。然后，ISE-PIC 解析信息，最终将用户名、IP 地址和域名传送到您也已从 ISE-PIC 配置的用户。

为了使 SPAN 侦听网络和提取 Active Directory 用户信息，ISE-PIC 和 Active Directory 必须连接到网络上的同一交换机。这样，SPAN 便可以从 Active Directory 复制并镜像所有用户身份数据。

使用 SPAN，将通过以下方式检索用户信息：

1. 用户终端登录网络。
2. 登录和用户数据存储在 Kerberos 消息中。
3. 一旦用户登录且用户数据通过交换机进行传递，SPAN 就会镜像网络数据。
4. 思科 ISE-PIC 侦听网络以获取用户信息，并从交换机检索镜像的数据。
5. 思科 ISE-PIC 解析用户信息并更新被动 ID 映射。
6. 思科 ISE-PIC 将已解析的用户信息传送到用户。

## 使用 SPAN

### 开始之前

要使 ISE-PIC 从网络交换机接收 SPAN 流量，必须先定义侦听此交换机的节点和节点接口。可以配置 SPAN 以侦听安装的不同 ISE-PIC 节点。对于每个节点，只能配置一个接口来侦听网络，用于侦听的接口只能专用于 SPAN。

此外，您必须牢记：

- 确保已在网络上配置 Active Directory。
- 在同样连接至 Active Directory 的网络中的交换机上运行 CLI，以确保交换机可以与 ISE-PIC 通信。
- 配置交换机以从 AD 镜像网络。
- 配置专用于 SPAN 的 ISE-PIC 网络接口卡 (NIC)。此 NIC 仅用于 SPAN 流量。
- 通过命令行界面，确保激活专用于 SPAN 的 NIC。
- 创建仅将 Kerberos 流量发送到 SPAN 端口的 VACL。

---

**步骤 1** 选择提供程序 (Providers) > SPAN 以配置 SPAN。

**步骤 2 注释** 我们建议 GigabitEthernet0 网卡 (NIC) 保持可用，并选择任何其他可用 NIC 来配置 SPAN。GigabitEthernet0 用于系统管理。

输入有意义的说明（可选），选择状态**已启用 (Enabled)**，并选择将用于侦听网络交换机的节点和相关 NIC。有关详细信息，请参阅[SPAN 设置，第 43 页](#)。

**步骤 3 单击保存 (Save)。**

系统将保存 SPAN 配置，ISE-PIC 现在主动侦听网络流量。

## SPAN 设置

从已部署的每个节点，通过在客户端网络上安装 SPAN，可快速轻松地配置 ISE-PIC 以接收用户身份。

表 12: SPAN 设置

字段	说明
说明 (Description)	输入唯一说明以向您提醒当前启用的节点和接口。
状态 (Status)	选择 <b>已启用 (Enabled)</b> 可在完成配置时立即启用客户端。
接口 NIC (Interface NIC)	为 ISE-PIC 选择一个或两个节点，然后对于每个选定节点，选择用于侦听网络以获取信息的节点接口。  注释 我们建议将 GigabitEthernet0 NIC 保持可用，并选择任何其他可用 NIC 来配置 SPAN。GigabitEthernet0 用于系统管理。

## 系统日志提供程序

ISE-PIC 会解析来自任何传送系统日志消息的任何客户端（身份数据提供程序）的系统日志消息，包括常规系统日志消息（来自 InfoBlox、Blue Coat、BlueCat 和 Lucent 等提供程序）以及 DHCP 系统日志消息，并发送回用户身份信息，包括 MAC 地址。然后将此映射的用户身份数据传送到用户。

您可以指定接收用户身份数据的系统日志客户端（请参阅[配置系统日志客户端，第 44 页](#)）。配置提供程序时，您必须指定连接方法（TCP 或 UDP）以及要用于解析的系统日志模板。



**注释** 当所配置的连接类型为 TCP 时，如果消息报头存在问题且无法解析主机名，则 ISE-PIC 会尝试将数据包中接收到的 IP 地址与已为 ISE-PIC 中的系统日志消息配置的提供程序列表中任何提供程序的 IP 地址进行匹配。要查看此列表，请选择**提供程序 (Providers) > 系统日志提供程序 (Syslog Providers)**。我们建议您检查消息报头并根据需要进行自定义，以便保证解析成功。有关自定义报头的详细信息，请参阅[自定义系统日志报头，第 50 页](#)。

系统日志探测器会将接收到的系统日志消息发送到 ISE-PIC 解析器，该解析器会映射用户身份信息，并将该信息发布到 ISE-PIC。然后，ISE-PIC 将已解析和已映射的用户身份信息传送到 ISE-PIC 用户。



**注释** DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便 ISE-PIC 可以首先检查在本地会话目录（从“实时会话” (Live Sessions) 中显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。

要从 ISE-PIC 解析用户身份的系统日志消息，请执行以下操作：

- 配置要从中接收用户身份数据的系统日志客户端。请参阅[配置系统日志客户端，第 44 页](#)。
- 自定义单个消息报头。请参阅[自定义系统日志报头，第 50 页](#)。
- 通过创建模板来自定义消息正文。请参阅[自定义系统日志消息正文，第 49 页](#)。
- 在将系统日志客户端配置为用于解析的消息模板时使用 ISE-PIC 中预定义的消息模板，或者基于这些预定义的模板自定义报头或正文模板。请参阅[使用系统日志预定义消息模板，第 54 页](#)。

## 配置系统日志客户端

为了使思科 ISE-PIC 能够从特定客户端侦听系统日志消息，必须首先从思科 ISE-PIC 定义该特定客户端。您可以使用不同 IP 地址定义多个提供程序。

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择**提供程序 (Providers) > 系统日志提供程序 (Syslog Providers)** 以查看当前配置的所有客户端、编辑和删除现有客户端，以及配置新客户端。系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

**步骤 2** 要配置新系统日志客户端，请从表的顶部单击**添加 (Add)**。

**步骤 3** 填写所有必填字段（请参阅[系统日志设置，第 45 页](#)以获取更多详细信息），并在必要时创建消息模板（请参阅[自定义系统日志消息正文，第 49 页](#)以获取更多详细信息），以便正确配置客户端。

**步骤 4** 单击**提交 (Submit)**。

## 系统日志设置

配置思科 ISE-PIC 以通过来自特定客户端的系统日志消息接收用户身份，包括 MAC 地址。您可以使用不同 IP 地址定义多个提供程序。

表 13: 系统日志提供程序

字段名称	说明
名称 (Name)	输入用于快速轻松地区分此已配置客户端的唯一名称。
说明 (Description)	此系统日志提供程序的有意义说明。
状态 (Status)	选择 <b>已启用 (Enabled)</b> 可在完成配置时立即启用客户端。
主机 (Host)	输入主机的 FQDN。
连接类型 (Connection Type)	<p>输入 UDP 或 TCP 以指示 ISE-PIC 用于侦听系统日志消息的通道。</p> <p><b>注释</b> 当所配置的连接类型为 TCP 时，如果消息报头存在问题且无法解析主机名，则思科 ISE 会尝试将数据包中接收到的 IP 地址与已为思科 ISE 中的系统日志消息配置的提供程序列表中任何提供程序的 IP 地址进行匹配。</p> <p>要查看此列表，请选择 <b>提供程序 (Providers) &gt; 系统日志提供程序 (Syslog Providers)</b>。我们建议您检查消息报头并根据需要进行自定义，以便确保解析成功。有关自定义报头的详细信息，请参阅 <a href="#">自定义系统日志报头</a>，第 50 页。</p>

字段名称	说明
模板 (Template)	



字段名称	说明
	<p>模板指示精确正文消息结构，以便解析器可以识别应解析、映射和传送的系统日志消息中的信息段。</p> <p>例如，模板可以指示用户名的确切位置，以便解析器能够在接收到的每条消息中查找用户名。</p> <p>从此字段中，指示要使用的模板（适用于系统日志消息的正文），以便识别并正确解析系统日志消息。</p> <p>从预定义下拉列表中进行选择，或者单击<b>新建 (New)</b> 以创建自己的自定义模板。有关创建新模板的详细信息，请参阅<a href="#">自定义系统日志消息正文，第 49 页</a>。大多数预定义模板都使用正则表达式，并且自定义模板也应使用正则表达式。</p> <p><b>注释</b> 只能编辑或删除自定义模板，而无法修改下拉列表中的预定义系统模板。</p> <p>ISE-PIC 当前提供下列预定义 DHCP 提供程序模板：</p> <ul style="list-style-type: none"> <li>• InfoBlox</li> <li>• BlueCat</li> <li>• Lucent_QIP</li> <li>• DHCPD</li> <li>• MSAD DHCP</li> </ul> <p><b>注释</b> DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便思科 ISE 可以首先检查在本地会话目录（从“实时会话” (Live Sessions) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。</p> <p>如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。</p> <p>思科 ISE 提供下列预定义常规系统日志提供程序</p>

字段名称	说明
	模板： <ul style="list-style-type: none"> <li>• ISE</li> <li>• ACS</li> <li>• F5_VPN</li> <li>• ASA_VPN</li> <li>• Blue Coat</li> <li>• Aerohive</li> <li>• Safe connect_NAC</li> <li>• Nortel_VPN</li> </ul> 有关模板的信息，请参阅 <a href="#">使用系统日志预定义消息模板，第 54 页</a> 。
<b>默认域 (Default Domain)</b>	如果在特定用户的系统日志消息中未识别域，则会将此默认域自动分配给用户，以便确保为所有用户都分配域。  通过默认域或通过从消息中解析的域，会将用户名附加到 <code>username@domain</code> ，从而包含该域，以便获取有关用户和用户组的详细信息。

## 自定义系统日志消息结构（模板）

模板指示精确消息结构，以便解析器可以识别应解析、映射和传送的系统日志消息中的信息段。例如，模板可以指示用户名的确切位置，以便解析器能够在接收到的每条消息中查找用户名。模板可确定新增和删除映射消息的受支持结构。

通过思科 ISE-PIC，您可以自定义单个消息报头和多个正文结构以供 ISE-PIC 解析器使用。

模板应包含正则表达式，用于定义用户名、IP 地址、MAC 地址和域的结构，以使 ISE-PIC 解析器能够正确识别消息是要添加还是删除用户身份映射，以及正确解析用户详细信息。

自定义消息模板时，可以选择基于 ISE-PIC 中预定义的消息模板进行自定义，参考这些预定义选项中使用的正则表达式和消息结构。有关预定义模板、正则表达式、消息结构、示例等的详细信息，请参阅[使用系统日志预定义消息模板，第 54 页](#)。

可以自定义：

- 单个消息报头 - [自定义系统日志报头，第 50 页](#)
- 多个消息正文 - [自定义系统日志消息正文，第 49 页](#)。



**注释** DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便思科 ISE 可以首先检查在本地会话目录（从“实时会话” (Live Sessions) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。

无法将正确匹配、分析和映射 DHCP 消息中的详细信息所需的延迟应用于自定义模板，因此不建议对 DHCP 消息模板进行自定义。请改为使用任何预定义 DHCP 模板。

## 自定义系统日志消息正文

通过思科 ISE-PIC，您可以自定义将由 ISE-PIC 解析器解析的自有系统日志消息模板（通过自定义消息正文）。模板应包含正则表达式，以定义用户名、IP 地址、MAC 地址和域的结构。



**注释** DHCP 系统日志消息不包含用户名。因此，系统从解析器传送这些消息并带有延迟，以便思科 ISE 可以首先检查在本地会话目录（从“实时会话” (Live Sessions) 进行显示）中注册的用户，并尝试按用户的 IP 地址将这些用户与接收到的 DHCP 系统日志消息中列出的 IP 地址进行匹配，从而正确解析和传送用户身份信息。如果从 DHCP 系统日志消息中接收到的数据无法与任何当前登录的用户匹配，则不会解析消息，并且不会传送用户身份。

无法将正确匹配、分析和映射 DHCP 消息中的详细信息所需的延迟应用于自定义模板，因此不建议对 DHCP 消息模板进行自定义。请改为使用任何预定义 DHCP 模板。

从系统日志客户端配置屏幕中创建和编辑系统日志消息正文模板。



**注释** 您只能编辑自己的自定义模板。无法更改系统提供的预定义模板。

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择提供程序 (Providers) > 系统日志提供程序 (Syslog Providers) 以查看当前配置的所有客户端、编辑和删除现有客户端，以及配置新客户端。

系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

**步骤 2** 单击添加(Add)以添加新系统日志客户端，或者单击编辑(Edit)来更新已配置的客户端。有关配置和更新系统日志客户端的详细信息，请参阅配置系统日志客户端，第 44 页。

**步骤 3** 在系统日志提供程序 (Syslog Providers) 窗口中，单击新建 (New) 以创建新消息模板。要编辑现有模板，请从下拉列表中选择该模板，然后单击编辑 (Edit)。

**步骤 4** 填写所有必填字段。

有关如何正确输入值的信息，请参阅系统日志自定义模板设置和示例，第 51 页。

**步骤 5** 单击测试 (Test) 以根据所输入的字符串正确解析消息。

步骤 6 单击保存 (Save)。

## 自定义系统日志报头

系统日志报头还包含消息源于的主机名。如果思科 ISE-PIC 消息解析器未识别系统日志消息，则可能需要通过配置前置于主机名的分隔符来自定义消息报头，从而使思科 ISE-PIC 能够正确识别主机名并解析消息。有关此屏幕中的字段的更多详细信息，请参阅[系统日志自定义模板设置和示例](#)，第 51 页。只要接收到消息，便会将自定义报头配置保存并添加到解析器所使用的报头类型。



**注释** 只能自定义单个报头。自定义报头后，在单击自定义报头 (**Custom Header**) 并创建模板时，将仅保存最新配置。

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (≡)，然后选择提供程序 (**Providers**) > 系统日志提供程序 (**Syslog Providers**) 以查看当前配置的所有客户端、编辑和删除现有客户端，以及配置新客户端。

系统将显示“系统日志提供程序”表，包括每个现有客户端的状态信息。

**步骤 2** 单击自定义报头 (**Custom Header**) 以打开“系统日志自定义报头” (Syslog Custom Header) 屏幕。

**步骤 3** 在粘贴示例系统日志 (**Paste sample syslog**) 字段中，输入系统日志消息中报头格式的示例。例如，从其中一条消息复制并粘贴以下报头：**<181>Oct 10 15:14:08 Cisco.com**。

**步骤 4** 在分隔符 (**Separator**) 字段中，指示单词是以空格还是制表符分隔。

**步骤 5** 在报头中的主机名位置 (**Position of hostname in header**) 字段中，指示报头中表示主机名的位置。例如，在以上提供的报头中，主机名是报头中的第四个单词。输入 4 可指示此位置。

**主机名 (Hostname)** 字段根据前三个字段中指示的详细信息来显示主机名。例如，如果粘贴示例系统日志中的报头示例如下：

```
<181>Oct 10 15:14:08 Cisco.com
```

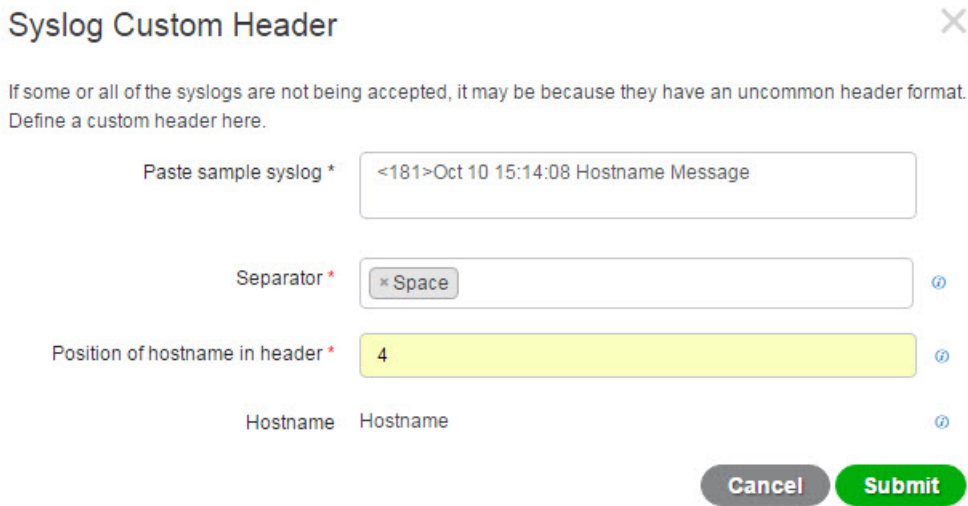
分隔符指示为空格，并且报头中的主机名位置输入为 4。

主机名将自动显示为 Cisco.com，这是粘贴示例系统日志字段中粘贴的报头短语中的第四个单词。

如果未正确显示主机名，请检查您已在分隔符 (**Separator**) 和报头中的主机名位置 (**Position of hostname in header**) 字段中输入的数据。

此示例与以下截屏相同：

图 3: 自定义系统日志报头



**Syslog Custom Header**

If some or all of the syslogs are not being accepted, it may be because they have an uncommon header format. Define a custom header here.

Paste sample syslog \*

Separator \*

Position of hostname in header \*

Hostname Hostname

**步骤 6 单击提交 (Submit)。**

只要接收到消息，便会将自定义报头配置保存并添加到解析器所使用的报头类型。

## 系统日志自定义模板设置和示例

通过思科 ISE-PIC，您可以自定义将由 ISE-PIC 解析器解析的自有系统日志消息模板。自定义模板确定了新增和删除映射消息的受支持结构。模板应包含正则表达式，用于定义用户名、IP 地址、MAC 地址和域的结构，以使 ISE-PIC 解析器能够正确识别消息是要添加还是删除用户身份映射，以及正确解析用户详细信息。



**注释** 大多数预定义模板都使用正则表达式。自定义模板也应使用正则表达式。

### 系统日志报头部分

您可以通过配置前置于主机名的分隔符来自定义系统日志探测器可识别的单个报头。

下表介绍可在自定义系统日志报头中包含的不同部分和字段。有关正则表达式的详细信息，请参阅[表 16: 自定义模板的正则表达式，第 53 页](#)。

表 14: 系统日志自定义报头

字段	说明
粘贴示例系统日志 (Paste sample syslog)	输入系统日志消息中的报头格式的示例。例如，复制并粘贴以下报头：  <181>Oct 10 15:14:08 Hostname Message
分隔符 (Separator)	指示单词是以空格还是制表符分隔。
报头中的主机名位置 (Position of hostname in header)	指示报头中表示主机名的位置。例如，在以上提供的报头中，主机名是报头中的第四个单词。输入 4 可指示此位置。
主机名 (Hostname)	根据前三个字段中指示的详细信息来显示主机名。例如，如果粘贴示例系统日志中的报头示例如下：  <181>Oct 10 15:14:08 Hostname Message  分隔符指示为空格，并且报头中的主机名位置输入为 4。  主机名将自动显示为 Hostname。  如果未正确显示主机名，请检查您已在分隔符和报头中的主机名位置字段中输入的数据。

#### 消息正文的系统日志模板部分和说明

下表介绍可在自定义系统日志消息模板中包含的不同部分和字段。有关正则表达式的详细信息，请参阅[表 16: 自定义模板的正则表达式，第 53 页](#)。

表 15: 系统日志模板

部 字 段 件	说明
名称 (Name)	用于识别此模板的用途的唯一名称。

部件	说明
新映射 (New Mapping)	描述与此模板配合用于添加新用户的映射类型的正则表达式。例如，在此字段中输入“logged on from”可指示已登录到 F5 VPN 的新用户。
已删除的映射 (Removed Mapping)	描述与此模板配合用于删除用户的映射类型的正则表达式。例如，在此字段中输入“session disconnect”可指示应为 ASA VPN 删除的用户。
用户 IP 地址 (IP Address)	指示要捕获的 IP 地址的正则表达式。 例如，对于 Bluecat 消息，要捕获此 IP 地址范围内的用户的身份，请输入： (on\s to\s)((?:25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)\.)\{3\}(?:25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)
用户名 (User Name)	指示要捕获的用户名格式的正则表达式。
域 (Domain)	指示要捕获的域的正则表达式。
MAC 地址 (Mac Address)	指示要捕获的 MAC 地址格式的正则表达式。

### 正则表达式示例

要解析消息，请使用正则表达式。此部分提供正则表达式示例，以便解析 IP 地址、用户名和添加映射消息。

例如，使用正则表达式解析以下消息：

```
<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session
```

```
<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user
```

正则表达式按下表中进行定义。

表 16: 自定义模板的正则表达式

部件	正则表达式
IP 地址	Address <([\s]+)> address ([\s]+)
用户名	User <([\s]+)> Username = ([\s]+)

部件	正则表达式
添加映射消息	(%ASA-4-722051 %ASA-6-713228)

## 使用系统日志预定义消息模板

系统日志消息具有包含报头和消息正文的标准结构。

本节介绍了思科 ISE-PIC 提供的预定义模板，包括根据消息源支持的报头以及受支持正文结构的内容详细信息。

此外，您可以使用系统中未预定义的源的自定义正文内容来创建自己的模板。本节还介绍了自定义模板的受支持结构。解析消息时，除系统中预定义的报头以外，您还可以配置要使用的单个自定义报头，并且可为消息正文配置多个自定义模板。有关自定义报头的详细信息，请参阅[自定义系统日志报头，第 50 页](#)。有关自定义正文的详细信息，请参阅[自定义系统日志消息正文，第 49 页](#)。



**注释** 大多数预定义模板都使用正则表达式，并且自定义模板也应使用正则表达式。

### 消息报头

有两种可由解析器识别的报头类型：适用于所有消息类型（新增和删除）和适用于所有客户端机器。这些报头如下：

- <171>Host message
- <171>Oct 10 15:14:08 Host message

收到后，系统将解析报头以获取主机名，它可以是 IP 地址、主机名或完整 FQDN。

此外，还可以自定义报头。要自定义报头，请参阅[自定义系统日志报头，第 50 页](#)。

## 系统日志 ASA VPN 预定义模板

ASA VPN 支持的系统日志消息格式和类型如下所述。

### 报头

如[使用系统日志预定义消息模板，第 54 页](#)中所述，对于所有客户端，解析器支持的报头都相同。

### 新映射正文消息

如下表所述，解析器可识别不同的 ASA VPN 正文消息。



正文消息	解析示例
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] 注释 从此消息类型解析的 IP 地址是私有 IP 地址，如消息中所示。
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <:::> assigned to session	[UserA,172.16.0.12] 注释 从此消息类型解析的 IP 地址是 IPv4 地址。

### 删除映射正文消息

解析器支持的 ASA VPN 删除映射消息如此部分所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

**[UserA,10.1.1.1]**

正文消息
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason

正文消息
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

## 系统日志 **Bluecat** 预定义模板

支持的系统日志消息格式和 **Bluecoat** 类型如下所述。

### 报头

如使用系统日志预定义消息模板，第 54 页中所述，对于所有客户端，解析器支持的报头都相同。

### 新映射正文消息

**Bluecat** 系统日志的新映射支持的消息如本部分所述。

收到正文消息后，如下解析正文以获取用户详细信息：

**[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]**

正文
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

### 删除映射消息

**Bluecat** 没有已知的删除映射消息。

## 系统日志 F5 VPN 预定义模板

F5 VPN 支持的系统日志消息格式和类型如下所述。

### 报头

如[使用系统日志预定义消息模板](#)，第 54 页中所述，对于所有客户端，解析器支持的报头都相同。

### 新映射正文消息

如下表所述，解析器可识别不同的 F5 VPN 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

**[user=UserA,ip=172.16.0.12]**

正文
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security [nnnnn]: [UserA @ vendor-abcr] User UserA login on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz \

### 删除映射消息

目前没有支持的 F5 VPN 删除消息。

## 系统日志 Infoblox 预定义模板

Infoblox 支持的系统日志消息格式和类型如下所述。

### 报头

如[使用系统日志预定义消息模板](#)，第 54 页中所述，对于所有客户端，解析器支持的报头都相同。

### 新映射正文消息

如下表所述，解析器可识别不同的 ASA VPN 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

**[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]**

正文消息
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:xx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xx:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xx:nn:nn) via eth1

### 删除映射消息

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

- 如果包含 MAC 地址：  
**[00:0c:29:a2:18:34,10.0.10.100]**
- 如果不包含 MAC 地址：  
**[10.0.10.100]**

正文消息
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCP_EXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCP_RELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

## 系统日志 Linux DHCPd3 预定义模板

Linux DHCPd3 支持的系统日志消息格式和类型如下所述。

### 报头

如[使用系统日志预定义消息模板](#)，第 54 页中所述，对于所有客户端，解析器支持的报头都相同。

### 新映射消息

如下表所述，解析器可识别不同的 Linux DHCPd3 正文消息。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

**[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]**

正文消息
Nov 11 23:37:32 dhcprsv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcprsv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

### 删除映射正文消息

解析器支持的 Linux DHCPd3 删除映射消息如此部分所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

**[00:0c:29:a2:18:34 ,10.0.10.100]**

正文消息
Nov 11 23:37:32 dhcprsv dhcpd: DHCP_EXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcprsv dhcpd: DHCP_RELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1

## 系统日志 MS DHCP 预定义模板

MS DHCP 支持的系统日志消息格式和类型如下所述。

### 报头

如[使用系统日志预定义消息模板，第 54 页](#)中所述，对于所有客户端，解析器支持的报头都相同。

### 新映射正文消息

解析器可识别不同的 MS DHCP 正文消息，如下表所述。

接收后，解析器会通过搜索逗号 (,) 来分隔数据，然后解析这些格式的消息，如以下示例所示：

**[macAddress=000C29912E5D,ip=10.0.10.123]**

正文消息
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,0x4D53465420352E30,MSFT,5.0

### 删除映射正文消息

解析器解析的 MS DHCP 支持的删除映射消息如此部分所述。

接收后，解析器会通过搜索逗号 (,) 来分隔数据，然后解析这些格式的消息，如以下示例所示：

**[macAddress=000C29912E5D,ip=10.0.10.123]**

正文消息
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\0,,,,,,,,,0

## 系统日志 SafeConnect NAC 预定义模板

SafeConnect NAC 支持的系统日志消息格式和类型如下所述。

### 报头

如[使用系统日志预定义消息模板，第 54 页](#)中所述，对于所有客户端，解析器支持的报头都相同。

### 新映射正文消息

解析器可识别不同的 SafeConnect NAC 正文消息，如下表所述。

收到正文后，系统按照如下所述解析正文以获取用户详细信息：

**[user=galindkli,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]**

正文消息

Apr 10 09:33:58 nac Safe\*Connect:  
authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

删除映射消息

目前没有 Safe Connect 支持的删除消息。

## 系统日志 **Aerohive** 预定义模板

Aerohive 支持的系统日志消息格式和类型如下所述。

报头

如[使用系统日志预定义消息模板](#)，第 54 页中所述，对于所有客户端，解析器支持的报头都相同。

新映射正文消息

如下表所述，解析器可识别不同的 Aerohive 正文消息。

从正文解析的详细信息包括用户名和 IP 地址。用于解析的正则表达式如以下示例所示：

- New mapping—auth\  
:
- IP—ip ([A-F0-9a-f:.]+)
- User name—UserA ([a-zA-Z0-9\\_]+)

收到正文消息后，如下解析正文以获取用户详细信息：

**[UserA,10.5.50.52]**

正文消息

2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

删除映射消息

系统当前不支持从 Aerohive 删除映射消息。

## 系统日志 **Blue Coat** 预定义模板 - 主代理、代理 **SG**、**Squid Web** 代理

系统支持 Blue Coat 的以下消息类型：

- BlueCoat 主代理
- BlueCoat 代理 SG
- BlueCoat Squid Web 代理

支持的系统日志消息格式和 Bluecoat 消息类型如下所述。

## 报头

如[使用系统日志预定义消息模板](#)，第 54 页中所述，对于所有客户端，解析器支持的报头都相同。

## 新映射正文消息

解析器可识别不同的 Blue Coat 正文消息，如下表所述。

收到正文消息后，如下解析正文以获取用户详细信息：

**[UserA,192.168.10.24]**

正文消息（此示例摘自 BlueCoat 代理 SG 消息）
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

下表介绍了每个客户端用于新映射消息的不同正则表达式结构。

客户端	正则表达式
BlueCoat 主代理	新映射 (TCP_HIT TCP_MEM){1} IP \((?:[0-9]{1,3}){3}(?:[0-9]{1,4} (?:[0-9]{1,2}){1,7}[0-9]{1,4})\)\$ 用户名 \s-\s([a-zA-Z0-9_]+)\s-\s
BlueCoat 代理 SG	新映射 (\sPROXIED){1} IP \((?:[0-9]{1,3}){3}(?:[0-9]{1,4} (?:[0-9]{1,2}){1,7}[0-9]{1,4})\)\$ 用户名 \s[0-9]{1,3}\s[0-9]{1,3}\s[0-9]{1,3}\s[0-9]{1,3}\s([a-zA-Z0-9_]+)\s-
BlueCoat Squid Web 代理	新映射 (TCP_HIT TCP_MEM){1} IP \((?:[0-9]{1,3}){3}(?:[0-9]{1,4} (?:[0-9]{1,2}){1,7}[0-9]{1,4})\)\$TCP 用户名 \s([a-zA-Z0-9_+])\s-

### 删除映射消息

Blue Coat 客户端支持删除映射消息，但当前没有提供相关示例。

下表介绍了每个客户端用于删除映射消息的不同的已知正则表达式结构示例。

客户端	正则表达式
BlueCoat 主代理	<code>(TCP_MISS TCP_NC_MISS){1}</code>
BlueCoat 代理 SG	当前无可用示例。
BlueCoat Squid Web 代理	<code>(TCP_MISS TCP_NC_MISS){1}</code>

## 系统日志 ISE 和 ACS 预定义模板

侦听 ISE 或 ACS 客户端时，解析器将接收以下消息类型：

- 通过身份验证：当用户经 ISE 或 ACS 进行身份验证后，通过身份验证消息将发出以通知身份验证已成功，并包含用户详细信息。系统将解析此消息，并保存此消息中的用户详细信息和会话 ID。
- 记帐启动和记帐更新消息（新映射）：从 ISE 或 ACS 接收的记帐启动或记帐更新消息将进行解析，并包含在通过身份验证消息中保存的用户详细信息和会话 ID，然后映射用户。
- 记帐停止（删除映射）：从 ISE 或 ACS 接收后，用户应设将从系统中删除。

ISE 和 ACS 支持的系统日志消息格式与类型如下所述。

### 通过身份验证消息

通过身份验证类型支持以下消息。

- 标题

```
<181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
```

例如：<181>Sep 13 10:51:41 Positron CISE\_PassiveID 0000005255 1 0 message

- 正文

```
Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE
Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12,
DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius,
RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA,
NAS-IP-Address=1.1.1.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5
```

- 解析示例

仅解析用户名和会话 ID。

```
[UserA,5]
```



## 记帐启动/更新（新映射）消息

新映射支持以下消息。

- 标题

```
<181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
```

例如: <181>Sep 13 10:51:41 Positron CISE\_PassiveID 0000005255 1 0 message

- 正文

```
CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE
Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP
Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice,
User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90,
Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5
```

- 解析示例

解析的详细信息包括用户名、成帧的 IP 地址以及 MAC 地址（如果消息中包括）。

```
[UserA,10.0.0.16]
```

## 删除映射消息

删除映射支持以下消息。

- 标题

```
<181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
```

例如: <181>Sep 13 10:51:41 Positron CISE\_PassiveID 0000005255 1 0 message

- 正文

```
2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting
stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13,
NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1,
Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop,
Acct-Session-Id=104, cisco-av-pair=audit-session-id=5
```

- 解析示例

解析的详细信息包括用户名、成帧的 IP 地址以及 MAC 地址（如果消息中包括）。

```
[UserA,10.0.0.16]
```

## 系统日志 Lucent QIP 预定义模板

Lucent QIP 支持的系统日志消息格式和类型如下所述。

### 报头

如[使用系统日志预定义消息模板](#)，第 54 页中所述，对于所有客户端，解析器支持的报头都相同。

### 新映射正文消息

如下表所述，解析器可识别不同的 Lucent QIP 正文消息。

这些消息的正则表达式结构如下：

**DHCP\_GrantLease|DHCP\_RenewLease**

收到正文消息后，如下解析正文以获取用户详细信息：

**[00:0C:29:91:2E:5D,10.0.0.11]**

正文消息
DHCP:subtype=0:Single:\$IGNORE_N\$ DHCP_GrantLease: Host=\$HOSTNAME\$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:\$IGNORE_N\$ DHCP_RenewLease: Host=\$HOSTNAME\$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

### 删除映射正文消息

这些消息的正则表达式结构如下所示：

**删除租约|DHCP 自动释放：**

收到正文消息后，如下解析正文以获取用户详细信息：

**[10.0.0.11]**

正文消息
DHCP:subtype=0:Single:\$IGNORE_N\$ Delete Lease: IP=10.0.0.11 \$IGNORE_N\$
DHCP:subtype=0:Single:\$IGNORE_N\$ DHCP Auto Release: IP=10.0.0.11 \$IGNORE_N\$

## 过滤被动身份服务

您可以根据用户名称或 IP 地址过滤某些用户。例如，如果 IT 服务中的管理员登录到终端以帮助该终端的常规用户，则可以过滤掉管理员活动，从而在“实时会话”中不显示管理员活动，而是仅显示该终端的常规用户。实时会话显示映射过滤器未过滤掉的被动身份服务组件。您可以按照需要添加很多过滤器。“OR”逻辑运算符适用于过滤器之间。如果在单个过滤器中同时指定两个字段，则在这两个字段之间使用“AND”逻辑运算符。

**步骤 1** 选择提供程序 (Providers) > 映射过滤器 (Mapping Filters)。

**步骤 2** 单击添加 (Add)，输入您想要过滤的用户的用户名和 Ip 地址，然后单击提交 (Submit)。

## 终端探测器

除可以配置的自定义提供程序以外，安装时默认在 ISE-PIC 中启用终端探测器，并且始终在后台运行。终端探测器会定期检查每个特定用户是否仍已登录到系统。



**注释** 为了确保终端在后台运行，您必须首先配置初始 Active Directory 加入点，并确保选择存储凭证。有关配置终端探测器的详细信息，请参阅[使用终端探测器](#)，第 66 页。

要手动检查终端状态，请转至实时会话 (Live Sessions)，从操作 (Actions) 列单击显示操作 (Show Actions)，然后选择检查当前用户 (Check current user)，如下图所示。

图 4: 检查当前用户

Session Status	Action	Endpoint ID	Identity
enticated	Show Actions		Identity
enticated	Show Actions		Administra
enticated	Show Actions	10.56.53.179	Administra
enticated	Show Actions	10.56.63.172	Administra
enticated	Show Actions	10.56.53.204	Administra
enticated	Show Actions	10.56.53.197	Administra

有关终端用户状态以及手动运行检查的详细信息，请参阅[实时会话](#)，第 137 页。

当终端探测器识别用户已连接时，如果自上次为特定终端更新会话已经过 4 小时，则它将检查该用户是否仍已登录并收集以下数据：

- MAC 地址
- 操作系统版本

根据此检查，探测器将执行以下操作：

- 当用户仍处于登录状态时，探测器将使用“活动用户” (Active User) 状态更新思科 ISE-PIC。
- 当用户已注销时，会话状态更新为“已终止”，15 分钟后，将从会话目录中删除用户。
- 当无法联系用户时（例如，当防火墙阻止联系或者终端已关闭时），状态更新为“无法访问”，并且用户策略将确定如何处理用户会话。终端将保持处于会话目录中。

## 使用终端探测器

### 开始之前

安装 ISE-PIC 后，默认情况下会启用终端探测器。要启用和禁用探测器，请首先确保您已配置下列各项：

- 终端必须具有与端口 445 的网络连接。
- 从 ISE-PIC 配置初始 Active Directory 加入点。有关加入点的详细信息，请参阅 [Active Directory 作为探测器和提供程序](#)，第 17 页。



**注** 为了确保终端在后台运行，您必须首先配置初始 Active Directory 加入点，通过它可使终端探测器即使在 Active Directory 未完全配置时也能够运行。

---

**步骤 1** 选择提供程序 (Providers) > 终端探测器 (Endpoint Probes)。

**步骤 2** 选择已启用 (Enabled) 或已禁用 (Disabled)。

屏幕不会更改。但是，探测器根据选择进行启用或禁用，如果已启用，则此时正在后台运行并收集数据。

---



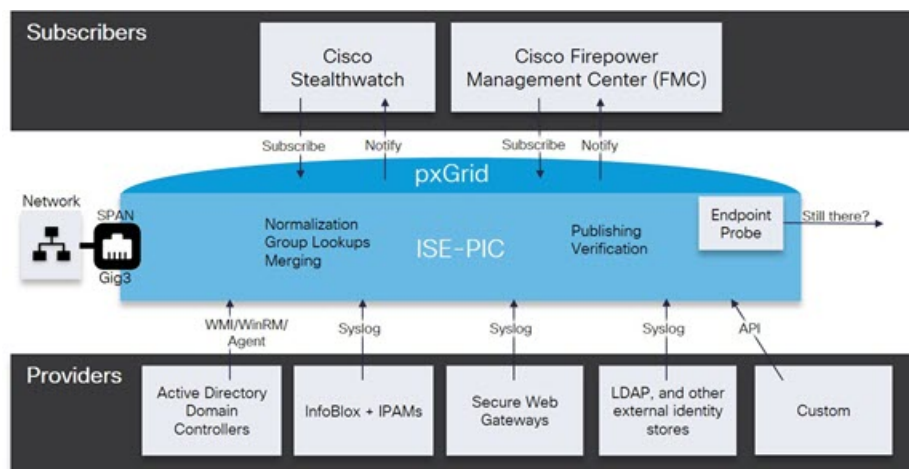
## 第 5 章

# 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 5: 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 68 页。

3. [启用用户，第 70 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 70 页](#)。



注释 您可能在用户 (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 68 页](#)
- [启用用户，第 70 页](#)
- [从实时日志查看用户事件，第 70 页](#)
- [配置用户设置，第 70 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 70 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)。





## 第 6 章

# 思科中的证书管理 ISE-PIC

证书是标识个人、服务器、公司或其他实体并将实体与公共密钥关联的电子文档。公共密钥基础设施 (PKI) 是一种加密技术，用于实现安全通信和验证使用数字签名的用户的身份。证书用于在网络中提供安全访问。证书可以自签名，也可以由外部证书颁发机构 (CA) 进行数字签名。自签证书由证书创建者签名。CA 签名的数字证书符合行业标准且更安全。ISE-PIC 可以作为 pxGrid 的外部 CA，为 pxGrid 用户数字签名 pxGrid 证书。

思科 ISE-PIC 使用证书进行节点间通信（每个节点将其证书提供给另一节点以相互通信）以及与 pxGrid 的通信（ISE-PIC 和 pxGrid 相互提供证书）。对于其中每个用途，每个节点可以生成一个证书。证书会向 pxGrid 标识思科 ISE 节点身份，并确保 pxGrid 与思科 ISE 节点之间的安全通信。

安装时，ISE-PIC 将为每个 ISE-PIC 节点自动生成自签证书（在安装期间，系统将提示管理员接受从主节点自动为辅助节点创建的证书），并为 pxGrid 服务自动生成由主 ISE-PIC 节点数字签名的证书。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。ISE-PIC 中提供证书 (Certificate) 菜单，从中可查看证书、生成其他 ISE-PIC 证书并执行某些高级任务。



注释

管理员能够使用企业证书，ISE-PIC 在默认情况下设计为使用内部颁发机构为用户颁发 pxGrid 证书。

- [思科 ISE-PIC 中的证书匹配，第 71 页](#)
- [通配符证书，第 72 页](#)
- [证书层次结构 ISE-PIC，第 74 页](#)
- [系统证书，第 75 页](#)
- [受信任证书库，第 79 页](#)
- [证书签名请求，第 85 页](#)
- [思科 ISE CA 服务，第 93 页](#)
- [OCSP 服务，第 101 页](#)

## 思科 ISE-PIC 中的证书匹配

设置部署中的思科 ISE-PIC 节点后，节点将互相通信。系统将检查每个思科 ISE-PIC 节点的 FQDN，以确保其匹配（例如 `ise1.cisco.com` 和 `ise2.cisco.com`，如果使用通配符证书，则为 `*.cisco.com`）。此

外，当外部机器向思科 ISE-PIC 服务器提供证书时，将根据思科 ISE-PIC 服务器中的证书对提供用于身份验证的外部证书进行检查（或匹配）。如果两个证书匹配，则身份验证成功。

思科 ISE-PIC 按以下方式检查匹配的主题名称：

1. 思科 ISE-PIC 查看证书的主题别名扩展。如果 SAN 包含一个或多个 DNS 名称，则其中必须有一个 DNS 名称与思科 ISE 节点的 FQDN 相匹配。如果使用通配符证书，则通配符域名必须与思科 ISE 节点的 FQDN 中的域匹配。
2. 如果使用者备选名称中不包含 DNS 名称、或使用者备选名称完全缺失，则证书使用者 (Subject) 字段中的公用名称或使用者 (Subject) 字段中的通配符域必须与节点的 FQDN 匹配。
3. 如果未找到匹配项，则会拒绝该证书。

## 通配符证书

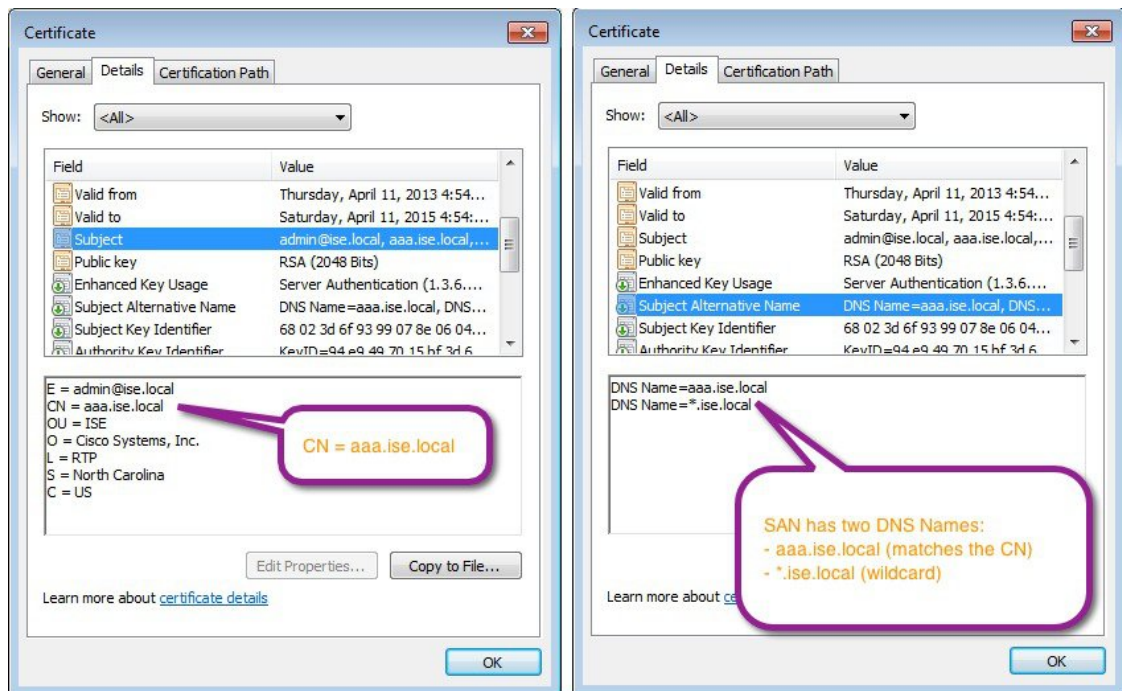
通配符证书使用通配符表示法（在域名前使用一个星号和句点），并且该证书可以在组织中的多个主机之间共享。例如，Certificate Subject 中的 CN 值可以是一个通用主机名（例如 aaa.ise.local），SAN 字段会包含相同的通用主机名和通配符表示法（例如 DNS.1=aaa.ise.local 和 DNS.2=\*.ise.local）。

如果将某个通配符证书配置为使用 \*.ise.local，可以使用同一证书来保护 DNS 名称以 “.ise.local” 结尾的任何其他主机，例如：psn.ise.local。

通配符证书用与普通证书一样的方式保护通信安全，并且使用相同的验证方法处理请求。

下图是用于保护 Web 站点的一个通配符证书的示例。

图 6: 通配符证书示例



360 173

通过在 SAN 字段中使用星号 (\*), 可以在所有节点上共享单个证书 (如果已安装多个节点), 并有助于防止证书名称不匹配警告。但是, 使用通配符证书的安全性要比向每个思科 ISE 节点分配唯一服务器证书的安全性低。



注释 FQDN 的一些示例取自完整的思科 ISE 安装, 因此可能不同于与 ISE-PIC 安装相关的地址。

## 使用通配符证书的优势

- 节省成本: 由第三方 CA 签名的证书非常昂贵, 尤其是随着服务器数量的增加。在思科 ISE 部署中, 可以在多个节点上使用通配符证书。
- 操作效率: 通配符证书允许所有 PSN 为 EAP 和 Web 服务共用同一证书。除了能显著节约成本之外, 由于可以只创建证书一次, 然后就可以将其应用于所有 PSN, 所以还能简化证书管理。
- 降低身份验证错误: 通配符证书可以解决 Apple iOS 设备常见的证书问题, 即客户端将受信任证书存储于配置文件中, 而不遵循信任签名 root 的 iOS Keychain。当 iOS 客户端首次与 PSN 通信时, 它不会明确信任 PSN 证书, 即使受信任 CA 已为该证书签名。使用通配符证书, 所有 PSN 上证书都将一样, 所以用户只须接受一次该证书, 接下来对不同 PSN 的身份验证就会继续进行, 而不会报错或出现提示。
- 简化请求者配置: 例如, 启用 PEAP-MSCHAPv2 和受信任服务器证书的 Microsoft Windows 请求者要求您指定要信任的各个服务器证书, 否则当客户端使用不同的 PSN 进行连接时, 系统会提示用户是否信任各个 PSN 证书。使用通配符证书, 可以信任一个统一的服务器证书, 而不需从每个 PSN 逐一信任各个证书。
- 通配符证书可以减少提示, 增强无缝连接, 从而提高用户体验。

## 使用通配符证书的缺点

以下是与使用通配符证书相关的一些安全问题:

- 失去可审核性和不可否认性。
- 提高了专用密钥的泄露风险。
- 不常见或管理员不了解。

通常认为通配符证书没有每个 ISE 节点均使用唯一的服务器证书那么安全。但是, 成本和运营因素比安全风险更重要。

思科自适应安全设备等安全设备也支持通配符证书。

部署通配符证书时, 一定要谨慎。例如, 如果您使用 \*.company.local 创建一个证书, 而某个攻击者能够发现其专用密钥, 则该攻击者就可以监听 company.local 域中的任意服务器。因此, 最好给域空间分区以避免这类威胁。

要解决可能出现的这个问题和限制使用范围，也可以使用通配符证书保护您的组织的具体子域。在您想要指定通配符的通用名称子域部分添加一个星号 (\*)。

例如，如果您为 \*.ise.company.local 配置通配符证书，则可以将该证书用于保护 DNS 名称以 “.ise.company.local” 结尾的任意主机，例如：

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

## 通配符证书兼容性

通常在创建通配符证书时，会将通配符列为证书使用者的通用名称。思科 ISE 支持这种类型的结构。但并不是所有的终端请求者都支持在证书使用者中使用通配符字符。

通过测试的所有 Microsoft 本地请求者（包括现在已经停产的 Windows Mobile）不支持在证书使用者中使用通配符字符。

您可以使用另一个请求者，例如思科 AnyConnect 网络访问管理器，它可能允许在“主题” (Subject) 字段中使用通配符字符。

您还可以使用特殊通配符证书（例如设计为与不兼容设备配合使用的 DigiCert 的 Wildcard Plus），方法是在证书的 Subject Alternative Name 中包含特定子域。

尽管 Microsoft 请求者限制似乎禁止使用通配符证书，但仍有其他方法创建通配符证书，允许它与通过测试的所有设备配合使用，从而实现安全访问，包括 Microsoft 本地请求者。

为此，您必须在“主题备用名称” (Subject Alternative Name) 字段中使用通配符字符，而不是在“主题” (Subject) 中使用通配符字符。“主题备用名称” (Subject Alternative Name) 字段保留专为检查域名而设计的扩展名 (DNS 名称)。有关详细信息，请参阅 RFC 6125 和 2128。

## 证书层次结构 ISE-PIC

在 ISE-PIC 中，请以查看所有证书的证书层次结构或证书信任链。证书层级包括证书、所有中间 CA 证书和根证书。例如，当选择从 ISE-PIC 查看系统证书时，会显示相应系统证书的详细信息。证书层级显示在该证书的顶部。单击层次结构中的证书可查看其详细信息。自签名证书没有任何层次结构或信任链。

在证书列表窗口的状态 (Status) 列中，您将会看到以下图标之一：

- 绿色图标：表示有效证书（有效信任链）。
- 红色图标：表示存在错误（例如，信任证书缺失或过期）。
- 黄色图标：警告证书即将到期并提示续约。

# 系统证书

思科 ISE-PIC 系统证书是向部署中的其他节点和客户端应用标识思科 ISE-PIC 节点身份的服务器证书。要访问系统证书，选择**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 系统证书 (System Certificates)**。系统证书的用途如下：

- 用于思科 ISE-PIC 部署中的节点间通信。选中这些证书的**使用情况 (Usage)**区域中的**管理 (Admin)**复选框。
- 用于与 pxGrid 控制器通信。选中这些证书的**使用情况 (Usage)**区域中的**pxGrid**复选框。

在思科 ISE-PIC 部署中的每个节点上安装有效的系统证书。默认情况下，在安装期间，将在思科 ISE-PIC 节点上创建两个自签证书和一个由内部思科 ISE CA 签名的证书：

- 指定用于用于管理员和 pxGrid 的自签名服务器证书（密钥长度为 2048，有效期为一年）。
- 可用于确保与 SAML 身份提供程序之间安全通信的自签名 SAML 服务器证书（密钥长度为 2048，有效期为一年）。
- 可用于确保与 pxGrid 客户端之间安全通信的内部思科 ISE CA 签名的服务器证书（密钥长度为 4096，有效期为一年）。

设置部署并注册辅助节点时，指定用于 pxGrid 控制器的证书将自动替换为由主要节点的 CA 签名的证书。因此，所有 pxGrid 证书将属于同一 PKI 信任层次结构。

有关对应于您的版本的支持密钥和密码信息，请参阅适当版本的《[思科身份识别服务引擎网络组件兼容性](#)》指南。

为了提高安全性，建议您使用 CA 签名的证书替换自签证书。要获取 CA 签名的证书，您必须：

1. [创建证书签名请求并将其提交给证书颁发机构，第 86 页](#)
2. [将根证书导入受信任证书库，第 83 页](#)
3. [将 CA 签名的证书绑定到证书签名请求，第 86 页](#)

## 查看系统证书

系统证书 (System Certificate) 窗口列出添加至思科 ISE-PIC 的所有系统证书。

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择 **证书 (Certificates) > 系统证书 (System Certificates)**。

**步骤 2** 系统证书 (System Certificates) 窗口中会显示以下列：

- **友好名称 (Friendly Name)**: 证书的名称。
- **使用情况 (Usage)**: 使用此证书的服务。
- **门户组标记 (Group Tag)**: 仅适用于指定用于门户用途的证书。此字段指定必须将哪个证书用于门户。

- 颁发给 (**Issued To**): 证书使用者的通用名称。
- 颁发者 (**Issued By**): 证书颁发者的通用名称。
- 生效日期 (**Valid From**): 创建证书的日期, 也称为开始时间证书属性。
- 到期日期 (**Expiration Date**): 证书的到期日期, 也称为“截止时间”证书属性。以下图标显示在到期日期旁边:
  - 绿色图标: 距到期还有 90 天以上。
  - 蓝色图标: 距到期还有 90 天或更短。
  - 黄色图标: 距到期还有 60 天或更短。
  - 橙色图标: 距到期还有 30 天或更短。
  - 红色图标: 已到期。

## 导入系统证书

您可以从管理门户为任意思科 ISE-PIC 节点导入系统证书。



**注释** 在主 PAN 节点上更改管理员角色证书的证书将在所有其他节点上重新启动服务。主 PAN 重启完成后, 系统会每次重新启动一个节点。

### 开始之前

- 确保您在运行客户端浏览器的系统上拥有系统证书和专用密钥文件。
- 如果您导入的系统证书由外部 CA 签名, 则将相关根 CA 或中间 CA 证书导入受信任证书存储区 (证书 (**Certificates**) > 受信任的证书 (**Trusted Certificates**))。
- 如果导入的系统证书中包含 CA 标志设置为 true 的基本约束扩展, 请确保有密钥用法扩展并且设置了 keyEncipherment 位或 keyAgreement 位。

**步骤 1** 选择证书 (**Certificates**) > 系统证书 (**System Certificates**)。

**步骤 2** 单击导入 (**Import**)。

将显示导入服务器证书 (**Import Server Certificate**) 窗口。

**步骤 3** 输入您要导入的证书的值。

**步骤 4** 单击提交 (**Submit**)。

## 生成自签证书

通过生成自签证书添加新的本地证书。思科建议仅采用自签证书，以满足内部测试和评估需求。如果计划在生产环境中部署思科 ISE-PIC，尽可能使用 CA 签名证书，确保生产网络中更统一地接受。



**注释** 如果您使用自签名证书并且必须更改思科 ISE-PIC 节点的主机名，请登录思科 ISE-PIC 节点的，删除采用旧主机名的自签证书，然后生成新的自签证书。否则，思科 ISE-PIC 会继续使用采用旧主机名的自签证书。

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择 **证书 (Certificates) > 系统证书 (System Certificates)**。

**步骤 2** 单击**生成自签证书 (Generate Self Signed Certificate)**并在显示的窗口中输入详细信息。

**步骤 3** 选中**允许通配符证书 (Allow Wildcard Certificates)**复选框以生成自签通配符证书（在主题的任何公用名中或主题备用名的 DNS 名称中包含星号 (\*)）。例如，分配给 SAN 的 DNS 名称可以是 \*.amer.cisco.com。

**步骤 4** 根据想要对其使用此证书的服务，选中 **Usage** 区域的复选框。

**步骤 5** 单击**提交 (Submit)**生成证书。

要从 CLI 重新启动辅助节点，则按给定顺序输入以下命令：

- a) **application stop ise**
- b) **application start ise**

## 编辑系统证书

使用此窗口来编辑系统证书，续订自签证书。当编辑通配符证书时，更改将被复制到部署中的所有节点上。当删除通配符证书时，此通配符证书将从部署中的所有节点删除。

**步骤 1** 选择 **证书 (Certificates) > 系统证书 (System Certificates)**。

**步骤 2** 选中要编辑的证书旁边的复选框，然后单击**编辑 (Edit)**。

**步骤 3** 要续约自签证书，请选中**续约期限 (Renewal Period)**复选框，然后输入以天、周、月或年为期单位的到期生存时间 (TTL)。从下拉列表中选择所需的值。

**步骤 4** 单击**保存 (Save)**。

如果选中**管理 (Admin)**复选框，则思科 ISE-PIC 节点上的应用服务器将重新启动。



**注释** 使用 Chrome 65 及更高版本启动思科 ISE 可能会导致 BYOD 门户或访客门户无法在浏览器中启动，即使 URL 已成功重定向也是如此。这是因 Google 引入的新安全功能所致，此功能要求所有证书具有“主题备用名称” (Subject Alternative Name) 字段。对于思科 ISE 2.4 及更高版本，必须填充“主题备用名称” (Subject Alternative Name) 字段。

要使用 Chrome 65 及更高版本启动，请执行以下步骤：

1. 通过填充“主题备用名称” (Subject Alternative Name) 字段，从思科 ISE GUI 生成新的自签证书。必须填充 DNS 和 IP 地址。
2. 思科 ISE 服务将重新启动。
3. 在 Chrome 浏览器中重定向门户。
4. 在浏览器中，“查看证书” (View Certificate) > “详细信息” (Details) > 通过选择 base-64 编码来复制证书。
5. 将证书安装到受信任路径。
6. 关闭 Chrome 浏览器，然后尝试重定向门户。



**注释** 在为操作系统 Win RS4 或 RS5 中的浏览器 Firefox 64 及更高版本配置无线 BYOD 设置时，可能无法添加证书例外。如果是全新安装 Firefox 64 及更高版本，此行为是预计行为，如果是从先前版本升级到 Firefox 64 及更高版本，则不会出现此行为。通过以下步骤，可以在此情况下添加证书例外：

1. 针对 BYOD 流程单或双 PEAP 或 TLS 进行配置。
2. 通过 Windows ALL 选项配置 CP 策略。
3. 在最终客户端 Windows RS4 或 Windows RS5 中连接 Dot1.x 或 MAB SSID。
4. 在 FF64 浏览器中键入 1.1.1.1 以重定向至访客或 BYOD 门户。
5. 单击添加例外 (Add Exception) > 无法添加证书 (Unable to add certificate)，然后继续执行流程。

对此的解决方法是，手动为 Firefox 64 添加证书。在 Firefox 64 浏览器中，选择选项 (Options) > 隐私和设置 (Privacy & Settings) > 查看证书 (View Certificates) > 服务器 (Servers) > 添加例外 (Add Exception)。

## 删除系统证书

您可以删除不再使用的系统证书。

尽管可以一次从系统证书存储区中删除多个证书，但必须至少具有一个可用于管理员身份验证的证书。此外，无法删除用于管理员或 pxGrid 控制器的任何证书。但是，在禁用服务时可以删除 pxGrid 证书。

如果您选择删除通配符证书，则系统会从部署中的所有思科 ISE 节点删除该证书。



**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择证书 (Certificates) > 系统证书 (System Certificates)。

**步骤 2** 选中想要删除的证书旁边的复选框，然后单击删除 (Delete)。

系统会显示一条警告消息。

**步骤 3** 单击是 (Yes)，删除证书。

## 导出系统证书

您可以导出系统证书或某个证书及其关联的专用密钥。如果您导出证书及其专用密钥以进行备份，如有必要，您以后也可以重新导入此证书与专用密钥。

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择证书 (Certificates) > 系统证书 (System Certificates)。。

**步骤 2** 选中要导出的证书旁边的复选框，然后单击导出 (Export)。

**步骤 3** 选择是仅导出证书，还是导出证书及其关联的专用密钥。

**提示** 由于可能会暴露专用密钥值，我们不建议导出与证书关联的专用密钥。如果您必须导出专用密钥（例如，导出要导入其他思科 ISE 节点以用于节点间通信的通配符系统证书时），请指定专用密钥加密密码。在将此证书导入另一思科 ISE-PIC 节点时，必须指定此密码以解密专用密钥。

**步骤 4** 如果您已选择导出专用密钥，请输入此密码。此密码至少必须包含 8 个字符。

**步骤 5** 单击导出 (Export) 以将证书保存至运行客户端浏览器的文件系统。

如果仅导出证书，证书将以 PEM 的格式进行存储。如果同时导出证书和专用密钥，则证书会导出为 .zip 文件，其中包含 PEM 格式的证书和已加密的专用密钥文件。

## 受信任证书库

受信任证书库包括用于信任和简单证书注册协议 (SCEP) 的 X.509 证书。

X.509 证书仅从特定日期开始有效。当受信任证书到期时，取决于证书的思科 ISE 功能会受到影响。当距离到期日还有 90 天时，思科 ISE 会通知您系统证书即将到期。系统以多种方式显示此通知：

- 彩色到期状态图标显示在系统证书 (System Certificates) 窗口中。
- 思科 ISE 系统诊断报告中出现的过期消息 (操作 (Operations) > 报告 (Reports) > 报告 (Reports) > 诊断 (Diagnostics) > 系统诊断 (System Diagnostic))。
- 在距离到期日 90 天、60 天、30 天时生成到期警报，而在最后 30 天内，每天生成一次警报。

如果即将到期的证书为自签证书，您可以编辑证书，延长到期日。对于 CA 签名的证书，要留出足够的时间，从 CA 获取替换证书。

思科 ISE 将受信任证书用于以下用途：

- 验证由终端和访问 ISE-PIC 的思科 ISE 管理员（使用基于证书的管理人员身份验证）用于身份验证的客户端证书。
- 确保部署中思科 ISE-PIC 节点之间的安全通信。受信任证书库必须包含与部署中每个节点上的系统证书建立信任所需的 CA 证书链。
  - 如果将自签证书用于系统证书，则各个节点的自签证书必须放在 PAN 的受信任证书库中。
  - 如果将自签证书用于系统证书，则 CA 根证书以及信任链中的任何中间证书都必须放在 PAN 的受信任证书库中。



注释

- 导入到思科 ISE 的 X.509 证书必须为 PEM 格式或可辨别编码规则格式。可以根据特定限制，导入包含证书链的文件，也就是系统证书以及签名的受信任证书的序列。
- 在向访客门户分配公共通配符证书并随根 CA 证书一起导入子 CA 时，直到思科 ISE 服务重新启动后才会发送证书链。

在安装时，将使用自动生成的受信任证书填充受信任证书库。根证书（思科根 CA）给生产（思科 CA 生产）证书签名。

## 受信任证书命名限制

CTL 中的受信任证书可以包含名称限制扩展。此扩展为证书链中后续证书的所有主题名称和主题替代名称的值定义命名空间。思科 ISE 不会检查根证书中指定的限制。

思科 ISE 支持以下名称限制：

- 目录名称
  - 目录名称限制应该是主题或主题备用名称字段中的目录名称前缀。例如：
    - 正确的主题前缀：
      - CA 证书名称限制：Permitted: O=Cisco
      - 客户端证书主题：O=Cisco,CN=Salomon
    - 不正确的主题前缀：
      - CA 证书名称限制：Permitted: O=Cisco
      - 客户端证书主题：CN=Salomon,O=Cisco
- DNS
- 电子邮箱
- URI（URI 限制必须以一个 URI 前缀开头，例如 http://、https://、ftp:// 或 ldap://）。

思科 ISE 不支持以下名称限制:

- IP 地址
- OtherName

当受信任证书包含不支持的限制并且验证的证书不包含相应字段时, 思科 ISE 会拒绝此证书, 因为它无法验证不支持的限制。

以下是受信任证书中名称限制的一个示例:

```
X509v3 Name Constraints: critical
  Permitted:
    othername:<unsupported>
    email:.abcde.at
    email:.abcde.be
    email:.abcde.bg
    email:.abcde.by
    DNS:.dir
    DirName: DC = dir, DC = emea
    DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
    DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
    DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
    DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100
    URI:.dir
    IP:172.23.0.171/255.255.255.255
  Excluded:
    DNS:.dir
    URI:.dir
```

以下是与以上定义匹配的一个可接受客户端证书主题:

```
Subject: DC=dir, DC=emea, OU+=DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

## 查看受信任的证书

受信任证书 (**Trusted Certificates**) 窗口列出所有已添加到思科 ISE-PIC 的受信任证书。

**步骤 1** 要查看所有证书, 选择选择证书 (**Certificates**) > 受信任证书 (**Trusted Certificates**)。系统将显示受信任证书窗口, 其中列出了所有受信任的证书。

**步骤 2** 选中受信任证书的复选框, 然后单击编辑 (**Edit**)、查看 (**View**)、导出 (**Export**) 或删除 (**Delete**) 以执行所需任务。

## 更改受信任证书库中的证书状态

必须启用证书状态, 思科 ISE-PIC 才能使用此证书建立信任。将证书导入受信任证书库时, 将自动启用此证书。

**步骤 1** 在 ISE-PIC GUI 中, 单击菜单图标 (☰), 然后选择 证书 (**Certificates**) > 受信任证书 (**Trusted Certificates**)。

**步骤 2** 选中想要启用或禁用的证书旁边的复选框，然后单击**编辑 (Edit)**。

**步骤 3** 从**状态 (Status)** 下拉列表中选择状态。

**步骤 4** 单击**保存 (Save)**。

---

## 在受信任的证书库中添加证书

您可以通过**受信任的证书 (Trusted Certificate)** 存储器窗口将 CA 证书添加到思科 ISE-PIC。

### 开始之前

- 您要添加的证书必须位于运行您的浏览器的计算机文件系统中。证书必须是 PEM 或 DER 格式。
- 要将证书用于管理员或 EAP 身份验证，请在证书中定义基本限制并将 CA 标志设置为 true。

---

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (≡)，然后选择 **证书 (Certificates) > 受信任证书 (Trusted Certificates)**。

**步骤 2** 单击**导入 (Import)**。

**步骤 3** 如有必要，配置这些字段值。

要使用证书链中的任何从属 CA 证书用于 EAP 身份验证或基于证书的**管理员身份验证**，请在向证书链导入所有证书直至根 CA 为止时，选中**信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)** 复选框。您可以导入具有同一证书持有者名称的多个 CA 证书。对于基于证书的**管理员身份验证**，在添加受信任的证书时，请选中**信任基于证书的**管理员身份验证 (Trust for certificate based admin authentication)**** 复选框。对于受信任存储区中的证书，如果存储区中有其他证书具有同一证书持有者，并且**信任基于证书的**管理员身份验证 (Trust for certificate based admin authentication)**** 复选框处于启用状态，则无法选中此证书的**信任基于证书的**管理员身份验证 (Trust for certificate based admin authentication)**** 复选框。

将身份验证类型从基于密码的身份验证改为基于证书的身份验证时，思科 ISE-PIC 将重新启动您的部署中每个节点上的应用服务器，从 PAN 上的应用服务器开始。

---

## 编辑受信任证书

在将证书添加到受信任证书库之后，可以通过使用**编辑 (Edit)** 选项进行进一步编辑。

---

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (≡)，然后选择 **证书 (Certificates) > 受信任证书 (Trusted Certificates)**。

**步骤 2** 选中要编辑的证书旁边的复选框，然后单击**编辑 (Edit)**。

**步骤 3** (可选) 在**友好名称 (Friendly Name)** 字段中，输入证书名称。如果没有指定友好的名称，系统会按以下格式生成一个默认名称：

```
common-name#issuer#nnnnn
```

**步骤 4** 通过在**受信任 (Trusted For)** 区域选中必要的复选框来定义证书的用途。

步骤 5（可选）在说明 (Description) 字段中输入证书的说明。

步骤 6 单击保存 (Save)。

---

## 删除受信任证书

可以删除不再需要的受信任证书。但是，不得删除思科 ISE-PIC 内部 CA 证书。思科 ISE-PIC 内部 CA 证书只能在替换整个部署的思科 ISE-PIC 根证书链时删除。

步骤 1 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择 证书 (Certificates) > 受信任证书 (Trusted Certificates)。

步骤 2 选中想要删除的证书旁边的复选框，然后单击删除 (Delete)。

系统会显示一条警告消息。要删除思科 ISE-PIC 内部 CA 证书，请单击以下选项之一：

- **删除 (Delete)**：删除思科 ISE-PIC 内部 CA 证书。思科 ISE-PIC 内部 CA 签名的所有终端证书都失效，终端无法加入网络。要允许终端再次接入网络，请将相同的思科 ISE-PIC 内部 CA 证书导入受信任证书存储区。
- **删除并撤销 (Delete & Revoke)**：删除并撤销思科 ISE-PIC 内部 CA 证书。思科 ISE-PIC 内部 CA 签名的所有终端证书都失效，终端无法连接到网络。此操作无法撤销。必须替换整个部署的思科 ISE-PIC 根证书链。

步骤 3 单击是 (Yes)，删除证书。

---

## 从受信任证书库导出证书

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。



**注释** 如果从内部 CA 导出证书，并计划使用导出的证书来从备份恢复，则必须使用 CLI 命令 `application configure ise`。请参阅[导出思科 ISE CA 证书和密钥](#)，第 99 页。

步骤 1 选中要导出的证书旁边的复选框，然后单击导出 (Export)。一次只能导出一个证书。

步骤 2 所选证书以 PEM 格式下载到运行客户端浏览器的文件系统中。

---

## 将根证书导入受信任证书库

导入根 CA 和中间 CA 证书时，指定要为其使用受信任 CA 证书的服务。

### 开始之前

您必须具有来自自己对证书签名请求进行签名并返回数字签名 CA 证书的 CA 的根证书和其他中间证书。

**步骤 1** 单击导入 (Import)。

**步骤 2** 在显示的将新证书导入证书存储区 (Import a new Certificate into the Certificate Store) 窗口中，单击选择文件 (Choose File) 以选择您的 CA 签名和返回的根 CA 证书。

**步骤 3** 在友好名称 (Friendly Name) 中输入友好的名称。

如果没有输入友好名称，思科 ISE-PIC 将使用 *common-name#issuer#nnnnn* 格式的名称填充此字段，其中 *nnnnn* 是唯一编号。您也可以稍后再编辑证书以更改友好名称。

**步骤 4** 选中要为其使用此受信任证书的服务旁边的复选框。

**步骤 5** (可选) 在说明 (Description) 字段中，输入此证书的说明。

**步骤 6** 单击提交 (Submit)。

### 下一步做什么

将中间 CA 证书导入到受信任证书库 (如果适用)。

## 证书链导入

您可以从单个文件导入多个证书，这个文件中包含从证书库接收的证书链。文件中的所有证书都必须为 PEM 格式，并且这些证书必须按照以下顺序排列：

- 文件中的最后一个证书必须是 CA 颁发的客户端证书或服务器证书。
- 前面的所有证书必须是根 CA 证书和所颁发证书的签名链中的所有中间 CA 证书。

导入证书链的过程分为两个步骤：

1. 在思科 ISE 管理门户中将证书链文件导入受信任证书库。此操作会将除最后一个证书之外的所有证书从文件导入受信任证书库。
2. 使用绑定 CA 签名的证书操作导入证书链文件。此操作会将文件中的最后一个证书导入作为本地证书。

## 受信任证书导入设置

下表说明了“受信任证书导入”(Trusted Certificate Import) 窗口上的字段，可以使用此窗口将 CA 证书添加到思科 ISE-PIC。要查看此处窗口，请单击菜单图标 (☰)，然后选择证书 (Certificates) > 受信任证书 (Trusted Certificates) > 导入 (Import)。

表 17: 受信任证书导入设置

字段名称	说明
证书文件 (Certificate File)	单击浏览 (Browse) 从运行浏览器的计算机选择证书文件。
友好名称 (Friendly Name)	输入证书的友好名称。如果您不指定名称，思科 ISE-PIC 会自动按照 <通用名称>#<颁发者>#<nnnnn> 的格式创建名称，其中 <nnnnn> 为唯一的五位数编号。
信任 ISE 中的身份验证 (Trust for authentication within ISE)	如果您希望将此证书用于验证服务器证书（从其他 ISE-PIC 节点或 LDAP 服务器），请选中此复选框。
信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)	（仅在选中了“信任 ISE-PIC 中的身份验证” (Trust for authentication within ISE) 复选框时适用）如果您想将此证书用于以下用途，请选中此复选框： <ul style="list-style-type: none"> <li>• 对使用 EAP 协议连接至 ISE-PIC 的终端进行身份验证</li> <li>• 信任系统日志服务器</li> </ul>
信任思科服务的身份验证 (Trust for authentication of Cisco Services)	如果您希望将此证书用于信任源服务等外部思科服务，请选中此复选框。
验证证书扩展名 (Validate Certificate Extensions)	（仅适用于同时选中“信任客户端身份验证和系统日志” (Trust for client authentication and Syslog) 选项和“证书扩展上启用验证” (Enable Validation of Certificate Extensions) 选项的情况下）确保有“keyUsage”扩展并且设置了“keyCertSign”位，而且有将 CA 标志设置为 true 的基本限制扩展。
说明 (Description)	输入可选的说明。

#### 相关主题

[受信任证书库](#)，第 79 页

[证书链导入](#)，第 84 页

[将根证书导入受信任证书库](#)，第 83 页

## 证书签名请求

对于 CA，要签发签名证书，您必须创建证书签名请求 (CSR) 并将其提交给 CA。

证书签名请求 (Certificate Signing Requests) 窗口会提供您已创建的证书签名请求的列表。要查看此窗口，单击菜单图标 (☰) 并选择 **管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书签名请求 (Certificate Signing Requests)**。要从 CA 获得签名，您必须导出证书签名请求，然后将证书发送至 CA。CA 给证书签名，然后返回证书。

您可以从思科 ISE 管理门户集中管理证书。您可以为您的部署中的所有节点创建证书签名请求并导出它们。然后，您应该将这些证书签名请求提交给 CA，从 CA 获取 CA 签名的证书，将 CA 返回的 root 和中间 CA 证书导入受信任证书库，并且将 CA 签名的证书与证书签名请求绑定。

## 创建证书签名请求并将其提交给证书颁发机构

可以生成证书签名请求，为部署中的节点获取 CA 签名的证书。可以为部署中的特定节点或所有节点生成证书签名请求。

---

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择 **证书 (Certificates) > 证书签名请求 (Certificate Signing Requests)**。

**步骤 2** 单击生成证书签名请求 (CSR) (Generate Certificate Signing Requests [CSR]) 以生成证书签名请求。

**步骤 3** 输入用于生成证书签名请求的值。有关显示的窗口中每个字段的信息，请参阅[受信任证书设置](#)，第 96 页。

**步骤 4** 选中签名请求复选框，然后单击**导出 (Export)** 以下载证书签名请求。

**步骤 5** 复制从“-----BEGIN CERTIFICATE REQUEST-----”到“-----END CERTIFICATE REQUEST-----”的所有文本。”。

**步骤 6** 将证书签名请求的内容粘贴到选定 CA 的证书请求中。

**步骤 7** 下载签名证书。

某些 CA 可能会将签名的证书通过邮件发送给您。签名的证书采用 ZIP 文件形式，其中包含必须添加到思科 ISE-PIC 受信任证书存储区的 CA 新颁发证书和公共签名证书。将数字签名的 CA 证书、根 CA 证书和其他中间 CA 证书（如果适用）下载到运行客户端浏览器的本地系统中。

---

## 将 CA 签名的证书绑定到证书签名请求

在 CA 返回数字签名的证书之后，您必须将其绑定到证书签名请求。您可以从思科 ISE 管理门户为部署中的所有节点执行绑定操作。

### 开始之前

- 您必须具有数字签名的证书，以及由 CA 返回的相关根和中间 CA 证书。
- 将相关的根和中间 CA 证书导入受信任证书库（**证书 (Certificates) > 受信任证书 (Trusted Certificates)**。）。



---

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择 **证书 (Certificates) > 证书签名请求 (Certificate Signing Requests)**。

选中您必须与 CA 签名证书绑定的证书签名请求旁边的复选框。

**步骤 2** 单击**绑定证书 (Bind Certificate)**。

**步骤 3** 在显示的**绑定 CA 签名证书 (Bind CA Signed Certificate)** 窗口中，单击**选择文件 (Choose File)** 以选择 CA 签名证书。

**步骤 4** 在**友好名称 (Friendly Name)** 字段中输入值。

**步骤 5** 如果您希望思科 ISE-PIC 验证证书扩展，请选中**验证证书扩展 (Validate Certificate Extensions)** 复选框。

如果您启用**验证证书扩展 (Validate Certificate Extensions)** 选项，且您导入的证书包含 CA 标志设置为 `ture` 的基本约束扩展，则请确保存在密钥用法扩展，且已设置 `keyEncipherment` 位或 `akeyAgreement` 位。

**注释** 思科 ISE 要求 EAP-TLS 客户端证书具有数字签名密钥用法扩展。

**步骤 6** (可选) 选中要为其将此证书用于**使用情况 (Usage)** 区域的服务。

如果您在生成证书签名请求时已启用**使用情况 (Usage)** 选项，则此信息会自动填充。您可以选择稍后编辑证书并指定用途。

在主 PAN 上更改**管理员用途**的证书会在所有其他节点上重新启动服务。在主 PAN 重启后，系统会每次重新启动一个节点。

**步骤 7** 单击**提交 (Submit)** 以便将证书签名请求绑定到 CA 签名的证书。

如果此证书已标记为用于思科 ISE-PIC 节点间通信，则思科 ISE-PIC 节点上的应用服务器会重新启动。

要在部署中的其他节点上绑定证书签名请求与 CA 签名的证书，请重复此流程。

---

下一步做什么

[将根证书导入受信任证书库，第 83 页](#)

## 导出证书签名请求

---

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择 **证书 (Certificates) > 证书签名请求 (Certificate Signing Requests)**。

**步骤 2** 选中想要导出的证书旁边的复选框，单击**导出 (Export)**。

**步骤 3** 证书签名请求将下载到本地文件系统中。

---

## 证书签名请求设置

通过思科 ISE-PIC，只需一个请求即可从管理员门户为部署中的节点生成证书签名请求。此外，还可以选择为部署中的单个节点或节点生成证书签名请求。如果选择为单个节点生成证书签名请求，则 ISE 会自动在证书使用者的 CN= 字段中替换特定节点的完全限定域名 (FQDN)。如果选择在证书的“主体可选名称 (SAN)” (Subject Alternative Name (SAN)) 字段中包含某个条目，则除了其他 SAN 属性之外，还必须输入 ISE-PIC 节点的 FQDN。如果选择为部署中的两个节点生成证书签名请求，请选中“允许通配符证书” (Allow Wildcard Certificates) 复选框，然后在 SAN 字段 (“DNS 名称” (DNS name)) 中输入通配符 FQDN 符号，例如，\*.amer.example.com。如果计划对 EAP 身份验证使用证书，请不要在 CN= 字段中输入通配符值。

通过使用通配符证书，不再需要为每个思科 ISE-PIC 节点生成一个唯一证书。此外，不再需要使用多个 FQDN 值填充 SAN 字段以防止证书警告。通过在 SAN 字段中使用星号 (\*)，可以在部署中的节点上共享单个证书，有助于防止证书名称不匹配警告。但是，使用通配符证书的安全性要比向每个思科 ISE-PIC 节点分配唯一服务器证书的安全性低。

下表列出了证书签名请求窗口中的字段，可以使用此页面生成可由证书颁发机构 (CA) 签名的证书签名请求。要查看此处窗口，请单击菜单图标 (☰)，然后选择 **证书 (Certificates) > 证书管理 (Certificate Management) > 证书签名请求 (Certificate Signing Request)**。

表 18: 证书签名请求设置

字段	使用指南
证书将用于 (Certificate(s) will be used for)	

字段	使用指南
	<p>选择即将对其使用证书的服务：</p> <p><b>思科 ISE 身份证书</b></p> <ul style="list-style-type: none"> <li>• <b>多用途 (Multi-Use)</b>: 用于多种服务（管理员、EAP-TLS 身份验证、pxGrid）。多用途证书同时使用客户端和服务器密钥用法。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性： <ul style="list-style-type: none"> <li>• <b>密钥用法 (Key Usage)</b>: 数字签名（签名）</li> <li>• <b>扩展密钥用法 (Extended Key Usage)</b>: TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 和 TLS Web 客户端身份验证 (1.3.6.1.5.5.7.3.2)</li> </ul> </li> <li>• <b>管理 (Admin)</b> - 用于服务器身份验证（以确保与管理员门户之间的安全通信，以及部署中 ISE-PIC 节点之间的安全通信）。签名 CA 的证书模板通常称为 Web 服务器证书模板。此模板具有以下属性： <ul style="list-style-type: none"> <li>• <b>密钥用法 (Key Usage)</b>: 数字签名（签名）</li> <li>• <b>扩展密钥用法 (Extended Key Usage)</b>: TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1)</li> </ul> </li> <li>• <b>ISE 消息服务 (ISE Messaging Service)</b>: 用于“经思科 ISE 消息传递的系统日志”功能，此功能可以对内置 UDP 系统日志收集目标（LogCollector 和 LogCollector2）实现 MnT WAN 有效性。 <ul style="list-style-type: none"> <li>• <b>密钥用法 (Key Usage)</b>: 数字签名（签名）</li> <li>• <b>扩展密钥用法 (Extended Key Usage)</b>: TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1)</li> </ul> </li> <li>• <b>pxGrid</b> - 同时用于客户端和服务器身份验证（以确保 pxGrid 客户端与服务器之间的安全通信）。签名 CA 的证书模板通常称为计算机证书模板。此模板具有以下属性： <ul style="list-style-type: none"> <li>• <b>密钥用法 (Key Usage)</b>: 数字签名（签名）</li> <li>• <b>扩展密钥用法 (Extended Key Usage)</b>: TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1) 和 TLS Web 客户端身份验证 (1.3.6.1.5.5.7.3.2)</li> </ul> </li> <li>• <b>SAML</b>: 用于确保与 SAML 身份提供程序 (IdP) 之间的安全通信的服务器证书。指定用于 SAML 的证书不可用于任何其他服务（例如管理员和 EAP 身份验证等）。 <ul style="list-style-type: none"> <li>• <b>密钥用法 (Key Usage)</b>: 数字签名（签名）</li> <li>• <b>扩展密钥用法 (Extended Key Usage)</b>: TLS Web 服务器身份验证 (1.3.6.1.5.5.7.3.1)</li> </ul> </li> </ul> <p>注释 建议您不要将包含值 2.5.29.37.0 的证书用于“扩展密钥用</p>

字段	使用指南
	<p>法” (Extended Key Usage) 属性中的任意用途对象标识符。如果将包含值 2.5.29.37.0 的证书用于“扩展密钥用法” (Extended Key Usage) 属性中的任意用途对象标识符，系统会将此证书视为无效，并显示以下错误消息：</p> <pre>source=local type=fatal message="unsupported certificate"</pre> <p><b>思科 ISE 证书颁发机构颁发的证书</b></p> <ul style="list-style-type: none"> <li>• <b>ISE 根 CA (ISE Root CA)</b> - (仅适用于内部 CA 服务) 用于重新生成整个内部 CA 证书链，包括主 PAN 上的根 CA 和 PSN 上的辅助 CA。</li> <li>• <b>ISE 中间 CA (ISE Intermediate CA)</b>: (仅适用于当 ISE-PIC 用作外部 PKI 的中间 CA 时的内部 CA 服务) 用于在主 PAN 上生成中间 CA 证书，在 PSN 上生成从属 CA 证书。签名 CA 的证书模板通常称为辅助证书颁发机构。此模板具有以下属性： <ul style="list-style-type: none"> <li>• <b>基本约束 (Basic Constraints)</b>: 关键、是证书颁发机构</li> <li>• <b>密钥用法 (Key Usage)</b>: 证书签名、数字签名</li> <li>• <b>扩展密钥用法 (Extended Key Usage)</b>: OCSP 签名 (1.3.6.1.5.5.7.3.9)</li> </ul> </li> <li>• <b>更新 ISE OCSP 响应方证书 (Renew ISE OCSP Responder Certificates)</b>: (仅适用于内部 CA 服务) 用于更新整个部署的 ISE-PIC OCSP 响应方证书 (不是证书签名请求)。出于安全原因，建议您每六个月更新一次 ISE-PIC OCSP 响应方证书。</li> </ul>
允许通配符证书 (Allow Wildcard Certificates)	选中此复选框以在 CN 中和/或证书的 SAN 字段的 DNS 名称中使用通配符 (*)。如果选中此复选框，系统会自动选择部署中的所有节点。必须在最左侧的标签位置使用星号 (*) 通配符。如果使用通配符证书，我们建议您对域名空间进行分区以提高安全性。例如，可以将域空间分区为 *.amer.example.com，而不是 *.example.com。如果不对域进行分区，可能会导致安全问题。
为这些节点生成 CSR (Generate CSRs for these Nodes)	选中要为其生成证书的节点旁边的复选框。要为部署中的选定节点生成 CSR，必须取消 Allow Wildcard Certificates 选项。
公共名称 (CN) (Common Name [CN])	默认情况下，公用名是您正为其生成证书签名请求的 ISE-PIC 节点的 FQDN。\$FQDN\$ 表示 ISE-PIC 节点的 FQDN。当为部署中的多个节点生成证书签名请求时，证书签名请求中的 CommonName 字段会替换为各个 ISE 节点的 FQDN。
组织单位 (OU) (Organizational Unit [OU])	组织单位名称。例如，Engineering。
组织 (O) (Organization [O])	组织名称。例如，Cisco。

字段	使用指南
城市 (L) (City [L])	(请勿缩写) 城市名称。例如, 圣何塞。
省/自治区/直辖市 (ST) (State [ST])	(请勿缩写) 省/自治区/直辖市名称。例如, 加州。
国家/地区 (C) (Country [C])	国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如, US。
主体可选名称 (SAN) (Subject Alternative Name [SAN])	<p>“IP 地址” (IP address)、 “DNS 名称” (DNS name)、 “统一资源标识符” (Uniform Resource Identifier, URI) 或与证书关联的 “目录名称” (Directory Name)。</p> <ul style="list-style-type: none"> <li>• <b>DNS 名称 (DNS name):</b> 如果选择 “DNS 名称” (DNS name), 请输入 ISE-PIC 节点的完全限定域名。如果已启用 Allow Wildcard Certificates 选项, 请指定通配符符号 (域名前的星号和句号)。例如: *.amer.example.com。</li> <li>• <b>IP 地址 (IP address):</b> 将与证书关联的 ISE-PIC 节点的 IP 地址。</li> <li>• <b>统一资源标识符 (Uniform Resource Identifier):</b> 您希望与证书关联的 URI。</li> <li>• <b>目录名称 (Directory Name):</b> 根据 RFC 2253 定义的可区分名称 (DN) 的字符串表示。使用逗号 (,) 隔开多个 DN。对于 “dnQualifier” RDN, 避免使用逗号而是使用反斜杠 “\” 作为分隔符。例如, CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL</li> </ul>
密钥类型 (Key Type)	指定要用于创建公共密钥的算法: RSA 或 ECDSA。

字段	使用指南
密钥长度 (Key Length)	<p>指定公共密钥的位大小。</p> <p>以下选项可用于 RSA:</p> <ul style="list-style-type: none"> <li>• 512</li> <li>• 1024</li> <li>• 2048</li> <li>• 4096</li> </ul> <p>以下选项可用于 ECDSA:</p> <ul style="list-style-type: none"> <li>• 256</li> <li>• 384</li> </ul> <p><b>注释</b> 对于同一安全级别，RSA 和 ECDSA 公共密钥可能具有不同的密钥长度。</p> <p>如果计划获取公共的 CA 签名证书或将思科 ISE-PIC 部署为符合 FIPS 标准的策略管理系统，请选择 2048 或更大长度。</p>
签名摘要 (Digest to Sign With)	选择下列散列算法之一：SHA-1 或 SHA-256。
证书策略 (Certificate Policies)	输入证书应符合的证书策略 OID 或 OID 列表。使用逗号或空格分隔 OID。

## 思科 ISE CA 服务

证书可以自签或由外部证书颁发机构 (CA) 进行数字签名。ISE-PIC 可用作 pxGrid 的外部证书颁发机构 (CA)，对 pxGrid 证书进行数字签名。CA 签名的数字证书被视为行业标准而且更安全。ISE-PIC CA 提供以下功能：

- 颁发证书：为连接您的网络的终端验证和签发证书签名请求 (CSR)。
- 密钥管理：在上生成并安全地存储密钥和证书。
- 存储证书：存储向用户和设备颁发的证书。
- 支持在线证书状态协议 (OCSP)：提供 OCSP 响应器以检查证书的有效性。

当 CA 服务在主管节点上禁用时，CA 服务仍被视为在辅助管理节点的 CLI 上运行。理想情况下，CA 服务应被视为禁用。此为已知的思科 ISE 问题。

## 省略曲线加密证书支持

思科 ISE-PIC CA 服务支持基于忽略曲线加密 (ECC) 算法的证书。与其他加密算法相比，ECC 提供的安全性和性能更高，即使使用更小的密钥大小也是如此。

下表比较了 ECC 和 RSA 的密钥大小以及安全强度。

ECC 密钥大小 (位)	RSA 密钥大小 (位)
160	1024
224	2048
256	3072
384	7680
521	15360

由于密钥大小较小，加密速度更快。

思科 ISE-PIC 支持以下 ECC 曲线类型。曲线类型越高，密钥规模越大，安全性就越强。

- P-192
- P-256
- P-384
- P-521

ISE-PIC 不支持证书中 EC 部分的显式参数。如果尝试导入具有显式参数的证书，将显示以下错误：“证书验证失败: 仅支持命名的 EC 参数” (Validation of certificate failed: Only named ECParameters supported)。

可以从证书调配门户生成 ECC 证书。



**注释** 在使用 EST 协议以及授权配置文件中的静态 IP 地址、FQDN 或主机名时，Android 客户端的 BYOD 流可能会失败。解决方法是使用 SCEP 而不是 EST。您可以在本地请求者配置文件中配置 SCEP。

## 思科 ISE-PIC 证书颁发机构证书

“证书颁发机构 (CA) 证书” (Certificate Authority (CA) Certificates) 页面列出了与内部思科 ISE-PIC CA 相关的所有证书。此页面按节点列出这些证书。可以展开某个节点以查看该特定节点的所有 ISE-PIC CA 证书。主要和辅助管理节点具有根 CA、节点 CA、从属 CA 和 OCSP 响应器证书。部署中的其他节点具有终端从属 CA 和 OCSP 证书。

启用思科 ISE-PIC CA 服务时，将在所有节点上自动生成和安装这些证书。此外，在替换整个 ISE-PIC 根 CA 链时，将在所有节点上自动重新生成和安装这些证书。不需要手动干预。



思科 ISE-PIC CA 证书遵循以下命名约定：证书服务 <终端从属 CA/节点 CA/根 CA/OCSP 响应器>-<节点主机名>#证书编号。

在“CA 证书” (CA Certificates) 页面中，可以编辑、导入、导出、删除和查看思科 ISE-PIC CA 证书。

## 编辑思科 ISE-PIC CA 证书

在添加证书到思科 ISE-PIC CA 证书存储区之后，可以采用编辑设置对其进行进一步编辑。

- 
- 步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择 **证书 (Certificates) > 证书颁发机构 (Certificate Authority) > 证书颁发机构证书 (Certificate Authority Certificates)**。
  - 步骤 2** 选中要编辑的证书旁边的复选框，然后单击 **编辑 (Edit)**。
  - 步骤 3** 根据需要修改可编辑字段。请参阅 [受信任证书设置](#)，第 96 页 以了解字段说明：
  - 步骤 4** 单击 **保存 (Save)** 以保存对证书库所做的更改。
- 

## 导出思科 ISE CA 证书

要导出思科 ISE 根 CA 和节点 CA 证书：

### 开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

- 
- 步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择 **证书 (Certificates) > 证书颁发机构 (Certificate Authority) > 证书颁发机构证书 (Certificate Authority Certificates)**。
  - 步骤 2** 选中要导出的证书旁边的复选框，然后单击 **导出 (Export)**。一次只能导出一个证书。
  - 步骤 3** 将需要加强保密的邮件文件保存到运行客户端浏览器的文件系统。
- 

## 导入思科 ISE-PIC CA 证书

如果客户端尝试使用来自其他部署的思科 ISE-PIC 颁发的证书对您的网络进行身份验证，您必须将来自该部署的思科 ISE-PIC 根 CA 证书、节点 CA 证书和终端从属 CA 证书导入到思科 ISE-PIC 受信任证书存储区。

### 开始之前

- 将 ISE-PIC 根 CA 证书、节点 CA 证书和终端从属 CA 证书从终端证书签名的部署中导出，并将其存储在浏览器运行所在的计算机的文件系统。
- 

- 步骤 1** 选择 **证书 (Certificates) > 受信任证书 (Trusted Certificates)**。

**步骤 2** 单击导入 (**Import**)。

**步骤 3** 如有必要，配置这些字段值。有关详细信息，请参阅[受信任证书导入设置](#)，第 84 页。

如果启用基于证书的客户端身份验证，则思科 ISE-PIC 将重新启动您的部署中每个节点上的应用服务器，从 PAN 。

## 受信任证书设置

下表介绍了受信任证书的**编辑 (Edit)** 窗口中的字段。在此窗口中编辑 CA 证书属性。要查看此处窗口，请单击菜单图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 证书 (Certificates) > 受信任证书 (Trusted Certificates)**。选中要编辑的受信任证书的复选框，然后单击**编辑 (Edit)**。

表 19: 受信任证书编辑设置

字段名称	使用指南
证书颁发者 (Certificate Issuer)	
友好名称 (Friendly Name)	输入证书的友好名称。此字段是可选字段。如果不输入友好名称，则系统会以以下格式生成默认名称： <i>common-name#issuer#nnnnn</i>
状态 (Status)	从下拉列表中选择 <b>启用 (Enabled)</b> 或 <b>禁用 (Disabled)</b> 。如果证书被禁用，则思科 ISE 将不使用此证书建立信任。
说明 (Description)	(可选) 输入说明。
使用情况 (Usage)	
信任 ISE 中的身份验证 (Trust for authentication within ISE)	如果您想要使用此证书验证服务器证书 (从其他思科 ISE 节点或 LDAP 服务器)，请选中此复选框。
信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)	(仅在选中了信任 ISE 中的身份验证” (Trust for authentication within ISE) 复选框时适用) 如果您想将此证书用于以下用途，请选中此复选框： <ul style="list-style-type: none"> <li>对使用 EAP 协议连接至思科 ISE 的终端进行身份验证。</li> <li>信任系统日志服务器。</li> </ul>
信任思科服务的身份验证 (Trust for authentication of Cisco Services)	如果您希望将此证书用于信任源服务等外部思科服务，请选中此复选框。

字段名称	使用指南
证书状态验证 (Certificate Status Validation)	思科 ISE 支持使用两种方法检查特定 CA 颁发的客户端或服务器证书的吊销状态。第一种方法是使用在线证书状态协议 (OCSP) 验证证书，其将向 CA 维护的 OCSP 服务发送请求。第二种方法是按照从 CA 下载至思科 ISE 的 CRL 验证证书。可以同时启用这两种方法，在这种情况下首先使用 OCSP 方法，只有在无法确定证书状态时，才会使用 CRL 方法。
验证 OCSP 服务 (Validate Against OCSP Service)	选中此复选框以按照 OCSP 服务验证证书。您必须先创建 OCSP 服务才能选中此复选框。
如果 OCSP 返回未知状态则拒绝请求 (Reject the request if OCSP returns UNKNOWN status)	如果 OCSP 服务无法确定证书状态，则选中此复选框以拒绝请求。在选中此复选框的情况下，如果 OCSP 服务返回未知状态值，此服务将导致思科 ISE 拒绝当前评估的客户端或服务器证书。
OCSP 响应器无法访问时拒绝请求 (Reject the request if OCSP Responder is unreachable)	选中此复选框供思科 ISE 在 OCSP 响应器无法访问时拒绝请求。
下载 CRL (Download CRL)	选中此复选框以使思科 ISE 下载 CRL。
CRL 分类的 URL (CRL Distribution URL)	输入用于从 CA 下载 CRL 的 URL。如果在证书颁发机构证书中指定了 URL，则系统会自动填写此字段。URL 必须以“http”、“https”或“ldap”开头。
检索 (Retrieve CRL)	可以自动或定期下载 CRL。请配置下载时间间隔。
如果下载失败，请稍候 (If download failed, wait)	配置在思科 ISE 再次尝试下载 CRL 之前等待的时间间隔。
如果 CRL 没有收到，绕过此 CRL 验证 (Bypass CRL Verification if CRL is not Received)	选中此复选框，以使系统在收到 CRL 之前接受客户端请求。如果取消选中此复选框，思科 ISE 会拒绝使用选定 CA 签名的证书的所有客户端请求，直到收到 CRL 文件为止。

字段名称	使用指南
忽略 CRL 无效或已过期 (Ignore that CRL is not yet valid or expired)	<p>如果您希望思科 ISE 忽略开始日期和到期日期并继续使用非活动或已过期 CRL 以及根据 CRL 内容允许或拒绝 EAP-TLS 身份验证，请选中此复选框。</p> <p>如果您希望思科 ISE 在 Effective Date 字段指定的开始日期和 Next Update 字段指定的到期日期检查 CRL 文件，请取消选中此复选框。如果 CRL 尚未激活或已到期，思科 ISE 会拒绝使用此 CA 签名的证书的所有身份验证。</p>

#### 相关主题

[受信任证书库](#)，第 79 页

[编辑受信任证书](#)，第 82 页

## 思科 ISE-PIC CA 证书和密钥的备份与恢复

必须安全地备份思科 ISE-PIC CA 证书和密钥，以在出现 PAN 故障以及您要将辅助管理节点升级作为外部 PKI 的根 CA 或中间 CA 的情况下在辅助管理节点上恢复这些证书和密钥。思科 ISE-PIC 配置备份不包括 CA 证书和密钥。您应使用命令行界面 (CLI) 将 CA 证书和密钥导出至存储库，然后再导入。**application configure ise** 命令现在包含导出和导入选项，用于备份和恢复 CA 证书和密钥。

来自受信任证书库的以下证书存储于辅助管理节点上：

- 思科 ISE Root CA 证书
- 思科 ISE 子 CA 证书
- 思科 ISE 终端 RA 证书
- 思科 ISE OCSP 响应器证书

在以下情况下，您必须备份和恢复思科 ISE CA 证书和密钥：

- 部署中有辅助管理节点
- 替换整个思科 ISE-PIC CA 根链
- 配置思科 ISE-PIC 根 CA 作为外部 PKI 的从属 CA
- 从配置备份恢复数据。在这种情况下，必须首先重新生成思科 ISE-PIC CA 根链，然后备份和恢复 ISE CA 证书和密钥。



**注释** 每次在部署中更换思科 ISE 内部 CA 后，还必须同时刷新 ISE 消息服务，以检索完整的证书链。

## 导出思科 ISE CA 证书和密钥

您必须从 PAN 导出 CA 证书和密钥，才能将其导入到辅助管理节点。通过此选项，辅助管理节点可以在 PAN 关闭和您将辅助管理节点升级到 PAN 时为终端颁发和管理证书。

### 开始之前

确保您已经创建了用于存储 CA 证书和密钥的存储库。

**步骤 1** 在思科 ISE CLI 上输入 **application configure ise** 命令。

**步骤 2** 输入 7 以导出证书和密钥。

**步骤 3** 输入存储库名称。

**步骤 4** 输入加密密钥。

系统将显示成功消息和已导出的证书列表，以及主题、颁发机构和序列号。

### 示例:

```
The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
  Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
  Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
  Serial#:0x621867df-568341cd-944cc77f-c9820765

  Subject:CN=Cisco ISE Endpoint CA of ise-vm1
  Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
  Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

  Subject:CN=Cisco ISE Endpoint RA of ise-vm1
  Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
  Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

  Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
  Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
  Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1
ISE CA keys export completed successfully
```

## 导入思科 ISE-PIC CA 证书和密钥

在注册辅助管理节点之后，您必须从 PAN 导出 CA 证书和密钥并将它们导入到辅助管理节点。

**步骤 1** 在思科 ISE-PIC CLI 上输入 **application configure ise** 命令。

**步骤 2** 输入 8 以导入 CA 证书和密钥。

**步骤 3** 输入存储库名称。

**步骤 4** 输入要导入的文件的名称。文件名应采用以下格式 **ise\_ca\_key\_pairs\_of\_<vm hostname>**。

**步骤 5** 输入加密密钥以解密文件。

系统将显示一条成功消息。

### 示例:

```

The following 4 CA key pairs were imported:
  Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
  Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
  Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

  Subject:CN=Cisco ISE Endpoint CA of ise-vm1
  Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
  Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

  Subject:CN=Cisco ISE Endpoint RA of ise-vm1
  Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
  Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

  Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
  Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
  Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully

```

**注释** 思科 ISE 版本 2.6 中引入了对导出的密钥文件的加密。从思科 ISE 版本 2.4 及更早版本导出密钥以及在思科 ISE 版本 2.6 及更高版本中导入密钥都不会成功。

## 生成根 CA 和从属 CA

设置部署时，思科 ISE-PIC 会在节点。但是，当更改节点的域名或主机名时，必须分别在主 PAN 上重新生成根 CA，在 PSN 上重新生成从属 CA。

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择 **证书 (Certificates) > 证书签名请求 (Certificate Signing Requests)**。

**步骤 2** 单击生成证书签名请求 (**Generate Certificate Signing Requests**)。

**步骤 3** 从证书将用于 (**Certificate(s) will be used for**) 下拉列表中选择 ISE 根 CA。

**步骤 4** 单击替换 ISE 根 CA 证书链 (**Replace ISE Root CA Certificate chain**)。

系统会为部署中的所有节点生成根 CA 和从属 CA 证书。

## 将思科 ISE-PIC 根 CA 配置为外部 PKI 的辅助 CA

如果您希望主 PAN 上的根 CA 作为外部 PKI 的从属 CA，则生成 ISE-PIC 中间 CA 证书签名请求，将其发送到外部 CA，获取根 CA 证书和 CA 签名的证书，将根 CA 证书导入受信任证书存储区，将 CA 签名的证书绑定到 CSR。在这种情况下，外部 CA 为根 CA，节点为外部 CA 的从属 CA，PSN 为节点的从属 CA。

**步骤 1** 依次选择 **证书 (Certificates) > 证书签名请求 (Certificate Signing Requests)**。

步骤 2 单击生成证书签名请求 (CSR) (Generate Certificate Signing Requests [CSR])。

步骤 3 从证书将用于 (Certificate(s) will be used for) 下拉列表选择 ISE 中级 CA。

步骤 4 单击生成 (Generate)。

步骤 5 导出 CSR，将其发送到外部 CA，获取 CA 签名的证书。

步骤 6 将根 CA 证书从外部 CA 导入受信任证书库。

步骤 7 将 CA 签名证书与 CSR 绑定。

## OCSP 服务

在线证书状态协议 (OCSP) 是一种用于检查 x.509 数字证书状态的协议。此协议替代证书吊销列表 (CRL) 并解决导致处理 CRL 的问题。

思科 ISE 能够通过 HTTP 与 OCSP 服务器进行通信，以在身份验证中验证证书的状态。OCSP 配置在可从思科 ISE 中配置的任何证书颁发机构 (CA) 证书引用的可重用配置对象中进行配置。

您可以根据 CA 配置 CRL 和/或 OCSP 验证。如果同时选择两者，则思科 ISE 会先通过 OCSP 执行验证。如果检测到主 OCSP 服务器和辅助 OCSP 服务器均有通信问题，或者如果针对给定证书返回未知状态，则思科 ISE 会切换至检查 CRL。

## 思科 ISE CA 服务在线证书状态协议响应器

思科 ISE CA OCSP 响应器是与 OCSP 客户端进行通信的服务器。思科 ISE CA 的 OCSP 客户端包括内部思科 ISE OCSP 客户端和自适应安全设备 (ASA) 上的 OCSP 客户端。OCSP 客户端应使用 RFC 2560 和 5019 中定义的 OCSP 请求/响应结构与 OCSP 响应器进行通信。

ISE CA 向 OCSP 响应器颁发证书。OCSP 响应器在端口 2560 上侦听任何传入请求。此端口配置为仅允许 OCSP 流量。

OCSP 响应器接受遵循 RFC 2560 和 5019 中定义的结构请求。OCSP 请求中支持随机数扩展。OCSP 响应器获取证书的状态，然后创建 OCSP 响应并对其进行签名。OCSP 响应不会缓存到 OCSP 响应器上，但您可以将 OCSP 响应缓存到客户端上，最长期限为 24 小时。OCSP 客户端应验证 OCSP 响应中的签名。

PAN 上的自签名 CA 证书（如果 ISE 用作外部 CA 的中间 CA，则是中间 CA 证书）颁发 OCSP 响应器证书。PAN 上的此 CA 证书颁发 PAN 和 PSN 上的 OCSP 证书。此自签名 CA 证书也是整个部署的根证书。整个部署中的所有 OCSP 证书都放在 ISE 的受信任证书库中，以验证任何使用这些证书签名的响应。



### 注释

思科 ISE 会从 OCSP 响应器服务器接收 thisUpdate 值，该值指明了自上次证书撤销以来的时间。如果 thisUpdate 值大于 7 天，则思科 ISE 中的 OCSP 证书验证失败。

## OCSP 证书状态值

OCSP 服务面向给定的证书请求返回以下值：

- Good - 表示对状态查询的肯定回答。它意味着仅在下次时间间隔（存活时间）值之前证书未被吊销并且状态良好。
- Revoked - 证书被吊销。
- Unknown - 证书状态未知。如果证书不是由此 OCSP 响应者的 CA 颁发，则 OCSP 服务会返回此值。
- Error - 没有收到 OCSP 请求的任何响应。

## OCSP 高可用性

思科 ISE 能够为每个 CA 配置最多两台 OCSP 服务器，我们将其称为主 OCSP 服务器和辅助 OCSP 服务器。每个 OCSP 服务器配置均包含以下参数：

- URL - OCSP 服务器 URL。
- Nonce - 请求中发送的随机数。此选项可确保重放攻击无法利用旧通信数据。
- Validate response - 思科 ISE 验证从 OCSP 服务器接收到的响应签名。

在超时（5 秒钟）情况下，当思科 ISE 与主要 OCSP 服务器进行通信时，它会切换为辅助 OCSP 服务器。

思科 ISE 在尝试再次使用主要服务器之前，会在可配置的时间内使用辅助 OCSP 服务器。

## OCSP 故障

以下是三个一般 OCSP 故障情况：

- OCSP 缓存或 OCSP 客户端（思科 ISE）故障。
- OCSP 响应器故障情况，例如：

第一个主要 OCSP 响应器无响应，辅助 OCSP 响应器响应思科 ISE OCSP 请求。

无法从思科 ISE OCSP 请求接收错误或响应。

OCSP 响应器可能不向思科 ISE OCSP 请求提供响应或可能返回一个不成功的 OCSP Response Status 值。可能的 OCSP Response Status 值如下所示：

- tryLater
- signRequired
- unauthorized
- internalError



- malformedRequest

OCSP 请求中有很多日期时间检查、签名验证检查等。有关详细信息，请参阅 *RFC 2560 X.509 互联网公共密钥基础结构在线证书状态协议 - OCSP*，其中描述了所有可能的状态，包括错误状态。

- OCSP 报告故障

## 添加 OCSP 客户端配置文件

您可以使用 OCSP Client Profile 页面，将新 OCSP 客户端配置文件添加到思科 ISE。

### 开始之前

如果 Certificate Authority (CA) 正在非标准端口（不是 80 或 443）上运行 OCSP 服务，则必须在交换机上配置 ACL，允许在思科 ISE 和 CA 之间通过此端口进行通信。例如：

```
permit tcp <source ip> <destination ip> eq <OCSP 端口号>
```

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择证书 (Certificates) > OCSP 客户端配置文件 (OCSP Client Profile)。

**步骤 2** 输入值，添加 OCSP 客户端配置文件。

**步骤 3** 单击提交 (Submit)。

## OCSP 统计计数器

思科 ISE 使用 OCSP 计数器记录并监控 OCSP 服务器的数据和运行状况。日志记录每五分钟记录进行一次。思科 ISE 将系统日志消息发送到监控节点，并在本地库中进行保存。本地库包含之前五分钟的数据。思科 ISE 发送系统日志消息后，计数器会重新开始计算下一个间隔。这表示在五分钟后，新的五分钟时间间隔将会启动。

以下表格列出 OCSP 系统日志消息及其说明。

表 20: OCSP 系统日志消息

消息	说明
OCSPPrimaryNotResponsiveCount	无响应的主请求数量
OCSPSecondaryNotResponsiveCount	无响应的辅助请求数量
OCSPPrimaryCertsGoodCount	对于使用 OCSP 主服务器的给定 CA 所返回的“good”证书数量

消息	说明
OCSPSecondaryCertsGoodCount	对于使用 OCSP 主服务器的给定 CA 所返回的“good”状态数量
OCSPPrimaryCertsRevokedCount	对于使用 OCSP 主服务器的给定 CA 所返回的“revoked”状态数量
OCSPSecondaryCertsRevokedCount	对于使用 OCSP 辅助服务器的给定 CA 所返回的“revoked”状态数量
OCSPPrimaryCertsUnknownCount	对于使用 OCSP 主服务器的给定 CA 所返回的“Unknown”状态数量
OCSPSecondaryCertsUnknownCount	对于使用 OCSP 辅助服务器的给定 CA 所返回的“Unknown”状态数量
OCSPPrimaryCertsFoundCount	主源缓存中查找到的证书数量
OCSPSecondaryCertsFoundCount	辅助源缓存中查找到的证书数量
ClearCacheInvokedCount	经过间隔时间后触发缓存清理的次数
OCSPCertsCleanedUpCount	经过间隔时间后清除的已缓存条目的数量
NumOfCertsFoundInCache	缓存中已执行的请求数量
OCSPCacheCertsCount	在 OCSP 缓存中查找到的证书数量



## 第 7 章

# 管理 ISE-PIC

- [管理 ISE-PIC 节点](#)，第 105 页
- [管理 ISE-PIC 安装](#)，第 110 页
- [管理设置 ISE-PIC](#)，第 129 页

## 管理 ISE-PIC 节点

添加或删除辅助节点，在节点之间同步数据，将辅助节点升级为主节点等。

## 思科 ISE-PIC 部署设置

在所有节点上安装思科 ISE-PIC 后，如《思科身份识别服务引擎硬件安装指南》所述，节点显示为独立状态。必须定义一个节点作为主管理节点 (PAN)，并将辅助节点注册到 PAN。

所有思科 ISE-PIC 系统和功能相关配置应当只在 PAN 上进行。在 PAN 上执行的配置更改将复制到部署中的辅助节点。从辅助节点可以执行的唯一操作是将辅助节点升级为 PAN。

在向 PAN 注册了辅助节点之后，在登录此辅助节点的管理员门户时，必须使用 PAN 的登录凭证。

## 将数据从主 ISE-PIC 节点复制到辅助节点

将思科 ISE 节点注册为辅助节点时，思科 ISE-PIC 会立即创建一个从主要节点到辅助节点的数据复制通道并开始执行复制进程。复制是从主节点向辅助节点共享思科 ISE-PIC 配置数据的过程。复制可确保作为您的部署组成部分的两个思科 ISE-PIC 节点中配置数据的一致性。

首次将 ISE-PIC 节点注册为辅助节点时通常会进行完全复制。完全复制之后进行增量复制，确保在辅助节点中反映所有新的更改，例如对 PAN 中配置数据的添加、修改或删除。复制过程可确保部署中的所有思科 ISE-PIC 节点保持同步。在思科 ISE-PIC 管理员门户的部署页面，可在“节点状态” (Node Status) 列查看复制的状态。将思科 ISE-PIC 节点注册为辅助节点或与 PAN 进行手动同步时，节点状态显示橙色图标，表示正在进行所请求的操作。操作完成后，节点状态变为绿色，表示辅助节点已与 PAN 同步。

## 在思科 ISE-PIC 中修改节点的影响

在思科 ISE-PIC 中对节点进行以下任一更改后，节点将重新启动，这会导致延迟：

- 注册节点（独立节点至辅助节点）
- 取消注册节点（辅助节点至独立节点）
- 将主要节点更改为独立节点（如果未向其注册任何其他节点；主要节点至独立节点）
- 升级节点（辅助节点升级为主节点）
- 恢复主要节点上的备份，然后系统会触发一项同步操作，将数据从主要节点复制到辅助节点



**注释** 当您将在辅助管理节点提升为主 PAN 位置时，主节点将承担辅助角色。这会导致主节点和辅助节点重新启动，从而导致延迟。

## 在部署中设置两个节点的指南

使用两个节点设置思科 ISE-PIC 之前，请仔细阅读以下声明。

- 为两个节点选择同一网络时间协议 (NTP) 服务器。要避免节点之间发生时区问题，您必须在每个节点的设置过程中提供同一 NTP 服务器名称。此设置可确保来自部署中的各种节点的报告和日志与时间戳始终同步。
- 安装思科 ISE-PIC 时配置思科 ISE-PIC 管理员密码。以前的思科 ISE-PIC 管理员默认登录凭证 (admin/cisco) 不再有效。使用初始设置过程中创建的用户名和密码或当前密码（如果后来更改了密码）。
- 配置域名系统 (DNS) 服务器。在 DNS 服务器中输入部署中包含的两个思科 ISE-PIC 节点的 IP 地址和完全限定域名 (FQDN)。否则，节点注册将失败。
- 从 DNS 服务器为高可用性部署中的两个思科 ISE-PIC 节点配置正向和反向 DNS 查找。否则，在注册并重新启动思科 ISE-PIC 节点时可能会遇到部署相关问题。如果没有为两个节点配置反向 DNS 查找，则性能可能会降低。
- （可选）从 PAN 对辅助思科 ISE-PIC 节点取消注册以从中卸载思科 ISE-PIC。
- 确保即将注册为辅助节点的 PAN 和独立节点运行的是同一版本的思科 ISE-PIC。

## 查看部署中的节点

在部署节点 (**Deployment Nodes**) 窗口，可以查看部署中的 ISE-PIC 节点（主节点和辅助节点）。

**步骤 1** 登录主思科 ISE-PIC 管理员门户。

**步骤 2** 选择管理 (**Administration**) > 部署 (**Deployment**)。

列出部署中的所有思科 ISE 节点。

## 注册辅助思科 ISE-PIC 节点

注册辅助节点后，辅助节点的配置会被添加到主要节点的数据库中，而辅助节点上的应用服务器会重启。完成重新启动后，可以查看您在 PAN 的“部署” (Deployment) 页面中做出的所有配置更改。但是，您的更改会延迟 5 分钟生效并出现在部署 (Deployment) 页面中。

**步骤 1** 登录到 PAN。

**步骤 2** 选择管理 (Administration) > 部署 (Deployment)。

如果部署中未注册辅助节点，则添加辅助节点 (Add Secondary Node) 部分将显示在页面底部。

**步骤 3** 在添加辅助节点 (Add Secondary Node) 部分中，输入辅助思科 ISE 节点的 DNS 可解析主机名。

如果在注册思科 ISE-PIC 节点时使用主机名，则准备注册的独立节点的完全限定域名 (FQDN) 必须从可 PAN 进行 DNS 解析，例如 *abc.xyz.com*。否则，节点注册将失败。您必须事先在 DNS 服务器中定义辅助节点的 IP 地址和 FQDN。

**步骤 4** 在“用户名” (Username) 和“密码” (Password) 字段中输入独立节点的基于 UI 的管理员凭证。

**步骤 5** 单击保存 (Save)。

思科 ISE-PIC 会与辅助节点通信，获取一些基本信息，例如主机名、默认网关等，并显示这些信息。

当辅助节点注册到部署时，节点将重新启动，这可能需要 5 分钟才能在“部署” (Deployment) 页面显示辅助节点信息。

成功注册辅助节点后，“部署” (Deployment) 页面会在辅助节点 (Secondary Node) 部分显示此节点的详细信息。

成功注册辅助节点后，您会在 PAN 上收到确认节点注册成功的警报。如果辅助节点与 PAN 注册失败，则不会生成警报。节点注册后，该节点上的应用服务器会重启。注册成功和数据库同步成功后，请输入主要管理节点的凭证登录到辅助节点的用户界面。



### 注释

除了部署中现有的主要节点外，当您成功注册新的节点时，不会显示新注册节点的对应警报。配置更改警报则会反应新注册节点的对应信息。您可以使用此信息确定新节点是否注册成功。

## 同步主要和辅助思科 ISE-PIC 节点

只能通过主 PAN 对思科 ISE-PIC 的配置进行更改。系统会将配置更改复制到所有辅助节点。如果出于某些原因未能正常执行复制，则可以手动同步辅助 PAN 与主 PAN。

**步骤 1** 登录到主 PAN。

**步骤 2** 选择管理 (Administration) > 部署 (Deployment)。

**步骤 3** 选中要与主 PAN 同步的节点旁边的复选框，然后单击同步 (Syncup) 强制执行数据库完全复制。

## 手动将辅助 PAN 升级为主 PAN

如果主 PAN 出现故障则必须手动将辅助 PAN 升级为主 PAN。

### 开始之前

确保已配置第二个思科 ISE-PIC 节点，以将其升级为主 PAN。

**步骤 1** 登录辅助 PAN GUI。

**步骤 2** 选择管理 (Administration) > 部署 (Deployment)。

**步骤 3** 单击升级为主节点 (Promote to Primary)。

**步骤 4** 单击保存 (Save)。

### 下一步做什么

如果原来为主 PAN 的节点恢复运行，则会自动降级成为辅助 PAN。必须对此节点（原来为主 PAN）执行手动同步，才能将其恢复到部署中。

## 从部署中删除节点

要从部署中删除节点，您必须取消注册该节点。已取消注册的节点会成为独立思科 ISE-PIC 节点。

取消注册节点时，终端数据将丢失。如果您希望节点在成为独立节点后保留终端数据，可以从主 PAN 获取备份，并在节点上恢复此数据备份。

可以在主 PAN 的部署 (Deployment) 窗口中查看这些更改。但是，预计更改会延迟 5 分钟生效并显示在部署 (Deployment) 窗口上。

### 开始之前

要从部署中删除节点，您必须取消注册该节点。从 PAN 取消注册辅助节点时，被取消注册的节点的状态更改为独立，主节点和辅节点之间的连接将丢失。复制更新不再发送到被取消注册的独立节点。

在从部署中删除某个辅助节点之前，请对思科 ISE-PIC 配置执行备份，稍后可在需要时恢复该备份。

**步骤 1** 选择管理 (Administration) > 部署 (Deployment)。

**步骤 2** 单击辅助节点详细信息旁的取消注册 (Deregister)。

**步骤 3** 单击确定 (OK)。

**步骤 4** 验证在主 PAN 上是否收到警报，以确认辅助节点成功取消注册。如果从主 PAN 取消注册辅助节点失败，则不会生成警报。

---

## 更改思科 ISE-PIC 节点的主机名或 IP 地址

可以更改独立思科 ISE-PIC 节点的主机名、IP 地址或域名。不能使用 **localhost** 作为节点的主机名。

### 开始之前

如果思科 ISE-PIC 节点是两节点部署的一部分，必须将其从部署中删除并确保该节点为独立节点。

---

**步骤 1** 从思科 ISE CLI 使用 **hostname**、**ip address**、或 **ip domain-name** 命令更改思科 ISE-PIC 节点的主机名或 IP 地址。

**步骤 2** 从思科 ISE CLI 使用 **application stop ise** 命令重置思科 ISE-PIC 应用配置以重新启动所有服务。

**步骤 3** 如果思科 ISE-PIC 节点为两节点部署的一部分，则将其注册到主 PAN。

**注释** 如果您在注册思科 ISE-PIC 节点时使用主机名，则将要注册的独立节点的完全限定域名 (FQDN) 必须可以从主 PAN 进行 DNS 解析，例如 FQDN 可以为 *abc.xyz.com*。否则，节点注册将失败。必须输入作为 DNS 服务器上部署一部分的思科 ISE-PIC 节点的 IP 地址和 FQDN。

将思科 ISE-PIC 注册为辅助节点后，主 PAN 会将 IP 地址、主机名或域名中的更改复制到您的分布式部署中另一个思科 ISE-PIC 节点。

---

## 更换思科 ISE-PIC 设备硬件

仅应在思科 ISE-PIC 设备硬件出现问题时更换硬件。对于任何软件问题，可以重新映像该设备并重新安装思科 ISE-PIC 软件。

---

**步骤 1** 在新的节点上重新映像或重新安装思科 ISE-PIC 软件。

**步骤 2** 借助 UDI 获取主要和辅助 PAN 的许可证，并安装到主 PAN 上。

**步骤 3** 恢复所更换的主 PAN 上的备份。

恢复脚本将尝试同步辅助 PAN 上的数据，但辅助 PAN 现已成为独立节点，同步将会失败。将数据设置为在主 PAN 上进行备份的时间。

**步骤 4** 通过主 PAN 将新节点注册为辅助服务器。

# 管理 ISE-PIC 安装

安装补丁、运行备份或实施系统恢复。

## 安装软件补丁

**步骤 1** 选择管理 (Administration) > 维护 (Maintenance) > 补丁管理 (Patch Management)，然后单击安装 (Install)。

**步骤 2** 单击浏览 (Browse)，然后选择已从 Cisco.com 下载的补丁。

**步骤 3** 单击安装 (Install) 安装补丁。

在 PAN 上安装补丁后，思科 ISE-PIC 会将您注销，您必须等待几分钟后才能再次登录。

**注释** 安装补丁期间，**Show Node Status** 是可在“补丁管理” (Patch Management) 页面上访问的唯一功能。

**步骤 4** 选择管理 (Administration) > 维护 (Maintenance) > 补丁管理 (Patch Management) 以返回至“补丁安装” (Patch Installation) 页面。

**步骤 5** 单击您在任意辅助节点上安装的补丁旁边的单选按钮，然后单击显示节点状态 (Show Node Status) 以验证是否已完成安装。

### 下一步做什么

如果需要在另一个辅助节点上安装补丁，请确保节点正在运行并重复此程序以在其余节点上安装补丁。

## 思科 ISE-PIC 软件补丁

思科 ISE-PIC 软件补丁始终会累积。思科 ISE-PIC 允许您执行补丁安装和从 CLI 或 GUI 回滚。

可以在部署中从主 PAN 为思科 ISE-PIC 服务器安装补丁。要从主 PAN 安装补丁，您必须从 Cisco.com 将补丁下载至运行您的客户端浏览器的系统。

如果从 GUI 安装补丁，补丁将先自动安装到主 PAN 上。系统随后将按照 GUI 中列出的顺序，在部署中的其他节点上安装补丁。无法控制节点的更新顺序。还可以手动安装、回滚和查看补丁版本。在思科 ISE GUI 中，单击菜单图标 (≡)，然后选择管理 (Administration) > 系统 (System) > 维护 (Maintenance) > 补丁管理 (Patch Management)。

如果从 CLI 安装补丁，可以控制节点的更新顺序。但是，建议您先在主 PAN 上安装补丁。

如果要在升级整个部署之前在某些节点上验证补丁，可以使用 CLI 在选定节点上安装补丁。使用以下 CLI 命令安装补丁：

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

有关详细信息，请参阅《思科身份识别服务引擎 CLI 参考指南》中“执行模式下的思科 ISE CLI 命令”一章中的“安装补丁”部分。



您可以直接安装所需的补丁版本。例如，如果您当前使用的是思科 ISE 2.x，并且希望安装思科 ISE 2.x 补丁 5，则可以直接安装思科 ISE 2.x 补丁 5，而无需安装以前的补丁（在本例中为思科 ISE 2.x 补丁 1-4）。要在 CLI 中查看补丁版本，请使用以下 CLI 命令：

```
show version
```

## 软件补丁安装指南

在 ISE 节点上安装补丁时，节点会在安装完成后重新引导。可能必须等待几分钟才能再次登录。可以在维护时段安排补丁安装，以避免临时中断。

确保安装了适用于网络中部署的思科 ISE-PIC 版本的补丁。思科 ISE-PIC 会报告任何版本不匹配问题，以及补丁文件中的任何错误。



**注释** 思科 ISE 补丁也可以安装在 ISE-PIC 上。

安装的补丁版本不能低于当前安装在思科 ISE-PIC 上的补丁版本。同样，如果思科 ISE-PIC 当前安装的是高版本补丁，则无法回滚低版本补丁的更改。例如，如果思科 ISE-PIC 服务器安装的是补丁 3，则无法安装或回滚补丁 1 或 2。

从两节点部署中的主 PAN 安装补丁时，思科 ISE-PIC 会先后在主节点和辅助节点上安装补丁。如果在主 PAN 上成功安装，思科 ISE-PIC 之后会继续在辅助节点上安装补丁。如果在主 PAN 上安装失败，则不会继续在辅助节点上安装。

## 回滚软件补丁

您从属于部署一部分的 PAN 回滚补丁时，思科 ISE-PIC 会在主节点上回滚补丁，然后在部署中的辅助节点上回滚补丁。

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择**管理 (Administration)** > **维护 (Maintenance)** > **补丁管理 (Patch Management)**。

**步骤 2** 单击您要回滚更改的补丁版本的单选按钮，然后单击**回滚 (Rollback)**。

**注释** 回滚补丁期间，在“补丁管理” (Patch Management) 页面上仅可访问 **Show Node Status** 功能。

从 PAN 回滚补丁后，思科 ISE 会将您注销，您必须等待几分钟，然后才能再次登录。

**步骤 3** 您登录之后，请单击页面底部的**警报 (Alarms)** 链接以查看回滚操作的状态。

**步骤 4** 要查看补丁回滚的进程，请在“补丁管理” (Patch Management) 页面选择补丁，然后单击**显示节点状态 (Show Node Status)**。

**步骤 5** 在辅助节点上，单击补丁的单选按钮，然后单击**显示节点状态 (Show Node Status)**，确保从部署中的所有节点回滚补丁。

如果没有从任意辅助节点回滚补丁，请确保该节点正常运行并且重复此程序以从其余节点回滚更改。思科 ISE-PIC 仅从仍安装此版本补丁的节点回滚补丁。

## 软件补丁回滚指南

要从部署中的思科 ISE-PIC 节点回滚补丁，必须先从 PAN 回滚更改。如果此操作成功，则系统会从辅助节点回滚补丁。如果 PAN 上的回滚流程失败，则系统不会从辅助节点回滚补丁。

当思科 ISE-PIC 从辅助节点回滚补丁时，可以继续从 PAN GUI 执行其他任务。辅助节点将会在回滚后重新启动。

## 备份和恢复数据



**注释** 思科 ISE-PIC 的作用在许多情况下与思科 ISE 备份和恢复程序相同，因此，术语思科 ISE 有时可能会互换使用，以表示与思科 ISE-PIC 相关的操作和功能。

思科 ISE-PIC 允许您从主节点或独立节点备份数据。可以从 CLI 或用户界面完成备份。

思科 ISE-PIC 允许您备份以下类型的数据：

- 配置数据 - 包含应用特定和思科 ADE 操作系统配置数据。
- 运行数据 - 包含监控和故障排除数据。

## 备份和恢复存储库

思科 ISE-PIC 允许您创建和删除存储库。您可以创建以下类型的存储库：

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

您可以为使用 KVM 创建的虚拟 CD-ROM，创建类型为 CD-ROM 的存储库。



**注释** 存储库位于每台设备本地位置。



注释

我们建议您为小型部署（100 个终端以下）创建 10 GB 大小的存储库，为中型部署创建 100 GB 大小的存储库，为大型部署创建 200 GB 大小的存储库。

## 创建存储库

可以使用 CLI 和 GUI 创建存储库。由于以下原因，我们建议您使用 GUI：

- 通过 CLI 创建的存储库保存在本地且不会被复制到其他部署节点。这些存储库不会列于 GUI 的存储库页面。
- 在主 PAN 创建的存储库会被复制到其他部署节点。

在 GUI 中，密钥仅在主 PAN 上生成，因此在升级期间，需要新的主管理节点的 GUI 中再次生成密钥，并将其导出到 SFTP 服务器。如果从部署中删除节点，需要在非管理节点的 GUI 中生成密钥，并将其导出到 SFTP 服务器。

可以在思科 ISE-PIC 中凭借 RSA 公共密钥身份验证配置 SFTP 存储库。您可以选择使用安全密钥的 RSA 公共密钥身份验证来加密数据库和日志，而不必使用管理员创建的密码。对于通过 RSA 公共密钥创建的 SFTP 存储库，在 GUI 中创建的存储库不会在 CLI 中复制，在 CLI 中创建的存储库也不会再在 GUI 中复制。要在 CLI 和 GUI 中配置相同存储库，请在 CLI 和 GUI 中生成 RSA 公共密钥，并将密钥输出到 SFTP 服务器。



注释

即使未在 ISE 上启用 FIPS 模式，思科 ISE 也会在 FIPS 模式下启动出站 SSH 或 SFTP 连接。确保与 ISE 通信的远程 SSH 或 SFTP 服务器允许 FIPS 140 批准的加密算法。

思科 ISE 使用嵌入式 FIPS 140 验证加密模块。有关 FIPS 合规要求的详细信息，请参阅 [FIPS 合规证明](#) 书。

### 开始之前

- 如果要使用 RSA 公共密钥身份验证创建 SFTP 存储库，请执行以下步骤：
  - 在 SFTP 存储库中启用 RSA 公共密钥身份验证。
  - 从思科 ISE CLI 使用 **crypto host\_key add** 命令输入 SFTP 服务器的主机密钥。主机密钥字符串应当与您在存储库配置页面的 **路径 (Path)** 字段中输入的主机名匹配。
  - 生成密钥对，并从 GUI 将公共密钥导出到您的本地系统。在思科 ISE CLI 中，使用 **crypto key generate rsa passphrase test123** 命令生成密钥对，其中 **passphrase** 必须超过 13 个字母，然后将密钥导出到任何存储库（本地磁盘或任何其他配置的存储库）。
  - 将导出的 RSA 公共密钥复制到启用 PKI 的 SFTP 服务器并将其添加到 “**authorized\_keys**” 文件。



**注释** 当主 PAN 和主 MnT 是独立的节点时，您可以使用**存储库列表 (Repository List)** 窗口中的**生成密钥对 (Generate Key Pairs)** 选项来为主 PAN 和主 MnT 节点生成 RSA 密钥。您可以使用**存储库列表 (Repository List)** 窗口中的**导出公共密钥 (Export Public Key)** 选项来同时从主 PAN 和主 MnT 节点导出生成的 RSA 密钥。

**步骤 1** 选择**管理 (Administration) > 维护 (Maintenance) > 存储库 (Repository)**。

**步骤 2** 单击**添加 (Add)** 以添加新存储库。

**步骤 3** 根据需要输入值以设置新存储库。请参阅 [存储库设置](#)，第 114 页 以了解字段说明：

**步骤 4** 单击**提交 (Submit)** 以创建存储库。

**步骤 5** 通过单击左侧**操作 (Operations)** 导航窗格中的**存储库 (Repository)** 来验证是否成功创建存储库，或单击**存储库 (Repository)** 窗口顶部的**存储库列表 (Repository List)** 链接以转至存储库列表页面。

#### 下一步做什么

- 确保已创建的存储库有效。可以从**存储库列表 (Repository listing)** 窗口执行此操作。选择对应存储库并单击**验证 (Validate)**。或者，您可以从思科 ISE 命令行界面执行以下命令：

```
show repository repository_name
```

其中 *repository\_name* 是已创建的存储库的名称。



**注释** 如果在创建存储库时提供的路径不存在，则会收到以下错误消息：

```
%Invalid Directory
```

- 运行**按需备份或安排备份**。

## 存储库设置

下表介绍了**存储库列表 (Repository List)** 窗口上的字段，可以使用此页面创建存储备份文件的存储库。要查看此处窗口，请单击**菜单** 图标 (☰)，然后选择**管理 (Administration) > 维护 (Maintenance) > 存储库 (Repository)**。

表 21: 存储库设置

字段	使用指南
存储库 (Repository)	输入存储库的名称。允许使用字母数字字符，最大长度为 80 个字符。

字段	使用指南
协议 (Protocol)	从可用协议中选择一个您想要使用的协议。
主机 (Host)	<p>(对于 TFTP、HTTP、HTTPS、FTP、SFTP 和 NFS 为必填字段) 输入您想要在其上创存储库的服务器的主机名或 IP 地址 (IPv4 或 IPv6)。</p> <p><b>注释</b> 如果要添加具有 IPv6 地址的存储库, 请确保 ISE eth0 接口已配置有 IPv6 地址。</p>
路径 (Path)	<p>输入存储库的路径。此路径必须有效而且在您创建数据库时必须存在。</p> <p>请注意, 某些特殊字符 (如 !、?、~ (不包括在上面的列表中) 允许通过 GUI 配置 FTP 和 SFTP 密码。但是, 这些特殊字符不允许通过 CLI 或开放式 API 进行配置。</p>

#### 相关主题

[备份和恢复存储库](#)  
[创建存储库](#), 第 113 页

## 在 SFTP 存储库中启用 RSA 公共密钥身份验证

在 SFTP 服务器中, 每个节点必须具有两个 RSA 公共密钥, 一个用于 CLI, 一个用于 GUI。要在 SFTP 存储库中启用 RSA 公共密钥身份验证, 请执行以下步骤:



**注释** 在 SFTP 存储库中启用 RSA 公共密钥身份验证后, 您将无法使用 SFTP 凭证登录。您可以使用基于 PKI 的身份验证或基于凭证的身份验证。如果要再次使用基于凭证的身份验证, 则必须从 SFTP 服务器中删除公共密钥对。

**步骤 1** 用有权限编辑 `/etc/ssh/sshd_config` 的帐户登录 SFTP 服务器。

**注释** `sshd_config` 文件的位置可能根据操作系统安装而有所不同。

**步骤 2** 输入 `vi /etc/ssh/sshd_config` 命令。

系统列出 `sshd_config` 文件的内容。

**步骤 3** 从以下行中删除 “#” 符号以启用 RSA 公共密钥身份验证:

- `RSAAuthentication` 是
- `PubkeyAuthentication` 是

注释 如果公共身份验证密钥为 no，则将其更改为 yes。

- AuthorizedKeysFile ~/.ssh/authorized\_keys

---

## 按需备份和计划备份

您可以配置主 PAN 的按需备份。当您希望立即备份数据时，系统会执行按需备份。

您可以安排一次性、每日、每周或每月运行系统级备份。由于备份操作持续时间较长，您可以将备份操作安排在空闲时间执行。您可以从管理门户安排备份。



---

注释 如果使用的是内部 CA，应使用 CLI 导出证书和密钥。在管理门户中使用的备份不会备份 CA 链。有关详细信息，请参阅《思科身份识别服务引擎管理员指南》的“基本设置”一章中的“导出思科 ISE CA 证书和密钥”部分。

---



---

注释 思科 ISE 上的配置和操作备份可能会在短时间内使系统过载。这种预期的临时系统过载行为将取决于系统的配置和监控数据库大小。

---

### 执行按需备份

可以执行按需备份以立即备份配置或监控（操作）数据。恢复操作可将思科 ISE-PIC 恢复到获取备份时的配置状态。

**重要事项**

当执行备份和恢复时，恢复功能会使用源系统中的证书列表覆盖目标系统上的受信任证书列表。需要注意的是，备份和恢复功能不包括与内部证书颁发机构(CA)证书关联的专用密钥，这一点至关重要。

如果正在从一个系统向另一个系统上执行备份和恢复，必须选择下面一个选项以避免错误：

**• 选项 1:**

通过 CLI 从源 ISE-PIC 节点导出 CA 证书并通过 CLI 将其导入到目标系统。

**优点：**从源系统向终端颁发的所有证书将继续受信任。由目标系统颁发的所有新证书将由同一密钥签名。

**缺点：**在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

**• 选项 2:**

在恢复过程之后，为内部 CA 生成所有新证书。

**优点：**推荐采用此选项，这是一种较为安全的方法，其中将使用原始源证书或原始目标证书。由原始源系统颁发的证书将继续受信任。

**缺点：**在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

**开始之前**

- 在执行按需备份之前，应对思科 ISE-PIC 中的备份数据类型有基本的了解。
- 确保已创建存储备份文件的存储库。
- 不要使用本地存储库进行备份。

**步骤 1** 在 ISE-PIC GUI 中，单击菜单图标 (☰)，然后选择管理 (Administration) > 维护 (Maintenance) > 备份和恢复 (Backup and Restore)。

**步骤 2** 选择备份类型：“配置” (Configuration) 或 “运行” (Operational)。

**步骤 3** 单击立即备份 (Backup Now)。

**步骤 4** 根据需要输入值以执行备份。

**步骤 5** 单击 备份 (Backup)。

**步骤 6** 验证备份是否成功完成。

思科 ISE-PIC 在备份文件名中附加时间戳并将文件存储在指定存储库中。除了时间戳外，思科 ISE-PIC 会为配置备份添加 CFG 标签，为运行备份添加 OPS 标签。确保备份文件位于指定的存储库中。

备份正在运行时，请勿升级节点。如果并发运行备份，这将关闭所有进程并可能导致数据不一致。在进行任何节点更改之前，请等待备份完成。

**注释** 备份正在运行时，可能会看到 CPU 使用率高并收到平均负载高的警报。备份完成时，CPU 使用率将恢复正常。

## 计划备份

可以执行按需备份以立即备份配置或监控（操作）数据。恢复操作可将思科 ISE-PIC 恢复到获取备份时的配置状态。



**重要事项** 当执行备份和恢复时，恢复功能会使用源系统中的证书列表覆盖目标系统上的受信任证书列表。需要注意的是，备份和恢复功能不包括与内部证书颁发机构 (CA) 证书关联的专用密钥，这一点至关重要。

如果您正在从一个系统向另一个系统上执行备份和恢复，您将必须选择下面一个选项以避免错误：

• **选项 1:**

通过 CLI 从源 ISE-PIC 节点导出 CA 证书并通过 CLI 将其导入到目标系统。

**优点:** 从源系统向终端颁发的所有证书将继续受信任。由目标系统颁发的所有新证书将由同一密钥签名。

**缺点:** 在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

• **选项 2:**

在恢复过程之后，为内部 CA 生成所有新证书。

**优点:** 推荐采用此选项，这是一种较为安全的方法，其中将使用原始源证书或原始目标证书。由原始源系统发布的证书将继续受信任。

**缺点:** 在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

### 开始之前

- 在安排备份之前，应对思科 ISE-PIC 中的备份数据类型有基本的了解。
- 确保已配置存储库。
- 不要使用本地存储库进行备份。



**注释** 对于备份和恢复操作，系统不支持以下存储库类型：CD-ROM、HTTP、HTTPS 或 TFTP。这是因为，这些存储库类型为只读或者协议不支持文件列表。



## 使用 CLI 备份

虽然可以从 CLI 和 GUI 安排备份，但是建议使用 GUI。不过，只能从 CLI 对辅助监控节点执行操作备份。

## 备份历史记录

备份历史记录提供关于定时备份和按需备份的基本信息。它会列出备份名称、备份文件大小、存储备份的库以及指明获得备份的时间的时间戳。此信息在操作审核报告以及历史记录表的 Backup and Restore 页面上列出。

对于故障备份，思科 ISE-PIC 将触发警报。备份历史记录页面提供故障原因。操作审核报告也引用故障原因。如果故障原因缺失或不清楚，您可以从思科 ISE CLI 运行 **backup-logs** 命令，查看 ADE.log 了解更多信息。

在备份操作运行的过程中，您可以使用 **show backup status** CLI 命令查看备份操作的进度。

备份历史记录与思科 ADE 操作系统配置数据一起存储。甚至在应用升级后历史记录依然存在，只有当您重置 PAN 映像时才能将历史记录删除。

## 备份失败

如果备份失败，请检查以下事宜：

- 检查是否存在任何 NTP 同步或服务失败问题。如果思科 ISE 上的 NTP 服务无效，思科 ISE 将发出 NTP 服务失败警报。当思科 ISE 无法与所有配置的 NTP 服务器同步时，思科 ISE 会发出 NTP 同步失败警报。如果 NTP 服务停止或有任何同步问题，思科 ISE 备份可能会失败。检查“警报” (Alarms) Dashlet 并修复 NTP 同步或服务问题，然后再重试备份操作。
- 确保没有同时运行任何其他备份。
- 检查已配置存储库的可用磁盘空间。
  - 如果监控数据占用的空间超过所分配的监控数据库大小的 75%，则监控（操作）备份会失败。例如，如果向节点分配的空间为 600 GB，而监控数据占用超过 450 GB 的存储空间，则监控备份会失败。
  - 如果数据库磁盘使用量超过 90%，系统会执行清除操作，使数据库的大小小于或等于所分配空间的 75%。
- 验证是否正在进行清除。进行清除时，备份和恢复操作不起作用。
- 验证存储库的配置是否正确。

## 思科 ISE 恢复操作

可以在主节点或独立管理节点上恢复配置数据。在主 PAN 上恢复数据后，必须手动将辅助节点与主 PAN 同步。



**注释** 思科 ISE-PIC 中新的备份/恢复用户界面利用备份文件名中的元数据。因此，在备份完成后，不应手动修改备份文件名。如果手动修改备份文件名，则思科 ISE-PIC 备份/恢复用户界面将无法识别备份文件。如果必须修改备份文件名，应使用思科 ISE CLI 恢复备份。

## 数据恢复指南

下面提供了恢复思科 ISE-PIC 备份数据时应遵守的指南。

- 利用思科 ISE，您可以从 ISE 节点 (A) 获取备份并将其存储到另一个 ISE 节点 (B) 上，这两个节点有相同的主机名（但 IP 地址不同）。但是，当您在节点 B 上恢复备份后，不会更改节点 B 的主机名，因为这样做可能会导致证书和门户组标记出现问题。
- 如果在一个时区内从主 PAN 获取备份，并尝试在另一时区中的另一个思科 ISE-PIC 节点上恢复该备份，恢复过程可能失败。如果备份文件中的时间戳晚于恢复备份所在的思科 ISE-PIC 节点上的系统时间，则会发生此故障。如果在获得备份之后一天恢复备份，那么备份文件中的时间戳则为过去时间，恢复过程将成功。
- 当主 PAN 上恢复的备份所使用的主机名不同于获得备份的主机名时，此主 PAN 将成为独立节点。部署已损坏，辅节点将无法运行。您必须使独立节点成为主节点，重置辅节点上的配置，并在主节点上重新注册这些辅节点。要重置思科 ISE-PIC 节点上的配置，请从思科 ISE CLI 输入以下命令：

- **application reset-config ise**

- 建议您在初始思科 ISE-PIC 安装和设置之后，不要更改系统时区。
- 如果更改了部署中的一个或多个节点上的证书配置，则必须获得另一个备份才能从独立思科 ISE-PIC 节点或主 PAN 恢复数据。否则，如果您尝试使用旧备份恢复数据，节点之间的通信可能失败。
- 在主 PAN 上恢复配置备份后，可以导入先前导出的思科 ISE CA 证书和密钥。



**注释** 如果没有导出思科 ISE CA 证书和密钥，则主 PAN 上恢复配置备份后，在主 PAN 上生成根 CA 和从属 CA。

- 如果尝试恢复白金级数据库而没有使用正确的 FQDN（白金级数据库的 FQDN），则需要重新生成 CA 证书。（要查看此处窗口，请单击菜单图标 (☰)，然后选择 **管理 (Administration) > 证书 (Certificates) > 证书签名请求 (Certificate Signing Requests) > 更换 ISE 根 CA 证书链 (Replace ISE Root CA certificate chain)**）。不过，如果使用正确的 FQDN 恢复白金级数据库，请注意 CA 证书将自动重新注册。
- 需要一个数据存储库，供思科 ISE-PIC 保存备份文件。您必须创建一个存储库，然后才能运行按需备份或定期备份。
- 如果有一个独立节点发生故障，则必须运行配置备份进行恢复。如果主 PAN 发生故障，则可以，将辅助管理节点升级为主管理节点。实现之后，可以在主 PAN 上恢复数据。



**注 释** 思科 ISE-PIC 还提供 **backup-logs** CLI 命令，可用于收集日志和配置文件以用于故障排除。

## 从 CLI 恢复配置或监控（操作）备份

要通过思科 ISE CLI 恢复配置数据，请在执行模式下使用 **restore** 命令。使用以下命令从配置或操作备份恢复数据：

**restore filename repository repository-name encryption-key hash|plain encryption-key name include-adeos**

语法说明

<b>restore</b>	键入此命令，从配置或操作备份恢复数据。
<i>filename</i>	驻留在存储库的备份文件的名称。最多支持 120 个字母数字字符。 <b>注释</b> 必须在文件名后面添加 .tar.gpg 扩展名（例如，myfile.tar.gpg）。
<b>repository</b>	指定包含备份的存储库。
<i>repository-name</i>	您想要从其恢复备份的存储库的名称。
<b>encryption-key</b>	（可选）指定用户定义的加密密钥以恢复备份。
<b>hash</b>	恢复备份的散列加密密钥。指定跟随的加密（散列）加密密钥。最多支持 40 个字符。
<b>plain</b>	用于恢复备份的明文加密密钥。指定跟随的未加密密文加密密钥。最多支持 15 个字符。
<i>encryption-key name</i>	输入加密密钥。
<b>include-adeos</b>	（可选，仅适用于配置备份）如果您想要从配置备份恢复 ADE-OS 配置，请输入此命令运算符参数。当您恢复配置备份，如果不包含此参数，思科 ISE 仅恢复思科 ISE 应用配置数据。

### 默认值

无默认行为或值。

### 命令模式

EXEC

## 使用指南

在思科 ISE-PIC 中使用 `restore` 命令时，思科 ISE-PIC 服务器会自动重新启动。

恢复数据时，加密密钥为可选。要在您未提供加密密钥的情况下，支持恢复更早的备份，您可以使用 `restore` 命令，无需加密密钥。

## 示例

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key plain
Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore. Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

## 相关命令

	说明
<b>backup</b>	执行备份（思科 ISE-PIC 和思科 ADE OS），将备份放在存储库中。
<b>backup-logs</b>	备份系统日志。
<b>repository</b>	输入备份配置的存储库子模式。
<b>show repository</b>	显示位于特定存储库上的可用备份文件。
<b>show backup history</b>	显示系统的备份历史记录。
<b>show backup status</b>	显示备份操作的状态。
<b>show restore status</b>	显示恢复操作的状态。

如果任何辅助节点的应用恢复后同步状态和复制状态为不同步 (*Out of Sync*)，则必须将此辅助节点的证书重新导入主 PAN，执行手动同步。

## 从 GUI 恢复配置备份

可以从管理门户恢复配置备份。GUI 只列出从当前版本提取的备份。要恢复此版本之前的备份，请从 CLI 使用恢复命令。

**步骤 1** 选择管理 (**Administration**) > 维护 (**Maintenance**) > 备份和恢复 (**Backup and Restore**)。

**步骤 2** 从配置备份列表中选择备份名称，然后单击恢复 (**Restore**)。

**步骤 3** 输入在备份过程中使用的加密密钥。

**步骤 4** 单击恢复 (**Restore**)。

### 下一步做什么

如果使用思科 ISE CA 服务，必须：

1. 重新生成整个思科 ISE CA 根链。
2. 从主 PAN 获取思科 ISE CA 证书和密钥的备份，然后在辅助 PAN 上恢复备份。这样确保了辅助 PAN 可以在主 PAN 故障时用作外部 PKI 的根 CA 或从属 CA，您可将辅助 PAN 升级为主 PAN。

## 恢复历史记录

可以从操作审核报告 (**Operations Audit Report**) 中获取所有恢复操作、日志事件和状态的相关信息。



**注释** 但操作审核报告 (**Operations Audit Report**) 窗口不提供与之前的恢复操作对应的起始时间的相关信息。

要获得故障排除信息，必须从思科 ISE CLI 运行 **backup-logs** 命令并查看 ADE.log 文件。

在恢复操作进行过程中，所有思科 ISE-PIC 服务都会停止。可以使用 CLI 命令 **show restore status** 查看恢复操作的进度。

## 同步主节点和辅助节点

在 PAN 上恢复备份文件之后，主节点和辅助节点中的思科 ISE-PIC 数据库有时不会自动同步。如果发生这种情况，可以手动强制从 PAN 完全复制到辅助 ISE-PIC 节点。只能强制从 PAN 同步到辅助节点。在同步操作过程中，无法进行任何配置更改。通过思科 ISE-PIC，只能在同步完成后导航至其他思科 ISE-PIC 管理员门户页面和进行配置更改。

**步骤 1** 选择管理 (**Administration**) > 部署 (**Deployment**)。

**步骤 2** 选中处于不同步复制状态的辅助节点旁边的复选框。

**步骤 3** 单击同步 (**Syncup**)，等到节点与 PAN 同步。必须等到此流程完成，然后才能再次访问思科 ISE-PIC 管理员门户。

## 恢复独立和两节点部署中断开的节点

此部分提供可用于恢复独立和两节点部署中断开的节点的故障排除信息。以下某些用例使用备份和恢复功能，而其他用例则使用复制功能恢复已丢失的数据。

### 使用现有 IP 地址和主机名恢复两节点部署中断开连接的节点

#### 场景

在两节点部署中，一场自然灾害导致丢失了所有节点。在恢复之后，您想要使用现有 IP 地址和主机名。

例如，您有两个节点：N1（主策略管理节点，即主 PAN）和 N2（辅助策略管理节点，即辅助 PAN）。可提供在时间 T1 执行的 N1 节点的备份。后来，由于自然灾害，N1 和 N2 节点都出现了故障。

#### 假定条件

部署中的所有思科 ISE-PIC 节点都已被破坏。已使用相同的主机名和 IP 地址对新硬件进行映像。

#### 解决步骤

1. 您必须更换 N1 和 N2 节点。N1 和 N2 节点现在具有独立配置。
2. 用 N1 和 N2 节点的 UDI 获取许可证并将其安装在 N1 节点上。
3. 然后，您必须在更换的 N1 节点上恢复备份。恢复脚本将尝试在 N2 上同步数据，但是，N2 现已成为独立节点，所以同步失败。N1 上的数据将重置至时间 T1。
4. 您必须登录 N1 Admin 门户以删除和重新注册 N2 节点。N1 和 N2 节点都将使数据重置至时间 T1。

### 使用新 IP 地址和主机名恢复两节点部署中断开的节点

#### 场景

在两节点部署中，一场自然灾害导致丢失了所有节点。新硬件在新位置进行了重新镜像并且需要新的 IP 地址和主机名。

例如，您有两个 ISE-PIC 节点：N1（主策略管理节点，即主 PAN）和 N2（辅助节点）。系统可以提供在时间 T1 执行的 N1 节点备份。后来，由于自然灾害，N1 和 N2 节点都出现了故障。思科 ISE-PIC 节点在新位置被替换，新主机名为 N1A（主 PAN）和 N2A（辅助节点）。此处 N1A 和 N2A 都是独立节点。

#### 假定条件

部署中的所有思科 ISE-PIC 节点都已被破坏。新硬件已使用不同的主机名和 IP 地址在另一位置进行镜像。

### 解决步骤

1. 获取 N1 备份并在 N1A 上恢复此备份。恢复脚本将识别主机名更改和域名更改，并且将根据当前主机名在部署配置中更新主机名和域名。
2. 您必须生成新的自签证书。
3. 删除旧 N2 节点。

将新 N2A 节点注册为辅助节点。系统会将 N1A 节点的数据复制到 N2A 节点。

## 使用现有 IP 地址和主机名恢复独立部署中的节点

### 场景

独立管理节点出现故障。

例如，您有一个独立管理节点 N1。已在时间 T1 执行 N1 数据库的备份。N1 节点由于物理故障宕机，必须重置映像此节点或需要使用新的硬件。必须以相同的 IP 地址和主机名恢复 N1 节点。

### 假定条件

此部署是独立部署，而且新硬件或重置映像的硬件具有相同的 IP 地址和主机名。

### 解决步骤

N1 节点在重置映像或您采用具有相同 IP 地址和主机名的新思科 ISE-PIC 节点后开始运行时，您必须从旧 N1 节点恢复备份。您无需执行任何角色变更。

## 使用新 IP 地址和主机名恢复独立部署中的节点

### 场景

独立管理节点出现故障。

例如，您有一个独立管理节点 N1。系统可以提供在时间 T1 执行的 N1 数据库备份。N1 节点由于物理故障而宕机，此节点更换为另一位置具有不同 IP 地址和主机名的新硬件。

### 假定条件

这是独立部署，并且所更换的硬件具有不同的 IP 地址和主机名。

### 解决步骤

1. 使用新硬件更换 N1 节点。此节点将处于独立状态，主机名为 N1B。
2. 您可以在 N1B 节点恢复备份。不需要更改角色。

## 配置回滚

### 问题

有时候，您可能会不小心更改配置，然后您发现所做的更改不正确。在这种情况下，可以通过恢复您在进行更改之前所做的备份，恢复原来的配置。

### 可能的原因

有两个节点：N1（主策略管理节点，即主 PAN）和 N2（辅助策略管理节点，即辅助 PAN），并且可提供 N1 节点的备份。您在 N1 节点上做了一些错误的配置更改并且想要撤消更改。

### 解决方案

获取在执行错误的配置更改之前所执行的 N1 节点备份。在 N1 节点上恢复此备份。恢复脚本会将数据从 N1 同步至 N2。

## 在两节点部署出现故障的情况下恢复主节点

### 场景

在多节点部署中，PAN 出现故障。

例如，您有两个思科 ISE-PIC 节点：N1 (PAN) 和 N2（辅助管理节点）。由于硬件问题，N1 出现了故障。

### 假定条件

仅两节点部署中的主节点出现故障。

### 解决步骤

1. 登录 N2 管理员门户。在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择，并将 N2 配置为主节点。

使用新硬件更换 N1 节点，重新镜像此节点并使之处于独立状态。

2. 从 N2 管理员门户，将新的 N1 节点注册为辅助节点。

现在，N2 节点就成为您的主要节点，而 N1 节点则成为您的辅助节点。

如果您希望重新将 N1 节点设置为主要节点，请登录 N1 Admin 门户并将其设置为主要节点。N2 就自动成为辅助服务器。不会有数据丢失。

## 在两节点部署出现故障的情况下恢复辅助节点

### 场景

在多节点部署中，一个辅助节点出现故障。无需恢复。



### 解决步骤

1. 将辅助节点重新映像到默认独立状态。
2. 从主节点登录管理员门户并删除辅助节点。
3. 重新注册辅助节点。  
数据从主节点复制到辅助节点。无需恢复。

## 数据库清除

清除过程允许您通过以月为单位指定在清除期间保留数据的时间，管理数据库的大小。默认值为三个月。当达到清除流程的磁盘空间使用率阈值（占磁盘空间的百分比）时，会用到此值。对于该选项，每月包括 30 天。三个月的默认值等于 90 天。

### 清除数据库指南

遵循这些与数据库磁盘使用量相关的最佳指南：

- 如果数据库磁盘使用量超过 80% 的阈值设置，则会生成严重警报，表示数据库大小已超过所分配的磁盘容量。如果磁盘使用量超过百分之九十，则会生成另一个警报。
- 清除同样依据数据库已使用的磁盘空间。当数据库已使用的磁盘空间达到或超过阈值时（默认为 80%），则会启动清除过程。此过程仅删除最近七天的监控数据，不论在管理员门户中进行了怎样的配置。系统将循环继续此过程直至磁盘空间使用量低于百分之八十。系统总会在检查数据库磁盘空间限制之后，才继续执行清除。

### 运营数据清除

思科 ISE 监控操作数据库包含作为思科 ISE 报告生成的信息。在思科 ISE 最新版本中，可以选择在运行思科 ISE 管理 **application configure ise CLI** 命令后清除监控操作数据并重置监控数据库。

清除选项用于清除数据，并会提示输入数据的保留天数。重置选项用于将数据库重置为出厂默认设置，这将永久删除所有备份的数据。如果文件占用了文件系统的过多空间，可指定数据库。



**注释** 重置选项会导致思科 ISE 服务在系统完成重启前暂时不可用。

### 相关主题

[清除较旧的运营数据](#)，第 127 页

### 清除较旧的运营数据

运营数据在一段时间内收集到服务器上。可以立即或定期清除它。

**步骤 1** 选择管理 (Administration) > 维护 (Maintenance) > 操作数据清除 (Operational Data Purging)。

**步骤 2** 执行以下操作之一：

- 在**数据保留期 (Data Retention Period)** 区域:
  1. 以日为单位指定 RADIUS 和 TACACS 数据的应保留期限。指定期限之前的所有数据都会导出到存储库。虽然 ISE-PIC 不提供 RADIUS 或 TACACS 功能，但与思科 ISE 共享某些基础设施，因此可能需要定期从数据库清除此类信息。
  2. 在**存储库 (Repository)** 区域中，选中**启用导出存储库 (Enable Export Repository)** 复选框以选择保存数据的存储库。
  3. 在**加密密钥 (Encryption Key)** 字段中，输入所需的密码。
  4. 单击**保存 (Save)**。
 

**注释** 如果配置的保留期限短于与诊断数据对应的现有保留阈值，则配置值将覆盖现有阈值。例如，如果将保留期配置为三天，而且该值小于诊断表中的现有阈值（例如，默认值为五天），则将根据在此窗口中配置的值（三天）清除数据。
  
- 在**立即清除数据 (Purge Data Now)** 区域:
  1. 选择清除所有数据或清除超过指定天数的数据。数据不会保存在任何存储库中。
  2. 单击**清除 (Purge)**。

## 将 ISE-PIC 升级到完整 ISE 安装

思科 ISE-PIC 基于完整思科 ISE GUI 显示在简单的用户直观 GUI 中。因此，通过安装 ISE-PIC，您可以快速高效地轻松升级到 ISE。从 ISE-PIC 升级到 ISE 的基本版许可证时，ISE 继续提供在升级之前 ISE-PIC 中可供您使用的所有功能，如果您使用已升级的 ISE-PIC 节点作为主 PAN，则无需重新配置已配置的任何设置。



**注释** 如果您不使用现有已升级的 ISE-PIC 节点作为主 PAN，则升级时将清除该节点上的数据，并且您将能够从新添加的节点访问现有完整 ISE 部署中的数据。

有关升级到 ISE 的优势的详细信息，请参阅[比较 ISE-PIC 与 ISE 和 CDA](#)，第 5 页。

## 通过注册许可证升级到 ISE

### 开始之前

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。

有关许可模型的详细信息，请参阅[ISE-PIC 智能许可](#)，第 10 页

- 
- 步骤 1** 如果已安装辅助节点，请在思科 ISE-PIC 主节点安装中，选择**管理 (Administration) > 部署 (Deployment)**，并取消注册辅助节点。两个节点随后都将成为主节点，并且其中一个节点可以升级。
- 步骤 2** 选择**管理 (Administration) > 许可 (Licensing)**。
- 步骤 3** 单击**导入许可证 (Import License)**。
- 步骤 4** 单击**选择文件 (Choose File)**，浏览升级许可证文件，然后单击**确定 (OK)**。
- 步骤 5** **注释** 如果将此 ISE-PIC 节点添加到现有 ISE 部署，则完成此步骤后即已完成升级，现在可以从此部署中的主节点注册此节点来添加此节点。有关详细信息，请参阅<https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html>《思科身份识别服务引擎管理员指南》。

在导入新许可证文件 (**Import New License File**) 屏幕中，单击**导入 (Import)**。

- 步骤 6** 要使此升级节点成为完整 ISE 部署中的主节点，请立即导入基本版许可证。再次单击**导入许可证 (Import License)**。
- 步骤 7** 单击**选择文件 (Choose File)**，浏览思科代表提供的许可证，然后单击**确定 (OK)**。
- 步骤 8** 在导入新许可证文件 (**Import New License File**) 屏幕中，单击**导入 (Import)**。
- 步骤 9** 单击**确定 (OK)**。  
升级为 ISE 主节点的过程将开始，并显示以下消息：“此节点现在正在后台中升级到 ISE。请等待几分钟，然后登录 ISE。” (*This node is now being upgraded to ISE in the background. Please wait several minutes and then log in to ISE.*)
- 步骤 10** 单击**确定 (OK)**。

几分钟后，将显示登录屏幕。重新登录并访问基本版许可证安装提供的所有菜单。

您现在已将主 ISE-PIC 节点升级为完整 ISE 安装中的主节点，以前的辅助节点现在是 ISE-PIC 独立安装中的主节点和唯一节点。现在可以使用相同方式单独升级最后一个 ISE-PIC 节点。

---

## 管理设置 ISE-PIC

### 基于角色的访问控制

思科 ISE-PIC 允许您定义基于角色的访问控制 (RBAC) 策略，以允许或拒绝向管理员授予某些系统操作权限。这些 RBAC 策略根据单个管理员或管理员所属管理员组的身份定义。

要进一步提高访问 Admin 门户的用户的安全和控制，您可以执行以下操作：

- 根据远程客户端的 IP 地址配置管理访问设置。
- 为管理帐户定义强密码策略。
- 为管理 GUI 会话配置会话超时。

## 思科 ISE-PIC 管理员

管理员可使用管理员门户执行下列操作：

- 管理部署节点监控和故障排除。
- 管理思科 ISE-PIC 服务管理员帐户以及系统配置和操作。
- 更改管理员和用户密码。

CLI 管理员可以启动和停止思科 ISE 应用、应用软件补丁和升级、重新加载或关闭思科 ISE 设备，以及查看所有系统和应用日志。由于授予 CLI 管理员的特殊权限，建议您保护 CLI 管理员凭证并创建基于 Web 的管理员来配置和管理思科 ISE 部署。

在设置过程中配置的用户名和密码仅用于对 CLI 进行管理访问。此角色被视为 CLI 管理员用户，也称为 CLI 管理员。默认情况下，CLI 管理员用户的用户名为 `admin`，密码是设置过程中定义的密码。没有默认密码。此 CLI 管理员用户是默认管理员用户，无法删除此用户帐户。不过，其他管理员可以编辑此用户帐户，包括启用、禁用相关帐户或者更改其密码。

可以创建管理员，也可以将现有用户升级为管理员角色。通过禁用对应的管理权限，还可以将管理员降级为简单网络用户状态。

管理员是具有配置和操作思科 ISE-PIC 系统的本地权限的用户。

管理员会分配到一个或多个管理员组。方便起见，这些管理员组已在系统中预定义，如以下部分所述。

### 相关主题

[思科 ISE-PIC 管理员组](#)，第 130 页

## 思科 ISE-PIC 管理员组

管理员组是思科 ISE 中基于角色的访问控制（RBAC）组。ISE-PIC 属于同一组的所有管理员共用同一身份并且具有相同的权限。管理员作为特定管理组成员的身份可用作授权策略中的条件。管理员可以属于不止一个管理员组。

具有任何访问权限级别的管理员帐户可以在其有权访问的任何窗口上，修改或删除其拥有权限的对象。

下表列出了思科 ISE-PIC 中预定义的管理组以及这些组成员可以执行的任务。只有这些预定义的组才能定义系统中的管理员用户。

表 22: 思科 ISE 管理员组、访问级别、权限和限制

管理组角色	访问级别	权限	限制
超级管理员	所有思科 ISE-PIC 管理功能。默认管理员帐户属于此组。	对所有思科 ISE-PIC 资源拥有创建、读取、更新、删除和执行 (CRUDX) 权限。	

管理组角色	访问级别	权限	限制
外部 RESTful 服务 (ERS) 管理员	对所有 ERS API 请求 (GET、POST、DELETE、PUT) 的完全访问权限	<ul style="list-style-type: none"> <li>创建、读取、更新和删除 ERS API 请求</li> </ul>	此角色仅适用于支持内部用户、身份组和终端的 ERS 授权

## CLI 管理员与基于 Web 管理员的权限对比

CLI 管理员可以启动和停止思科 ISE-PIC 应用、应用软件补丁和升级、重新加载或关闭思科 ISE-PIC 设备，以及查看所有系统和应用日志。由于授予 CLI 管理员的特殊权限，我们建议您保护 CLI 管理员凭证并创建基于 Web 的管理员来配置和管理思科 ISE-PIC 部署。

## 创建新管理员

思科 ISE-PIC 管理员需要分配有特定角色的帐户才能执行特定管理任务。您可以创建多个管理员帐户，并根据管理员必须执行的管理任务向这些管理员分配一个或多个角色。

使用管理员用户 (Admin Users) 窗口查看、创建、修改、删除、复制或搜索思科 ISE-PIC 管理员的属性或更改其状态。



**注释** 如果管理员用户的域在 CLI 和 GUI 中相同，建议您先在 CLI 中配置 Active Directory 访问权限，然后再将其加入 GUI。另外，必须从 GUI 重新加入域，以避免此域发生身份验证失败。

**步骤 1** 选择管理 (Administration) > 管理员访问权限 (Admin Access) > 管理员用户 (Admin Users) > 添加 (Add) > 创建管理员用户 (Create an Admin User)。

**步骤 2** 在字段中输入值。名称 (Name) 字段支持的字符为 # \$ ' ( ) \* + - . / @ \_。

管理员用户名必须唯一。如果输入了现有用户名，错误弹出窗口将显示以下消息：

```
User can't be created. A User with that name already exists.
```

**步骤 3** 单击提交 (Submit) 在思科 ISE-PIC 内部数据库中创建新管理员。

### 相关主题

[只读管理员策略](#)

[自定义只读管理员的菜单访问权限](#)

## 对思科 ISE-PIC 进行管理访问

思科 ISE-PIC 管理员可以根据其所属的管理组执行各种管理任务。这些管理任务至关重要。仅向有权在网络中管理思科 ISE-PIC 的用户授予管理访问权限。

利用思科 ISE-PIC，您可以通过此处介绍的选项来控制对其 Web 界面的管理访问。。



**注释** 当将思科 ISE 服务器添加到网络时，一旦其 Web 界面出现，它就会被标记为处于运行状态。但是，由于一些高级服务（如安全评估服务）可能需要更长的时间才能完全可用，因此可能需要更多时间才能使所有服务完全运行。

### 管理访问方法

有多种方式可以连接到 思科 ISE 服务器。策略管理节点 (PAN) 运行管理员门户。需要管理员密码才能登录。其他 ISE 角色服务器可通过 SSH 或控制台（在其中运行 CLI）进行访问。本节介绍可用于每种连接类型的进程和密码选项。

- **管理员密码：**默认情况下，安装期间创建的 思科 ISE 管理员用户在 45 天内超时。可以通过在 **管理 (Administration) > 系统 (System) > 管理设置 (Admin Settings)** 中关闭密码使用时间来防止此情况。单击**密码策略 (Password Policy)** 选项卡，并取消选中**密码有效期 (Password Lifetime)** 下的**管理密码到期 (Administrative passwords expire)** 复选框。

如果不执行此操作，当密码到期时，可以在 CLI 中运行 **application reset-passwd** 命令以重置管理员密码。要重置管理密码，可以连接至控制台以访问 CLI，或重新引导 ISE 映像文件以访问引导选项菜单。

- **CLI 密码 (CLI password)：**必须在安装期间输入 CLI 密码。如果在登录 CLI 时因密码无效而遇到问题，可以重置 CLI 密码。连接至控制台，并运行 **password CLI** 命令以重置密码。有关详细信息，请参阅《[思科身份识别服务引擎 CLI 参考指南](#)》。

•

## 管理员访问设置

思科 ISE-PIC 允许为管理员帐户定义某些规则以增强安全性。您可以限制对管理接口的访问，强制管理员使用强密码和定期更改密码等。在思科 ISE-PIC 中的“管理员帐户设置” (Administrator Account Settings) 中定义的密码策略适用于所有管理员帐户。

思科 ISE-PIC 支持包含 UTF-8 字符的管理员密码。

### 配置最大数量的并发管理会话和登录横幅

您可以配置最大数量的并发管理 GUI 或 CLI (SSH) 会话和登录横幅，它们对访问您的管理 Web 或 CLI 界面的管理员有帮助和指导作用。您可以将登录横幅配置为在管理员登录之前和登录之后显示。默认情况下，这些登录横幅处于禁用状态。

**步骤 1** 选择**管理 (Administration) > 管理员访问 (Admin Access) > 访问设置 (Access Settings) > 会话 (Session)**。

**步骤 2** 输入您要允许通过 GUI 和 CLI 界面的最大数量的并发管理会话。并发管理 GUI 会话的有效范围为 1 至 20。并发管理 CLI 会话的有效范围为 1 至 10。

**步骤 3** 如果希望思科 ISE-PIC 在管理员登录之前显示消息，请选中**登录前横幅 (Pre-login banner)** 复选框，然后在文本框中输入消息。

**步骤 4** 如果希望思科 ISE-PIC 在管理员登录之后显示消息，请选中**登录后横幅 (Post-login banner)** 复选框，然后在文本框中输入消息。

**步骤 5** 单击**保存 (Save)**。

---

### 允许从“选择 IP 地址” (Select IP Addresses) 对思科 ISE-PIC 进行管理访问

思科 ISE-PIC 允许您配置 IP 地址列表，管理员可通过列表中的 IP 地址访问思科 ISE-PIC 管理界面。

**步骤 1** 选择**管理 (Administration) > 管理员访问 (Admin Access) > 访问设置 (Access Settings) > IP 访问 (IP Access)**。

**步骤 2** 单击**仅允许列出的 IP 地址进行连接 (Allow only listed IP addresses to connect)** 单选按钮。

**注释** 端口 161 上的连接 (SNMP) 用于管理访问。但是，在配置 IP 访问限制时，如果从一个节点执行 snmpwalk 而没有为其配置管理访问，则 snmpwalk 会失败。

**步骤 3** 在配置访问限制的 **IP 列表 (Configure IP List for Access Restriction)** 区域中，单击**添加 (Add)**。

**步骤 4** 在添加 **IP CIDR (Add IP CIDR)** 对话框中，在 **IP 地址 (IP Address)** 字段中输入无类域间路由 (CIDR) 格式的 IP 地址。

**注释** 该 IP 地址可以是 IPv4 或 IPv6 地址。您可以为一个 ISE 节点配置多个 IPv6 地址。

**步骤 5** 在 **CIDR 格式的子网掩码 (Netmask in CIDR format)** 字段中输入网络掩码。

**步骤 6** 单击**确定 (OK)**。重复步骤 4-7 在此列表中添加更多 IP 地址范围。

**步骤 7** 单击**保存 (Save)** 保存所做的更改。

**步骤 8** 单击**重置 (Reset)** 以刷新 **IP 访问 (IP Access)** 窗口。

---

### 为管理员帐户配置密码策略

思科 ISE-PIC 还允许您为管理员帐户创建密码策略，以增强安全性。您在此处定义的密码策略将应用于思科 ISE-PIC 中的所有管理员帐户。



#### 注释

- 内部管理员用户的电子邮件通知将发送到 root@host。无法配置电子邮件地址，并且许多 SMTP 服务会拒绝此电子邮件。  
遵循开放缺陷 CSCui5583，此增强允许您更改电子邮件地址。
- 思科 ISE-PIC 支持包含 UTF-8 字符的管理员密码。

**步骤 1** 选择**管理 (Administration) > 管理员访问权限 (Admin Access) > 身份验证 (Authentication)**。

**步骤 2** 单击**密码策略 (Password Policy)** 选项卡并输入所需的值，以便配置思科 ISE GUI 和 CLI 密码要求。

**步骤 3** 单击**保存 (Save)** 保存管理员密码策略。

**注释** 如果在登录时使用外部身份库验证管理员的身份，请记住，即便为应用到该管理员配置文件的密码策略配置了此设置，外部身份库也仍会验证管理员的用户名和密码。

---

## 为管理员帐户配置帐户禁用策略

如果在配置连续几天内，管理员帐户没有通过身份验证，思科 ISE-PIC 允许您禁用该管理员帐户。

---

**步骤 1** 选择管理 (**Administration**) > 管理员访问 (**Admin Access**) > 身份验证 (**Authentication**) > 帐户禁用策略 (**Account Disable Policy**)。

**步骤 2** 选定在 **n** 天不活跃之后禁用帐户 (**Disable account after n days of inactivity**) 复选框，并在相应的字段中输入天数。  
如果管理员帐户在一段指定时间内处于不活跃状态，通过该选项，您可以禁用管理员帐户。

**步骤 3** 单击保存 (**Save**) 为管理员配置全局帐户禁用策略。

---

## 配置管理员会话超时

在思科 ISE-PIC 中，可以确定管理 GUI 会话处于非活动状态但仍保持连接的时间长度。可以指定思科 ISE-PIC 在注销管理员之前经过的时间（以分钟为单位）。会话超时后，管理员必须重新登录才能访问思科 ISE-PIC 管理员门户。

---

**步骤 1** 选择管理 (**Administration**) > 管理员访问权限 (**Admin Access**) > 会话设置 (**Session Settings**) > 会话超时 (**Session Timeout**)。

**步骤 2** 输入思科 ISE-PIC 在没有活动的情况下注销管理员之前需要等待的时间（以分钟为单位）。默认值为 60 分钟。有效范围为 6 至 100 分钟。

**步骤 3** 单击保存 (**Save**)。

---

## 终止活动管理会话

思科 ISE-PIC 显示所有活动管理会话，您可以从中选择任意会话并在必要时随时终止所选会话。并行管理 GUI 会话的最大数量为 20 个。如果达到 GUI 会话的最大数量，属于超级管理员组的管理人员可以登录并阻止某些会话。

---

**步骤 1** 选择管理 (**Administration**) > 管理员访问权限 (**Admin Access**) > 会话设置 (**Session Settings**) > 会话信息 (**Session Info**)。

**步骤 2** 选中要终止的会话 ID 旁边的复选框，然后单击失效 (**Invalidate**)。

---



## 管理门户使用的端口

管理门户使用 HTTP 80 端口和 HTTPS 443 端口，并且您无法更改这些设置。您不能将任何最终用户门户配置为使用这些端口，以便降低管理门户的风险。

## 配置 SMTP 服务器以支持通知

配置简单邮件传输协议 (SMTP) 服务器，以执行以下操作：发送警报的电子邮件通知。

发送电子邮件的 ISE 节点

以下列表显示了分布式 ISE 环境中哪些节点会发送电子邮件。

电子邮件用途	发送电子邮件的节点
访客过期	主 PAN
alarms	活动 MnT
来自访客和发起人门户的发起人和访客通知	PSN
密码过期	主 PAN

**步骤 1** 选择 **设置 (Settings) > SMTP 服务器 (SMTP Server)**。

**步骤 2** 在 **SMTP 服务器 (SMTP Server)** 字段中输入出站 SMTP 服务器的主机名。必须可从思科 ISE-PIC 服务器访问该 SMTP 主机服务器。该字段长度不得超过 60 个字符。

**步骤 3** 单击 **保存 (Save)**。

警报通知的收件人可以是已启用在电子邮件中包括系统警报 (**Include system alarms in emails**) 选项的任何内部管理员用户。发送警报通知的发件人的邮件地址硬编码为 `ise@<hostname>`。

## 从 GUI 启用外部 RESTful 服务 API - ERS 设置

开始之前

您必须启用 Cisco ISE REST API 对于思科 ISE 开发的应用 REST API 可以访问思科 ISE。Cisco REST API 使用 HTTPS 端口 9060，默认情况下会关闭。Cisco ISE REST API 在思科 ISE 管理员服务器上未启用，客户端应用程序从所有访客 REST API 请求的服务器将收到超时错误。

所有类型外部宁静的服务请求的主要 ESS 节点有效。辅助节点可以访问（GET 请求）。

**步骤 1** 选择 **设置 (Settings) > ERS 设置 (ERS Settings)**。

**步骤 2** 选择 **启用 ERS 进行读/写 (Enable ERS for Read/Write)** 并单击 **保存 (Save)**。

### 下一步做什么

有关 API 调用和 ISE-PIC 的详细信息，请参阅 [《ISE API 参考指南》](#)。



## 第 8 章

# ISE-PIC 中的监控和故障排除服务

监控和故障排除服务是面向所有思科 ISE-PIC 运行时服务的综合身份解决方案，并使用以下组件：

- 监控 - 提供代表网络访问活动状态的有意义数据的实时展示。通过查看展示，您可以轻松地解释并影响操作条件。
- 故障排除 - 提供解决网络访问问题的情景指南。之后，您即可了解用户的问题并及时提供解决方案。
- 报告 - 提供一类标准报告，您可以用这些报告来分析趋势和监控系统性能以及网络活动。您可以用各种方式自定义这些报告，并可保存这些报告以供将来使用。您可以使用通配符以及“身份”、“终端 ID”和“节点”字段的多个值来搜索记录。

在本节中详细了解如何使用监控、故障排除和报告工具来管理 ISE-PIC。

- [实时会话](#)，第 137 页
- [可用报告](#)，第 140 页
- [思科 ISE-PIC 警报](#)，第 143 页
- [用于验证传入流量的 TCP Dump 实用工具](#)，第 151 页
- [日志记录机制](#)，第 154 页
- [Active Directory 故障排除](#)，第 154 页
- [获取其他故障排除信息](#)，第 166 页

## 实时会话

下表说明了 **实时会话 (Live Sessions)** 窗口中的字段，此窗口显示实时会话。从主菜单栏中，选择**实时会话 (Live Sessions)**。

表 23: 实时会话

字段名称	说明
启动时间 (Initiated)	显示启动会话时的时间戳。
已更新 (Updated)	显示会话上次由于任何更改而更新时的时间戳。

字段名称	说明
帐户会话时间 (Account Session Time)	显示用户会话的时间跨度（秒）。
会话状态 (Session Status)	显示终端设备的当前状态。
操作 (Action)	单击“操作”图标以打开 <b>操作 (Actions)</b> 弹出窗口。可以执行以下操作： <ul style="list-style-type: none"> <li>• 清除会话</li> <li>• 检查当前用户的会话状态</li> </ul>
终端 ID (Endpoint ID)	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
身份 (Identity)	显示终端设备的用户名。
IP 地址 (IP Address)	显示终端设备的 IP 地址。
服务器 (Server)	指示已从中生成日志的 PIC 节点。
身份验证方式 (Auth Method)	显示 RADIUS 协议使用的身份验证方式，例如“密码身份验证协议” (Password Authentication Protocol)、 “质询握手身份验证协议” (Challenge Handshake Authentication Protocol)、 IEE 802.1x 或 dot1x 等等。
会话源 (Session Source)	指示它是 RADIUS 会话还是 PassiveID 会话。
用户域名 (User Domain Name)	显示用户的注册 DNS 名称。
用户 NetBIOS 名称 (User NetBIOS Name)	显示用户的 NetBIOS 名称。

字段名称	说明
提供程序 (Provider)	<p>终端活动获悉自不同的系统日志源。这些系统日志源称为提供程序。</p> <ul style="list-style-type: none"> <li>• Windows Management Instrumentation (WMI) - WMI 是一种 Windows 服务，用于提供通用接口和对象模型来访问有关操作系统、设备、应用和服务的管理信息。</li> <li>• 代理 - 代表客户端或另一个程序在客户端上运行的程序。</li> <li>• 系统日志 - 客户端发送活动消息的日志记录服务器。</li> <li>• REST - 客户端通过终端服务器进行身份验证。对于此系统日志源，将会显示“TS代理 ID”、“源端口开始时间”、“源端口结束时间”和“源第一个端口”值。</li> <li>• SPAN - 使用 SPAN 探测器发现的网络信息。</li> <li>• DHCP - DHCP 事件。</li> <li>• 终端</li> </ul> <p>从终端会话获悉来自不同提供程序的两个事件后，提供程序在实时会话页面中显示为逗号分隔值。</p>
MAC 地址 (MAC Address)	显示客户端的 MAC 地址。
终端检查时间 (Endpoint Check Time)	显示终端探测器上次检查终端的时间。
终端检查结果 (Endpoint Check Result)	<p>显示终端探测的结果。可能的值包括：</p> <ul style="list-style-type: none"> <li>• 无法接通</li> <li>• 用户退出</li> <li>• 活动用户</li> </ul>
起始源端口 (Source Port Start)	(仅为 REST 提供程序显示值) 显示端口范围内的第一个端口号。
结束源端口 (Source Port End)	(仅为 REST 提供程序显示值) 显示端口范围内的最后一个端口号。

字段名称	说明
源第一个端口 (Source First Port)	<p>(仅为 REST 提供程序显示值) 显示由终端服务器 (TS) 代理分配的端口。</p> <p>终端服务器 (TS) 指允许多个终端在无需调制解调器或网络接口的情况下连接到其上的服务器或网络设备, 可实现多个终端到 LAN 网络的连接。多个终端可能会有相同的 IP 地址, 因此难以识别特定用户的 IP 地址。所以, 为了识别特定用户, 需在服务器上安装 TS 代理, 为每个用户分配一个端口范围。这有助于创建 IP 地址 - 端口 - 用户映射。</p>
TS 代理 ID (TS Agent ID)	(仅为 REST 提供程序显示值) 显示安装在终端上的终端服务器 (TS) 代理的唯一标识。
AD 用户解析的身份 (AD User Resolved Identities)	(仅为 AD 用户显示值) 显示匹配的潜在账户。
AD 用户解析的 DN (AD User Resolved DNs)	(仅为 AD 用户显示值) 显示 AD 用户的可分辨名称, 例如 CN=chris,CN=Users,DC=R1,DC=com

## 可用报告

下表按照报告类别分组列出系统预配置的报告。此外还提供对报告功能和日志记录类别的说明。

报告名称	说明	日志记录类别
IDC 报告		
AD Connector Operations	<p>“AD 连接器操作” 报告提供 AD 连接器所执行的操作的日志, 例如 ISE-PIC 服务器密码更新、Kerberos 票证管理、DNS 查询、DC 发现、LDAP 和 RPC 连接管理等。</p> <p>如果遇到某些 AD 故障, 您可以在此报告中查看详细信息以确定可能的原因。</p>	选择管理 ( <b>Administration</b> ) > 系统 ( <b>System</b> ) > 日志记录 ( <b>Logging</b> ) > 日志记录类别 ( <b>Logging Categories</b> ), 然后选择 “AD 连接器” (AD Connector)。
Administrator Logins	管理员登录报告提供关于所有基于 GUI 的管理员登录事件以及成功的 CLI 登录事件的信息。	选择 <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> , 然后选择 <b>Administrative and Operational Audit</b> 。

报告名称	说明	日志记录类别
Change Configuration Audit	更改配置审核报告提供关于指定时间内配置更改的详细信息。如果需要对某个功能进行故障排除，此报告可以帮助您确定是不是最近的配置更改导致了问题。	选择管理 ( <b>Administration</b> ) > 系统 ( <b>System</b> ) > 日志记录 ( <b>Logging</b> ) > 日志记录类别 ( <b>Logging Categories</b> )，然后选择“管理和操作审核” (Administrative and Operational Audit)。
Current Active Sessions	您可以通过当前活动会话报告导出包含关于指定时间内哪些用户正在访问网络的详细信息的报告。  如果用户无法访问网络，您可以查看会话是否经过了身份验证或是否中断，或会话是否存在其他问题。	选择管理 ( <b>Administration</b> ) > 系统 ( <b>System</b> ) > 日志记录 ( <b>Logging</b> ) > 日志记录类别 ( <b>Logging Categories</b> )，然后选择以下日志记录类别：“记账” (Accounting) 和“RADIUS 记账” (RADIUS Accounting)。
Health Summary	运行状况摘要报告提供与控制面板类似的详细信息。但是，控制面板仅显示前 24 小时的数据，而您可以使用此报告查看更久之前的历史数据。  您可以评估这些数据，以查看数据中的一致模式。例如，您可能预计当大多数员工都开始工作时，CPU 使用率较高。如果您发现这些趋势存在不一致性，您可以确定潜在的问题。  CPU 使用率表列出不同 ISE-PIC 功能的 CPU 使用率的百分比。此表中提供 <b>show cpu usage</b> CLI 命令的输出，您可以将这些值与部署中的问题相关联，从而识别可能的原因。	选择管理 ( <b>Administration</b> ) > 系统 ( <b>System</b> ) > 日志记录 ( <b>Logging</b> ) > 日志记录类别 ( <b>Logging Categories</b> )，然后选择以下日志记录类别：“管理和操作审核” (Administrative and Operational Audit)、 “系统诊断” (System Diagnostics) 及“系统统计信息” (System Statistics)。
Operations Audit	“操作审核” 报告提供有关任何操作变更的详细信息，例如运行备份、注册思科 ISE-PIC 节点或重新启动应用。	选择管理 ( <b>Administration</b> ) > 系统 ( <b>System</b> ) > 日志记录 ( <b>Logging</b> ) > 日志记录类别 ( <b>Logging Categories</b> )，然后选择“管理和操作审核” (Administrative and Operational Audit)。

报告名称	说明	日志记录类别
PassiveID	通过“被动 ID”报告，可以监控与域控制器的 WMI 连接的状态并收集与其相关的统计信息（例如接收的通知数量、每秒钟用户登录/注销的次数等）。	选择 <b>管理 (Administration)</b> > <b>系统 (System)</b> > <b>日志记录 (Logging)</b> > <b>日志记录类别 (Logging Categories)</b> ，然后选择“身份映射” (Identity Mapping)。
pxGrid Administrator Audit	<p>“pxGrid 管理员审核”报告提供 pxGrid 管理操作的详细信息，例如注册客户端、注销客户端、审批客户端、创建主题、删除主题、添加发布者/用户以及删除发布者/用户。</p> <p>每条记录都会注明在节点上执行相应操作的管理员名称。</p> <p>您可以根据管理员和消息条件过滤 pxGrid 管理员审核报告。</p>	-
System Diagnostic	<p>“系统诊断”报告提供有关 ISE-PIC 节点的状态的详细信息。如果 ISE-PIC 节点无法注册，可以查看此报告来对问题进行故障排除。</p> <p>此报告要求首先启用几个诊断日志记录类别。收集这些日志可能会对 ISE-PIC 性能产生不利影响。因此，默认情况下未启用这些类别。如果您启用这些类别，应使其启用持续时间刚好满足收集数据的要求即可。否则，30 分钟后系统会自动禁用这些类别。</p>	选择 <b>管理 (Administration)</b> > <b>日志记录 (Logging)</b> > <b>日志记录类别 (Logging Categories)</b> ，然后选择以下日志记录类别：“内部操作诊断” (Internal Operations Diagnostics)、 <b>“分布式管理” (Distributed Management)</b> 、 <b>“管理员身份验证” (Administrator Authentication)</b> 和 <b>“授权” (Authorization)</b> 。
User Change Password Audit	用户更改密码审核报告显示关于员工密码更改的验证信息。	选择 <b>管理 (Administration)</b> > <b>系统 (System)</b> > <b>日志记录 (Logging)</b> > <b>日志记录类别 (Logging Categories)</b> ，然后选择“管理和操作审核” (Administrative and Operational Audit)。



## 思科 ISE-PIC 警报

警报显示在“警报”(Alarms) Dashlet 中，通知您网络中的情况。有三种警报严重级别：严重、警告和信息。警报还会提供关于系统活动的信息，如数据清除事件。可以配置要接收系统活动通知的方式，或完全禁用警报。还可以为某些警报配置阈值。

大多数警报没有关联的计划，会在事件发生后立即发送。在任何给定时间点，系统只会保留最新的 15,000 个警报。

如果事件再次发生，则系统会在一个小时内抑制相同的警报。在事件再次发生期间，可能需要经过一个小时，警报才会再次出现，该取决于触发器。

下表列出了所有思科 ISE-PIC 警报、说明及其解决方法。

表 24: 思科 ISE-PIC 警报

警报名称	警报说明	警报解决方法
管理和操作审核管理		
部署升级失败	ISE PIC 节点升级失败。	检查故障节点的 ADE.log，以查找升级失败的原因并制定纠正措施。
升级捆绑包下载失败	ISE-PIC 节点升级捆绑包下载失败。	检查故障节点的 ADE.log，以查找升级失败的原因并制定纠正措施。
由于 CRL 查找到已吊销的证书，安全 LDAP 连接重新连接	CRL 检查结果是用于 LDAP 连接的证书已吊销。	检查 CRL 配置并检验它是否有效。检查 LDAP 服务器证书及其颁发机构证书是否已吊销。如果已吊销，颁发新证书并将其安装在 LDAP 服务器上。
由于 OCSP 查找到已吊销的证书，安全 LDAP 连接重新连接	OCSP 检查结果是用于 LDAP 连接的证书已吊销。	检查 OCSP 配置并检验它是否有效。检查 LDAP 服务器证书及其颁发机构证书是否已吊销。如果已吊销，颁发新证书并将其安装在 LDAP 服务器上。
由于 CRL 查找到已吊销的证书，安全系统日志连接重新连接	CRL 检查结果是用于系统日志连接的证书已吊销。	检查 CRL 配置并检验它是否有效。检查系统日志服务器证书及其颁发机构证书是否已吊销。如果已吊销，颁发新证书并将其安装在系统日志服务器上。

警报名称	警报说明	警报解决方法
由于 OCSP 查找到已吊销的证书，安全系统日志连接重新连接	OCSP 检查结果是用于系统日志连接的证书已吊销。	检查 OCSP 配置并检验它是否有效。检查系统日志服务器证书及其颁发机构证书是否已吊销。如果已吊销，颁发新证书并将其安装在系统日志服务器上。
管理员帐户已锁定/禁用	由于密码过期或登录尝试不正确，系统锁定或禁用管理员帐户。有关详细信息，请参阅管理员密码策略。	管理员密码可以由其他管理员使用 GUI 或 CLI 进行重置。
ERS 识别已弃用的 URL	ERS 识别已弃用的 URL	请求的 URL 已被弃用，建议避免使用它。
ERS 识别过时的 URL	ERS 识别过时的 URL	请求的 URL 已过时，建议使用更新的 URL。未来的版本不会删除此 URL。
ERS 请求“内容-类型”标头已过时	ERS 请求的内容类型报头已过时。	请求“内容-类型”标头中描述的请求资源版本已过时。这表明资源方案已被修改。可能已添加或删除一个或多个属性。为使用过时的方案解决这一问题，ERS 引擎将使用默认值。
ERS XML 输入有 XSS 或注入攻击的嫌疑	ERS XML 输入有 XSS 或注入攻击的嫌疑。	请检查您的 xml 输入。
备份失败	思科 ISE-PIC 备份操作失败。	检查思科 ISE-PIC 与存储库之间的网络连接性。确保： <ul style="list-style-type: none"> <li>• 用于存储库的凭证是正确的。</li> <li>• 存储库中有足够的磁盘空间。</li> <li>• 存储库用户具有写入权限。</li> </ul>
CA 服务器已关闭	CA 服务器已关闭。	检查以确保 CA 服务已启动并正在 CA 服务器上运行。
CA 服务器已启动	CA 服务器已启动。	通知管理员 CA 服务器已启动。

警报名称	警报说明	警报解决方法
证书到期	此证书即将到期。证书到期时，思科 ISE-PIC 可能无法与客户端建立安全通信。	更换证书。对于信任证书，请联系证书颁发机构 (CA)。对于 CA 签名的本地证书，请生成 CSR 并使 CA 创建新证书。对于自签名的本地证书，请使用思科 ISE-PIC 延长有效期。如果不再使用证书，可将其删除。
证书被吊销	管理员被吊销由内部 CA 颁发给终端的证书。	从头完成 ISE-PIC 流程以获得新证书。
证书调配初始化错误	证书调配初始化失败	在主题中找到多个具有相同 CN (CommonName) 属性值的证书，无法构建证书链。检查系统中的所有证书。
证书复制失败	到辅助节点的证书复制失败	证书在辅助节点上无效，或存在某些其他永久错误条件。检查辅助节点是否有预先存在的冲突证书。如果找到，请删除辅助节点上预先存在的证书，然后在主节点上导出新证书，删除证书，然后将其导入以重新尝试复制。
证书复制暂时失败	到辅助节点的证书复制暂时失败	由于网络故障等临时条件，证书未复制到辅助节点。系统将重试复制，直至成功。
证书已过期	此证书已过期。思科 ISE-PIC 可能无法与客户端建立安全通信。节点到节点通信可能也会受到影响。	更换证书。对于信任证书，请联系证书颁发机构 (CA)。对于 CA 签名的本地证书，请生成 CSR 并使 CA 创建新证书。对于自签名的本地证书，请使用思科 ISE-PIC 延长有效期。如果不再使用证书，可将其删除。
证书请求转发失败	证书请求转发失败。	确保传入的认证请求与发件人的属性相匹配。
配置已更改	思科 ISE 配置已更新。系统没有为任何用户和终端的配置更改触发此警报。	检查是否应存在配置更改。

警报名称	警报说明	警报解决方法
CRL 检索失败	无法从服务器检索 CRL。如果指定的 CRL 不可用，就可能会出现这种情况。	确保下载 URL 正确且可用于服务。
DNS 解析失败	节点上的 DNS 解析失败。	检查是否可访问使用 <b>ip name-server</b> 命令配置的 DNS 服务器。  如果您收到的警报为“DNS Resolution failed for CNAME <hostname of the node>”，则确保为每个思科 ISE 节点创建 CNAME RR 以及 A 记录。
需要进行固件更新	需要在此主机上进行固件更新。	联系思科技术支持中心 (TAC) 获取固件更新
虚拟机资源不足	此主机上的虚拟机 (VM) 资源（如 CPU、RAM、磁盘空间或 IOPS）不足。	确保 VM 主机达到《思科 ISE 硬件安装指南》中指定的最低要求。
NTP 服务故障	此节点上的 NTP 服务已关闭。	这可能是因为 NTP 服务器与思科 ISE-PIC 节点之间存在较大的时间差异（超过 1000 秒）。确保 NTP 服务器正常工作并使用 <b>ntp server &lt;servername&gt;</b> CLI 命令重新启动 NTP 服务并修复时间差。
NTP 同步失败	在此节点配置上的所有 NTP 服务器均无法访问。	从 CLI 执行 <b>show ntp</b> 命令，进行故障排除。确保可从思科 ISE-PIC 访问 NTP 服务器。如果已配置 NTP 身份验证，请确保密钥 ID 和值与服务器的相匹配。
未安排配置备份	未安排思科 ISE-PIC 配置备份。	创建配置备份计划。
操作数据库清除失败	无法从操作数据库中清除较旧的数据。如果 M&T 节点繁忙，就可能会出现这种情况。	检查数据清除审核报告并确保 <b>used_space</b> 小于 <b>threshold_space</b> 。使用 CLI 登录到 M&T 节点，手动执行清除操作。

警报名称	警报说明	警报解决方法
复制失败	辅助节点无法使用复制的消息。	登录思科 ISE-PIC GUI 并从部署页面执行手动同步。取消注册并重新注册受影响的思科 ISE-PIC 节点。
恢复失败	思科 ISE-PIC 恢复操作失败。	确保思科 ISE-PIC 与存储库之间存在网络连接。确保用于存储库的凭证正确。确保备份文件未损坏。从 CLI 执行 <b>reset-config</b> 命令并恢复已知的最后一次有效备份。
补丁失败	服务器上的补丁进程失败。	在服务器上重新安装补丁进程。
补丁成功	服务器上的补丁进程成功。	-
复制已停止	ISE-PIC 节点无法从主节点复制配置数据。	登录思科 ISE-PIC GUI 以从部署页面执行手动同步，或取消注册并重新注册带必填字段的受影响思科 ISE-PIC 节点。
终端证书已过期	终端证书已由每天安排的作业标记为过期。	请重新注册终端设备，获取新的终端证书。
终端证书已清除	过期的终端证书已由每天安排的作业清除。	不需要采取行动 - 这是管理员发起的清理操作。
复制减慢错误	系统检测到复制减慢或停滞。	请验证节点是否可访问并是部署的一部分。
复制减慢信息	系统检测到复制减慢或停滞。	请验证节点是否可访问并是部署的一部分。
复制减慢警告	系统检测到复制减慢或停滞。	请验证节点是否可访问并是部署的一部分。
EST 服务已停止	EST 服务已停止。	确保 CA 和 EST 服务正常运行，且证书服务终端子 CA 证书链完整。
EST 服务已启动	EST 服务已启动。	通知管理员 EST 服务已启动。
Smart Call Home 通信故障	Smart Call Home 消息未成功发送。	确保思科 ISE-PIC 和思科系统之间存在网络连接。
遥测通信故障	遥测消息未成功发送。	确保思科 ISE 和思科系统之间存在网络连接。

警报名称	警报说明	警报解决方法
ISE 服务		
AD 连接器必须重新启动	AD 连接器意外停止，必须重新启动。	如果此问题仍然存在，请联系思科 TAC 寻求帮助。
Active Directory 林不可用	Active Directory 林 GC（全局目录）不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
身份验证域不可用	身份验证域不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
ID 映射。身份验证处于非活动状态	身份映射服务在过去 15 分钟未收集任何用户身份验证事件。	如果这是一个应进行用户身份验证的时间（例如，工作时间），则检查到 Active Directory 域控制器的连接。
配置的名称服务器已关闭	配置的名称服务器已关闭或不可用。	检查 DNS 配置和网络连接。
AD: 计算机 TGT 刷新失败	ISE-PIC 服务器 TGT（根凭证）刷新失败；它用于 AD 连接和服务。	检查思科 ISE-PIC 计算机帐户是否存在且有效。另请检查是否存在时钟偏差、复制、Kerberos 配置和/或网络错误。
AD: ISE 帐户密码更新失败	ISE-PIC 服务器未能更新其 AD 计算机帐户密码。	检查思科 ISE-PIC 计算机帐户密码是否未更改，计算机帐户是否未禁用或受限制。检查到 KDC 的连接。
所加入的域不可用	所加入的域不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
身份库不可用	思科 ISE-PIC 策略服务节点无法访问配置的身份库。	检查思科 ISE-PIC 与身份库之间的网络连接。
AD: ISE 计算机帐户没有获取组所需的权限。	思科 ISE-PIC 计算机帐户没有获取组所需的权限。	检查思科 ISE-PIC 计算机帐户是否有权获取 Active Directory 中的用户组。
系统运行状况		

警报名称	警报说明	警报解决方法
高磁盘 I/O 利用率	思科 ISE-PIC 系统遇到高磁盘 I/O 利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高磁盘空间利用率	思科 ISE-PIC 系统遇到高磁盘空间利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高平均负载	思科 ISE-PIC 系统遇到高平均负载。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高内存利用率	思科 ISE-PIC 系统遇到高内存利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高操作数据库使用率	思科 ISE-PIC 监控节点遇到的系统日志数据量高于预期数据量。	检查并缩小操作数据的清除配置窗口。
运行状态不可用	监控节点未收到思科 ISE-PIC 节点的运行状态。	确保思科 ISE-PIC 节点已启动并且正在运行。确保思科 ISE-PIC 节点能够与监控节点通信。
进程已关闭	其中一个思科 ISE-PIC 进程未运行。	重新启动思科 ISE-PIC 应用。
已达到 OCSP 事务阈值	已达到 OCSP 事务阈值。当内部 OCSP 服务达到较高流量时触发此警报。	请检查系统是否有足够的资源。
许可		
PIC 许可证已过期	思科 ISE-PIC 节点上安装的许可证已过期。	联系思科客户团队购买新许可证。
在 30 天内到期的 PIC 许可证	思科 ISE-PIC 节点上安装的许可证将在 30 天后到期。	请联系思科销售团队以延期 ISE-PIC 许可证。
在 60 天内到期的 PIC 许可证	思科 ISE-PIC 节点上安装的许可证将在 60 天后到期。	请联系思科销售团队以延期 ISE-PIC 许可证。
在 90 天内到期的 PIC 许可证	思科 ISE-PIC 节点上安装的许可证将在 90 天后到期。	请联系思科销售团队以延期 ISE-PIC 许可证。

警报名称	警报说明	警报解决方法
系统错误		
日志收集错误	思科 ISE-PIC 监控收集器进程无法留存从策略服务节点生成的审核日志。	这不会影响策略服务节点的实际功能。如需进一步解决问题，请联系 TAC。
计划的报告导出失败	无法将导出的报告（CSV 文件）复制到配置的存储库。	验证配置的存储库。如果存储库已删除，请重新添加存储库。如果存储库不可用或不可访问，请将其重新配置为有效存储库。

将用户或终端添加到思科 ISE-PIC 时，系统不会触发警报。

## 警报设置

下表说明了警报设置 (Alarm Settings) 窗口（设置 (Settings) > 警报设置 (Alarm Settings)）中的字段。

字段名称	说明
警报类型 (Alarm Type)	警报类型。
警报名称 (Alarm Name)	警报的名称。
说明 (Description)	警报说明。
建议的操作 (Suggested Actions)	触发警报时要执行的操作。
状态 (Status)	启用或禁用警报规则。
严重性 (Severity)	选择警报的严重性级别。有效的选项包括： <ul style="list-style-type: none"> <li>“严重” (Critical): 指示严重错误情况。</li> <li>“警告” (Warning): 指示正常但重要的情况。这是默认情况。</li> <li>“信息” (Info): 指示信息性的消息。</li> </ul>
发出系统日志消息 (Send Syslog Message)	为思科 ISE-PIC 生成的每个系统警报发送系统日志消息。
输入以逗号分隔的多个电子邮件 (Enter multiple e-mails separated with comma)	电子邮件地址和/或 ISE-PIC 管理员名称的列表。
电子邮件中的备注 (0 到 4000 个字符) (Notes in Email [0 to 4000 characters])	您希望与系统警报关联的自定义文本消息。



## 添加自定义报警

思科 ISE-PIC 包含 5 个默认警报类型，例如“配置更改” (Configuration Changed)、“高磁盘 I/O 利用率” (High Disk I/O Utilization)、“高磁盘空间利用率” (High Disk Space Utilization)、“高内存利用率” (High Memory Utilization) 和“ISE 身份验证处于非活动状态” (ISE Authentication Inactivity)。思科定义的系统警报列在“警报设置” (Alarm Settings) 页面 (“设置” (Settings) > “警报设置” (Alarm Settings))。您只能编辑系统报警。

除现有系统报警外，您还可以添加、编辑或删除现有报警类型下的自定义报警。

对于每种报警类型，您最多可以创建 5 个报警，而且报警总数限制为 200。

要添加报警，请按以下步骤操作：

---

**步骤 1** 选择设置 (Settings) > 警报设置 (Alarm Settings)。

**步骤 2** 在报警配置 (Alarm Configuration) 选项卡中，单击添加 (Add)。

**步骤 3** 输入必要的详细信息。请参阅[警报设置](#)部分了解详细信息。

根据警报类型，“警报配置” (Alarm Configuration) 页面会显示其他属性。例如，对于“配置更改” (Configuration Changed) 警报，将显示“对象名称” (Object Name)、“对象类型” (Object Type) 和“管理员名称” (Admin Name) 字段。您可以为规定不同条件的相同报警添加多个实例。

**步骤 4** 单击提交 (Submit)。

---

## 用于验证传入流量的 TCP Dump 实用工具

TCP 转储实用工具嗅探数据包，可以使用此实用工具验证预计数据包是否已到达节点。例如，当报告中没有显示传入身份验证或日志时，您可能会怀疑没有传入流量或传入流量无法到达思科 ISE。在这种情况下，您可以运行此工具进行验证。

可以配置 TCP 转储选项，然后从网络流量收集数据以帮助您对网络问题进行故障排除。

## 使用 TCP Dump 监控网络流量

“TCP 转储” (TCP Dump) 窗口列出了您创建的 TCP 转储进程文件。可以创建不同文件以用于不同目的，根据需要运行这些文件，然后在不需要这些文件时将其删除。

您可以通过指定大小、文件数量以及进程运行时间来控制收集的数据。如果进程在时间限制之前完成，并且文件小于最大大小，并且您启用了多个文件，则进程会继续并创建另一个转储文件。

可以对更多接口运行 TCP 转储，包括绑定接口。



---

**注释** 不再提供人可读格式选项，转储文件始终为原始格式。

---

支持与存储库的 IPv6 连接。

### 开始之前

**TCP 转储 (TCP Dump)** 窗口页面中的**网络接口 (Network Interface)** 下拉列表仅显示已配置 IPv4 或 IPv6 地址的网络接口卡 (NIC)。在 VMware 中，默认情况下将连接所有 NIC，因此，所有 NIC 均具有 IPv6 地址，并显示在**网络接口 (Network Interface)** 下拉列表中。

**步骤 1** 从**主机名称 (Host Name)** 下拉列表中选择 TCP Dump 实用工具的源。

**步骤 2** 从**网络接口 (Network Interface)** 下拉列表中选择要监控的接口。

**步骤 3** 在**过滤器 (Filter)** 字段中，输入要对其进行过滤的布尔表达式。

系统支持以下标准 TCP 转储过滤器表达式：

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 and not 10.77.122.119

**步骤 4** 输入此 TCP 转储进程的**文件名 (File Name)**。

**步骤 5** 从**存储库 (Repository)** 下拉列表中选择用于存储 TCP 转储日志文件的存储库。

**步骤 6** 从**文件大小 (File Size)** 下拉列表中选择最大文件大小。

如果转储超出此文件大小，则一个新文件将打开以继续转储。转储可通过新文件继续的次数受限制为**(Limit to)** 设置的限制。

**步骤 7** 限制为**(Limit to)** 选项用于限制转储可扩展到的文件数。

**步骤 8** 时间限制**(Time Limit)** 选项可用于配置转储在运行多长时间后结束。

**步骤 9** 单击开**(On)** 或关**(Off)**，设置混合模式**(Promiscuous Mode)**。默认值为开**(On)**。

混合模式为默认嗅探模式，在此模式下，网络接口将所有流量都传输到系统的 CPU。我们建议将该选项设置为 On。



**注释** 思科 ISE 不支持大于 1500 MTU 的帧（巨帧）。

## 保存 TCP Dump 文件

### 开始之前

您应按照[使用 TCP Dump 文件监控网络流量](#)一节中所描述的内容成功完成任务。



**注释** 还可以通过思科 ISE CLI 访问 TCP 转储。有关详细信息，请参阅思科身份服务引擎 CLI 参考指南。

**步骤 1** 从格式 (**Format**) 下拉列表中选择选项。默认设置为人可读 (**Human Readable**)。

**步骤 2** 单击下载 (**Download**)，导航至所需位置，并单击保存 (**Save**)。

**步骤 3** (可选) 若要清除以前的转储文件而无需保存，请单击删除 (**Delete**)。

## TCP Dump 设置

下表介绍 **tcpdump** 实用工具页面上的字段，此页面监控网络接口上的数据包内容，并对网络上出现的问题进行故障排除。此页面的导航路径为：**故障排除 (Troubleshoot)**。

表 25: TCP Dump 设置

选项	使用指南
状态 (Status)	<ul style="list-style-type: none"> <li>• Stopped - tcpdump 实用工具不在运行</li> <li>• Start - 单击以启动监控网络的 tcpdump 实用工具。</li> <li>• Stop - 单击以停止 tcpdump 实用工具</li> </ul>
主机名 (Host Name)	从下拉列表选择要监控的主机的名称。
网络接口 (Network Interface)	从下拉列表选择要监控的网络接口。 <b>注释</b> 您必须配置使用 IPv4 或 IPv6 地址的所有网络接口卡 (NIC)，使其显示于思科 ISE Admin 门户中。
混杂模式 (Promiscuous Mode)	<ul style="list-style-type: none"> <li>• On - 单击以打开混杂模式 (默认设置)。</li> <li>• Off - 单击以关闭混杂模式。</li> </ul> 混杂模式是默认的数据包嗅探模式。我们建议您将其设置为 On。在此模式下，网络接口会将所有流量传递到系统的 CPU。

选项	使用指南
过滤器 (Filter)	输入用于筛选的布尔表达式。支持的标准 tcpdump 过滤器表达式： ip host 10.77.122.123 ip host 10.77.122.123 and not 10.177.122.119 ip host ISE123
格式 (Format)	选择 tcpdump 文件的格式。
转储文件 (Dump File)	显示最后一个转储文件上的数据，例如以下数据： Last created on Wed Apr 27 20:42:38 UTC 2011 by admin  File size: 3,744 bytes Format: Raw Packet Data Host Name: Positron Network Interface: GigabitEthernet 0 Promiscuous Mode: On  <ul style="list-style-type: none"> <li>• Download - 单击以下载最新的转储文件。</li> <li>• Delete - 单击以删除最新的转储文件。</li> </ul>

## 日志记录机制

### 思科 ISE-PIC 日志记录机制

#### 配置系统日志清除设置

使用此流程可设置本地日志存储期，并可在一定时间后删除本地日志。

## Active Directory 故障排除

### 将 Active Directory 与思科 ISE-PIC 集成的前提条件

本节介绍配置 Active Directory 以与思科 ISE-PIC 集成所需的手动步骤。但是，在大多数情况下，可以启用思科 ISE-PIC 来自动配置 Active Directory。以下是将 Active Directory 与思科 ISE-PIC 集成的前提条件。

- 确保您拥有对 AD 域配置进行更改所需的 Active Directory 域管理员凭证。

- 使用网络时间协议 (NTP) 服务器设置来同步思科 ISE-PIC 服务器和 Active Directory 之间的时间。您可以从思科 ISE-PIC CLI 配置 NTP 设置。
- 您必须在思科 ISE-PIC 加入到的域中具有至少一个可由思科 ISE-PIC 运行并访问的全局目录服务器。

## 执行各种操作所需的 Active Directory 帐户权限

加入操作	退出操作	思科 ISE-PIC 机器帐户
加入操作需要以下帐户权限： <ul style="list-style-type: none"> <li>• 搜索 Active Directory（以查看思科 ISE-PIC 机器帐户是否存在）</li> <li>• 将思科 ISE-PIC 机器帐户创建到域（如果机器帐户尚不存在）</li> <li>• 在新机器帐户上设置属性（例如，思科 ISE-PIC 机器帐户密码、SPN、dnsHostname）</li> </ul>	退出操作需要以下帐户权限： <ul style="list-style-type: none"> <li>• 搜索 Active Directory（以查看思科 ISE-PIC 机器帐户是否存在）</li> <li>• 从域中删除思科 ISE-PIC 机器帐户</li> </ul> 如果执行强制退出（在没有密码的情况下退出），则不会从域中删除计算机帐户。	用于传达到 Active Directory 连接的思科 ISE-PIC 机器帐户需要以下权限： <ul style="list-style-type: none"> <li>• 更改密码</li> <li>• 读取与已联系的用户和机器对应的用户和机器对象。</li> <li>• 查询 Active Directory 以获取信息（例如，受信任域和替代 UPN 后缀等）</li> <li>• 读取 tokenGroups 属性</li> </ul> 可以在 Active Directory 中预创建机器帐户。如果 SAM 名称与思科 ISE-PIC 设备主机名匹配，则应在加入操作期间找到该名称并重复使用。 <p>如果具有多个加入操作，则会在思科 ISE-PIC 中维护多个机器帐户，每个加入操作对应一个帐户。</p>



**注释** 用于加入或退出操作的凭证不存储在思科 ISE-PIC 中。仅存储新创建的思科 ISE-PIC 机器帐户凭证。

Microsoft Active Directory 中的网络访问权限：限制允许远程调用 SAM 的客户端安全策略已修改。因此，思科 ISE 可能无法每 15 天更新一次其机器帐户密码。如果机器帐户密码未更新，思科 ISE 不会再通过 Microsoft Active Directory 对用户进行身份验证。您将在思科 ISE 控制板上收到 **AD: ISE 密码更新失败 (AD: ISE password update failed)** 警报，以通知您此事件。

安全策略可使用户枚举本地安全帐户管理器 (SAM) 数据库和 Microsoft Active Directory 中的用户和组。要确保思科 ISE 可更新其机器帐户密码，请检查 Microsoft Active Directory 中的配置是否正确。有关受影响的 Windows 操作系统和 Windows Server 版本的详细信息，包括这对您的网络意味着什么、可能需要哪些更改，请参阅：

<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls>

## 必须开放用于通信的网络端口

协议	端口（远程-本地）	目标	备注
DNS (TCP/UDP)	随机数大于或等于 49152	DNS 服务器/AD 域控制器	-
MSRPC	445	域控制器	-
Kerberos (TCP/UDP)	88	域控制器	MS AD/KDC
LDAP (TCP/UDP)	389	域控制器	-
LDAP (GC)	3268	全局目录服务器	-
NTP	123	NTP 服务器/域控制器	-
IPC	80	对于辅助 ISE-PIC 节点	—

## 支持 ISE-PIC 的 Active Directory 要求

ISE-PIC 使用 Active Directory 域控制器生成的 Active Directory 登录审核事件来收集用户登录信息。必须正确配置 Active Directory 服务器，才能使 ISE 用户能够连接和获取用户登录信息。以下各部分说明如何配置 Active Directory 域控制器（Active Directory 端的配置）以支持 ISE-PIC。

要配置 Active Directory 域控制器（Active Directory 端的配置）以支持，请按照以下步骤操作：



**注释** 必须配置所有域中的所有域控制器。

1. 从 ISE-PIC 设置 Active Directory 加入点和域控制器。请参阅[添加 Active Directory 加入点](#)并将[思科 ISE-PIC 节点](#)加入到该加入点，[第 20 页](#) 和 [#unique\\_35](#)。
2. 根据域控制器配置 WMI。请参阅[#unique\\_36](#)。
3. 从 Active Directory 执行以下步骤：
  - 为被动身份服务配置 Active Directory，[第 157 页](#)
4. （可选）使用以下步骤在 Active Directory 上对 ISE 执行的自动配置进行故障排除：
  - 为域管理员组中的 Microsoft Active Directory 用户设置权限，[第 160 页](#)
  - 不在域管理员组中的 Microsoft Active Directory 用户的权限，[第 160 页](#)
  - 在域控制器上使用 DCOM 的权限，[第 161 页](#)
  - 设置访问 WMI Root 和 CIMv2 命名空间的权限，[第 163 页](#)

- 授权访问 AD 域控制器上的安全事件日志，第 164 页

## 为被动身份服务 配置 Active Directory

ISE-PIC Active Directory 域控制器生成的 Active Directory 登录审核事件来收集用户登录信息。ISE-PIC 连接到 Active Directory 并获取用户登录信息。

应从 Active Directory 域控制器执行以下步骤：

### 步骤 1 确保相关 Microsoft 补丁安装在 Active Directory 域控制器上。

- 需要以下 Windows Server 2008 补丁：

- <http://support.microsoft.com/kb/958124>

此补丁可修复 Microsoft WMI 中的内存泄漏，这会阻止 ISE 与域控制器建立成功连接。

- <http://support.microsoft.com/kb/973995>

此补丁修复 Microsoft 的 WMI 中的不同的内存泄漏，该泄漏偶尔阻止 Active Directory 域控制器将必要的用户登录事件写入至域控制器的安全日志。

- Windows Server 2008 R2 需要以下补丁（除非安装 SP1）：

- <http://support.microsoft.com/kb/981314>

此补丁修复 Microsoft 的 WMI 中的内存泄漏，该泄漏偶尔阻止 Active Directory 域控制器将必要的用户登录活动事件写入至域控制器的安全日志。

- <http://support.microsoft.com/kb/2617858>

此补丁修复 Windows Server 2008 R2 中的启动或登录过程意外缓慢。

- 需要以下链接中列出的 Windows 平台 WMI 相关问题补丁：

- <http://support.microsoft.com/kb/2591403>

这些热修复与 WMI 服务及其相关组件的操作和功能相关。

### 步骤 2 确保 Active Directory 在 Windows 安全日志中记录用户登录事件。

验证“审核策略” (Audit Policy) 设置（“组策略管理” [Group Policy Management] 设置的一部分）支持成功登录在 Windows 安全日志中生成必要事件（这是 Windows 默认设置，但是，您必须明确保证此设置正确）。

### 步骤 3 您必须拥有具备足够权限的 Active Directory 用户才能将 ISE-PIC 连接到 Active Directory。以下说明显示如何为管理域组用户或无管理域组用户定义权限：

- Active Directory 用户为域管理员组成员时需要的权限
- Active Directory 用户不是域管理员组成员时需要的权限

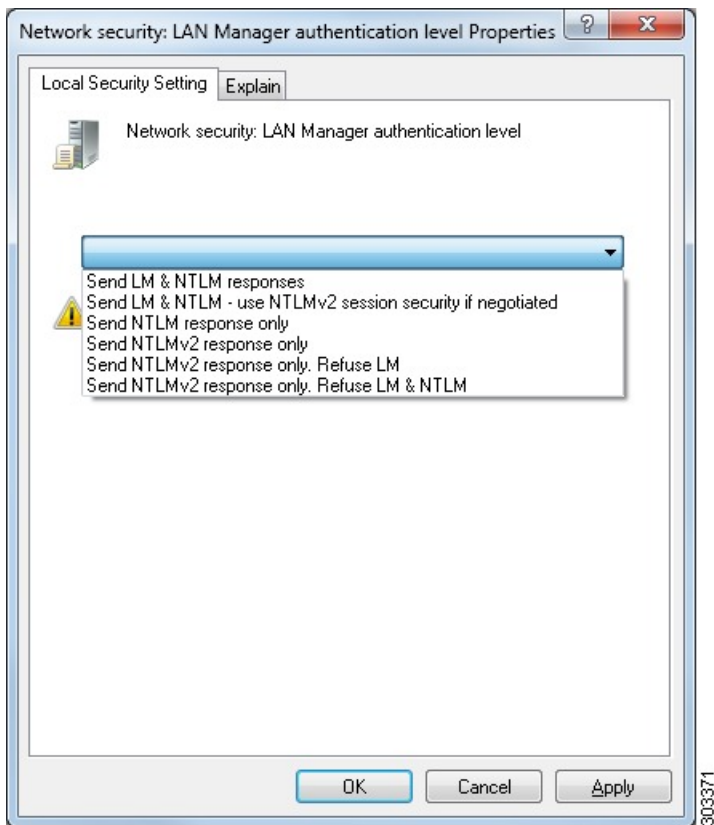
**步骤 4** ISE-PIC 使用的 Active Directory 用户可以通过 NT LAN Manager (NTLM) v1 或 v2 进行身份验证。您需要验证 Active Directory NTLM 设置是否与 ISE-PIC NTLM 设置一致，以确保 ISE-PIC 和 Active Directory 域控制器之间的连接成功进行身份验证。下表显示所有 Microsoft NTLM 选项及支持哪些 ISE-PIC NTLM 操作。如果 ISE-PIC 设置为 NTLMv2，则支持所述的全部六个选项。如果 ISE-PIC 设置为支持 NTLMv1，则仅支持前五个选项。

表 26: 基于 ISE-PIC 和 AD NTLM 版本的受支持身份验证类型

ISE-PIC NTLM 设置选项 / Active Directory (AD) NTLM 设置选项 NTLMv1 NTLMv2	NTLMv1	NTLMv2
发送 LM & NTLM 响应	允许连接	允许连接
发送 LM & NTLM - 如果有协商，使用 NTLMv2 会话安全	允许连接	允许连接
仅发送 NTLM 响应	允许连接	允许连接
仅发送 NTLMv2 响应	允许连接	允许连接
仅发送 NTLMv2 响应。拒绝 LM	允许连接	允许连接
仅发送 NTLMv2 响应。拒绝 LM & NTLM	拒绝连接	允许连接



图 7: MS NTLM 身份验证类型选项



**步骤 5** 确保您已创建一个防火墙规则允许流量去往 Active Directory 域控制器中的 `dllhost.exe`。

您可以关闭防火墙，或者允许在特定 IP（ISE-PIC IP 地址）访问以下端口：

- TCP 135: 通用 RPC 端口。在执行异步 RPC 呼叫时，侦听此端口的服务告知客户端为此请求服务的组件使用哪个端口。
- UDP 137: Netbios 名称解析
- UDP 138: Netbios 数据报服务
- TCP 139: Netbios 会话服务
- TCP 445: SMB

可以动态分配更高的端口，也可以手动进行配置。我们建议您添加 `%SystemRoot%\System32\dllhost.exe` 作为目标。此程序可动态管理端口。

所有防火墙规则均可分配到特定 IP (ISE-PIC IP)。

## 为域管理员组中的 Microsoft Active Directory 用户设置权限

默认情况下，对于 Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2，域管理员组对 Windows 操作系统中的某些注册表项没有完全控制权限。Microsoft Active Directory 管理员必须给予 Microsoft Active Directory 用户对以下注册表项的完全控制权限：

- **HKEY\_CLASSES\_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

以下 Microsoft Active Directory 版本不需要对注册表进行更改：

- Windows 2003
- Windows 2003R2
- Windows 2008

要授予完全控制权限，Microsoft Active Directory 管理员必须首先获得注册表项的所有权：

**步骤 1** 右键单击注册表项图标，然后选择所有者 (Owner) 选项卡。

**步骤 2** 单击 **Permissions** (权限)。

**步骤 3** 单击高级 (Advanced)。

## 不在域管理员组中的 Microsoft Active Directory 用户的权限

对于 Windows Server 2012 R2，授予 Microsoft AD 用户对以下注册表项的完全控制权限：

- HKEY\_CLASSES\_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

在 Windows PowerShell 中使用以下命令来检查是否提供了对注册表项的完整权限：

- ```
get-acl -path "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list
```
- ```
get-acl -path "hkmlm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list
```

当 Microsoft AD 用户不在域管理员组，但在域用户组中时，还需要以下权限：

- 添加注册表项以允许 ISE-PIC 连接到域控制器。
- [在域控制器上使用 DCOM 的权限，第 161 页](#)
- [设置访问 WMI Root 和 CIMv2 命名空间的权限，第 163 页](#)

只有以下 Active Directory 版本要求具有这些权限：

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

### 添加注册表项以允许ISE-PIC 连接到域控制器

必须手动将一些注册表项添加到域控制器，以允许ISE-PIC以域用户身份进行连接，并检索登录身份验证事件。域控制器或该域中的任何其他机器都不需要代理。

以下注册脚本显示了要添加的密钥。您可以将其复制并粘贴到一个文本文件，并另存为扩展名为 .reg 的文件，然后双击该文件进行注册更改。要添加注册密钥，用户必须是根密钥的所有者。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "
```

确保 DllSurrogate 注册表项的值包含两个空格。如果手动更新注册表，必须仅包含两个空格，不包含引号。手动更新注册表时，请确保 AppID、DllSurrogate 及其值中不包含引号。

如前一步脚本所示，保留所有空行，包括文件末尾的空行。

在 Windows 命令提示符下使用以下命令，以确认注册表项是否已创建并包含正确值：

- reg query "HKEY\_CLASSES\_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e
- reg query HKEY\_CLASSES\_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e
- reg query HKEY\_CLASSES\_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e

### 在域控制器上使用 DCOM 的权限

用于ISE-PIC被动身份服务的 Microsoft Active Directory 用户必须具有在域控制器服务器上使用 DCOM 的权限。通过 **dcomcnfg** 命令行工具配置权限。

**步骤 1** 从命令行运行 **dcomcnfg** 工具。

步骤 2 扩展组件服务 (Component Services)。

步骤 3 扩展计算机 (Computers) > 我的计算机 (My Computer)。

步骤 4 从菜单栏中选择操作 (Action)，单击属性 (Properties)，然后单击 COM 安全性 (COM Security)。

步骤 5 思科 ISE 用于访问和启动的帐户必须具有允许权限。将 Microsoft Active Directory 用户添加至所有四个选项（访问权限 (Access Permissions) 和启动并激活权限 (Launch and Activation Permissions) 的编辑限制设置 (Edit Limits) 和编辑默认设置 (Edit Default)）。

步骤 6 对于访问权限 (Access Permissions) 和启动并激活权限 (Launch and Activation Permissions)，允许所有本地和远程访问。

图 8: 访问权限的本地和远程访问

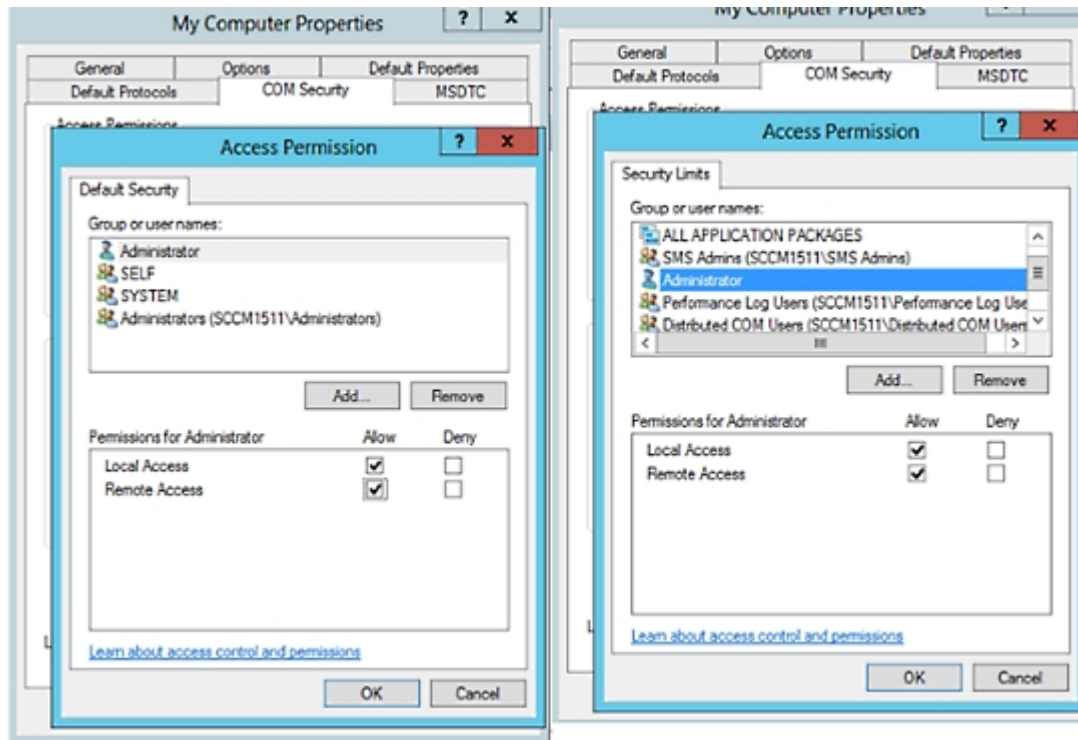
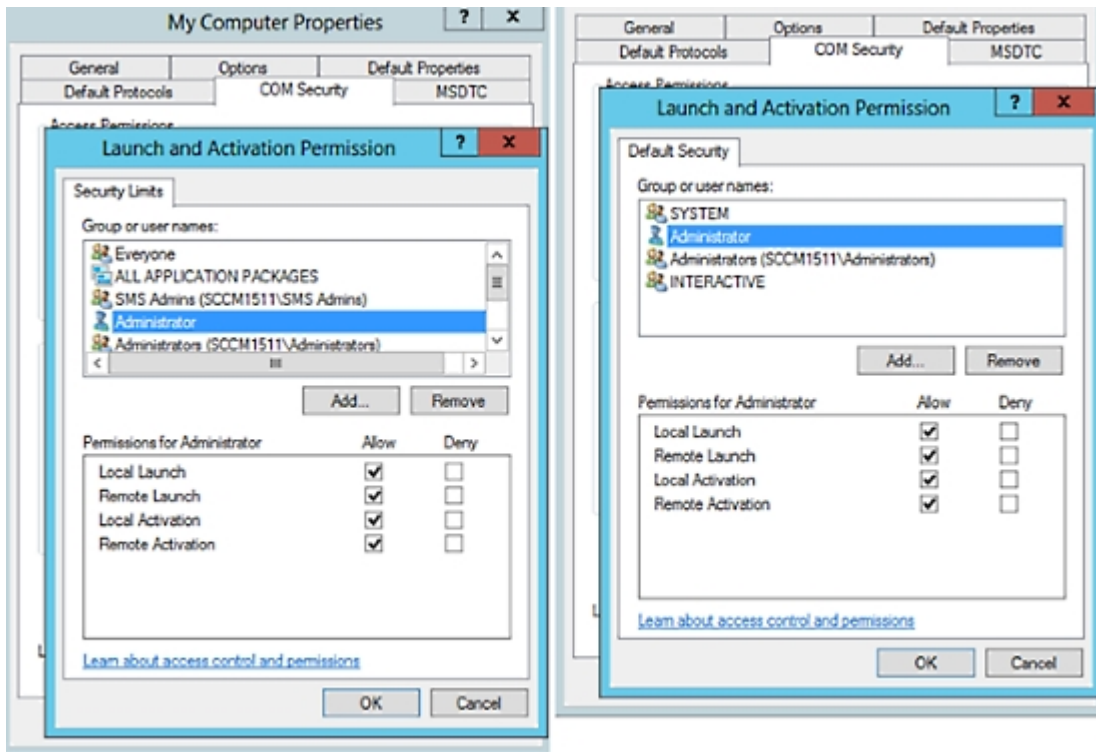


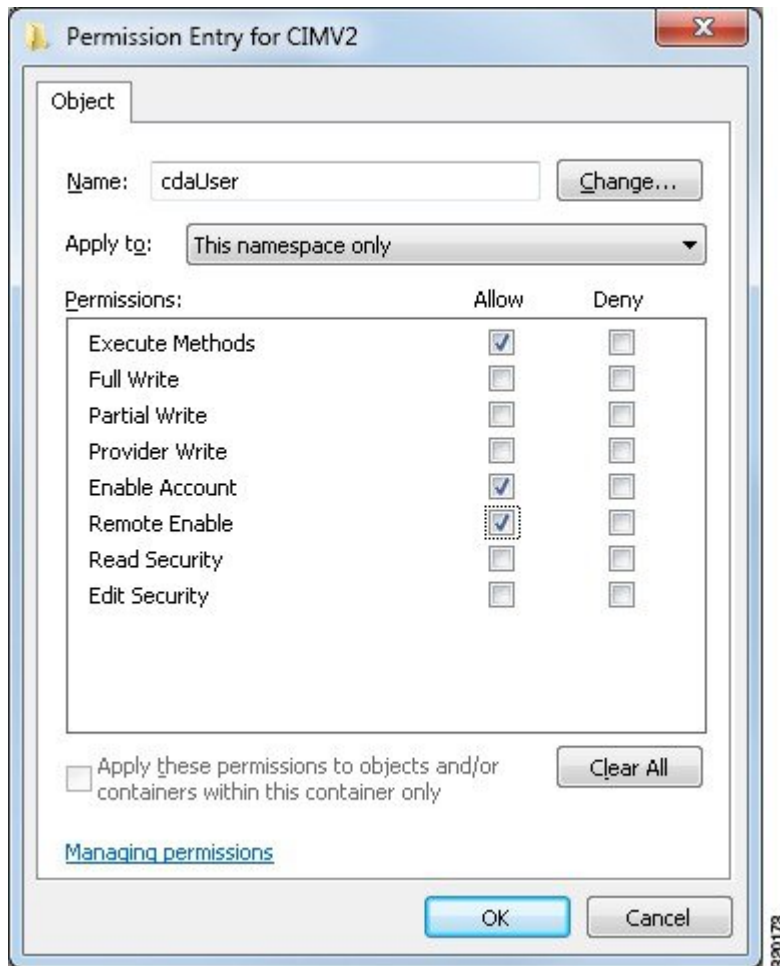
图 9: 启动和激活权限的本地和远程访问



### 设置访问 WMI Root 和 CIMv2 命名空间的权限

默认情况下，Microsoft Active Directory 用户没有对“执行方法” (Execute Methods) 和“远程启用” (Remote Enable) 的权限。您可以使用 `wimgmt.msc` MMC 控制台授予访问权限。

- 步骤 1 选择开始 (Start) > 运行 (Run)，然后输入 `wimgmt.msc`。
- 步骤 2 右键单击 WMI 控制 (WMI Control) 并单击属性 (Properties)。
- 步骤 3 在安全 (Security) 选项卡下，展开根 (Root) 并选择 CIMV2。
- 步骤 4 单击安全 (Security)。
- 步骤 5 添加 Active Directory 用户，并按如下所示配置所需的权限。



## 授权访问 AD 域控制器上的安全事件日志

在 Windows 2008 及更高版本上，您可以通过将 ISE-PIC ID 映射用户添加到名为“事件日志读取器”的组中来授予对 AD 域控制器日志的访问权限。

在 Windows 所有旧版本上，您必须编辑一个注册表项，如下所示。

**步骤 1** 要委托访问至安全事件日志，请查找该帐户的 SID。

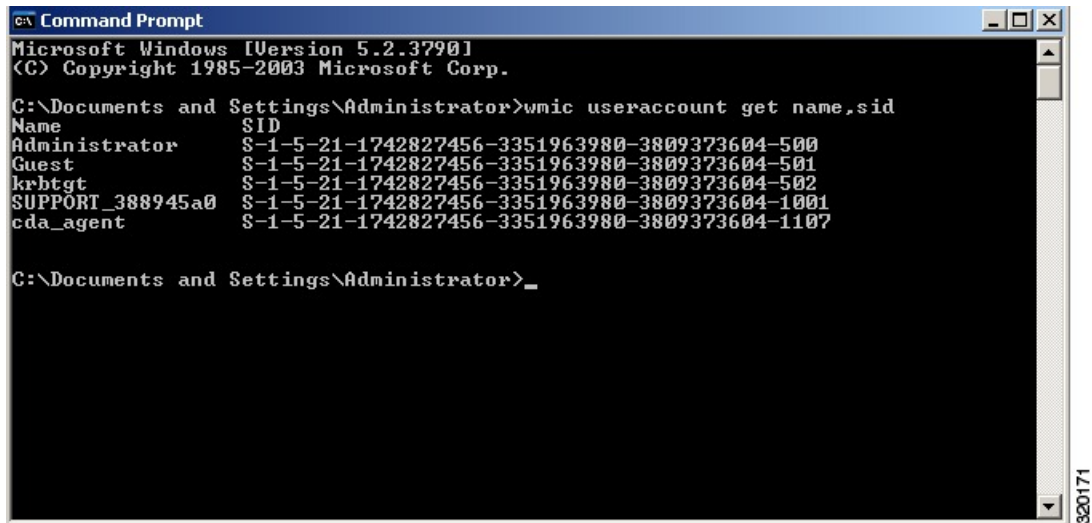
**步骤 2** 在命令行处使用以下命令，列出所有 SID 帐户，也如下图所示。

```
wmic useraccount get name,sid
```

您可以使用用于特定用户名和域的以下命令：

```
wmic useraccount where name="iseUser" get domain,name,sid
```

图 10: 列出所有 SID 帐户



```

c:\ Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>wmic useraccount get name,sid
Name                SID
Administrator      S-1-5-21-1742827456-3351963980-3809373604-500
Guest               S-1-5-21-1742827456-3351963980-3809373604-501
krbtgt              S-1-5-21-1742827456-3351963980-3809373604-502
SUPPORT_388945a0    S-1-5-21-1742827456-3351963980-3809373604-1001
cda_agent           S-1-5-21-1742827456-3351963980-3809373604-1107

C:\Documents and Settings\Administrator>_

```

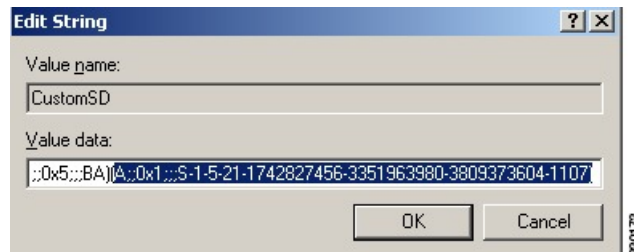
步骤 3 查找 SID，打开“注册表编辑器” (Registry Editor)，并对以下位置进行浏览：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog
```

步骤 4 单击安全 (Security)，然后双击 CustomSD。

例如，要允许读访问 ise\_agent 帐户 (SID - S-1-5-21-1742827456-3351963980-3809373604-1107)，请输入 (A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)。

图 11: 编辑 CustomSD 字符串



步骤 5 重启域控制器上的 WMI 服务。您可以通过以下两种方式重启 WMI 服务：

a) 在 CLI 处运行以下命令：

```
net stop winmgmt
```

```
net start winmgmt
```

b) 运行 Services.msc，打开 Windows 服务管理工具。在 Windows 服务管理窗口中，找到 Windows 管理规范 (Windows Management Instrumentation) 服务，右键单击，然后选择重启 (Restart)。

## 获取其他故障排除信息

通过思科 ISE-PIC，可以从管理员门户下载支持和故障排除信息。可以使用支持捆绑包为思科技术支持中心 (TAC) 准备诊断信息来对思科 ISE-PIC 的问题进行故障排除。



**注释** 支持捆绑包和调试日志为 TAC 提供高级故障排除信息，并且难以解释。可以使用思科 ISE-PIC 提供的各种报告和故障排除工具对在网络中面临的问题进行诊断和故障排除。

## 思科 ISE-PIC 支持捆绑包

您可以配置日志，使其成为支持捆绑包的一部分。例如，您可以配置来自特定服务的日志，使其成为调试日志的一部分。此外，您还可以根据日期过滤日志。

您可以下载的日志分类如下：

- 完整配置数据库：包含可读 XML 格式的思科 ISE-PIC 配置数据库。当您尝试解决问题时，可以将此数据库配置导入另一个思科 ISE 节点，以便重新创建场景。
- 调试日志：捕获引导程序、应用配置、运行时、部署、公共密钥基础设施 (PKI) 信息以及监控和报告。  
调试日志为特定的思科 ISE 组件提供故障排除信息。要启用调试日志，请参阅第 11 章日志记录。如果不启用调试日志，所有信息消息 (INFO) 将包含在支持捆绑包中。有关详细信息，请参阅 [思科 ISE-PIC 调试日志，第 168 页](#)。
- 本地日志：包含来自思科 ISE 上运行的各种进程的系统日志消息。
- 核心文件 - 包含有助于识别突发事件的原因的重要信息。这些日志在应用发生崩溃并且包含大量转储时创建。
- 监控和报告日志：包含关于警报和报告的信息。
- 系统日志 - 包含思科应用部署引擎 (ADE) 相关信息。
- 策略配置：包含在思科 ISE 中配置的可读格式的策略。

使用 `backup-logs` 命令可以从思科 ISE CLI 下载这些日志。有关详细信息，请参阅思科身份服务引擎 CLI 参考指南。

如果选择从 Admin 门户下载这些日志，您可以执行以下操作：

- 根据日志类型（例如调试日志或系统日志），仅下载日志子集。
- 对于所选日志类型，仅下载最新的  $n$  个文件。此选项允许您控制支持捆绑包的大小以及下载所需的时间。



监控日志提供关于监控、报告和故障排除功能的信息。有关下载日志的详细信息，请参阅 [下载思科 ISE-PIC 日志文件。](#)，第 167 页。

## 支持捆绑包

您可以将支持捆绑包以简单 tar.gpg 文件的形式下载至您的本地计算机。支持捆绑包将按照 ise-support-bundle\_ise-support-bundle-mm-dd-yyyy--hh-mm.tar.gpg 的格式用日期和时间戳命名。浏览器会提示您将支持捆绑包保存至适当的位置。您可以提取支持捆绑包的内容并查看 README.TXT 文件，此文件介绍该支持捆绑包的内容，以及在支持捆绑包包含 ISE 数据库内容的情况下如何导入 ISE 数据库内容。

## 下载思科 ISE-PIC 日志文件。

在对网络中的问题进行故障排除时，可以下载思科 ISE-PIC 日志文件，以查找更多信息。您也可以下载包含 ADE-OS 和其他日志文件的系统日志来排除安装和升级方面的问题。

### 开始之前

- 应已配置调试日志和调试日志级别。

---

**步骤 1** 选择 **管理 (Administration)** > **日志记录 (Logging)** > **下载日志 (Download Logs)** > **设备节点列表 (Appliance Node List)**。

**步骤 2** 单击要从其下载支持捆绑包的节点。

**步骤 3** 在 **支持捆绑包 (Support Bundle)** 选项卡中，选择要填充在您的支持捆绑包中的参数。

如果您将所有日志包含在内，则您的支持捆绑包会非常大，下载会需要较长时间。要优化下载流程，请选择只下载最新的  $n$  个文件。

**步骤 4** 输入生成支持捆绑包的**起始日期 (From)** 和**结束日期 (To)**。

**步骤 5** 选择以下其中一个选项：

- **公共密钥加密 (Public Key Encryption)**：如果您想要向思科 TAC 提供支持捆绑包以进行故障排除，请选择此选项。
- **共享密钥加密 (Shared Key Encryption)**：如果您希望在现场排除故障，请选择此选项。如果选择此选项，您必须输入支持捆绑包的加密密钥。

**步骤 6** 单击 **创建支持捆绑包 (Create Support Bundle)**。

**步骤 7** 单击 **下载 (Download)** 以下载新创建的支持捆绑包。

支持捆绑包是下载到正在运行您的应用浏览器的客户端系统的一个 tar.gpg 文件。

---

### 下一步做什么

下载特定组件的调试日志。

## 思科 ISE-PIC 调试日志

调试日志为各种思科 ISE-PIC 组件提供故障排除信息。调试日志包含过去 30 天生成的紧急和警告警报以及在过去 7 天生成的信息警报。报告问题时，可能会要求您启用并发送这些调试日志，以便诊断和解决问题。



**注释** 启用具有高负载的调试日志（例如监控调试日志）会生成有关高负载的警报。

## 获取调试日志

**步骤 1** 配置您希望获取调试日志的组件。

**步骤 2** 下载调试日志。

## 思科 ISE-PIC 组件和相应的调试日志

**注释** 以下列表是 ISE 中可用组件的完整列表。表格中列出的某些组件可能与 ISE-PIC 不相关。

表 27: 组件和相应的调试日志

组件	调试日志
Active Directory	ad_agent.log
Cache Tracker	tracking.log
Entity Definition Framework (EDF)	edf.log
JMS	ise-psc.log
License	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log

组件	调试日志
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
client	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
Guest Access Admin	guest.log
Guest Access	guest.log
MyDevices	guest.log
Portal	guest.log
Portal-Session-Manager	guest.log
Portal-web-action	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log

组件	调试日志
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

## 下载调试日志

**步骤 1** 选择 **管理 (Administration)** > **日志记录 (Logging)** > **下载日志 (Download Logs)**。

**步骤 2** 在“设备节点” (Appliance node) 列表中，单击您希望下载调试日志的节点。

**步骤 3** 单击调试日志 (**Debug Logs**) 选项卡。

系统会显示调试日志类型和调试日志的列表。此列表显示的内容取决于您的调试日志配置。

**步骤 4** 单击您希望下载的日志文件并将其保存到正在运行客户端浏览器的系统中。

您可以根据需要重复此过程下载其他日志文件。可以从**调试日志 (Debug Logs)** 页面下载以下额外的调试日志：

- isebootstrap.log: 提供引导日志消息
- monit.log: 提供监视程序消息
- pki.log: 提供第三方加密库日志
- iseLocalStorage.log: 提供本地存储文件相关日志
- ad\_agent.log: 提供 Microsoft Active Directory 第三方库日志
- catalina.log: 提供第三方日志