



## 思科身份服务引擎管理员指南，版本 3.2

首次发布日期: 2022 年 8 月 16 日

上次修改日期: 2024 年 2 月 23 日

### **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 NONINFRINGEMENT 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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2022 Cisco Systems, Inc. 保留所有权利。



## 目录

---

第 1 章	<b>新信息及变更内容 1</b>
	新信息及变更内容 1

---

第 2 章	<b>思科 ISE 概述 7</b>
	思科 ISE 简介 7
	思科 ISE 功能 8
	思科 ISE 管理员 9
	CLI 管理员与基于 Web 管理员的权限对比 9
	创建新管理员 10
	思科 ISE 管理员组 10
	创建管理员组 14
	对思科 ISE 进行管理访问 15
	思科 ISE 中基于角色的管理员访问控制 15
	基于角色的权限 16
	RBAC 策略 16
	默认菜单访问权限 16
	配置菜单访问权限 17
	默认数据访问权限 18
	配置数据访问权限 18

---

第 3 章	<b>许可 21</b>
	思科 ISE 许可证 21
	层级许可证 22
	设备管理许可证 24

虚拟设备许可证	24
评估许可证	24
思科 ISE 智能许可证	24
注册并激活智能许可证	25
在思科 ISE 中管理智能许可	26
故障排除：未注册的许可证使用情况	27
气隙网络的智能许可	28
为智能许可配置本地智能软件管理器	28

---

**第 4 章****思科 ISE 的部署 31**

思科 ISE 部署术语	32
分布式思科 ISE 部署中的角色	32
配置思科 ISE 节点	32
配置主策略管理节点	33
注册辅助思科 ISE 节点	33
支持多种部署方案	34
思科 ISE 分布式部署	35
思科 ISE 部署设置	35
从主要 ISE 节点将数据复制至辅助思科 ISE 节点	35
思科 ISE 节点取消注册	36
设置分布式部署的规定	36
主要节点和辅助节点上可用的菜单选项	37
部署和节点设置	38
部署节点列表窗口	38
常规节点设置	39
分析节点的设置	42
日志记录设置	44
远程日志记录目标设置	44
配置日志记录类别	45
管理员访问设置	46
管理员密码策略设置	46

会话超时和会话信息设置	48
管理节点	48
管理节点的高可用性	48
手动将辅助 PAN 升级为主 PAN	48
策略服务节点	49
策略服务节点的高可用性	49
用于在 PSN 之间均匀分配请求的负载均衡器	50
策略服务节点中的会话故障切换	50
策略服务节点组中的节点数量	50
监控节点	50
手动修改 MnT 角色	51
MnT 节点中的自动故障切换	51
监控数据库	52
备份和恢复监控数据库	52
监控数据库清除	53
清除监控数据库指南	53
清除较旧的监控数据	53
配置用于自动故障切换的监控节点	54
思科 pxGrid 节点	54
思科 pxGrid 客户端和功能管理	56
启用 pxGrid 服务	56
部署思科 pxGrid 节点	56
思科 pxGrid 实时日志	57
ISE pxGrid 身份映射	57
配置身份映射	58
过滤器身份映射	59
Inline Posture 节点	59
Inline Posture 节点的安装	60
注册 Inline Posture 节点	60
查看部署中的节点	60
数据库崩溃或文件损坏问题	61

设备的监控配置	61
同步主要和辅助思科 ISE 节点	61
更改节点角色和服务	62
在思科 ISE 中修改节点的影响	62
创建策略服务节点组	63
从部署中删除节点	63
关闭思科 ISE 节点	64
更改独立思科 ISE 节点的主机名或 IP 地址	64

---

**第 5 章****基本设置 67**

管理门户	67
思科 ISE 主页控制板	69
配置主页控制面板	70
情景可视性视图	71
Dashlet	73
在视图中过滤显示的数据	74
创建自定义过滤器	76
使用高级过滤器按条件过滤数据	77
使用快速过滤器按字段属性过滤数据	77
Dashlet 视图中的终端操作	77
思科 ISE 控制面板	78
思科 ISE 国际化和本地化	78
支持的语言	79
最终用户 Web 门户本地化	79
支持 UTF-8 字符数据条目	80
UTF-8 凭证身份验证	80
UTF-8 策略和安全评估	80
思科 NAC 和 MAC 代理 UTF-8 支持	80
对发送至请求方的消息的 UTF-8 支持	81
报告和警报 UTF-8 支持	81
门户中的 UTF-8 字符支持	81

思科 ISE 用户界面外的 UTF-8 支持	84
支持导入和导出 UTF-8 值	84
REST 上的 UTF-8 支持	84
身份库授权数据的 UTF-8 支持	84
MAC 地址标准化	85
思科 ISE 部署升级	86
思科 ISE 中的证书管理	86
在思科 ISE 中配置证书以启用安全访问	86
证书使用	87
思科 ISE 中的证书匹配	89
X.509 证书的有效性	89
在思科 ISE 中启用公共密钥基础设施	89
通配符证书	90
思科 ISE 中的通配符证书支持	91
适用于 HTTPS 和扩展身份验证协议通信的通配符证书	91
URL 重定向中的完全限定域名	92
使用通配符证书的优势	93
使用通配符证书的缺点	93
通配符证书兼容性	94
系统证书	94
查看系统证书	95
导入系统证书	95
系统证书导入设置	96
生成自签证书	97
自签证书设置	98
编辑系统证书	99
导出系统证书	101
受信任证书库	101
受信任证书库中的证书	102
受信任证书列表	102
受信任证书命名限制	103

查看受信任的证书	104
更改受信任证书库中的证书状态	105
在受信任的证书库中添加证书	105
编辑受信任证书	105
受信任证书设置	105
从受信任证书库导出证书	107
将根证书导入受信任证书库	108
受信任证书导入设置	109
证书链导入	109
为思科 ISE 节点间通信安装受信任证书	110
思科 ISE 中的默认受信任证书	110
证书签名请求	113
创建证书签名请求并将其提交给证书颁发机构	113
将 CA 签名的证书绑定到证书签名请求	114
导出证书签名请求	115
证书签名请求设置	115
设置供门户使用的证书	119
用户和终端证书续订	119
策略条件中用于证书续订的字典属性	120
证书续订的授权策略条件	120
用于续订证书的 CWA 重定向	120
将思科 ISE 配置为允许用户续订证书	120
更新允许的协议配置	121
为 CWA 重定向创建授权策略配置文件	121
创建授权策略规则以更新证书	122
在访客门户中启用 BYOD 设置	122
Apple iOS 设备的证书续订失败	122
从 .pfx 文件提取证书和私钥	123
思科 ISE CA 服务	123
简单证书注册协议配置文件	123
终端证书	124



终端证书概述窗口 (Endpoint Certificate Overview Window)	124
思科 ISE CA 证书和密钥的备份与恢复	125
导出思科 ISE CA 证书和密钥	125
导入思科 ISE CA 证书和密钥	126
在主 PAN 和 PSN 上生成根 CA 和从属 CA	127
将思科 ISE 根 CA 配置为外部 PKI 的辅助 CA	127
配置思科 ISE 以使用证书对个人设备进行身份验证	128
将用户添加到 Employee 用户组	129
为基于 TLS 的身份验证创建证书身份验证配置文件	129
为基于 TLS 的身份验证创建身份源序列	129
配置证书颁发机构设置	130
创建 CA 模板	131
内部 CA 设置	132
创建要用于客户端调配策略的本地请求方配置文件	132
从思科下载适用于 Windows 和 Mac OS X 操作系统的代理资源	133
为 Apple iOS、Android 和 MAC OS X 设备创建客户端调配策略规则。	133
为基于 TLS 的身份验证配置 Dot1X 身份验证策略规则	134
为集中式 Web 身份验证和请求方调配流程创建授权配置文件	135
创建授权策略规则	135
CA 服务策略参考	136
证书服务的客户端调配策略规则	136
证书服务的授权配置文件	137
证书服务的授权策略规则	137
吊销终端证书	138
OCSP 服务	138
思科 ISE CA 服务在线证书状态协议响应器	139
OCSP 证书状态值	139
OCSP 高可用性	140
OCSP 故障	140
添加 OCSP 客户端配置文件	140
OCSP 客户端配置文件设置	141

OCSP 统计计数器	143
配置管理员访问策略	144
管理员访问设置	145
配置最大数量的并发管理会话和登录横幅	145
允许从“选择 IP 地址” (Select IP Addresses) 对思科 ISE 进行管理访问	145
为管理员帐户配置密码策略	146
配置管理员会话超时	147
终止活动管理会话	147
更改管理员名称	148
管理员访问设置	148
管理员密码策略设置	148
会话超时和会话信息设置	150

---

**第 6 章**

<b>维护和监控</b>	<b>151</b>
<b>152</b>	
在思科 ISE 中启用	152
配置网络访问设置	153
通过 创建网络访问的授权配置文件	153
通过 为网络访问创建例外策略	154
隔离和取消隔离流程	154
NAS 端口关闭流程	155
终端清除设置	156
隔离的终端在策略更改后不会重新进行身份验证	157
当无法找到 IP 地址或 MAC 地址时，操作失败。	157
通过外部身份验证的管理员无法执行操作	158
备份数据类型	158
备份和恢复存储库	158
创建存储库	159
存储库设置	160
按需备份和计划备份	160
执行按需备份	161

- 按需备份设置 162
- 计划备份 162
- 计划备份设置 164
- 使用 CLI 备份 164
- 备份历史记录 164
- 备份失败 165
- 思科 ISE 恢复操作 165
  - 数据恢复指南 165
  - 从 CLI 恢复配置或监控（操作）备份 167
  - 从 GUI 恢复配置备份 168
  - 恢复监控数据库 169
    - 在独立环境中恢复监控（运行）备份 169
    - 通过管理和监控角色恢复监控备份 170
    - 通过监控角色恢复监控备份 170
  - 恢复历史记录 171
- 导出身份验证和授权策略配置 171
- 在分布式环境中同步主节点和辅助节点 171
- 恢复独立和分布式部署中断开的节点 172
  - 使用现有 IP 地址和主机名恢复分布式部署中断开连接的节点 172
  - 使用新 IP 地址和主机名恢复分布式部署中断开的节点 173
  - 使用现有 IP 地址和主机名恢复独立部署中的节点 173
  - 使用新 IP 地址和主机名恢复独立部署中的节点 174
- 配置回滚 174
  - 在分布式部署出现故障的情况下恢复主节点 174
  - 在分布式部署出现故障的情况下恢复辅助节点 175
- 思科 日志记录机制 175
  - 配置系统日志清除设置 176
- 思科 ISE 系统日志 176
- 配置远程系统日志收集位置 177
- 思科 ISE 消息代码 178
  - 设置消息代码的严重性级别 178

思科 ISE 消息目录	179
调试日志	179
查看节点的日志记录组件	179
配置调试日志严重性级别	180
终端调试日志收集器	180
下载特定终端的调试日志	180
集合过滤器	181
配置集合过滤器	181
事件抑制绕行过滤器	182
思科 ISE 报告	182
运行并查看报告	182
报告导航	183
导出报告	183
我的报告	184
安排思科 ISE 报告	185
使用案例：计划的报告	186
添加收藏的报告	187
思科 ISE 活动 RADIUS 会话	187
更改 RADIUS 会话的授权	188
可用报告	189

---

**第 7 章**

<b>设备管理</b>	<b>201</b>
TACACS+ 设备管理	201
设备管理工作中心	202
设备管理策略集	203
创建设备管理策略集	203
设备管理 - 授权策略结果	204
TACACS+ 命令集	204
命令集中的通配符和正则表达式	204
命令行和命令集列表匹配	205
含多个命令集的处理规则	206

创建 TACACS+ 命令集	206
TACACS+ 配置文件	207
创建 TACACS+ 配置文件	208
通过 CLI 更改启用密码	208
配置全局 TACACS+ 设置	209
从思科安全 ACS 将数据迁移至思科 ISE	209
监控设备管理活动	210
TACACS 实时日志	210

---

## 第 8 章

### 访客和安全 WiFi 213

思科 ISE 访客服务	213
分布式环境中的最终用户访客门户和发起人门户	214
访客和发起人帐户	214
访客类型和用户身份组	215
创建或编辑访客类型	215
禁用访客类型	217
安排清除过期访客帐户的时间	218
添加用于创建访客帐户的自定义字段	219
为邮件通知指定邮箱地址和 SMTP 服务器	219
分配访客位置和 SSID	219
访客密码策略规则	220
设置访客密码策略和到期时间	221
访客用户名策略规则	221
设置访客用户名策略	221
SMS 运营商和服务	222
配置 SMS 网关以向访客发送 SMS 通知	222
访客门户	223
访客门户的凭证	223
访客使用热点访客门户进行访问	224
访客使用需要提供凭证的访客门户进行访问	224
员工使用需要提供凭证的访客门户进行访问	225

访客设备合规性	225
访客门户配置任务	225
启用策略服务	226
为访客门户添加证书	226
创建外部身份源	226
创建身份源序列	227
创建终端身份组	227
创建热点访客门户	228
创建发起人管理的访客门户	229
创建自注册访客门户	230
授权门户	230
自定义访客门户	232
发起人门户	232
在发起人门户上管理客户帐户	232
管理发起人帐户	233
为创建发起人帐户配置帐户内容	236
配置发起人门户流程	237
启用策略服务	237
添加用于访客服务的证书	238
创建外部身份源	238
创建身份源序列	238
创建发起人门户	239
自定义发起人门户	240
为创建发起人帐户配置帐户内容	240
发起人无法登录发起人门户	240
监控访客和发起人活动	241
指标控制面板	241
AUP 接受状态报告	241
访客记账报告	241
主访客报告	242
发起人登录和审核报告	242

访客门户和发起人门户的审核日志记录	242
访客访问 Web 身份验证选项	242
采用集中式 Web 身份验证流程的 NAD	243
使用本地 Web 身份验证流程的无线 LAN 控制器	244
带本地网络身份验证进程的有线 NAD	245
Login.html 页面所需的 IP 地址和端口值	245
在 NAD 上启用的 HTTPS 服务器	246
NAD 自定义身份验证代理 Web 页面的支持	246
在 NAD 上配置 Web 身份验证	246
设备注册 Web 身份验证流程	247
访客门户设置	248
门户标识设置	248
热点访客门户的门户设置	249
热点访客门户的可接受使用政策 (AUP) 页面设置	251
热点门户的访问后横幅页面设置	252
需要提供凭证的访客门户的门户设置	252
需要提供凭证的访客门户的登录页面设置	254
需要提供凭证的访客门户的自助注册页面设置	254
自行注册成功页面设置	259
需要提供凭证的访客门户的可接受使用政策 (AUP) 页面设置	260
需要提供凭证的访客门户的访客更改密码设置	261
需要提供凭证的访客门户的访客设备注册设置	261
需要提供凭证的访客门户的 BYOD 设置	261
需要提供凭证的访客门户的登录后横幅页面设置	263
需要提供凭证的访客门户的访客设备合规性设置	263
访客门户的 VLAN DHCP 释放页面设置	263
访客门户的身份验证成功设置	264
访客门户的支持信息页面设置	265
发起人门户应用设置	266
门户标识设置	266
发起人门户的门户设置	267

发起人门户的登录页面设置	269
发起人门户的可接受使用政策 (AUP) 页面设置	269
发起人门户的发起人更改密码设置	270
发起人门户的登录后横幅页面设置	270
发起人门户的支持信息页面设置	270
自定义从发起人门户发送至访客的通知	272
自定义发起人门户的“管理和审批”选项卡	272
访客和发起人门户的全局设置	272
访客类型设置	273
发起人组设置	273
最终用户门户	276
自定义最终用户 Web 门户	276
门户内容类型	278
门户的基本自定义	279
修改门户主题颜色	279
更改门户显示语言	280
更改门户图标、图像和徽标	280
更新门户的横幅和页脚元素	281
更改标题、说明、按钮和标签文本	282
格式和样式文本框内容	282
用于门户页面自定义的变量	283
查看您的自定义	286
门户的高级自定义	286
启用高级门户自定义	287
门户的主题和结构 CSS 文件	287
使用 jQuery Mobile 更改主题颜色	288
使用 jQuery Mobile 更改主题颜色	289
基于位置的自定义	290
基于用户设备类型的自定义	291
导出门户的默认主题 CSS 文件	291
创建自定义门户主题 CSS 文件	292



在门户内容中嵌入链接	292
插入动态文本更新的变量	293
使用源代码设置文本格式和包含链接	294
将图像添加为广告	295
设置轮播广告	296
根据访客位置自定义问候语	298
根据用户设备类型自定义问候语	299
修改门户页面布局	300
导入自定义门户主题 CSS 文件	302
删除自定义门户主题	302
查看您的自定义	303
门户语言自定义	303
导出语言文件	305
从语言文件添加或删除语言	305
导入更新的语言文件	306
自定义访客通知、审批和错误消息	307
自定义邮件通知	307
自定义 SMS 文本消息通知	308
自定义打印通知	309
自定义审批请求邮件通知	309
编辑错误消息	310
门户页面标题、内容和标签的字符限制	311
门户页面标题、内容和标签的字符限制	311
门户自定义	313
最终用户门户页面布局的 CSS 类和说明	313
门户语言文件的 HTML 支持	314
黑名单门户语言文件的 HTML 支持	315
自带设备门户语言文件的 HTML 支持	315
客户端调配门户语言文件的 HTML 支持	316
凭证访客门户语言文件的 HTML 支持	317
热点访客门户语言文件的 HTML 支持	320

- 对移动设备管理门户语言文件的 HTML 支持 321
- 我的设备门户语言文件的 HTML 支持 322
- 发起人门户语言文件的 HTML 支持 323

---

**第 9 章****资产可视性 327**

- 使用外部身份库对思科 ISE 进行管理访问 328
  - 外部身份验证和授权 329
    - 使用外部身份库配置基于密码的身份验证 329
    - 创建外部管理员组 329
    - 为外部管理员组配置菜单访问和数据访问权限 330
    - 创建用于外部管理员身份验证的 RBAC 策略 330
  - 使用外部身份库配置管理员访问权限以使用内部授权进行身份验证 331
    - 外部身份验证流程 331
- 外部身份源 332
  - LDAP 身份源设置 332
  - RADIUS 令牌身份源设置 337
  - RSA SecurID 身份源设置 337
- 思科 ISE 用户 339
  - 用户身份 339
  - 用户组 339
  - 用户身份组 339
  - 用户角色 340
  - 用户帐户自定义属性 340
  - 用户身份验证设置 340
- 内部用户操作 341
  - 添加用户 341
  - 导出思科 ISE 用户数据 342
  - 导入思科 ISE 内部用户 342
  - 终端设置 342
  - 从 LDAP 设置导入终端 344
- 身份组操作 345

创建用户身份组	345
导出用户身份组	345
导入用户身份组	346
终端身份组设置	346
内部和外部身份源	347
创建外部身份源	348
证书身份验证配置文件	349
添加证书身份验证配置文件	349
将 Active Directory 用作外部身份源	349
支持 Active Directory 的身份验证协议和功能	350
用于授权策略的 Active Directory 属性和组检索	351
基于证书的身份验证的 Active Directory 证书检索	351
Active Directory 用户身份验证流程	352
支持 Active Directory 多域林	352
将 Active Directory 与思科集成的前提条件	352
执行各种操作所需的 Active Directory 帐户权限	353
必须开放用于通信的网络端口	354
DNS 服务器	354
将 Active Directory 配置为外部身份源	354
添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点	355
添加域控制器	356
对被动 ID 配置 WMI	357
退出 Active Directory 域	358
配置身份验证域	359
配置 Active Directory 用户组	359
配置 Active Directory 用户和计算机属性	360
修改密码更改、设备身份验证和设备访问限制设置	361
对 Active Directory 多加入配置的支持	361
创建新范围，添加 Active Directory 加入点	362
身份重写	362
启用身份重写	363

身份解析设置	364
避免身份解析问题	364
配置身份解析设置	364
对用户进行 Active Directory 身份验证测试	365
删除 Active Directory 配置	365
查看节点的 Active Directory 加入	366
诊断 Active Directory 问题	366
启用 Active Directory 调试日志	367
获取 Active Directory 日志文件来进行故障排除	367
Active Directory 警报和报告	367
Active Directory 高级调整	368
使用 Active Directory 设置思科 ISE 的补充信息	368
在 Active Directory 中配置组策略	368
配置 Odyssey 5.X 请求方，依据 Active Directory 对 EAP-TLS 计算机进行身份验证	369
为机器身份验证配置代理	370
LDAP	370
LDAP 目录服务	370
多个 LDAP 实例	370
LDAP 故障切换	371
LDAP 连接管理	371
LDAP 用户身份验证	371
在授权策略中使用的 LDAP 组和属性检索	372
LDAP 服务器返回的错误	373
LDAP 用户查找	374
LDAP MAC 地址查找	374
添加 LDAP 身份源	374
LDAP 身份源设置	375
配置主要和辅助 LDAP 服务器	380
允许思科 ISE 从 LDAP 服务器获取属性	380
从 LDAP 服务器检索组成员身份详细信息	381
从 LDAP 服务器检索用户属性	381

使用 LDAP 身份源进行安全身份验证	382
RADIUS 令牌身份源	382
支持 RADIUS 令牌服务器的身份验证协议	383
RADIUS 令牌服务器用于通信的端口	383
RADIUS 共享密钥	383
RADIUS 令牌服务器中的故障切换	383
RADIUS 令牌服务器中的可配置密码提示	383
RADIUS 令牌服务器用户身份验证	384
RADIUS 令牌服务器中的用户属性缓存	384
身份序列中的 RADIUS 身份源	384
RADIUS 服务器为所有错误返回相同消息	384
Safeword 服务器支持特殊用户名格式	385
RADIUS 令牌服务器中的身份验证请求和响应	385
RADIUS 令牌身份源设置	386
添加 RADIUS 令牌服务器	386
删除 RADIUS 令牌服务器	387
RSA 身份源	387
思科 ISE 和 RSA SecurID 服务器集成	388
思科 ISE 中的 RSA 配置	388
针对 RSA SecurID 服务器进行的 RSA 代理身份验证	388
思科 ISE 分布式环境中的 RSA 身份源	388
思科 ISE 部署中的 RSA 服务器更新	388
覆盖自动 RSA 路由	388
RSA 节点密钥重置	389
RSA 自动可用性重置	389
RSA SecurID 身份源设置	389
添加 RSA 身份源	390
导入 RSA 配置文件	391
为思科 ISE 服务器配置选项文件并重置 SecurID 和 sdstatus.12 文件	391
为 RSA 身份源配置身份验证控制选项	392
配置 RSA 提示	392

配置 RSA 消息	392
身份源序列	393
创建身份源序列	393
删除身份源序列	394
报告中的身份源详细信息	394
身份验证面板	394
身份源报告	395
网络上已分析的终端	395
分析器条件设置	395
思科 ISE 分析服务	396
使用分析服务的终端资产	396
思科 ISE 分析器队列限制配置	396
Martian IP 地址	397
在思科 ISE 节点中配置分析服务	397
分析服务使用的网络探测功能	398
IP 地址和 MAC 地址绑定	398
NetFlow 探测功能	398
DHCP 探测功能	399
DHCP 桥接模式下的无线 LAN 控制器配置	400
DHCP SPAN 探测功能	400
HTTP 探测功能	400
HTTP SPAN 探测功能	400
无法在 VMware 上运行的思科 ISE 中收集 HTTP 属性	401
pxGrid 探测器	401
RADIUS 探测功能	402
网络扫描 (NMAP) 探测功能	402
NMAP 手动子网扫描的 SNMP 只读社区字符串	403
最新网络扫描结果	403
DNS 探测功能	404
DNS FQDN 查找	404
在桥接模式下通过 Inline Posture 节点部署执行 DNS 查找	404

在 WLC Web 界面中配置呼叫站 ID 类型	405
SNMP 查询探测功能	405
使用 SNMP 查询的思科发现协议支持	405
使用 SNMP 查询的链路层发现协议支持	406
SNMP 陷阱探测功能	407
为每个思科 ISE 节点配置探测功能	407
设置 CoA、SNMP RO 社区和终端属性过滤器	408
对已通过身份验证的终端的授权更改全局配置	409
发出授权更改的使用案例	409
发出授权更改的豁免	410
对各类型 CoA 配置发出的授权更改	411
针对 ISE 数据库持久性和性能的属性过滤器	411
过滤器终端属性的全局设置	412
从思科 IOS 传感器嵌入式交换机收集属性	413
思科 IOS 传感器嵌入式网络接入设备	414
支持思科 IOS 传感器的网络访问设备的配置核对表	414
分析器条件	415
分析网络扫描操作	416
创建新的网络扫描操作	416
NMAP 操作系统扫描	417
操作系统端口	417
NMAP SNMP 端口扫描	421
NMAP 通用端口扫描	421
通用端口	422
创建分析器条件	422
终端分析策略规则	423
终端分析策略设置	423
创建终端分析策略	426
每个终端分析策略的授权更改配置	428
导入终端分析策略	428
导出终端分析策略	429

预定义终端分析策略	429
在升级期间覆盖预定义终端分析策略	430
无法删除终端分析策略	430
用于 Draeger 医疗设备的预定义分析策略	431
用于未知终端的终端分析策略	431
用于静态添加的终端的终端分析策略	431
静态 IP 设备的终端分析策略	432
终端分析策略匹配	432
用于授权的终端分析策略	432
终端分析策略分组为逻辑配置文件	432
创建逻辑配置文件	433
分析例外操作	433
创建例外操作	433
使用策略和身份的静态分配创建终端	434
从 CSV 文件导入终端	434
可用于终端的默认导入模板	435
导入过程中重新分析的未知终端	435
静态分配导入过程中保留的终端的策略和身份组	436
不导入具有无效属性的终端	436
从 LDAP 服务器导入终端	437
以 CSV 文件导出终端	437
已识别的终端	438
策略服务节点数据库中本地存储的已识别终端	438
集群中的策略服务节点	439
创建终端身份组	440
已识别终端划分为终端身份组	440
为终端创建的默认终端身份组	440
为匹配的终端分析策略创建的终端身份组	441
向终端身份组中添加静态终端	441
在身份组中添加或删除终端后重新分析动态终端	441
用于授权规则的终端身份组	442



分析器源服务	442
配置分析器源服务	442
删除终端分析策略的更新	443
分析器报告	444
思科 ISE 与思科 NAC 设备集成	444
管理节点中的思科 Clean Access Manager 配置	444
思科 ISE 分析器和思科 Clean Access Manager 通信	445
添加思科 Clean Access Manager	445
客户端设备上的代理下载问题	446
终端	446
终端设置	447
从 LDAP 设置导入终端	448
终端分析策略设置	449
IF-MIB	453
SNMPv2-MIB	453
IP-MIB	454
CISCO-CDP-MIB	454
CISCO-VTP-MIB	455
CISCO-STACK-MIB	456
BRIDGE-MIB	456
OLD-CISCO-INTERFACE-MIB	456
CISCO-LWAPP-AP-MIB	456
CISCO-LWAPP-DOT11-CLIENT-MIB	458
CISCO-AUTH-FRAMEWORK-MIB	458
EEE8021-PAE-MIB: RFC IEEE 802.1X	459
HOST-RESOURCES-MIB	459
LLDP-MIB	459
终端的会话跟踪	460
从目录清除会话	462
终端的全局搜索	462

公司网络上的个人设备 (BYOD)	465
分布式环境中的最终用户设备门户	465
设备门户的全局设置	466
个人设备门户	466
访问设备门户	467
黑名单门户	467
自带设备门户	467
客户端调配门户	468
移动设备管理门户	468
我的设备门户	468
BYOD 部署选项和状态流	469
限制员工注册的个人设备的数量	471
支持使用本地请求方注册设备	471
本地请求方支持的操作系统	472
允许员工使用需要提供凭证的访客门户注册个人设备	472
提供用于重新连接 BYOD 注册流程的 URL	472
设备门户配置任务	473
启用策略服务	474
将证书添加到设备门户	474
创建外部身份源	475
创建身份源序列	475
创建终端身份组	476
编辑黑名单门户	476
创建 BYOD 门户	478
创建客户端调配门户	480
创建 MDM 门户	481
创建我的设备门户	482
创建授权配置文件	483
创建授权配置文件	484
创建授权策略规则	484
自定义设备门户	485

管理员工添加的个人设备	485
显示员工添加的设备	485
向我的设备门户添加设备时出错	485
从我的设备门户删除的设备仍保留在终端数据库中	486
限制员工注册的个人设备的数量	486
监控我的设备门户和终端活动	486
我的设备登录和审核报告	486
注册的终端报告	487

---

**第 11 章****安全接入 489**

管理网络设备组	489
网络设备组设置	489
网络设备组导入设置	490
网络设备组	491
思科 ISE 在策略评估中使用的网络设备属性	492
将网络设备组导入到思科 ISE	492
从思科 ISE 导出网络设备组	492
管理网络设备组	493
网络设备组设置	493
网络设备组导入设置	493
在思科 ISE 中导入模板	494
网络设备导入模板格式	494
网络设备组导入模板格式	497
移动设备管理器与思科 ISE 的互操作性	498
支持的移动设备管理使用情形	498
支持的 MDM 服务器	501
移动设备管理服务器使用的端口	501
移动设备管理集成流程	502
使用思科 ISE 设置移动设备管理服务器	502
将移动设备管理服务器证书导入思科 ISE	503
在思科 ISE 中配置移动设备管理服务器	503

在思科 ISE 中定义 Microsoft System Center Configuration Manager 服务器	506
为 WMI 访问开放防火墙端口	506
配置用于重定向未注册设备的授权配置文件	507
为 MDM 使用案例配置授权策略规则	507
在无线控制器上配置 ACL 以实现 MDM 互操作性	508
擦除或锁定设备	509
查看移动设备管理报告	510
查看移动设备管理日志	510

---

**第 12 章****分段 511**

策略集	511
身份验证策略	512
身份验证失败类型 - 故障转移	514
配置身份验证策略	515
基于密码的身份验证	516
使用加密密码和加密技术的安全身份验证	516
身份验证方法和授权权限	516
身份验证面板	516
查看身份验证结果	517
身份验证报告和故障排除工具	517
授权策略	518
思科 ISE 授权配置文件	518
授权配置文件的权限	518
可下载 ACL	519
针对 Active Directory 用户授权的设备访问限制	520
配置授权策略和配置文件的指南	520
配置授权策略	521
授权配置文件设置	523
授权策略和例外	526
策略条件	526
字典和字典属性	527

系统定义的字典和字典属性	532
显示系统字典和字典属性	532
用户定义的字典和字典属性	532
创建用户定义的字典	532
创建用户定义的字典属性	533
RADIUS 供应商字典	533
创建 RADIUS 供应商字典	533
创建 RADIUS 供应商字典属性	534
RADIUS 供应商字典属性设置	534
浏览 Conditions Studio	536
配置、编辑和管理策略条件	540
特殊网络访问条件	545
配置设备网络条件	545
配置设备端口网络条件	545
配置终端站网络条件	546
创建时间和日期条件	546
在授权策略中使用 IPv6 条件属性	547
用于身份验证的协议设置	549
支持的身份验证协议	549
将 EAP-FAST 用作身份验证协议的指南	549
配置 EAP-FAST 设置	550
为 EAP-FAST 生成 PAC	550
EAP-FAST 设置	551
PAC 设置	551
配置 EAP-TLS 设置	552
EAP-TLS 设置	553
配置 PEAP 设置	553
PEAP 设置	553
配置 RADIUS 设置	553
RADIUS 设置	554
配置安全设置	555

思科 ISE 中的 RADIUS 协议支持	558
允许的协议	559
PAC 选项	565
将思科 ISE 用作 RADIUS 代理服务器	568
配置外部 RADIUS 服务器	569
定义 RADIUS 服务器序列	569
网络访问服务	570
为网络访问定义允许的协议	570
用户的网络接入	571
从非思科设备启用 MAB	576
从思科设备启用 MAB	577
TrustSec 架构	578
TrustSec 组件	579
TrustSec 术语	580
TrustSec 支持的交换机和需要的组件	581
配置 TrustSec 全局设置	581
TrustSec 设置	581
配置 TrustSec 设备	584
OOB TrustSec PAC	584
从设置屏幕生成 TrustSec PAC	584
从网络设备屏幕生成 TrustSec PAC	584
从“网络设备”(Network Devices)列表屏幕生成 TrustSec PAC	585
按钮	585
配置思科 TrustSec AAA 服务器	586
安全组配置	586
添加安全组	587
将安全组导入思科 ISE	587
从思科 ISE 导出安全组	588
添加安全组访问控制列表	588
出口策略	590
源树视图	590

目标树视图	591
矩阵视图	591
矩阵维度	591
压缩视图	591
矩阵操作	591
出口策略表单元格配置	592
添加出口策略单元格映射	592
导出出口策略	593
导入出口策略	593
从出口策略配置 SGT	593
监控模式	594
监控模式功能	594
未知安全组	594
默认策略	594
SGT 分配	595
NDAC 授权	595
配置 NDAC 授权	595
配置最终用户授权	596
添加单个 IP 到 SGT 映射	596
添加组 IP 到 SGT 映射	597
导入安全组映射主机	597
导出安全组映射主机	598
部署 IP 到 SGT 映射	598
TrustSec 配置和策略推送	599
支持 CoA 的网络设备	599
向不支持 CoA 的设备推送配置更改	599
SSH 密钥验证	600
环境 CoA 通知流程	601
环境 CoA 触发器	602
更新 SGACL 内容流程	603
启动更新 SGACL 命名的列表 CoA	604

策略更新 CoA 通知流程	604
更新 SGT 矩阵 CoA 流程	605
发起从出口策略更新 SGT 矩阵 CoA	605
TrustSec CoA 摘要	605
按用户报告运行前 N 个 RBACL 丢包	606

---

**第 13 章****合规性 609**

终端安全评估类型	610
安全评估管理设置	611
客户端安全评估要求	611
客户端的计时器设置	612
设定补救计时器，使客户端在指定时间内补救	612
设置网络转换延迟计时器，使客户端实现转换	612
将登录成功窗口设置为自动关闭	613
设置非代理设备的终端安全评估状态	613
安全评估租约	613
定期重新评估	614
配置定期重新评估	615
安全评估故障排除设置	615
安全评估常规设置	616
将安全评估更新下载至思科 ISE	617
思科 ISE 离线更新	618
618	
自动下载安全评估更新	619
安全评估可接受使用政策配置设置	619
配置安全评估的可接受使用政策	621
安全评估条件	621
简单安全评估条件	621
创建简单安全评估条件	622
复合安全评估条件	622
创建复合安全评估条件	622



字典复合条件设置	623
用于在 Windows 客户端中启用自动更新的预定义条件	624
预配置的防病毒和反间谍软件条件	625
防病毒和反间谍软件支持图表	625
Inline Posture 节点	625
Inline Posture 节点的安装	626
注册 Inline Posture 节点	626
合规性模块	626
检查安全评估合规性	628
创建补丁管理条件	628
创建磁盘加密条件	629
安全评估条件设置	629
文件条件设置	629
注册表条件设置	630
应用条件设置	631
服务条件设置	631
安全评估复合条件设置	631
防病毒条件设置	632
反间谍软件复合条件设置	633
字典简单条件设置	635
字典复合条件设置	635
配置安全评估策略	636
配置 AnyConnect 工作流程	637
客户端安全评估	638
终端安全状态评估选项	639
安全评估补救选项	639
安全评估的自定义条件	639
自定义安全评估补救措施	639
添加反间谍程序补救	639
添加防病毒软件补救	640
添加文件补救	640

- 添加启动程序补救 640
  - 排除启动程序补救故障 641
- 添加链接补救 641
- 添加 Windows 服务器更新服务补救 642
- 添加 Windows 更新补救 642
- 终端安全评估要求 642
  - 客户端系统处于不合规状态 643
  - 创建客户端安全评估要求 644
- 重新进行安全评估配置设置 645
- 自定义安全评估权限 646
- 配置标准授权策略 647
- 安全评估故障排除工具 647
- 在思科 ISE 中配置客户端调配 647
- 客户端调配资源 648
  - 从思科添加客户端调配资源 649
  - 从本地计算机添加思科提供的客户端调配资源 650
  - 从本地计算机添加 AnyConnect 的客户创建资源 650
- 创建本地请求者配置文件 651
  - 本地请求者配置文件设置 652
- 思科 AnyConnect 安全移动 653
  - 创建 AnyConnect 配置 654
  - 创建终端安全评估代理配置文件 655
  - 客户端 IP 地址刷新配置 655
  - 安全评估协议设置 658
- 思科 Web 代理 658
  - 思科 NAC 代理 XML 文件安装目录 658
  - 适用于 Windows 客户端的思科 NAC 代理 658
    - 从 Windows 7 及早期版本客户端中卸载思科 NAC 代理 659
    - 在 Windows 8 客户端中卸载思科 NAC 代理 659
    - Windows 8 Metro 和 Metro 应用支持 - Toast 通知 659
  - 适用于 Macintosh 客户端的思科 NAC 代理 660

- 从 Macintosh 客户端卸载思科 NAC 代理 660
- 思科 Web 代理 660
- 思科 NAC 代理日志 661
- 为思科 NAC 代理创建代理自定义文件 661
  - 自定义 nac\_login.xml 文件模板 661
  - 自定义 nacStrings\_xx.xml 文件模板 662
  - 扩展的 nacStrings\_xx.xml 文件示例 672
  - UpdateFeed.xml 描述符文件模板 672
  - 使用创建配置文件功能生成的 XML 文件示例 673
- 配置客户端调配资源策略 674
  - 在客户端调配策略中配置思科 ISE 安全评估代理 675
  - 为个人设备配置本地请求方 675
- 客户端调配报告 676
- 客户端调配事件日志 676
- 客户端调配门户语言文件的 HTML 支持 677

---

## 第 14 章

### 威胁控制 679

- 以威胁防护为中心的 NAC 服务 679
  - 启用威胁中心 NAC 服务 682
  - 添加 Sourcefire FireAMP 适配器 682
  - 思科 ISE 中的漏洞评估支持 683
    - 支持的漏洞评估生态系统合作伙伴 683
    - Qualys 漏洞评估流程 684
  - 启用并配置漏洞评估服务 684
    - 启用威胁中心 NAC 服务 684
    - 配置 Qualys 适配器 685
    - 配置授权配置文件 688
    - 配置隔离易受攻击的终端的例外规则 688
  - 漏洞评估日志 688
- 部署和节点设置 689
  - 部署节点列表窗口 689

常规节点设置	690
分析节点的设置	693
Inline Posture 节点设置	695
受信任证书设置	695
证书存储设置	697
自签证书设置	697
证书签名请求设置	699
终端证书概述窗口 (Endpoint Certificate Overview Window)	703
系统证书导入设置	704
受信任证书列表	705
受信任证书导入设置	706
OCSP 客户端配置文件设置	707
内部 CA 设置	709
证书模板设置	710
日志记录设置	711
远程日志记录目标设置	711
配置日志记录类别	712
维护设置	713
存储库设置	713
按需备份设置	714
计划备份设置	715
管理员访问设置	715
管理员密码策略设置	716
会话超时和会话信息设置	717
TrustSec 设置	718
设置	720
安全评估常规设置	720
重新进行安全评估配置设置	721
安全评估可接受使用政策配置设置	722
EAP-FAST 设置	723
PAC 设置	724

EAP-TLS 设置	725
PEAP 设置	725
RADIUS 设置	725
SMS 网关设置	727
身份管理	728
终端	728
终端设置	729
从 LDAP 设置导入终端	730
终端身份组设置	731
外部身份源	732
LDAP 身份源设置	732
RADIUS 令牌身份源设置	738
RSA SecurID 身份源设置	738
网络资源	739
对会话感知网络 (SAnet) 的支持	739
网络设备	739
网络设备定义设置	740
默认网络设备定义设置	746
设备安全设置	748
网络设备导入设置	748
管理网络设备组	749
网络设备组设置	749
网络设备组导入设置	750
外部 RADIUS 服务器设置	750
RADIUS 服务器序列	751
NAC 管理器设置	753
设备门户管理	753
配置设备门户设置	753
设备门户的全局设置	753
设备门户的门户标识设置	754
黑名单门户的门户设置	755

BYOD 和 MDM 门户的门户设置	756
BYOD 门户的 BYOD 设置	758
客户端调配门户的门户设置	759
MDM 门户的员工移动设备管理设置	761
我的设备门户的门户设置	762
我的设备门户的登录页面设置	764
我的设备门户的可接受使用策略页面设置	764
我的设备门户的登录后横幅页面设置	765
我的设备门户的员工更改密码设置	765
管理我的设备门户的设备设置	765
为我的设备门户自定义添加、编辑和定位设备	767
设备门户的支持信息页面设置	767

---

**第 15 章****Cisco pxGrid 769**

思科 pxGrid 节点	769
思科 pxGrid 客户端和功能管理	770
启用 pxGrid 服务	770
部署思科 pxGrid 节点	771
思科 pxGrid 实时日志	771

---

**第 16 章****集成 773**

使交换机能够支持标准 Web 身份验证	773
为综合 RADIUS 事务定义本地用户名和密码	774
配置 NTP 服务器以获得准确的日志和记账时间戳	774
启用 AAA 功能的命令	774
交换机上的 RADIUS 服务器配置	775
将交换机配置为向 Inline Posture 节点发送 RADIUS 记帐开始/停止消息	775
启用交换机处理 RADIUS 更改授权 (CoA)	776
在交换机端口上启用设备跟踪和 DHCP 监听	776
为交换机端口启用 802.1X 基于端口的身份验证	776
为关键身份验证启用 EAP	777

使用恢复延迟来限制 AAA 请求	777
根据实施状态定义 VLAN	777
交换机上的本地（默认）访问列表 (ACL) 定义	778
对 802.1X 和 MAB 启用交换机端口	779
启用 EPM 日志记录	781
启用交换机以接收 SNMP 陷阱	781
在交换机上启用 SNMP v3 查询以进行分析	781
启用 MAC 通知陷阱以使分析器进行收集	781
在交换机上配置 RADIUS 空闲超时	782
用于 iOS 请求方调配的无线控制器配置	782
Apple 设备的无线 LAN 控制器支持	782
在无线控制器上配置 ACL 以实现 MDM 互操作性	783

---

## 第 17 章

### 故障排除 785

思科 ISE 中的监控和故障排除服务	785
网络权限框架	785
网络权限框架事件流程	786
用于监控和故障排除功能的用户角色和权限	786
监控数据库中存储的数据	787
网络处理状态	787
监控网络处理状态	787
网络身份验证	787
监控网络身份验证	788
Smart Call Home	788
Smart Call Home 配置文件	788
Anonymous Reporting	788
为 Smart Call Home 服务进行注册	789
日志收集	789
警报系统日志收集位置	789
RADIUS 实时日志	790
实时身份验证	792

监控实时身份验证	793
在“实时身份验证”(Live Authentications) 页面过滤数据	793
RADIUS 实时会话	794
导出摘要	796
身份验证摘要报告	798
网络接入问题故障排除	798
故障排除诊断工具	798
RADIUS 身份验证故障排除工具	798
对意外 RADIUS 身份验证结果进行故障排除	799
执行网络设备命令诊断工具	799
执行思科 IOS show 命令以检查配置	800
评估配置验证程序工具	800
解决网络设备配置问题	800
排除终端安全评估故障	800
用于验证传入流量的 TCP Dump 实用工具	801
使用 TCP Dump 监控网络流量	801
保存 TCP Dump 文件	802
比较终端或用户的意外 SGACL	802
出口策略诊断流程	803
使用 SXP-IP 映射排除支持 TrustSec 的网络中的连接问题	803
通过 IP-SGT 映射解决支持 TrustSec 的网络中的连接问题	803
设备 SGT 工具	804
通过对比设备 SGT 映射排除启用 TrustSec 的网络中的连接故障	804
获取其他故障排除信息	804
思科 支持捆绑包	804
支持捆绑包	805
下载思科 日志文件。	805
思科 调试日志	806
获取调试日志	806
思科 组件和相应的调试日志	807
下载调试日志	808





# 第 1 章

## 新信息及变更内容

- [新信息及变更内容](#), on page 1

## 新信息及变更内容

下表总结了新增和更改的功能，以及有关记录这些功能的位置的信息。

**Table 1:** 思科 ISE 版本 3.2 中新增和变更的功能

特性	说明
<b>思科 ISE 版本 3.2 补丁 5</b>	
仅为思科 ISE 提交 TAC 支持案例	从思科 ISE 版本 3.2 补丁 5 开始，您只能从思科 ISE GUI 打开思科 ISE 的 TAC 支持案例。
使用“立即同步”(Sync Now) 进行按需 pxGrid 直接数据同步	从思科 ISE 版本 3.2 补丁 5 开始，您可以使用 <b>立即同步 (Sync Now)</b> 功能从 pxGrid Direct 连接器执行数据按需同步。您可以按需执行完全同步和增量同步。可以通过思科 ISE GUI 或使用 OpenAPI 来执行按需数据同步。 <a href="#">请参阅使用“立即同步”(Sync Now) 进行按需 pxGrid 直接数据同步。</a>
<b>思科 ISE 版本 3.2 补丁 4</b>	
来自 Cisco Catalyst 9800 无线局域网控制器的 Wi-Fi 设备分析数据	您可以使用与思科 ISE 集成的思科无线局域网控制器的设备分析数据，为 Apple、Intel 和 Samsung 终端创建分析策略、授权条件以及身份验证条件和策略。  <a href="#">请参阅 Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller</a>

特性	说明
客户体验调查	<p>思科 ISE 现在会在管理门户网站上邀请用户参加客户满意度调查。定期管理客户满意度调查有助于我们更好地了解您的思科 ISE 体验，跟踪哪些方面做得好，并确定需要改进的方面。在提交调查后，接下来的 90 天内不会再向您显示其他调查。</p> <p>在所有思科 ISE 部署中，调查都将默认启用。您可以在用户级别或针对思科 ISE 部署禁用调查。</p> <p>请参阅 <a href="#">客户体验调查</a></p>
<b>思科 ISE 版本 3.2 补丁 3</b>	
将外部 LDAP 用户链接到思科 ISE 终端组	<p>从思科 ISE 版本 3.2 补丁 3 开始，您可以使用 <b>动态 (Dynamic)</b> 选项将外部 LDAP 用户组分配给访客设备的终端身份组。有关详细信息，请参阅《思科身份服务引擎管理员指南，版本 3.2》“访客和安全 Wi-Fi”一章中的 <a href="#">创建或编辑访客类型</a>。</p>
门户中的乌克兰语支持	<p>访客、发起人、我的设备和客户端调配门户现在纳入了乌克兰语作为支持的本地化语言。</p>
<b>思科 ISE 版本 3.2 补丁 2</b>	
pxGrid Direct 增强功能	<p>pxGrid Direct 不再是受控引入功能。在从思科 ISE 版本 3.2 或 3.2 补丁 1 升级到思科 ISE 版本 3.2 补丁 2 之前，建议您删除所有已配置的 pxGrid Direct 连接器以及任何使用 pxGrid Direct 连接器数据的授权配置文件和策略。升级到思科 ISE 版本 3.2 补丁 2 后，请重新配置 pxGrid Direct 连接器。</p> <p>请参阅 <a href="#">思科 pxGrid Direct</a></p> <p><b>Note</b> 如果不删除已配置的 pxGrid Direct 连接器，连接器会在升级过程中自动被删除。此删除操作会导致授权配置文件和策略无法编辑和使用，您必须删除并用新的配置文件和策略来取代它。</p>
<b>思科 ISE 版本 3.2 补丁 1</b>	
适用于思科 ISE 的 Meraki 连接器	<p>思科 ISE 3.2 补丁 1 及更高版本支持思科 ISE 和思科 Meraki 集成。思科 ISE 和基于云的思科 Meraki 是支持 TrustSec 的系统，是 TrustSec 策略的策略管理点。如果您同时使用思科和 Meraki 网络设备，则可以将一个或多个思科 Meraki 控制面板连接到思科 ISE，以将 TrustSec 策略和元素从思科 ISE 复制到属于每个组织的思科 Meraki 网络。</p> <p>有关配置 Meraki 连接器的信息，请参阅《思科身份服务引擎管理员指南，版本 3.2》“<a href="#">分段</a>”一章中的“<a href="#">将思科 Meraki 控制面板与思科 ISE 连接</a>”。</p>

特性	说明
支持思科 AI 分析	思科 ISE 3.2 补丁 1 及更高版本支持思科 AI 分析。思科 AI 分析代理从思科 ISE 查询终端数据，并定期将其发送到 AI 云。通过提供基于人工智能的终端分组、自动自定义分析规则和众包终端标签，这些数据可用于减少网络中未知终端的数量。有关详细信息，请参阅《思科 ISE 管理员指南，版本 3.2》“ <a href="#">资产可视性</a> ”一章中的“启用思科 AI 分析”。
<b>思科 ISE 版本 3.2</b>	
安全评估条件脚本支持	您可以创建并上传终端安全评估条件脚本，以检查终端的合规性状态。Windows、MacOS 和 Linux 平台支持此功能。
思科 AnyConnect 更名	思科 AnyConnect 已更名为 Cisco Secure 客户端。尽管思科 ISE GUI 已更新为使用重新命名的术语，但思科 ISE 3.2 仍同时支持重新命名的代理和传统代理。  请参阅 <a href="#">合规性, on page 609</a> 。
系统 360	系统 360 包括 <a href="#">监控</a> 和 <a href="#">日志分析</a> 。  通过 <a href="#">监控</a> 功能，您可以从集中式控制台监控各种应用和系统统计信息，以及部署中所有节点的关键性能指标 (KPI)。KPI 有助于深入了解节点环境的整体运行状况。统计信息提供系统配置和利用率特定数据的简化表示。  思科 ISE 3.2 及更高版本与 Grafana 和 Prometheus 集成。Grafana 是第三方指标控制面板和图形编辑器。它以图形或文本形式表示 Prometheus 数据库中收集的统计信息和计数器。Prometheus 用作数据存储库，以时间序列格式存储 KPI。  <a href="#">日志分析</a> 提供了一个灵活的分析系统，用于对终端身份验证、授权和审计 (AAA) 以及安全评估系统日志数据进行深入分析。您还可以分析 ISE 运行状况摘要和 ISE 进程状态。  Kibana 是一个开放源码数据可视化平台，用于分析和可视化系统日志数据。ElasticSearch 用于存储和索引系统日志数据。
移动设备管理增强功能	当终端未向主 MDM 或 UEM 服务器注册时，或者无法访问主 MDM 或 UEM 服务器时，您可以配置 <a href="#">常规 MDM 或 UEM 设置</a> 以查询多个 MDM 服务器。
ERS API 的开放式 API 规范	ERS API 的 API 规范 (JSON 文件) 可在思科 ISE GUI 的 <a href="#">API 设置 (API Settings)</a> 窗口的 <a href="#">概述 (Overview)</a> 部分中下载 ( <a href="#">管理 (Administration)</a> > <a href="#">系统 (System)</a> > <a href="#">设置 (Settings)</a> > <a href="#">API 设置 (API Settings)</a> > <a href="#">概述 (Overview)</a> )。  此开放式 API JSON 文件可用于使用任何编程语言 (例如 Python、JAVA 等) 自动生成 API 客户端代码。有关开放式 API 规范和工具的其他信息，请参阅 <a href="https://openapi.tools/">https://openapi.tools/</a> 。

特性	说明
ERS API PATCH 请求支持	思科 ISE 现在支持 ERS API 的 PATCH 请求。PATCH 请求有助于更新资源的属性子集。只更新作为请求一部分发送的属性，而不是该资源的整个配置。有关详细信息，请参阅《 <a href="#">API 参考指南</a> 》。
终端情景可视性窗口中具有 GUID 的终端的单个条目	在思科 ISE GUI 的情景可视性 ( <b>Context Visibility</b> ) > 终端 ( <b>Endpoints</b> ) 窗口中，具有 GUID 的终端及其最新的随机 MAC 地址仅列出一次。
在默认或深色模式下查看思科 ISE	现在，您可以在默认（浅色）或深色模式下查看思科 ISE。从思科 ISE 管理员门户的帐户设置 ( <b>Account Settings</b> ) 对话框中选择默认或暗模式。
使用 Microsoft Entra ID 进行 EAP-TLS 和 TEAP 身份验证	思科 ISE 支持基于证书的身份验证和 Microsoft Entra ID 授权。您可以从 Microsoft Entra ID 中选择属性并将其添加到思科 ISE 字典中，以便在授权策略中使用。
管理思科 ISE 用户的密码	从思科 ISE 版本 3.2 开始，作为思科 ISE 的内部用户，您可以使用 <b>密码有效期 (Password Lifetime)</b> 选项来管理启用和登录密码的有效期。 请参阅 <a href="#">思科 ISE 用户, on page 339</a> 。
思科专用 5G 服务	从思科 ISE 版本 3.2 开始，思科 ISE 支持思科专用 5G 和会话管理功能 (SMF) 软件。思科 ISE 为 5G 授权提供策略配置，通过 RADIUS 仅授权和审计流实施。
数据连接	<p>数据连接功能使用开放式数据库连接 (ODBC) 或 Java 数据库连接 (JDBC) 驱动程序来为思科 ISE 提供数据库访问，这样您就可以直接查询数据库服务器，生成您所选择的报告。仅提供对数据的读取访问权限。</p> <p>您可以根据您的业务要求提取有关网络的任何配置或操作数据，并使用它来生成有见地的报告和控制面板。</p> <p><b>Note</b> 如果数据连接功能在思科 ISE 3.2 版有限可用性版本上处于活动状态，则在升级到思科 ISE 3.2 版通用版本时，必须先禁用再启用数据连接功能。</p>
为 PassiveID 登录用户配置授权策略	<p>如果要为 PassiveID 登录用户配置授权策略，请选中 <b>Active Directory 高级设置 (Active Directory Advanced Settings)</b> 窗口中的<b>授权流程 (Authorization Flow)</b> 复选框。</p> <p>您可以配置授权策略，以根据 Active Directory 组成员身份将 SGT 分配给用户。这允许您为 PassiveID 授权创建 TrustSec 策略规则。</p>

特性	说明
安全设置增强功能	<p>如果用了允许 <b>SHA-1 密码 (Allow SHA-1 Ciphers)</b> 选项（在管理 <b>(Administration)</b> &gt; 系统 <b>(System)</b> &gt; 设置 <b>(Settings)</b> &gt; 安全设置 <b>(Security Settings)</b> 下），思科 ISE 将允许使用 SHA-1 密码与以下思科 ISE 组件通信：</p> <ul style="list-style-type: none"> <li>• 管理员访问 UI</li> <li>• 思科 ISE 门户</li> <li>• ERS</li> <li>• pxGrid</li> </ul> <p>默认情况下该选项处于禁用状态。</p> <p>升级到思科 ISE 版本 3.2 时，<b>允许 SHA-1 密码 (Allow SHA-1 Ciphers)</b> 选项将被禁用，即使您在升级前已启用此选项。如果要允许仅使用 SHA-1 密码的客户端与思科 ISE 通信，可以在升级后启用此选项。启用或禁用此选项后，部署中的所有节点都必须重新启动。</p> <p>请参阅 <a href="#">配置安全设置, on page 555</a>。</p>
终端和逻辑配置文件摘要报告	此报告列出逻辑和终端配置文件，以及与这些配置文件匹配的终端数量。
pxGrid Direct	<p>思科 pxGrid Direct 可帮助您连接到为终端属性提供 JSON 数据的外部 REST API。收集的数据基于您在 pxGrid Direct 配置中指定的属性。然后，pxGrid Direct 将收集的数据存储在思科 ISE 数据库中。</p> <p>此数据可用于授权策略。pxGrid Direct 有助于更快地评估和授权终端，因为授权策略中会使用获取的数据。这消除了每次必须对终端进行授权时查询终端属性数据的需要。</p>





## 第 2 章

# 思科 ISE 概述

- 思科 ISE 简介，第 7 页
- 思科 ISE 功能，第 8 页
- 思科 ISE 管理员，第 9 页
- 思科 ISE 管理员组，第 10 页
- 对思科 ISE 进行管理访问，第 15 页

## 思科 ISE 简介

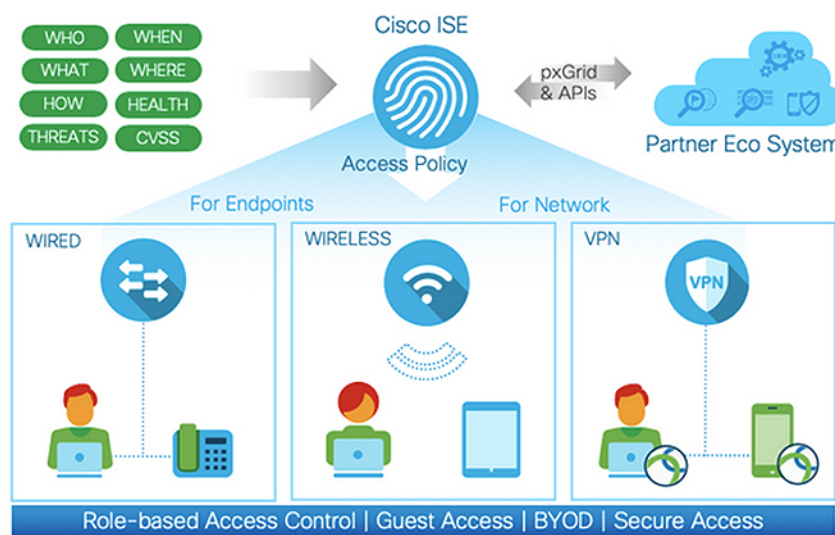


**注释** 此产品的文档集力求使用无偏见语言。在本文档集中，无偏见定义为不暗示基于年龄、残障、性别、种族身份、族群身份、性取向、社会经济地位和交叉性的歧视的语言。由于产品软件的用户界面中使用的硬编码语言，基于 RFP 文档使用的语言或引用的第三方产品使用的语言，文档中可能存在例外情况。

### Cisco ISE

Cisco Identity Services Engine (ISE) is a Network Access Control and Policy Enforcement platform

- Visibility**  
Context about everything touching the network
- Control**  
Network access control and segmentation
- Compliance**  
Enterprises comply to industry regulations



思科身份服务引擎 (ISE) 是一个基于身份的网络访问控制和策略实施系统。它作为一个通用策略引擎，让企业能够控制终端访问和管理网络设备。

您可以利用思科 ISE 确保合规、增强基础设施安全性并简化服务操作。

思科 ISE 管理员可以收集网络的实时情景数据，包括用户和用户组（谁？）、设备类型（什么？）、访问时间（何时？）、访问位置（哪里？）、访问类型（有线、无线或 VPN）（如何？）以及网络威胁和漏洞。

作为思科 ISE 管理员，您可以使用此信息制定网络监管决策。您还可以将身份数据与各种网络元素绑定，以创建监管网络访问和使用的策略。

## 思科 ISE 功能

思科 ISE 软件必须按原样安装。不能在底层操作系统级别安装任何其他第三方应用。

思科 ISE 为您提供以下功能：

- **设备管理 (Device Administration):** 思科 ISE 使用 TACACS+ 安全协议来控制并审核网络设备的配置。它可以促进对谁可以访问哪个网络及更改关联网络设置进行精细控制。网络设备可以配置为向思科 ISE 查询对设备管理员操作所进行的身​​份验证和授权。这些设备还会向思科 ISE 发送记账消息，以记录此类操作。
- **访客和安全无线 (Guest and Secure Wireless):** 思科 ISE 使您能够为访客、承包商、顾问和客户提供安全的网络访问。您可以使用基于 Web 的门户和移动门户将访客加入公司的网络和内部资源。您可以为不同类型的访客定义访问权限，并分配发起人以创建和管理访客帐户。
- **自带设备 (BYOD) (Bring Your Own Device [BYOD]):** 思科 ISE 可以让您的员工和访客在企业网络上安全地使用他们的个人设备。BYOD 功能的最终用户可以使用所配置的路径添加其设备，并调配预定义的身​​份验证和网络访问级别。
- **资产可视性 (Asset Visibility):** 思科 ISE 在无线连接、有线连接和 VPN 连接中提供一致的可视性，并控制网络上的人员和内容。思科 ISE 使用探测器和设备传感器来侦听设备连接到网络的方式。然后，庞大的思科 ISE 配置文件数据库将对设备进行分类。这可以提供您所需要的可视性和情景，以便授予适当级别的网络访问权限。
- **安全访问:** 思科 ISE 使用各种身份验证协议为网络设备和终端提供安全网络访问。这些协议包括但不限于 802.1X、RADIUS、MAB、基于 Web 的、EasyConnect 和启用外部代理的身份验证方法。
- **分段 (Segmentation):** 思科 ISE 使用有关网络设备和终端的情景数据来促进网络分段。安全组标记、访问控制列表、网络访问协议，以及用来定义授权、访问和身份验证的策略集是思科 ISE 实现安全网络分段的一些方式。
- **终端安全评估或合规性 (Posture or Compliance):** 思科 ISE 可以让您检查终端的合规性（也称为终端安全评估），然后再允许它们连接您的网络。您可以确保终端接收适当的终端安全评估代理以提供终端安全评估服务。



- **威胁遏制 (Threat Containment):** 如果思科 ISE 检测到来自终端的威胁或漏洞属性，则发送自适应网络控制策略以动态更改终端访问级别。在评估并解决威胁或漏洞后，终端将获得其原始访问策略。
- **安全生态系统集成 (Security Ecosystem Integrations):** 通过 pxGrid 功能，思科 ISE 可以与相连的网络设备、第三方供应商或思科合作伙伴系统安全地共享情景相关信息、策略和配置数据等。

## 思科 ISE 管理员

管理员可使用管理员门户执行下列操作：

- 管理部署、服务中心操作、网络设备以及节点监控和故障排除。
- 管理思科 ISE 服务、策略、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。

您可以创建管理员，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 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。



---

**注释** 从思科 ISE 版本 2.7 起，在思科 ISE 中创建用户账户时，请使用字母数字值。

---

**相关主题**

[思科 ISE 管理员组](#)，第 10 页

## 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 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，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 部署。

## 创建新管理员

思科 ISE 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 管理员的属性或更改其状态。

**步骤 1** 选择 **管理 (Administration) > 系统 (System) > 管理员访问权限 (Admin Access) > 管理员 (Administrators) > 管理员用户 (Admin Users) > 添加 (Add)**。

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

- **创建管理员用户 (Create an Admin User)**

如果选择**创建管理员用户 (Create an Admin User)**，将显示**新建管理员 (New Administrator)** 窗口，从中可配置新管理员用户的帐户信息。

- **从网络访问用户选择 (Select from Network Access Users)**

如果选择**从网络访问权限用户中选择 (Select from Network Access Users)**，将显示当前用户列表，从中可创建用户。然后将显示与此用户对应的**管理员用户 (Admin User)** 窗口。

**步骤 3** 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 4** 点击**提交 (Submit)** 在思科 ISE 内部数据库中创建新管理员。

### 相关主题

[只读管理员策略](#)

[创建内部只读管理员](#)

[自定义只读管理员的菜单访问权限](#)

[将外部组映射至只读管理员组](#)

## 思科 ISE 管理员组

管理员组是思科 ISE 中基于角色的访问控制 (RBAC) 组。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。

思科 ISE 支持多个外部身份库，以加强管理员的用户访问管理。

在思科 ISE 中，只读功能不可用于任何管理访问权限。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。

在思科 ISE 安全模式下，管理员只能创建与其具有相同权限集的管理组。提供的权限基于思科 ISE 数据库中定义的用户管理角色。这样，管理组就形成了定义访问思科 ISE 系统的权限的依据。

下表列出了思科 ISE 中预定义的管理组以及这些组成员可以执行的任务。

表 2: 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
自定义管理员	管理发起人、访客和个人设备门户。	<ul style="list-style-type: none"> <li>配置访客和发起人访问权限。</li> <li>管理访客访问设置。</li> <li>自定义最终用户 Web 门户。</li> </ul>	<ul style="list-style-type: none"> <li>无法在思科 ISE 中执行任何策略管理、身份管理或系统级别配置任务。</li> <li>无法查看任何报告</li> </ul>
帮助台管理员	查询监控和故障排除操作	<ul style="list-style-type: none"> <li>运行所有报告。</li> <li>运行所有故障排除流程。</li> <li>查看思科 ISE 控制板和实时日志。</li> <li>查看警报。</li> </ul>	无法创建、更新或删除报告、故障排除流程、实时身份验证或警报。
身份管理员	<ul style="list-style-type: none"> <li>管理用户帐户和终端。</li> <li>管理身份源。</li> </ul>	<ul style="list-style-type: none"> <li>添加、编辑和删除用户帐户和终端。</li> <li>添加、编辑和删除身份源。</li> <li>添加、编辑和删除身份源序列。</li> <li>为用户帐户配置常规设置（属性和密码策略）。</li> <li>查看思科 ISE 控制板、实时日志、警报和报告。</li> <li>运行所有故障排除流程。</li> </ul>	无法在思科 ISE 中执行任何策略管理或系统级别配置任务。
MnT 管理员	执行所有监控和故障排除操作。	<ul style="list-style-type: none"> <li>管理所有报告（运行、创建和删除）。</li> <li>运行所有故障排除流程。</li> <li>查看思科 ISE 控制板和实时日志。</li> <li>管理警报（创建、更新、查看和删除）。</li> </ul>	无法在思科 ISE 中执行任何策略管理、身份管理或系统级别配置任务。

管理组角色	访问级别	权限	限制
网络设备管理员	管理思科 ISE 网络设备和网络设备存储库。	<ul style="list-style-type: none"> <li>对网络设备拥有读写权限</li> <li>对网络设备组和所有网络资源对象类型拥有读写权限。</li> <li>查看思科 ISE 控制板、实时日志、警报和报告。</li> <li>运行所有故障排除流程。</li> </ul>	无法在思科 ISE 中执行任何策略管理、身份管理或系统级别配置任务。
策略管理员	为所有与身份验证、授权、安全评估、分析器和客户端调配有关的跨网络思科 ISE 服务创建和管理策略。	<ul style="list-style-type: none"> <li>对策略中使用的所有元素（例如授权配置文件、网络设备组 (NDG) 和条件）拥有读写权限。</li> <li>对身份、终端和身份组（用户身份组和终端身份组）拥有读写权限。</li> <li>对服务策略和设置拥有读写权限。</li> <li>查看思科 ISE 控制板、实时日志、警报和报告。</li> <li>运行所有故障排除流程。</li> </ul>	无法在思科 ISE 中执行任何身份管理或系统级别配置任务
RBAC 管理员	<b>操作 (Operations)</b> 菜单下除之外的所有任务，以及对 <b>管理 (Administration)</b> 下某些菜单项的部分访问权限。	<ul style="list-style-type: none"> <li>查看身份验证详细信息。</li> <li>启用或禁用</li> <li>创建、编辑和删除警报；生成和查看报告；以及使用思科 ISE 对网络中的问题进行故障排除。</li> <li>对管理员帐户设置和管理组设置拥有读取权限</li> <li>对管理员访问和数据访问权限以及 <b>RBAC 策略 (RBAC Policy)</b> 窗口拥有查看权限。</li> <li>查看思科 ISE 控制板、实时日志、警报和报告。</li> <li>运行所有故障排除流程。</li> </ul>	无法在思科 ISE 中执行任何身份管理或系统级别配置任务

管理组角色	访问级别	权限	限制
超级管理员	所有思科 ISE 管理功能。默认管理员帐户属于此组。	<p>对所有思科 ISE 资源拥有创建、读取、更新、删除和执行 (CRUDX) 权限。</p> <p>超级管理员可以随时修改任何思科 ISE 本地用户的凭证。</p> <p><b>注释</b> 超级管理员用户无法修改系统生成的默认 RBAC 策略和权限。要执行此操作，您必须根据您的需要利用必要的权限创建新的 RBAC 策略，并且将这些策略映射至管理员组。</p>	<ul style="list-style-type: none"> <li>只有默认超级管理员组的管理员用户才能修改或删除其他管理员用户。即使是管理员组中克隆有超级管理员组的菜单和数据访问权限的外部映射用户也无法修改或删除管理员用户。</li> </ul>
系统管理员	所有思科 ISE 配置和维护任务。	<p>拥有执行操作 (<b>Operations</b>) 选项卡下所有活动的完全访问权限 (读写权限)，以及对管理 (<b>Administration</b>) 选项卡下某些菜单项的部分访问权限：</p> <ul style="list-style-type: none"> <li>对管理员帐户设置和管理员组设置拥有读取权限。</li> <li>对管理员访问和数据访问权限以及 <b>RBAC 策略 (RBAC policy)</b> 窗口拥有读取权限。</li> <li>对管理 (<b>Administration</b>) &gt; 系统 (<b>System</b>) 菜单下的所有选项拥有读写权限。</li> <li>查看身份验证详细信息。</li> <li>启用或禁用</li> <li>创建、编辑和删除警报；生成和查看报告；以及使用思科 ISE 对网络中的问题进行故障排除。</li> </ul>	无法在思科 ISE 中执行任何策略管理或系统级别配置任务。

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 ERS 授权的内部用户、身份组、终端、终端组和 SGT。
外部 RESTful 服务 (ERS) 运算符	对 ERS API、仅 GET 的只读访问权限	<ul style="list-style-type: none"> <li>只能读取 ERS API 请求</li> </ul>	此角色仅适用于支持 ERS 授权的内部用户、身份组、终端、终端组和 SGT。

#### 相关主题

[思科 ISE 管理员](#)，第 9 页

## 创建管理员组

管理员组 (**Admin Groups**) 窗口允许您查看、创建、修改、删除、复制或过滤思科 ISE 网络管理员组。

#### 开始之前

要配置外部管理员组类型，您必须已经指定了一个或多个外部身份库。

**步骤 1** 选择管理 (**Administration**) > 系统 (**System**) > 管理员访问 (**Admin Access**) > 管理员 (**Administrators**) > 管理员组 (**Admin Groups**)。

**步骤 2** 点击添加 (**Add**)，并输入名称和说明。

名称 (**Name**) 字段支持的特殊字符包括：空格、# \$ & ‘ ( ) \* + - . / @ \_。

**步骤 3** 选中相应的复选框以指定要配置的管理员组的类型：

- **内部 (Internal)**：分配到此组类型的管理员将对存储在思科 ISE 内部数据库中的凭证进行身份验证。
- **外部 (External)**：分配给此组的管理员根据您在管理 (**Administration**) > 系统 (**System**) > 管理员访问 (**Admin Access**) > 身份验证 (**Authentication**) > 身份验证方式 (**Authentication Method**) 窗口中选择的外部身份库中存储的凭证进行身份验证。如果需要，您可以指定外部组。

**注释** 如果内部用户配置了用于身份验证的外部身份库，则在登录到 ISE 管理员门户时，内部用户必须选择外部身份库作为身份源。如果选择了内部身份源 (**Internal Identity Source**)，身份验证将失败。

**步骤 4** 点击成员用户 (**Member Users**) 区域中的添加 (**Add**) 将用户添加到此管理员组。要删除管理员组中的用户，请选中您希望删除的用户所对应的复选框，并点击删除 (**Remove**)。

**步骤 5** 点击提交。

## 对思科 ISE 进行管理访问

思科 ISE 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 的用户授予管理访问权限。

### 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 (Admin password):** 默认情况下，在安装期间创建的思科 ISE 管理员用户将在 45 天后超时。您可以通过在**管理 (Administration) > 系统 (System) > 管理设置 (Admin Settings)** 中关闭密码使用时间 (**Password Lifetime**) 来防止此情况。点击**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-password** 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](#)》。
- **SSH 访问 CLI (SSH access to the CLI):** 可以在安装期间或安装后使用 **service sshd** 命令启用 SSH 访问。还可以强制 SSH 连接使用密钥。请注意，在执行此操作时，与所有网络设备的 SSH 连接也会使用该密钥。有关详细信息，请参阅[SSH 密钥验证](#)，第 600 页。您可以强制 SSH 密钥使用 Diffie-Hellman 算法。请注意，SSH 密钥不支持 ECDSA 密钥。

## 思科 ISE 中基于角色的管理员访问控制

思科 ISE 提供角色型访问控制 (RBAC) 策略，通过限制管理权限确保安全性。RBAC 策略与默认管理组关联，以定义角色和权限。每个预定义管理组都配有一套标准权限（适用于菜单和数据访问），因此，与关联的角色和工作职能保持一致。

用户界面中的某些功能要求具备特定权限才可使用。如果功能不可用，或者不允许您执行特定任务，您的管理组可能没有执行利用此功能的任务所需的权限。

无论访问权限级别如何，任何管理员帐户都可以在任何它能够访问的窗口上，修改或删除其拥有权限的对象。只读功能对任何管理访问都不可用。



**注释** 只有具有超级管理员或只读管理员权限的系统定义管理员用户才能查看不属于用户组的基于身份的用户。如果创建的管理员没有这些权限，将无法看到这些用户。

## 基于角色的权限

思科 ISE 允许您在菜单和数据级别配置权限：它们称为菜单访问权限和数据访问权限。

菜单访问权限允许您显示或隐藏思科 ISE 管理界面的菜单项。您可以通过此功能创建权限，从而限制或允许菜单级别的访问。

通过数据访问权限，您可以允许读/写访问、访问或禁止访问思科 ISE 界面中以下数据：管理员组 (Admin Groups)、用户身份组 (User Identity Groups)、终端身份组 (Endpoint Identity Groups)、位置 (Locations) 和设备类型 (Device Types)。

## RBAC 策略

RBAC 策略确定是否可以授予管理员对菜单项或其他身份组数据元素的特定类型的访问权限。可以使用 RBAC 策略基于管理员组向管理员授予或拒绝对菜单项或身份组数据元素的访问权限。当管理员登录到管理门户时，他们可以访问基于为与其关联的管理员组定义的策略和权限的菜单和数据。

RBAC 策略将管理员组映射到菜单访问权限和数据访问权限。例如，您可以防止网络管理员查看 Admin Access 操作菜单和策略数据元素。通过为与网络管理员关联的管理员组创建自定义 RBAC 策略，可以实现此目的。



**注释** 如果使用自定义 RBAC 策略授予或拒绝管理员访问权限，请确保对给定的数据访问权限提供所有相关的菜单访问权限。例如，要添加或删除具有身份或策略管理员数据访问权限的终端，必须提供对工作中心 (Work Center) > 网络访问 (Network Access) 以及管理 (Administration) > 身份管理 (Identity Management) 的菜单访问权限。

## 默认菜单访问权限

思科 ISE 提供一组与一系列预定义的管理员组相关联的现成权限。通过预定义管理员组权限，您可以设置权限，以便管理员组的成员可以完全或有限地访问管理界面中的菜单项（称为菜单访问权限）和委派管理员组使用其他管理员组的数据访问要素（称为数据访问权限）。这些权限可进一步用于制定多种管理员组的 RBAC 策略的可重用的实体。思科 ISE 提供已用于默认 RBAC 策略的一组系统定义的菜单访问权限。下表列出了默认菜单访问权限。除了预定义的菜单访问权限外，思科 ISE 还允许您在 RBAC 策略中使用的自定义菜单访问权限。

表 3: 默认菜单访问权限

菜单访问权限名称	RBAC 组	允许的菜单项集合
超级管理员菜单访问权限	超级管理员	Operations > All menu items 策略 > 所有菜单项 管理 > 所有菜单项



菜单访问权限名称	RBAC 组	允许的菜单项集合
策略管理员菜单访问权限	策略管理员	Operations > All menu items 策略 > 所有菜单项 “管理” (Administration) > “身份管理” (Identity Management) > 所有菜单项 系统 > 设置
帮助台管理员菜单访问权限	帮助台管理员	“操作” (Operations) > 所有菜单项
身份管理员菜单访问权限	身份管理员	Operations > All menu items “管理” (Administration) > “身份管理” (Identity Management) > 所有菜单项
网络设备菜单访问权限	网络设备管理员	Operations > All menu items “管理” (Administration) > “网络资源” (Network Resources) > 所有菜单项
系统管理员菜单访问权限	系统管理员	“操作” (Operations) > “身份验证、报警、报告以及故障排除” (Authentications, Alarms, Reports, and Troubleshoot) “管理” (Administration) > 所有菜单项
RBAC 管理员菜单访问权限	RBAC 管理员	“操作” (Operations) > 除了之外的所有菜单项 “管理” (Administration) > “管理员访问权限” (Admin Access) > 所有菜单项
MnT 管理员菜单访问权限	MnT 管理员	“操作” (Operations) > 所有菜单项



**注释** 对于超级管理员用户，所有菜单项均可用。对于其他管理员用户，此列中的所有菜单项均可供独立部署及分布式部署中的主要节点使用。对于分布式部署中的辅助节点，“管理” (Administration) 选项卡下的菜单项不可用。

## 配置菜单访问权限

思科 ISE 允许创建可映射到 RBAC 策略的自定义菜单访问权限。根据管理员的角色，您可以仅允许其访问特定菜单选项。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 授权 (Authorization) > 权限 (Permissions) > 菜单访问 (Menu Access)。

**步骤 2** 点击添加 (Add)，输入名称 (Name) 和说明 (Description) 字段的值。

- a) 将 ISE 导航结构 (ISE Navigation Structure) 菜单展开至所需的级别，然后单击要为其创建权限的选项。
- b) 在菜单访问的权限 (Permissions for Menu Access) 窗格中，点击显示 (Show)。

**步骤 3** 点击提交。

## 默认数据访问权限

思科 ISE 具有一系列预定义的数据访问权限。这些权限允许多名管理员在同一个用户群中具有数据访问权限。您可以启用数据访问权限或将其限制在一个或多个管理员组范围。此过程允许向一个管理员组的管理人员授予自主委派控制，通过选择性关联允许所选管理员组重复使用数据访问权限。对于查看所选管理员组或网络设备组，数据访问权限范围从完全访问权限直到无访问权限。下表列出了默认的数据访问权限。通过基于策略的管理人员 (RBAC) 组菜单访问和数据访问权限定义。您应首先创建菜单访问和数据访问权限，然后创建将管理员组与对应菜单访问和数据访问权限关联的 RBAC 策略。RBAC 策略采用以下形式 - If admin\_group=Super Admin then assign SuperAdmin Menu Access permission + SuperAdmin Data Access permission。除了预定义的数据访问权限外，思科 ISE 还允许您创建可与 RBAC 策略的自定义数据访问权限。

表 4: 默认数据访问权限

数据访问名称	RBAC 组	允许的管理员组	允许的网络设备组
超级管理员数据访问	超级管理员	管理员组、用户身份组、终端身份组	所有位置、所有设备类型
策略管理员数据访问	策略管理员	用户身份组、终端身份组	无
身份管理员数据访问	身份管理员	用户身份组、终端身份组	无
网络管理员数据访问	网络设备管理员	无	所有位置、所有设备类型
系统管理员数据访问	系统管理员	管理员组	无
RBAC 管理员数据访问	RBAC 管理员	管理员组	无

## 配置数据访问权限

通过思科 ISE，可以创建自定义数据访问权限，并将其映射到 RBAC 策略。根据管理员的角色，可以选择仅为他们提供选择数据的访问权限。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 授权 (Authorization) > 权限 (Permissions)。

**步骤 2** 选择 权限 (Permissions) > 数据访问 (Data Access)。

**步骤 3** 点击添加 (**Add**)，输入名称 (**Name**) 和说明 (**Description**) 字段的值。

- a) 单击以展开管理员组，选择对应的管理员组。
- b) 点击完全访问 (**Full Access**)。

**步骤 4** 点击保存 (**Save**)。

---





## 第 3 章

# 许可

- 思科 ISE 许可证，第 21 页
- 思科 ISE 智能许可证，第 24 页
- 气隙网络的智能许可，第 28 页

## 思科 ISE 许可证

思科 ISE 服务可为网络中越来越多的终端提供可视性和可控性。思科 ISE 功能会被映射到特定许可证，而您可以启用提供满足组织需求所需的思科 ISE 功能的许可证。

思科 ISE 捆绑了具有以下主要功能的许可机制：

- 内置许可证：思科 ISE 随附一个有效期为 90 天的内置评估许可证。安装思科 ISE 后，无需立即安装思科 ISE 许可证。您可以使用提供完整思科 ISE 功能的评估许可证。
- 许可证集中管理：思科 ISE 主管理节点 (PAN) 可集中管理思科 ISE 许可证。在具有主 PAN 和辅助 PAN 的分布式部署中，主 PAN 会自动与辅助 PAN 共享许可信息。
- 并发活动终端计数：思科 ISE 许可证包括每个层许可证的计数值。每层许可证可随时支持特定数量的活动终端。计数值是指整个部署中随时使用特定思科 ISE 服务的活动终端的数量。思科 ISE 许可依赖 RADIUS 记帐，因此您必须在网络设备上启用 RADIUS 服务。

并发活动终端是指支持的用户和设备总数。在这里，终端可能意味着用户、个人计算机、笔记本电脑、IP 电话、智能手机、游戏机、打印机、传真机或其他类型的网络设备。

思科 ISE 版本 3.0 及更高版本不支持思科 ISE 版本 2.x 中使用的传统许可证，例如 Base、Plus 和 Apex 许可证。思科 ISE 版本 3.x 许可证完全通过叫做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。

为最大限度地提高客户的经济性，思科 ISE 的许可可在以下软件包中提供：

- 层级许可证

从思科 ISE 版本 3.0 开始，一组称为“层级许可证”的新许可证将取代 3.0 之前版本中使用的 Base、Apex 和 Plus 许可证。层级许可证包含三种许可证 — Essentials、Advantage 和 Premier。

如果您当前拥有 Base、Apex 和 Plus 许可证，请使用 CSSM 将其转换为新的许可证类型。

- 设备管理许可证

上面启用了 TACACS+ 角色的策略服务节点 (PSN) 将使用设备管理许可证。

- 虚拟设备许可证

虚拟设备许可证有三种形式：VM 小型、VM 中型和 VM 大型。

如果使用虚拟设备，但您的思科 ISE 没有有效的 VM 许可证，那么您将收到不合规许可证使用的警告和通知，直到您获取并安装 VM 许可证。但是，思科 ISE 服务不会中断。

- 评估许可证

当您首次安装 思科 ISE Release 3.0 及更高版本并支持多达 100 个端点时，默认情况下会激活评估许可证。评估许可证是 90 天的许可证，允许您访问所有思科 ISE 功能。在评估期间，许可证使用量不会报告给 CSSM。

如果用 Base、Apex 和 Plus 智能许可证升级到思科 ISE 版本 3.0 或更高版本，您的智能许可证将升级到思科 ISE 中的新许可证类型。但是，您必须在 CSSM 中注册新的许可证类型，才能激活您所升级至的思科 ISE 版本中的许可证。

如果您拥有传统思科 ISE 许可证，必须将其转换为智能许可证，才能在思科 ISE 版本 3.0 和更高版本中开始使用许可证。要将思科 ISE 2.x 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。

有关许可证使用不合规的通知也会显示在思科 ISE 中。如果您的许可证使用在 45 天内不合规，您将失去对思科 ISE 的所有管理控制，直到您购买并激活所需的许可证。

从一个许可包升级到另一个许可包时，思科 ISE 会继续提供升级之前的早期包中提供的所有功能。但是，您必须重新配置之前已经配置的任何设置。例如，您当前使用 Essentials 许可证并在以后添加 Advantage 许可证，则使用 Essentials 许可证已配置的功能不会更改。

- 试用期结束，而您尚未注册您的许可证。
- 您的许可证已过期。
- 终端使用量超过您的许可协议。

## 层级许可证

下表指定新的层级许可证启用的功能。

表 5: 思科 ISE 层级许可证

许可证名称	此许可证可启用什么功能？
<b>Essentials</b>	<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>
<b>Advantage</b>	<ul style="list-style-type: none"> <li>• 思科 ISE Essentials 许可证启用的所有功能。</li> <li>• 自带设备 (BYOD) 设备注册和调配，内置证书颁发机构。设备注册通过已配置的“我的设备”门户进行。</li> <li>• 安全组标记、TrustSec 和思科以应用为中心的基础设施 (ACI) 集成。</li> <li>• 分析服务，包括基本资产可视性和实施功能。</li> <li>• 源服务。</li> <li>• 情景共享（如 pxGrid）和安全生态系统集成。</li> <li>• 快速遏制威胁（使用自适应网络控制和情景共享服务）。</li> </ul>
<b>Premier</b>	<ul style="list-style-type: none"> <li>• 思科 ISE Essentials 和 Advantage 许可证启用的所有功能。</li> <li>• 终端安全评估可视性和实施。</li> <li>• 通过企业移动管理和移动设备管理实现的合规可视性和实施。</li> <li>• 以威胁为中心的网络访问控制可视性和实施。</li> </ul>



**注释** 如果终端的隐私设置允许 MAC 随机化或轮换和更改 MAC，则您可能会看到更高的思科 ISE 许可证消耗计数。当终端使用新的随机 MAC 地址进行身份验证时，就会创建一个新的思科 ISE 会话。

## 设备管理许可证

设备管理许可证允许您在策略服务节点上使用 TACACS 服务。在高可用性 (HA) 独立部署中，设备管理许可证允许您在 HA 对中的单个策略服务节点上使用 TACACS 服务。

## 虚拟设备许可证

## 评估许可证

当您安装或升级到 思科 ISE Release 3.0 及更高版本并支持多达 100 个终端时，默认情况下会激活评估许可证。评估许可证有效期为 90 天，您可以在在此期间访问所有思科 ISE 功能。当使用评估许可证时，思科 ISE 被视为处于评估模式。

思科 ISE GUI 显示带有评估模式剩余天数的消息。



---

**注释** 您必须在评估模式结束前购买和注册思科 ISE 许可证，才能继续使用所需的思科 ISE 功能。

---

## 思科 ISE 智能许可证

思科提供智能许可，可以让您监控思科 ISE 软件许可证和终端许可证的使用情况。您可以使用单个注册令牌轻松高效地监控许可证使用情况，而不是分别导入各个许可证。在集中式数据库 - 思科智能软件管理器 (CSSM) 中，查看和管理您购买的所有思科产品和许可证的详细信息。登录 CSSM 门户，可轻松跟踪可用的终端许可证和使用统计信息。

当激活智能许可证令牌并在思科 ISE 管理门户中注册该令牌后，CSSM 会监控每个产品许可证各个终端会话的许可证使用情况。智能许可通过思科 ISE 中的简单表格布局通知管理员终端会话的许可证使用情况。智能许可 (Smart Licensing) 每天向集中式数据库报告各个以启用许可证的高峰使用情况。当许可证可用且未使用时，管理员会收到可用许可证通知，并可继续监控使用情况。当使用量超过可用许可证数量时，系统会激活警报，并通过警报和通知来告知管理员。

借助智能许可，还可以通过 Cisco 智能账户管理所包含的不同许可证权益，如 Base、Plus、Apex 或 TACACS。通过思科 ISE，可以监控每个许可证权益的基本使用量统计信息。通过 CSSM 帐户，您可以查看更多信息、统计数据 and 通知，以及更改您的帐户和授权。



---

**注释** 中不支持 CSSM 卫星。

---

思科 ISE 每 30 分钟获取一次内部许可证使用样本。系统会相应地更新许可证合规性和使用情况。要在思科 ISE 中的许可证 (Licenses) 表中查看此信息，请从主菜单中选择管理 (Administration) > 系统 (System) > 许可 (Licensing)，然后单击刷新 (Refresh)。



从您向 CSSM 注册思科 ISE 主管理节点 (PAN) 以来，思科 ISE 会每六小时向 CSSM 服务器报告一次许可证使用峰值计数。峰值计数报告可帮助确保思科 ISE 中的许可证使用符合所购买和注册的许可证。思科 ISE 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。

如果思科 ISE 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 Compliancy) 列中会显示它们处于不合规状态的天数。此外，还会在许可 (Licensing) 区域顶部显示的“通知” (Notifications) 中，以及思科 ISE 工具栏的许可警告 (License Warning) 链接旁指明不合规。除通知之外，还可以查看警报。



**注释** TACACS 许可证会在思科 ISE 与 CSSM 服务器通信时获得授权，但它们不基于会话，因此许可证 (Licenses) 表中没有与之关联的使用量计数。

许可证 (Licenses) 表的合规性列显示以下值之一：

- **合规 (In Compliance)**：此许可证的使用符合规定。
- **已发放权益 (Released Entitlement)**：已购买并发放许可证以供使用，但到目前为止，此思科 ISE 部署中尚未使用其中任何许可证。在这种情况下，许可证的使用计数 (Consumption Count) 为 0。
- **评估 (Evaluation)**：可使用评估许可证。

图 1: 许可证使用情况表

License	Status	Compliance	Yesterday's Peak Count	Consumption Count*	Days Out of Compliancy	Last Authorization
Base	Enabled	Released Entitlement	0	0	-	-
Plus	Enabled	Released Entitlement	0	0	-	-
Apex	Enabled	Released Entitlement	0	0	-	-
Tacacs	Enabled	In Compliance	Uncounted	Uncounted	-	May 19, 2016 3:23:53 PM

\*Consumption Count Updated: May 19, 2016 17:00:00 IST

## 注册并激活智能许可证

开始之前

- 如果您有传统的思科 ISE 许可证，必须将其转换为智能许可证。
- 如果要使用现有智能许可证升级到思科 ISE 版本 3.0 和更高版本，请在 CSSM 中将许可证转换为新的智能许可证类型。
- 在 CSSM 中注册新的智能许可证类型，以接收注册令牌。

**步骤 1** 在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择管理 (Administration) > 系统 (System) > 许可 (Licensing)。

**步骤 2** 在显示的许可 (Licensing) 窗口中，单击注册详细信息 (Registration Details)。

**步骤 3** 在显示的注册详细信息 (**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。
- **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。(如果在注册思科 ISE 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。思科 ISE 使用更新的代理服务器与 CSSM 建立连接, 避免思科 ISE 服务中断。)
- **SSM 本地部署服务器**以连接到配置的 SSM 本地服务器。此选项在思科 ISE 版本 3.0 补丁 2 及更高版本中可用。请参阅[气隙网络的智能许可](#), 第 28 页。

**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 跟踪其使用情况。

**步骤 6** 点击注册。

---

## 在思科 ISE 中管理智能许可

激活并注册智能许可令牌后, 即可通过以下操作从思科 ISE 管理许可证授权:

- 启用、禁用和刷新许可证授权证书。
- 更新智能许可注册。
- 识别合规和不合规的许可问题。

### 开始之前

确保已激活并注册您的智能许可令牌。

---

**步骤 1** (可选) 首次激活智能许可时, 将自动启用所有许可证授权并将其作为评估模式的一部分。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, 则思科 ISE 中将显示不合规通知。将这些授权添加到您的 CSSM 帐户 (请联系您的 CSSM 客户代表寻求帮助), 然后在许可证 (**Licenses**) 表中单击**刷新 (Refresh)** 以删除不合规通知并继续使用相关功能。刷新授权后, 注销然后重新登录思科 ISE 以删除相关的不合规消息。

**步骤 2** (可选) 如果每天自动授权由于任何原因失败, 则显示不合规消息。单击**刷新 (Refresh)** 重新获得您的授权。刷新授权后, 注销然后重新登录思科 ISE 以删除相关的不合规消息。

**步骤 3** (可选) 首次激活智能许可时, 将自动启用所有许可证授权并将其作为评估期的一部分。注册令牌后, 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, 仍然可以在 ISE 中通过智能许可禁用这些授权, 以避免不必要的违规通知。从许可证 (**Licenses**) 表中, 选中令牌中未包括的许可证授权的复选框, 然后在工具栏上单击**禁用 (Disable)**。禁用许可证授权后, 注销然后重新登录思科 ISE 以从菜单中删除相关的功能, 并且删除不合规消息。

**步骤 4** (可选) 为您的帐户添加授权后, 请启用这些授权。从许可证 (**Licenses**) 表中, 选中所需的已禁用许可证的复选框, 并在工具栏上单击**启用 (Enable)**。

- 步骤 5**（可选）如果最初仅使用一个 UDI 设置智能许可并且未输入辅助 UDI，可以稍后更新您的信息。点击**思科智能许可注册详细信息 (Cisco Smart Licensing Registration Details)** 链接以打开该区域。重新输入令牌，输入新的**辅助 UDI** 并点击**更新 (Update)**。
- 步骤 6**（可选）注册证书每六个月自动刷新一次。要手动刷新智能许可证书注册，请在**许可 (Licensing)** 窗口顶部点击**更新注册 (Renew Registration)**。
- 步骤 7**（可选）要从智能账户删除思科 ISE 注册（由 UDI 指示），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)**。例如，如果需要更改在注册过程中指定的 UDI，可以执行此操作。如果评估期仍有剩余时间，则思科 ISE 仍处于智能许可中。如果评估期已结束，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。
- 步骤 8**（可选）要从智能账户完全删除思科 ISE 注册（由 UDI 指示）并恢复为传统许可，请在**思科智能许可 (Cisco Smart Licensing)** 区域的顶部单击**禁用 (Disable)**。例如，如果需要更改在注册过程中指定的 UDI，可以执行此操作。在禁用智能许可证后，您可以遵循注册流程以相同或不同的 UDI 再次激活并注册。

## 故障排除：未注册的许可证使用情况

### 问题

终端许可证使用量依赖于与终端匹配的授权策略中使用的属性。

假设只在系统中注册了思科 ISE Base 许可证的情况（已删除 90 天的评估许可证），因为您删除了 90 天评估许可证。您将能够查看和配置相应的思科 ISE Base 菜单项和功能。

如果将授权策略配置为使用需要 Apex 许可证的功能（例如：您使用了 Session.PostureStatus 属性），且如果终端与此授权策略相匹配，那么：

- 终端会使用思科 ISE Apex 许可证，即使尚未在系统中注册思科 Apex 许可证。
- 您每次登录时都会看到不合规许可证使用的通知。
- 思科 ISE 会显示通知和警报，以及超出允许的许可证使用范围 (Exceeded license usage than allowed) 消息。这是因为，您的思科 ISE 没有在 CSSM 中注册的思科 ISE Apex 许可证，但终端却正在使用许可证。



**注释** 即使您通过注册必要的许可证来解决许可问题，许可警报也会在首次出现不合规许可证使用后显示约 60 天。

### 可能的原因

由于授权策略的配置，**许可 (Licensing)** 表会报告思科 ISE 使用了您尚未购买和注册的许可证。在购买 Plus 或 Apex 许可证之前，思科 ISE 管理门户不会显示这些许可证所涵盖的功能。但在您购买这些许可证后，即使许可证已过期或许可证的终端使用量超过设置的限制，GUI 也会继续显示其启用的功能。因此，即使当前没有系统的有效许可证，这些功能仍可以进行配置。

### 解决方案

在思科 ISE 管理门户中，点击菜单图标(☰)并选择策略 (Policy) > 授权 (Authorization)，确定正在使用尚无注册许可证的功能的授权规则，然后重新配置该规则。

## 气隙网络的智能许可

气隙网络不允许在安全网络和外部网络之间进行任何通信。思科 ISE 智能许可要求将思科 ISE 与 CSSM 通信。如果您的网络是气隙，则思科 ISE 无法向 CSSM 报告许可证使用情况，缺少报告会导导致失去对思科 ISE 的管理访问权限并限制思科 ISE 功能。

为避免间隙网络中出现许可问题并启用完整的思科 ISE 功能，您可以配置智能软件管理器 (SSM) 本地服务器。此许可方法可用在版本。

您必须配置 SSM 本地服务器，并确保思科 ISE 可以访问此服务器。此服务器接管间隙网络中的 CSSM 角色，根据需要发布许可证授权，并跟踪使用指标。SSM 内部部署服务器还会发送与许可使用和有效性相关的通知、警报和警告消息。

## 为智能许可配置本地智能软件管理器

### 开始之前

配置 SSM 本地服务器，并确保思科 ISE 可以访问此服务器。有关更多信息，请参阅 [智能软件管理器本地部署资源](#)。

如果您购买更多许可证或修改购买的许可证，则必须将本地 SSM 服务器连接到 CSSM，以便让更改在本地服务器中可供使用。



注释 ISE-PIC 2.7 及更早版本不支持智能许可。

**步骤 1** 选择 **管理 (Administration)** > **系统 (System)** > **许可 (Licensing)**。

**步骤 2** 单击 **思科智能许可 (Cisco Smart Licensing)**。

**步骤 3** 从 **连接方法 (Connection Method)** 下拉列表中选择 **SSM 本地部署服务器 (SSM On-Prem Server)**。

SSM 内部部署门户中的 **证书 (Certificate)** 窗口会显示连接的 SSM 内部部署服务器的 IP 地址或主机名（或 FQDN）。

**步骤 4** 在 **SSM 内部部署服务器主机 (SSM On-Prem server Host)** 字段中输入配置的 IP 地址或主机名（或 FQDN）。

**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 跟踪其使用情况。

**步骤 6** 点击 **Register**。

注释 向 SSM On-Prem 服务器注册思科 ISE 时，请确保端口 443 和用于 ICMP 通信的端口处于打开状态。

---





## 第 4 章

# 思科 ISE 的部署

- 思科 ISE 部署术语，第 32 页
- 分布式思科 ISE 部署中的角色，第 32 页
- 配置思科 ISE 节点，第 32 页
- 支持多种部署方案，第 34 页
- 思科 ISE 分布式部署，第 35 页
- 部署和节点设置，第 38 页
- 日志记录设置，第 44 页
- 管理员访问设置，第 46 页
- 管理节点，第 48 页
- 策略服务节点，第 49 页
- 监控节点，第 50 页
- 监控数据库，第 52 页
- 配置用于自动故障切换的监控节点，第 54 页
- 思科 pxGrid 节点，第 54 页
- ISE pxGrid 身份映射，第 57 页
- Inline Posture 节点，第 59 页
- 查看部署中的节点，第 60 页
- 数据库崩溃或文件损坏问题，第 61 页
- 设备的监控配置，第 61 页
- 同步主要和辅助思科 ISE 节点，第 61 页
- 更改节点角色和服务，第 62 页
- 在思科 ISE 中修改节点的影响，第 62 页
- 创建策略服务节点组，第 63 页
- 从部署中删除节点，第 63 页
- 关闭思科 ISE 节点，第 64 页
- 更改独立思科 ISE 节点的主机名或 IP 地址，第 64 页

## 思科 ISE 部署术语

以下是讨论思科 ISE 部署方案时常用的术语：

- **服务：**服务是角色提供的特定功能，例如网络访问、分析器、终端安全评估、安全组访问、监控和故障排除等。
- **节点：**节点是运行思科 ISE 软件的单个实例。思科 ISE 可用作设备，也可用作能在 VMware 上运行的软件。运行思科 ISE 软件的每个实例（设备或 VMware）叫节点。
- **角色：**节点的角色决定节点提供的服务。思科 ISE 节点可以承担以下任意角色：  
• **Inline Posture** 角色需要使用专用思科 ISE 节点。通过管理员门户可用的菜单选项取决于思科 ISE 节点承担的职责和角色。
- **部署模式：**决定您的部署是分布式、独立式还是作为基本双节点部署的独立式高可用性部署。

## 分布式思科 ISE 部署中的角色

思科 ISE 节点可以根据它承担的角色提供各种服务。部署中的每个节点 **Inline Posture** 节点除外均可承担管理、策略服务和监控角色。在分布式部署中，您可以在网络中使用以下节点组合：

- 支持高可用性的主策略管理节点（主 PAN）和辅助策略管理节点（辅助 PAN）
- 支持高可用性的主监控节点（主 MnT 节点）和辅助监控节点（辅助 MnT 节点）
- 用于主 PAN 自动故障转移的一对运行状况检查节点或单个运行状况检查节点
- 用于会话故障转移的一个或多个策略服务节点 (PSN)
- 用于高可用性的一对 **Inline Posture** 节点

## 配置思科 ISE 节点

在安装思科 ISE 节点后，系统会在其上运行管理、策略服务和监控角色提供的默认服务。此节点将处于独立状态。您必须登录思科 ISE 节点的 **Admin** 门户进行配置。您无法编辑独立思科 ISE 节点的角色或服务。但是，您可以编辑主要和辅助思科 ISE 节点的角色和服务。您必须先配置主要 ISE 节点，然后向主要 ISE 节点注册辅助 ISE 节点。

如果首次登录节点，您必须更改默认管理员密码并安装有效许可证。

我们建议不要更改生产中在思科 ISE 上配置的主机名和域名。如有必要，则在初始部署期间为设备重置映像，执行更改，并配置详细信息。

### 开始之前

您应该对如何在思科 ISE 中设置分布式部署有基本了解。请参阅[设置分布式部署的规定](#)。



**步骤 1** 依次选择管理 (Administration) > 系统 (System) > 部署 (Deployment)。

**步骤 2** 选中您要配置的思科 ISE 节点旁边的复选框，然后单击 **Edit**。

**步骤 3** 按照需要输入相应值，然后单击保存 (Save)。

## 配置主策略管理节点

要设置分布式部署，必须首先将思科 ISE 节点配置为主 PAN。

**步骤 1** 依次选择管理 (Administration) > 系统 (System) > 部署 (Deployment)。

一开始 **Register** 按钮将会处于禁用状态。要启用此按钮，必须配置主 PAN。

**步骤 2** 选中当前节点旁边的复选框，然后单击 **Edit**。

**步骤 3** 点击设为主 (Make Primary) 以配置主 PAN。

**步骤 4** 点击 **Save**，保存节点配置。

### 下一步做什么

1. 向您的部署添加辅助节点。
2. 如有必要，请启用分析器服务并配置探测功能。

## 注册辅助思科 ISE 节点

您可以将思科 ISE 节点注册到主 PAN 以形成多节点部署。部署中除主 PAN 以外的节点称为辅助节点。在注册节点时，可以选择必须在节点上启用的角色和服务。注册的节点可从主 PAN 管理（例如，管理节点角色、服务、证书、许可证、应用补丁等）。

注册辅助节点后，主 PAN 会将配置数据推送到辅助节点，而辅助节点上的应用服务器会重启。在完成数据复制后，在主 PAN 上完成的进一步配置更改将复制到辅助节点。在辅助节点上复制更改所需的时间取决于各种因素，如网络延迟、系统负载等。

### 开始之前

确保主 PAN 和正在注册的节点可相互进行 DNS 解析。如果正在注册的节点使用不受信任的自签证书，则系统会提示包含证书详细信息的证书警告。如果接受该证书，则会将其添加到主 PAN 的受信任证书存储区，以启用与节点的 TLS 通信。

如果节点使用非自签证书（例如，由外部 CA 签名），则必须将该节点的相关证书链手动导入到主 PAN 的受信任证书库。当将辅助节点的证书导入受信任证书库时，请选中受信任证书 (Trusted Certificates) 窗口中的信任 ISE 中的身份验证 (Trust for Authentication within ISE) 复选框，以便主 PAN 验证辅助节点的证书。

在注册启用了会话服务（如网络访问、访客、终端安全评估等）的节点时，可以将其添加到节点组。有关更多详细信息，请参阅[创建策略服务节点组](#)，第 63 页。

**步骤 1** 登录到主 PAN。

**步骤 2** 依次选择管理 (**Administration**) > 系统 (**System**) > 部署 (**Deployment**)。

**步骤 3** 点击注册 (**Register**) 以开始注册辅助节点。

**步骤 4** 输入要注册的独立节点的可 DNS 解析完全限定域名 (FQDN)，采用的格式为 `hostname.domain-name`，例如，`abc.xyz.com`。主 PAN 的 FQDN 和正在注册的节点必须能够相互解析。

**步骤 5** 在用户名 (**Username**) 和 密码 (**Password**) 字段中，输入辅助节点的基于 GUI 的管理员凭证。

**步骤 6** 单击下一步。

主 PAN 会在节点注册后尝试建立 TLS 通信（首次）。

- 如果节点使用受信任的证书，则可以继续执行第 7 步。
- 如果节点使用了不受信任的自签证书，则证书警告消息显示有关证书的详细信息（如颁发给、颁发者、序列号等），可对照节点上的实际证书进行验证。点击**导入证书并继续 (Import Certificate and Proceed)** 选项以信任此证书并继续注册。思科 ISE 会将该节点的默认自签证书导入到主 PAN 的受信任证书库。如果不想使用默认的自签证书，请点击**取消注册 (Cancel Registration)** 并将该节点的相关证书链手动导入到主 PAN 的受信任证书库。当将辅助节点的证书导入到受信任证书库时，请选中相应 PAN 旁边的**信任 ISE 内部的身份验证 (Trust for Authentication within ISE)** 复选框，以验证辅助节点的证书。
- 如果节点使用 CA 签名的证书，则系统会显示一条错误消息，表示在设置证书信任之前无法继续注册。

**步骤 7** 选中复选框，以便选择要在节点上启用的角色和服务，然后点击**保存 (Save)**。

注册节点时，主 PAN 上会生成警报（确认已将节点添加到部署中）。在思科 ISE GUI 控制板 (**Dashboard**) 的警报 (**Alarms**) Dashlet 中查看此警报。注册节点同步并重新启动后，您可以使用主 PAN 上所用的相同凭证登录到辅助节点 GUI。

#### 下一步做什么

- 对于时间敏感型任务（例如访客用户访问和授权、登录等），请确保节点上的系统时间已经同步。
- 如果您注册了辅助 PAN，并计划使用内部思科 ISE CA 服务，则必须备份主 PAN 的思科 ISE CA 证书和密钥，并在辅助 PAN 恢复这些证书和密钥。

## 支持多种部署方案

可以在企业基础网络架构中部署思科 ISE，支持 802.1X 有线、无线和虚拟专用网络 (VPN)。

思科 ISE 架构同时支持独立和分布式（也称为高可用性 或冗余）部署，其中一台计算机承担主要角色，另一台 备份计算机承担辅助角色。思科 ISE 具有不同的可配置角色、服务和职责，允许创建和

应用网络中所需的思科 ISE 服务。这样得到的是一个用作功能齐全的综合式系统的全面思科 ISE 部署。

可以使用一个或多个管理、监控和策略服务角色部署思科 ISE 节点。每个角色在整体网络策略管理拓扑中发挥不同但很重要的作用。使用管理角色安装思科 ISE，可以从集中式门户配置和管理网络以提高效率和易用性。

思科 ISE 平台还可以部署为“内联终端安全评估”(Inline Posture)节点，以便在用户通过无线控制器或 VPN 集中器（它们不支持便于思科 ISE 策略管理所需的功能）访问网络时进行策略实施并执行授权更改 (CoA) 请求。

## 思科 ISE 分布式部署

具有不止一个思科 ISE 节点的部署称作分布式部署。要支持故障切换和提高性能，您可以以分布式方式为您的部署设置多个思科 ISE 节点。在思科 ISE 分布式部署中，管理和监控活动会进行集中，而处理则分布在多个 PSN 上。根据您的性能要求，您可以扩展您的部署。部署中的每个思科 ISE 节点都可以担任其中任何一个角色 - 管理、策略服务和监控。Inline Posture 节点由于具有专用性质而不能承担任何其他角色。Inline Posture 节点必须为专用节点。

## 思科 ISE 部署设置

在所有节点上安装思科 ISE 后，如《思科身份服务引擎硬件安装指南》所述，节点显示为独立状态。然后必须定义一个节点作为主 PAN。定义主 PAN 时，必须在该节点上启用管理和监控角色。您可以在主 PAN 上选择启用策略服务角色。在主 PAN 上完成定义角色的任务后，可以向主 PAN 注册其他辅助节点，为辅助节点定义角色。

所有思科 ISE 系统和功能相关配置应当只在主 PAN 上进行。在主 PAN 上执行的配置更改被复制到部署中的所有辅助节点上。

分布式部署中必须至少有一个 MnT。配置主 PAN 时，必须启用监控角色。在部署中注册 MnT 节点后，如果需要，可以编辑主 PAN 并禁用监控角色。

## 从主要 ISE 节点将数据复制至辅助思科 ISE 节点

当您为思科 ISE 节点注册为辅助节点时，思科 ISE 会立即创建一个从主节点到辅助节点的数据复制通道并开始执行复制进程。复制是从主要节点向辅助节点共享思科 ISE 配置数据的过程。复制可确保部署中的所有思科 ISE 节点的配置数据一致。单击相应的单选按钮，以便启用或禁用在思科 ISE 部署中的所有节点之间复制动态发现的终端：

首次将思科 ISE 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 节点保持同步。在思科 ISE 管理员门户的部署 (Deployment) 窗口中，可从节点状态 (Node Status) 列查看复制状态。当您为思科 ISE 节点注册为辅助节点或执行与 PAN 的手动同步时，节点状态显示橙色图标，表示正在进行所请求的操作。同步完成后，节点状态会变为绿色，表示辅助节点已与 PAN 同步。节点状态变为绿色后，思科 ISE 应用服务器需要大约 5 分钟时间来重新启动和运行，才能完成辅助 ISE 节点配置。

## 思科 ISE 节点取消注册

要从部署中删除节点，您必须对该节点取消注册。从主 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，主节点和辅助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。



注释 无法取消注册主 PAN。

## 设置分布式部署的规定

在分布式环境中设置思科 ISE 之前，请仔细阅读以下声明：

- 选择思科 ISE 服务器节点类型或内联终端安全评估节点。对于管理、策略服务和监控功能，必须选择思科 ISE 节点。对于 Inline Posture 服务，必须选择 Inline Posture 节点。
- 为所有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，您必须在设置每个节点时提供同一 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 时配置思科 ISE 管理员密码。以前的思科 ISE 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 DNS 服务器。在 DNS 服务器中输入分布式部署中包含的所有思科 ISE 节点的 IP 地址和完全限定域名 (FQDN)。否则，节点注册将失败。
- 在 DNS 服务器中为分布式部署中的所有思科 ISE 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 节点时可能会遇到部署相关问题。如果未为所有节点配置反向 DNS 查找，则性能可能会降低。
- （可选）从主 PAN 注销辅助思科 ISE 节点以从中卸载思科 ISE。
- 备份主 MnT，然后将数据恢复到新的辅助 MnT。由于会复制新的更改，因此这可确保主 MnT 的历史记录与新 MnT 同步。
- 确保即将注册为辅助节点的主 PAN 和独立节点运行的是同一版本的思科 ISE。
- 在将其他节点添加到部署之前，在思科 ISE 主 PAN 上启用内部 CA 设置 (Internal CA Settings)，以确保思科 ISE 证书服务按预期运行。要启用内部 CA 设置，选择管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书颁发机构 (Certificate Authority) > 内部 CA 设置 (Internal CA Settings)。
- 在向部署中添加新节点时，请确保通配符证书的颁发者证书链是新节点的受信任证书的一部分。将新节点添加到部署中时，通配符证书会被复制到新节点。
- 在将思科 ISE 部署配置为支持思科 TrustSec 时，或者在思科 ISE 与 Cisco Catalyst Center 集成时，请勿将 PSN 配置为仅 SXP。SXP 是思科 TrustSec 和非思科 TrustSec 设备之间的接口。SXP 不与支持思科 TrustSec 的网络设备通信。

- 确保主节点和辅助节点的数据库密码相同。如果在节点安装过程中以不同方式设置这些密码，则您可以使用以下命令对其进行修改：

- `application reset-passwd ise internal-database-admin`

- `application reset-passwd ise internal-database-user`

## 主要节点和辅助节点上可用的菜单选项

作为分布式部署组成部分的思科 ISE 节点中可用的菜单选项取决于在节点上启用的角色。您必须通过主 PAN 执行所有管理和监控活动。对于其他任务，您必须使用辅助节点。因此，根据辅助节点上启用的角色，辅助节点的用户界面提供有限的菜单选项。

如果节点担任不止一个角色，例如某个主职责同时具备策略服务角色和监控角色，则针对 PSN 和主 MnT 列出的菜单选项在该节点上可用。

下表列出在担任不同角色的思科 ISE 节点上可用的菜单选项。

表 6: 思科 ISE 节点和可用的菜单选项

思科 ISE 节点	可用的菜单选项
所有节点	<ul style="list-style-type: none"> <li>• 查看和配置系统时间以及 NTP 服务器设置。</li> <li>• 安装服务器证书并管理证书签名请求。</li> </ul> <p><b>注释</b> 必须直接在各个节点上进行服务器证书操作。私钥不存储于本地数据库中，也不从相关节点复制。私钥存储于本地文件系统中。</p>
主策略管理节点 (主 PAN)	所有菜单和子菜单。
主监控节点 (主 MnT 节点)	<ul style="list-style-type: none"> <li>• 提供对监控数据的访问。</li> </ul>
PSN (策略服务节点)	加入、离开和测试 Active Directory 连接的选项可用。必须单独将每个 PSN 加入到 Active Directory 域中。必须先定义域信息并且将 PAN 联接到 Active Directory 域中。然后，逐一将其他 PSN 加入到 Active Directory 域中。
辅助策略管理节点 (辅助 PAN)	<p>将辅助 PAN 升级为主 PAN 的选项。</p> <p><b>注释</b> 在向主 PAN 注册了辅助节点之后，在登录任意辅助节点的管理员门户时，您必须使用主 PAN 的登录凭证。</p>

## 部署和节点设置

您可以通过部署节点 (**Deployment Nodes**) 窗口配置思科 ISE (PAN、PSN 和 MnT) 节点和内联终端安全评估节点并设置部署。

### 部署节点列表窗口

表 7: 部署节点列表

字段名称	使用指南
主机名	显示节点的主机名。
Node Type	显示节点类型。 它可以是下列类型之一： <ul style="list-style-type: none"> <li>• 思科 ISE (PAN、PSN、Mnt) 节点</li> <li>• Inline Posture 节点</li> </ul>
相关角色	(只有在节点类型为思科 ISE 时才显示) 列出思科 ISE 节点承担的角色，例如管理 (Administration)、策略服务 (Policy Service)、监控 (Monitoring) 或 pxGrid。 例如，管理 ( <b>Administration</b> )、策略服务 ( <b>Policy Service</b> )、监控 ( <b>Monitoring</b> ) 或 <b>pxGrid</b> 。
角色	如果在此节点上启用了管理和监控角色，则指示管理和监控角色承担的职责 (主要、辅助或独立职责)。职责可以是以下一项或多项： <ul style="list-style-type: none"> <li>• <b>PRI(A)</b>: 指主 PAN。</li> <li>• <b>SEC(A)</b>: 指辅助 PAN。</li> <li>• <b>PRI(M)</b>: 指主 MnT。</li> <li>• <b>SEC(M)</b>: 指辅助 MnT。</li> </ul>
服务	(只有在启用策略服务角色时才显示) 列出此思科 ISE 节点上运行的服务。服务可包括以下任意一项： <ul style="list-style-type: none"> <li>• 身份映射</li> <li>• 会话</li> <li>• 剖析</li> <li>• 全部</li> </ul>

字段名称	使用指南
<b>Node Status</b>	<p>指示部署中每个思科 ISE 节点的数据复制状态：</p> <ul style="list-style-type: none"> <li>• 绿色（已连接）：表示部署中已注册的思科 ISE 节点与主 PAN 处于同步状态。</li> <li>• 红色（断开）：表示思科 ISE 节点无法到达、已断开或未进行数据复制。</li> <li>• 橙色（处理中）：表示向主 PAN 新注册了新思科 ISE 节点、您已执行手动同步操作或思科 ISE 节点与主 PAN 不同步。</li> </ul> <p>有关详细信息，请点击节点状态 (<b>Node Status</b>) 列中每个思科 ISE 节点的快速查看图标。</p>

#### 相关主题

[思科 ISE 分布式部署](#)，第 35 页

[思科 ISE 部署术语](#)，第 32 页

[配置思科 ISE 节点](#)，第 32 页

[注册辅助思科 ISE 节点](#)，第 33 页

## 常规节点设置

下表说明思科 ISE 节点的常规设置 (**General Settings**) 窗口中的字段。在此窗口中，可以将角色分配给节点并配置要在其上运行的服务。此窗口的导航路径为：**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **部署节点 (Deployment Node)** > **编辑 (Edit)** > **常规设置 (General Settings)**。

表 8: 常规节点设置

字段名称	使用指南
<b>主机名</b>	显示思科 ISE 节点的主机名。
<b>FQDN</b>	显示思科 ISE 节点的完全限定域名，例如 ise1.cisco.com。
<b>IP 地址</b>	显示思科 ISE 节点的 IP 地址。
<b>Node Type</b>	显示节点类型。可以为以下任一项：身份服务引擎 (ISE)、Inline Posture 节点
<b>相关角色</b>	

字段名称	使用指南
管理	<p>如果思科 ISE 节点承担管理角色，请选中此复选框。只有在受许可提供管理服务的节点上才可以启用 Administration 角色。</p> <p><b>角色 (Role)</b> - 显示管理角色在部署中承担的职责。个人可以选择其中一种值 - <b>独立 (Standalone)</b>、<b>主要 (Primary)</b> 或<b>辅助 (Secondary)</b>。</p> <p><b>设为主要 (Make Primary)</b> - 选择它可使该节点成为主思科 ISE 节点。在部署中您只能有一个主要思科 ISE 节点。当您将此节点设置为主要节点之后，此窗口中的其他选项将进入活动状态。在部署中您只能有两个 Administration 节点。如果节点具有<b>独立 (Standalone)</b>角色，则旁边会显示<b>设为主要 (Make Primary)</b>按钮。如果节点具有<b>辅助 (Secondary)</b>角色，则旁边会显示<b>升级为主要 (Promote to Primary)</b>按钮。如果节点具有<b>主要 (Primary)</b>角色，并且没有其他节点注册到该节点，则旁边会显示<b>设为独立 (Make Standalone)</b>按钮。点击<b>设为独立 (Make Standalone)</b>按钮以使您的主要节点成为独立节点。</p>
Monitoring	<p>如果要思科 ISE 节点承担监控角色并充当日志收集器，请选中此复选框。分布式部署中必须至少有一个监控节点。配置主 PAN 时，必须启用监控角色。在部署中注册辅助监控节点之后，如有必要，可以编辑主 PAN 和禁用监控角色。</p> <p>要在 VMware 平台上将思科 ISE 节点配置为您的日志收集器，请使用以下规定确定您所需要的最低磁盘空间：您的网络中每天每个终端 180 KB，您的网络中每天每个思科 ISE 节点 2.5 MB。</p> <p>您可以根据您想要将多少个月的数据至于监控模式下，计算您所需的最大磁盘空间。如果您的部署中只有一个监控节点，则该节点会承担独立职责。如果在部署中有两个监控节点，思科 ISE 还会显示另一个监控节点的名称以供您配置主要/辅助角色。要配置这些职责，请选择以下选项之一：</p> <ul style="list-style-type: none"> <li>• <b>主 (Primary)</b>: 使当前节点成为主监控节点。</li> <li>• <b>辅助 (Secondary)</b>: 使当前节点成为辅助监控节点。</li> <li>• <b>无 (None)</b> - 如果要使监控节点不承担主要-辅助角色。</li> </ul> <p>如果您将您的一个监控节点配置为主要或辅助节点，另一个监控节点相应地自动成为辅助或主要节点。主要监控节点和辅助监控节点都接收管理和策略服务日志。如果将一个监控节点的角色改为<b>无 (None)</b>，则另一个监控节点的角色也会成为<b>无 (None)</b>，从而会在您将某个节点指定为监控节点之后取消高可用性对。您会在<b>远程日志记录目标 (Remote Logging Targets)</b>窗口中发现此节点被列为系统日志目标：<b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 远程日志记录目标 (Remote Logging Targets)</b>。</p>



字段名称	使用指南
策略服务	<p>选中此复选框可启用以下任一或所有服务：</p> <ul style="list-style-type: none"> <li>• <b>启用会话服务 (Enable Session Services)</b>：选中此复选框可启用网络访问、终端安全评估、访客和客户端调配服务。从在节点组中包含节点 (<b>Include Node in Node Group</b>) 下拉列表中选择此策略服务节点所属的组。请注意，证书颁发机构 (CA) 和安全传输注册 (EST) 服务只能在已启用会话服务的策略服务节点上运行。</li> </ul> <p>对于在节点组中包含节点 (<b>Include Node in Node Group</b>)，如果不希望此策略服务节点加入某个组，请选择无 (<b>None</b>)。</p> <p>同一个节点组中的所有节点都应在网络接入设备上配置为 RADIUS 客户端，并获 CoA 授权，因为这些节点中的任何一个节点均可通过节点组中的任何节点建立的会话发出 CoA 请求。如果您未使用负载均衡器，则节点组中的节点应与在 NAD 上配置的 RADIUS 服务器和客户端相同，或作为 RADIUS 服务器和客户端的子集。这些节点还将配置为 RADIUS 服务器。</p> <p>虽然单个 NAD 可以配置多个思科 ISE 节点以作为 RADIUS 服务器和动态授权客户端，但节点不必全部位于同一个节点组。</p> <p>一个节点组中的所有成员应通过高速 LAN 连接（例如，千兆以太网）互相建立连接。虽然节点组成员不需要在第二层相邻，但是我们依然建议节点组成员在第 2 层相邻，以确保足够的宽带和可达性。有关详细信息，请参阅<a href="#">创建策略服务节点组</a>，第 63 页。</p> <ul style="list-style-type: none"> <li>• <b>启用分析服务 (Enable Profiling Service)</b>：选中此复选框可启用分析服务。如果启用分析服务，必须点击<b>分析配置 (Profiling Configuration)</b> 选项卡并根据要求输入详细信息。当您启用或禁用策略服务节点上运行的任意服务或对此节点做任何更改时，您将重新启动运行这些服务的应用服务器进程。这些服务重新启动时，预计会有延迟。您可以从 CLI 使用 <b>show application status ise</b> 命令，确定何时在节点上重新启动了应用服务器。</li> </ul>
pxGrid	<p>选中此复选框可启用 pxGrid 角色。思科 pxGrid 用于将来自思科 ISE 会话目录区分上下文的信息共享给其他策略网络系统，如思科自适应安全设备 (ASA)。此 pxGrid 框架还可用于在节点之间交换策略和配置数据，例如在思科 ISE 和第三方供应商之间共享标签和策略对象，以及交换威胁信息等非思科 ISE 相关信息。</p>

#### 相关主题

[分布式思科 ISE 部署中的角色](#)，第 32 页

[管理节点](#)，第 48 页

[策略服务节点](#)，第 49 页

[监控节点](#)，第 50 页

[思科 pxGrid 节点](#)，第 54 页

[同步主要和辅助思科 ISE 节点](#)，第 61 页

[创建策略服务节点组](#)，第 63 页

[部署思科 pxGrid 节点，第 56 页](#)

[更改节点角色和服务，第 62 页](#)

[配置用于自动故障切换的监控节点，第 54 页](#)

## 分析节点的设置

下表介绍分析配置 (**Profiling Configuration**) 窗口上的字段，您可以使用此窗口为分析器服务配置探测功能。此窗口的导航路径为：**管理 (Administration) > 系统 (System) > 部署 (Deployment) > ISE 节点 (ISE Node) > 编辑 (Edit) > 分析配置 (Profiling Configuration)**。

表 9: 分析节点的设置

字段名称	使用指南
<b>NetFlow</b>	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 NetFlow，以便接收从路由器发送的 NetFlow 数据包。为以下选项输入所需的值： <ul style="list-style-type: none"> <li>• <b>接口 (Interface):</b> 选择思科 ISE 节点上的接口。</li> <li>• <b>端口 (Port):</b> 输入从路由器接收 NetFlow 导出数据的 NetFlow 侦听器端口号。默认端口为 9996。</li> </ul>
<b>DHCP</b>	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 DHCP，以便侦听来自 IP 帮助程序的 DHCP 数据包。为以下选项提供值： <ul style="list-style-type: none"> <li>• <b>接口 (Interface):</b> 选择思科 ISE 节点上的接口。</li> <li>• <b>端口 (Port):</b> 输入 DHCP 服务器 UDP 端口号。默认端口为 67。</li> </ul>
<b>DHCP SPAN</b>	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 DHCP，以便收集 DHCP 数据包。 <ul style="list-style-type: none"> <li>• <b>接口 (Interface):</b> 选择思科 ISE 节点上的接口。</li> </ul>
<b>HTTP</b>	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 HTTP，以便接收并解析 HTTP 数据包。 <ul style="list-style-type: none"> <li>• <b>接口 (Interface):</b> 选择思科 ISE 节点上的接口。</li> </ul>
<b>RADIUS</b>	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 RADIUS 服务器，以便收集 RADIUS 会话属性，以及来自已启用思科 IOS 传感器的设备的思科设备协议 (CDP) 和链路层发现协议 (LLDP) 属性。
<b>Network Scan (NMAP)</b>	选中此复选框可启用 NMAP 探测。

字段名称	使用指南
<b>DNS</b>	<p>选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 DNS，以便对 FQDN 执行 DNS 查找。以秒为单位输入<b>超时 (Timeout)</b> 期间。</p> <p><b>注释</b> 要使 DNS 探测功能在分布式部署中特定思科 ISE 节点上运行，您必须启用这些探测功能 - DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP。对于 DNS 查找，必须连同 DNS 探测功能一起启用这些探测功能之一。</p>
<b>SNMP Query</b>	<p>选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 SNMP 查询，以便按照指定的间隔轮询网络设备。在<b>重试 (Retries)</b>、<b>超时 (Timeout)</b>、<b>事件超时 (Event Timeout)</b>（必填）和<b>说明 (Description)</b>（可选）字段中输入值。</p> <p><b>注释</b> 除配置 SNMP 查询探测功能之外，还必须在<b>管理 (Administration)</b> &gt; <b>网络资源 (Network Resources)</b> &gt; <b>网络设备 (Network Devices)</b> 中配置其他 SNMP 设置。当在网络设备上配置 SNMP 设置时，请确保在网络设备上全局启用 CDP 和 LLDP。</p>
<b>SNMP 陷阱</b>	<p>选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 SNMP 陷阱探测，以便从网络设备接收链路接通、链路断开和 MAC 通知陷阱。提供或启用以下信息：</p> <ul style="list-style-type: none"> <li>• <b>链接陷阱查询 (Link Trap Query)</b>：选中此复选框可接收和解释通过 SNMP 陷阱接收的通知。</li> <li>• <b>MAC 陷阱查询 (MAC Trap Query)</b>：选中此复选框可接收和解释通过 SNMP 陷阱接收的 MAC 通知。</li> <li>• <b>接口 (Interface)</b>：选择思科 ISE 节点上的接口。</li> <li>• <b>端口 (Port)</b>：输入要使用的主机 UDP 端口。默认端口为 162。</li> </ul>
<b>Active Directory</b>	<p>选中此复选框可扫描所定义的 Active Directory 服务器，以获取有关 Windows 用户的信息。</p> <ul style="list-style-type: none"> <li>• <b>重新扫描前的天数 (Days before rescan)</b>：选择您希望经过多少天后再次运行扫描。</li> </ul>

#### 相关主题

[思科 ISE 分析服务](#)，第 396 页

[分析服务使用的网络探测功能](#)，第 398 页

[在思科 ISE 节点中配置分析服务](#)，第 397 页

## 日志记录设置

下面的小节解释了如何配置调试日志的严重性、创建外部日志目标，并使思科 ISE 能够将日志消息发送到这些外部日志目标。

### 远程日志记录目标设置

下表介绍远程日志记录目标 (**Remote Logging Targets**) 窗口中的字段，您可以使用此窗口创建外部位置（系统日志服务器）来存储日志记录消息。此页面的导航路径为**管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 远程日志记录目标 (Remote Logging Targets)**。单击**添加 (Add)**。

表 10: 远程日志记录目标设置

字段名称	使用指南
<b>Name</b>	为新的系统日志目标输入名称。
<b>Target Type</b>	从下拉列表中选择目标类型。默认值为 <b>UDP 系统日志 (UDP Syslog)</b> 。
<b>Description</b>	输入新目标的简短说明。
<b>IP 地址</b>	输入将存储日志的目标计算机的 IP 地址或主机名。
<b>端口</b>	输入目标计算机的端口号。
<b>Facility Code</b>	从下拉列表中选择必须用于记录的系统日志设备代码。有效选项为 Local0 至 Local7。
<b>Maximum Length</b>	输入远程日志目标消息的最大长度。有效值为 200 至 1024 字节。
<b>包括此目标的警报 (Include Alarms For This Target)</b>	选中此复选框时，警报消息也会发送到远程服务器。
<b>符合 RFC 3164 (Comply to RFC 3164)</b>	选中此复选框时，即使使用了反斜线 (\)，发送到远程服务器的系统日志消息中的分隔符 ( ; { } \ ) 也不会转义。
<b>Buffer Message When Server Down</b>	当您从目标类型 ( <b>Target Type</b> ) 下拉列表中选择 <b>TCP 系统日志 (TCP Syslog)</b> 或 <b>安全系统日志 (Secure Syslog)</b> 时，系统会显示此复选框。如果希望思科 ISE 在 TCP 系统日志目标或安全系统日志目标不可用时缓冲系统日志消息，请选中此复选框。思科 ISE 会在与目标的连接恢复时重新尝试将消息发送到目标。连接恢复后，将按从最旧到最新的顺序发送消息。缓冲消息会始终在新消息之前发送。如果缓冲区已满，则会丢弃旧消息。
<b>Buffer Size (MB)</b>	设置每个目标的缓冲区大小。默认情况下设置为 100 MB。更改缓冲区大小会清除缓冲区，并且特定目标的所有现有缓冲消息都会丢失。

字段名称	使用指南
<b>Reconnect Timeout (Sec)</b>	输入时间（以秒为单位），以便配置在服务器关闭的情况下，TCP 和安全系统日志在被丢弃之前将会保留多长时间。
<b>Select CA Certificate</b>	当您从目标类型 ( <b>Target Type</b> ) 下拉列表中选择 <b>安全系统日志 (Secure Syslog)</b> 时，系统会显示此下拉列表。从下拉列表中选择一个客户端证书。
<b>Ignore Server Certificate Validation</b>	当您从目标类型 ( <b>Target Type</b> ) 下拉列表中选择 <b>安全系统日志 (Secure Syslog)</b> 时，系统会显示此复选框。选中此复选框，以便让思科 ISE 忽略服务器证书身份验证并接受任何系统日志服务器。默认情况下，除非在禁用此复选框时系统处于 FIPS 模式，否则此选项设置为关闭。

#### 相关主题

- [思科 日志记录机制](#)，第 175 页
- [思科 ISE 系统日志](#)，第 176 页
- [思科 ISE 消息目录](#)，第 179 页
- [集合过滤器](#)，第 181 页
- [事件抑制绕行过滤器](#)，第 182 页
- [配置远程系统日志收集位置](#)，第 177 页
- [配置集合过滤器](#)，第 181 页

## 配置日志记录类别

下表介绍了可用于配置日志记录类别的字段。设置日志严重性级别，然后为日志记录类别的日志选择日志记录目标。此窗口的导航路径为**管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)**。

单击想要查看的日志记录类别旁边的单选按钮，单击**编辑 (Edit)**。下表对日志记录类别的编辑窗口中显示的字段进行了说明。

表 11: 日志记录类别设置

字段名称	使用指南
<b>Name</b>	显示日志记录类别的名称。

字段名称	使用指南
<b>Log Severity Level</b>	<p>对于某些日志记录类别，默认情况下会设置此值，并且您无法对其进行编辑。对于某些日志记录类别，您可以从下拉列表中选择以下严重性级别之一：</p> <ul style="list-style-type: none"> <li>• <b>严重 (FATAL)</b>：紧急级别。此级别意味着您无法使用思科 ISE，并且必须立即采取必要的操作。</li> <li>• <b>错误 (ERROR)</b>：此级别表示严重错误情况。</li> <li>• <b>警告 (WARN)</b>：此级别表示正常但值得注意的情况。这是会为很多日志记录类别设置的默认级别。</li> <li>• <b>信息 (Info)</b>：此级别表示供参考的消息。</li> <li>• <b>调试 (DEBUG)</b>：此级别表示诊断错误消息。</li> </ul>
<b>Local Logging</b>	选中此复选框可为本地节点上的类别启用日志记录事件。
目标	<p>该区域允许您使用左侧和右侧图标在可用 (<b>Available</b>) 和所选 (<b>Selected</b>) 区域之间转移目标，从而更改类别的目标。</p> <p>可用 (<b>Available</b>) 区域包含本地（预定义）和外部（用户定义）的现有日志记录目标。</p> <p>选定 (<b>Selected</b>) 区域最初为空，然后会显示为该类别选择的目标。</p>

#### 相关主题

[思科 ISE 消息代码](#)，第 178 页

[配置远程系统日志收集位置](#)，第 177 页

[设置消息代码的严重性级别](#)，第 178 页

## 管理员访问设置

您可以通过这些部分来为管理员配置访问设置。

### 管理员密码策略设置

下表介绍了密码策略 (**Password Policy**) 选项卡中的字段，可以使用此选项卡来定义管理员密码应满足的条件。此窗口的导航路径为：**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **身份验证 (Authentication)** > **密码策略 (Password Policy)**。。

表 12: 管理员密码策略设置

字段名称	使用指南
最小长度 (Minimum Length)	指定密码的最小长度（以字符数为单位）。默认值为 6 个字符。

字段名称	使用指南
密码不可包含管理员姓名或其反向顺序的字符	选中此复选框可限制使用管理员用户名或其反向顺序的字符。
密码不可包含“cisco”或其反向顺序的字符	选中此复选框可限制使用字词“cisco”或其反向顺序的字符。
密码不可包含_____或其反向顺序的字符	选中此复选框可限制使用您定义的任何字词或其反向顺序的字符。
密码不可包含连续重复四次或以上的字符	选中此复选框可限制使用连续重复四次或以上的字符。
必用字符	指定管理员密码必须包含从以下选项中选择的地类型的至少一个字符： <ul style="list-style-type: none"> <li>• 小写字母字符</li> <li>• 大写字母字符</li> <li>• 数字字符</li> <li>• 非字母数字字符</li> </ul>
密码历史记录 (Password History)	指定必须与新密码不同的先前密码的数量，以防止重复使用同一密码。 此外，指定必须与先前密码不同的字符的数量。 输入在其之前不能重复使用密码的天数。
“密码有效期” (Password Lifetime)	指定以下选项来强制用户在经过指定时间段后更改密码： <ul style="list-style-type: none"> <li>• “如果此时间（按天计）过后未更改密码，则禁用管理员帐户。” (Time (in days) before the administrator account is disabled if the password is not changed.) （允许的范围是 0 至 2147483647 天。）</li> <li>• “禁用管理员帐户之前的提醒时间（按天计）。” (Reminder (in days) before the administrator account is disabled.)</li> </ul>
“不正确的登录尝试之后锁定或暂停帐户” (Lock or Suspend Account with Incorrect Login Attempts)	指定思科 ISE 在将管理员锁定以及暂停或禁用帐户凭证之前记录错误管理员密码的次数。 系统会向其帐户已锁定的管理员发送邮件。您可以输入自定义邮件补救消息。

## 相关主题

[思科 ISE 管理员](#)，第 9 页

[创建新管理员](#)，第 10 页

## 会话超时和会话信息设置

下表介绍会话 (Session) 窗口中的字段，您可以使用此窗口定义会话超时和终止活动管理会话。此窗口的导航路径为：[管理 \(Administration\)](#) > [系统 \(System\)](#) > [管理员访问 \(Admin Access\)](#) > [设置 \(Settings\)](#) > [会话 \(Session\)](#)。

表 13: 会话超时和会话信息设置

字段名称	使用指南
会话超时	
会话空闲超时 (Session Idle Timeout)	输入思科 ISE 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。
会话信息	
失效 (Invalidate)	选中要终止的会话 ID 旁边的复选框，然后单击失效 (Invalidate)。

## 相关主题

[管理员访问设置](#)，第 145 页

[配置管理员会话超时](#)，第 147 页

[终止活动管理会话](#)，第 147 页

## 管理节点

通过具有管理角色的思科 ISE 节点，您可以在思科 ISE 上进行所有管理操作。此节点处理与诸如身份验证、授权和审核等功能有关的所有系统相关配置。在分布式环境中，最多可以具有两个运行管理角色的节点。管理角色可以承担以下角色 - 独立角色、主角色或辅助角色。

## 管理节点的高可用性

### 手动将辅助 PAN 升级为主 PAN

如果主 PAN 出现故障而且您没有配置 PAN 自动故障切换，则必须手动将辅助 PAN 升级为主 PAN。



## 开始之前

确保已配置具有管理角色的第二个思科 ISE 节点，以将其升级为主 PAN。

**步骤 1** 登录辅助 PAN GUI。

**步骤 2**

**步骤 3** 在编辑节点 (**Edit Node**) 窗口中，点击升级为主节点 (**Promote to Primary**)。

**注释** 只能将辅助 PAN 升级为主 PAN。仅承担策略服务角色和/或监控角色的思科 ISE 节点无法升级为主 PAN。

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。

在辅助节点的编辑节点 (**Edit Node**) 页面，无法修改角色或服务，因为这些选项已禁用。您必须登录 Admin 门户才能进行更改。

**步骤 4** 点击保存 (**Save**)。

## 策略服务节点

策略服务节点 (PSN) 是承担策略服务角色的思科 ISE 节点，提供网络访问、终端安全评估、访客访问、客户端调配和分析服务。

分布式设置中至少有一个节点应当承担策略服务角色。此角色评估策略并制定所有决策。通常，分布式部署中有多个 PSN。

驻留在同一高速局域网 (LAN) 中或负载均衡器后面的所有 PSN 可以组合在一起，形成一个节点组。如果节点组中的一个节点发生故障，其他节点会检测到故障，并重置 URL 重定向会话（如有）。

## 策略服务节点的高可用性

要检测节点故障并在故障节点上重置所有 URL 重定向的会话，可将两个或多个 PSN 放置在同一节点组中。当属于节点组的节点出现故障时，同一个节点组中的另一个节点会为故障节点上的所有 URL 重定向会话发出授权更改 (CoA) 请求。

同一个节点组中的所有节点都应在网络接入设备 (NAD) 上配置为 RADIUS 客户端并拥有 CoA 授权，因为这些节点中的任何一个节点均可通过该节点组中的任一节点建立的会话发出 CoA 请求。如果您未使用负载均衡器，节点组中的节点应与在 NAD 上配置的 RADIUS 服务器和客户端相同，或是 RADIUS 服务器和客户端的子集。这些节点还应配置为 RADIUS 服务器。



**注释** 虽然单个 NAD 可以配置多个思科 ISE 节点以作为 RADIUS 服务器和动态授权客户端，但节点不必全部位于同一个节点组。

一个节点组中的所有成员应通过高速 LAN 连接（例如，千兆以太网）互相建立连接。虽然节点组成员不需要在第二层相邻，但是我们依然建议节点组成员在第 2 层相邻，以确保足够的带宽和可达性。有关更多详细信息，请参阅[创建策略服务节点组](#)，第 63 页。

## 用于在 PSN 之间均匀分配请求的负载均衡器

如果您在部署中具有多个 PSN，则可以使用负载均衡器均匀分配请求。负载均衡器会将请求分配给其后面的功能节点。请参阅《[思科和 F5 部署指南：使用 BIG-IP 的 ISE 负载均衡](#)》中的信息并了解有关在负载均衡器后面部署 PSN 的最佳实践。

## 策略服务节点中的会话故障切换

节点组中的 PSN 共享会话信息。节点交换心跳消息以检测节点故障。如果某个节点出现故障，其节点组中的一个对等体会了解故障 PSN 上的会话并发出 CoA 以断开这些会话。大多数客户端会自动重新连接并建立新会话。

某些客户端不会自动重新连接。例如，如果客户端通过 VPN 连接，则此客户端可能看不到 CoA。作为 IP 电话、多主机 802.1X 端口或虚拟机的客户端也可能看不到或无法响应 CoA。URL 重定向客户端 (webauth) 也无法自动连接。这些客户端必须手动重新连接。

时间问题也会阻止重新连接，例如，如果发生 PSN 故障转移，终端安全评估处于待处理状态。

分布式部署中的 PSN 不会彼此共享其计算机访问限制 (MAR) 缓存。如果启用了思科 ISE 的 MAR 功能，当对客户端计算机进行身份验证的 PSN 发生故障时，该部署内的另一个 PSN 会处理用户身份验证。但是，用户身份验证会失败，因为第二个 PSN 的 MAR 缓存中没有主机身份验证信息。

## 策略服务节点组中的节点数量

节点组中可以具有的节点数量取决于部署要求。节点组确保检测到节点故障，并且对等节点针对已获授权但尚未进行安全评估的会话发出 CoA。节点组的规模不必非常大。

如果节点组的规模增大，那么节点之间交换的消息和心跳数量也会显著增加。因此，流量也会随之增加。节点组中的节点较少时，有助于减少流量，同时提供足够的冗余来检测 PSN 故障。

节点组集群可以包含的 PSN 数量没有硬性限制。

## 监控节点

承担监控角色的思科 ISE 节点用作日志收集器，并将来自 PAN 和 PSN 的日志消息存储在网络中。此角色提供高级监控和故障排除工具，可用于有效地管理网络和资源。承担此角色的节点会整合并关联收集到的数据，以报告形式向您提供有意义的信息。

思科 ISE 最多允许有两个节点承担此角色（由主或辅助节点承担此角色），以实现高可用性。主要和辅助 MnT 节点均收集日志消息。如果主 MnT 断开，则主 PAN 将指向辅助节点以收集监控数据。但辅助节点不会自动升级为主节点。这可以按照[手动修改 MnT 角色](#)中所述的程序来完成。

分布式设置中至少有一个节点应承担监控角色。我们建议您不要对同一个思科 ISE 节点启用监控和策略服务角色，而应只将该节点用于监控以实现最佳性能。

您可以从部署中的 PAN 和主监控节点访问监控 (Monitoring) 菜单。

## 手动修改 MnT 角色

您可以从主要 PAN 手动修改 MnT 角色（从主要改为辅助，从辅助改为主要）。

**步骤 1** 登录到主 PAN GUI。

**步骤 2** 依次选择管理 (Administration) > 系统 (System) > 部署 (Deployment)。

**步骤 3** 从节点列表中，选中要更改角色的 MnT 节点旁边的复选框。

**步骤 4** 单击编辑。

**步骤 5** 在监控 (Monitoring) 部分中，将角色更改为主要 (Primary) 或辅助 (Secondary)。

如果要禁用该节点上启用的所有其他角色和服务，可以启用 选项。启用此选项后，系统将停止该节点上的配置数据复制过程。这有助于提高 MnT 节点的性能。当禁用此选项时，将触发手动同步。

**步骤 6** 点击保存 (Save)。

## MnT 节点中的自动故障切换

MnT 节点不提供高可用性，但支持主用备用。PSN 会将操作审核数据同时复制到主 MnT 节点和辅助 MnT 节点。

### 自动故障切换过程

当主 MnT 节点断开时，辅助 MnT 节点会接管所有监控和故障排除信息。

要将辅助节点转换为主节点，请参阅[手动修改 MnT 角色](#)。如果主节点在辅助节点升级后恢复运行，则主节点将承担辅助节点的角色。如果未升级辅助节点，则主 MnT 节点将在恢复运行后继续承担主要角色。



**注意** 当主节点在故障转移后恢复正常时，请备份辅助节点并恢复数据以更新主节点。

### MnT 节点主用备用对设置指南

您可以在思科 ISE 网络上指定两个 MnT 节点，然后将它们配置为主用备用对。我们建议备份主 MnT 节点，然后将数据恢复到新的辅助 MnT 节点。由于会复制新数据，因此这可确保主 MnT 节点的历史记录与新的辅助节点同步。以下规则适用于主用备用对：

- 所有更改都会记录到主 MnT 节点。辅节点为只读。
- 对主节点所做的更改会在辅助节点上自动复制。

- 主节点和辅助节点列为日志收集器，其他所有节点会向其发送日志。
- 思科 ISE 控制面板是监控和故障排除的主要入口点。控制板上显示来自主监控节点的监控信息。如果主节点关闭，可以从辅助节点获得信息。
- 备份和清除 MnT 数据不在标准思科 ISE 节点备份过程中。必须同时在主辅 MnT 节点上为备份和数据清除配置存储库，并且在每个节点上使用相同的存储库。

### MnT 节点故障转移方案

以下方案适用于 MnT 节点对应的主用备用或单节点配置：

- 在 MnT 节点的主用备用配置中，主 PAN 始终指向主 MnT 节点以收集监控数据。在主 MnT 节点故障后，PAN 会指向备用 MnT 节点。从主节点到辅助节点的故障转移发生在其关闭超过五分钟后。  
但是，在主节点发生故障后，辅助节点不会成为主节点。如果主节点启动，PAN 会再次开始从恢复的主节点收集监控数据。
- 如果主 MnT 节点关闭，并且您希望将备用 MnT 节点升级为活动状态，则可以按照[手动修改 MnT 角色](#)中提供的程序或通过注销现有主 MnT 节点来实现。注销现有 MnT 节点时，备用节点成为主 MnT 节点，并且 PAN 自动指向新升级的主节点。
- 在主用-备用对中，如果注销辅助 MnT 节点或辅助 MnT 节点关闭，则现有主 MnT 节点仍然为当前主节点。
- 如果思科 ISE 部署中只有一个 MnT 节点，则该节点用作主 MnT 节点，并向 PAN 提供监控节点。但是，当注册新 MnT 节点并使其成为部署中的主节点时，现有主 MnT 节点会自动成为备用节点。PAN 会指向新注册的主 MnT 节点以收集监控数据。

## 监控数据库

鉴于监控功能使用的数据的比例和数量，需要在专用节点上将一个单独的数据库用于这些用途。

像 PSN 一样，MnT 节点有一个专用数据库，要求您执行维护任务，如本节所涵盖的主题所述：

### 备份和恢复监控数据库

监控数据库处理大量数据。随着时间推移，MnT 节点的性能和效率取决于您对这些数据的管理水平。要提高效率，我们建议您定期备份数据并将其传输到远程存储库。通过计划自动备份，您可以将此任务自动化。



**注释** 如果正在进行清除操作，则不应执行备份。如果在清除操作过程中启动备份，则清除操作会停止或失败。

如果注册辅助 MnT 节点，我们建议先备份主 MnT 节点，然后将数据恢复到新的辅助 MnT 节点。在复制新的更改时，这可确保主 MnT 节点的历史记录与新的辅助节点同步。

## 监控数据库清除

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，管理监控数据库的大小。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 80%）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。

## 清除监控数据库指南

请遵循这些准则以优化 监控数据库磁盘的使用：

- 如果监控数据库磁盘使用率大于阈值设置的 80%，即总磁盘空间的 60%，则会生成严重警报，表示数据库大小即将超过分配的最大磁盘大小。如果磁盘使用率大于阈值设置的 90%，即总磁盘空间的 70%，则会生成另一个警报，表示数据库大小已超过分配的最大磁盘大小。

系统将运行清除过程，并创建状态历史报告，可以在**数据清除审核 (Data Purging Audit)** 窗口中查看该报告。此窗口的导航路径为**操作 (Operations) > 报告 (Reports) > 报告 (Reports) > 审核 (Audit) > 数据清除审核 (Data Purging Audit)**。清除完成后会生成信息 (INFO) 警报。

- 清除同样依据数据库已使用的磁盘空间。当监控数据库已使用的磁盘空间达到或超过阈值时（默认为总磁盘空间的 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 80%。系统总会在检查监控数据库磁盘空间限制之后，才继续执行清除。

## 清除较旧的监控数据

### 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** 依次选择 **Administration > System > Maintenance > Data Purging**。

**步骤 2** 以月为单位指定数据的保留期限。指定期限之前的所有数据都会清除。对于该选项，每月包括 30 天。三个月默认等于 90 天。

**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 3 天，而且该值小于诊断表中的现有阈值（例如，默认值为 5 天），则根据在此页面中配置的值（3 天）清除数据。

**步骤 3** 点击 **Submit**。

**步骤 4** 查看数据清除审核报告，验证数据清除是否成功。

---

### 下一步做什么

思科 ISE 日志收集

执行按需备份

## 配置用于自动故障切换的监控节点

如果部署中有两个 MnT 节点，则可以配置用于自动故障切换的主节点-辅助节点对，以避免思科 ISE 监控服务出现停机。主节点-辅助节点对可确保辅助 MnT 节点在主节点出现故障时自动提供监控。

### 开始之前

- 在配置用于自动故障转移的 MnT 节点之前，必须将这些节点注册为思科 ISE 节点。
- 您必须在两个节点上配置监控角色和服务，适当地根据其主要和辅助角色进行命名。
- 在主要和辅助 MnT 节点上同时配置用于备份和数据清除的存储库。要让备份和清除功能正常运行，请对这两个节点使用相同的存储库。清除同时在冗余对的主要和辅助节点中发生。例如，如果主要 MnT 节点将两个存储库用于备份和清除，则必须为辅助节点指定相同的存储库。

使用系统 CLI 中的 **repository** 命令为 MnT 节点配置数据存储库。



**注释** 要让计划的备份和清除在监控冗余对的节点上正常工作，请使用 CLI 在主节点和辅助节点上同时配置相同的存储库。存储库不会自动在两个节点之间同步。

在思科 ISE 控制板中，验证 MnT 节点是否准备就绪。**系统摘要 (System Summary) Dashlet** 会在 MnT 节点服务准备就绪时显示左侧带绿色复选标记的 MnT 节点。

**步骤 1** 依次选择**管理 (Administration) > 系统 (System) > 部署 (Deployment)**。

**步骤 2** 在**部署节点 (Deployment Nodes)** 窗口中，选中要指定主节点的 MnT 节点旁边的复选框，然后单击 **Edit**。

**步骤 3** 单击 **General Settings** 选项卡，然后从 **Role** 下拉列表中选择 **Primary**。

选择 MnT 节点作为主节点时，另一个 MnT 节点将自动成为辅助节点。如果是独立部署，主要和辅助角色配置会处于禁用状态。

**步骤 4** 单击 **Save**。主节点和辅助节点都会重新启动。

## 思科 pxGrid 节点

可以使用思科 pxGrid 与其他网络系统（例如思科 ISE 生态系统合作伙伴系统）和其他思科平台共享思科 ISE 会话目录中的情景相关信息。pxGrid 框架也可用来在思科 ISE 与第三方供应商之间、在节

点（例如共享标记）与策略对象之间交换策略和配置数据，还能进行其他信息的交换。思科 pxGrid 还允许第三方系统调通过自适应网络控制操作来隔离用户和/或设备以应对网络或安全事件。可通过思科 TrustSec 主题将标签定义、值和说明等思科 TrustSec 信息从思科 ISE 传输到其他网络。可通过终端配置文件元主题，将具有完全限定名称 (FQN) 的终端配置文件从思科 ISE 传输到其他网络。思科 pxGrid 还支持标签和终端配置文件的批量下载。

在高可用性配置中，思科 pxGrid 服务器通过 PAN 在节点之间复制信息。当 PAN 关闭时，思科 pxGrid 服务器会停止处理客户端注册和订用。需要手动升级 PAN，以激活思科 pxGrid 服务器。

在具有 pxGrid 角色的活动思科节点上，这些进程会显示为正在运行 (**Running**)。在备用思科 pxGrid 节点上，它们会显示为备用 (**Standby**)。如果活动 pxGrid 节点关闭，备用 pxGrid 节点会检测到此情况，并启动四个 pxGrid 进程。在几分钟内，这些进程显示为正在运行 (**Running**)，备用节点成为活动节点。可以运行 CLI 命令 **show logging application pxgrid/pxgrid.state** 来验证思科 pxGrid 服务在此节点上是否处于备用状态。

启动面向辅助思科 pxGrid 节点的自动故障切换后，如果原始主思科 pxGrid 节点重新接入网络，则除非当前主节点关闭，否则原始主思科 pxGrid 节点将继续具有辅助角色，并且不会重新升级到主角色。




---

注释 有时，原始主思科 pxGrid 节点可能会自动重新升级回主角色。

---

在高可用性部署中，当主 pxGrid 节点关闭时，可能需要大约 3 到 5 分钟来切换到辅助 pxGrid 节点。我们建议客户端等待故障切换完成，然后再清除缓存数据，以防主思科 pxGrid 节点发生故障。

以下日志可用于思科 pxGrid 节点：

- pxgrid.log: 通过状态变更通知。
- pxgrid-cm.log: 显示有关客户端与服务器之间的发布者和/或用户以及数据交换活动的更新。
- pxgrid-controller.log: 显示客户端功能、组和客户端授权的详细信息。
- pxgrid-jabberd.log: 显示与系统状态和身份验证相关的所有日志。
- pxgrid-pubsub.log: 显示与发布者和用户事件相关的所有信息。




---

注释

---




---

注释 可以使用 Base 许可证启用思科 pxGrid，但必须使用 Plus 许可证才能启用思科 pxGrid 角色。

---




---

注释

---

## 思科 pxGrid 客户端和功能管理

使用 Cisco pxGrid 服务之前，连接到思科 ISE 的客户端必须注册并获得帐户审批。Cisco pxGrid 客户端使用 Cisco pxGrid SDK 中提供的 Cisco pxGrid 客户端库成为客户端。思科 ISE 同时支持自动和手动批准。客户端可以使用唯一名称和基于证书的相互身份验证登录 Cisco pxGrid。类似于交换机上的 AAA 设置，客户端可以连接已配置的 Cisco pxGrid 服务器主机名或 IP 地址。

Cisco pxGrid 功能是指 Cisco pxGrid 上供客户端发布和订用的信息主题或信道。在思科 ISE 中，仅支持身份、自适应网络控制 (ANC) 和安全组访问 (SGA) 等功能。您可以启用或禁用功能。如果禁用这些功能，客户端就被取消订用。可通过发布、定向查询或批量下载查询，从发布方获取功能信息。

### 相关主题

[生成思科 pxGrid 证书](#)

## 启用 pxGrid 服务

### 开始之前

- 至少在一个节点上启用 pxGrid 角色，以查看思科 pxGrid 客户端发送的请求。
- 启用身份映射。有关详细信息，请参阅[配置身份映射](#)，第 58 页。

---

**步骤 1** 选择管理 (Administration) > pxGrid 服务 (pxGrid Services)。

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

**步骤 3** 要查看功能，请点击右上角的根据功能查看 (View by Capabilities)。

**步骤 4** 点击刷新 (Refresh) 查看最新的状态。

**步骤 5** 选择要启用的功能，并点击启用 (Enable)。

**步骤 6** 单击刷新 (Refresh) 查看最新的状态。

---

## 部署思科 pxGrid 节点

在独立节点和分布式部署节点上都可以启用思科 pxGrid 角色。

### 开始之前

- 所有节点都将 CA 证书用于思科 pxGrid 服务用途。如果在升级之前对思科 pxGrid 服务使用默认证书，则升级时会将该证书替换为内部 CA 证书。
- 如果您使用的是分布式部署或从思科 ISE 1.2 升级，则需要为证书启用 pxGrid 用途选项。您可以在系统证书 (System Certificates) 窗口中启用 pxGrid 用途选项。此窗口的导航路径为管理 (Administration) > 证书 (Certificates) > 系统证书 (System Certificates)。选择用于部署的证书，然后点击编辑 (Edit) 选中 pxGrid: 使用 pxGrid 控制器证书 (pxGrid: use certificate for the pxGrid Controller) 复选框。



- 必须为 Websocket (pxGrid 2.0) 打开端口 8910，并为 XMPP (pxGrid V1.0) 打开端口 5222。如果在节点上禁用思科 pxGrid 服务，则端口 5222 将关闭，但是端口 8910 仍正常工作，并继续响应请求。

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

**步骤 2** 在部署节点 (Deployment Nodes) 窗口中，选中要为其启用思科 pxGrid 服务的节点旁的复选框，然后点击编辑 (Edit)。

**步骤 3** 点击常规设置 (General Settings) 选项卡，选中 pxGrid 复选框。

**步骤 4** 点击 Save。

**注释** 当从以前的版本升级时，系统可能会禁用保存 (Save) 选项。当浏览器缓存引用以前版本的思科 ISE 中的旧文件时，就会发生这种情况。清除浏览器缓存以启用保存 (Save) 选项。

## 思科 pxGrid 实时日志

“实时日志” (Live Logs) 窗口会显示所有 pxGrid 管理事件。事件信息包括客户端和功能名称，以及事件类型和时间戳。

此窗口的导航路径为管理 (Administration) > pxGrid 服务 (pxGrid Services) > 实时日志 (Live Log)。您还可以清除日志并重新同步或刷新列表。

## ISE pxGrid 身份映射

使用身份映射，您可以监控通过域控制器 (DC) 而不是通过思科 ISE 进行身份验证的用户。在思科 ISE 不主动对用户进行网络访问身份验证的网络中，可以使用身份映射从 Active Directory (AD) 域控制器收集用户身份验证信息。此身份映射选项使用 MS WMI 接口连接至 Windows 系统并且从 Windows 事件消息查询日志。用户登录网络并通过 Active Directory 的身份验证之后，域控制器将生成一份事件日志，此日志中包含用户名和为此用户分配的 IP 地址。

即使思科 ISE 主动执行身份验证，也仍可以启用身份映射。在这种情况下，同一会话可能会被验证两次。运行数据有一个指示来源的会话属性。您可以转至 Operations > Authentications，然后点击 Show Live Sessions 以检查会话来源。

身份映射组件从域控制器检索用户登录情况并将其导入至思科 ISE 会话目录。因此，通过 Active Directory (AD) 身份验证的用户会显示在思科 ISE 实时会话视图中，而且可以使用思科 pxGrid 接口由第三方应用从会话目录进行查询。已知信息为用户名、IP 地址、ADDC 主机名以及 ADDC NetBios 名称。

思科 ISE 仅扮演被动角色并且不执行身份验证。当身份映射处于活动状态时，思科 ISE 从 AD 收集登录信息并将数据纳入会话目录中。

### 主要特性

- 身份映射从思科 ISE 管理控制台进行配置。此配置包括以下设置：
  - 定义身份映射从中收集用户身份验证信息的所有 DC。这包括使用 \*.csv 文件导入和导出 DC 列表。
  - DC 连接属性，例如身份验证安全协议（NTLMv1 或 NTLMv2）以及用户会话老化时间
  - 连接测试，用于验证 DC 是否设置正确以启动与身份映射的有效连接
- 身份映射报告。此报告提供关于身份映射组件的信息以进行故障排除。
- 身份映射调试日志
- 思科 ISE 会话目录保留所收集的用户信息，从而使客户可以从实时会话查看这些信息并且可以从 pxGrid 接口进行查询
- 使用 CLI 命令 **show application status** 可以提供使用身份映射的节点的运行状态
- 支持高可用性

### 配置身份映射

ID 映射需要 ISE 中的配置，且 Active Directory 域服务器必须具有正确的补丁和配置。有关为 ISE 配置 Active Directory 域控制器的信息，请参阅 [用于支持身份映射的 Active Directory 要求](#)

## 配置身份映射

ISE 必须能与 AD 域控制器 (DC) 建立连接。

### 开始之前

启用 pxGrid 服务以配置身份映射。选择 **管理 (Administration) > 系统 (System) > 部署 (Deployment)** 以启用 pxGrid 服务。

要为身份映射添加一个新域控制器 (DC)，您需要该 DC 的登录凭证。

确保为 ISE 身份映射正确配置域控制器。

---

**步骤 1** 选择 **管理 (Administration) > pxGrid 身份映射 (pxGrid Identity Mapping) > AD 域控制器 (AD Domain Controller)**。

**步骤 2** 点击 **General Settings**。

**步骤 3** 系统将显示 Directory General Settings 弹出窗口。设置所需的值，然后点击 **Save**。

- **历史间隔 (History interval)** 是身份映射读取已发生的用户登录信息的时间。在启动或重新启动身份映射以跟进生成的事件时（事件生成于身份映射不可用期间），需要使用此项。
- **用户会话老化时间 (User session aging time)** 是用户可登录的时间量。身份映射会识别 DC 中的新用户登录事件，但是 DC 不会报告用户的注销时间。通过老化时间，思科 ISE 可以确定用户登录的时间间隔。

- 您可以选择 **NTLMv1** 或 **NTLMv2** 作为 ISE 与 DC 之间的通信协议。

**步骤 4** 点击添加 (**Add**)。

**步骤 5** 在 **General Settings** 部分，输入 DC 的 **Display Name**、**Domain FQDN** 和 **Host FQDN**。

**步骤 6** 在 **Credentials** 部分，输入 DC 的 Username 和 Password。

**步骤 7** (可选) 通过点击验证 **DC 连接设置 (Verify DC Connection Settings)** 来测试到指定域的连接。

此测试可确保到 DC 的连接是正常的。但是它不会检查思科 ISE 是否可以在登录后获取用户信息。

**步骤 8** 点击提交 (**Submit**)。系统会显示更新的表 (新定义的 DC 已经包含在 DC 列表中)。状态列指示 DC 的不同状态。

您也可以导入或导出 DC 列表。

**注释** 当导入时，您需要在模板中提供密码。因为文件包含密码，导入模板应被视为敏感信息。Export 选项不会导出密码。

---

## 过滤器身份映射

您可以根据用户名称或 IP 地址过滤某些用户。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。监控实时会话显示映射过滤器未过滤掉的身份映射组件。

**步骤 1** 依次选择管理 (**Administration**) > **pxGrid 身份映射 (pxGrid Identity Mapping)** > **映射过滤器 (Mapping Filters)**。

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

**步骤 3** 要查看当前登录到监控会话目录中的未过滤用户，请选择操作 (**Operations**) > **身份验证 (Authentications)**。

---

## Inline Posture 节点

Inline Posture 节点是守门节点，放在网络访问设备后面，例如网络上的无线 LAN 控制器 (WLC) 和 VPN 集线器。Inline Posture 节点在用户通过身份验证并被授予访问权限后实施访问策略，并且处理 WLC 或 VPN 无法满足的授权更改 (CoA) 请求。思科 ISE 允许您有两个 Inline Posture 节点，承担主要或辅助角色，提供高可用性。

Inline Posture 节点必须为专用节点。它必须仅用于内联状态服务，不能与其他思科 ISE 服务同时运行。同样，由于其服务的专业化性质，Inline Posture 节点无法承担任何角色。例如，它不能用作管理节点提供管理服务，不能用作策略服务节点提供网络访问、安全评估、配置文件和访客服务，也不能用作监控节点为思科 ISE 网络提供监控和故障排除服务。

思科 ISE 3495 平台不支持 Inline Posture 角色。确保在以下任何受支持的平台上安装 Inline Posture 角色：思科 ISE 3315、思科 ISE 3355、思科 ISE 3395 或思科 ISE 3415。

您不能访问 Inline Posture 节点的基于 Web 的用户界面，只能从 PAN 配置这些节点。

## Inline Posture 节点的安装

您必须从 Cisco.com 下载 Inline Posture ISO (IPN ISO) 映像，然后将其安装到任何支持的平台上。然后，您必须通过命令行界面 (CLI) 配置证书。接下来，您可以从管理员门户注册此节点。



**注释** 不提供版本的 Inline Posture ISO 映像。使用 1.2 IPN ISO 映像安装并设置 Inline Posture 节点。

安装和设置 Inline Posture 应用后，您必须先配置证书，然后才能注册 Inline Posture 节点。有关详细信息，请参阅《[思科身份服务引擎硬件安装指南](#)》。

## 注册 Inline Posture 节点

我们建议您在注册时确定节点的类型（思科 ISE 或 Inline Posture）。如果希望稍后更改节点类型，您必须将该节点从部署中注销，重启独立节点上的思科 ISE 并重新注册该节点。

### 开始之前

- 确保主节点的证书信任列表 (CTL) 具有适当的证书颁发机关 (CA) 证书，以验证要注册的辅助节点的 HTTPS 证书。
- 向主要节点注册辅助节点之后，如果您更改辅助节点上的 HTTPS 证书，您必须将相应的 CA 证书导入主要节点的 CTL。

**步骤 1** 登录到 PAN。

**步骤 2** 依次选择管理 (Administration) > 系统 (System) > 部署 (Deployment)。

**步骤 3** 点击左侧导航窗格中的 Deployment。

**步骤 4** 选择注册 (Register) > 注册 Inline Posture 节点 (Register an Inline Posture Node) 以注册 Inline Posture 节点。

## 查看部署中的节点

在部署节点 (Deployment Nodes) 窗口，可以查看部署中的所有思科 ISE 节点（主节点和辅助节点）。

**步骤 1** 登录主思科 ISE 管理员门户。

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

**步骤 3** 点击左侧导航窗格中的部署 (Deployment)。

列出部署中的所有思科 ISE 节点。

## 数据库崩溃或文件损坏问题

如果 Oracle 数据库文件因断电或其他原因导致数据丢失而损坏，则思科 ISE 可能会崩溃。根据具体的事件，按照以下说明恢复丢失的数据。

- 如果部署中发生 PAN 损坏，则应将辅助 PAN 升级为主 PAN。
- 如果由于小型部署或任何其他原因导致无法升级辅助 PAN，请恢复最新的可用备份，如《Cisco 身份识别服务引擎 CLI 参考指南》中所述。
- 如果 PSN 损坏，请按照《Cisco 身份识别服务引擎 CLI 参考指南》中的说明，执行以下步骤取消注册、重置配置和注册。
- 如果是独立设备，请按照《Cisco 身份识别服务引擎 CLI 参考指南》中的说明恢复最新的可用备份。



---

注释 定期从独立设备中获取备份，以避免丢失最新的配置更改。

---

## 设备的监控配置

MnT 节点会接收网络中设备的数据，并用于填充控制板显示内容。要启用 MnT 节点与网络设备之间的通信，必须正确配置交换机和 NAD。

## 同步主要和辅助思科 ISE 节点

只能通过主 PAN 对思科 ISE 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) > 系统 (System) > 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。

---

## 更改节点角色和服务



**注释** 当启用或禁用在 PSN 上运行的任何服务或对 PSN 进行任何更改时，将会重新启动运行这些服务的应用服务器进程。这些服务重新启动时，预计会有延迟。由于服务重新启动时的这一延迟，可能会启动自动故障转移（如果在部署中已启用）。要避免此问题，请确保关闭自动故障转移配置。

您可以编辑思科 ISE 节点配置来更改在节点上运行的角色和服务。

**步骤 1** 登录到主 PAN。

**步骤 2** 依次选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

**步骤 3** 选中要更改其角色或服务的节点旁边的复选框，然后点击 **Edit**。

**步骤 4** 选择您要修改的角色和服务。

**步骤 5** 点击**保存**。

**步骤 6** 验证在主 PAN 上是否收到警报，以确认角色或服务更改。如果未成功保存角色或服务更改，则不会生成警报。

## 在思科 ISE 中修改节点的影响

在思科 ISE 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）
- 升级管理节点（辅助节点升级为主节点）
- 更改角色（当向某个节点分配策略服务或监控角色或从该节点删除角色时）
- 修改策略服务节点中的服务（启用或禁用会话和分析器服务）
- 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。

## 创建策略服务节点组

当两个或多个策略服务节点 (PSNs) 连接到同一高速局域网 (LAN) 时, 建议您将他们放入同一个节点组中。通过保留较少的本地组重要属性以及减少复制到网络中远程节点的信息, 此设计对终端分析数据复制进行了优化。节点组成员还检查对等组成员的可用性。如果该组检测到某成员发生故障, 则尝试重置和恢复失败节点上所有 URL 重定向的会话。

节点组用于对实施 URL 重定向 (终端安全评估服务、访客服务和 MDM) 的会话执行 PSN 故障转移。



**注释** 建议将所有 PSN 放在同一个本地网络中, 并作为同一个节点组的一部分。要加入同一个节点组, PSN 不需要成为负载均衡集群的一部分。但是, 负载均衡集群中的每个本地 PSN 通常应该属于同一个节点组。

节点组成员可以通过 TCP/7800 通信。

在将 PSN 作为成员添加进某个节点组之前, 您必须创建该节点组。您可以从管理员门户的**部署 (Deployment)** 窗口创建、编辑和删除 PSN 组。

**步骤 1** 依次选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

**步骤 2** 单击左侧导航窗格顶部的**设置 (Settings)** 图标。

**步骤 3** 单击**创建组 (Create Group)**。

**步骤 4** 输入节点组的唯一名称。

**注释** 建议不要配置名称为**无 (None)**的节点组, 否则可能会在节点注册时引起问题。

**步骤 5** (可选) 输入节点组的说明。

**步骤 6** (可选) 选中启用**MAR 缓存分布 (Enable MAR Cache Distribution)**复选框并填写其他选项。在选中此复选框之前, 请确保在**Active Directory**窗口中启用 MAR。

**步骤 7** 单击**Submit**保存节点组。

保存节点组之后, 节点组应显示在左侧的导航窗格中。如果节点组未显示在左侧窗格中, 则可能已隐藏。单击导航窗格中的**展开 (Expand)**按钮可查看隐藏的对象。

从**策略服务 (Policy Service)**区域的在节点组中包含节点 (**Include node in node group**) 下拉列表中选择对应的节点组, 以便将节点添加到节点组或者对节点进行编辑。

## 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 节点。

它保留其从主 PAN 接收的最新配置，并且承担独立节点的默认角色，包括“管理” (Administration)、“策略服务” (Policy Service) 或“监控” (Monitoring)。如果取消注册 MnT 节点，则此节点将不再是系统日志目标。

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

在从部署中删除某个辅助节点之前，请对思科 ISE 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) > 系统 (System) > 部署 (Deployment)。

**步骤 2** 选择要删除的辅助节点旁边的复选框，然后点击取消注册 (Deregister)。

**步骤 3** 点击确定 (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，则意味着不会生成警报。

---

## 关闭思科 ISE 节点

从思科 ISE CLI 发出 **halt** 命令之前，我们建议您停止思科 ISE 应用服务，并确保它不执行备份、恢复、安装、升级或删除操作。如果在思科 ISE 执行上述任一操作时发出 **halt** 命令，您将会收到以下其中一条警告消息：

```
WARNING: A backup or restore is currently in progress! Continue with halt?
```

```
WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```

在使用 **halt** 命令时，如果系统没有运行任何进程，或如果您输入是 (Yes) 来回应显示的警告消息，则必须回答以下问题：

```
Do you want to save the current configuration?
```

如果输入 **yes** 保存现有思科 ISE 配置，系统将显示以下消息：

```
Saved the running configuration to startup successfully.
```



---

**注释** 我们建议您在重新引导设备之前停止应用进程。

---

也可以重新引导思科 ISE。有关详细信息，请参阅[思科身份服务引擎 CLI 参考指南](#)。

## 更改独立思科 ISE 节点的主机名或 IP 地址

可以更改独立思科 ISE 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 节点是分布式部署的一部分，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 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 应用配置以重新启动所有服务。

**步骤 3** 如果思科 ISE 节点为分布式部署的一部分，则将其注册到主 PAN。

**注释** 如果您在注册思科 ISE 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 服务器上分布式部署一部分的思科 ISE 节点的 IP 地址和 FQDN。

将思科 ISE 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 节点。

---





## 第 5 章

# 基本设置

- 管理门户，第 67 页
- 思科 ISE 国际化和本地化，第 78 页
- MAC 地址标准化，第 85 页
- 思科 ISE 部署升级，第 86 页
- 思科 ISE 中的证书管理，第 86 页
- 思科 ISE CA 服务，第 123 页
- OCSP 服务，第 138 页
- 配置管理员访问策略，第 144 页
- 管理员访问设置，第 145 页

## 管理门户

管理门户提供思科 ISE 配置和报告的访问权限。下图显示管理门户菜单栏的主要元素。

图 2: 思科 ISE 管理门户

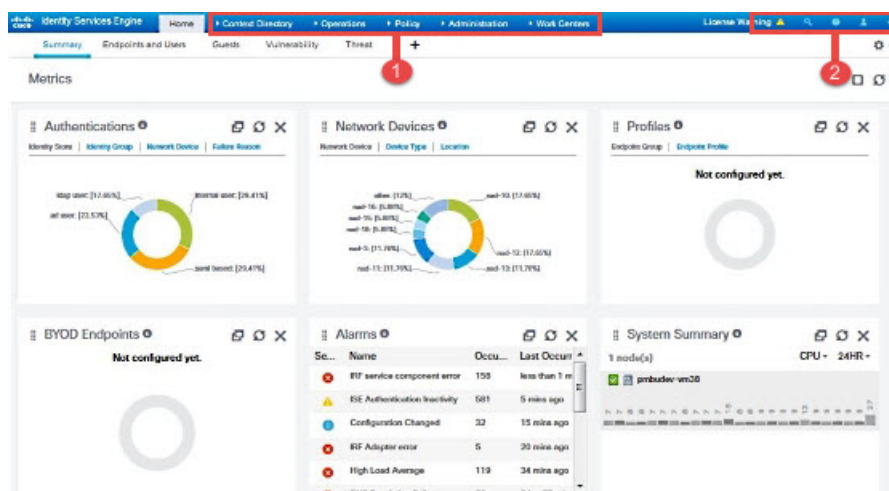







表 14: 思科 ISE 管理门户的组件

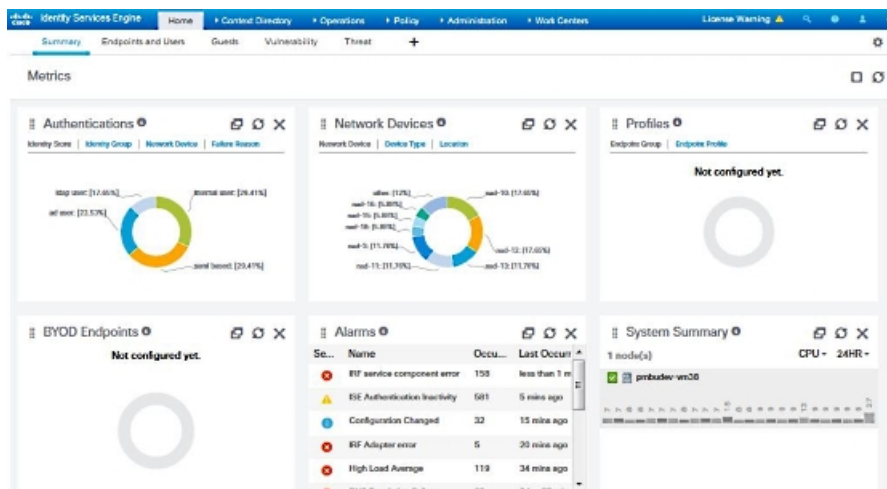
1	菜单下拉列表	<p>左侧窗格中的菜单选项包括：</p> <ul style="list-style-type: none"> <li>• <b>情景可视性 (Context Visibility):</b> 情景可视性窗口显示有关终端、用户和网络访问设备 (NAD) 的信息。情景可视性信息按功能、应用、自带设备 (BYOD) 和其他类别进行分组，具体取决于您注册的许可证。情景可视性窗口使用中央数据库并从数据库表、缓存和缓冲区收集信息。因此，情景可视性 Dashlet 和列表中的内容会快速更新。情景可视性窗口由上方的 Dashlet 和底部的信息列表组成。通过修改列表中的列属性来过滤数据时，Dashlet 会刷新以显示修改的内容。</li> <li>• <b>操作:</b> 操作窗口包括用于查看 RADIUS、TACACS+ 和 TC-NAC 实时日志的工具、自适应网络控制 (ANC) 策略以及用于诊断和调试与思科 ISE 部署相关的问题的故障排除选项。</li> <li>• <b>策略 (Policy):</b> “策略” (Policy) 窗口包含用于管理身份验证、授权、分析、安全评估和客户端调配区域中的网络安全的工具。</li> <li>• <b>管理 (Administration):</b> “管理” (Administration) 窗口包含用于管理思科 ISE 节点、许可证、证书、网络设备、用户、终端和访客服务的工具。</li> <li>• <b>工作中心:</b> 工作中心列出了以下可扩展的子菜单。这些子菜单是思科 ISE 管理员配置思科 ISE 部署中相关功能的单一起点。 <ul style="list-style-type: none"> <li>• 网络接入</li> <li>• <b>Guest Access</b></li> <li>• <b>TrustSec</b></li> <li>• 自带设备</li> <li>• <b>Profiler</b></li> <li>• 终端安全评估</li> <li>• 设备管理</li> <li>• <b>PassiveID</b></li> </ul> </li> </ul>
---	--------	--

2	右上角菜单图标	<ul style="list-style-type: none"> <li>•  <p>显示通知的数量。将鼠标悬停在数字上，以显示列表。在示例中，许可证错误掩盖了通知。</p> </li> <li>•  <p>使用此图标搜索终端并按配置文件、故障、身份库、位置、设备类型等显示其分布。</p> </li> <li>•  <p>点击此图标可查看一个下拉列表，您可以通过该下拉列表访问当前显示页面的在线帮助，以及指向思科 ISE 社区、门户生成器等位置的链接。</p> </li> <li>•  <p>用户配置文件图片。对于该 ISE 服务器：</p> <ul style="list-style-type: none"> <li>• 运行“设置助理：访问” (Setup Assistant: Access) 向导可创建基本配置，以演示网络中的思科 ISE 特性功能。</li> <li>• 查看网络设备配置</li> <li>• 服务器信息</li> </ul> </li> <li>•  <p>点击此图标可查看系统活动的菜单，包括启动在线帮助和配置帐户设置。</p> </li> </ul>
---	---------	--

## 思科 ISE 主页控制板

思科 ISE 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统计数据。控制板元素通常显示 24 小时内的活动。下图是思科 ISE 控制板上提供的一些信息示例。仅可以在主策略管理节点 (PAN) 门户上查看思科 ISE 控制板数据。

图 3: 思科 ISE 主页控制面板



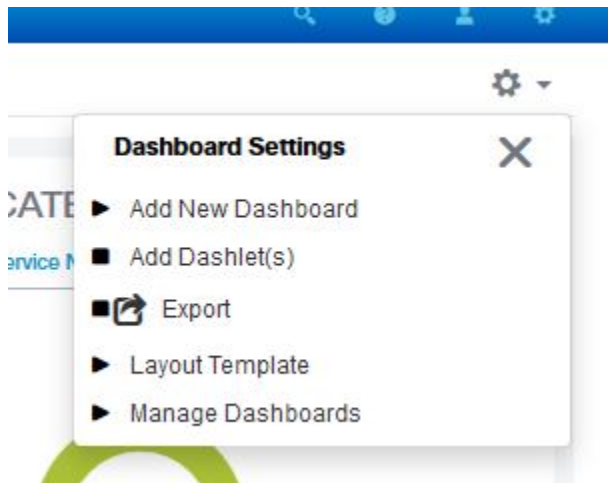
主页有五个显示思科 ISE 数据的默认控制面板。其中每个控制面板都有多个预定义的 Dashlet。

- **摘要 (Summary):** 此控制面板包含线性指标 Dashlet、饼形图 Dashlet 和列表 Dashlet。指标 Dashlet 不可配置。默认情况下，此控制面板包含状态 (Status)、终端 (Endpoints)、终端类别 (Endpoint Categories) 和网络设备 (Network Devices) 面板。
- **终端 (Endpoints):** 默认情况下，此控制面板包含状态 (Status)、终端 (Endpoints)、终端类别 (Endpoint Categories) 和网络设备 (Network Devices) Dashlet。
- **访客 (Guests):** 此控制面板包含提供有关访客用户类型、登录失败和活动位置的信息的 Dashlet。
- **漏洞 (Vulnerability):** 此控制面板显示漏洞服务器向思科 ISE 报告的信息。
- **威胁 (Threat):** 此控制面板显示从威胁服务器报告发送给思科 ISE 的信息。

## 配置主页控制面板

您可以点击页面右上角的齿轮图标来自定义主页控制面板：

图 4: 自定义控制板



下拉列表中显示以下选项：

- **添加新控制板 (Add New Dashboard)** 可以让您添加新的控制板。在显示的字段中输入值，然后点击**应用 (Apply)**。
- 添加 **Dashlet (Add Dashlet(s))** 会显示一个对话框，其中包含可用的 Dashlet 列表。点击 Dashlet 名称旁边的**添加 (Add)** 或**删除 (Remove)**，可从控制板添加或删除 Dashlet。
- **导出 (Export)** 会将选定的主页视图保存为 PDF。
- **布局模板 (Layout Template)** 会配置此视图中显示的列数。
- **管理控制板 (Manage Dashboards)** 包含两个选项：
  - **标记为默认控制板 (Mark As Default Dashboard)**：选择此选项可将当前控制板设为您选择主页时的默认视图。
  - **重置所有控制板 (Reset All Dashboards)**：使用此选项可以重置所有控制板，并删除所有主页控制板上的配置。

## 情景可视性视图

情景可视性 (**Context Visibility**) 窗口的结构类似于主页，不同之处在于“情景可视性” (Context Visibility) 窗口：

- 当您过滤显示数据时，保留当前环境（浏览器窗口）
- 可定制程度更高
- 侧重终端数据

您可以仅从主 PAN 上查看情景可视性数据。

情景可视性 (**Context Visibility**) 窗口中的 Dashlet 显示有关终端和终端到 NAD 的连接信息。当前显示的信息取决于每个窗口上的 Dashlet 下数据列表中的内容。每个窗口会根据选项卡名称显示终端数据。过滤数据时，列表和 Dashlet 都将更新。您可以点击圆形图的一个或多个部分，也可以过滤表中的行，或者任意组合这些操作来过滤数据。在您选择过滤器时，效果是可以叠加的，也称为级联过滤器，可让您深入查找想要的特定数据。您也可以点击列表中的终端，获得该终端的详细视图。

情景可视性 (**Context Visibility**) 下有三个主视图：

- **终端 (Endpoints)**: 根据设备类型、合规状态、身份验证类型、等过滤要查看的终端。



**注释** 我们建议在网络访问设备 (NAD) 上启用记账设置，以确保将记账开始和更新信息发送到思科 ISE。

仅当启用记账后，思科 ISE 才能收集记账信息，如最新的 IP 地址、会话状态（已连接、已断开或已拒绝）、终端的非活动天数。这些信息显示在实时日志 (**Live Logs**)、实时会话 (**Live Session**) 和情景可视性 (**Context Visibility**) 窗口中。在 NAD 上禁用记账时，实时日志 (**Live Logs**)、实时会话 (**Live Session**) 和情景可视性 (**Context Visibility**) 窗口之间的记账信息可能缺失、不正确或不匹配。



**注释** 通过思科 ISE 管理门户主页上提供的可视性设置 (**Visibility Setup**) 工作流程，您可以为终端发现添加 IP 地址范围列表。配置此工作流程后，思科 ISE 会对终端进行身份验证，但未包含在配置的 IP 地址范围内的终端不会显示在情景可视性 (**Context Visibility**) > 终端 (**Endpoints**) 窗口和终端 (**Endpoints**) 列表页面（工作中心 (**Work Centers**) > 网络访问 (**Network Access**) > 身份 (**Identities**) > 终端 (**Endpoints**)）。

- **网络设备 (Network Devices)**: 此窗口会显示已连接终端的 NAD 列表。对于任何 NAD，请单击相应的终端数量 (**# of endpoints**) 列中显示的终端数量。系统将显示一个窗口，其中会列出该 NAD 过滤的所有设备。



**注释** 如果已使用 SNMPv3 参数配置网络设备，则无法生成思科 ISE 监控服务提供的网络设备会话状态摘要 (**Network Device Session Status Summary**) 报告（操作 (**Operations**) > 报告 (**Reports**) > 目录 (**Catalog**) > 网络设备 (**Network Device**) > 会话状态摘要 (**Session Status Summary**)）。如果网络设备使用 SNMPv1 或 SNMPv2c 参数配置，则可以成功生成此报告。

您可以在情景可视性 (**Context Visibility**) 窗口中创建新的选项卡，然后创建自定义列表来进行其他过滤。自定义视图不支持 Dashlet。



单击 Dashlet 中圆形图的一部分，以查看包含该 Dashlet 的已过滤数据的新窗口。在该新窗口中，您可以继续过滤显示的数据，如在视图中过滤显示的数据，第 74 页中所述。

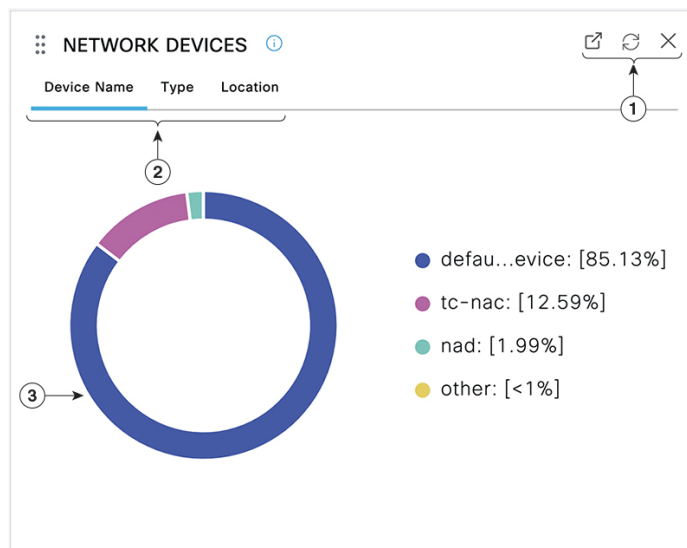
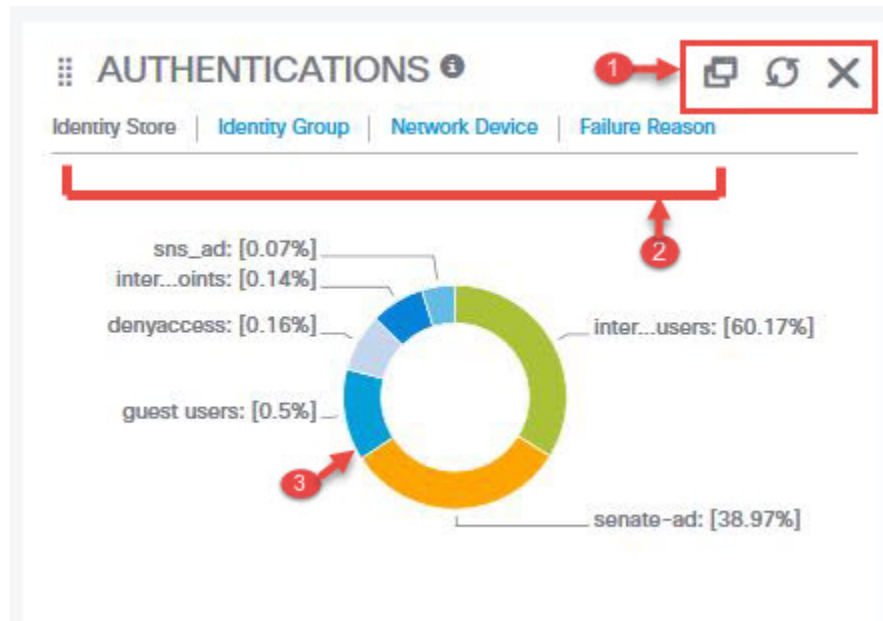
有关使用情景可视性窗口来查找终端数据的详细信息，请参阅以下使用 ISE 2.1 <https://www.youtube.com/watch?v=HvonGhrydfg> 的思科 YouTube 视频。

相关主题

[硬件控制板](#)

## Dashlet

下图是 Dashlet 的示例：



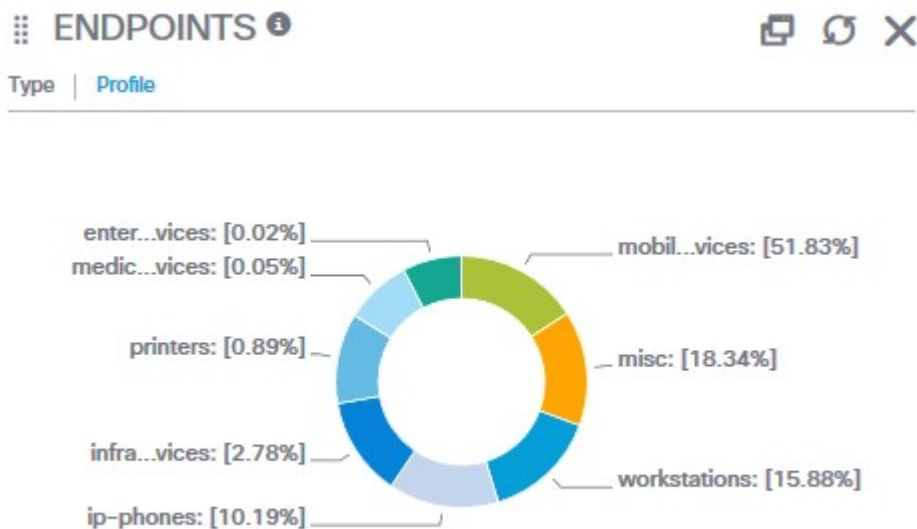
1. 堆叠窗口符号“分离”，打开新窗口图标表示可在新的浏览器窗口中打开此 Dashlet。饼图将会刷新。单击 **X** 以删除此 Dashlet。此选项仅在主页上可用。使用屏幕右上角的齿轮符号可删除“情景可视性” (Context Visibility) 窗口中的 Dashlet。
2. 某些 Dashlet 具有不同类别的数据。点击类别以查看该数据集的饼形图。
3. 饼形图显示您已选择的数据。单击其中一个饼形区域将在新选项卡中打开，其中包含基于该饼形区域过滤得到的数据。

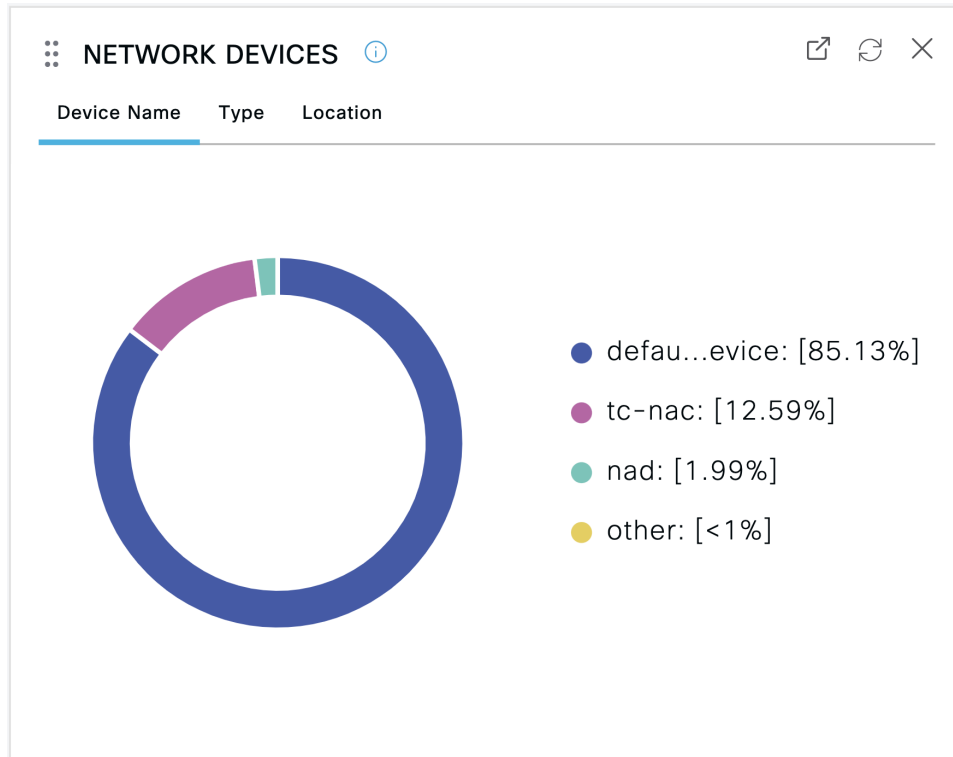
单击主页控制面板中的饼图部分，在新的浏览器窗口中打开该图表。新窗口将显示按单击的饼图部分过滤的数据。

当您在“情景可视性” (Context Visibility) 窗口中单击饼图的一部分时，显示的数据会被过滤，但情景不会发生变化。您在同一浏览器窗口中查看过滤的数据。

## 在视图中过滤显示的数据

当您在“情景可视性” (Context Visibility) 窗口中单击 dashlet 时，相应的数据将按您单击和显示的项目进行过滤。例如，当您单击饼图的某个部分时，系统会过滤并显示所选部分的数据。





如果在终端 (Endpoints) Dashlet 中单击 **mobile devices**，则窗口将刷新显示并包含两个终端 (Endpoints) Dashlets、一个网络设备 Dashlet 和一个数据列表。这些 Dashlet 和列表显示移动设备的数据，如以下示例所示系统会显示包含数据的新窗口，如下图所示：

Filters:

**ENDPOINTS**

Type | Profile

mobile\_vision [100%]

**ENDPOINTS**

OS | OS Types | Identity Group

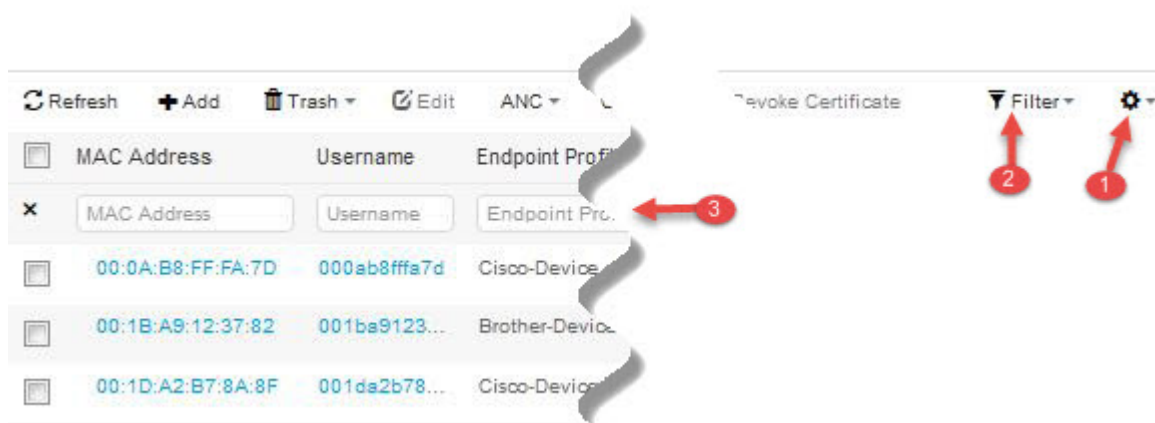
**NETWORK DEVICE**

Location | Type | Device Na

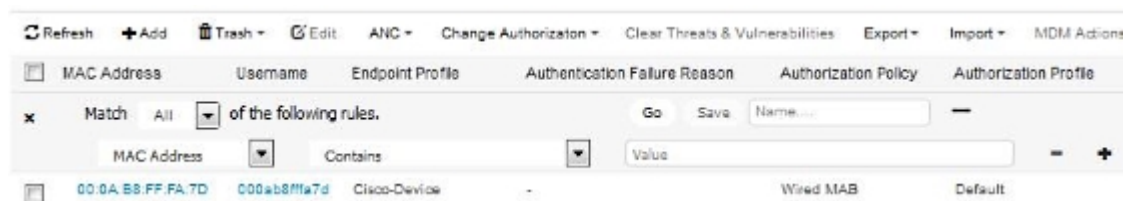
local\_vision [100%]

MAC Address	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description
<input type="text" value="MAC Address"/>	<input type="text" value="IPv4 Address"/>	<input type="text" value="Username"/>	<input type="text" value="Hostname"/>	<input type="text" value="Location"/>	<input type="text" value="Endpoint Profile"/>	<input type="text" value="Description"/>
<input type="checkbox"/> 00:02:F3:C9:C1:78	192.168.144.184	0002f3c9c178		Location#All Locations	Android	
<input type="checkbox"/> 00:03:AA:C5:36:B7	192.168.105.219	0003aac536b7		Location#All Locations	Android	

您可以通过点击饼图的更多部分或者通过数据列表上的控件来继续过滤数据。



1. 齿轮图标过滤显示的列。从下拉列表中，选择要在此控制面板列表中查看的列。
2. 默认会显示快速过滤器。在框中（标签号3）输入字符可根据结果来过滤列表。自定义过滤器提供更精细的过滤器，如下图所示：



保存您的自定义过滤器。

## 创建自定义过滤器

创建并保存只有您才能访问的用户特定的自定义过滤器。其他登录思科 ISE 的用户无法查看您创建的自定义过滤器。这些自定义过滤器不会保存在思科 ISE 数据库中。您可以从登录思科 ISE 的任何计算机或浏览器访问它们。

- 步骤 1 单击**显示 (Show)**，然后从下拉列表中选择**高级过滤器 (Advanced Filter)**。
- 步骤 2 从 **Filter** 菜单中指定搜索属性，如字段、运算符和值。
- 步骤 3 单击 **+** 可添加更多条件。
- 步骤 4 单击 **Go** 可显示与指定属性匹配的条目。
- 步骤 5 单击**保存 (Save)** 以保存过滤器。
- 步骤 6 输入名称，然后单击 **Save**。过滤器现在会出现在**过滤器 (Filter)** 下拉列表中。

## 使用高级过滤器按条件过滤数据

您可以使用高级过滤器根据指定的条件（例如 First Name = Mike and User Group = Employee）过滤信息。您可以指定不止一个条件。

**步骤 1** 单击显示 (Show)，然后选择高级过滤器 (Advanced Filter) 下拉列表。

**步骤 2** 从过滤器菜单指定搜索属性（例如字段、运算符和值）。

**步骤 3** 单击 + 可添加更多条件。

**步骤 4** 单击开始 (Go) 可查看与指定属性匹配的条目。

## 使用快速过滤器按字段属性过滤数据

通过快速过滤器，您可以输入列表页面中显示的任何字段属性的值，引用页面，并且仅列出与筛选条件相匹配的记录。

**步骤 1** 单击显示 (Show)，然后从下拉列表中选择快速过滤器 (Quick Filter)。

**步骤 2** 在一个或多个属性字段中输入搜索条件，然后与指定属性相匹配的条目会自动显示。

## Dashlet 视图中的终端操作

列表顶部的工具栏允许您对所选列表中的终端执行操作。并非每个列表都启用了所有操作。某些操作要取决于所启用的功能。以下列表显示了必须在思科 ISE 中启用后才能使用的两项终端操作。

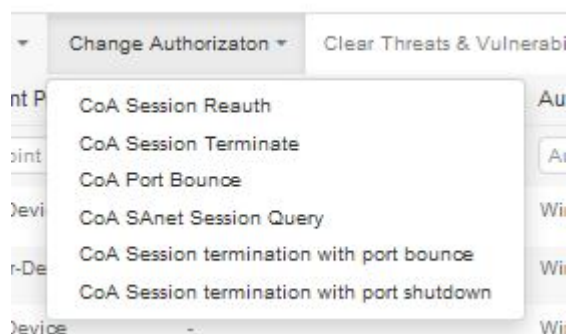
- 自适应网络控制操作

如果启用了自适应网络控制服务，您可以选择列表中的终端，并分配或撤销网络访问。您也可以发出授权更改。

在自适应网络服务 (Adaptive Network Service) 窗口中启用思科 ISE 中的自适应网络服务或终端保护服务。在思科 ISE GUI 中，单击菜单图标 (≡) 并选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 终端保护服务 (Endpoint Protection Service) > 自适应网络控制 (Adaptive Network Control)。有关详细信息，请参阅在思科 ISE 中启用，第 152 页。

当您单击主页 Dashlet 上的饼形图时，显示的新窗口将包含 ANC 和更改授权 (Change Authorization) 选项。选中要对其执行操作的终端的复选框，然后从 ANC 和更改授权 (Change Authorization) 的下拉列表中选择必要的操作。

图 5: Dashlet 视图中的终端操作



#### • MDM 操作

如果将 MDM 服务器连接到思科 ISE，则可以在所选终端上执行 MDM 操作。从 **MDM 操作 (MDM Actions)** 下拉列表中选择必要的操作。

## 思科 ISE 控制面板

思科 ISE 控制板或主页（主页 **(Home)** > **摘要 (Summary)**）是您登录思科 ISE 管理门户之后会看到的登录页面。此控制面板是一个集中管理控制台，由窗口顶部的仪表和下面的 Dashlet 组成。默认控制面板为 **摘要 (Summary)**、**终端 (Endpoints)**、**客户 (Guests)**、**漏洞 (Vulnerability)** 和 **威胁 (Threat)**。

控制板的实时数据概要显示访问您的网络的设备和用户的状态以及系统的运行状况。



**注释** 必须安装有 Adobe Flash Player，才可以正常查看 Dashlet 以及所有相应的向下钻取窗口。



**注释** 您不能重命名或删除默认控制面板。

- **分离 (Detach)**: 在单独的窗口中查看 Dashlet。
- **刷新 (Refresh)**: 刷新 Dashlet。
- **删除 (Remove)**: 从控制面板中删除 Dashlet。

## 思科 ISE 国际化和本地化

思科 ISE 国际化调整用户界面以适应受支持的语言。用户界面本地化采用区域特定组件和翻译文本。在 Windows、MAC OSX 和 Android 设备中，本地请求方调配向导可用于以下任何受支持的语言。

在思科 ISE 中，国际化和本地化支持专注于支持（面向最终用户的门户中的）采用 UTF-8 编码的非英语文本以及管理门户中的选择性字段。

## 支持的语言

思科 ISE 为以下语言和浏览器区域设置提供本地化和国际化支持。

表 15: 支持的语言和区域设置

语言	浏览器区域设置
中文（繁体）	zh-tw
中文（简体）	zh-cn
捷克语	cs-cz
荷兰语	nl-nl
英语	en
法语	fr-fr
德语	de-de
匈牙利语	hu-hu
意大利语	it-it
日语	ja-jp
韩语	ko-kr
波兰语	pl-pl
葡萄牙语（巴西）	pt-br
俄语	ru-ru
西班牙语	es-es

## 最终用户 Web 门户本地化

访客门户、发起人门户、我的设备门户和客户端调配门户会本地化为所有受支持的语言和区域设置。这包括文本、标签、消息、字段名称和按钮标签。如果客户端浏览器请求的区域设置未映射到思科 ISE 中的模板，则门户会使用英语模板显示内容。

通过使用管理门户，您可以针对每种语言修改用于访客门户、发起人门户和我的设备门户的字段。您还可以添加其他语言。当前，您无法自定义客户端调配门户的这些字段。

您可以通过将 HTML 页面上传到思科 ISE，进一步自定义访客门户。上传自定义页面时，您负责为部署提供相应的本地化支持。思科 ISE 通过可以用作指南的样本 HTML 页面提供本地化支持示例。思科 ISE 可以让您上传、存储和呈现自定义国际化 HTML 页面。



---

注释 NAC 和 MAC 代理安装程序及 WebAgent 页面未本地化。

---

## 支持 UTF-8 字符数据条目

向最终用户公开的思科 ISE 字段（通过思科客户端代理或请求方，或者发起人门户、访客门户、我的设备门户和客户端调配门户）支持所有语言的 UTF-8 字符集。UTF-8 是 Unicode 字符集的多字节字符编码，其中包括许多不同语言字符集，例如希伯来语、梵语和阿拉伯语。

字符集以 UTF-8 形式存储在管理配置数据库中，并且 UTF-8 字符集正确显示在报告 and 用户界面组件中。

### UTF-8 凭证身份验证

网络访问身份验证支持 UTF-8 用户名和密码凭证。这包括来自访客和管理门户登录身份验证的 RADIUS、扩展身份验证协议 (EAP)、RADIUS 代理、RADIUS 令牌和 Web 身份验证。对用户名和密码的 UTF-8 支持适用于对照本地身份库及外部身份库进行的身份验证。

UTF-8 身份验证取决于用于网络登录的客户端请求方。某些 Windows 本地请求方不支持 UTF-8 凭证。



---

注释 RSA 不支持 UTF-8 用户，因此，使用 RSA 的 UTF-8 身份验证不受支持。兼容思科 ISE 的 RSA 服务器也不支持 UTF-8。

---

### UTF-8 策略和安全评估

思科 ISE 中以属性值为条件的策略规则可以包含 UTF-8 文本。规则评估支持使用 UTF-8 属性值。此外，也可以通过管理门户使用 UTF-8 值配置条件。

终端安全评估要求根据 UTF-8 字符集修改为文件、应用和服务条件。这包括向 NAC 代理发送 UTF-8 要求。然后，NAC 代理相应地评估终端，并且在适当的情况下报告 UTF-8 值。

### 思科 NAC 和 MAC 代理 UTF-8 支持

思科 NAC 代理支持文本、消息以及与思科 ISE 互换的任何 UTF-8 数据的国际化。这包括在条件中使用的要求消息、要求名称，以及文件和流程名称。

以下限制适用：

- UTF-8 支持仅适用于基于 Windows 的 NAC 代理。
- 思科 NAC 和 MAC 代理界面目前不支持本地化。



- WebAgent 不支持基于 UTF-8 的规则和要求。
- 如果已配置可接受使用政策 (AUP)，则根据在配置中指定的浏览器区域设置和语言集，在客户端提供策略页面。您负责提供本地化 AUP 捆绑包或网站 URL。

## 对发送至请求方的消息的 UTF-8 支持

RSA 提示符和消息使用 RADIUS 属性 REPLY-MESSAGE 转发到请求方，或者在 EAP 数据中。如果文本包含 UTF-8 数据，请求方将根据客户端的本地操作系统语言支持显示文本。某些 Windows 本地请求方不支持 UTF-8 凭证。

思科 ISE 提示和消息可能与请求方运行所在的客户端操作系统的区域设置不同步。您必须调整最终用户请求方区域设置与思科 ISE 支持的语言，使它们保持一致。

## 报告和警报 UTF-8 支持

对于思科 ISE 中支持的语言，监控和故障排除报告和警报支持相关属性使用 UTF-8 值：支持以下活动：

- 查看实时身份验证。
- 查看详细的报告记录页面。
- 导出和保存报告。
- 查看思科 ISE 控制板。
- 查看警报信息。
- 查看 tcpdump 数据。

## 门户中的 UTF-8 字符支持

思科 ISE 字段中支持的字符集 (UTF-8) 比门户和最终用户消息中的本地化支持的字符集多得多。例如，尽管支持字符集本身，但是思科 ISE 不支持从右到左书写的语言（例如希伯来语或阿拉伯语）。

下表列出管理员和最终用户门户中支持 UTF-8 字符的字段，这些字符用于数据输入和查看，带有以下限制：

- 思科 ISE 不支持包含 UTF-8 字符的访客用户名和密码。
- 思科 ISE 不支持证书中的 UTF-8 字符。

表 16: 管理门户 UTF-8 字符字段

管理门户要素	UTF-8 字段
Network access user configuration	<ul style="list-style-type: none"> <li>• <b>Username</b></li> <li>• 名字</li> <li>• 姓氏</li> <li>• 邮件</li> </ul>
User list	<ul style="list-style-type: none"> <li>• 所有过滤器字段。</li> <li>• “用户列表” (User List) 窗口中显示的值。</li> <li>• 左侧导航快速视图上显示的值。</li> </ul>
User password policy	<p>密码可以包含大写和小写字母、数字和特殊字符的任意组合（包括：“!”、@、#、\$、^、&amp;、*、(和)）。密码字段接受任何字符，包括 UTF-8 字符，但不接受控制字符。</p> <p>某些语言不支持大写或小写字母。如果用户密码策略要求用户输入含大写或小写字母的密码，并且如果用户的语言不支持这些字符，则用户无法设置密码。要让用户密码字段支持 UTF-8 字符，请在用户密码策略页面中取消选中以下复选框（管理 (<b>Administration</b>) &gt; 身份管理 (<b>Identity Management</b>) &gt; 设置 (<b>Settings</b>) &gt; 用户身份验证设置 (<b>User Authentication Settings</b>) &gt; 密码策略 (<b>Password Policy</b>)）：</p> <ul style="list-style-type: none"> <li>• 小写字母字符</li> <li>• 大写字母字符</li> </ul> <p>您不能使用字典字词、其反序字符或用其他字符替换的字母。</p>
Administrator list	<ul style="list-style-type: none"> <li>• 所有过滤器字段。</li> <li>• 在管理员列表窗口中显示的值。</li> <li>• 左侧导航快速视图中显示的值。</li> </ul>
Admin login page	<ul style="list-style-type: none"> <li>• <b>Username</b></li> </ul>
RSA	<ul style="list-style-type: none"> <li>• 消息</li> <li>• 提示符</li> </ul>
RADIUS token	<ul style="list-style-type: none"> <li>• Authentication tab &gt; Prompt</li> </ul>

管理门户要素	UTF-8 字段
Posture Requirement	<ul style="list-style-type: none"> <li>• Name</li> <li>• Remediation action &gt; Message shown to Agent User</li> <li>• 要求列表显示</li> </ul>
Posture conditions	<p>策略 (Policy) &gt; 策略元素 (Policy Elements) &gt; 条件 (Conditions) &gt; 终端安全评估 (Posture) 窗口中的以下字段:</p> <ul style="list-style-type: none"> <li>• 文件条件 (File Condition) &gt; 添加 (Add) &gt; 文件路径 (File Path)。</li> <li>• 应用条件 (Application Condition) &gt; 添加 (Add) &gt; 进程名称 (Process Name)。</li> <li>• 服务条件 (Service Condition) &gt; 添加 (Add) &gt; 服务名称 (Service Name)。</li> <li>• 会显示条件列表。</li> </ul>
Guest and My Devices settings	<ul style="list-style-type: none"> <li>• “发起人” (Sponsor) &gt; “语言模板: ” (Language Template:) 所有支持的语言, 所有字段。</li> <li>• “访客” (Guest) &gt; “语言模板: ” (Language Template:) 所有支持的语言, 所有字段。</li> <li>• “我的设备” (My Devices) &gt; “语言模板: ” (Language Template:) 所有支持的语言, 所有字段。</li> </ul>
System settings	<ul style="list-style-type: none"> <li>• “SMTP 服务器” (SMTP Server) &gt; “默认电子邮件地址” (Default email address)</li> </ul>
Operations > Alarms > Rule	<ul style="list-style-type: none"> <li>• Criteria &gt; User</li> <li>• “通知” (Notification) &gt; “电子邮件通知用户列表” (email notification user list)</li> </ul>
Operations > Reports	<ul style="list-style-type: none"> <li>• Operations &gt; Live Authentications &gt; Filter fields</li> <li>• Operations &gt; Reports &gt; Catalog &gt; Report filter fields</li> </ul>
Operations > Troubleshoot	<ul style="list-style-type: none"> <li>• General Tools &gt; RADIUS Authentication Troubleshooting &gt; Username</li> </ul>
Policies	<ul style="list-style-type: none"> <li>• “身份验证” (Authentication) &gt; 策略条件中的防病毒表达式的值</li> <li>• “身份验证” (Authorization) 或 “终端安全评估” (Posture) 或 “客户端调配” (Client Provisioning) &gt; 其他条件 &gt; 策略条件中的防病毒表达式的值</li> </ul>

管理门户要素	UTF-8 字段
Attribute value in policy library conditions	<ul style="list-style-type: none"> <li>• “身份验证” (Authentication) &gt; 简单条件或复合条件 &gt; 防病毒表达式的值</li> <li>• Authentication &gt; simple condition list display</li> <li>• Authentication &gt; simple condition list &gt; left navigation quick view display</li> <li>• “身份验证” (Authorization) &gt; 简单条件或复合条件 &gt; 防病毒表达式的值</li> <li>• Authorization &gt; simple condition list &gt; left navigation quick view display</li> <li>• “终端安全评估” (Posture) &gt; 字典中的简单条件或字典中的复合条件 &gt; 防病毒表达式的值</li> <li>• “访客” (Guest) &gt; 简单条件或复合条件 &gt; 防病毒表达式的值</li> </ul>

## 思科 ISE 用户界面外的 UTF-8 支持

本节包含在思科 ISE 用户界面之外提供 UTF-8 支持的区域。

### 调试日志和 CLI 相关的 UTF-8 支持

某些调试日志中会显示属性值和安全评估条件详细信息。所有调试日志都接受 UTF-8 值。您可以下载包含原始 UTF-8 数据的调试日志，使用支持 UTF-8 的查看器便能够查看这些数据。

### 思科安全 ACS 迁移 UTF-8 支持

思科 ISE 允许迁移思科安全访问控制服务器 (ACS) UTF-8 配置对象和值。思科 ISE UTF-8 语言可能不支持某些 UTF-8 对象的迁移，它可能会使用管理门户或报告方法，使迁移过程中提供的某些 UTF-8 数据变得无法读取。将无法读取的 UTF-8 值（从思科安全 ACS 迁移）转换为 ASCII 文本。有关从思科安全 ACS 迁移到思科 ISE 的详细信息，请参阅适用于您的思科 ISE 版本的[思科安全 ACS 到思科 ISE 迁移工具](#)。

## 支持导入和导出 UTF-8 值

管理和发起人门户都支持纯文本与 CSV 文件，并且支持在导入用户账号详细信息时使用 UTF-8 值。所提供的导出文件为 CSV 文件。

## REST 上的 UTF-8 支持

外部具象状态传输 (REST) 通信可支持 UTF-8 值。这适用于思科 ISE 用户界面上支持 UTF-8 的可配置项，但管理员身份验证除外。REST 中的管理员身份验证要求使用 ASCII 文本凭证进行登录。

## 身份库授权数据的 UTF-8 支持

思科 ISE 允许 Microsoft Active Directory 和轻型目录访问协议 (LDAP) 在授权策略中使用 UTF-8 数据进行策略处理。

## MAC 地址标准化

思科 ISE 支持对以下列任意格式输入的 MAC 地址进行标准化：

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

在以下 ISE 窗口中提供完整或部分 MAC 地址：

- Policy > Authorization
- 策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 授权 (Authorization)
- Authentications > Filters (Endpoint and Identity columns)
- 全局搜索
- 操作 (Operations) > 报告 (Reports) > 报告过滤器 (Report Filters)
- 操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > 终端调试 (Endpoint Debug)

在以下 ISE 窗口中提供完整的 MAC 地址（六个八位字节，用 “:” 或 “-” 或 “.” 分隔）：

- 操作 (Operations) >
- 操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > RADIUS 身份验证故障排除 (RADIUS Authentication Troubleshooting)
- 操作 (Operations) > 故障排除 (Troubleshooting) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > 终端安全评估故障排除 (Posture Troubleshooting)
- Administration > Identities > Endpoints
- 管理 (Administration) > 系统 (System) > 部署 (Deployment)
- 管理 (Administration) > 日志记录 (Logging) > 集合过滤器 (Collection Filters)

REST API 也支持完整 MAC 地址的标准化。

八位组的有效范围为 0 到 9、a 到 f 或 A 到 F。

## 思科 ISE 部署升级

通过思科 ISE，可以从管理门户执行基于 GUI 的集中式升级。升级进度和节点状态显示在思科 ISE GUI 中。有关必须执行的升级前和升级后任务的信息，请参阅要升级到的思科 ISE 版本的《思科身份服务引擎升级指南》。

升级概述 (Overview) 窗口 (管理 (Administration) > 系统 (System) > 升级 (Upgrade) > 概述 (Overview)) 列出了部署中的所有节点、这些节点上启用的角色、当前正在使用的思科 ISE 版本以及每个节点的状态 (节点是处于活动状态还是非活动状态)。只有在节点处于活动 (Active) 状态时，才能开始升级。

## 思科 ISE 中的证书管理

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。自签证书由其证书创建者签名。证书可以自签或由外部 CA 进行数字签名。CA 签名的数字证书被视为行业标准而且比自签证书更安全。

证书用于在网络中提供安全访问。证书会标识连接终端的思科 ISE 节点并且保护该终端和思科 ISE 节点之间的通信。

思科 ISE 将证书用于：

- 思科 ISE 节点之间的通信。
- 思科 ISE 与外部服务器 (例如系统日志和源服务器) 之间的通信。
- 思科 ISE 与最终用户门户 (例如访客、发起人和 BYOD 门户) 之间的通信。

通过思科 ISE 管理门户管理您的部署中的所有节点证书。

## 在思科 ISE 中配置证书以启用安全访问

思科 ISE 依赖公共密钥基础设施 (PKI) 提供与终端和管理员之间的安全通信，以及多节点部署内思科 ISE 节点之间的安全通信。PKI 依赖 X.509 数字证书传输用于消息加密和解密的公钥，并验证代表用户和设备的其他证书的真实性。通过思科 ISE 管理门户，您可以管理两类 X.509 证书：

- 系统证书：这些证书是识别思科 ISE 节点到客户端应用的服务器证书。每个思科 ISE 节点都有自己的系统证书，每个证书及相应的私钥均存储在该节点上。



---

**注释** 思科 ISE 无法导入多个具有相同私钥的证书。如果在不更改私钥的情况下续订并导入证书，则现有证书将替换为导入的证书。

---

- **受信任证书**: 这些 CA 证书用于为从用户和设备接收的公共密钥建立信任。受信任证书库还包含由简单证书注册协议(SCEP)分发的证书, 可将移动设备注册到企业网络中。受信任的证书在主 PAN 上管理, 并且系统会自动将这些证书复制到思科 ISE 部署中的所有其他节点。

在分布式部署中, 您只能将证书导入到 PAN 的证书信任列表(CTL)中。证书会被复制到辅助节点。

为了确保思科 ISE 中的证书身份验证功能不会受到证书驱动的身份验证功能中细微差别的影响, 请为网络中部署的所有思科 ISE 节点使用小写主机名。

## 证书使用

在将证书导入到思科 ISE 中时, 请指定证书的用途。选择 **管理 (Administration) > 系统 (System) > 证书 (Certificates) > 系统证书 (System Certificates)**, 然后单击 **导入 (Import)**。

选择以下一个或多个用途:

- **管理 (Admin)**: 用于节点间通信, 以及对管理门户进行身份验证。
- **EAP 身份验证 (EAP Authentication)**: 用于基于 TLS 的 EAP 身份验证。
- **门户 (Portal)**: 用于与所有思科 ISE 最终用户门户进行通信。
- **SAML**: 用于验证是否从正确的身份提供程序收到了 SAML 响应。
- **pxGrid**: 用于与 pxGrid 控制器进行通信。

关联每个节点中的不同证书, 以便与管理门户(管理用途)、pxGrid 控制器(pxGrid 用途)进行通信, 以及进行基于 TLS 的 EAP 身份验证(EAP 身份验证用途)。但针对其中的每种用途, 您只能关联每个节点中的一个证书。

您必须始终为导入思科 ISE 的每个证书使用新的私钥。跨证书重复使用私钥时, 由于 Red Hat NSS 数据库限制, 可能会发生应用初始化错误。

将新证书导入 Red Hat NSS 数据库时, 具有相同私钥的任何现有证书都将被覆盖。如果管理员证书的私钥被覆盖, 则思科 ISE 应用初始化会受到影响。

由于部署中有多个 PSN 可以支持 Web 门户请求, 所以思科 ISE 需要使用唯一标识符来标识必须用于门户通信的证书。当您添加或导出指定用于门户用途的证书时, 请定义证书组标签并将其与您的部署中各个节点上的对应证书关联。将此证书组标签与对应的最终用户门户关联(访客、发起人和个人设备门户)。此证书组标签是一种唯一标识符, 帮助思科 ISE 标识与这每一个门户通信时必须使用的证书。您只能从每个节点为每个门户指定一个证书。



注释 对于以下密码，EAP-TLS 客户端证书应具有 KeyUsage=密钥协议和 ExtendedKeyUsage=客户端身份验证：

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

对于以下密码，EAP-TLS 客户端证书应具有 KeyUsage=密钥加密和 ExtendedKeyUsage=客户端身份验证：

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

要绕过此要求，请选择管理 (**Administration**) > 系统 (**System**) > 设置 (**Settings**) > 安全设置 (**Security Settings**)，然后选中接受证书而不验证用途 (**Accept Certificates without Validating Purpose**) 复选框。



## 思科 ISE 中的证书匹配

设置部署中的思科 ISE 节点后，节点将互相通信。系统将检查每个思科 ISE 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 服务器提供证书时，将根据思科 ISE 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。

对于思科，匹配操作将在节点之间（如果有两个）或思科与 pxGrid 之间执行。

思科 ISE 按以下方式检查匹配的主题名称：

1. 思科 ISE 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。



**注释** 导入到思科 ISE 的 X.509 证书必须为隐私增强邮件 (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）。

## X.509 证书的有效性

X.509 证书从特定日期开始有效。当系统证书到期时，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：

- 彩色到期状态图标会出现在系统证书 (**System Certificates**) 窗口中。导航路径为 **管理 (Administration) > 系统 (System) > 证书管理 (Certificate Management) > 系统证书 (System Certificates)**。
- 到期消息显示在思科 ISE 系统诊断报告中。导航路径为 **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 天和 30 天时生成到期警报。而在最后 30 天内，每天都会生成一次到期警报。

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。对于证书颁发机构签名的证书，必须留出足够的时间，从证书颁发机构获取替换证书。

## 在思科 ISE 中启用公共密钥基础设施

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。

**步骤 1** 在部署中的以下每个节点上配置系统证书：

- 支持 TLS 的身份验证协议，例如 EAP-TLS。
- 管理门户身份验证。
- 允许浏览器和 REST 客户端访问思科 ISE Web 门户。
- 允许访问 pxGrid 控制器。

默认情况下，思科 ISE 节点预先安装了用于 EAP 身份验证，以及用于访问管理门户、最终用户门户和 pxGrid 控制器的自签证书。在典型的企业环境中，此自签证书由受信任 CA 签名的服务器证书代替。

**步骤 2** 用与用户建立信任的 CA 签名证书以及向思科 ISE 出示的设备证书填充受信任证书库。

要使用包含一个根 CA 证书以及一个或多个中间 CA 证书的证书链来验证用户或设备证书的真实性，请执行以下操作：

- 为根 CA 启用相关的信任选项。

在思科 ISE GUI 中，选择**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书管理 (Certificate Management) > 受信任证书 (Trusted Certificates)**。在此窗口中，选中根 CA 证书的复选框，然后单击**编辑 (Edit)**。在使用情况 (Usage) 区域中，选中信任范围 (Trusted For) 区域中的必要的复选框。

- 如果不想为根 CA 启用信任选项，请将整个 CA 签名证书链导入受信任证书存储区。

对于节点间通信，您必须使用验证思科 ISE 部署中每个节点的管理员系统证书的信任证书来填充受信任证书库。要使用默认自签证书进行节点间通信，请从每个思科 ISE 节点的“系统证书” (System Certificates) 窗口导出该证书并将其导入受信任证书库。如果您用 CA 签名的证书代替自签证书，只需用相应的根 CA 和中间 CA 证书填充受信任证书库。在完成此步骤之前，您无法在思科 ISE 部署中注册节点。

如果您想获得公共签名证书，或者要在 FIPS 模式下运行思科 ISE 部署，您必须确保所有系统和受信任证书都兼容 FIPS。这意味着每个证书都必须具有 2048 个字节的最小密钥长度并且使用 SHA-1 或 SHA-256 加密。

**注释** 在您从独立思科 ISE 节点或 PAN 获取备份后，如果您更改您的部署中一个或多个节点上的证书配置，您必须再获得一个备份以恢复数据。否则，如果您尝试使用较旧的备份恢复数据，节点之间的通信可能会发生故障。

## 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：。：

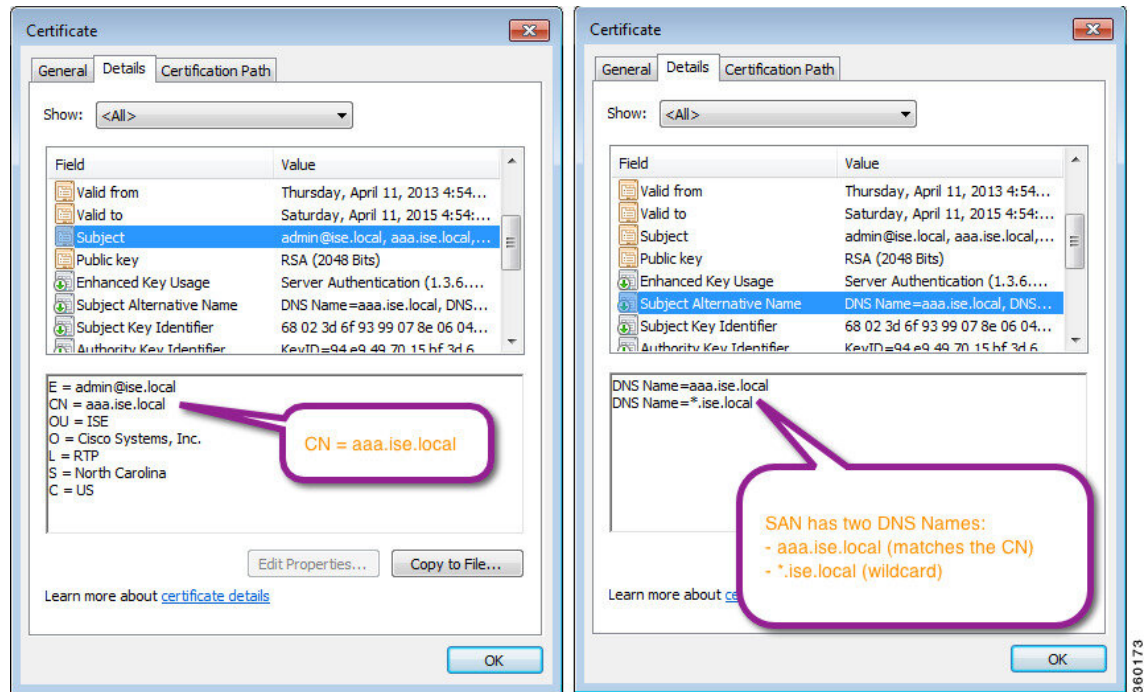
- aaa.ise.local

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



## 思科 ISE 中的通配符证书支持

思科 ISE 支持通配符证书。在较低版本中，思科 ISE 会验证为 HTTPS 启用的任何证书以确保通用名称字段与主机的主机名 FQDN 完全一致。如果字段不一致，则证书无法用于 HTTPS 通信。

在较低版本中，思科 ISE 使用该公用名称值来替换 url-redirect A-V 对字符串中的变量。此公用名称值还曾用于所有集中式 Web 身份验证、自行激活、安全评估重定向等。

思科 ISE 使用 ISE 节点的主机名作为公用名称。

## 适用于 HTTPS 和扩展身份验证协议通信的通配符证书

您可以在思科 ISE 中将通配符服务器证书用于使用 SSL 或 TLS 隧道的管理（基于 Web 的服务）和 EAP 协议。在使用通配符证书时，您不需要为每个思科 ISE 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。在 SAN 字段中使用星号 (\*)，以便在部署中的多个节点上共享单个证书，同时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。

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。



**注释** 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，就可能导致严重的安全问题。

通配符证书在域名前使用星号(\*)和一个句点。例如，证书的使用者名称的公共名称值是一般主机名称（例如 aaa.ise.local），SAN 字段可以使用通配符，例如 \*.ise.local。思科 ISE 支持使用通配符证书，其中通配符(\*)是所显示标识符最左侧的字符。例如，\*.example.com 或 \*.ind.example.com。思科 ISE 不支持所显示的标识符中连通配符一起显示其他字符的证书。例如，abc\*.example.com 或 a\*b.example.com 或 \*abc.example.com。

## URL 重定向中的完全限定域名

授权配置文件重定向用于集中 Web 身份验证、设备注册 Web 身份验证、本地请求方调配、移动设备管理、客户端调配与安全评估服务。当思科 ISE 构建授权配置文件重定向时，生成的 cisco-av-pair 包含类似于以下内容的字符串：

```
url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

处理此请求时，思科 ISE 会用实际值代替此字符串中的某些关键字。例如，思科 ISE 会将 SessionIdValue 替换为该请求的实际会话 ID。对于 eth0 接口，思科 ISE 将 URL 中的 IP 替换为思科 ISE 节点的 FQDN。对于非 eth0 接口，思科 ISE 使用 URL 中的 IP 地址。您可以为接口 eth1 至 eth3 分配主机别名（名称），然后在 URL 重定向期间，思科 ISE 可以用其代替 IP 地址。

要实现此操作，可以在配置模式下从 ISE CLI ISE /admin(config)# 提示符处使用 **ip host** 命令：

```
ip host IP_address host-alias FQDN-string
```

其中 *IP\_address* 是网络接口的 IP 地址（eth1 或 eth2 或 eth3），*host-alias* 是您分配给网络接口的名称。*FQDN-string* 是网络接口的完全限定域名。使用此命令，您可以向网络接口分配 *host-alias* 或 *FQDN-string*，或同时分配两者。

这是使用 **ip host** 命令的一个示例：`ip host a.b.c.d sales sales.amerxyz.com`

向非 eth0 接口分配主机别名之后，您必须在思科 ISE 上使用 **application start ise** 命令重新启动应用服务。

使用此命令的 **no** 形式可删除主机别名与网络接口的关联。

```
no ip host IP_address host-alias FQDN-string
```

使用 **show running-config** 命令可查看主机别名定义。

如果您提供 *FQDN-string*，思科 ISE 会使用 FQDN 替换 URL 中的 IP 地址。如果您仅提供主机别名，思科 ISE 会将主机别名与所配置的 IP 域名组合以形成完整的 FQDN，并用 FQDN 替换 URL 中的 IP 地址。如果您不将网络接口映射至主机别名，则思科 ISE 会使用 URL 中的网络接口的 IP 地址。

当您为非 eth0 接口用于客户端调配或本地请求方或访客流程时，请确保在 PSN 证书的 SAN 字段中正确配置非 eth0 接口的 IP 地址或主机别名。

## 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。

## 系统证书

思科 ISE 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 节点身份的服务器证书。系统证书的用途如下：

- 用于思科 ISE 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。
- 由浏览器和连接到思科 ISE Web 门户的 REST 客户端使用。选中这些证书的使用情况 (Usage) 区域中的门户 (Portal) 复选框。
- 用于与 PEAP 和 EAP-FAST 组成外部 TLS 隧道。选中使用情况 (Usage) 区域中的 EAP 身份验证 (EAP Authentication) 复选框，以使用 EAP-TLS、PEAP 和 EAP-FAST 进行相互身份验证。
- 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 部署中的每个节点上安装有效的系统证书。默认情况下，系统会在安装过程中在思科 ISE 节点上创建自签名的证书，并且将此证书指定用于 EAP、管理员、门户和 pxGrid（此证书的密钥长度为 1024，有效期为一年）。



### 注释

- 当导出要导入其他节点的通配符系统证书（用于节点间通信）时，请确保导出证书和专用密钥，并指定加密密码。在导入过程中，将需要证书、专用密钥和加密密码。

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 113 页](#)
2. [将根证书导入受信任证书库，第 108 页](#)
3. [将 CA 签名的证书绑定到证书签名请求，第 114 页](#)

## 查看系统证书

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

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** 选择 **管理 (Administration) > 系统 (System) > 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 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（管理 (**Administration**) > 系统 (**System**) > 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。
- 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** 选择管理 (**Administration**) > 系统 (**System**) > 证书 (**Certificates**) > 系统证书 (**System Certificates**)。

**步骤 2** 点击导入 (**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** 点击提交。

## 系统证书导入设置

表 17: 系统证书导入设置

字段名称	说明
<b>Select Node</b>	(必填) 从下拉列表中选择您要导入系统证书的思科 ISE 节点。
<b>Certificate File</b>	(必填) 单击浏览 ( <b>Browse</b> )，从本地系统中选择证书文件。
<b>Private Key File</b>	(必需) 单击浏览 ( <b>Browse</b> )，从本地系统中选择私钥文件。
密码	(必填) 输入密码以解密私钥文件。
<b>友好名称 (Friendly Name)</b>	输入证书的友好名称。如果未指定名称，思科 ISE 会自动创建以下格式的名称：  <common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是一个唯一的五位数。
<b>Allow Wildcard Certificates</b>	如果要导入通配符证书，请选中此复选框。通配符证书使用通配符号（在域名前带一个星号和一个句点）。通配符证书会在组织中的多个主机之间共享。  如果选中此复选框，思科 ISE 会将此证书导入到部署中的所有其他节点。



字段名称	说明
	如果希望思科 ISE 验证证书扩展，请选中此复选框。如果选中此复选框，并且要导入的证书包含 CA 标志设为 true 的基本限制扩展，请确保密钥用法扩展存在。还必须设置 keyEncipherment 位和/或 keyAgreement 位。
使用情况	<p>选择必须使用此系统证书的服务：</p> <ul style="list-style-type: none"> <li>• <b>管理员 (Admin):</b> 用于确保与部署中的管理门户和思科 ISE 节点之间安全通信的服务器证书。            注释 在主 PAN 上更改管理员角色证书的证书将在所有其他思科 ISE 节点上重新启动服务。</li> <li>• <b>EAP 身份验证 (EAP Authentication):</b> 用于使用 EAP 协议建立 SSL 或 TLS 隧道的身份验证的服务器证书。</li> <li>• <b>pxGrid:</b> 用于确保 pxGrid 客户端和服务器之间的安全通信的客户端和服务证书。</li> <li>• <b>：</b> 用于经思科 ISE 消息传递的系统日志 (<b>Syslog Over Cisco ISE Messaging</b>) 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。</li> <li>• <b>门户 (Portal):</b> 用于确保与所有思科 ISE Web 门户的安全通信的服务器证书。</li> </ul>



**注释** 如果证书是由其他第三方工具而不是思科 ISE 生成的，则无法将证书或其私钥导入思科 ISE。

#### 相关主题

[系统证书](#)，第 94 页

[查看系统证书](#)，第 95 页

[导入系统证书](#)，第 95 页

## 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，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 节点的主机名，请登录思科 ISE 节点的管理门户，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 会继续使用采用旧主机名的自签证书。

## 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。

## 自签证书设置

表 18: 自签证书设置

字段名称	使用指南
<b>Select Node</b>	(必填) 从下拉列表中选择您要为其生成系统证书的节点。
<b>Common Name (CN)</b>	(如果您不指定 SAN, 则此字段必填) 默认情况下, Common Name 为您要生成自签证书的思科 ISE 节点的 FQDN。
<b>组织单位 (OU) (Organizational Unit [OU])</b>	组织单位名称。例如, Engineering。
<b>Organization (O)</b>	组织名称。例如, Cisco。
<b>City (L)</b>	(请勿缩写) 城市名称。例如, 圣何塞。
<b>省/自治区/直辖市 (ST) (State [ST])</b>	(请勿缩写) 省/自治区/直辖市名称。例如, 加州。
<b>国家/地区 (C) (Country [C])</b>	国家/地区名称。输入两个字母 ISO 国家/地区代码。例如, US。
<b>主体可选名称 (SAN) (Subject Alternative Name [SAN])</b>	与该证书关联的。
<b>密钥长度</b>	<p>公共密钥的位大小。从 RSA 的下拉列表中选择以下选项之一:</p> <ul style="list-style-type: none"> <li>• 512</li> <li>• 1024</li> <li>• 2048</li> <li>• 4096</li> </ul> <p>从 ECDSA 的下拉列表中选择以下选项之一:</p> <ul style="list-style-type: none"> <li>• 256</li> <li>• 384</li> </ul> <p>如果您计划获得公共 CA 签名的证书, 请选择 2048。</p>

字段名称	使用指南
<b>Digest to Sign With</b>	从下拉列表中选择以下散列算法之一： <ul style="list-style-type: none"> <li>• SHA-1</li> <li>• SHA-256</li> </ul>
<b>Expiration TTL</b>	指定证书到期之前的天数。从下拉列表中选择值。
<b>友好名称 (Friendly Name)</b>	输入证书的友好名称。如果未指定名称，思科 ISE 会自动创建以下格式的名称： <common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是唯一的五位数数字。
<b>使用情况</b>	选择必须使用此系统证书的服务： <ul style="list-style-type: none"> <li>• <b>管理员 (Admin)</b>：用于确保与部署中的管理门户和思科 ISE 节点之间安全通信的服务器证书。</li> <li>• <b>EAP 身份验证 (EAP Authentication)</b>：用于使用 EAP 协议建立 SSL 或 TLS 隧道的身份验证的服务器证书。</li> <li>• <b>pxGrid</b>：用于确保 pxGrid 客户端和服务端之间的安全通信的客户端和服务端证书。</li> <li>• <b>门户 (Portal)</b>：用于确保与所有思科 ISE Web 门户的安全通信的服务器证书。</li> </ul>

#### 相关主题

[系统证书](#)，第 94 页

[查看系统证书](#)，第 95 页

[生成自签证书](#)，第 97 页

## 编辑系统证书

使用此窗口来编辑系统证书，续订自签证书。

#### 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** 选择管理 (**Administration**) > 系统 (**System**) > 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，请选中复选框，然后输入以天、周、月或年为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 节点上的应用服务器将重新启动。此外，如果思科 ISE 节点是部署中的 PAN，则部署中所有其他节点上的应用服务器也将重新启动。主 PAN 重启完成后，系统会每次重新启动一个节点。

有关故障排除的信息，请参阅[使用 Google Chrome 65 启动 BYOD 门户](#)，第 100 页使用[Mozilla Firefox 64 配置无线 BYOD 设置](#)，第 100 页。

---

## 使用 Google Chrome 65 启动 BYOD 门户

在使用 Chrome 65 及更高版本启动思科 ISE 时，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 BYOD 门户，请执行以下步骤：

- 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。
- 步骤 2** 思科 ISE 服务将重新启动。
- 步骤 3** 在 Chrome 浏览器中重定向门户。
- 步骤 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。**
- 步骤 5** 将证书安装到受信任路径。
- 步骤 6** 关闭 Chrome 浏览器，然后尝试重定向门户。

---

## 使用 Mozilla Firefox 64 配置无线 BYOD 设置

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：

- 步骤 1** 针对 BYOD 流程单或双 PEAP 或 TLS 进行配置。
- 步骤 2** 通过 Windows ALL 选项配置 CP 策略。
- 步骤 3** 在最终客户端 Windows RS4 或 Windows RS5 中连接 Dot1.x 或 MAB SSID。
- 步骤 4** 在 FF64 浏览器中键入任意 URL 以重定向至访客或 BYOD 门户。
- 步骤 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)**。

## 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私钥以进行备份，如有必要，您以后也可以重新导入此证书与私钥。

### 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** 管理 (Administration) > 系统 (System) > 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，然后点击导出 (Export)。

**步骤 3** 选择是仅导出证书，还是导出证书及其关联的私钥。

**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 节点时，必须指定此密码以解密专用密钥。

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

**步骤 5** 点击 **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。

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。

受信任证书库中的证书在主 PAN 上进行管理，并且复制至思科 ISE 部署中的每个节点。思科 ISE 支持通配符证书。

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 管理门户的思科 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 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。

- 实现安全的 LDAP 身份验证，在定义将通过 SSL 访问的 LDAP 身份源时，必须从证书存储区选择证书。
- 向准备使用个人设备门户在网络中进行注册的个人设备进行分配。思科 ISE 在 PSN 上实施 SCEP 以支持个人设备注册。注册设备使用 SCEP 协议从 PSN 请求客户端证书。PSN 包含充当中间证书的注册机构 (RA)。RA 会接收并验证来自注册设备的请求，然后将请求转发给颁发客户端证书的外部 CA 或内部思科 ISE CA。CA 将证书发送回 RA，RA 再将其返回至设备。

思科 ISE 使用的每个 SCEP CA 都通过 SCEP RA 配置文件定义。当创建 SCEP RA 配置文件时，系统将以下两个证书自动添加到受信任证书库：

- CA 证书（自签证书）
- RA 证书（证书请求代理证书），由 CA 签名。

SCEP 协议要求 RA 将这两个证书提供给注册设备。通过将这两个证书放入受信任证书库，系统将其复制至所有 PSN 节点，以供这些节点上的 RA 使用。



**注释** 删除 SCEP RA 配置文件时，关联的 CA 链也会从受信任证书库中删除。不过，如果安全系统日志、LDAP、系统或信任证书参考了相同证书，则仅删除 SCEP 配置文件。

## 受信任证书库中的证书

受信任证书库中包含受信任的证书：生产证书、根证书、终端 CA、终端 RA 和其他受信任的证书。根证书（思科根 CA）给生产（思科 CA 生产）证书签名。默认情况下禁用这些证书。如果您在部署中将思科 IP 电话作为终端，请启用根和制造证书，从而对用于电话的思科签名的客户端证书进行身份验证。

## 受信任证书列表

表 19: 受信任证书窗口列

字段名称	使用指南
<b>Friendly Name</b>	显示证书的名称。
<b>状态</b>	此列会显示已启用 ( <b>Enabled</b> ) 或已禁用 ( <b>Disabled</b> )。如果证书被禁用，则思科 ISE 将不使用此证书建立信任。
<b>Trusted for</b>	显示以下一项或多项使用此证书的服务。 <ul style="list-style-type: none"> <li>• 基础设施</li> <li>• 思科服务</li> <li>• 终端</li> </ul>

字段名称	使用指南
<b>Issued To</b>	显示证书持有者的通用名称。
颁发者	显示证书颁发机构的通用名称。
<b>Valid From</b>	显示证书的颁发日期和时间。该值也称为“不早于”(Not Before)证书属性。
到期日期	显示证书到期的日期和时间。该值也称为“不迟于”(Not After)证书属性。
<b>Expiration Status</b>	提供有关证书到期状态的信息。此列会显示五个图标和提示消息类别： <ul style="list-style-type: none"> <li>• 绿色：距到期还有 90 天以上</li> <li>• 蓝色：距到期还有 90 天或更短</li> <li>• 黄色：距到期还有 60 天或更短</li> <li>• 橙色：距到期还有 30 天或更短</li> <li>• 红色：已到期</li> </ul>

#### 相关主题

[受信任证书库](#)，第 101 页

[查看受信任的证书](#)，第 104 页

[更改受信任证书库中的证书状态](#)，第 105 页

[在受信任的证书库中添加证书](#)，第 105 页

## 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 的受信任证书。要查看受信任的证书, 您必须成为超级管理员或系统管理员。

### 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** 要查看所有证书, 选择**管理 (Administration)** > **系统 (System)** > **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 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。

## 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。

### 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。
- 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上。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。

## 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。

### 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 管理 (Administration) > 系统 (System) > 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，然后点击**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** 点击**保存 (Save)**。

## 受信任证书设置

表 20: 受信任证书编辑设置

字段名称	使用指南
证书颁发者 (Certificate Issuer)	

字段名称	使用指南
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)	从下拉列表中选择启用 (Enabled) 或禁用 (Disabled)。如果证书被禁用，则思科 ISE 将不使用此证书建立信任。
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 LADP 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>
信任基于证书的管理人员身份验证	仅当选择信任客户端身份验证和系统日志 (Trust for client authentication and Syslog) 时，才能选中此复选框。 选中此复选框可启用基于证书的身份验证用于管理员访问。将所需的证书链导入受信任证书存储区。
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。
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。

字段名称	使用指南
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证书。
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。
忽略 CRL 无效或已过期 (Ignore that CRL is not yet valid or expired)	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。 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。

#### 相关主题

[受信任证书库](#)，第 101 页

[编辑受信任证书](#)，第 105 页

## 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 125 页。

**步骤 1** 选择 **管理 (Administration) > 系统 (System) > 证书 (Certificates) > 受信任的证书 (Trusted Certificates)**。

**步骤 2** 选中要导出的证书旁边的复选框，然后点击**导出 (Export)**。一次只能导出一个证书。

**步骤 3** 将 PEM 文件保存到运行客户端浏览器的文件系统。

## 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。

导入外部根 CA 证书时，请在以下任务的步骤 5 中启用“信任基于证书的管理员身份验证”选项。

### 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** 选择 **管理 (Administration) > 系统 (System) > 证书 (Certificates) > 受信任的证书 (Trusted Certificates)**。

**步骤 2** 点击**导入 (Import)**。

**步骤 3** 在**将新证书导入证书存储区 (Import a new Certificate into the Certificate Store)** 窗口中，点击**选择文件 (Choose File)** 以选择您的 CA 签名和返回的根 CA 证书。

**步骤 4** 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 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 5** 选中要为其使用此受信任证书的服务旁边的复选框。

**步骤 6** （可选）在**说明 (Description)** 字段中，输入此证书的说明。

**步骤 7** 点击**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）。

## 受信任证书导入设置

表 21: 受信任证书导入设置

字段名称	说明
	点击 <b>浏览 (Browse)</b> 从运行浏览器的计算机选择证书文件。
<b>友好名称 (Friendly Name)</b>	输入证书的友好名称。如果您不指定名称，思科ISE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。
<b>信任 ISE 中的身份验证 (Trust for authentication within ISE)</b>	如果您希望将此证书用于验证服务器证书（从其他ISE节点或LDAP服务器），请选中此复选框。
<b>信任客户端身份验证和系统日志 (Trust for client authentication and Syslog)</b>	（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 ISE 的终端进行身份验证</li> <li>• 信任系统日志服务器</li> </ul>
<b>信任思科服务的身份验证 (Trust for authentication of Cisco Services)</b>	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。
	（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。
<b>说明 (Description)</b>	输入可选的说明。

### 相关主题

[受信任证书库](#)，第 101 页

[证书链导入](#)，第 109 页

[将根证书导入受信任证书库](#)，第 108 页

## 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。

## 为思科 ISE 节点间通信安装受信任证书

当您设置部署时，在注册辅助节点之前，您必须使用适当 CA 证书填充 PAN 的 CTL，这些证书用于验证辅助节点的管理员证书。对于不同的场景，填充 PAN 的 CTL 的程序也不同。

- 如果辅助节点使用 CA 签名的证书与思科 ISE 管理门户通信，则您必须将辅助节点的 CA 签名证书、相关的中间证书（如果有）和根 CA 证书（属于签署辅助节点证书的 CA）导入到 PAN 的 CTL。
- 如果辅助节点使用自签证书与思科 ISE 管理门户通信，则您可以将辅助节点的自签证书导入到 PAN 的 CTL。



### 注释

- 如果您更改了已注册辅助节点的管理员证书，则您必须获取适当 CA 证书（可用于验证辅助节点的管理员证书）并将其导入到 PAN 的 CTL。
- 当自带设备用户从一个位置移动到另一个位置时，如果您使用自签证书确保部署中客户端与 PSN 之间的安全通信，EAP-TLS 用户身份验证会失败。对于这种必须在某些 PSN 之间实现的身份验证请求，您必须通过外签 CA 证书或使用外部 CA 签名的通配符证书确保客户端与 PSN 之间的通信。

确保由外部 CA 颁发的证书已经定义了基本约束且 CA 标记设置为 true。要为节点间通信安装 CA 签名证书：

**步骤 1** [创建证书签名请求并将其提交给证书颁发机构，第 113 页](#)

**步骤 2** [将根证书导入受信任证书库，第 108 页](#)

**步骤 3** [将 CA 签名的证书绑定到证书签名请求，第 114 页](#)

## 思科 ISE 中的默认受信任证书

思科 ISE 中受信任证书存储库（**管理 (Administration) > 系统 (System) > 证书 (Certificates) > 受信任证书 (Trusted Certificates)**）包含默认可用的一些证书。这些证书会自动导入到库中，以满足安全要求。但是，并非必须使用所有这些证书。除非下表中另有说明，否则您可以使用您选择的证书，而不是已提供的证书。

表 22: 默认受信任的证书

受信任证书名称	序列号	证书的用途	含证书的思科 ISE 版本
<b>Baltimore CyberTrust Root CA</b>	02 00 00 B9	在某些地区，此证书可用作 <a href="https://s3.amazonaws.com">cisco.com</a> 使用的 CA 链中的根 CA 证书。 <a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a> 上托管的 ISE 2.4 终端安全评估/CP 更新 XML 文件中也使用该证书。	版本 2.4 及更高版本。
<b>DST Root CA X3 Certificate Authority</b>	44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B	此证书可用作 <a href="https://s3.amazonaws.com">cisco.com</a> 使用的 CA 链的根 CA 证书。	版本 2.4 及更高版本。
<b>Thawte Primary Root CA</b>	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	此证书可用作 <a href="https://s3.amazonaws.com">cisco.com</a> 和 <a href="https://s3.amazonaws.com">perfigo.com</a> 使用的 CA 链的根 CA 证书。	版本 2.4 及更高版本。
<b>VeriSign Class 3 Public Primary Certification Authority</b>	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	此证书用作 VeriSign Class 3 Secure Server CA-G3 的根 CA 证书。  在思科 ISE 中配置 Profiler Feed Service 时，必须使用此证书。	版本 2.4 及更高版本。
<b>VeriSign Class 3 Secure Server CA - G3</b>	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	这是一个中级 CA 证书，于 2020 年 2 月 7 日到期。您不需要更新此证书。  您可以按照以下任务删除证书。	版本 2.4 及更高版本。
<b>Cisco CA Manufacturing</b>	6A 69 67 B3 00 00 00 00 00 03	连接到思科 ISE 的某些思科设备可能使用此证书。默认情况下禁用此证书。	版本 2.4 和 2.6。
<b>Cisco Manufacturing CA SHA2</b>	02	此证书可在管理员身份验证、终端身份验证和部署基础设施流的 CA 链中使用。	版本 2.4 及更高版本。

受信任证书名称	序列号	证书的用途	含证书的思科 ISE 版本
<b>Cisco Root CA 2048</b>	5F F8 7B 28 2B 54 DC 8D 42 A3 15 B5 68 C9 AD FF	连接到思科 ISE 的某些思科设备可使用此证书。默认情况下禁用此证书。	版本 2.4 及更高版本。
<b>Cisco Root CA M2</b>	01	此证书可在管理员身份验证、终端身份验证和部署基础设施流的 CA 链中使用。	版本 2.4 及更高版本。
<b>DigiCert Root CA</b>	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	必须在使用 Facebook 的访客登录流中使用此证书。	版本 2.4 及更高版本。
<b>DigiCert SHA2 High Assurance Server CA</b>	04 E1 E7 A4 DC 5C F2 F3 6D C0 2B 42 B8 5D 15 9F	必须在使用 Facebook 的访客登录流中使用此证书。	版本 2.4 及更高版本。
<b>HydrantID SSL ICA G2</b>	75 17 16 77 83 D0 43 7E B5 56 C3 57 94 6E 45 63 B8 EB D3 AC	思科服务的受信任证书。	版本 2.4 和 2.6。
<b>QuoVadis Root CA 2</b>	05 09	您必须在分析器、终端安全评估和客户端调配流中使用此证书。	版本 2.4 及更高版本。
<b>Cisco ECC Root CA</b>	01	此证书是思科 ISE 中使用的思科信任根存储库捆绑包的一部分。	版本 2.6。
<b>Cisco Licensing Root CA</b>	01	此证书是思科 ISE 中使用的思科信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
<b>Cisco Root CA 2099</b>	01 9A 33 58 78 CE 16 C1 C1	此证书是思科 ISE 中使用的思科信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
<b>Cisco Root CA M1</b>	2E D2 0E 73 47 D3 33 83 4B 4F DD 0D D7 B6 96 7E	此证书是思科 ISE 中使用的思科信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
<b>Cisco RXC-R2</b>	01	此证书是思科 ISE 中使用的思科信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。



受信任证书名称	序列号	证书的用途	含证书的思科 ISE 版本
<b>DigiCert Global Root CA</b>	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	此证书是思科 ISE 中使用的思科信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。
<b>Cisco ECC Root CA 2099</b>	03	此证书是思科 ISE 中使用的思科信任根存储库捆绑包的一部分。	版本 2.6 及更高版本。

### 从思科 ISE 删除默认受信任证书

- 导出要删除的证书并保存，以便在需要时再次导入。  
选中要导出的证书对应的复选框，然后单击上方菜单栏上的**导出 (Export)**。密钥链会下载到您的系统。
- 删除证书。选中要删除的证书对应的复选框，然后单击上方菜单栏上的**删除 (Delete)**。如果任何 CA 链、安全系统日志或安全 LDAP 在使用该证书，则不允许删除它。
- 进行必要的配置更改，从 CA 链、安全系统日志和证书所属的系统日志中移除证书。然后删除证书。
- 在删除证书后，检查相关服务（请参阅证书用途）是否如期运行。

## 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** 窗口会提供您已创建的证书签名请求的列表。选择 **管理 > 系统 > 证书 > 证书签名请求**。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** 选择 **管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书签名请求 (Certificate Signing Requests)**。

**步骤 2** 点击**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 105 页。

**步骤 4** （可选）选中要下载的签名请求的复选框，然后单击**导出 (Export)** 以下载请求。

**步骤 5** 复制从“-----BEGIN CERTIFICATE REQUEST-----”到“-----END CERTIFICATE REQUEST-----”的所有文本。”并将请求的内容粘贴到所选 CA 的证书请求中。

**步骤 6** 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 受信任证书存储区的 CA 新颁发证书和公共签名证书。数字签名的 CA 证书、根 CA 证书和其他中间 CA 证书（如果适用）可被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 发送的相关根和中间 CA 证书。
- 将相关的根和中间 CA 证书导入受信任证书库（**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **受信任证书 (Trusted Certificates)**）。

---

**步骤 1** 选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书签名请求 (Certificate Signing Requests)**。

**步骤 2** 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 3** 单击**绑定 (Bind)**。

**步骤 4** 在显示的**绑定 CA 签名证书 (Bind CA Signed Certificate)** 窗口中，单击**浏览 (Browse)** 以选择 CA 签名证书。

**步骤 5** 在**友好名称 (Friendly Name)** 字段中输入值。

**步骤 6** 如果您希望思科 ISE 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** 选项，且您导入的证书包含 CA 标志设置为 True 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 7** （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。

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 8** 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 节点间通信，则思科 ISE 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 108 页](#)

## 导出证书签名请求

### 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** 选择 **管理 (Administration) > 系统 (System) > 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，点击**导出 (Export)**。

**步骤 3** 点击**确定 (OK)**，将文件保存到正在运行客户端浏览器的文件系统中。

**步骤 4** 证书签名请求可下载到本地文件系统中。

---

## 证书签名请求设置

通过思科 ISE，只需一个请求即可从管理门户为部署中的所有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多个两个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)。如果在 CN 字段中输入的域名不是节点的 FQDN，思科 ISE 将拒绝使用该证书进行身份验证。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 节点的 FQDN。如有必要，您还可以在 SAN 字段中添加其他 FQDN。如果选择为部署中的所有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 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 (\*)，可以在部署中的多个两个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 节点分配唯一服务器证书的安全性低。

表 23: 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>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 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>EAP 身份验证 (EAP Authentication)</b>: 用于服务器身份验证。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)</li> </ul> </li> </ul> <p><b>注释</b>          EAP-TLS 客户端证书需要使用数字签名密钥。</p> <ul style="list-style-type: none"> <li>• <b>门户 (Portal)</b>: 用于服务器身份验证（以确保与所有 ISE Web 门户之间的安全通信）。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)</li> </ul> </li> <li>• <b>pxGrid</b> - 同时用于客户端和服务端身份验证（以确保 pxGrid 客户端与服务端之间的安全通信）。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> </ul> <p><b>注释</b>          建议您不要将包含值 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。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>

字段	使用指南
	<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 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 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 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 节点的 FQDN。\$FQDN\$ 表示 ISE 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 Common Name 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。
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。

字段	使用指南
主体可选名称 (SAN) (Subject Alternative Name [SAN])	<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 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 节点的 IP 地址。</li> </ul>
密钥长度 (Key Length)	如果计划获取公共的 CA 签名证书或将思科 ISE 部署为符合 FIPS 标准的策略管理系统, 请选择 2048 或更大长度。
签名摘要 (Digest to Sign With)	选择下列散列算法之一: SHA-1 或 SHA-256。

#### 相关主题

[证书签名请求, 第 113 页](#)

[创建证书签名请求并将其提交给证书颁发机构, 第 113 页](#)

[将 CA 签名的证书绑定到证书签名请求, 第 114 页](#)

## 设置供门户使用的证书

由于部署中有多个 PSN 可以支持 Web 门户请求, 所以思科 ISE 需要使用唯一标识符来标识必须用于门户通信的证书。当您添加或导出指定用于门户用途的证书时, 请定义证书组标签并将其与您的部署中各个节点上的对应证书关联。将此证书组标签与对应的最终用户门户关联 (访客、发起人和个人设备门户)。此证书组标签是一种唯一标识符, 帮助思科 ISE 标识与这每一个门户通信时必须使用的证书。您只能从每个节点为每个门户指定一个证书。



**注释** 思科 ISE 在 TCP 端口 8443 (或者您为使用门户而配置的端口) 上提供门户证书。

**步骤 1** [创建证书签名请求并将其提交给证书颁发机构, 第 113 页。](#)

您必须选择您已定义的证书组标签或为门户创建一个新证书组标签。例如 mydevicesportal。

**步骤 2** [将根证书导入受信任证书库, 第 108 页。](#)

**步骤 3** [将 CA 签名的证书绑定到证书签名请求, 第 114 页。](#)

## 用户和终端证书续订

默认情况下, 思科 ISE 拒绝来自证书已过期设备的请求。但是, 您可以更改此默认行为并配置 ISE 以满足这些请求并提示用户更新证书。

如果选择允许用户更新证书，思科建议您配置一个授权策略规则，检查在进一步处理请求之前证书是否已续签。处理来自证书过期设备的请求可能导致潜在的安全威胁。因此，必须配置正确的授权配置文件和规则来确保贵公司的安全不受影响。

在证书到期前或到期后，有些设备支持证书续订。但是在 Windows 设备上，您只能在证书到期前续订证书。Apple iOS、Mac OSX 和 Android 设备支持在证书到期前或到期后，进行证书续订。

## 策略条件中用于证书续订的字典属性

思科 ISE 证书字典包含在策略条件中用于允许用户续订证书的以下属性：

- **Days to Expiry:** 此属性规定证书有效的天数。您可以使用此属性创建可用于授权策略的条件。此属性可采用 0 至 15 之间的值。值 0 表示证书已过期。值 1 表示证书不到 1 天就要到期。
- **Is Expired:** 此布尔属性表示证书是否已到期。如果想要只允许在证书接近到期时而不是在证书已到期之后续订证书，请在授权策略条件中使用此属性。

## 证书续订的授权策略条件

您可以使用授权策略中的 `CertRenewalRequired` 简单条件（默认情况下可用）以确保在思科 ISE 进一步处理请求之前更新证书（已到期或即将到期）。

## 用于续订证书的 CWA 重定向

如果用户证书在证书到期前已被吊销，则思科 ISE 会检查 CA 发布的 CRL 并拒绝身份验证请求。如果被撤消的证书已过期，则 CA 不得在其 CRL 中发布此证书。在此场景中，思科 ISE 可更新被撤消的证书。要避免此问题，在更新证书之前，请确保请求重新定向到集中式 Web 身份验证 (CWA) 以进行完整的身份验证。必须创建授权配置文件才能重定向用户以进行 CWA。

## 将思科 ISE 配置为允许用户续订证书

您必须完成此程序中列出的任务，才能将思科 ISE 配置为允许用户续订证书。

### 开始之前

在 WLC 上配置受限访问 ACL 以重定向 CWA 请求。

---

步骤 1 [更新允许的协议配置，第 121 页](#)

步骤 2 [为 CWA 重定向创建授权策略配置文件，第 121 页](#)

步骤 3 [创建授权策略规则以更新证书，第 122 页](#)

步骤 4 [在访客门户中启用 BYOD 设置，第 122 页](#)

---



## 更新允许的协议配置

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 身份验证 (Authentication) > 允许的协议 (Allowed Protocols) > 默认网络访问 (Default Network Access)。

**步骤 2** 选中 EAP-TLS 协议以及 PEAP 和 EAP-FAST 协议的 EAP-TLS 内部方法下的 **Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy** 复选框。

使用 EAP-TLS 协议的请求将通过 NSP 流。

对于 PEAP 和 EAP-FAST 协议，您必须手动安装和配置思科 AnyConnect 以便思科 ISE 处理请求。

**步骤 3** 点击提交。

下一步做什么

[为 CWA 重定向创建授权策略配置文件，第 121 页](#)

## 为 CWA 重定向创建授权策略配置文件

开始之前

确保您已在 WLC 上配置受限访问 ACL。

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles)。

**步骤 2** 点击添加 (Add)。

**步骤 3** 为授权配置文件输入名称。例如 CertRenewal\_CWA。

**步骤 4** 在“常见任务” (Common Tasks) 区域，选中 **Web 重定向 (CWA、DRW、MDM、NSP、CPP) (Web Redirection (CWA, DRW, MDM, NSP, CPP))** 复选框。

**步骤 5** 从下拉列表和受限访问 ACL 选择集中式 **Web 身份验证 (Centralized Web Auth)**。

**步骤 6** 选中显示证书续订消息 (**Display Certificates Renewal Message**) 复选框。

URL-redirect 属性值改变并且包含证书有效的天数。

**步骤 7** 点击提交。

下一步做什么

[创建授权策略规则以更新证书，第 122 页](#)

## 创建授权策略规则以更新证书

### 开始之前

确保您已创建集中式 Web 身份验证重定向的授权配置文件。

在**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **策略设置 (Policy Settings)** 上启用策略集。

---

**步骤 1** 选择策略 (Policy) > 策略集 (Policy Sets)。

**步骤 2** 点击创建于...之上 (Create Above)。

**步骤 3** 输入新规则的名称。

**步骤 4** 选择以下简单条件和结果：

如果 CertRenewalRequired 等于 True，则为权限选择先前创建的授权配置文件 (CertRenewal\_CWA)。

**步骤 5** 单击保存。

---

### 下一步做什么

当使用其证书已到期的设备访问公司网络时，请点击**续订 (Renew)** 重新配置设备。

## 在访客门户中启用 BYOD 设置

要使用户能够更新个人设备证书，必须在所选访客门户中启用 BYOD 设置。

---

**步骤 1 a)** 选择所选 CWA 门户并点击**编辑 (Edit)**。

**步骤 2** 从 BYOD 设置中，选中允许员工在网络上使用个人设备 (Allow employees to use personal devices on the network) 复选框。

**步骤 3** 点击保存 (Save)。

---

## Apple iOS 设备的证书续订失败

当您使用 ISE 在 Apple iOS 设备上续订终端证书时，您可能会遇到“Profiled Failed to Install”错误消息。如果在相同策略服务节点 (PSN) 或另一个 PSN 上，与处理续订所使用的证书不同的管理员 HTTPS 证书已签名要过期或已过期的网络配置文件，则系统会显示此错误消息。

作为一个解决方案，请为部署中的所有 PSN 上的管理员 HTTPS 使用多域 SSL 证书（通常称为统一通信证书 [UCC]）或通配符证书。

## 从 .pfx 文件提取证书和私钥

思科 ISE 不允许导入 .pfx 格式的证书。因此，如果要导入的证书为 .pfx 格式，则必须在导入之前将其转换为 .pem 或 .key 文件格式。

### 开始之前

确保在包含 SSL 证书的服务器中安装了 OpenSSL。

**步骤 1** 从 OpenSSL\bin 文件夹启动 OpenSSL。

**步骤 2** 打开命令提示符并转到包含 .pfx 文件的文件夹。

**步骤 3** 运行以下命令以 .pem 格式提取私钥：**openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes**

系统将提示您键入导入密码。键入创建 .pfx 文件时用于保护密钥对的密码。系统将再次提示您提供新密码以保护正在创建的 .pem 文件。将密钥文件的密码存储在安全的位置，以避免滥用。

**步骤 4** 运行以下命令以 .pem 格式提取证书：**openssl pkcs12 -in certname.pfx -nokeys -out cert.pem**

**步骤 5** 运行以下命令以解密私钥：**openssl rsa -in key.pem -out server.key**

键入您在上一步中创建的用于保护私钥文件的密码。

.pem 文件以及已解密和加密的 .key 文件位于您启动 OpenSSL 的路径中。

## 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。思科 ISE 内部证书颁发机构 (ISE CA) 从集中控制台为终端颁发和管理数字证书，以允许员工在公司网络上使用其个人设备。CA 签名的数字证书被视为行业标准而且更安全。ISE 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 PAN 和 PSN 节点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。

## 简单证书注册协议配置文件

为了帮助用户可在网络上注册的各类移动设备启用证书调配功能，思科 ISE 允许您配置一个或多个简单证书注册协议 (SCEP) 证书颁发机构 (CA) 配置文件（称为思科 ISE 外部 CA 设置），从而使思科 ISE 指向多个 CA 位置。允许多个配置文件的优点在于，可帮助确保高可用性并在您指定的 CA

位置执行负载均衡。如果对特定的 SCEP CA 请求连续三次未获得应答，则思科 ISE 会声明该特定服务器不可用，并会自动移至下一个具有已知最低负载和最少响应次数的 CA，然后即会开始进行定期轮询直至服务器恢复联机。

关于如何设置 Microsoft SCEP 服务器与思科 ISE 互操作的详细信息，请参阅

[http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto\\_60\\_byod\\_certificates.pdf](http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf)。

## 终端证书

管理门户列出了内部 ISE CA 颁发给终端的所有证书（“管理” (Administration) > “系统” (System) > “证书” (Certificates) > “终端证书” (Endpoint Certificates)）。终端证书 (Endpoint Certificates) 页面提供证书状态概览。如果证书已被吊销，可以将鼠标悬停在 Status 列上找出吊销原因。您可以将鼠标悬停在“证书模板” (Certificate Template) 列上查看更多详细信息，如证书的、主题、主题备选名称 (SAN) 和有效期。可以点击终端证书来查看证书。

例如，如果要查看颁发给 user7 的证书，请在出现在 Friendly Name 字段下方的文本框中输入 user7。系统会显示思科 ISE 颁发给此用户的所有证书。从文本框中删除搜索条件可取消筛选。还可以根据各种搜索条件，使用 Advanced Filter 选项查看记录。

此 Endpoint Certificates 页面还为您提供用于在必要时撤销终端证书的选项。

Certificate Management Overview 页面显示部署中每个 PSN 节点颁发的终端证书的总数。还可以查看每个节点的被吊销证书的总数，以及已失败的证书的总数。可以根据任意属性筛选此页面上的数据。



注释 pxGrid 证书不会在终端证书 (Endpoint Certificates) 页面中列出。

## 终端证书概述窗口 (Endpoint Certificate Overview Window)

表 24: 证书管理概述 (Certificate Management Overview)

字段名称	使用指南
<b>Node name</b>	发出证书的策略服务节点 (PSN) 的名称。
<b>Endpoint Certificates Issued</b>	PSN 节点发出的终端证书的数量。
<b>Endpoint Certificates Revoked</b>	已吊销的证书的数量（已由 PSN 节点发出的证书）。
<b>Endpoint Certificates Requests</b>	PSN 节点处理的基于证书的身份验证请求数量。
<b>Endpoint Certificates Failed</b>	PSN 节点处理的失败身份验证请求数量。



注释 已过期或已撤销的证书将在 30 天后自动删除。

#### 相关主题

[终端证书](#)，第 124 页

[用户和终端证书续订](#)，第 119 页

[配置思科 ISE 以使用证书对个人设备进行身份验证](#)，第 128 页

[将思科 ISE 配置为允许用户续订证书](#)，第 120 页

[吊销终端证书](#)，第 138 页

## 思科 ISE CA 证书和密钥的备份与恢复

必须安全地备份思科 ISE CA 证书和密钥，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 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 CA 根链
- 配置思科 ISE 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 CA 根链，然后备份和恢复 ISE CA 证书和密钥。

### 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 OSCP 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 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 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 OSCP 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。

---

## 在主 PAN 和 PSN 上生成根 CA 和从属 CA

设置部署时，思科 ISE 会在主 PAN 上为思科 ISE CA 服务生成根 CA，在 PSN 上生成从属 CA 证书。但是，当更改 PAN 或 PSN 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。

如果您要在 PSN 上更改主机名，而不是分别在 PAN 和 PSN 上重新生成根 CA 和从属 CA，则您可以在更改主机名之前对 PSN 取消注册，然后重新注册。新的辅助证书会在 PSN 上自动调配。

---

**步骤 1** 选择管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书签名请求 (Certificate Signing Requests)

**步骤 2** 点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** 点击替换 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。

---

### 下一步做什么

如果部署中具有辅助 PAN，请从主 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 故障时用作根 CA，您可将辅助 PAN 升级为主 PAN。

---

## 将思科 ISE 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 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，主 PAN 为外部 CA 的从属 CA，PSN 为主 PAN 的从属 CA。

---

**步骤 1** 依次选择管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书签名请求 (Certificate Signing Requests)。

**步骤 2** 点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** 点击生成 (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。

---

### 下一步做什么

如果部署中具有辅助 PAN，请从主 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。然后，服务器和根证书会在辅助 PAN 中自动复制。这可确保在管理节点发生故障切换时，辅助 PAN 可用作外部 PKI 的从属 CA。

## 配置思科 ISE 以使用证书对个人设备进行身份验证

可以配置思科 ISE，为连接到网络的终端（个人设备）发送和管理证书。可以使用内部思科 ISE CA 服务签署来自终端的证书签名请求，或者将 CSR 转发到外部 CA。

### 开始之前

- 从主 PAN 获取思科 ISE CA 证书和密钥备份，将其保存在安全位置，用于灾难恢复目的。
- 如果部署中具有辅助 PAN，请从主 PAN 备份思科 ISE CA 证书和密钥，然后在辅助 PAN 上恢复备份。

---

**步骤 1** 将用户添加到 Employee 用户组，第 129 页。

可以将用户添加到内部身份库或外部身份库，例如 Microsoft Active Directory。

**步骤 2** 为基于 TLS 的身份验证创建证书身份验证配置文件，第 129 页。

**步骤 3** 为基于 TLS 的身份验证创建身份源序列，第 129 页。

**步骤 4** 创建客户端调配策略：

- a) 配置证书颁发机构设置，第 130 页
- b) 创建 CA 模板，第 131 页
- c) 创建要用于客户端调配策略的本地请求方配置文件，第 132 页
- d) 从思科下载适用于 Windows 和 Mac OS X 操作系统的代理资源，第 133 页
- e) 为 Apple iOS、Android 和 MAC OS X 设备创建客户端调配策略规则。，第 133 页

**步骤 5** 为基于 TLS 的身份验证配置 Dot1X 身份验证策略规则，第 134 页

**步骤 6** 为基于 TLS 的身份验证配置授权策略规则。

- a) 为集中式 Web 身份验证和请求方调配流程创建授权配置文件，第 135 页



b) [创建授权策略规则，第 135 页](#)

---

## 将用户添加到 **Employee** 用户组

以下程序介绍如何在思科 ISE 身份库中将用户添加到 **Employee** 用户组。如果使用外部身份库，请确保具有可向其添加用户的 **Employee** 用户组。

**步骤 1** 选择管理 (**Administration**) > 身份管理 (**Identity Management**) > 身份 (**Identities**) > 用户 (**Users**)。

**步骤 2** 点击 **Add**。

**步骤 3** 输入用户详细信息。

**步骤 4** 从 User Group 下拉列表中选择 **Employee**。

属于 **Employee** 用户组的所有用户共享同一组权限。

**步骤 5** 点击提交。

---

下一步做什么

[为基于 TLS 的身份验证创建证书身份验证配置文件，第 129 页](#)

## 为基于 **TLS** 的身份验证创建证书身份验证配置文件

要使用证书对连接到您网络的终端进行身份验证，您必须在思科 ISE 中定义证书身份验证配置文件或编辑默认的 `Preloaded_Certificate_Profile`。证书身份验证配置文件包括应用作主体用户名的证书字段。例如，如果用户名在通用名称字段中，则您可以使用主体用户名定义证书身份验证配置文件，即主题 - 通用名称，该名称可对身份库进行验证。

**步骤 1** 选择管理 (**Administration**) > 身份管理 (**Identity Management**) > 外部身份源 (**External Identity Sources**) > 证书身份验证配置文件 (**Certificate Authentication Profile**)。

**步骤 2** 输入证书身份验证配置文件的名称。例如，CAP。

**步骤 3** 选择主题 - 通用名称作为 **Principal Username X509 Attribute**。

**步骤 4** 点击保存 (**Save**)。

---

下一步做什么

[为基于 TLS 的身份验证创建身份源序列，第 129 页](#)

## 为基于 **TLS** 的身份验证创建身份源序列

在创建证书身份验证配置文件后，必须将其添加到身份源序列，以便思科 ISE 可从证书获取属性并将其与您在身份源序列中定义的身份源进行匹配。

### 开始之前

确保您已完成以下任务：

- 向 Employee 用户组添加用户。
- 为基于证书的身份验证创建证书身份验证配置文件。

**步骤 1** 依次选择 **Administration > Identity Management > Identity Source Sequences**。

**步骤 2** 点击 **Add**。

**步骤 3** 输入身份源序列的名称。例如 Dot1X。

**步骤 4** 选中**选择证书身份验证配置文件 (Select Certificate Authentication Profile)** 复选框，然后选择之前创建的证书身份验证配置文件，即 CAP。

**步骤 5** 将包含您的用户信息的身份源移至 Authentication Search List 区域的 **Selected** 列表框。

您可以添加更多身份源，思科 ISE 会按照顺序搜索这些数据存储区，直到找到匹配项。

**步骤 6** 点击 **Treat as if the user was not found and proceed to the next store in the sequence** 单选按钮。

**步骤 7** 点击**提交**。

### 下一步做什么

[配置证书颁发机构设置，第 130 页](#)

## 配置证书颁发机构设置

如果您计划将外部 CA 用于为证书签名请求 (CSR) 提供签名，则必须配置外部 CA 设置。在以前版本的思科 ISE 中，外部 CA 设置称为 SCEP RA 配置文件。如果您使用的是思科 ISE CA，则不必明确配置 CA 设置。您可以在 Administration > System > Certificates > Internal CA Settings 下查看内部 CA 设置。

用户的设备收到已验证的证书后，会按照下表中的说明驻留于设备上。

表 25: 设备证书位置

设备	证书存储位置	访问方法
iPhone/iPad	标准证书库	Settings > General > Profile
Android	加密证书库	不对最终用户显示。 注释 可以使用 Settings > Location & Security > Clear Storage 选项删除证书。
Windows	标准证书库	从 /cmd 提示符启动 mmc.exe 或在 snap-in 证书中进行查看。

设备	证书存储位置	访问方法
Mac	标准证书库	Application > Utilities > Keychain Access

### 开始之前

如果您计划将外部证书颁发机构用于为证书签名请求 (CSR) 提供签名，您必须拥有外部 CA 的 URL。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 证书 (Certificates) > 外部 CA 设置 (External CA Settings)。

**步骤 2** 点击 Add。

**步骤 3** 为外部 CA 设置输入名称。例如 EXTERNAL\_SCEP。

**步骤 4** 在 URL 文本框中输入外部 CA 服务器 URL。

点击 **Test Connection**，检查是否可以访问外部 CA。点击 + 按钮以添加更多 CA 服务器 URL。

**步骤 5** 点击提交。

### 下一步做什么

[创建 CA 模板，第 131 页](#)

## 创建 CA 模板

证书模板定义必须（用于内部或外部 CA）的 SCEP RA 配置文件、使用者、使用者备选名称 (SAN)、证书有效期和扩展密钥用法。此示例假定您即将使用内部思科 ISE CA。对于外部 CA 模板，有效期由外部 CA 确定，而您无法指定有效期。

您可以创建新的 CA 模板或编辑默认证书模板 EAP\_Authentication\_Certificate\_Template。

### 开始之前

确保您已配置 CA 设置。

**步骤 1** 选择管理 (Administration) > 系统 (System) > CA 服务 (CA Service) > 内部 CA 证书模板 (Internal CA Certificate Template)。

**步骤 2** 输入内部 CA 模板的名称。例如 Internal\_CA\_Template。

**步骤 3** （可选）输入“组织单位” (Organizational Unit)、 “企业” (Organization)、 “城市” (City)、 “省” (State) 和 “国家/地区” (Country) 字段的值。

在证书模板字段（“组织单位” [Organizational Unit]、 “企业” [Organization]、 “城市” [City]、 “省” [State] 和 “国家/地区” [Country]）中不支持 UTF-8 字符。如果在证书模板中使用 UTF-8 字符，则证书调配将会失败。

生成证书的内部用户的用户名用作证书的通用名称。思科 ISE 内部 CA 的“通用名称” (Common Name) 字段不支持 “+” 或 “\*” 字符。确保用户名不包含特殊字符 “+” 或 “\*”。

**步骤 4** 指定使用者备选名称 (SAN) 和证书的有效期。

**步骤 5** 指定密钥大小。您必须选择 1024 或更高的密钥大小。

**步骤 6** 指定扩展密钥用法。如果要证书用于客户端身份验证，选中**客户端验证 (Client Authentication)** 复选框。如果要证书用于服务器身份验证，选中**服务器身份验证 (Server Authentication)** 复选框。

**步骤 7** 点击**提交 (Submit)**。

系统将创建内部 CA 证书模板并供内部客户端调配策略使用。

下一步做什么

[创建要用于客户端调配策略的本地请求方配置文件，第 132 页](#)

## 内部 CA 设置

表 26: 内部 CA 设置

字段名称	使用指南
<b>Disable Certificate Authority</b>	点击此按钮以禁用内部 CA 服务。
主机名	运行 CA 服务的思科 ISE 节点的主机名。
相关角色	在运行 CA 服务的节点上启用的思科 ISE 节点角色。例如管理角色、策略服务角色等。
<b>Role(s)</b>	运行 CA 服务的思科 ISE 节点承担的职责。例如，独立、主要或辅助职责。
<b>CA &amp; OCSP Responder Status</b>	启用或禁用
<b>OCSP Responder URL</b>	思科 ISE 节点用于访问 OCSP 服务器的 URL。

相关主题

[思科 ISE CA 服务，第 123 页](#)

[配置思科 ISE 以使用证书对个人设备进行身份验证，第 128 页](#)

## 创建要用于客户端调配策略的本地请求方配置文件

可以创建本地请求方配置文件，使用户能够将个人设备带入公司网络。思科 ISE 对不同的操作系统使用不同的策略规则。每个客户端调配策略规则都包含一个本地请求方配置文件，其指定针对哪个操作系统而使用哪个调配向导。

开始之前

- 在思科 ISE 中配置 CA 证书模板。
- 打开 TCP 端口 8905 和 UDP 端口 8905 以启用客户端代理和请求方调配向导的安装。有关端口用法的详细信息，请参阅《思科身份服务引擎硬件安装指南》中的“思科 ISE 设备端口参考”附录。

- 
- 步骤 1 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources)。
  - 步骤 2 选择添加 (Add) > 本地请求方配置文件 (Native Supplicant Profile)。
  - 步骤 3 输入本地请求方配置文件的名称。例如 EAP\_TLS\_INTERNAL。
  - 步骤 4 从操作系统 (Operating System) 下拉列表中选择“全部” (ALL)。
  - 步骤 5 选中有线 (Wired) 或无线 (Wireless) 复选框。
  - 步骤 6 从允许协议 (Allowed Protocol) 下拉列表中选择 TLS。
  - 步骤 7 选择之前创建的 CA 证书模板。
  - 步骤 8 点击提交。
- 

#### 下一步做什么

[从思科下载适用于 Windows 和 Mac OS X 操作系统的代理资源，第 133 页](#)

## 从思科下载适用于 Windows 和 Mac OS X 操作系统的代理资源

对于 Windows 和 Mac OS X 操作系统，您必须从思科站点下载远程资源。

#### 开始之前

验证是否已为您的网络正确配置代理设置，确保能够访问相应的远程位置以将客户端调配资源下载至思科 ISE。

- 
- 步骤 1 选择策略 (Policy) > 策略元素 (Policy Elements) > 资源 (Resources) > 客户端调配 (Client Provisioning) > 资源 (Resources)。
  - 步骤 2 选择添加 (Add) > 思科站点的代理资源 (Agent resources from Cisco site)。
  - 步骤 3 选中 Windows 和 MAC OS X 包旁边的复选框。确保包含最新的版本。
  - 步骤 4 点击保存 (Save)。
- 

#### 下一步做什么

[为 Apple iOS、Android 和 MAC OS X 设备创建客户端调配策略规则。》，第 133 页](#)

## 为 Apple iOS、Android 和 MAC OS X 设备创建客户端调配策略规则。

客户端调配资源策略可确定哪些用户会在登录和用户会话启动后从思科 ISE 收到什么版本的资源（代理、代理合规性模块和代理自定义包/配置文件）。

当您下载代理合规性模块时，它始终会覆盖系统中可用的现有模块（如果有）。

要允许员工携带 iOS、Android、MAC OS X 设备，必须在“客户端调配策略”页面为上述每一种设备创建策略规则。

#### 开始之前

您必须已经配置了所需的本地请求方配置文件并已从 Client Provisioning Policy 页面下载了所需的代理。

---

**步骤 1** 选择策略 (Policy) > 客户端调配 (Client Provisioning)。

**步骤 2** 为 Apple iOS、Android 和 MAC OS X 设备创建客户端调配策略规则。

**步骤 3** 点击保存 (Save)。

---

#### 下一步做什么

[为基于 TLS 的身份验证配置 Dot1X 身份验证策略规则，第 134 页](#)

## 为基于 TLS 的身份验证配置 Dot1X 身份验证策略规则

您必须为基于 TLS 的身份验证更新 Dot1X 身份验证策略规则。

#### 开始之前

确保您已为基于 TLS 的身份验证创建证书身份验证配置文件。

---

**步骤 1** 依次选择 **Policy > Authentication**。

**步骤 2** 点击 Rule-Based 单选按钮。

默认基于规则的身份验证策略包括一条适用于 Dot1X 身份验证的规则。

**步骤 3** 编辑此 Dot1X 身份验证策略规则。

**步骤 4** 从 Dot1X 策略规则下，依次选择 **Actions > Insert new row above**。

**步骤 5** 为规则输入名称。例如，eap-tls。

**步骤 6** 使用表达式生成器创建以下策略条件：如果 Network Access:EapAuthentication 等于 EAP-TLS，则使用您之前创建的证书身份验证配置文件。

**步骤 7** 保留默认规则。

**步骤 8** 点击保存 (Save)。

---

#### 下一步做什么

[为集中式 Web 身份验证和请求方调配流程创建授权配置文件，第 135 页](#)

## 为集中式 Web 身份验证和请求方调配流程创建授权配置文件

必须定义授权配置文件以确定在基于证书的身份验证成功后必须授予用户的访问权限。

### 开始之前

确保已在无线 LAN 控制器 (WLC) 上配置所需的访问控制列表 (ACL)。有关如何在 WLC 上创建 ACL 的信息，请参阅《TrustSec 操作指南：将证书用于差异化访问》。

本示例假定已在 WLC 上创建以下 ACL。

- NSP-ACL - 适用于本地请求方调配
- BLACKHOLE - 适用于限制对列入阻止列表的设备的访问
- NSP-ACL-Google - 适用于调配 Android 设备

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles)。

**步骤 2** 点击 **Add** 以创建新的授权配置文件。

**步骤 3** 为授权配置文件输入名称。

**步骤 4** 从 **Access Type** 下拉列表中选择 ACCESS\_ACCEPT。

**步骤 5** 点击 **Add**，为集中式 Web 身份验证、适用于 Google Play 的集中式 Web 身份验证、本地请求方调配和适用于 Google 的本地请求方调配添加授权配置文件。

**步骤 6** 点击保存 (Save)。

---

### 下一步做什么

[创建授权策略规则，第 135 页](#)

## 创建授权策略规则

思科 ISE 评估授权策略规则并授予对基于策略规则中指定的授权配置文件的网络资源的用户访问权限。

### 开始之前

确保已创建所需的授权配置文件。

---

**步骤 1** 依次选择策略 (Policy) > 授权 (Authorization)。

**步骤 2** 请在默认规则之上插入其他策略规则。

**步骤 3** 点击保存 (Save)。

---

## CA 服务策略参考

本节提供您在启用思科 ISE CA 服务之前必须创建的授权和客户端调配策略规则的参考信息。

### 证书服务的客户端调配策略规则

本节将列出在使用思科 ISE 证书服务时，您必须创建的客户端调配策略规则。下表将提供详细信息。

规则名称	身份组	操作系统	其他条件	结果
iOS	任意	Apple iOS 全部	条件	EAP_TLS_INTERNAL (较早创建的本地请求方配置文件)。如要使用外部 CA，请选择您已经为外部 CA 创建的本地请求方配置文件。
Android	任意	Android	条件	EAP_TLS_INTERNAL (较早创建的本地请求方配置文件)。如要使用外部 CA，请选择您已经为外部 CA 创建的本地请求方配置文件。
Mac OS X	任意	MACOSX	条件	在本地请求方配置下，指定以下项目：  <ol style="list-style-type: none"> <li>1. 配置向导：选择您从思科网站上下载的 MAC OS X 请求方向导。</li> <li>2. 向导配置文件：选择您较早创建的 EAP_TLS_INTERNAL 本地请求方配置文件。如要使用外部 CA，请选择您已经为外部 CA 创建的本地请求方配置文件。</li> </ol>



## 证书服务的授权配置文件

本节列出您在思科 ISE 中启用基于证书的身份验证时必须创建的授权配置文件。您必须已在无线 LAN 控制器 (WLC) 上创建 ACL (NSP-ACL 和 NSP-ACL-Google)。

- CWA - 此配置文件用于完成集中式 Web 身份验证流程的设备。选中 **Web Authentication** 复选框，从下拉列表中选择 **Centralized**，然后在 ACL 文本字段中输入 NSP-ACL。
- CWA\_GooglePlay - 此配置文件用于完成集中式 Web 身份验证流程的 Android 设备。此配置文件使 Android 设备能够访问 Google Play 商店并下载思科网络设置助理。选中 **Web Authentication** 复选框，从下拉列表中选择 **Centralized**，然后在 ACL 文本框中输入 NSP-ACL-Google。
- NSP - 此配置文件用于完成请求方调配流程的非 Android 设备。选中 **Web Authentication** 复选框，从下拉列表中选择 **Supplicant Provisioning**，然后在 ACL 文本框中输入 NSP-ACL。
- NSP Google - 此配置文件用于完成请求方调配流程的 Android 设备。选中 **Web Authentication** 复选框，从下拉列表中选择 **Supplicant Provisioning**，然后在 ACL 文本框中输入 NSP-ACL-Google。

查看默认 Blackhole\_Wireless\_Access 授权配置文件。Advanced Attributes Settings 应为如下所示：

- Cisco:cisco-av-pair = url-redirect=https://ip:port/blacklistportal/gateway?portal=PortalID
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

## 证书服务的授权策略规则

本节列出您在启用思科 ISE CA 服务时必须创建的授权策略规则。

- Corporate Assets - 此规则适用于使用 802.1X 和 MSCHAPV2 协议连接到公司无线 SSID 的公司设备。
- Android\_SingleSSID - 此规则适用于访问 Google Play Store 以下载思科网络设置助理进行调配的 Android 设备。此规则专门针对单一 SSID 设置。
- Android\_DualSSID - 此规则适用于访问 Google Play Store 以下载思科网络设置助理进行调配的 Android 设备。此规则专门针对双 SSID 设置。
- CWA - 此规则适用于需要完成集中式 Web 身份验证流程的设备。
- NSP - 此规则适用于需要通过使用证书进行 EAP-TLS 身份验证来完成本地请求方调配流程的设备。
- EAP-TLS - 此规则适用于已完成请求方调配流程并使用证书调配的设备。系统将向设备授予访问网络的权限。

下表列出您在配置适用于思科 ISE CA 服务的授权策略规则时必须选择的属性和值。本示例假设您在思科 ISE 中已配置相应的授权配置文件。

规则名称	条件	权限（要应用的授权配置文件）
Corporate Assets	Corp_Assets AND (Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	PermitAccess

规则名称	条件	权限（要应用的授权配置文件）
Android_SingleSSID	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	NSP_Google
Android_DualSSID	(Wireless_MAB AND Session:Device-OS EQUALS Android)	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	NSP
EAP-TLS	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI)	PermitAccess

## 吊销终端证书

如果您需要吊销向员工个人设备颁发的证书，您可以从终端证书 (Endpoint Certificates) 页面进行吊销。例如，如果员工的设备被盗或丢失，您可以登录思科 ISE Admin 门户，然后从终端证书 (Endpoint Certificates) 页面吊销颁发给该设备的证书。在此页面上，您可以根据友好名称 (Friendly Name)、设备唯一 Id (Device Unique Id) 或序列号 (Serial Number) 过滤数据。

如果 PSN（子 CA）已被破坏，您可以通过从终端证书 (Endpoint Certificates) 页面过滤 Issued By 字段，吊销 PSN 颁发的所有证书。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书颁发机构 (Certificate Authority) > 已颁发的证书 (Issued Certificates)。

**步骤 2** 选中您要吊销的终端证书旁边的复选框，然后点击吊销 (Revoke)。

您可以根据友好名称 (Friendly Name) 和设备类型 (Device Type) 搜索证书。

**步骤 3** 输入吊销证书的原因。

**步骤 4** 点击 Yes。

## 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 port number>
```

**步骤 1** 选择 **管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书管理 (Certificate Management) > 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** 点击提交。

## OCSP 客户端配置文件设置

表 27: OCSP 客户端配置文件设置

字段名称	使用指南
<b>Name</b>	OCSP 客户端配置文件的名称。
说明	输入可选的说明。
启用辅助服务器	选中此复选框来以启用高可用性辅助 OCSP 服务器。
总是先访问主服务器	使用此选项以在尝试移至辅助服务器之前先检查主要服务器。即使之前已检查主要服务器并且发现主服务器无响应，思科 ISE 在移至辅助服务器之前仍会尝试向主要服务器发送请求。
在 <i>n</i> 分钟后回退至主服务器	当您希望思科 ISE 移至辅助服务器，然后再回退到主服务器时，请使用此选项。在这种情况下，系统将跳过所有其他请求，并按照该文本框中配置的时间使用辅助服务器。允许的时间范围是 1 至 999 分钟。
<b>URL</b>	输入主要和/或辅助 OCSP 服务器的 URL。
启用 Nonce 扩展支持	您可以配置一个作为 OCSP 请求的一部分发送的 Nonce。Nonce 会在 OCSP 请求中包含一个伪随机数。系统会验证在响应中接收的数值是否与请求中包含的此数相同。此选项可确保重放攻击无法利用旧通信数据。

字段名称	使用指南
验证响应签名	<p>OCSP 响应器用以下一个证书为响应签名：</p> <ul style="list-style-type: none"> <li>• CA 证书</li> <li>• 与 CA 证书不同的证书</li> </ul> <p>为了使思科 ISE 验证响应签名，OCSP 响应器需要连同该证书一起发送响应，否则响应验证会失败，而且证书状态不可靠。根据 RFC，OCSP 可以使用不同的证书给响应签名。只要 OCSP 发送给响应签名的证书以供思科 ISE 进行验证，就会如此。如果 OCSP 使用思科 ISE 中未配置的其他证书给响应签名，响应验证将失败。</p>
缓存条目生存时间 $n$ 分钟 (Cache Entry Time To Live $n$ Minutes)	<p>以分钟为单位输入缓存项目在多长时间之后过期。来自 OCSP 服务器的每个响应都有一个 <code>nextUpdate</code> 值。此值显示服务器上接下来将于何时更新证书的状态。缓存 OCSP 响应时，系统会比较两个值（一个是来自配置的值，另一个是来自响应的值），系统会按照这两个值中最低的值将响应缓存相应的时间。如果 <code>nextUpdate</code> 值为 0，则根本不缓存响应。思科 ISE 将 OCSP 响应缓存所配置的时间。缓存不复制，也不是持久性的，所以当思科 ISE 重新启动时，系统会清除缓存。使用 OCSP 缓存是为了保持 OCSP 响应以及出于以下原因：</p> <ul style="list-style-type: none"> <li>• 减少网络流量和降低 OCSP 服务器对已知证书带来的负载</li> <li>• 通过缓存已知证书状态提高思科 ISE 性能</li> </ul>
清除缓存	<p>点击 <a href="#">清除缓存</a> 以清除连接至 OCSP 服务的所有证书颁发机构的条目。</p> <p>在部署中，<a href="#">清楚缓存</a> 与所有节点交互并执行此操作。此机制可更新部署中的每个节点。</p>

#### 相关主题

[OCSP 服务](#)，第 138 页

[思科 ISE CA 服务在线证书状态协议响应器](#)，第 139 页

[OCSP 证书状态值](#)，第 139 页

[OCSP 高可用性](#)，第 140 页

[OCSP 故障](#)，第 140 页

[OCSP 统计计数器](#)，第 143 页

[添加 OCSP 客户端配置文件](#)，第 140 页

## 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 28: 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
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

## 配置管理员访问策略

RBAC 策略以 if-then 的格式表示，其中 if 是 RBAC Admin Group 的值，then 是 RBAC Permissions 的值。

RBAC 策略窗口（**管理 (Administration)** > **系统 (System)** > **管理访问 (Admin Access)** > **授权 (Authorization)**）包含默认策略列表。您无法编辑或删除这些默认策略。通过 RBAC 策略页面，还可以为工作场所的专门管理员组创建自定义 RBAC 策略，并将其应用于个性化管理员组。

分配有限菜单访问权限时，请确保数据访问权限允许管理员访问使用指定菜单时所必需的数据。例如，如果给予对 MyDevices 门户的菜单访问权限，但不允许对终端身份组进行数据访问，则该管理员无法修改该门户。



**注释** 管理员用户可以将终端 MAC 地址从他们拥有只读访问权限的终端身份组移动到他们拥有完全访问权限的终端身份组。反之则不可能。

### 开始之前

- 创建要为其定义基于角色的访问控制 (RBAC) 策略的所有管理员组。
- 确保这些管理员组映射到各对应的管理员用户。
- 确保您已配置 RBAC 权限，例如菜单访问和数据访问权限。

**步骤 1** 选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **授权 (Authorization)** > **策略 (Policy)**。

RBAC Policies 页面包含一系列适用于默认管理员组的现成的预定义策略。您无法编辑或删除这些默认策略。

**步骤 2** 点击任意默认 RBAC 策略规则旁边的 **Actions**。

在这里，您可以插入新的 RBAC 策略，复制现有 RBAC 策略和删除现有 RBAC 策略。

**步骤 3** 点击 **Insert new policy**。

**步骤 4** 为 Rule Name、RBAC Group(s) 和 Permissions 字段输入相应值。

在创建 RBAC 策略时，您不能选择多个菜单访问和数据访问权限。

**步骤 5** 点击**保存 (Save)**。



## 管理员访问设置

思科 ISE 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 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 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。但是，您无法为单个管理员帐户配置最大并发会话数。

### 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** 选择管理 (**Administration**) > 系统 (**System**) > 管理员访问权限 (**Admin Access**) > 设置 (**Settings**) > 访问权限 (**Access**) > 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 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 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** 点击保存。

---

### 相关主题

[允许从“选择 IP 地址” \(Select IP Addresses\) 对思科 ISE 进行管理访问](#)，第 145 页

## 允许从“选择 IP 地址” (Select IP Addresses) 对思科 ISE 进行管理访问

思科 ISE 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 管理界面。

管理员访问控制设置仅适用于承担管理、策略服务或监控角色的思科 ISE 节点。这些限制会从主要节点复制到辅助节点。这些限制不适用于 Inline Posture 节点。

### 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** 选择 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 设置 (Settings) > 访问 (Access) > IP 访问 (IP Access)**。

**步骤 2** 点击仅允许列出的 IP 地址进行连接 (**Allow only Listed IP addresses to Connect**) 单选按钮。

**步骤 3** 在配置访问限制的 IP 列表 (**Configure IP List for Access Restriction**) 区域中，点击添加 (**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。您可以为一个思科 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** 点击确定 (**OK**)。

重复步骤 4-7 在此列表中添加更多 IP 地址范围。

**步骤 7** 点击保存 (**Save**) 保存所做的更改。

**步骤 8** 点击重置 (**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 还允许您为管理员帐户创建密码策略，以增强安全性。您可以定义是否需要基于密码或基于客户端证书的管理员身份验证。您在此处定义的密码策略将应用于思科 ISE 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 支持包含 UTF-8 字符的管理员密码。

### 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** 选择 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 身份验证 (Authentication)**。

**步骤 2** 点击以下身份验证方式之一的单选按钮：

- **基于密码 (Password Based)**：选择此选项可使用标准用户 ID 和密码凭证进行管理员登录。从身份源 (**Identity Source**) 下拉列表中选择内部 (**Internal**) 或外部 (**External**)。

**注释** 如果您已配置外部身份源（例如 LDAP）并且想要使用该身份源作为向管理员用户授予访问权限的身份验证源，则必须从 Identity Source 列表框中选择该特定身份源。

- **基于客户端证书 (Client Certificate Based):** 选择此选项以指定基于证书的策略。从证书身份验证配置文件 (Certificate Authentication Profile) 下拉列表中，选择现有的身份验证配置文件。从身份源 (Identity Source) 下拉列表中选择所需的值。

**步骤 3** 点击**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 4** 点击**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。

---

#### 相关主题

[管理员密码策略设置](#)，第 46 页  
[为管理员帐户配置帐户禁用策略](#)

## 配置管理员会话超时

在思科 ISE 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 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 管理员门户。

#### 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** 选择**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **设置 (Settings)** > **会话 (Session)** > **会话超时 (Session Timeout)**。

**步骤 2** 输入思科 ISE 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** 点击**保存 (Save)**。

---

## 终止活动管理会话

思科 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员可以登录并阻止某些会话。

#### 开始之前

要执行以下任务，您必须是超级管理员。

步骤 1 选择管理 (Administration) > 系统(System) > 管理员访问权限 (Admin Access) > 设置 (Settings) > 会话 (Session) > 会话信息 (Session Info)。

步骤 2 选中要终止的会话 ID 旁边的复选框，然后点击失效 (Invalidate)。

## 更改管理员名称

思科 ISE 允许您从思科 ISE GUI 更改用户名。

### 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 登录思科 ISE 管理门户。

步骤 2 单击思科 ISE GUI 右上角的齿轮图标 (⚙️)，然后从下拉列表中选择帐户设置 (Account Settings)。

步骤 3 在显示的管理员用户 (Admin User) 对话框中输入新用户名。

步骤 4 编辑有关要更改的帐户的任何其他详细信息。

步骤 5 点击保存 (Save)。

## 管理员访问设置

您可以通过这些部分来为管理员配置访问设置。

### 管理员密码策略设置

下表介绍了密码策略 (Password Policy) 选项卡中的字段，可以使用此选项卡来定义管理员密码应满足的条件。此窗口的导航路径为：管理 (Administration) > 系统 (System) > 管理员访问权限 (Admin Access) > 身份验证 (Authentication) > 密码策略 (Password Policy)。。

表 29: 管理员密码策略设置

字段名称	使用指南
最小长度 (Minimum Length)	指定密码的最小长度（以字符数为单位）。默认值为 6 个字符。
密码不可包含管理员姓名或其反向顺序的字符	选中此复选框可限制使用管理员用户名或其反向顺序的字符。

字段名称	使用指南
密码不可包含“cisco”或其反向顺序的字符	选中此复选框可限制使用字词“cisco”或其反向顺序的字符。
密码不可包含_____或其反向顺序的字符	选中此复选框可限制使用您定义的任何字词或其反向顺序的字符。
密码不可包含连续重复四次或以上的字符	选中此复选框可限制使用连续重复四次或以上的字符。
必用字符	指定管理员密码必须包含从以下选项中选择的地类型的至少一个字符： <ul style="list-style-type: none"> <li>• 小写字母字符</li> <li>• 大写字母字符</li> <li>• 数字字符</li> <li>• 非字母数字字符</li> </ul>
密码历史记录 (Password History)	指定必须与新密码不同的先前密码的数量，以防止重复使用同一密码。 此外，指定必须与先前密码不同的字符的数量。 输入在其之前不能重复使用密码的天数。
“密码有效期” (Password Lifetime)	指定以下选项来强制用户在经过指定时间段后更改密码： <ul style="list-style-type: none"> <li>• “如果此时间（按天计）过后未更改密码，则禁用管理员帐户。” (Time (in days) before the administrator account is disabled if the password is not changed.) （允许的范围是 0 至 2147483647 天。）</li> <li>• “禁用管理员帐户之前的提醒时间（按天计）。” (Reminder (in days) before the administrator account is disabled.)</li> </ul>
“不正确的登录尝试之后锁定或暂停帐户” (Lock or Suspend Account with Incorrect Login Attempts)	指定思科 ISE 在将管理员锁定以及暂停或禁用帐户凭证之前记录错误管理员密码的次数。 系统会向其帐户已锁定的管理员发送邮件。您可以输入自定义邮件补救消息。

#### 相关主题

[思科 ISE 管理员](#)，第 9 页

[创建新管理员](#)，第 10 页

## 会话超时和会话信息设置

下表介绍会话 (Session) 窗口中的字段，您可以使用此窗口定义会话超时和终止活动管理会话。此窗口的导航路径为：**管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 设置 (Settings) > 会话 (Session)**。

表 30: 会话超时和会话信息设置

字段名称	使用指南
会话超时	
会话空闲超时 (Session Idle Timeout)	输入思科 ISE 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。
会话信息	
失效 (Invalidate)	选中要终止的会话 ID 旁边的复选框，然后单击失效 (Invalidate)。

### 相关主题

[管理员访问设置](#)，第 145 页

[配置管理员会话超时](#)，第 147 页

[终止活动管理会话](#)，第 147 页



## 第 6 章

# 维护和监控

- , 第 152 页
- 在思科 ISE 中启用 , 第 152 页
- 配置网络访问设置 , 第 153 页
- 隔离和取消隔离流程 , 第 154 页
- NAS 端口关闭流程 , 第 155 页
- 终端清除设置 , 第 156 页
- 隔离的终端在策略更改后不会重新进行身份验证 , 第 157 页
- 当无法找到 IP 地址或 MAC 地址时 , 操作失败。 , 第 157 页
- 通过外部身份验证的管理员无法执行操作 , 第 158 页
- 备份数据类型 , 第 158 页
- 备份和恢复存储库 , 第 158 页
- 按需备份和计划备份 , 第 160 页
- 思科 ISE 恢复操作 , 第 165 页
- 导出身份验证和授权策略配置 , 第 171 页
- 在分布式环境中同步主节点和辅助节点 , 第 171 页
- 恢复独立和分布式部署中断开的节点 , 第 172 页
- 思科 日志记录机制 , 第 175 页
- 思科 ISE 系统日志 , 第 176 页
- 配置远程系统日志收集位置 , 第 177 页
- 思科 ISE 消息代码 , 第 178 页
- 思科 ISE 消息目录 , 第 179 页
- 调试日志 , 第 179 页
- 终端调试日志收集器 , 第 180 页
- 集合过滤器 , 第 181 页
- 思科 ISE 报告 , 第 182 页
- 运行并查看报告 , 第 182 页
- 报告导航 , 第 183 页
- 导出报告 , 第 183 页
- 我的报告 , 第 184 页

- 安排思科 ISE 报告，第 185 页
- 添加收藏的报告，第 187 页
- 思科 ISE 活动 RADIUS 会话，第 187 页
- 可用报告，第 189 页

是一项在管理节点上运行的服务。此服务可监控和控制终端的网络访问。由 ISE 管理员在管理 GUI 上调用，也可以通过 pxGrid 从第三方系统调用。支持有线和无线部署，并且需要 Plus 许可证。

您可以使用更改授权状态，无需修改系统的总体授权策略。允许您在隔离终端时设置授权状态。结果会建立授权策略，这些授权策略定义为检查 EPSSatus 以限制或拒绝网络访问。您可以取消隔离终端，使其获得完整的网络访问权限。您也可以关闭网络连接系统 (NAS) 上的端口，断开终端与网络之间的连接。

一次可以隔离的用户数量没有限制。此外，隔离期长度没有时间限制。

您可以执行以下操作，以便通过 监控和控制网络访问：

- 隔离：允许您使用例外策略（授权策略）限制或拒绝终端接入网络。必须创建例外策略，以根据 EPSSatus 分配不同的授权配置文件（权限）。设置为隔离状态，本质上是将其终端从其默认 VLAN 迁移到指定的隔离 VLAN。您必须提前定义隔离 VLAN，在同一 NAS 上作为终端获得支持。
- 取消隔离：允许您解除隔离状态，让终端获得完整的网络访问权限。这是通过使终端返回原 VLAN 实现的。
- 关闭：允许您禁用 NAS 上的端口，断开终端与网络之间的连接。当终端连接的 NAS 上的端口关闭后，应重新手动重置 NAS 上的端口。这可以让终端连接到网络（不适用于无线部署）。

隔离和取消隔离操作可以从活动终端的会话目录报告触发。



**注释** 如果取消隔离已隔离的会话，新取消隔离的会话的发起方法将取决于交换机配置指定的身份验证方法。

## 在思科 ISE 中启用

默认情况下禁用。您必须在管理员门户中手动启用 服务。

您必须拥有超级管理员和策略管理员角色权限才能在思科 ISE 中启用。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 设置 (Settings)。

**步骤 2** 点击 Service Status 下拉列表，然后选择 **Enabled**。

**步骤 3** 点击保存 (Save)。



## 配置网络访问设置

可以让您重置终端的网络访问状态，以便对端口进行隔离、取消隔离或关闭端口。这些定义了网络中终端的授权程度。

您可以使用终端 IP 地址或 MAC 地址隔离或取消隔离终端抑或关闭终端所连接的网络访问服务器 (NAS) 端口。您可以在同一终端上多次执行隔离和取消隔离操作，但不能同时执行这两种操作。如果在网络上发现恶意终端，可以使用 关闭 NAS 端口，从而禁止终端访问。

### 开始之前

- 启用。
- 为 创建授权配置文件和例外类型授权策略。

---

**步骤 1** 选择操作 (Operations)。

**步骤 2** 在策略列表 (Policy List) 窗口中，输入终端的 IP 地址或 MAC 地址。

**步骤 3** 点击操作 (Action) 下拉列表，选择以下操作之一：

- 隔离 (Quarantine) - 隔离终端，限制其在网络上的访问。
- 取消隔离 (Unquarantine) - 取消隔离进程，允许完全访问网络。
- 关闭 (Shutdown) - 关闭终端连接的 NAS 端口。

**步骤 4** 点击提交。

---

## 通过创建网络访问的授权配置文件

您必须创建一个应该与 配合使用的授权配置文件。您可以在标准授权配置文件列表中查看该授权配置文件。终端可在网络中进行身份验证和授权，但是限于接入网络。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles)。

**步骤 2** 点击添加 (Add)。

**步骤 3** 为授权配置文件输入唯一名称和说明，并将访问类型 (Access Type) 更新为 ACCESS\_ACCEPT。

**步骤 4** 选中 DACL Name 复选框，然后从下拉列表中选择 DENY\_ALL\_TRAFFIC。

**步骤 5** 点击 Submit。

---

## 通过 为网络访问创建例外策略

对于授权，应创建隔离例外策略，该策略先于所有标准授权策略进行处理。例外授权策略用于授权有限访问，满足特殊条件或权限或直接要求。标准授权策略应当保持稳定，适用于大型用户组、设备组以及共享一套常用权限的组。

### 开始之前

已创建标准授权配置文件以与 配合使用。

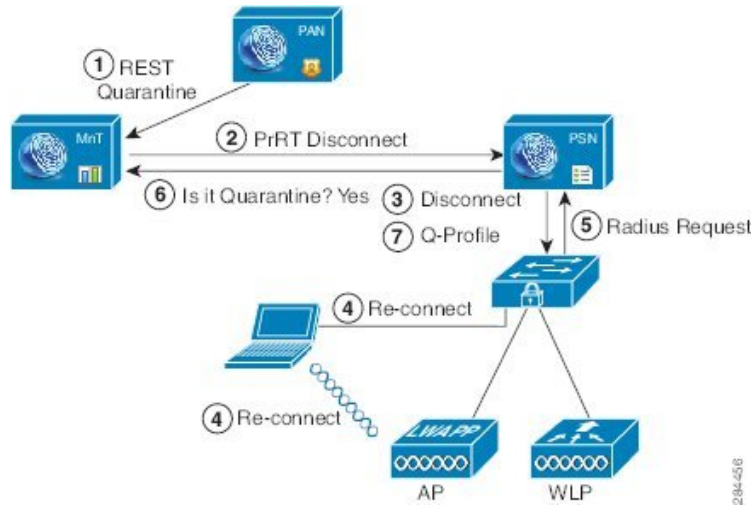
- 步骤 1** 选择策略 (Policy) > 授权 (Authorization)，然后展开例外 (Exceptions)。
- 步骤 2** 选择启用 (Enabled) 或禁用 (Disabled) 或监控唯一选项 (Monitor Only option)。
- 步骤 3** 点击创建新规则 (Create a New Rule)。
- 步骤 4** 输入例外规则名称。
- 步骤 5** 点击加号 [+]，选择身份组。
- 步骤 6** 点击加号 [+]，选择创建新条件（高级选项）(Create New Condition (Advanced Option))。
- 步骤 7** 点击第一个字段中的向下箭头，显示字典列表，依次选择会话 (Session) > EPSStatus。
- 步骤 8** 从第二个字段中的下拉列表选择等于 (Equals)。
- 步骤 9** 从第三个字段中的下拉列表选择隔离 (Quarantine)。
- 步骤 10** 点击保存 (Save)。

## 隔离和取消隔离流程

可以使用 隔离所选终端，以限制其对网络的访问。您可以隔离终端并建立根据状态分配不同授权配置文件的例外授权策略。授权配置文件用作您在授权策略中定义的允许访问指定网络服务的权限的容器。当授权完成时，系统会为网络访问请求授予权限。如果之后对终端进行了验证，则可以对终端取消隔离以允许其对网络进行完全访问。

此图显示了隔离流程，它假定已配置授权规则并已建立 会话。

图 7: 隔离流程



1. 客户端设备通过无线设备 (WLC) 登录到网络，并且系统会从管理节点 (PAP) 向监控节点 (MnT) 发出隔离 REST API 调用。
2. 然后，监控节点会通过策略服务思科 ISE 节点 (PDP) 来调用 PrRT，从而引发授权证书 (CoA)。
3. 客户端设备的连接会断开。
4. 然后，客户端设备会重新进行身份验证并重新连接。
5. 对客户端设备的 RADIUS 请求会发回到监控节点。
6. 在进行检查时，系统将隔离客户端设备。
7. 系统将应用 Q-Profile 授权策略并验证客户端设备。
8. 系统会对客户端设备取消隔离，并向其提供对网络的完全访问权限。

## NAS 端口关闭流程

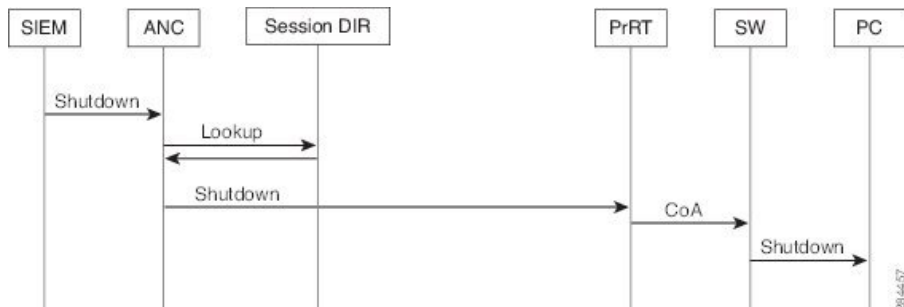
您可以使用终端 IP 地址或 MAC 地址关闭终端所连接的 NAS 端口。

通过此关闭功能您可以根据 MAC 地址的指定 IP 地址关闭 NAS 端口。您必须手动恢复该端口，才能将此终端重新接入网络，这仅对通过有线媒介连接的终端有效。

并非所有设备都支持此关闭功能。不过，大多数交换机应该都支持关闭命令。您可以使用 `getResult()` 命令验证关闭是否执行成功。

下图说明 关闭流程。对于客户端设备，关闭操作是在客户端设备用于访问网络的 NAS 上执行的。

图 8: 关闭流程



## 终端清除设置

可以根据身份组和其他条件，通过配置规则来定义终端清除策略。选择**管理 (Administration) > 身份管理 (Identity Management) > 设置 (Settings) > 终端清除 (Endpoint Purge)**。您可以选择不清除特定终端以及根据选择的分析条件清除终端。

您可以安排终端清除作业计划。默认情况下，此终端清除计划处于启用状态。默认情况下，思科ISE会删除超出 30 天的终端和已注册设备。系统根据主 PAN 中配置的时区于每日凌晨 1 点（午夜）执行清除作业。

终端清除作业每 3 分钟删除 5000 多个终端。

以下是您可以用于清除终端的一些条件以及示例：

- **InactivityDays** - 距离终端上最后一次分析活动或更新的天数
  - 此条件用于清除随时间推移累积的陈旧设备，通常是临时访客或个人设备或废弃的设备。在您的部署中，这些终端容易形成干扰，因为它们在网上不再活动或近期不再可能出现。如果它们偶然再进行连接，系统将在必要的情况下对其进行发现、分析、注册等。
  - 当存在来自终端的更新时，只要启用分析功能，**InactivityDays** 便会重置为 0。
- **ElapsedDays** - 创建对象之后经过的天数。
  - 此条件适用于获得特定时间段内未经身份验证或有条件的访问权限的终端，例如访客或承包商终端，或利用 **webauth** 进行网络访问的员工。在所允许的连接期限到期之后，他们必须重新进行完全身份验证和注册。
- **PurgeDate** - 要清除终端的日期。
  - 此选项用于在不考虑创建或开始时间的情况下，获得特定时间的访问权限的特殊事件或组。此选项允许同时清除所有终端。例如，贸易展览、会议或每周都有新成员的每周培训课程，在这种情况下，访问权限是根据特定周或月份授予的，而不是绝对的天、周、月。

## 隔离的终端在策略更改后不会重新进行身份验证

### 问题

策略或其他身份更改后，身份验证失败，并且系统不会重新进行身份验证。身份验证失败或有问题的终端仍然无法连接网络。根据分配给用户角色的终端安全策略，未能通过安全评估的客户端计算机上经常会出现此问题。

### 可能的原因

客户端计算机上身份验证计时器的设置不正确，或者交换机上身份验证时间间隔的设置不正确。

### 解决方案

要解决此问题，有几种可能的办法：

1. 在思科 ISE 中查看指定 NAD 或交换机的会话状态摘要 (**Session Status Summary**) 报告，确保该界面已配置适当的身份验证间隔。
2. 在 NAD/交换机上输入 “show running configuration” 命令，确保接口已配置适当的 “authentication timer restart” 设置。（例如，“authentication timer restart 15” 和 “authentication timer reauthenticate 15”。）
3. 输入 “interface shutdown” 和 “no shutdown” 退回 NAD/交换机上的端口，并在思科 ISE 的潜在配置更改后，强制重新进行身份验证。



**注释** 由于 CoA 需要 MAC 地址或会话 ID，因此我们建议您不要重启网络设备 SNMP 报告中显示的端口。

## 当无法找到 IP 地址或 MAC 地址时，操作失败。

当终端的活动会话不包含关于 IP 地址的信息时，在该终端上执行的操作会失败。对于该终端的 MAC 地址和会话 ID，也存在这种情况。



**注释** 如果要通过更改终端的授权状态时，则必须提供该终端的 IP 地址或 MAC 地址。如果在终端的活动会话中无法找到 IP 地址或 MAC 地址，则会看到以下错误消息：

```
No active session found for this MAC address, IP Address or Session ID
```

。

## 通过外部身份验证的管理员无法执行 操作

如果通过外部身份验证的管理员尝试从实时会话发出 CoA 隔离，思科 ISE 会返回以下错误消息：

```
CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated. (Cause:User not found internally. Possible use of unsupported externally authenticated user
```

如果通过外部身份验证的管理员在思科 ISE 使用终端的 IP 地址或 MAC 地址从操作 (**Operations**) > 终端保护服务 (**Endpoint Protection Service**) > 自适应网络控制 (**Adaptive Network Control**) 执行操作，思科 ISE 会返回以下错误消息：

```
Server failure: User not found internally. Possible use of unsupported externally authenticated user
```

## 备份数据类型

思科 ISE 允许您从主 PAN 和从监控节点备份数据。可以从 CLI 或用户界面完成备份。

思科 ISE 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。备份可以使用 GUI 或 CLI 通过主 PAN 完成。
- 运行数据 - 包含监控和故障排除数据。备份可以通过主 PAN GUI 或使用监控节点的 CLI 来完成。

只要以前的版本在以后版本支持的直接升级路径中，就可以使用更低版本的思科 ISE 的备份文件执行恢复操作并且可以在更高版本上执行恢复操作。上恢复此备份。



**注释** 在备份和恢复数据后重新创建部署时，需要主 PAN 和辅助 PAN 的情景可视性重置以确保两个节点上的数据同步。

## 备份和恢复存储库

思科 允许您通过管理员门户创建和删除存储库。您可以创建以下类型的存储库：

- DISK
- FTP
- SFTP
- NFS

- CD-ROM
- HTTP
- HTTPS



**注释** 存储库位于每台设备本地位置。

您应为小型部署（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。

### 开始之前

- 必须具有超级管理员或系统管理员权限才能执行以下任务。

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

**步骤 2** 点击**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 160 页 以了解字段说明：

**步骤 4** 点击**提交 (Submit)** 以创建存储库。

**步骤 5** 通过点击左侧**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，或点击**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。选择对应存储库并点击**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

表 31: 存储库设置

字段	使用指南
<b>Repository</b>	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。
<b>协议 (Protocol)</b>	从可用协议中选择一个您想要使用的协议。
<b>服务器名称 (Server Name)</b>	<p>(对于 TFTP、HTTP、HTTPS、FTP、SFTP 和 NFS 为必填字段) 输入您想要在其上创建存储库的服务器的主机名或 IPv4 地址。</p> <p>注释 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>
<b>路径 (Path)</b>	<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>此值可以用双前斜杠 (//) 或单前斜杠 (/) 开头，表示服务器的根目录。但是，对于 FTP 协议，单前斜杠 (/) 表示 FTP 的本地设备主目录，而不是根目录。</p>
<b>用户名</b>	(对于 FTP、SFTP 和 NFS 为必填字段) 输入对指定服务器拥有写入权限的用户名。用户名可以包含字母数字和 _、/、@、\$ 字符。
<b>密码 (Password)</b>	(对于 FTP、SFTP 和 NFS 为必填字段) 输入用于访问指定服务器的密码。密码可以包含以下字符：0-9、a-z、A-Z、-、.、 、@、#、\$、^、&、*、(、)、+、和 =。

### 相关主题

[备份和恢复存储库](#)，第 158 页

[创建存储库](#)，第 159 页

## 按需备份和计划备份

您可以配置主 PAN 和主监控节点的按需备份。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。

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。

#### 相关主题

[维护设置](#)，第 713 页

## 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。您无法在远程监控节点的本地存储库中备份监控数据。

- 确保在获取备份之前执行所有证书相关的更改。
- 要执行以下任务，您必须是超级管理员或系统管理员。



**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。要恢复备份，请选择存储库，然后点击**恢复 (Restore)**。

#### 相关主题

[思科 ISE 恢复操作](#)，第 165 页

[导出身份验证和授权策略配置](#)，第 171 页

## 按需备份设置

下表介绍**按需备份 (On-Demand Backup)** 窗口上的字段，您可以随时使用此窗口获取备份。此窗口的导航路径为：**管理 (Administration) > 系统 (System) > 备份和恢复 (Backup & Restore)**。

表 32: 按需备份设置

字段名称	使用指南
<b>Backup Name</b>	输入备份文件的名称。
<b>Repository Name</b>	应该保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
<b>Encryption Key</b>	此密钥用于加密和解密备份文件。

#### 相关主题

[备份数据类型](#)，第 158 页

[按需备份和计划备份](#)，第 160 页

[备份历史记录](#)，第 164 页

[备份失败](#)，第 165 页

[思科 ISE 恢复操作](#)，第 165 页

[导出身份验证和授权策略配置](#)，第 171 页

[在分布式环境中同步主节点和辅助节点](#)，第 171 页

[执行按需备份](#)，第 161 页

## 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。您无法在远程监控节点的本地存储库中备份监控数据。
- 要执行以下任务，您必须是超级管理员或系统管理员。

**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。

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

**步骤 2** 点击 **创建 (Create)**，安排配置或操作备份。

**步骤 3** 输入安排备份所需的值。

**步骤 4** 点击 **保存 (Save)**，安排备份。

**步骤 5** 点击此页面顶部的 **刷新 (Refresh)** 链接，查看计划的备份列表。

一次只能为配置或操作备份创建一个计划。可以启用或禁用计划的备份，但不能将其删除。

## 计划备份设置

下表介绍“定期备份”(Scheduled Backup)窗口上的字段，您可以使用此窗口恢复完整备份或增量备份。此窗口的导航路径为：**管理 (Administration) > 系统 (System) > 备份和恢复(Backup and Restore)**。

表 33: 计划备份设置

字段名称	使用指南
<b>Name</b>	输入备份文件的名称。您可以输入您所选的描述性名称。思科 ISE 会将时间戳附加到备份文件名之后并将其存储在存储库中。即使您配置了一系列备份，也要有唯一的备份文件名。在“定期备份”(Scheduled Backup)列表窗口上，备份文件名前面将附加“backup_occur”，表示文件是一次 <b>kron</b> 作业。
<b>Description</b>	输入对备份的说明。
<b>Repository Name</b>	选择保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
<b>Encryption Key</b>	输入用于加密和解密备份文件的密钥。
<b>Schedule Options</b>	选择计划备份的频率并相应地填写其他选项。

### 相关主题

[备份数据类型](#)，第 158 页

[按需备份和计划备份](#)，第 160 页

[备份历史记录](#)，第 164 页

[备份失败](#)，第 165 页

[思科 ISE 恢复操作](#)，第 165 页

[导出身份验证和授权策略配置](#)，第 171 页

[在分布式环境中同步主节点和辅助节点](#)，第 171 页

[使用 CLI 备份](#)，第 164 页

[计划备份](#)，第 162 页

## 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：

- 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，如果向监控节点分配的空间为 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

可以在主管理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。

恢复运营数据的过程根据部署类型而异。



注释

思科中新的备份/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 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，则在主 PAN 上恢复配置备份后，在主 PAN 和策略服务节点 (PSN) 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。（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 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。
- 如果有一个独立管理节点发生故障，则必须运行配置备份进行恢复。如果主 PAN 发生故障，则可以使用分布式设置，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 还提供 **backup-logs** CLI 命令，可用来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。 注释 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 中使用 **restore** 命令时，思科 ISE 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 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。

### 开始之前

在配置备份期间，如果您的部署是双节点部署，请确保满足以下条件：

- 如果用于恢复的源节点和目标节点与用于配置备份的相应节点相同，目标节点可以是独立节点或主节点。
- 如果用于恢复的源节点和目标节点与用于配置备份的相应节点不同，目标节点必须是独立节点。





**注释** 可以仅在主 PAN 上恢复配置数据库备份和重新生成根 CA。不过，无法恢复注册 PAN 上的配置数据库备份。

**步骤 1** 选择 **选择管理 (Administration) > 系统 (System) > 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 **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。

## 恢复监控数据库

恢复监控数据库的流程因部署类型不同而异。以下各节介绍如何在独立和分布式部署中恢复监控数据库。

必须使用 CLI 从思科 ISE 的先前版本恢复按需监控数据库备份。不支持跨思科 ISE 版本恢复定期备份。



**注释** 如果尝试将数据恢复到调取数据所在节点以外的节点，必须将日志记录目标设置配置为指向新节点。这可以确保监控系统日志发送到正确节点。

## 在独立环境中恢复监控（运行）备份

GUI 只列出从当前版本提取的备份。要恢复从早期版本获取的备份，请从 CLI 使用恢复命令。

#### 开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

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

**步骤 2** 从操作备份列表中选择备份的名称，然后单击 **Restore**。

**步骤 3** 输入在备份过程中使用的加密密钥。

**步骤 4** 单击 **Restore**。

---

## 通过管理和监控角色恢复监控备份

您可以使用管理和监控角色在分布式环境中恢复监控备份。

### 开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

---

**步骤 1** 如果使用的是主 PAN 和辅助 PAN，请同步 PAN。

同步 PAN 时，必须选择一个 PAN 并将其升级为活动的主 PAN。

**步骤 2** 在注销监控节点之前，应将监控角色分配给部署中的其他节点。

每个部署必须至少有一个正常运行的监控节点。

**步骤 3** 注销监控节点以进行备份。

**步骤 4** 将监控备份恢复到最近注销的节点。

**步骤 5** 向当前管理节点注册新恢复的节点。

**步骤 6** 将新恢复和注册的节点升级为主用监控节点。

---

## 通过监控角色恢复监控备份

只能通过监控角色恢复分布式环境中的监控备份。

### 开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

---

**步骤 1** 准备取消注册要恢复的节点。这是通过将监控角色分配给部署中的另一个节点来完成的。

部署必须至少有一个正常运行的监控节点。

**步骤 2** 取消注册要恢复的节点。

**注释** 请等待，直到取消注册完成后，再继续执行恢复操作。该节点必须处于独立状态，然后您才能继续执行恢复操作。

**步骤 3** 将监控备份恢复到最近注销的节点。

**步骤 4** 向当前管理节点注册新恢复的节点。

**步骤 5** 将新恢复和注册的节点升级为主用监控节点。

---

## 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。

---

## 导出身份验证和授权策略配置

您可以将身份验证和授权策略配置导出为 XML 文件，您可以离线阅读此文件以识别任何配置错误并用于故障排除。此 XML 文件包括身份验证和授权策略规则、简单和复合策略条件、自主访问控制列表 (dACL) 和授权配置文件。您可以选择以邮件方式发送 XML 文件或将其保存在本地系统中。

**步骤 1** 选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup & Restore)**。

**步骤 2** 点击**策略导出 (Policy Export)**。

**步骤 3** 根据需要输入值。

**步骤 4** 点击**导出 (Export)**。

使用文本编辑器，例如 WordPad，查看 XML 文件的内容。

---

## 在分布式环境中同步主节点和辅助节点

在分布式环境中，在 PAN 上恢复备份文件之后，主节点和辅助节点中的思科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，只能在同步完成后导航至其他思科管理员门户页面和进行配置更改。

### 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** 选择 **管理 (Administration) > 系统 (System) > 部署 (Deployment)**。

**步骤 2** 选中处于不同步复制状态的辅助 ISE 节点旁边的复选框。

**步骤 3** 点击**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管理员门户。

## 恢复独立和分布式部署中断开的节点

此部分提供可用于恢复独立和分布式部署中断开的节点的故障排除信息。以下某些使用案例使用备份和恢复功能，而其他使用案例则使用复制功能恢复已丢失的数据。

## 使用现有 IP 地址和主机名恢复分布式部署中断开连接的节点

### 场景

在分布式部署中，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 地址和主机名恢复分布式部署中断开的节点

### 场景

在分布式部署中，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，您有两个节点：N1（主策略管理节点，即主 PAN）和 N2（辅助策略服务节点）。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。思科节点在新位置被替换，新主机名为 N1A（主 PAN）和 N2A（辅助策略服务节点）。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. 必须在 N1A 上登录思科管理员门户，选择**管理 (Administration) > 系统 (System) > 部署 (Deployment)**，然后执行以下操作：
  - 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。例如，您可能会错误地删除几个 NAD 或修改一些 RADIUS 属性，然后在数小时后才发现这个问题。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。

## 在分布式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

仅分布式部署中的主节点出现故障。

### 解决步骤

1. 登录 N2 管理员门户。选择**管理 (Administration) > 系统 (System) > 部署 (Deployment)**，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。

## 在分布式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。

例如，具有多个节点：N1（主 PAN）、N2（辅助 PAN）、N3（辅助策略服务节点）、N4（辅助策略服务节点）。其中一个辅助节点 N3 出现故障。

### 解决步骤

1. 将新的 N3A 节点重新映像到默认独立状态。
2. 登录到 N1 管理门户并删除 N3 节点。
3. 重新注册 N3A 节点。

数据将从 N1 复制到 N3A。无需恢复。

## 思科 日志记录机制

思科 提供用于审核、故障管理和故障排除的日志记录机制。日志记录机制可以帮助您识别所部署的服务中的故障情况并有效地对相应问题进行故障排除。它还以一致的方式从监控和故障排除主要节点提供日志记录输出。

您可以将思科 ISE 配置为使用虚拟环回地址在本地系统中收集日志。要从外部收集日志，您可以配置外部系统日志服务器，这些服务器称为目标。日志分为多个预定义的类别。您可以根据各个类别的目标、严重性级别等编辑各个类别，以自定义日志记录输出。

作为最佳实践，请勿将网络设备配置为思科 ISE 监控和故障排除 (MnT) 节点，因为这会导致一些网络访问设备 (NAD) 系统日志丢失，并使 MnT 服务器过载，进而导致加载问题。



**注释** 如果将监控节点配置为网络设备的系统日志服务器，请确保该日志源按照如下格式发送正确的网络接入服务器 (NAS) IP 地址：

```
<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>
```

否则，这可能会影响依赖 NAS IP 地址的功能。

## 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。

**步骤 1** 选择 **选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 本地日志设置 (Local Log Settings)**。

**步骤 2** 在 **Local Log Storage Period** 字段中，输入要将日志条目保留在配置源中的最大天数。

如果 localStore 文件夹达到 97 GB，则可能会早于配置的本地日志存储期 (**Local Log Storage Period**) 而删除日志。

**步骤 3** 点击**立即删除日志 (Delete Logs Now)**可在存储期到期前的任何时间删除现有日志文件。

**步骤 4** 点击**保存 (Save)**。

## 思科 ISE 系统日志

在思科 ISE 中，日志记录目标的位置会收集系统日志。目标是指收集和存储日志的服务器的 IP 地址。您可以在本地生成和存储日志，也可以使用 FTP 工具将日志传输至外部服务器。思科 ISE 具有以下默认目标，在本地系统的环回地址中会动态配置这些目标：

- LogCollector - 日志收集器的系统日志默认目标。
- ProfilerRadiusProbe - 分析器 RADIUS 探测功能的默认系统日志目标。

默认情况下，在执行全新思科 ISE 安装或升级期间会禁用 AAA 诊断子类别和系统诊断子类别日志记录目标，以减少磁盘空间。您可以为这些子类别手动配置日志记录目标，但这些子类别的本地日志记录始终处于启用状态。

您可以使用在思科 ISE 安装结束时在本地配置的默认日志记录目标，也可以创建外部目录来存储日志。

### 相关主题

[思科 ISE 消息代码](#)，第 178 页



## 配置远程系统日志收集位置

您可以使用 Web 界面创建向其发送系统日志消息的远程系统日志服务器目标。日志消息根据系统日志协议标准被发送至远程系统日志服务器目标（请参阅 RFC-3164）。系统日志协议为非安全 UDP。

当发生某一事件时，系统会生成消息。事件可能是显示状态的事件，例如当存在某个程序时显示的消息，或报警。诸如内核、电子邮件和用户级别等多个设施会生成不同类型的事件消息。事件消息与严重性级别相关，它允许管理员过滤消息并将其进行优先级排序。数字代码被分配给该设备和严重性级别。系统日志服务器为事件消息收集器并从这些设施收集事件消息。管理员可以基于其严重性级别选择将消息转发至哪个事件消息收集器。

UDP 系统日志（日志收集器）是默认远程日志记录目标。当禁用此日志记录目标时，它不会再充当日志收集器，并且系统会将其从日志记录类别 (**Logging Categories**) 窗口中删除。当启用此日志记录目标时，它会成为日志记录类别 (**Logging Categories**) 窗口中的日志收集器。



**注释** 对默认远程日志记录目标 **SecureSyslogCollector** 的任何更改都会导致思科 ISE 监控和故障排除日志处理器服务重新启动。

**步骤 1** 选择管理 (**Administration**) > 系统 (**System**) > 日志记录 (**Logging**) > 远程日志记录目标 (**Remote Logging Targets**)。

**步骤 2** 点击添加 (**Add**)。

**步骤 3** 输入必要的详细信息。

**步骤 4** 点击 **Save**。

**步骤 5** 转至 Remote Logging Targets 页面，然后验证新的目标是否创建。

然后，可以将日志记录目标映射到下面的每个日志记录类别。PSN 节点根据这些节点上启用的服务将相关日志发送到远程日志记录目标。

- AAA 审核
- AAA 诊断
- 记账
- 外部 MDM
- 被动 ID
- 终端安全评估和客户端调配审核
- 终端安全评估和客户端调配诊断
- Profiler

部署中的所有节点会将以下类别的日志发送到日志记录目标：

- 管理和操作审核

- 系统诊断
- 系统统计项

---

## 思科 ISE 消息代码

日志记录类别是用于说明功能、流程或用例的消息代码的捆绑包。在思科 ISE 中，每条日志根据日志消息内容与日志记录类别所捆绑的消息代码相关联。日志记录类别帮助说明其包含的消息的内容。

日志记录类别可升级日志记录配置。每个类别具有可以根据应用要求进行设置的名称、目标和严重性级别。

思科 ISE 为可以向其分配日志目标的 Posture、Profiler、Guest、AAA（身份验证、授权和记帐）等服务提供预定义日志记录类别。

对于日志记录类别**通过的身份验证 (Passed Authentications)**，默认情况下禁用允许本地日志记录的选项。启用此类别的本地日志记录将导致操作空间利用率高，并填写 prrt-server.log 与 iseLocalStore.log。

如果您选择为**通过的身份验证 (Passed Authentications)**启用本地日志记录，请转至**管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)**，从类别部分中单击**通过的身份验证 (Passed Authentications)**然后选中本地日志记录 (**Local Logging**) 复选框。

### 相关主题

[设置消息代码的严重性级别](#)，第 178 页

## 设置消息代码的严重性级别

您可以设置日志严重性级别，选择存储所选类别的日志的日志记录目标。

---

**步骤 1** 选择**管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)**。

**步骤 2** 点击想要编辑的类别旁边的单选按钮，点击 **Edit**。

**步骤 3** 修改必填字段值。

**步骤 4** 点击 **Save**。

**步骤 5** 转至 Logging Categories 页面，验证对特定类别所做的配置更改。

---

## 思科 ISE 消息目录

您可以使用“消息目录”(Message Catalog) 页面查看所有可能的日志消息和说明。依次选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **消息目录 (Message Catalog)**。。

系统将显示“日志消息目录”(Log Message Catalog) 页面，您可以在该页面查看所有显示在日志文件中可能的日志消息。此页面中的数据仅供显示。

请参阅[思科 ISE 系统日志](#)，了解思科 ISE 发送的系统日志消息的综合列表、它们的含义以及它们如何记录在本地和远程目标中。

## 调试日志

调试日志可捕获引导程序(bootstrap)、应用配置、运行时间、部署、监控、报告和公共密钥基础设施(PKI) 信息。调试日志包含过去 30 天内的严重和警告警报和过去 7 天内的信息警报。

您可以为单个组件配置调试日志严重级别。

您可以将调试日志存储在本地服务器中。



---

**注释** 从备份恢复系统或将其升级后，未保存调试日志配置。

---

### 相关主题

[配置调试日志严重性级别](#)，第 180 页

## 查看节点的日志记录组件

---

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

**步骤 2** 选择要查看其日志记录组件的节点，然后单击**编辑 (Edit)**。

系统将显示“调试级别配置 (Debug Level Configuration)” 页面。您可以查看以下详细信息：

- 基于所选节点上运行的服务的日志记录组件列表
- 每个组件的说明
- 为各个组件设置的当前日志级别

---

### 相关主题

[配置调试日志严重性级别](#)，第 180 页

## 配置调试日志严重性级别

可以配置调试日志的严重性级别。

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

**步骤 2** 选择节点，然后单击编辑 (Edit)。

“调试日志配置” (Debug Log Configuration) 页面会根据在选定节点中运行的服务显示组件列表，以及为各个组件设置的当前日志级别。

**步骤 3** 选择要为其配置调试日志严重性级别的组件，然后单击编辑 (Edit)。从日志级别 (Log Level) 下拉列表中选择所需的日志严重性级别，然后单击保存 (Save)。

**注释** 更改 runtime-AAA 组件的日志严重性级别，会导致其子组件 prrt-JNI 的日志级别也发生更改。子组件日志级别的更改不会影响其父组件。

### 相关主题

[配置调试日志严重性级别](#)，第 180 页

[思科 调试日志](#)，第 806 页

## 终端调试日志收集器

要排除特定终端的问题，可以根据其 IP 地址或 MAC 地址为该特定终端下载调试日志。该特定终端专用部署中的各个节点的日志收集在一个文件中，从而帮助您快速、有效地排除问题。一次只能对一个终端运行此故障排除工具。日志文件列于 GUI 中。您可以为部署中的一个节点或所有节点的终端下载日志。

## 下载特定终端的调试日志

要解决与网络中的特定终端相关的问题，可以从管理员门户使用调试终端工具。或者，可以从 Authentications 页面运行此工具。从 Authentications 页面右键点击 Endpoint ID，然后点击 **Endpoint Debug**。此工具在一个文件中提供关于特定终端的所有服务的所有调试信息。

### 开始之前

需要准备收集其调试日志的终端的 IP 地址或 MAC 地址。

**步骤 1** 选择操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > 终端调试 (Endpoint Debug)。

**步骤 2** 点击 MAC Address 或 IP 单选按钮，输入终端的 MAC 或 IP 地址。

**步骤 3** 如果想要在指定的时间之后停止日志收集，请选中 **Automatic disable after n Minutes** 复选框。如果选中此复选框，必须输入 1 和 60 分钟之间的时间值。

显示以下消息：“Endpoint Debug degrades the deployment performance. Would you like to continue?”

**步骤 4** 点击 **Continue** 收集日志。

**步骤 5** 当想要手动停止日志收集时，请点击 **Stop**。

#### 相关主题

[终端调试日志收集器](#)，第 180 页

## 集合过滤器

您可以配置集合过滤器来禁止将系统日志消息发送到监控节点和外部服务器。可以根据不同属性类型在策略服务节点级别执行禁止。您可以使用特定属性类型和对应的值定义多个过滤器。

在将系统日志消息发送到监控节点或外部服务器之前，思科 ISE 会将这些值与要发送的系统日志消息中的字段进行比较。如果找到任何匹配项，则不会发送对应的消息。



**注释** 如果为任何属性和过滤器类型配置了收集过滤器（管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 收集过滤器 (Collection Filter)）；并且您还选中了在 **n** 天不活动后禁用账户 (Disable account after n days of inactivity) 复选框（管理 (Administration)、> 身份管理 (Identity Management)、> 用户身份验证设置 (User Authentication Settings)、> 禁用账户策略 (Disable Account Policy)），您的账户可能会因身份验证成功的系统日志消息未中继到监控节点而被禁用。

## 配置集合过滤器

您可以根据各种属性类型配置一系列集合过滤器。建议将过滤器数限制在 20 个以内。您可以添加、编辑或删除集合过滤器。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 集合过滤器 (Collection Filters)。

**步骤 2** 点击 **Add**。

**步骤 3** 从以下列表选择 **Filter Type**:

- User Name
- MAC Address
- Policy Set Name
- NAS IP Address
- Device IP Address

**步骤 4** 为您已选的过滤器类型选择对应的 **Value**。

**步骤 5** 从下拉列表中选择 **Result**。结果可能是 All、Passed 或 Failed。

步骤 6 点击提交 (Submit)。

#### 相关主题

[集合过滤器](#)，第 181 页

[事件抑制绕行过滤器](#)，第 182 页

## 事件抑制绕行过滤器

思科 ISE 允许您设置过滤器，以禁止向监控节点和使用收集过滤器的其他外部服务器发送某些系统日志消息。有时，您需要访问这些禁止发送的日志消息。思科 ISE 现在为您提供根据特定属性（例如用户名）在可配置的时间内绕过事件抑制的选项。默认值为 50 分钟，但您可以将持续时间配置为 5 分钟至 480 分钟（8 小时）。配置事件抑制绕行后，该功能会立即生效。如果您设置的持续时间结束，则绕行抑制过滤器将过期。

您可以在思科 ISE 用户界面的 **Collection Filters** 页面中配置抑制绕行过滤器。使用此功能，您现在可以查看某个特定身份（用户）的所有日志并实时解决该身份遇到的问题。

您可以启用或禁用过滤器。如果您在绕行事件过滤器中配置的持续时间结束，则过滤器会自动禁用，直至您再次启用该过滤器。思科 ISE 在更改配置审核报告中捕获这些配置更改。此报告提供了事件抑制或绕行抑制配置人员的相关信息，以及抑制事件或绕行抑制的持续时间。

## 思科 ISE 报告

思科身份服务引擎 (ISE) 报告用于监控和故障排除功能分析趋势、和，监控系统性能和网络活动从中心位置。

思科 ISE 从您的网络收集日志和配置数据。然后，将数据聚合到报告，供您查看和分析。思科 ISE 提供一套标准的预定义报告，您可以直接使用，也可以自定义以满足自己的需求。

思科 ISE 报告经过预配置，划分为不同的类别，包含有关身份验证、会话流量、设备管理、配置和管理以及故障排除的信息。

#### 相关主题

[运行并查看报告](#)，第 182 页

[导出报告](#)，第 183 页

[添加收藏的报告](#)，第 187 页

[可用报告](#)，第 189 页

## 运行并查看报告

本节描述如何使用报告视图运行、查看并导航报告。您可以指定报告中所显示数据的时间增量。

步骤 1 选择操作 (Operations) > 报告 (Reports) > ISE 报告 (ISE Reports)。

**步骤 2** 单击 " 可用报告页上的类别的报告。

**步骤 3** 选择一个或多个过滤器以运行报告。每个报告都具有不同的可用过滤器，某些过滤器为必选而某些则为可选。

**步骤 4** 为过滤器输入适当的值。

**步骤 5** 运行该报告。

---

#### 相关主题

[导出报告](#)，第 183 页

[添加收藏的报告](#)，第 187 页

[可用报告](#)，第 189 页

## 报告导航

您可以从报告输出中获得详细信息。例如，如果您为五个月的一个时间段生成了报告，其图表将按月列出报告的汇总数据。

您可以从表格中点击特定值以查看与此特定字段相关的其他报告。例如，身份验证摘要报告将显示用户或用户组的失败计数。当您点击失败计数时，系统就会打开该特定失败计数的身份验证摘要报告。

## 导出报告

可以将报告数据导出到 Excel 电子表格，作为逗号分隔值 (.csv) 文件。导出数据之后，会收到一封详细说明报告位置的邮件。

无法导出以下报告：

- 身份验证摘要
- 运行状况摘要
- RBACL 丢弃摘要



---

**注释** RBACL 丢弃的数据包流仅适用于 Cisco Catalyst 6500 系列交换机。

---

- 访客赞助商摘要
- 终端配置文件修改
- 网络设备会话状态



**注释** 要在导出报告后正确查看非英文字符，必须通过启用 UTF-8 字符编码，将文件导入 Microsoft Excel。如果选择在不启用 UTF-8 字符编码的情况下直接在 Microsoft Excel 中打开导出的 .csv 文件，则报告中的非英文字符可能会显示一些乱码。



**注释** 只能从主 PAN 将报告数据导出为 .csv 格式。

**步骤 1** 如“运行和查看报告” (Running and Viewing Reports) 一节所述运行报告。

**步骤 2** 点击报告摘要页面右上角的**导出 (Export)**。

**步骤 3** 指定要导出的数据列。

**步骤 4** 从下拉列表中选择存储库。

**步骤 5** 点击**导出 (Export)**。

**步骤 6** 选择以下选项之一：

- 存储库 (CSV)：将报告以 CSV 文件格式导出到存储库
- 本地 (CSV)：将报告以 CSV 文件格式导出到本地磁盘
- 本地 (PDF)：将报告以 PDF 文件格式导出到本地磁盘

**注释**

- 当选择本地 CSV 或 PDF 选项时，仅会导出前 500 条记录。您可以使用存储库 CSV 选项导出所有记录。
- 使用本地 pdf 选项导出多部分报告时，每个部分仅导出前 100 行。

## 我的报告

您可以将预配置的系统报告和个人过滤的报告添加到 **我的报告** 部分。保存到 **我的报告** 部分的报告会保留对其应用的过滤器。

**步骤 1** 在 **报告** 窗口 (**操作 > 报告**) 中，从左侧显示的 **报告** 下拉菜单中点击需要的报告。

**步骤 2** (可选) 打开所选报告后，添加所需的过滤器以自定义报告。

**步骤 3** 点击窗口右上角的 **添加到我的报告** 按钮。

**步骤 4** 系统将打开 **保存到我的报告** 对话框。报告的名称和说明会自动填充。如果需要，您可以编辑这些字段。

**步骤 5** (可选) 所选报告与适用的过滤器一起保存，从而保留其自定义。

**步骤 6** 点击 **保存** 将报告另存为。系统将显示一个对话框，说明报告已成功保存。



步骤 7 所选报告现在将显示在 **我的报告** 下拉列表中，以便于访问。

您可以通过点击窗口右上角的 **从我的报告中删除** 按钮来删除添加到 **我的报告** 部分的报告。在显示的“警报”对话框中点击 **确定**，报告将从“我的报告”部分中删除。

## 安排思科 ISE 报告

您可以安排 思科 ISE 报告，以在特定时间或时间间隔运行和重新运行。您还可以将适当的过滤器应用于您选择的报告。您可以安排在思科 ISE 上以每小时、每天、每周、每月和每年的频率运行报告。它也可以是一次性报告计划作业。您可以选择报告的开始日期和结束日期，并选择要安排报告的星期几。您可以决定计划报告的运行时间。

对于生成的报告，还可以发送和接收电子邮件通知。这些电邮通知将告诉您计划的报告是否已成功运行，还将包含存储库的详细信息、计划报告的时间等。

以**每小时 (Hourly)** 频率安排报告时，可以让报告运行多天，但时间段不能跨越两天。

例如，在安排从 2019 年 5 月 4 日到 2019 年 5 月 8 日的每小时报告时，可以将时间间隔设置为每天上午 6:00 至晚上 11:00，但不能设置为某日下午 6:00 到次日上午 11:00。思科 ISE 会显示错误消息，说明在后一种情况下的时间范围无效。

无法安排以下报告：

- 身份验证摘要
- 运行状况摘要
- RBACL 丢弃摘要



注释 RBACL 丢弃的数据包流仅适用于 Cisco Catalyst 6500 系列交换机。

- 访客赞助商摘要
- 终端配置文件更改
- 网络设备会话状态

**步骤 1** 在 **报告** 窗口（**操作 > 报告**）中，从左侧显示的 **报告** 下拉菜单中选择要计划的报告。

**步骤 2** （可选）打开所选报告时，应用要应用于该报告的过滤器。

**步骤 3** 点击窗口右上角的 **计划** 按钮。

**步骤 4** **另存为计划** 对话框随即打开。

**步骤 5** 填写计划作业的详细信息，例如名称、说明、电邮、日期和时间。

**步骤 6** 从 **存储库** 下拉列表中，选择将保存计划报告的外部存储库。有关详细信息，请参阅“表 1。思科 ISE 管理员指南”的“备份和恢复存储库”部分下的“外部存储库可支持性矩阵”。

- 步骤 7** 从 **频率** 下拉列表中，根据需要选择计划的频率。例如，如果您只需要过去 12 小时的数据，请在安排报告时选择 **过去 12 小时** 数据字段。
- 步骤 8** 根据需要选择 **开始日期** 和 **结束日期**，然后点击 **保存**。
- 步骤 9** 在计划报告时，所有选定的过滤器都将自动应用于报告。
- 步骤 10** 您可以在窗口底部的 **计划的报告** 部分中查看创建的计划和应用的过滤器。

---

您还可以根据需要编辑和删除计划报告。从计划报告下拉列表（**操作 > 报告 > 计划报告**）中选择您选择的计划报告。点击 **编辑计划** 以更改计划的报告，然后点击 **保存**。点击 **删除计划** 以删除计划的报告。

## 使用案例：计划的报告

要在当日上午 12 点获取前一天的数据，请按照以下程序安排报告：

- 
- 步骤 1** 在 **报告** 窗口（**操作 > 报告**）中，从左侧显示的 **报告** 下拉菜单中选择要计划的报告。
- 步骤 2** （可选）打开所选报告时，应用要应用于该报告的过滤器。
- 步骤 3** 在此场景中，要获取前一天的数据，请选择 **记录时间** 字段并应用 **昨天** 过滤器。每当计划的报告运行时，这将返回前一天的数据。如果您只需要过去 12 小时的数据，请在计划报告时选择 **另存为计划** 对话框中的 **过去 12 小时** 数据字段。
- 步骤 4** 点击窗口右上角的 **计划** 按钮。
- 步骤 5** **另存为计划** 对话框随即打开。
- 步骤 6** 填写计划作业的详细信息，例如名称、说明、电邮、日期和时间。
- 步骤 7** 从 **存储库** 下拉列表中，选择将保存计划报告的外部存储库。有关详细信息，请参阅“表 1。思科 ISE 管理员指南”的“备份和恢复存储库”部分下的“外部存储库可支持性矩阵”。
- 步骤 8** 从 **频率** 下拉列表中，根据需要选择计划的频率。例如，如果您只需要过去 12 小时的数据，请在安排报告时选择 **过去 12 小时** 数据字段。
- 步骤 9** 根据需要选择 **开始日期** 和 **结束日期**，然后点击 **保存**。
- 步骤 10** 在计划报告时，所有选定的过滤器都将自动应用于报告。
- 步骤 11** 您可以在窗口底部的 **计划的报告** 部分中查看创建的计划和应用的过滤器。
-

**注释**

- 大多数计划报告都以 .csv 格式导出。但是，Radius 身份验证、Radius 审计、TACACS 身份验证、TACACS 审计和操作审核的计划报告导出到包含 .csv 文件的 .zip 文件夹中。
- 如果外部管理员（例如 Active Directory 管理员）在未填写电子邮件 ID 字段的情况下创建计划报告，则不会发送任何电子邮件通知。
- 只有在删除由特定用户创建的计划报告后，才能删除内部或外部思科 ISE 用户，以确保在删除用户后没有活动计划正在运行。
- 只能从 PAN 保存或安排（使用过滤器）思科 ISE 报告。
- 计划的报告作业在主 MnT 和辅助 MnT 节点上运行。如果主 MnT 关闭，则辅助 MnT 将执行计划的报告作业。在这种情况下，辅助 MnT 首先对主 MnT 执行 ping 操作。仅当 ping 失败时，辅助 MnT 才会运行计划的导出作业。
- 从思科 ISE 3.1 补丁 1 开始，导出的报告中的日期格式已从 YYYY-MM-DD 更改为 DD-MM-YY。时间格式已从 hh:mm:ss.sss 更改为 hh:mm:ss.sss AM/PM（24 小时制改为 12 小时制）。

## 添加收藏的报告

您可以将预配置的系统报告，以及已自定义的报告添加到您的收藏夹列表。

您可以将常用的报告添加到收藏夹列表，让它们更易于查找，就像在浏览器中收藏喜爱的网站一样。您可以查看和编辑收藏报告的参数，然后保存自定义报告以重复使用。

**注释**

系统会为每个管理员帐户分配一个或多个管理角色。根据分配给您的帐户的角色，您可能无法执行本部分所述的任务。

**步骤 1** 按“运行和查看报告”部分所述运行报告。

**步骤 2** 点击报告摘要页面右上角的 **Favorite**。

报告将显示在收藏夹列表中。

**注释** 您只能从 PAN 将预配置的系统报告添加到收藏夹列表。

## 思科 ISE 活动 RADIUS 会话

思科 ISE 为实时会话提供动态的授权更改 (CoA) 功能，通过此功能，可以动态地控制活动 RADIUS 会话。可以将重新验证或断开请求发送到网络接入设备 (NAD) 以执行以下任务：

- 排除与身份验证相关的问题 - 可以使用 **Session reauthentication** 选项继续尝试重新验证。但是，不能使用此选项来限制访问。要限制访问，请使用 **shutdown** 选项。
- 阻止有问题主机 - 可以将 **Session termination** 与 **port shutdown** 选项一起使用，以阻止在网络上发送大量流量的被感染主机。但是，RADIUS 协议当前不支持重新启用已关闭端口的的方法。
- 强制终端重新获取 IP 地址 - 可以将 **Session termination** 与 **port bounce** 选项一起使用，以便没有请求方或客户端的终端在 VLAN 更改之后生成 DHCP 请求。
- 将更新的授权策略推送到终端 - 可以使用 **Session reauthentication** 选项执行更新的策略配置，例如，根据管理员的决定更改现有会话的授权策略。例如，如果启用终端安全评估验证，当终端初次获得访问权限时，通常会被隔离。已知终端的身份和终端安全评估之后，可将 **Session reauthentication** 命令发送到终端，以便该终端根据其终端安全评估获取实际授权策略。

为了让设备读懂 CoA 命令，应适当地配置选项，这一点非常重要。

为了使 CoA 正常工作，必须为每台需要动态授权更改的设备配置共享密钥。思科 ISE 使用共享密钥配置向设备请求访问权限并向其发出 CoA 命令。



**注释** 在此思科 ISE 版本中，可以显示的经过身份验证的最大活动终端会话数限制为 100000。

#### 相关主题

[更改 RADIUS 会话的授权](#)，第 188 页

## 更改 RADIUS 会话的授权

您网络中的某些网络接入设备可能不会在重新加载后发送 **Accounting Stop** 或 **Accounting Off** 数据包。因此，您可能在 **Session Directory** 报告中找到两个会话，其中一个已过期。

要动态地更改活动 RADIUS 会话的授权或断开活动 RADIUS 会话的连接，请务必选择最近的会话。

**步骤 1** 依次选择操作 (**Operations**) > 身份验证 (**Authentications**)。

**步骤 2** 将视图切换到 **Show Live Session**。

**步骤 3** 点击要发出 CoA 的 RADIUS 会话的 CoA 链接，然后选择以下其中一个选项：

**注释** 在已经使用 **Inline Posture** 节点和无线 LAN 控制器 (WLC) 的情况下，只有两个选项可用：**Session reauthentication** 和 **Session termination**。

- **SAnet Session Query** - 使用此选项查询有关支持 SAnet 的设备的信息。
- **Session reauthentication** - 重新对会话进行身份验证。如果您为在支持 COA 的 ASA 设备上建立的会话选择此选项，则此操作将会调用 **Session Policy Push CoA**。
- **Session reauthentication with last** - 为此会话使用最后一个成功身份验证方法。
- **Session reauthentication with rerun** - 从头开始运行配置的身份验证方法。

注释 思科 IOS 软件中当前不支持 **Session reauthentication with last** 和 **Session reauthentication with rerun** 选项。

- **Session termination** - 仅终止会话。交换机会在不同的会话中重新对客户端进行身份验证。
- **Session termination with port bounce** - 终止会话并重新启动报告。
- **Session termination with port shutdown** - 终止会话并关闭报告。

**步骤 4** 点击 **Run** 使用选定的 **reauthenticate** 或 **terminate** 选项发出 CoA。

如果您的 CoA 失败，可能是由于以下其中一个原因引起：

- 设备不支持 CoA。
- 身份或授权策略已发生更改。
- 共享密钥不匹配。

## 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。

表 34: 可用报告

报告名称	说明	日志记录类别
身份验证服务状态		
AAA 诊断	AAA 诊断报告提供思科 ISE 和用户之间所有网络会话的详细信息。如果用户无法访问网络，您可查看此报告以确定其动态并明确问题是仅限于特定用户还是普遍存在。	依次选择管理 ( <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：“策略诊断” (Policy Diagnostics)、 “身份库诊断” (Identity Stores Diagnostics)、 “身份验证流程诊断” (Authentication Flow Diagnostics) 和 “RADIUS 诊断” (RADIUS Diagnostics)。
RADIUS 身份验证	您可以通过 RADIUS 身份验证报告查看身份验证失败和成功的历史记录。如果用户无法访问网络，您可以在此报告中查看详细信息以确定可能的原因。	依次选择管理 ( <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：“已通过的身份验证” (Passed Authentications) 和 “失败的尝试” (Failed Attempts)。

报告名称	说明	日志记录类别
RADIUS 错误	<p>您可以通过 RADIUS 错误报告检查已丢失的 RADIUS 请求（从未知网络访问设备丢弃的身份验证/记帐请求）、EAP 连接超时和未知 NAD。</p> <p><b>注释</b>        有时，如果正在进行用户身份验证，ISE 会以静默方式丢弃终端的计费停止 (Accounting Stop) 请求。但是，一旦用户身份验证完成，ISE 将开始确认所有计费请求。</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“失败尝试” (Failed Attempts)。
RADIUS 计费	RADIUS 计费报告指出用户访问网络持续的时间。如果用户失去了网络连接，您可以使用此报告确定是不是思科 ISE 导致的网络连接问题。	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“RADIUS 计费” (RADIUS Accounting)。

报告名称	说明	日志记录类别
身份验证摘要	<p>身份验证摘要报告以 RADIUS 身份验证为基础。您可以通过此报告确定最常见的身份验证以及任何身份验证失败的原因。例如，如果一个思科 ISE 服务器处理的身份验证明显多于其他服务器，您可能需要重新将用户分配给其他思科 ISE 服务器，以实现更好的负载均衡。</p> <p><b>注释</b> 由于身份验证摘要报告或控制面板要收集和显示与失败或成功的身份验证对应的最新数据，所以报告的内容会延迟几分钟才显示。</p>	-
OCSP 监控	<p>OCSP 监控报告指明在线证书状态协议 (OCSP) 服务的状态。它可以确定思科 ISE 能否成功连接证书服务器并提供证书状态审核，还提供对思科 ISE 执行的所有 OCSP 证书验证操作的汇总。此外，它可从 OCSP 服务器检索关于正常和已吊销主要证书与辅助证书的信息。思科 ISE 缓存响应并利用响应生成后续 OCSP 监控报告。如果缓存已清除，它将从 OCSP 服务器检索信息。</p>	<p>选择管理 (<b>Administration</b>) &gt; 系统 (<b>System</b>) &gt; 日志记录 (<b>Logging</b>) &gt; 日志记录类别 (<b>Logging Categories</b>)，然后选择“系统诊断” (System Diagnostics)。</p>

报告名称	说明	日志记录类别
AD 连接器操作	AD Connector Operations 报告提供关于 AD 连接器执行的操作的日志，例如思科 ISE 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。  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。	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)。
身份映射	您可以通过身份映射报告监控与域控制器的 WMI 连接的状态并收集与之相关的统计信息（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“身份映射” (Identity Mapping)。
部署状态		
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)。
内部管理员摘要	您可以通过内部管理员摘要报告验证管理员用户的注册情况。您还可以从此报告访问管理员登录和更改配置审核报告，从而可以查看每个管理员的此类详细信息。	-
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)。



报告名称	说明	日志记录类别
Secure Communications Audit	安全通信审核报告提供关于思科 ISE 管理员 CLI 中的安全性相关事件的审核详细信息，该管理员 CLI 包括：身份验证失败、可能的入侵尝试、SSH 登录、失效密码、SSH 注销和无效用户帐户等。	-
操作审核	操作审核报告提供关于任何操作变更的详细信息，例如运行备份、注册思科 ISE 节点或重新启动应用。	选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)，然后选择“管理和操作审核” (Administrative and Operational Audit)。
系统诊断	系统诊断报告提供关于思科 ISE 节点的状态的详细信息。如果思科 ISE 节点无法注册，您可查看此报告以对问题进行故障排除。  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思科 ISE 性能产生负面影响。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。	依次选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)，然后选择以下日志记录类别：“内部操作诊断” (Internal Operations Diagnostics)、 “分布式管理” (Distributed Management)、 “管理员身份验证和授权” (Administrator Authentication and Authorization)。
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。	选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)，然后选择以下日志记录类别：“系统统计信息” (System Statistics)、 “系统诊断” (System Diagnostics)，以及“管理和操作审核” (Administrative and Operational Audit)。

报告名称	说明	日志记录类别
网络设备会话状态	<p>您可以通过网络设备会话状态摘要报告显示交换机配置，而无需直接登录交换机。</p> <p>思科 ISE 使用 SNMP 查询功能获取这些详细信息，而且要求用 SNMP v1/v2c 配置您的网络设备。</p> <p>如果用户遇到网络问题，此报告可帮助您识别问题是否与交换机配置相关，而与思科 ISE 无关。</p>	-
数据清除审核	<p>数据清除审核报告记录何时清除了日志记录数据。</p> <p>此报告会反映两个数据清除来源。</p> <p>每天凌晨 4 点，思科 ISE 会检查是否有任何日志记录文件符合您在“管理” (Administration) &gt; “维护” (Maintenance) &gt; “数据清除” (Data Purging) 页面设置的条件。如有，思科 ISE 会删除这些文件并将其记录于此报告中。此外，思科 ISE 继续为日志文件保留最多 80% 的已用存储空间。思科 ISE 每小时都会检查此百分比并删除最早的数据，直到再次达到此 80% 的阈值。这些信息也会记录于此报告中。</p>	-

报告名称	说明	日志记录类别
pxGrid Administrator Audit	<p>pxGrid 管理员审核报告提供关于 pxGrid 管理操作的详细信息，例如在主 PAN 上注册客户端、注销客户端、批准客户端、创建主题、删除主题、添加发布者-订用者，以及删除发布者-订用者。</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>	-
配置有误的请求方	<p>配置有误的请求方报告提供配置错误的请求方的列表以及对具体请求方执行的失败尝试的统计信息。如果您已采取纠正措施并修复配置错误的请求方，此报告会显示修复确认信息。</p> <p><b>注释</b>        应启用 RADIUS 抑制才能运行此报告。</p>	-
配置有误的 NAS	<p>配置有误的 NAS 报告提供关于记帐频率不正确（通常指频繁地发送记帐信息）的 NAD 的信息。如果您已采取纠正措施并修复配置错误的 NAD，此报告会显示修复确认信息。</p> <p><b>注释</b>        应启用 RADIUS 抑制才能运行此报告。</p>	-
终端和用户		

报告名称	说明	日志记录类别
客户端调配	客户端调配报告显示应用于特定终端的客户端调配代理。您可以使用此报告验证应用于每个终端的策略以确定是否正确调配了终端。	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“终端安全评估和客户端调配审核与终端安全评估和客户调配诊断”(Client Provisioning Audit and Posture and Client Provisioning Diagnostics)。
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: “记帐”(Accounting) 和 “Radius 记帐”(Radius Accounting)。
	报告以 RADIUS 记账为基础。它可以显示每个终端所有网络会话的历史报告数据。	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“已通过身份验证”(Passed Authentications) 和 RADIUS 计费 (RADIUS Accounting)。
外部移动设备管理	外部移动设备管理报告提供关于思科 ISE 与外部移动设备管理 (MDM) 服务器之间的集成的详细信息。  您可以使用此报告查看哪些终端经过了 MDM 服务器调配, 而无需直接登录 MDM 服务器。此报告还显示注册和 MDM 合规状态等信息。	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 MDM。
终端安全详细评估	终端安全详细评估报告提供关于特定终端的安全评估合规性的详细信息。如果某个终端之前能访问网络, 然后突然无法访问网络, 您可以根据此报告确定是否出现了安全评估违规问题。	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“终端安全评估和客户端调配审核与终端安全评估和客户调配诊断”(Client Provisioning Audit and Posture and Client Provisioning Diagnostics)。

报告名称	说明	日志记录类别
已分析的终端摘要	<p>已分析的终端摘要报告提供关于正在访问网络的终端的分析详细信息。</p> <p><b>注释</b> 对于不注册会话时间的终端（例如思科 IP 电话），“终端会话时间” (Endpoint session time) 字段中会显示“不适用” (Not Applicable)。</p>	选择管理 ( <b>Administration</b> ) > 系统 ( <b>System</b> ) > 日志记录 ( <b>Logging</b> ) > 日志记录 ( <b>Logging</b> )，然后选择“分析器” (Profiler)。
终端配置文件更改	<p>终端配置文件更改报告用于以下两种用途：</p> <ul style="list-style-type: none"> <li>• 比较特定终端的配置文件更改以验证是否应用的是最新的配置文件。</li> <li>• 显示分析器源服务（使用思科 ISE Plus 许可证可获得此服务）发起的配置文件更改。</li> </ul>	-
按终端查看顶级授权	终端顶级授权 (MAC 地址) 报告显示思科 ISE 已授权每个终端 MAC 地址访问网络的次数。	已通过身份验证、失败尝试
按用户查看顶级授权	按用户查看顶级授权报告显示思科 ISE 已授权每个用户访问网络的次数。	已通过身份验证、失败尝试
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。	管理和操作审核
请求方调配	请求方调配报告提供关于调配至员工个人设备的请求方的详细信息。	终端安全评估和客户端调配审核
注册终端	注册终端报告显示员工注册的所有个人设备。	-

报告名称	说明	日志记录类别
终端清除活动	用户可以通过终端清除活动报告查看终端清除活动的历史记录。此报告要求启用“分析器”(Profiler)日志记录类别。该类别在默认情况下已启用。	选择管理 ( <b>Administration</b> ) > 系统 ( <b>System</b> ) > 日志记录 ( <b>Logging</b> ) > 日志记录 ( <b>Logging</b> )，然后选择“分析器”(Profiler)。
访客接入报告		
AUP Acceptance Status	AUP Acceptance Status 报告提供从所有 Guest 门户接受的 AUP 的详细信息。	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“访客”(Guest)。
Sponsor Login and Audit	Sponsor Login and Audit 报告提供关于访客用户的登录、添加、删除、启用、暂停和更新操作以及发起人在发起人门户上的登录活动的详细信息。  如果批量添加访客用户，则“访客用户”(Guest Users) 列下会显示这些用户。此列默认处于隐藏状态。在导出时，这些批量用户也会显示于导出的文件上。	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“访客”(Guest)。
我的设备登录和审核	我的设备登录和审核报告提供关于用户通过设备在“我的设备门户”(My Devices Portal) 中执行的登录活动和操作的详细信息。	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“我的设备”(My Devices)。

报告名称	说明	日志记录类别
主访客报告	<p>主访客报告综合各个访客接入报告的数据，并且允许您从不同报告来源导出数据。主访客报告还提供关于访客用户正在访问的网站的信息。您可以使用此报告进行安全审核，以证明访客用户何时访问了网络以及他们在网络上执行了什么活动。</p> <p>您还必须在用于访客流量的网络访问设备 (NAD) 上启用 HTTP 检查。这些信息由 NAD 发送回思科 ISE。</p> <p>要检查客户端何时达到最大并行会话限制数，从管理员门户选择<b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> 并执行以下操作：</p> <ol style="list-style-type: none"> <li>1. 将“身份验证流量诊断” (Authentication Flow Diagnostics) 日志类别的日志级别从警告提高到信息。</li> <li>2. 从 AAA 诊断“日志记录类别”下，将 LogCollector 目标从可用的更改为已选的。</li> </ol>	选择 <b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 日志记录类别 (Logging Categories)</b> ，然后选择已通过的身份验证 (Passed Authentications)。
访客计费	访客计费报告是 RADIUS 计费报告的一部分。此报告中显示分配至激活访客或访客身份组的所有用户。	-
TrustSec		

报告名称	说明	日志记录类别
RBACL 丢包摘要	<p>RBACL 丢包摘要报告专用于 TrustSec 功能，只有在具备思科 ISE 高级许可证的情况下才可用。</p> <p>此报告还要求您将网络设备配置为向思科 ISE 发送关于丢包事件的 NetFlow 事件。</p> <p>如果用户违反特定策略或访问权限，系统会丢弃数据包并在此报告中指明。</p>	—
按用户前 N 个 RBACL 丢包	<p>按用户前 N 个 RBACL 丢包报告专用于 TrustSec 功能，只有在具备思科 ISE 高级许可证的情况下才可用。</p> <p>此报告还要求您将网络设备配置为向思科 ISE 发送关于丢包事件的 NetFlow 事件。</p> <p>此报告显示特定用户违反策略的情况（依据数据包丢弃情况）。</p>	—





## 第 7 章

# 设备管理

- TACACS+ 设备管理，第 201 页
- 设备管理工作中心，第 202 页
- 设备管理策略集，第 203 页
- 创建设备管理策略集，第 203 页
- 设备管理 - 授权策略结果，第 204 页
- 通过 CLI 更改启用密码，第 208 页
- 配置全局 TACACS+ 设置，第 209 页
- 从思科安全 ACS 将数据迁移至思科 ISE，第 209 页
- 监控设备管理活动，第 210 页

## TACACS+ 设备管理

思科 ISE 支持设备管理通过使用终端访问控制器访问控制系统 (TACACS+) 安全协议控制，来控制 and 审计网络设备的配置。网络设备可以配置为向思科 ISE 查询对设备管理员操作所进行的身份验证和授权，并发送思科 ISE 的记账信息以记录操作。它可以促进对谁可以访问哪个网络及更改关联网络设置进行精细控制。思科 ISE 管理员可以创建策略集，允许在设备管理访问服务的授权策略规则中选择 TACACS 结果（如命令集和外壳配置文件）。思科 ISE 监控节点可提供与设备管理相关的增强型报告。“工作中心” (Work Center) 菜单中包含所有设备管理页面，可作为 ISE 管理员的单一入手机点。

思科 ISE 需要设备管理许可证才能使用 TACACS+。

设备管理中存在两种类型的管理员

- 设备管理员
- 思科 ISE 管理员

设备管理员是指登录到交换机、无线接入点、路由器和网关（一般通过 SSH）等网络设备以执行对所管理设备进行配置和维护的用户。思科 ISE 管理员可登录思科 ISE，配置并协调设备管理员所登录的设备。

思科 ISE 管理员是本文档的目标读者，他们可登录思科 ISE 以配置相应的设置，控制设备管理员的操作。思科 ISE 管理员使用设备管理功能（工作中心 (Work Centers) > 设备管理 (Device

**Administration**) 来控制和审核网络设备的配置。设备可配置为使用终端访问控制器访问控制系统 (TACACS) 安全协议来查询思科 ISE 服务器。思科 ISE 监控节点可提供与设备管理相关的增强型报告。思科 ISE 管理员可以执行以下任务：

- 配置带有 TACACS+ 详细信息（共享密钥）的网络设备。
- 添加设备管理员为内部用户，并根据需要为其设置启用密码。
- 创建策略集，这些策略集可使得 TACACS 结果（例如，命令集和 shell 配置文件）被选中到设备管理访问服务中的授权策略规则中。
- 在思科 ISE 中配置 TACACS 服务器，允许设备管理员基于策略集来访问设备。

设备管理员负责设置设备以与思科 ISE 服务器进行通信。当设备管理员登录到设备时，设备将查询思科 ISE 服务器，后者进而查询内部或外部身份存储区，以验证设备管理员的详细信息。当思科 ISE 服务器完成验证后，设备将通知思科 ISE 服务器每个会话或用于记账和审核的命令授权操作的最终结果。

思科 ISE 管理员可以使用 TACACS 和思科 ISE 2.0 及更高版本来进行设备管理。与设备管理相关的配置也可以从思科安全访问控制系统 (ACS) 服务器版本 5.5 和 5.6 中迁移。更早期的版本需在迁移之前升级到版本 5.5 或 5.6。



**注释** 您应勾选以下页面中的启用设备管理服务 (**Enable Device Admin Service**) 复选框来启用 TACACS+ 操作：**管理 (Administration) > 系统 (System) > 发展 (Deployment) > 通用设置 (General Settings)**。确保部署中每个 PSN 都启用了此选项。



**注释** 思科 ISE 需要设备管理许可证才能在现有的 Base 或 Mobility 许可证之上使用 TACACS+ 服务。设备管理许可证是一种永久许可证。当从较早版本升级到思科 ISE 版本 2.0 及更高版本，并且要启用 TACACS+ 服务时，必须订购设备管理许可证作为单独的附加许可证。整个 ISE 部署需要一个设备管理许可证。

## 设备管理工作中心

“工作中心” (Work Center) 菜单中包含所有设备管理页面，可以作为思科 ISE 管理员的单一入手点。然而，未指定用于设备管理的页面（例如，“用户” (Users)、 “用户身份组” (User Identity Groups)、 “网络设备” (Network Devices)、 “默认网络设备” (Default Network Devices)、 “网络设备组” (Network Device Groups)、 “身份验证” (Authentication) 和 “授权条件” (Authorization Conditions)）依然可从其原始菜单选项（例如，“管理” (Administration)）访问。仅在获得并安装了正确的 TACACS+ 许可证后，“工作中心” (Work Centers) 选项才可用。

“设备管理菜单” (Device Administration Menu) 包含了以下菜单选项：“概述” (Overview)、 “设备管理策略集” (Device Admin Policy Sets)、 “身份” (Identities)、 “用户身份组” (User Identity Groups)、

“网络资源” (Network Resources)、 “网络设备组” (Network Device Groups)、 “策略条件” (Policy Conditions)、 “策略结果” (Policy Results)、 “报告” (Reports) 和 “设置” (Settings)。

## 设备管理策略集

常规策略集包括一个身份验证规则表和一个授权规则表。身份验证规则表由一组“外部”规则组成，这些规则用于选择可支持的协议。每个“外部”规则包含一个或多个用于选择要使用的特定身份存储的“内部”规则。这些授权规则表由一组规则组成，这些规则用于选择要实施授权业务模式所需的特定授权结果。每个规则都包含一个或多个条件（匹配时才能使用该规则）、一组命令集和/或一个外壳配置文件，选中后即可控制授权过程。每个规则集有一个可用于在特定条件下覆盖这些规则的授权例外规则表，例外表通常在临时情况下使用。



注释 不支持 TACACS + CHAP 出站身份验证。

一个代理策略集包含单个的所选代理顺序。如果策略集处于此模式，则使用一个或多个远程代理服务器处理请求（虽然本地计费可由代理顺序进行配置）。

## 创建设备管理策略集

创建设置的设备管理策略集：

开始之前

- 确保已为 TACACS+ 操作启用管理 (Administration) > 系统 (System) > 部署 (Deployment) > 编辑节点 (Edit Node) > 常规设置 (General Settings) 窗口中的启用设备管理服务 (Enable Device Admin Service) 复选框。
- 确保用户身份组（例如 System\_Admin、服务中心）已创建。（工作中心 (Work Centers) > 设备管理 (Device Administration) > 用户身份组 (User Identity Groups) 窗口）
- 确保成员用户（例如 ABC、XYZ）包含在用户身份组中。（工作中心 (Work Centers) > 设备管理 (Device Administration) > 身份 (Identities) > 用户 (Users) 窗口）
- 确保在需要管理的设备上配置 TACACS 设置。（工作中心 (Work Centers) > 设备管理 (Device Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices) > 添加 (Add) > TACACS 身份验证设置 (TACACS Authentication Settings) 复选框已启用，并且用于 TACACS 和设备的共享密钥相同，以便于设备查询思科 ISE。）
- 确保网络设备组已根据设备类型和位置创建。（工作中心 (Work Centers) > 设备管理 (Device Administration) > 网络设备组 (Network Device Groups) 窗口）

步骤 1 选择工作中心 (Work Centers) > 设备管理 (Device Administration) > 设备管理策略集 (Device Admin Policy Sets)。

**步骤 2** 在左侧窗格中，选择一个新策略集将要添加至其之上（之下）的当前策略集。

**步骤 3** 在左侧窗格中，点击**创建于...之上 (Create Above)** 创建新策略集。

**步骤 4** 点击**编辑 (Edit)** 并输入名称、说明和条件，（例如，名称：Device\_Admin\_Policy\_1，说明：ISE 管理员、条件：DEVICE:Device Type EQUALS Device Type#All Device Types #Cisco\_switches）以配置基于该条件的规则。

**步骤 5** 点击 **Done**。

**步骤 6** 创建所需的身份验证策略，（例如名称：ATN\_Internal\_Users，规则：if DEVICE:Location EQUALS Location #All Locations#Europe，条件：Allow Protocols: Device\_Admin\_protocols 和默认：Use Internal Users - 该策略仅匹配位于欧洲的设备，支持在设备管理员协议下定义的协议和对内部用户的身份验证）。

**步骤 7** 创建所需的授权策略。

示例 1：规则名称：Sys\_Admin\_rule, Conditions: if SysAdmin and TACACS User Equals ABC then cmd\_Sys\_Admin AND Profile\_priv\_8 - 该策略匹配用户名为 ABC 的系统管理员，支持要执行的指定命令，并分配权限级别 8。

示例 2：规则名称：HelpDesk AND TACACS User EQUALS XYZ then cmd\_HDesk\_show AND cmd\_HDesk\_ping AND Profile\_priv\_1 - 该策略匹配用户名为 XYZ 系统管理员，支持要执行的指定命令，并分配权限级别 1。

在上述示例中：

- cmd\_Sys\_Admin 和 cmd\_HDesk 命令集是在工作中心 (**Work Centers**) > 设备管理 (**Device Administration**) > 策略元素 (**Policy Elements**) > TACACS 命令集 (**TACACS Command Sets**) > 添加 (**Add**) 窗口中创建的。
- TACACS 配置文件 Profile\_Priv\_1 和 Profile\_priv\_8 是在工作中心 (**Work Centers**) > 设备管理 (**Device Administration**) > 策略结果 (**Policy Results**) > TACACS 配置文件 (**TACACS Profiles**) > 添加 (**Add**) 窗口中创建的。

**注释** 建议在策略集创建之前创建策略结果，以便当创建授权结果时策略结果随时可用。

**步骤 8** 点击**提交 (Submit)** 以创建新的策略集。

## 设备管理 - 授权策略结果

思科 ISE 管理员可以使用 TACACS+ 命令集和 TACACS+ 配置文件（策略结果）对授予给设备管理员的权限和命令进行控制。策略与网络设备协同工作，从而防止可能发生的意外或恶意配置更改。如果发生此种更改，您可以使用设备管理审计报告对执行特定命令的设备管理员进行跟踪。

### TACACS+ 命令集

命令集实施可由设备管理员执行的指定命令列表。当设备管理员在网络设备上发出操作命令时，查询思科 ISE 确定管理员是否被授权发出这些命令。这也称为命令授权。

### 命令集中的通配符和正则表达式

命令行包括命令和零个或多个参数。当思科 ISE 收到命令行（请求）时，它可以以不同的方式处理命令及其参数：

- 使用通配符匹配模式将请求中的命令与命令集列表中指定的命令进行匹配。

示例：Sh?? or S\*

- 使用正则表达式 (regex) 匹配模式将请求中的参数与命令集列表中指定的参数进行匹配。

示例：Show interface[1-4] port[1-9]:tty\*

## 命令行和命令集列表匹配

将请求的命令行与包含通配符和 Regrex 的命令集列表进行匹配：

1. 循环访问命令集列表以检测匹配的命令。

通配符匹配允许：

- 不区分大小写。
- 命令集的命令中的任意字符都可以为“?”，它与请求的命令中必须存在的任意单个字符匹配。
- 命令集的命令中的任意字符都可以为“\*”，它与请求的命令中的 0 或多个字符匹配。

示例：

请求	命令集	匹配	备注
show	show	支持	—
show	SHOW	支持	不区分大小写
show	Sh??	支持	匹配任意字符
show	Sho??	N	第二个“?”与不存在的字符相交
show	S*	支持	“*”匹配任意字符
show	S*w	支持	“*”匹配字符“ho”
show	S*p	N	请求中没有字符与字符“p”对应

2. 对于每个匹配的命令，思科 ISE 会验证参数。

对于每个命令，命令集列表包含一组以空格隔开的参数。

示例：Show interface[1-4] port[1-9]:tty.\*

该命令含有两个参数。

1. 参数 1: interface[1-4]
2. 参数 2: port[1-9]:tty.\*

对于请求中的命令参数，按照它们在数据包中的位置重要性顺序进行匹配。如果命令定义中的所有参数与请求中的参数匹配，那么该命令或参数可被认为是匹配的。请求中的任何外来参数都会被忽略。



注释 在参数中使用标准 Unix 正则表达式。

## 含多个命令集的处理规则

1. 如果命令集包含命令及其参数的匹配项，并且匹配项具有“始终拒绝” (Deny Always)，则思科 ISE 会指定该命令集为 Commandset-DenyAlways。
2. 如果命令集中不包含与命令匹配的“始终拒绝”，思科 ISE 会按顺序检查命令集中的所有命令，查找第一个匹配命令。
  1. 如果第一个匹配项具有“允许” (Permit)，则思科 ISE 会指定命令集为 Commandset-Permit。
  2. 如果第一个匹配项具有“拒绝” (Deny)，则思科 ISE 会指定命令集为 Commandset-Deny。
3. 在思科 ISE 分析所有命令集后，它会授权以下命令：
  1. 如果思科 ISE 指定任何命令集为 Commandset-DenyAlways，则思科 ISE 拒绝该命令。
  2. 如果没有 Commandset-DenyAlways，且任意命令集为 Commandset-Permit，则思科 ISE 允许该命令；否则，思科 ISE 将拒绝该命令。唯一的例外情况是不匹配 (Unmatched) 复选框已选中。

## 创建 TACACS+ 命令集

要使用 TACACS+ 命令集策略结果创建策略集，请按照以下步骤操作：

- 步骤 1 依次选择工作中心 (Work Centers) > 设备管理 (Device Administration) > 策略结果 (Policy Results) > TACACS 命令集 (TACACS Command Sets)。
- 步骤 2 您还可以在工作中心 (Work Centers) > 设备管理 (Device Administration) > 设备管理策略集 (Device Admin Policy Sets) 页面中配置 TACACS 命令集。
- 步骤 3 点击添加 (Add)。
- 步骤 4 输入名称和说明。
- 步骤 5 点击添加 (Add) 指定授予权限、命令和参数。
- 步骤 6 在授予 (Grant) 下拉列表，您可以选择以下选项之一：
  - 允许 (Permit)：允许指定的命令（例如，permit show, permit con\* Argument terminal）。
  - 拒绝 (Deny)：拒绝指定的命令（例如，deny mtrace）。

- **始终拒绝 (Deny Always)**：覆盖在其他命令集中允许的命令（例如，clear auditlogs）

注释 单击操作图标以增加或减少授予、命令和参数字段的列宽。

**步骤 7** 选中允许以下未列出的任何命令 (**Permit any command that is not listed below**) 复选框允许未在“授予”列中指定为允许、拒绝或始终拒绝的命令和参数。

## TACACS+ 配置文件

TACACS+ 配置文件控制设备管理员的初始登录会话。会话是指每个单独的身份验证、授权或记帐请求。对网络设备的会话授权请求会引发思科 ISE 响应。响应包括由网络设备解释的令牌，限制可能在会话期限执行的命令。用于设备管理访问服务的授权策略可以包含单个外壳配置文件和多个命令集。TACACS+ 配置文件定义分为两个组件：

- 常见任务
- 自定义用户属性

“TACACS+ 配置文件”页面存在两种视图（**工作中心 (Work Centers) > 设备管理 (Device Administration) > 策略结果 (Policy Results) > TACACS 配置文件 (TACACS Profiles)**）- “任务属性视图” (Task Attribute View) 和 “原始视图” (Raw View)。您可以使用“任务属性视图” (Task Attribute View) 输入普通任务，并在“任务属性视图” (Task Attribute View) 和 “原始视图” (Raw View) 中创建自定义属性。

您可通过**常见任务 (Common Tasks)** 部分为配置文件选择并配置常用的属性。这里包含的属性为与外壳服务特别相关的 TACACS+ 协议草案说明定义的那些属性。但是值可用于来自其他服务的请求授权。在**任务属性视图 (Task Attribute View)** 中，思科 ISE 管理员可以设置分配给设备管理员的权限。

- 外壳
- 思科 WLC
- 思科 Nexus
- 通用

**自定义属性 (Custom Attributes)** 部分允许您配置其他属性。它提供不被**常见任务 (Common Tasks)** 部分识别的属性列表。每个定义包括属性名称、该属性是强制还是可选的说明和属性值。



注释 您可以为启用 TACACS 的网络设备定义总共 24 个任务属性。如果定义的任务属性超过 24 个，则不会将这些属性发送到启用 TACACS 的网络设备。

在**原始视图 (Raw View)** 中，可以在属性名称及其值之间使用等号 (=) 输入强制属性，在属性名称及其值之间使用一个星号 (\*) 可输入可选属性。**原始视图 (Raw View)** 中输入的属性反映在**任务属性视图 (Task Attribute View)** 中的自定义属性 (**Custom Attributes**) 部分，反之亦然。**原始视图 (Raw View)**

部分也用于将属性列表（例如，另一产品的属性列表）从剪贴板复制并粘贴到思科 ISE 上。可为非外壳服务定义自定义属性。

## 创建 TACACS+ 配置文件

要创建 TACACS+ 配置文件：

**步骤 1** 选择工作中心 (**Work Centers**) > 设备管理 (**Device Administration**) > 策略元素 (**Policy Elements**) > 结果 (**Results** > **TACACS 配置文件 (TACACS Profiles)**)。

**步骤 2** 点击 **Add**。

**步骤 3** 在 **TACACS 配置文件 (TACACS Profile)** 部分中，请输入名称和说明。

**步骤 4** 在任务属性视图 (**Task Attribute View**) 选项卡自定义属性 (**Custom Attributes**) 部分中，点击添加 (**Add**) 输入必要的属性。

## 通过 CLI 更改启用密码

要更改启用密码，请执行以下步骤：

### 开始之前

某些命令会分配到特权模式。因此，只能在设备管理员经过身份验证进入此模式时执行它们。

当设备管理员尝试进入特权模式时，设备会发送特殊的启用身份验证类型。思科 ISE 支持使用单独的启用密码来验证此特殊的启用身份验证类型。当使用内部身份库对设备管理员进行身份验证时，系统将使用单独的启用密码。对于使用外部身份库进行的身份验证，系统将使用相同的密码来进行常规登录。

**步骤 1** 登录到交换机。

**步骤 2** 按 Enter 键显示以下提示符：

```
Switch>
```

**步骤 3** 执行以下命令来配置启用密码。

```
Switch> enable
Password: (Press Enter to leave the password blank.)
Enter Old Password: (Enter the old password.)
Enter New Password: (Enter the new password.)
Enter New Password Confirmation: (Confirm the new password.)
```



**注释** 如果为登录密码和启用密码配置了密码有效期，则在指定时段内未更改密码时，用户账号将禁用。如果将思科 ISE 配置为 TACACS+ 服务器，并在网络设备上配置了启用旁路 (**Enable Bypass**) 选项，则无法通过 CLI（通过 telnet）更改启用密码。选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**，更改内部用户的启用密码。

## 配置全局 TACACS+ 设置

配置全局 TACACS+ 设置

**步骤 1** 选择工作站 (**Work Centers**) > 设备管理 (**Device Administration**) > 设置 (**Settings**)。

在连接设置 (**Connection Settings**) 选项卡，您可以更改所需字段的默认值。

- **单连接支持 (Single Connect Support)**: 如果禁用单连接模式，则 ISE 对每个 TACACS+ 请求使用新的 TCP 连接。

**步骤 2** 在密码更改控制 (**Password Change Control**) 选项卡，定义所需字段以控制是否通过 TACACS+ 允许密码更新。

只有选中此选项，才会启用启用 **Telnet 更改密码 (Enable Telnet Change Password)** 部分中的提示。否则，会启用 **禁用 Telnet 更改密码 (Disable Telnet Change Password)** 提示。密码提示可完全自定义，并可根据需要进行修改。

**步骤 3** 在会话密钥分配 (**Session Key Assignment**) 选项卡，请选择所需的字段以将 TACACS+ 请求链接到会话。

监控节点使用会话密钥来链接来自客户端的 AAA 请求。默认设置为启用 NAS 地址、端口、远程地址和用户字段。

**步骤 4** 点击保存 (**Save**)。

相关主题

[TACACS+ 身份验证设置和共享密钥](#)

## 从思科安全 ACS 将数据迁移至思科 ISE

您可以使用迁移工具导入来自 ACS 5.5 和 5.6 的数据，然后为所有网络设备设置默认 TACACS+ 密钥。导航至 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **概述 (Overview)**，然后在 **准备 (Prepare)** 部分，单击迁移工具链接以打开迁移工具。将工具保存到您的 PC，然后在 migTool 文件夹中，运行 migration.bat 文件以开始迁移过程。有关迁移的完整信息，请参阅您的思科 ISE 版本的 [迁移指南](#)。

## 监控设备管理活动

思科ISE提供各种报告和日志，通过这些报告和日志，您可以查看通过TACACS+配置的设备计费、身份验证、授权和命令计费相关的信息。您可以按需或按计划运行这些报告。

**步骤 1** 选择工作中心 (Work Centers) > 设备管理 (Device Administration) > 报告 (Reports) > ISE 报告 (ISE Reports)。

您还可以在操作 (Operations) > 报告 (Reports) > ISE 报告 (ISE Reports) 页面查看报告。

**步骤 2** 在报告选择器 (Report Selector) 中，展开设备管理 (Device Administration) 以查看、TACACS 记账 (TACACS Accounting)、TACACS 身份验证 (TACACS Authentication)、TACACS 授权 (TACACS Authorization) 和 报告。

**步骤 3** 选择报告并选取您想要使用 **Filters** 下拉列表搜索的数据。

**步骤 4** 在 **Time Range** 中选择您想要查看的数据的时间范围。

**步骤 5** 点击运行 (Run)。

## TACACS 实时日志

下表列出“TACACS+ 实时日志” (TACACS Live Logs) 窗口的字段，其中会显示 TACACS+ AAA 详细信息。此页面的导航路径为：**操作 (Operations) > TACACS > 实时日志 (Live Logs)**。您只能在主 PAN 中查看 TACACS 实时日志。

表 35: TACACS 实时日志

字段名称	使用指南
生成时间 (Generated Time)	根据特定事件触发时间显示系统日志生成时间。
日志记录时间 (Logged Time)	显示监控节点处理和存储系统日志的时间。此列为必选项，无法取消选择。
状态	显示身份验证成功还是失败。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。
详细信息	在单击放大镜图标时显示报告，使您能够深入查看有关所选身份验证方案的更多详细信息。此列为必选项，无法取消选择。
会话密钥 (Session Key)	显示由 ISE 返回到网络设备的会话密钥（在 EAP 成功或 EAP 失败消息中查找）。
用户名	显示设备管理员的用户名。此列为必选项，无法取消选择。
Type	包括两种类型 - 身份验证和授权。显示身份验证或授权已成功或失败的用户名称，或二者均成功和失败的用户名称。此列为必选项，无法取消选择。

字段名称	使用指南
身份验证策略 (Authentication Policy)	显示为特定身份验证选择的策略的名称。
授权策略 (Authorization Policy)	显示为特定授权选择的策略的名称。
ISE 节点 (ISE Node)	显示处理访问请求的 ISE 节点的名称。
网络设备名称	显示网络设备的名称。
网络设备 IP (Network Device IP)	显示访问请求已处理的网络设备的 IP 地址。
网络设备组 (Network Device Groups)	显示网络设备所属相应网络设备组的名称。
设备类型 (Device Type)	显示用于处理来自不同网络设备的访问请求的设备类型。
位置	显示用于处理来自网络设备的访问请求的基于位置的策略。
设备端口 (Device Port)	显示发出访问请求的设备端口号。
故障原因 (Failure Reason)	显示拒绝网络设备发出的访问请求的原因。
远程地址 (Remote Address)	显示唯一标识终端站的 IP 地址、MAC 地址，或任何其他字符串。
匹配的命令集	如果 MatchedCommandSet 属性值存在，则显示该值，或如果 MatchedCommandSet 属性值为空或属性本身不存在于系统日志，则显示一个空值。
外壳配置文件 (Shell Profile)	显示已授予设备管理员用于在网络设备执行命令的权限。

您可以在 TACACS 实时日志 (TACACS Live Logs) 窗口中执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。

- 对列值排序。



---

注释 所有用户自定义将存储为用户首选项。

---



## 第 8 章

# 访客和安全 WiFi

- [思科 ISE 访客服务](#)，第 213 页
- [访客和发起人帐户](#)，第 214 页
- [访客门户](#)，第 223 页
- [发起人门户](#)，第 232 页
- [监控访客和发起人活动](#)，第 241 页
- [访客访问 Web 身份验证选项](#)，第 242 页
- [访客门户设置](#)，第 248 页
- [发起人门户应用设置](#)，第 266 页
- [访客和发起人门户的全局设置](#)，第 272 页
- [访客类型设置](#)，第 273 页
- [发起人组设置](#)，第 273 页
- [最终用户门户](#)，第 276 页
- [自定义最终用户 Web 门户](#)，第 276 页
- [门户内容类型](#)，第 278 页
- [门户的基本自定义](#)，第 279 页
- [门户的高级自定义](#)，第 286 页
- [门户语言自定义](#)，第 303 页
- [自定义访客通知、审批和错误消息](#)，第 307 页
- [门户页面标题、内容和标签的字符限制](#)，第 311 页
- [门户自定义](#)，第 313 页
- [门户语言文件的 HTML 支持](#)，第 314 页

## 思科 ISE 访客服务

使用思科身份识别服务引擎（思科 ISE）访客服务，可以提供对访客（例如宾客、承包商、顾问和客户）的安全网络访问。您可以支持具有基本思科 ISE 许可证的访客，此外，还可以根据公司的基础设施和功能要求，从若干部署选项中选择。

思科 ISE 提供基于 Web 的门户和移动门户，让访客和员工注册公司的网络以及内部资源和服务。

从 Admin 门户，您可以创建和编辑访客和发起人门户，通过定义访客类型配置访客接入权限，以及分配发起人权限，创建和管理访客帐户。

- [访客门户，第 223 页](#)
- [访客类型和用户身份组，第 215 页](#)
- [发起人门户，第 232 页](#)
- [发起人组，第 233 页](#)

## 分布式环境中的最终用户访客门户和发起人门户

思科 ISE 最终用户 Web 门户根据管理、策略服务和监控角色，提供配置、会话支持和报告功能。

- **策略管理节点 (PAN):** 您对用户、设备和最终用户门户所做的配置更改会写入 PAN。
- **策略服务节点 (PSN):** 最终用户门户在 PSN 上运行，后者处理所有会话流量，包括网络访问、客户端调配、访客服务、终端安全评估和分析。如果 PSN 是节点组的一部分，并且一个节点发生故障，则其他节点会检测到故障，并重置任何挂起的会话。
- **监控节点 (MnT 节点):** MnT 节点在我的设备门户、发起人门户和访客门户上收集、聚合和报告有关最终用户和设备活动的的数据。如果主 MnT 节点故障，则辅助 MnT 节点自动成为主 MnT 节点。

## 访客和发起人帐户

- **访客帐户 (Guest Accounts):** 访客通常表示授权访客、承包商、客户，或者需要临时访问网络的其他用户。如果您更愿意使用其中一个访客部署场景以允许员工访问该网络，也可以让员工使用访客帐户。您可以访问发起人门户，查看由发起人和自注册访客创建的访客帐户。
- **发起人帐户 (Sponsor Accounts):** 使用发起人门户为授权访客创建用于安全访问公司网络或互联网的临时帐户。在创建访客帐户后，您还可以使用发起人门户管理这些帐户并向访客提供帐户详细信息。

访客帐户可以通过以下方式创建：

- **发起人 (Sponsors):** 在管理员门户上，您可以为发起人定义访问权限和功能支持，发起人可以访问发起人门户以创建和管理访客帐户。
- **访客 (Guests):** 访客也可以通过自助注册访客门户创建自己的帐户。根据门户配置，自助注册的访客可能需要发起人批准后才能获得登录凭证。

访客还可以使用热点访客门户来访问网络，而无需创建访客帐户及用户名和密码等登录凭证。

- **员工 (Employees):** 包括在身份库（例如 Active Directory、LDAP、内部用户）中的员工同样可以通过已配置的需要凭证的访客门户（发起人管理的和自助注册的访客门户）进行访问。

访客帐户创建完毕后，访客即可使用发起人管理的访客门户进行登录并获得访问网络的权限。

## 访客类型和用户身份组

每个访客帐户必须与访客类型关联。访客类型允许发起人向访客帐户配分各种访问级别以及不同的网络连接时间。这些访客类型与特定的网络接入策略相关联。思科 ISE 包括以下默认访客类型：

- 承包商 (Contractor)：需要在长达 1 年时间内访问网络的用户。
- 日 (Daily)：仅需在 1 至 5 天内访问网络资源的访客。
- 周 (Weekly)：需在数周内访问网络的用户。

在创建访客帐户时，可限制某些发起人组使用特定的访客类型。这种组的成员可以创建仅具有针对其访客类型特定功能的访客。例如，发起人组 ALL\_ACCOUNTS 可设置为仅使用承包商访客类型，而发起人组 OWN\_ACCOUNTS 和 GROUP\_ACCOUNTS 则可设置为仅使用每日和每周访客类型。此外，由于使用自助注册访客门户的自助注册访客通常仅需访问一天，因此您可以向其分配每日访客类型。

访客类型定义访客的用户身份组。

有关详情，请参阅：

- [用户身份组，第 339 页](#)
- [创建用户身份组，第 345 页](#)

## 创建或编辑访客类型

除了创建新的访客类型外，您还可以编辑默认访客类型的默认访问权限和设置。所做更改将应用到使用此访客类型创建的现有访客帐户。登录的访客用户不会看到这些更改，直到这些用户注销并重新登录为止。还可以复制访客类型，使用相同的访问权限创建其他访客类型。

对于现有访客帐户，按访客类型配置该帐户的属性。

如果您正在编辑现有的访客类型以变更时段或其他属性，则新属性不会应用于现有的访客帐户。

要更改现有访客帐户的属性，需使用新属性创建一个新访客类型，并将该访客类型应用于现有的帐户。该帐户会具有新访客类型的所有属性，包括默认访问时间、日期和持续时间。此外，原始访客类型的自定义字段会复制到新访客帐户，即使自定义字段为空。

每个访客类型都有名称、说明以及可以使用此访客类型创建访客帐户的发起人组列表。如下所示，可以按如下方式指定某些访客类型：仅用于自行注册访客，或者不用于（由任何发起人组）创建访客帐户。

---

填写以下字段。

- **访客类型名称 (Guest type name)**：提供一个名称（1 至 256 个字符），将此访客类型与其他访客类型区分开来。
- **说明 (Description)**：提供有关此访客类型推荐用途的更多信息（最多 2000 个字符），例如用于自行注册访客。

- **语言文件 (Language File):** 使用此字段可导出和导入语言文件，文件包含所有受支持语言的电子邮件主题、电子邮件和 SMS 消息的内容。这些语言和内容用于有关过期帐户的通知中，并发送给分配了此访客类型的访客。如果您正在创建新的访客类型，在保存访客类型之前，此功能将被禁用。有关编辑语言文件的详细信息，请参阅 [门户语言自定义](#)，第 303 页。
- **收集其他数据 (Collect Additional Data):** 单击自定义字段 (Custom Fields) 选项，选择要用于向使用此访客类型的访客收集其他数据的自定义字段。

要管理自定义字段，请选择工作中心 (Work Centers) > 访客访问 (Guest Access) > 设置 (Settings) > 自定义字段 (Custom Fields)。

- **最长接入时间**

- **最长帐户持续时间 (Maximum account duration):** 输入分配给此访客类型的访客可以登录的天数、小时数或分钟数。

**注释** 帐户清除策略检查过期的访客帐户，并发送过期通知。此策略每 20 分钟运行一次，因此，如果将帐户持续时间设置为少于 20 分钟，则在清除帐户之前可能不会发出过期通知。

您可以使用**仅在这些日期和时间允许访问 (Allow Access only on these Days and Times)** 选项指定向此类型的访客提供访问权限的持续时间和星期几。

- 您选择的星期几限制了在发起人的日历中可选择的访问日期。
- 当发起人选择持续时间和日期时，发起人门户中将实施最长帐户持续时间。

您在此进行的访问时间设置会影响创建访客帐户时发起人门户上可用的时间设置。

- **登录选项**

- **最大同时登录数 (Maximum simultaneous logins):** 输入分配此访客类型的用户可以同时运行的最大用户会话数。
- **当访客超过限制时 (When Guest Exceeds Limit):** 如果选择最大同时登录数 (Maximum simultaneous logins)，还必须同时选择用户在达到最大登录数后连接时要执行的操作。
  - **断开最早的连接 (Disconnect the oldest connection)**
  - **断开最近的连接 (Disconnect the newest connection):** 如果选择将用户重定向至显示错误信息的门户页面 (Redirect user to a portal page showing an error message)，错误消息将在配置的时长内显示，然后会话断开，用户重定向到访客门户。错误页面的内容在**消息 (Messages) > 错误消息 (Error Messages)**窗口上的“门户页面自定义” (Portal Page Customization) 对话框中进行配置。
- **访客可以注册的最大设备数 (Maximum Devices Guests can Register):** 输入每个访客可以注册的最大设备数。您可以将限制设为小于已为此访客类型的访客注册的设备数的数值。这只会影响新创建的访客帐户。当添加新设备并达到最大值时，最早的设备将断开连接。
- **用于注册访客设备的终端身份组 (Endpoint identity group for guest device registration):** 选择要分配访客设备的终端身份组。思科 ISE 提供 **GuestEndpoints** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。



- **允许访客绕过访客门户 (Allow Guest to bypass the Guest portal):** 允许用户绕过需要提供凭证的访客类型强制网络门户 (Web 身份验证页面)，通过向有线和无线 (dot1x) 请求方或 VPN 客户端提供凭证来访问网络。访客帐户进入活动状态，绕过等待初始登录状态和 AUP 页面，即使 AUP 是必填项也是如此。

如果不启用此设置，用户必须首先通过需要提供凭证的访客强制网络门户登录，然后才能访问网络的其他部分。

- **帐户过期通知**

- **在帐户过期之前 \_\_ 天，发送帐户过期通知 (Send account expiration notification \_\_ days before account expires):** 在帐户过期之前向访客发送通知，指定距离过期还剩多少天、多少小时或多少分钟。
- **查看消息的语言 (View messages in):** 指定在按照您的设置显示电子邮件或 SMS 通知时使用的语言。
- **电子邮件 (Email):** 通过电子邮件发送帐户过期通知。
- **使用自定义设置源 (Use customization from):** 将您为所选门户配置的相同自定义设置应用于此访客类型的帐户过期邮件。
- **复制文本自 (Copy text from):** 重复使用您为另一访客类型的帐户过期电子邮件而创建的电子邮件文本。
- **SMS:** 通过 SMS 发送帐户过期通知。

SMS 的设置与电子邮件通知的设置相同，不同之处在于您选择了**向我发送测试 SMS (Send test SMS to me)** 对应的 SMS 网关。

- **发起人组 (Sponsor Groups):** 指定成员可以使用此访客类型创建访客帐户的发起人组。删除您不希望访问此访客类型的发起人组。

---

### 下一步做什么

- 创建或修改发起人组，以使用此访客类型。有关详细信息，请参阅[发起人组](#)，第 233 页。
- 如果适用，请在自行注册访客门户中将此访客类型分配给自行注册访客。有关详细信息，请参阅[创建自注册访客门户](#)，第 230 页。

## 禁用访客类型

您无法删除最后一个剩余的访客类型，或访客帐户正在使用的访客类型。如果您希望删除使用中的访客类型，请首先确保其不再可供使用。禁用访客类型不会影响到使用该访客类型创建的访客帐户。

以下步骤介绍如何准备和禁用目标访客类型。

- 
- 步骤 1** 确定允许发起人使用目标访客类型创建访客的发起人组。依次选择 > **访客访问 (Guest Access)** > **配置 (Configure)** > **发起人组 (Sponsor Groups)**，然后打开每个发起人组并检查此发起人组可以使用这些访客类型创建帐户 (**This sponsor group can create accounts using these guest types**) 列表。

- 步骤 2** 确定分配目标访客类型的自注册门户。依次选择**访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals)**。打开每个自注册访客门户。如果门户使用特定访客类型，请展开门户设置 (**Portal Settings**)，并在使用此门户的员工作为访客继承登录选项于：**(Employees using this portal as guests inherit login options from:)** 字段。
- 步骤 3** 打开要删除的访客类型，并删除您在之前的步骤中确定的所有发起人组。此操作会有效地防止所有发起人使用此访客类型创建新的访客帐户。依次选择**访客访问 (Guest Access) > 配置 (Configure) > 访客类型 (Guest Type)**。

## 安排清除过期访客帐户的时间

当活动或挂起访客帐户达到其帐户持续时间（按照创建帐户时发起人的定义）结束时，帐户过期。当访客帐户过期时，受影响的访客无法访问网络。发起人可以在清除之前延长到期帐户的期限。然而，帐户清除之后，发起人必须创建新的帐户。

清除过期访客帐户时，关联的终端以及报告和日志记录信息仍然保留。

默认情况下，思科 ISE 每 15 天自动清除一次过期访客帐户。**Date of next purge** 指示下次清除的时间。您还可以：

- 计划每 X 天执行清除操作。第一次清除会在 X 天之后在指定的清除时间 (**Time of Purge**) 进行，然后每 X 天执行一次清除操作。
- 计划每 X 周在指定周的固定某天执行清除操作。第一次清除在下一周的某天 (**Day of Week**) 的指定的清除时间 (**Time of Purge**) 执行，随后清除会每 X 周 (X 为设置的周值) 在指定的日期和时间进行。例如，如果您在本周的星期一设置每 5 周在星期四执行清除操作，则下次清除将在本周的星期四进行，而不是 5 周之后的星期四。
- 通过点击**立即清除 (Purge Now)** 可立即强制执行清除操作。

如果思科 ISE 服务器在按计划运行清除时关闭，不会执行清除。假设服务器在下一次计划清除时可以运行，清除进程将在那时再次运行。

**步骤 1** 选择**访客访问 (Guest Access) > 设置 (Settings) > 访客帐户清除策略 (Guest Account Purge Policy)**。

**步骤 2**

**步骤 3** 选择以下选项之一：

- 点击 **Purge Now**，立即清除过期的访客帐户记录。
- 选中 **Schedule purge of expired guest accounts** 复选框，安排清除。

注释 每次完成清除后，**Date of next purge** 重置为下一次计划清除。

**步骤 4** 指定多少 **days of inactivity** 后清除思科 ISE 数据库中为 LDAP 和 Active Directory 用户维护的用户特定门户记录。

**步骤 5** 点击 **Save**。如果不想保存对设置进行的任何更新，请点击 **Reset** 以恢复为上次保存的值。

## 添加用于创建访客帐户的自定义字段

当提供访客接入时，可能不仅仅从访客收集其姓名、邮箱地址和电话号码信息。可以将思科 ISE 提供的自定义字段用于针对公司需求收集其他访客信息。可以将自定义字段与访客类型，以及自注册的访客门户和发起人门户相关联。思科 ISE 不提供任何默认自定义字段。

### 下一步做什么

在以下情况下，可以包含所需的自定义字段：

- 当定义访客类型，使得使用该访客类型创建的帐户将包含此信息时。请参阅[创建或编辑访客类型，第 215 页](#)。
- 当配置发起人门户，供发起人在创建访客帐户的时候使用时。请参阅[自定义发起人门户，第 240 页](#)。
- 当使用自注册的访客门户从自注册访客请求信息时。请参阅[创建自注册访客门户，第 230 页](#)。

## 为邮件通知指定邮箱地址和 SMTP 服务器

通过思科 ISE，可以将邮件发送到发起人和访客，向他们通知相关信息和说明。可以配置 SMTP 服务器来传送这些邮件通知。还可以指定将通知发送到访客的发件人邮箱地址。

## 分配访客位置和 SSID

访客位置定义时区的名称，并由 ISE 用于执行已登录访客的时间相关设置。访客位置由创建访客帐户的发起人以及由自行注册的访客分配给访客帐户。默认访客位置为 San Jose。如果未添加其他访客位置，则为所有帐户分配此访客位置。除非您创建一个或多个新位置，否则无法删除 San Jose 访客位置。除非所有访客都将位于与 San Jose 相同的时区中，否则请创建至少一个具有所需时区的访客位置。



**注释** 访客访问时间基于访客位置的时区。如果访客位置的时区与系统时区不匹配，访客用户可能无法登录。在这种情况下，访客用户可能会收到“身份验证失败”错误。您可能会在调试报告中看到“访客活动时间段未开始 (Guest active time period not yet started)”错误消息。作为解决方法，您可以使用管理帐户 (Manage Accounts) 选项来调整访客接入开始时间，以匹配访客用户的本地时区。

您在此处添加的 SSID 可供发起人门户使用，因此发起人可以告知访客要连接的 SSID。

如果访客位置或 SSID 在发起人门户中进行配置或者分配给访客帐户，则无法删除。

**步骤 1** 要添加、编辑或删除访客门户和发起人门户的访客位置和 SSID，请选择[访客访问 \(Guest Access\)](#) > [设置 \(Settings\)](#) > [访客位置和 SSID \(Guest Locations and SSIDs\)](#)。

**步骤 2**

**步骤 3** 对于 **Guest Locations**：

- a) 对于需要支持的每个时区，请输入 **Location name** 并从下拉列表中选择 **Time zone**。
- b) 点击 **Add**。

**注释** 在 Guest Location 中，位置的名称、时区的名称和 GMT 时差是静态的；无法对其进行更改。GMT 时差不随夏令时更改而更改。GMT 偏移与列表中显示的相反。例如，*Etc/GMT+3* 实际上是 GMT-3。

#### 步骤 4 对于 Guest SSIDs:

- a) 输入将可供访客在访客位置使用的网络的 **SSID** 名称。
- b) 点击添加 (**Add**)。

**步骤 5** 点击保存 (**Save**)。要恢复为上次保存的值，请点击重置 (**Reset**)。

#### 下一步做什么

如果您已添加新的访客位置或 SSID，则可以：

- 提供 SSID 以供发起人在创建访客帐户时使用。请参阅[发起人门户的门户设置](#)，第 267 页。
- 向发起人组中添加访客位置，以使分配到该组的发起人在创建访客帐户时可以使用这些访客位置。请参阅[配置发起人组](#)，第 234 页。
- 使用自行注册的访客门户分配自行注册的访客可用的访客位置。请参阅[创建自注册访客门户](#)，第 230 页。
- 对于现有访客帐户，请手动编辑它们以添加 SSID 或位置。

## 访客密码策略规则

对于访客密码，思科 ISE 具有以下内置规则：

- 访客密码策略适用于发起人门户、自注册门户、以 CSV 文件格式上传的帐户、使用 ERS API 创建的密码和用户创建的密码。
- 对访客密码策略的更改不会影响现有用户，直到访客密码过期并且需要更改为止。
- 密码区分大小写。
- 不能使用特殊字符 <、>、/、和 %。
- 最低长度和最小字符数要求适用于所有密码。
- 密码不能与用户名一样。
- 新密码不能与当前密码一样。
- 与访客帐户到期情况不一样，访客在密码到期之前不会收到通知。当访客密码到期时，发起人可以将密码重置为随机密码，或者访客也可以使用当前的登录凭证登录，然后更改其密码。



**注释** 客户默认用户名是四位字母字符，而密码是四位数字字符。简短、易于记忆的用户名和密码适用于短期客户。如果需要，您可以在 ISE 中更改用户名和密码长度。

## 设置访客密码策略和到期时间

您可以为所有访客门户定义密码策略。访客密码策略决定着如何为所有访客帐户生成密码。密码可以是字母、数字或特殊字符的组合。您还可以设置访客密码到期的天数，使系统在经过这些天之后要求访客重置其密码。

访客密码策略适用于发起人门户、自注册门户、以 CSV 文件格式上传的帐户、使用 ERS API 创建的密码和用户创建的密码。

### 下一步做什么

您应自定义与密码策略相关的错误消息以提供密码要求。

1. 选择访客访问 (Guest Access) > 配置 (Configure) > 发起人管理的访客门户或自注册访客门户 (Sponsored-Guest Portals or Self-Registered Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 错误消息 (Error Messages)。
2. 搜索关键字 policy。

## 访客用户名策略规则

对于访客用户名策略，思科 ISE 支持以下内置规则：

- 对访客用户名策略的更改不会影响现有用户，直到访客帐户过期并且需要更改为止。
- 不能使用特殊字符 <、>、/、和 %。
- 最低长度和最小字符数要求适用于所有系统生成的用户名，包括基于邮件地址的用户名。
- 密码不能与用户名一样。

## 设置访客用户名策略

您可以对访客用户名的创建规则进行配置。生成的用户名可以根据电子邮件地址或基于访客的名字和姓氏创建。当创建多个访客或访客姓名和电子邮件地址不可用时，发起人还可以创建任意数量的访客帐户以节省时间。随机生成的访客用户名由字母、数字和特殊字符组成。这些设置会影响所有访客。

### 下一步做什么

您应自定义与用户名策略相关的错误消息以提供用户名要求。

1. 选择访客访问 (Guest Access) > 配置 (Configure) > 发起人管理的访客门户、自注册访客门户、发起人门户或我的设备门户 (Sponsored-Guest Portals, Self-Registered Guest Portals, Sponsor Portals, or My Devices Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 错误消息 (Error Messages)。
2. 搜索关键字 policy。

## SMS 运营商和服务

SMS 服务会向使用需要提供凭证的访客门户的访客发送 SMS 通知。如果计划发送 SMS 消息，请启用此服务。尽可能配置和提供免费的 SMS 服务运营商，以降低您公司的支出。

思科 ISE 支持向其自己的用户提供免费 SMS 服务的各种移动服务运营商。您可以使用这些运营商，而无需签订服务合同且无需在思科 ISE 中配置其帐户凭证。其中包括 ATT、Orange、Sprint、T-Mobile 和 Verizon。

您还可以添加其他提供免费 SMS 服务的移动服务运营商或 Click-A-Tell 等全球 SMS 服务运营商。默认全局 SMS 服务运营商要求签订服务合同并且您必须在思科 ISE 中配置其帐户凭证。

- 如果自行注册访客在 Self-Registration 窗体中选择自己的免费 SMS 服务运营商，系统将免费向他们发送包含其登录凭证的 SMS 通知。如果他们不选择 SMS 服务提供商，则由公司签约的默认全局 SMS 服务提供商发送 SMS 通知。
- 若要允许发起人向他们创建的访客发送 SMS 通知，应自定义发起人门户并选择所有可用的相应 SMS 服务提供商。如果没有为发起人门户选择任何 SMS 服务提供商，将由公司签约的默认全局 SMS 服务提供商提供 SMS 服务。

在思科 ISE 中，SMS 提供商配置为 SMS 网关。SMS 网关会将来自思科 ISE 的电子邮件转换为 SMS。

### 配置 SMS 网关以向访客发送 SMS 通知

您必须在思科 ISE 中对 SMS 网关进行如下设置：

- 使发起人能够向访客手动发送 SMS 通知以提供访客登录凭证和密码重置说明。
- 使访客能够在成功注册之后使用其登录凭证自动接收 SMS 通知。
- 使访客能够自动接收关于在访客帐户到期之前要采取的操作的 SMS 通知。

当在这些字段输入信息时，您应使用您的 SMS 运营商帐户的具体信息更新 [ ]（例如 [USERNAME]、[PASSWORD]、[PROVIDER\_ID] 等）中的所有文本。

#### 开始之前

配置用于 SMS Email Gateway 选项的默认 SMTP 服务器。

#### 下一步做什么

如果您配置了新的 SMS 网关，您可以：

- 选择要在将有关帐户即将到期的 SMS 通知发送到访客时使用的 SMS 运营商。请参阅[创建或编辑访客类型](#)，第 215 页。
- 指定哪些已配置的 SMS 运营商应显示在 Self-Registration 表单以供自注册用户选取。请参阅[创建自注册访客门户](#)，第 230 页。

## 访客门户

当访问公司的人员希望使用公司网络访问互联网或者您的网络上的资源和服务时，您可以通过访客门户为他们提供网络访问权限。在进行配置后，员工可以使用这些访客门户访问您的公司网络。

三种默认访客门户：

- 热点访客门户：授予网络访问权限，而不需要任何凭证。通常，必须在授予网络访问权限之前接受可接受的用户策略 (AUP)。
- 发起人管理的访客门户：网络访问权限由创建访客帐户的发起人授予，并为访客提供登录凭证。
- 自注册访客门户：访客可以创建自己的帐户和凭证，可能需要发起人批准后才能获得网络访问权限。

思科 ISE 可托管多个访客门户，包括一组预定义的默认门户。

默认门户主题有标准思科品牌推广，您可以通过管理员门户进行自定义。

无线设置有自己的默认主题 (CSS)，您可以修改一些基本设置，如徽标、横幅、背景图像、颜色和字体。在思科 ISE 中，还可以选择更改更多设置来进一步自定义门户，并进入高级自定义设置。

## 访客门户的凭证

思科 ISE 通过要求访客使用各种凭证，提供安全的网络访问。您可以要求访客使用以下一个或多个凭证登录。

- 用户名：必填。适用于使用最终用户门户（热点访客门户除外）的所有访客，系统根据用户名策略派生用户名。用户名策略仅适用于系统生成的用户名，而不适用于使用访客 API 编程接口或自行注册流程指定的用户名。您可以在[访客访问 \(Guest Access\) > 设置 \(Settings\) > 访客用户名策略 \(Guest Username Policy\)](#) 中配置应用于用户名的策略设置。可以通过邮件、SMS 或打印形式告知访客其用户名。
- 密码：必填。适用于使用最终用户门户（热点访客门户除外）的所有访客，根据密码策略派生密码。您可以在[访客访问 \(Guest Access\) > 设置 \(Settings\) > 访客密码策略 \(Guest Password Policy\)](#) 中配置应用于密码的策略设置。可以通过邮件、SMS 或打印形式告知访客其密码。
- 访问代码：可选。适用于使用热点访客门户和需要提供凭证的访客门户的访客。访问代码主要是提供给实际存在的访客（通过白板以肉眼方式或通过前台接待人员以口头方式）的本地已知代码。不在场的人无法获悉和使用此代码以获得网络访问权限。如果启用了访问代码设置，将出现以下情况：
  - 系统会提示发起人管理的访客在 Login 页面上输入此代码（以及用户名和密码）。

- 系统会提示使用热点访客门户的访客在可接受使用政策 (AUP) 页面输入此代码。
- 注册码：可选。适用于自行注册访客，在如何向自行注册访客提供此代码方面其类似于访问代码。如果启用注册代码设置，系统会提示自行注册访客在 **Self-Registration** 窗体上输入此代码。

用户名和密码可由您公司的发起人提供（发起人管理的访客），也可以将需要提供凭证的访客门户配置为允许访客自行注册以获取这些凭证。

#### 相关主题

[访客类型和用户身份组](#)，第 215 页

## 访客使用热点访客门户进行访问

思科 ISE 提供的网络接入功能包括“热点”，访客无需凭证登录即可使用这些接入点访问互联网。当访客使用计算机或任何设备的浏览器连接到热点网络并试图连接到某个网站时，就会被自动重定向至热点访客门户。该功能同时支持有线和无线 (Wi-Fi) 连接。

作为备选访客门户，热点访客门户允许您提供网络接入而无需访客具备用户名和密码，由此可减少访客帐户进行管理的需求。相反，思科 ISE 与网络接入设备 (NAD) 和设备注册 Web 身份验证相配合，向访客设备直接提供网络接入。某些情况下，访客可能需要使用访问代码才能登录。通常情况下，该访问代码是本地提供给公司内部实际存在的访客的代码。

如果您支持热点访客门户：

- 根据热点访客门户的配置和设置，如果满足访客访问条件，访客即可访问网络。
- 思科 ISE 为您提供默认访客身份组、访客终端，使您可以密切跟踪访客设备。

## 访客使用需要提供凭证的访客门户进行访问

您可以使用需要提供凭证的访客门户识别并授权外部用户临时访问内部网络和服务以及互联网。发起人可以为能够通过门户的 **Login** 页面中输入这些凭证来访问网络的授权访问者创建临时用户名和密码。

可以设置需要提供凭证的访客门户，以便访客可以使用获取的用户名和密码登录：

- 来自发起人。在此访客流程中，当访客进入公司场地并设置具有单独访客帐户时，发起人（例如前台接待人员）会向其致意。
- 在访客使用可选注册代码或访问代码自行注册后。在此访客流程中，访客可以在没有任何人为交互的情况下访问互联网，并且思科 ISE 可确保这些访客具有可用于合规的唯一标识符。
- 在访客使用可选注册代码或访问代码自行注册后，但是仅在发起人批准对访客帐户的请求后。在此访客流程中，系统会为访客提供网络访问权限，但是仅在执行额外的筛选后才提供。

您还可以强制用户在登录时输入新密码。

通过思科 ISE，您可以创建多个需要提供凭证的访客门户，您可以使用这些门户基于不同条件允许进行访客访问。例如，对于每月承包商，您可能具有与用于日常访问者的门户不同的门户。



## 员工使用需要提供凭证的访客门户进行访问

员工还可以通过使用员工凭证在须提供凭证的访客门户上注册来访问网络，只要为该门户配置的身份源序列可以获取其凭证即可。

## 访客设备合规性

当访客和非访客通过需要提供凭证的访客门户访问网络时，您可以在允许获得访问权限之前检查其设备的合规性。可以将他们路由至“客户端调配”(Client Provisioning)窗口，要求他们首先下载终端安全评估代理，查看其终端安全评估配置文件，验证他们的设备是否合规。具体做法是，在需要提供凭证的访客门户的**访客设备合规性设置 (Guest Device Compliance Settings)**中启用此选项，此门户将在访客流程中显示“客户端调配”(Client Provisioning)窗口。



**注释** 访客流程中的客户端终端安全评估仅支持临时代理。

客户端调配服务为访客提供终端安全评估和补救。客户端调配门户只通过中心网络身份验证 (CWA) 访客部署提供。访客登录流程执行 CWA，在执行可接受的使用策略和更改密码检查后，需要提供凭证的访客门户被重新定向到客户端调配门户。终端安全评估子系统在网络访问设备上执行授权更改 (CoA)，在终端安全评估后，重新授权客户端连接。

## 访客门户配置任务

您可以使用默认门户及其默认设置，例如证书、终端身份组、身份源序列、门户主题、图像和思科 ISE 提供的其他详细信息。如果您不想使用默认设置，则应创建新门户或编辑现有门户来满足需要。如果要创建多个具有相同设置的门户，则可以复制门户。

在创建新门户或编辑默认门户后，您必须授权使用该门户。授权使用门户后，您所进行的任何后续配置更改便会立即生效。

如果您选择删除门户，则必须先删除与其关联的任何授权策略规则和授权配置文件，或者将其修改为使用其他门户。

使用以下针对配置不同访客门户相关任务编制的表格。

任务	热点访客门户	发起人管理的访客门户	自注册的访客门户
<a href="#">启用策略服务，第 226 页</a>	必填	必填	必填
<a href="#">为访客门户添加证书，第 226 页</a>	必填	必填	必填
<a href="#">创建外部身份源，第 226 页</a>	不适用	必填	必填

任务	热点访客门户	发起人管理的访客门户	自注册的访客门户
创建身份源序列，第 227 页	不适用	必填	必填
创建终端身份组，第 440 页	必填	不是必填项（由访客类型定义）	不是必填项（由访客类型定义）
创建热点访客门户，第 228 页	必填	不适用	不适用
创建发起人管理的访客门户，第 229 页	不适用	必填	不适用
创建自注册访客门户，第 230 页	不适用	不适用	必填
授权门户，第 230 页	必填	必填	必填
自定义访客门户，第 232 页	可选	可选	可选

## 启用策略服务

为了支持思科 ISE 最终用户 Web 门户，您必须在用于托管门户的节点上启用门户-策略服务。

**步骤 1** 依次选择管理 (Administration) > 系统 (System) > 部署 (Deployment)。

**步骤 2** 点击节点并点击 **Edit**。

**步骤 3** 在常规设置 (General Settings) 选项卡下，选中策略服务 (Policy Service) 复选框。

**步骤 4** 选中启用会话服务 (Enable Session Services) 复选框。

**步骤 5** 点击保存 (Save)。

## 为访客门户添加证书

如果不希望使用默认证书，您可以添加一个有效证书，并将其分配到证书组标签。用于所有最终用户 Web 门户的默认证书组标签为默认门户证书组。

## 创建外部身份源

思科 ISE 能够与外部身份源（例如 Active Directory、LDAP、RADIUS 令牌和 RSA SecurID 服务器）连接，以获取用于身份验证和授权的用户信息。外部身份源还包括执行基于证书的身份验证所需的证书身份验证配置文件。

**步骤 1** 选择管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources)。

步骤 2 选择以下选项之一：

- 选择证书身份验证配置文件 (**Certificate Authentication Profile**) 执行基于证书的身份验证。
- 选择 **Active Directory** 作为外部身份源连接到 Active Directory。有关更多详细信息，请参阅[将 Active Directory 用作外部身份源，第 349 页](#)。
- 选择 **LDAP** 以添加 LDAP 身份源。有关更多详细信息，请参阅[LDAP，第 370 页](#)。
- 选择 **RADIUS 令牌 (RADIUS Token)** 以添加 RADIUS 令牌服务器。有关更多详细信息，请参阅[RADIUS 令牌身份源，第 382 页](#)。
- 选择 **RSA SecurID** 以添加 RSA SecurID 服务器。有关更多详细信息，请参阅[RSA 身份源，第 387 页](#)。

## 创建身份源序列

### 开始之前

确保您已经在思科 ISE 中配置了外部身份源。

要执行以下任务，您必须是超级管理员或系统管理员。

要允许访客用户通过本地 WebAuth 进行身份验证，必须同时配置访客门户身份验证源和身份源序列，使它们包含相同的身份存储区。

步骤 1 选择 **管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences) > 添加 (Add)**。

步骤 2 输入身份源序列的名称。您还可以输入可选的说明。

步骤 3 选中 **Select Certificate Authentication Profile** 复选框并为基于证书的身份验证选择证书身份验证配置文件。

步骤 4 在**选定列表 (Selected List)** 字段中选择您希望包括在身份源序列中的数据库。

步骤 5 在**选定列表 (Selected List)** 字段中重新调整数据库的顺序，调整为您希望思科 ISE 搜索数据库的顺序。

步骤 6 如果无法访问所选身份库进行身份验证，请在 **高级搜索列表** 区域中选择以下选项之一：

- 请勿访问序列中的其他库并将 **“AuthenticationStatus”** 属性设置为 **“ProcessError”**
- 将用户视为未找到，然后继续到序列中的下一个库

在处理请求时，思科 ISE 会按照序列搜索这些身份源。确保“选定列表” (Selected list) 字段所列出的身份源的顺序是您希望思科 ISE 搜索身份源的顺序。

步骤 7 点击 **Submit** 创建您可以稍后在策略中使用的身份源序列。

## 创建终端身份组

思科 ISE 将其所发现的终端划分至相应的终端身份组。思科 ISE 拥有若干个系统定义的终端身份组。您还从**终端身份组 (Endpoint Identity Groups)** 窗口创建更多终端身份组。您可以编辑或删除您已创建的终端身份组。只能编辑系统定义的终端身份组的说明。无法编辑或删除这些组的名称。

**步骤 1** 选择 **管理 (Administration) > 身份管理 (Identity Management) > 组 (Groups) > 终端身份组 (Endpoint Identity Groups)**。

**步骤 2** 单击添加。

**步骤 3** 为您想要创建的终端身份组输入名称（请勿在终端身份组的名称中包含空格）。

**步骤 4** 为您想要创建的终端身份组输入说明。

**步骤 5** 单击 **Parent Group** 下拉列表，选择您要与新创建的终端身份组关联的终端身份组。

**步骤 6** 点击提交。

## 创建热点访客门户

您可以提供热点访客门户，以使访客能够在无需用户名和密码进行登录的情况下连接到网络。进行登录可能需要访问代码。

您可以创建新的热点访客门户，也可以编辑或复制现有热点访客门户。您可以删除任何热点访客门户，包括思科 ISE 提供的默认门户。

您在 **Portal Behavior and Flow Settings** 选项卡上对 **Page Settings** 进行的任何更改都会反映在访客流程图中的图形流程中。如果您启用某个页面（例如 AUP 页面），则该页面会显示在流程中，并且访客将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除，并为访客显示下一个已启用页面。

所有页面设置（**Authentication Success Settings** 除外）都可选。

### 开始之前

- 确保您具有配置用于此门户的所需证书和终端身份组。
- 确保思科 ISE 支持访客将为热点门户连接到的 WLC。请参阅思科 ISE 版本对应的《[身份服务引擎网络组件兼容性](#)》指南，。

**步骤 1** 选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate)**。

**步骤 2** 如果是创建新门户，请在 **Create Guest Portal** 对话框中，选择 **Hotspot Guest Portal** 作为门户类型，然后单击 **Continue**。

**步骤 3** 在 **门户名称 (Portal Name)** 中提供唯一的门户名称，并在 **说明 (Description)** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

**步骤 4** 使用 **语言文件 (Language File)** 下拉菜单导出和导入要与门户一起使用的语言文件。

**步骤 5** 更新 **Portal Settings** 中的端口、以太网接口、证书组标签、终端身份组等的默认值，然后定义适用于整体门户的行为。

**步骤 6** 更新以下适用于每个特定页面的设置：

- **Acceptable Use Policy (AUP) Page Settings** - 要求访客接受可接受使用策略。

- **Post-Access Banner Page Settings** - 通知访客其访问状态以及任何其他附加操作（如果需要）。
- **VLAN DHCP 释放页面设置 (VLAN DHCP Release Page Settings)** - 从访客 VLAN 释放访客设备 IP 地址并进行更新，以访问网络上的其他 VLAN。
- **身份验证成功设置 (Authentication Success Settings)** - 指定访客通过身份验证后应看到的内容。
- **支持信息页面设置 (Support Information Page Settings)** - 帮助访客提供服务台可以用于排除网络接入问题的信息。

**步骤 7** 点击**保存 (Save)**。系统生成的 URL 显示为门户测试 URL (**Portal test URL**)，您可以使用它来访问门户并进行测试。

### 下一步做什么

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。

## 创建发起人管理的访客门户

您可以提供发起人管理的访客门户，让指定发起人向访客授予访问权限。

您可以创建一个新的发起人管理的访客门户，也可以编辑或复制现有门户。您可以删除任何发起人管理的访客门户，包括思科 ISE 提供的默认门户。

您在 **Portal Behavior and Flow Settings** 选项卡上对 **Page Settings** 进行的任何更改都会反映在访客流程图中的图形流程中。如果您启用某个页面（例如 AUP 页面），则该页面会显示在流程中，并且访客将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除，并为访客显示下一个已启用页面。

通过以下所有页面设置，您可以为访客显示可接受使用政策 (AUP) 并要求访客接受政策：

- 登录页面设置
- 可接受使用政策 (AUP) 页面设置
- BYOD 设置

### 开始之前

确保您具有为配合此门户使用而配置的所需证书、外部身份源和身份源序列。

### 下一步做什么



**注释** 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，ISE 会选择第一个活动 PSN。

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。

## 创建自注册访客门户

您可以提供自注册门户以允许访客自行注册并创建自己的帐户，从而可以访问网络。您还可以要求这些帐户须经发起人批准后才能授予访问权限。

您可以创建新的自注册访客门户，也可以编辑或复制现有的门户。您可以删除任何自注册访客门户，包括思科 ISE 提供的默认门户。

您在 **Portal Behavior and Flow Settings** 选项卡上对 **Page Settings** 进行的任何更改都会反映在访客流程图中的图形流程中。如果您启用某个页面（例如 AUP 页面），则该页面会显示在流程中，并且访客将在门户中体验该页面。如果禁用该页面，则系统会从流程中将其删除，并为访客显示下一个已启用页面。

通过以下所有页面设置，您可以为访客显示可接受使用政策 (AUP) 并要求访客接受政策：

- 登录页面设置
- 自注册页面设置
- 自注册成功页面设置
- 可接受使用政策 (AUP) 页面设置
- BYOD 设置

### 开始之前

确保您已为该门户配置了必要的证书、外部身份源和身份源序列。

### 下一步做什么



---

**注释** 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，ISE 会选择第一个活动 PSN。

---

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。

## 授权门户

当授权门户时，将会设置网络访问的网络授权配置文件和规则。

### 开始之前

您必须先创建门户，然后才能对其进行授权。

---

**步骤 1** 为门户设置特殊授权配置文件。

**步骤 2** 为配置文件创建授权策略规则。

## 创建授权配置文件

各门户要求您为其设置特殊的授权配置文件。

### 开始之前

如果不打算使用默认门户，您必须先创建门户以便将门户名称与授权配置文件关联。

### 下一步做什么

您应当创建门户授权策略规则，用于新创建的授权配置文件。

## 创建用于热点和 MDM 门户的授权策略规则

要配置供门户在响应用户（访客、发起人、员工）的访问请求时使用的重定向 URL，请为该门户定义授权策略规则。

url-redirect 会根据门户类型采取以下形式，其中：

*ip:port*: IP 地址和端口号

*PortalID*: 唯一端口名称

对于热点访客门户：

`https://ip:port/guestportal/gateway?sessionID=SessionIdValue&portal=PortalID&action=cwa&type=drw`

对于移动设备管理 (MDM) 门户：

`https://ip:port/mdmportal/gateway?sessionID=SessionIdValue&portal=PortalID&action=mdm`

**步骤 1** 依次选择策略 (Policy) > 授权 (Authorization) 以在标准 (Standard) 策略下创建新授权策略。

如果已启用策略集，选择您计划用于此门户的策略集，展开授权策略，并添加新规则。

**步骤 2** 对于条件 (Conditions)，请选择要用于门户验证的终端身份组。例如，对于热点访客门户，选择默认的 **GuestEndpoints** 终端身份组；而对于 MDM 门户，选择默认的 **RegisteredDevices** 终端身份组。

**注释** 热点访客门户支持重新身份验证和终止 CoA 类型。仅当“热点访客门户”中选择“重新授权 CoA 类型”时，您可将 Network Access:UseCase EQUALS Guest Flow 用作热点访客授权策略中的一个验证条件。

**步骤 3** 对于 Permissions，请选择创建的门户授权配置文件。



**注释** 在使用启用了 MAC 选项的字典属性创建授权条件（例如 RADIUS.Calling-Station-ID）时，必须使用 Mac 运算符（例如 Mac\_equals）支持不同的 MAC 格式。

## 自定义访客门户

可以通过自定义门户主题、更改门户页面上的 UI 元素以及编辑向用户显示的错误消息与通知来自定义门户外观和用户（访客、发起人，在适当的情况下也可以是员工）体验。有关自定义门户的详细信息，请参阅 [自定义最终用户 Web 门户](#)，第 276 页。

## 发起人门户

发起人门户是思科 ISE 访客服务主要的组件之一。使用发起人门户，发起人可以为授权的访客创建和管理临时帐户，以安全地访问公司网络或互联网。创建访客帐户后，发起人还可以使用发起人门户以打印文件、邮件或短信的形式向访客提供帐户详细信息。向自助注册的访客提供对公司网络的访问权限之前，系统可能会通过邮件要求发起人批准其访客帐户。

## 在发起人门户上管理客户帐户

### 发起人门户登录流程

发起人组指定分配给发起人用户的一组权限。当发起人登录发起人门户时：

1. ISE 验证发起人的凭证。
2. 如果发起人成功通过身份验证，思科 ISE 会搜索所有可用发起人组，以查找发起人所属的发起人组。如果符合以下两个条件，则发起人匹配或属于发起人组：
  - 发起人是一个已配置成员组的成员。
  - 如果您使用的是其他条件，则此发起人的所有条件评估为 `true`。
3. 如果发起人属于发起人组，则发起人将从此组获取权限。发起人可以属于多个发起人组，在此情况下，这些组的权限将合并。如果发起人不属于任何发起人组，则登录发起人门户时将失败。

发起人组及其权限独立于发起人门户。无论发起人登录哪个发起人门户，均使用相同的算法来匹配发起人组。

### 使用发起人门户

使用发起人门户为授权访问者创建用于安全访问企业网络或互联网的临时访客帐户。在创建访客帐户后，可以使用发起人门户管理这些帐户并向访客提供帐户详细信息。

在发起人门户上，发起人可以单独创建新的访客帐户，或从文件导入一组用户。



**注释** 从外部身份存储区（例如 Active Directory）授权的 ISE 管理员可以是发起人组的一部分。但是，内部管理员帐户（例如，默认“管理员”帐户）不能是发起人组的一部分。

有多种方法可打开发起人门户：



- 在管理员控制台中，使用**管理帐户 (Manage Accounts)** 链接。在管理员控制台上，点击**访客访问 (Guest Access) > 管理帐户 (Manage Accounts)**。点击**管理帐户 (Manage Accounts)** 时，您将分配到可访问 ALL\_ACCOUNTS 的默认发起人组。可以创建新的访客帐户，但无法通知这些访客，因为没有电子邮件地址可用于接收来自访客的帐户激活请求。具有相同权限的发起人在登录发起人门户并搜索这些帐户时，可以发送通知。

此步骤要求您在发起人门户的门户行为和流程设置 (**Portal Behavior and Flow Settings**) 窗口中配置的 FQDN 在 DNS 服务器中。

如果通过 NAT 防火墙访问发起人门户，连接将使用端口 9002。

- 在管理员控制台的“发起人门户配置” (Sponsor Portal configuration) 窗口中。单击**访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals)**，打开发起人门户，然后单击**说明 (Description)** 字段右侧的门户测试 URL (**Portal Test URL**) 链接。
- 在浏览器中，打开在发起人门户的门户设置 (**Portal Settings**) 窗口中配置的 URL (FQDN) (必须在 DNS 服务器中定义)。

### 后续操作

有关如何使用发起人门户的信息，请参阅适用于您的 ISE 版本的《发起人门户用户指南》

<https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html>。

## 管理发起人帐户

发起人用户是通过发起人门户创建和管理访客用户帐户的组织员工或承包商。思科 ISE 会通过本地数据库或通过外部轻型目录访问协议 (LDAP)、Microsoft Active Directory 或 SAML 身份库对发起人进行身份验证。如果不使用外部资源，则必须为发起人创建内部用户帐户。

### 发起人组

在使用任何发起人门户时，发起人组控制对发起人的授权。如果发起人是发起人组的成员，则该发起人拥有在该组中定义的权限。

如果发起人属于在发起人组中定义的至少一个成员组，则将该发起人视为发起人组的成员。成员组可以是用户身份组或从外部身份源中选择的组，例如 Active Directory。

一个发起人可以是多个发起人组的成员。如果是，该发起人拥有所有这些组的权限，如下所述：

- 如果在任何组中启用了某个权限，例如“删除访客帐户”，则会授权其该权限。
- 发起人可以使用任何组中的访客类型创建访客。
- 发起人可以在任何组中的位置创建访客。
- 对于诸如批次大小限制的数值，将使用各组中的最大值。

如果发起人不是任何发起人组的成员，则不允许该发起人登录任何发起人门户。

- ALL\_ACCOUNTS: 发起人可以管理所有访客帐户。
- GROUP\_ACCOUNTS: 发起人可以管理同一发起人组中的发起人创建的访客帐户。

- OWN\_ACCOUNTS: 发起人只能管理他们创建的访客帐户。

您可以自定义特定发起人组的可用功能，从而限制或扩展发起人门户的功能。

## 创建发起人帐户并分配到发起人组

要创建内部发起人用户帐户并指定可使用发起人门户的发起人，请执行以下操作：

**步骤 1 注释** 默认身份组 Guest\_Portal\_Sequence 已分配到默认发起人组。

**步骤 2** 选择 在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人组 (Sponsor Groups) > 创建、编辑或复制 (Create, Edit or Duplicate)**，单击成员 (Members)。将发起人用户身份组映射到发起人组。

### 下一步做什么

您还可以创建特定于贵组织的额外用户身份组以用于发起人。依次选择**管理 (Administration) > 身份管理 (Identity Management) > 组 (Groups) > 用户身份组 (User Identity Groups)**。

## 配置发起人组

思科提供默认发起人组。如果不想使用默认选项，可以创建新的发起人组，或者编辑默认的发起人组，并且更改设置。还可以复制发起人组，以创建更多具有相同设置和权限的发起人组。

可以禁用发起人组，阻止发起人组成员登录发起人门户。可以删除任何发起人组，但思科 ISE 提供的默认发起人组除外。

**步骤 1** 选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人组 (Sponsor Groups) > 创建、编辑或复制 (Create, Edit or Duplicate)**。

**步骤 2** 输入 **Sponsor group name** 和 **Description**。

**步骤 3** **成员组 (Member Groups)** - 点击成员 (Members) 以选择一个或多个用户（身份）组以及来自外部身份源的组，然后添加这些组。要成为此发起人组的成员，用户必须属于至少一个已配置的组。

**步骤 4** 点击**成员 (Members)**，选择用户（身份）组，添加这些组作为此发起人组的组成员。

**步骤 5** 要指定哪些访客类型可由基于此发起人组的发起人创建，请点击**此发起人组可使用以下访客类型创建帐户 (This sponsor group can create accounts using these guest types)**，然后选择一个或多个访客类型。

可以点击**创建访客类型在 (Create Guest Types at)** 下的链接，创建更多访客类型，分配给此发起人组。创建新的访客类型后，必须先保存、关闭并重新打开发起人组，然后才能选择新建的访客类型。

**步骤 6** 使用**选择访客将访问的位置 (Select the locations that guests will be visiting)** 指定在创建访客帐户时，此发起人组中的发起人可以选择的位置（用于设置访客时区）。

通过点击**配置访问位置在 (Configure guest locations at)** 下方的链接，并且添加访客位置，可以添加更多位置以供选择。创建新的访客位置后，必须先保存、关闭并重新打开发起人组，然后才能选择新建的访客位置。

这不会限制访客从其他位置登录。

**步骤 7** 在发起人可创建 (**Sponsor Can Create**) 下，配置此发起人组中的发起人用来创建访问帐户的选项。

- **分配给特定访客的多个访客帐户（导入）(Multiple guest accounts assigned to specific guests [Import]):** 允许发起人通过从文件中导入访客详细信息（例如名字和姓氏）创建多个访客帐户。

如果启用此选项，则**导入 (Import)** 选项将显示在发起人门户的**创建帐户 (Create Accounts)** 窗口中。Import 选项仅在桌面浏览器（而非移动）上可用，例如 Internet Explorer、Firefox、Safari 等。

- **批处理帐户数限制 (Limit to batch of):** 如果允许此发起人组同时创建多个帐户，请指定在单个导入操作中创建的访客帐户数。

虽然发起人可以创建最多 10000 个帐户，但是由于潜在的性能问题，我们建议您限制创建的帐户数。

- **分配给任意访客的多个访客帐户（随机）(Multiple guest accounts to be assigned to any guests [Random]):** 允许发起人为尚且未知的访客以占位符形式创建多个随机访客帐户，或快速创建多个帐户。

如果启用此选项，则**随机 (Random)** 选项将显示在发起人门户的**创建帐户 (Create Accounts)** 窗口中。

- **默认用户名前缀 (Default username prefix):** 指定发起人在创建多个随机访客帐户时可以使用的用户名前缀。如果指定，则在创建随机访客帐户时，发起人门户中会出现此前缀。此外，如果 **Allow sponsor to specify a username prefix** 的状态为：

- 已启用 (Enabled): 发起人可以在发起人门户中编辑默认前缀。
- 未启用 (Not enabled): 发起人无法在发起人门户中编辑默认前缀。

如果您不指定用户名前缀或者不允许发起人指定用户名前缀，则发起人将无法在发起人门户中分配用户名前缀。

- **允许发起人指定用户名前缀 (Allow sponsor to specify a username prefix):** 如果允许此发起人组同时创建多个帐户，请指定在单个导入操作中创建的访客帐户数。

虽然发起人可以创建最多 10000 个帐户，但是由于潜在的性能问题，我们建议您限制创建的帐户数。

**步骤 8** 在发起人可管理 (**Sponsor Can Manage**) 下，可以限制此发起人组的成员可以查看和管理哪些访客帐户。

- **仅发起人创建的帐户 (Only accounts sponsor has created):** 此组中的发起人只能根据发起人的电子邮件帐户，查看和管理他们创建的访客帐户。
- **此发起人组的成员创建的帐户 (Accounts created by members of this sponsor group):** 此组中的发起人可查看和管理此发起人组中任意发起人创建的访客帐户。
- **所有访客帐户 (All guest accounts):** 发起人查看并管理所有待处理访客帐户。

**步骤 9** 在发起人可以 (**Sponsor Can**) 下，可以向此发起人组的成员提供更多关于访客密码和帐户的权限。

- **查看访客的密码 (View guests' passwords):** 对于他们可以管理的访客帐户，允许发起人查看密码。

如果访客已更改密码，则发起人无法再对其进行查看；除非发起人将其重置为由思科 ISE 生成的随机密码。

**注释** 如果此选项针对某个发起人组禁用，则该组的成员无法向他们管理的访客帐户发送关于登录凭证（访客密码）的电子邮件和 SMS 通知。

- **重置访客帐户密码 (Reset guest account passwords):** 对于他们可以管理的访客帐户，允许发起人将访客的密码重置为由思科 ISE 生成的随机密码。
- **延长访客帐户有效期 (Extend guests' accounts):** 对于他们可以管理的访客帐户，允许发起人将其延长至到期日期之后。发起人自动复制到发送给访客的、有关帐户到期的邮件通知上。
- **删除访客帐户 (Delete guests' accounts):** 对于他们可以管理的访客帐户，允许发起人删除帐户并阻止访客访问您公司的网络。
- **暂停访客帐户 (Suspend guests' accounts):** 对于他们可以管理的访客帐户，允许发起人暂停其帐户，以阻止访客临时登录。

此操作还会发出授权变更 (CoA) 终止，以从网络中删除暂停的访客。

- **要求发起人提供原因 (Require sponsor to provide a reason):** 要求发起人提供暂停访客帐户的原因。
- **批准并查看自行注册访客的请求 (Approve and view requests from self-registering guests):** 此发起人组中的发起人可以查看自行注册访客的所有待处理帐户请求（待审批），或仅在用户（作为被访问人）输入发起人电子邮件地址时的请求。此功能要求选中自注册访客使用的门户中的**要求自注册访客需获得批准 (Require self-registered guests to be approved)**，而且列有发起人（作为联系人）的电子邮件。此功能还要求在发起人的身份源中正确配置**邮件 (Email)** 属性。
  - 任何待处理帐户：属于此组的发起人可以批准并审核由任何发起人创建的帐户。
  - 仅分配给此发起人的待处理帐户：属于此组的发起人只能查看和批准自己创建的帐户。
- **使用编程接口（访客 REST API）访问思科 ISE 访客帐户 (Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)):** 对于他们可以管理的访客帐户，允许发起人使用访客 REST API 编程接口访问访客帐户。

**步骤 10** 点击保存 (Save)，然后点击关闭 (Close)。

## 为创建发起人帐户配置帐户内容

您可以配置访客和发起人创建新访客帐户时必须提供的用户数据类型。某些字段是识别 ISE 帐户所必需的，但您可以删除其他字段，并添加自己的自定义字段。

配置发起人创建帐户时使用的字段：

1. 选择工作中心 (Work Centers) > 访客访问 (Guest Access) > 门户和组件 (Portals & Components) > 发起人门户 (Sponsor Portals)，然后编辑发起人门户。
2. 选择门户页面自定义 (Portal Page Customization) 选项卡。
3. 向下滚动并选择为已知访客创建帐户 (Create Account for Known Guests)。
4. 在右侧的预览屏幕上，选择设置 (Settings)。

这些设置决定了在发起人门户上创建访客帐户时显示哪些字段以及哪些是必填字段。此配置适用于“已知”(Known)、“随机”(Random)和“导入”(Imported)访客类型。发起人为导入新用户而下载的模板是动态创建的，因此仅包括在已知访客中设置的字段。

### 发起人门户的特殊设置

以下设置是发起人门户“门户页面自定义”(Portal Page Customization)选项卡上的“为导入的访客创建帐户”(Create Account for Imported Guest)页面的独有设置。

- **允许在访客凭证电子邮件中复制发起人 (Allow sponsor to be copied in Guest Credentials email):** 如果启用此选项，则发送到成功导入的访客的每封访客凭证电子邮件也会发送到发起人。默认为不向发起人发送电子邮件。
- **允许发起人接收摘要邮件 (Allow sponsor to receive summary email):** 当发起人导入用户列表时，ISE 会发送一封包含所有导入用户摘要的电子邮件。如果取消选中此选项，发起人会收到每个导入用户的单独电子邮件。

## 配置发起人门户流程

您可以使用默认门户及其默认设置，例如证书、终端身份组、身份源序列、门户主题、图像和思科 ISE 提供的其他详细信息。如果您不想使用默认设置，则应创建新门户或编辑现有门户来满足需要。如果要创建多个具有相同设置的门户，则可以复制门户。

如果贵公司的公司办公室及其零售点拥有不同的品牌，或者贵公司拥有不同产品品牌，或者驻某城市的办公室希望消防、警察和其他部门具有不同主题的门户，则您可能希望创建多个发起人门户。

这些是与配置发起人门户有关的任务。

### 开始之前

配置或编辑站点的现有发起人组，如[配置发起人组](#)，第 234 页中所述。

- 
- 步骤 1 启用策略服务，第 237 页。
  - 步骤 2 添加用于访客服务的证书，第 238 页。
  - 步骤 3 创建外部身份源，第 238 页。
  - 步骤 4 创建身份源序列，第 238 页。
  - 步骤 5 创建发起人门户，第 239 页。
  - 步骤 6 (可选) 自定义发起人门户，第 240 页。

## 启用策略服务

为了支持思科 ISE 最终用户 Web 门户，您必须在用于托管门户的节点上启用门户-策略服务。

- 
- 步骤 1 依次选择管理 (Administration) > 系统 (System) > 部署 (Deployment)。

步骤 2 点击节点并点击 **Edit**。

步骤 3 在常规设置 (**General Settings**) 选项卡下，选中策略服务 (**Policy Service**) 复选框。

步骤 4 选中启用会话服务 (**Enable Session Services**) 复选框。

步骤 5 点击保存 (**Save**)。

---

## 添加用于访客服务的证书

如果不希望使用默认证书，您可以添加一个有效证书，并将其分配到证书组标签。用于所有最终用户 Web 门户的默认证书组标签为默认门户证书组。

## 创建外部身份源

思科 ISE 能够与外部身份源（例如 Active Directory、LDAP、RADIUS 令牌和 RSA SecurID 服务器）连接，以获取用于身份验证和授权的用户信息。外部身份源还包括执行基于证书的身份验证所需的证书身份验证配置文件。

---

步骤 1 选择 **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources)**。

步骤 2 选择以下选项之一：

- 选择证书身份验证配置文件 (**Certificate Authentication Profile**) 执行基于证书的身份验证。
- 选择 **Active Directory** 作为外部身份源连接到 Active Directory。有关更多详细信息，请参阅[将 Active Directory 用作外部身份源，第 349 页](#)。
- 选择 **LDAP** 以添加 LDAP 身份源。有关更多详细信息，请参阅[LDAP，第 370 页](#)。
- 选择 **RADIUS 令牌 (RADIUS Token)** 以添加 RADIUS 令牌服务器。有关更多详细信息，请参阅[RADIUS 令牌身份源，第 382 页](#)。
- 选择 **RSA SecurID** 以添加 RSA SecurID 服务器。有关更多详细信息，请参阅[RSA 身份源，第 387 页](#)。

---

## 创建身份源序列

### 开始之前

确保您已经在思科 ISE 中配置了外部身份源。

要执行以下任务，您必须是超级管理员或系统管理员。

要允许访客用户通过本地 WebAuth 进行身份验证，必须同时配置访客门户身份验证源和身份源序列，使它们包含相同的身份存储区。

---

步骤 1 选择 **管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences) > 添加 (Add)**。

步骤 2 输入身份源序列的名称。您还可以输入可选的说明。

**步骤 3** 选中 **Select Certificate Authentication Profile** 复选框并为基于证书的身份验证选择证书身份验证配置文件。

**步骤 4** 在**选定列表 (Selected List)** 字段中选择您希望包括在身份源序列中的数据库。

**步骤 5** 在**选定列表 (Selected List)** 字段中重新调整数据库的顺序，调整为希望思科 ISE 搜索数据库的顺序。

**步骤 6** 如果无法访问所选身份库进行身份验证，请在 **高级搜索列表** 区域中选择以下选项之一：

- 请勿访问序列中的其他库并将 **“AuthenticationStatus”** 属性设置为 **“ProcessError”**
- 将用户视为未找到，然后继续到序列中的下一个库

在处理请求时，思科 ISE 会按照序列搜索这些身份源。确保 **“选定列表” (Selected list)** 字段所列出的身份源的顺序是您希望思科 ISE 搜索身份源的顺序。

**步骤 7** 点击 **Submit** 创建您可以稍后在策略中使用的身份源序列。

---

## 创建发起人门户

您可以提供发起人门户，支持发起人为要连接到您的网络访问互联网及内部资源和服务的访客创建、管理和审批帐户。

思科 ISE 为您提供了默认发起人门户，您可以使用该门户，而不必创建另一个门户。但是，您可以创建新的发起人门户，也可以编辑或复制现有门户。您可以删除上述任何门户，默认发起人门户除外。发起人门户登录不支持 IPv6。

您对门户行为和流程设置 (**Portal Behavior and Flow Settings**) 选项卡上的 **“页面设置” (Page Settings)** 所做的任何更改均会反映到发起人流程图中的图形流程中。如果您启用某个页面，例如 AUP 页面，它会显示在流程中，并且发起人会在门户中看到此页面。如果您禁用某个页面，它会从流程中删除，并且系统会为发起人显示下一个启用的页面。

### 开始之前

确保您具有为配合此门户使用而配置的所需证书、外部身份源和身份源序列。

---

**步骤 1** 配置门户设置 (**Portal Settings**) 页面，如 [发起人门户的门户设置](#)，第 267 页中所述。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

**步骤 2** 配置登录设置 (**Login Settings**) 页面，如 [发起人门户的登录页面设置](#)，第 269 页中所述。

**步骤 3** 配置可接受的使用策略 (AUP) 页面设置 (**Acceptable Use Policy [AUP] Page Settings**) 页面，如 [发起人门户的可接受使用政策 \(AUP\) 页面设置](#)，第 269 页中所述。

**步骤 4** 配置发起人更改密码设置 (**Sponsor Change Password Settings**) 选项，如 [发起人门户的发起人更改密码设置](#)，第 270 页中所述。

**步骤 5** 配置登录后横幅页面设置 (**Post-Login Banner Page Settings**) 页面，如 [发起人门户的登录后横幅页面设置](#)，第 270 页中所述。

**步骤 6** 如果要自定义门户，请点击发起人门户应用设置 (**Sponsor Portal Application Settings**)。

**步骤 7** 单击保存。



**注释** 当使用 LDAP 和 SAML GuestID 存储库作为登录发起人门户的身份存储库时，我们建议您使用发起人电子邮件地址登录。如果您使用发起人 ID 登录，可能无法看到已批准的用户。

## 自定义发起人门户

可以通过自定义门户主题、更改门户页面上的 UI 元素以及编辑向用户显示的错误消息与通知来自定义门户外观和用户体验。有关自定义门户的详细信息，请参阅[自定义最终用户 Web 门户](#)，第 276 页。

## 为创建发起人帐户配置帐户内容

您可以配置访客和发起人创建新访客帐户时必须提供的用户数据类型。某些字段是识别 ISE 帐户所必需的，但您可以删除其他字段，并添加自己的自定义字段。

配置发起人创建帐户时使用的字段：

1. 选择工作中心 (**Work Centers**) > 访客访问 (**Guest Access**) > 门户和组件 (**Portals & Components**) > 发起人门户 (**Sponsor Portals**)，然后编辑发起人门户。
2. 选择门户页面自定义 (**Portal Page Customization**) 选项卡。
3. 向下滚动并选择为已知访客创建帐户 (**Create Account for Known Guests**)。

在右侧的预览屏幕上，选择**设置 (Settings)**。这些设置决定了在发起人门户上创建访客帐户时显示哪些字段，以及哪些是必填字段。

此配置适用于“已知”(Known)、“随机”(Random)和“导入”(Imported)访客类型。发起人为导入新用户而下载的模板是动态创建的，因此仅包括在已知访客中设置的字段。

## 发起人无法登录发起人门户

### 问题

当发起人尝试登录 Sponsor 门户时，系统显示以下错误消息：

```
“Invalid username or password. Please try again.”
```

### 原因

- 发起人输入了无效凭证。
- 由于数据库（内部用户数据库或 Active Directory）中没有此用户记录，此发起人无效。
- 发起人所属的发起人组已禁用。
- 发起人的用户帐户不属于活动/已启用的发起人组，这意味着发起人用户的身份组不是任何发起人组的成员。



- 发起人的内部用户帐户已禁用（暂停）。

#### 解决方案

- 验证用户的凭证。
- 启用发起人组。
- 如果该用户帐户已禁用，则恢复该用户帐户。
- 将发起人用户的身份组添加为发起人组的成员。

## 监控访客和发起人活动

思科 ISE 提供各种报告和日志，您可以通过这些报告和日志查看终端与用户管理信息以及访客与发起人活动。

您可以按需或按计划运行这些报告。

---

**步骤 1** 选择 **操作 (Operations) > 报告 (Reports) > 报告 (Reports)**。

**步骤 2** 选择 **访客 (Guest)** 或 **终端和用户 (Endpoints and Users)** 以查看各种访客、发起人和终端相关报告

**步骤 3** 选择要使用 **过滤器 (Filters)** 下拉列表搜索的数据。

**步骤 4** 在 **Time Range** 中选择您想要查看的数据的时间范围。

**步骤 5** 点击 **运行 (Run)**。

---

## 指标控制面板

思科 ISE 会在思科 ISE 主页的指标控制面板中提供网络中经过身份验证的访客 (**Authenticated Guests**) 和 **活动终端 (Active Endpoints)** 的概览视图。

## AUP 接受状态报告

您可以使用此报告跟踪特定时间的所有已接受和已拒绝的 AUP 连接。

## 访客记账报告

访客记账报告显示指定时间段内的访客登录历史记录。报告位于：**操作 (Operations) > 报告 (Reports) > 访客访问权限报告 (Guest Access Reports) > 访客记账 (Guest Accounting)**。

## 主访客报告

“主访客报告” (Primary Guest Report) 将各种报告的数据融入一个视图中，让您可以导出来自不同报告来源的数据。您可以添加更多数据列，删除您不想查看或导出的数据列。此报告的导航路径为：**操作 (Operations) > 报告 (Reports) > 报告 (Reports) > 访客 (Guest) > 主访客报告 (Master Guest Report)**。

此报告收集所有访客活动并提供有关访客用户访问的网站的信息。您可以使用此报告进行安全审核，以查看访客用户何时访问了网络以及他们在网络上执行了什么活动。要查看访客的互联网活动（例如他们访问的网站的 URL），您必须首先执行以下操作：

- 在防火墙上启用用于访客流量的以下选项：
  - 检查 HTTP 流量并将数据发送到思科 ISE 监控节点。思科 ISE 仅要求获取 Guest Activity 报告的 IP 地址和已访问 URL；所以，尽可能将数据限制为仅包含这些信息。
  - 向思科 ISE 监控节点发送系统日志。

## 发起人登录和审核报告

发起人登录和审核报告是用于跟踪以下内容的组合报告：

- 发起人门户中的发起人登录活动。
- 发起人门户中由发起人执行的访客相关操作。

## 访客门户和发起人门户的审核日志记录

在访客门户和发起人门户内执行特定操作的过程中，系统会向基础审核系统发送审核日志消息。使用命令 **show logging application localStore/iseLocalStore.log** 来查看这些消息。

您可以将这些消息配置为由系统日志发送到监控和故障排除系统及日志收集器。监控子系统会在相应的发起人和设备审核日志及访客活动日志中提供此信息。

无论访客登录成功还是失败，访客登录流程都会记录在审核日志中。

## 访客访问 Web 身份验证选项

思科 ISE 访客和 Web 身份验证服务支持多个部署选项，可实现安全的访客访问。可以使用本地或集中式 Web 身份验证和设备注册 Web 身份验证，提供有线或无线访客连接。

- 集中式 Web 身份验证（集中式 WebAuth）：适用于所有访客门户。对于有线和无线连接请求，将由中央思科 ISE RADIUS 服务器使用 Web 身份验证。访客通过在热点访客门户上输入可选访问代码，或在需要提供凭证的访客门户上输入用户名和密码来进行身份验证。

- 本地 Web 身份验证（本地 WebAuth）：适用于需要提供凭证的访客门户。访客连接到交换机进行有线连接，或连接到无线 LAN 控制器 (WLC) 进行无线连接。网络接入设备 (NAD) 会将其定向到网页以进行身份验证。访客在需要提供凭证的访客门户上输入用户名和密码以进行身份验证。
- 设备注册 Web 身份验证（设备注册 WebAuth）：仅适用于热点访客门户。思科 ISE 在 Web 身份验证之前注册并授权访客设备。当访客连接到有线或无线 NAD 时，会定向到热点访客门户。访客无需提供凭证（用户名和密码）即可访问网络。

## 采用集中式 Web 身份验证流程的 NAD

在此方案中，网络访问设备 (NAD) 从未知终端连接向思科 ISE RADIUS 服务器发送新的授权请求。然后，终端接收到向思科 ISE 的 URL 重定向。



**注释** 仅 IOS XE 3.7E、IOS 15.2(4)E 或更高版本支持 `webauth-vrf-aware` 命令。其他交换机在虚拟路由和转发 (VRF) 环境中不支持 Web 身份验证 URL 重定向。在这种情况下，作为解决办法，您可以在全局路由表中添加路由，以将流量泄漏回 VRF。

如果访客设备已连接 NAD，则访客服务交互采取 MAC 身份验证绕行 (MAB) 请求的形式，导致访客通过访客门户进行集中式 Web 身份验证登录。以下是对后续集中式 Web 身份验证的概述，此集中式 Web 身份验证适用于无线和有线网络访问设备。

1. 访客设备通过硬线连接方式连接至 NAD。访客设备上无 802.1X 请求方。
2. 包含适用于 MAB 的服务类型的身份验证策略允许在 MAB 失败的情况下继续运行并返回包含集中式 Web 身份验证用户界面的 URL 重定向的受限网络配置文件。
3. NAD 配置为对向思科 ISE RADIUS 服务器发出的 MAB 请求进行身份验证。
4. 思科 ISE RADIUS 服务器处理 MAB 请求，但找不到适用于访客设备的终端。

这种 MAB 失败导致产生受限制网络配置文件并且在配置文件中返回指向 `access-accept` 中 NAD 的 `url-redirect` 值。要支持此功能，请确保已有授权策略而且其支持相应的有线或无线 MAB（在复合条件下），此外可以选择使用“`Session:Posture Status=Unknown`”条件。NAD 使用此值将默认端口 8443 上的所有访客 HTTP 流量重定向至 `url-redirect` 值。

此案例中标准 URL 值为：

```
https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&portal=<PortalID>&action=cwa
```

5. 访客设备通过 Web 浏览器向重定向 URL 发出 HTTP 请求。
6. NAD 将此请求重定向至从初始 `access-accept` 返回的 `url-redirect` 值。
7. 带操作 CWA 的网关 URL 值重定向至访客门户登录页面。
8. 访客输入其登录凭证，然后提交登录窗体。
9. 访客服务器对登录凭证进行身份验证。

#### 10. 根据流量类型，会发生以下情况：

- 如果为非安全评估流量（无进一步验证的身份验证），其中访客门户未配置为执行客户端调配，访客服务器会向 NAD 发送 CoA。此 CoA 将导致 NAD 使用思科 ISE RADIUS 服务器对访客设备进行重新身份验证。系统向已配置网络访问权限的 NAD 返回新的 access-accept 响应。如果未配置客户端调配并且需要更改 VLAN，则访客门户执行 VLAN IP 更新。访客无需重新输入登录凭证。系统自动使用首次登录时输入的用户名和密码。
- 如果是安全评估流量，其中访客门户配置为执行客户端调配，访客设备 Web 浏览器显示关于安全评估代理安装和合规性的 Client Provisioning 页面。（您也可以配置客户端调配资源策略以设置“NetworkAccess:UseCase=GuestFlow”条件。）

访客门户将重定向至客户端调配门户（因为没有适用于 Linux 的客户端调配或终端安全评估代理），此门户转而重定向回到访客身份验证 servlet，以执行可选 IP 释放/更新，然后执行 CoA。

重定向至 Client Provisioning 门户时，客户端调配服务将非永久性 Web 代理下载至访客设备并对设备执行安全评估检查。或者，还可以配置带有“NetworkAccess:UseCase=GuestFlow”条件的终端安全评估策略。

如果访客设备不合规，请确保已配置带有“NetworkAccess:UseCase=GuestFlow”和“Session:Posture Status=NonCompliant”条件的授权策略。

当访客设备合规时，请确保已配置带有“NetworkAccess:UseCase=GuestFlow”和“Session:Posture Status=Compliant”条件的授权策略。从此处，客户端调配服务向 NAD 发出 CoA。此 CoA 导致 NAD 使用思科 ISE RADIUS 服务器对访客进行重新身份验证。系统向已配置网络访问权限的 NAD 返回新的 access-accept 响应。




---

**注释** “NetworkAccess:UseCase=GuestFlow”还可应用于 Active Directory 和以访客身份登录的 LDAP 用户。

---

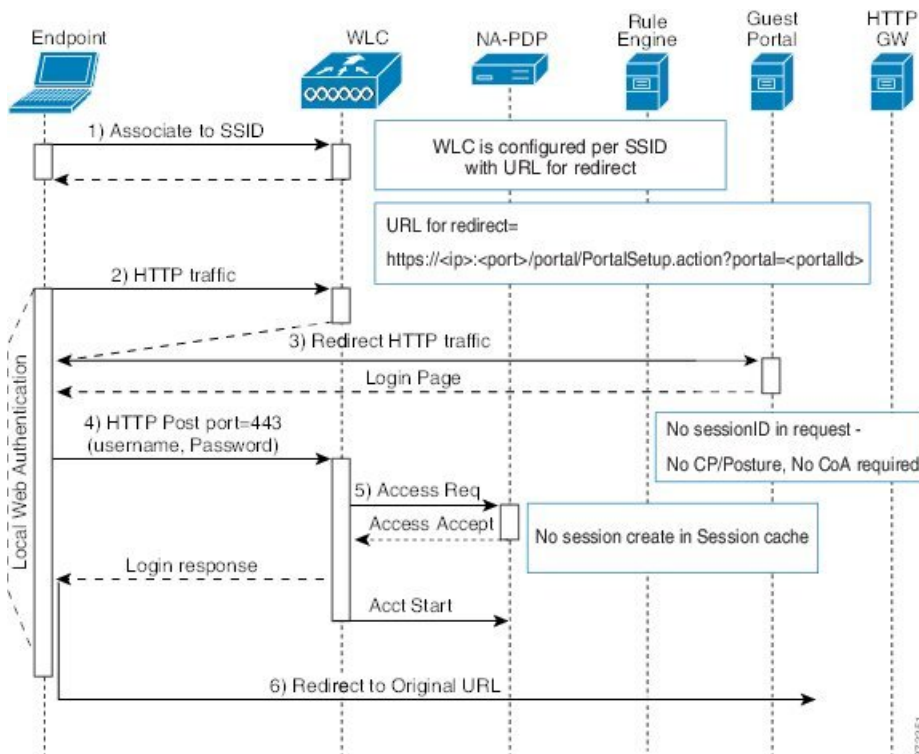
## 使用本地 Web 身份验证流程的无线 LAN 控制器

在这种方案下，访客登录并被重定向至无线 LAN 控制器 (WLC)。然后，WLC 将访客重定向到访客门户，在门户中系统会提示访客输入他们的登录凭证，接受可选的可接受使用政策 (AUP) 并可选择更改密码。

完成此操作后，访客设备的浏览器将重定向回到 WLC 以通过 POST 提供登录凭证。

现在，WLC 可以通过思科 ISE RADIUS 服务器让访客登录。完成此操作后，WLC 将客户设备浏览器重定向至原 URL 目标地址。要支持用于访客门户的原 URL 重定向，无线 LAN 控制器 (WLC) 和网络接入设备 (NAD) 要求为运行 IOS-XE 3.6.0.E 和 15.2(2)E 版本的 WLC 5760 与 Cisco Catalyst 3850、3650、2000、3000 和 4000 系列接入交换机。

图 9: 使用本地 Web 身份验证非安全评估流程的 WLC



## 带本地网络身份验证进程的有线 NAD

在此场景中，访客门户将访客登录请求重定向到交换机（有线 NAD）。登录请求采用 HTTPS URL 形式发布到交换机，并且包含登录凭证。交换机接收访客登录请求，并使用已配置的思科 ISE RADIUS 服务器验证访客。

1. 思科 ISE 要求将 HTML 重定向的 login.html 文件上传到 NAD。此 login.html 文件返回到访客设备的浏览器，响应任何 HTTPS 请求。
2. 访客设备的浏览器被重定向到访客门户，在此输入访客的登录凭证。
3. 处理可接受使用政策 (AUP) 和更改密码（两项均可选）后，访客门户重定向访客设备的浏览器，在 NAD 上发布登录凭证。
4. NAD 向思科 ISE RADIUS 服务器发出 RADIUS 请求，要求对访客进行身份验证和授权。

### Login.html 页面所需的 IP 地址和端口值

IP 地址和端口值必须在 login.html 页面的以下 HTML 代码中更改为思科 ISE 策略服务节点正在使用的值。默认端口为 8443，但是您可以更改此值，以便确保您分配给交换机的值与思科 ISE 中的设置相匹配。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
```

```

<head>
<title>ISE Guest Portal</title>
<meta Http-Equiv="Cache-Control" Content="no-cache">
<meta Http-Equiv="Pragma" Content="no-cache">
<meta Http-Equiv="Expires" Content="0">
<meta http-equiv="content-type" content="text/html; charset=UTF-8">

<meta http-equiv="REFRESH"
content="0;url=https://ip:port/portal/PortalSetup.action?switch_url=wired">

</HEAD>
<BODY>

<center>
Redirecting ... Login
<br>
<br>
<a href="https://ip:port/portal/PortalSetup.action?switch_url=wired">ISE Guest Portal</a>
</center>

</BODY>
</HTML>

```

自定义登录页面是公共 Web 表单，因此请考虑以下准则：

- 登录表必须接受用户名和密码的用户条目，并且将它们显示为 **uname** 和 **pwd**。
- 自定义登录页应当遵循 Web 表最佳实践，例如页面超时、隐藏密码和防止冗余提交。

## 在 NAD 上启用的 HTTPS 服务器

要使用基于 Web 的身份验证，您必须使用 **ip http secure-server** 命令在交换机内启用 HTTPS 服务器。

## NAD 自定义身份验证代理 Web 页面的支持

您可以向 NAD 上传自定义的成功、过期和失败页面。思科 ISE 无需任何特定的自定义，因此您可以根据 NAD 的标准配置说明来创建这些页面。

## 在 NAD 上配置 Web 身份验证

需要使用自定义文件替换默认 HTML 页面，在 NAD 上完成 Web 身份验证。

### 开始之前

在基于 Web 的身份验证期间，创建四个替代 HTML 页面，而不使用交换机默认 HTML 页面。

**步骤 1** 要指定使用自定义身份验证代理 Web 页面，首先在交换机闪存上存储自定义 HTML 文件。要将 HTML 文件复制到交换机闪存中，请在交换机上运行以下命令：

```
copy tftp/ftp flash
```

**步骤 2** 将 HTML 文件复制到交换机之后，在全局配置模式下执行以下命令：

<b>ip admission proxy http login page file</b> <b>device:login-filename</b>	指定自定义 HTML 文件在交换机内存文件系统中的位置，替换默认登录页面。设备：为闪存。
<b>ip admission proxy http success page file</b> <b>device:success-filename</b>	指定自定义 HTML 文件的位置，替换默认登录成功页面。
<b>ip admission proxy http failure page file</b> <b>device:fail-filename</b>	指定自定义 HTML 文件的位置，替换默认登录失败页面。
<b>ip admission proxy http login expired page file</b> <b>device:expired-filename</b>	指定自定义 HTML 文件的位置，替换默认登录过期页面。

**步骤 3** 请遵循交换机提供的指南，配置自定义身份验证代理 Web 页面。

**步骤 4** 如下列所示，验证自定义身份验证代理 Web 页面的配置：

```
Switch# show ip admission configuration
Authentication proxy webpage
Login page           : flash:login.htm
Success page        : flash:success.htm
Fail Page           : flash:fail.htm
Login expired Page  : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

## 设备注册 Web 身份验证流程

通过使用设备注册 Web 身份验证和热点访客门户，您可以允许访客设备连接到专用网络，而无需用户名和密码。

在此场景中，访客使用无线连接来连接到网络。有关设备注册 Web 身份验证流程的示例，请参阅图 10: 无线设备注册 Web 身份验证流程。

以下是后续设备注册 Web 身份验证过程的概要，此过程与无线和有限连接类似：

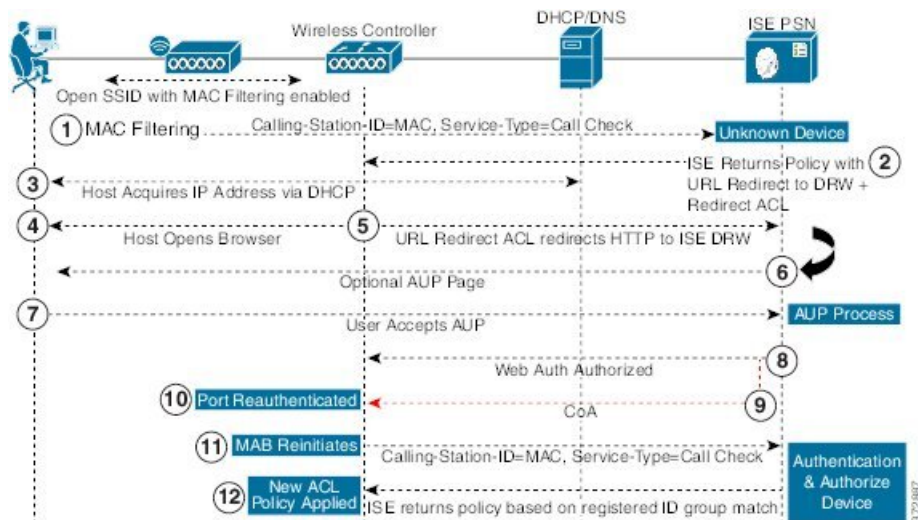
1. 网络接入设备 (NAD) 将重定向发送到热点访客门户。
2. 如果访客设备的 MAC 地址不在任何终端身份组中或者未通过将可接受使用政策 (AUP) 接受的属性设置为 true 进行标记，则思科 ISE 会利用授权配置文件中指定的 URL 重定向进行响应。
3. URL 重定向会在访客尝试访问任何 URL 时向其显示 AUP 页面（如果启用）。
  - 如果访客接受 AUP，则与其设备 MAC 地址关联的终端会分配给已配置的终端身份组。此终端现在通过将 AUP 接受的属性设置为 true 进行标记，从而对访客是否接受 AUP 进行跟踪。

- 如果客户不接受 AUP 或者如果发生错误（例如，在创建或更新终端时），系统会显示错误消息。
4. 根据热点访客门户配置，可能会出现包含其他信息的访问后横幅页面（如果启用）。
  5. 创建或更新终端后，将向 NAD 发送授权变更 (CoA) 终止请求。
  6. 在 CoA 后，NAD 会使用新的 MAC 身份验证绕行 (MAB) 请求对访客连接重新进行身份验证。新的身份验证会使用终端的关联终端身份组查找该终端，并且返回对 NAD 的已配置访问。
  7. 根据热点访客门户配置，访客会被定向到其请求访问的 URL、管理员指定的自定义 URL 或 Authentication Success 页面。

有线和无线的 CoA 类型均是 Termination CoA。您可以配置热点访客门户来执行 VLAN DHCP Release（和更新），从而将有线与无线的 CoA 类型均重新授权为 Change of Auth。

VLAN DHCP Release 支持仅适用于 Windows 设备。它不适用于移动设备。如果进行注册的设备是移动设备，并且启用了 VLAN DHCP Release 选项，则会请求访客手动更新其 IP 地址。对于移动设备用户，我们建议使用 WLC 上的访问控制列表 (ACL)，而不是使用 VLAN。

图 10: 无线设备注册 Web 身份验证流程



## 访客门户设置

### 门户标识设置

这些设置的导航路径为：**访客访问 (Guest Access) > 配置 (Configure) > 访客门户或发起人门户 (Guest Portals or Sponsor Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 访客门户或发起人门户设置和自定义 (Guest Portals or Sponsor Portals Settings and Customization)**。



- **门户名称 (Portal Name):** 输入用于访问此门户的唯一门户名称。请勿将此门户名称用于任何其他发起人门户、访客门户或非访客门户，如黑名单门户、自带设备 (BYOD) 门户、客户端调配门户、移动设备管理 (MDM) 门户或我的设备门户。

此名称显示在用于重定向选择的授权配置文件门户选择中。它应用于门户列表，以便在其他门户中轻松识别。

- **描述 (Description):** 可选。
- **门户测试 URL (Portal test URL):** 点击**保存 (Save)**后，系统生成的 URL 会显示为链接。使用此连接来测试门户。

点击该链接可打开新的浏览器标签页，其中显示此门户的 URL。必须打开具有策略服务的策略服务节点 (PSN)。如果禁用策略服务，则 PSN 仅显示管理员门户。



**注释** 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，思科 ISE 会选择第一个活动 PSN。

- **语言文件 (Language File):** 默认情况下，每个门户类型支持 15 种语言，这些语言可作为在单个压缩语言文件中捆绑在一起的单独属性文件使用。导出或导入要用于门户的压缩语言文件。压缩语言文件包含可用于显示门户的文本的所有单独语言文件。

语言文件包含到特定浏览器区域设置的映射，以及该语言下整个门户的所有字符串设置。单个语言文件包含所有受支持的语言，因此它可轻松用于实现翻译和本地化目的。

如果您更改一种语言的浏览器区域设置，则更改会应用于所有其他最终用户 Web 门户。例如，如果在热点访客门户中将 French.properties 浏览器区域设置从 fr,fr-fr,fr-ca 更改为 fr,fr-fr，则更改还会应用于我的设备门户。

在门户页面自定义 (**Portal Page Customizations**) 选项卡中自定义任何文本时，系统都会显示警报图标。警报消息会提醒您在自定义门户时对一种语言所做的任何更改必须同时添加到所有受支持的语言属性文件。您可以使用下拉列表选项手动关闭警报图标；或者它会在您导入更新后的压缩语言文件后自动关闭。

## 热点访客门户的门户设置

这些设置的导航路径为：**访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 新建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流设置 (Portal Behavior and Flow Settings) > 门户设置 (Portal Settings)**。

- **HTTPS 端口 (HTTPS Port):** 输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此窗口之前会遵循这些设置。如果修改此窗口，应更新端口设置以遵守此限制。

如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。



**注释** 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces)**: 选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

- 以太网接口必须使用不同子网上的 IP 地址。
- 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
- 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
- 在思科 ISE CLI 中配置 **ip host x.x.x.x, x.yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
- **证书组标签 (Certificate Group tag)**: 选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。

- **终端身份组 (Endpoint Identity Group):** 选择用于跟踪访客设备的终端身份组。思科 ISE 提供 **GuestEndpoints** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。

选择用于跟踪员工设备的终端身份组。思科 ISE 提供 **RegisteredDevices** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。
- **当此身份组中的终端达到 \_\_ 天时将其清除 (Purge Endpoints in this Identity Group when they Reach \_\_ Days):** 指定从思科 ISE 数据库中清除设备之前应经历的天数。每天都会进行清除，并且清除活动与整体清除时间同步。更改全局应用于此终端身份组。

如果根据其他策略条件对终端清除策略进行更改，则此设置不可再使用。
- **显示语言**
  - **使用浏览器区域设置 (Use Browser Locale):** 使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language):** 选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use):** 选择要用于门户的显示语言。此设置会覆盖用户浏览器区域 (**User Browser Locale**) 选项。

## 热点访客门户的可接受使用政策 (AUP) 页面设置

此页面的导航路径为 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流量设置 (Portal Behavior and Flow Settings) > 可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy (AUP) Page Settings)**。

- **包含 AUP (Include an AUP):** 在单独的页面上向用户显示公司的网络使用条款和条件。
- **要求访问代码 (Require an Access Code):** 分配访问代码，作为多个访客在获取网络访问权限时应使用的登录凭证。访问代码主要是提供给实际存在的访客（通过白板以肉眼方式或通过前台接待人员以口头方式）的本地已知代码。它不会被场地外的人员获知和使用以访问网络。

除作为登录凭证提供给单独访客的用户名和密码以外，您还可以使用此选项。
- **要求滚动至 AUP 的末尾 (Require scrolling to end of AUP) -** 确保用户已完全阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活**接受 (Accept)** 按钮。配置何时向用户显示 AUP。

配置热点访客门户流时，AUP 访问代码取决于终端身份组设备注册。

仅在从与热点门户配置绑定的终端身份组中删除 MAC 地址后，才会显示 AUP 访问代码页面。通过思科 ISE 上的“情景可视性” (Context Visibility) 页面从数据库中手动删除终端，或者通过终端清除功能和配置的终端清除策略清除终端。

## 热点门户的访问后横幅页面设置

此页面的导航路径为：**访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流量设置 (Portal Behavior and Flow Settings) > 访问接入后横幅页面设置 (Post-Access Banner Page Settings)**。

使用此设置可通知访客其访问状态以及任何其他附加操作（如果需要）。

字段	使用指南
包含访问后横幅页面 ( <b>Include a Post-Access Banner page</b> )	在对访客成功进行身份验证后并在向其授予网络访问权限之前显示其他信息。

## 需要提供凭证的访客门户的门户设置

这些设置的导航路径为：**访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 新建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流设置 (Portal Behavior and Flow Settings) > 门户设置 (Portal Settings)**。

- **HTTPS 端口 (HTTPS Port)**: 输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此窗口之前会遵循这些设置。如果修改此窗口，应更新端口设置以遵守此限制。

如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。



**注释** 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces):** 选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

- 以太网接口必须使用不同子网上的 IP 地址。
  - 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - 在思科 ISE CLI 中配置 **ip host x.x.x.x、x.yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
- 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - **身份源序列 (Identity Source Sequence):** 选择将哪个身份源序列用于用户身份验证。身份源序列是验证用户凭证时，按顺序搜索的身份存储区列表。

思科 ISE 包含适用于发起人门户的默认身份源序列：Sponsor\_Portal\_Sequence。

要配置身份源序列，请依次选择**管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences)**。

- **显示语言**
  - **使用浏览器区域设置 (Use Browser Locale):** 使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language):** 选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use):** 选择要用于门户的显示语言。此设置会覆盖用户浏览器区域 (User Browser Locale) 选项。

## 需要提供凭证的访客门户的登录页面设置

此页面的导航路径为：**访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流设置 (Portal Behavior and Flow Settings) > 登录页面设置 (Login Page Settings)**。

- **要求访问代码 (Require an Access Code):** 分配访问代码，作为多个访客在获取网络访问权限时应使用的登录凭证。访问代码主要是提供给实际存在的访客（通过白板以肉眼方式或通过前台接待人员以口头方式）的本地已知代码。它不会被场地外的人员获知和使用以访问网络。  
除作为登录凭证提供给单独访客的用户名和密码以外，您还可以使用此选项。
- **速率限制之前最大失败登录尝试次数 (Maximum Failed Login Attempts Before Rate Limiting):** 指定思科 ISE 开始限制该帐户之前从单个浏览器会话尝试登录时的失败次数。这不会导致帐户锁定。限制的速率在**限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts When Rate Limiting)** 中进行配置。
- **限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts when Rate Limiting):** 设置用户在达到速率限制之前最大失败登录尝试次数 (**Maximum failed login attempts before rate limiting**) 中定义的登录失败次数后，尝试再次登录（限制速率）之前必须等待的时间长度（分钟）。
- **包含 AUP (Include an AUP):** 将可接受使用政策窗口添加到流。可以将 AUP 添加到窗口，或链接到另一个窗口。
- **允许访客创建自己的帐户 (Allow Guests to Create their Own Accounts):** 在此门户的登录页面上为访客提供自行注册的选项。如果未选中此选项，则发起人需创建访客帐户。启用该选项会同时启用该页面中的选项卡以供您配置**自注册页面设置**和**自注册成功页面设置**。  
如果访客选择此选项，则为其提供自注册表单，他们可在其中输入请求的信息来创建其自己的访客帐户。
- **允许访客在登录后更改密码 (Allow guests to change password after login):** 允许访客在成功进行身份验证并接受 AUP 后更改其密码（如果需要）。如果访客更改其密码，则在丢失登录凭证的情况下发起人无法为访客提供其登录凭证。发起人只能将访客的密码重置为随机密码。

## 需要提供凭证的访客门户的自助注册页面设置

此页面的导航路径为 **Guest Access > Configure > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Self Registration Page Settings**。使用这些设置使访客可以自助注册并指定访客需要在 Self-Registration 表单中提供的信息。

字段	使用指南
Assign self-registered guests to guest type	选择应该将使用此门户的所有自助注册访客分配到哪个访客类型。

字段	使用指南
Account valid for	以天、小时或分钟为单位指定帐户的持续时间，经过此时间之后，帐户就会到期，除非您或发起人在 Sponsor 门户中延长此帐户持续时间。
Require a registration code for self registration	为自助注册访客分配成功提交其 Self-Registration 表单所必须输入的代码。注册代码与接入代码类似，都是通过离线方式提供给访客，以防外部的用户访问系统。
Fields to include / Required	检查您要在 Self-Registration 表单上显示的字段。然后检查哪些字段是访客提交此表单和接收访客帐户必须填写的强制字段。您可能需要强制填写 <b>SMS Service Provider</b> 和 <b>Person being Visited</b> 等字段，以从自助注册访客收集重要信息。
Guests can choose from these locations to set their time zone	<p>输入自助注册的访客在注册时使用您所定义的位置列表可以选择的位置。这将自动分配相关时区，作为这些访客的有效访问时间。位置名称应该明确，以免在选择时出现含糊（例如 Boston Office、500 Park Ave New York、Singapore 等）</p> <p>如果您只提供一个位置，系统会将其自动分配为默认位置并且不在门户中显示此位置以供访客查看。此外，在 <b>Fields to include</b> 列表中，系统会禁用 <b>Location</b>。</p>
SMS Service Provider	在 Self-Registration 表单上显示 SMS 运营商，使自助注册的访客可以选择他们自己的 SMS 运营商。您可以使用访客的 SMS 服务向他们发送 SMS 通知以最大程度地降低公司开支。
Guests can choose from these SMS providers	<p>选择应该在 Self-Registration 表单上显示的 SMS 运营商。</p> <p>如果您只选择一个 SMS 运营商作为供访客使用的默认 SMS 运营商，则此提供商不会显示于 Self-Registration 表单上。</p>
Custom Fields	选择您想要从自助注册的访客收集的其他信息。然后检查哪些字段是访客提交 Self-Registration 表单和接收访客帐户必须填写的字段。系统按名称字母顺序列出这些字段。
包含一个 AUP（在页面上/作为链接）(Include an AUP [on page/as link])	将公司的网络使用条款和条件显示为当前为用户显示的窗口上的文本或者显示为用于打开包含 AUP 文本的新选项卡或窗口的链接。

字段	使用指南
要求接受 (Require Acceptance)	要求用户在其帐户完全启用之前接受 AUP。除非用户接受 AUP，否则不会启用登录 (Login) 按钮。如果用户不接受 AUP，将不会获取网络访问权限。
要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)	仅在启用在页面上包含一个 AUP (Include an AUP on page) 的情况下，才会显示此选项。 确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用接受 (Accept) 按钮。
Only allow guests with an email address from	指定允许的电子邮件地址域，来自这些域的自行注册访客可以进入电子邮件地址并成功接收他们的帐户凭证；例如 cisco.com、example.com。 在本示例中，如果用户输入 myname@cisco.com 作为其邮件地址，在成功创建帐户之后，他们会收到其登录凭证。但如果他们输入的是 myname@hotmail.com（或并非来自 cisco.com 或 example.com 的任何其他地址），则系统不会创建任何帐户而且他们也不会收到凭证。 如果将此字段留空，则可从任意域进行注册，禁止电子邮件地址来自以下域的访客 (Do not allow guests with email address from) 中列出的拦截域除外。
Do not allow guests with an email address from	指定拦截的电子邮件地址域，来自这些域的自行注册访客不能进入电子邮件地址并成功接收他们的帐户凭证；例如 cisco.com、example.com。 在本示例中，如果用户输入 myname@cisco.com 作为其邮件地址，则系统不会创建任何帐户并且他们也不会收到凭证。



字段	使用指南
Require self-registered guests to be approved	<p>指定使用此门户的自助注册的访客需要获得发起人的批准，才能收到其访客凭证。</p> <p>然后在此页面的 <b>After registration submission, direct guest to</b> 下选择一个以下选项：</p> <ul style="list-style-type: none"> <li>• Self-Registration Success page</li> <li>• Login page with instructions about how to obtain login credentials</li> <li>• URL</li> </ul> <p>如果启用此字段，您还应该在此页面上在 <b>Send credential notification upon approval using</b> 下启用 <b>Email</b> 和 <b>SMS</b> 中的一个字段或这两个字段。</p> <p>启用要求自助注册访客需获得批准 (Require self-registered guests to be approved) 将启用以下额外配置字段，其具有以下属性：</p> <p>批准/拒绝链接设置 (Approve/Deny Link Settings) - 其他设置允许您配置：</p> <ul style="list-style-type: none"> <li>• 链接有效性 (<b>Links are valid for</b>)，天数。</li> <li>• 要求审批人输入身份验证用户名和密码以进行身份验证 (Require approver to enter a username and password for authentication) - 基于以下经过排序的发起人门户列表对发起人进行身份验证</li> <li>• 基于以下经过排序的发起人门户列表对发起人进行身份验证 (Authenticate sponsors based on the following ordered list of sponsor portals) - 如果有多个发起人可以审批此帐户，则选择发起人必须登录才能审批该帐户的门户。</li> </ul>

字段	使用指南
Email approval request to	<p>如果您选择：</p> <ul style="list-style-type: none"> <li>• <b>sponsor email addresses listed below</b>，请输入指定为批准人的发起人邮件地址，或应该接收全部访客批准请求的邮件地址或邮件收发器。</li> <li>• <b>被访问者 (person being visited)</b>，“要包括的字段” (Fields to include) 列表中的被访问者 (<b>Person being visited</b>) 和必填 (<b>Required</b>) 选项也将启用（如果之前已禁用这些选项）。Self-Registration 表单上将显示这些字段，要求自助注册的访客提供这些信息。</li> </ul> <p>这些人将收到一封邮件通知，邮件中会说明自助注册的访客要求获得批准。</p>
Self-Registration Success page	<p>将自助注册成功的访客定向至 Self-Registration Success 页面，此页面会显示您在 <b>Self Registration Success Page Settings</b> 中指定的字段和消息。</p> <p>可能无需显示所有信息，因为系统可能正在等待批准帐户（如已在此页面启用此选项）或根据此页面中指定的允许域和拦截域向电子邮件地址或电话号码发送登录凭证。</p> <p>如果您在 <b>Self-Registration Success Page Settings</b> 中启用 <b>Allow guests to log in directly from the Self-Registration Success page</b>，则自助注册成功的访客可以直接从此页面登录。如未启用，则在显示 Self-Registration Success 页面之后，系统会将访客定向至门户的 Login 页面。</p>
Login page with instructions about how to obtain login credentials	<p>将自助注册成功的访客定向回到该门户的 Login 页面并显示 “Please wait for your guest credentials to be delivered either via email, SMS, or print format and proceed with logging in” 之类的消息。</p> <p>要自定义默认消息，请点击 <b>Portal Page Customization</b> 选项卡并选择 <b>Self-Registration Page Settings</b>。</p> <p>系统可能正在等待批准帐户（如已在此页面启用此选项）或根据此页面上指定的允许域和拦截域向电子邮件地址或电话号码发送登录凭证。</p>

字段	使用指南
URL	<p>将自助注册成功的访客定向至指定的URL，同时等待发送其帐户凭证。</p> <p>系统可能正在等待批准帐户（如已在此页面启用此选项）或根据此页面上指定的允许域和拦截域向电子邮件地址或电话号码发送登录凭证。</p>
Email	<p>选择将邮件作为自助注册成功的访客用于接收其登录凭证信息的选项。如果您选择此选项，<b>Email address</b> 会成为 <b>Fields to include</b> 列表中的必填字段，而且您再也无法禁用此选项。</p>
SMS	<p>选择将 SMS 作为自助注册成功的访客用于接收其登录凭证信息的选项。如果您选择此选项，<b>SMS Service Provider</b> 会成为 <b>Fields to include</b> 列表中的必填字段，而且您再也无法禁用此选项。</p>

## 自行注册成功页面设置

此页面的导航路径为：访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流设置 (Portal Behavior and Flow Settings) > 自行注册成功页面设置 (Self Registration Success Page Settings)。使用这些设置可向成功自注册的访客通知他们获取网络访问权限所需的凭证。

字段	使用指南
<p>自行注册成功页面中纳入该信息 (Include this information on the Self-Registration Success page)</p>	<p>选中要在“自行注册成功” (Self-Registration Success) 页面上为成功自注册访客显示的字段。</p> <p>如果不需要访客的赞助商审批，请选中用户名 (Username) 和 密码 (Password)，为访客显示这些凭证。如果需要赞助商审批，则这些字段将被禁用，因为凭证只能在得到批准之后发送到访客。</p>
<p>允许访客通过以下方式向自己发送信息 (Allow guest to send information to self using)</p>	<p>选中成功自注册访客可用于向自己传送凭证信息的方式的选项：打印 (Print)、电子邮件 (Email) 或 SMS。</p>
<p>包含一个 AUP（在页面上/作为链接）(Include an AUP [on page/as link])</p>	<p>将公司的网络使用条款和条件显示为当前为用户显示的窗口上的文本或者显示为用于打开包含 AUP 文本的新选项卡或窗口的链接。</p>

字段	使用指南
要求接受 ( <b>Require Acceptance</b> )	要求用户在其帐户完全启用之前接受 AUP。除非用户接受 AUP，否则不会启用 <b>登录 (Login)</b> 按钮。如果用户不接受 AUP，将不会获取网络访问权限。
要求滚动至 AUP 的末尾 ( <b>Require scrolling to end of AUP</b> )	如果选择了页面上的 <b>AUP (AUP on page)</b> 选项，系统会显示此字段。  确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用 <b>接受 (Accept)</b> 按钮。
允许访客直接通过自注册成功页面登录 (Allow guests to log in directly from the Self-Registration Success page)	“自注册成功” ( <b>Self-Registration Success</b> ) 页面底部显示 <b>登录 (Login)</b> 按钮。这使得访客能够绕过“登录” ( <b>Login</b> ) 页面，自动将登录凭证传送到门户并在门户流程中显示下一个页面（例如，AUP 页面）。

## 需要提供凭证的访客门户的可接受使用政策 (AUP) 页面设置

- **包含 AUP (Include an AUP)**: 在单独的页面上向用户显示公司的网络使用条款和条件。
- **对员工使用不同的 AUP (Use Different AUP for Employees)**: 仅为员工显示不同的 AUP 及网络使用条款和条件。如果您选择此选项，则不能同时选择跳过面向员工的 **AUP (Skip AUP for employees)**。
- **对员工跳过 AUP (Skip AUP for Employees)**: 员工在访问网络之前无需接受 AUP。如果您选择此选项，则不能同时选择使用面向员工的不同 **AUP (Use different AUP for employees)**。
- **要求滚动至 AUP 末尾 (Require Scrolling to End of AUP)**: 此选项仅在已启用在页面上包含 **AUP (Include an AUP on page)** 时显示。

确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 的末尾时，才会激活 **接受 (Accept)** 按钮。配置何时向用户显示 AUP。

- **仅首次登录时 (On First Login only)**: 仅在用户首次登录网络或门户时显示 AUP。
- **每次登录时 (On Every Login)**: 每次用户登录网络或门户时都显示 AUP。
- **每 \_\_ 天 (从首次登录算起) (Every \_\_ Days [starting at first login])**: 在用户首次登录网络或门户后定期显示 AUP。

## 需要提供凭证的访客门户的访客更改密码设置

### 访客更改密码设置

此页面的导航路径为：访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流量设置 (Portal Behavior and Flow Settings) > 访客更改密码设置 (Guest Change Password Settings)

- **允许访客在登录后更改密码 (Allow guests to change password after login):** 允许访客在成功进行身份验证并接受 AUP 后更改其密码（如果需要）。如果访客更改其密码，则在丢失登录凭证的情况下发起人无法为访客提供其登录凭证。发起人只能将访客的密码重置为随机密码。

## 需要提供凭证的访客门户的访客设备注册设置

此页面的导航路径为：访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流设置 (Portal Behavior and Flow Settings) > 访客设备注册设置 (Guest Device Registration Settings)。

使用这些设置可确保在登录到访客设备时思科 ISE 自动注册访客设备，或者允许访客在登录后手动注册其设备。

在访客访问 (Guest Access) > 配置 (Configure) > 访客类型 (Guest Types) 中为每个访客类型指定最大设备数量。

- **自动注册访客设备 (Automatically Register Guest Devices):** 自动为访客用来访问此门户的设备创建终端。此终端将添加到为此门户指定的终端身份组并且适用该身份组的清除策略。

现在，可以创建授权规则来允许访问该身份组中的终端，以便不再需要 Web 身份验证。

如果达到最大注册设备数，则系统会自动删除第一个注册设备，注册访客尝试登录所使用的设备，并且通知访客。选择访客访问 (Guest Access) > 配置 (Configure) > 访客类型 (Guest Types) 以更改可向其注册访客的设备的最大数量。

- **允许访客注册设备 (Allow Guests to Register Devices):** 访客可以通过提供名称、说明和 MAC 地址手动注册其设备。MAC 地址与终端身份组相关联。

如果达到最大注册设备数，则访客需要删除至少一个设备，然后才允许其注册其他设备。

## 需要提供凭证的访客门户的 BYOD 设置

此页面的导航路径为：访客访问 (Guest Access) > 门户和组件 (Portals & Components) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流设置 (Portal Behavior and Flow Settings) > BYOD 设置 (BYOD Settings)。

使用这些设置为非访客（例如使用需要提供凭证的访客门户访问企业网络的员工）启用自带设备 (BYOD) 功能。

字段	使用指南
允许员工在网络中使用个人设备 (Allow Employees to use Personal Devices on the Network)	向此门户添加“BYOD注册”(BYOD Registration) 窗口，允许员工完成员工设备注册过程，并且可能进行本地请求方和证书调配，具体视员工的个人设备类型（例如，iOS、Android、OSX）对应的客户端调配设置而定。
终端身份组	选择用于跟踪访客设备的终端身份组。思科 ISE 提供 <b>GuestEndpoints</b> 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。
当此身份组中的终端达到__天时将其清除 (Purge Endpoints in this Identity Group when they Reach __ Days)	更改用户设备自注册以来到其从思科 ISE 数据库中清除的天数。每天都会进行清除，并且清除活动与整体清除时间同步。更改全局应用于此终端身份组。  如果根据其他策略条件对终端清除策略进行更改，则此设置不可再使用。
Allow employees to choose to get guest access only	使员工可以访问访客网络并避免在访问企业网络时可能需要另行调配和注册。
在注册期间显示设备 ID 字段 (Display Device ID Field During Registration)	在注册过程中向用户显示设备 ID，即使设备 ID 已预配置并在使用 BYOD 门户时无法更改也如此。
原始 URL (Originating URL)	成功对网络进行身份验证后，将用户的浏览器重定向到用户正在尝试访问的原始网站（如果适用）。如果不适用，则系统会显示“身份验证成功”(Authentication Success) 窗口。请确保允许重定向 URL 通过 NAD 上的访问控制列表和在该 NAD 的思科 ISE 中配置的授权配置文件，在 PSN 的端口 8443 上工作。  对于 Windows、MAC 和 Android 设备，控制权交给自助调配向导应用，后者负责调配。因此，这些设备不会被重定向到原始 URL。但是，iOS (dot1X) 和不受支持的设备（允许进行网络访问）会重定向到此 URL。
注册成功页面	显示设备注册成功的页面。
URL	成功对网络进行身份验证后，将用户的浏览器重定向到指定的 URL，例如贵公司的网站。

## 需要提供凭证的访客门户的登录后横幅页面设置

此页面的导航路径为：访客访问 (Guest Access) > 配置 (Configure) > 访客门户或发起人门户 (Guest Portals or Sponsor Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流量设置 (Portal Behavior and Flow Settings) > 访问后横幅页面设置 (Post-Access Banner Page Settings)。

使用此设置可在用户（适用情况下的访客、发起人或员工）成功登录后向其通知其他信息。

字段	使用指南
包含登录后横幅页面 (Include a Post-Login Banner page)	在用户成功登录后并在向其授予网络访问权限之前显示其他信息。

## 需要提供凭证的访客门户的访客设备合规性设置

此页面的导航路径为：访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流设置 (Portal Behavior and Flow Settings) > 访客设备合规性设置 (Guest Device Compliance Settings)。使用这些设置可要求使用访客门户的访客和员工对其设备进行客户端调配，以便获取对网络的访问权限。

- 需要访客设备合规性 (Require guest device compliance) - 将访客重定向到“客户端调配” (Client Provisioning) 页面，这会要求其下载终端安全评估代理。这会将客户端调配添加到访客流，您可以在其中配置访客的终端安全评估策略，如检查病毒防护软件。

如果访客是使用需要提供证书的访客门户来访问网络的员工，并且：

- 如果您已启用 **BYOD Settings** 中的 **Allow employees to use personal devices on the network**，则员工会被重定向到 BYOD 流程，并且不会进行客户端调配。
- 如果您同时启用 **BYOD Settings** 中的 **Allow employees to use personal devices on the network** 和 **Allow employees to choose to get guest access only**，并且员工选择访客接入，则他们会被重定向到 Client Provisioning 页面。

## 访客门户的 VLAN DHCP 释放页面设置

此页面的导航路径为：访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流设置 (Portal Behavior and Flow Settings) > VLAN DHCP 释放页面设置 (VLAN DHCP Release Page Settings)。

- 启用 **VLAN DHCP 释放 (Enable VLAN DHCP release)**：在有线与无线环境中发生 VLAN 更改后刷新访客的 Windows 设备 IP 地址。

这会在网络访问将访客 VLAN 更改为新 VLAN 时影响最终授权过程中的集中式 Web 身份验证 (CWA) 流程。在 VLAN 更改之前必须释放访客的旧 IP 地址，并且必须在访客连接新 VLAN 时通过 DHCP 请求新访客 IP 地址。仅在使用 DirectX 控件的 Internet Explorer 浏览器上支持 IP 地址释放和续订操作。

“VLAN DHCP 释放” (VLAN DHCP Release) 选项不适用于移动设备。相反，系统会请求访客手动重置 IP 地址。此方法因设备而异。例如，在 Apple iOS 设备上，访客可以选择 Wi-Fi 网络并点击 **Renew Lease** 按钮。

- **延迟 \_\_ 秒释放 (Delay to Release \_\_ Seconds)**: 输入延迟释放时间。我们建议使用较短的值，因为释放必须紧随在下载小应用程序之后、在思科 ISE 服务器指示 NAD 对 CoA 请求重新进行身份验证之前发生。
- **延迟 \_\_ 秒执行 CoA (Delay to CoA \_\_ Seconds)**: 输入使思科 ISE 延迟执行 CoA 的时间。提供足够时间（使用默认值作为规定值），以允许下载小程序并在客户端上执行 IP 释放。
- **延迟 \_\_ 秒续订 (Delay to Renew \_\_ Seconds)**: 输入延迟续订值。此时间会添加到 IP 释放值，并且在下载控件之前不会开始计时。提供足够时间（使用默认值作为规定值），以便允许 CoA 进行处理并授予新的 VLAN 访问权限。

## 访客门户的身份验证成功设置

此页面的导航路径为：**访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流设置 (Portal Behavior and Flow Settings) > 身份验证成功设置 (Authentication Success Settings)**。

这些设置会通知用户（适用的访客、发起人或员工）身份验证成功或显示 URL。在经过身份验证后将访客转到：**(Once authenticated, take guest to:)** 下，配置以下字段：

- **原始 URL (Originating URL)**: 成功对网络进行身份验证后，将用户的浏览器重定向到用户正在尝试访问的原始网站（如果适用）。如果不适用，则系统会显示“身份验证成功” (Authentication Success) 窗口。请确保允许重定向 URL 通过 NAD 上的访问控制列表和在该 NAD 的 ISE 中配置的授权配置文件，在 PSN 的端口 8443 上工作。

对于 Windows、MAC 和 Android 设备，控制权交给自助调配向导应用，后者负责调配。因此，这些设备不会被重定向到原始 URL。但是，iOS (dot1X) 和不受支持的设备（允许进行网络访问）会重定向到此 URL。

- **身份验证成功 (Authentication Success) 页面**: 通知用户身份验证成功。
- **URL**: 成功对网络进行身份验证后，将用户的浏览器重定向到指定的 URL，例如您公司的网站。



### 注释

如果您在身份验证后将一个访客重定向到外部 URL，可能会在解析 URL 地址和重定向会话时有延迟。请确保允许重定向 URL 通过 NAD 上的访问控制列表和在该 NAD 的 ISE 中配置的授权配置文件，在 PSN 的端口 8443 上工作。



## 访客门户的支持信息页面设置

此页面的导航路径为：访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流量设置 (Portal Behavior and Flow Settings) > 支持信息页面设置 (Support Information Page Settings)。

使用这些设置可显示服务中心可用于对用户（适用情况下的访客、发起人或员工）遇到的访问问题进行故障排除的信息。

字段	使用指南
包含支持信息页面 (Include a Support Information Page)	在门户的所有已启用窗口上显示指向信息窗口（例如联系我们 [Contact Us]）的链接。
MAC 地址	在支持信息 (Support Information) 窗口上包含设备的 MAC 地址。
IP 地址	在支持信息 (Support Information) 窗口上包含设备的 IP 地址。
浏览器用户代理	在支持信息 (Support Information) 窗口上包含浏览器详细信息，如产品名称和版本、布局引擎，以及发起请求的用户代理的版本。
策略服务器 (Policy Server)	在支持信息 (Support Information) 窗口上包含服务此门户的 ISE 策略服务节点 (PSN) 的 IP 地址。
故障代码	如果适用，请包含日志消息目录中的对应编号。要查看消息目录，选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 消息目录 (Message Catalog)。
隐藏字段 (Hide Field)	如果字段标签将会包含的信息不存在，请勿在支持信息 (Support Information) 窗口上显示任何字段标签。例如，如果故障代码未知并因此为空白，请勿显示故障代码 (Failure code)，即使已选择故障代码也如此。
显示不含任何值的标签 (Display Label with no Value)	在支持信息 (Support Information) 窗口上显示所有选定字段标签，即使其将会包含的信息不存在也如此。例如，如果故障代码未知，请显示故障代码 (Failure code)，即使其为空白也如此。
显示含默认值的标签 (Display Label with Default Value)	如果标签将会包含的信息不存在，请在支持信息 (Support Information) 窗口上的任何选定字段中显示此文本。例如，如果在此字段中输入“不可用” (Not Available)，并且故障代码未知，则故障代码 (Failure Code) 将显示不可用 (Not Available)。

# 发起人门户应用设置

## 门户标识设置

这些设置的导航路径为：**访客访问 (Guest Access) > 配置 (Configure) > 访客门户或发起人门户 (Guest Portals or Sponsor Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 访客门户或发起人门户设置和自定义 (Guest Portals or Sponsor Portals Settings and Customization)**。

- **门户名称 (Portal Name):** 输入用于访问此门户的唯一门户名称。请勿将此门户名称用于任何其他发起人门户、访客门户或非访客门户，如黑名单门户、自带设备 (BYOD) 门户、客户端调配门户、移动设备管理 (MDM) 门户或我的设备门户。

此名称显示在用于重定向选择的授权配置文件门户选择中。它应用于门户列表，以便在其他门户中轻松识别。

- **描述 (Description):** 可选。
- **门户测试 URL (Portal test URL):** 点击**保存 (Save)**后，系统生成的 URL 会显示为链接。使用此连接来测试门户。

点击该链接可打开新的浏览器标签页，其中显示此门户的 URL。必须打开具有策略服务的策略服务节点 (PSN)。如果禁用策略服务，则 PSN 仅显示管理员门户。



**注释** 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，思科 ISE 会选择第一个活动 PSN。

- **语言文件 (Language File):** 默认情况下，每个门户类型支持 15 种语言，这些语言可作为在单个压缩语言文件中捆绑在一起的单独属性文件使用。导出或导入要用于门户的压缩语言文件。压缩语言文件包含可用于显示门户的文本的所有单独语言文件。

语言文件包含到特定浏览器区域设置的映射，以及该语言下整个门户的所有字符串设置。单个语言文件包含所有受支持的语言，因此它可轻松用于实现翻译和本地化目的。

如果您更改一种语言的浏览器区域设置，则更改会应用于所有其他最终用户 Web 门户。例如，如果在热点访客门户中将 French.properties 浏览器区域设置从 fr,fr-fr,fr-ca 更改为 fr,fr-fr，则更改还会应用于我的设备门户。

在门户页面自定义 (Portal Page Customizations) 选项卡中自定义任何文本时，系统都会显示警报图标。警报消息会提醒您在自定义门户时对一种语言所做的任何更改必须同时添加到所有受支持的语言属性文件。您可以使用下拉列表选项手动关闭警报图标；或者它会在您导入更新后的压缩语言文件后自动关闭。

## 发起人门户的门户设置

配置这些设置以标识门户并选择要用于所有门户页面的语言文件。

- **HTTPS 端口 (HTTPS Port):** 输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此窗口之前会遵循这些设置。如果修改此窗口，应更新端口设置以遵守此限制。

如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。



**注释** 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在门户设置 (Portal Settings) 中仅配置接口 0，也可以使用 CLI 命令 `ip host` 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces):** 选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

- 以太网接口必须使用不同子网上的 IP 地址。

- 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
- 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
- 在思科 ISE CLI 中配置 **ip host x.x.x.x, x.yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
- **证书组标签 (Certificate Group tag)**: 选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **完全限定域名 (FQDN) (Fully Qualified Domain Name [FQDN])**: 为发起人门户或我的设备门户输入至少一个唯一 FQDN 或主机名。例如，可以输入 **sponsorportal.yourcompany.com, sponsor**，以便在用户将其中任一名称输入到浏览器中时，发起人门户会打开。以逗号分隔名称，但条目之间不包含空格。

如果更改默认 FQDN，还需执行以下操作：

- 更新 DNS，以便新 URL 的 FQDN 解析为有效的策略服务节点 (PSN) IP 地址。或者，此地址可能指向提供 PSN 池的负载均衡器虚拟 IP 地址。
- 要避免由于名称不匹配而出现证书警告消息，请在思科 ISE PSN 的本地服务器证书的使用者备选名称 (SAN) 属性中加入自定义 URL 的 FQDN 或通配符。
- **身份源序列 (Identity Source Sequence)**: 选择将哪个身份源序列用于用户身份验证。身份源序列是验证用户凭证时，按顺序搜索的身份存储区列表。

思科 ISE 包含适用于发起人门户的默认身份源序列：Sponsor\_Portal\_Sequence。

要配置身份源序列，请依次选择**管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences)**。

- **空闲超时 (Idle Timeout)**: 输入思科 ISE 在门户中没有活动的情况下注销用户之前要等待的时间（以分钟为单位）。有效范围为 1 至 30 分钟。
- **允许 Kerberos (Allow Kerberos)**: 使用 Kerberos 对发起人进行身份验证，用于访问发起人门户。在浏览器与 ISE 建立 SSL 连接后，在安全隧道内执行 Kerberos SSO。

Kerberos 身份验证要求以下项目位于同一域中：

- 发起人的 PC
- ISE PSN
- 为此发起人门户配置的 FQDN




---

注释 访客门户不支持 Kerberos 身份验证。

---

- 显示语言

- **使用浏览器区域设置 (Use Browser Locale):** 使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言, 则使用回退语言 (Fallback Language) 作为语言门户。
- **回退语言 (Fallback Language):** 选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
- **始终使用 (Always Use):** 选择要用于门户的显示语言。此设置会覆盖用户浏览器区域 (User Browser Locale) 选项。
- **发起人的可用 SSID (SSIDs Available to Sponsors):** 输入网络的名称或 SSID (会话服务标识符), 发起人可以告知访客该网络是可以连接访问的正确网络。

## 发起人门户的登录页面设置

### 发起人门户的登录页面设置

此页面的导航路径为: 访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流设置 (Portal Behavior and Flow Settings) > 登录页面设置 (Login Page Settings)。

- **速率限制之前最大失败登录尝试次数 (Maximum Failed Login Attempts Before Rate Limiting):** 指定思科 ISE 开始限制该帐户之前从单个浏览器会话尝试登录时的失败次数。这不会导致帐户锁定。限制的速率在限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts When Rate Limiting) 中进行配置。
- **限制速率时登录尝试之间的间隔时间 (Time Between Login Attempts when Rate Limiting):** 设置用户在达到速率限制之前最大失败登录尝试次数 (Maximum failed login attempts before rate limiting) 中定义的登录失败次数后, 尝试再次登录 (限制速率) 之前必须等待的时间长度 (分钟)。
- **包含 AUP (Include an AUP):** 将可接受使用政策窗口添加到流。可以将 AUP 添加到窗口, 或链接到另一个窗口。

## 发起人门户的可接受使用政策 (AUP) 页面设置

此页面的导航路径为 访客访问 (Guest Access) > 配置 (Configure) > 发起者门户 (Sponsor Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流量设置 (Portal Behavior and Flow Settings) > 可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy (AUP) Page Settings)。

使用这些设置可定义用户 (适用情况下的访客、发起人或员工) 的 AUP 体验。

字段	使用指南
包含 AUP 页面 (Include AUP page)	在单独的页面上向用户显示公司的网络使用条款和条件。

字段	使用指南
要求滚动至 AUP 的末尾 ( <b>Require scrolling to end of AUP</b> )	确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用接受 ( <b>Accept</b> ) 按钮。
仅首次登录时 ( <b>On First Login only</b> )	仅在用户首次登录到网络或门户时显示 AUP。
每次登录时 ( <b>On Every Login</b> )	每次用户登录到网络或门户时显示 AUP。
每 __ 天 (从首次登录算起) ( <b>Every __ Days [starting at first login]</b> )	在用户首次登录到网络或门户时定期显示 AUP。

## 发起人门户的发起人更改密码设置

要为使用发起人门户的发起人配置密码要求，请选择访客访问 (**Guest Access**) > 发起人门户 (**Sponsor Portals**) > 创建、编辑或复制 (**Create, Edit or Duplicate**) > 门户行为和流量设置 (**Portal Behavior and Flow Settings**) > 发起人更改密码设置 (**Sponsor Change Password Settings**)。

字段	使用指南
Allow sponsors to change their own passwords	允许发起人在登录发起人门户后更改密码。此选项仅在发起人在内部用户数据库中时才显示“更改密码” ( <b>Change Password</b> ) 页面。

## 发起人门户的登录后横幅页面设置

此页面的导航路径为：访客访问 (**Guest Access**) > 配置 (**Configure**) > 访客门户或发起人门户 (**Guest Portals or Sponsor Portals**) > 创建、编辑或复制 (**Create, Edit or Duplicate**) > 门户行为和流量设置 (**Portal Behavior and Flow Settings**) > 访问后横幅页面设置 (**Post-Access Banner Page Settings**)。

使用此设置可在用户（适用情况下的访客、发起人或员工）成功登录后向其通知其他信息。

字段	使用指南
包含登录后横幅页面 ( <b>Include a Post-Login Banner page</b> )	在用户成功登录后并在向其授予网络访问权限之前显示其他信息。

## 发起人门户的支持信息页面设置

此页面的导航路径为：访客访问 (**Guest Access**) > 配置 (**Configure**) > 发起人门户 (**Sponsor Portals**) > 创建、编辑或复制 (**Create, Edit or Duplicate**) > 门户行为和流量设置 (**Portal Behavior and Flow Settings**) > 支持信息页面设置 (**Support Information Page Settings**)。

使用这些设置可显示服务中心可用于对用户（适用情况下的访客、发起人或员工）遇到的访问问题进行故障排除的信息。

字段	使用指南
包含支持信息页面 ( <b>Include a Support Information Page</b> )	在门户的所有已启用窗口上显示指向信息窗口（例如联系我们 [ <b>Contact Us</b> ]）的链接。
MAC 地址	在支持信息 ( <b>Support Information</b> ) 窗口上包含设备的 MAC 地址。
IP 地址	在支持信息 ( <b>Support Information</b> ) 窗口上包含设备的 IP 地址。
浏览器用户代理	在支持信息 ( <b>Support Information</b> ) 窗口上包含浏览器详细信息，如产品名称和版本、布局引擎，以及发起请求的用户代理的版本。
策略服务器 ( <b>Policy Server</b> )	在支持信息 ( <b>Support Information</b> ) 窗口上包含服务此门户的 ISE 策略服务节点 (PSN) 的 IP 地址。
故障代码	如果适用，请包含日志消息目录中的对应编号。要查看消息目录，选择 <b>管理 (Administration)</b> > <b>系统 (System)</b> > <b>日志记录 (Logging)</b> > <b>消息目录 (Message Catalog)</b> 。
隐藏字段 ( <b>Hide Field</b> )	如果字段标签将会包含的信息不存在，请勿在支持信息 ( <b>Support Information</b> ) 窗口上显示任何字段标签。例如，如果故障代码未知并因此为空白，请勿显示 <b>故障代码 (Failure code)</b> ，即使已选择故障代码也如此。
显示不含任何值的标签 ( <b>Display Label with no Value</b> )	在支持信息 ( <b>Support Information</b> ) 窗口上显示所有选定字段标签，即使其将会包含的信息不存在也如此。例如，如果故障代码未知，请显示 <b>故障代码 (Failure code)</b> ，即使其为空白也如此。
显示含默认值的标签 ( <b>Display Label with Default Value</b> )	如果标签将会包含的信息不存在，请在支持信息 ( <b>Support Information</b> ) 窗口上的任何选定字段中显示此文本。例如，如果在此字段中输入“不可用” (Not Available)，并且故障代码未知，则 <b>故障代码 (Failure Code)</b> 将显示不可用 ( <b>Not Available</b> )。

## 自定义从发起人门户发送至访客的通知

这些设置的导航路径为：[访客访问 \(Guest Access\)](#) > [配置 \(Configure\)](#) > [发起人门户 \(Sponsor Portals\)](#) > [创建、编辑或复制 \(Create, Edit or Duplicate\)](#) > [门户页面自定义 \(Portal Page Customization\)](#) > [通知访客 \(Notify Guests\)](#)。

在 **Page Customizations** 下，您可以自定义发起人从发起人门户发送至访客的通知上显示的消息、标题、内容、说明和字段与按钮标签。

在 **Settings** 下，您可以指定发起人是否可以使用邮件或 SMS 单独向访客发送用户名和密码。您还可以指定发起人是否可以向访客显示 Support Information 页面，以提供技术支持可用于对访问问题进行故障排除的信息。

## 自定义发起人门户的“管理和审批”选项卡

这些设置的导航路径为：[访客访问 \(Guest Access\)](#) > [配置 \(Configure\)](#) > [发起人门户 \(Sponsor Portals\)](#) > [创建、编辑或复制 \(Create, Edit or Duplicate\)](#) > [门户页面自定义 \(Portal Page Customization\)](#) > [管理和审批 \(Manage and Approve\)](#)。

在 **Page Customizations** 下，您可以自定义发起人门户的 Manage 和 Approve 选项卡上显示的消息、标题、内容、说明以及字段和按钮标签。

其中包括帐户（已注册和待处理）摘要和详细视图、根据发起人对访客帐户执行的操作（例如编辑、扩展、暂停等）显示的弹出对话框，以及常规门户和帐户操作消息。

## 访客和发起人门户的全局设置

选择 [访客访问 \(Guest Access\)](#) > [设置 \(Settings\)](#)。您可以配置以下常规设置应用于思科 ISE 的访客和发起人门户、访客类型以及发起人组：

- 清除访客帐户和生成用户名和密码的策略。
- 向访客和发起人发送邮件和 SMS 通知时使用的 SMTP 服务器和 SMS 网关。
- 使用自助注册访客门户创建访客帐户和注册访客时可选择的位置、时区、SSID 和自定义字段。

配置这些全局设置后，在配置特定访客和发起人门户、访客类型和发起人组时，可以根据需要使用这些设置。

“门户设置” (Portal settings) 页面中提供以下选项卡：

- **访客帐户清除策略 (Guest Account Purge Policy)**：当要清除已过期的访客帐户时安排。有关详细信息，请参阅[安排清除过期访客帐户的时间](#)，第 218 页。
- **自定义字段 (Custom Fields)**：添加用于访客门户的自定义字段，以检索来自用户的其他信息。有关详细信息，请参阅[添加用于创建访客帐户的自定义字段](#)，第 219 页。
- **访客邮件设置 (Guest Email Settings)**：确定是否发送邮件将其帐户的变更通知访客。有关详细信息，请参阅[为邮件通知指定邮箱地址和 SMTP 服务器](#)，第 219 页。



- **访客位置和 SSID (Guest Locations and SSIDs):** 配置位置和访客可以在这些位置中使用的网络服务集标识符 (SSID)。有关详细信息，请参阅[分配访客位置和 SSID](#)，第 219 页。
- **访客用户名策略 (Guest Username Policy):** 配置创建访客用户名的方式。有关详细信息，请参阅[设置访客用户名策略](#)，第 221 页和[访客密码策略规则](#)，第 220 页。
- **访客密码策略 (Guest Password Policy):** 定义所有访客和发起人门户的访客密码策略。有关详细信息，请参阅[设置访客密码策略和到期时间](#)，第 221 页。
- **SMS 网关设置 (SMS Gateway Settings):** 定义用于向访客和发起人发送 SMS 通知的 SMS 网关。有关详细信息，请参阅[配置 SMS 网关以向访客发送 SMS 通知](#)，第 222 页。

## 访客类型设置

这些设置的导航路径为 [访客访问权限 \(Guest Access\)](#) > [配置 \(Configure\)](#) > [访客类型 \(Guest Types\)](#)。使用这些设置可以创建能够访问网络的访客类型及其访问权限。您也可以指定哪些发起人组能够创建此访客类型。

## 发起人组设置

这些设置的导航路径为 [访客访问权限 \(Guest Access\)](#) > [配置 \(Configure\)](#) > [发起人组 \(Sponsor Groups\)](#)。使用这些设置可向发起人组添加成员，定义访客类型和位置权限，以及设置与创建和管理访客帐户相关的权限。

- **禁用发起人组 (Disable Sponsor Group)** - 禁止此发起人组的成员访问发起人门户。

例如，您可能希望在管理门户中进行配置更改时暂时阻止发起人登录到发起人门户。或者，您可能希望禁用不频繁活动（例如，年度会议的发起访客）中涉及的发起人组，直至其需要再次激活。
- **发起人组名称 (Sponsor group name)** - 输入唯一名称（1 至 256 个字符）。
- **Description**

— 包含有用信息（最多 2000 个字符），例如此发起人组使用的访客类型。
- **成员 (Members)** - 点击显示 **选择发起人组成员 (Select Sponsor Group Members)** 复选框，您可以在其中选择可用的用户身份组（从内部和外部身份存储中选择）并将其添加为此发起人组的成员。
- **发起人组成员 (Sponsor Group Members)** - 搜索和筛选所选发起人组的列表，并删除不希望包含的任意组。
- **此发起人组可以使用这些访客类型创建帐户 (This sponsor group can create accounts using these guest types)** - 指定此发起人组的成员在创建访客帐户时可以使用的访客类型。要启用发起人组，该发起人组必须具有至少一个可使用的访客类型。

如果您仅向此发起人组分配一个访客类型，则可以选择不在发起人门户中显示该访客类型，因为它是可供使用的唯一访客类型。依次选择 [访客访问权限 \(Guest Access\)](#) > [配置 \(Configure\)](#)

> 发起人门户 (Sponsor Portal) > 页面自定义 (Page Customization) > 创建帐户 (Create Accounts) > 访客类型 (Guest Types) > 设置 (Settings)。选中 **Hide guest type if only one is available to sponsor** 复选框可启用此选项。

- **配置访客类型 (Configure Guest Types)**

—如果您需要的访客类型不可用，请依次点击 **访客访问权限 (Guest Access) > 配置 (Configure) > 访客类型 (Guest Types)** 并创建新访客类型或编辑现有访客类型。

- **选择访客将访问的位置 (Select the locations that guests will be visiting)** - 选择不同的位置，此组的发起人在创建访客帐户时可将这些位置分配给访客。这可帮助定义这些访客帐户的有效时区，并且指定适用于访客的所有时间参数，如有效访问时间等。这不会阻止访客从其他位置连接到网络。

要启用发起人组，该发起人组必须具有至少一个可使用的位罝。

如果仅向此发起人组分配一个位置，则该位置将是其成员创建的访客帐户的唯一有效时区。默认情况下，该位置不会显示在发起人门户中。

### 发起人可以创建

- **分配给特定访客的多个访客帐户 (导入)** - 允许发起人通过从文件中导入访客详细信息 (例如名字和姓氏) 创建多个访客帐户。

如果启用此选项，则**导入 (Import)** 按钮将显示在发起人门户的**创建帐户 (Create Accounts)** 页面中。Import 选项仅在桌面浏览器 (而非移动) 上可用，例如 Internet Explorer、Firefox、Safari 等。

- **批处理帐户帐户数限制** - 如果允许此发起人组同时创建多个帐户，指定在单个导入操作中可以创建的访客帐户数。

虽然发起人可以创建最多 10000 个帐户，但是由于潜在的性能问题，我们建议您限制创建的帐户数。

- **分配给任意访客的多个访客帐户 (随机) (Multiple guest accounts to be assigned to any guests (Random))** - 允许发起人为尚且未知的访客以占位符形式创建多个随机访客帐户，或快速创建多个帐户。

如果启用此选项，则**随机 (Random)** 按钮将显示在发起人门户的**创建帐户 (Create Accounts)** 页面中。

- **默认用户名前缀** - 指定发起人在创建多个随机访客帐户时可以使用的用户名前缀。如果指定，则在创建随机访客帐户时，发起人门户中会出现此前缀。此外，如果 **Allow sponsor to specify a username prefix** 的状态为：

- 已启用 - 发起人可以在发起人门户中编辑默认前缀。
- 未启用 - 发起人无法在发起人门户中编辑默认前缀。

如果您不指定用户名前缀或者不允许发起人指定用户名前缀，则发起人将无法在发起人门户中分配用户名前缀。

- **允许发起人指定用户名前缀** - 如果允许此发起人组同时创建多个帐户，指定在单个导入操作中创建的访客帐户数。  
虽然发起人可以创建最多 10000 个帐户，但是由于潜在的性能问题，我们建议您限制创建的帐户数。
- **开始日期不能超过未来 \_\_ 天** - 启用并指定天数，而且在此期间，发起人需为其所创建的多个访客帐户设置开始日期。

#### 发起人可以管理

- **仅发起人创建的帐户 (Only accounts sponsor has created)** - 此组中的发起人只能根据发起人的邮件帐户，查看和管理他们创建的访客帐户。
- **此发起人组的成员创建的帐户 (Accounts created by members of this sponsor group)** - 此组中的发起人可查看和管理此发起人组中任意发起人创建的访客帐户。
- **所有访客帐户 (All guest accounts)** - 发起人查看并管理所有待处理访客帐户。



**注释** 无论组成员身份如何，所有发起人都可以查看所有待处理的帐户，除非您选中发起人可以 (**Sponsor Can**) 下面批准并查看自注册访客的请求 (**Approve and view requests from self-registering guests**) 的仅分配给此发起人的待处理帐户 (**Only pending accounts assigned to this sponsor**) 选项。

#### 发起人可以

- **查看访客的密码** - 对于他们可以管理的访客帐户，允许发起人查看密码。  
如果访客密码已更改，则发起人无法再查看；除非发起人将其重置为由思科 ISE 生成的随机密码。



**注释** 如果此选项针对某个发起人组禁用，则该组的成员无法向他们管理的访客帐户发送关于登录凭证（访客密码）的电子邮件和 SMS 通知。

- **重置访客帐户密码** - 对于他们可以管理的访客帐户，允许发起人将访客的密码重置为由思科 ISE 生成的随机密码。
- **延长访客帐户有效期** - 对于他们可以管理的访客帐户，允许发起人将其延长至到期日期之后。发起人自动复制到发送给访客的、有关帐户到期的邮件通知上。
- **发送含访客凭证的 SMS 通知** - 对于他们可以管理的访客帐户，允许发起人向访客发送包含其帐户详细信息和登录凭证的 SMS（文本）通知。
- **删除访客帐户 (Delete guests' accounts)** - 对于他们可以管理的访客帐户，允许发起人删除帐户并阻止访客访问您公司的网络。
- **暂停访客帐户** - 对于他们可以管理的访客帐户，允许发起人暂停其帐户，以阻止访客临时登录。

此操作还会发出授权变更 (CoA) 终止，以从网络中删除暂停的访客。

- **要求发起人提供原因 (Require sponsor to provide a reason)** - 要求发起人提供暂停访客帐户的原因。
- **恢复访客的密码** - 对于他们可以管理的访客帐户，允许发起人恢复暂停的帐户。
- **批准自注册访客的请求** - 对于他们可以管理的访客帐户，允许发起人在收到请求其批准的邮件时批准自注册的访客。
- **批准并查看自注册访客的请求 (Approve and view requests from self-registering guests)** - 此发起人组中的发起人可以查看自注册访客的所有待处理帐户请求（待审批），或仅在用户（作为被访问人）输入发起人邮箱地址时的请求。此功能要求选中自注册访客使用的门户中的**要求自注册访客需获得批准 (Require self-registered guests to be approved)**，而且列有发起人（作为联系人）的电子邮件。
- **使用编程接口（访客 REST API）访问思科 ISE 访客帐户** - 对于他们可以管理的访客帐户，允许发起人使用访客 REST API 编程接口访问访客帐户。

## 最终用户门户

思科 ISE 为三类主要最终用户提供基于 Web 的门户：

- 需要使用访客门户（热点和有凭证访客门户）临时访问企业网络的访客。
- 被指定为发起人，可以使用 Sponsor 门户创建和管理访客帐户的员工。
- 使用各种非访客门户（例如 Bring Your Own Device (BYOD) 门户、Mobile Device Management (MDM) 门户和 My Devices 门户）在企业网络上使用其个人设备的员工。

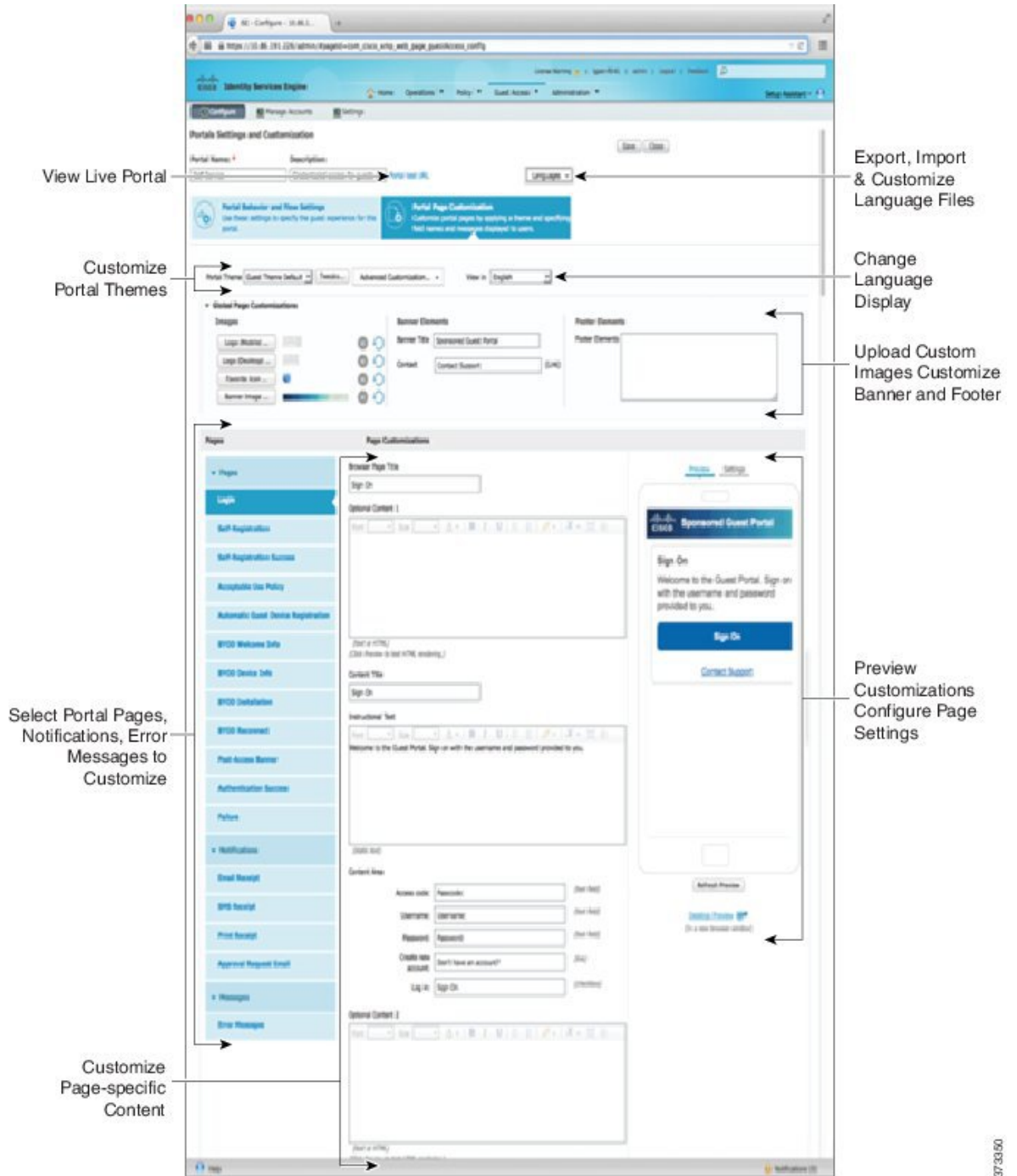
## 自定义最终用户 Web 门户

您可以编辑、复制和创建更多门户。您也可以完全自定义门户外观以及门户体验。您可以单独自定义每个门户，而不影响其他门户。

您可以自定义门户界面的各个要素，这些自定义设置可以适用于整个门户，也可以适用于门户的特定页面，例如：

- 主题、图像、颜色、横幅和页脚
- 用于显示门户文本、错误消息和通知的语言
- 标题、内容、说明以及字段和按钮标签
- 通过邮件、SMS 和打印机发送给访客的通知（仅适用于自行注册访客门户和发起人门户）
- 显示给用户的错误消息和信息性消息
- 对于自注册访客和发起人门户，可以创建自定义字段以搜集特定于您的需求的访客信息

图 11: 自定义门户页面布局



### 自定义方法

自定义最终用户门户页面的方法有多种，各自需要不同的知识水平。

- **基本：**您可以修改门户“自定义”页面：

- 上传条幅和徽标
- 更改某些颜色（按钮除外）
- 更改屏幕上的文本以及整个门户上使用的语言

- 中级

- 使用迷你编辑器添加 HTML 和 Javascript



注释 要在迷你编辑器中输入 HTML，需要先单击 HTML 图标。

- 使用 jQuery 移动主题滚动条可更改所有页面元素的颜色

- 高级

- 手动修改属性和 CSS 文件。

自定义门户后，可以通过复制该门户来创建（相同类型的）多个门户。例如，如果已为一家商业实体自定义热点访客门户，则可以复制此门户，稍作更改，为其他商业实体创建自定义热点访客门户。

#### 使用迷你编辑器自定义门户的技巧

- 迷你编辑器框中的长字词可能会滚动出门户的屏幕区域。可以使用 HTML 段落属性 `style="word-wrap: break-word"` 中断行。例如：

```
<p style="word-wrap:break-word">
```

```
thisisaverylonglineoftextthatwillexceedthewidthoftheplacethatyouwanttoputitsousethisstructure
```

```
</p>
```

- 使用 HTML 或 javascript 自定义门户页面时，应确保使用有效的语法。思科 ISE 不会验证输入迷你编辑器的标签和代码。无效语法有可能在门户流程中造成问题。

## 门户内容类型

思科 ISE 提供一组默认门户主题，您可以“按原样”使用或使用现有 CSS 文件作为模型进行自定义，以创建新的自定义文件。但是，可以在不使用自定义 CSS 文件的情况下修改门户的外观。

例如，如果想要使用唯一的公司徽标和横幅图像，只需上传和使用这些新的图像文件。可以通过更改门户的不同元素和区域的颜色来自定义默认配色方案。甚至可以选择在进行自定义更改时查看更改所要使用的语言。

当设计要替换徽标和横幅的图像时，尽可能让图像接近以下像素大小：

横幅	1724 X 133
桌面徽标	86 X 45

移动徽标	80 X 35
------	---------

请注意，ISE 会调整图像的大小以适合门户，但过小的图像在调整大小之后可能无法正确显示。

要执行高级自定义，如更改页面布局或在门户页面上添加视频剪辑或广告，可以使用自定义 CSS 文件。

在特定门户内，这些类型的更改会全局应用到该门户的所有页面。对页面布局的更改可以全局应用或只应用到门户中的某个特定页面。

#### 门户页面标题、内容和标签

您可以自定义标题、文本框、说明、字段与按钮标签，以及访客在最终用户 Web 门户页面上查看的其他可视元素。在自定义页面时，甚至可以动态编辑页面设置。

这些更改只适用于您所自定义的特定页面。

## 门户的基本自定义

选择最适合您的需求的预定义主题，并使用其大多数默认设置。然后，您可以执行基本的自定义，例如：

- [修改门户主题颜色，第 279 页](#)
- [更改门户图标、图像和徽标，第 280 页](#)
- [更新门户的横幅和页脚元素，第 281 页](#)
- [更改门户显示语言，第 280 页](#)
- [更改标题、说明、按钮和标签文本，第 282 页](#)
- [格式和样式文本框内容，第 282 页](#)



**提示** 当您进行更新时，您可以[查看您的自定义，第 286 页](#)。

## 修改门户主题颜色


可以自定义默认门户主题中的默认配色方案，并更改门户的不同元素和区域的颜色。这些更改将应用于您自定义的所有门户。

如果计划更改门户颜色，请注意以下事项：

- 无法使用此选项更改可能已导入用于此门户的任何自定义门户主题中的配色方案。必须编辑自定义主题 CSS 文件才能更改其颜色设置。
- 更改门户主题中的颜色之后，如果从 **Portal Theme** 下拉菜单中选择其他门户主题，则原始门户主题中的更改将丢失，颜色将恢复到其默认颜色。

- 如果使用已修改的配色方案调整门户主题的颜色，然后在保存方案前重置其颜色，则配色方案将恢复到其默认颜色，且之前所做的所有修改都将丢失。

**步骤 1** 导航至以下门户：

- 对于访客门户，选点击菜单图标 ()，然后选择 访客访问 (Guest Access) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。
- 对于发起人门户，选择 访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。

**步骤 2** 从 **Portal Theme** 下拉列表选择一个默认主题。

**步骤 3** 点击 **Tweaks** 以覆盖选定默认门户主题中的某些颜色设置。

- a) 更改横幅和页面背景、文本和标签的颜色设置。
- b) 如果要恢复到主题的默认配色方案，请点击 **Reset Colors**。
- c) 如果要在 **Preview** 中查看颜色更改，请点击 **OK**。

**步骤 4** 点击保存 (Save)。

## 更改门户显示语言

您可以选择您想要用于查看您所做的自定义更改的语言。此更改适用于您所自定义的整个门户。

**步骤 1** 导航至以下门户：

- 对于发起人门户，选择 访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 全局自定义 (Global Customization)。
- 对于设备门户，选择 管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 全局自定义 (Global Customization)。

**步骤 2** 从 **View In** 下拉列表选择您想要用于在自定义页面时查看文本的语言。

此下拉列表包含与特定门户关联的语言文件中的所有语言。

下一步做什么

确保将您在自定义门户页面期间以所选语言所做的任何更改都更新至所支持的语言属性文件中。

## 更改门户图标、图像和徽标

如果要使用唯一的公司徽标、图标和横幅图像，只需通过上传自定义图像即可替换现有图像。支持的图像格式包括：.gif、.jpg、.jpeg 和 .png。这些更改将应用于您自定义的所有门户。



## 开始之前

要在门户的页脚（例如，广告）中包含图像，应该能够访问具有这些图像的外部服务器。

### 步骤 1 导航至以下门户：

- 对于访客门户， 选点击菜单图标 (☰)，然后选择 访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。
- 对于发起人门户，选择 访客访问 (Guest Access) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。
- 对于设备门户，选择 管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。

步骤 2 在 **Images** 下方，点击任意徽标、图标和图像按钮，然后上传自定义图像。

步骤 3 点击保存 (Save)。

## 更新门户的横幅和页脚元素

您可以自定义门户各页面中横幅和页脚部分所显示信息。这些更改将应用于您自定义的所有门户。

### 步骤 1 导航至以下门户：

- 对于访客门户， 选点击菜单图标 (☰)，然后选择 访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。
- 对于发起人门户，选择 访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。
- 对于设备门户，选择 管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。

步骤 2 更改显示在各门户页面中的横幅标题 (Banner title)。

步骤 3 包括这些使用门户的访客链接：

- **帮助 (Help)** - 在线帮助（仅提供给发起人和我的设备门户）。
- **联系方式 (Contact)** - 技术支持（设置支持信息页面以启用它）。

步骤 4 在各门户页面上显示的页脚元素 (Footer Elements) 中添加免责声明或版权声明。

步骤 5 点击保存 (Save)。

## 更改标题、说明、按钮和标签文本

您可以更新门户中显示的所有文本。您所自定义的页面上的每个 UI 元素对于您可以输入的字符数都有最高和最低范围限制。有些文本块提供小型编辑器，您可以使用此编辑器将视觉风格应用于相应文本。这些更改只适用于您自定义的特定门户页面。这些页面元素对于邮件、SMS 和打印通知是不同的。

**步骤 1** 导航至以下门户：

- 对于访客门户，选点击菜单图标 (☰)，然后选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。

**步骤 2** 在 **Pages** 下，选择您想要更改的页面。

**步骤 3** 在 **Page Customizations** 下，更新任何显示的 UI 元素。所有页面均包含浏览器页面标题 (**Browser Page Title**)、内容标题 (**Content Title**)、说明文本 (**Instructional Text**)、内容 (**Content**) 和两个可选内容 (**Optional Content**) 文本块。**Content** 区域的字段是特定于各页面的。

## 格式和样式文本框内容

使用说明文本 (**Instructional Text**)、可选内容 1 (**Optional Content 1**) 和 可选内容 2 (**Optional Content 2**) 文本框中可用的小型编辑器对文本执行基本格式处理。这些更改仅用于您自定义的特定门户页面。

使用切换全屏 (**Toggle Full Screen**) 按钮可在使用文本框时缩放其大小。

**步骤 1** 导航至以下门户：

- 对于访客门户，选点击菜单图标 (☰)，然后选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。

**步骤 2** 在 **Pages** 下，选择您想要更改的页面。

**步骤 3** 在页面自定义 (**Page Customizations**) 下，在说明文本 (**Instructional Text**) 和 可选文本 (**Optional Content**) 文本块中，您可以执行以下操作：

- 更改文本的字体、大小和颜色。
- 将文本样式设置为粗体、斜体或带下划线。
- 创建带项目符号和编号的列表。

**注释** 您可以使用 **切换 HTML 源 (Toggle HTML Source)** 按钮查看应用于您使用小型编辑器进行格式设置的文本的 HTML 标记。如果在 **HTML 源 (HTML Source)** 视图中编辑文本，请再次单击**切换 HTML 源 (Toggle HTML Source)** 按钮，然后再在门户页面自定义 (**Portal Page Customization**) 窗口中保存所做更改。

## 用于门户页面自定义的变量

这些门户页面文本框的导航路径为：

- 对于访客门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 页面 (Pages)**。
- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 页面 (Pages)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 页面 (Pages)**。

为门户内容和访客通知创建模板时，请使用这些变量，从而确保向门户用户（访客、发起人和员工）显示的信息的一致性。对每个门户，请使用此处列出的变量名称替换**说明文本 (Instructional Text)**、**可选内容 1 (Optional Content 1)** 和**可选内容 2 (Optional Content 2)** 文本框中的文本。

表 36: 访客门户的变量列表

显示名称	用以下变量名称替换
Access code 用于以电子邮件、文本或打印通知的形式向访客提供访问代码。	ui_access_code
BYOD IOS SSID 用于指定在双 SSID 流程中完成自行激活之后设备应该连接的网络。	ui_byod_success_ios_ssid
Client Provisioning Agent Type 用于指定客户端调配策略中当前配置的代理。	ui_client_provision_agent_type
Client Provisioning Agent URL 用于指定安全评估代理的下载 URL。	ui_client_provision_agent_url

显示名称	用以下变量名称替换
Client Provisioning agent install minutes 用于向访客通知其必须在多长时间内（由补救计时器设置）按照客户端调配 (Client Provisioning) 窗口上的说明完成安装。如果访客未在计时结束前按照说明完成安装，就必须刷新浏览器页面并再次执行登录过程。	ui_client_provision_install_agent_mins
Company	ui_company
Email address	ui_email_address
End date and time	ui_end_date_time
First name	ui_first_name
Last name	ui_last_name
Location name	ui_location_name
Maximum registered devices	ui_max_reg_devices
Maximum simultaneous logins	ui_max_siml_login
Password	ui_password
Person being visited (email)	ui_person_visited
Phone number	ui_phone_number
Reason for visit	ui_reason_visit
SMS Provider	ui_sms_provider
SSID 用于指定访客可用于连接网络的无线网络。	ui_ssid
Start date and time	ui_start_date_time
Time left	ui_time_left
Username	ui_user_name

表 37: 发起人门户的变量列表

显示名称	用以下变量名称替换
Guest - Company	ui_guest_company
Guest - Email address	ui_guest_email_address
Guest - End date and time	ui_guest_end_date_time

显示名称	用以下变量名称替换
Guest - First name	ui_guest_first_name
Guest - Last name	ui_guest_last_name
Guest - Location name	ui_guest_location_name
Guest - Maximum registered devices	ui_guest_max_reg_devices
Guest - Maximum simultaneous logins	ui_guest_max_siml_login
Guest - Password	ui_guest_password
Guest - Person being visited (email)	ui_guest_person_visited
Guest - Phone number	ui_guest_phone_number
Guest - Reason for visit	ui_guest_reason_visit
Guest - SMS Provider	ui_guest_sms_provider
Guest - SSID 用于指定访客可用于连接网络的无线网络。	ui_guest_ssid
Guest - Start date and time	ui_guest_start_date_time
Guest - Time left	ui_guest_time_left
Guest - Username	ui_guest_user_name
Username 用于指定登录门户的用户的用户名。	ui_sponsor_user_name

表 38: MDM 门户的变量列表

显示名称	用以下变量名称替换
MDM - Vendor Name	ui_mdm_vendor_name

表 39: My Devices 门户的变量列表

显示名称	用以下变量名称替换
MyDevices - Login Failure Rate Limit	\$user_login_failure_rate_limit\$
MyDevices - Max Devices to Register	ui_max_register_devices
MyDevices - User Name 用于指定登录门户的用户的用户名。	\$session_username\$

## 查看您的自定义

您可以查看自己的自定义向门户用户（访客、发起人或员工）的显示方式。

**步骤 1** 点击 **Portal test URL** 查看您做出的更改。

**步骤 2** （可选）点击**预览 (Preview)** 以动态查看所做的更改如何出现在各类设备上：

- 移动设备：在**预览 (Preview)** 下查看做出的更改。
- 桌面设备：单击**预览 (Preview)** 并单击**桌面预览 (Desktop Preview)**。

如果没有显示更改，请点击 **Refresh Preview**。所显示的门户仅用于查看您做出的更改；您无法点击按钮或输入数据。

**注释** 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。如果有多个 PSN，思科 ISE 会选择第一个活动 PSN。

## 门户的高级自定义

如果不想使用思科 ISE 提供的任一默认门户主题，您可以对门户进行自定义来满足您的需求。为此，您必须熟悉使用 CSS 和 JavaScript 文件以及 jQuery Mobile ThemeRoller 应用。

您不能修改默认门户主题，但可以执行以下操作：

- [导出门户的默认主题 CSS 文件，第 291 页](#)，将其用作创建自定义门户主题的基础。
- [创建自定义门户主题 CSS 文件，第 292 页](#)，方法是编辑默认门户主题并将其另存为新文件。
- [导入自定义门户主题 CSS 文件，第 302 页](#)，并将其应用于门户。

基于您的专业知识程度和具体要求，您可执行各种高级自定义。您可以使用预定义变量来实现显示信息的一致性，在门户页面上添加广告，使用 HTML、CSS 和 Javascript 代码来自定义您的内容，以及修改门户页面布局。

您可以通过将 HTML、CSS 和 javascript 添加到每个门户的门户页面定制 (**Portal Page Customization**) 选项卡上的内容框中来修改门户。本文档提供使用 HTML 和 CSS 进行定制的示例。使用 javascript 定制的示例位于此处的 ISE 社区：<http://cs.co/ise-community>。更多 HTML、CSS 和 Javascript 示例位于此处的 ISE 社区：

<https://community.cisco.com/t5/security-documents/how-to-ise-web-portal-customization-options/ta-p/3619042>。



**注释** TAC 不支持思科 ISE 门户的 Javascript 定制。如果您在使用 Javascript 定制时遇到问题，请将您的问题发布到 ISE 社区 <https://community.cisco.com/t5/identity-services-engine-ise/bd-p/5301j-disc-ise>。

## 启用高级门户自定义

思科 ISE 可以让您自定义最终用户门户上显示的内容。在门户页面自定义 (**Portal Page Customization**) 下列出的不同页面上的文本框中输入 HTML、CSS 和 Javascript 代码。

- 
- 步骤 1** 选择 **管理 (Administration) > 系统 (System) > 管理员访问权限 (Admin Access) > 设置 (Settings) > 门户定制 (Portal Customization)**。
- 步骤 2** 验证在默认情况下是否已选中 **Enable portal customization with HTML**。此设置可以让您在说明文本 (**Instructional Text**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 字段中包含 HTML 标签。
- 步骤 3** 选中启用 **HTML 和 JavaScript 门户自定义 (Enable portal customization with HTML and Javascript)** 后，可以通过包含以下字段进行高级 JavaScript 自定义：`<script>` tags in the 说明文本 (**Instructional Text**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 字段。
- 

## 门户的主题和结构 CSS 文件

如果您具有使用 CSS 文件方面的经验，则可以自定义默认门户主题 CSS 文件以修改门户演示和操作页面布局、颜色和字体等元素。自定义 CSS 文件使您在指定演示特征时能够灵活控制，从而使您能够在多个页面上共享格式，并降低结构内容的复杂性和重复性。

思科 ISE 最终用户门户使用两种不同类型的 CSS 文件：`structure.css` 和 `theme.css`。每个门户主题都有其自己的 `theme.css` 文件，但每个门户类型只有一个 `structure.css` 文件；例如，适用于访客门户的 `guest.structure.css`、适用于发起人门户的 `sponsor.structure.css`，以及适用于我的设备门户的 `mydevices.structure.css`。

`structure.css` 为页面布局和结构提供样式。它定义每个页面上的元素的定位，并且包括 jQuery Mobile 结构样式。只可以查看 `structure.css` 文件，但不能进行编辑。但是，当更改 `theme.css` 文件中的页面布局时，请将这些文件导入门户，并进行应用，最新更改将优先于 `structure.css` 样式。

`theme.css` 文件指定字体、按钮颜色和标题背景等样式。您可以导出 `theme.css` 文件，更改主题设置，然后导入这些设置，用作门户的自定义主题。对 `theme.css` 文件所做的所有页面布局样式更改都将优先于在 `structure.css` 文件中定义的样式。

无法修改任何思科提供的默认门户 `theme.css` 文件。但是，可以编辑文件中的设置并将这些设置保存到新的自定义 `theme.css` 文件。可以对自定义 `theme.css` 文件进行进一步编辑，但将其导入回思科 ISE 时，记得要使用与最初所用主题名称相同的名称。无法将两个不同的主题名称用于同一个 `theme.css` 文件。

例如，可以使用默认的 `green theme.css` 文件创建新的自定义 `blue theme.css` 文件并将该文件命名为 `Blue`。之后，可以编辑 `blue theme.css` 文件，但是当您再次导入此文件时，必须重新使用 `Blue` 主题名称。不能将其命名为 `Red`，因为思科 ISE 会检查文件名与其名称之间的关系，以及主题名称的唯一性。但是，可以编辑 `blue theme.css` 文件，将其另存为 `red theme.css`，导入新文件，然后将其命名为 `Red`。

## 使用 jQuery Mobile 更改主题颜色

思科最终用户门户的颜色主题与 jQuery ThemeRoller 兼容。您可以使用 ThemeRoller 网站轻松编辑整个门户的颜色。

ThemeRoller 颜色“样本”包含一个独特的颜色主题，用于定义主要 UI 元素（例如工具栏、内容块、按钮、列表项和字体文本阴影）的颜色、底纹和字体设置。颜色主题还定义按钮各种交互状态设置：正常、悬停和按下。

思科使用三种样本：

- 样本 A - 默认样本。
- 样本 B - 定义着重强调的元素，例如 **Accept** 按钮。
- 样本 C - 定义关键元素，例如警告、错误消息、无效输入字段和删除按钮。

您无法应用其他样本，除非您添加包含使用新增样本的元素的 HTML 代码（例如添加至 **Optional Content** 中）。

要编辑思科提供的默认 CSS 文件或创建基于默认主题中定义的 CSS 类和新结构的新文件，请使用规定版本的 [jQuery Mobile ThemeRoller \(1.3.2 版本\)](#)。

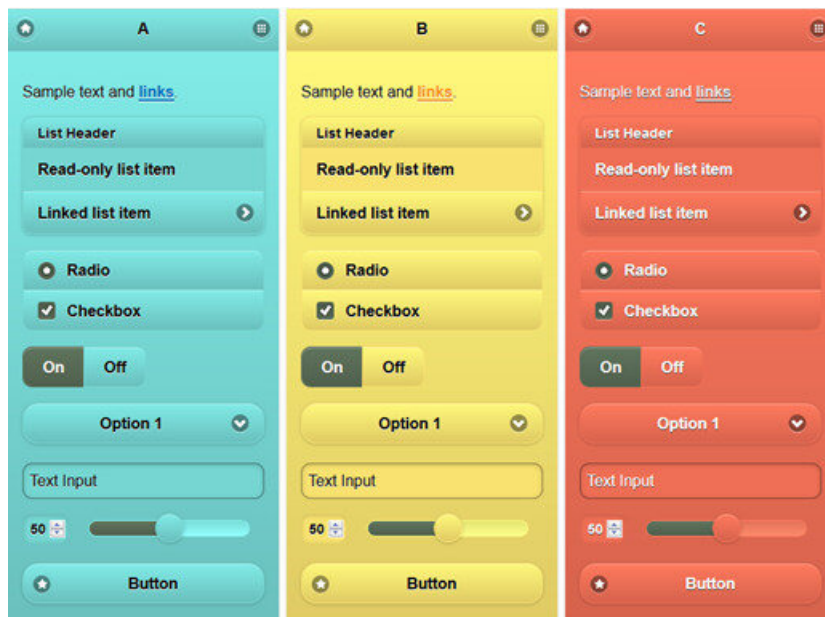
有关 jQuery Mobile ThemeRoller 中样本和主题的更多信息，请参阅 [使用 ThemeRoller 创建自定义主题](#) 中的“创建主题概述”。请使用 jQuery Mobile ThemeRoller 在线帮助了解如何下载、导入和共享您的自定义主题。

有关如何使用 HTML、CSS 和 Javascript 代码自定义在门户页面上显示的文本和内容的教程，请访问 [CodeAcademy](#)。

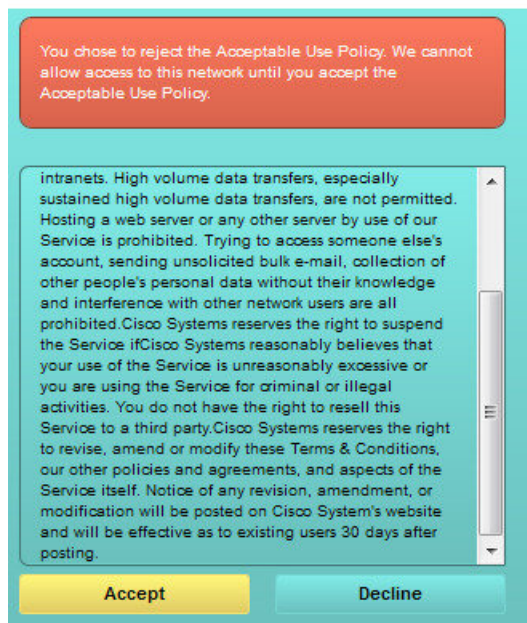
### 显示思科样本的主题示例

为了演示如何使用样本，我们在 ThemeRoller 中编辑了用于访客门户的默认主题以显示颜色差异。





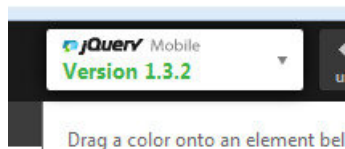
以下屏幕显示访客门户登录错误（样本 C）以及要求用户操作的按钮（样本 B），屏幕的其余部分为样本 A。



## 使用 jQuery Mobile 更改主题颜色

开始之前

确保您使用的是 1.3.2 版本的 jQuery Mobile ThemeRoller。屏幕左上角会显示您所使用的版本，如下所示。



**步骤 1** 在门户上点击配置 (**Configuration**) 选项卡，从门户中导出您想要更改的现有主题。

**步骤 2** 选择高级定制 (**Advanced Customization**) > 导出/导入主题 (**Export/Import Themes**)。

**步骤 3** 在自定义主题 (**Custom Theming**) 对话框中，导出您要更新的主题。

**步骤 4** 在文本编辑器中打开该主题，全选并复制。

**步骤 5** 将该文本 (CSS) 粘贴到 jQuery 网站的导入主题 (**Import Theme**) 字段。

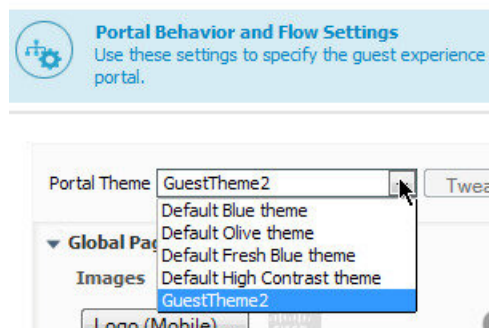
**步骤 6** 在 jQuery Mobil Web 版应用中执行更改。

**步骤 7** 从 jQuery 网站导出更新的主题 (导出格式为 ZIP)。

**步骤 8** 解压缩更新的主题，从主题文件夹中将更新的主题提取至您的 PC。主题名称即您在 jQuery 网站提供的名称。

**步骤 9** 在门户配置页面的自定义主题 (**Custom Theming**) 对话框中将提取的 CSS 主题文件导入您的门户。

您可以点击门户配置 (**Portal Configuration**) 窗口上的门户主题 (**Portal Theme**) 下拉列表，在新旧主题之间来回切换。



## 基于位置的自定义

创建访客帐户后，您可以将其与某个位置关联并指定服务集标识符 (SSID) 属性。位置和 SSID 均可用作 CSS 类，您可以将 CSS 类用于根据访客的位置和 SSID 向门户页面应用不同的 CSS 样式。

例如：

- 访客位置 - 当使用 *San Jose* 或 *Boston* 作为位置的帐户的用户登录需要提供凭证的访客门户时，以下一个类可用于每个门户页面：**guest-location-san-jose** 或 **guest-location-boston**。
- 访客 SSID - 对于名称为 *Coffee Shop Wireless* 的 SSID，以下 CSS 类可用于每个门户页面：**guest-ssid-coffee-shop-wireless**。此 SSID 是您在访客帐户上指定的 SSID，而不是访客在登录时连接的 SSID。



**注释** 此信息仅适用于需要提供凭证的访客门户（在访客登录之后）。

当您向网络添加交换机和无线 LAN 控制器 (WLC) 等设备时，也可以指定位置。此位置还可用作根据网络设备的位置向门户页面应用不同 CSS 样式的 CSS 类。

例如，如果向 *Seattle* 分配 WLC 并且访客从 *Seattle-WLC* 重定向至思科 ISE，以下 CSS 类可用于每个门户页面：**device-location-my-locations-usa-seattle**。

**相关主题**

[根据访客位置自定义问候语](#)，第 298 页

## 基于用户设备类型的自定义

思科 ISE 会检测用来访问公司网络或最终用户 Web 门户（访客、发起人和设备）的客户端设备类型（访客、发起人或员工）。它会被检测为移动设备（Android、iOS 等）或桌面设备（Windows、MacOS 等）。设备类型可作为 CSS 类，您可以根据用户的设备类型，使用该类将不同的 CSS 样式应用到门户页面。

当用户登录任何思科 ISE 最终用户 Web 门户时，门户页面上提供以下类：**cisco-ise-mobile** 或 **cisco-ise-desktop**。

**相关主题**

[根据用户设备类型自定义问候语](#)，第 299 页

## 导出门户的默认主题 CSS 文件

您可以下载思科提供的默认门户主题并按照您的需求进行自定义。您可以将其用作执行高级自定义的基础。

**步骤 1** 导航至以下门户：

- 对于访客门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 页面 (Pages)**。
- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 页面 (Pages)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 页面 (Pages)**。

**步骤 2** 从高级自定义 (Advanced Customization) 下拉列表中，选择导出/导入主题 (Export/Import Themes)。

**步骤 3** 在自定义主题 (Custom Theming) 对话框中，使用下拉菜单选择您想要自定义的主题。

**步骤 4** 点击导出主题 CSS (Export Theme CSS) 以下载默认 *theme.css* 文件进行自定义。

**步骤 5** 点击保存 (Save) 将文件保存至您的桌面。

## 创建自定义门户主题 CSS 文件

通过自定义现有默认门户主题和在新门户 *theme.css* 文件中保存更改，可以创建自定义门户主题。可以修改默认主题设置和样本，对选中的门户进行全局更改。

### 开始之前

- 将 *theme.css* 文件从想要自定义的门户下载到桌面。
- 此任务需要拥有使用 HTML、CSS 和 Javascript 代码的经验。
- 使用 jQuery Mobile ThemeRoller 版本 1.3.2

---

**步骤 1** 将已下载的门户 *theme.css* 文件内容导入 jQuery Mobile ThemeRoller 工具。

**提示** 做出更改时，您可以 [查看您的自定义](#)，第 303 页。

**步骤 2** (可选) [在门户内容中嵌入链接](#)，第 292 页

**步骤 3** (可选) [插入动态文本更新的变量](#)，第 293 页

**步骤 4** (可选) [使用源代码设置文本格式和包含链接](#)，第 294 页

**步骤 5** (可选) [将图像添加为广告](#)，第 295 页

**步骤 6** (可选) [根据访客位置自定义问候语](#)，第 298 页

**步骤 7** (可选) [根据用户设备类型自定义问候语](#)，第 299 页

**步骤 8** (可选) [设置轮播广告](#)，第 296 页

**步骤 9** (可选) [修改门户页面布局](#)，第 300 页

**步骤 10** 将自定义文件另存为新的 *theme.css* 文件。

**注释** 不能将编辑保存到默认 CSS 主题文件。只能使用已进行的任何编辑创建新的自定义文件。

**步骤 11** 当新 *theme.css* 文件就绪时，可以将其导入思科 ISE。

---

## 在门户内容中嵌入链接

您可以添加链接以使访客可以从门户页面访问各种网站。这些更改仅用于您进行自定义的特定门户页面。

使用**切换全屏 (Toggle Full Screen)** 选项可在使用字段时缩放其大小。

---

**步骤 1** 导航至以下门户：

- 对于访客门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。

- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。

**步骤 2** 在 **页面 (Pages)** 下，选择想要更新的页面。

**步骤 3** 在 **页面自定义 (Page Customizations)** 下，使用带有可选内容 (**Optional Content**) 文本块的小型编辑器向门户页面添加链接。

**步骤 4** 点击 **创建链接 (Create Link)** 按钮。

此时将显示 **链接属性 (Link Properties)** 对话框。

**步骤 5** 输入 **URL** 并且在 **URL 的描述 (Description)** 窗口输入您要添加超链接的文本。

为使链接正常工作，URL 中应包括协议标识符。例如使用 `http://www.cisco.com` 而不是 `www.cisco.com`。

**步骤 6** 点击 **设置 (Set)**，然后点击 **保存 (Save)**。

可以使用 **切换 HTML 源 (Toggle HTML Source)** 选项查看应用于您使用小型编辑器进行格式设置的文本的 HTML 标记。

---

## 插入动态文本更新的变量

通过替代动态更新内容的预定义变量 (`$variable$`)，您可以为显示在门户的文本创建模板。这可以使向访客显示的文本和信息保持一致。这些更改仅用于您自定义的特定门户页面。

使用 **切换全屏 (Toggle Full Screen)** 选项可在使用字段时缩放其大小。

---

**步骤 1** 导航至以下门户：

- 对于访客门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。

**步骤 2** 在 **Pages** 下，选择要更新的页面。

**步骤 3** 在 **页面定制 (Page Customizations)** 下，使用 **说明文本 (Instructional Text)**、**可选内容 1 (Optional Content 1)** 和 **可选内容 2 (Optional Content 2)** 字段随附的小型编辑器创建门户页面的文本模板。

例如，您可以为多个访客创建一个欢迎消息模板，但只有在访客成功登录并连接到网络之后才能看到个性化设置的消息。

**步骤 4** 像往常一样在字段中输入信息。

例如，您可以为您的门户输入一条欢迎消息：

```
Welcome to our company' s Guest portal,
```

**步骤 5** 如果要用变量替代文本，请点击**插入变量 (Insert Variable)**。

变量列表将显示在弹出菜单中。

**步骤 6** 选择用于替代文本的变量。

例如，选择**名字 (First name)** 以在欢迎消息中显示每位访客的名字。变量 `$ui_first_name$` 插入到光标位置：

```
Welcome to our company' s Guest portal,$ui_first_name$.
```

此欢迎消息会出现在名叫 John 的访客的门户欢迎页面上：**Johen**，欢迎访问我们公司的访客门户。

**步骤 7** 根据需要使用变量列表，直到您在文本框中完成信息输入。

**步骤 8** 点击 **Save**。

可以使用 **切换 HTML 源 (Toggle HTML Source)** 选项查看应用于您使用小型编辑器进行格式设置的文本的 HTML 标记。

## 使用源代码设置文本格式和包含链接

除了可以将小型编辑器的格式设置和链接图标用于纯文本，您还可以使用 HTML、CSS 和 Javascript 代码来自定义在门户页面上显示的文本。这些更改仅用于您自定义的特定门户页面。

使用**切换全屏 (Toggle Full Screen)** 选项可在使用文本框时缩放其大小。

### 开始之前

确保在**管理 (Administration) > 系统 (System) > 管理访问 (Admin Access) > 设置 (Settings) > 门户自定义 (Portal Customization)** 中默认启用**启用 HTML 的门户自定义 (Enable portal customization with HTML)**。

**步骤 1** 导航至以下门户：

- 对于访客门户，选点击菜单图标 (☰)，然后选择**访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，选择**访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，选择**管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。

**步骤 2** 在**页面 (Pages)** 下，选择想要更新的页面。

**步骤 3** 在**页面定制 (Page Customizations)** 下，使用**说明文本 (Instructional Text)**、**可选内容 1 (Optional Content 1)** 和**可选内容 2 (Optional Content 2)** 字段随附的小型编辑器输入和查看源代码。

**步骤 4** 点击**切换 HTML 源 (Toggle HTML Source)**。

**步骤 5** 输入您的源代码。

例如，要为文本添加下划线，请输入：

```
<p style="text-decoration:underline;">Welcome to Cisco!</p>
```

例如，要使用 HTML 代码加入一个链接，请输入：

```
<a href="http://www.cisco.com">Cisco</a>
```

**重要事项** 当在 HTML 代码中插入外部 URL 时，确保您输入的是包括“http”或“https”的绝对（完整）URL 路径。

**步骤 6** 点击保存 (Save)。

相关主题

[启用高级门户自定义](#)，第 287 页

## 将图像添加为广告

您可以加入要在门户页面的特定区域中显示的图像和广告。

使用切换全屏 (**Toggle Full Screen**) 选项可在使用文本框时缩放其大小。

开始之前

确保在 **管理 > 系统 > 管理访问 > 设置 > 门户自定义** 中启用 **启用 HTML** 的门户自定义。

**步骤 1** 导航至以下门户：

- 对于访客门户，选点击菜单图标 (☰)，然后选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。

**步骤 2** 在 **页面 (Pages)** 下，选择想要更新的页面。

**步骤 3** 在 **页面定制 (Page Customizations)** 下，使用 **说明文本 (Instructional Text)**、**可选内容 1 (Optional Content 1)** 和 **可选内容 2 (Optional Content 2)** 字段随附的小型编辑器输入和查看源代码。

**步骤 4** 点击切换 **HTML 源 (Toggle HTML Source)**。

**步骤 5** 输入您的源代码。

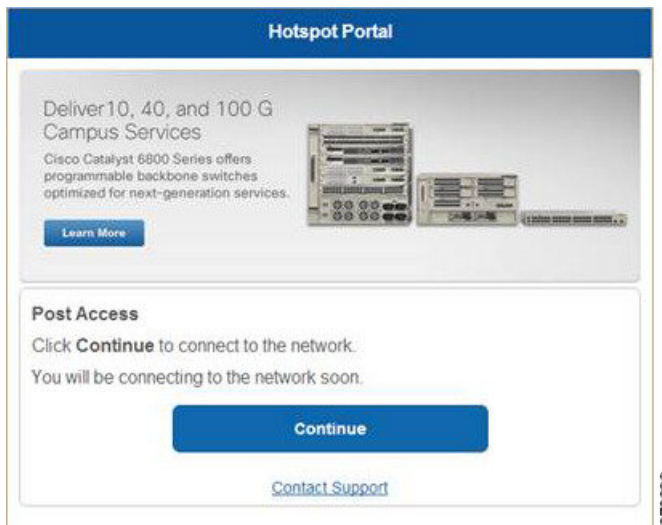
例如，要使用 HTML 代码在热点访客门户访问后横幅上加入产品广告及其图像，请在 **Post-Access Banner** 页面上的 **Optional Content 1** 文本框中输入此代码：

```
<p style="text-decoration:underline;">Optimized for 10/40/100 Campus Services!</p>

```

**注释** 当在 HTML 代码中插入外部 URL 时，确保您输入的是包括“http”或“https”的绝对（完整）URL 路径。

图 12: 广告图像示例



步骤 6 点击保存 (Save)。

## 设置轮播广告


轮播广告是一种广告格式，在一个横幅内显示多个产品图像和文本说明并且重复循环播放。在您的访客门户上使用轮播广告以推广多个相关产品或您公司提供的各种不同产品。

使用切换全屏 (**Toggle Full Screen**) 选项可在使用文本框时缩放其大小。

开始之前

选择 **管理 (Administration)** > **系统 (System)** > **管理访问 (Admin Access)** > **设置 (Settings)** > **门户自定义 (Portal Customization)**，然后选中通过 **HTML** 和 **Javascript** 启用门户自定义 (**Enable portal customization with HTML and Javascript**)。

步骤 1 导航至以下门户：

- 对于访客门户，选点击菜单图标 ()，然后选择 **访客访问 (Guest Access)** > **配置 (Configure)** > **访客门户 (Guest Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，选择 **访客访问 (Guest Access)** > **配置 (Configure)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > (任何门户 [any Portals]) > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)**。

步骤 2 在页面 (**Pages**) 下，选择想要更新的页面。

步骤 3 在页面定制 (**Page Customizations**) 下，使用说明文本 (**Instructional Text**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 字段随附的小型编辑器输入和查看源代码。



**步骤 4** 点击切换 **HTML 源 (Toggle HTML Source)**。

**步骤 5** 输入您的源代码。

例如，要在访客门户上使用产品图像实施轮播广告，请在访问后横幅 (**Post-Access Banner**)（对于热门门户）或登录后横幅 (**Post Login Banner**) 窗口（对于需要提供凭证的访客门户）可选内容 **1 (Optional Content 1)** 字段中输入以下 HTML 和 Javascript 代码：

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 5000);

function changeBanner(){
var bannersArray = ["<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_0/
n21v1DrawerContainer.img.jpg/1400748629549.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_1/
n21v1DrawerContainer.img.jpg/1376556883237.jpg' width='100%' />"
];
var div = document.getElementById("image-ads");
if(div){
    currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
    div.innerHTML = bannersArray[currentIndex];
}
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
</style>
<div class="grey" id="image-ads">
<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/ content_parsys/overview/layout-
overview/gd12v2/gd12v2-left/n21v1_cq/ n21v1DrawerContainer.img.jpg/1379452035953.jpg' />
</div>
```

例如，要在访客门户上使用文本产品说明实施轮播广告，请在访问后横幅 (**Post-Access Banner**)（对于热门门户）或登录后横幅 (**Post Login Banner**) 窗口（对于需要提供凭证的访客门户）可选内容 **2 (Optional Content 2)** 字段中输入以下 HTML 和 Javascript 代码：

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 2000);

function changeBanner(){
var bannersArray = ["Optimize branch services on a single platform while delivering an optimal
application experience across branch and WAN infrastructure", "Transform your Network Edge to
deliver high-performance, highly secure, and reliable services to unite campus, data center,
and branch networks", "Differentiate your service portfolio and increase revenues by delivering
end-to-end scalable solutions and subscriber-aware services"];

var colorsArray = ["grey", "blue", "green"];
var div = document.getElementById("text-ads");
if(div){
    currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;

```

```

        div.innerHTML = bannersArray[currentIndex];
        div.className = colorsArray[currentIndex];
    }
}
</script>
<style>
.grey{
color: black;
background-color: lightgrey;
}
.blue{
color: black;
background-color: lightblue;
}
.green{
color: black;
background-color: lightgreen;
}
</style>
<div class="grey" id="text-ads">
Optimize branch services on a single platform while delivering an optimal application
experience across branch and WAN infrastructure
</div>

```

**注释** 当在 HTML 代码中插入外部 URL 时，您不需输入绝对（完整）URL 路径，包括“http”或“https”。

**步骤 6** 点击保存 (Save)。

## 根据访客位置自定义问候语

此示例显示如何根据访客类型中配置的位置，自定义访客在登录需要提供凭证的访客门户（不是热点）后所看到的登录成功的消息。

使用切换全屏 (**Toggle Full Screen**) 选项可在使用字段时缩放其大小。

**步骤 1** 导航到这些门户之一：

- 对于访客门户，选点击菜单图标 (☰)，然后选择 访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。
- 对于发起人门户，选择 访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。

**步骤 2** 在页面 (Pages) 中，点击身份验证成功 (Authentication Success)。

**步骤 3** 在页面自定义 (Page Customizations) 下，使用可选内容 1 (Optional Content 1) 字段随附的小型编辑器输入和查看 HTML 源代码。

**步骤 4** 点击切换 HTML 源 (Toggle HTML Source)。

**步骤 5** 输入您的源代码。

例如，要包含基于位置的问候语，在目录选项 1 (Optional Content 1) 中键入此代码：

```

<style>
    .custom-greeting {
        display: none;
    }

```

```

    }
    .guest-location-san-jose .custom-san-jose-greeting {
        display: block;
    }
    .guest-location-boston .custom-boston-greeting {
        display: block;
    }
}
</style>
<div class="custom-greeting custom-san-jose-greeting">
    Welcome to The Golden State!
</div>
<div class="custom-greeting custom-boston-greeting">
    Welcome to The Bay State!
</div>

```

访客将根据其特定位置，在登录成功后看到不同的问候语。

## 根据用户设备类型自定义问候语

可以根据客户端设备类型（移动设备或桌面设备）自定义在用户登录任何思科 ISE 最终用户 Web 门户（访客、发起人和设备）之后向其发送的问候语。

使用切换全屏 (**Toggle Full Screen**) 选项可在使用字段时缩放其大小。

**步骤 1** 导航至以下门户：

- 对于访客门户，选点击菜单图标 (☰)，然后选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。

**步骤 2** 在 **页面 (Pages)** 下，选择想要更新的页面。

**步骤 3** 在 **页面自定义 (Page Customizations)** 下，使用 **可选内容 1 (Optional Content 1)** 字段随附的小型编辑器输入和查看 HTML 源代码。

**步骤 4** 点击 **切换 HTML 源 (Toggle HTML Source)**。

**步骤 5** 输入您的源代码。

例如，要在 AUP 页面中包含基于设备类型的问候语，请在 AUP 页面中的 **可选内容 (Optional Content 1)** 文本框中输入以下代码：

```

<style>
    .custom-greeting {
        display: none;
    }
    .cisco-ise-desktop .custom-desktop-greeting {
        display: block;
    }
    .cisco-ise-mobile .custom-mobile-greeting {
        display: block;
    }
</style>

```

```
<div class="custom-greeting custom-mobile-greeting">
  Try our New Dark French Roast! Perfect on the Go!
</div>
<div class="custom-greeting custom-desktop-greeting">
  We brough back our Triple Chocolate Muffin!
  Grab a seat and dig in!
</div>
```

用户将在 AUP 页面上看到不同的问候语，视用户用于获取网络或门户访问权限的设备类型而定。

## 修改门户页面布局

可以操作页面的整体布局；例如，可以将边栏添加到 AUP 页面，以提供其他信息或信息链接。

**步骤 1** 将以下 CSS 代码添加到创建并计划应用于门户的自定义 *theme.css* 文件的底部。这会更改 AUP 页面布局。可选内容 **1 (Optional Content 1)** 字段在桌面和移动设备模式下显示为侧栏。

```
#page-aup .cisco-ise-optional-content-1 {
  margin-bottom: 5px;
}
@media all and ( min-width: 60em ) {
  #page-aup .cisco-ise-optional-content-1 {
    float: left;
    margin-right: 5px;
    width: 150px;
  }
  #page-aup .cisco-ise-main-content {
    float: left;
    width: 800px;
  }
  #page-aup .cisco-ise-main-content h1,
  #page-aup .cisco-ise-main-content p {
    margin-right: auto;
    margin-left: -200px;
  }
}
```

之后，可以在该门户的 AUP 窗口的可选内容 **1 (Optional Content 1)** 字段中使用 HTML 代码添加链接。

**步骤 2** 导航至以下门户：

- 对于访客门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。

**步骤 3** 在 **Pages** 下，选择要在其中包含边栏的页面。

**步骤 4** 在页面定制 (**Page Customizations**) 下，使用可选内容 **1 (Optional Content 1)** 字段随附的小型编辑器输入和查看源代码。

**步骤 5** 点击切换 **HTML 源 (Toggle HTML Source)**。

## 步骤 6 输入您的源代码。

例如，要为 AUP 窗口添加侧栏，请在 AUP 窗口上的可选内容 1 (Optional Content 1) 字段中输入此代码：

```
<ul data-role="listview">
  <li>Rent a Car</li>
  <li>Top 10 Hotels</li>
  <li>Free Massage</li>
  <li>Zumba Classes</li>
</ul>
```

图 13: AUP 页面示例的边栏视图（桌面设备上）

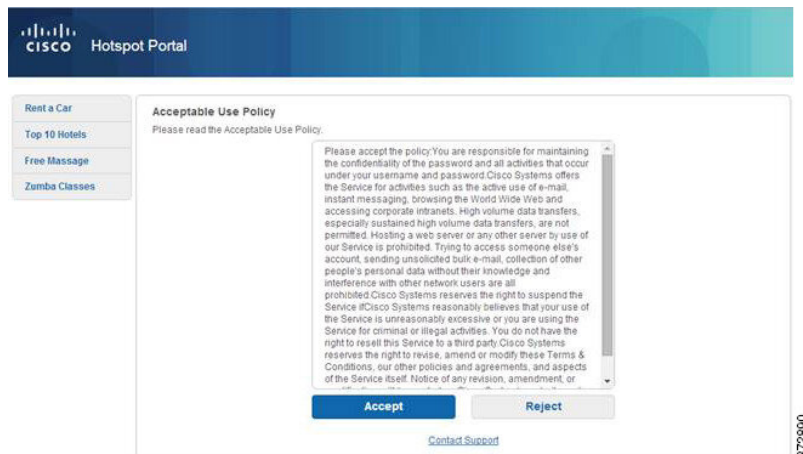
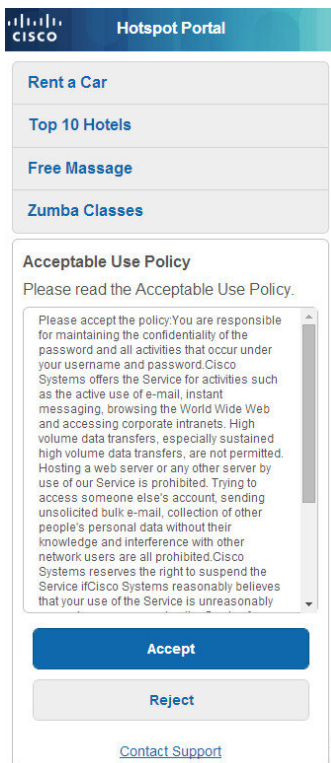


图 14: AUP 页面示例的边栏视图（移动设备上）



步骤 7 单击保存。

#### 下一步做什么

可以通过在可选内容 (Optional Content) 字段中输入不同的文本或 HTML 代码来定制其他页面。

## 导入自定义门户主题 CSS 文件

您可以上传已创建的任何自定义 *theme.css* 文件并将其应用于任何最终用户门户。这些更改将应用于您自定义的所有门户。

任何时候编辑自定义 *theme.css* 文件并将其导入回到思科 ISE 中时，请记住使用原先对其使用的同一主题名称。无法将两个不同的主题名称用于同一个 *theme.css* 文件。

步骤 1 导航至以下门户：

- 对于访客门户，选点击菜单图标 (☰)，然后选择 访客访问 (Guest Access) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。
- 对于发起人门户，选择 访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。
- 对于设备门户，选择 管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)。

步骤 2 从高级自定义 (Advanced Customization) 下拉列表中，选择导出/导入主题 (Export/Import Themes)。

步骤 3 在自定义主题 (Custom Theming) 对话框中，点击浏览 (Browse) 查找新的 *theme.css* 文件。

步骤 4 输入新文件的主题名称 (Theme Name)。

步骤 5 点击保存 (Save)。

#### 下一步做什么

您可以将此自定义门户主题应用于要自定义的门户。

1. 从门户主题 (Portal Themes) 下拉列表中选择已更新的主题来应用于整个门户。
2. 点击保存 (Save)。

## 删除自定义门户主题

可以删除已导入思科 ISE 中的任何自定义门户主题，除非某个门户正在使用该主题。不能删除思科 ISE 提供的任何默认主题。

## 开始之前

想要删除的门户主题不应被任何门户使用。

**步骤 1** 导航至以下门户：

- 对于访客门户，选点击菜单图标 (☰)，然后选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization)**。

**步骤 2** 从高级自定义 (**Advanced Customization**) 下拉列表选择 **删除主题 (Delete Themes)**。

**步骤 3** 从主题名称 (**Theme Name**) 下拉列表选择想要删除的门户主题。

**步骤 4** 点击删除 (**Delete**)，然后点击保存 (**Save**)。

## 查看您的自定义

您可以查看自己的自定义向门户用户（访客、发起人或员工）的显示方式。

**步骤 1** 点击 **Portal test URL** 查看您做出的更改。

**步骤 2** （可选）点击预览 (**Preview**) 以动态查看所做的更改如何出现在各类设备上：

- 移动设备：在预览 (**Preview**) 下查看做出的更改。
- 桌面设备：单击预览 (**Preview**) 并单击桌面预览 (**Desktop Preview**)。

如果没有显示更改，请点击 **Refresh Preview**。所显示的门户仅用于查看您做出的更改；您无法点击按钮或输入数据。

**注释** 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。如果有多个 PSN，思科 ISE 会选择第一个活动 PSN。

## 门户语言自定义

访客门户、发起人门户、我的设备门户和客户端调配门户会本地化为所有受支持的语言和区域设置。这包括文本、标签、消息、字段名称和按钮标签。如果客户端浏览器请求未映射到思科 ISE 中的模板的区域设置，则门户使用英语模板显示内容。

通过使用管理门户，您可以针对每种语言单独修改用于访客门户、发起人门户和我的设备门户的字段，并且可以添加更多语言。当前，您无法自定义客户端调配门户的这些字段。

默认情况下，每种类型的门户都支持 15 种语言。您可以在门户页面自定义 (**Portal Page Customization**) 窗口中选择门户使用的语言，还可以选择更新该语言的页面内容。请注意，如果更改页面上一种语言的字体和内容，则这些更改不会影响其他语言。导出语言文件时，会包含您在门户页面自定义 (**Portal Page Customization**) 窗口中所做的更改。

支持的语言为：

- 中文（简体）
- 中文（繁体）
- 捷克语
- 荷兰语
- 英语
- 法语
- 德语
- 匈牙利语
- 意大利语
- 日语
- 韩语
- 波兰语
- 葡萄牙语
- 俄语
- 西班牙语



---

注释 NAC 和 MAC 代理安装程序及 WebAgent 页面未本地化。

---

#### 编辑门户使用的语言

1. 打开要编辑的门户。
2. 在门户页面自定义 (**Portal Page Customization**) 选项卡上，从查看 (**view in**) 下拉列表中选择要编辑的语言。
3. 根据需要更改内容、标题和字体。
4. 保存该门户配置，并对要更新的其他语言重复此流程。



### 要编辑语言文件

每个门户页面自定义 (**Portal Page Customization**) 窗口还提供一个语言文件。语言文件是属性文件的 ZIP 文件，可用于自定义作为门户流程一部分的标题和文本，但不可用来在门户页面自定义 (**Portal Page Customization**) 窗口中自定义。

语言文件还包含到特定浏览器区域设置的映射，以及该语言下整个门户的所有字符串设置。如果您更改一种语言的浏览器区域设置，则更改会应用于所有其他最终用户 Web 门户。例如，如果在热点访客门户中将 French.properties 浏览器区域设置从 fr,fr-fr,fr-ca 更改为 fr,fr-fr，则更改还会应用于我的设备门户。

您可以导出压缩语言文件并对其进行更新，包括添加新语言或删除不需要的现有语言。

有关如何更新语言文件的说明，请参阅：

- [导出语言文件，第 305 页](#)
- [从语言文件添加或删除语言，第 305 页](#)
- [导入更新的语言文件，第 306 页](#)

## 导出语言文件

可以导出可供每个门户类型使用的语言文件，用以编辑和自定义其中指定的现有值，并添加或删除语言。



**注释** 语言属性文件中只有一些字典键支持在其值（文本）中使用 HTML。

**步骤 1** 导航至以下门户：

- 对于访客门户，选择 **访客访问 (Guest Access)** > **配置 (Configure)** > **编辑 (Edit)**。
- 对于发起人门户，选择 **访客访问 (Guest Access)** > **配置 (Configure)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)**。
- 对于设备门户，选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > (任何门户 [any Portals]) > **编辑 (Edit)**。

**步骤 2** 点击**语言文件 (Language File)**，然后从下拉列表中选择**导出 (Export)**。

**步骤 3** 在桌面上保存压缩后的语言文件。

## 从语言文件添加或删除语言

如果想用于门户类型的语言在该语言文件中不存在，则可以创建新的语言属性文件，并将其添加到压缩语言文件中。如果有不需要的语言，则可以删除其语言属性文件。

## 开始之前

要添加或删除语言属性文件，请导出适于各个门户类型的压缩语言文件。

**步骤 1** 使用任何显示 UTF-8 的编辑器（例如 Notepad ++），为想要添加或删除语言的门户类型打开预定义语言文件。

如果想要为多个门户类型添加或删除语言，请使用所有适当的门户属性文件。

**步骤 2** 要添加新的语言，请将现有语言属性文件另存为新语言属性文件，与压缩语言文件中的其他文件使用相同的命名规范。例如，要创建新的日语语言属性文件，请将该文件另存为 `Japanese.properties (LanguageName.properties)`。

**步骤 3** 在新语言属性文件的第一行指定浏览器本地值，将新语言与其浏览器区域设置关联起来。例如，`LocaleKeys=ja,ja-jp (LocaleKeys=browser locale value)` 应当是 `Japanese.properties` 文件的第一行。

**步骤 4** 更新新语言属性文件中的所有字典键值（文本）。

无法更改字典键。只能更新其值。

**注释** 仅部分字典键支持在键值（文本）中使用 HTML。

## 下一步做什么

1. 压缩所有属性文件（新文件和现有文件），创建新的压缩语言文件。不包含任何文件夹或目录。



**注释** 使用 Mac 时，解压 zip 文件将生成 DS 存储区。在编辑语言文件后进行压缩时，请勿在 zip 中包含 DS 存储区。要了解提取 DS 存储区的方法，请参阅 <https://superuser.com/questions/198569/compressing-folders-on-a-mac-without-the-ds-store>。

2. 为压缩语言文件创建新名称或使用其原始名称。

3. 将压缩语言文件导入您从其导出的特定门户。

## 导入更新的语言文件

可以导入通过添加或删除语言属性文件或通过更新现有属性文件中的文本进行自定义的已编辑语言文件。

**步骤 1** 导航至以下门户：

- 对于访客门户，选择 **访客访问 (Guest Access)** > **配置 (Configure)** > **访客门户 (Guest Portals)** > **编辑 (Edit)**。
- 对于发起人门户，选择 **访客访问 (Guest Access)** > **配置 (Configure)** > **发起人门户 (Sponsor Portals)** > **编辑 (Edit)**。
- 对于设备门户，选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > (任何门户 [any Portals]) > **编辑 (Edit)**。

**步骤 2** 点击 **Language File**，然后从下拉列表中选择 **Import**。

**步骤 3** 浏览以在桌面上查找新的压缩语言文件。

**步骤 4** 将语言文件重新导入从其导出文件的门户类型。

### 下一步做什么

要显示更改的文本或添加的新语言，请从 **View In** 下拉列表中选择特定语言。

## 自定义访客通知、审批和错误消息

在每个门户中，您可以自定义访客接收通知的方式，可以通过邮件、SMS 文本消息和打印方式。使用这些通知以邮件、文本发送登录凭证或打印登录凭证：

- 当访客使用自注册访客门户且成功进行自注册时。
- 当发起人创建访客帐户且要向访客提供详细信息时。当创建发起人组时，您可以确定是否授权发起人使用 SMS 通知。如果这些设施可用，则发起人总是可以使用邮件发送并打印通知。

您还可以自定义发送给发起人的邮件通知，用于发起人批准尝试获得访问网络权限的自助注册访客的请求。此外，您还可以自定义向访客和发起人显示的默认错误消息。

## 自定义邮件通知

可以自定义通过邮件发送给访客的信息。

### 开始之前

- 将 SMTP 服务器配置为启用邮件通知。选择 **管理 (Administration) > 系统 (System) > 设置 (Settings) > SMTP 服务器 (SMTP Server)**。
- 配置对向访客发送邮件通知的支持。选择 **访客访问 (Guest Access) > 设置 (Settings) > 访客邮件设置 (Guest Email Settings)**。选中对访客启用邮件通知 (**Enable email notifications to guests**)。
- 确保在**管理 (Administration) > 系统 (System) > 管理访问 (Admin Access) > 设置 (Settings) > 门户自定义 (Portal Customization)** 中默认启用启用 HTML 的门户自定义 (**Enable portal customization with HTML**)。

**步骤 1** 对于自行注册的发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 通知访客 (Notify Guests) > 邮件通知 (Email Notification)**。

**步骤 2** 可以更改在全局页面自定义 (**Global Page Customizations**) 下指定的徽标 (**Logo [Email]**) 默认值。

**步骤 3** 指定 **Subject** 和 **Email body**。使用预定义变量指定邮件中包含的访客帐户信息。使用小型编辑器和 HTML 标记自定义文本。

步骤 4 在设置 (Settings) 下，可以：

- 选择分别发送用户名和密码 (Send username and password separately)，使用不同的邮件单独发送用户名和密码。如果选择此选项，两个单独的选项卡会显示在页面自定义 (Page Customizations) 中，用于自定义用户名邮件 (Username Email) 和密码邮件 (Password Email) 通知。
- 选择发送测试邮件 (Send Test Email)，将测试邮件发送到邮箱地址，以在所有设备上预览自定义设置，从而确保信息正确显示。

步骤 5 点击保存 (Save)，然后点击关闭 (Close)。

---

## 自定义 SMS 文本消息通知

您可以自定义通过 SMS 文本消息发送给访客的信息。

开始之前

- 配置用于将邮件发送到 SMS 网关以传达 SMS 文本消息的 SMTP 服务器。选择 **管理 (Administration) > 系统 (System) > 设置 (Settings) > SMTP 服务器 (SMTP Server)**。
- 将发起人组配置为支持 SMS 文本通知。
- 设置具有第三方 SMS 网关的帐户。选择 **管理 (Administration) > 系统 (System) > 设置 (Settings) > SMS 网关 (SMS Gateway)**。思科 ISE 将文本消息作为邮件发送到网关，该网关通过 SMS 运营商将消息转发给指定用户。
- 确保在 **管理 (Administration) > 系统 (System) > 管理访问 (Admin Access) > 设置 (Settings) > 门户自定义 (Portal Customization)** 中默认启用启用 HTML 的门户自定义 (Enable portal customization with HTML)。

---

步骤 1 对于自行注册的访客门户或发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客或发起人门户 (Guest or Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > SMS 回执或 SMS 通知 (SMS Receipt or SMS Notification)**。

步骤 2 使用迷你编辑器和 HTML 标签自定义消息文本 (Message Text)。使用预定义变量指定要在 SMS 文本消息中包含的访客帐户信息。

步骤 3 在设置 (Settings) 下，可以：

- 选择分别发送用户名和密码 (Send username and password separately)，以使用不同文本消息单独发送用户名和密码。如果选择此选项，则在页面自定义 (Page Customizations) 中会出现两个单独的选项卡，用于自定义用户名消息 (Username Message) 和密码消息 (Password Message) 通知。
- 选择发送测试消息 (Send Test Message)，向手机发送文本消息，以预览自定义，确保信息按预期显示。支持的电话号码格式包括：+1 ### ## ## ## ##、###-###-####、(###) ### ## ## ##、#####、1##### 等。

步骤 4 点击保存 (Save)，然后点击关闭 (Close)。

---

## 自定义打印通知

您可以自定义为访客打印的信息。



注释 在每个门户中，打印通知徽标沿用自邮件通知徽标设置。

### 开始之前

确保在管理 (Administration) > 系统 (System) > 管理访问 (Admin Access) > 设置 (Settings) > 门户自定义 (Portal Customization) 中默认启用启用 HTML 的门户自定义 (Enable portal customization with HTML)。

- 步骤 1** 对于自行注册的访客门户和发起人门户，选择 访客访问 (Guest Access) > 配置 (Configure) > 访客或发起人门户 (Guest or Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 打印回执或打印通知 (Print Receipt or Print Notification)。
- 步骤 2** 指定打印说明文本 (Print Introduction Text)。使用预定义变量指定邮件中包含的访客帐户信息。使用小型编辑器和 HTML 标记自定义文本。
- 步骤 3** 在缩略图中预览自定义或点击打印预览 (Print Preview)。您无法在缩略图中查看任何 HTML 自定义。如果选择打印预览 (Print Preview) 选项，则会显示一个窗口，从中可以打印帐户详细信息来确保信息按预期显示。
- 步骤 4** 点击保存 (Save)，然后点击关闭 (Close)。

## 自定义审批请求邮件通知

您可以要求发起人需要批准自行注册的访客，才能创建访客帐户且访客才可以获取登录凭证。您可以自定义通过邮件发送至发起人，请求发起人批准的信息。只有在您已指定使用 Self-Registered Guest 门户的自行注册的访客必须经过批准才能获得网络访问权限的情况下，才会显示此通知。

### 开始之前

- 将 SMTP 服务器配置为启用邮件通知。选择 管理 (Administration) > 系统 (Systems) > 设置 (Settings) > SMTP 服务器 (SMTP Server)。
- 配置对向访客发送邮件通知的支持。选择 访客访问 (Guest Access) > 设置 (Settings) > 访客邮件设置 (Guest Email Settings)。选中对访客启用邮件通知 (Enable email notifications to guests)。
- 如果希望发起人批准自注册帐户请求，请在门户行为和流设置 (Portal Behavior and Flow Settings) 选项卡中的自注册页面设置 (Self-Registration Page Settings) 下选中需要批准自注册访客 (Require self-registered guests to be approved) 复选框。这会启用门户页面自定义 (Portal Page Customization) 页面中通知 (Notifications) 下方的请求批准电子邮件 (Approval Request Email) 选项卡，在这里可以自定义发送给发起人的电子邮件。

---

**步骤 1** 选择 **访客访问 (Guest Access) > 自注册访客门户 (Self-Registered Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 请求批准电子邮件 (Approval Request Email)**。在此，您可以：

**步骤 2** 执行以下操作：

- a) 在 **Global Page Customizations** 下更改在 **Logo** 中指定的默认标志。
- b) 指定 **Subject** 和 **Email body**。使用预定义变量指定邮件中包含的访客帐户信息。使用小型编辑器和 HTML 标记自定义文本。例如，要在请求批准电子邮件中包含指向发起人门户的链接，请点击 **创建链接 (Create a Link)** 按钮，然后将 FQDN 添加到发起人门户。
- c) 在所有设备上使用 **Send Test Email** 预览您的自定义，确保其显示符合预期。
- d) 点击 **Save**，然后点击 **Close**。

**步骤 3** 自定义发起人发送的批准电子邮件内容：

- a) 选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals)**。
- b) 点击 **门户页面自定义 (Portal Page Customization)**。
- c) 点击 **电子邮件通知 (Email Notification)** 选项卡并输入所需的详细信息。

---

## 编辑错误消息

可以完全自定义为访客、发起人和员工显示在“故障” (Failure) 页面中的错误消息。所有最终用户 Web 门户都具有“故障” (Failure) 页面，但黑名单门户除外。

---

**步骤 1** 执行以下操作之一：

- 对于访客门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 消息 (Messages) > 错误消息 (Error Messages)**。
- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 消息 (Messages) > 错误消息 (Error Messages)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 消息 (Messages) > 错误消息 (Error Messages)**。

**步骤 2** 从 **查看语言 (View In)** 下拉列表中选择在自定义消息时查看文本所要使用的语言。

下拉列表包含与特定门户关联的语言文件中的所有语言。确保将自定义门户页面时所做的任何更改更新到支持的语言属性文件中。

**步骤 3** 更新错误消息文本。可以通过键入 **aup** 等关键字来搜索特定错误消息，以便查找 AUP 相关的错误消息。

**步骤 4** 点击 **保存 (Save)**，然后点击 **关闭 (Close)**。

---

## 门户页面标题、内容和标签的字符限制

可以在 **Portal Page Customization** 选项卡的标题、文本框、说明、字段和按钮标签以及其他视觉元素中输入的最大和最小字符范围限制。

### 门户页面标题、内容和标签的字符限制

这些门户页面 UI 元素的导航路径如下：

- 对于访客门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 访客门户 (Guest Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 页面 (Pages)**。
- 对于发起人门户，选择 **访客访问 (Guest Access) > 配置 (Configure) > 发起人门户 (Sponsor Portals) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 页面 (Pages)**。
- 对于设备门户，选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > (任何门户 [any Portals]) > 编辑 (Edit) > 门户页面自定义 (Portal Page Customization) > 页面 (Pages)**。

在标题、文本框、说明、字段与按钮标签，以及您自定义的其他门户页面可视元素中输入内容时，请使用此信息。这些更新仅适用于您自定义的特定页面。



**注释** 无论您输入的是单字节还是多字节字符，您最多都只能输入字段指定的最大字符数。多字节字符不影响字符限制。

字段类别	字段	字段标签：最小字符数	字段标签：最大字符数	字段输入值：最小字符数	字段输入值：最大字符数
常见页面元素	横幅标题				256
	页脚元素			0	2000
	浏览器页面标题			0	256
	说明文本			0	2000
	内容标题			0	256
	可选内容 1			0	2000
	可选内容 2			0	2000
	按钮标签	0	64		

字段类别	字段	字段标签：最小字符数	字段标签：最大字符数	字段输入值：最小字符数	字段输入值：最大字符数
	复选框标签	0	64		
	选项卡标签	0	64		
	链接标签	0	256		
AUP	AUP 文本			0	50000
消息文本	消息文本（显示在页面上）			0	2000
	消息文本（显示在弹出窗口中）			0	256
字段标签	所有字段标签	0	256		
字段输入（常规）	一般字段输入（请参阅下面的特殊情况）			0	256
字段输入（特殊情况）	“访问代码” (Access Code) 字段			1	20
	“注册代码” (Registration Code) 字段			1	20
	“用户名” (Username) 字段			1	64
	“密码” (Password) 字段			1	256
	“电话号码” (Phone Number) 字段			0	64
	“设备 ID” (Device ID) 字段			12	17



# 门户自定义

您可以自定义最终用户 Web 门户的外观和访客体验。如果您熟悉级联样式表 (CSS) 语言和 Javascript，您可以使用 jQuery Mobile ThemeRoller 应用，通过更改门户页面布局来自定义门户主题。

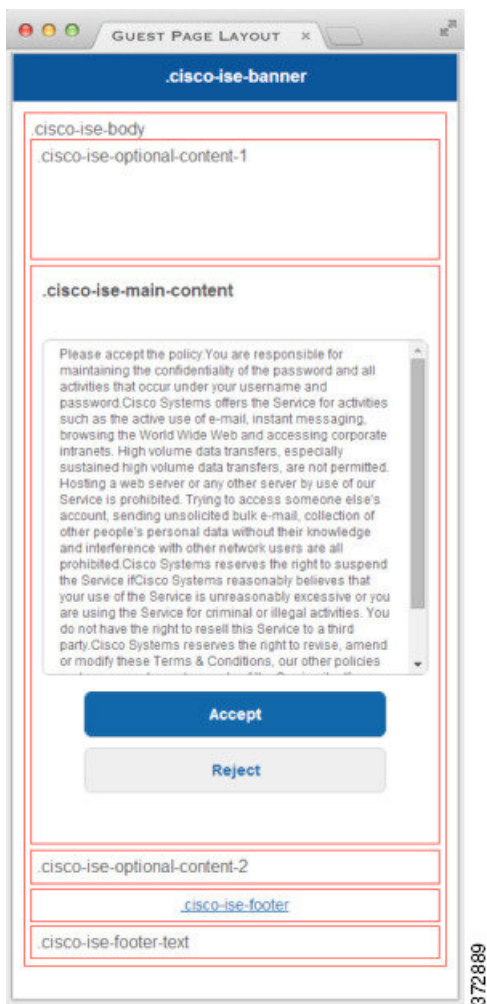
您可以通过从所需门户页面导出 CSS 主题或语言属性查看所有字段。有关详细信息，请参阅[导出门户的默认主题 CSS 文件](#)。

## 最终用户门户页面布局的 CSS 类和说明

使用这些 CSS 类可定义和修改思科 ISE 最终用户 Web 门户的页面布局。

CSS 类名	说明
cisco-ise-banner	包括徽标、横幅图像和横幅文本。  在发起人门户和我的设备门户上，此类还包含可激活上下文菜单的按钮。例如，菜单可能会显示具有 <b>Log Out</b> 和 <b>Change Password</b> 等选项的弹出窗口。
cisco-ise-body	包含不属于横幅的一部分的所有页面元素。
cisco-ise-optional-content-1	默认情况下为空。您可以添加文本、链接以及 HTML 和 JavaScript 代码。
cisco-ise-main-content	包含门户页面的主要内容，例如说明性文本、操作按钮和 cisco-ise-footer 容器。
cisco-ise-optional-content-2	默认情况下为空。您可以添加文本、链接以及 HTML 和 JavaScript 代码。
cisco-ise-footer	页脚的一部分，它是 <b>Contact Support</b> 和在线 <b>Help</b> 等链接的占位符。
cisco-ise-footer-text	默认情况下为空。它是要在门户页面底部显示的任何内容（例如版权声明或免责声明）的占位符。

图 15: 最终用户门户页面布局中使用的 CSS 类



## 门户语言文件的 HTML 支持

每个门户的压缩语言文件包含该门户的默认语言属性文件。每个属性文件包含用于定义门户上显示的内容的字典键。

您可以自定义门户上显示的文本，包括说明文本 (**Instructional Text**)、内容 (**Content**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 字段中的内容。其中一些字段具有默认内容，而有些字段则为空。

其中，只有与这些字段关联的一些字典键在其值（文本）中支持 HTML。

## 黑名单门户语言文件的 HTML 支持

该门户的说明文本 (**Instructional Text**)、内容 (**Content**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 文本框的导航路径为 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **黑名单门户 (Blacklist Portals)** > **编辑 (Edit)** > **门户页面自定义 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。



---

注释 以下是文件中字典键的不完整列表。

---

- key.blacklist.ui\_reject\_message

## 自带设备门户语言文件的 HTML 支持

此门户的说明文本 (**Instructional Text**)、内容 (**Content**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 文本框的访问路径为：**管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **BYOD 门户 (BYOD Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。



---

注释 以下是文件中字典键的不完整列表。

---

- key.guest.ui\_contact\_instruction\_message
- key.guest.ui\_byod\_welcome\_optional\_content\_1
- key.guest.ui\_byod\_welcome\_optional\_content\_2
- key.guest.ui\_byod\_reg\_limit\_message
- key.guest.ui\_byod\_reg\_content\_message
- key.guest.ui\_byod\_success\_manual\_reconnect\_message
- key.guest.ui\_byod\_install\_winmac\_instruction\_message
- key.guest.ui\_byod\_install\_optional\_content\_1
- key.guest.ui\_byod\_reg\_optional\_content\_2
- key.guest.ui\_byod\_install\_optional\_content\_2
- key.guest.ui\_byod\_reg\_optional\_content\_1

- key.guest.ui\_byod\_reg\_instruction\_message
- key.guest.ui\_byod\_welcome\_aup\_text
- key.guest.ui\_contact\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_byod\_install\_ios\_instruction\_message
- key.guest.ui\_byod\_welcome\_instruction\_message
- key.guest.ui\_error\_optional\_content\_2
- key.guest.ui\_error\_optional\_content\_1
- key.guest.ui\_byod\_welcome\_renew\_cert\_message
- key.guest.ui\_byod\_install\_android\_instruction\_message
- key.guest.ui\_byod\_install\_instruction\_message
- key.guest.ui\_byod\_welcome\_config\_device\_message
- key.guest.ui\_byod\_success\_message
- key.guest.ui\_byod\_success\_unsupported\_device\_message
- key.guest.ui\_byod\_success\_optional\_content\_1
- key.guest.ui\_byod\_success\_optional\_content\_2
- key.guest.ui\_error\_instruction\_message

## 客户端调配门户语言文件的 HTML 支持

此门户的说明 (**Instructional Text**)、内容 (**Content**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 文本框的导航路径为 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配门户 (Client Provisioning Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。



**注释** 以下是文件中字典键的不完整列表。

- key.guest.ui\_client\_provision\_agent\_installed\_instructions\_without\_java\_message
- key.guest.ui\_contact\_instruction\_message
- key.guest.ui\_success\_message

- key.guest.ui\_client\_provision\_unable\_to\_detect\_message
- key.guest.ui\_client\_provision\_instruction\_message
- key.guest.ui\_client\_provision\_agent\_installation\_message
- key.guest.ui\_client\_provision\_posture\_agent\_check\_message
- key.guest.ui\_vlan\_instruction\_message
- key.guest.ui\_client\_provision\_agent\_installation\_instructions\_with\_no\_java\_message
- key.guest.ui\_success\_instruction\_message
- key.guest.ui\_vlan\_optional\_content\_1
- key.guest.ui\_vlan\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_client\_provision\_posture\_check\_compliant\_message
- key.guest.ui\_client\_provision\_optional\_content\_2
- key.guest.ui\_client\_provision\_optional\_content\_1
- key.guest.ui\_error\_optional\_content\_2
- key.guest.ui\_error\_optional\_content\_1
- key.guest.ui\_client\_provision\_posture\_check\_non\_compliant\_message
- key.guest.ui\_vlan\_install\_message
- key.guest.ui\_success\_optional\_content\_1
- key.guest.ui\_success\_optional\_content\_2
- key.guest.ui\_client\_provision\_posture\_agent\_scan\_message

## 凭证访客门户语言文件的 HTML 支持

此门户的说明文本 (**Instructional Text**)、内容 (**Content**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 文本框的导航路径为 访客访问 (**Guest Access**) > 配置 (**Configure**) > 访客门户 (**Guest Portals**) > 编辑 (**Edit**) > 门户页面自定义 (**Portal Page Customization**) > 页面 (**Pages**)。您可以使用小型编辑器中的查看 HTML 源代码 (**View HTML Source**) 图标，并在内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。



---

注释 以下是文件中字典键的不完整列表。

---

- key.guest.ui\_contact\_instruction\_message
- key.guest.ui\_login\_optional\_content\_1
- key.guest.ui\_login\_optional\_content\_2
- key.guest.ui\_client\_provision\_unable\_to\_detect\_message
- key.guest.ui\_client\_provision\_instruction\_message
- key.guest.ui\_device\_reg\_optional\_content\_2
- key.guest.ui\_device\_reg\_optional\_content\_1
- key.guest.ui\_byod\_success\_manual\_reconnect\_message
- key.guest.ui\_byod\_reg\_optional\_content\_2
- key.guest.ui\_byod\_reg\_optional\_content\_1
- key.guest.ui\_client\_provision\_agent\_installation\_instructions\_with\_no\_java\_message
- key.guest.ui\_success\_instruction\_message
- key.guest.ui\_max\_devices\_instruction\_message
- key.guest.ui\_max\_devices\_optional\_content\_1
- key.guest.ui\_self\_reg\_results\_instruction\_message
- key.guest.notification\_credentials\_email\_body
- key.guest.ui\_max\_devices\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_byod\_install\_ios\_instruction\_message
- key.guest.ui\_changepwd\_instruction\_message
- key.guest.ui\_client\_provision\_posture\_check\_compliant\_message
- key.guest.ui\_aup\_instruction\_message
- key.guest.ui\_changepwd\_optional\_content\_2
- key.guest.ui\_changepwd\_optional\_content\_1
- key.guest.ui\_self\_reg\_results\_optional\_content\_2
- key.guest.ui\_self\_reg\_results\_optional\_content\_1

- key.guest.ui\_device\_reg\_instruction\_message
- key.guest.ui\_byod\_welcome\_renew\_cert\_message
- key.guest.ui\_vlan\_execute\_message
- key.guest.ui\_byod\_install\_android\_instruction\_message
- key.guest.ui\_client\_provision\_posture\_check\_non\_compliant\_message
- key.guest.ui\_byod\_install\_instruction\_message
- key.guest.ui\_device\_reg\_max\_reached\_message
- key.guest.ui\_byod\_success\_message
- key.guest.ui\_byod\_success\_unsupported\_device\_message
- key.guest.ui\_byod\_success\_optional\_content\_1
- key.guest.ui\_byod\_success\_optional\_content\_2
- key.guest.ui\_aup\_employee\_text
- key.guest.ui\_client\_provision\_agent\_installed\_instructions\_without\_java\_message
- key.guest.ui\_success\_message
- key.guest.ui\_byod\_welcome\_optional\_content\_1
- key.guest.ui\_byod\_welcome\_optional\_content\_2
- key.guest.ui\_self\_reg\_optional\_content\_2
- key.guest.ui\_self\_reg\_optional\_content\_1
- key.guest.ui\_byod\_reg\_limit\_message
- key.guest.notification\_credentials\_print\_body
- key.guest.ui\_byod\_reg\_content\_message
- key.guest.ui\_client\_provision\_agent\_installation\_message
- key.guest.ui\_post\_access\_message
- key.guest.ui\_vlan\_instruction\_message
- key.guest.ui\_byod\_install\_winmac\_instruction\_message
- key.guest.ui\_aup\_guest\_text
- key.guest.ui\_byod\_install\_optional\_content\_1
- key.guest.ui\_byod\_install\_optional\_content\_2
- key.guest.ui\_byod\_reg\_instruction\_message

- key.guest.ui\_aup\_optional\_content\_1
- key.guest.ui\_aup\_optional\_content\_2
- key.guest.ui\_self\_reg\_aup\_text
- key.guest.ui\_login\_instruction\_message
- key.guest.ui\_vlan\_optional\_content\_1
- key.guest.ui\_vlan\_optional\_content\_2
- key.guest.ui\_self\_reg\_results\_aup\_text
- key.guest.ui\_device\_reg\_register\_message
- key.guest.ui\_byod\_welcome\_instruction\_message
- key.guest.ui\_client\_provision\_optional\_content\_2
- key.guest.ui\_self\_reg\_instruction\_message
- key.guest.ui\_vlan\_install\_message
- key.guest.ui\_success\_optional\_content\_1
- key.guest.ui\_success\_optional\_content\_2
- key.guest.ui\_post\_access\_instruction\_message
- key.guest.ui\_post\_access\_optional\_content\_2
- key.guest.ui\_post\_access\_optional\_content\_1
- key.guest.ui\_byod\_welcome\_config\_device\_message
- key.guest.ui\_client\_provision\_posture\_agent\_scan\_message

## 热点访客门户语言文件的 HTML 支持

此门户的说明文本 (**Instructional Text**)、内容 (**Content**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 文本框的导航路径为 访客访问 (**Guest Access**) > 配置 (**Configure**) > 访客门户 (**Guest Portals**) > 编辑 (**Edit**) > 门户页面自定义 (**Portal Page Customization**) > 页面 (**Pages**)。您可以使用小型编辑器中的查看 HTML 源代码 (**View HTML Source**) 图标，并在内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。




---

注释 以下是文件中字典键的不完整列表。

---

- key.guest.ui\_contact\_instruction\_message



- key.guest.ui\_success\_message
- key.guest.ui\_post\_access\_message
- key.guest.ui\_vlan\_instruction\_message
- key.guest.ui\_success\_instruction\_message
- key.guest.ui\_aup\_optional\_content\_1
- key.guest.ui\_aup\_optional\_content\_2
- key.guest.ui\_vlan\_unsupported\_error\_message
- key.guest.ui\_vlan\_optional\_content\_1
- key.guest.ui\_vlan\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_aup\_instruction\_message
- key.guest.ui\_aup\_hotspot\_text
- key.guest.ui\_vlan\_execute\_message
- key.guest.ui\_vlan\_install\_message
- key.guest.ui\_success\_optional\_content\_1
- key.guest.ui\_success\_optional\_content\_2
- key.guest.ui\_post\_access\_instruction\_message
- key.guest.ui\_post\_access\_optional\_content\_2
- key.guest.ui\_post\_access\_optional\_content\_1

## 对移动设备管理门户语言文件的 HTML 支持

此门户的说明文本 (**Instructional Text**)、内容 (**Content**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 文本框的访问路径为：管理 (**Administration**) > 设备门户管理 (**Device Portal Management**) > MDM 门户 (**MDM Portals**) > 编辑 (**Edit**) > 门户页面定制 (**Portal Page Customization**) > 页面 (**Pages**)。您可以使用小型编辑器中的查看 HTML 源代码 (**View HTML Source**) 图标，并在内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。

- key.mdm.ui\_contact\_instruction\_message
- key.mdm.ui\_mdm\_enrollment\_after\_message
- key.mdm.ui\_error\_optional\_content\_2

- key.mdm.ui\_error\_optional\_content\_1
- key.mdm.ui\_mdm\_enroll\_optional\_content\_1
- key.mdm.ui\_mdm\_enroll\_optional\_content\_1
- key.mdm.ui\_mdm\_enroll\_optional\_content\_2
- key.mdm.ui\_mdm\_enroll\_instruction\_message
- key.mdm.ui\_error\_instruction\_message
- key.mdm.ui\_mdm\_enrollment\_link\_message
- key.mdm.ui\_mdm\_not\_reachable\_message
- key.mdm.ui\_contact\_optional\_content\_2
- key.mdm.ui\_mdm\_continue\_message
- key.mdm.ui\_contact\_optional\_content\_1

## 我的设备门户语言文件的 HTML 支持

此门户的说明文本 (**Instructional Text**)、内容 (**Content**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 文本框的访问路径为：**管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **我的设备门户 (My Devices Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。




---

**注释** 以下是文件中字典键的不完整列表。

---

- key.mydevices.ui\_add\_optional\_content\_1
- key.mydevices.ui\_add\_optional\_content\_2
- key.mydevices.ui\_post\_access\_instruction\_message
- key.mydevices.ui\_edit\_instruction\_message
- key.mydevices.ui\_contact\_optional\_content\_2
- key.mydevices.ui\_contact\_optional\_content\_1
- key.mydevices.ui\_changepwd\_optional\_content\_1
- key.mydevices.ui\_changepwd\_optional\_content\_2
- key.mydevices.ui\_post\_access\_message

- key.mydevices.ui\_home\_instruction\_message
- key.mydevices.ui\_edit\_optional\_content\_1
- key.mydevices.ui\_edit\_optional\_content\_2
- key.mydevices.ui\_add\_instruction\_message
- key.mydevices.ui\_post\_access\_optional\_content\_2
- key.mydevices.ui\_post\_access\_optional\_content\_1
- key.mydevices.ui\_error\_instruction\_message
- key.mydevices.ui\_actions\_instruction\_message
- key.mydevices.ui\_home\_optional\_content\_2
- key.mydevices.ui\_aup\_optional\_content\_1
- key.mydevices.ui\_aup\_optional\_content\_2
- key.mydevices.ui\_home\_optional\_content\_1
- key.mydevices.ui\_changepwd\_instruction\_message
- key.mydevices.ui\_contact\_instruction\_message
- key.mydevices.ui\_aup\_employee\_text
- key.mydevices.ui\_login\_optional\_content\_2
- key.mydevices.ui\_login\_optional\_content\_1
- key.mydevices.ui\_login\_instruction\_message
- key.mydevices.ui\_error\_optional\_content\_1
- key.mydevices.ui\_error\_optional\_content\_2
- key.mydevices.ui\_aup\_instruction\_message

## 发起人门户语言文件的 HTML 支持

此门户的说明文本 (**Instructional Text**)、内容 (**Content**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 文本框的导航路径为 访客访问 (**Guest Access**) > 配置 (**Configure**) > 发起人门户 (**Sponsor Portals**) > 编辑 (**Edit**) > 门户页面自定义 (**Portal Page Customization**) > 页面 (**Pages**)。您可以使用小型编辑器中的查看 HTML 源代码 (**View HTML Source**) 图标，并在内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。



---

注释 以下是文件中字典键的不完整列表。

---

- key.sponsor.ui\_aup\_instruction\_message
- key.sponsor.ui\_create\_random\_instruction\_message
- key.sponsor.ui\_home\_instruction\_message
- key.sponsor.ui\_post\_access\_instruction\_message
- key.sponsor.notification\_credentials\_print\_body
- key.sponsor.ui\_aup\_sponsor\_text
- key.sponsor.ui\_create\_accounts\_access\_info\_instruction\_message
- key.sponsor.ui\_login\_instruction\_message
- key.sponsor.notification\_credentials\_email\_body
- key.sponsor.ui\_create\_known\_instruction\_message
- key.sponsor.ui\_create\_import\_instruction\_message
- key.sponsor.ui\_suspend\_account\_instruction\_message
- key.sponsor.ui\_post\_access\_message
- key.sponsor.ui\_login\_optional\_content\_2
- key.sponsor.ui\_login\_optional\_content\_1
- key.sponsor.notification\_credentials\_email\_password\_body
- key.sponsor.ui\_contact\_optional\_content\_2
- key.sponsor.ui\_contact\_optional\_content\_1
- key.sponsor.ui\_login\_aup\_text
- key.sponsor.ui\_changepwd\_instruction\_message
- key.sponsor.ui\_create\_accounts\_guest\_type\_instruction\_message
- key.sponsor.ui\_changepwd\_optional\_content\_1
- key.sponsor.ui\_changepwd\_optional\_content\_2
- key.sponsor.notification\_credentials\_email\_username\_body
- key.sponsor.ui\_aup\_optional\_content\_1
- key.sponsor.ui\_aup\_optional\_content\_2
- key.sponsor.ui\_post\_access\_optional\_content\_1

- key.sponsor.ui\_post\_access\_optional\_content\_2
- key.sponsor.ui\_contact\_instruction\_message





## 第 9 章

# 资产可视性

- 使用外部身份库对思科 ISE 进行管理访问，第 328 页
- 外部身份源，第 332 页
- 思科 ISE 用户，第 339 页
- 内部和外部身份源，第 347 页
- 证书身份验证配置文件，第 349 页
- 将 Active Directory 用作外部身份源，第 349 页
- LDAP，第 370 页
- RADIUS 令牌身份源，第 382 页
- RSA 身份源，第 387 页
- 身份源序列，第 393 页
- 报告中的身份源详细信息，第 394 页
- 网络上已分析的终端，第 395 页
- 分析器条件设置，第 395 页
- 思科 ISE 分析服务，第 396 页
- 在思科 ISE 节点中配置分析服务，第 397 页
- 分析服务使用的网络探测功能，第 398 页
- 为每个思科 ISE 节点配置探测功能，第 407 页
- 设置 CoA、SNMP RO 社区和终端属性过滤器，第 408 页
- 针对 ISE 数据库持久性和性能的属性过滤器，第 411 页
- 从思科 IOS 传感器嵌入式交换机收集属性，第 413 页
- 分析器条件，第 415 页
- 分析网络扫描操作，第 416 页
- 创建分析器条件，第 422 页
- 终端分析策略规则，第 423 页
- 终端分析策略设置，第 423 页
- 创建终端分析策略，第 426 页
- 预定义终端分析策略，第 429 页
- 终端分析策略分组为逻辑配置文件，第 432 页
- 分析例外操作，第 433 页

- 使用策略和身份的静态分配创建终端，第 434 页
- 已识别的终端，第 438 页
- 创建终端身份组，第 440 页
- 分析器源服务，第 442 页
- 分析器报告，第 444 页
- 思科 ISE 与思科 NAC 设备集成，第 444 页
- 客户端设备上的代理下载问题，第 446 页
- 终端，第 446 页
- IF-MIB，第 453 页
- SNMPv2-MIB，第 453 页
- IP-MIB，第 454 页
- CISCO-CDP-MIB，第 454 页
- CISCO-VTP-MIB，第 455 页
- CISCO-STACK-MIB，第 456 页
- BRIDGE-MIB，第 456 页
- OLD-CISCO-INTERFACE-MIB，第 456 页
- CISCO-LWAPP-AP-MIB，第 456 页
- CISCO-LWAPP-DOT11-CLIENT-MIB，第 458 页
- CISCO-AUTH-FRAMEWORK-MIB，第 458 页
- IEEE8021-PAE-MIB: RFC IEEE 802.1X，第 459 页
- HOST-RESOURCES-MIB，第 459 页
- LLDP-MIB，第 459 页
- 终端的会话跟踪，第 460 页
- 终端的全局搜索，第 462 页

## 使用外部身份库对思科 ISE 进行管理访问

在思科 ISE 中，您可以通过外部身份库（例如，Active Directory、LDAP 或 RSA SecureID）对管理员进行身份验证。您可以使用两种模式，通过外部身份库提供身份验证：

- 外部身份验证和授权：没有在本地图 ISE 数据库中为管理员指定的凭证，授权仅基于外部身份库组成员身份。此模式用于 Active Directory 和 LDAP 身份验证。
- 外部身份验证和内部授权：管理员的身份验证凭证来自外部身份源，并使用本地思科 ISE 数据库分配授权和管理员职责。此模式用于 RSA SecurID 身份验证。此方法要求您同时在外地图身份库和本地图 ISE 数据库中配置相同的用户名。

在身份验证过程中，如果与外部身份库的通信尚未建立或失败，思科 ISE 将“后退”，并尝试从内部身份数据库执行身份验证。此外，无论已为其设置外部身份验证的管理员何时启动浏览器和发起登录会话，该管理员都可以从登录对话中的**身份存储区 (Identity Store)** 下拉列表中选择**内部 (Internal)**，请求通过思科 ISE 本地数据库进行身份验证。



属于超级管理员组且配置为使用外部身份存储区进行身份验证和授权的管理员也可以使用外部身份存储区进行身份验证，以访问命令行界面 (CLI)。



**注释** 您可以将此方法配置为仅通过 Admin 门户提供外部管理员身份验证。思科 ISE CLI 不具备这些功能。

如果网络没有一个或多个现有外部身份库，请确保已安装必要的外部身份库，并已将思科 ISE 配置为访问这些身份库。

## 外部身份验证和授权

默认情况下，思科 ISE 提供内部管理员身份验证。要设置外部身份验证，您必须为您在外部身份库中定义的外部管理员帐户创建密码策略。然后，您可以将此策略应用于最终成为外部管理员 RBAC 策略一部分的外部管理员组。

要配置外部身份验证，必须执行以下操作：

- 使用外部身份库，配置基于密码的身份验证。
- 创建外部管理员组。
- 为外部管理员组配置菜单访问和数据访问权限。
- 为外部管理员身份验证创建 RBAC 策略。

除了通过外部身份库提供身份验证之外，您的网络还可能要求您使用通用访问卡 (CAC) 身份验证设备。

### 使用外部身份库配置基于密码的身份验证

必须先为使用外部身份库（例如 Active Directory 或 LDAP）进行身份验证的管理员配置基于密码的身份验证。

#### 步骤 1

**步骤 2** 在身份验证方式 (Authentication Method) 选项卡上，选择基于密码 (Password Based)，然后选择您应已配置的外部身份源之一。例如，您已创建的 Active Directory 实例。

**步骤 3** 为使用外部身份库进行身份验证的管理员配置您所需的特定密码策略设置。

**步骤 4** 点击保存 (Save)。

### 创建外部管理员组

您需要创建一个外部 Active Directory 或 LDAP 管理员组。这可确保思科 ISE 使用外部 Active Directory 或 LDAP 身份存储区中定义的用户名验证您登录时输入的管理员用户名和密码。

思科 ISE 将从外部资源导出 Active Directory 或 LDAP 组信息并将其存储为字典属性。然后，在为此外部管理员身份验证方法配置 RBAC 策略时，您可以将该属性指定为策略元素之一。

**步骤 1** 依次选择管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 管理员 (Administrators) > 管理员组 (Admin Groups)

**步骤 2** 点击添加 (Add)。

**步骤 3** 输入名称和可选说明。

**步骤 4** 点击外部 (External)。

如果已连接并加入 Active Directory 域，则名称 (Name) 字段中会显示 Active Directory 实例名称。

**步骤 5** 从外部组 (External Groups) 下拉列表框中，选择要为此外部管理员组映射的 Active Directory 组。

点击“+”号以将更多 Active Directory 组映射至此外部管理员组。

**步骤 6** 点击保存 (Save)。

## 为外部管理员组配置菜单访问和数据访问权限

您必须配置可以分配给外部管理员组的菜单访问和数据访问权限。

**步骤 1** 选择 管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 权限 (Permissions)。

**步骤 2** 点击以下选项之一：

- **菜单访问 (Menu Access)**: 属于外部管理员组的所有管理员都可以获得菜单或子菜单级别的权限。菜单访问权限决定着管理员可以访问的菜单或子菜单。
- **数据访问 (Data Access)**: 属于外部管理员组的所有管理员都可以获得数据级别的权限。数据访问权限决定着管理员可以访问的数据。

**步骤 3** 为外部管理员组指定菜单访问或数据访问权限。

**步骤 4** 点击保存 (Save)。

## 创建用于外部管理员身份验证的 RBAC 策略

必须配置新的 RBAC 策略，以便使用外部身份存储区对管理员进行身份验证，并指定自定义菜单和数据访问权限。此策略必须拥有用于身份验证的外部管理员组以及思科 ISE 菜单和数据访问权限以管理外部身份验证和授权。



**注释** 您无法修改现有（系统预设）RBAC 策略以指定这些新外部属性。如果想要将某个现有策略用作模板，则必须复制该策略，为其重命名，然后分配新属性。

**步骤 1** 选择 **管理 (Administration) > 系统 (System) > 管理员访问 (Admin Access) > 授权 (Authorization) > 策略 (Policy)**。

**步骤 2** 指定规则名称、外部管理员组和权限。

请记住，必须向正确的管理员用户 ID 分配相应的外部管理员组。确保管理员与正确的外部管理员组关联。

**步骤 3** 点击 **Save**。

如果您以管理员身份登录，而且思科ISE RBAC 策略无法验证您的管理员身份，则思科ISE会显示“unauthenticated”消息，而且您无法访问 Admin 门户。

## 使用外部身份库配置管理员访问权限以使用内部授权进行身份验证

此方法要求您同时在外部身份库和本地思科 ISE 数据库中配置相同的用户名。当您配置思科 ISE 使用外部 RSA SecurID 身份库来提供管理员身份验证时，管理员凭证身份验证将由 RSA 身份库执行。但是，授权（策略应用）仍根据思科 ISE 内部数据库进行。此外，还要记住两个与外部身份和授权不同的重要因素：

- 您不需要为管理员指定任何特定的外部管理员组。
- 您必须同时在外部身份库和本地思科 ISE 数据库中配置相同的用户名。

**步骤 1**

**步骤 2** 确保外部 RSA 身份库中的管理员用户名也存在于思科 ISE 中。确保点击“密码” (Password) 下的 **外部 (External)** 选项。

**注释** 您不需要为此外部管理员用户 ID 指定密码，也不需要任何特殊配置的外部管理员组应用到关联的 RBAC 策略。

**步骤 3** 点击 **保存 (Save)**。

## 外部身份验证流程

当管理员登录时，登录会话会完成流程中的以下步骤：

1. 管理员发送 RSA SecurID 质询。
2. RSA SecurID 返回质询响应。
3. 管理员在思科 ISE 登录对话框中输入用户名和 RSA SecurID 质询响应，就像输入用户 ID 和密码。
4. 管理员确保指定的身份库为外部 RSA SecurID 资源。
5. 管理员点击 **Login**。

登录之后，管理员仅可查看在 RBAC 策略中指定的菜单和数据访问项目。

## 外部身份源

您可以通过这些窗口配置和管理包含思科 ISE 用于身份验证和授权的用户数据的外部身份源。

### LDAP 身份源设置

#### LDAP 常规设置

下表介绍常规 (**General**) 选项卡上的字段。

表 40: LDAP 常规设置

字段名称	使用指南
<b>Name</b>	输入 LDAP 实例的名称。此值在搜索中用于获取主题 DN 和属性。此值为字符串类型，最大长度为 64 个字符。
<b>Description</b>	输入对 LDAP 实例的说明。此值为字符串类型，最大长度为 1024 个字符。
<b>架构 (Schema)</b>	<p>您可以选择以下任一内置架构类型或创建自定义架构：</p> <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Sun 目录服务器 (Sun Directory Server)</li> <li>• Novell eDirectory</li> </ul> <p>您可以点击 Schema 旁边的箭头以查看架构详细信息。</p> <p>如果您编辑该预定义架构的属性，思科 ISE 会自动创建自定义架构。</p>
<b>注释</b>	仅在您选择定制架构时，可以编辑以下字段。
<b>Subject Objectclass</b>	输入在搜索中用于获取主题 DN 和属性的值。此值为字符串类型，最大长度为 256 个字符。
<b>主题名称属性 (Subject Name Attribute)</b>	输入包含请求中用户名的属性的名称。此值为字符串类型，最大长度为 256 个字符。
<b>证书属性 (Certificate Attribute)</b>	输入包含证书定义的属性。对于基于证书的身份验证，这些定义用于验证由客户端提供的证书。
<b>Group Objectclass</b>	输入在搜索中用于指定识别为组的对象的值。此值为字符串类型，最大长度为 256 个字符。

字段名称	使用指南
组映射属性 (Group Map Attribute)	指定包含映射信息的属性。根据选择的参考方向，此属性可以是用户或组属性。
主题对象包含对组的引用 (Subject Objects Contain Reference To Groups)	如果使用者对象包含指定这些对象所属组的属性，请点击此选项。
组对象包含对主题的引用 (Group Objects Contain Reference To Subjects)	如果组对象包含指定使用者的属性，请点击此选项。此值为默认值。
组对象作为...存储于成员属性中 (Subjects in Groups Are Stored in Member Attribute As)	(仅适用于启用组对象包含对使用者的引用 (Group Objects Contain Reference To Subjects) 选项时) 指定在组成员属性中如何搜索成员，其默认值为 DN。



注释 配置的主题名称属性应在外部 ID 存储区中编入索引。

### LDAP 连接设置

下表介绍连接设置 (Connection Settings) 选项卡中的字段。

表 41: LDAP 连接设置

字段名称	使用指南
启用辅助服务器	选中此选项以在主要 LDAP 服务器出现故障的时候启用辅助 LDAP 服务器作为备份。如果选中此复选框，则必须输入辅助 LDAP 服务器的配置参数。
主服务器和辅助服务器	
Hostname/IP	输入运行 LDAP 软件的设备的 IP 地址或 DNS 名称。此主机可以包含 1 至 256 个字符或以字符串表示的有效 IP 地址。对于主机名，仅字母数字字符 (a 至 z; A 至 Z; 0 至 9)、点 (.) 和连字符 (-) 为有效字符。
端口	输入 LDAP 服务器侦听的 TCP/IP 端口号。有效值为 1 至 65535。默认值为 389，如 LDAP 规范中所述。如果您不知道端口号，可以向 LDAP 服务器管理员查询此信息。

字段名称	使用指南
访问	<p><b>匿名访问 (Anonymous Access):</b> 点击此选项可确保在 LDAP 目录中进行匿名搜索。服务器不识别客户端身份并且会允许客户端读取配置为允许任何未经身份验证的客户端访问的任何数据。在缺少要向服务器发送的具体策略许可身份信息的情况下，客户端应该使用匿名连接。</p> <p><b>身份验证访问 (Authenticated Access):</b> 点击此选项可确保使用管理凭证在 LDAP 目录上进行搜索。如果选择此选项，请为“管理员 DN” (Admin DN) 字段和“密码” (Password) 字段输入信息。</p>
管理员 DN (Admin DN)	输入管理员的 DN。管理员 DN 是有权限搜索“用户目录子树” (User Directory Subtree) 下所有必要用户和有权限搜索组的 LDAP 帐户。如果指定的管理员没有权限在搜索中查看组名称属性，对于由该 LDAP 服务器进行身份验证的用户，组映射将失败。
密码	输入 LDAP 管理员帐户密码。
安全身份验证 (Secure Authentication)	点击此字段以对思科 ISE 和主 LDAP 服务器之间的通信进行加密。验证“端口” (Port) 字段是否包含用于 LDAP 服务器上的 SSL 的端口号。如果启用此选项，则必须选择一个根 CA。
“LDAP 服务器根 CA” (LDAP Server Root CA)	从下拉列表中选择受信任根证书颁发机构，以启用使用证书的安全身份验证。
服务器超时 (Server Timeout)	以秒为单位输入思科 ISE 在确定与主要 LDAP 服务器的连接或身份验证失败之前等待该服务器响应的的时间。有效值为 1 至 99。默认值为 10。
最大管理员连接数 (Max. Admin Connections)	输入利用 LDAP 管理员帐户权限对于特定 LDAP 配置可以运行的并发连接的最大数量（大于 0）。这些连接用于在“用户目录子树” (User Directory Subtree) 和“组目录子树” (Group Directory Subtree) 下搜索目录中的用户和组。有效值为 1 至 99。默认值为 20。
测试与服务器的绑定 (Test Bind to Server)	点击此选项以测试并确保可以成功绑定 LDAP 服务器详细信息和凭证。如果测试失败，请编辑您的 LDAP 服务器详细信息并重新测试。
<b>Failover</b>	
Always Access Primary Server First	如果您希望思科 ISE 在进行身份验证和授权时始终先访问主 LDAP 服务器，请选择该选项。
...后故障恢复到主服务器 (Failback to Primary Server after)	如果思科 ISE 尝试连接的主 LDAP 服务器无法访问，思科 ISE 会尝试连接辅助 LDAP 服务器。如果您希望思科 ISE 再次使用主 LDAP 服务器，请点击此选项并在文本框中输入值。

## LDAP 目录组织设置

下表介绍目录组织 (Directory Organization) 选项卡上的字段。

表 42: LDAP 目录组织设置

字段名称	使用指南
<b>主题搜索库 (Subject Search Base)</b>	<p>输入包含所有主题的子树的 DN。例如：</p> <p>o=corporation.com</p> <p>如果包含主题的树是基本 DN，请输入：</p> <p>o=corporation.com</p> <p>或</p> <p>dc=corporation,dc=com</p> <p>根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。</p>
<b>组搜索库 (Group Search Base)</b>	<p>输入包含所有组的子树的 DN。例如：</p> <p>ou=organizational unit, ou=next organizational unit, o=corporation.com</p> <p>如果包含组的树是基本 DN，请键入：</p> <p>o=corporation.com</p> <p>或</p> <p>dc=corporation,dc=com</p> <p>根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。</p>
<b>搜索该格式的 MAC 地址 (Search for MAC Address in Format)</b>	<p>输入一个 MAC 地址格式供思科 ISE 用于在 LDAP 数据库中进行搜索。在内部身份源中的 MAC 地址按照 xx-xx-xx-xx-xx-xx 格式进行搜索。LDAP 数据库中的 MAC 地址可以按照不同格式进行搜索。但是，当思科 ISE 收到主机查找请求时，思科 ISE 会将 MAC 地址从内部格式转换为此字段指定的格式。</p> <p>使用下拉列表以启用按照指定的格式搜索 MAC 地址，其中 <i>&lt;format&gt;</i> 可以是以下任何一种格式：</p> <ul style="list-style-type: none"> <li>• xxxx.xxxx.xxxx</li> <li>• xxxxxxxxxxxx</li> <li>• xx-xx-xx-xx-xx-xx</li> <li>• xx:xx:xx:xx:xx:xx</li> </ul> <p>您选择的格式必须与在 LDAP 服务器中搜索的 MAC 地址的格式一致。</p>

字段名称	使用指南
主题名称条开始直到最后一次出现分隔符 (Strip Start of Subject Name Up To the Last Occurrence of the Separator)	<p>输入适当的文本以删除用户名的域前缀。</p> <p>如果思科 ISE 在用户名中找到此字段中指定的分隔符，则会删除从用户名的开头一直到该分隔符的所有字符。如果用户名包含 &lt;start_string&gt; 框中指定的多个字符，思科 ISE 会删除从用户名的开头一直到该分隔符之前的最后一个匹配字符之间的所有字符。例如，如果分隔符为反斜线 (\)，用户名为 DOMAIN\user1，则思科 ISE 会向 LDAP 服务器提交 user1。</p> <p>注释 &lt;start_string&gt; 不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (&gt;) 和左尖括号 (&lt;)。思科 ISE 不允许在用户名中使用这些字符。</p>
从第一次出现分隔符时主题名称条结束 (Strip End of Subject Name from the First Occurrence of the Separator)	<p>输入适当的文本以删除用户名的域后缀。</p> <p>如果思科 ISE 在用户名中找到此字段中指定的分隔符，则会删除从该分隔符一直到用户名结尾的所有字符。如果用户名包含此字段中指定的多个字符，思科 ISE 会删除从该分隔符之后的第一个匹配字符开始的所有字符。例如，如果分隔符为 @，用户名为 user1@domain，则思科 ISE 会向 LDAP 服务器提交 user1。</p> <p>注释 &lt;end_string&gt; 框不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (&gt;) 和左尖括号 (&lt;)。思科 ISE 不允许在用户名中使用这些字符。</p>

## LDAP 组设置

表 43: LDAP 组设置

字段名称	使用指南
添加	<p>选择 <b>Add</b>; 添加组添加新组或从目录中选择 <b>Add</b>; 选择 Group 选择组从 LDAP 目录。</p> <p>如果您选择添加组，请输入新组的名称。如果您正在从目录中选择，请输入过滤器条件，然后点击<b>检索组 (Retrieve Groups)</b>。点击要选择的组旁边的复选框，然后点击<b>确定 (OK)</b>。选中的组将显示在<b>组 (Groups)</b> 窗口中。</p>



## LDAP 属性设置

表 44: LDAP 属性设置

字段名称	使用指南
添加	<p>选择 <b>Add</b>; 添加属性添加新属性或从目录中选择 <b>Add</b>; 选择属性从 LDAP 服务器的属性。</p> <p>如果选择添加属性，则为新属性输入名称。如果从目录中选择，请输入用户名，然后点击<b>检索属性 (Retrieve Attributes)</b>以检索属性。选中想要选择的属性旁边的复选框，然后点击“确定”。</p>

### 相关主题

[LDAP 目录服务](#)，第 370 页

[LDAP 用户身份验证](#)，第 371 页

[LDAP 用户查找](#)，第 374 页

[添加 LDAP 身份源](#)，第 374 页

## RADIUS 令牌身份源设置

### 相关主题

[RADIUS 令牌身份源](#)，第 382 页

[添加 RADIUS 令牌服务器](#)，第 386 页

## RSA SecurID 身份源设置

### RSA 提示设置

下表介绍 **RSA 提示 (RSA Prompts)** 选项卡上的字段。

表 45: RSA 提示设置

字段名称	使用指南
<b>Enter Passcode Prompt</b>	输入文本字符串以获取密码。
<b>Enter Next Token Code</b>	输入文本字符串以请求下一个令牌。
<b>Choose PIN Type</b>	输入文本字符串以请求 PIN 类型。
<b>Accept System PIN</b>	输入文本字符串以接受系统生成的 PIN。
<b>Enter Alphanumeric PIN</b>	输入文本字符串以请求字母数字 PIN。

字段名称	使用指南
<b>Enter Numeric PIN</b>	输入文本字符串以请求数字 PIN。
<b>Re-enter PIN</b>	输入文本字符串以请求用户重新输入 PIN。

### RSA 消息设置

下表介绍 **RSA 消息 (RSA Messages)** 选项卡上的字段。

表 46: RSA 消息设置

字段名称	使用指南
<b>Display System PIN Message</b>	输入文本字符串以编辑系统 PIN 消息。
<b>Display System PIN Reminder</b>	输入文本字符串以通知用户记住新 PIN。
<b>Must Enter Numeric Error</b>	输入一条消息，指导用户仅输入数字作为 PIN。
<b>Must Enter Alpha Error</b>	输入一条消息，指导用户仅输入字母数字字符作为 PIN。
<b>PIN Accepted Message</b>	输入在系统接受用户的 PIN 时用户所看到的消息。
<b>PIN Rejected Message</b>	输入在系统拒绝用户的 PIN 时用户所看到的消息。
<b>User Pins Differ Error</b>	输入在用户输入错误 PIN 时所看到的消息。
<b>System PIN Accepted Message</b>	输入在系统接受用户的 PIN 时用户所看到的消息。
<b>Bad Password Length Error</b>	输入用户指定的 PIN 不属于在 PIN 长度策略中指定的范围时用户所看到的消息。

### 相关主题

[RSA 身份源](#)，第 387 页

[思科 ISE 和 RSA SecurID 服务器集成](#)，第 388 页

[添加 RSA 身份源](#)，第 390 页

## 思科 ISE 用户

在本主题中，用户一词是指定期访问网络的员工和承包商，以及发起人用户和访客用户。发起人用户是通过发起人门户创建和管理访客用户账户的组织的员工或承包商。访客用户是在一段有限时间内需要访问组织的网络资源的外部访问者。

您必须为所有要获取对思科 ISE 网络上的资源和服务的访问权限的用户创建帐户。员工、承包商和发起人用户都应从管理门户创建。

从思科 ISE 版本 3.2 起，您可以选择将启用日期 (**Date Enabled**) 列（设置 (**Settings**) > 列 (**Columns**) > 启用日期 (**Date Enabled**)) 和密码过期前天数 (**Days Until Password Expires**) 列（设置 (**Settings**) > 列 (**Columns**) > 密码过期前天数 (**Days Until Password Expires**)) 添加到网络访问用户 (**Network Access Users**) 窗口中的网络访问用户 (**Network Access User**) 表（管理 (**Administration**) > 身份管理 (**Identity Management**) > 身份 (**Identities**) > 用户 (**Users**))，以便帮助您根据密码到期信息对网络访问用户进行排序。默认情况下并未添加启用日期 (**Date Enabled**) 和密码过期前天数 (**Days Until Password Expires**) 字段。您可以使用窗口中的自定义选项将它们添加到网络访问用户 (**Network Access User**) 表中。

## 用户身份

用户身份就像一个容纳关于用户的信息并形成其网络访问凭证的容器。每个用户的身份都由数据定义并且包括：用户名、邮件地址、密码、帐户说明、关联管理组、用户组和角色。

## 用户组

用户组是单个用户的集合，这些用户拥有一系列允许其访问特定思科 ISE 服务和功能的相同权限。

## 用户身份组

用户的组身份包含用于标识和说明属于同一个组的一组特定用户的元素。组名是此组的成员具有的功能角色的说明。组是属于此组的用户的列表。

### 默认用户身份组

思科 ISE 提供以下预定义用户身份组：

- **Employee** - 贵公司的员工属于此组。
- **SponsorAllAccount** - 可以暂停或恢复思科 ISE 网络中的所有访客帐户的发起人用户。
- **SponsorGroupAccounts** - 可以暂停由同一发起人用户组中的发起人用户创建的访客帐户的发起人用户。
- **SponsorOwnAccounts** - 只能暂停其已创建的访客帐户的发起人用户。
- **Guest** - 需要临时访问网络中的资源的访问者。

- ActivatedGuest - 其帐户已启用并处于活动状态的访客用户。

## 用户角色

用户角色是决定用户可以执行什么任务以及可以访问思科 ISE 网络上的什么服务的一系列权限。用户角色与用户组关联。例如，网络接入用户。

## 用户帐户自定义属性

思科 ISE 允许根据用户属性限制网络访问用户和管理员的网络访问。思科 ISE 具有一系列预定义的用户属性并且允许创建自定义属性。两种属性都可以用于定义身份验证策略的条件中。您还可以为用户帐户定义密码策略，以使密码符合指定的条件。

### 自定义用户属性

在用户自定义属性设置 (**User Custom Attributes Setting**) 窗口上，您可以使用自定义属性 (**Custom Attributes**) 窗格定义更多的用户帐户属性。思科 ISE 提供一系列不可配置的预定义属性。然而，通过配置下列内容，您可以定义自定义属性：

- 属性名称
- 数据类型

## 用户身份验证设置

并非所有外部身份存储区都允许网络访问用户更改其密码。有关详细信息，请参阅每个身份源对应的部分。

网络使用密码规则是在 **管理 > 身份管理 > 设置 > 用户身份验证设置** 中配置的。

以下部分提供有关 **密码策略** 选项卡上某些字段的更多信息。

- **必要字符 (Required Characters)**: 如果配置要求使用大写或小写字符的用户密码策略，而用户的语言不支持这些字符，则用户无法设置密码。要支持 UTF-8 字符，请取消选中以下复选框：
  - 小写字母字符
  - 大写字母字符
- **密码更改增量 (Password Change Delta)**: 指定在将当前密码更改为新密码时必须更改的最小字符数。思科 ISE 不会将字符位置更改视为更改。例如，如果密码增量为 3，当前密码为 “?Aa1234?”，则 “?Aa1567?”（“5”、“6”和“7”是三个新字符）是有效的新密码。“?Aa1562?”失败，因为“?”、“2”和“?”字符包含在当前密码中。“Aa1234??”失败，因为尽管字符位置已更改，但当前密码中的字符是相同的。

密码更改增量也会考虑以前的 X 个密码，其中 X 是密码必须与以前的版本不同 (**Password must be different from the previous versions**) 的值。如果密码增量为 3，密码历史记录为 2，则必须更改未包含在过去两个密码中的四个字符。

- 您可以使用密码生存期 (**Password Lifetime**) 部分更新密码重置间隔和提醒。要设置密码的有效期限，请选中每\_\_天更改密码（有效范围1到3650）复选框，并在输入字段中输入天数。如果用户未在指定时间内更改密码，则可以通过选择 **禁用用户账户** 选项来禁用用户账户。选择 **下次登录时需要更改密码**，以提示用户在下次登录思科 ISE 时更改其密码。

要发送密码重置提醒邮件，请选中在密码到期前 \_\_ 天显示提醒 (**Display reminder \_\_ days prior to password expiration**) 复选框，然后输入将提醒邮件发送到为网络访问用户配置的邮件地址的提前天数。在创建网络访问用户时，您可以在**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users) > 添加网络访问用户 (Add Network Access User)** 窗口中添加邮件地址，以发送密码重置邮件通知。



#### 注释

- 提醒邮件从以下邮件地址发送：iseadminportal@<ISE-Primary-FQDN>。您必须明确允许该发件人的访问权限。
- 默认情况下，提醒邮件包含以下内容：您的网络访问密码将在 <密码到期日期和时间> 到期。如需帮助，请联系您的系统管理员。  
从思科 ISE 版本 3.2 开始，您可以在邮件通知的 **请联系系统管理员寻求帮助** 部分之后自定义邮件内容。

- **锁定/暂停账户前的错误登录尝试数**：如果登录尝试失败次数超过所指定的值，使用此选项暂停或锁定账户。有效范围为 3 到 20。
- **账号禁用策略**：配置有关何时禁用现有用户账户的规则。

#### 相关主题

[用户帐户自定义属性](#)，第 340 页

[添加用户](#)，第 341 页

## 内部用户操作

### 添加用户

通过思科 ISE，您可以查看、创建、修改、复制、删除、导入、导出、搜索思科 ISE 用户的属性，或更改用户属性的状态。

如果您使用思科 ISE 内部数据库，则必须为需要访问思科 ISE 中资源或服务的任何新用户创建账户。

**步骤 1** 选择**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 用户 (Users)**。

**步骤 2** 点击 **Add (+)** 以创建新用户。

**步骤 3** 在所有字段中输入值。

**注释** 用户名中不要包含空格、+ 和 \* 字符。

步骤 4 点击 **Submit** 在思科 ISE 内部数据库中创建新用户。

## 导出思科 ISE 用户数据

您可以从思科 ISE 内部数据库中导出用户数据。思科 ISE 允许您以受密码保护的 CSV 文件格式导出用户数据。

步骤 1 选择管理 (**Administration**) > 身份管理 (**Identity Management**) > 身份 (**Identities**) > 用户 (**Users**)。

步骤 2 选中与要导出其数据的用户对应的复选框。

步骤 3 点击 **Export Selected**。

步骤 4 在密钥 (**Key**) 字段中，输入加密密码的密钥。

步骤 5 点击开始导出 (**Start Export**) 创建 users.csv 文件。

步骤 6 点击 **OK** 导出 users.csv 文件。

## 导入思科 ISE 内部用户

您可以使用 CSV 文件将新用户数据导入思科 ISE 以创建新的内部帐户。可在导入用户账号时下载模板 CSV 文件。

步骤 1 选择管理 (**Administration**) > 身份管理 (**Identity Management**) > 身份 (**Identities**) > 用户 (**Users**)。

步骤 2 点击导入 (**Import**)，从逗号隔开的文本文件导入用户。

如果没有逗号分隔的文本文件，请单击生成模版 (**Generate a Template**)，以创建已填充标题行的 CSV 文件。

步骤 3 在文件 (**File**) 字段中，输入包含要导入的用户名的文件名，或者点击浏览 (**Browse**)，导航至文件所在的位置。

步骤 4 要创建新的用户和更新现有用户详细信息，请选中以新数据创建新用户和更新现有用户 (**Create new user(s) and update existing user(s) with new data**) 复选框。

步骤 5 点击保存。

我们建议您不要一次性删除所有网络访问用户，因为这可能会导致 CPU 使用率达到峰值和服务崩溃，尤其是在使用一个非常大的数据库时。

## 终端设置

表 47: 终端设置

字段名称	使用指南
MAC 地址	输入十六进制格式的 MAC 地址以静态创建终端。 MAC 地址是连接到启用思科 ISE 的网络的接口设备标识符。

字段名称	使用指南
<b>Static Assignment</b>	<p>如果您想要在“终端”(Endpoints)窗口静态地创建终端并且已将静态分配的状态设置为静态,请选中此复选框。</p> <p>您可以将终端静态分配的状态从静态切换至动态或从动态切换至静态。</p>
<b>Policy Assignment</b>	<p>(除非选中<b>静态分配 (Static Assignment)</b>复选框,否则会默认禁用此字段)从<b>策略分配 (Policy Assignment)</b>下拉列表选择匹配的终端策略。</p> <p>您可以执行以下操作之一:</p> <ul style="list-style-type: none"> <li>如果您不选择匹配的终端策略,而是使用默认终端策略Unknown,则对于允许对终端进行动态分析的终端,其静态分配状态要设置为动态。</li> <li>如果您选择“未知”(Unknown)之外的匹配终端策略,则对该终端,静态分配状态应设置为静态并且系统会自动选中<b>静态分配 (Static Assignment)</b>复选框。</li> </ul>
<b>Static Group Assignment</b>	<p>当您想要向身份组静态分配终端时,请选中此复选框。</p> <p>如果您选中此复选框,下一次为之前动态分配至其他终端身份组的这些终端评估终端策略期间,分析服务不会更改终端身份组。</p> <p>如果您取消选中此复选框,则像ISE分析器根据策略配置所分配的一样,终端身份组处于动态状态。如果不选择Static Group Assignment选项,下一次评估终端策略期间,系统会自动将终端分配至匹配的身份组。</p>
<b>Identity Group Assignment</b>	<p>选择您要将终端分配至哪个终端身份组。</p> <p>当您静态创建终端,或在为某个终端评估终端策略期间不想使用<b>创建匹配身份组 (Create Matching Identity Group)</b>选项时,可将终端分配至身份组。</p> <p>思科ISE包括以下系统创建的终端身份组:</p> <ul style="list-style-type: none"> <li>黑名单</li> <li>GuestEndpoints</li> <li>Profiled <ul style="list-style-type: none"> <li>Cisco IP-Phone</li> <li>Workstation</li> </ul> </li> <li>RegisteredDevices</li> <li>Unknown</li> </ul>

#### 相关主题

[已识别的终端](#), 第 438 页

[使用策略和身份的静态分配创建终端](#), 第 434 页

## 从 LDAP 设置导入终端

表 48: 从 LDAP 设置导入终端

字段名称	使用指南
<b>连接设置</b>	
<b>主机</b>	输入 LDAP 服务器的主机名或 IP 地址。
<b>Port</b>	输入 LDAP 服务器的端口号。您可以使用默认端口 389 从 LDAP 服务器导入，并使用默认端口 636 通过 SSL 从 LDAP 服务器导入。  注释 思科 ISE 支持配置的任何端口号。配置值应与 LDAP 服务器连接的详细信息匹配。
<b>Enable Secure Connection</b>	选中启用安全连接 ( <b>Enable Secure Connection</b> ) 复选框，通过 SSL 从 LDAP 服务器导入。
<b>Root CA Certificate Name</b>	点击下拉箭头，查看受信任的 CA 证书。  根 CA 证书名称指连接 LDAP 服务器所需的受信任 CA 证书。您可以在思科 ISE 中添加（导入）、编辑、删除并导出受信任的 CA 证书。
<b>Anonymous Bind</b>	您必须选中匿名绑定 ( <b>Anonymous Bind</b> ) 复选框，或输入 slapd.conf 配置文件中的 LDAP 管理员凭证。
<b>Admin DN</b>	输入 slapd.conf 配置文件中为 LDAP 管理员配置的可分辨名称 (DN)。  管理员 DN 格式示例：cn=Admin、dc=cisco.com、dc=com
<b>密码 (Password)</b>	输入 slapd.conf 配置文件中为 LDAP 管理员配置的密码。
<b>Base DN</b>	输入父项的可分辨名称。  基本 DN 格式示例：dc=cisco.com、dc=com。
<b>查询设置</b>	
<b>MAC Address objectClass</b>	输入用于导入 MAC 地址的查询过滤器，例如，ieee802Device。
<b>MAC Address Attribute Name</b>	输入导入操作返回的属性名称，例如，macAddress。



字段名称	使用指南
<b>Profile Attribute Name</b>	<p>输入 LDAP 属性的名称。此属性为 LDAP 服务器中定义的每个终端条目保留策略名称。</p> <p>当配置分析属性名称 (<b>Profile Attribute Name</b>) 字段时，请考虑以下事项：</p> <ul style="list-style-type: none"> <li>• 如果未在分析属性名称 (<b>Profile Attribute Name</b>) 字段中指定此 LDAP 属性或错误地配置此属性，则执行导入操作期间系统会将终端标记为“未知” (Unknown)，并且会根据匹配的终端分析策略单独分析这些终端。</li> <li>• 如果您在分析属性名称 (<b>Profile Attribute Name</b>) 字段中配置此 LDAP 属性，系统会验证属性值，以确保终端策略与思科 ISE 中的现有策略相匹配，然后导入终端。如果终端策略与现有策略不匹配，则不会导入这些终端。</li> </ul>
<b>超时</b>	输入时间值（以秒为单位）。有效范围是从 1 到 60 秒。

**相关主题**

[已识别的终端](#)，第 438 页

[从 LDAP 服务器导入终端](#)，第 437 页

## 身份组操作

### 创建用户身份组

您必须创建用户身份组，才能为其分配用户。

**步骤 1** 选择管理 (**Administration**) > 身份管理 (**Identity Management**) > 组 (**Groups**) > 身份组 (**Identity Groups**) > 用户身份组 (**User Identity Groups**) > 添加 (**Add**)。

**步骤 2** 在“名称” (Name) 字段和“描述” (Description) 字段输入相应值。“名称” (Name) 字段支持的字符为空格 # \$ & ‘ ( ) \* + - . / @ \_。

**步骤 3** 点击提交。

**相关主题**

[用户身份组](#)，第 339 页

### 导出用户身份组

思科 ISE 允许您以 csv 文件格式导出本地配置的用户身份组。

**步骤 1** 选择管理 (**Administration**) > 身份管理 (**Identity Management**) > 组 (**Groups**) > 身份组 (**Identity Groups**) > 用户身份组 (**User Identity Groups**)。

**步骤 2** 选中想要导出的用户身份组对应的复选框，点击导出 (**Export**)。

步骤 3 点击确定。

## 导入用户身份组

思科 ISE 允许以 CSV 文件的形式导入用户身份组。

步骤 1 选择管理 (Administration) > 身份管理 (Identity Management) > 组 (Groups) > 身份组 (Identity Groups) > 用户身份组 (User Identity Groups)。

步骤 2 点击 **Generate a Template** 获取用于导入文件的模板。

步骤 3 点击 **Import** 以从逗号分隔的文本文件导入网络访问用户。

步骤 4 如果您想要同时添加新用户身份组并更新现有用户身份组，请选中 **Overwrite existing data with new data** 复选框。

步骤 5 点击 **Import**。

步骤 6 点击 **Save** 以将您的更改保存至思科 ISE 数据库。

## 终端身份组设置

表 49: 终端身份组设置

字段名称	使用指南
<b>Name</b>	输入您要创建的终端身份组的名称。
<b>Description</b>	输入对您要创建的终端身份组的说明。
<b>Parent Group</b>	<p>从父级组 (<b>Parent Group</b>) 下拉列表选择您要关联新创建的终端身份组的终端身份组。</p> <p>思科 ISE 包括以下终端身份组：</p> <ul style="list-style-type: none"> <li>• Blacklist</li> <li>• GuestEndpoints</li> <li>• Profiled</li> <li>• RegisteredDevices</li> <li>• Unknown</li> </ul> <p>此外，它还会再创建两个身份组：Cisco-IP-Phone 和 Workstation，这两个身份组与 Profiled（父）身份组关联。</p>

### 相关主题

[已识别终端划分为终端身份组](#)，第 440 页

[创建终端身份组](#)，第 440 页

## 内部和外部身份源

身份源是存储用户信息的数据库。思科 ISE 在身份验证期间使用身份源中的用户信息来验证用户凭证。用户信息包括组信息和与用户关联的其他属性。您可以添加、编辑以及从身份源删除用户信息。

思科 ISE 支持内部和外部身份源。您可以使用两个来源对发起人和访客用户进行身份验证。

### 内部身份源

思科 ISE 有一个内部用户数据库，用来存储用户信息。内部用户数据库中的用户称为内部用户。思科 ISE 还有一个内部终端数据库，存储关于所有设备以及与其相连的终端的信息。

### 外部身份源

思科 ISE 允许您配置包含用户信息的外部身份源。思科 ISE 连接外部身份源，获取身份验证所需的用户信息。外部身份源还包括思科 ISE 服务器的证书信息以及证书身份验证配置文件。思科 ISE 使用身份验证协议与外部身份源进行通信。

下表列出了身份验证协议以及它们支持的外部身份源。

表 50: 身份验证协议和支持的外部身份源

协议（身份验证类型）	内部数据库	Active Directory	LDAP	RADIUS 令牌服务器或 RSA	ODBC
EAP-GTC, PAP（纯文本密码）	是	是	是	是	是
MS-CHAP 密码散列： MSCHAPv1/v2 EAP/MSCHAP2 （作为 PEAP 或 EAP-FAST 的内部方法） LEAP	是	是	否	不兼容	是
EAP-MD5 CHAP	是	否	不兼容	不兼容	是

协议（身份验证类型）	内部数据库	Active Directory	LDAP	RADIUS 令牌服务器或 RSA	ODBC
EAP-TLS PEAP-TLS  （证书检索） 注释	不兼容   对于 TLS 身份验证（EAP-TLS 和 PEAP-TLS），身份源不是必需的，可选择性地添加到授权策略条件中。	是	是	否	不兼容

凭证的存储方式不同，具体取决于外部数据源连接类型和使用的功能。

- 当加入 Active Directory 域（但不用于被动 ID）时，不会保存用于加入的凭证。思科ISE会创建 AD计算机帐户（如果不存在），并使用该帐户对用户进行身份验证。
- 对于 LDAP 和被动 ID，用于连接到外部数据源的凭证也用于对用户进行身份验证。

## 创建外部身份源

思科ISE能够与外部身份源（例如 Active Directory、LDAP、RADIUS 令牌和 RSA SecurID 服务器）连接，以获取用于身份验证和授权的用户信息。外部身份源还包括执行基于证书的身份验证所需的证书身份验证配置文件。

**步骤 1** 选择 **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources)**。

**步骤 2** 选择以下选项之一：

- 选择**证书身份验证配置文件 (Certificate Authentication Profile)** 执行基于证书的身份验证。
- 选择 **Active Directory** 作为外部身份源连接到 Active Directory。有关更多详细信息，请参阅[将 Active Directory 用作外部身份源，第 349 页](#)。
- 选择 **LDAP** 以添加 LDAP 身份源。有关更多详细信息，请参阅[LDAP，第 370 页](#)。
- 选择 **RADIUS 令牌 (RADIUS Token)** 以添加 RADIUS 令牌服务器。有关更多详细信息，请参阅[RADIUS 令牌身份源，第 382 页](#)。
- 选择 **RSA SecurID** 以添加 RSA SecurID 服务器。有关更多详细信息，请参阅[RSA 身份源，第 387 页](#)。

# 证书身份验证配置文件

对于每个配置文件，必须指定应用作主体用户名的证书字段，以及是否希望对证书进行二进制比较。

## 添加证书身份验证配置文件

您必须创建证书验证配置文件，如果您想要使用可扩展身份验证协议 - 传输层安全 (EAP-TLS) 基于证书的身份验证方法，即必须创建证书身份验证配置文件。思科 ISE 不是通过传统的用户名与密码方法进行身份验证，而是将从客户端接收的证书与服务器中的证书进行比较，从而验证用户的身份。

### 开始之前

您必须是超级管理员或系统管理员。

#### 步骤 1

**步骤 2** 为证书身份验证配置文件输入名称和可选说明。

**步骤 3** 从下拉列表中选择身份库。

基本证书检查不需要使用身份源。如果希望对证书进行二进制比较，就必须选择身份源。如果您选择 Active Directory 作为身份源，使用者和通用名称以及使用者替代名称（所有值）都可用于查找用户。

**步骤 4** 从证书属性或证书中的任何主体或备选名称属性中选择身份的使用。此身份将用于日志以及查找。

如果选择证书中的任何主体或备选名称属性，则 Active Directory UPN 将用作日志的用户名，并将尝试使用证书中的所有主体名称和备选名称来查找用户。只有选择 Active Directory 作为身份源时，此选项才可用。

**步骤 5** 如果您想要将客户端证书与身份库中的证书进行匹配，请选择 **Match Client Certificate Against Certificate In Identity Store**。为此，您必须选择身份源（LDAP 或 Active Directory）。如果您选择 Active Directory，您可以选择仅为解决身份不明情况而匹配证书。

- **从不 (Never)**: 此选项从不执行二进制比较。
- **仅用于解决身份模糊 (Only to resolve identity ambiguity)**: 此选项仅在遇到身份不明情况时，才将客户端证书与 Active Directory 中帐户的证书进行二进制比较。例如，系统发现若干个 Active Directory 帐户与证书中的身份名称匹配，就属于身份不明情况。
- **始终执行二进制比较 (Always perform binary comparison)**: 此选项始终将客户端证书与身份库（Active Directory 或 LDAP）中帐户的证书进行二进制比较。

**步骤 6** 点击 **Submit** 以添加证书身份验证配置文件或保存更改。

## 将 Active Directory 用作外部身份源

思科 ISE 使用 Microsoft Active Directory 作为外部身份源以访问用户、设备、组和属性等资源。Active Directory 中的用户和设备身份验证仅允许对 Active Directory 中列出的用户和设备进行网络访问。

## 支持 Active Directory 的身份验证协议和功能

Active Directory 支持使用某些协议对用户和设备进行身份验证、更改 Active Directory 用户密码等功能。下表列出了 Active Directory 支持的身份验证协议及相应功能。

表 51: Active Directory 支持的身份验证协议

身份验证协议	功能
EAP-FAST 和基于密码的受保护的可扩展身份验证协议 (PEAP)	用户和设备身份验证, 能够使用 EAP-FAST 和 PEAP 结合 MS-CHAPv2 和 EAP-GTC 的内部方法更改密码
密码身份验证协议 (PAP)	用户和设备身份验证
Microsoft 质询握手身份验证协议版本 1 (MS-CHAPv1)	用户和设备身份验证
Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)	用户和设备身份验证
可扩展身份验证协议 - 通用令牌卡 (EAP-GTC)	用户和设备身份验证
可扩展身份验证协议 - 传输层安全 (EAP-TLS)	<ul style="list-style-type: none"> <li>• 用户和设备身份验证</li> <li>• 组和属性检索</li> <li>• 二进制证书比较</li> </ul>
可扩展身份验证协议 - 通过安全隧道的灵活身份验证-传输层安全 (EAP-FAST-TLS)	<ul style="list-style-type: none"> <li>• 用户和设备身份验证</li> <li>• 组和属性检索</li> <li>• 二进制证书比较</li> </ul>
受保护的可扩展身份验证协议 - 传输层安全 (PEAP-TLS)	<ul style="list-style-type: none"> <li>• 用户和设备身份验证</li> <li>• 组和属性检索</li> <li>• 二进制证书比较</li> </ul>
轻型可扩展身份验证协议 (LEAP)	用户身份验证

## 用于授权策略的 Active Directory 属性和组检索

思科 ISE 从 Active Directory 检索用户或设备属性和组以用于授权策略规则。这些属性可用于思科 ISE 策略并且决定了用户或设备的授权级别。思科 ISE 在身份验证成功后会检索用户和设备 Active Directory 属性，还可以为与身份验证无关的授权检索属性。

思科 ISE 可以使用外部身份存储区中的组来为用户或计算机分配权限；例如，将用户映射到发起人组。请注意 Active Directory 中的以下组成员身份限制：

- 策略规则条件可引用以下任意组：用户或计算机的主要组、用户或计算机作为直接成员的组，或者间接（嵌套）组。
- 不支持在用户或计算机的帐户域外的域本地组。

系统按加入点检索和管理属性和组。这些属性和组将用于授权策略（方法是首先选择加入点，然后选择属性）。您无法按范围为授权定义属性或组，但可以对身份验证策略使用范围。当您在身份验证策略中使用范围时，可以通过一个加入点对用户进行身份验证，但要通过另一个具有用户帐户域信任路径的加入点检索属性和/或组。您可以使用身份验证域来确保一个范围中的任两个加入点在身份验证域中都没有任何重叠。



**注释** 在多加入点配置的授权过程中，思科 ISE 会按照加入点在授权策略中列出的顺序搜索它们，直到找到特定用户才会停止。找到用户后，在加入点中分配给用户的属性和组将用于评估授权策略。



**注释** 请参阅 Microsoft 对可用 Active Directory 组的最大数量限制：[http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx)

如果规则包含带有特殊字符（例如 /、!、@、\、#、\$、%、^、&、\*、(、)、\_、+ 或 ~）的 Active Directory 组名称，则授权策略会失败。

如果管理员用户名包含 \$ 字符，则通过 Active Directory 进行的管理员用户登录可能会失败。

### 使用显式 UPN

要在将用户信息与 Active Directory 的用户主体名称 (UPN) 属性进行匹配时降低模糊性，您必须将 Active Directory 配置为使用显式 UPN。如果两个用户具有相同的 *sAMAccountName* 值，则使用显式 UPN 可能会产生模糊结果。

要在 Active Directory 中设置显式 UPN，请打开高级调整页面，并将属性 *REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN* 设置为 1。

## 基于证书的身份验证的 Active Directory 证书检索

思科 ISE 支持为使用 EAP-TLS 协议的用户和设备身份验证检索证书。Active Directory 上的用户或设备记录包括二进制数据类型的证书属性。此证书属性可以包含一个或多个证书。思科 ISE 将此属性

标识为 `userCertificate`，并且不允许为此属性配置任何其他名称。思科 ISE 会检索此证书并将其用于执行二进制比较。

证书身份验证配置文件决定从哪个字段（例如 Subject Alternative Name (SAN) 或 Common Name 字段）获取用户名以在 Active Directory 中查找用于检索证书的用户。思科 ISE 检索到证书后，会将此证书与客户端证书进行二进制比较。当接收到多个证书时，思科 ISE 会对这些证书进行比较以确定相匹配的证书。找到匹配的证书后，则用户或设备身份验证通过。

## Active Directory 用户身份验证流程

当对用户进行身份验证或查询时，思科 ISE 会检查以下内容：

- MS-CHAP 和 PAP 身份验证会检查用户是否被禁用、锁定、过期或者登录超时，如果上述任一条件为真，则身份验证失败。
- EAP-TLS 身份验证会检查用户是否被禁用或锁定，如果满足上述任一条件，则身份验证失败。

## 支持 Active Directory 多域林

思科 ISE 支持带多域林的 Active Directory。在每个林中，思科 ISE 连接到单个域，但如果在思科 ISE 连接到的域与其他域之间建立信任关系，则可从 Active Directory 林中的其他域访问资源。

请参阅思科身份服务引擎的版本说明，以获取支持 Active Directory 服务的 Windows 服务器操作系统列表。



---

**注释** 思科 ISE 不支持位于网络地址转换器背后并具有网络地址转换 (NAT) 地址的 Microsoft Active Directory 服务器。

---

## 将 Active Directory 与思科集成的前提条件

本节介绍配置 Active Directory 以与思科集成所需的手动步骤。但是，在大多数情况下，可以启用思科来自动配置 Active Directory。以下是将 Active Directory 与思科集成的前提条件。

- 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。
- 确保您在思科 ISE 中具有超级管理员或系统管理员权限。
- 使用网络时间协议 (NTP) 服务器设置来同步思科服务器和 Active Directory 之间的时间。您可以从思科 CLI 配置 NTP 设置。
- 思科 ISE 能够连接没有双向信任或者具有零信任的多个 Active Directory 域。如果要从特定加入点查询其他域，请确保加入点和其他具有需要访问的用户和计算机信息的域之间存在信任关系。如果信任关系不存在，您必须为不受信任的域创建另一个加入点。有关建立信任关系的详细信息，请参阅 Microsoft Active Directory 文档。
- 您必须在思科加入到的域中具有至少一个可由思科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 机器账户
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 机器账户是否存在）</li> <li>• 将思科 机器账户创建到域（如果机器账户尚不存在）</li> <li>• 在新机器账户上设置属性（例如，思科 机器账户密码、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 机器账户是否存在）</li> <li>• 从域中删除思科 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 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 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 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 中。仅存储新创建的思科 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。



**注释** 由于 Windows Server 2016 Active Directory 或更高版本以及 Windows 10 版本 1607 中的限制，会出现此问题。要克服此限制，当您将 Windows Server 2016 Active Directory 或更高版本或 Windows 10 版本 1607 与思科 ISE 集成时，您需要将以下注册表中的注册表值从非零设置为空，以提供对所有项的访问权限：Registry:HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\restrictremotesam 这允许思科 ISE 更新其计算机账户密码。

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	已通过身份验证	备注
DNS (TCP/UDP)	随机数大于或等于 49152	DNS 服务器/AD 域控制器	否	-
MSRPC	445	域控制器	是	—
Kerberos (TCP/UDP)	88	域控制器	是 (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	域控制器	是	—
LDAP (GC)	3268	全局目录服务器	是	—
NTP	123	NTP 服务器/域控制器	否	-
IPC	80	部署中的其他 ISE 节点	是（使用 RBAC 凭证）	-

## 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。

## 将 Active Directory 配置为外部身份源

在您将 Active Directory 配置为外部身份源之前，请确保：

- 思科 ISE 主机名长度为 15 个字符及以下。Active Directory 不允许主机名长度超过 15 个字符。
- 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。
- 您拥有 ISE 的超级管理员或系统管理员权限。



**注释** 如果您在思科 ISE 连接到 Active Directory 时发现操作问题，请查看操作 > 报告下的“AD 连接器操作报告”。

您必须执行以下任务，从而将 Active Directory 配置配为外部身份源。

1. [添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点](#)，第 355 页
2. [配置身份验证域](#)，第 359 页
3. [配置 Active Directory 用户组](#)，第 359 页
4. [配置 Active Directory 用户和计算机属性](#)，第 360 页
5. (选件) [修改密码更改、设备身份验证和设备访问限制设置](#)，第 361 页

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

### 开始之前

确保思科 ISE 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。您可以通过运行域诊断工具来检查这些参数。

必须创建加入点才能使用 Active Directory 以及使用被动 ID 工作中心的代理、系统日志、SPAN 和终端探测器。

**步骤 1** 选择管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > Active Directory。

**步骤 2** 点击添加 (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。

**步骤 3** 点击提交 (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，请点击是 (Yes)。

如果已点击否 (No)，则保存配置将会全局保存 Active Directory 域配置（在主策略服务节点和辅助策略服务节点中），但不会将任何 ISE 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点击编辑 (Edit)，或者从左侧的导航窗格中点击新的 Active Directory 加入点。系统将显示部署加入/退出表，其中包含所有思科 ISE 节点、节点角色及其状态。

**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 节点旁边的复选框，然后点击加入 (Join) 将思科 ISE 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 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 节点，则应对每个思科 ISE 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。

强烈建议您选择**存储凭证**，在此情况下将会保存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 `jd@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 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 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 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** 点击**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。点击每个节点的失败消息可查看该节点的详细日志。

---

在配置加入点时，请注意以下几点：

- 加入完成后，思科 ISE 将更新其 AD 组和对应的安全标识符 (SID)。思科 ISE 自动启动 SID 更新过程。您必须确保允许此过程完成。
- 如果缺少 DNS 服务 (SRV) 记录，您可能无法将思科 ISE 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）。
- 建议您在指定的维护窗口后重新加入 AD。这可确保使用最新更新刷新 AD 缓存。

## 添加域控制器

---

**步骤 1** 依次选择工作中心 (**Work Centers**) > **PassiveID** > **提供程序 (Providers)**，然后从左侧面板中选择 **Active Directory**。

**步骤 2** 选中所创建的 Active Directory 加入点旁边的复选框，然后点击**编辑 (Edit)**。系统将显示部署加入/退出表，其中包含所有思科节点、节点角色及其状态。

**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，然后点击**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，然后点击**确定 (OK)**。域控制器显示在 **PassiveID** 选项卡的“域控制器” (Domain Controllers) 列表中。

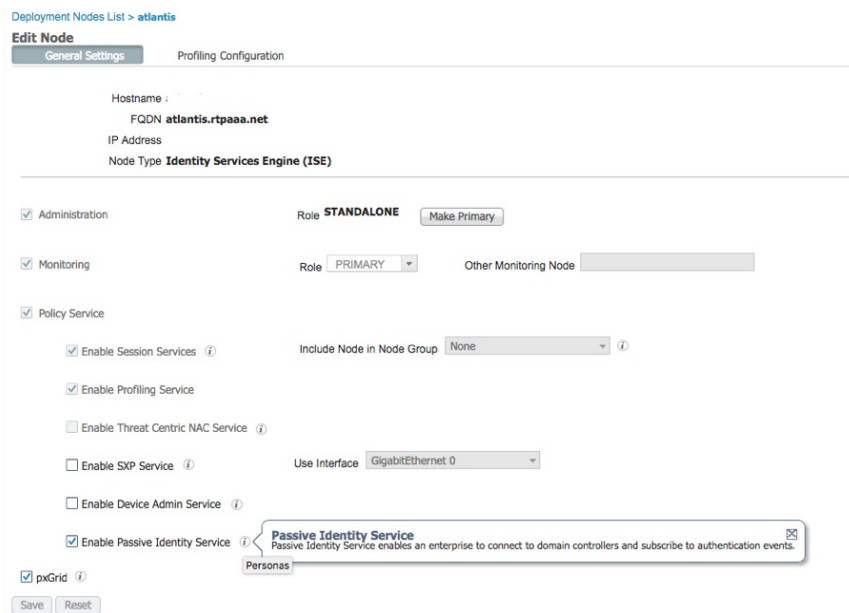
**步骤 5** 配置域控制器:

- a) 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。
- b) 或者，编辑不同的域控制器字段。
- c) 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。

**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。

图 16:

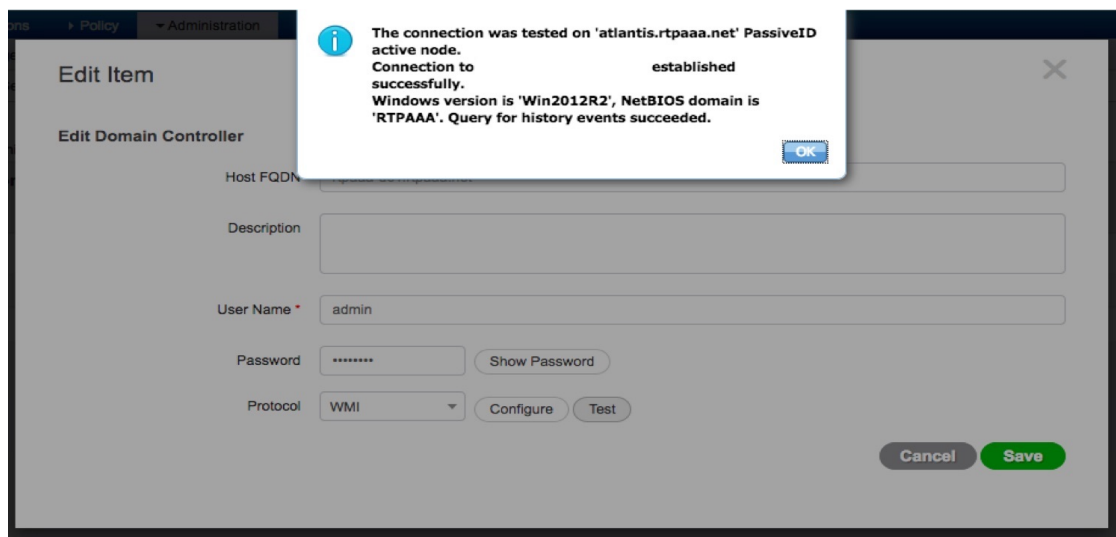


**步骤 1** 选择**管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > Active Directory**。

**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，其中包含所有思科节点、节点角色及其状态。

**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)** 以使能够自动配置所选的域控制器。

图 17:



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 与思科集成的前提条件](#)，第 352 页。

图 18:

## 退出 Active Directory 域

如果不再需要从此 Active Directory 域或从此加入点对用户或机器进行身份验证，则可以退出 Active Directory 域。

从命令行界面重置思科 ISE 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 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 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 主机名时，也建议您如此操作。

### 开始之前

如果您退出 Active Directory 域，但是仍然使用 Active Directory 作为身份验证的身份源（直接使用或作为身份源序列的一部分），则身份验证会失败。

**步骤 1** 选择管理 > 身份管理 > 外部身份源 > **Active Directory**。

**步骤 2** 选中所创建的 Active Directory 加入点旁边的复选框，然后点击**编辑 (Edit)**。系统将显示部署加入/退出表，其中包含所有思科 ISE 节点、节点角色及其状态。

**步骤 3** 选中思科 ISE 节点旁边的复选框，然后点击**退出 (Leave)**。

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

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

**注释** 要从 Active Directory 数据库中删除思科 ISE 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，然后点击**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 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。

---

## 配置身份验证域

对于与其有信任关系的其他域，思科 ISE 加入的域具有可视性。默认情况下，思科 ISE 设置为允许依据所有可信任域进行身份验证。可以将与 Active Directory 部署的交互限制到身份验证域子集。通过配置身份验证域，可以为每个加入点选择特定域，以便仅对选择的域执行身份验证。身份验证域可以提高安全性，因为这些域指示思科 ISE 仅对来自所选域（而不是来自加入点信任的所有域）的用户进行身份验证。身份验证域还可改善性能以及身份验证请求处理延迟，因为身份验证域限制搜索区域（即，将搜索帐户与传入用户名或身份匹配的范围）。这在传入用户名或身份不包含域标记（前缀或后缀）时尤为重要。由于上述原因，配置身份验证域是最佳实践，我们强烈推荐此最佳实践。

---

**步骤 1** 选择**管理 > 身份管理 > 外部身份源 > Active Directory**。

**步骤 2** 点击 **Active Directory** 加入点。

**步骤 3** 点击**身份验证域 (Authentication Domains)** 选项卡。

系统会显示一个表，其中包含受信任域列表。默认情况下，思科 ISE 允许对所有受信任域执行身份验证。

**步骤 4** 要仅允许指定域，请取消选中 **Use all Active Directory domains for authentication** 复选框。

**步骤 5** 选中想要允许对其执行身份验证的域旁边的复选框，并点击**启用已选择 (Enable Selected)**。在**身份验证 (Authenticate)** 列中，此域的状态会更改为“是” (Yes)。

还可以禁用选定的域。

**步骤 6** 点击**显示无法使用的域 (Show Unusable Domains)** 以查看无法使用的域的列表。无法使用的域是思科 ISE 由于单向信任、选择性身份验证等原因而无法用于身份验证的域。

---

下一步做什么

配置 Active Directory 用户组。

## 配置 Active Directory 用户组

您必须配置 Active Directory 用户组，使其可以用于授权策略中。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** 选择管理 > 身份管理 > 外部身份源 > Active Directory。

**步骤 2** 点击组 (Groups) 选项卡。

**步骤 3** 执行以下操作之一：

a) 选择添加 (Add) > 从目录中选择组 (Select Groups From Directory) 以选择现有组。

b) 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，然后点击检索组 (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，然后点击确定 (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** 点击确定 (OK)。

**步骤 8** 点击保存 (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，则必须点击更新 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。

### 下一步做什么

配置 Active Directory 用户属性。

## 配置 Active Directory 用户和计算机属性

必须配置 Active Directory 用户和计算机属性，以便在授权策略的条件中使用这些属性。

**步骤 1** 选择管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > Active Directory。

**步骤 2** 点击属性 (Attributes) 选项卡。

**步骤 3** 依次选择添加 (Add) > 添加属性 (Add Attribute) 以手动添加属性，或者依次选择添加 (Add) > 从目录中选择属性 (Select Attributes From Directory) 以从目录中选择属性列表。

**步骤 4** 如果选择从目录添加属性，请在示例用户或机器账户 (Sample User or Machine Account) 字段中输入用户的名称，然后点击检索属性 (Retrieve Attributes) 以获取用户属性的列表。例如，输入 administrator 以获取管理员属性列表。您还可以输入星号 (\*) 通配符过滤结果。

**注释** 当输入示例用户名时，确保从思科 ISE 连接到的 Active Directory 域选择用户。当您选择示例计算机获得计算机属性时，请务必在计算机名称前面加上 “host/” 或使用 SAM\$ 格式。例如，可以使用 host/myhost。检索属性时显示的示例值仅用于说明，不能存储。

**步骤 5** 选中想要选择的 Active Directory 的属性旁边的复选框，并且点击确定 (OK)。

**步骤 6** 如果选择手动添加属性，请输入新属性的名称。



步骤 7 点击保存 (Save)。

---

## 修改密码更改、设备身份验证和设备访问限制设置

### 开始之前

您必须将思科 ISE 加入到 Active Directory 域。有关详细信息，请参阅[添加 Active Directory 加入点并将思科 ISE 节点加入到该加入点](#)，第 355 页。

步骤 1 选择管理 > 身份管理 > 外部身份源 > **Active Directory**。

步骤 2 选中相关思科 ISE 节点旁边的复选框，然后点击编辑 (Edit)。

步骤 3 点击高级设置 (Advanced Settings) 选项卡。

步骤 4 根据需要，修改 Password Change、Machine Authentication 和 Machine Access Restrictions (MAR) 设置。

步骤 5 如果您想要使用 Kerberos 进行纯文本身身份验证，请选中 **Use Kerberos for Plain Text Authentications** 复选框。默认和推荐选项为 MS-RPC。

---

## 对 Active Directory 多加入配置的支持

思科 ISE 支持对 Active Directory 域执行多加入。思科 ISE 最多支持 50 个 Active Directory 加入。思科 ISE 能够连接没有双向信任或者具有零信任的多个 Active Directory 域。Active Directory 多域加入包括一组不同的 Active Directory 域，每个加入均有其自己的组、属性和授权策略。

您可以多次联接同一个域林，也即是说，如有必要，您可以在同一个域林中联接不止一个域。

思科 ISE 现在允许联接具有单向信任的域。此选项有助于绕过单向信任导致的权限问题。您可以联接以下任一受信任域，因此能够看见这两个域。

- **加入点**：在思科 ISE 中，每个到 Active Directory 域的独立加入都叫作一个加入点。Active Directory 加入点是思科 ISE 身份库，可用于身份验证策略。它有助于属性和组的关联字典，这些属性和组可用于授权条件。
- **范围**：一部分 Active Directory 加入点组合到一起就叫做范围。您可以在身份验证策略中使用范围代替单个加入点并用作身份验证结果。范围用于按照多个加入点对用户进行身份验证。如果您使用范围，就无需为每个加入点设置多个规则，可以创建只有单个策略的相同策略，节约了思科 ISE 用于处理请求的时间并且有助于提高性能。一个加入点可以用于多个范围中。范围可以包含在身份源序列中。因为范围不具有任何关联字典，所以您无法将范围用于授权策略条件中。

当您执行思科 ISE 全新安装时，默认情况下并无范围。这称为无范围模式。当您添加范围时，思科 ISE 进入多范围模式。如果需要，您可以返回无范围模式。所有加入点将移至 Active Directory 文件夹。

- **Initial\_Scope** 是用于存储在无范围模式中添加的 Active Directory 加入点的隐式范围。当启用多范围模式时，所有 Active Directory 加入点将移至自动创建的 Initial\_Scope。您可以重命名 Initial\_Scope。
- **All\_AD\_Instances** 是在 Active Directory 配置中不显示的一个内置伪范围。它只在策略和身份序列中作为身份验证结果显示。如果您要选择思科 ISE 中配置的所有 Active Directory 加入点，就可以选择此范围。

## 创建新范围，添加 Active Directory 加入点

**步骤 1** 依次选择 **Administration > Identity Management > External Identity Sources > Active Directory**。

**步骤 2** 点击 **Scope Mode**。

默认情况下，系统创建名为 Initial\_Scope 的范围，当前所有加入点都放在此范围中。

**步骤 3** 要创建更多范围，请点击 **Add**。

**步骤 4** 输入新范围的名称和说明。

**步骤 5** 点击提交。

## 身份重写

身份重写是一种定向思科 ISE 的高级功能，使其在传递至外部 Active Directory 系统之前处理其身份。您可以创建规则以将身份改为包含或排除域前缀和/或后缀或您所选择的其他附加标记的相应格式。

身份重写规则应用于传递至 Active Directory 之前从客户端接收的用于使用者搜索、身份验证和授权查询等操作的用户名或主机名。思科 ISE 将匹配条件标记，在发现第一个匹配项时，思科 ISE 停止处理策略并根据结果重写身份字符串。

在重写期间，以方括号"[]"括起来的所有内容（例如 [IDENTITY]）是变量，在评估端不会对其进行评估，但会添加与字符串中该位置匹配的字符串。没有方括号的所有内容在规则的评估端和重写端都会评估为固定字符串。

以下是身份重写的一些示例，假设用户输入的身份是 ACME\jdoe:

- 如果身份与 **ACME[IDENTITY]** 匹配，则重写为 **[IDENTITY]**。  
结果是 jdoe。此规则指示思科 ISE 删掉所有用户名的 ACME 前缀。
- 如果身份与 **ACME[IDENTITY]** 匹配，则重写为 **[IDENTITY]@ACME.com**。  
结果是 jdoe@ACME.com。此规则指示思科 ISE 将格式从前缀更改为后缀表示法，或从 NetBIOS 格式更改为 UPN 格式。
- 如果身份与 **ACME[IDENTITY]** 匹配，则重写为 **ACME2[IDENTITY]**。  
结果是 ACME2jdoe。此规则指示思科 ISE 将具有特定前缀的所有用户名更改为使用备用前缀。

- 如果身份与 `[ACME]\jdoe.USA` 匹配，则重写为 `[IDENTITY]@[ACME].com`。  
结果是 `jdoe\ACME.com`。此规则指示思科 ISE 删掉点后面的领域（在本例中是国家/地区），替换为正确的领域。
- 如果身份与 `E=[IDENTITY]` 匹配，则重写为 `[IDENTITY]`。  
结果是 `jdoe`。如果身份来自证书，字段是邮件地址，而且 Active Directory 配置为按使用者搜索，则可以创建此示例规则。此规则指示思科 ISE 删除“E=”。
- 如果身份与 `E=[EMAIL],[DN]` 匹配，则重写为 `[DN]`。  
此规则会将证书使用者从 `E=jdoe@acme.com, CN=jdoe, DC=acme, DC=com` 转变为纯 DN, `CN=jdoe, DC=acme, DC=com`。如果身份取自证书使用者，且 Active Directory 配置为按 DN 搜索用户，则可以创建此示例规则。此规则指示思科 ISE 删掉邮件前缀并生成 DN。

以下是编写身份重写规则的一些常见错误：

- 如果身份与 `[DOMAIN]\[IDENTITY]` 匹配，则重写为 `[IDENTITY]@DOMAIN.com`。  
结果是 `jdoe@DOMAIN.com`。此规则在规则的重写端没有用方括号 [] 括起来的 [DOMAIN]。
- 如果身份与 `DOMAIN\[IDENTITY]` 匹配，则重写为 `[IDENTITY]@[DOMAIN].com`。  
同样，结果是 `jdoe@DOMAIN.com`。此规则在规则的评估端没有用方括号 [] 括起来的 [DOMAIN]。

身份重写规则始终应用在 Active Directory 加入点的情景中。即使由于身份验证策略而选择了范围，重写规则也适用于每个 Active Directory 加入点。如果使用的是 EAP-TLS，这些重写规则还适用于取自证书的身份。

## 启用身份重写



**注释** 此配置任务是可选的。您可以执行此任务来减少因各种原因（例如不明身份错误）造成的身份验证失败。

### 开始之前

您必须将思科 ISE 加入到 Active Directory 域。

**步骤 1** 依次选择 **管理 > 身份管理 > 外部身份源 > Active Directory**。

**步骤 2** 点击 **Advanced Settings** 选项卡。

**步骤 3** 在 **Identity Rewrite** 部分下，选择是否要应用重写规则来修改用户名。

**步骤 4** 输入匹配条件和重写结果。您可以删除出现的默认规则并根据要求输入规则。思科 ISE 按顺序处理规则，并会应用与请求用户名相匹配的第一个条件。您可以使用匹配令牌（方括号中包含的文本）将原始用户名的元素传输到结果。如果无任何规则匹配，则身份名称保持不变。您可以点击 **Launch Test** 按钮预览重写处理。

## 身份解析设置

某些身份类型包括域标记，如前缀或后缀。例如，在如 ACME\jdoe 这样的 NetBIOS 身份中，“ACME”是域标记前缀，同样在如 jdoe@acme.com 这样的 UPN 身份中，“acme.com”是域标记后缀。域前缀应该与组织中 Active Directory 域的 NetBIOS (NTLM) 名称匹配，域后缀应该与组织中 Active Directory 域的 DNS 名称或备选 UPN 后缀匹配。例如，jdoe@gmail.com 会视为没有域标记，因为 gmail.com 不是 Active Directory 域的 DNS 名称。

身份解析设置允许您配置重要设置来调整安全和性能的平衡，以符合您的 Active Directory 部署。您可以使用这些设置来调整没有域标记的用户名和主机名的身份验证。在思科 ISE 不知道用户域的情况下，可以将其配置为在所有身份验证域中搜索用户。即使在一个域中找到了用户，思科 ISE 仍将等待所有响应以确保不存在模糊身份。这可能需要较长时间，具体取决于域的数量、网络中的延迟、负载等。

### 避免身份解析问题

强烈建议在身份验证期间，使用完全限定的用户和主机名称（即，带有域标记的名称）。例如，用户使用 UPN 和 NetBIOS 名称，主机使用 FQDN SPN 名称。这在您频繁遇到模糊错误的情况下尤其重要，例如，多个 Active Directory 帐户匹配传入用户名；例如，jdoe m 匹配 jdoe@emea.acme.com 和 jdoe@amer.acme.com。在某些情况下，使用完全限定名称是解决问题的唯一方法。在其他情况下，保证用户拥有唯一密码即可。因此，如果最初使用唯一身份，则更加高效，而且可以减少密码锁定问题。

### 配置身份解析设置



**注释** 此配置任务是可选的。您可以执行此任务来减少因各种原因（例如不明身份错误）造成的身份验证失败。

#### 开始之前

您必须将思科 ISE 节点加入到 Active Directory 域。

**步骤 1** 依次选择管理 > 身份管理 > 外部身份源 > Active Directory。

**步骤 2** 点击 **Advanced Settings** 选项卡。

**步骤 3** 在 **Identity Resolution**（身份解析）部分下，对用户名或计算机名称的身份解析定义以下设置。此设置可提供用于用户搜索和身份验证的高级控制。

第一个设置适用于没有标记的身份。在这种情况下，可以选择以下任一选项：

- **拒绝请求 (Reject the request):** 此选项将导致没有任何域标记的用户（例如 SAM 名称）的身份验证失败。如果有多个加入域，而思科 ISE 必须在所有加入的全局目录中查找身份（这可能不太安全），则此选项非常有用。此选项强制用户使用具有域标记的名称。
- **仅搜索加入的林中的“身份验证域” (Only search in the “Authentication Domains” from the joined forest):** 此选项只在加入点所在林的域（这些域在身份验证域部分中指定）中搜索身份。这是默认选项。

- **搜索所有“身份验证域”部分 (Search in all the “Authentication Domains” sections):** 此选项在所有受信任林的所有身份验证域中搜索身份。这可能会增加延迟并影响性能。

根据身份验证域在思科 ISE 中的配置方式来选择选项。如果只选择特定身份验证域，将只搜索这些域（无论是选择“加入的林”还是“所有林”）。

如果思科 ISE 无法与它所需的所有全局目录 (GC) 通信，则使用第二个设置，以符合在“Authentication Domains”部分中指定的配置。在这种情况下，可以选择以下任一选项：

- **继续使用可用域 (Proceed with available domains):** 如果在任一可用的域中找到匹配项，此选项将继续执行身份验证。
- **丢弃请求 (Drop the request):** 如果身份解析遇到某些无法访问或不可用的域，此选项将删除身份验证请求。

---

## 对用户进行 Active Directory 身份验证测试

“测试用户”工具可用于从 Active Directory 验证用户身份验证。您还可以获取组和属性并对其进行检查。您可以对单个加入点或对范围运行测试。

**步骤 1** 选择管理 > 身份管理 > 外部身份源 > 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，请选择该加入点并点击编辑 (Edit)。选择思科 ISE 节点并点击测试用户 (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 节点。

**步骤 6** 如果要从 Active Directory 检索组和属性，请选中“检索组” (Retrieve Groups) 和“检索属性” (Retrieve Attributes) 复选框。

**步骤 7** 点击测试 (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。

---

## 删除 Active Directory 配置

如果您不会使用 Active Directory 作为外部身份源，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。

开始之前

确保您已退出 Active Directory 域。

**步骤 1** 选择管理 > 身份管理 > 外部身份源 > 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** 点击删除 (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。

## 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 节点的所有 Active Directory 加入点的状态或所有思科 ISE 节点上的所有加入点列表。

**步骤 1** 选择管理 > 身份管理 > 外部身份源 > Active Directory。

**步骤 2** 点击节点视图 (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 节点，则更新此表可能需要几分钟时间。

**步骤 4** 点击加入点名称 (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** 点击诊断摘要 (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 节点上运行的服务。当思科 ISE 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 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 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** 选择管理 > 身份管理 > 外部身份源 > Active Directory。

**步骤 2** 点击高级工具 (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 节点。

如果未选择思科 ISE 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** 点击在所有节点上运行测试 (**Run All Tests on Node**) 开始测试。

**步骤 6** 点击查看测试详情 (**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。

---

## 启用 Active Directory 调试日志

默认情况下，不会记录 Active Directory 调试日志。必须在您的部署中承担策略服务角色的思科 ISE 节点上启用此选项。启用 Active Directory 调试日志可能会影响 ISE 性能。

- 
- 步骤 1** 选择管理 (**Administration**) > 系统 (**System**) > 日志记录 (**Logging**) > 调试日志配置 (**Debug Log Configuration**)。
  - 步骤 2** 点击要从中获取 Active Directory 调试信息的思科 ISE 策略服务节点旁边的单选按钮，然后点击编辑 (**Edit**)。
  - 步骤 3** 点击 **Active Directory** 单选按钮，然后点击编辑 (**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** 点击保存 (**Save**)。

---

## 获取 Active Directory 日志文件来进行故障排除

下载并查看 Active Directory 调试日志，对您可能遇到的问题进行故障排除。

开始之前

必须启用 Active Directory 调试日志记录。

- 
- 步骤 1** 依次选择操作 > 故障排除 > 下载日志。
  - 步骤 2** 点击您要从其获得 Active Directory 调试日志文件的节点。
  - 步骤 3** 点击 **Debug Logs** 选项卡。
  - 步骤 4** 向下滚动此页面找到 ad\_agent.log 文件。点击该文件并下载该文件。

---

## Active Directory 警报和报告

思科 ISE 提供多种警报和报告，用于对 Active Directory 相关活动进行监控和故障排除。

警报

Active Directory 错误和故障会触发以下警报：

- 配置的名称服务器不可用
- 所加入的域不可用
- 身份验证域不可用
- Active Directory 林不可用
- AD 连接器必须重新启动
- AD: ISE 帐户密码更新失败
- AD: 计算机 TGT 刷新失败

## 报告

您可以通过以下两种报告监控 Active Directory 相关活动:

- “RADIUS 身份验证报告” (RADIUS Authentications Report): 此报告显示 Active Directory 身份验证和授权的详细步骤。您可以在以下位置找到此报告: **操作 (Operations) > 报告 (Reports) > 身份验证服务状态 (Auth Services Status) > RADIUS 身份验证 (RADIUS Authentications)**。
- “AD 连接器操作报告” (AD Connector Operations Report): AD 连接器操作报告提供 AD 连接器所执行后台操作的日志, 例如思科 ISE 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。如果遇到 Active Directory 失败, 您可以查看此报告的详细信息以确定可能的原因。您可以在以下位置找到此报告: **操作 (Operations) > 报告 (Reports) > 身份验证服务状态 (Auth Services Status) > AD 连接器操作 (AD Connector Operations)**。

## Active Directory 高级调整

高级调整功能提供节点特定的设置, 用于在思科支持人员指导下的支持操作, 更深入地调整系统中的参数。这些设置不适用于正常管理流程, 只应在指导下使用。

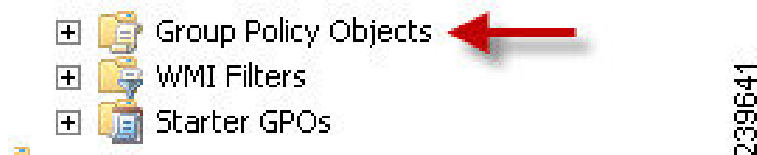
## 使用 Active Directory 设置思科 ISE 的补充信息

要使用 Active Directory 配置思科 ISE, 必须配置组策略, 并配置请求方以对计算机进行身份验证。

### 在 Active Directory 中配置组策略

有关如何访问组策略管理编辑器的详细信息, 请参阅 Microsoft Active Directory 文档。

**步骤 1** 打开组策略管理编辑器, 如下图所示。

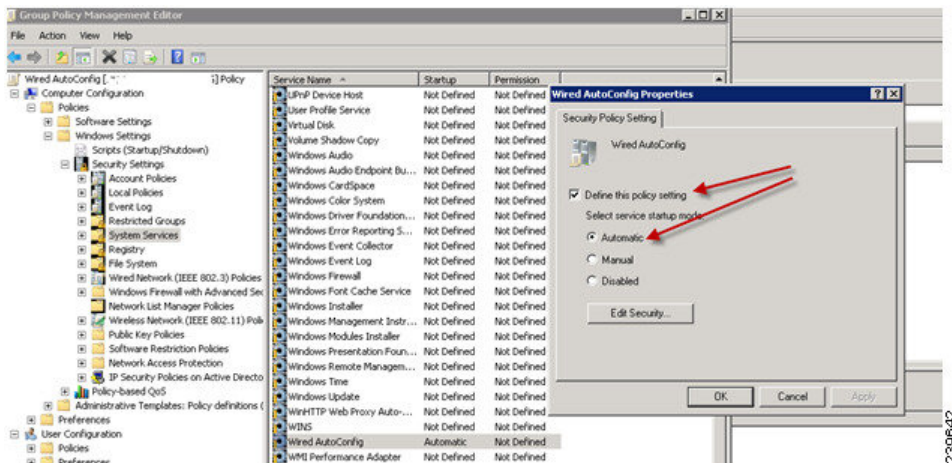




步骤 2 创建新策略并为其输入描述性名称，或者将其添加到现有域策略。

在以下示例中，使用 Wired Autoconfiguration 作为策略名称。

步骤 3 选中 **Define this policy setting** 复选框，然后针对服务启动模式点击 **Automatic** 单选按钮，如下图所示。



步骤 4 在所需的组织单元或域 Active Directory 级别应用策略。

## 配置 Odyssey 5.X 请求方，依据 Active Directory 对 EAP-TLS 计算机进行身份验证

如果使用 Odyssey 5.x 请求方，依据 Active Directory 对 EAP-TLS 计算机进行身份验证，则必须在请求方进行以下配置。

步骤 1 启动 Odyssey 访问客户端。

步骤 2 从 Tools 菜单选择 **Odyssey Access Client Administrator**。

步骤 3 双击 **Machine Account** 图标。

步骤 4 从计算机帐户 (**Machine Account**) 窗口，必须配置 EAP-TLS 身份验证配置文件：

- a) 选择配置 (**Configuration**) > 配置文件 (**Profiles**)。
- b) 为 EAP-TLS 配置文件输入名称。
- c) 在“身份验证” (Authentication) 选项卡上，选择 **EAP-TLS** 作为身份验证方法。
- d) 在“证书” (Certificate) 选项卡上，选中允许使用我的证书登录 (**Permit login using my certificate**) 复选框，然后为请求方计算机选择证书。
- e) 在用户信息 (**User Info**) 选项卡上，选中使用计算机凭证 (**Use machine credentials**) 复选框。

如果启用此选项，Odyssey 请求方将以 `host\<machine_name>` 格式发送计算机名称，Active Directory 识别来自计算机的请求，并且查找要执行身份验证的计算机对象。如果禁用此选项，Odyssey 请求方将发送不带 `host\` 前缀的计算机名称，Active Directory 将查找用户对象，身份验证失败。

## 为机器身份验证配置代理

当您为计算机身份验证配置 AnyConnect 代理时，可以执行下列操作之一：

- 使用默认的计算机主机名，包括前缀“host/”。
- 配置新的配置文件，在这种情况下必须包括前缀“host/”，然后是计算机名称。

## LDAP

轻型目录访问协议 (LDAP) 是 RFC 2251 定义用于查询和修改在 TCP/IP 上运行的目录服务的网络协议。LDAP 是用于访问基于 X.500 的目录服务器的轻型机制。

思科 ISE 使用 LDAP 协议集成 LDAP 外部数据库，此外部数据库也称为身份源。

## LDAP 目录服务

LDAP 目录服务以客户端-服务器模式为基础。客户端通过连接至 LDAP 服务器并向服务器发送运行请求，启动 LDAP 会话。然后服务器发送其响应。一个或多个 LDAP 服务器包含来自 LDAP 目录树或 LDAP 后端数据库的数据。

目录服务管理一个目录，此目录是存储信息的一个数据库。目录服务使用分布式模式存储信息，而且通常会在目录服务器之间复制这些信息。

LDAP 目录以简单树状层次结构排列，可以分布在多个服务器中。每台服务器都可包含整个目录的复制版本，系统会定期同步此复制版本。

树中的每个条目都包含一组属性，其中每个属性都有一个名称（属性类型或属性说明）以及一个或多个值。这些属性在架构中定义。

每个条目都有一个唯一标识符：其可分辨名称 (DN)。此名称包含相对可分辨名称 (RDN)，RDN 由条目中的属性，然后加上父条目的 DN 构成。您可以将 DN 视为完整文件名，将 RDN 视为文件夹的相对文件名。

## 多个 LDAP 实例

通过使用不同的 IP 地址或端口设置创建多个 LDAP 实例，可以将思科 ISE 配置为使用不同的 LDAP 服务器或同一个 LDAP 服务器中的不同数据库进行身份验证。每个主要服务器 IP 地址和端口配置，以及辅助服务器 IP 地址和端口配置，组成对应于一个思科 ISE LDAP 身份源实例的一个 LDAP 实例。

思科 ISE 不要求每个 LDAP 实例都对应一个 LDAP 数据库。可以设置多个 LDAP 实例来访问同一个数据库。当 LDAP 数据库包含多个用户或组子树时，此方法非常有用。由于每个 LDAP 实例仅支持一个用户子树目录和一个组子树目录，因此，必须为每个用户目录和组目录子树组合配置单独的 LDAP 实例，思科 ISE 为该组合提交身份验证请求。

## LDAP 故障切换

思科 ISE 支持在主要 LDAP 服务器和辅助 LDAP 服务器之间进行故障转移。当 LDAP 服务器宕机或因其他原因而无法访问，导致思科 ISE 无法连接 LDAP 服务器，从而使得身份验证请求失败时，就会发生故障转移。

如果您建立故障转移设置并且思科 ISE 尝试连接的第一个 LDAP 服务器无法访问，思科 ISE 始终会尝试连接第二个 LDAP 服务器。如果您希望思科 ISE 再次使用第一个 LDAP 服务器，您必须在 Failback Retry Delay 文本框中输入一个值。



**注释** 思科 ISE 始终使用主要 LDAP 服务器从 Admin 门户获取用于授权策略的组和属性，因此当您配置这些项目时必须可以访问主要 LDAP 服务器。根据故障切换配置，思科 ISE 仅将辅助 LDAP 服务器用于运行时的身份验证和授权。

## LDAP 连接管理

思科 ISE 支持多个并行 LDAP 连接。首次进行 LDAP 身份验证时，根据需要打开连接。为每个 LDAP 服务器配置最大连接数。事先打开连接可缩短身份验证时间。可以设置最大连接数以用于并发绑定连接。每台 LDAP 服务器（主要或辅助）的打开连接数量可以不同，此数量根据为每台服务器配置的最大管理连接数来确定。

思科 ISE 会为思科 ISE 中配置的每台 LDAP 服务器保留打开的 LDAP 连接列表（包括绑定信息）。在身份验证流程中，连接管理器会尝试从池中查找打开的连接。如果打开的连接不存在，系统会打开新的连接。

如果 LDAP 服务器关闭连接，则连接管理器会在对搜索目录的第一个调用过程中报告错误，并会尝试更新连接。身份验证流程完成之后，连接管理器会发布连接。

## LDAP 用户身份验证

您可以将 LDAP 配置为外部身份存储库。思科 ISE 使用明文密码身份验证。用户身份验证包括：

- 在 LDAP 服务器中搜索与请求中的用户名相匹配的条目。
- 使用 LDAP 服务器中查找到的用户密码检查用户密码。
- 检索用于策略的组成员信息。
- 检索指定属性的值以用于策略和授权配置文件。

若要验证用户，思科 ISE 会向 LDAP 服务器发送绑定请求。绑定请求会包含明文显示的用户 DN 和密码。如果用户的 DN 和密码与 LDAP 目录中的用户名和密码匹配，则用户通过身份验证。



## 注释

- 思科 ISE 会为每个用户身份验证发送两条 searchRequest 消息。这不会影响思科 ISE 授权或网络性能。第二个 LDAP 请求用于确保思科 ISE 与正确的身份通信。
- 思科 ISE 作为 DNS 客户端，仅使用 DNS 响应中返回的第一个 IP 来执行 LDAP 绑定。

我们建议您使用安全套接字层 (SSL) 保护与 LDAP 服务器的连接。

## 在授权策略中使用的 LDAP 组和属性检索

思科 ISE 可以依据 LDAP 身份源验证主题（用户或主机），具体方法是在目录服务器上执行绑定操作，查找和验证主题。成功进行身份验证后，思科 ISE 可以在必要时检索属于主题的组和属性。通过选择管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > LDAP，您可以在思科 ISE 管理员门户中配置要检索的属性。思科 ISE 可以使用这些组和属性授权主题。

要验证用户或查询 LDAP 身份源，思科 ISE 连接到 LDAP 服务器并维护连接池。

当 Active Directory 配置为 LDAP 存储时，应当注意下列关于组成员身份的限制：

- 用户或计算机必须是策略条件中定义的组的直接成员，才符合策略规则。
- 定义的组可能不是用户或计算机的主组。此限制仅在 Active Directory 配置为 LDAP 存储时适用。

### LDAP 组成员身份信息检索

对于用户身份验证、用户查找和 MAC 地址查找，思科 ISE 必须从 LDAP 数据库检索组成员身份信息。LDAP 服务器通过以下其中一种方式表示使用者（用户或主机）与组之间的关联：

- 组引用使用者 (Groups Refer to Subjects)：组对象包含用于指定使用者的属性。使用者的标识符可以作为以下内容在组中寻源：
  - 可分辨名称
  - 明文用户名
- 使用者引用组 (Subjects Refer to Groups)：使用者对象包含用于指定其所属的组的属性。

LDAP 身份源包含以下用于组成员身份信息检索的参数：

- 引用方向 (Reference direction)：此参数指定在确定组成员身份时要使用的方法（组引用使用者或使用者引用组）。
- 组映射属性 (Group map attribute)：此参数指示包含组成员身份信息的属性。
- 组对象类 (Group object class)：此参数确定特定对象可识别为组。
- 组搜索子树 (Group search subtree)：此参数指示用于组搜索的搜索库。

- 成员类型选项 (Member type option): 此参数指定成员在组成员属性中的存储方式 (作为 DN 或明文用户名)。

### LDAP 属性检索

针对用户身份验证、用户查找和 MAC 地址查找，思科 ISE 必须从 LDAP 数据库检索主题属性。对于 LDAP 身份源的每个实例，将创建身份源字典。这些字典支持以下数据类型的属性：

- 字符串
- 无符号整数 32
- IPv4 地址

对于无符号整数和 IPv4 属性，思科 ISE 会对已检索的相应数据类型的字符串进行转换。如果转换失败或未检索到属性的值，则思科 ISE 将记录调试消息，但身份验证或查找进程不会失败。

您同样可以配置属性的默认值，当转换失败或思科 ISE 未检索到任何属值时，思科 ISE 即可使用该默认值。

### LDAP 证书检索

如果您已将证书检索配置为用户查找的一部分，那么思科 ISE 必须从 LDAP 检索证书属性值。要从 LDAP 检索证书属性值，在配置 LDAP 身份源时，先前必须将属性列表中的证书属性配置为可访问。

## LDAP 服务器返回的错误

在身份验证过程中可能会出现以下错误：

- 身份验证错误 - 思科 ISE 会在思科 ISE 日志文件中记录身份验证错误。

LDAP 服务器返回绑定 (身份验证) 错误的可能原因如下：

- 参数错误 - 输入了无效的参数
- 用户帐户受限制 (已禁用、已锁定、已到期、密码已到期等)
- 初始化错误 - 使用 LDAP 服务器超时设置配置思科 ISE 在确定该服务器上的连接或身份验证是否已失败之前，应该等待从 LDAP 服务器接收响应的秒数。

LDAP 服务器返回初始化错误的可能原因如下：

- 不支持 LDAP。
- 服务器宕机。
- 服务器内存不足。
- 用户无权限。
- 管理员凭证配置不正确。

以下错误记录为外部资源错误，指示 LDAP 服务器可能有问题：

- 发生连接错误
- 超时到期
- 服务器宕机
- 服务器内存不足

以下错误记录为 Unknown User 错误：

- 用户在数据库中不存在

以下错误记录为 Invalid Password 错误，虽然用户存在，但是发送的密码无效：

- 输入了无效密码

## LDAP 用户查找

思科 ISE 支持 LDAP 服务器的用户查找功能。通过此功能，可以在未经身份验证的情况下在 LDAP 数据库中搜索用户和检索信息。用户查找流程包括以下操作：

- 在 LDAP 服务器中搜索与请求中的用户名相匹配的条目
- 检索要用于策略的用户组成员身份信息
- 检索指定属性的值以用于策略和授权配置文件

## LDAP MAC 地址查找

思科 ISE 支持 MAC 地址查找功能。您可以通过此功能在 LDAP 数据库中搜索 MAC 地址以及在未经身份验证的情况下检索信息。MAC 地址查找过程包括以下操作：

- 在 LDAP 服务器中搜索与设备 MAC 地址匹配的条目
- 为策略中使用的设备检索 MAC 地址组信息
- 为策略中使用的指定属性检索值

## 添加 LDAP 身份源

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。
- 思科 ISE 始终使用主要 LDAP 服务器获取用于授权策略的组和属性。因此，当您配置这些项目时，必须可访问您的主要 LDAP 服务器。

步骤 1 选择 管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > LDAP > 添加 (Add)。

步骤 2 输入相应值。

步骤 3 点击 **Submit** 以创建 LDAP 实例。

## LDAP 身份源设置

### LDAP 常规设置

下表介绍常规 (General) 选项卡上的字段。

表 52: LDAP 常规设置

字段名称	使用指南
<b>Name</b>	输入 LDAP 实例的名称。此值在搜索中用于获取主题 DN 和属性。此值为字符串类型，最大长度为 64 个字符。
<b>Description</b>	输入对 LDAP 实例的说明。此值为字符串类型，最大长度为 1024 个字符。
<b>架构 (Schema)</b>	<p>您可以选择以下任一内置架构类型或创建自定义架构：</p> <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Sun 目录服务器 (Sun Directory Server)</li> <li>• Novell eDirectory</li> </ul> <p>您可以点击 Schema 旁边的箭头以查看架构详细信息。</p> <p>如果您编辑该预定义架构的属性，思科 ISE 会自动创建自定义架构。</p>
<b>注释</b>	仅在您选择定制架构时，可以编辑以下字段。
<b>Subject Objectclass</b>	输入在搜索中用于获取主题 DN 和属性的值。此值为字符串类型，最大长度为 256 个字符。
<b>主题名称属性 (Subject Name Attribute)</b>	输入包含请求中用户名的属性的名称。此值为字符串类型，最大长度为 256 个字符。
<b>证书属性 (Certificate Attribute)</b>	输入包含证书定义的属性。对于基于证书的身份验证，这些定义用于验证由客户端提供的证书。
<b>Group Objectclass</b>	输入在搜索中用于指定识别为组的对象的值。此值为字符串类型，最大长度为 256 个字符。

字段名称	使用指南
组映射属性 (Group Map Attribute)	指定包含映射信息的属性。根据选择的参考方向，此属性可以是用户或组属性。
主题对象包含对组的引用 (Subject Objects Contain Reference To Groups)	如果使用者对象包含指定这些对象所属组的属性，请点击此选项。
组对象包含对主题的引用 (Group Objects Contain Reference To Subjects)	如果组对象包含指定使用者的属性，请点击此选项。此值为默认值。
组对象作为...存储于成员属性中 (Subjects in Groups Are Stored in Member Attribute As)	(仅适用于启用组对象包含对使用者的引用 (Group Objects Contain Reference To Subjects) 选项时) 指定在组成员属性中如何搜索成员，其默认值为 DN。



注释 配置的主题名称属性应在外部 ID 存储区中编入索引。

### LDAP 连接设置

下表介绍连接设置 (Connection Settings) 选项卡中的字段。

表 53: LDAP 连接设置

字段名称	使用指南
启用辅助服务器	选中此选项以在主要 LDAP 服务器出现故障的时候启用辅助 LDAP 服务器作为备份。如果选中此复选框，则必须输入辅助 LDAP 服务器的配置参数。
主服务器和辅助服务器	
Hostname/IP	输入运行 LDAP 软件的设备的 IP 地址或 DNS 名称。此主机可以包含 1 至 256 个字符或以字符串表示的有效 IP 地址。对于主机名，仅字母数字字符 (a 至 z; A 至 Z; 0 至 9)、点 (.) 和连字符 (-) 为有效字符。
端口	输入 LDAP 服务器侦听的 TCP/IP 端口号。有效值为 1 至 65535。默认值为 389，如 LDAP 规范中所述。如果您不知道端口号，可以向 LDAP 服务器管理员查询此信息。



字段名称	使用指南
访问	<p><b>匿名访问 (Anonymous Access):</b> 点击此选项可确保在 LDAP 目录中进行匿名搜索。服务器不识别客户端身份并且会允许客户端读取配置为允许任何未经身份验证的客户端访问的任何数据。在缺少要向服务器发送的具体策略许可身份信息的情况下，客户端应该使用匿名连接。</p> <p><b>身份验证访问 (Authenticated Access):</b> 点击此选项可确保使用管理凭证在 LDAP 目录上进行搜索。如果选择此选项，请为“管理员 DN” (Admin DN) 字段和“密码” (Password) 字段输入信息。</p>
管理员 DN (Admin DN)	输入管理员的 DN。管理员 DN 是有权限搜索“用户目录子树” (User Directory Subtree) 下所有必要用户和有权限搜索组的 LDAP 帐户。如果指定的管理员没有权限在搜索中查看组名称属性，对于由该 LDAP 服务器进行身份验证的用户，组映射将失败。
密码	输入 LDAP 管理员帐户密码。
安全身份验证 (Secure Authentication)	点击此字段以对思科 ISE 和主 LDAP 服务器之间的通信进行加密。验证“端口” (Port) 字段是否包含用于 LDAP 服务器上的 SSL 的端口号。如果启用此选项，则必须选择一个根 CA。
“LDAP 服务器根 CA” (LDAP Server Root CA)	从下拉列表中选择受信任根证书颁发机构，以启用使用证书的安全身份验证。
服务器超时 (Server Timeout)	以秒为单位输入思科 ISE 在确定与主要 LDAP 服务器的连接或身份验证失败之前等待该服务器响应的的时间。有效值为 1 至 99。默认值为 10。
最大管理员连接数 (Max. Admin Connections)	输入利用 LDAP 管理员帐户权限对于特定 LDAP 配置可以运行的并发连接的最大数量（大于 0）。这些连接用于在“用户目录子树” (User Directory Subtree) 和“组目录子树” (Group Directory Subtree) 下搜索目录中的用户和组。有效值为 1 至 99。默认值为 20。
测试与服务器的绑定 (Test Bind to Server)	点击此选项以测试并确保可以成功绑定 LDAP 服务器详细信息和凭证。如果测试失败，请编辑您的 LDAP 服务器详细信息并重新测试。
<b>Failover</b>	
Always Access Primary Server First	如果您希望思科 ISE 在进行身份验证和授权时始终先访问主 LDAP 服务器，请选择中该选项。
...后故障恢复到主服务器 (Failback to Primary Server after)	如果思科 ISE 尝试连接的主 LDAP 服务器无法访问，思科 ISE 会尝试连接辅助 LDAP 服务器。如果您希望思科 ISE 再次使用主 LDAP 服务器，请点击此选项并在文本框中输入值。

## LDAP 目录组织设置

下表介绍目录组织 (**Directory Organization**) 选项卡上的字段。

表 54: LDAP 目录组织设置

字段名称	使用指南
<b>主题搜索库 (Subject Search Base)</b>	<p>输入包含所有主题的子树的 DN。例如：</p> <p>o=corporation.com</p> <p>如果包含主题的树是基本 DN，请输入：</p> <p>o=corporation.com</p> <p>或</p> <p>dc=corporation,dc=com</p> <p>根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。</p>
<b>组搜索库 (Group Search Base)</b>	<p>输入包含所有组的子树的 DN。例如：</p> <p>ou=organizational unit, ou=next organizational unit, o=corporation.com</p> <p>如果包含组的树是基本 DN，请键入：</p> <p>o=corporation.com</p> <p>或</p> <p>dc=corporation,dc=com</p> <p>根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。</p>
<b>搜索该格式的 MAC 地址 (Search for MAC Address in Format)</b>	<p>输入一个 MAC 地址格式供思科 ISE 用于在 LDAP 数据库中进行搜索。在内部身份源中的 MAC 地址按照 xx-xx-xx-xx-xx-xx 格式进行搜索。LDAP 数据库中的 MAC 地址可以按照不同格式进行搜索。但是，当思科 ISE 收到主机查找请求时，思科 ISE 会将 MAC 地址从内部格式转换为为此字段指定的格式。</p> <p>使用下拉列表以启用按照指定的格式搜索 MAC 地址，其中 <i>&lt;format&gt;</i> 可以是以下任何一种格式：</p> <ul style="list-style-type: none"> <li>• xxxx.xxxx.xxxx</li> <li>• xxxxxxxxxxxxxx</li> <li>• xx-xx-xx-xx-xx-xx</li> <li>• xx:xx:xx:xx:xx:xx</li> </ul> <p>您选择的格式必须与在 LDAP 服务器中搜索的 MAC 地址的格式一致。</p>

字段名称	使用指南
主题名称条开始直到最后一次出现分隔符 (Strip Start of Subject Name Up To the Last Occurrence of the Separator)	<p>输入适当的文本以删除用户名的域前缀。</p> <p>如果思科 ISE 在用户名中找到此字段中指定的分隔符，则会删除从用户名的开头一直到该分隔符的所有字符。如果用户名包含 &lt;start_string&gt; 框中指定的多个字符，思科 ISE 会删除从用户名的开头一直到该分隔符之前的最后一个匹配字符之间的所有字符。例如，如果分隔符为反斜线(\)，用户名为 DOMAIN\user1，则思科 ISE 会向 LDAP 服务器提交 user1。</p> <p>注释 &lt;start_string&gt; 不能包含以下特殊字符：井号(#)、问号(?)、引号(“)、星号(*)、右尖括号(&gt;)和左尖括号(&lt;)。思科 ISE 不允许在用户名中使用这些字符。</p>
从第一次出现分隔符时主题名称条结束 (Strip End of Subject Name from the First Occurrence of the Separator)	<p>输入适当的文本以删除用户名的域后缀。</p> <p>如果思科 ISE 在用户名中找到此字段中指定的分隔符，则会删除从该分隔符一直到用户名结尾的所有字符。如果用户名包含此字段中指定的多个字符，思科 ISE 会删除从该分隔符之后的第一个匹配字符开始的所有字符。例如，如果分隔符为 @，用户名为 user1@domain，则思科 ISE 会向 LDAP 服务器提交 user1。</p> <p>注释 &lt;end_string&gt; 框不能包含以下特殊字符：井号(#)、问号(?)、引号(“)、星号(*)、右尖括号(&gt;)和左尖括号(&lt;)。思科 ISE 不允许在用户名中使用这些字符。</p>

## LDAP 组设置

表 55: LDAP 组设置

字段名称	使用指南
添加	<p>选择 <b>Add</b>；添加组添加新组或从目录中选择 <b>Add</b>；选择 Group 选择组从 LDAP 目录。</p> <p>如果您选择添加组，请输入新组的名称。如果您正在从目录中选择，请输入过滤器条件，然后点击<b>检索组 (Retrieve Groups)</b>。点击要选择的组旁边的复选框，然后点击<b>确定 (OK)</b>。选中的组将显示在<b>组 (Groups)</b>窗口中。</p>

## LDAP 属性设置

表 56: LDAP 属性设置

字段名称	使用指南
添加	<p>选择 <b>Add</b>; 添加属性添加新属性或从目录中选择 <b>Add</b>; 选择属性从 LDAP 服务器的属性。</p> <p>如果选择添加属性，则为新属性输入名称。如果从目录中选择，请输入用户名，然后点击<b>检索属性 (Retrieve Attributes)</b>以检索属性。选中想要选择的属性旁边的复选框，然后点击“确定”。</p>

### 相关主题

- [LDAP 目录服务](#)，第 370 页
- [LDAP 用户身份验证](#)，第 371 页
- [LDAP 用户查找](#)，第 374 页
- [添加 LDAP 身份源](#)，第 374 页

## 配置主要和辅助 LDAP 服务器

在创建 LDAP 实例之后，您必须为主要 LDAP 服务器配置连接设置。配置辅助 LDAP 服务器为可选操作。

**步骤 1** 选择在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > LDAP**。

**步骤 2** 选中希望编辑的 LDAP 实例旁的复选框并点击**编辑 (Edit)**。

**步骤 3** 点击 **Connection** 选项卡以配置主要和辅助服务器。

**步骤 4** 输入作为 LDAP 身份源设置中描述的值。

**步骤 5** 点击 **Submit** 保存连接参数。

## 允许思科 ISE 从 LDAP 服务器获取属性

为了让思科 ISE 从 LDAP 服务器获取用户和组数据，您必须在思科 ISE 中配置 LDAP 目录详细信息。对于 LDAP 身份源，适用以下三种搜索：

- 搜索组子树中的所有组用于管理
- 搜索主题子树中的用户以定位用户
- 搜索用户在其中为成员的组

**步骤 1** 选择在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > LDAP**。

步骤 2 选中希望编辑的 LDAP 实例旁的复选框并点击 **Edit**。

步骤 3 点击 **Directory Organization** 选项卡。

步骤 4 输入作为 LDAP 身份源设置中描述的值。

步骤 5 点击 **Submit** 保存配置。

---

## 从 LDAP 服务器检索组成员身份详细信息

您可以添加新组或从 LDAP 目录选择组。

步骤 1 选择在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > LDAP**。

步骤 2 选中希望编辑的 LDAP 实例旁的复选框并点击 **编辑 (Edit)**。

步骤 3 点击 **组 (Groups)** 选项卡。

步骤 4 选择 **添加 (Add) > 添加组 (Add Group)** 可添加新组，或选择 **添加 (Add) > 从目录选择组 (Select Groups From Directory)** 可从 LDAP 目录选择组。

a) 如果您选择添加组，请输入新组的名称。

b) 如果您正在从目录中选择，请输入过滤器条件，然后点击 **检索组 (Retrieve Groups)**。搜索条件可以包含星号 (\*) 通配符。

步骤 5 点击要选择的组旁边的复选框，然后点击 **确定 (OK)**。

选择的组将显示在“组” (Groups) 页面。

步骤 6 点击 **提交 (Submit)** 保存组选择。



注释 当 Active Directory 配置为思科 ISE 中的 LDAP 身份存储时，不支持 Active Directory 内置组。

---

## 从 LDAP 服务器检索用户属性

可以从 LDAP 服务器获取用户属性，以便在授权策略中使用。

步骤 1 选择 **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > LDAP**。

步骤 2 选中希望编辑的 LDAP 实例旁的复选框并点击 **Edit**。

步骤 3 点击 **Attributes** 选项卡。

步骤 4 选择 **添加 (Add) > 添加属性 (Add Attribute)** 添加新属性，或选择 **添加 (Add) > 从目录中选择属性 (Select Attributes From Directory)** 以便从 LDAP 服务器选择属性。

a) 如果选择添加属性，则为新属性输入名称。

- b) 如果从目录选择，则输入示例用户，点击**检索属性 (Retrieve Attributes)**，检索用户的属性。可以使用星号 (\*) 通配符。

**步骤 5** 选中想要选择的属性旁边的复选框，然后点击 **OK**。

**步骤 6** 点击 **Submit**，保存属性选择。

---

## 使用 LDAP 身份源进行安全身份验证

在“LDAP 配置” (LDAP configuration) 页面上选择“安全身份验证” (Secure Authentication) 选项时，思科 ISE 使用 SSL 保护与 LDAP 身份源的通信。通过以下方式建立到 LDAP 身份源的安全连接：

- SSL 隧道：使用 SSL v3 或 TLS v1（LDAP 服务器支持的最强大的版本）
- 服务器身份验证（LDAP 服务器身份验证）：基于证书
- 客户端身份验证（思科 ISE 身份验证）：无（在 SSL 隧道中使用管理员绑定）
- 密码套件：思科 ISE 支持的所有密码套件

我们建议您使用带有思科 ISE 支持的最强加密和密码的 TLS v1。

要使思科 ISE 与 LDAP 身份源安全通信，请执行以下操作：

开始之前

- 思科 ISE 必须连接到 LDAP 服务器
- TCP 端口 636 应当开放

---

**步骤 1** 将向 LDAP 服务器签发服务器证书的 CA 的完整证书授权 (CA) 链导入思科 ISE（管理 [Administration] > 系统 [System] > 证书 [Certificates] > 受信任证书 [Trusted Certificates]）。

完整 CA 链指的是根 CA 和中级 CA 证书；不是 LDAP 服务器证书。

**步骤 2** 配置思科 ISE 在与 LDAP 身份源通信时使用安全身份验证（管理 [Administration] > 身份管理 [Identity Management] > 外部身份源 [External Identity Sources] > LDAP；务必选中“连接设置” (Connection Settings) 选项卡中的“安全身份验证” (Secure Authentication) 复选框）。

**步骤 3** 在 LDAP 身份存储区中选择根 CA 证书。

---

## RADIUS 令牌身份源

支持 RADIUS 协议并向用户和设备提供身份验证、授权和记账 (AAA) 服务的服务器称为 RADIUS 服务器。RADIUS 身份源只是一个外部身份源，包含一系列的主题及其凭证，使用 RADIUS 协议进

行通信。例如，Safeword 令牌服务器是一个身份源，可以包含若干用户以及作为一次性密码的凭证，提供一个您可以使用 RADIUS 协议查询的界面。

思科 ISE 支持任何符合 RADIUS RFC 2865 的服务器作为外部身份源。思科 ISE 支持多个 RADIUS 令牌服务器身份，例如 RSA SecurityID 服务器和 SafeWord 服务器。RADIUS 身份源可以与任何用于验证用户的 RADIUS 令牌服务器配合使用。RADIUS 身份源将用户数据报协议 (UDP) 端口用于身份验证会话。所有 RADIUS 通信都使用同一 UDP 端口。



**注释** 必须为 MAB 身份验证启用“处理主机查找”(Process Host Lookup) 选项。我们建议不要为 MAB 身份验证配置用作外部身份源的 RADIUS 令牌服务器，因为使用 MAB 身份验证的设备无法生成 OTP 或 RADIUS 令牌（这是 RADIUS 令牌服务器身份验证所需的）。因此，身份验证将失败。您可以使用外部 RADIUS 服务器选项来处理 MAB 请求。

## 支持 RADIUS 令牌服务器的身份验证协议

对于 RADIUS 身份源，思科 ISE 支持以下身份验证协议：

- RADIUS PAP
- 使用内部可扩展身份验证协议 - 通用令牌卡 (EAP-GTC) 的受保护的可扩展身份验证协议 (PEAP)
- 使用内部 EAP-GTC 的 EAP-FAST

## RADIUS 令牌服务器用于通信的端口

RADIUS 令牌服务器将 UDP 端口用于身份验证会话。此端口用于所有 RADIUS 通信。为了让思科 ISE 将 RADIUS 一次性密码 (OTP) 消息发送到已启用 RADIUS 的令牌服务器，必须确保思科 ISE 和已启用 RADIUS 的令牌服务器之间的网关设备能够通过 UDP 端口进行通信。您可以通过管理员门户配置 UDP 端口。

## RADIUS 共享密钥

您在思科 ISE 中配置 RADIUS 身份源时必须提供共享密钥。此共享密钥应与 RADIUS 令牌服务器上配置的共享密钥相同。

## RADIUS 令牌服务器中的故障切换

思科 ISE 允许您配置多个 RADIUS 身份源。每个 RADIUS 身份源可以使用 RADIUS 主服务器和辅助服务器。当思科 ISE 无法连接到主服务器时，则会使用辅助服务器。

## RADIUS 令牌服务器中的可配置密码提示

RADIUS 身份源允许您配置密码提示。您可以通过管理员门户配置密码提示。

## RADIUS 令牌服务器用户身份验证

思科 ISE 会获取用户凭证（用户名和密码）并将这些凭证发送到 RADIUS 令牌服务器。思科 ISE 还会将 RADIUS 令牌服务器身份验证处理的结果中继到用户。

## RADIUS 令牌服务器中的用户属性缓存

默认情况下，RADIUS 令牌服务器不支持用户查找。但是，用户查找功能对于以下思科 ISE 功能非常重要。

- PEAP 会话恢复：此功能允许在建立 EAP 会话期间在身份验证成功之后恢复 PEAP 会话。
- EAP/FAST 快速重新连接：此功能允许在建立 EAP 会话期间在身份验证成功之后快速进行重新连接。
- TACACS+ 授权：在 TACACS+ 身份验证成功后发生。

思科 ISE 缓存成功的身份验证的结果以为这些功能处理用户查找请求。对于每次成功的身份验证，系统会缓存经过身份验证的用户的名称和所检索的属性。失败的身份验证不写入缓存。

在运行时内存中可提供缓存，在分布式部署中不可在思科 ISE 节点之间进行复制。您可以通过 Admin 门户为缓存配置有效时间 (TTL) 限制。您还必须启用身份缓存选项并以分钟为单位设置老化时间。在指定的时间内，内存中可提供缓存。

## 身份序列中的 RADIUS 身份源

您可以在身份源序列中添加身份验证序列的 RADIUS 身份源。但是，由于您无法查询不带身份验证的 RADIUS 身份源，因此无法添加属性检索序列的 RADIUS 身份源。思科 ISE 在使用 RADIUS 服务器进行身份验证时无法区分不同的错误。RADIUS 服务器针对所有错误都返回 Access-Reject 消息。例如，当在 RADIUS 服务器中找不到用户时，RADIUS 服务器会返回 Access-Reject 消息，而不是返回 User Unknown 状态。

## RADIUS 服务器为所有错误返回相同消息

当在 RADIUS 服务器中未找到某名用户时，RADIUS 服务器会返回一条访问 - 拒绝消息。思科 ISE 提供一个选项可通过管理员门户配置此消息，显示为身份验证失败或未找到用户的消息。但是，对于用户未知和所有失败的情况，此选项均会返回一条未找到用户的消息。

下表列出 RADIUS 身份服务器可能出现的各种失败情况。



表 57: 错误处理

失败情况	失败的原因
身份验证失败	<ul style="list-style-type: none"> <li>• 用户未知。</li> <li>• 用户尝试使用错误的验证码登录。</li> <li>• 用户登录时长过期。</li> </ul>
处理失败	<ul style="list-style-type: none"> <li>• RADIUS 服务器在思科 ISE 中配置错误。</li> <li>• RADIUS 服务器不可用。</li> <li>• 检测到 RADIUS 包错误。</li> <li>• 发送或接收 RADIUS 服务器包期间出现问题。</li> <li>• 超时。</li> </ul>
未知用户	身份验证失败，并且 Fail on Reject 选项设置为 False。

## Safeword 服务器支持特殊用户名格式

Safeword 令牌服务器支持使用以下用户名格式进行身份验证：

Username—Username, OTP

思科 ISE 一收到身份验证请求，便会解析用户名并将其转换为以下用户名：

Username—Username

SafeWord 令牌服务器同时支持这两种格式。思科 ISE 适用于各种令牌服务器。在配置 SafeWord 服务器时，您必须选中思科 ISE 的管理门户中的 SafeWord Server 复选框，以解析用户名并将其转换为指定格式。在将请求发送到 RADIUS 令牌服务器之前，系统会在 RADIUS 令牌服务器身份源中执行此转换。

## RADIUS 令牌服务器中的身份验证请求和响应

当思科 ISE 向支持 RADIUS 的令牌服务器转发身份验证请求时，RADIUS 身份验证请求包含以下属性：

- 用户名（RADIUS 属性 1）
- 用户密码（RADIUS 属性 2）
- NAS IP 地址（RADIUS 属性 4）

思科 ISE 预期收到以下任一响应：

- 接受访问：无需任何属性，但是响应可能包含根据 RADIUS 令牌服务器配置的各种属性。

- 拒绝访问：无需任何属性。
- 质询访问：每个 RADIUS RFC 所需的属性如下：
  - 状态（RADIUS 属性 24）
  - 回复信息（RADIUS 属性 18）
  - 以下一个或多个属性：供应商特定、空闲超时（RADIUS 属性 28）、会话超时（RADIUS 属性 27）、代理状态（RADIUS 属性 33）质询访问中不允许使用任何其他属性。

## RADIUS 令牌身份源设置

### 相关主题

[RADIUS 令牌身份源](#)，第 382 页

[添加 RADIUS 令牌服务器](#)，第 386 页

## 添加 RADIUS 令牌服务器

### 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** 选择在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 **管理 (Administration)** > **外部身份源 (External Identity Sources)** > **RADIUS 令牌 (RADIUS Token)** > **添加 (Add)**。

**步骤 2** 在 **General** 和 **Connection** 选项卡中输入值。

**步骤 3** 点击 **Authentication** 选项卡。

通过此选项卡，您可以控制 RADIUS 令牌服务器对 Access-Reject 消息的响应。此响应可能意味着凭证无效或用户未知。思科 ISE 收到以下其中一个响应：Failed authentication 或 User not found。通过此选项卡，您可以启用身份缓存和设置缓存的老化时间。您还可以配置请求密码的提示。

- 如果您要将从 RADIUS 令牌服务器收到的 Access-Reject 响应处理为失败身份验证，请点击将拒绝视为“身份验证失败” (Treat Rejects as ‘authentication failed’) 单选按钮。
- 如果您要将从 RADIUS 令牌服务器收到的 Access-Reject 响应处理为未知用户失败，请点击将拒绝视为“未找到用户” (Treat Rejects as ‘user not found’) 单选按钮。

**步骤 4** 点击 **Authorization** 选项卡。

通过此选项卡，您可以配置该属性的显示名称。该属性是 RADIUS 令牌服务器向思科 ISE 发送 Access-Accept 响应时返回的属性。此属性可用于授权策略条件。默认值为 CiscoSecure-Group-Id。

**注释** 如果要从外部 ID 源发送 Access-Accept 中的任何属性，则外部 ID 源需要发送 <ciscoavpair> 作为属性名称，值格式为 ACS:<attrname>=<attrvalue>，其中 <attrname> 是在授权 (Authorization) 选项卡中配置的。

步骤 5 点击提交。

## 删除 RADIUS 令牌服务器

### 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。
- 确保您未选择身份源序列中的 RADIUS 令牌服务器。如果您选择身份源序列中的 RADIUS 令牌服务器，删除操作将失败。

**步骤 1** 选择在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > RADIUS 令牌 (RADIUS Token)**。

**步骤 2** 选中要删除的 RADIUS 令牌服务器旁边的复选框，然后点击 **Delete**。

**步骤 3** 点击 **OK** 以删除您已选择的 RADIUS 令牌服务器。

如果您选择删除多个 RADIUS 令牌服务器，且其中一个服务器用于身份源序列，则删除操作将失败，任何 RADIUS 令牌服务器都不会被删除。

## RSA 身份源

思科 ISE 支持 RSA SecurID 服务器作为外部数据库。RSA SecurID 双因素身份验证由用户的 PIN 和单独注册的 RSA SecurID 令牌组成，该令牌基于时间代码算法生成一次性令牌代码。其他令牌代码按固定时间间隔（通常每 30 或 60 秒）生成。RSA SecurID 服务器会验证此动态身份验证代码。每个 RSA SecurID 令牌都是唯一的，并且无法根据以往令牌预测未来令牌的值。因此，在提供正确的令牌代码与 PIN 时，大致可以确定该人员是有效用户。因此，RSA SecurID 服务器提供的身份验证机制比传统可重用密码更可靠。

思科 ISE 支持以下 RSA 身份源：

- RSA ACE/Server 6.x 系列
- RSA Authentication Manager 7.x 和 8.0 系列

您可以通过以下任何一种方式与 RSA SecurID 身份验证技术集成：

- 使用 RSA SecurID 代理：用户通过 RSA 本地协议使用其用户名和密码进行身份验证。
- 使用 RADIUS 协议：用户通过 RADIUS 协议使用其用户名和密码进行身份验证。

思科 ISE 中的 RSA SecurID 令牌服务器通过使用 RSA SecurID 代理与 RSA SecurID 身份验证技术相连接。

思科 ISE 仅支持一个 RSA 领域。

## 思科 ISE 和 RSA SecurID 服务器集成

以下是将思科 ISE 与 RSA SecurID 服务器连接所涉及的两个管理角色：

- RSA 服务器管理员：配置和维护 RSA 系统与集成
- 思科 ISE 管理员：将思科 ISE 配置为连接到 RSA SecurID 服务器并维护配置

本节介绍将思科 ISE 与 RSA SecurID 服务器连接作为外部身份源所涉及的流程。有关 RSA 服务器的更多信息，请参考 RSA 文档。

### 思科 ISE 中的 RSA 配置

RSA 管理系统生成 `sdconf.rec` 文件，RSA 系统管理员将为您提供此文件。您可以通过此文件在领域中添加思科 ISE 服务器作为 RSA SecurID 代理。您必须浏览至此文件并将其添加至思科 ISE 中。通过复制过程，主要思科 ISE 服务器将此文件分发至所有辅助服务器。

### 针对 RSA SecurID 服务器进行的 RSA 代理身份验证

在所有思科 ISE 服务器上安装 `sdconf.rec` 文件之后，RSA 代理模块进行初始化，并且每个思科 ISE 服务器上都将使用 RSA 生成的凭证进行身份验证。在部署中的每个思科 ISE 服务器上的代理都成功通过身份验证之后，RSA 服务器和代理模块将一起下载 `securid` 文件。此文件位于思科 ISE 文件系统中，而且是在 RSA 代理定义的已知位置。

### 思科 ISE 分布式环境中的 RSA 身份源

管理分布式思科 ISE 环境中的 RSA 身份源涉及以下操作：

- 将主服务器上的 `sdconf.rec` 和 `sdopts.rec` 文件分布到辅助服务器。
- 删除 `securid` 和 `sdstatus.12` 文件。

### 思科 ISE 部署中的 RSA 服务器更新

在思科 ISE 中添加 `sdconf.rec` 文件后，RSA SecurID 管理员可能在停用 RSA 服务器或添加新的 RSA 辅助服务器时更新 `sdconf.rec` 文件。RSA SecurID 管理员将为您提供更新的文件。您可以使用更新的文件重新配置思科 ISE。在思科 ISE 中的复制流程将更新的文件分布到部署中的辅助思科 ISE 服务器。思科 ISE 首先更新文件系统中的文件，然后与 RSA 代理模块协调，酌情逐步执行重启流程。更新 `sdconf.rec` 文件时，将重置（删除）`sdstatus.12` 和 `securid` 文件。

### 覆盖自动 RSA 路由

一个领域中可以有不止一个 RSA 服务器。`sdopts.rec` 文件执行负载均衡器的职责。思科 ISE 服务器和 RSA SecurID 服务器通过代理模块运行。位于思科 ISE 上的代理模块维护一分基于成本的路由表以充分利用领域中的 RSA 服务器。但是，您可以通过 Admin 门户使用名称为 `sdopts.rec` 的文本文件

为该领域的每个思科 ISE 服务器进行手动配置，以选择覆盖此路由。有关如何创建此文件的信息，请参阅 RSA 文档。

## RSA 节点密钥重置

SecurID 文件是秘密节点密钥文件。RSA 经过初始设置后，会使用密钥验证代理。位于思科 ISE 中的 RSA 代理第一次成功对 RSA 服务器进行身份验证后，会在客户端计算机上创建一个名为 SecurID 的文件，并会使用该文件确保在设备之间交换的数据有效。有时，可能必须从部署中的特定思科 ISE 服务器或一组服务器中删除 SecurID 文件（例如，在 RSA 服务器上重置密钥之后）。可以使用思科 ISE 管理门户从该领域的思科 ISE 服务器中删除此文件。思科 ISE 中的 RSA 代理在下次成功进行身份验证时，会创建新的 SecurID 文件。



**注释** 如果在升级到最新版本的思科 ISE 之后，身份验证失败，请重置 RSA 密钥。

## RSA 自动可用性重置

sdstatus.12 文件提供有关领域中的 RSA 服务器可用性的信息。例如，它提供有关哪些服务器处于活动状态和哪些已关闭的信息。代理模块与领域中的 RSA 服务器协作维护此可用性状态。此信息在 sdstatus.12 文件中连续列出，此文件位于思科 ISE 文件系统中的常见位置。有时，此文件会变成旧文件，而当前状态未反映在此文件中。您必须删除此文件，以便可以重新创建当前状态。您可以使用管理门户从特定领域的特定思科 ISE 服务器中删除此文件。思科 ISE 与 RSA 代理协调并确保正确的重新启动阶段化。

每当重置 securid 文件或者更新 sdconf.rec 或 sdopts.rec 文件时，便会删除 sdstatus.12 文件。

## RSA SecurID 身份源设置

### RSA 提示设置

下表介绍 **RSA 提示 (RSA Prompts)** 选项卡上的字段。

表 58: RSA 提示设置

字段名称	使用指南
<b>Enter Passcode Prompt</b>	输入文本字符串以获取密码。
<b>Enter Next Token Code</b>	输入文本字符串以请求下一个令牌。
<b>Choose PIN Type</b>	输入文本字符串以请求 PIN 类型。
<b>Accept System PIN</b>	输入文本字符串以接受系统生成的 PIN。
<b>Enter Alphanumeric PIN</b>	输入文本字符串以请求字母数字 PIN。

字段名称	使用指南
<b>Enter Numeric PIN</b>	输入文本字符串以请求数字 PIN。
<b>Re-enter PIN</b>	输入文本字符串以请求用户重新输入 PIN。

### RSA 消息设置

下表介绍 **RSA 消息 (RSA Messages)** 选项卡上的字段。

表 59: RSA 消息设置

字段名称	使用指南
<b>Display System PIN Message</b>	输入文本字符串以编辑系统 PIN 消息。
<b>Display System PIN Reminder</b>	输入文本字符串以通知用户记住新 PIN。
<b>Must Enter Numeric Error</b>	输入一条消息，指导用户仅输入数字作为 PIN。
<b>Must Enter Alpha Error</b>	输入一条消息，指导用户仅输入字母数字字符作为 PIN。
<b>PIN Accepted Message</b>	输入在系统接受用户的 PIN 时用户所看到的消息。
<b>PIN Rejected Message</b>	输入在系统拒绝用户的 PIN 时用户所看到的消息。
<b>User Pins Differ Error</b>	输入在用户输入错误 PIN 时所看到的消息。
<b>System PIN Accepted Message</b>	输入在系统接受用户的 PIN 时用户所看到的消息。
<b>Bad Password Length Error</b>	输入用户指定的 PIN 不属于在 PIN 长度策略中指定的范围时用户所看到的消息。

### 相关主题

[RSA 身份源](#)，第 387 页

[思科 ISE 和 RSA SecurID 服务器集成](#)，第 388 页

[添加 RSA 身份源](#)，第 390 页

## 添加 RSA 身份源

要创建 RSA 身份源，必须导入 RSA 配置文件 (sdconf.rec)。必须从 RSA 管理员那里获取 sdconf.rec 文件。要执行此任务，您必须是超级管理员或系统管理员。

添加 RSA 身份源需要执行以下任务：

## 导入 RSA 配置文件

必须导入 RSA 配置文件，才能在思科 ISE 中添加 RSA 身份源。

**步骤 1** 选择在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > RSA SecurID > 添加 (Add)**。

**步骤 2** 点击 **Browse**，从正运行客户端浏览器的系统中选择新建或更新的 sdconf.rec 文件。

首次创建 RSA 身份源时，Import new sdconf.rec file 字段为必填字段。从那以后，可以用更新的 sdconf.rec 文件替换现有的 sdconf.rec 文件，但替换现有文件是可选操作。

**步骤 3** 以秒为单位输入服务器超时值。在超时之前，思科 ISE 将在指定的时间内等待 RSA 服务器做出响应。该值可以是 1 至 199 之间的任意整数。默认值为 30 秒。

**步骤 4** PIN 发生更改时，选中 **Reauthenticate on Change PIN** 复选框，强制执行重新验证。

**步骤 5** 点击 **Save**。

思科 ISE 也支持以下场景：

- 为思科 ISE 服务器配置选项文件，重置 SecurID 和 sdstatus.12 文件。
- 为 RSA 身份源配置身份验证控制选项。

## 为思科 ISE 服务器配置选项文件并重置 SecurID 和 sdstatus.12 文件

**步骤 1** 登录思科 ISE 服务器。

**步骤 2** 选择**管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > RSA SecurID > 添加 (Add)**。

**步骤 3** 点击 **RSA Instance Files** 选项卡。

此页面列出您的部署中所有思科 ISE 服务器的 sdopts.rec 文件。

**步骤 4** 点击特定思科 ISE 服务器 sdopts.rec 文件旁边的单选按钮，然后点击 **Update Options File**。

Current File 区域会显示现有文件。

**步骤 5** 选择如下选项之一：

- Use the Automatic Load Balancing status maintained by the RSA agent - 如果希望 RSA 代理自动管理负载均衡，请选择此选项。
- Override the Automatic Load Balancing status with the sdopts.rec file selected below - 如果想要根据您的具体需求手动配置负载均衡，请选择此选项。如果选择此选项，则必须点击**浏览 (Browse)**，然后从运行客户端浏览器的系统选择新的 sdopts.rec 文件。

步骤 6 点击 **OK**。

步骤 7 点击与思科 ISE 服务器对应的行以重置该服务器的 securid 和 sdstatus.12 文件：

- a) 点击下拉箭头，然后在“重置 securid 文件” (Reset securid File) 列和“重置 sdstatus.12 文件” (Reset sdstatus.12 File) 列中选择提交时删除 (**Remove on Submit**)。

注释 Reset sdstatus.12 File 字段隐藏在您的视线之外。在最内部的框中使用垂直和水平滚动条，向下滚动，然后向右滚动以查看此字段。

- b) 在此行中点击**保存 (Save)** 以保存更改。

步骤 8 点击**保存 (Save)**。

## 为 RSA 身份源配置身份验证控制选项

您可以指定思科 ISE 如何定义身份验证失败和启用身份缓存。RSA 身份源不会区分“Authentication failed”和“User not found”错误，并且会发送 Access-Reject 响应。

您可以定义在处理请求和报告失败时思科 ISE 应如何处理此类失败。身份缓存让思科 ISE 可以第二次处理在思科 ISE 服务器上验证失败的请求。缓存中具有从上一次身份验证检索的结果和属性。

### 配置 RSA 提示

思科 ISE 允许您配置系统在处理发送给 RSA SecurID 服务器的请求时向用户显示的 RSA 提示。

#### 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 选择在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > RSA SecurID**。

步骤 2 点击 **Prompts**。

步骤 3 输入“RSA SecurID 身份源设置”中所述的值。

步骤 4 点击**提交**。

### 配置 RSA 消息

通过思科 ISE，您可以配置在处理发送到 RSA SecurID 服务器的请求时向用户显示的消息。

#### 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 选择在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > RSA SecurID**。



步骤 2 点击 **Prompts**。

步骤 3 点击 **Messages** 选项卡。

步骤 4 输入“RSA SecurID 身份源设置”中所述的值。

步骤 5 点击提交。

---

## 身份源序列

身份源序列定义思科 ISE 在不同数据库中查找用户凭证的顺序。

如果您在多个连接到思科 ISE 的数据库中有用户信息，您可以定义您希望思科 ISE 在这些身份源中查找信息的顺序。找到匹配后，思科 ISE 不会继续查找，而是评估证书，将结果返回给用户。此策略是第一个匹配策略。

## 创建身份源序列

### 开始之前

确保您已经在思科 ISE 中配置了外部身份源。

要执行以下任务，您必须是超级管理员或系统管理员。

要允许访客用户通过本地 WebAuth 进行身份验证，必须同时配置访客门户身份验证源和身份源序列，使它们包含相同的身份存储区。

---

步骤 1 选择 **管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences) > 添加 (Add)**。

步骤 2 输入身份源序列的名称。您还可以输入可选的说明。

步骤 3 选中 **Select Certificate Authentication Profile** 复选框并为基于证书的身份验证选择证书身份验证配置文件。

步骤 4 在**选定列表 (Selected List)** 字段中选择您希望包括在身份源序列中的数据库。

步骤 5 在**选定列表 (Selected List)** 字段中重新调整数据库的顺序，调整为您希望思科 ISE 搜索数据库的顺序。

步骤 6 如果无法访问所选身份库进行身份验证，请在 **高级搜索列表** 区域中选择以下选项之一：

- 请勿访问序列中的其他库并将“**AuthenticationStatus**”属性设置为“**ProcessError**”
- 将用户视为未找到，然后继续到序列中的下一个库

在处理请求时，思科 ISE 会按照序列搜索这些身份源。确保“**选定列表**” (Selected list) 字段所列出的身份源的顺序是您希望思科 ISE 搜索身份源的顺序。

步骤 7 点击 **Submit** 创建您可以稍后在策略中使用的身份源序列。

---

## 删除身份源序列

您可以删除不再在策略中使用的身份源序列。

### 开始之前

- 确保您即将删除的身份源序列未在任何身份验证策略中使用。
- 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** 选择管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences)。

**步骤 2** 选中要删除的一个或多个身份源序列旁边的复选框，然后点击 **Delete**。

**步骤 3** 点击 **OK** 删除一个或多个身份源序列。

## 报告中的身份源详细信息

思科 ISE 通过 Authentications dashlet 报告和 Identity Source 报告提供关于身份源的信息。

## 身份验证面板

在身份验证面板中，您可以逐步向下展开，找到包括故障原因在内的更多信息。

下图显示 Authentications 页面，并突出显示您必须点击才能深入了解详细信息的放大镜图标。

图 19: Authentications 页面

Time	Status	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Nov 15, 11 03:01:21.508 PM	✓	uma	00:00:00:00:00:81		Switches	2222	PermitAccess
Nov 15, 11 03:01:20.717 PM	✓	uma	00:00:00:00:00:81		Switches	2222	PermitAccess
Nov 15, 11 03:01:20.359 PM	✓	uma	00:00:00:00:00:81		Switches	2222	PermitAccess
Nov 15, 11 03:01:19.952 PM	✓	uma	00:00:00:00:00:81		Switches	2222	PermitAccess
Nov 15, 11 03:01:19.252 PM	✓	uma	00:00:00:00:00:81		Switches	2222	PermitAccess
Nov 15, 11 03:01:19.089 PM	✓	uma	00:00:00:00:00:81		Switches	2222	PermitAccess
Nov 15, 11 03:01:18.474 PM	✓	uma	00:00:00:00:00:81		Switches	2222	PermitAccess
Nov 15, 11 03:01:18.103 PM	✓	uma	00:00:00:00:00:81		Switches	2222	PermitAccess
Nov 15, 11 03:01:17.907 PM	✓	uma	00:00:00:00:00:81		Switches	2222	PermitAccess
Nov 15, 11 03:01:17.479 PM	✓	uma	00:00:00:00:00:81		Switches	2222	PermitAccess

Additional interface details: Refresh: Every 30 seconds, Show: Latest 20 records, within: Last 60 minutes. Last update: Nov 15, 11 03:39:51.374 PM IST. Records shown: 20.

## 身份源报告

思科 ISE 提供包含身份源相关信息的各种报告。有关这些报告的说明，请参阅“可用报告”一节。

## 网络上已分析的终端

分析器服务可协助识别、查找和确定您的网络上所有终端的功能（在思科 ISE 中叫作身份），而无论其设备类型如何，从而确保和保持对您的企业网络的适当访问。思科 ISE 分析器功能使用大量的探测功能收集您的网络上所有终端的属性，并将这些属性传递至分析服务分析器，此分析器根据已知终端的关联策略和身份组给已知终端分类。

分析器源服务允许管理员通过思科 ISE 中的订用从指定思科源服务器检索新的和已更新的终端分析策略以及作为源的已更新 OUI 数据库。

## 分析器条件设置

下表介绍“分析器条件” (Profiler Condition) 窗口中的字段。此页面的导航路径为：**策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **分析 (Profiling)**。

表 60: 分析器条件设置

字段名称	使用指南
<b>Name</b>	分析器条件的名称。
<b>Description</b>	分析器条件的说明。
<b>Type</b>	选择任何一个预定义类型。
<b>Attribute Name</b>	选择分析器条件所基于的属性。
<b>Operator</b>	选择运算符。
<b>Attribute Value</b>	输入已选择的属性的值。对于包含预定义属性值的属性名称，此选项显示具有预定义值的下拉列表，并且您可以选择值。
<b>System Type</b>	分析条件可以是以下任何一个类型： <ul style="list-style-type: none"> <li>• <b>思科提供 (Cisco Provided)</b>: 在部署时由思科 ISE 提供的分析条件标识为“思科提供” (Cisco Provided)。您不能从系统编辑或删除这些条件。</li> <li>• <b>管理员创建 (Administrator Created)</b>: 您以思科 ISE 管理员身份创建的分析条件标识为“管理员创建” (Administrator Created)。</li> </ul>

### 相关主题

[思科 ISE 分析服务](#)，第 396 页

- [分析器条件](#)，第 415 页
- [分析器源服务](#)，第 442 页
- [创建分析器条件](#)，第 422 页

## 思科 ISE 分析服务

思科身份服务引擎 (ISE) 中的分析服务能够识别连接到网络的设备及其位置。它根据在思科 ISE 中配置的终端分析策略来分析终端。然后，思科 ISE 会根据策略评估的结果，向终端授予访问网络资源的权限。

分析服务：

- 利用 IEEE 802.1X 基于端口的标准身份验证访问控制、MAC 身份验证绕行 (MAB) 身份验证，以及适用于各种规模和复杂性的任何企业网络的网络准入控制 (NAC)，可以实现高效和有效的部署以及对身份验证的持续管理。
- 识别、查找并确定连接的所有网络终端的功能，无论终端类型是什么都如此。
- 防止意外拒绝对某些终端的访问。

## 使用分析服务的终端资产

您可以使用分析服务发现、找到和确定连接到网络的所有终端的功能。无论设备类型如何，都可以确保和维护终端对企业网络的适当访问。

分析服务从网络设备和网络收集终端属性，根据配置文件将终端归到特定组，以及在思科 ISE 数据库中存储终端及其匹配的配置文件。分析服务处理的所有属性都需要在分析器字典中定义。

分析服务识别网络上的每个终端，并根据配置文件将这些终端归入系统中的现有终端身份组，或者归入您在系统中创建的新组。通过对终端分组以及将终端分析策略应用到终端身份组，您可以确定终端到相应终端分析策略的映射。

## 思科 ISE 分析器队列限制配置

思科 ISE 分析器可在短时间内从网络收集大量终端数据。由于某些速度较慢的思科 ISE 组件在处理分析器生成的数据时会产生积压（造成性能下降和稳定性问题），因此这将导致 Java 虚拟机 (JVM) 内存使用率增加。

为确保分析器不会增加 JVM 内存使用率并防止 JVM 内存不足和重新启动，系统会对分析器的以下内部组件应用限制：

- 终端缓存：内部缓存大小有限，当大小超过限制时，必须定期清除（根据最近最少使用的策略）。
- 转发器：分析器收集的终端信息的主入口队列。
- 事件处理程序：用于断开快速组件（该组件会向较慢的处理组件 [通常与数据库查询相关] 提供数据）的连接的内部队列。

### 终端缓存

- maxEndpointsInLocalDb = 100000（缓存中的终端对象数）
- endpointsPurgeIntervalSec = 300（终端缓存清除线程时间间隔，以秒为单位）
- numberOfProfilingThreads = 8（线程数）

限制适用于所有分析器内部事件处理程序。当达到队列大小限制时，会触发监控警报。

### 思科 ISE 分析器队列大小限制

- forwarderQueueSize = 5000（终端集合事件数）
- eventHandlerQueueSize = 10000（事件数）

### 事件处理程序

- NetworkDeviceEventHandler: 除筛选已经缓存的重复网络接入设备 (NAD) IP 地址外，还用于处理网络设备事件。
- ARPCacheEventHandler: 用于处理 ARP 缓存事件。

## Martian IP 地址

Martian IP 地址不会在情景可视性 (Context Visibility) > 终端 (Endpoints) 和工作中心 (Work Centers) > 分析器 (Profiler) > 终端分类 (Endpoint Classification) 窗口中显示，因为 RADIUS 解析器会在这些地址到达分析服务之前将其删除。Martian IP 地址容易受到攻击，因此是安全隐患。但是，出于审核目的，MnT 日志中会显示 Martian IP 地址。此行为在组播 IP 地址的情况下也是如此。有关 Martian IP 地址的详细信息，请参阅

[https://www.cisco.com/assets/sol/sb/Switches\\_Emulators\\_v2\\_3\\_5\\_xx/help/250/index.html#page/tesla\\_250\\_olh/martian\\_addresses.html](https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/250/index.html#page/tesla_250_olh/martian_addresses.html)

## 在思科 ISE 节点中配置分析服务

可以配置分析服务，该服务为您提供正在任何启用思科 ISE 的网络中使用网络资源的所有终端的上下文资产。

可以将分析服务配置为在单一思科 ISE 节点上运行，默认情况下，此节点承担所有管理、监控和策略服务角色。

在分布式部署中，分析服务仅在承担策略服务角色的思科 ISE 节点上运行，不在承担管理和监控角色的其他思科 ISE 节点上运行。

### 步骤 1

步骤 2 选择承担策略服务角色的思科 ISE 节点。

步骤 3 在 Deployment Nodes 页面上点击 **Edit**。

**步骤 4** 在常规设置 (**General Settings**) 选项卡上, 选中**策略服务 (Policy Service)** 复选框。如果取消选中 **Policy Service** 复选框, 会话服务和分析服务复选框均被禁用。

**步骤 5** 执行以下任务:

- a) 选中 **Enable Session Services** 复选框, 运行网络访问、终端安全评估、访客和客户端调配会话服务。
- b) 选中 **Enable Profiling Services** 复选框, 运行分析服务。

**步骤 6** 点击 **Save**, 保存节点配置。

## 分析服务使用的网络探测功能

网络探测功能是一种用于从网络上的终端收集属性或属性集的方法。通过探测功能, 您可以使用思科 ISE 数据库中的终端匹配配置文件创建或更新终端。

思科 ISE 可以使用许多网络探测功能来分析设备, 这些网络探测功能会分析网络上设备的行为并确定设备的类型。网络探测功能可帮助您获取更多网络可视性。

### IP 地址和 MAC 地址绑定

您只能通过在企业网络中使用终端的 MAC 地址来创建或更新终端。如果您在 ARP 缓存中找不到条目, 则可以通过在思科 ISE 中使用 HTTP 数据包的 L2 MAC 地址和 NetFlow 数据包的 IN\_SRC\_MAC 来创建或更新终端。当终端只是一个跃点之隔时, 分析服务依赖于 L2 邻接。当终端是 L2 邻接时, 表明已映射终端的 IP 地址和 MAC 地址, 无需进行 IP-MAC 缓存映射。

如果终端不是 L2 邻接并且间隔多个跃点, 则映射可能不可靠。您收集的 NetFlow 数据包的一些已知属性包括 PROTOCOL、L4\_SRC\_PORT、IPV4\_SRC\_ADDR、L4\_DST\_PORT、IPV4\_DST\_ADDR、IN\_SRC\_MAC、OUT\_DST\_MAC、IN\_SRC\_MAC 和 OUT\_SRC\_MAC。当终端不是 L2 邻接并且间隔多个 L3 跃点时, IN\_SRC\_MAC 属性只能运载 L2 网络设备的 MAC 地址。当在思科 ISE 中启用 HTTP 探测时, 您只能通过使用 HTTP 数据包的 MAC 地址创建终端, 因为 HTTP 请求消息在负载数据中不会运载终端的 IP 地址和 MAC 地址。

思科 ISE 在分析服务中实施 ARP 缓存, 以便您能够可靠地映射终端的 IP 地址和 MAC 地址。为使 ARP 缓存正常运行, 您必须启用 DHCP 探测或 RADIUS 探测。DHCP 和 RADIUS 探测在负载数据中运载终端的 IP 地址和 MAC 地址。DHCP 探测中的 dhcp-requested 地址属性和 RADIUS 探测中的 Framed-IP-address 属性运载终端的 IP 地址, 及其可在 ARP 缓存中映射和存储的 MAC 地址。

### NetFlow 探测功能

思科 ISE 分析器使用思科 IOS NetFlow 版本 9。我们建议使用 NetFlow 版本 9, 因为其具有增强此分析器以支持思科 ISE 分析服务的更多功能。

您可以从支持 NetFlow 的网络访问设备收集 NetFlow 版本 9 属性以在思科 ISE 数据库中创建终端或更新现有终端。您可以将 NetFlow 版本 9 配置为连接终端和更新终端的源与目标 MAC 地址。您还可以创建 NetFlow 属性字典以支持基于 NetFlow 的分析。

有关 NetFlow 版本 9 记录格式的更多信息，请参阅 NetFlow 版本 9 流程-记录格式文档的表 6 “NetFlow 版本 9 字段类型定义”。

此外，思科 ISE 支持低于 5 以下的 NetFlow 版本。如果您在网络使用 NetFlow 版本 5，则只能在接入层主要网络访问设备 (NAD) 上使用版本 5，因为此版本在其他位置无法运行。

思科 IOS NetFlow 版本 5 程序包不包含终端的 MAC 地址。从 NetFlow 版本 5 收集的属性不能直接添加至思科 ISE 数据库。您可以通过使用终端的 IP 地址发现终端，并且通过将网络访问设备的 IP 地址与从 NetFlow 版本 5 属性获取的 IP 地址组合，将 NetFlow Version 5 属性附加到终端上。但是，之前必须已使用 RADIUS 或 SNMP 探测功能发现这些终端。

在早期 NetFlow 版本 5 中，MAC 地址不是 IP 流的组成部分，这就要求您关联从终端缓存中的网络访问设备收集的属性信息，才能用终端 IP 地址分析终端。

有关 NetFlow 版本 5 记录格式的更多信息，请参阅《NetFlow 服务解决方案指南》中表 2 “思科 ISE NetFlow 流程记录和导出格式内容信息”。

## DHCP 探测功能

在思科 ISE 部署中，动态主机配置协议探测功能允许思科 ISE 分析服务仅根据 INIT-REBOOT 和 SELECTING 消息类型的新请求，重新分析终端。虽然系统会处理 RENEWING 和 REBINDING 等其他 DHCP 消息类型，但是这些消息类型不会用于分析终端。在 DHCP 数据包之外解析的任何属性都会映射至终端属性。

### 在 INIT-REBOOT 状态期间生成的 DHCPREQUEST 消息

如果 DHCP 客户端进行检查以验证之前分配和缓存的配置，则客户端不得填写 Server identifier (server-ip) 选项，而应该用之前分配的 IP 地址填写 Requested IP address (requested-ip) 选项，并且在其 DHCPREQUEST 消息中用零填写 Client IP Address (ciaddr) 字段。然后，如果所请求的 IP 地址不正确或客户端位于错误的网络上，则 DHCP 服务器将向该客户端发送 DHCPNAK 消息。

### 在 SELECTING 状态期间生成的 DHCPREQUEST 消息

DHCP 客户端在 Server identifier (server-ip) 选项中插入所选 DHCP 服务器的 IP 地址，用客户端选择的 DHCP OFFER 的 Your IP Address (yiaddr) 字段的值填写 Requested IP address (requested-ip) 选项，并且在“ciaddr”字段中填写零。

表 61: 来自不同状态的 DHCP 客户端消息

-	INIT-REBOOT	SELECTING	RENEWING	REBINDING
广播 / 单播	广播	广播	单播	广播
server-ip	不得填写	必须填写	不得填写	不得填写
requested-ip	必须填写	必须填写	不得填写	不得填写
ciaddr	零	零	IP 地址	IP 地址

## DHCP 桥接模式下的无线 LAN 控制器配置

我们建议您在动态主机配置协议 (DHCP) 桥接模式下配置无线 LAN 控制器 (WLC)，这样您就可以将所有来自无线客户端的 DHCP 数据包转发至思科 ISE。您必须在 WLC Web 界面取消选中“启用 DHCP 代理” (Enable DHCP Proxy) 复选框：**控制器 (Controller) > 高级 (Advanced) > DHCP 主控制器模式 (DHCP Master Controller Mode) > DHCP 参数 (DHCP Parameters)**。您还必须确保 DHCP IP 帮助程序命令指向思科 ISE 策略服务节点。

## DHCP SPAN 探测功能

当在思科 ISE 节点中初始化 DHCP 交换端口分析器 (SPAN) 探测功能时，即可监听网络流量，而该网络流量来自特定接口的网络接入设备。您需要对网络接入设备进行配置，从 DHCP 服务器向思科 ISE 分析器转发 DHCP SPAN 数据包。分析器接收这些 DHCP SPAN 数据包并对其进行分析以抓取终端的属性，而这些属性可用于分析终端。

例如，

```
switch(config)# monitor session 1 source interface Gi1/0/4
switch(config)# monitor session 1 destination interface Gi1/0/2
```

## HTTP 探测功能

在 HTTP 探测中，标识字符串在 HTTP 请求报头字段 **User-Agent** 中进行传输，该字段是可用于创建 IP 类型的分析条件以及检查 Web 浏览器信息的属性。分析器从 **User-Agent** 属性以及请求消息中的其他 HTTP 属性捕获 Web 浏览器信息，并将其添加到终端属性列表。

思科 ISE 同时在端口 80 和端口 8080 上侦听来自 Web 浏览器的通信。思科 ISE 提供许多默认配置文件，这些配置文件内置到系统中以根据 **User-Agent** 属性识别终端。

默认情况下，HTTP 探测器处于启用状态。多个 ISE 服务（例如 CWA、热点、BYOD、MDM 和终端安全评估）依赖于客户端 Web 浏览器的 URL 重定向。重定向的流量包括所连接终端的 RADIUS 会话 ID。当 PSN 终止这些 URL 重定向的流时，它对已解密的 HTTPS 数据具有可视性。即使在 PSN 上禁用 HTTP 探测器，节点也会通过 Web 流量来解析浏览器用户代理字符串，并根据其关联的会话 ID 将数据关联到终端。通过此方法收集浏览器字符串时，数据源将列出为访客门户或 CP（客户端调配），而不是 HTTP 探测器。

## HTTP SPAN 探测功能

思科 ISE 部署中的 HTTP 探测功能随交换端口分析器 (SPAN) 探测功能一起启用时，允许分析器从指定的接口捕获 HTTP 数据包。您可以在端口 80 上使用 SPAN 功能，在该端口上思科 ISE 服务器会侦听来自 Web 浏览器的通信。

HTTP SPAN 收集 HTTP 请求报头消息的 HTTP 属性以及 IP 报头 (L3 报头) 中的 IP 地址，IP 地址可根据 L2 报头中终端的 MAC 地址与某个终端关联。此信息有助于识别具备 IP 功能的不同的移动和便携式设备（例如 Apple 设备）以及安装不同操作系统的计算机。由于思科 ISE 服务器在访客登录或下载客户端调配期间会重定向捕获的数据包，因此能够更加可靠地识别具备 IP 功能的不同的移



动和便携式设备。这样，分析器就可以从请求消息中收集用户-代理属性和其他 HTTP 属性，然后识别设备，例如 Apple 设备。

## 无法在 VMware 上运行的思科 ISE 中收集 HTTP 属性

如果您在 ESX 服务器 (VMware) 上部署思科 ISE，思科 ISE 分析器会收集动态主机配置协议流量，但由于 vSphere 客户端上的配置问题，它不会收集 HTTP 流量。要在 VMware 设置上收集 HTTP 流量，请将您为思科 ISE 分析器创建的虚拟交换机的 Promiscuous Mode 从 Reject（默认设置）改为 Accept，配置安全设置。当为 DHCP 和 HTTP 启用交换端口分析器 (SPAN) 探测功能时，思科 ISE 分析器会同时收集 DHCP 流量和 HTTP 流量。

## pxGrid 探测器

pxGrid 探测器利用思科 pxGrid 从外部源接收终端情景。在早于思科 ISE 2.4 的版本中，思科 ISE 仅充当发布程序，并向外部用户共享各种情景信息，例如会话身份和组信息以及配置元素。当在思科 ISE 2.4 中引入 pxGrid 探测器后，其他解决方案将充当发布程序，思科 ISE 策略服务节点将成为用户。

pxGrid 探测器基于 pxGrid v2 规范并使用终端资产主题 `/topic/com.cisco.endpoint.asset` 和服务名称 `com.cisco.endpoint.asset`。下表显示了主题属性，所有这些属性前面都带有前缀 `asset`。

表 62: 终端资产主题

属性名称	Type	Description
<b>assetId</b>	长	资产 ID
<b>assetName</b>	字符串	资产名称
<b>assetIpAddress</b>	字符串	IP 地址
<b>assetMacAddress</b>	字符串	MAC 地址
<b>assetVendor</b>	字符串	Manufacturer
<b>assetProductId</b>	字符串	产品代码
<b>assetSerialNumber</b>	字符串	序列号
<b>assetDeviceType</b>	字符串	设备类型
<b>assetSwRevision</b>	字符串	软件修订号
<b>assetHwRevision</b>	字符串	硬件修订号
<b>assetProtocol</b>	字符串	协议
<b>assetConnectedLinks</b>	阵列	网络链接对象阵列
<b>assetCustomAttributes</b>	阵列	自定义名称-值对数组

除了通常用于跟踪网络资产的属性（例如设备 MAC 地址 (`assetMacAddress`) 和 IP 地址 (`assetIpAddress`)）之外，该主题还允许供应商将唯一终端信息发布为自定义属性 (`assetCustomAttributes`)。在思科 ISE

中使用终端自定义属性，使主题可扩展到各种使用情形，而无需为通过 pxGrid 共享的每组新的唯一供应商属性更新架构。

## RADIUS 探测功能

您可以将思科 ISE 配置为使用 RADIUS 进行身份验证，您可以定义在客户端服务器交易中使用的共享密钥。利用从 RADIUS 服务器接收的 RADIUS 请求和响应消息，分析器可以收集 RADIUS 属性，用于分析终端。

思科 ISE 可以用作 RADIUS 服务器以及其他 RADIUS 服务器的 RADIUS 代理客户端。充当代理客户端时，它可以使用外部 RADIUS 服务器处理 RADIUS 请求和响应消息。

RADIUS 探测还会收集设备传感器在 RADIUS 记账数据包中发送的属性。有关详细信息，请参阅[思科 IOS 传感器嵌入式交换机收集属性](#)，第 413 页和[支持思科 IOS 传感器的网络访问设备的配置核对表](#)，第 414 页。

默认情况下，即使对于未配置分析服务的系统，RADIUS 探测也会运行，以确保 ISE 可以跟踪终端身份验证和授权详细信息，以便在情景可视性服务中使用。

RADIUS 探测和分析服务还用于跟踪已注册终端的创建和更新时间，以进行清除操作。

表 63: 使用 RADIUS 探测功能收集的常见属性

用户名 (User Name)	正在呼叫站 ID	已呼叫站 ID	成帧的 IP 地址
NAS-IP-Address	NAS-Port-Type	NAS-Port-Id	NAS-Identifier
设备类型 (NAD)	位置 (NAD)	身份验证策略 (Authentication Policy)	授权策略

## 网络扫描 (NMAP) 探测功能

通过思科 ISE，您可以使用 NMAP 安全扫描器检测子网中的设备。您可以在已启用运行分析服务的策略服务节点上启用 NMAP 探测功能。可以在终端分析策略中使用该探测的结果。

每个 NMAP 手动子网扫描都有唯一的数字 ID，用于使用该扫描 ID 更新终端源信息。检测终端时，终端源信息也被更新，表示网络扫描探测功能发现此终端。

NMAP 手动子网扫描对于检测持续连接思科 ISE 网络的设备（例如，已为其分配静态 IP 地址的打印机）很有帮助，因此，这些设备无法被其他探测器发现。

### NMAP 扫描限制

扫描子网会耗费大量资源。扫描子网的过程很漫长，具体取决于子网的规模和密度。活动扫描的数量始终限制为一个扫描，这意味着您一次只能扫描一个子网。在子网扫描期间，您可以随时取消子网扫描。您可以使用 **Click** 按钮查看最新扫描结果链接，了解存储于 **Administration > Identities > Latest Network Scan Results** 位置的最新网络扫描结果。

## 手动 NMAP 扫描

以下 NMAP 命令扫描子网并发送输出至 nmapSubnet.log:

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
--append-output -oX - <subnet>
```

表 64: 用于手动子网扫描的 NMAP 命令

-O	启用操作系统检测
-sU	UDP 扫描
-p <端口范围>	仅扫描指定端口。例如, U:161, 162
oN	正常输出
oX	XML 输出

## NMAP 手动子网扫描的 SNMP 只读社区字符串

只要 NMAP 手动子网扫描发现 UDP 端口 161 在终端上处于打开状态, 该扫描就会使用 SNMP 查询进行扩展, 导致收集更多属性。在 NMAP 手动子网扫描过程中, 网络扫描探测功能会检测 SNMP 端口 161 在设备上是否处于打开状态。如果端口处于打开状态, 则系统会使用 SNMP 版本为 2c 的默认社区字符串 (public) 触发 SNMP 查询。

如果设备支持 SNMP, 并且默认只读社区字符串设置为 public, 则您可以从 MIB 值 “ifPhysAddress” 获取设备的 MAC 地址。

此外, 还可以在分析器配置 (Profiler Configuration) 窗口中为 NMAP 手动网络扫描配置以逗号分隔的其他 SNMP 只读社区字符串。您也可以为 SNMP 版本为 1 和 2c 的 SNMP MIB walk 指定新的只读社区字符串。有关配置 SNMP 只读社区字符串的信息, 请参阅[设置 CoA、SNMP RO 社区和终端属性过滤器](#), 第 408 页。

## 最新网络扫描结果

最新网络扫描结果存储位置为: 管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 最新网络扫描结果 (Latest Manual Network Scan Results)。

最新网络扫描结果终端 (Latest Network Scan Results Endpoints) 页面仅显示检测到的最新终端、其关联终端的配置文件、其 MAC 地址和作为您在任何子网上执行的手动网络扫描结果的静态分配状态。如有必要, 您可以通过此页面编辑从终端子网检测的点以实现更好的分类。

思科 ISE 允许您从已启用运行分析服务的策略服务节点执行手动网络扫描。您必须从您的部署中的主要管理 ISE 节点用户界面选择策略服务节点, 才能从策略服务节点运行手动网络扫描。在任何子网上执行手动网络扫描期间, 网络扫描探测功能都会检测指定子网上的终端、其操作系统并检查 UDP 端口 161 和 162 是否在运行 SNMP 服务。

下面提供了与手动 NMAP 扫描结果相关的其他信息:

- 要检测未知终端, NMAP 应能够通过 NMAP 或支持的 SNMP 扫描获知 IP/MAC 绑定。
- ISE 通过 Radius 身份验证或 DHCP 分析了解已知终端的 IP/MAC 绑定。

- IP/MAC 绑定不会跨部署中的 PSN 节点复制。因此，必须从 PSN 触发手动扫描，此 PSN 在其本地数据库中具有 IP/MAC 绑定（例如，上次对其进行 MAC 地址身份验证的 PSN）。
- NMAP 扫描结果不显示与 NMAP 之前手动或自动扫描的终端相关的任何信息。

## DNS 探测功能

您的思科 ISE 部署中的域名服务 (DNS) 探测功能允许分析器查找终端并获取完全限定域名 (FQDN)。在启用思科 ISE 的网络中检测到终端之后，系统会从 NetFlow、DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP 探测功能收集一系列终端属性。

当您首次在独立环境或分布式环境中部署思科 ISE 时，系统将提示您运行设置实用程序以配置思科 ISE 设备。当您运行实用程序设置时，您要配置域名系统 (DNS) 域和主要名称服务器（主要 DNS 服务器），其中您可以配置一个或多个名称服务器。您也可以在部署思科 ISE 之后，随时使用 CLI 命令更改或添加 DNS 名称服务器。

### DNS FQDN 查找

在可执行 DNS 查找前，必须随 DNS 探测功能一起启用以下一个探测功能：DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP。这将允许分析器中的 DNS 探测功能对您在思科 ISE 部署中定义的指定名称服务器执行 DNS 反向查找（FQDN 查找）。系统会为终端在属性列表中添加新属性，可将此属性用于终端分析策略评估。FQDN 是系统 IP 字典中存在的新属性。您可以创建终端分析条件以验证 FQDN 属性及其用于分析的值。以下是 DNS 查找和收集这些属性的探测功能需要的特定终端属性：

- dhcp-requested-address 属性 - DHCP 和 DHCP SPAN 探测功能收集的属性。
- SourceIP 属性 - HTTP 探测功能收集的属性。
- Framed-IP-Address 属性 - RADIUS 探测功能收集的属性
- cdpCacheAddress 属性 - SNMP 探测功能收集的属性

### 在桥接模式下通过 **Inline Posture** 节点部署执行 DNS 查找

要在桥接模式下配合 **Inline Posture** 部署使用域名服务探测功能，您必须为无线 LAN 控制器 (WLC) 配置在 RADIUS 消息中发送的 `callStationIdType` 信息。RADIUS 消息中的 `Framed-IP-Address` 属性不包含 MAC 地址格式的呼叫站 ID 类型。因此，RADIUS 消息不能与终端的 MAC 地址关联，DNS 探测功能也无法执行反向 DNS 查找。为了分析终端，您必须在思科 ISE 中启用 RADIUS 和 DNS 探测，然后将 WLC 配置为在 RADIUS 消息中以 MAC 地址格式（而不是当前的 IP 地址格式）发送呼叫站 ID。必须将 WLC 配置为在 RADIUS 消息中以 MAC 地址格式（而不是当前的 IP 地址格式）发送呼叫站 ID。在 WLC 中配置 `callStationIdType` 后，该配置会使用选定的呼叫站 ID 与 RADIUS 服务器及其他应用进行通信。该配置引发终端身份验证后，DNS 探测功能会根据指定名称服务器执行反向 DNS 查找（FQDN 查找）并更新终端的 FQDN。

## 在 WLC Web 界面中配置呼叫站 ID 类型

可以使用 WLC Web 界面配置呼叫站 ID 类型信息。可以转到 WLC Web 界面的 Security 选项卡，在 RADIUS Authentication Servers 页面配置呼叫站 ID。默认情况下，WLC 用户界面中的 MAC Delimiter 字段设置为 Colon。

关于如何在 WLC Web 界面中进行配置的详细信息，请参阅《思科无线 LAN 控制器配置指南》7.2 版第 6 章“配置安全解决方案”。

关于如何使用 `config radius callStationIdType` 命令在 WLC CLI 中进行配置的详细信息，请参阅《思科无线 LAN 控制器命令参考指南》7.2 版第 2 章“控制器命令”。

**步骤 1** 登录无线 LAN 控制器用户界面。

**步骤 2** 点击 **Security**。

**步骤 3** 展开 **AAA**，然后选择 **RADIUS > 身份验证 (Authentication)**。

**步骤 4** 从 Call Station ID Type 下拉列表选择 **System MAC Address**。

**步骤 5** 在 FIPS 模式下运行思科 ISE 时，请选中 **AES Key Wrap** 复选框。

**步骤 6** 从 MAC Delimiter 下拉列表选择 **Colon**。

## SNMP 查询探测功能

除在“编辑节点” (Edit Node) 页面中配置 SNMP 查询探测以外，您还必须在以下位置配置其他简单管理协议设置：**管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)**。

您可以在 Network Devices 列表页面中的新网络接入设备 (NAD) 中配置 SNMP 设置。在 SNMP 查询探测中或在网络接入设备中的 SNMP 设置中指定的轮询间隔按定期间隔查询 NAD。

您可以根据以下配置为特定 NAD 打开和关闭 SNMP 查询：

- 在收到表明链路已启动并新增 MAC 的通知时打开或关闭 SNMP 查询
- 针对思科发现协议信息，在收到表明链路已启动并新增 MAC 的通知时打开或关闭 SNMP 查询
- 默认情况下，SNMP 查询计时器针对每个交换机每小时进行一次计时

对于 iDevice 和其他不支持 SNMP 的移动设备，可以通过 ARP 表发现 MAC 地址，而该表可由 SNMP 查询探测功能从网络接入设备进行查询。

## 使用 SNMP 查询的思科发现协议支持

当在网络设备上配置 SNMP 设置时，必须确保网络设备的所有端口上均启用思科发现协议（默认情况下）。如果在网络设备的任意端口上禁用思科发现协议，则可能会因为缺少有关所有已连接终端的思科发现协议信息而无法进行正确的分析。可以通过在网络设备上使用 `cdp run` 命令来全局启用思科发现协议，或通过网络接入设备的任意接口上使用 `cdp enable` 命令来启用思科发现协议。要禁用网络设备或接口上的思科发现协议，请在命令开头使用 `no` 关键字。

## 使用 SNMP 查询的链路层发现协议支持

思科 ISE 分析器使用 SNMP 查询收集 LLDP 属性。您也可以使用 RADIUS 探测功能从思科 IOS 传感器（嵌入网络设备中）收集 LLDP 属性。以下是默认 LLDP 配置设置，您可以使用这些设置在网络访问设备上配置 LLDP 全局配置命令和 LLDP 接口配置命令。

表 65: 默认 LLDP 配置

属性	设置
LLDP 全局状态	已禁用
LLDP 维持时间 (丢弃前)	120 秒
LLDP 计时器 (数 据包更新频率)	30 秒
LLDP 重新初始化 延迟	2 秒
LLDP tlv-select	启用, 发送和接收所有 TLV。
LLDP 接口状态	已启用
LLDP 接收	已启用
LLDP 传输	已启用
LLDP med-tlv 选择	启用, 发送所有 LLDP-MED TLV

### 以单个字符显示的 CDP 和 LLDP 功能代码

终端的 Attribute List 显示 lldpCacheCapabilities 和 lldpCapabilitiesMapSupported 属性的单一字符值。这些值是针对运行 CDP 和 LLDP 的网络访问设备显示的功能代码。

#### 示例 1

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

#### 示例 2

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

#### 示例 3

```
Switch#show cdp neighbors
Capability Codes:
```

```

R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,
r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay
...
Switch#

Switch#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
...
Switch#

```

## SNMP 陷阱探测功能

SNMP 陷阱探测功能能够接收来自支持 MAC 通知、LinkUp、LinkDown 和 INFORM 的网络访问设备的信息。SNMP 陷阱探针能够在端口连接或中断以及终端与您的网络断开连接或进行连接时接收来自特定网络访问设备的信息。

要使 SNMP 陷阱探测功能充分运行并创建终端，您必须启用 SNMP 查询，从而在收到陷阱时，使 SNMP 查询探测功能在网络访问设备的特定端口上触发轮询事件。要使此功能充分运行，您应该配置网络访问设备和 SNMP 陷阱。



**注释** 思科 ISE 不支持从无线 LAN 控制器 (WLC) 和接入点 (AP) 接收的 SNMP 陷阱。

## 为每个思科 ISE 节点配置探测功能

您可以在 Profiling Configuration 选项卡上为您的部署中承担策略服务角色的每个思科 ISE 节点配置一个或多个探测功能，其中节点可能是以下节点：

- 独立节点：如果在默认承担所有管理、监控和策略服务角色的单一节点中部署了思科 ISE。
- 多个节点：如果在部署中部署了承担策略服务角色的多个节点。



**注释** 并非所有探测都默认处于启用状态。某些探测器即使未通过复选标记显式启用，也会部分启用。目前，分析配置对于每个 PSN 来说是唯一的。我们建议为部署中的每个 PSN 配置相同的分析器配置设置。

### 开始之前

您只能从管理节点为每个思科 ISE 节点配置探测功能，在分布式部署的辅助管理节点上无法执行此配置。

- 步骤 1 依次选择在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择管理 (Administration) > 系统 (System) > 部署 (Deployment)。
- 步骤 2 选择承担策略服务角色的思科 ISE 节点。
- 步骤 3 在 Deployment Nodes 页面上点击 **Edit**。
- 步骤 4 在常规设置 (General Settings) 选项卡上，选中策略服务 (Policy Service) 复选框。如果取消选中 Policy Service 复选框，会话服务和分析服务复选框均被禁用。
- 步骤 5 选中 **Enable Profiling Services** 复选框。
- 步骤 6 点击 **Profiling Configuration** 选项卡。
- 步骤 7 为每个探测功能配置相应值。
- 步骤 8 点击 **Save** 以保存探测功能配置。

## 设置 CoA、SNMP RO 社区和终端属性过滤器

思科 ISE 允许全局配置在 Profiler Configuration 页面中发布授权更改 (CoA)，从而增强分析服务对已通过身份验证的终端的控制。

此外，您还可以在 Profiler Configuration 页面中为 NMAP 手动网络扫描配置以逗号分隔的其他 SNMP 只读社区字符串。SNMP RO 社区字符串使用的顺序与它们在当前自定义 SNMP 社区字符串字段中显示的顺序相同。

您还可以在 Profiler Configuration 页面中配置终端属性筛选。

步骤 1 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 分析 (Profiling)。

步骤 2 选择以下设置之一配置 CoA 类型：

- **No CoA** (默认) - 可以使用此选项禁用 CoA 的全局配置。此设置会根据终端分析策略覆盖任何已配置的 CoA。如果只是为了获得可见性，请保留默认值无 CoA (No CoA)。
- **Port Bounce** - 如果交换机端口只存在一个会话，您可以使用此选项。如果端口存在多个会话，则使用 Reauth 选项。如果目标是根据配置文件更改立即更新访问策略，请选择端口退回 (Port Bounce) 选项，这将确保重新授权所有无客户端终端，并在需要时刷新 IP 地址。
- **Reauth** - 您可以使用此选项强制重新验证分析时已通过身份验证的终端。如果在重新授权当前会话后预计不会发生 VLAN 或地址更改，请选择重新验证 (Reauth) 选项。

**注释** 如果一个端口有多个活动会话，分析服务会通过重新验证 (Reauth) 选项发布 CoA，即便您已使用端口退回 (Port Bounce) 选项配置了 CoA 也是如此。该功能可避免断开其他会话，而使用端口退回 (Port Bounce) 选项就有可能发生这种情况。



**步骤 3** 在更改自定义 SNMP 社区字符串 (Change Custom SNMP Community Strings) 字段中输入新的 SNMP 社区字符串（用逗号分隔）以执行 NMAP 手动网络扫描，然后在确认自定义 SNMP 社区字符串 (Confirm Custom SNMP Community Strings) 字段中重新输入字符串进行确认。

默认 SNMP 社区字符串为 *public*。点击当前自定义 SNMP 社区字符串 (Current Custom SNMP Community Strings) 部分中的显示 (Show) 以验证这一点。

**步骤 4** 选中 **Endpoint Attribute Filter** 复选框启用终端属性筛选。

启用终端属性过滤器 (EndPoint Attribute Filter) 后，思科 ISE 分析器仅保留允许的属性并丢弃所有其他属性。有关详细信息，请参阅[过滤器终端属性的全局设置](#)，第 412 页和[针对 ISE 数据库持久性和性能的属性过滤器](#)，第 411 页两节。作为最佳实践，我们建议您在生产部署中启用终端属性过滤器 (EndPoint Attribute Filter)。

**步骤 5** 点击保存 (Save)。

## 对已通过身份验证的终端的授权更改全局配置

您可以使用全局配置功能以通过使用默认的“无 CoA” (No CoA) 选项禁用授权更改 (CoA)，或使用端口退回和重新身份验证选项启用 CoA。如果您在思科 ISE 中配置了 CoA 的端口回退，则分析服务可能仍会发出“CoA 例外”一节描述的其他 CoA。

所选的全局配置仅在没有更具体的设置的情况下规定默认 CoA 行为。请参阅[每个终端分析策略的授权更改配置](#)，第 428 页。

您可以使用 RADIUS 探测或监控角色 REST API 对终端进行身份验证。您可以启用 RADIUS 探测获得更快的性能。如果您已启用 CoA，我们建议您在思科 ISE 应用中启用 RADIUS 探测时同时启用您的 CoA 配置以获得更快的性能。通过使用已收集的 RADIUS 属性，分析服务可发出终端适当的 CoA。

如果您已在思科 ISE 应用中禁用 RADIUS 探测，那么您可以通过监控角色 REST API 来发出 CoA。这将允许分析服务支持更多种类的终端。在分布式部署中，您的网络必须至少有一个作为监控角色的思科 ISE 节点从而通过监控角色 REST API 发出 CoA。

因为主要和次要监控节点都具有相同的会话目录信息，思科 ISE 会随意指定主要或次要监控节点作为您分布式部署中 REST 查询的默认目标。

## 发出授权更改的使用案例

分析服务在以下情况下会发出授权更改：

- 删除终端：当从“终端” (Endpoints) 页面删除终端并且从网络上断开或移除该终端时。
- 配置例外操作：如果您根据配置文件配置了例外操作，导致该终端出现异常或不可接受的事件。分析服务会通过发出 CoA 将该终端移至相应的静态配置文件。
- 首次分析某个终端：当在未静态分配某个终端的情况下首次分析该终端时；例如配置文件从未知配置文件变为已知配置文件。
  - 终端身份组已更改：当为授权策略使用的终端身份组添加或删除终端时。

当某个终端身份组中有任何变更并且在以下情况下将该终端身份组用于授权策略时，分析服务会发出 CoA：

- 动态分析终端时，终端身份组因这些终端而变更
- 当某个动态终端的静态分配标志设置为 `true` 时，终端身份组变更
- 终端身份组策略已变更并且此策略用于授权策略中：当终端分析策略变更，并且用于授权策略的逻辑配置文件中包含该策略时。终端分析策略可能因分析策略匹配或终端被静态分配至与逻辑配置文件关联的终端分析策略而改变。在这两种情况下，都只有在将终端分析策略用于授权策略时，分析服务才会发出 CoA。

## 发出授权更改的豁免

当终端身份组发生更改且静态分配已设置为 `true` 时，分析服务不会发出 CoA。

出于以下原因，思科 ISE 不会发出 CoA：

- An Endpoint disconnected from the network - 当发现与网络断开连接的终端时。
- Authenticated wired (Extensible Authentication Protocol) EAP - 当发现支持 EAP 且经过身份验证的有线终端时。
- Multiple active sessions per port - 当一个端口上存在多个活动会话时，分析服务会发出带 Reauth 选项的 CoA，即使您已配置带 Port Bounce 选项的 CoA 亦如此。
- Packet-of-Disconnect CoA (Terminate Session) when a wireless endpoint is detected - 如果发现的终端为无线终端，则分析服务会发出 Packet-of-Disconnect (Terminate-Session)，而不是 Port Bounce CoA。此更改的益处是支持无线 LAN 控制器 (WLC) CoA。
- 当在逻辑配置文件中抑制终端的分析器 CoA (**Suppress Profiler CoA for endpoints in Logical Profile**) 选项用于在授权配置文件中配置的逻辑配置文件时，将抑制分析器 CoA。默认情况下，将为所有其他终端触发分析器 CoA。
- Global No CoA Setting overrides Policy CoA - Global No CoA 设置会覆盖终端分析策略中的所有配置设置，因为不管每个终端分析策略是否配置了 CoA，思科 ISE 中都不会发出 CoA。



---

注释 No CoA 和 Reauth CoA 配置不受影响，并且分析器服务会为有线和无线终端应用相同的 CoA 配置。

---

## 对各类型 CoA 配置发出的授权更改

表 66: 对各类型 CoA 配置发出的授权更改

情景	No CoA 配置	端口重启配置	Reauth 配置	更多信息
思科 ISE 中的 CoA 全局配置（典型配置）	No CoA	端口重启	重新身份验证	-
终端与您的网络断开连接	No CoA	No CoA	No CoA	授权更改由 RADIUS 属性 Acct-Status-Type 值停止决定。
支持相同交换机端口上的多个活动的会话	No CoA	重新身份验证	重新身份验证	重新身份验证可避免断开其他会话连接。
无线终端	No CoA	Packet-of-Disconnect CoA（终止会话）	重新身份验证	支持无线局域网控制器。
不完整的 CoA 数据	No CoA	No CoA	No CoA	由于缺少 RADIUS 属性。

## 针对 ISE 数据库持久性和性能的属性过滤器

思科 ISE 为动态主机配置协议（DHCP 帮助程序和 DHCP SPAN）、HTTP、RADIUS 和简单网络管理协议探测功能（针对性能下降问题的 NetFlow 探测功能除外）实施过滤器。每个探测功能过滤器都包含与终端分析无关的临时属性的列表，并且会从探测功能收集的属性中移除那些属性。

isebootstrap 日志 (isebootstrap-yyyymmdd-xxxxxx.log) 包含处理字典创建和从字典中过滤属性的消息。您还可以配置在终端经过过滤阶段时记录调试消息以指示已经进行过滤。

思科 ISE 分析器会调用以下终端属性过滤器：

- 用于 DHCP 帮助程序和 DHCP SPAN 的 DHCP 过滤器包含所有不必要并且在解析 DHCP 数据包后被移除的属性。对于终端，过滤之后的属性会与终端缓存中的现有属性合并。
- 系统使用 HTTP 过滤器从 HTTP 数据包过滤属性，过滤之后属性集中不会有重大变更。
- 系统日志解析完成后会立即使用 RADIUS 过滤器，并且终端属性会并入终端缓存中以进行分析。
- 用于 SNMP 查询的 SNMP 过滤器包括单独的 CDP 过滤器和 LLDP 过滤器，这些过滤器都用于 SNMP-Query 探测功能。

## 过滤器终端属性的全局设置

您可以通过在收集点减少不会频繁变更的终端属性的数量，减少持久性事件和复制事件的数量。启用终端属性过滤器 (EndPoint Attribute Filter) 会使思科 ISE 分析器仅保留允许的属性并丢弃所有其他属性。

要启用终端属性过滤器 (EndPoint Attribute Filter)，请参阅[设置 CoA、SNMP RO 社区和终端属性过滤器，第 408 页](#)部分。

允许列表是自定义终端分析策略中用于分析终端的一系列属性，这些属性至关重要，关系到授权更改 (CoA)、自带设备 (BYOD)、设备注册 WebAuth (DRW) 等在思科 ISE 中是否正常运行。允许列表始终用作终端所有权变更时（由多个策略服务节点收集属性时）的标准，即使禁用允许列表也不例外。

默认情况下禁用允许列表，并且只有在启用属性过滤器时才会丢弃属性。当终端分析策略变更（包括数据源变更，以在分析策略中包含新属性）时，允许列表会动态更新。在收集属性时，允许列表中不存在的任何属性会被立即丢弃，并且这些属性不用于分析终端。当与缓冲相结合时，可以减少持久性事件的数量。

您必须确保允许列表包含根据以下两个来源确定的一系列属性：

- 用于默认配置文件中的一系列属性，从而使您可以将终端与配置文件进行匹配。
- 对于使授权更改 (CoA)、自带设备 (BYOD)、设备注册 Web 身份验证 (DRW) 等正常运行很重要的一系列属性。



**注释** 要向允许列表添加新属性，管理员需要创建使用该属性的新分析器条件和策略。该新属性将自动添加到已存储和复制属性的允许列表。

表 67: 允许的属性

AAA-Server	BYODRegistration
Calling-Station-ID	Certificate Expiration Date
Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	Description
DestinationIPAddress	Device Identifier
Device Name	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID
EndPointProfilerServer	EndPointSource
FQDN	FirstCollection

Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type
NmapScanCount	NmapSubnetScanID
OS Version	OUI
PolicyVersion	PortalUser
PostureApplicable	Product
RegistrationTimeStamp	-
StaticAssignment	StaticGroupAssignment
TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress
cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities
lldpCapabilitiesSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	—

## 从思科 IOS 传感器嵌入式交换机收集属性

思科 IOS 传感器集成允许思科 ISE 运行时间和思科 ISE 分析器收集交换机发送的任何或所有属性。您可以利用 RADIUS 协议，直接从交换机收集 DHCP、CDP 和 LLDP 属性。系统会收集 DHCP、

CDP 和 LLDP 的属性，进行解析后，会将其映射至以下位置的分析器词典中的属性：**策略 (Policy) > 策略元素 (Policy Elements) > 词典 (Dictionaries)**。

有关设备传感器支持的 Catalyst 平台的信息，请参阅 <https://communities.cisco.com/docs/DOC-72932>。

## 思科 IOS 传感器嵌入式网络接入设备

将思科 IOS 传感器嵌入式网络接入设备与思科 ISE 集成涉及以下组件：

- 思科 IOS 传感器
- 嵌入在网络接入设备（交换机）中的数据收集器，用于收集 DHCP、CDP 和 LLDP 数据
- 用于处理数据并确定终端的设备类型的分析器

部署分析器有两种方法，但它们不应相互结合使用：

- 分析器可以部署在思科 ISE 中
- 分析器可以作为传感器嵌入在交换机中

## 支持思科 IOS 传感器的网络访问设备的配置核对表

本节概述您必须在支持思科 IOS 传感器的交换机上和思科 ISE 中配置的一系列任务，以直接从交换机收集 DHCP、CDP 和 LLDP 属性。

- 确保在思科 ISE 中启用 RADIUS 探测功能。
- 确保网络访问设备支持用于收集 DHCP、CDP 和 LLDP 信息的 IOS 传感器。
- 确保网络访问设备运行以下 CDP 和 LLDP 命令以从终端捕获 CDP 和 LLDP 信息：

```
cdp enable
lldp run
```

- 确保通过使用标准 AAA 命令和 RADIUS 命令，单独启用会话记帐。

例如，使用以下命令：

```
aaa new-model
aaa accounting dot1x default start-stop group radius

radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
radius-server vsa send accounting
```

- 确保运行 IOS 传感器特定的命令。

- 启用计帐扩大

您必须启用网络访问设备以向 RADIUS 记帐消息添加思科 IOS 传感器协议数据以及在其检测到新传感器协议数据时生成更多记帐事件。这意味着所有 RADIUS 记帐消息都应包含所有 CDP、LLDP 和 DHCP 属性。

请输入以下全局命令：

```
device-sensor accounting
```

- 禁用计帐扩大

对于在特定端口上托管的会话，要禁用（记帐）网络访问设备和向 RADIUS 记帐消息添加思科 IOS 传感器协议数据（如果已全局启用记帐功能），请在相应端口输入以下命令：

```
no device-sensor accounting
```

- TLV 更改跟踪

默认情况下，对于每个支持的对等协议，只有在传入数据包包含之前在特定会话情景中未接收过的类型、长度和值 (TLV) 时，才会生成客户端通知和记帐事件。

您必须为所有 TLV 更改（即出现新 TLV，或之前接收的 TLV 拥有不同的值的情况）启用客户端通知和记帐事件。请输入以下命令：

```
device-sensor notify all-changes
```

- 请务必在网络访问设备中禁用思科 IOS 设备分类器（本地分析器）。

请输入以下命令：

```
no macro auto monitor
```



**注释** 此命令可阻止网络访问设备对一项更改发送两个相同的 RADIUS 记帐消息。

## 分析器条件

分析条件是策略元素，而且与其他条件相似。但是不同于身份验证、授权和访客条件，分析条件可以基于有限数量的属性。Profiler Conditions 页面列出思科 ISE 中可用的属性及其说明。

分析器条件可以是以下任一条件：

- “思科提供” (Cisco Provided)：思科 ISE 包含部署时预定义的分析条件，在“分析器条件” (Profiler Conditions) 页面中标识为 Cisco Provided。您不能删除 Cisco Provided 分析条件。

您还可以在以下位置在系统分析字典中找到“思科提供” (Cisco Provided) 条件：**策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 系统 (System)**。

例如，MAC 字典。对于某些产品，OUI（组织唯一标识符）是您可以首先用于标识设备的生产组织的唯一属性。它是设备 MAC 地址的组成部分。MAC 字典包含 MACAddress 和 OUI 属性。

- “管理员创建” (Administrator Created)：您以思科 ISE 管理员的身份创建的分析器条件或复制的预定义分析条件标识为“管理员创建” (Administrator Created) 条件。您可以使用分析器条件 (Profiler Conditions) 窗口中的分析字典，创建 DHCP、MAC、SNMP、IP、RADIUS、NetFlow、CDP、LLDP 和 NMAP 类型的分析器条件。

虽然建议的分析策略数上限为 1000，但是您可以扩展到多达 2000 个分析策略。

## 分析网络扫描操作

终端扫描操作是终端分析策略中可以引用的一种可配置操作，当满足与网络扫描操作关联的条件时，就会触发该操作。

终端扫描用于扫描终端，从而限制思科 ISE 系统中的资源使用。网络扫描操作扫描的是单个终端，而不像涉及整体资源的网络扫描。它可以提高终端的整体分类，并且可以为终端重新定义终端配置文件。一次仅能处理一个终端扫描。

您可以将单个网络扫描操作与终端分析策略关联。思科 ISE 为网络扫描操作预定义三个扫描类型，一个扫描操作可以包含一个扫描类型，也可以包含全部三个扫描类型：例如 OS 扫描、SNMPPortsAndOS 扫描和 CommonPortsAndOS 扫描。您不能编辑或删除 OS 扫描、SNMPPortsAndOS 扫描和 CommonPortsAndOS 扫描，这些扫描是思科 ISE 中预定义的网络扫描操作。您还可以创建自己的新网络扫描操作。

正确分析某个终端之后，就无法对该终端使用所配置的网络扫描操作。例如，您可以通过扫描 Apple-Device 将所扫描的终端归类为 Apple 设备。OS 扫描确定了终端运行的操作系统之后，终端就不再与 Apple-Device 配置文件匹配，而是与 Apple 设备的相应配置文件匹配。

## 创建新的网络扫描操作

与终端分析策略关联的网络扫描操作会扫描终端的操作系统、简单网络管理协议 (SNMP) 端口和通用端口。思科为最常见的 NMAP 扫描提供网络扫描操作，但是您也可以创建自己的网络扫描操作。

当您创建新的网络扫描时，可定义 NMAP 检测要扫描的信息类型。

### 开始之前

必须首先启用网络扫描 (NMAP) 检测，才能定义规则触发网络扫描操作。关于启用网络扫描检测的操作程序，请参阅[为每个思科 ISE 节点配置探测功能](#)。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 分析 (Profiling) > 网络扫描 (NMAP) 操作 (Network Scan [NMAP] Actions)。

**步骤 2** 点击 **Add**。

**步骤 3** 输入要创建的网络扫描操作的名称和说明。

**步骤 4** 当您要对终端扫描以下各项时，请选中一个或多个复选框：

- 扫描 OS (Scan OS)：扫描操作系统
- 扫描 SNMP 端口 (Scan SNMP Port)：扫描 SNMP 端口 (161、162)
- “扫描通用端口” (Scan Common Port)：扫描通用端口。



步骤 5 点击提交。

## NMAP 操作系统扫描

操作系统扫描（OS 扫描）类型用于扫描终端运行的操作系统（OS 版本）。这种扫描会占用大量资源。

NMAP 工具对可能导致不可靠的结果的 OS 扫描有限制。例如，当扫描交换机和路由器等网络设备的操作系统时，NMAP 操作系统扫描针对这些设备提供的操作系统数据不正确。即使准确度不是 100%，思科 ISE 也会显示操作系统属性。

您应在规则中使用 NMAP 操作系统属性的终端分析策略配置为具有较低的可信度值条件（可信度值）。我们建议，每当您基于 NMAP:operating-system 属性创建终端分析策略时，都应包含 AND 条件以帮助从 NMAP 中过滤掉错误结果。

以下 NMAP 命令用于在您将操作系统扫描与终端分析策略关联时扫描操作系统：

```
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>
```

以下 NMAP 命令扫描子网并发送输出至 nmapSubnet.log：

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
--append-output -oX - <subnet>
```

表 68: 用于手动子网扫描的 NMAP 命令

-O	启用操作系统检测
-sU	UDP 扫描
-p <端口范围>	仅扫描指定端口。例如，U:161, 162
oN	正常输出
oX	XML 输出

## 操作系统端口

下表列出 NMAP 用于 OS 扫描的 TCP 端口。此外 NMAP 使用 ICMP 和 UDP 端口 51824。

1	3	4	6	7	9	13	17	19
20	21	22	23	24	25	26	30	32
33	37	42	43	49	53	70	79	80
81	82	83	84	85	88	89	90	99
100	106	109	110	111	113	119	125	135
139	143	144	146	161	163	179	199	211
212	222	254	255	256	259	264	280	301

306	311	340	366	389	406	407 个	416	417
425	427	443	444	445	458	464	465	481
497	500	512	513	514	515	524	541	543
544	545	548	554	555	563	587	593	616
617	625	631	636	646	648	666	667	668
683	687	691	700	705	711	714	720	722
726	749	765	777	783	787	800	801	808
843	873	880	888	898	900	901	902	903
911	912	981	987	990	992	993	995	999
1000	1001	1002	1007	1009	1010	1011	1021	1022
1023	1024	1025	1026	1027	1028	1029	1030	1031
1032	1033	1034	1035	1036	1037	1038	1039	1040-1100
1102	1104	1105	1106	1107	1108	1110	1111	1112
1113	1114	1117	1119	1121	1122	1123	1124	1126
1130	1131	1132	1137	1138	1141	1145	1147	1148
1149	1151	1152	1154	1163	1164	1165	1166	1169
1174	1175	1183	1185	1186	1187	1192	1198	1199
1201	1213	1216	1217	1218	1233	1234	1236	1244
1247	1248	1259	1271	1272	1277	1287	1296	1300
1301	1309	1310	1311	1322	1328	1334	1352	1417
1433	1434	1443	1455	1461	1494	1500	1501	1503
1521	1524	1533	1556	1580	1583	1594	1600	1641
1658	1666	1687	1688	1700	1717	1718	1719	1720
1721	1723	1755	1761	1782	1783	1801	1805	1812
1839	1840	1862	1863	1864	1875	1900	1914	1935
1947	1971	1972 年	1974	1984	1998-2010	2013	2020 年	2021
2022	2030	2033	2034	2035	2038	2040-2043	2045-2049	2065
2068	2099	2100	2103	2105-2107	2111	2119	2121	2126
2135	2144	2160	2161	2170	2179	2190	2191	2196

2200	2222	2251	2260	2288	2301	2323	2366	2381-2383
2393	2394	2399	2401	2492	2500	2522	2525	2557
2601	2602	2604	2605	2607	2608	2638	2701	2702
2710	2717	2718	2725	2800	2809	2811	2869	2875
2909	2910	2920	2967	2968	2998	3000	3001	3003
3005	3006	3007	3011	3013	3017	3030	3031	3052
3071	3077	3128	3168	3211	3221	3260	3261	3268
3269	3283	3300	3301	3306	3322	3323	3324	3325
3333	3351	3367	3369	3370	3371	3372	3389	3390
3404	3476	3493	3517	3527	3546	3551	3580	3659
3689	3690	3703	3737	3766	3784	3800	3801	3809
3814	3826	3827	3828	3851	3869	3871	3878	3880
3889	3905	3914	3918	3920	3945	3971	3986	3995
3998	4000-4006	4045	4111	4125	4126	4129	4224	4242
4279	4321	4343	4443	4444	4445	4446	4449	4550
4567	4662	4848	4899	4900	4998	5000-5004	5009	5030
5033	5050	5051	5054	5060	5061	5080	5087	5100
5101	5102	5120	5190	5200	5214	5221	5222	5225
5226	5269	5280	5298	5357	5405	5414	5431	5432
5440	5500	5510	5544	5550	5555	5560	5566	5631
5633	5666	5678	5679	5718	5730	5800	5801	5802
5810	5811	5815	5822	5825	5850	5859	5862	5877
5900-5907	5910	5911	5915	5922	5925	5950	5952	5959
5960-5963	5987-5989	5998-6007	6009	6025	6059	6100	6101	6106
6112	6123	6129	6156	6346	6389	6502	6510	6543
6547	6565-6567	6580	6646	6666	6667	6668	6669	6689
6692	6699	6779	6788	6789	6792	6839	6881	6901
6969	7000	7001	7002	7004	7007	7019	7025	7070
7100	7103	7106	7200	7201	7402	7435	7443	7496

7512	7625	7627	7676	7741	7777	7778	7800	7911
7920	7921	7937	7938	7999	8000	8001	8002	8007
8008	8009	8010	8011	8021	8022	8031	8042	8045
8080-8090	8093	8099	8100	8180	8181	8192	8193	8194
8200	8222	8254	8290	8291	8292	8300	8333	8383
8400	8402	8443	8500	8600	8649	8651	8652	8654
8701	8800	8873	8888	8899	8994	9000	9001	9002
9003	9009	9010	9011	9040	9050	9071	9080	9081
9090	9091	9099	9100	9101	9102	9103	9110	9111
9200	9207	9220	9290	9415	9418	9485	9500	9502
9503	9535	9575	9593	9594	9595	9618	9666	9876
9877	9878	9898	9900	9917	9929	9943	9944	9968
9998	9999	10000	10001	10002	10003	10004	10009	10010
10012	10024	10025	10082	10180	10215	10243	10566	10616
10617	10621	10626	10628	10629	10778	11110	11111	11967
12000	12174	12265	12345	13456	13722	13782	13783	14000
14238	14441	14442	15000	15002	15003	15004	15660	15742
16000	16001	16012	16016	16018	16080	16113	16992	16993
17877	17988	18040	18101	18988	19101	19283	19315	19350
19780	19801	19842	20000	20005	20031	20221	20222	20828
21571	22939	23502	24444	24800	25734	25735	26214	27000
27352	27353	27355	27356	27715	28201	30000	30718	30951
31038	31337	32768	32769	32770	32771	32772	32773	32774
32775	32776	32777	32778	32779	32780	32781	32782	32783
32784	32785	33354	33899	34571	34572	34573	34601	35500
36869	38292	40193	40911	41511	42510	44176	44442	44443
44501	45100	48080	49152	49153	49154	49155	49156	49157
49158	49159	49160	49161	49163	49165	49167	49175	49176
49400	49999	50000	50001	50002	50003	50006	50300	50389

50500	50636	50800	51103	51493	52673	52822	52848	52869
54045	54328	55055	55056	55555	55600	56737	56738	57294
57797	58080	60020	60443	61532	61900	62078	63331	64623
64680	65000	65129	65389					

## NMAP SNMP 端口扫描

SNMPPortsAndOS 扫描类型扫描终端运行的操作系统（和操作系统版本）并在打开 SNMP 端口（161 和 162）时触发 SNMP 查询。其可用于一开始识别为与 Unknown 配置文件匹配的终端，以更好地进行分类。

以下 NMAP 命令用于在将 Scan SNMP 端口与终端分析策略关联时扫描 SNMP 端口（UDP 161 和 162）：

```
nmap -sU -p U:161,162 -oN /opt/CSCOCpm/logs/nmap.log --append-output -oX - <IP-address>
```

表 69: 用于终端 SNMP 端口扫描的 NMAP 命令

-sU	UDP 扫描。
-p <端口范围>	仅扫描指定端口。例如，扫描 UDP 端口 161 和 162。
oN	正常输出。
oX	XML 输出。
IP-address	所扫描终端的 IP 地址。

## NMAP 通用端口扫描

CommonPortsAndOS-scan type 扫描终端所运行的操作系统（和操作系统版本）以及通用端口（TCP 和 UDP），但不扫描 SNMP 端口。当您扫描 Common Port 与终端分析策略关联时，以下 NMAP 命令会扫描通用端口：  

```
nmap -sTU -p T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOCpm/logs/nmap.log --append-output -oX - <IP 地址>
```

表 70: 用于终端通用端口扫描的 NMAP 命令

-sTU	TCP 连接扫描和 UDP 扫描。
-p <端口范围>	扫描 TCP 端口：21,22,23,25,53,80,110,135,139,143, 443,445,3306,3389,8080 和 UDP 端口：53,67,68,123,135,137, 138,139,161,445,500,520,631,1434,1900
oN	正常输出。
oX	XML 输出。
IP 地址	所扫描终端的 IP 地址。

## 通用端口

下表列出 NMAP 用于扫描的端口。

表 71: 通用端口

TCP 端口		UDP 端口	
端口	服务	端口	服务
21/tcp	ftp	53/udp	domain
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	domain	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

## 创建分析器条件

思科 ISE 中的终端分析策略允许您对网络上已发现的终端进行分类，并将它们分配到特定的终端身份组。这些终端分析策略由分析条件构成，思科 ISE 评估这些条件对终端进行分类和分组。

### 开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 分析 (Profiling) > 添加 (Add)。

**步骤 2** 输入终端分析策略设置，第 423 页中所描述的字段的价值。

**步骤 3** 点击 **Submit** 保存分析器条件。

**步骤 4** 重复此过程创建更多条件。

## 终端分析策略规则

您可以定义一条规则来允许您从库中选择您之前创建并保存在策略元素库中的一个或多个分析条件，并且允许关联针对每个条件的可信度的整数值，或者为该条件关联例外操作或网络扫描操作。例外操作或网络扫描操作用于触发可配置的操作，而思科 ISE 则就终端整体分类对分析策略进行评估。

使用 OR 运算符单独评估特定策略中的规则时，每个规则的可信度都会影响终端配置文件与特定终端类别的整体匹配。如果终端分析策略的规则匹配，在您的网络上动态发现分析策略和匹配的策略时，对于该终端分析策略和匹配的策略相同。

### 规则中的逻辑分组条件

终端分析策略（配置文件）包含单已条件或使用 AND 或 OR 运算符从逻辑上组合的多个单一条件，您可以根据这些条件为策略中的具体规则对终端进行检查、分类和分组。

条件用于按照终端条件中指定的值检查所收集的终端属性值。如果映射不止一个属性，您可以按逻辑给条件分组，这样可以帮助您给您的网络上的终端分类。您可以根据一个或多个条件检查终端，在规则中为其关联相应的可信度指标（即您所定义的整数值），也可以触发与条件关联的例外操作或与条件关联的网络扫描操作。

### 可信度

分析策略中的最低可信度用于评估终端的匹配配置文件。终端分析策略中每条规则都有一个与分析条件关联的最低可信度指标（一个整数）。可信度指标是为终端分析策略中所有有效规则增加的一个衡量标准，用于衡量终端分析策略中各个条件对于提高终端整体分类的影响。

各条规则的可信度都会影响终端配置文件与具体终端类别的整体匹配度。所有有效规则的可信度相加形成匹配可信度。它必须超过终端分析策略中定义的最低可信度。默认情况下，所有新分析策略规则和预定义分析策略的最低可信度为 10。

## 终端分析策略设置

表 72: 终端分析策略设置

字段名称	使用指南
<b>Name</b>	输入要创建的终端分析策略的名称。
<b>Description</b>	输入要创建的终端分析策略的说明。
<b>Policy Enabled</b>	默认情况下， <b>Policy Enabled</b> 复选框处于选中状态，以便在您分析终端时关联匹配的分析策略。 如果未选中此复选框，则在您分析终端时会排除终端分析策略。
<b>Minimum Certainty Factor</b>	输入要与分析策略相关联的最小值。默认值为 10。

字段名称	使用指南
<b>Exception Action</b>	<p>选择在分析策略中定义规则时要与条件关联的例外操作。</p> <p>默认值为 NONE。例外操作在以下位置定义：<b>策略 (Policy) &gt; 策略元素 (Policy Elements) &gt; 结果 (Results) &gt; 分析 (Profiling) &gt; 例外操作 (Exception Actions)</b>。</p>
<b>Network Scan (NMAP) Action</b>	<p>从列表中选择在分析策略中定义规则时（如有必要）要与条件关联的网络扫描操作。</p> <p>默认值为 NONE。例外操作在以下位置定义：<b>策略 (Policy) &gt; 策略元素 (Policy Elements) &gt; 结果 (Results) &gt; 分析 (Profiling) &gt; 网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)</b>。</p>
<b>Create an Identity Group for the policy</b>	<p>选择以下选项之一以创建终端身份组：</p> <ul style="list-style-type: none"> <li>• <b>Yes, create matching Identity Group</b></li> <li>• <b>No, use existing Identity Group hierarchy</b></li> </ul>
<b>Yes, create matching Identity Group</b>	<p>选择此选项以使用现有的分析策略。</p> <p>此选项可为那些终端创建匹配的身份组，当终端配置文件与现有的分析策略相匹配时，身份组将是已分析的终端身份组的子项。</p> <p>例如，在网络中发现的终端与 Xerox-Device 配置文件相匹配时，系统会在 Endpoints Identity Groups 页面创建 Xerox-Device 终端身份组。</p>
<b>No, use existing Identity Group hierarchy</b>	<p>选中此复选框可使用分析策略和身份组的层次结构将终端分配给匹配的父终端身份组。</p> <p>通过此选项，可以使用终端分析策略层次结构将终端分配给其中一个匹配的父终端身份组，以及父身份组的关联终端身份组。</p> <p>例如，与现有配置文件相匹配的终端会归入相应的父终端身份组中。在本例中，与 Unknown 配置文件相匹配的终端会归入 Unknown 终端身份组中，与现有配置文件相匹配的终端会归入 Profiled 终端身份组中。例如，</p> <ul style="list-style-type: none"> <li>• 如果终端与 Cisco-IP-Phone 配置文件相匹配，则这些终端会归入 Cisco-IP-Phone 终端身份组中。</li> <li>• 如果终端与 Workstation 配置文件相匹配，则这些终端会归入 Workstation 终端身份组中。</li> </ul> <p>Cisco-IP-Phone 和 Workstation 终端身份组与系统中的 Profiled 终端身份组相关联。</p>
<b>Parent Policy</b>	<p>选择在系统中定义的、要与新终端分析策略相关联的父分析策略。</p> <p>可以选择可将规则和条件继承到其子项的父分析策略。</p>



字段名称	使用指南
<b>Associated CoA Type</b>	<p>选择以下要与终端分析策略相关联的 CoA 类型之一：</p> <ul style="list-style-type: none"> <li>• No CoA</li> <li>• 端口重启</li> <li>• Reauth</li> <li>• Global Settings，该设置是从在 Administration &gt; System &gt; Settings &gt; Profiling 中设置的分析器配置进行应用</li> </ul>
<b>Rules</b>	<p>在终端分析策略中定义的一个或多个规则为终端确定了匹配的分析策略，这允许您根据终端配置文件对终端进行分组。</p> <p>策略要素库中的一个或多个分析条件用于规则，以验证终端属性及其整体分类值。</p>
<b>条件</b>	<p>点击加号 [+] 展开 Conditions 固定重叠，点击减号 [-] 或点击固定重叠的外部可将其折叠。</p> <p>点击 <b>Select Existing Condition from Library</b> 或 <b>Create New Condition (Advanced Option)</b>。</p> <p><b>从库中选择现有条件 (Select Existing Condition from Library)</b>：可以通过从策略元素库中选择思科预定义条件来定义表达式。</p> <p><b>创建新条件 (Create New Condition) (高级选项)</b>：可以通过从各种系统或用户定义的字典中选择属性来定义表达式。</p> <p>可以将以下其中一项与分析条件相关联：</p> <ul style="list-style-type: none"> <li>• 每种条件的可信度的整数值。</li> <li>• 为该条件输入例外操作或网络扫描操作</li> </ul> <p>选择以下其中一个要与分析条件相关联的预定义设置：</p> <ul style="list-style-type: none"> <li>• “可信度增加” (Certainty Factor Increases)：为每个规则输入可信度值，可以为与整体分类相关的所有匹配规则添加此可信度值。</li> <li>• “采取例外操作” (Take Exception Action)：触发在此终端分析策略的“例外操作” (Exception Action) 字段中配置的例外操作。</li> <li>• “采取网络扫描操作” (Take Network Scan Action)：触发在此终端分析策略的“网络扫描 (NMAP) 操作” (Network Scan (NMAP) Action) 字段中配置的网络扫描操作。</li> </ul>

字段名称	使用指南
<b>Select Existing Condition from Library</b>	<p>可以执行以下操作：</p> <ul style="list-style-type: none"> <li>• 可以选择策略要素库中可用的思科预定义条件，然后使用 AND 或 OR 运算符添加多个条件。</li> <li>• 点击 Action 图标，在后续步骤中执行以下操作： <ul style="list-style-type: none"> <li>• 添加属性/值 (<b>Add Attribute/Value</b>): 可以添加临时属性或值对</li> <li>• 从库中添加条件 (<b>Add Condition from Library</b>): 可以添加思科预定义条件</li> <li>• 复制 (<b>Duplicate</b>): 创建选定条件的副本</li> <li>• 将条件添加到库 (<b>Add Condition to Library</b>): 可以将自行创建的临时属性/值对保存到策略元素库中</li> <li>• 删除 (<b>Delete</b>): 删除所选条件。</li> </ul> </li> </ul>
<b>Create New Condition (Advance Option)</b>	<p>可以执行以下操作：</p> <ul style="list-style-type: none"> <li>• 可以将临时属性/值对添加到表达式，然后使用 AND 或 OR 运算符添加多个条件。</li> <li>• 点击 Action 图标，在后续步骤中执行以下操作： <ul style="list-style-type: none"> <li>• 添加属性/值 (<b>Add Attribute/Value</b>): 可以添加临时属性或值对</li> <li>• 从库中添加条件 (<b>Add Condition from Library</b>): 可以添加思科预定义条件</li> <li>• 复制 (<b>Duplicate</b>): 创建选定条件的副本</li> <li>• 将条件添加到库 (<b>Add Condition to Library</b>): 可以将自行创建的临时属性/值对保存到策略元素库中</li> <li>• 删除 (<b>Delete</b>): 删除所选条件。可以使用 AND 或 OR 运算符</li> </ul> </li> </ul>

#### 相关主题

[思科 ISE 分析服务](#)，第 396 页

[创建终端分析策略](#)，第 426 页

## 创建终端分析策略

您可以通过使用 New Profiler Policy 页面中的以下选项，创建用于分析终端的新分析策略：

- Policy Enabled

- Create an Identity Group，让策略创建匹配的终端身份组或使用终端身份组层次结构
- Parent Policy
- Associated CoA Type



**注释** 当您选择在分析策略 (Profiling Policies) 窗口中创建终端策略时，请勿使用 Web 浏览器中的“停止” (Stop) 按钮。此操作会导致以下结果：停止加载新分析器策略 (New Profiler Policy) 窗口、在访问时加载其他列表页面及列表页面内的菜单，以及防止您对列表页面内的所有菜单执行操作，“过滤器” (Filter) 菜单除外。您可能需要注销思科 ISE，然后重新登录才能对列表菜单内的所有菜单执行操作。

您可以通过复制终端分析策略来创建类似特征的分析策略，这样您就可以修改现有的分析策略，而不是通过重新定义所有条件来创建新分析策略。

**步骤 1** 选择 **策略 (Policy) > 分析 (Profiling) > 分析 (Profiling) 分析策略 (Profiling Policies)**。

**步骤 2** 点击添加 (Add)。

**步骤 3** 输入要创建的新终端政策的名称和说明。**Policy Enabled** 复选框在默认情况下处于选中状态，以包含用于在分析终端时进行验证的终端分析策略。

**步骤 4** 输入最低可信度的值，有效范围为 1 至 65535。

**注释** 创建自定义分析策略时，必须考虑以下注意事项：

- 如果自定义策略中配置的不同属性已被默认分析策略配置为评估对象，并且默认分析策略的确定性因素 (CF) 大于自定义策略，则自定义分析策略将永远不会被分配给任何终端。这是因为 CF 增幅较高的分析政策将优先于 CF 增幅较低的其他政策。
- 许多默认分析策略都被配置为 10、20 和 30 的 CF 增量。

**步骤 5** 点击 **Exception Action** 下拉列表旁边的箭头以关联例外操作，或点击 **Network Scan (NMAP) Action** 下拉列表旁边的箭头以关联网络扫描操作。

**步骤 6** 为 **Create an Identity Group for the policy** 选择以下其中一个选项：

- **Yes, create matching Identity Group**
- **No, use existing Identity Group hierarchy**

**步骤 7** 点击 **Parent Policy** 下拉列表旁边的箭头将父策略关联到新终端策略。

**步骤 8** 在 **Associated CoA Type** 下拉列表中选择要关联的 CoA 类型。

**步骤 9** 点击规则以添加条件并为每个条件的可信度关联一个整数值或为该条件关联例外操作或网络扫描操作，以对终端进行整体分类。

**步骤 10** 在新建分析器策略 (New Profiler Policy) 页面中点击**提交 (Submit)** 以添加终端策略，或点击**分析器策略列表 (Profiler Policy List)** 链接以返回分析策略 (Profiling Policies) 页面。

## 每个终端分析策略的授权更改配置

除了思科 ISE 中授权更改 (CoA) 类型的全局配置，您还可以配置为每个终端分析策略发出特定类型的关联 CoA。

全局 No CoA 类型配置会覆盖终端分析策略中配置的每个 CoA 类型。如果全局 CoA 类型设置的不是 No CoA 类型，则系统允许每个终端分析策略覆盖全局 CoA 配置。

当触发 CoA 时，每个终端分析策略都可以决定实际 CoA 类型，如下所示：

- **General Setting** - 这是适用于所有终端分析策略的根据全局配置发出 CoA 的默认设置。
- **No CoA** - 此设置会覆盖任何全局配置并为配置文件禁用 CoA。
- **Port Bounce** - 此设置会覆盖全局 Port Bounce 和 Reauth 配置类型，并发出端口退回 CoA。
- **Reauth** - 此设置会覆盖全局 Port Bounce 和 Reauth 配置类型，并且发出重新身份验证 CoA。



**注释** 如果分析器全局 CoA 配置设置为 Port Bounce（或 Reauth），请确保您将相应终端分析策略配置为基于策略的 CoA 选项 No CoA，从而使您的移动设备不会出现自带设备流程中断。

请参阅下表中对所有 CoA 类型和根据全局和终端分析策略设置在每个案例中实际发出的 CoA 类型的配置总结。

**表 73:** 为各种配置组合发出的 CoA 类型

全局 CoA 类型	根据策略设置的默认 CoA 类型	根据策略的 No CoA 类型	根据策略的端口退回类型	根据策略的重新身份验证类型
No CoA	No CoA	No CoA	No CoA	No CoA
端口重启	Port Bounce	No CoA	端口重启	Re-Auth
Reauth	Reauth	No CoA	端口重启	Re-Auth

## 导入终端分析策略

使用可以在导出功能中创建的同格式，从 XML 文件导入终端分析策略。如果导入已关联父策略的新建分析策略，则必须在定义子策略之前定义父策略。

导入的文件包含终端分析策略层级结构，首先包含父策略，其次是导入的配置文件，然后是在策略中定义的规则和考核。

步骤 1 选择 **策略 (Policy)** > **分析 (Profiling)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

步骤 2 点击 **Import**。

步骤 3 点击 **Browse**，找到您之前导出而现在想要导入的文件。

步骤 4 点击 **Submit**。

步骤 5 单击分析器策略列表 (**Profiler Policy List**) 链接，返回分析策略 (**Profiling Policies**) 窗口。

## 导出终端分析策略

您可以将终端分析策略导出到其他思科 ISE 部署中。或者，您可以使用 XML 文件作为模板创建您自己的策略并导入。您还可以将该文件下载到您系统中的默认位置，以用于日后的导入。

当您导出终端分析策略时会出现一个对话框，提示您使用适当的应用打开 `profiler_policies.xml` 或其保存。此文件的格式为 XML，您可以使用网页浏览器打开，也可以用其他适当的应用打开。

步骤 1 选择 **策略 (Policy)** > **分析 (Profiling)** > **分析 (Profiling)** > **分析策略 (Profiling Policies)**。

步骤 2 选择 **Export**，并选择以下一项：

- **导出所选 (Export Selected)**：您仅可以导出在分析策略 (**Profiling Policies**) 窗口中选择的终端分析策略。
- **导出所选及终端 (Export Selected with Endpoints)**：可以导出所选择的终端分析策略，以及使用所选择的终端分析策略分析的终端。
- **全部导出 (Export All)**：默认情况下，可以导出分析策略 (**Profiling Policies**) 窗口中的所有分析策略。

步骤 3 单击确定 (**OK**) 以在 `profiler_policies.xml` 文件中导出终端分析策略。

## 预定义终端分析策略

部署思科 ISE 时，思科 ISE 包含预定义的默认分析策略，这些策略的分层结构允许您对网络上的已识别终端进行分类，并将它们分配给匹配的终端身份组。因为终端分析策略采用分层结构，所以您会发现，**分析策略 (Profiling Policies)** 窗口显示设备的通用（母）策略列表，“分析策略” (**Profiling Policies**) 列表窗口显示与母策略关联的子策略。

无论是否启用以用于验证，**分析策略 (Profiling Policies)** 窗口都显示终端分析策略及其名称、类型、描述和状态。

终端分析策略类型分类如下：

- **“思科提供” (Cisco Provided)**：在思科 ISE 中预定义的终端分析策略被识别为“思科提供” (**Cisco Provided**) 类型。

- “管理员已修改” (Administrator Modified): 修改预定义的终端分析策略时，终端分析策略被识别为“管理员已修改” (Administrator Modified) 类型。思科 ISE 将在升级过程中覆盖您在预定义终端分析策略中所做的更改。
- “管理员已创建” (Administrator Created): 您创建的终端分析策略或者当您复制 Cisco 提供的终端分析策略时，被识别为“管理员已创建” (Administrator Created) 类型。

我们建议为一组终端创建通用策略（母策略），其子策略能够继承规则和条件。如果终端必须归类，那么终端配置文件必须首先匹配母策略，当您分析终端时，再匹配后代（子）策略。

例如，Cisco-Device 是一个适用于所有思科设备的通用终端分析策略，适用于思科设备的其他策略则为 Cisco-Device 的子策略。如果终端必须归类为 Cisco-IP-Phone 7960，那么此终端的终端配置文件必须首先匹配母 Cisco-Device 策略、子 Cisco-IP-Phone 策略，然后匹配 Cisco-IP-Phone 7960 分析策略，以便更好地分类。



**注释** 思科 ISE 不会覆盖管理员修改的策略及其子策略，即使这些策略仍标记为“思科提供” (Cisco Provided)。如果管理员修改的策略被删除，它会恢复为以前的思科提供的策略。下一次发生源更新时，所有子策略都会更新。

## 在升级期间覆盖预定义终端分析策略

您可以在 Profiling Policies 页面编辑现有的终端分析策略。此外，当您想要修改预定义终端分析策略时，必须在预定义终端配置文件副本中保存所有配置。

在升级过程中，思科 ISE 重写您在预定义终端配置文件中保存的任何配置。

## 无法删除终端分析策略

您可以在分析策略 (Profiling Policies) 窗口中删除选定的或所有终端分析策略。默认情况下，可以从分析策略 (Profiling Policies) 窗口删除所有终端分析策略。当在分析策略 (Profiling Policies) 窗口中选择所有终端分析策略并尝试删除它们时，如果其中有些终端分析策略映射至其他终端分析策略或映射至授权策略，则可能不会删除它们。

- 您无法删除思科提供的终端分析策略，
- 当终端配置文件定义为其他终端配置文件的父级时，您无法在分析策略 (Profiling Policies) 窗口中删除父配置文件。例如，Cisco-Device 是用于思科设备的其他终端分析策略的父级。
- 当某个终端配置文件映射至授权策略时，您无法删除此终端配置文件。例如，Cisco-IP-Phone 映射至 Profiled Cisco IP Phones 授权策略而且是用于思科 IP 电话的其他终端分析策略的父级。

## 用于 Draeger 医疗设备的预定义分析策略

思科 ISE 包含默认终端分析策略，这些策略包括用于 Draeger 医疗设备的通用策略、用于 Draeger-Delta 医疗设备的策略，以及用于 Draeger-M300 医疗设备的策略。两个医疗设备共用端口 2050 和 2150，因此当您使用默认 Draeger 终端分析策略时，您无法给 Draeger-Delta 和 Draeger-M300 医疗设备分类。

如果这些 Draeger 设备在您的环境中共用端口 2050 和 2150，除了在默认 Draeger-Delta 和 Draeger-M300 终端分析策略中检查设备目标 IP 地址之外，您还必须增加一条规则以确保您可以区分这些医疗设备。

思科 ISE 包括用于 Draeger 医疗设备终端分析策略的以下分析策略：

- 包含端口 2000 的 Draeger-Delta-PortCheck1
- 包含端口 2050 的 Draeger-Delta-PortCheck2
- 包含端口 2100 的 Draeger-Delta-PortCheck3
- 包含端口 2150 的 Draeger-Delta-PortCheck4
- 包含端口 1950 的 Draeger-M300PortCheck1
- 包含端口 2050 的 Draeger-M300PortCheck2
- 包含端口 2150 的 Draeger-M300PortCheck3

## 用于未知终端的终端分析策略

不匹配现有的配置文件且无法在思科 ISE 中分析的终端为未知终端。未知配置文件是分配给终端的默认系统分析策略，为此终端收集的一个属性或一组属性与思科 ISE 中现有的配置文件不匹配。

在以下情境中分配未知配置文件：

- 在思科 ISE 中动态地发现终端，并且没有适用于此终端的匹配终端分析策略时，将终端分配给未知配置文件。
- 当思科 ISE 中静态地添加终端，且没有适用于静态添加的终端的匹配终端分析策略时，将终端分配给未知配置文件。

如果将终端静态地添加到网络，思科 ISE 中的分析服务不分析静态添加的终端。稍后，您可以将未知配置文件更改为相应的配置文件，思科 ISE 不会重新分配您已分配的分析策略。

## 用于静态添加的终端的终端分析策略

对于静态添加以进行分析的终端，分析服务将新的 MATCHEDPROFILE 属性添加到终端，为终端计算配置文件。如果动态分析终端，那么计算的配置文件则是该终端的实际配置文件。这样，您可以发现静态添加的终端的计算配置文件与动态分析的终端的匹配配置文件不匹配的情况。

## 静态 IP 设备的终端分析策略

如果您的终端拥有静态分配的 IP 地址，则您可以为这些静态 IP 设备创建配置文件。

必须启用 RADIUS 探测功能或 SNMP 查询和 SNMP 陷阱探测功能，分析拥有静态 IP 地址的终端。

## 终端分析策略匹配

当在分析策略中满足一个或多个规则中定义的分析条件时，思科 ISE 会始终将终端的所选策略视为匹配策略而不是已评估的策略。此处，该终端的静态分配的状态在系统中设置为 `false`。但是，通过在终端编辑过程中使用静态分配功能，可以在将该终端重新静态分配给系统中的现有分析策略后将状态设置为 `true`。

以下操作适用于终端的匹配策略：

- 对于静态分配的终端，分析服务会计算 `MATCHEDPROFILE`。
- 对于动态分配的终端，`MATCHEDPROFILE` 与匹配终端配置文件相同。

您可以使用分析策略中定义的一个或多个规则确定动态终端的匹配分析策略，并且相应地分配终端身份组以进行分类。

当终端映射到现有策略时，分析服务会搜索分析策略的层次结构以查找具有匹配策略组的最近父配置文件，并将终端分配给相应的终端策略。

## 用于授权的终端分析策略

您可以在授权规则中使用终端分析策略，在其中您可以创建作为属性的新条件，使之包含终端分析策略检查，并且该属性以终端分析策略的名称作为属性值。您可以从终端字典选择终端分析策略，其中包含以下属性：`PostureApplicable`、`EndPointPolicy`、`LogicalProfile` 和 `BYODRegistration`。

`PostureApplicable` 的属性值根据操作系统自动设置。对于 IOS 和 Android 设备，它设置为否 (*No*)，因为这些平台上不能使用 AnyConnect 支持来执行安全评估。对于 Mac OSX 和 Windows 设备，该值设置为是 (*Yes*)。

您可以定义包括 `EndPointPolicy`、`BYODRegistration` 和身份组的组合的授权规则。

## 终端分析策略分组为逻辑配置文件

逻辑配置文件是一类配置文件或相关联配置文件的容器，无需考虑终端分析策略是由思科提供还是由管理员创建。一个终端分析策略可以与多个逻辑配置文件关联。

您可以在授权策略条件中使用逻辑配置文件，来帮助您创建针对某类别配置文件的整体网络接入策略。您可以创建授权的简单条件，该条件可包括在授权规则中。您可以在授权条件中使用的属性-值对是逻辑配置文件（属性）和逻辑配置文件名称（值），该属性-值对位于终端系统字典中。

例如，通过将移动设备类别匹配的终端分析策略分配至逻辑配置文件，可以为所有移动设备（如安卓、苹果 iPhone 或黑莓）创建一个逻辑配置文件。思科 ISE 包含 IP 电话，这是一个针对所有 IP



电话的默认逻辑配置文件，包括 IP 电话、思科 IP 电话、Nortel IP 电话 2000 系列和 AVAYA IP 电话配置文件。

## 创建逻辑配置文件

您可以创建可用于对某个类别的终端分析策略进行分组的逻辑配置文件，借此可创建整体类别的配置文件或关联配置文件。您还可以从分配的集合中删除终端分析策略，从而将其移回到可用集合。

**步骤 1** 选择 **政策 (Policy) > 分析 (Profiling) > 分析 (Profiling) > 逻辑配置文件 (Logical Profiles)**。

**步骤 2** 点击添加 (**Add**)。

**步骤 3** 在名称 (**Name**) 和说明 (**Description**) 的文本框中输入新逻辑配置文件的名称和说明。

**步骤 4** 从可用策略 (**Available Policies**) 中选择终端分析策略以在逻辑配置文件中对其进行分配。

**步骤 5** 点击向右箭头以将所选终端分析策略移至分配策略 (**Assigned Policies**)。

**步骤 6** 点击提交。

## 分析例外操作

例外操作是终端分析策略中可以引用的一个可配置操作，当符合该操作关联的例外条件时就会触发例外操作。

例外操作可以是以下任一类型：

- **Cisco-provided** - 您不能删除思科提供的例外操作。当您要在思科 ISE 中分析终端时，思科 ISE 从系统中触发以下非可编辑的分析例外操作：
  - **Authorization Change** - 当从授权策略使用的终端身份组添加或删除终端时，此分析服务发出授权更改。
  - **Endpoint Delete** - 当在 **Endpoints** 页面从系统中删除终端或在思科 ISE 网络中从 **Edit** 页面向已知配置文件分配终端时，在思科 ISE 中会触发例外操作并且会发出 **CoA**。
  - **FirstTimeProfiled** - 当在思科 ISE 中首次分析某个终端时，如果该终端的配置文件从未知配置文件转变为现有配置文件，但是在思科 ISE 网络中该终端身份验证未成功，则在思科 ISE 中会触发例外操作并且会发出 **CoA**。
- **Administrator-created** - 思科 ISE 触发您所创建的分析例外操作。

## 创建例外操作

您可以定义一个或多个例外规则并将其关联到单个分析策略。此关联会在分析策略和至少一个例外规则在思科 ISE 中的分析终端中匹配时触发例外操作（单个可配置操作）。

**步骤 1** 选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 分析 (Profiling) > 例外操作 (Exception Actions)**。

**步骤 2** 点击添加 (**Add**)。

**步骤 3** 在 **Name** 和 **Description** 的文本框中输入例外操作的名称和说明。

**步骤 4** 选中 **CoA Action** 复选框。

**步骤 5** 选中 **Policy Assignment** 下拉列表以选择终端策略。

**步骤 6** 点击提交。

## 使用策略和身份的静态分配创建终端

在终端页面中，您可以使用终端的 MAC 地址静态创建新的终端。在终端页面中，您还可以选择静态分配的终端分析策略和身份组。

常规和移动设备 (MDM) 终端会显示在终端身份列表中。在列表页面中会显示 MDM 终端的属性列，这些属性包括主机名、设备类型、设备标识符。其他列如静态分配和静态组分配在默认情况下不显示。



**注释** 您无法使用此页面添加、编辑、删除、导入或导出 MDM 终端。

**步骤 1** 选择 **管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 终端 (Endpoints)**。

**步骤 2** 点击添加 (**Add**)。

**步骤 3** 输入十六进制格式的终端 MAC 地址，以冒号分隔。

**步骤 4** 从 **Policy Assignment** 下拉列表选择一个匹配的终端策略，将其静态分配状态从动态更改为静态。

**步骤 5** 选中 **Static Assignment** 复选框，将分配到终端的静态分配的状态从动态更改为静态。

**步骤 6** 从 **Identity Group Assignment** 下拉列表中选择您希望分配到新创建终端的终端身份组。

**步骤 7** 选中 **Static Group Assignment** 复选框，将终端身份组的动态分配更改为静态。

**步骤 8** 点击提交。

## 从 CSV 文件导入终端

您可以从已从思科 ISE 服务器为其导出终端的 CSV 文件或者从思科 ISE 创建并使用终端详情更新的 CSV 文件导入终端。

文件格式必须是在默认导入模板指定的格式，使终端列表看起来如下所示：MAC、Endpoint Policy、Endpoint Identity Group。

对于在 CSV 文件中导入终端，终端策略和终端身份组都是可选的。如果想要导入终端身份组而不导入终端的终端策略，值依然用逗号分隔。

例如，

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4

**步骤 1** 选择管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 终端 (Endpoints) > 导入 (Import)。

**步骤 2** 点击 **Import From File**。

**步骤 3** 点击 Browse，找到已从思科 ISE 服务器导出的 CSV 文件或者以指定文件格式创建并使用终端更新的 CSV 文件。

**步骤 4** 点击提交。

## 可用于终端的默认导入模板

您可以生成可以在其中更新终端的模板，您可将其用于导入终端。默认情况下，您可以使用 **Generate a Template** 链接，在 Microsoft Office Excel 应用中创建 CSV 文件并将文件保存在您的系统本地位置上。此文件位于管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 终端 (Endpoints) > 导入 (Import) > 从文件导入 (Import From File)。您可以使用 **Generate a Template** 链接创建模板，并且思科 ISE 服务器将显示 **Opening template.csv** 对话框。您可以通过此对话框打开默认 **template.csv** 文件，或将 **template.csv** 文件保存在您的系统本地位置上。如果您选择从此对话框打开 **template.csv** 文件，系统会使用 Microsoft Office Excel 应用打开此文件。默认的 **template.csv** 文件包含一个标题行，其中显示 MAC 地址、终端策略、终端身份组列。

您必须更新终端的 MAC 地址、终端分析策略和终端身份组并以不同文件名保存该文件以用于导入终端。请参阅您使用 **Generate a Template** 时创建的 **template.csv** 文件中的标题行。

表 74: CSV 模板文件

MAC	终端策略	终端身份组
00:1f:f3:4e:c1:8e	Cisco-Device	RegisteredDevices

## 导入过程中重新分析的未知终端

如果用于导入的文件包含具有 MAC 地址的终端，并且其已分配的终端分析策略是 **Unknown** 配置文件，则这些终端会在思科 ISE 中立即重新分析到导入过程中的匹配终端分析策略。但是，系统不会将它们静态分配到 **Unknown** 配置文件。如果终端在 CSV 文件中没有向其分配的终端分析策略，则它们会分配到 **Unknown** 配置文件，然后重新分析到匹配的终端分析策略。请参阅以下内容，了解思科 ISE 如何在导入过程中重新分析与 **Xerox\_Device** 配置文件匹配的 **Unknown** 配置文件，以及思科 ISE 如何重新分析未分配的终端。

表 75: Unknown 配置文件: 从文件导入

MAC 地址	思科 ISE 中导入前分配的终端分析策略	思科 ISE 中导入后分配的终端分析策略
00:00:00:00:01:02	未知	Xerox-Device
00:00:00:00:01:03	未知	Xerox-Device
00:00:00:00:01:04	未知	Xerox-Device
00:00:00:00:01:05	如果未向终端分配配置文件, 则该终端会分配到 Unknown 配置文件, 并且还会重新分析到匹配的配置文件。	Xerox-Device

## 静态分配导入过程中保留的终端的策略和身份组

如果用于导入的文件包含具有 MAC 地址的终端, 并且其已分配的终端分析策略是静态分配, 则在导入过程中不会对其重新分析。请参阅以下内容, 了解思科 ISE 如何保留 Cisco-Device 配置文件, 即在导入过程中静态分配终端。

表 76: 静态分配: 从文件导入

MAC 地址	思科 ISE 中导入前分配的终端分析策略	思科 ISE 中导入后分配的终端分析策略
00:00:00:00:01:02	Cisco-Device (静态分配)	Cisco-Device

## 不导入具有无效属性的终端

如果 CSV 文件中存在的任何终端具有无效属性, 则不导入该终端, 并显示错误消息。

例如, 如果终端被分配至用于导入的文件中的无效配置文件, 因为思科 ISE 中没有匹配的配置文件, 所以不会导入这些无效配置文件。请参阅下文, 了解当终端被分配至 CSV 文件中的无效配置文件时, 如何不导入终端。

表 77: 无效配置文件: 从文件导入

MAC 地址	思科 ISE 中导入前分配的终端分析策略	思科 ISE 中导入后分配的终端分析策略
00:00:00:00:01:02	未知	Xerox-Device
00:00:00:00:01:05	如果向无效配置文件而不是向思科 ISE 中可用的配置文件分配 00:00:00:00:01:05 等终端, 则思科 ISE 会显示警告消息, 提示此策略名称无效并且将不导入该终端。	因为思科 ISE 中没有匹配的配置文件, 所以不会导入该终端。

## 从 LDAP 服务器导入终端

可以安全地从 LDAP 服务器导入终端的 MAC 地址、关联的配置文件和终端身份组。

### 开始之前

在开始导入终端之前，请确保已安装 LDAP 服务器。

必须配置连接设置和查询设置才能从 LDAP 服务器导入。如果思科 ISE 中的连接设置或查询设置配置不正确，则系统会显示“LDAP import failed:”错误消息。

---

**步骤 1** 选择 **管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 终端 (Endpoints) > 导入 (Import) > 从 LDAP 导入 (Import From LDAP)**。

**步骤 2** 输入连接设置的值。

**步骤 3** 输入查询设置的值。

**步骤 4** 点击提交。

---

## 以 CSV 文件导出终端

您可以使用 CSV 文件导出所有终端，或者只导出所选的终端。列出的终端将包括其 MAC 地址、终端分析策略以及为其分配的终端身份组。



---

**注释** 要将从一个部署导出的终端自定义属性导入到另一个中，必须在**管理 (Administration) > 身份管理 (Identity Management) > 设置 (Settings) > 终端自定义属性 (Endpoint Custom Attributes)** 窗口中创建相同的自定义属性，并使用与原始部署中相同的数据类型。

---

默认选项为**全部导出 (Export All)**。如果已在**终端 (Endpoints)** 窗口中过滤终端，则当使用**全部导出 (Export All)** 选项时，系统只会导出过滤的终端。默认情况下，`profiler_endpoints.csv` 是 CSV 文件，而 Microsoft Office Excel 是默认应用，用于从 Opening `profiler_endpoints.csv` 对话框打开 CSV 文件，或保存 CSV 文件。例如，您可以在 `profiler_endpoints.csv` 文件中导出选定的终端或所有终端，也可以使用该文件导入上述终端。

要使用 CSV 文件导出终端，请执行以下操作：

---

**步骤 1** 选择 **选择管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 终端 (Endpoints)**。

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

**步骤 3** 单击**确定 (OK)** 以保存 CSV 文件。

导出的电子表格中的大多数属性都很简单。以下属性需要说明：

- **UpdateTime:** 由于终端属性更改，分析器上次更新终端的时间。如果自终端会话启动以来没有更新，则值为 0。在更新期间，它将短暂为空

- *InactivityTime*: 终端处于活动状态后的时间。

## 已识别的终端

思科ISE显示已识别的终端，这些终端在**终端 (Endpoints)**窗口中连接到您的网络并使用您网络上的资源。终端通常是一个支持网络的设备，该设备通过有线和无线网络接入设备和VPN连接到您的网络。终端可以是个人计算机、笔记本、IP电话、智能手机、游戏主机、打印机、传真机等等。

以十六进制显示的终端MAC地址通常唯一地表示一个终端，但是您也可以使用一组变化的属性以及与此些属性关联的值（属性-值对）来标识终端。您可以根据终端的功能、网络接入设备的配置以及您用于收集这些属性的方法（探测），收集一组变化的终端属性。

### 已动态分析的终端

当在您的网络上发现终端时，根据已配置的终端分析策略，即可对这些终端进行动态分析，并按照配置文件将这些终端分配到匹配的终端身份组。

### 已静态分析的终端

当您使用终端的MAC地址在思科ISE中创建终端并将配置文件及终端身份组与其关联时，即可静态分析该终端。思科ISE不会重新分配已静态分配终端的分析策略和身份组。

### 未知终端

如果终端缺少匹配的分析策略，您可以分配一个未知分析策略（未知），而终端则会被分析为未知。由未知终端策略分析的终端需要您使用已收集的一个终端属性或一组终端属性来创建配置文件。与所有配置文件均不匹配的终端会被分组到未知终端身份组中。

## 策略服务节点数据库中本地存储的已识别终端

思科ISE在本地将已识别的终端写入策略服务节点数据库。将这些终端在本地存储于数据库中之后，只有在终端中重要属性出现变更时，在管理节点数据库中这些终端才可用（远程写入），并且被复制到其他策略服务节点数据库中。重要属性是指思科ISE系统使用的属性或特别用于终端分析策略或规则的属性。

以下是重要属性：

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment

- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

当您在思科 ISE 中更改终端配置文件定义时，所有终端都必须重新进行分析。收集终端属性的策略服务节点负责重新分析这些终端。

当策略服务节点开始收集关于某个终端的属性时，如果一开始该终端是由另一个不同的策略服务节点收集其属性，则该终端的所有权就改为属于当前策略服务节点。新策略服务节点会从之前的策略服务节点检索最新属性，并且将所收集的这些属性与已经收集的那些属性进行比较。

当终端中某个重要属性发生变更时，该终端的属性会自动保存在管理节点数据库中，这样您就会获得该终端中最新的重要变更。如果拥有某个终端的策略服务节点由于某些原因不可用，则管理员 ISE 节点将会重新分析失去所有者的终端而且您必须为这些终端配置新的策略服务节点。

## 集群中的策略服务节点

思科 ISE 将策略服务节点组用作集群，如果集群中两个或多个节点为同一终端收集属性，集群将允许交换终端属性。我们建议您为负载均衡器后面的所有策略服务节点创建集群。

如果与当前所有者不同的节点接收到同一终端的属性，此节点会在集群中发送一条向当前所有者请求最新属性的消息以合并属性并确定是否需要更改所有权。如果您未在思科 ISE 中定义节点组，系统会假定所有节点都处于同一集群中。

思科 ISE 不会更改终端创建和复制，只会根据从静态属性和动态属性构建的用于分析的许可属性列表决定是否更改终端的所有权。

在以后的属性收集中，如果以下任一属性发生更改，管理节点上会更新终端：

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

在管理节点中编辑和保存终端时，系统会从当前终端所有者检索属性。

## 创建终端身份组

思科ISE 将其所发现的终端划分至相应的终端身份组。思科ISE 拥有若干个系统定义的终端身份组。您还从**终端身份组 (Endpoint Identity Groups)** 窗口创建更多终端身份组。您可以编辑或删除您已创建的终端身份组。只能编辑系统定义的终端身份组的说明。无法编辑或删除这些组的名称。

**步骤 1** 选择 **管理 (Administration) > 身份管理 (Identity Management) > 组 (Groups) > 终端身份组 (Endpoint Identity Groups)**。

**步骤 2** 单击添加。

**步骤 3** 为您想要创建的终端身份组输入**名称**（请勿在终端身份组的名称中包含空格）。

**步骤 4** 为您想要创建的终端身份组输入**说明**。

**步骤 5** 点击 **Parent Group** 下拉列表，选择您要与新创建的终端身份组关联的终端身份组。

**步骤 6** 点击提交。

## 已识别终端划分为终端身份组

思科ISE 根据终端分析策略，将已发现的终端划分为对应的终端身份组。分析策略分为不同的层级，在思科ISE 中在终端身份组级应用。通过将终端划分为终端身份组，并且将分析策略应用到终端身份组，思科ISE 使您能够查看对应的终端分析策略，确定终端到终端配置文件的映射。

默认情况下，思科ISE 创建终端身份组集合，允许您创建自己的身份组，动态或静态地向其分配终端。您可以创建终端身份组，将身份组关联到系统创建的身份组之一。此外，您还可以将您创建的终端静态地分配到系统中存在的身份组之一，分析服务不能重新分配身份组。

## 为终端创建的默认终端身份组

思科ISE 创建以下终端身份组：

- **黑名单**：此终端身份组包括思科ISE 中静态分配给此组的终端和在设备注册门户中列入阻止名单的终端。可以在思科ISE 中定义授权配置文件以允许或拒绝为该组中的终端提供网络接入。
- **GuestEndpoints**：此终端身份组包括访客用户使用的终端。
- **Profiled**：此终端身份组包括思科ISE 中除思科IP 电话和工作站之外与终端分析策略匹配的终端。
- **RegisteredDevices**：此终端身份组包括属于员工通过设备注册门户添加的已注册设备的终端。当这些设备分配至该组时，分析服务会继续正常分析这些设备。终端在思科ISE 中会静态分配至该组，而且分析服务无法将其重新分配到任何其他身份组。这些设备会像任何其他终端一样显示在终端列表上。您可以在思科ISE 中的“终端”(Endpoints) 窗口从终端列表编辑、删除和阻



止通过设备注册门户添加的这些设备。您在设备注册门户中阻止的设备会分配至黑名单终端身份组，而且思科 ISE 中存在的一个授权配置文件会将被阻止的设备重定向显示“未授权的网络访问” (Unauthorised Network Access) 的 URL，这是被阻止设备的默认门户页面。

- **Unknown:** 此终端身份组包括与思科 ISE 中任何配置文件都不匹配的终端。

除了上述系统创建的终端身份组，思科 ISE 还会创建以下终端身份组，这些身份组与“分析” (Profiled) 身份组关联：父组是系统中存在的默认身份组：

- **Cisco-IP-Phone:** 此身份组包含您的网络上所有已分析的思科 IP 电话。
- **Workstation:** 此身份组包含您的网络上所有已分析的工作站。

## 为匹配的终端分析策略创建的终端身份组

如果您有终端策略与现有策略匹配，则分析服务可以创建一个匹配的终端身份组。此身份组就成为已分析终端身份组的子级。当您创建终端策略时，您可以在 **Profiling Policies** 页面选中 **Create Matching Identity Group** 复选框，以创建匹配的终端身份组。除非删除配置文件的映射，否则无法删除匹配的身份组。

## 向终端身份组中添加静态终端

您可以在任意终端身份组中添加或移除静态添加的终端。

您仅可从 **Endpoints** 小组件向特定身份组添加终端。如果您向某个终端身份组添加某个终端，该终端就会从其之前动态分组的终端身份组删除。

在从您最近添加了某个终端的终端身份组删除该终端后，系统会重新分析该终端，使之回到相应身份组。这不会从系统删除终端，而只是从终端身份组删除终端。

---

**步骤 1** 选择 **管理 (Administration) > 身份管理 (Identity Management) > 组 (Groups) > 终端身份组 (Endpoint Identity Groups)**。

**步骤 2** 选择终端身份组，然后点击 **Edit**。

**步骤 3** 点击添加 (**Add**)。

**步骤 4** 在 **Endpoints** 小组件中选择终端，以将所选终端添加至终端身份组。

**步骤 5** 点击 **Endpoint Group List** 链接以返回 **Endpoint Identity Groups** 页面。

---

## 在身份组中添加或删除终端后重新分析动态终端

如果终端身份组分配不是静态的，则在终端身份组中添加或删除终端后重新分析终端。由 ISE 分析器动态识别的终端显示在相应的终端身份组中。如果从终端身份组删除动态添加的终端，思科 ISE 则显示一条消息，指明您已成功从身份组删除终端，但在终端身份组中重新分析这些终端。

## 用于授权规则的终端身份组

您可以在授权策略中有效地使用终端身份组来向所发现的终端提供相应的网络接入权限。例如，在思科 ISE 中，以下位置默认提供适用于所有类型思科 IP 电话的授权规则：**策略 (Policy) > 授权 (Authorization) > 标准 (Standard)**。

您必须确保终端分析策略为独立策略（而不是其他终端分析策略的父策略），或确保未禁用终端分析策略的父策略。

## 分析器源服务

分析器条件、例外操作和 NMAP 扫描操作分类为由思科提供或由管理员创建，如“系统类型” (System Type) 属性所示。终端分析策略会分类为由思科提供、由管理员创建或由管理员修改。这些分类显示在“系统类型” (System Type) 属性中。

您可以根据系统类型属性，对分析器条件、例外操作、NMAP 操作和终端分析策略执行不同的操作。您无法编辑或删除由思科提供的条件、例外操作和 NMAP 扫描操作。无法删除由思科提供的终端策略。编辑策略时，这些策略称为管理员修改的策略。源服务更新策略后，管理员修改的策略将替换为所基于的由思科提供的最新版本策略。

可以从思科源服务器检索新的和更新后的策略及更新的 OUI 数据库。必须已订阅思科 ISE。还可以接收有关已应用、成功和失败消息的电子邮件通知。可以将有关源服务操作的匿名信息发送回思科，这有助于思科改进源服务。

OUI 数据库包含分配给供应商的 MAC OUI。以下是 OUI 列表：<http://standards.ieee.org/develop/regauth/oui/oui.txt>

默认情况下，分析器源服务被禁用，并且需要 Plus 许可证启用该服务。启用分析器源服务时，思科 ISE 会在本地思科 ISE 服务器时区每天凌晨 1:00 下载策略和 OUI 数据库更新。思科 ISE 自动应用这些已下载的源服务器策略，其中存储了更改，因此可以将这些更改恢复到先前状态。恢复到先前状态时，将删除新的终端分析策略，而已更新的终端分析策略将恢复到先前状态。此外，分析器源服务将自动禁用。

## 配置分析器源服务

分析器源服务会从思科源服务器中检索新的和更新后的终端分析策略及 MAC OUI 数据库更新。如果源服务不可用或发生其他错误，系统会在 Operations Audit 报告中报告。

您可以将思科 ISE 配置为将匿名的馈送服务使用情况报告发回思科，这会向思科发送以下信息：

- Hostname: 思科 ISE 主机名
- MaxCount: 终端总数
- ProfiledCount: 已分析的终端计数
- UnknownCount: 未知终端计数
- MatchSystemProfilesCount: 思科提供的配置文件计数

- UserCreatedProfiles: 用户创建的配置文件计数

您可以更改由思科提供分析策略中的 CoA 类型。当源服务更新该策略时，CoA 类型不会更改，但该策略的其余属性仍会更新。

#### 开始之前

分析器源服务只可以从分布式部署中的思科 ISE 管理门户或在独立 ISE 节点中配置。

如果您计划从管理门户发送有关馈送更新的邮件通知，请设置简单邮件传输协议 (SMTP) 服务器 (**Administration > System > Settings**)。

- 
- 步骤 1** 选择 **管理 (Administration) > 证书 (Certificates) > 受信任证书 (Trusted Certificates)**，然后检查是否已启用 **Verisign Class 3 Public Primary Certification Authority** 和 **Verisign Class 3 Server CA - G3**。
  - 步骤 2** 选择 **管理 (Administration) > FeedService > 分析器 (Profiler)**。
  - 步骤 3** 选中 **Enable Profiler Feed Service** 复选框。
  - 步骤 4** 在 **Feed Service Scheduler** 部分以 HH:MM 格式（思科 ISE 服务器的本地时区）输入时间。默认情况下，思科 ISE 源服务安排在每天凌晨 1.00 点运行。
  - 步骤 5** 选中 **Administrator Notification Options** 部分中的 **Notify administrator when download occurs** 复选框，然后在 **Administrator email address** 文本框中输入您作为思科 ISE 管理员的邮箱地址。
  - 步骤 6** 选中 **Feed Service Subscriber Information** 部分中的 **Provide subscriber information to Cisco** 复选框，然后输入您作为思科 ISE 管理员的详细信息，以及作为备用思科 ISE 管理员的详细信息。
  - 步骤 7** 点击 **Accept**。
  - 步骤 8** 点击 **Save**。
  - 步骤 9** 点击 **Update Now**。

指示思科 ISE 联系思科源服务对自上次源服务以来创建的新的和更新后的配置文件进行更新。此操作会重新分析系统中的所有终端，这可能导致系统负载增加。由于终端分析策略经过更新，某些当前连接到思科 ISE 的终端的授权策略可能会发生更改。

当您对自上次源服务以来创建的新的和更新后的配置文件进行更新时，**Update Now** 按钮会被禁用，并且只会在下载完成后启用。您必须通过导航操作离开分析器源服务的配置窗口，然后返回此窗口。

- 步骤 10** 点击 **Yes**。

---

#### 相关主题

[离线配置分析器源服务](#)

## 删除终端分析策略的更新

您可以恢复在之前更新中已经更新的终端分析策略，并删除通过之前更新分析器源服务新添加的终端分析策略，但 OUI 更新不会更改。

如果在源服务器更新之后修改了终端分析策略，则系统中的终端分析策略不会更改。

步骤 1 选择 **选择管理 (Administration) > FeedService > 分析器 (Profiler)**。

步骤 2 选中 **Enable Profiler Feed Service** 复选框。

步骤 3 如果想要查看在 Change Configuration Audit 报告中所做的配置更改，请点击 **转到更新报告页面 (Go to Update Report Page)**。

步骤 4 点击 **Undo Latest**。

## 分析器报告

思科 ISE 为您提供关于终端分析的各种报告，以及可用于管理您的网络的故障排除工具。可以生成历史以及当前数据的报告。您还可以向下钻取报告的某个部分以查看更多详细信息。对于大型报告，您还可以安排报告计划并以各种格式下载这些报告。

您可以从 **操作 (Operations) > 报告 (Reports) > 终端和用户 (Endpoints and Users)** 为终端运行以下报告：

- Endpoint Session History
- Profiled Endpoint Summary
- Endpoint Profile Changes
- Top Authorizations by Endpoint
- Registered Endpoints

## 思科 ISE 与思科 NAC 设备集成

思科 ISE 仅支持与思科网络准入控制 (NAC) 设备版本 4.9 集成，并在思科 ISE 中已安装高级或无线许可证时可用。

思科 ISE 分析器类似于管理思科 NAC 部署中的终端的思科网络准入控制 (NAC) 分析器。通过此集成，您可以替换安装在思科 NAC 部署中的现有思科 NAC 分析器。您还可以将思科 ISE 分析器的配置文件名称和终端分类结果同步到 Cisco Clean Access Manager (CAM)。

## 管理节点中的思科 Clean Access Manager 配置

思科 ISE 允许您在分布式部署中的主 PAN 上注册多个 Clean Access Manager (CAM)，用于 REST API 通信设置。在思科 ISE 中注册的 CAM 列表是接收所有分析器配置更改通知的列表。主 PAN 负责思科 ISE 和思科 NAC 设备之间的所有通信。只能在思科 ISE 的主 PAN 中配置 CAM。在主 PAN 中注册一个或多个 CAM 时使用的凭证用来验证与 CAM 的连接。

思科 ISE 和思科网络准入控制设备之间通过安全套接字层 (SSL) 进行通信，安全可靠。此通信在本质上也是双向的，因为思科 ISE 将分析器配置更改推送到 CAM，CAM 会从思科 ISE 定期获取终端 MAC 地址及其对应配置文件的列表和所有配置文件名称列表。

您必须从 Clean Access Manager（管理 (Administration) > Clean Access Manager > SSL）导出 X509 证书的内容，并将其导入思科 ISE 中“管理” (Administration) > “系统” (System) > “证书” (Certificates) > “受信任证书库” (Trusted Certificates Store) 下的主 PAN，确保思科 ISE 和 CAM 之间实现正确、安全的通信。

关于如何设置 CAM 对以实现高可用性的详细信息，请参考下面的链接。

## 思科 ISE 分析器和思科 Clean Access Manager 通信

思科 ISE 分析器会向从主 PAN 注册的所有 Clean Access Manager (CAM) 通知分析器配置的更改。这样，可以避免在思科 ISE 分布式部署中发出重复通知。当思科 ISE 数据库中添加或删除终端并且终端分析策略发生变更时，分析器会使用 REST API 通知分析器配置的更改。导入终端期间，思科 ISE 分析器仅会在导入完成后通知 CAM。

实施以下 REST API 流程，将分析器配置的更改推送到 CAM：

思科 ISE 分析器终端更改推送 - 当终端经过分析并且思科 ISE 中的终端配置文件发生更改时，思科 ISE 分析器会向注册的所有 CAM 通知终端配置文件中的更改。

您可以在 CAM 中配置思科 ISE，这样便可以根据 CAM 中的同步设置，将 CAM 与思科 ISE 进行同步。您必须创建规则，即从思科 ISE 配置文件列表选择一个或多个匹配的配置文件，并将终端映射到 CAM 中的任何一种访问类型。CAM 会定期从思科 ISE 分析器检索终端及其相应的配置文件，以及所有配置文件名称的列表。

实施以下 REST API 流程，从思科 ISE 分析器提取分析器配置的更改：

- NAC 管理器终端提取 - 提取终端的 MAC 地址列表以及已知终端相应的配置文件。
- NAC 管理器配置文件提取 - 从思科 ISE 分析器提取配置文件的名称。

思科 ISE 分析器向思科 ISE 监控角色通知可用于监控思科 ISE 和思科网络准入控制设备版本 4.9 集成并排除其故障的所有事件。

思科 ISE 分析器日志捕获以下事件，以实现监控和故障排除的集成：

- NAC 设置的配置更改（信息）
- NAC 通知事件故障（错误）

## 添加思科 Clean Access Manager

如果将思科 ISE 与思科 NAC 设备版本 4.9 集成，您就可以在思科 NAC 部署中使用思科 ISE 分析服务。

您可以通过 NAC Managers 页面配置多个思科访问管理器 (CAM)，CAM 提供用于过滤您已注册的 CAM 的选项。此页面列出 CAM 及其名称、说明、IP 地址和显示是否已为这些 CAM 启用终端通知的状态。

步骤 1 选择管理 (Administration) > 网络资源 (Network Resources) > NAC 管理器 (NAC Managers)。

步骤 2 点击 Add。

步骤 3 输入思科访问管理器的名称。

步骤 4 点击 Status 复选框，启用从对连接进行身份验证的思科 ISE 分析器服务到 CAM 的 REST API 通信。

步骤 5 为 CAM 输入 IP 地址，0.0.0.0 和 255.255.255.255 这两个 IP 地址除外。

步骤 6 输入用于登录 CAM 用户界面的 CAM 管理员的用户名和密码。

步骤 7 点击提交。

## 客户端设备上的代理下载问题

### 问题

执行用户身份验证和授权之后，客户端设备浏览器显示“no policy matched”错误消息。此问题适用于身份验证的客户端调配阶段的用户会话。

### 可能的原因

客户端调配策略缺失必要的设置。

### 安全评估代理下载问题

请记住，下载安全评估代理安装程序需要满足以下要求：

- 首次在客户端设备上安装代理时，用户必须在浏览器会话中允许 ActiveX 安装程序。客户端调配下载页面会提示此要求。
- 客户端设备必须接入互联网。

### 解决方法

- 确保思科 ISE 中已有客户端调配策略。如果有，则验证策略中定义的策略身份组、条件和代理类型。另外，请确认在以下位置是否配置了任何代理配置文件：策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources) 添加 (Add) NAC 或 AnyConnect 终端安全评估配置文件 (NAC or AnyConnect Posture Profile)，包括采用所有默认值的配置文件。
- 尝试在接入交换机上回弹端口，对客户端设备重新执行身份验证。

## 终端

通过这些窗口，您可以配置和管理连接到您的网络的终端。

## 终端设置

表 78: 终端设置

字段名称	使用指南
<b>MAC 地址</b>	<p>输入十六进制格式的 MAC 地址以静态创建终端。</p> <p>MAC 地址是连接到启用思科 ISE 的网络的接口设备标识符。</p>
<b>Static Assignment</b>	<p>如果您想要在“终端”(Endpoints)窗口静态地创建终端并且已将静态分配的状态设置为静态，请选中此复选框。</p> <p>您可以将终端静态分配的状态从静态切换至动态或从动态切换至静态。</p>
<b>Policy Assignment</b>	<p>(除非选中<b>静态分配 (Static Assignment)</b>复选框，否则会默认禁用此字段)从<b>策略分配 (Policy Assignment)</b>下拉列表选择匹配的终端策略。</p> <p>您可以执行以下操作之一：</p> <ul style="list-style-type: none"> <li>如果您不选择匹配的终端策略，而是使用默认终端策略 Unknown，则对于允许对终端进行动态分析的终端，其静态分配状态要设置为动态。</li> <li>如果您选择“未知”(Unknown)之外的匹配终端策略，则对该终端，静态分配状态应设置为静态并且系统会自动选中<b>静态分配 (Static Assignment)</b>复选框。</li> </ul>
<b>Static Group Assignment</b>	<p>当您想要向身份组静态分配终端时，请选中此复选框。</p> <p>如果您选中此复选框，下一次为之前动态分配至其他终端身份组的这些终端评估终端策略期间，分析服务不会更改终端身份组。</p> <p>如果您取消选中此复选框，则像 ISE 分析器根据策略配置所分配的一样，终端身份组处于动态状态。如果不选择 Static Group Assignment 选项，下一次评估终端策略期间，系统会自动将终端分配至匹配的身份组。</p>

字段名称	使用指南
<b>Identity Group Assignment</b>	<p>选择您要将终端分配至哪个终端身份组。</p> <p>当您静态创建终端，或在为某个终端评估终端策略期间不想使用<b>创建匹配身份组 (Create Matching Identity Group)</b> 选项时，可将终端分配至身份组。</p> <p>思科 ISE 包括以下系统创建的终端身份组：</p> <ul style="list-style-type: none"> <li>• 黑名单</li> <li>• GuestEndpoints</li> <li>• Profiled <ul style="list-style-type: none"> <li>• Cisco IP-Phone</li> <li>• Workstation</li> </ul> </li> <li>• RegisteredDevices</li> <li>• Unknown</li> </ul>

#### 相关主题

[已识别的终端](#)，第 438 页

[使用策略和身份的静态分配创建终端](#)，第 434 页

## 从 LDAP 设置导入终端

表 79: 从 LDAP 设置导入终端

字段名称	使用指南
连接设置	
主机	输入 LDAP 服务器的主机名或 IP 地址。
Port	<p>输入 LDAP 服务器的端口号。您可以使用默认端口 389 从 LDAP 服务器导入，并使用默认端口 636 通过 SSL 从 LDAP 服务器导入。</p> <p>注释 思科 ISE 支持配置的任何端口号。配置值应与 LDAP 服务器连接的详细信息匹配。</p>
Enable Secure Connection	选中启用安全连接 ( <b>Enable Secure Connection</b> ) 复选框，通过 SSL 从 LDAP 服务器导入。
Root CA Certificate Name	<p>点击下拉箭头，查看受信任的 CA 证书。</p> <p>根 CA 证书名称指连接 LDAP 服务器所需的受信任 CA 证书。您可以在思科 ISE 中添加（导入）、编辑、删除并导出受信任的 CA 证书。</p>



字段名称	使用指南
<b>Anonymous Bind</b>	您必须选中 <b>匿名绑定 (Anonymous Bind)</b> 复选框，或输入 slapd.conf 配置文件中的 LDAP 管理员凭证。
<b>Admin DN</b>	输入 slapd.conf 配置文件中为 LDAP 管理员配置的可分辨名称 (DN)。 管理员 DN 格式示例：cn=Admin、dc=cisco.com、dc=com
<b>密码 (Password)</b>	输入 slapd.conf 配置文件中为 LDAP 管理员配置的密码。
<b>Base DN</b>	输入父项的可分辨名称。 基本 DN 格式示例：dc=cisco.com、dc=com。
<b>查询设置</b>	
<b>MAC Address objectClass</b>	输入用于导入 MAC 地址的查询过滤器，例如，ieee802Device。
<b>MAC Address Attribute Name</b>	输入导入操作返回的属性名称，例如，macAddress。
<b>Profile Attribute Name</b>	输入 LDAP 属性的名称。此属性为 LDAP 服务器中定义的每个终端条目保留策略名称。 当配置分析属性名称 ( <b>Profile Attribute Name</b> ) 字段时，请考虑以下事项： <ul style="list-style-type: none"> <li>• 如果未在分析属性名称 (<b>Profile Attribute Name</b>) 字段中指定此 LDAP 属性或错误地配置此属性，则执行导入操作期间系统会将终端标记为“未知” (Unknown)，并且会根据匹配的终端分析策略单独分析这些终端。</li> <li>• 如果您在分析属性名称 (<b>Profile Attribute Name</b>) 字段中配置此 LDAP 属性，系统会验证属性值，以确保终端策略与思科 ISE 中的现有策略相匹配，然后导入终端。如果终端策略与现有策略不匹配，则不会导入这些终端。</li> </ul>
<b>超时</b>	输入时间值（以秒为单位）。有效范围是从 1 到 60 秒。

**相关主题**

[已识别的终端](#)，第 438 页

[从 LDAP 服务器导入终端](#)，第 437 页

## 终端分析策略设置

表 80: 终端分析策略设置

字段名称	使用指南
<b>Name</b>	输入要创建的终端分析策略的名称。

字段名称	使用指南
<b>Description</b>	输入要创建的终端分析策略的说明。
<b>Policy Enabled</b>	默认情况下， <b>Policy Enabled</b> 复选框处于选中状态，以便在您分析终端时关联匹配的分析策略。 如果未选中此复选框，则在您分析终端时会排除终端分析策略。
<b>Minimum Certainty Factor</b>	输入要与分析策略相关联的最小值。默认值为 10。
<b>Exception Action</b>	选择在分析策略中定义规则时要与条件关联的例外操作。 默认值为 NONE。例外操作在以下位置定义： <b>策略 (Policy) &gt; 策略元素 (Policy Elements) &gt; 结果 (Results) &gt; 分析 (Profiling) &gt; 例外操作 (Exception Actions)</b> 。
<b>Network Scan (NMAP) Action</b>	从列表中选择在分析策略中定义规则时（如有必要）要与条件关联的网络扫描操作。 默认值为 NONE。例外操作在以下位置定义： <b>策略 (Policy) &gt; 策略元素 (Policy Elements) &gt; 结果 (Results) &gt; 分析 (Profiling) &gt; 网络扫描 (NMAP) 操作 (Network Scan (NMAP) Actions)</b> 。
<b>Create an Identity Group for the policy</b>	选择以下选项之一以创建终端身份组： <ul style="list-style-type: none"> <li>• <b>Yes, create matching Identity Group</b></li> <li>• <b>No, use existing Identity Group hierarchy</b></li> </ul>
<b>Yes, create matching Identity Group</b>	选择此选项以使用现有的分析策略。 此选项可为那些终端创建匹配的身份组，当终端配置文件与现有的分析策略相匹配时，身份组将是已分析的终端身份组的子项。 例如，在网络中发现的终端与 Xerox-Device 配置文件相匹配时，系统会在 Endpoints Identity Groups 页面创建 Xerox-Device 终端身份组。

字段名称	使用指南
<b>No, use existing Identity Group hierarchy</b>	<p>选中此复选框可使用分析策略和身份组的层次结构将终端分配给匹配的父终端身份组。</p> <p>通过此选项，可以使用终端分析策略层次结构将终端分配给其中一个匹配的父终端身份组，以及父身份组的关联终端身份组。</p> <p>例如，与现有配置文件相匹配的终端会归入相应的父终端身份组中。在本例中，与 Unknown 配置文件相匹配的终端会归入 Unknown 终端身份组中，与现有配置文件相匹配的终端会归入 Profiled 终端身份组中。例如，</p> <ul style="list-style-type: none"> <li>• 如果终端与 Cisco-IP-Phone 配置文件相匹配，则这些终端会归入 Cisco-IP-Phone 终端身份组中。</li> <li>• 如果终端与 Workstation 配置文件相匹配，则这些终端会归入 Workstation 终端身份组中。</li> </ul> <p>Cisco-IP-Phone 和 Workstation 终端身份组与系统中的 Profiled 终端身份组相关联。</p>
<b>Parent Policy</b>	<p>选择在系统中定义的、要与新终端分析策略相关联的父分析策略。</p> <p>可以选择可将规则和条件继承到其子项的父分析策略。</p>
<b>Associated CoA Type</b>	<p>选择以下要与终端分析策略相关联的 CoA 类型之一：</p> <ul style="list-style-type: none"> <li>• No CoA</li> <li>• 端口重启</li> <li>• Reauth</li> <li>• Global Settings，该设置是从在 Administration &gt; System &gt; Settings &gt; Profiling 中设置的分析器配置进行应用</li> </ul>
<b>Rules</b>	<p>在终端分析策略中定义的一个或多个规则为终端确定了匹配的分析策略，这允许您根据终端配置文件对终端进行分组。</p> <p>策略要素库中的一个或多个分析条件用于规则，以验证终端属性及其整体分类值。</p>

字段名称	使用指南
条件	<p>点击加号 [+] 展开 Conditions 固定重叠，点击减号 [-] 或点击固定重叠的外部可将其折叠。</p> <p>点击 <b>Select Existing Condition from Library</b> 或 <b>Create New Condition (Advanced Option)</b>。</p> <p><b>从库中选择现有条件 (Select Existing Condition from Library):</b> 可以通过从策略元素库中选择思科预定义条件来定义表达式。</p> <p><b>创建新条件 (Create New Condition) (高级选项):</b> 可以通过从各种系统或用户定义的字典中选择属性来定义表达式。</p> <p>可以将以下其中一项与分析条件相关联：</p> <ul style="list-style-type: none"> <li>• 每种条件的可信度的整数值。</li> <li>• 为该条件输入例外操作或网络扫描操作</li> </ul> <p>选择以下其中一个要与分析条件相关联的预定义设置：</p> <ul style="list-style-type: none"> <li>• “可信度增加” (Certainty Factor Increases): 为每个规则输入可信度值，可以为与整体分类相关的所有匹配规则添加此可信度值。</li> <li>• “采取例外操作” (Take Exception Action): 触发在此终端分析策略的“例外操作” (Exception Action) 字段中配置的例外操作。</li> <li>• “采取网络扫描操作” (Take Network Scan Action): 触发在此终端分析策略的“网络扫描 (NMAP) 操作” (Network Scan (NMAP) Action) 字段中配置的网络扫描操作。</li> </ul>
<b>Select Existing Condition from Library</b>	<p>可以执行以下操作：</p> <ul style="list-style-type: none"> <li>• 可以选择策略要素库中可用的思科预定义条件，然后使用 AND 或 OR 运算符添加多个条件。</li> <li>• 点击 Action 图标，在后续步骤中执行以下操作： <ul style="list-style-type: none"> <li>• <b>添加属性/值 (Add Attribute/Value):</b> 可以添加临时属性或值对</li> <li>• <b>从库中添加条件 (Add Condition from Library):</b> 可以添加思科预定义条件</li> <li>• <b>复制 (Duplicate):</b> 创建选定条件的副本</li> <li>• <b>将条件添加到库 (Add Condition to Library):</b> 可以将自行创建的临时属性/值对保存到策略元素库中</li> <li>• <b>删除 (Delete):</b> 删除所选条件。</li> </ul> </li> </ul>

字段名称	使用指南
<b>Create New Condition (Advance Option)</b>	<p>可以执行以下操作：</p> <ul style="list-style-type: none"> <li>• 可以将临时属性/值对添加到表达式，然后使用 AND 或 OR 运算符添加多个条件。</li> <li>• 点击 Action 图标，在后续步骤中执行以下操作： <ul style="list-style-type: none"> <li>• <b>添加属性/值 (Add Attribute/Value)</b>：可以添加临时属性或值对</li> <li>• <b>从库中添加条件 (Add Condition from Library)</b>：可以添加思科预定义条件</li> <li>• <b>复制 (Duplicate)</b>：创建选定条件的副本</li> <li>• <b>将条件添加到库 (Add Condition to Library)</b>：可以将自行创建的临时属性/值对保存到策略元素库中</li> <li>• <b>删除 (Delete)</b>：删除所选条件。可以使用 AND 或 OR 运算符</li> </ul> </li> </ul>

#### 相关主题

[思科 ISE 分析服务](#)，第 396 页

[创建终端分析策略](#)，第 426 页

## IF-MIB

对象	OID
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8

## SNMPv2-MIB

对象	OID
system	1.3.6.1.2.1.1

对象	OID
sysDescr	1.3.6.1.2.1.1.1.0
sysObjectID	1.3.6.1.2.1.1.2.0
sysUpTime	1.3.6.1.2.1.1.3.0
sysContact	1.3.6.1.2.1.1.4.0
sysName	1.3.6.1.2.1.1.5.0
sysLocation	1.3.6.1.2.1.1.6.0
sysServices	1.3.6.1.2.1.1.7.0
sysORLastChange	1.3.6.1.2.1.1.8.0
sysORTable	1.3.6.1.2.1.1.9.0

## IP-MIB

对象	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2

## CISCO-CDP-MIB

对象	OID
cdpCacheEntry	1.3.6.1.4.1.9.9.23.1.2.1.1
cdpCacheIfIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.1
cdpCacheDeviceIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.2
cdpCacheAddressType	1.3.6.1.4.1.9.9.23.1.2.1.1.3
cdpCacheAddress	1.3.6.1.4.1.9.9.23.1.2.1.1.4
cdpCacheVersion	1.3.6.1.4.1.9.9.23.1.2.1.1.5
cdpCacheDeviceId	1.3.6.1.4.1.9.9.23.1.2.1.1.6
cdpCacheDevicePort	1.3.6.1.4.1.9.9.23.1.2.1.1.7

对象	OID
cdpCachePlatform	1.3.6.1.4.1.9.9.23.1.2.1.1.8
cdpCacheCapabilities	1.3.6.1.4.1.9.9.23.1.2.1.1.9
cdpCacheVIPMgmtDomain	1.3.6.1.4.1.9.9.23.1.2.1.1.10
cdpCacheNativeVLAN	1.3.6.1.4.1.9.9.23.1.2.1.1.11
cdpCacheDuplex	1.3.6.1.4.1.9.9.23.1.2.1.1.12
cdpCacheApplianceID	1.3.6.1.4.1.9.9.23.1.2.1.1.13
cdpCacheVlanID	1.3.6.1.4.1.9.9.23.1.2.1.1.14
cdpCachePowerConsumption	1.3.6.1.4.1.9.9.23.1.2.1.1.15
cdpCacheMTU	1.3.6.1.4.1.9.9.23.1.2.1.1.16
cdpCacheSysName	1.3.6.1.4.1.9.9.23.1.2.1.1.17
cdpCacheSysObjectID	1.3.6.1.4.1.9.9.23.1.2.1.1.18
cdpCachePrimaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.19
cdpCachePrimaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.20
cdpCacheSecondaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.21
cdpCacheSecondaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.22
cdpCachePhysLocation	1.3.6.1.4.1.9.9.23.1.2.1.1.23
cdpCacheLastChange	1.3.6.1.4.1.9.9.23.1.2.1.1.24

## CISCO-VTP-MIB

对象	OID
vtpVlanIfIndex	1.3.6.1.4.1.9.9.46.1.3.1.1.18.1
vtpVlanName	1.3.6.1.4.1.9.9.46.1.3.1.1.4.1
vtpVlanState	1.3.6.1.4.1.9.9.46.1.3.1.1.2.1

## CISCO-STACK-MIB

对象	OID
portIfIndex	1.3.6.1.4.1.9.5.1.4.1.1.11
vlanPortVlan	1.3.6.1.4.1.9.5.1.9.3.1.3.1

## BRIDGE-MIB

对象	OID
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

## OLD-CISCO-INTERFACE-MIB

对象	OID
locIfReason	1.3.6.1.4.1.9.2.2.1.1.20

## CISCO-LWAPP-AP-MIB

对象	OID
cLApEntry	1.3.6.1.4.1.9.9.513.1.1.1
cLApSysMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1
cLApIfMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.2
dApMxNmbrOfDtlsSts	1.3.6.1.4.1.9.9.513.1.1.1.3
cLApEntPhysicalIndex	1.3.6.1.4.1.9.9.513.1.1.1.4
cLApName	1.3.6.1.4.1.9.9.513.1.1.1.5
cLApUpTime	1.3.6.1.4.1.9.9.513.1.1.1.6
cLLwappUpTime	1.3.6.1.4.1.9.9.513.1.1.1.7
cLLwappJoinTakenTime	1.3.6.1.4.1.9.9.513.1.1.1.8
dApMxNmbrOfHuntSts	1.3.6.1.4.1.9.9.513.1.1.1.9



对象	OID
dApPrimaryControlAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.10
dApPrimaryControlAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.11
dApSecondaryControlAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.12
dApSecondaryControlAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.13
dApTertiaryControlAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.14
dApTertiaryControlAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.15
cLApLastRebootReason	1.3.6.1.4.1.9.9.513.1.1.1.1.16
cLApEncryptionEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.17
cLApFailoverPriority	1.3.6.1.4.1.9.9.513.1.1.1.1.18
cLApPowerStatus	1.3.6.1.4.1.9.9.513.1.1.1.1.19
cLApTelnetEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.20
cLApSshEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.21
cLApPreStdStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.22
dApPwrInjectorStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.23
cLApPwrInjectorSelection	1.3.6.1.4.1.9.9.513.1.1.1.1.24
dApPwrInjectorSwMacAddr	1.3.6.1.4.1.9.9.513.1.1.1.1.25
cLApWipsEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.26
dApMonitorModeOptimization	1.3.6.1.4.1.9.9.513.1.1.1.1.27
cLApDomainName	1.3.6.1.4.1.9.9.513.1.1.1.1.28
dApNameServerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.29
dApNameServerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.30
cLApAMSDUEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.31
cLApEncryptionSupported	1.3.6.1.4.1.9.9.513.1.1.1.1.32
dApRegulationDetectionEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.33

## CISCO-LWAPP-DOT11-CLIENT-MIB

对象	OID
cldcClientEntry	1.3.6.1.4.1.9.9.599.1.3.1.1
cldcClientMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.1
cldcClientStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.2
cldcClientWanProfileName	1.3.6.1.4.1.9.9.599.1.3.1.1.3
cldcClientWgbStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.4
cldcClientWgbMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.5
cldcClientProtocol	1.3.6.1.4.1.9.9.599.1.3.1.1.6
cldcAssociationMode	1.3.6.1.4.1.9.9.599.1.3.1.1.7
cldcApMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.8
cldcIfType	1.3.6.1.4.1.9.9.599.1.3.1.1.9
cldcClientIPAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.10
cldcClientNacState	1.3.6.1.4.1.9.9.599.1.3.1.1.11
cldcClientQuarantineVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.12
cldcClientAccessVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.13
cldcClientLoginTime	1.3.6.1.4.1.9.9.599.1.3.1.1.14
cldcClientUpTime	1.3.6.1.4.1.9.9.599.1.3.1.1.15
cldcClientPowerSaveMode	1.3.6.1.4.1.9.9.599.1.3.1.1.16
cldcClientCurrentTxRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.17
cldcClientDataRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.18

## CISCO-AUTH-FRAMEWORK-MIB

对象	OID
cafPortConfigEntry	1.3.6.1.4.1.9.9.656.1.2.1.1
cafSessionClientMacAddress	1.3.6.1.4.1.9.9.656.1.4.1.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.1.5

对象	OID
cafSessionDomain	1.3.6.1.4.1.9.9.656.1.4.1.1.6
cafSessionAuthUserName	1.3.6.1.4.1.9.9.656.1.4.1.1.10
cafSessionAuthorizedBy	1.3.6.1.4.1.9.9.656.1.4.1.1.12
cafSessionAuthVlan	1.3.6.1.4.1.9.9.656.1.4.1.1.14

## EEE8021-PAE-MIB: RFC IEEE 802.1X

对象	OID
dot1xAuthControlPcStat	1.0.8802.1.1.1.2.1.1.5
dot1xAuthControlPcCtrl	1.0.8802.1.1.1.2.1.1.6
dot1xAuthSessionUserName	1.0.8802.1.1.1.2.4.1.9

## HOST-RESOURCES-MIB

对象	OID
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5

## LLDP-MIB

对象	OID
lldpEntry	1.0.8802.1.1.2.1.4.1.1
lldpTimeMark	1.0.8802.1.1.2.1.4.1.1.1
lldpLocalPortNum	1.0.8802.1.1.2.1.4.1.1.2
lldpIndex	1.0.8802.1.1.2.1.4.1.1.3
lldpChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4
lldpChassisId	1.0.8802.1.1.2.1.4.1.1.5
lldpPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6
lldpPortId	1.0.8802.1.1.2.1.4.1.1.7

对象	OID
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
lldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12

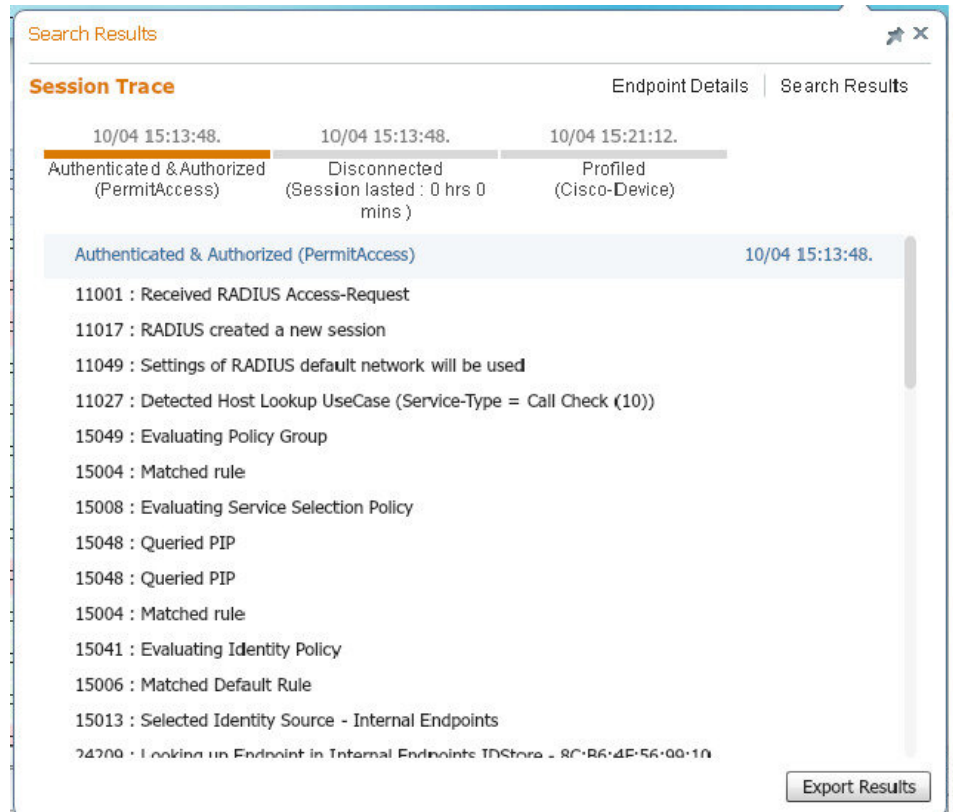
## 终端的会话跟踪

您可以使用思科 ISE 首页顶部的全局搜索框来获得某个终端的会话信息。当使用条件进行搜索时，您将会看到终端列表。点击其中任意终端以查看该终端的会话跟踪信息。下图所示为终端会话跟踪信息的示例。



**注释** 用于搜索的数据集基于作为索引的终端 ID。因此，当进行身份验证时，对于包括在搜索结果集中的身份验证，必须具有终端 ID。

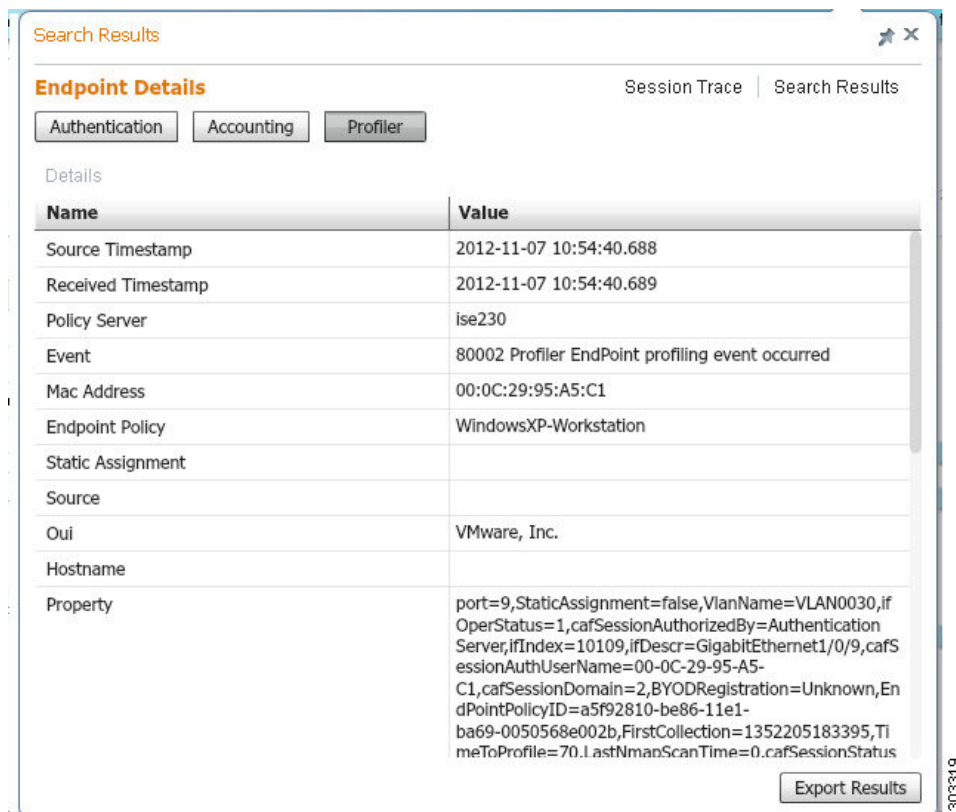
图 20: 终端的会话跟踪



您可以使用顶部可点击的时间表来查看主要的授权过渡。还可以使用导出结果 (**Export Results**) 选项导出 .csv 格式的结果。报告会下载到您的浏览器。

可以点击终端详细信息 (**Endpoint Details**) 链接查看特定终端的更多身份验证、记帐和分析器信息。下图所示为所显示的终端详细信息。

图 21: 终端详细信息



## 从目录清除会话

在监控和故障排除节点上，会话按以下方式从会话目录中清除：

- 已终止会话会在终止 15 分钟后清除。
- 如果存在身份验证但无记账，则此类会话将在一个小时后清除。
- 所有非活动会话在五天之后清除。

## 终端的全局搜索

您可以使用思科 ISE 首页顶部全局搜索框搜索终端。您可以使用以下任何条件搜索终端：

- 用户名
- MAC 地址
- IP 地址
- 授权配置文件

- 终端配置文件
- 失败原因
- 身份组
- 身份库
- 网络设备名称
- 网络设备类型
- 操作系统
- 安全评估状态
- 位置
- 安全组
- 用户类型

对于任何搜索条件，您应在搜索字段中至少输入三个字符以显示数据。

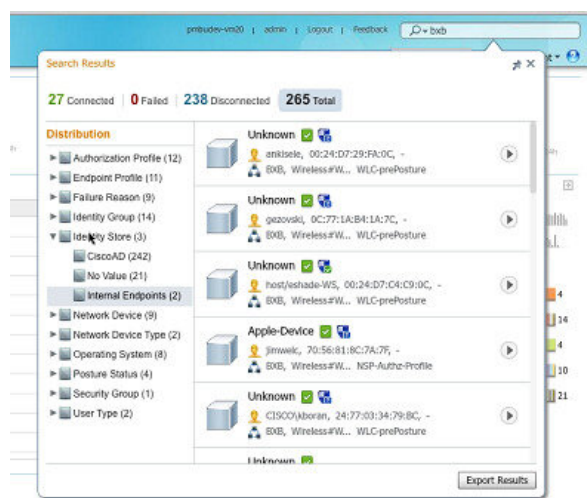


**注释** 如果终端已由思科 ISE 进行身份验证，或其审计更新已收到，则可通过全局搜索找到该终端。搜索结果中不会显示已手动添加但未由思科 ISE 进行身份验证或未在思科 ISE 中说明的终端。

搜索结果提供终端当前状态的详细和概览信息，可用于故障排除。搜索结果仅显示前25个条目。您可以使用过滤器来缩小结果范围。

下图为搜索结果的示例：

图 22: 终端的搜索结果



您可以使用左侧面板中的任何属性过滤结果。您也可以点击任意终端查看该终端的详细信息，例如：

- 跟踪会话
- 身份验证详细信息
- 记帐详细信息
- 安全评估详细信息
- 分析器详细信息
- 客户端调配详细信息
- 访客记帐和活动





## 第 10 章

# 自带设备 (BYOD)

- [公司网络上的个人设备 \(BYOD\)](#)，第 465 页
- [个人设备门户](#)，第 466 页
- [支持使用本地请求方注册设备](#)，第 471 页
- [设备门户配置任务](#)，第 473 页
- [管理员工添加的个人设备](#)，第 485 页
- [监控我的设备门户和终端活动](#)，第 486 页

## 公司网络上的个人设备 (BYOD)

支持公司网络上的个人设备时，必须验证和授权用户（员工、承包商和访客）及其设备，保护网络服务和企业数据。思科 ISE 提供相关工具，允许员工在公司网络上安全地使用个人设备。

登录访客门户时，访客能够自动注册其设备。访客可以注册更多设备，直到达到您为其访客类型定义的最大限制。这些设备会根据门户配置注册到终端身份组中。

访客可以通过运行本地请求方调配（网络设置助手）或通过将其设备添加到“我的设备” (MyDevices) 门户，将其个人设备添加到网络。您可以根据操作系统创建本地请求方配置文件，后者决定着应该使用的适当本地请求方调配向导。

因为不是所有设备都能够使用本地请求方配置文件，所以用户可以使用我的设备门户手动添加这些设备；或者您可以配置 BYOD 规则，注册这些设备。

## 分布式环境中的最终用户设备门户

思科 ISE 最终用户 Web 门户根据管理、策略服务和监控角色，提供配置、会话支持和报告功能。

- **策略管理节点 (PAN)**：您对用户、设备和最终用户门户所做的配置更改会写入 PAN。
- **策略服务节点 (PSN)**：最终用户门户在 PSN 上运行，后者处理所有会话流量，包括网络访问、客户端调配、访客服务、终端安全评估和分析。如果 PSN 是节点组的一部分，并且一个节点发生故障，则其他节点会检测到故障，并重置任何挂起的会话。

- **监控节点 (MnT 节点)**：MnT 节点在我的设备门户、发起人门户和访客门户上收集、聚合和报告有关最终用户和设备活动的的数据。如果主 MnT 节点故障，则辅助 MnT 节点自动成为主 MnT 节点。

## 设备门户的全局设置

选择 **工作中心 (Work Centers) > BYOD > 设置 (Settings) > 员工注册的设备 (Employee Registered Devices)** 或 **管理 (Administration) > 设备门户管理 (Device Portal Management) > 设置 (Settings)**。

您可以为 BYOD 门户和 My Devices 门户配置以下常规设置：

- **员工注册的设备 (Employee Registered Devices)**：在 **将员工限制为 (Restrict employees to)** 中输入员工可注册的最大设备数量。默认情况下，此值设置为 **5** 台设备。
- **重试 URL (Retry URL)**：在 **重试激活 URL (Retry URL for onboarding)** 中输入可用于将设备重定向至思科 ISE 的 URL。

当您配置这些常规设置后，它们适用于为您的公司设置的所有 BYOD 门户和 My Devices 门户。

### 相关主题

[限制员工注册的个人设备的数量](#)，第 471 页

[提供用于重新连接 BYOD 注册流程的 URL](#)，第 472 页

[分布式环境中的最终用户设备门户](#)，第 465 页

## 个人设备门户

思科 ISE 提供若干基于 Web 的门户，支持员工自有的个人设备。这些设备门户不参与访客或发起人门户流。

- **黑名单门户 (Blacklist Portal)**：提供关于被列入阻止列表且无法用于获得网络访问权限的个人设备的信息。
- **BYOD 门户 (BYOD Portals)**：使员工能够使用本地请求方调配功能注册其个人设备。
- **客户端调配门户 (Client Provisioning Portals)**：强制员工在其设备上下载终端安全评估代理，用来检查合规性。
- **MDM 门户 (MDM Portals)**：使员工能够在外部移动设备管理 (MDM) 系统中登记其移动设备。
- **我的设备门户 (My Devices Portals)**：使员工能够添加和注册个人设备，包括不支持本地请求方调配的个人设备，然后管理这些设备。

通过思科 ISE，您可以在思科 ISE 服务器上托管多个设备门户，包括一组预定义的默认门户。默认门户主题具有标准思科品牌，您可以通过管理员门户（**管理 (Administration) > 设备门户管理 (Device Portal Management)**）对其进行自定义。此外，还可以选择上传组织特有的图片、徽标和级联样式表 (CSS) 文件，进一步自定义门户。

## 访问设备门户

可以从思科 ISE GUI 访问任何个人设备门户，如下所示：

**步骤 1** 选择 **管理 (Administration) > 设备门户管理 (Device Portal Management)**。

**步骤 2** 选择您要配置的特定设备门户。

## 黑名单门户

员工不直接访问该门户，但可被重新定向到该门户。

如果员工丢失个人设备或设备被盗，他们可以在我的设备门户更新设备状态，将设备添加到黑名单终端身份组。这可以防止其他人使用该设备进行未经授权的网络访问。如果有人尝试使用黑名单中的某个设备连接网络，他们将被重新定向到 **Blacklist** 门户，并且被告知该设备禁止接入网络。如果找到设备，员工可以恢复设备（在我的设备门户），在无需重新注册设备的情况下重新获得网络访问权限。根据设备是丢失还是被盗，设备可能需要经过额外调配，才能连接到网络。

您可以为黑名单门户配置端口设置（默认为端口 8444）。如果更改端口号，请确保此端口号未被其他最终用户门户使用。

有关配置黑名单门户的信息，请参阅[编辑黑名单门户](#)，第 476 页。

## 自带设备门户

员工无法直接访问该门户。

当员工使用本地请求方注册个人设备时，员工会被重定向至自带设备 (BYOD) 门户。员工首次尝试使用个人设备访问网络时，系统会提示员工手动下载并启动网络设置助理 (NSA) 向导并引导他们完成注册和安装本地请求方。员工注册设备后，就可以使用 My Devices 门户管理设备。

如果您使用 Microsoft Edge 93 或 Microsoft Edge 94 作为下载 NSA 和 AnyConnect 向导的 Web 浏览器，请在新选项卡中复制并粘贴重定向的 **redirected URL** 或 **下载链接**，然后按键盘上的 **Enter** 键。

或者，您也可以单击 **下载图标** > 右键单击下载的文件 **Microsoft Edge 93** 或 **Microsoft Edge 94** 浏览器上的 > **保留文件 (Keep file)**。

如果您使用 Google Chrome 93 或 Google Chrome 95 作为 Web 浏览器来下载 Network Setup Assistant (NSA) 和 AnyConnect 向导，请点击下载通知中的 **保留 (Keep)** 选项，以便在系统上保留和安装 NSA 和 AnyConnect 软件包。



### 注释

- 当设备连接到使用网络访问管理器 (NAM) 的网络时，不支持 BYOD 流量。
- 如果您为 Android 设备使用 BYOD 流程，请升级到 Android 11 或在 WLAN 配置中启用“广播 SSID” (Broadcast SSID) 选项。

### 相关主题

[创建 BYOD 门户](#)，第 478 页

[公司网络上的个人设备 \(BYOD\)](#)，第 465 页

## 客户端调配门户

员工不直接访问该门户，但可被重新定向到该门户。

客户端调配系统为尝试访问公司网络的设备提供终端安全评估和补救。当员工使用设备请求网络访问时，您可以将他们路由至客户端调配门户，要求他们首先下载终端安全评估代理。终端安全评估代理扫描设备以检查合规性，例如验证设备是否已安装病毒防护软件，操作系统是否受支持。

### 相关主题

[创建客户端调配门户](#)，第 480 页

## 移动设备管理门户

员工不直接访问该门户，但可被重新定向到该门户。

许多公司使用移动设备管理 (MDM) 系统管理员工的移动设备。

思科 ISE 允许与外部 MDM 系统集成，员工使用这些系统注册他们的移动设备并访问公司网络。思科提供一个外部 MDM 接口，员工可用其注册他们的设备并连接到网络。

MDM 门户允许员工在一个外部 MDM 系统中注册。

员工可使用“我的设备”门户管理他们的移动设备，例如使用 PIN 码锁定设备、恢复设备出厂设置、或移除注册设备时所安装的应用和设置。

有关将 MDM 服务器配置为与思科 ISE 配合使用的信息，请参阅[创建 MDM 门户](#)，第 481 页。

## 我的设备门户

员工可以直接访问我的设备门户。

某些需要网络接入的网络设备不受本地请求方调配支持，并且无法使用 BYOD 门户进行注册。但是，员工可以使用“我的设备” (My Devices) 门户添加和注册其操作系统不受支持或没有 Web 浏览器的个人设备（例如打印机、互联网广播和其他设备）。

员工可以通过输入设备的 MAC 地址添加和管理新设备。当员工使用我的设备门户添加设备时，思科 ISE 将设备作为 **RegisteredDevices** 终端身份组的成员添加到“终端” (Endpoints) 窗口（**管理 (Administration) > 情景可视性 (Context Visibility) > 终端 (Endpoints)**），除非它们已经静态分配到其他终端身份组。设备如同思科 ISE 中的任何其他终端一样进行分析，并且完成注册过程以接入网络。

当用户向“我的设备” (My Devices Portal) 门户中输入一台设备上的两个 MAC 地址时，分析会确定它们具有相同主机名，并在思科 ISE 中将它们合并为单个条目。例如，用户注册具有有线和无线地址的笔记本电脑。该设备的所有操作（例如删除）对两个地址都会执行。

从门户中删除注册设备时，**DeviceRegistrationStatus** 和 **BYODRegistration** 属性会分别更改为未注册 (**Not Registered**) 和否 (**No**)。但是，当访客（不是员工）使用需要提供凭证的访客门户中的“访客设备注册” (**Guest Device Registration**) 窗口注册设备时，这些属性保持不变，因为这些 BYOD 属性仅在员工设备注册过程中使用。

无论员工使用 BYOD 门户还是我的设备门户注册其设备，他们都可以使用我的设备门户管理这些设备。

#### 相关主题

[创建我的设备门户](#)，第 482 页

## BYOD 部署选项和状态流

支持个人设备的 BYOD 部署流程根据以下因素而略有不同：

- **单或双 SSID**：使用单 SSID 时，认证登记、调配和网络访问都使用同一无线本地区域网络 (WLAN)。在双 SSID 部署中，有两个 SSID。一个用来登记和调配，另一个提供安全网络访问。
- **Windows、MacOS、iOS 或 Android 设备**：无论设备类型如何，本地请求方流程开始时都相似：将使用支持的个人设备的员工重定向至 BYOD 门户以确认其设备信息。此流程因设备类型而异。

#### 员工连接至网络

1. 思科 ISE 根据公司 Active Directory 或其他公司身份存储区对员工的凭证进行身份验证并提供授权策略。
2. 设备被重定向至 BYOD 门户。设备的 MAC 地址字段已预配置，用户可以添加设备名称和说明。
3. 已配置本地请求方 (MacOS、Windows、iOS、Android)，但是此流程因设备而异：
  - **MacOS 和 Windows 设备**：员工在 BYOD 门户中点击注册 (**Register**) 以下载和安装请求方调配向导 (网络设置助理)，此向导会配置请求方并提供证书 (如果必要)，用于基于 EAP-TLS 证书的身份验证。颁发的证书嵌有设备的 MAC 地址和员工的用户名。

从 MacOS 10.15 开始，用户必须允许下载请求方调配向导 (SPW)。用户设备上会显示一个窗口，要求他们允许或拒绝从思科 ISE 服务器下载。



**注释** 网络设置助理无法下载到 Windows 设备，除非该设备的用户具有管理权限。如果无法授予最终用户管理权限，则使用组策略对象 (GPO) 将证书推送到用户的设备，而不是使用 BYOD 流。

- **iOS 设备**：思科 ISE 策略服务器使用 Apple 的 iOS 空中下载功能向 iOS 设备发送新配置文件，其中包括：
  - 颁发的证书 (如已配置) 嵌有 iOS 设备的 MAC 地址和员工的用户名。

- 强制使用 EAP-TLS 进行 802.1X 身份验证的 Wi-Fi 请求方配置文件。可在终端设备上安装额外的配置文件，以保护无线 (OTA) 通信。

仅在隐藏实际 Wi-Fi 网络时，选中目标网络隐藏时启用 (**Enable if Target Network is Hidden**) 复选框。否则，不能为某些 iOS 设备调配 Wi-Fi 网络配置，尤其是在单 SSID 流中（在这种情况下，激活和连接使用同一个 Wi-Fi 网络或 SSID）。

- **Android 设备：**思科 ISE 会提示并引导员工从 Google Play 商店下载网络设置助理 (NSA)。安装应用后，员工可以打开 NSA 并启动设置向导，该向导会生成请求方配置和用于配置设备的已颁发证书。
4. 在用户完成激活流程后，思科 ISE 会发起授权更改 (CoA)。这会导致 MacOS、Windows 和 Android 设备重新连接到安全 802.1X 网络。对于单 SSID，iOS 设备也会自动连接；但是对于双 SSID，向导会提示 iOS 用户手动连接新网络。

您可以配置不使用请求方的 BYOD 流。有关详细信息，请参阅[思科 ISE 社区资源](#)文档。



**注释** 此流未启用 MAC 随机化。

每当创建新的连接配置文件时，Android 10 都会生成随机 MAC 地址，因此您必须修改默认规则，从授权配置文件中删除 *BYOD\_is\_Registered* 和 *MAC\_in\_SAN* 条件，BYOD 流程才能与 Android 客户端配合使用。

### BYOD 会话终端属性

终端属性 *BYODRegistration* 的状态在 BYOD 流期间更改为以下状态。

- 未知 (*Unknown*): 设备尚未通过 BYOD 流。
- 是 (*Yes*): 设备已通过 BYOD 流，并已注册。
- 否 (*No*): 设备已通过 BYOD 流，但未注册。这意味着设备已删除。

### 设备注册状态终端属性

终端属性 *DeviceRegistrationStatus* 的状态在设备注册期间更改为以下状态。

- 已注册 (*Registered*): 设备已通过 BYOD 流，并且已注册。属性从待处理状态更改为已注册状态之间有 20 分钟的延迟。
- 待处理 (*Pending*): 设备已通过 BYOD 流，并且已注册。但是，思科 ISE 尚未在网络上看到它。
- 未注册 (*Not Registered*): 设备尚未通过 BYOD 流。未注册 (*Not Registered*) 是 *DeviceRegistrationStatus* 属性的默认状态。
- 被盗 (*Stolen*): 用户登录我的设备门户，并将当前已激活的设备标记为“被盗” (*Stolen*)。这会在以下情况下发生：

- 如果设备是通过调配证书和配置文件激活的，则思科 ISE 会撤销调配到设备的证书，并将设备的 MAC 地址分配给黑名单终端身份组。该设备不再具有网络访问权限。
- 如果设备是通过调配配置文件（无证书）激活的，则思科 ISE 会将设备分配到黑名单终端身份组。设备仍然具有网络访问权限，除非您为此情况创建授权策略。例如，**IF Endpoint Identity Group is Blacklist AND BYOD\_is\_Registered THEN DenyAccess**。

管理员执行能够禁用多个设备的网络访问的操作，如删除或撤销证书。

如果用户恢复被盗的设备，则状态会恢复为未注册 (*Not Registered*)。用户必须删除该设备，然后重新添加。这会启动激活过程。

- 丢失 (*Lost*): 用户登录“我的设备”门户，并将当前已激活的设备标记为丢失 (*Lost*)，从而导致以下操作：
  - 设备被分配到黑名单身份组。
  - 调配到设备的证书不会被撤销。
  - 设备状态更新为丢失 (*Lost*)。
  - *BYODRegistration* 状态更新为否 (*No*)。

除非创建授权策略来阻止丢失的设备，否则丢失的设备仍具有网络访问权限。您可以在规则中使用黑名单身份组或 *endpoint:BYODRegistration* 属性。例如，**IF Endpoint Identity Group is Blacklist AND EndPoints:BYODRegistrations Equals No THEN BYOD**。如需更精细的访问，还可以将 *NetworkAccess:EAPAuthenticationMethod Equals PEAP or EAP-TLS or EAP-FAST*，*InternalUser:IdentityGroup Equals <<group>>* 添加到规则的 IF 部分。

## 限制员工注册的个人设备的数量

可以允许员工注册 1 至 100 台个人设备。无论员工用于注册个人设备的门户如何，此设置均可定义在所有门户上注册的最大设备数量。

**步骤 1** 选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **设置 (Settings)** > **员工注册的设备 (Employee Registered Devices)**。

**步骤 2** 在将员工限制为 (**Restrict employees to**) 中输入员工可注册的最大设备数量。默认情况下，此值设置为 5 台设备。

**步骤 3** 点击 **Save**。如果不想保存对设置进行的任何更新，请点击 **Reset** 以恢复为上次保存的值。

## 支持使用本地请求方注册设备

您可以创建本地请求方配置文件来支持思科 ISE 网络上的个人设备。根据您与用户的授权要求相关联的配置文件，思科 ISE 提供必要的请求方向来设置用户的个人设备以访问网络。

员工首次尝试使用个人设备访问网络时，系统会自动引导其完成注册和请求方配置。在其注册设备后，可以使用我的设备门户管理其设备。

## 本地请求方支持的操作系统

以下操作系统支持本地请求方：

- Android（Amazon Kindle 和 B&N Nook 除外）
- Mac OS（适用于 Apple Mac 计算机）
- Apple iOS 设备（Apple iPod、iPhone 和 iPad）
- Microsoft Windows 7 和 8（RT 除外）、Vista 和 10

## 允许员工使用需要提供凭证的访客门户注册个人设备

使用需要提供凭证的访客门户的员工可以注册其个人设备。员工通过 BYOD 门户提供的自行调配流程可以使用本地请求方（可用于 Windows、MacOS、iOS 和 Android 设备）将设备直接连接至网络。

### 开始之前

您必须创建本地请求方配置文件。

---

**步骤 1** 选择 **访客访问 (Guest Access) > 访客门户 (Guest Portals)**。

**步骤 2** 选择您希望允许员工用于使用本地请求方注册其个人设备的需要提供凭证的访客门户，然后点击 **Edit**。

**步骤 3** 点击门户行为和流设置 (**Portal Behavior and Flow Settings**) 选项卡。

**步骤 4** 在 **BYOD 设置 (BYOD Settings)** 下，选中允许员工在网络上使用个人设备 (**Allow employees to use personal devices on the network**) 复选框。

**步骤 5** 点击保存 (**Save**)。

---

## 提供用于重新连接 BYOD 注册流程的 URL

您可以提供信息，让使用 BYOD 门户注册其个人设备遇到问题的员工重新连接到注册过程。

---

**步骤 1** 选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > 设置 (Settings) > 重试 URL (Retry URL)**。

**步骤 2** 在 **重试激活 URL (Retry URL for onboarding)** 字段中，输入用于将设备重定向至思科 ISE 的 URL。

当设备在注册过程中遇到问题时，它将尝试自动重新连接到互联网。此时，您在此处输入的 URL 会将设备重定向到思科 ISE（重新启动激活过程）。默认值为 1.1.1.1。

**步骤 3** 点击 **Save**。



如果不想保存对设置进行的任何更新，请点击 **Reset** 以恢复为上次保存的值。

## 设备门户配置任务

您可以使用默认门户及其默认设置，例如证书、终端身份组、身份源序列、门户主题、图像和思科 ISE 提供的其他详细信息。如果您不想使用默认设置，则应创建新门户或编辑现有门户来满足需要。如果要创建多个具有相同设置的门户，则可以复制门户。

在创建新门户或编辑默认门户后，您必须授权使用该门户。授权使用门户后，您所进行的任何后续配置更改便会立即生效。

不需要授权使用我的设备门户。

如果您选择删除门户，则必须先删除与其关联的任何授权策略规则和授权配置文件，或者将其修改为使用其他门户。

使用以下针对配置不同设备门户相关任务编制的表格。

任务	黑名单门户	BYOD 门户	客户端调配门户	MDM 门户	我的设备门户
<a href="#">启用策略服务，第 474 页</a>	必填	必填	必填	必填	必填
<a href="#">将证书添加到设备门户，第 474 页</a>	必填	必填	必填	必填	必填
<a href="#">创建外部身份源，第 475 页</a>	不是必填项	不是必填项	不是必填项	不是必填项	必填
<a href="#">创建身份源序列，第 475 页</a>	不是必填项	不是必填项	不是必填项	不是必填项	必填
<a href="#">创建终端身份组，第 476 页</a>	不是必填项	必填	不是必填项	必填	必填
<a href="#">编辑黑名单门户</a>	必填	不适用	不适用	不适用	不适用
<a href="#">创建 BYOD 门户，第 478 页</a>	不适用	必填	不适用	不适用	不适用
<a href="#">创建客户端调配门户，第 480 页</a>	不适用	不适用	必填	不适用	不适用

任务	黑名单门户	BYOD 门户	客户端调配门户	MDM 门户	我的设备门户
创建 MDM 门户，第 481 页	不适用	不适用	不适用	必填	不适用
创建我的设备门户，第 482 页	不适用	不适用	不适用	不适用	必填
创建授权配置文件，第 483 页	不适用	必填	必填	必填	不是必填项
自定义设备门户，第 485 页	可选	可选	可选	可选	可选

## 启用策略服务

为了支持思科 ISE 最终用户 Web 门户，您必须在用于托管门户的节点上启用门户-策略服务。

**步骤 1** 依次选择管理 (Administration) > 系统 (System) > 部署 (Deployment)。

**步骤 2** 点击节点并点击 **Edit**。

**步骤 3** 在常规设置 (General Settings) 选项卡下，选中策略服务 (Policy Service) 复选框。

**步骤 4** 选中启用会话服务 (Enable Session Services) 复选框。

**步骤 5** 点击保存 (Save)。

## 将证书添加到设备门户

如果不希望使用默认证书，您可以添加一个有效证书，并将其分配到证书组标签。用于所有最终用户 Web 门户的默认证书组标签为默认门户证书组 (Default Portal Certificate Group)。

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

**步骤 2** 添加一个系统证书并将其分配到您希望用于该门户的证书组标签。

在创建或编辑门户期间，此证书组标签可供选择。

**步骤 3** 选择 管理 (Administration) > 设备门户管理 (Device Portal Management) > (任意门户) > 创建或编辑 (Create or Edit) > 门户设置 (Portal Settings)。

**步骤 4** 从与新添加证书关联的 **Certificate Group Tag** 下拉列表中选择特定的证书组标签。



注释

- BYOD 不支持超过三个证书的证书链。
- 在 BYOD 激活期间，系统会为 iOS 设备颁发两次证书。

## 创建外部身份源

思科 ISE 能够与外部身份源（例如 Active Directory、LDAP、RADIUS 令牌和 RSA SecurID 服务器）连接，以获取用于身份验证和授权的用户信息。外部身份源还包括执行基于证书的身份验证所需的证书身份验证配置文件。

**步骤 1** 选择 **管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources)**。

**步骤 2** 选择以下选项之一：

- 选择 **证书身份验证配置文件 (Certificate Authentication Profile)** 执行基于证书的身份验证。
- 选择 **Active Directory** 作为外部身份源连接到 Active Directory。有关更多详细信息，请参阅[将 Active Directory 用作外部身份源，第 349 页](#)。
- 选择 **LDAP** 以添加 LDAP 身份源。有关更多详细信息，请参阅[LDAP，第 370 页](#)。
- 选择 **RADIUS 令牌 (RADIUS Token)** 以添加 RADIUS 令牌服务器。有关更多详细信息，请参阅[RADIUS 令牌身份源，第 382 页](#)。
- 选择 **RSA SecurID** 以添加 RSA SecurID 服务器。有关更多详细信息，请参阅[RSA 身份源，第 387 页](#)。

## 创建身份源序列

开始之前

确保您已经在思科 ISE 中配置了外部身份源。

要执行以下任务，您必须是超级管理员或系统管理员。

要允许访客用户通过本地 WebAuth 进行身份验证，必须同时配置访客门户身份验证源和身份源序列，使它们包含相同的身份存储区。

**步骤 1** 选择 **管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences) > 添加 (Add)**。

**步骤 2** 输入身份源序列的名称。您还可以输入可选的说明。

**步骤 3** 选中 **Select Certificate Authentication Profile** 复选框并为基于证书的身份验证选择证书身份验证配置文件。

**步骤 4** 在 **选定列表 (Selected List)** 字段中选择您希望包括在身份源序列中的数据库。

**步骤 5** 在 **选定列表 (Selected List)** 字段中重新调整数据库的顺序，调整为您希望思科 ISE 搜索数据库的顺序。

**步骤 6** 如果无法访问所选身份库进行身份验证，请在 **高级搜索列表** 区域中选择以下选项之一：

- 请勿访问序列中的其他库并将 “**AuthenticationStatus**” 属性设置为 “**ProcessError**”
- 将用户视为未找到，然后继续到序列中的下一个库

在处理请求时，思科 ISE 会按照序列搜索这些身份源。确保 “选定列表” (Selected list) 字段所列出的身份源的顺序是您希望思科 ISE 搜索身份源的顺序。

**步骤 7** 点击 **Submit** 创建您可以稍后在策略中使用的身份源序列。

---

## 创建终端身份组

思科 ISE 将其所发现的终端划分至相应的终端身份组。思科 ISE 拥有若干个系统定义的终端身份组。您还从 **终端身份组 (Endpoint Identity Groups)** 窗口创建更多终端身份组。您可以编辑或删除您已创建的终端身份组。只能编辑系统定义的终端身份组的说明。无法编辑或删除这些组的名称。

**步骤 1** 选择 **管理 (Administration) > 身份管理 (Identity Management) > 组 (Groups) > 终端身份组 (Endpoint Identity Groups)**。

**步骤 2** 单击添加。

**步骤 3** 为您想要创建的终端身份组输入 **名称**（请勿在终端身份组的名称中包含空格）。

**步骤 4** 为您想要创建的终端身份组输入 **说明**。

**步骤 5** 点击 **Parent Group** 下拉列表，选择您要与新创建的终端身份组关联的终端身份组。

**步骤 6** 点击提交。

---

## 编辑黑名单门户

思科 ISE 提供一个黑名单门户，它会在被列入思科 ISE 阻止列表的丢失或被盗设备试图访问您的公司网络时显示信息。

您只能编辑默认门户设置以及自定义为门户显示的默认消息。您不能创建新的黑名单门户，也不能复制或删除默认门户。

### 开始之前

确保您具有为配合此门户使用而配置的证书。

**步骤 1** 选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > 黑名单门户 (Blacklist Portal) > 编辑 (Edit)**。

**步骤 2** 在 **门户名称 (Portal Name)** 中提供唯一的门户名称，并在 **说明 (Description)** 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

**步骤 3** 在语言文件 (**Language File**) 下拉列表中, 选择所需的操作以便导出或导入要与门户一起使用的语言文件。

**步骤 4** 点击门户测试 URL 链接以打开显示此门户 URL 的新浏览器标签页。必须打开具有策略服务的策略服务节点 (PSN)。如果禁用策略服务, 则 PSN 仅显示管理员门户。

**注释** 测试门户不支持 RADIUS 会话, 因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如, 重定向到外部 URL 时不起作用。如果有多个 PSN, 思科 ISE 会选择第一个活动 PSN。

**步骤 5** 展开门户设置 (**Portal Settings**)。更新端口、证书组标签、终端身份组等的默认值, 然后定义适用于整体门户的行为。

- **HTTPS 端口 (HTTPS Port):** 输入 8000 至 8999 之间的端口值; 对于所有默认门户, 默认值为 8443 (黑名单门户除外, 其端口值为 8444)。如果已使用此范围外的端口值进行升级, 则在您修改此窗口之前会遵循这些设置。如果修改此窗口, 应更新端口设置以遵守此限制。

如果向访客门户分配由非访客 (例如“我的设备”) 门户使用的端口, 系统会显示错误消息。

仅针对安全评估和补救, 客户端调配门户还使用 8905 和 8909 端口。否则, 它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合, 则必须使用同一证书组标签。例如:

- 有效的组合包括 (以发起人门户为例):
  - 发起人门户: 端口 **8443**, 接口 **0**, 证书标签 **A** 和我的设备门户: 端口 **8443**, 接口 **0**, 证书组 **A**。
  - 发起人门户: 端口 **8443**, 接口 **0**, 证书组 **A** 和我的设备门户: 端口 **8445**, 接口 **0**, 证书组 **B**。
  - 发起人门户: 端口 **8444**, 接口 **1**, 证书组 **A** 和黑名单门户: 端口 **8444**, 接口 **0**, 证书组 **B**。
- 无效组合包括:
  - 发起人门户: 端口 **8443**, 接口 **0**, 证书组 **A** 和我的设备门户: **8443**, 接口 **0**, 证书组 **B**。
  - 发起人门户: 端口 **8444**, 接口 **0**, 证书标签 **A** 和黑名单门户: 端口 **8444**, 接口 **0**, 证书组 **A**。

**注释** 我们建议为访客服务使用接口 0, 以获得最佳性能。您可以在门户设置 (**Portal Settings**) 中仅配置接口 0, 也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces):** 选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时, PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

这些接口必须在所有 PSN 上都可用, 包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向, 因此要求如此。

- 以太网接口必须使用不同子网上的 IP 地址。
- 您此处启用的接口必须在所有 PSN 上可用, 包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向, 因此要求如此。
- 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。

- 在思科 ISE CLI 中配置 `ip host x.x.x、x.yyy.domain.com` 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
- **证书组标签 (Certificate Group tag)**: 选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **显示语言**
  - **使用浏览器区域设置 (Use Browser Locale)**: 使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language)**: 选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use)**: 选择要用于门户的显示语言。此设置会覆盖用户浏览器区域 (User Browser Locale) 选项。

**步骤 6** 在 **Portal Page Customization** 选项卡中，自定义在未授权的设备试图获取网络访问权限时显示在门户中的页面标题和消息文本。

**步骤 7** 点击**保存 (Save)**，然后点击**关闭 (Close)**。

## 创建 BYOD 门户

可以提供自带设备 (BYOD) 门户，使员工能够注册其个人设备，以便可在允许访问网络之前完成注册和请求方配置。

您可以创建新 BYOD 门户，也可以编辑或复制现有 BYOD 门户。您可以删除任何 BYOD 门户，包括思科 ISE 提供的默认门户。

您在门户行为和流设置 (**Portal Behavior and Flow Settings**) 选项卡下对门户和页面设置 (**Portal & Page Settings**) 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个窗口（例如**支持信息 (Support Information)** 窗口），则该窗口会显示在流程中，并且员工将在门户中体验该页面。禁用窗口会将其从流中删除。

### 开始之前

确保您具有配置用于此门户的所需证书和终端身份组。

**步骤 1** 选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **BYOD** > **创建 (Create)**。

**步骤 2** 在门户名称 (**Portal Name**) 中提供唯一的门户名称，并在说明 (**Description**) 中提供门户说明。

确保您在此处使用的门户名称未用于任何其他最终用户门户。

**步骤 3** 在语言文件 (**Language File**) 下拉列表中，选择所需的操作以便导出或导入要与门户一起使用的语言文件。

**步骤 4** 点击门户行为和流设置 (**Portal Behavior and Flow Settings**) 选项卡。

**步骤 5** 展开门户设置 (**Portal Settings**)。更新端口、证书组标签、终端身份组等的默认值，然后定义适用于整体门户的行为。

**步骤 6** 展开支持信息页面设置 (**Support Information Page Settings**)。更新此处要求的信息以帮助员工提供可供服务中心用于对网络访问问题进行故障排除的信息。

**步骤 7** 点击门户页面自定义 (**Portal Page Customization**) 选项卡。向下滚动到页面自定义 (**Page Customizations**) 区域，以自定义以下最终用户门户窗口。通过单击左侧菜单中**页面 (Pages)**下列出的相应选项，选择要自定义的门户窗口。

• **BYOD 欢迎 (BYOD Welcome):**

- **需要设备配置 (Device Configuration Required):** 输入当设备首次重定向到 BYOD 门户并需要证书调配时应显示的内容。
- **证书需要更新 (Certificate Needs Renewal):** 输入当需要更新先前证书时应显示的内容。

• **BYOD 设备信息 (BYOD Device Information):**

- **达到最大设备数 (Maximum Devices Reached):** 输入当达到员工可注册的设备的最大限制时应显示的内容。
- **需要的设备信息 (Required Device Information):** 输入当请求需要的设备信息以使员工能够注册设备时应显示的内容。

• **BYOD 安装 (BYOD Installation):**

- **桌面安装 (Desktop Installation):** 输入当提供桌面设备的安装信息时应显示的内容。
- **iOS 安装 (iOS Installation):** 输入当提供 iOS 移动设备的安装说明时应显示的内容。
- **Android 安装 (Android Installation):** 输入当提供 Android 移动设备的安装说明时应显示的内容。

• **BYOD 成功 (BYOD Success):**

- **成功 (Success):** 输入当设备已配置并自动连接到网络时应显示的内容。
- **成功：手动说明 (Success: Manual Instructions):** 输入当设备配置成功并且员工必须手动连接到网络时应显示的说明。
- **成功：不受支持的设备 (Success: Unsupported Device):** 输入当允许不受支持的设备连接到网络时应显示的内容。

**步骤 8** 单击**保存 (Save)**，然后单击**关闭 (Close)**。

---

### 下一步做什么

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。

## 创建客户端调配门户

可以提供一个客户端调配门户，使员工可以下载思科 AnyConnect 终端安全评估组件或思科 NAC 代理，此组件或代理将在允许设备访问网络之前验证设备的终端安全评估合规性。

您可以创建新 Client Provisioning 门户，也可以编辑或复制现有 Client Provisioning 门户。您可以删除任意 Client Provisioning 门户，包括思科 ISE 提供的默认门户。

对于能够访问该门户并为自己生成证书的其他用户，请配置“证书调配门户” (Certificate Provisioning Portal) 设置。此窗口的导航路径为：**管理 (Administration) > 设备门户管理 (Device Portal Management) > 客户端调配 (Client Provisioning) > 编辑 (Edit) > 门户行为和流程设置 (Portal Behavior and Flow Settings) > 门户设置 (Portal Settings)**。确保您在身份验证方法 (Authentication Method) 下选择适当的身份源或身份源序列，并且在配置授权组 (Configure Authorized Groups) 下选择用户组。属于您所选择用户组的所有用户可以访问该门户，并且可以生成自己的证书。

您在门户行为和流设置 (Portal Behavior and Flow Settings) 选项卡下对门户和页面设置 (Portal & Page Settings) 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个窗口（例如支持信息 (Support Information) 窗口），则该窗口会显示在流程中，并且员工将在门户中体验该页面。禁用窗口会将其从流中删除。

### 开始之前

确保已为此门户配置必需的证书和客户端调配策略。

**步骤 1** 选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > 客户端调配 (Client Provisioning) > 创建 (Create)**。

**步骤 2** 在门户名称 (Portal Name) 中提供唯一的门户名称，并在说明 (Description) 中提供门户说明。  
确保门户名称

**步骤 3** 在语言文件 (Language File) 下拉列表中，选择所需的操作以便导出或导入要与门户一起使用的语言文件。

**步骤 4** 点击门户行为和流设置 (Portal Behavior and Flow Settings) 选项卡。

**步骤 5** 展开门户设置 (Portal Settings)。更新端口、证书组标签、终端身份组等的默认值，然后定义适用于整体门户的行为。

**步骤 6** 展开支持信息页面设置 (Support Information Page Settings)。更新此处要求的信息以帮助员工提供可供服务中心用于对网络访问问题进行故障排除的信息。

**步骤 7** 点击门户页面自定义 (Portal Page Customization) 选项卡。向下滚动到页面自定义 (Page Customizations) 区域，以自定义以下最终用户门户窗口。通过单击左侧菜单中页面 (Pages) 下列出的相应选项，选择要自定义的门户窗口。

- 客户端调配门户 (Client Provisioning Portals):
  - 未知代理 (Agent Unknown): 输入当代理未知时应显示的内容。
  - 检查、扫描和合规 (Checking, Scanning and Compliant): 输入当终端安全评估代理已安装成功并且检查、扫描和验证设备是否符合终端安全评估要求时应显示的内容。
  - 不合规 (Non-compliant): 输入当终端安全评估代理确定设备不符合终端安全评估要求时应显示的内容。
- 客户端调配 (未找到代理) (Client Provisioning [Agent Not Found]):



- **未找到代理 (Agent Not Found)**: 输入在设备上未检测到终端安全评估代理时应显示的内容。
- **手动安装说明 (Manual Installation Instructions)**: 输入当设备上未安装 Java 或 Active X 软件时应显示的内容, 说明如何手动下载和安装终端安全评估代理。
- **安装, 无 Java/ActiveX (Install, No Java/ActiveX)**: 输入当设备上未安装 Java 或 Active X 软件时应显示的内容, 说明如何下载和安装 Java 插件。
- **已安装代理 (Agent Installed)**: 输入在设备上检测到终端安全评估代理时应显示的内容, 说明如何启动终端安全评估代理以检查设备是否符合终端安全评估要求。

**步骤 8** 单击保存 (Save), 然后单击关闭 (Close)。

#### 下一步做什么

您必须对门户授权才能使用门户。在对门户授权之前或之后, 您都可以对门户进行自定义。

#### 相关主题

[授权门户](#), 第 230 页

[自定义设备门户](#), 第 485 页

## 创建 MDM 门户

您可以提供移动设备管理 (MDM) 门户, 以使员工能够管理其注册以供在公司网络上使用的移动设备。

您在门户行为和流设置 (**Portal Behavior and Flow Settings**) 选项卡下对门户和页面设置 (**Portal & Page Settings**) 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个窗口 (例如支持信息 (**Support Information**) 窗口), 则该窗口会显示在流程中, 并且员工将在门户中体验该页面。禁用窗口会将其从流中删除。

#### 开始之前

确保您具有配置用于此门户的所需证书和终端身份组。

- 步骤 1** 选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > 移动设备管理 (Mobile Device Management) > 创建、编辑或复制 (Create, Edit or Duplicate)**。
- 步骤 2** 在门户名称 (**Portal Name**) 中提供唯一的门户名称, 并在说明 (**Description**) 中提供门户说明。  
确保您在此处使用的门户名称未用于任何其他最终用户门户。
- 步骤 3** 在语言文件 (**Language File**) 下拉列表中, 选择所需的操作以便导出或导入要与门户一起使用的语言文件。
- 步骤 4** 点击门户行为和流设置 (**Portal Behavior and Flow Settings**) 选项卡。
- 步骤 5** 展开门户设置 (**Portal Settings**)。更新端口、证书组标签、终端身份组等的默认值, 然后定义适用于整体门户的行为。

- 步骤 6** 展开MDM 门户的员工移动设备管理设置 (**Employee Mobile Device Management Settings**)。访问提供用于配置第三方 MDM 提供商的链接，然后使用 MDM 门户定义员工的接受策略行为。
- 步骤 7** 展开支持信息页面设置 (**Support Information Page Settings**)。更新此处要求的信息以帮助员工提供可供服务中心用于对网络访问问题进行故障排除的信息。
- 步骤 8** 点击门户页面自定义 (**Portal Page Customization**) 选项卡。
- 步骤 9** 自定义设备注册过程中显示在 MDM 门户中的内容区域 (**Content Area**) 消息。
- **无法接通 (Unreachable)**: 输入当无法访问所选 MDM 系统时显示的内容。
  - **不合规 (Non-compliant)**: 输入当正在注册的设备不符合 MDM 系统要求时显示的内容。
  - **继续 (Continue)**: 输入当设备在发生连接问题的情况下尝试连接网络时显示的内容。
  - **注册 (Enroll)**: 输入当设备需要 MDM 代理并需要在 MDM 系统中注册时显示的内容。
- 步骤 10** 单击保存 (**Save**)，然后单击关闭 (**Close**)。

### 下一步做什么

您必须对门户授权才能使用门户。在对门户授权之前或之后，您都可以对门户进行自定义。另请参阅以下主题：

- [将证书添加到设备门户，第 474 页](#)
- [创建终端身份组，第 476 页](#)
- [创建授权配置文件，第 483 页](#)
- [自定义设备门户，第 485 页](#)

## 创建我的设备门户

您可以提供我的设备门户，以使员工能够添加并注册其个人设备，这些设备不支持本地请求方且无法使用自带设备 (BYOD) 门户进行添加。然后，您可以使用我的设备门户管理已使用任一门户添加的所有设备。

您可以创建新的我的设备门户，也可以编辑或复制现有我的设备门户。您可以删除任何我的设备门户，包括思科 ISE 提供的默认门户。

您在门户行为和流设置 (**Portal Behavior and Flow Settings**) 选项卡下对门户和页面设置 (**Portal & Page Settings**) 所做的任何更改都会反映在设备门户流程图中的图形流程中。如果您启用某个窗口（例如支持信息 (**Support Information**) 窗口），则该窗口会显示在流程中，并且员工将在门户中体验该页面。禁用窗口会将其从流中删除。

### 开始之前

确保您具有配置用于此门户的所需证书、外部身份存储区、身份源序列和终端身份组。

- 
- 步骤 1 选择 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **我的设备 (My Devices)** > **创建 (Create)**。
  - 步骤 2 在 **门户名称 (Portal Name)** 中提供唯一的门户名称，并在 **说明 (Description)** 中提供门户说明。  
确保您在此处使用的门户名称未用于任何其他最终用户门户。
  - 步骤 3 在 **语言文件 (Language File)** 下拉列表中，选择所需的操作以便导出或导入要与门户一起使用的语言文件。
  - 步骤 4 点击 **门户行为和流设置 (Portal Behavior and Flow Settings)** 选项卡。
  - 步骤 5 展开 **门户设置 (Portal Settings)** 以更新端口、证书组标签、终端身份组等的默认值，然后定义适用于整体门户的行为。
  - 步骤 6 展开 **登录页面设置 (Login Page Settings)** 以指定员工凭证和登录准则。
  - 步骤 7 展开 **可接受使用政策 (AUP) 页面设置 (Acceptable Use Policy [AUP] Page Settings)** 以添加单独的 AUP 页面，并规定员工的可接受使用政策行为。
  - 步骤 8 展开 **登录后横幅页面设置 (Post-Login Banner Page Settings)** 以便在员工登录到门户后向其通知其他信息。
  - 步骤 9 展开 **员工更改密码设置 (Employee Change Password Settings)** 以允许员工更改其自己的密码。仅在员工是内部用户数据库的一部分时，才会启用此选项。
  - 步骤 10 在 **Portal Page Customization** 选项卡中，自定义注册和管理过程中显示在我的设备门户中的以下信息：
    - 标题、说明、内容、字段和按钮标签
    - 错误消息和通知消息
  - 步骤 11 点击 **保存 (Save)**，然后点击 **关闭 (Close)**。
- 

#### 下一步做什么

如果希望更改门户外观，您可以对其进行自定义。

#### 相关主题

[自定义设备门户](#)，第 485 页

[我的设备门户](#)，第 468 页

[显示员工添加的设备](#)，第 485 页

## 创建授权配置文件

当授权门户时，将会设置网络访问的网络授权配置文件和规则。

#### 开始之前

您必须先创建门户，然后才能对其进行授权。

- 
- 步骤 1 为门户设置特殊授权配置文件。

步骤 2 为配置文件创建授权策略规则。

## 创建授权配置文件

各门户要求您为其设置特殊的授权配置文件。

### 开始之前

如果不打算使用默认门户，您必须先创建门户以便将门户名称与授权配置文件关联。

### 下一步做什么

您应当创建门户授权策略规则，用于新创建的授权配置文件。

## 创建授权策略规则

要配置供门户在响应用户（访客、发起人、员工）的访问请求时使用的重定向 URL，请为该门户定义授权策略规则。

url-redirect 会根据门户类型采取以下形式，其中：

*ip:port*: IP 地址和端口号

*PortalID*: 唯一端口名称

对于热点访客门户：

`https://ip:port/guestportal/gateway?sessionID=SessionIdValue&portal=PortalID&action=cwa&type=drw`

对于移动设备管理 (MDM) 门户：

`https://ip:port/mdmportal/gateway?sessionID=SessionIdValue&portal=PortalID&action=mdm`

步骤 1 依次选择策略 (Policy) > 授权 (Authorization) 以在标准 (Standard) 策略下创建新授权策略。

如果已启用策略集，选择您计划用于此门户的策略集，展开授权策略，并添加新规则。

步骤 2 对于条件 (Conditions)，请选择要用于门户验证的终端身份组。例如，对于热点访客门户，选择默认的 **GuestEndpoints** 终端身份组；而对于 MDM 门户，选择默认的 **RegisteredDevices** 终端身份组。

注释 热点访客门户支持重新身份验证和终止 CoA 类型。仅当“热点访客门户”中选择“重新授权 CoA 类型”时，您可将 Network Access:UseCase EQUALS Guest Flow 用作热点访客授权策略中的一个验证条件。

步骤 3 对于 Permissions，请选择创建的门户授权配置文件。



注释 在使用启用了 MAC 选项的字典属性创建授权条件（例如 RADIUS.Calling-Station-ID）时，必须使用 Mac 运算符（例如 Mac\_equals）支持不同的 MAC 格式。

## 自定义设备门户

可以通过自定义门户主题、更改门户页面上的 UI 元素以及编辑向用户显示的错误消息与通知来自定义门户外观和用户（访客、发起人，在适当的情况下也可以是员工）体验。有关自定义门户的详细信息，请参阅 [自定义最终用户 Web 门户](#)，第 276 页。

## 管理员工添加的个人设备

当员工使用自带设备 (BYOD) 或我的设备门户注册设备时，此注册设备将显示在**终端 (Endpoints)** 列表中。虽然员工可以通过删除设备取消该设备与其帐户之间的关联，但设备依然留在思科 ISE 数据库中。因此，当员工使用自己的设备时，可能需要您协助他们解决遇到的错误。

## 显示员工添加的设备

您可以使用**终端 (Endpoints)** 列表窗口上显示的门户用户 (**Portal User**) 字段查找特定员工添加的设备。如果需要删除特定用户注册的设备，这可能会有所帮助。默认情况下，此字段不显示，因此在搜索之前必须先将其启用。

---

**步骤 1** 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **终端 (Endpoints)**。

**步骤 2** 在 Dashlet 下方，点击终端列表右上角可用的**设置 (Settings)** 图标。

**步骤 3** 选中门户用户 (**Portal User**) 复选框启用门户用户 (**Portal User**) 切换按钮以在终端列表中显示这些信息。

**步骤 4** 单击 **Go**（前往）。

**步骤 5** 点击过滤器 (**Filter**) 下拉列表，并选择快速过滤器 (**Quick Filter**)。

**步骤 6** 在 **Portal User** 字段中输入用户的名称，以仅显示分配给该特定用户的终端。

---

## 向我的设备门户添加设备时出错

如果设备已由其他员工添加，并且该设备仍在终端数据库中，则员工无法添加该设备。

如果员工尝试添加思科 ISE 数据库中已存在的设备：

- 如果设备支持本地请求者调配，则我们建议通过 BYOD 门户添加设备。此操作将覆盖该设备最初添加到网络时创建的任何注册详细信息。
- 如果该设备是 MAC 身份验证绕行 (MAB) 设备，如打印机，则必须先解决设备的所有权。如果适当，您可以使用管理员的门户从终端数据库中删除该设备，以便新的所有者可以使用“我的设备” (My Devices) 门户成功添加该设备。

## 从我的设备门户删除的设备仍保留在终端数据库中

当员工从“我的设备” (My Devices) 门户删除设备时，系统会从员工的已注册设备列表删除设备，但是设备仍保留在思科 ISE 终端数据库中并且显示于终端 (Endpoints) 列表上。

您可以从“终端” (Endpoints) 窗口永久删除设备。此窗口的导航路径为：**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 终端 (Endpoints)**。

## 限制员工注册的个人设备的数量

可以允许员工注册 1 至 100 台个人设备。无论员工用于注册个人设备的门户如何，此设置均可定义在所有门户上注册的最大设备数量。

---

**步骤 1** 选择 **管理 (Administration) > 设备门户管理 (Device Portal Management) > 设置 (Settings) > 员工注册的设备 (Employee Registered Devices)**。

**步骤 2** 在将员工限制为 (**Restrict employees to**) 中输入员工可注册的最大设备数量。默认情况下，此值设置为 **5** 台设备。

**步骤 3** 点击 **Save**。如果不想保存对设置进行的任何更新，请点击 **Reset** 以恢复为上次保存的值。

---

## 监控我的设备门户和终端活动

思科 ISE 提供各种报告和日志，您可以通过这些报告和日志查看终端与用户管理信息以及访客与发起人活动。

您可以按需或按计划运行这些报告。

---

**步骤 1** 选择 **操作 (Operations) > 报告 (Reports) > 报告 (Reports)**。

**步骤 2** 选择访客 (**Guest**) 或终端和用户 (**Endpoints and Users**) 以查看各种访客、发起人和终端相关报告

**步骤 3** 选择要使用过滤器 (**Filters**) 下拉列表搜索的数据。

**步骤 4** 在 **Time Range** 中选择您想要查看的数据的时间范围。

**步骤 5** 点击运行 (**Run**)。

---

## 我的设备登录和审核报告

我的设备登录和审核 (**My Devices Login and Audit**) 报告是跟踪以下信息的一种综合报告：

- 员工在 My Devices 门户上的登录活动。
- 员工在“我的设备” (My Devices) 门户中执行的与设备相关的操作。

此报告的导航路径为：操作 (Operations) > 报告 (Reports) > 报告 (Reports) > 访客 (Guest) > 我的设备登录和审核 (My Devices Login and Audit)。

## 注册的终端报告

注册终端 (**Registered Endpoints**) 报告提供有关由员工注册的所有终端的信息。此报告位于：操作 (Operations) > 报告 (Reports) > 报告 (Reports) > 终端和用户 (Endpoints and Users) > 注册终端 (**Registered Endpoints**)。可以过滤身份 (**Identity**)、终端 ID (**Endpoint ID**)、身份组 (**Identity Group**)、终端配置文件 (**Endpoint Profile**) 等属性并生成报告。

可以查询分配给注册设备 (**Registered Devices**) 终端身份组的终端的终端数据库。还可以为将门户用户 (**Portal User**) 属性设置为非空值的特定用户生成报告。

注册终端 (**Registered Endpoints**) 报告提供有关选定时间段内由特定用户通过设备注册门户注册的终端列表的信息。







# 第 11 章

## 安全接入

- 管理网络设备组，第 489 页
- 网络设备组，第 491 页
- 在思科 ISE 中导入模板，第 494 页
- 移动设备管理器与思科 ISE 的互操作性，第 498 页
- 使用思科 ISE 设置移动设备管理服务器, on page 502

## 管理网络设备组

通过以下窗口，您可以配置和管理网络设备组。

## 网络设备组设置

表 81: “网络设备组” (*Network Device Group*) 窗口中的字段

字段名称	使用指南
<b>Name</b>	为根网络设备组输入一个名称。对于添加到该根网络设备组的所有后续子网络设备组，请输入这个新建网络设备组的名称。  网络设备组的全称最多可以包含 100 个字符。例如，如果在父组 <b>全球 (Global)</b> > <b>亚洲 (Asia)</b> 下创建一个名为 <b>印度 (India)</b> 的子组，则您创建的网络设备组的全称将为 <b>全球 (Global)</b> > <b>亚洲 (Asia)</b> > <b>印度 (India)</b> 。全称不能超过 100 个字符。如果网络设备组的全称超过 100 个字符，则网络设备组创建失败。
<b>Description</b>	为根网络设备组或子网络设备组输入一段说明。
<b>Parent Group</b>	要将所创建的组添加到现有父组，请从下拉列表中选择父组。要将此新组添加为根组，请从下拉列表中选择 <b>添加为根组 (Add as root group)</b> 。

字段名称	使用指南
<b>Type</b>	<p>输入根网络设备组 (NDG) 的类型。</p> <p>所有添加到根网络设备组的子网络设备组都将继承组类型。</p> <p>如果此网络设备组是根网络设备组，则其类型可作为设备字典中的属性使用。您可以基于此属性定义条件。网络设备组的名称是此属性可以采用的值之一。</p>

#### 相关主题

[网络设备组](#)，第 491 页

[思科 ISE 在策略评估中使用的网络设备属性](#)，第 492 页

[在思科 ISE 中添加网络设备](#)

## 网络设备组导入设置

表 82: 网络设备组导入窗口中的字段

字段名称	使用指南
<b>生成模板 (Generate a Template)</b>	<p>点击此链接下载 CSV 模板文件。</p> <p>使用相同格式的网络设备组信息更新模板。将模板保存在本地，以便将网络设备组导入任何思科 ISE 部署中。</p>
<b>文件</b>	<p>点击 <b>浏览</b>，导航至您要上传的 CSV 文件的位置。该文件可能是新文件，也可能是从另一个思科 ISE 部署中导出的文件。</p> <p>可以将包含新的和更新后的网络设备组信息的网络设备组从一个思科 ISE 部署导入另一部署。</p>
<b>用新数据覆盖现有数据 (Overwrite Existing Data with New Data)</b>	<p>如果您希望思科 ISE 用您的导入文件中的设备组替换现有网络设备组，请选中此复选框。</p> <p>如果未选中此复选框，则只会将导入文件中的新网络设备组添加到网络设备组存储库。系统会忽略重复条目。</p>
<b>Stop Import on First Error</b>	<p>选中此复选框，可在导入期间遇到错误的第一个实例时停止导入。</p> <p>如果未选中此复选框并且遇到错误，思科 ISE 将报告错误，并继续导入剩余设备组。</p>

#### 相关主题

[网络设备组](#)，第 491 页

[思科 ISE 在策略评估中使用的网络设备属性](#)，第 492 页

[将网络设备组导入到思科 ISE](#)，第 492 页

## 网络设备组

思科 ISE 支持创建分层网络设备组。使用网络设备组根据不同的条件（例如地理位置、设备类型或其在网络中的相对位置 [例如，“接入层”或“数据中心”等]）对网络设备进行逻辑分组。

要查看“网络设备组” (Network Device Group) 窗口，选择 **管理 (Administration) > 网络资源 (Network Resources) > 网络设备组 (Network Device Groups)**。

例如，要按地理位置组织网络设备，可以按大洲、区域和国家/地区将设备进行分组：

- 非洲 > 南部 > 纳米比亚
- 非洲 > 南部 > 南非
- 非洲 > 南部 > 博茨瓦纳

根据设备类型对网络设备进行分组：

- 非洲 > 南部 > 博茨瓦纳 > 防火墙
- 非洲 > 南部 > 博茨瓦纳 > 路由器
- 非洲 > 南部 > 博茨瓦纳 > 交换机

将网络设备分配给一个或多个分层网络设备组。当思科 ISE 通过已配置的网络设备组的有序列表确定要分配给特定设备的适当组时，它可能会发现同一设备配置文件适用于多个设备组。在这种情况下，思科 ISE 将应用匹配的第一个设备组。

对可创建的网络设备组的最大数量没有限制。对层级的最大数量没有限制。

要在 **网络设备组** 窗口中添加网络设备组，请点击 **添加**。在 **父级组 (Parent Group)** 下拉列表中，选择网络设备组必须添加到的父级组，或选择 **添加为根组 (Add As Root Group)** 选项将新网络设备组添加为父级组。



**注释** 如果已向设备组分配了任何设备，则无法删除该设备组。在删除设备组之前，您必须将所有现有设备移动到另一个设备组。

### 根网络设备组

思科 ISE 包含两个预定义的根网络设备组：**所有设备类型 (All Device Types)** 和 **所有位置 (All Locations)**。无法编辑、复制或删除这些预定义的网络设备组，但可以在这些组中添加新设备组。

您可以创建根网络设备组（网络设备组），然后在 **网络设备组** 窗口中的根组下创建子网络设备组，如前所述。创建新的根网络设备组时，必须提供网络设备组的名称和类型。当在根网络设备组中创建子项时，不需要此信息。

## 思科 ISE 在策略评估中使用的网络设备属性

创建新网络设备组时，新网络设备属性将添加至系统字典 (**System Dictionaries**) 中的设备 (**Device**) 字典 (**策略 (Policy) > 策略元素 (Policy Elements) > 词典 (Dictionaries)**)。添加的设备属性随后将在策略定义中使用。

思科 ISE 允许您使用设备 (**Device**) 字典属性 (例如设备类型、位置、型号名称或网络设备上运行的软件版本) 配置身份验证和授权策略。

## 将网络设备组导入到思科 ISE

您可以使用逗号分隔值 (CSV) 文件将网络设备组导入到思科 ISE 节点。请注意，您不能同时从两个不同的导入文件导入网络设备组。

从思科 ISE 管理员门户下载 CSV 模板。在模板中输入网络设备组详细信息，并将模板另存为 CSV 文件，然后将编辑的文件导入到思科 ISE。

导入设备组时，您可以创建新记录或更新现有记录。导入设备组时，您还可以定义在思科 ISE 遇到第一个错误时希望思科 ISE 使用新组覆盖现有设备组还是停止导入过程。

---

**步骤 1** 选择 **管理 (Administration) > 网络资源 (Network Resources) > 网络设备组 (Network Device Groups)**。

**步骤 2** 单击导入。

**步骤 3** 在对话框中，单击浏览 (**Browse**)，从正在运行客户端浏览器的系统中选择 CSV 文件。

要下载用于添加网络设备组的 CSV 模板文件，请点击生成模板 (**Generate a Template**)。

**步骤 4** 要覆盖现有网络设备组，请选中 **用新数据覆盖现有数据** 复选框。

**步骤 5** 选中 **Stop Import on First Error** 复选框。

**步骤 6** 单击导入 (**Import**)。

---

## 从思科 ISE 导出网络设备组

您可以用 CSV 文件的形式导出在思科 ISE 中配置的网络设备组。然后，您可以将这些网络设备组导入另一个思科 ISE 节点。

---

**步骤 1** 选择 **管理 (Administration) > 网络资源 (Network Resources) > 网络设备组 (Network Device Groups) > 所有组 (All Groups)**。

**步骤 2** 要导出网络设备组，可以执行以下操作之一：

- 选中您要导出的设备组旁边的复选框，然后选择导出 (**Export**) > 导出选定对象 (**Export Selected**)。
- 依次选择 导出 > 全部导出，导出已定义的所有网络设备组。

CSV 文件可下载到您的本地硬盘。

## 管理网络设备组

通过以下窗口，您可以配置和管理网络设备组。

### 网络设备组设置

表 83: “网络设备组” (Network Device Group) 窗口中的字段

字段名称	使用指南
<b>Name</b>	<p>为根网络设备组输入一个名称。对于添加到该根网络设备组的所有后续子网络设备组，请输入这个新建网络设备组的名称。</p> <p>网络设备组的全称最多可以包含 100 个字符。例如，如果在父组<b>全球 (Global)</b> &gt; <b>亚洲 (Asia)</b> 下创建一个名为<b>印度 (India)</b> 的子组，则您创建的网络设备组的全称将为<b>全球 (Global)</b> &gt; <b>亚洲 (Asia)</b> &gt; <b>印度 (India)</b>。全称不能超过 100 个字符。如果网络设备组的全称超过 100 个字符，则网络设备组创建失败。</p>
<b>Description</b>	为根网络设备组或子网络设备组输入一段说明。
<b>Parent Group</b>	要将所创建的组添加到现有父组，请从下拉列表中选择一个父组。要将此新组添加为根组，请从下拉列表中选择 <b>添加为根组 (Add as root group)</b> 。
<b>Type</b>	<p>输入根网络设备组 (NDG) 的类型。</p> <p>所有添加到根网络设备组的子网络设备组都将继承组类型。</p> <p>如果此网络设备组是根网络设备组，则其类型可作为设备字典中的属性使用。您可以基于此属性定义条件。网络设备组的名称是此属性可以采用的值之一。</p>

#### 相关主题

[网络设备组](#)，第 491 页

[思科 ISE 在策略评估中使用的网络设备属性](#)，第 492 页

[在思科 ISE 中添加网络设备](#)

### 网络设备组导入设置

表 84: 网络设备组导入窗口中的字段

字段名称	使用指南
<b>生成模板 (Generate a Template)</b>	<p>点击此链接下载 CSV 模板文件。</p> <p>使用相同格式的网络设备组信息更新模板。将模板保存在本地，以便将网络设备组导入任何思科 ISE 部署中。</p>

字段名称	使用指南
文件	<p>点击 <b>浏览</b>，导航至您要上传的 CSV 文件的位置。该文件可能是新文件，也可能是从另一个思科 ISE 部署中导出的文件。</p> <p>可以将包含新的和更新后的网络设备组信息的网络设备组从一个思科 ISE 部署导入另一部署。</p>
用新数据覆盖现有数据 (Overwrite Existing Data with New Data)	<p>如果您希望思科 ISE 用您的导入文件中的设备组替换现有网络设备组，请选中此复选框。</p> <p>如果未选中此复选框，则只会将导入文件中的新网络设备组添加到网络设备组存储库。系统会忽略重复条目。</p>
Stop Import on First Error	<p>选中此复选框，可在导入期间遇到错误的第一个实例时停止导入。</p> <p>如果未选中此复选框并且遇到错误，思科 ISE 将报告错误，并继续导入剩余设备组。</p>

#### 相关主题

[网络设备组](#)，第 491 页

[思科 ISE 在策略评估中使用的网络设备属性](#)，第 492 页

[将网络设备组导入到思科 ISE](#)，第 492 页

## 在思科 ISE 中导入模板

思科 ISE 可以让您使用 CSV 文件导入大量网络设备和网络设备组。模板包含用于定义字段格式的标题行。除非添加下表中提到的列，否则不得编辑此标题行。

在网络设备和网络设备组的相关导入流中，可以使用**生成模板 (Generate a Template)**链接在 Microsoft Office Excel 应用中下载 CSV 文件，并在系统本地保存该文件格式。点击 **Generate a Template** 链接时，思科 ISE 服务器会显示 **Opening template.csv** 对话框。通过此对话框，您可以打开 **template.csv** 文件，并且针对网络设备和网络设备组使用相应的名称将 **template.csv** 文件以本地方式保存在系统上。如果您选择从对话框打开 **template.csv** 文件，默认情况下，文件会在 Microsoft Office Excel 应用中打开。

## 网络设备导入模板格式

下表列出了重要网络设备 CSV 模板文件标题中的字段，并进行了说明。

表 85: 网络设备的 CSV 模板字段和说明

字段	使用指南
<b>Name:String(32)</b>	输入网络设备的名称。名字必须是一个最多包含 32 个字符的字母数字字符串。

字段	使用指南
<b>Description:String(256)</b>	(可选) 输入网络设备的说明, 最多 256 个字符。
<b>IP Address:Subnets(a.b.c.d/m ...)</b>	输入网络设备的 IP 地址和子网掩码。您可以输入多个值, 使用竖线 “ ” 符号分隔这些值。  IPv4 地址是支持网络设备 (TACACS 和 RADIUS) 配置以及外部 RADIUS 服务器配置。
<b>Model Name:String(32)</b>	输入网络设备的型号名称, 最多 32 个字符。
<b>Software Version:String(32)</b>	输入网络设备的软件版本, 最多 32 个字符。
<b>Network Device Groups:String(100)</b>	输入现有网络设备组的名称。如果是子组, 必须同时包含由空格分隔的父组和子组。字符串必须是一个最多包含 100 个字符的字符串, 例如, <i>Location#All Location#US</i> 。
<b>Authentication:Protocol:String(6)</b>	输入要使用的身份验证协议。唯一有效的值为 <b>RADIUS</b> (不区分大小写)。
<b>Authentication:Shared Secret:String(128)</b>	(如果在 <b>身份验证: 协议: 字符串 (6)</b> 字段中输入一个值, 则此字段为必填字段) 此字段是一个最多为 128 个字符的字符串。
<b>EnableKeyWrap:Boolean(true false)</b>	KeyWrap 仅在网络设备上支持此字段时才启用。输入 <b>true</b> 或 <b>false</b> 。
<b>EncryptionKey:String(ascii:16 hexa:32)</b>	(如果启用 KeyWrap, 则此字段为必填字段) 输入用于会话加密的加密密钥。  ASCII 值: 长度为 16 个字符 (字节)。 十六进制值 - 长度为 32 个字符 (字节)。
<b>AuthenticationKey:String(ascii:20 hexa:40)</b>	(如果启用 KeyWrap, 则此字段为必填字段。) 输入 RADIUS 消息键控散列消息验证码 (HMAC) 计算的密钥。  ASCII 值: 长度为 20 个字符 (字节)。 十六进制值 - 长度为 40 个字符 (字节)。
<b>InputFormat:String(32)</b>	输入加密和身份验证密钥输入格式。接受 ASCII 和十六进制值。
<b>SNMP:Version:Enumeration ( 2c 3)</b>	输入分析器服务必须使用的 SNMP 协议版本 - 1、2c 或 3。
<b>SNMP:RO Community:String(32)</b>	(如果在 <b>SNMP:Version:Enumeration ( 2c 3)</b> 字段中输入值, 则为必填项)。为只读社区输入最多 32 个字符的字符串

字段	使用指南
<b>SNMP:RW Community:String(32)</b>	（如果在 <b>SNMP:Version:Enumeration ( 2c 3)</b> 字段中输入值，则为必填项）。为读写社区输入最多包含 32 个字符的字符串。
<b>SNMP:Username:String(32)</b>	输入一个最多为 32 个字符的字符串。
	（如果在 <b>SNMP:Version:Enumeration ( 2c 3)</b> 字段中输入 SNMP 版本 3，则为必填项）输入 <b>Auth</b> 、 <b>No Auth</b> 或 <b>Priv</b> 。
<b>SNMP:Authentication Protocol:Enumeration(MD5 SHA)</b>	（如果已输入 <b>Auth</b> 或 <b>Priv</b> 作为 SNMP 安全级别，则此字段为必填字段。）输入 <b>MD5</b> 或 <b>SHA</b> 。
<b>SNMP:Authentication Password:String(32)</b>	（如果已在 <b>SNMP:Security Level:Enumeration(Auth No Auth Priv)</b> 字段中输入 <b>Auth</b> ，则为必填项。）输入一个最多为 32 个字符的字符串。
<b>SNMP:Privacy Protocol:Enumeration(DES AES128 AES192 AES256 3DES)</b>	（如果您在 <b>SNMP:Security Level:Enumeration(Auth No Auth Priv)</b> 字段中输入了 <b>Priv</b> ，则为必填项。）输入 <b>DES</b> 、 <b>AES128</b> 、 <b>AES192</b> 、 <b>AES256</b> 或 <b>3DES</b> 。
<b>SNMP:Privacy Password:String(32)</b>	（如果您在 <b>SNMP:Security Level:Enumeration(Auth No Auth Priv)</b> 字段中输入了 <b>Priv</b> ，则为必填项。）输入一个最多为 32 个字符的字符串。
<b>SNMP:Polling Interval:Integer:600-86400 seconds</b>	输入 SNMP 轮询间隔（秒）。有效值为介于 600 和 86400 之间的整数。
<b>SNMP:Is Link Trap Query:Boolean(true false)</b>	通过输入 <b>true</b> 或 <b>false</b> 来启用或禁用 SNMP 链路陷阱。
<b>SNMP:Is MAC Trap Query:Boolean(true false)</b>	通过输入 <b>true</b> 或 <b>false</b> 来启用或禁用 SNMP MAC 陷阱。
<b>SNMP:Originating Policy Services Node:String(32)</b>	指示必须用于轮询 SNMP 数据的思科 ISE 服务器。它默认情况下是自动的，但可以通过在此字段中分配不同的值来覆盖该设置。
<b>Trustsec:Device Id:String(32)</b>	输入思科 Trustsec 设备 ID，是最多为 32 个字符的字符串。
<b>Trustsec:Device Password:String(256)</b>	（如果已输入思科 TrustSec 设备 ID，则为必填项。）输入思科 TrustSec 设备密码，该密码是最多包含 256 个字符的字符串。
<b>Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds</b>	输入思科 TrustSec 环境数据下载时间间隔。有效值为介于 1 和 2147040000 之间的整数。



字段	使用指南
<b>Trustsec:Peer Authorization Policy Download</b> <b>Interval:Integer:1-2147040000 seconds</b>	输入 TrustSec 对等体授权策略下载时间间隔。有效值为介于 1 和 2147040000 之间的整数。
<b>Trustsec:Reauthentication</b> <b>Interval:Integer:1-2147040000 seconds</b>	输入 TrustSec 重新身份验证时间间隔。有效值为介于 1 和 2147040000 之间的整数。
<b>Trustsec:SGACL List Download</b> <b>Interval:Integer:1-2147040000 seconds</b>	输入思科 TrustSec 安全组 ACL 列表下载间隔。有效值为介于 1 和 2147040000 之间的整数。
<b>Trustsec:Is Other Trustsec Devices Trusted:Boolean(true false)</b>	通过输入 <b>true</b> 或 <b>false</b> 指示思科 TrustSec 设备是否受信任。
<b>Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL DISABLE_ALL)</b>	通过输入 <b>ENABLE_ALL</b> 或 <b>DISABLE_ALL</b> 通知思科 TrustSec 配置更改到思科 TrustSec 设备。
<b>Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true false)</b>	通过输入 <b>true</b> 或 <b>false</b> 指示思科 TrustSec 设备是否包含在安全组标签中。
<b>Deployment:Execution Mode Username:String(32)</b>	输入有权编辑设备配置的用户名。这是一个最多为 32 个字符的字符串。
<b>Deployment:Execution Mode Password:String(32)</b>	输入设备密码，该密码是包含最多 32 个字符的字符串。
<b>Deployment:Enable Mode Password:String(32)</b>	输入设备的密码，可以让您编辑设备的配置。这是一个最多为 32 个字符的字符串。
<b>Trustsec:PAC issue date:Date</b>	输入思科 ISE 为思科 TrustSec 设备生成的最后一个思科 Trustsec PAC 的颁发日期。
<b>Trustsec:PAC expiration date:Date</b>	输入思科 ISE 为思科 TrustSec 设备生成的最后一个思科 Trustsec PAC 的到期日期。
<b>Trustsec:PAC issued by:String</b>	输入思科 ISE 为思科 TrustSec 设备生成的最后一个思科 Trustsec PAC 的颁发者（思科 TrustSec 管理员）名称。它必须是一个字符串值。

## 网络设备组导入模板格式

下表列出模板标题中的字段并提供网络设备组 CSV 文件中的字段描述。

表 86: 网络设备组的 CSV 模板字段和描述

字段	说明
Name:String(100):	(必填) 此字段为网络设备组的名称。它是长度最大为 100 个字符的字符串。NDG 全名的长度最大为 100 个字符。例如, 如果在父组“全球”(Global)>“亚洲”(Asia)下创建一个“印度”(India)的子组, 那么您创建的 NDG 的全称将是 Global#Asia#India。全称的长度不能超过 100 个字符。如果 NDG 的全名超过 100 个字符, 则 NDG 将无法创建。
Description:String(1024)	此字段是可选字段。它是长度不超过 1024 个字符的字符串。
Type:String(64):	(必填) 此字段为网络设备组的类型。它是长度最大为 64 个字符的字符串。
Is Root:Boolean(true/false):	(必填) 此字段用于确定特定的网络设备组是否为根组。有效值为 true 或 false。

## 移动设备管理器与思科 ISE 的互操作性

移动设备管理 (MDM) 服务器保护、监控、管理和支持跨移动运营商、服务提供商和企业部署的移动设备。传统上, MDM 服务器仅支持移动设备。某些 MDM 服务器现在管理网络中的所有类型的设备 (移动电话、平板电脑、笔记本电脑和台式机), 称为统一终端管理 (UEM) 服务器。MDM 服务器作为策略服务器运行, 用于控制移动设备上的某些应用 (例如, 电子邮件应用) 在部署环境中的使用。思科 ISE 向连接的 MDM 服务器查询可用于创建网络授权策略的各种属性的相关信息。

在此示例图中, 思科 ISE 是执行点, 而 MDM 策略服务器是策略信息点。思科 ISE 从 MDM 服务器获取数据, 以提供完整的解决方案。

有关思科 ISE 支持的 MDM 供应商的列表, 请参阅[支持的 MDM 服务器, 第 501 页](#)。

## 支持的移动设备管理使用情形

思科 ISE 与外部 MDM 服务器联合执行以下功能:

- 管理设备注册: 访问网络的未注册终端会重定向到 MDM 服务器上托管的注册页面。设备注册包括用户角色、设备类型等。
- 处理设备补救: 在补救期间向终端授予有限访问权限。
- 增强终端数据: 使用来自 MDM 服务器的信息更新终端数据库, 这些信息是无法使用思科 ISE 分析服务收集的。思科 ISE 使用可在终端 (**Endpoints**) 页面中查看的多个设备属性。选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **终端 (Endpoints)**。

以下是可用设备属性的示例。

- MDMei: xx xxxxxx xxxxxx x
- MDManufacturer: Apple

- MDMModel: iPhone
- MDMMOSVersion: iOS 6.0.0
- MDMPhoneNumber: 5550100
- MDMSerialNumber: DNPGQZGUDTFx
- 每 4 小时轮询一次 MDM 服务器，获取设备合规性数据。在外部 MDM 服务器 (External MDM Servers) 页面中配置轮询间隔。（要查看此页面，选择。
- 通过 MDM 服务器发出设备指示：思科 ISE 通过 MDM 服务器发出针对用户设备的远程操作。通过终端 (Endpoints) 页面从思科 ISE 管理门户发起远程操作。要查看此页面，选择情景可视性 (Context Visibility) > 终端 (Endpoints)。选中 MDM 服务器旁的复选框，然后点击 MDM 操作 (MDM Actions)。从显示的下拉列表中选择所需的操作。

### 供应商 MDM 属性

在思科 ISE 中配置 MDM 服务器时，思科 ISE 会查询 MDM 服务器以获取设备属性信息，并将该信息添加到 MDM 系统词典。以下属性用于注册状态，通常受 MDM 供应商支持。

思科 ISE 使用 API 向 MDM 服务器查询所需的设备属性。思科 ISE 版本 3.1 及更高版本支持 MDM API 版本 3。版本 3 API 包括允许思科 ISE 向 MDM 服务器发送查询的 API，以帮助思科 ISE 识别使用 MAC 地址随机化的终端。思科 ISE 向 MDM 服务器查询以下属性：

- GUID：唯一的设备标识符，用于代替 MAC 地址来标识设备。
- MAC 地址：UEM 或 MDM 服务器为特定设备记录的 MAC 地址列表。一台设备最多可共享五个 MAC 地址。

如果 MDM 服务器未提供所需属性的值，思科 ISE 将使用下表中提到的默认值填充属性字段。

表 87: MDM 属性和值

属性名称	属性词典	默认值	预期来自 UEM 或 MDM 服务器的数据	预期来自 Microsoft SCCM 服务器的数据
DaysSinceLastCheckin 从 MDM API 版本 3 开始支持	MDM	无	自用户上次签入设备或将设备与 UEM 或 MDM 服务器同步以来的天数。有效范围为 1 至 365 天。	自用户上次签入设备或将设备与 SCCM 服务器同步以来的天数。有效范围为 1 至 365 天。
DeviceCompliantStatus	MDM	不合规	合规 或 非合规。	合规 或 非合规。
DeviceRegisterStatus	MDM	已注销	已注册 或 已注销。	已注册 或 已注销。

属性名称	属性词典	默认值	预期来自 UEM 或 MDM 服务器的数据	预期来自 Microsoft SCCM 服务器的数据
DiskEncryptionStatus	MDM	熄灭	开启 或 关闭。	开启 或 关闭。
IMEI	MDM	无	设备的 IMEI 编号。	不适用。
JailBrokenStatus	MDM	不间断	可访问 或 无法访问。	可访问 或 无法访问。
MDM 失败原因	MDM	无	设备故障原因。	设备故障原因。
MDMServerName	MDM	无	服务器的名称。	服务器的名称。
MDMServerReachable	MDM	可访问	可访问 或 无法访问。	可访问 或 无法访问。
MEID	MDM	无	设备的 MEID 值。	不适用。
Manufacturer	MDM	无	设备制造商的名称。	不适用。
型号	MDM	无	设备型号的名称。	不适用。
OsVersion	MDM	无	设备的操作系统版本。	不适用。
无法	MDM	无	设备的电话号码。	不适用。
PinLockStatus	MDM	熄灭	开启 或 关闭。	不适用。
SerialNumber	MDM	无	设备的序列号。	不适用。
服务器类型	MDM	无	移动设备管理器服务器的 <b>MDM</b> 。 桌面设备管理器服务器的 <b>DM</b> 。	桌面设备管理器服务器的 <b>DM</b> 。
UDID	MDM	无	设备的 UDID 编号。	不适用。
UserNotified	MDM	否	是 或 否	不适用。

如果不支持供应商的唯一属性，可以使用 ERS API 来交换供应商特定属性。请查阅供应商的文档，了解有关支持的 ERS API 的信息。

新 MDM 字典属性可以在授权策略中使用。

当这些 MDM 字典属性用于策略时，无法从思科 ISE 中删除 MDM 服务器配置。要删除 MDM 服务器配置，必须先从策略中删除相关的 MDM 字典属性，然后从思科 ISE 中删除 MDM 服务器。

## 支持的 MDM 服务器

支持的 MDM 服务器包括来自以下供应商的产品：

- Airwatch, Inc.
- Good Technology
- MobileIron, Inc.
- Zenprise, Inc.
- SAP Afaria
- Fiberlink/IBM MaaS
- Meraki

## 移动设备管理服务使用的端口

下表列出思科 ISE 和 MDM 服务器之间要相互通信必须打开的端口。有关必须在 MDM 代理和服务器的列表，请参阅 MDM 供应商的文档。

表 88: MDM 服务器使用的端口

MDM 服务器	端口
MobileIron	443
Citrix XenMobile 10.x (On-Prem)	443
Blackberry - Good Secure EMM	19005
VMware Workspace ONE (之前称为 AirWatch)	443
SAP Afaria	443
IBM MaaS360	443
Cisco Meraki	443
Microsoft Intune	80 和 443
Microsoft SCCM	80 和 443

## 移动设备管理集成流程

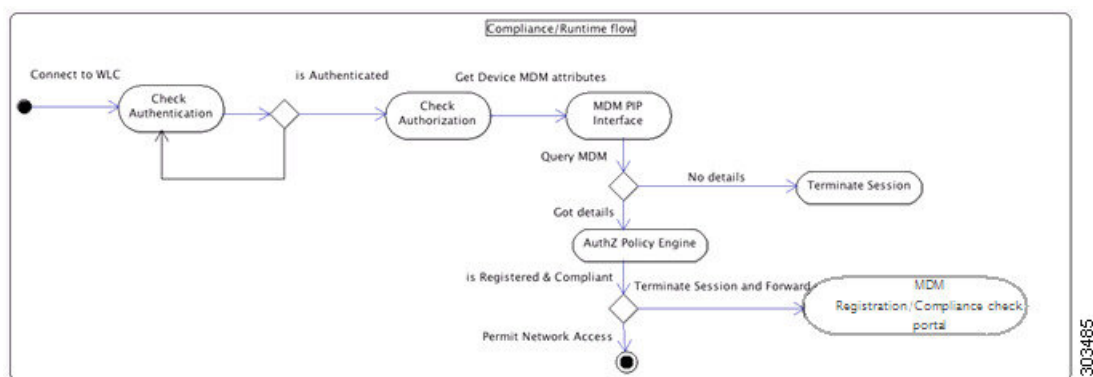
1. 用户将设备与 SSID 关联。
2. ISE 向 MDM 服务器发出 API 调用。
3. 此 API 调用会返回用户的设备列表和这些设备的终端安全评估状态。



注释 输入参数是终端设备的 MAC 地址。对于异地 Apple iOS 设备，输入参数为 UDID。

4. 思科 ISE 使用 MDM 调配设备并向用户显示相应的页面供其注册设备。
5. 用户在 MDM 服务器中注册设备，然后 MDM 服务器通过自动重定向或手动刷新浏览器将此请求重定向至思科 ISE。
6. 思科 ISE 重新查询 MDM 服务器获取安全评估状态。
7. 如果用户的设备不符合 MDM 服务器上配置的终端安全评估（合规性）策略，系统会向用户告知设备不合规。用户必须采取必要的措施来确保设备合规。
8. 用户设备合规后，MDM 服务器会在其内部表中更新设备状态。
9. 如果用户现在刷新浏览器，思科 ISE 将恢复控制。
10. 思科 ISE 每四小时会对 MDM 服务器进行轮询，以获取合规性信息并发出适当的授权更改 (CoA)。您可以配置轮询间隔。思科 ISE 还会每五分钟检查一次 MDM 服务器以确保其可用。

图 23: 思科 ISE 中的 MDM 流程



## 使用思科 ISE 设置移动设备管理服务器

要使用思科 ISE 设置 MDM 服务器，您必须执行以下高级任务：

步骤 1 将 MDM 服务器证书导入思科 ISE。

- 步骤 2 创建移动设备管理器定义。
- 步骤 3 在思科 WLC 上配置 ACL。
- 步骤 4 配置将非注册设备重定向到 MDM 服务器的授权配置文件。
- 步骤 5 为 MDM 使用案例配置授权策略规则。

---

## 将移动设备管理服务器证书导入思科 ISE

要使思科 ISE 连接 MDM 服务器，您必须将 MDM 服务器证书导入思科 ISE 受信任证书库。如果您的 MDM 服务器有一个 CA 签名的证书，您必须将根证书导入思科 ISE 受信任证书库。

- 
- 步骤 1 从您的 MDM 服务器导出 MDM 服务器证书并将其保存至您的本地计算机上。
  - 步骤 2 管理 (Administration) > 证书 (Certificates) > 证书库 (Certificate Store) > 导入 (Import)。
  - 步骤 3 在将新证书导入证书库 (Import a new Certificate into the Certificate Store) 窗口中，点击浏览 (Browse)，选择从 MDM 服务器获取的 MDM 服务器证书。
  - 步骤 4 在友好名称 (Friendly Name) 字段中，输入证书名称。
  - 步骤 5 点击 Submit。
  - 步骤 6 确认信任证书 (Trust Certificates) 窗口列出新添加的 MDM 服务器证书。

---

## 在思科 ISE 中配置移动设备管理服务器

向思科 ISE 提供终端信息的第一个 MDM 服务器显示在 情景可视性 > 终端 窗口中的终端信息中。当终端与其他 MDM 服务器连接时，MDM 服务器信息不会自动更新。您必须从 情景可视性 窗口中删除终端，然后终端必须与 MDM 服务器重新连接，以便 情景可视性 窗口显示更新的信息。

下图显示了在此任务期间必须使用的思科 ISE GUI 字段。图中的编号对应于以下任务中的步骤编号。

图 24: 在思科 ISE 中添加 MDM 服务器



**步骤 1** 选择管理 (Administration) > 网络资源 (Network Resources) > 外部 MDM (External MDM)。

**步骤 2** 在 MDM 服务器 窗口中，点击 添加。

**步骤 3** 在相应的字段中输入要添加的 MDM 服务器的名称和说明。

**步骤 4** 从服务器类型 (Server Type) 下拉列表中，选择移动设备管理器 (Mobile Device Manager)。

**步骤 5** 从身份验证类型 (Authentication Type) 下拉列表中，选择基础 (Basic) 或 OAuth-客户端凭证 (OAuth - Client Credentials)。

如果选择基础 (Basic) 身份验证类型，则会显示以下字段：

- **主机名/IP 地址 (Host Name/IP Address):** 输入 MDM 服务器主机名或 IP 地址。
- **端口:** 指定连接至 MDM 服务器时要使用的端口，通常为 443。
- **实例名称 (Instance Name):** 如果此 MDM 服务器有多个实例，应输入要连接到的实例。
- **用户名 (Username):** 输入连接到 MDM 服务器时必须使用的用户名。
- **密码 (Password):** 输入连接到 MDM 服务器所必须使用的密码。

如果您选择 OAuth-客户端凭证 (OAuth - Client Credentials) 身份验证类型，则会显示以下字段：

- 从自动发现 (Auto Discovery) 下拉列表中，选择是 (Yes) 或否 (No)。
- **自动发现 URL:** 输入 Microsoft Azure 管理门户中的 Microsoft Azure AD 图形 API 终端值。此 URL 是应用可使用图形 API 访问 Microsoft Azure AD 中的目录数据的终端。有关详细信息，请参阅 [将 MDM 和 UEM 服务器与思科 ISE 集成](#)。
- **客户端 ID (Client ID):** 应用的唯一标识符。如果应用访问其他应用中的数据，如 Microsoft Azure AD Graph API、Microsoft Intune API 等，则需要使用此属性。
- **颁发令牌的 URL:** 输入 OAuth2.0 授权终端值。在该终端上，思科 ISE 可以使用 OAuth2.0 获得访问令牌。
- **令牌受众 (Token Audience):** 令牌面向的接收资源，通常为指向 Microsoft Intune API 的公共知名 APP ID URL。

**合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query):** 当终端通过身份验证或重新进行身份验证时，思科 ISE 使用缓存获取该终端的 MDM 变量。如果缓存值的期限高于该字段中配置的值，则思科 ISE 会向 MDM 服务器进行设备查询以获取新值。如果合规性状态已变化，则思科 ISE 会触发相应的 CoA。有效范围为 1 到 1440 分钟。默认值为 1 分钟。

**轮询间隔:** 输入思科 ISE 轮询 MDM 服务器以获取合规性检查信息的轮询间隔（以分钟为单位）。此值应与 MDM 服务器上的轮询间隔相同。默认值为 240 分钟。我们建议您在生产环境中将轮询间隔设置为 60 分钟以上，以最大限度地减少因大量不合规终端而可能产生的任何性能影响。

如果将轮询间隔设置为 0，则思科 ISE 会禁用与 MDM 服务器的投票。

**注释** 如果外部 MDM 服务器收到来自超过 20000 个不合规终端的请求，则外部 MDM 服务器轮询间隔会被自动设置为 0。您还会在思科 ISE 上收到以下警报：

MDM 合规性轮询已禁用：原因是定期合规性轮询收到大量不合规设备信息。

**步骤 6** 从 状态 下拉列表中，选择 已启用。

**步骤 7** 要验证 MDM 服务器是否已连接到思科 ISE，请点击 **测试连接**。请注意 **测试连接** 并非旨在检查所有使用案例的权限（获取基准、获取设备信息等）。这些在服务器添加到思科 ISE 时进行验证。

**步骤 8** 点击**保存**。

---

## 在思科 ISE 中定义 Microsoft System Center Configuration Manager 服务器

---

**步骤 1** 选择**管理 (Administration) > 网络资源 (Network Resources) > 外部 MDM (External MDM) > MDM 服务器 (MDM Servers)**。

**步骤 2** 在 **MDM 服务器 (MDM Servers)** 窗口中，单击**添加 (Add)**。

**步骤 3** 从 **服务器类型 (Server Type)** 下拉列表选择 **桌面设备管理器 (Desktop Device Manager)**。

**步骤 4** 在 **主机名 / IP 地址 (Host Name / IP Address)** 字段中，输入 Microsoft SCCM 服务器主机名或 IP 地址。

**步骤 5** 在 **实例名称 (Instance Name)** 字段中，如果 Microsoft SCCM 服务器有多个实例，输入要连接到的实例。

**步骤 6** 在 **用户名 (Username)** 字段中，输入连接到 Microsoft SCCM 服务器所必须使用的用户名。

**步骤 7** 在 **密码 (Password)** 字段中，输入连接到 Microsoft SCCM 服务器所必须使用的密码。

**步骤 8** 在 **合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)** 字段中，输入一个介于 1 和 1440 分钟之间的值。默认值为 1 分钟。**合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)**：当终端通过身份验证或重新进行身份验证时，思科 ISE 使用缓存获取该终端的 MDM 变量。如果缓存值的期限高于该字段中配置的值，则思科 ISE 会向 MDM 服务器进行设备查询以获取新值。如果合规性状态已变化，则思科 ISE 会触发相应的 CoA。

**步骤 9** 从 **状态 (Status)** 下拉列表中选择 **已启用 (Enabled)**。

**步骤 10** 单击**测试连接 (Test Connection)** 以检查思科 ISE 是否可以连接到定义的 Microsoft SCCM 服务器。

**步骤 11** 点击**保存 (Save)**。

---

## 为 WMI 访问开放防火墙端口

Microsoft Active Directory 域控制器上的防火墙软件可能会阻止对 WMI 的访问。您可以关闭防火墙，或者允许在特定 IP 地址（思科 ISE 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处理此请求的组件使用哪个端口。
- UDP 138：NetBIOS 数据报服务
- TCP 139：NetBIOS 会话服务
- TCP 445：服务器消息块 (SMB)



---

**注释** 思科 ISE 支持 SMB 2.0。

---

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\dlhhost.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 地址（思科 ISE IP）。

## 配置用于重定向未注册设备的授权配置文件

### 开始之前

- 确保您已在思科 ISE 中创建 MDM 服务器定义。只有在成功将思科 ISE 与 MDM 服务器集成后才会填充 MDM 词典。然后，您可以使用 MDM 词典属性来创建授权策略。
- 在思科 WLC 上配置 ACL 以重定向未注册的设备。

---

**步骤 1** 选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles) > 添加 (Add)**。

**步骤 2** 创建用于重定向不合规或未注册的非注册设备的授权配置文件。

**步骤 3** 在名称 (Name) 字段中，为授权配置文件输入与 MDM 服务器名称匹配的名称。

**步骤 4** 从访问类型 (Access Type) 下拉列表中，选择 **ACCESS\_ACCEPT**。

**步骤 5** 在常见任务 (Common Tasks) 部分中，选中 **Web 重定向 (Web Redirection)** 复选框，然后从下拉列表中选择 **MDM 重定向 (MDM Redirect)**。

**步骤 6** 从 **ACL** 下拉列表中，选择输入您在无线 LAN 控制器上配置的 ACL 的名称。

**步骤 7** 点击提交 (Submit)。

---

### 下一步做什么

[为 MDM 使用案例配置授权策略规则。](#)

## 为 MDM 使用案例配置授权策略规则

在思科 ISE 中配置授权策略规则以完成 MDM 配置。

### 开始之前

- 将 MDM 服务器证书添加到思科 ISE 证书库。
- 确保您已在思科 ISE 中创建了 MDM 服务器定义。只有在成功将思科 ISE 与 MDM 服务器集成之后，才会填充 MDM 字典，您才可以使用 MDM 字典属性创建授权策略。
- 在思科 WLC 上配置 ACL 以重定向未注册或不合规设备。

---

**步骤 1** 选择策略 (Policy) > 授权 (Authorization) > 下方插入新规则 (Insert New Rule Below)。

步骤 2 选择策略 (Policy) > 策略集 (Policy Sets)，然后展开策略集以查看授权策略规则。

步骤 3 添加以下规则：

- **MDM\_Un\_Registered\_Non\_Compliant**：适用于尚未向 MDM 服务器注册或不符合 MDM 策略的设备。当请求与此规则匹配之后，系统会显示思科 ISE MDM 窗口，其中包含有关向 MDM 注册设备的信息。

注释 请勿在此策略中使用 **MDM.MDMServerName** 条件。使用此条件时，仅当终端注册到 MDM 服务器注册后，才与策略匹配。

- **PERMIT**：如果设备已注册到思科 ISE、MDM，并符合思科 ISE 和 MDM 策略，则系统将根据思科 ISE 中配置的访问控制策略向它授予网络访问权限。

下图显示了此配置的示例。

图 25: MDM 使用案例的授权策略规则



步骤 4 点击保存 (Save)。

## 在无线控制器上配置 ACL 以实现 MDM 互操作性

在无线控制器上配置 ACL 以用于授权策略，从而重定向未注册的设备和证书调配。ACL 必须采用以下顺序。

步骤 1 允许所有从服务器到客户端的出站流量。

步骤 2 （可选）允许从客户端到服务器的 ICMP 入站流量以进行故障排除。

步骤 3 允许未注册和不合规设备访问 MDM 服务器，以下载 MDM 代理和执行合规检查。

步骤 4 允许从客户端到服务器再到 ISE 的所有入站流量以执行 Web 门户和请求方以及证书调配流程。

步骤 5 允许从客户端到服务器的入站域名系统 (DNS) 流量以进行名称解析。

步骤 6 允许从客户端到服务器的入站 DHCP 流量以获取 IP 地址。

步骤 7 拒绝所有从客户端到服务器再到企业资源的入站流量，以重定向至思科 ISE（根据公司策略）。

步骤 8 （可选）允许其余流量。

### 示例

以下示例显示的 ACL 用于将未注册的设备重定向至 BYOD 流程。在本例中，思科 ISE IP 地址为 10.35.50.165，内部企业网络 IP 地址为 192.168.0.0 和 172.16.0.0（重定向），MDM 服务器子网为 204.8.168.0。

图 26: 用于重定向未注册设备的 ACL

General										
Access List Name:		NSP-ACL								
Deny Counters:		0								
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720	<input checked="" type="checkbox"/>
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227	<input checked="" type="checkbox"/>
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626	<input checked="" type="checkbox"/>
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505	<input checked="" type="checkbox"/>
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864	<input checked="" type="checkbox"/>
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0	<input checked="" type="checkbox"/>
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4	<input checked="" type="checkbox"/>
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457	<input checked="" type="checkbox"/>
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256	<input checked="" type="checkbox"/>
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310	<input checked="" type="checkbox"/>
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0	<input checked="" type="checkbox"/>
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819	<input checked="" type="checkbox"/>

## 擦除或锁定设备

思科 ISE 可以让您擦除已丢失的设备或启用其 pin 锁。您可以从终端 (Endpoints) 窗口配置此特性。

**步骤 1** 选择 管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 终端 (Endpoints)。

**步骤 2** 选中您想要擦除或锁定的设备旁边的复选框。

**步骤 3** 从 MDM 操作 (MDM Actions) 下拉列表中，选择以下选项之一：

- **完全擦除 (Full Wipe)**: 此选项会删除公司应用或将设备重置为出厂设置，具体取决于 MDM 供应商。
- **企业擦除 (Corporate Wipe)**: 此选项会删除您在 MDM 服务器策略中配置的应用。
- **PIN 锁定**: 此选项会锁定设备。

**步骤 4** 点击 **Yes** 擦除或锁定设备。

## 查看移动设备管理报告

思科 ISE 记录 MDM 服务器定义的所有添加、更新和删除操作。可以在**更改配置审核 (Change Configuration Audit)** 报告中查看这些事件，该报告显示选定时段内任何系统管理员的全部配置更改。

选择 **操作 (Operations) > 报告 (Reports) > 报告 (Reports) > 审核 (Audit) > 更改配置审核 (Change Configuration Audit)**。检查您要查看的 MDM 服务器的**对象类型 (Object Type)** 和**对象名称 (Object Name)** 列中的条目，然后点击相应的事件 (Event) 值以查看配置事件的详细信息。

## 查看移动设备管理日志

您可以使用消息目录 (Message Catalog) 窗口查看移动设备管理器日志消息。选择**管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 消息目录 (Message Catalog)**。MDM 日志条目的默认报告级别为“INFO”。您可以将报告级别更改为“调试” (DEBUG) 或“跟踪” (TRACE)。



## 第 12 章

# 分段

- [策略集](#)，第 511 页
- [身份验证策略](#)，第 512 页
- [授权策略](#)，第 518 页
- [策略条件](#)，第 526 页
- [特殊网络访问条件](#)，第 545 页
- [用于身份验证的协议设置](#)，第 549 页
- [从非思科设备启用 MAB](#)，第 576 页
- [从思科设备启用 MAB](#)，第 577 页
- [TrustSec 架构](#)，第 578 页
- [配置 TrustSec 全局设置](#)，第 581 页
- [配置 TrustSec 设备](#)，第 584 页
- [配置思科 TrustSec AAA 服务器](#)，第 586 页
- [安全组配置](#)，第 586 页
- [出口策略](#)，第 590 页
- [SGT 分配](#)，第 595 页
- [TrustSec 配置和策略推送](#)，第 599 页
- [按用户报告运行前 N 个 RBACL 丢包](#)，第 606 页

# 策略集

思科 ISE 是基于策略的网络访问控制解决方案，可提供网络访问策略集，允许您管理多个不同的网络访问用例，如无线、有线、访客和客户端调配。通过策略集（网络访问集和设备管理集），您可以对同一集合内的身份验证策略和授权策略进行逻辑分组。您可以基于区域具有若干策略集，例如基于位置、访问类型和类似参数的策略集。安装思科 ISE 时，始终有一个定义的策略集，即默认策略集，默认策略集包含预定义和默认的身份验证、授权和例外策略规则。

创建策略集时，可以配置这些规则（使用条件和结果进行配置），以便选择策略集级别的网络访问服务、身份验证策略级别的身份源，以及授权策略级别的网络权限。从适用于不同供应商的思科 ISE 支持的字典中，可以使用任何属性定义一个或多个条件。思科 ISE 允许您将条件创建为单个策略元素。

每个策略集用于与网络设备进行通信的网络访问服务是在该策略集的顶层定义的。网络访问服务包括：

- 允许的协议 - 为处理初始请求和协议协商而配置的协议。
- 代理服务 - 将请求发送至外部 RADIUS 服务器进行处理。



**注释** 从工作中心 (**Work Centers**) > 设备管理 (**Device Administration**)，您还可以为策略集选择相关的 TACACS 服务器序列。使用 TACACS 服务器序列可配置要处理的 TACACS 代理服务器序列。

策略集按层次结构进行配置，其中位于策略集顶层的规则（可从**策略集**表中查看）适用于整个策略集，并先于其余策略和例外规则进行匹配。此后，按以下顺序应用集合的规则：

1. 身份验证策略规则
2. 本地策略例外
3. 全局策略例外
4. 授权策略规则



**注释** 对于网络访问和设备管理策略，策略集功能是相同的。在使用**网络访问**和**设备管理**工作中心时，可以应用本章中介绍的所有流程。本章专门讨论网络访问工作中心策略集。选择工作中心 (**Work Centers**) > **网络访问 (Network Access)** > **策略集 (Policy Sets)**。

## 身份验证策略

每个策略集可以包含多个身份验证规则，它们共同代表该策略集的身份验证策略。身份验证策略的优先级根据这些策略在策略集本身中的显示顺序来确定（从“身份验证策略” (**Authentication Policy**) 区域中的“集合视图” (**Set view**) 页面）。

思科 ISE 根据策略集级别配置的设置动态选择网络访问服务（允许的协议或服务器序列），然后从身份验证和授权策略级别检查身份源和结果。您可以定义一个或多个使用思科 ISE 字典中任何属性的条件。思科 ISE 可以让您将条件单个策略元素，它们可以存储在系统库中，然后重复用于其他基于规则的策略。

身份验证方法是身份验证策略的结果，可以是以下任何一种：

- 拒绝访问 - 系统拒绝用户的访问并且不执行身份验证。
- 身份数据库 - 可以是下述单个身份数据库中的一个：
  - 内部用户
  - 访客用户



- 内部终端
  - Active Directory
  - 轻量级目录访问协议 (LDAP) 数据库
  - RADIUS 令牌服务器 (RSA 或 SafeWord 服务器)
  - 证书身份验证配置文件
- 身份源序列 - 用于身份验证的身份数据库的序列。

初始思科 ISE 安装时实施的默认策略集包括默认 ISE 身份验证和授权规则。默认策略集还包括用于身份验证和授权的其他灵活内置规则（不是默认规则）。可向这些策略添加其他规则，也可以删除和更改内置规则，但不能删除默认规则，也不能删除默认策略集。

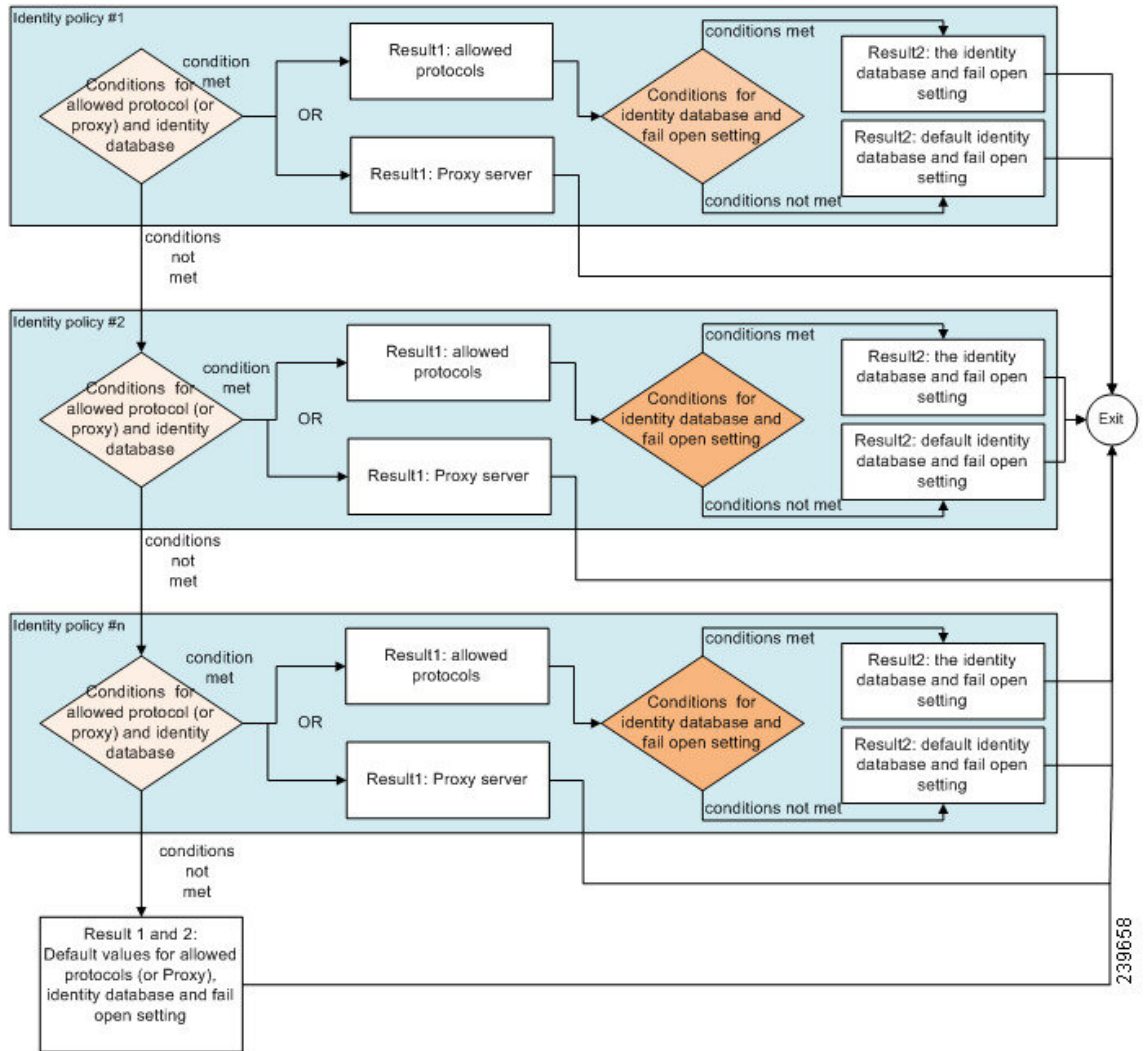
### 身份验证策略流

在身份验证策略中，可以定义多个由条件和结果组成的规则。ISE 会评估您所指定的条件，然后根据评估的结果分配相应的结果。系统根据匹配条件的第一个规则选择身份数据库。

您还可以定义包括不同数据库的身份源序列。您可以定义您希望思科 ISE 查询这些数据库的顺序。思科 ISE 将依次访问这些数据库，直至身份验证成功。如果在外部数据库中同一用户有多个实例，则身份验证失败。身份源中只能有一个用户记录。

我们建议您在身份源序列中仅使用三个，或者最多四个数据库。

图 27: 身份验证策略流



## 身份验证失败类型 - 故障转移

如果您选择的身份方法为拒绝访问，则会发送拒绝消息作为对请求的响应。如果选择身份数据库或身份源序列，并且身份验证成功，则会继续处理授权策略。某些身份验证失败，这些失败情况会按照以下方式分类：

- **Authentication failed** - 收到身份验证已失败的明确响应，例如错误凭证、禁用的用户等。默认操作是拒绝。
- **User not found** - 在任何身份数据库中均未找到此用户。默认操作是拒绝。
- **Process failed** - 无法访问身份数据库。默认操作是丢弃。

思科 ISE 允许您配置下列任意一条身份验证失败的操作：

- Reject - 发送拒绝响应。
- Drop - 不发送任何响应。
- Continue - 思科 ISE 继续处理授权策略。

即使您选择继续选项，可能会存在一些实例，在这些实例中，由于正在使用的协议受到限制，思科 ISE 无法继续处理请求。对于使用 PEAP、LEAP、EAP-FAST、EAP-TLS 或 RADIUS MSCHAP 的身份验证，当身份验证失败时或未找到用户时，无法继续处理请求。

当身份验证失败时，可继续处理 PAP/ASCII 和 MAC 身份验证绕行（MAB 或主机查找）的授权策略。对于其他所有身份验证协议，当身份验证失败时将发生以下情况：



- Authentication failed - 发送拒绝响应。
- User or host not found - 发送拒绝响应。
- Process failure - 不发送响应，并丢弃请求。

## 配置身份验证策略

根据需要，通过配置和维护多个身份验证规则，为每个策略集定义身份验证策略。

### 开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

- 步骤 1** 有关网络访问策略，请选择工作中心 (**Work Centers**) > 网络访问 (**Network Access**) > 策略集 (**Policy Sets**)。有关设备管理策略，请选择工作中心 (**Work Centers**) > 设备管理 (**Device Administration**) > 设备管理策略集 (**Device Admin Policy Sets**)。
- 步骤 2** 从要添加或更新身份验证策略的策略集对应的行中，从策略集表中的“视图”列点击 ，以便访问所有策略集详细信息并创建身份验证和授权策略以及策略例外。
- 步骤 3** 点击页面“身份验证策略”（**Authentication Policy**）部分旁边的箭头图标，展开并查看表中的所有身份验证策略规则。
- 步骤 4** 在操作 (**Actions**) 列中，点击齿轮图标。从下拉菜单中，根据需要选择任何插入或重复选项来插入新的身份验证策略规则。  
身份验证策略表中会显示一个新行。
- 步骤 5** 在状态 (**Status**) 列中，点击当前状态 (**Status**) 图标，然后从下拉列表中根据需要更新策略集的状态。有关状态的详细信息，请参阅 [身份验证策略配置设置](#)。
- 步骤 6** 对于表中的任意规则，点击规则名称 (**Rule Name**) 或说明 (**Description**) 单元格，可做出任何必要的自由文本更改。
- 步骤 7** 要添加或更改条件，请将鼠标悬停在条件 (**Conditions**) 列中的单元格上，然后点击 。Conditions Studio 将打开。  
有关详细信息，请参阅 [特殊网络访问条件](#)，第 545 页。

不是您选择的所有属性都包含“等于”、“不等于”、“位于”、“不位于”、“匹配”、“开头为”或“开头非”运算符选项。

“Matches”运算符支持并使用正则表达式 (REGEX)，而不使用通配符。

**注释** 您必须使用“equals”运算符进行直接比较。“包含”运算符可用于多值属性。“匹配”运算符应用于正则表达式比较。当使用“匹配”运算符时，将解译正则表达式中的静态值和动态值。如果是列表，“位于”运算符会检查列表中是否存在特定值。如果是单个字符串，“位于”运算符会检查字符串是否与“等于”运算符相同。

**步骤 8** 按照检查和匹配策略的顺序来组织表中的策略。要更改规则的顺序，请将这些行拖放到正确位置。

**步骤 9** 点击**保存 (Save)** 以保存和实施所做的更改。

### 下一步做什么

1. 配置授权策略。

## 基于密码的身份验证

身份验证对用户信息进行验证，以确认用户身份。传统身份验证使用名称和固定密码。这是最普遍、最简单和最经济的身份验证方法。缺点在于此信息可能会被告知他人、被猜到或捕获。使用简单、未加密用户名和密码的方法不被视为强身份验证机制，但是对于低授权或低权限级别（例如互联网访问）可能已足够。

## 使用加密密码和加密技术的安全身份验证

应使用加密来降低网络中的密码捕获风险。客户端和服务端访问控制协议（例如 RADIUS）可对密码加密，以防止在网络中捕获密码。但是，RADIUS 仅在身份验证、授权和记账 (AAA) 客户端与思科 ISE 之间运行。在身份验证流程中的以下位置点之前，未经授权的人员可以获取明文密码，如下示例所示：

- 在通过电话线路拨号的最终用户客户端之间的通信中。
- 在终止于网络接入服务器的 ISDN 线路上。
- 在最终用户客户端与托管设备之间的 Telnet 会话中

安全性较高的方法会采用加密技术，例如，那些用于质询握手身份验证协议 (CHAP)、一次性密码 (OTP) 和基于 EAP 的高级协议中的加密技术。思科 ISE 支持各种身份验证方法。

## 身份验证方法和授权权限

身份验证与授权之间存在基本的隐式关系。向用户授予的授权权限越多，身份验证的能力就越强。思科 ISE 通过提供各种身份验证方法来支持此关系。

## 身份验证面板

思科 ISE 控制板会概述网络中和设备发生的全部身份验证。它提供**身份验证 (Authentications) Dashlet** 中的身份验证和身份验证失败的概览信息。

**RADIUS 身份验证 (RADIUS Authentications) Dashlet** 提供以下有关思科 ISE 已处理身份验证的统计信息：

- 思科 ISE 已处理 RADIUS 身份验证请求的总数，包括已通过的身份验证、已失败的身份验证以及相同用户的同时登录数。
- 思科 ISE 已处理的 RADIUS 已失败的身份验证请求的总数。

您还可以查看 TACACS + 身份验证的摘要。TACACS + 身份验证 Dashlet 提供设备身份验证的统计信息。

## 查看身份验证结果

思科 ISE 提供多种方式查看实时身份验证摘要。

### 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** 选择操作 (**Operations**) > 身份验证 (**Authentications**) 以查看实时身份验证摘要。

**步骤 2** 您可以通过以下方式查看身份验证摘要：

- 将鼠标悬停在“状态” (**Status**) 图标上，以查看身份验证的结果和简短摘要。系统将显示一个包含状态详细信息的弹出窗口。
- 在列表顶部显示的任何一个或多个文本框中输入搜索条件，然后按 **Enter** 键以筛选您的结果。
- 单击**详细信息 (Details)** 列中的放大镜图标以查看详细报告。

**注释** 由于**身份验证摘要 (Authentication Summary)** 报告或控制板会收集和显示与失败或成功的身份验证对应的最新数据，因此报告内容会延迟几分钟后显示。

## 身份验证报告和故障排除工具

除身份验证详细信息外，思科 ISE 还提供各种可用于有效管理网络的报告和故障排除工具。

可以运行各种报告，了解网络中的身份验证趋势和流量。可以生成历史以及当前数据的报告。以下是身份验证报告列表：

- AAA 诊断
- RADIUS 记账
- RADIUS 身份验证
- 身份验证摘要

## 授权策略

授权策略是思科 ISE 网络授权服务的组件。此服务允许您为访问网络资源的特定用户和组定义授权策略并配置授权配置文件。

授权策略可包含条件要求，即使用复合条件组合一个或多个身份组，而该复合条件包括可返回一个或多个授权配置文件的授权检查。此外，除了使用特定的身份组外，可能存在条件要求。

在思科 ISE 中创建授权配置文件时使用授权策略。授权策略包括授权规则。授权规则具有三个元素：名称、属性以及权限。权限元素映射到授权配置文件。

## 思科 ISE 授权配置文件

授权策略将规则与特定用户和组身份关联以创建相应的配置文件。只要这些规则与已配置的属性匹配，策略就会返回授予权限的相应授权配置文件并且相应地授予网络访问权限。

例如，授权配置文件可以包括以下类型中包含的一系列权限：

- 标准配置文件
- 例外配置文件
- 基于设备的配置文件

配置文件包括从一组资源中选择的属性，这些属性存储于任何可用供应商字典中，并且在满足特定授权策略的复合条件时就会返回这些属性。由于授权策略可以包括映射到单个网络服务规则的复合条件，这些策略还可以包括授权检查列表。

对于简单情况，所有授权检查都是在规则内使用 AND 布尔运算符执行的。对于复杂情况，可以使用任何类型的授权验证表达式，但是这些授权验证都必须符合要返回的授权配置文件。授权验证通常由一个或多个条件组成，包括可添加至库中的用户定义的名称，其他授权策略然后可以重复使用这些条件。

## 授权配置文件的权限

在开始配置授权配置文件的权限之前，请确保：

- 了解授权策略与配置文件之间的关系。
- 熟悉**授权配置文件 (Authorization Profile)** 页面。
- 知悉在配置策略和配置文件时要遵守的基本规定。
- 了解在授权配置文件中构成权限的内容。

要使用授权配置文件，选择**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results)**。从左侧菜单中选择**授权 (Authorization) > 授权配置文件 (Authorization Profiles)**。

使用**结果 (Results)** 导航窗格作为用于显示、创建、修改、删除、复制或搜索网络上不同类型授权配置文件的策略元素权限的过程的起点。**结果 (Results)** 窗格初始显示“身份验证” (Authentication)、

“授权” (Authorization)、 “分析” (Profiling)、 “终端安全评估” (Posture)、 “客户端调配” (Client Provisioning) 和 Trustsec 选项。

通过授权配置文件，您可以选择在接受 RADIUS 请求时要返回的属性。思科 ISE 提供可以通过配置常见任务设置 (**Common Tasks Settings**) 来支持常用属性的机制。您必须输入常见任务属性 (**Common Tasks Attributes**) 的值，思科 ISE 会将这些值转换为基础 RADIUS 值。

## 可下载 ACL

访问控制列表 (ACL) 是访问控制条目 (ACE) 的列表，可由策略实施点（例如，交换机）应用到资源。每个 ACE 可确定每个用户该对象的允许权限，如读取、写入、执行等。例如，可以为网络销售区域的两个用户配置 ACL，其中一个 ACE 允许其中一个用户拥有读取和写入权限，另一个 ACE 只允许另一个用户拥有读取权限。

借助思科 ISE，可在授权策略中配置和实施可下载 ACL (DACL)，以控制不同用户和用户组访问网络的方式。还可以使用自定义用户属性和 AD 属性配置 DACL。



**注释** 如果身份提供程序 (IdP) 授权策略中使用的 DACL 为空，则授权将失败。

要在思科 ISE 中将 DACL 实施到网络授权策略中，请执行以下操作：

1. 从以下位置配置新的或现有的 DACL：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 可下载 ACL (Downloadable ACLs)**。有关详细信息，请参阅[为可下载 ACL 配置权限](#)，第 519 页。
2. 使用您已配置的任何 DACL 从以下位置配置新的或现有授权配置文件：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权配置文件 (Authorization Profiles)**。

使用 RADIUS 协议时，ACL 通过过滤源和目标 IP 地址、传输协议和其他参数来进行授权。静态 ACL 位于交换机上，可直接通过交换机进行配置，并可通过 ISE GUI 应用于授权策略中。

### 为可下载 ACL 配置权限

默认授权 DACL 可在安装 ISE 后可用，包括以下默认配置文件：

- DENY\_ALL\_TRAFFIC
- PERMIT\_ALL\_TRAFFIC

使用 DACL 时，无法更改这些默认值，但可以复制它们以创建其他类似的 DACL。

**步骤 1** 选择**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authorization) > 可下载的 ACL (Downloadable ACLs)**。

**步骤 2** 单击可下载 ACL 表顶部的**添加 (Add)**，或者，选择任何现有的 DACL，然后单击表顶部的**复制 (Duplicate)**。

**步骤 3** 输入或编辑所需的 DACL 值，牢记以下规则：

- 名称字段支持的字符为：字母数字、连字符 (-)、点号 (.) 和下划线 (\_)

- 关键字 **Any** 必须是 DACL 中所有 ACE 的源。DACL 推送之后，源中的 **Any** 会被替换为连接到交换机的客户端的 IP 地址。

**注释** 当将 DACL 映射到任何授权配置文件时，**IP 版本(IP Version)** 字段不可编辑。在这种情况下，请从**授权配置文件 (Authorization Profiles)** 中删除 DACL 引用，编辑 IP 版本并在**授权配置文件 (Authorization Profiles)** 中重新映射 DACL。

**步骤 4** 或者，当完成创建完整的 ACE 列表后，点击**检查 DACL 语法 (Check DACL Syntax)** 以验证列表。如果存在验证错误，系统会在自动打开的窗口中显示特定的说明，指明无效的语法。

**步骤 5** 点击提交。

---

## 针对 Active Directory 用户授权的设备访问限制

思科 ISE 包含计算机访问限制 (MAR) 组件，提供另外一种控制 Microsoft Active Directory 身份验证用户授权的方法。此授权形式基于访问思科 ISE 网络所用的计算机的计算机身份验证。对于每个成功的计算机身份验证，思科 ISE 会将 RADIUS Calling-Station-ID 属性（属性 31）中收到的值缓存为成功计算机身份验证的证据。

在达到 Active Directory Settings 页面的“Time to Live”参数中配置的小时数之前，思科 ISE 会保留缓存中的每个 Calling-Station-ID 属性值。参数过期之后，思科 ISE 会从参数缓存中删除该参数。

当用户从最终用户客户端进行身份验证时，思科 ISE 会在缓存中搜索在用户身份验证请求中收到的 Calling-Station-ID 值的成功计算机身份验证的 Calling-Station-ID 值。如果思科 ISE 在缓存中找到匹配的用户身份验证 Calling-Station-ID 值，这会以如下方式影响思科 ISE 为请求身份验证的用户分配权限：

- 如果在思科 ISE 缓存中找到与 Calling-Station-ID 值相匹配的值，则会分配成功授权的授权配置文件。
- 如果在思科 ISE 缓存中未找到与 Calling-Station-ID 值相匹配的值，则会分配成功用户身份验证（不含计算机身份验证）的授权配置文件。

## 配置授权策略和配置文件的指南

管理授权策略和配置文件时，请遵循以下规定：

- 您创建的规则名称必须仅使用以下支持的字符：
  - 符号：加号 (+)、连字符 (-)、下划线 (\_)、句点 (.) 和空格 ( )。
  - 字母字符：A-Z 以及 a-z。
  - 数字字符：0-9。
- 身份组默认为“Any”（您可以将此全局默认设置应用于所有用户）。
- 您可以通过条件设置一个或多个策略值。但是，条件是可选的，不一定要选择条件才能创建授权策略。以下是创建条件的两种方法：



- 从供选择的相应字典选择现有条件或属性。
- 创建允许您选择建议值或使用文本框来输入自定义值的自定义条件。
- 您创建的条件名称必须仅使用以下支持的字符：
  - 符号：连字符 (-)、下划线 ( \_ ) 和句点 ( . )。
  - 字母字符：A-Z 以及 a-z。
  - 数字字符：0-9。
- 选择用于策略的授权配置文件时，权限非常重要。权限可以允许访问特定资源或允许您执行特定任务。例如，如果用户属于特定身份组（例如设备管理员组）并且用户符合所定义的条件（例如属于波士顿的某个站点），则此用户可以获得与该身份组关联的权限（例如访问特定网络资源或在设备上执行特定操作的权限）。
- 在授权条件中使用 **radius** 属性 **Tunnel-Private-Group-ID** 时，必须在使用 **EQUALS** 运算符时在条件中同时提及标签和值，例如：


```
Tunnel-Private-Group-ID EQUALS (tag=0) 77
```
- 确保您点击 **Save** 以将新的或修改的策略或配置文件保存在思科 ISE 数据库中。


## 配置授权策略

在为授权策略创建属性和构建块后，应用这些属性并创建授权策略。

### 开始之前

在开始此程序之前，您应该对用于创建授权策略（如身份组和条件）的不同构建块有基本的了解。


- 步骤 1** 有关网络访问策略，请选择工作中心 (**Work Centers**) > 网络访问 (**Network Access**) > 策略集 (**Policy Sets**)。有关设备管理策略，请选择工作中心 (**Work Centers**) > 设备管理 (**Device Administration**) > 设备管理策略集 (**Device Admin Policy Sets**)。
- 步骤 2** 从“视图” (**View**) 列中，点击  以访问所有策略集详细信息，并创建身份验证和授权策略以及策略例外。
- 步骤 3** 点击页面“授权策略” (**Authorization Policy**) 部分旁的箭头图标以展开并查看授权策略表。
- 步骤 4** 在操作 (**Actions**) 列中，点击齿轮图标。从下拉菜单中，根据需要选择任何插入或重复选项来插入新的授权策略规则。  
授权策略表中将显示新行。
- 步骤 5** 要设置策略的状态，请点击当前状态 (**Status**) 图标，然后从下拉列表中选择状态 (**Status**) 列中的必要状态。有关状态的详细信息，请参阅[授权策略设置](#)。
- 步骤 6** 对于表中的任何策略，请点击规则名称 (**Rule Name**) 单元格，进行必要的自由文本更改，并创建唯一的规则名称。

**步骤 7** 要添加或更改条件，请将鼠标悬停在条件 (Conditions) 列中的单元格上，然后点击 。Conditions Studio 将打开。有关更多信息，请参阅[策略条件](#)，第 526 页。


不是您选择的所有属性都包含“等于”、“不等于”、“位于”、“不位于”、“匹配”、“开头为”或“开头非”运算符选项。

“Matches”运算符支持并使用正则表达式 (REGEX)，而不使用通配符。


**注释** 您必须使用“equals”运算符进行直接比较。“包含”运算符可用于多值属性。“匹配”运算符应用于正则表达式比较。当使用“匹配”运算符时，将解译正则表达式中的静态值和动态值。如果是列表，“位于”运算符会检查列表中是否存在特定值。如果是单个字符串，“位于”运算符会检查字符串是否与“等于”运算符相同。

**步骤 8** 对于网络访问结果配置文件，请从结果配置文件 (Results Profiles) 下拉列表中选择相关授权配置文件，或者选择或点击 ，选择创建新授权配置文件 (Create a New Authorization Profile)，然后在添加新标准配置文件 (Add New Standard Profile) 屏幕打开时，执行以下步骤：

- a) 根据需要输入值以配置新的授权配置文件。请注意以下事项：
  - 名称字段中支持的字符包括：空格 ! # \$ % & ‘ ( ) \* + , - . / ; = ? @ \_ { 。
  - 您可以从动态显示在屏幕底部的属性详细信息 (Attributes Details) 中仔细检查授权配置文件 RADIUS 语法。
- b) 点击保存 (Save) 以将所做的更改保存到思科 ISE 系统数据库，以便创建授权配置文件。
- c) 要在策略集区域之外创建、管理、编辑和删除配置文件，请选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles)。

**步骤 9** 对于网络访问结果安全组，请从结果安全组 (Results Security Groups) 下拉列表中选择相关安全组，或者点击 ，选择创建新安全组 (Create a New Security Group)，然后在“创建新安全组” (Create New Security Group) 屏幕打开时，执行以下步骤：

- a) 为新安全组输入名称和说明（可选）。
- b) 如果要将此 SGT 传播至 Cisco ACI，请选中传播至 ACI (Propagate to ACI) 复选框。只有当与此 SGT 相关的 SXP 映射属于在 Cisco ACI “设置” (Settings) 页面中选择的同一 VPN 时，它们才会传播至 Cisco ACI。  
默认情况下该选项处于禁用状态。
- c) 输入 Tag Value。标签值可以设置为手动输入或自动生成。您还可以为 SGT 保留范围。您可以从以下位置对其进行配置：管理 (Administration) > 系统 (System) > 设置 (Settings) > Trustsec 设置 (Trustsec Settings) 下的 Trustsec 全局设置页面。
- d) 点击 Submit。  
有关详细信息，请参阅[安全组配置](#)，第 586 页。

**步骤 10** 对于 TACACS+ 结果，请从结果 (Results) 下拉列表中选择相关命令集和外壳配置文件，或者点击命令集 (Command Sets) 或外壳配置文件 (Shell Profiles) 列中的 ，分别打开添加命令 (Add Commands) 屏幕或添加外壳配置文件 (Add Shell Profile)。选择创建新命令集 (Create a New Command Set) 或创建新外壳配置文件 (Create a New Shell Profile)，然后输入字段。

**步骤 11** 在表中组织用来检查和匹配策略的顺序。

**步骤 12** 点击 **Save** 保存您对思科 ISE 系统数据库所做的更改，并创建这条新的授权策略。

## 授权配置文件设置

授权配置文件 (**Authorization Profiles**) 窗口中的以下字段定义网络访问属性。此窗口的导航路径为：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles)**。

### 授权配置文件设置

- **名称 (Name)**: 输入此新授权配置文件的名称。
- **说明 (Description)**: 输入此授权配置文件的说明。
- **访问类型 (Access Type)**: 选择访问类型: **ACCESS\_ACCEPT** 或 **ACCESS\_REJECT**。
- **服务模板 (Service Template)**: 启用此选项以支持与有 SAnet 功能的设备的会话。思科 ISE 在授权配置文件中实施服务模板, 用一个特殊标志将其标记为兼容服务模板 (*Service Template*)。由于服务模板也是授权配置文件, 因此它充当支持 SAnet 和非 SAnet 设备的单个策略。
- **跟踪移动 (Track Movement)**: 启用此选项可通过思科移动服务引擎 (MSE) 跟踪用户位置。



**注释** 此选项可能会影响思科 ISE 性能, 仅适用于高安全性位置。

### 常见任务

常见任务是适用于网络访问的特定权限和操作。

- **DAACL 名称 (DAACL Name)**: 启用此选项可使用可下载的 ACL。例如, 思科 ISE 在下拉列表中提供两个默认值: **PERMIT\_ALL\_TRAFFIC** 或 **DENY\_ALL\_TRAFFIC**。此列表将包含本地数据库中的所有当前 DAACL。
- **安全组 (Security Group)**: 启用此选项可分配授权的安全组 (SGT) 部分。
  - 如果思科 ISE 未与 Cisco DNA Center 集成, 则思科 ISE 会分配 VLAN ID 1。
  - 如果思科 ISE 与 Cisco DNA Center 集成, 则选择 Cisco DNA Center 与思科 ISE 共享的虚拟网络 (VN), 选择数据类型 (**Data Type**) 和子网/地址池。

一个安全组任务包括一个安全组和一个可选 VN。如果配置安全组, 则无法单独配置 VLAN。终端设备只能分配给一个虚拟网络。

- **VLAN**: 启用此选项可指定虚拟 LAN (VLAN) ID。您可以为 VLAN ID 输入整数或字符串值。此条目的格式为 `Tunnel-Private-Group-ID:VLANnumber`。

- **语音域权限 (Voice Domain Permission):** 启用此选项可使用可下载的 ACL。供应商专用属性 (VSA) `cisco-av-pair` 与值 `device-traffic-class=voice` 相关联。在多域授权模式下，如果网络交换机收到此 VSA，则授权后终端将连接到语音域。
- **Web 重定向 (CWA、DRW、MDM、NSP、CPP) (Web Redirection (CWA, DRW, MDM, NSP, CPP)):** 启用此选项可在身份验证后启用 Web 重定向。

- 选择重定向类型。您选择的 Web 重定向类型会显示其他选项，如下所述。
- 输入 ACL 以支持让思科 ISE 发送到 NAD 的重定向。

您输入的发送到 NAD 的 ACL 在属性详细信息 (Attributes Details) 窗格中显示为 `cisco-av-pair`。例如，输入 `acl119`，它会在属性详细信息 (Attributes Details) 窗格中显示为：

```
cisco-av-pair = url-redirect-acl = acl119。
```

- 选择所选 Web 重定向类型的其他设置。

选择以下 Web 重定向类型之一：

- **集中式 Web 身份验证 (Centralized Web Auth):** 重定向到您从值 (Value) 下拉列表中选择的门户。
- **客户端调配 (安全评估) (Client Provisioning (Posture)):** 重定向到您从值 (Value) 下拉列表中选择的客户端调配门户，以在客户端上启用安全评估。
- **热点: 重定向 (Hot Spot: Redirect):** 重定向到您从值 (Value) 下拉列表中选择的热点门户。
- **MDM 重定向 (MDM Redirect):** 重定向到您指定的 MDM 服务器上的 MDM 门户。
- **本地请求方调配 (Native Supplicant Provisioning):** 重定向到您从值 (Value) 下拉列表中选择的 BYOD 门户。

在选择 Web 重定向类型并输入所需参数后，配置以下选项：

- **显示证书续约消息 (Display Certificates Renewal Message):** 启用此选项可显示证书续约消息。URL-redirect 属性值改变并且包含证书有效的天数。此选项仅适用于集中式 Web 身份验证重定向。
- **静态 IP/主机名/FQDN (Static IP/Host Name/FQDN):** 启用此选项可将用户重定向到其他 PSN。输入目标 IP 地址、主机名或 FQDN。如果不配置此选项，用户将重定向到收到此请求的策略服务节点的 FQDN。
- **在逻辑配置文件中抑制终端的分析器 CoA (Suppress Profiler CoA for endpoints in Logical Profile):** 启用此选项可取消特定类型终端设备的重定向。
- **自动智能端口 (Auto SmartPort):** 启用此选项可使用自动智能端口功能。输入事件名称，它会创建一个 VSA `cisco-av-pair`，该值为 `auto-smart-port=event_name`。此值显示在属性详细信息 (Attributes Details) 窗格中。
- **访问漏洞 (Access Vulnerabilities):** 启用此选项可作为授权的一部分在此终端上运行以威胁防护为中心的 NAC 漏洞评估。选择适配器以及运行扫描的时间。

- **重新验证身份 (Reauthentication):** 启用此选项可在重新验证身份期间保持终端连接。通过选择使用 **RADIUS-Request (1)**，选择在重新验证身份的过程中保持连接。默认 RADIUS-Request (0) 会断开现有会话。您还可以设置非活动计时器。
- **MACSec 策略:** 启用此选项可在启用 MACSec 的客户端连接到思科 ISE 时使用 MACSec 加密策略。选择以下选项之一：**must-secure**、**should-secure** 或 **must-not-secure**。您的设置在属性详细信息 (**Attributes Details**) 窗格中显示为：`cisco-av-pair = linksec-policy=must-secure`。
- **NEAT:** 启用此选项可使用网络边缘接入拓扑 (NEAT)，它能在网络之间扩展身份识别。如果选中此复选框，属性详细信息 (**Attributes Details**) 窗格中将显示 `cisco-av-pair = device-traffic-class=switch`。
- **Web 身份验证 (本地 Web 身份验证) (Web Authentication (Local Web Auth)):** 启用此选项可对此授权配置文件使用本地 Web 身份验证。通过由思科 ISE 发送 VSA 以及 DACL，此值使交换机能够识别用于 Web 身份验证的授权。VSA 为 `cisco-av-pair = priv-lvl=15`，显示在属性详细信息 (**Attributes Details**) 窗格中。
- **Airespace ACL名称 (Airespace ACL Name):** 启用此选项可向思科 Airespace 无线控制器发送 ACL 名称。Airespace VSA 使用此 ACL 向 WLC 上的连接授权本地定义的 ACL。例如，输入 **rsa-1188**，它会在属性详细信息 (**Attributes Details**) 窗格中显示为 `Airespace-ACL-Name = rsa-1188`。
- **ASA VPN:** 选中此选项可分配自适应安全设备 (ASA) VPN 组策略。从下拉列表中选择一个 VPN 组策略。
- **AVC 配置文件名称 (AVC Profile Name):** 启用此选项可在此终端上运行应用可视性。输入要使用的 AVC 配置文件。

### 高级属性设置

- **目录 (Dictionaries):** 点击向下箭头图标可查看目录 (**Dictionaries**) 窗口中的可用选项。在第一个字段中选择应配置的字典和属性。
- **属性值 (Attribute Values):** 点击向下箭头图标可显示属性值 (**Attribute Values**) 窗口中的可用选项。选择所需的属性组和属性值。此值与第一个字段中选择的值匹配。您配置的任何高级属性 (**Advanced Attributes**) 设置都将显示在属性详细信息 (**Attributes Details**) 面板中。
- **属性详细信息 (Attributes Details):** 此窗格显示您为常见任务 (**Common Tasks**) 和高级属性 (**Advanced Attributes**) 设置的已配置属性值。

属性详细信息 (**Attributes Details**) 窗格中显示的值是只读的。



**注释** 要修改或删除属性详细信息 (**Attributes Details**) 窗格中显示的任何只读值，请在对应的常见任务 (**Common Tasks**) 字段中或在高级属性设置 (**Advanced Attributes Settings**) 窗格的属性值 (**Attribute Values**) 字段中选择的属性中修改或删除这些值。

### 相关主题

[思科 ISE 授权配置文件](#)，第 518 页

[授权配置文件的权限](#)，第 518 页

[配置用于重定向未注册设备的授权配置文件](#)，第 507 页

[创建授权配置文件](#)，第 231 页

## 授权策略和例外

在每个策略集中，您可以定义常规授权策略，以及本地例外规则（从每个策略集的“集”(Set)视图中的“授权策略本地例外”(Authorization Policy Local Exceptions)部分定义)和全局例外规则（从每个策略集的“集”(Set)视图中的“授权策略全局例外”(Authorization Policy Global Exceptions)部分定义）。

使用全局授权例外策略，可以定义覆盖所有策略集中所有授权规则的规则。配置全局授权例外策略后，系统会将其添加到所有策略集。然后，可以从任何当前配置的策略集中更新全局授权例外策略。每次更新全局授权例外策略时，这些更新都会应用于所有策略集。

本地授权例外规则会覆盖全局例外规则。系统按以下顺序处理授权规则：首先处理本地例外规则，然后处理全局例外规则，最后处理授权策略常规规则。

授权例外策略规则的配置与授权策略规则相同。有关授权策略的信息，请参阅[配置授权策略](#)，第 521 页。



---

**注释** 为了避免安全问题，思科 ISE 不支持在授权策略中使用 % 字符。

---

## 策略条件

思科 ISE 使用基于规则的策略提供网络访问。策略是一组规则和结果，其中规则由条件组成。思科 ISE 可以让您将条件创建为可在系统库中存储的单个策略元素，然后从 **Conditions Studio** 重复用于其他基于规则的策略。

条件可以很简单，或者，必要时可以使用运算符（等于、不等于、大于，等等）和值，或者通过包含多个属性、运算符和复杂层次结构，使之变得复杂。在运行时，思科 ISE 会评估策略条件，然后根据策略评估返回的 **true** 值或 **false** 值，应用您所定义的结果。

在创建条件并为其分配唯一名称后，可以从 **Conditions Studio** 库中选择该条件，多次将其重复用于各种规则和策略，例如：

```
Network Conditions.MyNetworkCondition EQUALS true
```

不能从 **Condition Studio** 中删除策略中使用的条件或作为其他条件组成部分的条件。

每个条件各自定义可包括在策略条件中的对象列表，从而得到与请求中的定义匹配的一组定义。

您可以使用运算符 `EQUALS true` 来检查网络条件是否为 `true`（无论请求中存在的值是否与网络条件中的至少一个条目匹配）或 `EQUALS false`，以测试网络条件是否为 `false`（不匹配网络条件中的任何条目）。

思科ISE还提供预定义的智能条件，您可以在策略中单独使用这些条件，也可以将其作为您自己的自定义条件中的构建块，并且可以根据需要进行更新和更改。

您可以创建以下唯一网络条件以限制对网络的访问：

- 终端站网络条件 - 基于发起和终止连接的终端站。

思科ISE会评估远程地址 `TO` 字段（根据它是 `TACACS+` 还是 `RADIUS` 请求而获取），确定它是终端的 `IP` 地址、`MAC` 地址、主叫线路标识 (`CLI`) 还是被叫号码识别服务 (`DNIS`)。

在 `RADIUS` 请求中，标识符在属性 `31 (Calling-Station-Id)` 中可用。

在 `TACACS+` 请求中，如果远程地址包含斜杠 (`/`)，则斜杠前的部分作为 `FROM` 值，斜杠后的部分作为 `TO` 值。例如，如果请求具有 `CLI/DNIS`，则 `CLI` 作为 `FROM` 值，`DNIS` 作为 `TO` 值。如果不包含斜杠，则整个远程地址作为 `FROM` 值（不论是 `IP` 地址、`MAC` 地址或 `CLI`）。

- 设备网络条件 - 基于处理请求的 `AAA` 客户端。

可通过 `IP` 地址、在网络设备存储库中定义的设备名称或网络设备组确定网络设备。

在 `RADIUS` 请求中，如果存在属性 `4 (NAS-IP-Address)`，思科ISE会从该属性中获取 `IP` 地址。如果存在属性 `32 (NAS-Identifier)`，思科ISE将从属性 `32` 获取 `IP` 地址。如果未找到这些属性，它将从其接收的数据包获取 `IP` 地址。

设备字典（`NDG` 字典）包含网络设备组属性，如位置、设备类型或其他动态创建的表示 `NDG` 的属性。反过来，这些属性包含与当前设备相关的组。

- 设备端口网络条件 - 基于设备的 `IP` 地址、名称、`NDG` 和端口（终端站连接到的设备物理端口）。

在 `RADIUS` 请求中，如果请求中存在属性 `5 (NAS-Port)`，则思科ISE会从该属性中获取值。如果请求中存在属性 `87 (NAS-Port-Id)`，思科ISE将从属性 `87` 获取请求。

在 `TACACS+` 请求中，思科ISE会从（每个阶段的）起始请求的端口字段中获取此标识符。

有关这些独特条件的详细信息，请参阅[特殊网络访问条件](#)，第 545 页。

## 字典和字典属性

字典是关于可用于为域定义访问策略的属性和允许值的域特定目录。单个字典是同种属性类型的集合。字典中定义的属性具有相同的属性类型并且其类型会指明特定属性的来源或上下文。

属性类型可以是以下一种类型：

- `MSG_ATTR`
- `ENTITY_ATTR`
- `PIP_ATTR`

除了属性和允许的值之外，字典还包含关于名称与说明、数据类型和默认值等属性的信息。一个属性可以有以下一种数据类型：BOOLEAN、FLOAT、INTEGER、IPv4、OCTET\_STRING、STRING、UNIT32 和 UNIT64。

思科 ISE 在安装时会创建系统字典并且允许您创建用户字典。

属性存储在不同的系统词典中。属性用于配置条件。属性可以在多个条件中重复使用。

要在创建策略条件时重复使用某个有效的属性，请从包含支持的属性的词典中选择该属性。例如，思科 ISE 提供名为 `AuthenticationIdentityStore` 的属性，该属性位于 `Networkaccess` 目录中。该属性识别验证用户身份期间访问的最后一个身份源：

- 在身份验证期间使用单个身份源时，该属性包括成功进行身份验证所在的身份库的名称。
- 在身份验证期间使用某个身份源序列时，该属性包括访问的最后一个身份源的名称。

您可以将 `AuthenticationStatus` 属性与 `AuthenticationIdentityStore` 属性组合使用，以定义用来识别成功验证某个用户的身份的身份源的条件。例如，要使用授权策略中的 LDAP 目录 (LDAP13) 检查用户通过身份验证的条件，您可以定义下列可重复使用的条件：

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```



**注释** `AuthenticationIdentityStore` 表示允许您为该条件输入数据的文本字段。确保向该字段中正确输入或复制名称。如果身份源的名称发生更改，您必须确保修改此条件，以与身份源的更改保持一致。

要定义基于之前已进行身份验证的终端身份组的条件，思科 ISE 支持在终端身份组 802.1X 身份验证状态期间定义的授权。当思科 ISE 执行 802.1X 身份验证时，它从 RADIUS 请求的“Calling-Station-ID”字段中提取 MAC 地址，并使用该值查找和填充设备终端身份组（被定义为 `endpointIDgroup` 属性）的会话缓存。此过程使 `endpointIDgroup` 属性在创建授权策略条件时可供使用，并且允许您根据使用该属性的终端身份组信息（用户信息除外）来定义授权策略。

可以在授权策略配置页面的 ID Groups 列中定义终端身份组的条件。需要在授权策略的“Other Conditions”部分中定义基于用户相关信息的条件。如果用户信息基于内部用户属性，请使用内部用户目录中的 ID 组属性。例如，您可以使用诸如“User Identity Group:Employee:US”等值，在身份组中输入完整的值路径。

### 支持的网络访问策略词典

思科 ISE 支持以下系统存储的词典，这些词典包含为身份验证和授权策略构建条件和规则时所需的属性：

- 系统定义的字典
  - CERTIFICATE
  - DEVICE
  - RADIUS



- RADIUS 供应商字典
  - Airespace
  - Cisco
  - Cisco-BBSM
  - Cisco-VPN3000
  - Microsoft
  - Network access

对于授权策略类型，条件中配置的验证必须符合要返回的授权配置文件。

验证通常包括一个或多个条件，条件中包含用户定义的名称，可以将这些条件添加到库中并供其他策略重复使用。

以下部分介绍可用于配置条件的受支持属性和词典。

#### 字典支持的属性

此表列出字典支持的固定属性，这些属性可用于策略条件中。并非所有这些属性都可用于创建所有类型的条件。

例如，创建在身份验证策略中选取访问服务的条件时，您将只看到以下网络访问属性：Device IP Address、ISE Host Name、Network Device Name、Protocol 和 Use Case。

您可以将下表中列出的属性用于策略条件中。

字典	属性	允许的协议规则和代理	身份规则
设备	Device Type（预定义的网络设备组）	是	是
	Device Location（预定义的网络设备组）		
	Other Custom Network Device Group		
	Software Version		
	Model Name		
RADIUS	所有属性	是	是

字典	属性	允许的协议规则和代理	身份规则
网络接入	ISE Host Name	是	是
	AuthenticationMethod	不兼容	是
	AuthenticationStatus	不兼容	不兼容
	CTSDeviceID	不兼容	不兼容
	Device IP Address	是	是
	EapAuthentication（设备用户身份验证期间使用的 EAP 方法）	不兼容	是
	EapTunnel（用于建立隧道的 EAP 方法）	不兼容	是
	Protocol	是	是
	UseCase	是	是
	UserName	不兼容	是
	WasMachineAuthenticated	不兼容	不兼容

字典	属性	允许的协议规则和代理	身份规则
Certificate	Common Name	不兼容	是
	Country		
	E-mail		
	LocationSubject		
	Organization		
	Organization Unit		
	Serial Number		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - E-mail		
	Subject Alternative Name - Other Name		
	Subject Serial Number		
	Issuer		
	Issuer - Common Name		
	Issuer - Organization		
	Issuer - Organization Unit		
	Issuer - Location		
	Issuer - Country		
	Issuer - Email		
	Issuer - Serial Number		
	Issuer - State or Province		
Issuer - Street Address			
Issuer - Domain Component			
Issuer - User ID			

## 系统定义的字典和字典属性

思科 ISE 会在安装期间创建系统字典，您可以在 **System Dictionaries** 页面找到这些系统字典。系统定义的字典属性为只读属性。由于其性质，您只能查看现有的系统定义的字典。您不能创建、编辑或删除系统定义的值或系统字典中的任何属性。

所显示的系统定义的字典属性会带有属性的描述性名称、域识别的内部名称和允许的值。

IETF RADIUS 属性集也是系统定义的字典的一部分，由互联网工程任务组 (IETF) 定义，思科 ISE 也会为此属性集创建字典默认设置。您可以编辑除 ID 之外的所有 IETF RADIUS 自由属性字段。

## 显示系统字典和字典属性

您无法创建、编辑或删除系统字典中的任何系统定义的属性。您只能查看系统定义的属性。您可以执行基于字典名称和说明的快速搜索或基于您所定义的搜索规则的高级搜索。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 系统 (System)。

**步骤 2** 在 System Dictionaries 页面上选择系统字典，然后点击 **View**。

**步骤 3** 点击 **Dictionary Attributes**。

**步骤 4** 从列表中选择系统字典属性，然后点击 **View**。

**步骤 5** 点击 **Dictionaries** 链接以返回 System Dictionaries 页面。

---

## 用户定义的字典和字典属性

思科 ISE 显示您在 User Dictionaries 页面中创建的用户定义字典。在系统中创建并保存现有用户字典的 Dictionary Name 或 Dictionary Type 值后，将不能修改这些值。

您可以在 User Dictionaries 页面执行以下操作：

- 编辑和删除用户字典。
- 根据名称和说明搜索用户字典。
- 添加、编辑和删除用户字典中的用户定义的字典属性。
- 添加或删除允许的字典属性值

## 创建用户定义的字典

您可以创建、编辑或删除用户定义的字典。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 用户 (User)。

**步骤 2** 点击添加 (Add)。

**步骤 3** 为用户字典输入名称、可选说明和用户字典版本。

**步骤 4** 从 Dictionary Attribute Type 下拉列表选择属性类型。

**步骤 5** 点击提交。

---

## 创建用户定义的字典属性

您可以在用户字典中添加、编辑和删除用户定义的字典属性以及添加或删除用于字典属性的允许值。

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 用户 (User)。

**步骤 2** 从 User Dictionaries 页面选择用户字典，然后点击 **Edit**。

**步骤 3** 点击 **Dictionary Attributes**。

**步骤 4** 点击 **Add**。

**步骤 5** 为字典属性输入属性名称、可选说明和内部名称。

**步骤 6** 从 Data Type 下拉列表选择数据类型。

**步骤 7** 点击 **Add** 以配置名称、允许值，并在 Allowed Values 表中设置默认状态。

**步骤 8** 点击提交。

---

## RADIUS 供应商字典

思科 ISE 允许您定义一套 RADIUS 供应商字典并且为每个字典定义一系列属性。列表中的每个供应商定义都包含供应商名称、供应商 ID 和扼要说明。

默认情况下，思科 ISE 为您提供以下 RADIUS 供应商字典：

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

RADIUS 协议支持这些供应商字典以及可用于授权策略和策略条件的供应商特定属性。

## 创建 RADIUS 供应商字典

还可以创建、编辑、删除、导出和导入 RADIUS 供应商字典。

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 系统 (System) > Radius > Radius 供应商 (Radius Vendors)。

步骤 2 点击添加 (Add)。

步骤 3 输入 RADIUS 供应商字典的名称、可选说明，以及由互连网号码分配机构 (IANA) 批准的 RADIUS 供应商的供应商 ID。

步骤 4 从 Vendor Attribute Type Field Length 下拉列表中选择从属性值提取用于指定属性类型的字节数。有效值为 1、2 和 4。默认值为 1。

步骤 5 从 Vendor Attribute Size Field Length 下拉列表中选择从属性值提取用于指定属性长度的字节数。有效值为 0 和 1。默认值为 1。

步骤 6 点击提交。

---

## 创建 RADIUS 供应商字典属性

您可以创建、编辑和删除思科 ISE 支持的 RADIUS 供应商属性。每个 RADIUS 供应商属性都有名称、数据类型、说明和方向，其指定属性是否仅与请求相关、仅与响应相关，还是与二者都相关。

---

步骤 1 选择策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 系统 (System) > Radius > Radius 供应商 (Radius Vendors)。

步骤 2 从 RADIUS 供应商字典列表选择 RADIUS 供应商字典，然后点击 **Edit**。

步骤 3 点击 **Dictionary Attributes**，然后点击 **Add**。

步骤 4 为 RADIUS 供应商属性输入属性名称和可选说明。

步骤 5 从 Data Type 下拉列表选择数据类型。

步骤 6 选中 **Enable MAC option** 复选框。

步骤 7 从 Direction 下拉列表选择仅应用于 RADIUS 请求、仅应用于 RADIUS 响应或同时应用于二者的方向。

步骤 8 在 ID 字段输入供应商属性 ID。

步骤 9 选中 **Allow Tagging** 复选框。

步骤 10 选中 **Allow multiple instances of this attribute in a profile** 复选框。

步骤 11 点击 **Add** 以在 Allowed Values 表中为供应商属性添加允许的值。

步骤 12 点击提交。

---

## RADIUS 供应商字典属性设置

本节介绍思科 ISE 中使用的 RADIUS 供应商字典。

下表介绍了 RADIUS 供应商的“字典” (Dictionary) 窗口中的字段，可以通过此窗口为 RADIUS 供应商配置字典属性。此窗口的导航路径为策略 (Policy) > 策略元素 (Policy Elements) > 字典 (Dictionaries) > 系统 (System) > RADIUS > RADIUS 供应商 (RADIUS Vendors)。

表 89: RADIUS 供应商字典属性设置

字段名称	使用指南
属性名称 (Attribute Name)	输入选定 RADIUS 供应商的供应商特定属性名称。
Description	输入供应商特定属性的可选说明。
内部名称 (Internal Name)	输入数据库内部所称呼的供应商特定属性的名称。
数据类型 (Data Type)	为供应商特定属性选择以下其中一种数据类型： <ul style="list-style-type: none"> <li>• STRING</li> <li>• OCTET_STRING</li> <li>• UNIT32</li> <li>• UNIT64</li> <li>• IPV4</li> </ul>
Enable MAC option	<p>选中此复选框可启用将 RADIUS 属性比作为 MAC 地址。默认情况下，对于 RADIUS 属性 <code>calling-station-id</code>，此选项标记为启用，您无法禁用此选项。对于 RADIUS 供应商字典中的其他（字符串类型）字典属性，可以启用或禁用此选项。</p> <p>启用此选项之后，在设置身份验证和授权条件时，可以通过选择 Text 选项来定义对比是否是明文字符串，或通过选择 MAC address 选项来定义是否是 MAC 地址。</p>
方向	选择一个适用于 RADIUS 消息的选项：
ID	输入供应商属性 ID。有效范围为 0 至 255。
允许标记 (Allow Tagging)	<p>根据 RFC2868 定义，选中该复选框，将属性标记为已被允许带有标签。该标签旨在允许将已建立隧道的用户的属性进行分组。有关详细信息，请参阅 RFC2868。</p> <p>已标记的属性支持确保有关指定隧道的所有属性在各自的标签字段中包含相同值，并且，每组包含一个 Tunnel-Preference 属性实例。这符合将用于多供应商网络环境中的隧道属性，以此消除不同供应商生产的网络接入服务器 (NAS) 之间的互通性问题。</p>

字段名称	使用指南
允许配置文件中存在该属性的多个实例 ( <b>Allow Multiple Instances of this Attribute in a Profile</b> )	当希望配置文件中存在此 RADIUS 供应商特定属性的多个实例时，请选中此复选框。

#### 相关主题

[系统定义的字典和字典属性](#)，第 532 页

[用户定义的字典和字典属性](#)，第 532 页



[RADIUS 供应商字典](#)，第 533 页

[创建 RADIUS 供应商字典](#)，第 533 页

## 浏览 Conditions Studio

使用 Conditions Studio 创建、管理和重复使用条件。条件可以包括多个规则，并且结构复杂性不限（包括仅一个级别或多个层级）。使用 Conditions Studio 创建新条件时，可以使用已存储在库中的条件块，也可以更新和更改这些存储的条件块。在稍后创建和管理条件时，可以使用快速类别过滤器等轻松查找需要的块和属性。

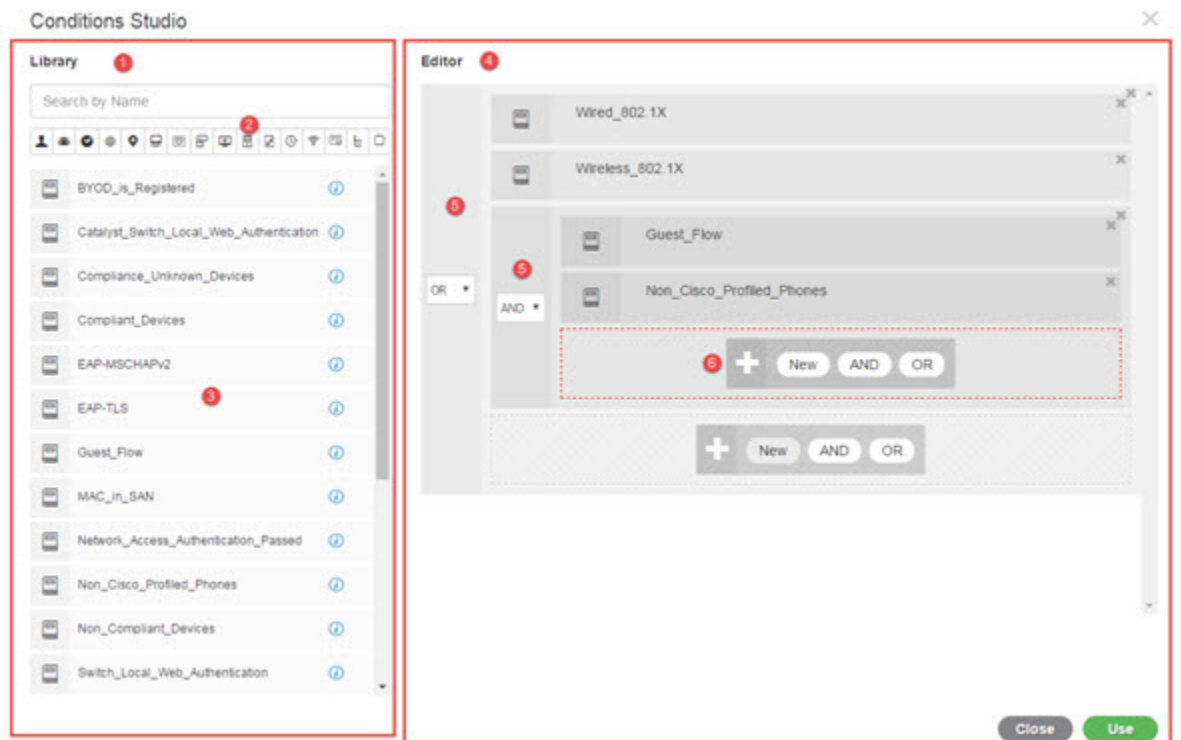
有关网络访问策略，请选择工作中心 (**Work Centers**) > 网络访问 (**Network Access**) > 策略集 (**Policy Sets**)。有关设备管理策略，请选择工作中心 (**Work Centers**) > 设备管理 (**Device Administration**) > 设备管理策略集 (**Device Admin Policy Sets**)。

要编辑或更改已应用于任何策略集中的特定规则的条件，请将鼠标悬停在条件 (**Conditions**) 列中的单元格上，然后点击 ，或者从策略集表中的条件 (**Conditions**) 列点击加号  以创建新列，随后可以立即将其应用于同一策略集，也可以将其保存在库中以供将来使用。

下图显示 Conditions Studio 的主要元素。




图 28: Conditions Studio



Condition Studio 分为两个主要部分：库和编辑器。库可以存储条件块以供重复使用，而编辑器可以让您编辑这些已保存的块和创建新的块。

下表介绍了 Condition Studio 的不同部分：

字段	使用指南
库	<p>显示已创建并保存在 ISE 数据库中以供重复使用的所有条件块的列表。若要在当前编辑的条件中使用这些条件块，请将其从库中拖放到编辑器中的相关级别，必要时更新运算符。</p> <p>存储在库中的条件全部用库图标  表示，原因是条件可以与多个类别相关联。</p> <p>在库中的每个条件旁，也可以找到该图标。将鼠标悬停在此图标上可查看条件的完整说明，查看其关联的类别，还可以从库中彻底删除条件。如果条件被策略使用，则无法删除这些条件。</p> <p>将任何库条件拖放到编辑器中，以便将其单独用于当前编辑的策略，或作为更复杂条件的构建块，以便在当前策略中使用或在库中另存为新条件。您还可以在编辑器中拖放条件，以便对该条件进行更改，然后在库中以相同名称或新名称保存该条件。</p> <p>安装后还有预定义条件。这些条件也可以更改和删除。</p>
搜索和过滤	<p>按名称搜索条件或按类别过滤条件。以类似的方式，还可以从编辑器中的 <b>点击以添加属性 (Click to add an attribute)</b> 字段搜索和过滤属性。工具栏上的图标代表不同的属性类别，如主题、地址等。点击图标可查看与特定类别相关的属性，而点击类别工具栏中的突出显示图标可取消选择该类别，从而删除过滤器。</p>
条件列表	<p>库中所有条件的完整列表，或库中基于搜索或过滤结果而显示的条件列表。</p>
编辑人	<p>创建要立即使用的新条件，以及要保存在系统库中以供将来使用的新条件，然后编辑现有条件并将这些更改保存在库中，以供立即使用和将来使用。</p> <p>当打开 Conditions Studio 以创建新条件时（点击任意策略集表中的加号），会显示只包含一个空行的编辑器，您可以在其中添加第一个规则。</p> <p>当编辑器打开并显示空字段时，不会显示任何运算符图标</p>

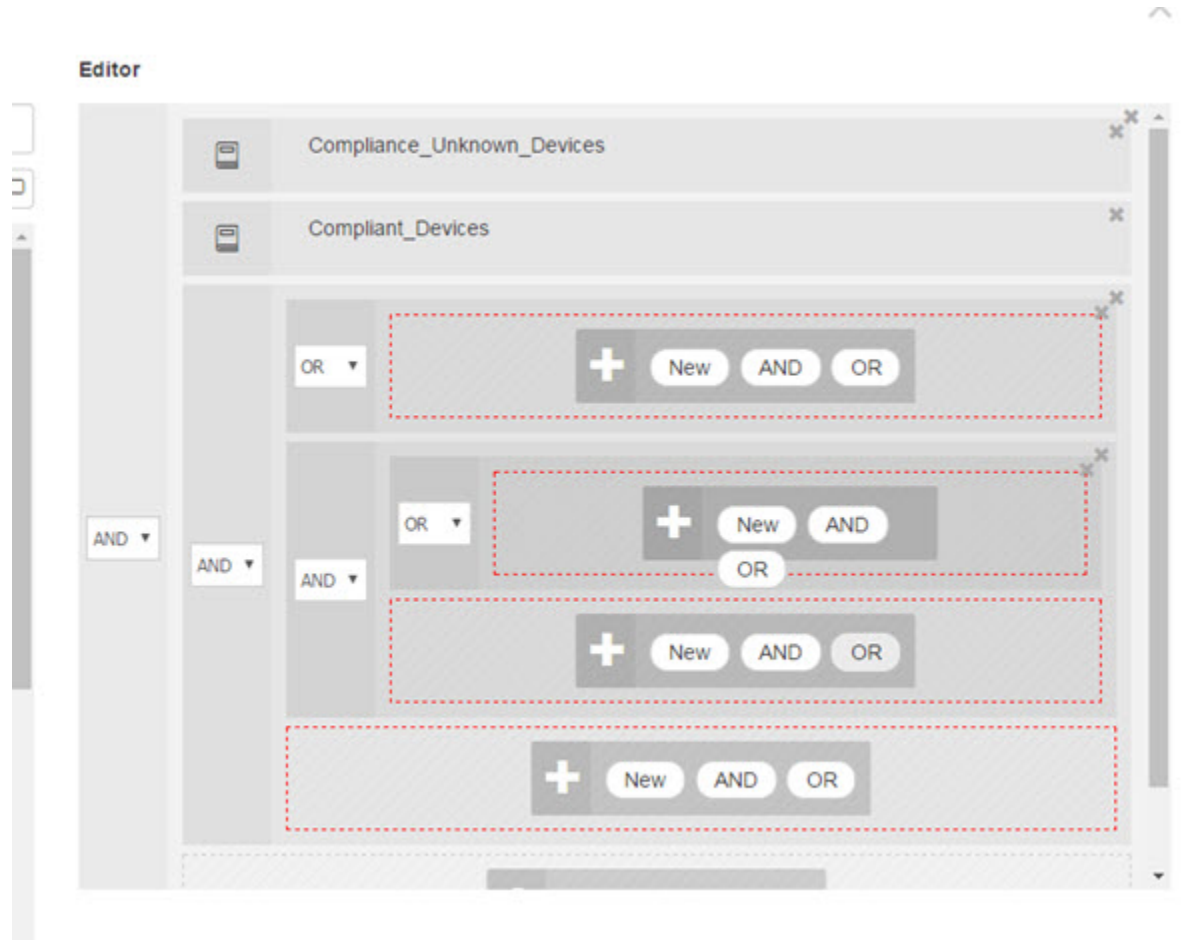
字段	使用指南
	<p>编辑器分为不同的虚拟列和行。</p> <p>列表示不同的层次结构级别，每列根据其在层次结构中的位置缩进；行代表单个规则。您可以为每个级别创建单个或多个规则，并且可以包含多个级别。</p> <p>上图中的示例显示了正在构建或编辑的条件，包括规则层次结构，图中的第一级和第二级均标有数字 5。顶级父级别的规则使用运算符 OR。</p> <p>要在选择运算符并创建层次结构级别后更改该运算符，只需从此列中显示的下拉列表中选择相关选项。</p> <p>除了运算符下拉列表之外，每个规则在此列中都有一个相关图标，指示其所属的类别。如果将鼠标悬停在图标上，工具提示会指示类别的名称。</p> <p>一旦保存到库中，系统将分配库图标，替换编辑器中显示的类别图标。</p> <p>最后，如果将规则配置为排除所有相关的匹配项目，则此列中也会显示“不是” (Is-Not) 标志。例如，如果将值为 London 的位置属性设置为“不是” (Is-Not)，则来自伦敦的所有设备都将被拒绝访问。</p>

字段	使用指南
	<p>此区域显示使用层次结构级别以及同一条件中的多个规则时可用的选项。</p> <p>当将鼠标悬停在任何列或行上时，会显示相关操作。选择操作时，该操作会应用于该部分和所有子部分。例如，当层次结构 A 中有五个级别时，如果从第三级中的任何规则中选择“和”(AND)，则会在原规则下创建新的层次结构 B，以便原规则成为层次结构 B 的父规则，嵌入在层次结构 A 中。</p> <p>当首次打开 Condition Studio 以从头创建新条件时，编辑器区域仅包含一行（用于您可配置的单个规则），以及用于选择相关运算符或从库中拖放相关条件的选项。</p> <p>使用和 (AND) 和或 (OR) 运算符选项可以向条件中添加其他级别。选择新建 (New)，可在点击选项的同一级别创建新规则。只有在层次结构的顶层配置至少一个规则后，新建 (New) 选项才会显示。</p>

## 配置、编辑和管理策略条件

使用 Conditions Studio 创建、管理和重复使用条件。条件可以包括多个规则，并且结构复杂性不限（包括仅一个级别或多个层级）。从 Conditions Studio 的编辑器侧管理条件层次结构，如下图所示：

图 29: 编辑器 - 条件层次结构



创建新条件时，可以使用已存储在库中的条件块，也可以更新和更改这些存储的条件块。在创建和管理条件时，可以使用快速类别过滤器等工具轻松找到所需的块和属性。

在创建和管理条件规则时，请使用属性、运算符和值。




思科 ISE 包含一些最常见用例的预定义复合条件。您可以编辑这些预定义条件来满足您的要求。为重用而保存的条件（包括即用型块）存储在 Condition Studio 的库中，如本任务中所述。

要执行以下任务，您必须是超级管理员或策略管理员。

**步骤 1** 访问“策略集” (Policy Sets) 区域。选择**策略 (Policy) > 策略集 (Policy Sets)**。

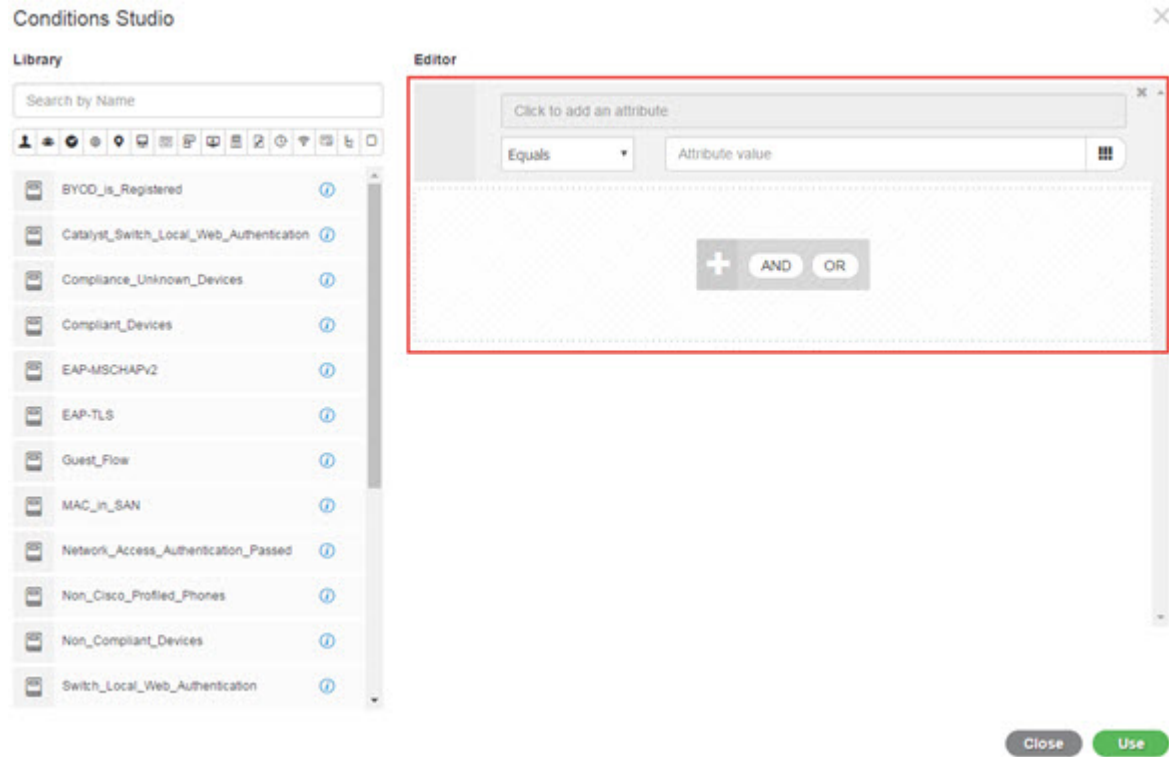
**步骤 2** 访问 Conditions Studio 以创建新条件并编辑现有条件块，以便随后将这些条件纳入您为特定策略集（及其关联策略和规则）配置的规则中，或保存到库以供将来使用：

- a) 从“策略集” (Policy Set) 主页面上的“策略集” (Policy Set) 表的“条件” (Conditions) 列中点击 **+**，以创建与整个策略集相关的条件（在匹配身份验证策略规则之前检查的条件）。

- b) 或者，从特定策略集行点击 ，以查看“设置”(Set)视图，包括所有身份验证和授权规则。在“设置”(Set)视图中，将鼠标悬停在任何规则表的**条件 (Conditions)**列中的单元格上，然后点击  打开 Conditions Studio。
- c) 如果您正在编辑已应用于策略集的条件，请点击  以访问 Conditions Studio。

Conditions Studio 将打开。如果您已打开它来创建新条件，则如下图所示。若要查看字段的说明，以及打开 Conditions Studio 后如何编辑策略集已应用的条件的示例，请参阅[浏览 Conditions Studio](#)，第 536 页。

图 30: *Conditions Studio* - 创建新条件



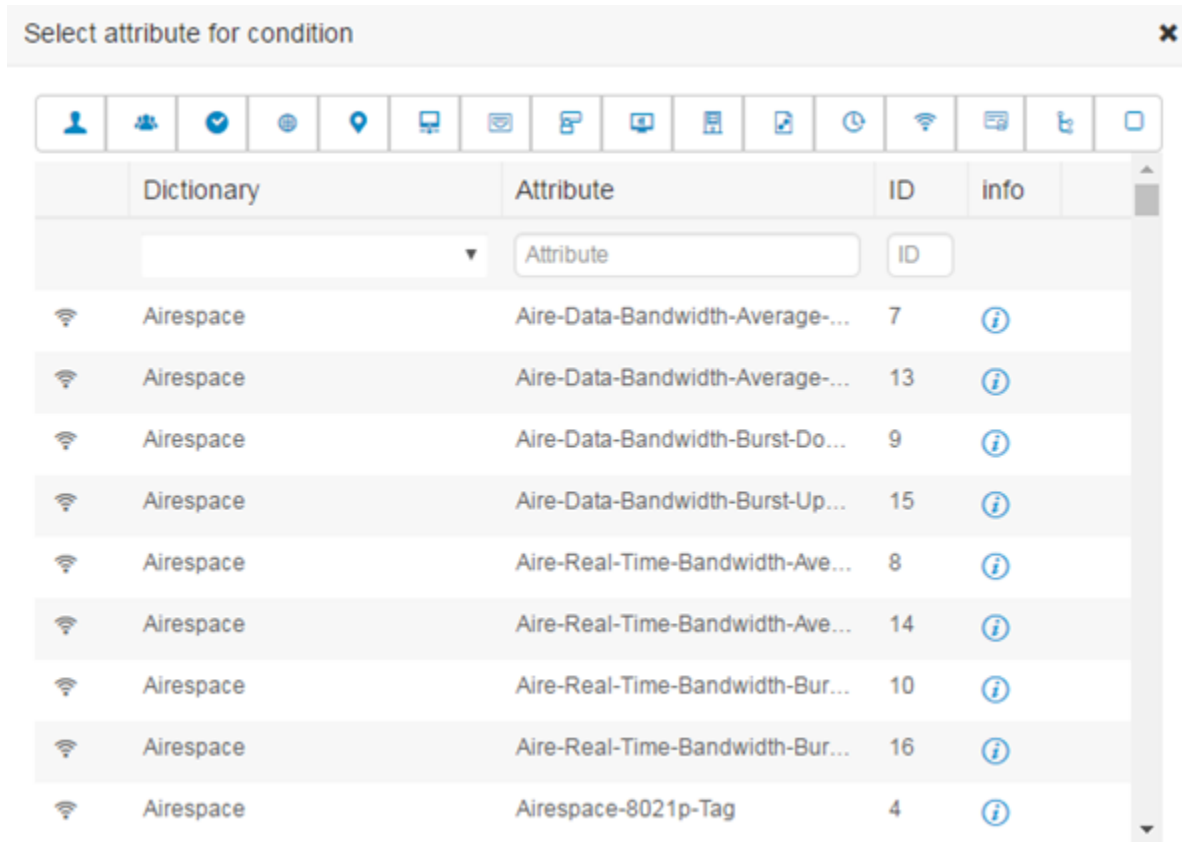
**步骤 3** 使用库中的现有条件块作为您正在创建或编辑的条件中的规则。

- 通过从类别工具栏中选择相关类别进行过滤 - 库中显示包含所选类别的属性的所有块。此外，还会显示包含多个规则但至少一个规则中使用了所选类别的属性的条件块。如果添加了其他过滤器，则显示的结果仅包括符合该特定过滤器而且与包含的其他过滤器也匹配的条件块。例如，从工具栏中选择“端口”(Ports)类别，并在**按名称搜索 (Search by Name)** 字段中输入自由文本“auth”，就会显示与名称中包含“auth”的端口相关的所有块。再次点击类别工具栏中突出显示的图标，取消选择它，从而删除该过滤器。
- 使用自由文本搜索条件块 - 在**按名称搜索 (Search by Name)** 自由文本字段中，输入要搜索的块名称中出现的任何术语或部分术语。在您键入内容时，系统会实时动态搜索相关结果。如果未选择类别（未突出显示任何图标），则结果包括来自所有类别的条件块。如果已选择类别图标（显示的列表已过滤），则显示的结果仅包括该特定类别中使用特定文本的块。
- 找到条件块后，将其拖到编辑器中，放到要构建的块的正确级别上。如果放置的位置不正确，您可以在编辑器中再次拖放，直至放置正确。
- 将鼠标悬停在编辑器中的条件块上，然后点击**编辑 (Edit)** 更改规则，以便对处理的条件做出相关的更改，用这些更改覆盖库中的规则，或者在库中将规则另存为新块。

放入编辑器时为只读状态的块现在可以编辑了，并且与编辑器中的所有其他自定义规则具有相同的字段、结构、列表和操作。继续执行后续步骤，了解有关编辑此规则的更多信息。

**步骤 4** 向当前级别添加运算符，以便随后在同一级别添加其他规则 - 选择 **AND**、**OR** 或 **Set to 'Is not'**。 **Set to 'Is not'** 也可应用于单个规则。

**步骤 5** 使用属性词典创建和编辑规则 - 点击 **点击以添加属性字段**。属性选择器随即打开，如下图所示：



属性选择器的各部分如下表所述：

字段	使用指南
属性类别工具栏	包含每个不同属性类别的唯一图标。选择任何属性类别图标，按类别过滤视图。 点击突出显示的图标可取消选择它，从而删除过滤器。
字典	表示存储属性的词典的名称。从下拉列表中选择特定词典，以便按供应商词典过滤属性。
属性	表示属性的名称。在可用字段中为属性名称键入自由文本来过滤属性。在您键入内容时，系统会实时动态搜索相关结果。

字段	使用指南
ID	表示唯一属性标识号。在可用字段中键入 ID 号来过滤属性。在您键入内容时，系统会实时动态搜索相关结果。
信息	将鼠标悬停在相关属性行上的信息图标上可查看有关属性的额外详细信息。

- a) 从属性选择器的搜索框中，过滤并搜索所需的属性。在属性选择器的任何部分过滤或输入自由文本时，如果未激活其他过滤器，则结果仅包括与所选过滤器相关的所有属性。如果使用多个过滤器，则显示的搜索结果与所有过滤器匹配。例如，点击工具栏中的“端口”(Port)图标并在“属性”(Attribute)列中键入“auth”，则仅显示端口类别中名称含“auth”的属性。选择类别时，工具栏中的图标以蓝色突出显示，并显示过滤后的列表。再次点击类别工具栏中突出显示的图标，取消选择它，从而删除过滤器。
- b) 选择相关属性，将其添加到规则中。  
属性选择器关闭，您选择的属性会添加到点击以添加属性 (Click to add an attribute) 字段。
- c) 从等于 (Equals) 下拉列表中，选择相关运算符。

不是您选择的所有属性都包含“Equals”、“Not Equals”、“Matches”、“Starts With”或“Not Starts With”运算符选项。

“Matches”运算符支持并使用正则表达式 (REGEX)，而不使用通配符。

您必须使用“equals”运算符进行直接比较。“包含”运算符可用于多值属性。“匹配”运算符应用于正则表达式比较。当使用“匹配”运算符时，将解译正则表达式中的静态值和动态值。

- d) 在属性值 (Attribute value) 字段中，执行以下操作之一：
  - 在字段中键入自由文本值
  - 从列表选择一个动态加载的值（相关时 - 取决于上一步中选择的属性）
  - 使用其他属性作为条件规则的值 - 选择字段旁边的表图标以打开属性选择器，然后搜索、过滤并选择相关属性。属性选择器关闭，您选择的属性会添加到属性值 (Attribute value) 字段。

**步骤 6** 在库中将规则另存为条件块。

- a) 将鼠标悬停在要在库中另存为块的规则或规则的层次结构上。任何可另存为单个条件块的规则或规则组都将显示复制 (Duplicate) 和保存 (Save) 按钮。如果要将一组规则另存为块，请在整个层次结构的阻止区域中从整个层次结构的底部选择操作按钮。
- b) 单击保存。系统将弹出“保存条件” (Save condition) 屏幕。
- c) 选择：
  - 保存到现有库条件 - 选择此选项可使用您创建的新规则覆盖库中的现有条件块，然后在从列表中选择 (Select from list) 下拉列表中选择要覆盖的条件块。
  - 另存为新库条件 - 在块的“条件名称” (Condition Name) 字段中键入唯一名称。
- d) (可选) 在说明 (Description) 字段中输入说明。当您将鼠标悬停在库中任何条件块的信息图标上时，系统会显示此说明，使您能够快速识别不同的条件块及其用途。



e) 点击**保存 (Save)** 在库中保存条件块。

**步骤 7** 在新的子级别上创建新规则 - 请点击 **AND** 或 **OR**，在现有父层级和您创建的子层级之间应用正确的运算符。新部分与所选运算符一起添加到编辑器层次结构中，作为提供所选运算符的规则或层次结构的子项。

**步骤 8** 在当前现有级别上创建新规则 - 从相关级别点击**新建 (New)**。在您开始的同一级别中，将显示新规则的一个空行。

**步骤 9** 点击 **X** 从编辑器中删除任何条件及其所有子项。

**步骤 10** 点击**复制 (Duplicate)** 可自动复制并粘贴层次结构中的特定条件，从而在同一级别创建其他相同的子项。您可以复制有或无子项的单个规则，具体取决于您点击**复制 (Duplicate)** 按钮的级别。

**步骤 11** 点击页面底部的**使用 (Use)** 保存在编辑器中创建的条件，并在策略集中实施该条件。

**注释** 当任何策略集中需要 AD 属性时，必须配置相应的 AD 条件。

---

## 特殊网络访问条件

本部分说明了在创建策略集时有用的独特条件。这些条件无法从条件 Studio 创建，因此具有其自己的唯一进程。

---

## 配置设备网络条件

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 网络条件 (Network Conditions) > 设备网络条件 (Device Network Conditions)。

**步骤 2** 点击 **Add**。

**步骤 3** 输入网络条件名称和说明。

**步骤 4** 输入下列详细信息：

- IP 地址 - 您可以添加 IP 地址或子网列表，每行一个。IP 地址/子网可以采用 IPV4 或 IPV6 格式。
- 设备名称 - 您可以添加设备名称列表，每行一个。必须输入在网络设备对象中配置的同设备名称。
- 设备组 - 可以添加元组列表（按以下顺序）：根 NDG、逗号、（在根 NDG 下的）NDG。必须每行一个元组。

**步骤 5** 点击**提交**。

---

## 配置设备端口网络条件

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 网络条件 (Network Conditions) > 设备端口网络条件 (Device Port Network Conditions)。

步骤 2 点击 **Add**。

步骤 3 输入网络条件名称和说明。

步骤 4 输入下列详细信息：

- IP 地址 (IP Addresses) - 按以下顺序输入详细信息：IP 地址或子网、逗号和（设备使用的）端口。必须每行一个元组。
- 设备 (Devices) - 按以下顺序输入详细信息：设备名称、逗号和端口。必须每行一个元组。您必须输入在网络设备对象中配置的同名设备名称。
- 设备组 (Device Groups) - 按以下顺序输入详细信息：根 NDG、逗号、（在根下的）NDG 和端口。必须每行一个元组。

步骤 5 点击提交。

---

## 配置终端站网络条件

步骤 1 选择策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 网络条件 (Network Conditions) > 终端站网络条件 (Endstation Network Conditions)。

步骤 2 点击 **Add**。

步骤 3 输入网络条件名称和说明。

步骤 4 输入下列详细信息：

- IP 地址 - 您可以添加 IP 地址或子网列表，每行一个。IP 地址/子网可以采用 IPV4 或 IPV6 格式。
- MAC 地址 - 您可以输入终端 MAC 地址和目标 MAC 地址的列表，用逗号分隔。每个 MAC 地址必须包含 12 个十六进制数字，且必须为以下格式之一：nn:nn:nn:nn:nn:nn、nn-nn-nn-nn-nn-nn、nnnn.nnnn.nnnn 或 nnnnnnnnnnnn。  
如果不需要终端站 MAC 或目标 MAC，请使用令牌“-ANY-”代替。
- CLI/DNIS - 您可以添加主叫方 ID (CLI) 和被叫方 ID (DNIS) 的列表，用逗号分隔。如果不需要主叫方 ID (CLI) 或被叫方 ID (DNIS)，请使用令牌“-ANY-”代替。

步骤 5 点击提交。

---

## 创建时间和日期条件

使用 Policy Elements Conditions 页面显示、创建、修改、删除、复制以及搜索时间和日期策略元素条件。策略元素是共享的对象，定义一个基于您所配置的特定时间和日期属性设置的条件。

使用时间和日期条件，使您可以按照您做出属性设置所指定的特定时间和日期来设置或限制访问思科 ISE 系统资源的权限。

### 开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 时间和日期 (Time and Date) > 添加 (Add)。

**步骤 2** 在字段中输入适当的值。

- 在 Standard Settings 区域中，指定提供访问的时间和日期。
- 在 Exceptions 区域中，指定限制访问的时间和日期。

**步骤 3** 点击提交。

## 在授权策略中使用 IPv6 条件属性

思科 ISE 可以检测、管理和保护来自终端的 IPv6 流量。

当一个支持 IPv6 的终端连接至思科 ISE 网络时，它通过 IPv6 网络与 NAD 通信。NAD 通过 IPv4 网络将来自终端的计费和分析信息（包括 IPv6 值）发送至思科 ISE。您可以使用规则条件中的 IPv6 属性在思科 ISE 中配置授权配置文件和策略，以处理来自支持 IPv6 终端的这些请求，并且确保终端合规。

您可以在 IPv6 前缀和 IPv6 接口值中使用通配符。例如：2001:db8:1234::/48。

支持的 IPv6 地址格式包括：

- 完整表示法：冒号分隔的八组四个十六进制数字。例如，2001:0db8:85a3:0000:0000:8a2e:0370:7334
- 缩短表示法：去除组中的前导零；使用两个连续的冒号替换零值组。例如：  
2001:db8:85a3::8a2e:370:7334
- 点分四组表示法（IPv4 映射和兼容 IPv4 的 Ipv6 地址）：例如，::ffff:192.0.2.128

支持的 IPv6 属性包括：

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Delegated-IPv6-Prefix
- Framed-IPv6-Address

- DNS-Server-IPv6-Address
- Route-IPv6-Information
- Delegated-IPv6-Prefix-Pool
- Stateful-IPv6-Address-Pool

下表列出了受支持的思科属性-值对其等效 IETF 属性：

思科属性值对	IETF 属性
ipv6:addrv6=<ipv6 address>	Framed-ipv6-Address
ipv6:stateful-ipv6-address-pool=<name>	Stateful-IPv6-Address-Pool
ipv6:delegated-ipv6-pool=<name>	Delegated-IPv6-Prefix-Pool
ipv6:ipv6-dns-servers-addr=<ipv6 address>	DNS-Server-IPv6-Address

RADIUS 实时日志页面、RADIUS 身份验证报告、RADIUS 记账报告、当前活动会话报告、RADIUS 错误报告、错误配置的 NAS 报告、EPS 审核报告、和错误配置的请求方客户端报告均支持 IPv6 地址。您可以从 RADIUS 实时日志页面或通过任何这些报告查看有关这些会话的详细信息。您可以根据 IPv4、IPv6 或 MAC 地址来过滤记录。



**注释** 如果将一个 Android 设备连接至支持 IPv6 的 DHCPv6 网络，它从 DHCP 服务器仅接收本地链路 IPv6 地址。因此，全局 IPv6 地址不在实时日志和终端页面（**管理 (Administration) > 身份管理 (Identity Management) > 身份 (Identities) > 终端 (Endpoints)**）中显示。

以下步骤描述了如何在授权策略中配置 IPv6 属性。

#### 开始之前

确保在您的部署中网络接入设备 (NAD) 支持具备 IPv6 的 AAA。有关如何在 NAD 上启用 AAA IPv6 支持的信息，请参阅 [AAA IPv6 支持](#)。

**步骤 1** 选择 **策略 (Policy) > 授权 (Authorization) > 标准 (Standard)**。

**步骤 2** 点击最右侧的向下箭头并选择在上面插入新规则 (**Insert New Rule Above**) 或在下面插入新规则 (**Insert New Rule Below**)。

**步骤 3** 输入规则名称并指定条件。

从 RADIUS 字典中选择 RADIUS IPv6 属性、运算符和值。

**步骤 4** 点击**完成 (Done)**。

## 用于身份验证的协议设置

必须先 在思科 ISE 中定义全局协议设置，然后才能使用这些协议创建、保存和实施策略集以处理身份验证请求。您可以使用 Protocol Settings 页面为 Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)、Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) 和 Protected Extensible Authentication Protocol (PEAP) 协议定义全局选项，这些协议可以与网络中的其他设备进行通信。

### 支持的身份验证协议

以下是您在定义身份验证策略时可以选择的协议的列表：

- 密码身份验证协议 (PAP)
- 受保护的可扩展身份验证协议 (PEAP)
- Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)
- 可扩展身份验证协议消息摘要 5 (EAP-MD5)
- 可扩展身份验证协议-传输层安全 (EAP-TLS)
- 可扩展身份验证协议-通过安全隧道的灵活身份验证 (EAP-FAST)
- 受保护的可扩展身份验证协议-传输层安全 (PEAP-TLS)

### 将 EAP-FAST 用作身份验证协议的指南

将 EAP-FAST 用作身份验证协议时，请遵循以下规定：

- 在经过身份验证的调配中启用 EAP-FAST 接受客户端证书时，强烈建议启用 EAP-TLS 内部方法。经过身份验证的调配中的 EAP-FAST 接受客户端证书不是一个单独的身份验证方法，而是一种更简短的客户端证书身份验证形式，它使用相同的证书凭证类型来对用户进行身份验证，但是不需要运行内部方法。
- 经过身份验证的调配中的接受客户端证书适用于无 PAC 完全握手和经过身份验证的 PAC 调配。它不适用于无 PAC 会话恢复、匿名 PAC 调配和基于 PAC 的身份验证。
- EAP 属性按身份显示（所以在 EAP 链中会显示两次），即使身份验证按照不同的顺序进行，在监控工具的身份验证详细信息中仍然会按照先用户后设备的顺序显示。
- 当使用 EAP-FAST 授权 PAC 时，实时日志中显示的 EAP 身份验证方法等于用于完全身份验证（如在 PEAP 中）而非用于查找的身份验证方法。
- 在 EAP 链接模式中，当隧道 PAC 到期，然后 ISE 退回调配且 AC 请求用户和设备授权 PAC 时 - 无法调配设备授权 PAC。当 AC 请求时，它将在后续基于 PAC 的身份验证对话中进行调配。

- 当为链接配置思科 ISE 并且为单一模式配置 AC 时，则 AC 使用身份类型 TLV 向 ISE 做出响应。但是，第二个身份的身份验证会失败。您可以通过此对话看到客户端适合执行链接，但当前未为单一模式执行配置。
- 思科 ISE 支持在仅适用于 AD 的 EAP-FAST 链中检索设备和用户的属性与组。对于 LDAP 和内部数据库，ISE 仅使用最后的身份属性。



**注释** 如果 EAP-FAST 身份验证协议用于 High Sierra、Mojave 或 Catalina MAC OSX 设备，可能会看到“EAP-FAST 加密绑定验证失败” (EAP-FAST cryptobinding verification failed) 消息。我们建议您配置“允许的协议” (Allowed Protocols) 页面中的“首选 EAP 协议” (Preferred EAP Protocol) 字段，以使这些 MAC OSX 设备使用 PEAP 或 EAP-TLS 而非 EAP-FAST。

## 配置 EAP-FAST 设置

### 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** 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > EAP-FAST > EAP Fast 设置 (EAP Fast Settings)。

**步骤 2** 按需输入详细信息，定义 EAP-FAST 协议。

**步骤 3** 如果要调用以前生成的所有主密钥和 PAC，请点击撤销 (Revoke)。

**步骤 4** 点击 **Save**，保存 EAP-FAST 设置。

## 为 EAP-FAST 生成 PAC

您可以使用思科 ISE 中的 Generate PAC 选项为 EAP-FAST 协议生成隧道或计算机 PAC。

### 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** 选择管理 (Administration) > 系统 (System) > 设置 (Settings)。

**步骤 2** 从左侧的 Settings 导航窗格中，点击 **Protocols**。

**步骤 3** 选择 **EAP-FAST > 生成 PAC (Generate PAC)**。

**步骤 4** 根据需要输入用于为 EAP-FAST 协议生成计算机 PAC 的详细信息。

**步骤 5** 点击 **Generate PAC**。

## EAP-FAST 设置

表 90: 配置 EAP-FAST 设置

字段名称	使用指南
<b>Authority Identity Info Description</b>	输入用于说明向客户端发送凭证的思科 ISE 节点的用户友好字符串。客户端可以在类型、长度和价值 (TLV) 的受保护访问凭证 (PAC) 信息中发现此字符串。默认值为 Identity Services Engine。
<b>Master Key Generation Period</b>	指定主键生成期（以秒、分钟、小时、天或周为单位）。值必须是范围在 1 至 2147040000 秒内的正整数。默认值为 604800 秒，相当于一周。
<b>Revoke all master keys and PACs</b>	点击“撤销” (Revoke) 可撤销所有主键和 PAC。
<b>Enable PAC-less Session Resume</b>	如果您要在没有 PAC 文件的情况下使用 EAP-FAST，请选中此复选框。
<b>PAC-less Session Timeout</b>	指定无 PAC 会话恢复超时的时间（以秒为单位）。默认值为 7200 秒。

### 相关主题

[用于身份验证的协议设置](#)，第 549 页

[将 EAP-FAST 用作身份验证协议的指南](#)，第 549 页

[EAP-FAST 的优势](#)，第 576 页

[配置 EAP-FAST 设置](#)，第 550 页

## PAC 设置

下表介绍“生成 PAC” (Generate PAC) 窗口上的字段，您可以使用此窗口为 EAP-FAST 身份验证配置受保护的访问凭证。此页面的导航路径为：要查看此处窗口，请单击菜单图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **协议 (Protocols)** > **EAP-FAST** > **生成 (Generate PAC)**。

表 91: 为 EAP-FAST 设置生成 PAC

字段名称	使用指南
<b>Tunnel PAC</b>	点击此单选按钮生成隧道 PAC。
<b>Machine PAC</b>	点击此单选按钮生成设备 PAC。
<b>Trustsec PAC</b>	点击此单选按钮生成 Trustsec PAC。

字段名称	使用指南
<b>Identity</b>	<p>(针对 Tunnel 和 Machine PAC) 指定 EAP-FAST 协议显示为“内部用户名”的用户名或设备名称。如果身份字符串与该用户名不匹配，则身份验证失败。</p> <p>这是主机定义在自适应安全设备 (ASA) 上定义的主机名。身份字符串必须与 ASA 主机名匹配，否则 ASA 无法导入生成的 PAC 文件。</p> <p>如果生成的是 Trustsec PAC，则 Identity 字段指定 Trustsec 网络设备的设备 ID 并且由 EAP-FAST 协议提供发起方 ID。如果在此处输入的 Identity 字符串与该设备 ID 不匹配，则身份验证失败。</p>
<b>PAC Time to Live</b>	<p>(对于隧道和设备 PAC) 请以秒为单位输入 PAC 的到期时间。默认值为 604800 秒，相当于一周。该值必须是介于 1 和 157680000 秒之间的正整数。对于 Trustsec PAC，请以天、周、月或年为单位输入一个值。默认情况下，该值为一年。最小值为一天，最大值为 10 年。</p>
<b>Encryption Key</b>	<p>输入加密密钥。密钥的长度必须介于 8 和 256 个字符之间。密钥可以包含大写或小写字母或数字，或字母数字字符的组合。</p>
<b>Expiration Data</b>	<p>(仅对于 Trustsec PAC) 到期日期根据 PAC Time to Live 计算。</p>

#### 相关主题

[用于身份验证的协议设置](#)，第 549 页

[将 EAP-FAST 用作身份验证协议的指南](#)，第 549 页

[为 EAP-FAST 生成 PAC](#)，第 550 页

## 配置 EAP-TLS 设置

### 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** 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > EAP-TLS。

**步骤 2** 根据需要输入详细信息可定义 EAP-TLS 协议。

**步骤 3** 点击 **Save** 保存 EAP-TLS 设置。



## EAP-TLS 设置

### 相关主题

- [用于身份验证的协议设置](#)，第 549 页
- [配置 EAP-TLS 设置](#)，第 552 页

## 配置 PEAP 设置

### 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** 选择管理 (**Administration**) > 系统 (**System**) > 设置 (**Settings**)。

**步骤 2** 从左侧的 Settings 导航窗格中，点击 **Protocols**。

**步骤 3** 选择 **PEAP**。

**步骤 4** 根据需要，输入详细信息以定义 PEAP 协议。

**步骤 5** 点击 **Save** 以保存 PEAP 设置。

---

## PEAP 设置

### 相关主题

- [用于身份验证的协议设置](#)，第 549 页
- [配置 PEAP 设置](#)，第 553 页
- [使用 PEAP 的优势](#)，第 574 页
- [PEAP 协议支持的请求方](#)，第 575 页
- [PEAP 协议流程](#)，第 575 页

## 配置 RADIUS 设置

您可以配置 RADIUS 设置，以检测未能通过身份验证的客户端，并禁止重复报告成功的身份验证。

---

**步骤 1** 选择管理 (**Administration**) > 系统 (**System**) > 设置 (**Settings**)。

**步骤 2** 在 Settings 导航窗格中，点击 **Protocols**。

**步骤 3** 选择 **RADIUS**。

**步骤 4** 输入定义 RADIUS 设置所需的详细信息。

**步骤 5** 点击 **保存**，保存设置。

---

## RADIUS 设置

当您启用异常客户端抑制并且在配置的检测间隔内终端身份验证失败两次时，思科 ISE 会将请求方标识为配置错误并抑制由于相同失败原因导致的失败身份验证。您可以通过在 **Live Authentications** 页面点击 **Misconfigured Supplicant Counter** 链接，找到关于此抑制功能的更多详细信息。如果从受抑制的终端成功完成身份验证，则会清除此抑制，而且会降低 **Live Authentications** 页面上 **Misconfigured Supplicant Counter** 的值。此外，如果在六小时的时间内受抑制终端没有任何身份验证活动，系统会自动清除抑制。

思科 ISE 允许通过启用 **Reject Requests After Detection** 选项，实施强抑制。如果您选中 **Reject Requests After Detection** 复选框，并且终端身份验证因同一失败原因失败五次，思科 ISE 就会激活强抑制。所有后续的身份验证，无论成功与否，都会被抑制，所以不会进行身份验证。经过所配置的 **Request Rejection Interval** 间隔或终端无身份验证活动达六小时后，系统会清除“强”抑制。



**注释** 如果配置 RADIUS 失败抑制，则在配置 RADIUS 日志抑制后，仍可能会收到错误“5440 终端已放弃会话并启动了新会话” (5440 Endpoint Abandoned EAP Session and started a new one)。有关详细信息，请参阅以下思科 ISE 社区帖子：

<https://community.cisco.com/t5/network-access-control/authentication-failed-quot-5440-endpoint-abandoned-eap-session/td-p/3191944>

表 92: RADIUS 设置

字段名称	使用指南
<b>Suppress Anomalous Clients</b>	选中此复选框以检查身份验证重复失败的客户端。每经过一个 <b>Reporting Interval</b> 间隔，系统会报告失败身份验证摘要。
<b>Detection Interval</b>	以分钟为单位输入检测客户端的时间间隔。
<b>Reporting Interval</b>	以分钟为单位输入报告失败身份验证的时间间隔。
<b>Reject Requests After Detection</b>	选中此复选框以拒绝来自被识别为异常或配置错误的客户端的请求。在请求拒绝间隔期间，系统会拒绝来自异常客户端的请求。
<b>Request Rejection Interval</b>	以分钟为单位输入拒绝请求的时间间隔。此选项仅在已选择在检测后拒绝请求 ( <b>Reject Requests After Detection</b> ) 复选框时可用。
<b>Suppress Repeated Successful Authentications</b>	选中此复选框以防重复报告前 24 小时内身份验证场景、网络设备和授权方面没有变更的成功身份验证。
<b>Accounting Suppression Interval</b>	以秒为单位输入抑制记帐请求报告的时间间隔。

字段名称	使用指南
<b>Long Processing Step Threshold Interval</b>	以毫秒为单位输入时间间隔。身份验证详细信息报告中会显示这些步骤。如果单个步骤的执行超出指定阈值，则在身份验证详细报告中会突出显示此步骤。
<b>RADIUS UDP 端口</b>	

#### 相关主题

[用于身份验证的协议设置](#)，第 549 页

[思科 ISE 中的 RADIUS 协议支持](#)，第 558 页

[配置 RADIUS 设置](#)，第 553 页

## 配置安全设置

执行以下程序以配置安全设置。

**步骤 1** 选择管理 (**Administration**) > 系统 (**System**) > 设置 (**Settings**) > 协议 (**Protocols**) > 安全设置 (**Security Settings**)。

**步骤 2** 在 安全设置 窗口中，选择所需的选项：

• **Allow TLS 1.0 (允许 TLS 1.0)**：在以下工作流程中允许 TLS 1.0 用于与以下传统对等体通信：

- 思科 ISE 配置为 EAP 服务器
- 思科 ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
- 思科 ISE 配置为安全 TCP 系统日志客户端
- 思科 ISE 配置为安全 LDAP 客户端
- 思科 ISE 配置为 ERS 服务器

还允许使用 TLS 1.0 与以下思科 ISE 组件通信：

- 所有门户
- 证书颁发机构
- MDM 客户端
- pxGrid
- PassiveID 代理

**注释** 我们建议客户端和服务器协商使用更高版本的 TLS，以增强安全性。

• **Allow TLS 1.1 (允许 TLS 1.1)**：在以下工作流程中允许 TLS 1.1 用于与以下传统对等体通信：

- 思科 ISE 配置为 EAP 服务器

- 思科 ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
- 思科 ISE 配置为安全 TCP 系统日志客户端
- 思科 ISE 配置为安全 LDAP 客户端
- 思科 ISE 配置为 ERS 服务器

还允许使用 TLS 1.1 与以下思科 ISE 组件通信：

- 所有门户
- 证书颁发机构
- 外部 RESTful 服务 (ERS)
- MDM 客户端
- pxGrid

注释 我们建议客户端和服务器协商使用更高版本的 TLS，以增强安全性。

- **允许 SHA-1 密码：** 在以下工作流程中允许 SHA-1 密码用于与对等体通信：

- 思科 ISE 配置为 EAP 服务器
- 思科 ISE 配置为 RADIUS DTLS 服务器
- 思科 ISE 配置为 RADIUS DTLS 客户端
- 思科 ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
- 思科 ISE 配置为安全系统日志客户端
- 思科 ISE 配置为安全 LDAP 客户端

还允许使用 SHA-1 密码与以下思科 ISE 组件通信：

- 管理员访问 UI
- 所有门户
- ERS
- pxGrid
- 管理员访问权限：443
- 思科 ISE 门户：9002、8443、8444、8445、8449
- ERS：9060、9061、9063
- pxGrid：8910

注释 默认情况下该选项处于禁用状态。

启用或禁用 **允许 SHA-1 密码** 选项后，必须重新启动部署中的所有节点。如果重新启动不成功，则不会应用配置更改。在这种情况下，必须使用以下命令手动重新启动所有节点：

**application stop ise** 和 **application start ise**。

注释 我们建议使用 SHA-256 或 SHA-384 密码以增强安全性。

- **允许 ECDHE-RSA 密码 (Allow ECDHE-RSA Ciphers):** 在以下工作流程中允许 ECDHE-RSA 密码用于与对等体通信：
    - 思科 ISE 配置为 EAP 服务器
    - 思科 ISE 配置为 RADIUS DTLS 服务器
    - 思科 ISE 配置为 RADIUS DTLS 客户端
    - 思科 ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
    - 思科 ISE 配置为安全系统日志客户端
    - 思科 ISE 配置为安全 LDAP 客户端
  - **允许 3DES 密码 (Allow 3DES Ciphers):** 在以下工作流程中允许 3DES 密码用于与对等体通信：
    - 思科 ISE 配置为 EAP 服务器
    - 思科 ISE 配置为 RADIUS DTLS 服务器
    - 思科 ISE 配置为 RADIUS DTLS 客户端
    - 思科 ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
    - 思科 ISE 配置为安全系统日志客户端
    - 思科 ISE 配置为安全 LDAP 客户端
  - **接受证书而不验证目的 (Accept Certificates without Validating Purpose):** 当思科 ISE 作为 EAP 或 RADIUS DTLS 服务器时，将接受客户端证书而无需检查是否：
    - “密钥使用” (Key Usage) 扩展包含 ECDHE-ECDSA 密码的 keyAgreement 或其他密码的 keyEncipherment。
    - “扩展密钥使用” (Extended Key Usage) 属性值为 ClientAuth
- 禁用此选项后，思科 ISE 将验证所有客户端证书的用途。只有满足以下条件之一，证书才会被视为有效：
- 如果“扩展密钥使用” (Extended Key Usage) 属性没有值：
    - 如果 cipherGroup 是 ECDHE-ECDSA，则密钥使用扩展必须包含 KeyAgreement 值。
    - 如果 cipherGroup 不是 ECDHE-ECDSA，则 Key Usage 扩展必须包含 keyEncipherment 和 digitalSignature 值。
  - 如果“扩展密钥使用” (Extended Key Usage) 属性值为 ClientAuth：
    - 如果 cipherGroup 是 ECDHE-ECDSA，则密钥使用扩展必须包含 KeyAgreement 值。

- 如果 cipherGroup 不是 ECDHE-ECDSA，则 Key Usage 扩展必须包含 keyEncipherment 和 digitalSignature 值。

如果不满足上述条件，证书验证将失败。

- **允许 DSS 密码用于作为客户端的 ISE：**当思科 ISE 充当客户端时，在以下工作流程中允许使用 DSS 密码与服务器通信：
  - 思科 ISE 配置为 RADIUS DTLS 客户端
  - 思科 ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - 思科 ISE 配置为安全系统日志客户端
  - 思科 ISE 配置为安全 LDAP 客户端
- **允许传统的不安全 TLS 重新协商用于作为客户端的 ISE (Allow Legacy Unsafe TLS Renegotiation for ISE as a Client)：**在以下工作流程中允许与不支持安全 TLS 重新协商的传统 TLS 服务器通信：
  - 思科 ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
  - 思科 ISE 配置为安全系统日志客户端
  - 思科 ISE 配置为安全 LDAP 客户端

步骤 3 点击保存 (Save)。

---

## 思科 ISE 中的 RADIUS 协议支持

RADIUS 是一个客户端/服务器协议，通过该协议，远程访问服务器与中央服务器发生通信，对拨入用户进行身份验证，并对拨入用户所请求的系统或服务的访问进行授权。您可以在所有远程服务器可共享的中央数据库中使用 RADIUS 维护用户配置文件。此协议提供更高的安全性，并且您可以使用它来设置策略以应用于单个管理的网络点。

RADIUS 还可以在思科 ISE 中用作 RADIUS 客户端以代理远程 RADIUS 服务器的请求，并且它还可以在活动会话期间提供授权更改 (CoA)。

思科 ISE 依据 RFC 2865 对 RADIUS 协议流程提供支持，并广泛支持所有 RADIUS 常规属性（如 RFC 2865 及其扩展中所描述）。思科 ISE 支持仅解析在思科 ISE 字典中定义的供应商特定属性。

RADIUS 接口支持下述在 RFC 2865 中定义的属性数据类型：

- 文本（Unicode 转换格式 [UTF]）
- 字符串（二进制）
- 地址 (IP)
- 整数

- 时间

## 允许的协议

下表介绍允许的协议 (Allowed Protocols) 窗口中的字段，您可以使用此窗口配置身份验证过程中要使用的协议。导航路径为：**策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 身份验证 (Authentication) > 允许协议 (Allowed Protocols)**。

表 93: 允许的协议

字段名称	使用指南
允许的协议 > 身份验证旁路	
流程主机查找	<p>如果希望思科 ISE 处理主机查询请求，请选中此复选框。当 RADIUS 服务类型等于 10 (呼叫-检查) 且用户名等于呼叫 - 站 - ID 时，对于 PAP/CHAP 协议，会对主机查询请求进行处理。当服务类型等于 1 (框到的) 且用户名等于呼叫 - 站 - ID 时，对于 EAP-MD5 协议，会对主机查询请求进行处理。如果您希望思科 ISE 忽略主机查找请求并使用系统用户名属性的原始值进行身份验证，请取消选中此复选框。当取消选中时，系统会根据协议 (例如 PAP) 进行消息处理。</p> <p>注释          禁用此选项可能会导致现有 MAB 身份验证失败。</p>
允许的协议 > 身份验证协议	
Allow PAP/ASCII	此选项可启用 PAP/ASCII。PAP 使用明文密码 (即，未加密的密码)，并且是最不安全的身份验证协议。
“允许 CHAP” (Allow CHAP)	此选项可启用 CHAP 身份验证。CHAP 使用带有密码加密的质询-响应机制。CHAP 不适用于 Microsoft Active Directory。
“允许 MS-CHAPv1” (Allow MS-CHAPv1)	选中此复选框可启用 MS-CHAPv1。
“允许 MS-CHAPv2” (Allow MS-CHAPv2)	选中此复选框可启用 MS-CHAPv2。
“允许 EAP-MD5” (Allow EAP-MD5)	选中此复选框可启用基于 EAP 的 MD5 密码散列身份验证。

字段名称	使用指南
<p>“允许 EAP-TLS” (Allow EAP-TLS)</p>	<p>选中此复选框可启用 EAP-TLS 身份验证协议并配置 EAP-TLS 设置。您可以指定思科 ISE 将如何按照来自最终用户客户端的 EAP 身份响应中的说明对用户身份进行验证。用户身份根据最终用户客户端提供的证书中的信息进行验证。在思科 ISE 与最终用户客户端之间建立 EAP-TLS 隧道后，会发生此比较。</p> <p><b>注释</b> EAP-TLS 是基于证书的身份验证协议。仅在您已完成配置证书的所需步骤后，才能发生 EAP-TLS 身份验证。</p> <ul style="list-style-type: none"> <li>• 在授权策略中允许过期证书的身份验证以允许证书续订 (<b>Allow authentication of expired certificates to allow certificate renewal in Authorization Policy</b>) 复选框：如果要允许用户续订证书，请选中此复选框。如果选中此复选框，请确保配置相应的授权策略规则，以检查在进一步处理请求之前是否已更新证书。</li> </ul>
<p>“允许 LEAP” (Allow LEAP)</p>	<p>选中此复选框可启用轻量级可扩展身份验证协议 (LEAP) 身份验证。</p>



字段名称	使用指南
<p>“允许 PEAP” (Allow PEAP)</p>	<p>选中此复选框可启用 PEAP 身份验证协议和 PEAP 设置。默认内部方法为 MS-CHAPv2。</p> <p>当选中“允许 PEAP” (Allow PEAP) 复选框时，您可以配置以下 PEAP 内部方法：</p> <ul style="list-style-type: none"> <li>• <b>允许 EAP-MS-CHAPv2 (Allow EAP-MS-CHAPv2)</b>：选中此复选框可使用 EAP-MS-CHAPv2 作为内部方法。 <ul style="list-style-type: none"> <li>• <b>允许密码更改 (Allow Password Change)</b>：选中此复选框可使思科 ISE 支持密码更改。</li> <li>• <b>重试尝试数 (Retry Attempts)</b>：指定思科 ISE 在显示登录失败之前请求用户凭证的次数。有效值为 0 至 3。</li> </ul> </li> <li>• <b>允许 EAP-GTC (Allow EAP-GTC)</b>：选中此复选框可使用 EAP-GTC 作为内部方法。 <ul style="list-style-type: none"> <li>• <b>允许密码更改 (Allow Password Change)</b>：选中此复选框可使思科 ISE 支持密码更改。</li> <li>• <b>重试尝试数 (Retry Attempts)</b>：指定思科 ISE 在显示登录失败之前请求用户凭证的次数。有效范围为 0 到 3。</li> </ul> </li> <li>• <b>允许 EAP-TLS (Allow EAP-TLS)</b>：选中此复选框可使用 EAP-TLS 作为内部方法。 如果要允许用户更新证书，请选中<b>允许过期证书的身份验证以允许身份验证策略中的证书更新 (Allow authentication of expired certificates to allow certificate renewal in Authorization Policy)</b>复选框。如果选中此复选框，请确保配置相应的授权策略规则，以检查在进一步处理请求之前是否已更新证书。</li> <li>• <b>仅对传统客户端允许 PEAPv0 (Allow PEAPv0 Only for Legacy Clients)</b>：选中此复选框可允许 PEAP 请求方使用 PEAPv0 进行协商。某些传统客户端不符合 PEAPv1 协议标准。要确保不丢弃此类 PEAP 对话，请选中此复选框。</li> </ul>

字段名称	使用指南
“允许 EAP-FAST” (Allow EAP-FAST)	

字段名称	使用指南
	<p>选中此复选框可启用 EAP-FAST 身份验证协议和 EAP-FAST 设置。EAP-FAST 协议可以在同一服务器上支持多个内部协议。默认内部方法为 MS-CHAPv2。</p> <p>当选中“允许 EAP-FAST” (Allow EAP-FAST) 复选框时，您可以将 EAP-FAST 配置为内部方法：</p> <ul style="list-style-type: none"> <li>• <b>“允许 EAP-MS-CHAPv2” (Allow EAP-MS-CHAPv2)</b> <ul style="list-style-type: none"> <li>• <b>允许密码更改 (Allow Password Change):</b> 选中此复选框可使思科 ISE 支持密码更改。</li> <li>• <b>重试尝试数 (Retry Attempts):</b> 指定思科 ISE 在显示登录失败之前请求用户凭证的次数。有效值为 0 至 3。</li> </ul> </li> <li>• <b>Allow EAP-GTC</b> <ul style="list-style-type: none"> <li><b>允许密码更改 (Allow Password Change):</b> 选中此复选框可使思科 ISE 支持密码更改。</li> <li><b>重试尝试数 (Retry Attempts):</b> 指定思科 ISE 在显示登录失败之前请求用户凭证的次数。有效值为 0 至 3。</li> </ul> </li> <li>• <b>使用 PAC (Use PACs):</b> 选中此选项可配置思科 ISE 以便为 EAP-FAST 客户端调配授权受保护访问凭证 (PAC)。系统显示其他 PAC 选项。</li> <li>• <b>不使用 PAC (Don't Use PACs):</b> 选择此选项可配置思科 ISE 以使用 EAP-FAST，而不发出或接受任何隧道或计算机 PAC。系统会忽略对 PAC 的所有请求，并且思科 ISE 会在没有 PAC 的情况下使用 Success-TLV 进行响应。 <ul style="list-style-type: none"> <li>当选择此选项时，您可以将思科 ISE 配置为执行计算机身份验证。</li> </ul> </li> <li>• <b>允许 EAP-TLS (Allow EAP-TLS):</b> 选中此复选框可使用 EAP-TLS 作为内部方法。 <ul style="list-style-type: none"> <li>如果要允许用户更新证书，请选中允许过期证书的身份验证以允许身份验证策略中的证书更新 (<b>Allow authentication of expired</b></li> </ul> </li> </ul>

字段名称	使用指南
	<p><b>certificates to allow certificate renewal in Authorization Policy</b>) 复选框。如果选中此复选框，请确保配置相应的授权策略规则，以检查在进一步处理请求之前是否已更新证书。</p> <ul style="list-style-type: none"> <li>• <b>启用 EAP 链接 (Enable EAP Chaining):</b> 选中此复选框可启用 EAP 链接。</li> </ul> <p>EAP 链接允许思科 ISE 将用户和计算机身份验证的结果相关联，并且使用 EAPChainingResult 属性应用相应的授权策略。</p> <p>EAP 链接要求请求方在客户端设备上支持 EAP 链接。选择请求方中的“用户和计算机身份验证”(User and Machine Authentication) 选项。</p> <p>当选择 EAP-FAST 协议（二者均处于基于 PAC 的模式和无 PAC 模式下）时，EAP 链接可用。</p> <p>对于基于 PAC 的身份验证，您可以使用用户授权 PAC 和/或计算机授权 PAC 跳过内部方法。</p> <p>对于基于证书的身份验证，如果您为 EAP-FAST 协议启用“接受客户端调配证书”(Accept Client Certificate for Provisioning) 选项（在允许的协议服务中），并且如果终端 (AnyConnect) 配置为在隧道内发送用户证书，则在隧道建立过程中，ISE 会使用证书对用户进行身份验证（跳过内部方法），而计算机身份验证会通过内部方法来完成。如果未配置这些选项，则 EAP-TLS 会作用于进行用户身份验证的内部方法。</p> <p>在您启用 EAP 链接后，使用 NetworkAccess:EapChainingResult 属性更新授权策略并添加条件，然后分配相应的权限。</p>
<b>Preferred EAP Protocol</b>	<p>选中此复选框可从以下任一选项中选择首选 EAP 协议：EAP-FAST、PEAP、LEAP、EAP-TLS、EAP-TTLS 和 EAP-MD5。如果没有指定首选协议，则默认情况下使用 EAP - TLS。</p>

字段名称	使用指南
允许 5G	选中此复选框以在思科 ISE 上启用思科私人 5G。  注释 在思科 ISE 中启用 5G 即服务 (5GaaS) 之前，您必须已在网络中部署思科专用 5G

#### 相关主题

[为网络访问定义允许的协议](#)，第 570 页

## PAC 选项

下表介绍了在允许协议服务列表 (**Allowed Protocols Services List**) 窗口中选择了“使用 PAC” (Use PACs) 后显示的字段。此页面的导航路径为：**策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **身份验证 (Authentication)** > **允许协议 (Allowed Protocols)**。

表 94: PAC 选项

字段名称	使用指南
使用 PAC (Use PAC)	

字段名称	使用指南
	<ul style="list-style-type: none"> <li>• “隧道 PAC 存活时间” (Tunnel PAC Time To Live): 存活时间 (TTL) 值限制 PAC 的生存期。指定生存期值和单位。默认值为 90 天。时间范围为 1 至 1825 天。</li> <li>• “当剩下 &lt;n%&gt; 的 PAC TTL 时主动进行 PAC 更新” (Proactive PAC Update When: &lt;n%&gt; of PAC TTL is Left): 更新值确保客户端拥有有效的 PAC。首次成功通过身份验证后, 但在 TTL 设置的到期时间前, 思科 ISE 启动更新。更新值是指 TTL 中的剩余时间百分比。默认为 90%。</li> <li>• “允许匿名带内 PAC 调配” (Allow Anonymous In-band PAC Provisioning): 选中此复选框, 使思科 ISE 与客户端建立安全的匿名 TLS 握手, 并使用 EAP-FAST 的零阶段和 EAP-MSCHAPv2, 通过 PAC 调配客户端。要启用匿名 PAC 调配, 必须选择这两种内部方法: EAP-MSCHAPv2 和 EAP-GTC。</li> <li>• “允许经验证的带内 PAC 调配” (Allow Authenticated In-band PAC Provisioning): 思科 ISE 使用 SSL 服务器侧身份验证, 在 EAP-FAST 的零阶段期间通过 PAC 调配客户端。此选项比匿名调配的安全性更高, 但要求在思科 ISE 上安装服务器证书和受信任的根 CA。  如果您选中此选项, 可将思科 ISE 配置为在成功对 PAC 调配进行身份验证后将 Access-Accept 消息传送至客户端。 <ul style="list-style-type: none"> <li>• “服务器在对调配进行身份验证后返回 Access-Accept 消息” (Server Returns Access Accept After Authenticated Provisioning): 如果希望思科 ISE 在成功对 PAC 调配进行身份验证后传送 Access-Accept 消息, 请选中此复选框。</li> </ul> </li> <li>• “允许机器身份验证” (Allow Machine Authentication): 选中此复选框, 使思科 ISE 使用计算机 PAC 调配最终用户客户端, 并执行计算机身份验证 (适用于没有计算机凭证的最终用户客户端)。可以通过请求 (频内) 或管理员 (频外) 将计算机 PAC 调配至</li> </ul>

字段名称	使用指南
	<p>客户端。当思科 ISE 收到最终用户客户端发送的有效计算机 PAC 时，会从 PAC 提取计算机身份详细信息，并在思科 ISE 外部身份源中进行验证。思科 ISE 只支持 Active Directory 作为计算机身份验证的外部身份源。正确验证这些详细信息后，不会再执行进一步的身份验证。</p> <p>如果您选中此选项，可以输入接受使用计算机 PAC 的时间值。当思科 ISE 收到过期的计算机 PAC 时，会自动使用新的计算机 PAC 重新调配最终用户客户端（无需等待最终用户客户端发送新的计算机 PAC 请求）。</p> <ul style="list-style-type: none"> <li>“启用无状态会话恢复” (Enable Stateless Session Resume): 选中此复选框后，思科 ISE 会为 EAP-FAST 客户端调配授权 PAC，并跳过 EAP-FAST 的第二阶段（默认为启用）。</li> </ul> <p>在下列情况下取消选中此复选框：</p> <ul style="list-style-type: none"> <li>如果您不希望思科 ISE 为 EAP-FAST 客户端调配授权 PAC</li> <li>要始终执行 EAP-FAST 的第二阶段</li> </ul> <p>如果您选中此选项，可以输入用户授权 PAC 的授权时间段。在此时间段后，PAC 过期。当思科 ISE 收到过期的授权 PAC 时，会执行执行 EAP-FAST 身份验证的第二阶段。</p>

#### 相关主题

[OOB TrustSec PAC](#)，第 584 页

[为 EAP-FAST 生成 PAC](#)，第 550 页

## 将思科 ISE 用作 RADIUS 代理服务器

思科 ISE 可用作 RADIUS 服务器和 RADIUS 代理服务器。用作代理服务器时，思科 ISE 从网络接入服务器 (NAS) 接受身份验证和记帐请求并将这些请求转发至外部 RADIUS 服务器。思科 ISE 接受请求的结果并将结果返回至 NAS。

思科 ISE 可以同时用作多个外部 RADIUS 服务器的代理服务器。您可以在 RADIUS 服务器序列中使用此处配置的外部 RADIUS 服务器。External RADIUS Server 页面会列出您已在思科 ISE 中定义的所有外部 RADIUS 服务器。您可以使用过滤器选项，根据名称或说明或同时根据名称和说明搜索具体



RADIUS 服务器。在简单身份验证策略和基于规则的身份验证策略中，您都可以使用 RADIUS 服务器序列来代理对 RADIUS 服务器的请求。

RADIUS 服务器序列从 RADIUS-Username 属性删除域名以进行 RADIUS 身份验证。这种域名删除操作不适用于使用 EAP-Identity 属性的 EAP 身份验证。RADIUS 代理服务器从 RADIUS-Username 属性获取用户名并从您配置 RADIUS 服务器序列时指定的字符删除用户名。对于 EAP 身份验证，RADIUS 代理服务器从 EAP-Identity 属性获取用户名。只有在 EAP-Identity 和 RADIUS-Username 值相同时，使用 RADIUS 服务器序列的 EAP 身份验证才会成功。

## 配置外部 RADIUS 服务器

您必须在思科 ISE 中配置外部 RADIUS 服务器，使其向外部 RADIUS 服务器转发请求。您可以定义超时时间和连接尝试的次数。

### 开始之前

- 您无法单独使用您在本节中创建的外部 RADIUS 服务器，而必须创建 RADIUS 服务器序列并将其配置为使用您在本节创建的 RADIUS 服务器。然后，您就可以在身份验证策略中使用 RADIUS 服务器序列。
- 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** 选择 **管理 (Administration) > 网络资源 (Network Resources) > 外部 RADIUS 服务器 (External RADIUS Servers)**。

系统将显示 RADIUS Servers 页面，其中包含已在思科 ISE 中定义的外部 RADIUS 服务器的列表。

**步骤 2** 点击 **Add** 以添加外部 RADIUS 服务器。

**步骤 3** 根据要求输入相应值。

**步骤 4** 点击 **Submit** 以保存外部 RADIUS 服务器配置。

---

## 定义 RADIUS 服务器序列

思科 ISE 中的 RADIUS 服务器序列允许您将 NAD 发送的请求代理到外部 RADIUS 服务器，此外部 RADIUS 服务器会处理该请求并将结果返回至思科 ISE，随后思科 ISE 会将响应转发至 NAD。

RADIUS Server Sequences 页面列出您在思科 ISE 中定义的所有 RADIUS 服务器序列。在此页面上，您可以创建、编辑或复制 RADIUS 服务器序列。

### 开始之前

- 在开始此程序之前，您应该基本了解代理服务，并且必须成功完成相关链接的第一个条目中的任务。
- 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** 选择 **管理 (Administration) > 网络资源 (Network Resources) > RADIUS 服务器序列 (RADIUS Server Sequences)**。

**步骤 2** 点击 **Add**。

**步骤 3** 根据要求输入相应值。

**步骤 4** 点击 **Submit** 以保存要用于策略的 RADIUS 服务器序列。

---

## 网络访问服务

网络访问服务包含请求的身份验证策略条件。可以为不同的使用案例创建单独的网络访问服务，例如，有线 802.1X、有线 MAB 等。要创建网络访问服务，请配置允许的协议或服务器序列。

### 为网络访问定义允许的协议

允许的协议定义了思科 ISE 可以用于与请求访问网络资源的设备通信的协议集。允许的协议访问服务是一个您应在配置身份验证策略前创建的独立实体。允许的协议访问服务是一个包含特定使用案例的选定协议的对象。

**Allowed Protocols Services** 页面列出了您创建的所有允许的协议服务。思科 ISE 中预定义了默认网络访问服务。

#### 开始之前

在开始此程序之前，您应该具备用于身份验证的协议服务的基本知识。

- 请查看本章节中的“思科 ISE 身份验证策略”部分，以了解身份验证类型和各种数据库支持的协议。
- 查看“PAC 选项”，了解每种协议服务的功能和选项，以便您可以做出适合您的网络的选择。
- 确保您已定义全局协议设置。

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** 选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 身份验证 (Authentication) > 允许的协议 (Allowed Protocols)**。

如果思科 ISE 设置为在 FIPS 模式下运行，则某些协议会在默认情况下处于禁用状态且无法配置。

**步骤 2** 点击 **Add**。

**步骤 3** 输入所需信息。

**步骤 4** 为您的网络选择适当的身份验证协议和选项。

**步骤 5** 如果您选择使用 PAC，请进行适当的选择。

要启用 **Anonymous PAC Provisioning**，您必须同时选择以下两个内部方法：**EAP-MSCHAPv2** 和 **可扩展身份验证协议-通用令牌卡 (EAP-GTC)**。另请注意，思科 ISE 只支持 **Active Directory** 作为计算机身份验证的外部身份源。

**步骤 6** 点击 **Submit** 保存允许的协议服务。

允许的协议服务在简单和基于规则的身份验证策略页面中显示为独立对象。您可以将此对象用于不同的规则。

您现在可以创建简单或基于规则的身份验证策略。

如果禁用 EAP-MSCHAP 作为内部方法并为 PEAP 或 EAP-FAST 启用 EAP-GTC 和 EAP-TLS 内部方法，则 ISE 会在内部方法协商过程中启动 EAP-GTC 内部方法。在第一个 EAP-GTC 消息发送到客户端之前，ISE 会执行身份选择策略以从身份库获取 GTC 密码。在执行此策略的过程中，EAP 身份验证等于 EAP-GTC。如果 EAP-GTC 内部方法被客户端拒绝且 EAP-TLS 已经过协商，则系统不会再次执行身份库策略。如果身份库策略基于 EAP 身份验证属性，则它可能会出现意外结果，因为实时 EAP 身份验证基于 EAP-TLS，但设置于身份策略评估之后。

## 用户的网络接入

对网络接入，主机会连接至网络设备并且请求使用网络资源。网络设备识别新连接的主机，并且将 RADIUS 协议用作传输机制，向思科 ISE 请求对用户进行身份验证和授权。

思科 ISE 根据基于 RADIUS 协议传输的协议支持网络接入流程。

### 不使用 EAP 的基于 RADIUS 的协议

不包含 EAP 的基于 RADIUS 的协议包含以下协议：

- 密码身份验证协议 (PAP)
- CHAP
- Microsoft 质询握手身份验证协议版本 1 (MS-CHAPv1)
- MS-CHAP 版本 2 (MS-CHAPv2)

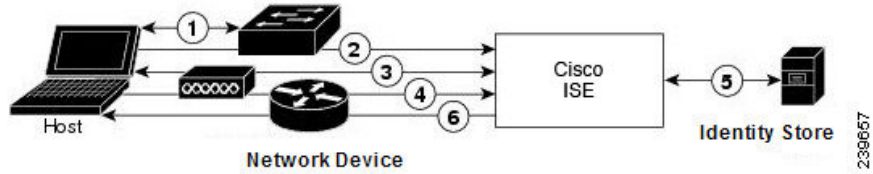
### 基于 RADIUS 的非 EAP 身份验证流程

本节介绍不使用 EAP 的基于 RADIUS 的身份验证。使用 PAP 身份验证的基于 RADIUS 的流程按以下程序进行：

1. 主机连接至网络设备。
2. 网络设备向思科 ISE 发送包含适用于所用具体协议（PAP、CHAP、MS-CHAPv1 或 MS-CHAPv2）的 RADIUS 属性的 RADIUS 请求。
3. 思科 ISE 使用身份存储区验证用户凭证。
4. 思科 ISE 向网络设备发送 RADIUS 响应（Access-Accept 或 Access-Reject），然后网络设备将应用此响应决策。

下图显示不使用 EAP 的基于 RADIUS 的身份验证。

图 31: 不使用 EAP 的基于 RADIUS 的身份验证



思科 ISE 支持的非 EAP 协议如下：

### 密码身份验证协议

PAP 使用双向握手为用户提供建立其身份的简单方法。PAP 密码使用共享密钥加密，是最简单的身份验证协议。PAP 不是强大的身份验证方法，因为其几乎无法抵御反复试错攻击。

### 思科 ISE 中基于 RADIUS 的 PAP 身份验证

思科 ISE 根据身份存储区检查用户名和密码对，直到其最终确认身份验证或终止连接。

您可以同时将不同安全级别应用于思科 ISE 以满足不同要求。PAP 使用二次握手过程。如果身份验证成功，思科 ISE 返回确认信息；否则，思科 ISE 将停止连接或向发起方提供第二次机会。

发起方完全控制尝试的频率和计时。因此，可以使用更强的身份验证方法的任意服务器都可以在 PAP 之前主动协商该方法。RFC 1334 定义 PAP。

思科 ISE 支持基于 RADIUS UserPassword 属性的标准 RADIUS PAP 身份验证。RADIUS PAP 身份验证与所有身份存储区都兼容。

RADIUS PAP 身份验证流程包括记录成功和失败的尝试。

### 质询握手身份验证协议

CHAP 使用质询响应机制，其中会对响应进行单向加密。CHAP 使思科 ISE 可以从最安全的加密机制向下协商到最不安全的加密机制，并且会保护流程中传输的密码。CHAP 密码可重复使用。如果使用思科 ISE 内部数据库进行身份验证，您可以使用 PAP 或 CHAP。CHAP 不适用于 Microsoft 用户数据库。与 RADIUS PAP 相比，CHAP 可在从最终用户客户端到 AAA 客户端的通信期间为密码加密实现更高的安全性。

思科 ISE 支持基于 RADIUS ChapPassword 属性的标准 RADIUS PAP 身份验证。思科 ISE 仅支持使用内部身份库进行 RADIUS CHAP 身份验证。

### Microsoft 质询握手身份验证协议版本 1

思科 ISE 支持 RADIUS MS-CHAPv1 身份验证和更改密码功能。RADIUS MS-CHAPv1 包含两个版本的更改密码功能：Change-Password-V1 和 Change-Password-V2。思科 ISE 不支持基于 RADIUS MS-CHAP-CPW-1 属性的 Change-Password-V1，仅支持基于 MS-CHAP-CPW-2 属性的 Change-Password-V2。以下身份源支持 RADIUS MS-CHAPv1 身份验证和更改密码功能：

- 内部身份库
- Microsoft Active Directory 身份库

## Microsoft 质询握手身份验证协议版本 2

RADIUS MS - CHAPv2 身份验证和更改密码功能受以下身份来源支持：

- 内部身份库
- Microsoft Active Directory 身份库

## 基于 RADIUS 的 EAP 协议

EAP 提供了可扩展的框架，支持各种身份验证类型。本节介绍思科 ISE 支持的 EAP 方法，包含下列主题：

### 简单的 EAP 方法

- EAP 消息摘要 5
- 轻型 EAP

### 使用思科 ISE 服务器证书进行身份验证的 EAP 方法

- PEAP/EAP-MS-CHAPv2
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

除了上面列出的方法，还有使用证书进行服务器和客户端身份验证的 EAP 方法。

## 基于 RADIUS 的 EAP 身份验证流程

只要身份验证流程中涉及 EAP，则开始此流程之前都要执行 EAP 协商以确定应该使用哪个具体的 EAP 方法（以及在适当的情况下使用内部方法）。基于 EAP 的身份验证按照以下程序进行：

1. 主机连接至网络设备。
2. 网络设备向主机发送 EAP 请求。
3. 主机向网络设备回复 EAP 响应。
4. 网络设备将其从主机接收的 EAP 响应封装入 RADIUS 访问请求（使用 EAP-Message RADIUS 属性）并将此 RADIUS 访问请求发送至思科 ISE。
5. 思科 ISE 从此 RADIUS 数据包提取 EAP 响应，并且创建新 EAP 请求，将其封装入 RADIUS 访问质询（也是使用 EAP-Message RADIUS 属性），然后将其发送至网络设备。
6. 网络设备提取 EAP 请求并将其发送至主机。

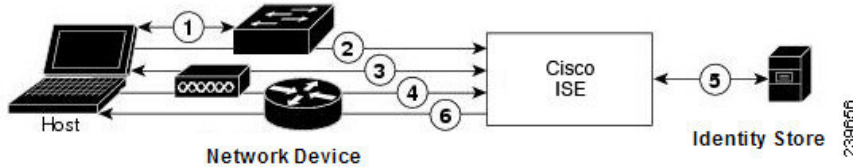
这样，主机和思科 ISE 就间接地交换 EAP 消息（通过 RADIUS 传输并穿过网络设备）。以此方式交换的首批 EAP 消息会协商以后用于执行身份验证的具体 EAP 方法。

之后交换的 EAP 消息就用于传输执行实际身份验证所需的数据。如果所协商的具体 EAP 身份验证方法需要，思科 ISE 会使用身份库来验证用户凭证。

思科 ISE 确定身份验证成功还是失败之后，会向网络设备（而且最终也向主机）发送封装入 RADIUS Access-Accept 或 Access-Reject 消息的 EAP-Success 或 EAP-Failure 消息。

下图显示使用 EAP 的基于 RADIUS 的身份验证。

图 32: 使用 EAP 的基于 RADIUS 的身份验证



### 可扩展身份验证协议-消息摘要 5

可扩展身份验证协议-消息摘要 5 (EAP - MD5) 提供单向客户端身份验证。服务器向客户端发送随机质询。客户端在响应中通过使用 MD5 加密质询及密码证明其身份。由于人为截取可看到质询和响应，所以在开放式媒体上使用时，EAP-MD5 容易遭受字典攻击。由于不发生服务器验证，所以也很容易遭受欺骗。思科 ISE 支持思科 ISE 内部身份库的 EAP-MD5 身份验证。在使用 EAP-MD5 协议时，还支持主机查找。

### 轻型可扩展身份验证协议

目前，思科 ISE 仅将轻型可扩展身份验证协议 (LEAP) 用于思科 Aironet 无线网络。如果不启用此选项，配置为执行 LEAP 身份验证的思科 Aironet 最终用户客户端就无法访问网络。如果所有思科 Aironet 最终用户客户端都使用不同的身份验证协议（例如，可扩展身份验证协议-传输层安全 [EAP-TLS]），我们建议您禁用此选项。



**注释** 如果用户使用 *Network Devices* 部分定义的 AAA 客户端作为 RADIUS（思科 Aironet）设备，则必须启用 LEAP、EAP-TLS 或同时启用这两项；否则思科 Aironet 用户将无法进行身份验证。

### 受保护的可扩展身份验证协议

受保护的可扩展身份验证协议 (PEAP) 提供相互身份验证，确保易受攻击的用户凭证的机密性和完整性，保护其自身抵御被动（窃听）和主动（中间人）攻击，以及安全地生成加密密钥材料。PEAP 与 IEEE 802.1X 标准和 RADIUS 协议兼容。思科 ISE 使用可扩展身份验证协议-Microsoft 质询握手身份验证协议 (EAP-MS-CHAP)、可扩展身份验证协议-通用令牌卡 (EAP-GTC) 和 EAP-TLS 内部方法支持 PEAP 版本 0 (PEAPv0) 和 PEAP 版本 1 (PEAPv1)。思科安全服务客户端 (SSC) 请求方支持思科 ISE 支持的所有 PEAPv1 内部方法。

### 使用 PEAP 的优势

使用 PEAP 有这些优势：PEAP 以 TLS 为基础，而 TLS 实施广泛，经过了大量安全审查；它在不派生密钥的方法建立密钥；它在隧道内发送身份；它保护内部方法交换和结果消息；它支持分段。

## PEAP 协议支持的请求方

PEAP 支持这些请求方：

- Microsoft 内置客户端 802.1X XP
- Microsoft 内置客户端 802.1X Vista
- 思科安全服务客户端 (SSC)，4.0 版
- Cisco SSC，5.1 版
- Funk Odyssey 访问客户端，4.72 版
- Intel，12.4.0.0 版

## PEAP 协议流程

PEAP 会话可以分为三部分：

1. 思科 ISE 和对等体建立 TLS 隧道。思科 ISE 提供其证书，但对等体不提供。对等体和思科 ISE 创建密钥以加密隧道内的数据。
2. 内部方法确定隧道内的数据流：
  - EAP-MS-CHAPv2 内部方法 - EAP-MS-CHAPv2 数据包在不带报头的情况下在隧道内传输。报头的第一个字节包含类型字段。EAP-MS-CHAPv2 内部方法支持更改密码功能。可以配置用户可以尝试通过管理门户更改密码的次数。用户身份验证尝试次数受此数值限制。
  - EAP-GTC 内部方法 - PEAPv0 和 PEAPv1 均支持 EAP-GTC 内部方法。支持的请求方不支持使用 EAP-GTC 内部方法的 PEAPv0。EAP-GTC 支持更改密码功能。可以配置用户可以尝试通过管理门户更改密码的次数。用户身份验证尝试次数受此数值限制。
  - EAP-TLS 内部方法 - Windows 内置请求方不支持在建立隧道后对消息分段，这会影响 EAP-TLS 内部方法。在建立隧道后，思科 ISE 不支持外部 PEAP 消息分段。在建立隧道时，分段会按照 PEAP 文档中的规定进行工作。在 PEAPv0 中，系统将删除 EAP-TLS 数据包信头，而在 PEAPv1 中，EAP-TLS 数据包在传输时保持不变。
  - 可扩展身份验证协议类型、长度、值 (EAP-TLV) 扩展 - EAP TLV 数据包在传输时保持不变。EAP-TLV 数据包在带标头的情况下在隧道内传输。
3. 如果会话已达到内部方法，会以一种受保护的方式确认成功和失败。

客户端 EAP 消息始终载于 RADIUS Access-Request 消息中，而服务器 EAP 消息始终载于 RADIUS Access-Challenge 消息中。EAP-Success 消息始终载于 RADIUS Access-Accept 消息中。EAP-Failure 消息始终载于 RADIUS Access-Reject 消息中。丢弃客户端 PEAP 消息会导致丢弃 RADIUS 客户端消息。



**注释** 思科 ISE 要求在 PEAPv1 通信期间确认 EAP-成功或 EAP-失败消息。对等体必须发送回带有空 TLS 数据字段的 PEAP 数据包，以确认收到成功或失败消息。

## 可扩展身份验证协议-通过安全隧道的灵活身份验证 (EAP-FAST)

可扩展身份验证协议-通过安全隧道的灵活身份验证 (EAP-FAST) 是提供相互身份验证和使用共享密钥建立隧道的一种身份验证协议。隧道用于保护基于密码的弱身份验证方法。共享密钥称为受保护的访问凭证 (PAC) 密钥，用于对客户端和服务器进行相互身份验证，同时保护隧道安全。

### EAP-FAST 的优势

EAP-FAST 相比其他身份验证协议提供以下优势：

- 相互身份验证 - EAP 服务器必须能够验证对等体的身份和真实性，而且对等体必须能够验证 EAP 服务器的真实性。
- 抵抗被动字典式攻击 - 许多身份验证协议要求对等体向 EAP 服务器明确地提供纯文本或散列形式密码。
- 抵抗中间人攻击 - 建立相互验证保护隧道时，协议必须阻止敌对者在对等体和 EAP 服务器之间的对话中成功插入信息。
- 确保支持许多不同的密码身份验证接口的灵活性，例如 MS-CHAPv2、通用令牌卡 (GTC) 及其他 - EAP-FAST 是一个扩展框架，允许同一服务器支持多个内部协议。
- 提高效率 - 使用无线介质时，对等体的计算资源和电力资源有限。EAP-FAST 使网络访问通信能够减少计算资源占用。
- 最大限度减少身份验证服务器的每用户身份验证状态要求 - 对于大型部署，通常有许多服务器充当多个对等体的身份验证服务器。此外，非常理想的情况是，对等体使用同一共享密钥保护隧道的方式，与它使用用户名和密码获得网络访问权限的方式基本相同。EAP-FAST 促进对等体使用一个强大的共享密钥，同时使服务器最大限度减少它必须缓存和管理的每用户和设备状态。

### EAP-FAST 流程

EAP-FAST 协议流程始终由以下阶段组成：

1. 调配阶段 - 此阶段是 EAP-FAST 的初始阶段。在此阶段，系统使用思科 ISE 和对等体之间共享的叫作 PAC 的唯一强密钥调配对等体。
2. 建立隧道阶段 - 客户端和服务器通过使用 PAC 建立全新隧道密钥相互进行身份验证。系统然后使用隧道密钥保护其余对话并实现消息机密性和可靠性。
3. 身份验证阶段 - 身份验证在隧道内部处理，其包含生成会话密码和受保护的终止。思科 ISE 支持 EAP-FAST 版本 1 和 1a。

## 从非思科设备启用 MAB

按顺序配置以下设置，可从非思科设备配置 MAB。

**步骤 1** 确保终端数据库中具有要进行身份验证的终端的 MAC 地址。可以添加这些终端或由分析器服务自动分析这些终端。

**步骤 2** 根据非思科设备 (PAP、CHAP 或 EAP-MD5) 使用的 MAC 身份验证的类型创建允许的协议服务。



- a) 选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 身份验证 (Authentication) > 允许的协议 (Allowed Protocols)**
- b) 输入允许的协议服务的名称。例如，MAB for NonCisco Devices。
- c) 根据非思科设备使用的 MAC 身份验证类型选择协议：

- PAP - 选中 Allow PAP/ASCII 复选框，然后选中 Detect PAP as Host Lookup 复选框。
- CHAP - 选中 Allow CHAP 复选框，然后选中 Detect CHAP as Host Lookup 复选框。
- EAP-MD5 - 选中 Allow EAP-MD5 复选框，然后选中 Detect EAP-MD5 as Host Lookup 复选框。

对于上面列出的每个协议，建议选中以下复选框：

- Check Password - 启用该选项，用以检查无关紧要的 MAB 密码，对发送网络设备进行身份验证。
- Check Calling-Station-Id equals MAC address - 启用该选项，用以在发送 Calling-Station-Id 时作为一项额外的安全检查。

**步骤 3** 配置用于从非思科设备启用 MAB 的身份验证策略规则。

- a) 选择 **策略 (Policy) > 身份验证 (Authentication)**。
- b) 选择基于规则的身份验证策略。
- c) 插入 MAB 的新规则。
- d) 选择在此规则的步骤 2 中创建的允许的协议服务 (MAB for NonCisco Devices)。
- e) 选择将内部终端数据库作为本规则的身份源。
- f) 保存身份验证策略。

---

## 从思科设备启用 MAB

按顺序配置以下设置从思科设备配置 MAB。

**步骤 1** 确保终端数据库中具有要进行身份验证的终端的 MAC 地址。可以添加这些终端或由分析器服务自动分析这些终端。

**步骤 2** 根据思科设备（PAP、CHAP 或 EAP-MD5）使用的 MAC 身份验证类型创建允许的协议服务。

- a) 选择 **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 身份验证 (Authentication) > 允许的协议 (Allowed Protocols)**
- b) 输入允许的协议服务的名称。例如，MAB for Cisco Devices。
- c) 选中 Process Host Lookup 复选框。
- d) 根据思科设备使用的 MAC 身份验证类型选择协议：
  - PAP - 选中 Allow PAP/ASCII 复选框，然后选中 Detect PAP as Host Lookup 复选框。
  - CHAP - 选中 Allow CHAP 复选框，然后选中 Detect CHAP as Host Lookup 复选框。
  - EAP-MD5 - 选中 Allow EAP-MD5 复选框，然后选中 Detect EAP-MD5 as Host Lookup 复选框。

对于上面列出的每个协议，建议选中以下复选框：

- Check Password - 启用该选项，用以检查无关紧要的 MAB 密码，对发送网络设备进行身份验证。
- Check Calling-Station-Id equals MAC address - 启用该选项，用以在发送 Calling-Station-Id 时作为一项额外的安全检查。

e) 保存允许的协议服务。

**步骤 3** 配置用于从思科设备启用 MAB 的身份验证策略规则。

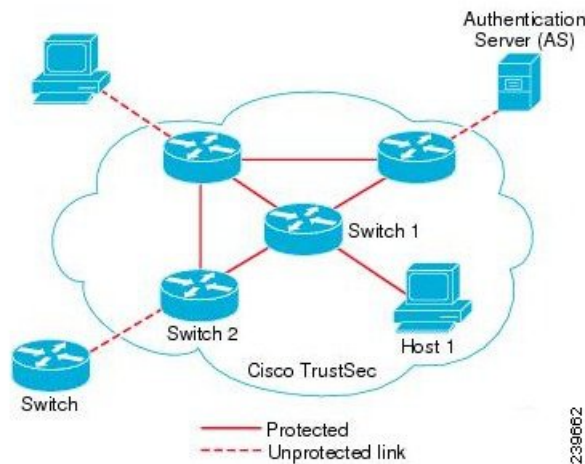
- 选择 **策略 (Policy) > 身份验证 (Authentication)**。
- 选择基于规则的身份验证策略。
- 插入 MAB 的新规则。
- 选择您在本规则的步骤 2 中创建的允许的协议服务 (MAB for Cisco Devices)。
- 选择将内部终端数据库作为本规则的身份源。
- 保存身份验证策略。

## TrustSec 架构

思科 TrustSec 解决方案可建立受信任的网络设备云以构建安全网络。思科 TrustSec 云中的每个设备都由其相邻设备（对等体）进行身份验证。TrustSec 云中设备之间的通信由加密、消息完整性检查和数据路径重放保护机制进行保护。TrustSec 解决方案使用在身份验证期间获取的设备和用户身份信息来在数据包进入网络时给数据包进行分类或确定颜色。此数据包分类在数据包进入 TrustSec 网络时由标记数据包进行维护，从而可以正确识别数据包，以沿着数据路径应用安全性和其他策略条件。此标签也称为安全组标签 (SGT)，思科 ISE 可通过此标签使终端设备在 SGT 上执行操作以过滤流量，从而实施访问控制策略。

下图显示 TrustSec 网络云的一个示例。

图 33: TrustSec 架构



## TrustSec 组件

TrustSec 的重要组件包括：

- 网络设备准入控制 (NDAC) - 在受信任网络中，在身份验证期间，TrustSec 云上的每个网络设备（例如以太网交换机）都由其对等设备对其凭证和可信度进行验证。NDAC 使用基于 IEEE 802.1X 端口的身份验证并且将可扩展身份验证协议-通过安全隧道的灵活身份验证 (EAP-FAST) 用作其可扩展身份验证协议 (EAP) 方法。如果在 NDAC 流程中身份验证和授权成功，则系统将为 IEEE 802.1AE 加密执行安全关联协议协商。思科 ISE 为从 IOSXE 17.1 开始的交换平台和从 IOSXE 17.6 开始的路由平台提供 CTS 调配 (EAP-FAST) TLSv1.2。
- 终端准入控制 (EAC) - 对连接 TrustSec 云的终端用户或设备执行的身份验证流程。EAC 通常发生于访问级别交换机上。如果在 EAP 流程中身份验证和授权成功，系统将向用户或设备分配 SGT。用于身份验证和授权的 EAC 访问方法包括：
  - 基于 802.1X 端口的身份验证
  - MAC 身份验证绕行 (MAB)
  - Web 身份验证 (WebAuth)
- 安全组 (SG) - 共用访问控制策略的一组用户、终端设备和资源。SG 由思科 ISE 中的管理员定义。当向 SGA 域添加新用户和设备时，思科 ISE 将这些新的实体分配到相应的安全组。
- 安全组标签 (SGT) - TrustSec 服务向每个安全组分配一个唯一 16 位安全组编号，其范围为 TrustSec 域内的全局范围。交换机内安全组的数量限制为已通过身份验证的网络实体的数量。您无需手动配置安全组数量。它们是自动生成的，但是您可以选择将一系列 SGT 保留用于 IP 到 SGT 的映射。
- 安全组访问控制列表 (SGACL) - SGACL 允许您根据所分配的 SG 控制访问和权限。将权限归入角色可以简化安全策略的管理。当您添加设备时，只需分配一个或多个安全组，这些安全组就会立即获得相应权限。您可以修改安全组以引入新的权限或限制当前权限。
- 安全交换协议 (SXP) - SGT 交换协议 (SXP) 是为 TrustSec 服务开发的一种协议，将整个不具有支持 SGT 的硬件的网络设备上的 IP 到 SGT 绑定表传送至支持 SGT/SGACL 的硬件。
- 环境数据下载 - TrustSec 设备在首次联接受信任网络时从思科 ISE 获取其环境数据。您也可以可以在设备上手动配置某些数据。设备必须在到期之前刷新环境数据。TrustSec 设备从思科 ISE 获取以下环境数据：
  - 服务器列表 - 列出客户端可以用于以后的 RADIUS 请求的服务器列表（适用于身份验证和授权）
  - 设备 SG - 设备自身所属的设备组
  - 过期超时 - 控制 TrustSec 设备应该多久下载或更新一次其环境变量的时间间隔
- SGT 保留 - 思科 ISE 中的一项增强功能，用于将一系列 SGT 保留用于启用 IP 到 SGT 的映射。
- IP 到 SGT 的映射 - 思科 ISE 中的一项增强功能，用于将终端 IP 与 SGT 绑定并将其调配至支持 TrustSec 的设备。思科 ISE 支持输入 1000 个 IP 到 SGT 的映射。

- 身份到端口的映射 - 交换机在终端所连接的端口上定义身份以及将身份用于在思科 ISE 服务器中查找特定 SGT 值所使用的方法。

## TrustSec 术语

下表列出某些用于 TrustSec 解决方案的常用术语及其在 TrustSec 环境中的含义。

表 95: TrustSec 术语

术语	含义
请求方	尝试加入受信任网络的设备。
身份验证	在允许每台设备加入受信任网络之前验证设备身份的过程。
授权	根据已经过身份验证的设备身份决定请求访问受信任网络上的资源的设备的访问级别的过程。
访问控制	根据分配给每个数据包的 SGT 对每个数据包应用访问控制的过程。
安全通信	为保护流经受信任网络中的每条链路的数据包进行加密、完整性和数据路径重放保护的过程。
TrustSec 设备	支持 TrustSec 解决方案的任何思科 Catalyst 6000 系列或 Cisco Nexus 7000 系列交换机。
支持 TrustSec 的设备	支持 TrustSec 的设备将具有支持 TrustSec 的硬件和软件。例如，带 Nexus 操作系统的 Nexus 7000 系列交换机。
TrustSec 种子设备	直接对思科 ISE 服务器进行身份验证的 TrustSec 设备。此设备同时用作验证器和请求方。
入口	当数据包首次遇到支持 TrustSec 的设备时，这些数据包会被标上 SGT 标记。该设备已加入启用了 Cisco TrustSec 解决方案的网络。进入受信任网络的这个点称为入口。
出口	当数据包通过最后一台支持 TrustSec 的设备时，这些数据包会被取消标记。该设备已加入启用了 Cisco TrustSec 解决方案的网络。退出受信任网络的这个点称为出口。

## TrustSec 支持的交换机和需要的组件

要设置启用思科 TrustSec 解决方案的思科 ISE 网络，您需要支持 TrustSec 解决方案的交换机和其他组件。除交换机外，您还需要其他组件用于基于身份的用户访问控制（使用 IEEE 802.1X 协议）。有关支持 TrustSec 的思科交换机平台和必要组件的完整的最新列表，请参阅[启用 TrustSec 的思科基础设施](#)。

## 配置 TrustSec 全局设置

为了让思科 ISE 充当 TrustSec 服务器并提供 TrustSec 服务，必须定义某些全局 TrustSec 设置。

### 开始之前

- 配置全局 TrustSec 设置之前，确保已定义全局 EAP-FAST 设置（选择 **Administration > System > Settings > Protocols > EAP-FAST > EAP-FAST Settings**）。

可以将 Authority Identity Info Description 更改为思科 ISE 服务器名称。此说明是用户友好字符串，描述向终端客户端发送凭证的思科 ISE 服务器。思科 TrustSec 架构中的客户端可以是运行 EAP-FAST 作为其 EAP 方法进行 IEEE 802.1X 身份验证的终端，也可以是执行网络设备访问控制 (NDAC) 的请求方网络设备。客户端可以在受保护的访问凭证 (PAC) 类型长度值 (TLV) 信息中发现此字符串。默认值为 Identity Services Engine。应该更改此值，以便可以在 NDAC 身份验证时在网络设备上唯一识别思科 ISE PAC 信息。

- 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** 选择管理 (**Administration**) > 系统 (**System**) > 设置 (**Settings**) > TrustSec 设置 (**TrustSec Settings**)。

**步骤 2** 在字段中输入值。有关这些字段的信息，请参阅 [TrustSec 设置](#)，第 581 页

**步骤 3** 点击保存 (**Save**)。

---

### 下一步做什么

- [配置 TrustSec 设备](#)，第 584 页

## TrustSec 设置

### 验证 TrustSec 部署 (Verify TrustSec Deployment)

此选项可帮助验证所有网络设备是否部署了最新的 TrustSec 策略。如果在思科 ISE 和网络设备上配置的策略之间存在任何差异，“警报” (Alarms) Dashlet 中会显示警报，该 Dashlet 位于工作中心 (**Work Centers**) > TrustSec > 控制板和主页 (**Dashboard and Home**) > 摘要 (**Summary**) 下。TrustSec 控制板中会显示以下警报：

- 每当验证过程开始或完成时，系统都会显示带有信息 (Info) 图标的警报。
- 如果由于新的部署请求而取消验证过程，则会显示带有信息 (Info) 图标的警报。
- 如果验证过程因错误而失败，则会显示带有警告 (Warning) 图标的警报。例如，无法打开与网络设备的 SSH 连接，或当网络设备不可用，或当思科 ISE 和网络设备上配置的策略之间存在任何差异。

验证部署 (Verify Deployment) 选项也可从以下窗口选择。

- 工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 (Security Groups)
- 工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 ACL (Security Group ACLs)
- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 矩阵 (Matrix)
- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 源树 (Source Tree)
- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 目标树 (Destination Tree)

**每次部署后自动验证 (Automatic Verification After Every Deploy):** 如果希望思科 ISE 在每次部署后验证所有网络设备上的更新，请选中此复选框。部署过程完成后，经过您在部署过程后的时间 (Time after Deploy Process) 字段中指定的时间后，验证过程开始。

**部署过程后的时间 (Time After Deploy Process):** 指定您希望思科 ISE 在部署过程完成后等待多长时间，然后再开始验证过程。有效范围为 10 - 60 分钟。

如果在等待期间收到新的部署请求或正在进行其他验证，则会取消当前验证过程。

**立即验证 (Verify Now):** 点击此选项可立即开始验证过程。

#### 受保护的访问凭证 (PAC)

- **隧道 PAC 生存时间 (Tunnel PAC Time to Live):**

指定 PAC 的到期时间。隧道 PAC 为 EAP-FAST 协议生成隧道。您可以秒、分钟、小时、天或周为单位指定时间。默认值为 90 天。以下是有效范围：

- 1 - 157680000 秒
  - 1 - 2628000 分钟
  - 1 - 43800 小时
  - 1 - 1825 天
  - 1 - 260 周
- **进行主动 PAC 更新前所经历的时间 (Proactive PAC Update Will Occur After):** 当剩余的隧道 PAC TTL 百分比达到设定值时，思科 ISE 会在成功身份验证后主动向客户端提供新 PAC。如果

第一次成功身份验证发生在 PAC 到期之前，则服务器会启动隧道 PAC 更新。此机制会为客户端更新有效的 PAC。默认值为 10%。

## 安全组标签编号

### APIC EPG 的安全组标签编号 (Security Group Tag Numbering for APIC EPGs)

**APIC EPG 的安全组标签编号 (Security Group Tag Numbering for APIC EPGs):** 选中此复选框，指定编号范围以用于根据从 APIC 获取的 EPG 创建的 SGT。

### 自动创建安全组

**创建授权规则时自动创建安全组 (Auto Create Security Groups When Creating Authorization Rules):** 选中此复选框可在创建授权策略规则时自动创建 SGT。

如果选中此选项，**授权策略 (Authorization Policy)** 窗口顶部会显示以下消息：开启自动安全组创建 (Auto Security Group Creation is On)。

系统会根据规则属性命名自动创建的 SGT。点击权限 (**Permissions**) 字段中显示的加号 (+) 标志可编辑 SGT 名称和值。



---

**注释** 当删除相应的授权策略规则时，不会删除自动创建的 SGT。

---

默认情况下，此选项在全新安装或升级后会被禁用。

### IP SGT 主机名静态映射

**IP SGT 主机名静态映射 (IP SGT Static Mapping of Hostnames):** 如果使用 FQDN 和主机名，则思科 ISE 会在部署映射和检查部署状态的同时在 PAN 和 PSN 节点中查找对应的 IP 地址。您可以使用此选项指定为 DNS 查询返回的 IP 地址创建的映射数。您可以选择以下其中一个选项：

- 为 DNS 查询返回的所有 IP 地址创建映射 (Create mappings for all IP addresses returned by a DNS query)
- 仅为 DNS 查询返回的第一个 IPv4 地址和第一个 IPv6 地址创建映射 (Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query)

### 相关主题

[TrustSec 架构](#)，第 578 页

[TrustSec 组件](#)，第 579 页

[配置 TrustSec 全局设置](#)，第 581 页

## 配置 TrustSec 设备

为了让思科 ISE 处理来自启用 TrustSec 的设备的请求，您必须在思科 ISE 中定义这些启用 TrustSec 的设备。

**步骤 1** 依次选择 **Administration > Network Resources > Network Devices**。

**步骤 2** 点击添加 (Add)。

**步骤 3** 在 **Network Devices** 部分中输入所需信息。

**步骤 4** 选中 **Advanced Trustsec Settings** 复选框以配置支持 Trustsec 的设备。

**步骤 5** 点击提交。

## OoB TrustSec PAC

所有 TrustSec 网络设备都将 TrustSec PAC 视为 EAP-FAST 协议的一部分。安全 RADIUS 协议也使用此 TrustSec PAC，其中 RADIUS 共享密钥是根据 PAC 携带的参数推导而来。这些参数中的 Initiator-ID 参数包含 TrustSec 网络设备身份，即设备 ID。

如果使用 TrustSec PAC 识别设备，并且在思科 ISE 上为该设备配置的设备 ID 和 PAC 上的 Initiator-ID 之间不匹配，则身份验证失败。

有些 TrustSec 设备（例如思科防火墙 ASA）不支持 EAP-FAST 协议。因此，思科 ISE 无法通过 EAP-FAST 使用 TrustSec PAC 调配这些设备。系统会在思科 ISE 上生成 TrustSec PAC 并且需要手动将其复制到设备上，所以这又称为带外 (OOB) TrustSec PAC 生成。

当从思科 ISE 生成 PAC 时，系统会生成使用加密密钥加密的 PAC 文件。

本节介绍以下主题：

### 从设置屏幕生成 TrustSec PAC

可以从设置屏幕生成 TrustSec PAC。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 设置 (Settings)。

**步骤 2** 从左侧的 Settings 导航窗格中，点击 **Protocols**。

**步骤 3** 依次选择 **EAP-FAST > Generate PAC**。

**步骤 4** 生成 TrustSec PAC。

### 从网络设备屏幕生成 TrustSec PAC

您可以从“网络设备” (Network Devices) 屏幕生成 TrustSec PAC。



---

**步骤 1** 依次选择管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)。

**步骤 2** 点击添加 (Add)。您还可以从“网络设备” (Network Devices) 导航窗格的操作图标上点击 添加新设备 (Add new device)。

**步骤 3** 如果要添加新设备，请提供设备名称。

**步骤 4** 选中 TrustSec 高级设置 (Advanced TrustSec Settings) 复选框以配置 TrustSec 设备。

**步骤 5** 在带外 (OOB) TrustSec PAC (Out of Band (OOB) TrustSec PAC) 子部分下，点击生成 PAC (Generate PAC)。

**步骤 6** 提供以下详细信息：

- PAC Time to Live - 输入值（单位：天、周、月或年）。默认情况下，该值为一年。最小值为一天，最大值为十年。
- Encryption Key - 输入加密密钥。密钥的长度必须介于 8 和 256 个字符之间。密钥可以包含大写或小写字母或数字，或字母数字字符的组合。

加密密钥用于对生成的文件中的 PAC 进行加密。此密钥也用于解密该设备上的 PAC 文件。因此，建议管理员保存加密密钥以供日后使用。

“身份” (Identity) 字段指定 TrustSec 网络设备的设备 ID，并且 EAP-FAST 协议会提供发起方 ID。如果此处输入的身份字符串与“网络设备创建” (Network Device creation) 页面中 TrustSec 部分下定义的设备 ID 不匹配，那么身份验证将会失败。

根据 PAC 存活时间 (PAC Time to Live) 计算到期日期。

**步骤 7** 点击生成 PAC (Generate PAC)。

---

## 从“网络设备” (Network Devices) 列表屏幕生成 TrustSec PAC

您可以从“网络设备” (Network Devices) 列表屏幕生成 TrustSec PAC。

---

**步骤 1** 依次选择管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)。

**步骤 2** 点击网络设备 (Network Devices)。

**步骤 3** 选中要为其生成 TrustSec PAC 的设备旁边的复选框，然后点击生成 PAC (Generate PAC)。

**步骤 4** 在字段中提供详细信息。

**步骤 5** 点击生成 PAC (Generate PAC)。

---

## 按钮

出口策略中的 Push 选项可以启动 CoA 通知，告知 Trustsec 设备立即从思科 ISE 请求关于出口策略中的配置更改的更新。

## 配置思科 TrustSec AAA 服务器

可以在 AAA 服务器列表中配置启用了思科 TrustSec 的思科 ISE 服务器列表。思科 TrustSec 设备向其中任意服务器进行身份验证。点击“推送” (Push) 时，此列表中的新服务器将下载到 TrustSec 设备。当思科 TrustSec 设备尝试进行身份验证时，它会从此列表中选择任意思科 ISE 服务器。如果第一台服务器关闭或繁忙，思科 TrustSec 设备可以向此列表中的任何其他服务器自行进行身份验证。默认情况下，主要思科 ISE 服务器是思科 TrustSec AAA 服务器。建议您配置更多思科 ISE 服务器，以获得更可靠的思科 TrustSec 环境。

此页面列出了部署中您已配置为思科 TrustSec AAA 服务器的思科 ISE 服务器。

### 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** 选择管理 (Administration) > 网络资源 (Network Resources) > TrustSec AAA 服务器 (TrustSec AAA Servers)。

**步骤 2** 点击添加 (Add)。

**步骤 3** 按如下所述输入值：

- **名称：**要分配至此 AAA 服务器列表中的思科 ISE 服务器的名称。此名称可与思科 ISE 服务器的主机名不同。
- **说明：**可选说明。
- **IP：**您正添加到 AAA 服务器列表的思科 ISE 服务器的 IP 地址。
- **端口：**TrustSec 设备与服务器之间进行通信所在的端口。默认值为 1812。

**步骤 4** 点击提交 (Submit)。

**步骤 5** 在随后显示的 AAA 服务器 窗口中，点击 推送。

---

### 下一步做什么

配置安全组。

## 安全组配置

安全组 (SG) 或安全组标签 (SGT) 是在 TrustSec 策略配置中用到的元素。在可信任的网络中移动时，SGT 连接到数据包。这些数据包在进入可信任的网络（入口）时被标记，离开可信任的网络（出口）时被取消标记。

SGT 按顺序生成，但您可以选择为 IP 到 SGT 映射保留一些 SGT。生成 SGT 时，思科 ISE 跳过保留的编号。

TrustSec 服务使用这些 SGT 在出口实施 TrustSec 策略。

您可以在 Admin 门户从以下页面配置安全组：

- **Policy > Policy Elements > Results > Trustsec > Security Groups**。
- 直接从出口策略页面，在 **Configure > Create New Security Group** 配置。

更新多个 SGT 后，点击 **Push** 按钮，发起环境 CoA 通知。此环境 CoA 通知转至全部 TrustSec 网络设备，强迫它们开始策略/数据刷新请求。



**注释** 建议不要频繁使用 **推送 (Push)** 或 **部署 (Deploy)** 按钮。当矩阵或 SGACL 发生变化时，请在执行下一个部署操作之前检查通知栏是否存在任何待处理的部署请求。

## 添加安全组

您应向 TrustSec 解决方案中的每个安全组分配一个唯一的 SGT。尽管思科 ISE 支持 65535 个 SGT，减少 SGT 的数量能够让您更轻松部署和管理 TrustSec 解决方案。我们建议最多使用 4000 个 SGT。

### 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** 选择策略 (**Policy**) > 策略元素 (**Policy Elements**) > 结果 (**Results**) > **TrustSec** > 安全组 (**Security Groups**)。

**步骤 2** 点击 **Add** 以添加新安全组。

**步骤 3** 为新安全组输入名称和说明（可选）。

**步骤 4** 输入 Tag Value。标签值可以设置为手动输入或自动生成。您还可以为 SGT 保留范围。您可以从以下位置对其进行配置：**管理 (Administration) > 系统(System) > 设置 (Settings) > Trustsec 设置 (Trustsec Settings)** 下的 Trustsec 全局设置页面。

**步骤 5** 单击保存。

### 下一步做什么

配置安全组访问控制列表 (SGACL)

## 将安全组导入思科 ISE

您可以使用逗号分隔值 (CSV) 文件将安全组导入思科 ISE 节点。您必须在更新模板之后才能将安全组导入思科 ISE。您不能同时运行同一资源类型的导入。例如，您无法同时导入来自两个不同导入文件的安全组。

您可以从管理员门户下载 CSV 模板，在模板中输入您的安全组详细信息，并将该目标保存为 CSV 文件，接着您就可以将此文件导入回思科 ISE。

在导入安全组的过程中，您可以在思科 ISE 遇到第一个错误时停止导入过程。

步骤 1 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > TrustSec > 安全组 (Security Groups)。

步骤 2 点击导入 (Import)。

步骤 3 点击浏览 (Browse) 从正在运行客户端浏览器的系统选择 CSV 文件。

步骤 4 选中 **Stop Import on First Error** 复选框。

步骤 5 点击导入 (Import)。

## 从思科 ISE 导出安全组

您可以将思科 ISE 中配置的安全组导出为 CSV 文件，您可以使用此文件将这些安全组导入到其他思科 ISE 节点中。

步骤 1 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > TrustSec > 安全组 (Security Groups)。

步骤 2 点击导出 (Export)。

步骤 3 要导出安全组，您可以执行下述操作中的一项：

- 选中您希望导出的组旁的复选框，并依次选择导出 (Export) > 导出选定对象 (Export Selected)。
- 选择导出 (Export) > 导出全部 (Export All) 以导出所有定义的安全组。

步骤 4 将 export.csv 文件保存到您的本地硬盘中。

## 添加安全组访问控制列表

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 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > TrustSec > 安全组 ACLs (Security Group ACLs)。

步骤 2 添加 **Add** 创建新安全组 ACL。

步骤 3 输入以下信息：

- Name - SGACL 的名称
- Description - SGACL 的可选说明
- IP Version - 此 SGACL 支持的 IP 版本：
  - IPv4 - 支持 IP 版本 4 (IPv4)

- IPv6 - 支持 IP 版本 6 (IPv6)
  - Agnostic - 同时支持 IPv4 和 IPv6
- Security Group ACL Content - 访问控制列表 (ACL) 命令。例如：

**permit icmp**

**deny ip**

在 ISE 中未检查 SGACL 输入的语法。确保使用正确的语法，以便交换机、路由器和接入点可以正确无误地应用它们。默认策略可以配置为 **permit IP**、**permit ip log**、**deny ip** 或 **deny ip log**。TrustSec 网络设备将默认策略附加到特定信元策略的末尾。

以下是两个指导性的 SGACL 示例。两者都包含一个 final catch all 规则。第一个拒绝为 final catch all 规则，第二个则允许。

Permit\_Web\_SGACL

```
permit tcp dst eq 80
permit tcp dst eq 443
deny ip
```

Deny\_JumpHost\_Protocols

```
deny tcp dst eq 23
deny tcp dst eq 23
deny tcp dst eq 3389
permit ip
```

下表列出适用于 IOS、IOS XE 和 NS-OS 操作系统的 SGACL 语法。

SGACL CLI 和 ACE	IOS、IOS XE 和 NX-OS 通用的语法
config acl	deny, exit, no, permit
deny permit	ahp, eigrp, gre, icmp, igmp, ip, nos, ospf, pcp, pim, tcp, udp
deny tcp deny tcp src deny tcp dst	dst, log, src
deny tcp dst eq deny tcp src eq	range 0 65535
deny udp deny udp src deny udp dest	Dst, log, src
deny tcp dst eq www deny tcp src eq www	range 0 65535

**注释** 某些思科交换机不允许使用连字符。所以 `permit dst eq 32767-65535` 无效。使用 `permit dst eq range 32767 65535`。某些思科交换机的命令语法中不需要使用 `eq`。因此，`permit dst eq 32767-65535` 在这些交换机中无效。请改为使用 `permit dst 32767-65535` 或 `permit dst range 32767 65535`。

#### 步骤 4 点击推送。

“推送” (Push) 选项可启动 CoA 通知，告知 Trustsec 设备立即向思科 ISE 请求关于配置更改的更新。



**注释** 思科 ISE 具有以下预定义的 SGACL：Permit IP、Permit IP Log、Deny IP 和 Deny IP Log。您可以使用这些 SGACL 通过 GUI 或 ERS API 配置 TrustSec 矩阵。虽然这些 SGACL 未在 GUI 的“安全组 ACL” (Security Group ACLs) 列表页面中列出，但当您使用 ERS API 列出可用的 SGACL (ERS getAll 调用) 时，这些 SGACL 将列出。

## 出口策略

出口表列出已保留和未保留的源和目标 SGT。此页还允许您过滤出口表以查看特定策略并保存这些预设过滤器。当源 SGT 尝试到达目标 SGT 时，基于出口策略中定义的 TrustSec 策略，支持 TrustSec 的设备会执行 SGACL。思科 ISE 创建并调配策略。

SGT 和 SGACL 是创建 TrustSec 策略的基础，在您创建 SGT 和 SGACL 后，通过将 SGACL 分配至源和目标 SGT，您就可以在二者之间建立起关系。

每个源 SGT 到目标 SGT 的组合即为出口策略中的一个信元。

您可以在 **Policy > TrustSec > Egress Policy** 页面中查看出口策略。

有三种方式查看出口策略：

- 源树视图
- 目标树视图
- 矩阵视图

## 源树视图

源树视图以折叠状态列出源 SGT 紧凑而且组织有序的视图。您可以展开任意源 SGT 以查看列出与所选源 SGT 相关的所有信息的内部表。该视图仅显示映射至目标 SGT 的源 SGT。如果您展开具体源 SGT，其将在表中列出映射至此源 SGT 的所有目标 SGT 和相应的策略 (SGACL)。

您将看到三个点 (...) 旁边的一些字段。这表示此单元格包含更多信息。您可以将光标放在这三个点上以在快速视图弹出窗口中查看其余信息。当您把光标放在 SGT 名称或 SGACL 名称上时，系统会打开一个快速查看弹出窗口，显示该具体 SGT 或 SGACL 的内容。

## 目标树视图

目标树视图以折叠状态列出目标 SGT 的精简和组织视图。可以展开任意目标 SGT，以查看列出所有与该选定目标 SGT 相关的信息的内部表。此视图仅显示映射到源 SGT 的目标 SGT。如果展开特定目标 SGT，该 SGT 会在表中列出映射到此目标 SGT 的所有源 SGT，以及对应的策略 (SGACL)。

您将看到三个点 (...) 旁边的一些字段。这表示此单元格包含更多信息。您可以将光标放在这三个点上以在快速视图弹出窗口中查看其余信息。当您把光标放在 SGT 名称或 SGACL 名称上时，系统会打开一个快速查看弹出窗口，显示该具体 SGT 或 SGACL 的内容。

## 矩阵视图

出口策略的矩阵视图与电子表格类似。它包含两个轴：

- 源轴 - 此垂直轴列出所有源 SGT。
- 目标轴 - 此水平轴列出所有目标 SGT。

源 SGT 到目标 SGT 的映射以单元格表示。如果某个单元格包含数据，则表示对应的源 SGT 和目标 SGT 之间有一个映射。此矩阵视图中有两类单元格：

- 有映射的单元格 - 源和目标 SGT 对与一组有序的 SGACL 关联并且具有指定的状态。
- 无映射的单元格 - 源和目标 SGT 对不与任何 SGACL 关联并且不具有指定的状态。

出口策略单元格显示源 SGT、目标 SGT 和在 SGACL 下作为单独列表的 **Final Catch All Rule**，以逗号隔开。如果 **Final Catch All Rule** 设置为 **None**，则不显示。矩阵中空单元格表示无映射的单元格。

在出口策略矩阵视图中，您可以滚动浏览矩阵以查看所需单元格集。浏览器不会一次性加载全部矩阵数据。浏览器会请求服务器加载属于您所滚动浏览区域的数据。这样可以防止内存溢出和性能问题。

此表格视图的 GUI 元素与源视图及目标视图的相同。但是，它还包括以下其他元素：

### 矩阵维度

通过 Matrix 视图中的 **Dimension** 下拉列表，可以设置矩阵的维度。

### 压缩视图

通过出口策略矩阵视图中的“压缩” (Condensed) 选项，您可以显示无空单元格的矩阵。选中 **压缩 (Condensed)** 复选框，隐藏空单元格。

### 矩阵操作

#### 通过矩阵进行导航

您可以通过矩阵进行导航，方法是使用光标拖曳矩阵内容区域，或者使用水平和垂直滚动条。您可以通过点击并按住某个单元格，沿任何方向拖曳该单元格以及整个矩阵内容。源栏和目标栏随单元格一

起移动。选中某个单元格时，矩阵视图突出显示该单元格以及相应的行（源 SGT）和列（目标 SGT）。选定单元格的坐标（源 SGT 和目标 SGT）显示在矩阵内容区域的下方。

### 选中矩阵中的单元格

要选中矩阵视图中的某个单元格，请点击该单元格。选定的单元格会显示不同的颜色，并且源 SGT 和目标 SGT 会突出显示。要取消选中某个单元格，只需再次点击该单元格或者选中另一个单元格即可。不允许在矩阵视图中选中多个单元格。双击单元格以编辑单元格的配置。

## 从出口策略配置 SGACL

您可以直接从“出口策略” (Egress Policy) 页面创建安全组 ACL。

---

**步骤 1** 依次选择策略 (Policy) > TrustSec > 出口策略 (Egress Policy)。

**步骤 2** 从“源或目标树视图” (Source or Destination Tree View) 页面，选择配置 (Configure) > 创建新的安全组 ACL (Create New Security Group ACL)。

**步骤 3** 输入所需的详细信息，并点击提交 (Submit)。

---

## 出口策略表单元格配置

通过思科 ISE，可以使用工具栏中可用的各种选项配置单元格。如果所选源和目标 SGT 与映射的单元格相同，则思科 ISE 不允许进行单元格配置。

## 添加出口策略单元格映射

您可以从 Policy 页面添加出口策略的映射单元格。

---

**步骤 1** 选择策略 (Policy) > TrustSec > 出口策略 (Egress Policy)。

**步骤 2** 要选择矩阵单元格，请执行以下操作：

- 在矩阵视图中，点击某个单元格将其选定。
- 在 Source 和 Destination 树状视图中，选中内部表中某一行的对应复选框以选定该行。

**步骤 3** 点击 Add 以添加新映射单元格。

**步骤 4** 选择下列各项的相应值：

- Source Security Group
- Destination Security Group
- Status, Security Group ACLs
- Final Catch All Rule



步骤 5 点击保存 (Save)。

---

## 导出出口策略

---

步骤 1 选择策略 (Policy) > TrustSec > 出口策略 (Egress Policy) > 矩阵 (Matrix)。

步骤 2 点击导出 (Export)。

步骤 3 将 CSV 文件保存到本地系统。

---

## 导入出口策略

您可以离线创建出口策略，然后将该策略导入思科 ISE。如果具有大量的安全组标记，那么逐个创建安全组 ACL 映射可能需要一些时间。相反，离线创建出口策略并将该策略导入思科 ISE 可节省时间。在导入过程中，思科 ISE 会将 CSV 文件中的条目附加到出口策略矩阵，并且不会覆盖数据。

如果出现以下情况，出口策略导入会失败：

- 源或目标 SGT 不存在
  - SGACL 不存在
  - 监控状态与当前在思科 ISE 中为该信元配置的状态不同
- 

步骤 1 选择策略 (Policy) > TrustSec > 出口策略 (Egress Policy) > 矩阵 (Matrix)。

步骤 2 点击生成模版 (Generate a Template)。

步骤 3 从“出口策略” (Egress Policy) 页面下载模板 (CSV 文件)，然后在 CSV 文件中输入以下信息：

- 源 SGT
- 目标 SGT
- SGACL
- 监控状态 (启用、禁用或监控)

步骤 4 请选中遇到第一个错误时停止导入 (Stop Import on First Error) 复选框，使思科 ISE 在遇到任何错误时取消导入。

步骤 5 点击导入 (Import)。

---

## 从出口策略配置 SGT

您可以直接从“出口策略” (Egress Policy) 页面创建安全组。

---

步骤 1 选择策略 (Policy) > TrustSec > 出口策略 (Egress Policy)。

**步骤 2** 从“源或目标树视图” (Source or Destination Tree View) 页面，选择配置 (Configure) > 创建新的安全组 (Create New Security Group)。

**步骤 3** 输入所需的详细信息，并点击提交 (Submit)。

## 监控模式

只需点击一下，您就可以通过出口策略中的 Monitor All 选项将整个出口策略配置状态改为监控模式。在出口策略页面，选中 **Monitor All** 复选框，将所有单元的出口策略配置状态改为监控模式。选中 Monitor All 复选框后，配置状态中会发生以下更改：

- 状态为 Enabled 的单元将显示受监控行为，但看起来仍然像处于启用状态一样。
- 状态为 Disable 的单元不受影响。
- 状态为 Monitored 的单元仍保持 Monitored 状态。

取消选中 **Monitor All** 复选框即可恢复原始配置状态。这不会更改数据库中单元的实际状态。如果您取消选择 **Monitor All**，出口策略中的每个单元将恢复原配置状态。

## 监控模式功能

监控模式的监控功能可帮助您：

- 知悉已筛选但受监控模式监控的流量
- 知悉 SGT-DGT 对是处于监控模式还是执行模式，并且观察网络中是否在发生任何异常丢包
- 了解 SGACL 丢弃实际是由执行模式执行还是由监控模式允许
- 根据监控类型（监控和/或执行）创建自定义报告
- 标识在 NAD 上已应用的 SGACL 并显示差异（如有）

## 未知安全组

未知安全组是一个无法修改、使用标签值 0 表示 Trustsec 的预配置安全组。

当思科安全组网络设备没有来源或目标的 SGT 时，这些设备会请求引用未知 SGT 的信元。如果仅来源未知，则请求适用于 <unknown, Destination SGT> 信元。如果仅目标未知，则请求适用于 <source SGT, unknown> 信元。如果来源和目标均未知，则请求适用于 <Unknown, Unknown> 信元。

## 默认策略

默认策略是指 <ANY,ANY> 信元。所有源 SGT 均映射到所有目标 SGT。此处，ANY SGT 不可修改，且未在任何源或目标 SGT 中列出。ANY SGT 仅可与 ANY SGT 配对。ANY SGT 无法与其他任何 SGT 配对。TrustSec 网络设备将默认策略附加到特定信元策略的末尾。

- 如果信元为空，则意味着该信元仅包含默认策略。

- 如果信元包含某种策略，则生成的策略为信元特定策略与默认策略的组合。

根据思科 ISE，信元策略和默认策略为两套独立的 SGACL，由设备分别获取以响应两个独立的策略查询。

默认策略的配置与其他信元不同：

- 状态仅可为两个值，启用或监控。
- 安全组 ACL 是默认策略的可选字段，因此可留空。
- 最终抓取所有规则可为以下任意项：允许 IP、拒绝 IP、允许 IP 日志或拒绝 IP 日志。显然此处 None 选项不可用，因为默认策略之外无安全网。

## SGT 分配

如果您知道设备主机名或 IP 地址，思科 ISE 允许向 TrustSec 设备分配 SGT。当具有特定主机名或 IP 地址的设备加入网络时，思科 ISE 会在对其进行身份验证之前分配 SGT。

有时需要手动将设备配置为将安全组标签映射至终端。您可以从 Security Group Mappings 页面创建此映射。在执行此操作前，请确保您保留了一系列 SGT。

ISE 允许创建最多 10000 个 IP 到 SGT 映射。您可以创建 IP 到 SGT 映射组，从逻辑上将这些大规模的映射进行分组。每组 IP 到 SGT 映射都包含一个 IP 地址列表，其要映射的单个安全组，以及作为这些映射的部署目标的网络设备或网络设备组。

## NDAC 授权

您可以通过向设备分配 SGT 配置 TrustSec 策略。您可以根据 TrustSec 设备 ID 属性向设备分配安全组。

### 配置 NDAC 授权

开始之前

- 确保创建用于策略中的安全组。
- 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** 选择策略 (Policy) > TrustSec > 网络设备授权 (Network Device Authorization)。

**步骤 2** 点击 Default Rule 行右侧的 Action 图标，然后点击 Insert New Row Above。


**步骤 3** 为此规则输入名称。

**步骤 4** 点击 Conditions 旁边的加号 (+) 以添加策略条件。

**步骤 5** 您可以点击 Create New Condition (Advance Option)，然后创建新条件。

**步骤 6** 从安全组 (Security Group) 下拉列表中，选择在此条件评估为 true 的情况下要分配的 SGT。

**步骤 7** 在此行中点击 **Action** 图标，根据设备属性在当前规则上方或下方添加更多的规则。您可以重复此过程，为 TrustSec

策略创建所需的所有规则。您可以通过点击  图标，拖放规则以为其重新排序。您还可以复制现有条件，但请确保更改策略名称。

评估为 **true** 的第一条规则决定评估的结果。如果没有匹配的规则，则将应用默认规则；您可以编辑默认规则以指定在没有匹配的规则的情况下必须应用的 SGT。

**步骤 8** 点击 **Save** 以保存您的 TrustSec 策略。

如果在您配置了网络设备策略后 SGA 设备尝试进行身份验证，设备将获取其 SGT 及其对等设备的 SGT 并且将可以下载所有相关的详细信息。

## 配置最终用户授权

思科 ISE 允许您分配安全组作为授权策略评估的结果。使用此选项，您可以将安全组分配到用户和终端。

### 开始之前

- 请参阅授权策略的信息。
- 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** 依次选择 **Policy > Authorization**。

**步骤 2** 创建新的授权策略。

**步骤 3** 选择安全组的权限。

如果在此授权策略中指定的条件对用户或终端为真，则此安全组会被分配到该用户或终端，且该用户或终端所发送的所有数据包会标记为此特定的 SGT。

## 添加单个 IP 到 SGT 映射

### 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** 选择策略 (**Policy**) > 策略元素 (**Policy Elements**) > 结果 (**Results**) > **TrustSec** > 安全组映射 (**Security Group Mappings**) > 主机 (**Hosts**)。

**步骤 2** 点击 **Add**，添加新的单个 IP 到 SGT 映射。

**步骤 3** 选择是想输入设备的 **Hostname** 还是 **IP Address**。您还可以输入 IP 地址的子网掩码。

步骤 4 选择如下选项之一：

- **Group Mapping** - 将 IP 映射设置为现有映射组的一部分。
- **Security Group Tag** - 在此 IP 和 SGT 之间创建平面映射。

步骤 5 选择希望部署此映射的目标网络设备。您可以在所有 Trustsec 设备、选定的网络设备组或选定的网络设备上部署该映射。

步骤 6 点击提交。

---

## 添加组 IP 到 SGT 映射

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 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > TrustSec > 安全组映射 (Security Group Mappings) > 组 (Groups)。

步骤 2 点击 **Add** 将新的组 IP 添加到 SGT 映射。

步骤 3 输入组的 **Name** 和 **Description**。

步骤 4 输入此组所映射的 **Security Group Tag**。

步骤 5 选择希望部署此映射的目标网络设备。您可以在所有 Trustsec 设备、选定的网络设备组或选定的网络设备上部署该映射。

步骤 6 点击提交。

---

## 导入安全组映射主机

您可以使用逗号分隔值 (CSV) 文件将安全组映射主机列表导入到思科 ISE 节点。不能同时运行相同资源类型的导入。例如，您不能从两个不同导入文件并发导入安全组映射主机。

您可以从策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > Trustsec > 安全组映射 (Security Group Mappings) > 主机 (Hosts) > 导入 (Import) 页面下载 CSV 模板。在模板中输入安全组映射主机详细信息，并将其另存为以后可导入回到思科 ISE 中的 CSV 文件。

导入主机时，您可以创建新记录或更新现有记录。思科 ISE 显示导入的主机数的摘要，并且还会报告导入过程中发现的任何错误。导入主机时，您还可以定义在思科 ISE 遇到第一个错误时是否希望思科 ISE 停止导入过程。

---

步骤 1 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > TrustSec > 安全组映射 (Security Group Mappings) > 主机 (Hosts)。

步骤 2 点击导入 (Import)。

**步骤 3** 点击浏览 (**Browse**) 从正在运行客户端浏览器的系统选择 CSV 文件。

**步骤 4** 如果需要，请选中遇到第一个错误时停止导入 (**Stop Import on First Error**) 复选框。

**步骤 5** 点击导入 (**Import**)。

---

## 导出安全组映射主机

您可以将在思科 ISE 中配置的安全组映射主机以 CSV 文件的形式导出，然后您可以使用此文件将这些主机导入另一思科 ISE 节点。

**步骤 1** 选择策略 (**Policy**) > 策略元素 (**Policy Elements**) > 结果 (**Results**) > TrustSec > 安全组映射 (**Security Group Mappings**) > 主机 (**Hosts**)。

**步骤 2** 点击导出 (**Export**)。

**步骤 3** 要导出安全组映射主机，您可以执行以下任一操作：

- 选中您要导出的主机旁边的复选框，然后依次选择导出 (**Export**) > 导出选定对象 (**Export Selected**)。
- 依次选择导出 (**Export**) > 导出全部 (**Export All**) 以导出所定义的所有安全组映射主机。

**步骤 4** 将 export.csv 文件保存到您的本地硬盘中。

---

## 部署 IP 到 SGT 映射

向思科 ISE 添加 IP 到 SGT 的映射后，您必须将这些映射部署到目标网络设备。即使您之前保存了这些映射，也必须明确地执行此操作。思科 ISE 为您提供部署全部映射或部分映射的选项。

### 开始之前

您必须向思科 ISE 添加了 IP 到 SGT 的映射或已创建包含 IP 到 SGT 的映射的 IP 到 SGT 映射组。

**步骤 1** 要向设备部署 IP 到 SGT 的映射，您可以执行以下操作之一：

- 如果您想要向设备部署 IP 到 SGT 映射组，请依次选择 **Policy > Policy Elements > Results > Trustsec > Security Group Mappings > Groups**。
- 如果您想要向设备部署单一 IP 到 SGT 的映射，请依次选择 **Policy > Policy Elements > Results > Trustsec > Security Group Mappings > Hosts**。

**步骤 2** 执行以下操作之一：

- 选中要部署的组或映射旁的复选框，然后选择部署 (**Deploy**) 以部署所选择的映射。选择要部署新映射的设备时，ISE 会选择将受新映射影响的所有设备。
- 选择 **Deploy** 以部署在思科 ISE 中配置的 IP 到 SGT 的映射。

思科 ISE 向组或映射中定义的特定网络设备部署映射。它还显示包含部署设备、配置、部署状态和故障原因（如有）等详细信息的报告。

## TrustSec 配置和策略推送

思科 ISE 支持授权更改 (CoA)，通过 CoA 思科 ISE 可以通知 TrustSec 设备 TrustSec 配置和策略更改，这样设备就可以用获取相关数据的请求作为回复。

CoA 通知可以触发 TrustSec 网络设备发送环境 CoA 或策略 CoA。

您可以向本身不支持 TrustSec CoA 功能的设备推送对设备的配置更改。

### 支持 CoA 的网络设备

思科 ISE 可向以下网络设备发送 CoA 通知：

- 具有单个 IP 地址的网络设备（不支持子网）
- 配置为 TrustSec 设备的网络设备
- 设置为支持 CoA 的网络设备

在有多个辅助设备与很多不同的设备互操作的分布式环境中部署思科 ISE 时，CoA 请求从思科 ISE 主节点发送至所有网络设备。因此，TrustSec 网络设备需要配置为将思科 ISE 主节点作为 CoA 客户端。

设备向思科 ISE 主节点返回 CoA NAK 或 ACK。但是，来自网络设备的以下 TrustSec 会话会发送至接收网络设备发送的所有其他 AAA 请求的思科 ISE 节点，而不一定会发送至主节点。

### 向不支持 CoA 的设备推送配置更改

某些平台不支持思科 ISE 的更改授权 (CoA) “推送”功能，例如：Nexus 网络设备的某些版本。对于这种情况，ISE 将连接到网络设备，使该设备触发对 ISE 的更新配置请求。为此，ISE 对网络设备开放 SSHv2 隧道，思科 ISE 发送触发刷新 TrustSec 策略矩阵的命令。此方法也可以在支持 CoA 推送的网络平台上实施。

**步骤 1** 选择 **设备管理 (Device Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)**。

**步骤 2** 选中所需网络设备旁边的复选框，然后点击 **编辑 (Edit)**。

验证网络设备的名称、IP 地址、RADIUS 和 TrustSec 设置是否已正确配置。

**步骤 3** 向下滚动至 **TrustSec 高级设置 (Advanced TrustSec Settings)**，在 **TrustSec 通知和更新 (TrustSec Notifications and Updates)** 部分，选中 **发送配置更改至设备 (Send configuration changes to device)** 复选框，点击 **CLI (SSH)** 单选按钮。

**步骤 4** （可选）提供 SSH 密钥。

- 步骤 5** 选中当部署安全组标记映射更新时包含此设备 (**Include this device when deploying Security Group Tag Mapping Updates**) 复选框, 使此 SGA 设备使用设备接口凭据获取 IP-SGT 映射。
- 步骤 6** 输入拥有在执行模式下编辑设备配置的权限的用户的用户名和密码。
- 步骤 7** (可选) 输入密码, 对设备启用执行模式密码, 将允许编辑设备配置。可以点击**显示 (Show)**, 显示已为此设备配置的执行模式密码。
- 步骤 8** 点击页面底部的**提交 (Submit)**。

---

现在, 网络设备已配置为推送 Trustsec 更改。更改思科 ISE 策略后, 点击**推送 (Push)**, 让新配置在网络设备上体现出来。

## SSH 密钥验证

可能想要使用 SSH 密钥增强安全性。思科 ISE 利用其 SSH 密钥验证功能支持此操作。

要使用此功能, 请打开从思科 ISE 到网络设备的 SSHv2 隧道, 然后使用网络设备的 CLI 检索 SSH 密钥。然后, 复制此密钥, 并将其粘贴到思科 ISE 中进行验证。如果 SSH 密钥错误, 思科 ISE 将终止连接。

**限制:** 目前, 思科 ISE 只能验证一个 IP (而不是 IP 范围, 或者 IP 内的子网)

### 开始之前

您将需要:

- 登录凭证
- 检索 SSH 密钥的 CLI 命令

希望思科 ISE 与其安全通信的网络设备。

---

### 步骤 1 在网络设备上:

- a) 登录想要思科 ISE 使用 SSH 密钥验证与其通信的网络设备。
- b) 使用设备的 CLI 显示 SSH 密钥。

#### 示例:

对于 Catalyst 设备, 命令是: `sho ip ssh`。

- c) 复制显示的 SSH 密钥。

### 步骤 2 从思科 ISE 用户界面:

- a) 选择 **设备管理 (Device Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)**, 验证所需网络设备的名称、IP 地址、RADIUS 和 TrustSec 设置是否已正确配置。
- b) 向下滚动至 **TrustSec 高级设置 (Advanced TrustSec Settings)**, 在 **TrustSec 通知和更新 (TrustSec Notifications and Updates)** 部分, 选中**发送配置更改到设备 (Send configuration changes to device)** 复选框, 点击 **CLI (SSH)** 单选按钮。
- c) 在 **SSH 密钥 (SSH Key)** 字段中, 粘贴之前从网络设备检索的 SSH 密钥。



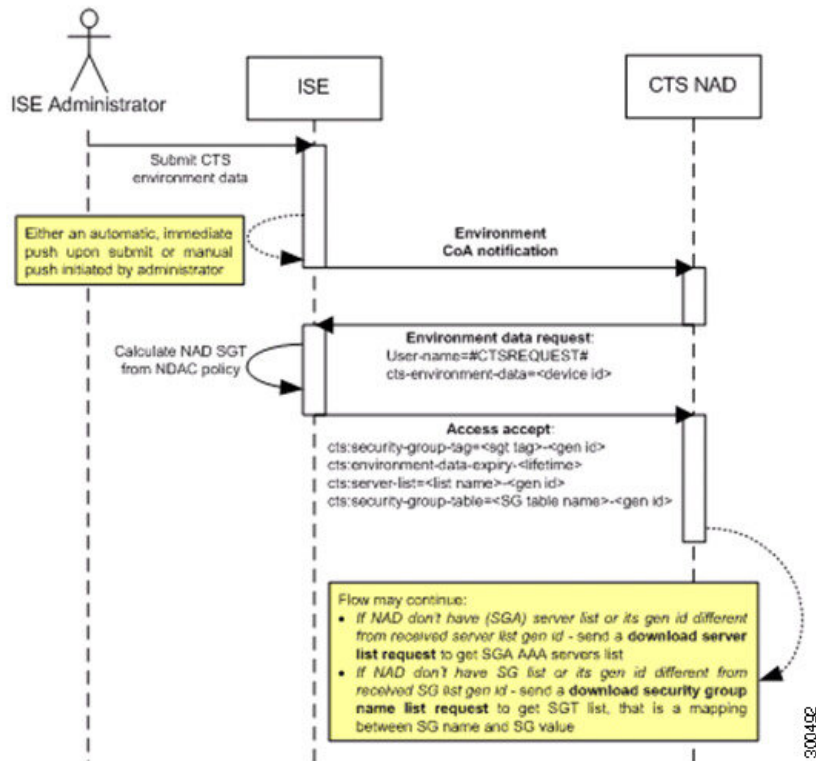
d) 点击页面底部的提交 (Submit)。

现在，网络设备可以使用 SSH 密钥验证与思科 ISE 的通信。

## 环境 CoA 通知流程

下图显示环境 CoA 通知流程。

图 34: 环境 CoA 通知流程



1. 思科 ISE 向 TrustSec 网络设备发送环境 CoA 通知。
2. 设备返回环境数据请求。
3. 思科 ISE 返回以下数据以响应环境数据请求：

发送请求的设备的环境数据 - 这包括 TrustSec 设备的 SGT（根据 NDAC 策略推断）和下载环境 TTL。

TrustSec AAA 服务器列表的名称和生成 ID。

SGT 表（可能有多个）的名称和生成 ID - 这些表列出 SGT 名称和 SGT 值，并且这些表共同提供 SGT 的完整列表。

4. 如果设备不包含 TrustSec AAA 服务器列表，或者生成 ID 与所接收的生成 ID 不同，设备会再发送另一个请求以获取 AAA 服务器列表内容。
5. 如果设备不包含响应中列出的 SGT 表，或生成 ID 不同于所接收的生成 ID，则设备会发送另一个请求以获取该 SGT 表的内容。

## 环境 CoA 触发器

系统可以为以下因素触发环境 CoA：

- 网络设备
- 安全组
- AAA 服务器

### 为网络设备触发环境 CoA

要为网络设备触发环境 CoA，请完成以下步骤：

---

**步骤 1** 选择管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices) 。

**步骤 2** 添加或编辑网络设备。

**步骤 3** 更新 Advanced TrustSec Settings 部分下的 TrustSec Notifications 和 Updates 参数。

只有发生更改的特定 TrustSec 网络设备会收到更改环境属性的通知。

由于只有一个设备受到影响，环境 CoA 通知会在提交后立即发送。所产生的结果是对设备的环境属性进行更新。

---

### 为安全组触发环境 CoA

要为安全组触发环境 CoA，请完成以下步骤。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > TrustSec > 安全组 (Security Groups)。

**步骤 2** 在 Security Group 页面中，更改 SGT 的名称，此操作将更改该 SGT 的映射值的名称。这会触发环境更改。

**步骤 3** 点击 **Push** 按钮，以在更改多个 SGT 的名称后发起环境 CoA 通知。此环境 CoA 通知会转至所有 TrustSec 网络设备并提供已更改的所有 SGT 的更新。

---

### 为 TrustSec AAA 服务器触发环境 CoA

要为 TrustSec AAA 服务触发环境 CoA，请完成以下步骤。

---

**步骤 1** 选择管理 (Administration) > 网络资源 (Network Resources) > TrustSec AAA 服务器 (TrustSec AAA Servers)。

**步骤 2** 在 TrustSec AAA Servers 页面可以创建、删除或更新 TrustSec AAA 服务器的配置。这会触发环境更改。

**步骤 3** 在配置多个 TrustSec AAA 服务器之后，点击 **推送 (Push)** 按钮发起环境 CoA 通知。此环境 CoA 通知将发送到所有 TrustSec 网络设备并提供已更改的所有 TrustSec AAA 服务器的更新。

## 为 NDAC 策略触发环境 CoA

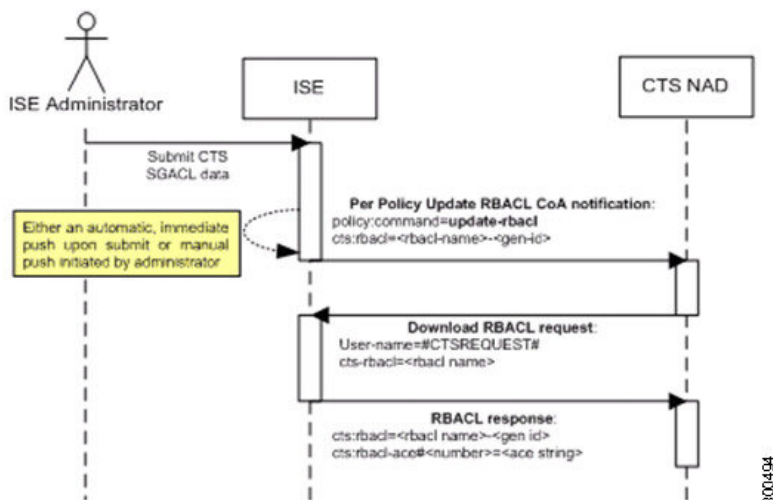
要为 NDAC 策略触发环境 CoA，请完成以下步骤。

您可以点击“NDAC 策略” (NDAC policy) 页面中的 **推送 (Push)** 按钮，发起环境 CoA 通知。此环境 CoA 通知将发送至所有 TrustSec 网络设备并更新网络设备自身 SGT。

## 更新 SGACL 内容流程

下图显示更新 SGACL 内容流程。

图 35: 更新 **SGACL** 内容流程



1. 思科 ISE 将更新 RBACL 命名列表 CoA 通知发送到 TrustSec 网络设备。通知包含 SGACL 名称和生成 ID。
2. 如果满足以下两个条件，设备可能会根据 SGT 数据请求进行重放：
  - 如果 SGACL 是设备所载出口信元的一部分。设备载有一个出口策略数据子集，这些数据是与相邻设备和终端的 SGT 相关的信元（选定目标 SGT 的出口策略列）。
  - CoA 通知中的生成 ID 与设备为此 SGACL 保留的生成 ID 不同。
3. 为了响应 SGACL 数据请求，思科 ISE 会返回 SGACL 的内容 (ACE)。

## 启动更新 SGACL 命名的列表 CoA

要触发更新 SGACL 命名的列表 CoA，请完成以下步骤：

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (results)。

**步骤 2** 从左侧“结果” (Results) 导航窗格，点击 TrustSec 旁边的按钮，然后点击安全组 ACL (Security Group ACLs)。

**步骤 3** 更改 SGACL 的内容。在您提交 SGACL 后，它会提高 SGACL 的生成 ID。

**步骤 4** 点击推送 (Push) 按钮以在您更改多个 SGACL 的内容之后发起更新 SGACL 命名的列表 CoA 通知。此通知将发送至所有 TrustSec 网络设备，并且在相关设备上提供该 SGACL 内容的更新。

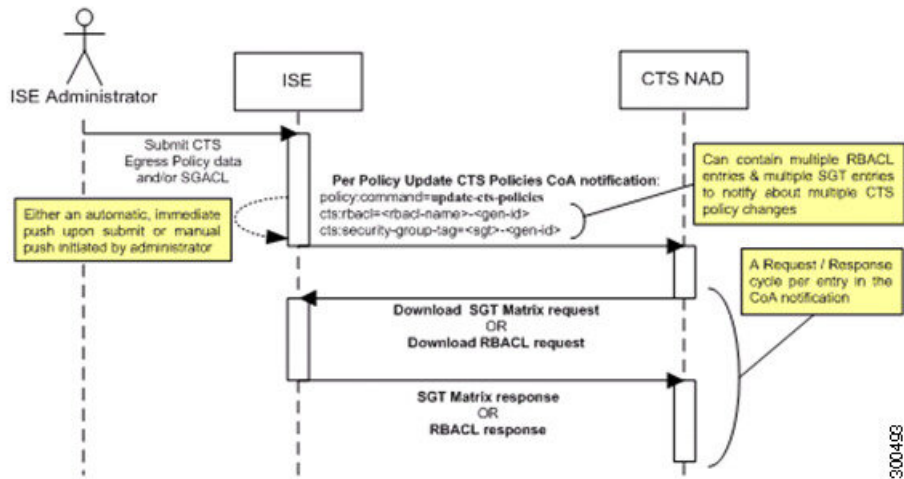
更改 SGACL 的名称或 IP 版本不会更改其生成 ID；因此不需要发送更新 RBACL 命名的列表 CoA 通知。

但是，如果更改出口策略中当前使用的 SGACL 的名称或 IP 版本，则会相应地更改包含该 SGACL 的单元格，并且这会更改该单元格目标 SGT 的生成 ID。

## 策略更新 CoA 通知流程

下图显示了策略 CoA 通知流程。

图 36: 策略 CoA 通知流程

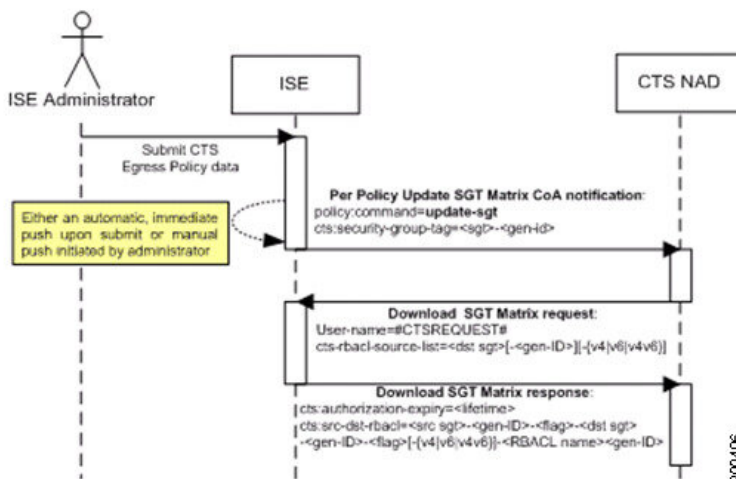


1. 思科 ISE 向 TrustSec 网络设备发送更新策略 CoA 通知。通知可以包含多个 SGACL 名称及其生成 ID，以及多个 SGT 值及其生成 ID。
2. 设备可能重放多个 SGACL 数据请求和/或多个 SGT 数据。
3. 作为对 SGACL 数据请求或 SGT 数据请求的响应，思科 ISE 返回相关数据。

## 更新 SGT 矩阵 CoA 流程

下图显示了更新 SGT 矩阵 CoA 的流程。

图 37: 更新 SGT 矩阵 CoA 流程



1. 思科 ISE 将更新的 SGT 矩阵 CoA 通知发送到 TrustSec 网络设备。通知包含 SGT 值和生成 ID。
2. 如果满足以下两个条件，设备可以重放 SGT 数据请求：
  - 如果 SGT 是毗邻设备或终端的 SGT，设备将下载并保留与毗邻设备和终端的 SGT（目标 SGT）相关的信元。
  - CoA 通知中的生成 ID 不同于设备为 SGT 保留的生成 ID。
3. 作为对 SGT 数据请求的响应，思科 ISE 返回所有出口信元的数据，例如源 SGT 和目标 SGT、信元状态以及在此信元中配置的 SGACL 名称的顺序列表。

### 发起从出口策略更新 SGT 矩阵 CoA

步骤 1 选择策略 (Policy) > TrustSec > 出口策略 (Egress Policy)。

步骤 2 在“出口策略”(Egress Policy) 页面，更改单元格的内容（状态、SGACL）。

步骤 3 在提交更改后，系统会提高该单元格目标 SGT 的生成 ID。

步骤 4 点击推送 (Push) 按钮以在您更改多个出口单元格的内容之后发起更新 SGACL 命名的列表 CoA 通知。此通知将发送至所有 TrustSec 网络设备，并且在相关设备上提供该单元格内容的更新。

## TrustSec CoA 摘要

下表汇总了可能要求发起 TrustSec CoA 的各种场景、每个场景中使用的 CoA 的类型以及相关 UI 页面。

表 96: TrustSec CoA 摘要

UI 页面	触发 CoA 的操作	触发方式	CoA 类型	发送到
Network Device	更改页面的 TrustSec 部分中的环境 TTL	在成功提交 TrustSec 网络设备后	环境	特定网络设备
TrustSec AAA Server	TrustSec AAA 服务器中的任何更改（创建、更新、删除、重新排序）	可以通过点击 TrustSec AAA 服务器列表页面中的 Push 按钮推送累积更改。	环境	所有 TrustSec 网络设备
Security Group	SGT 中的任何更改（创建、重命名、删除）	可以通过点击 SGT 列表页面中的 Push 按钮推送累积更改。	环境	所有 TrustSec 网络设备
NDAC Policy	NDAC 策略中的任何更改（创建、更新、删除）	可以通过点击 NDAC 策略页面中的 Push 按钮推送累积更改。	环境	所有 TrustSec 网络设备
SGACL	更改 SGACL ACE	可以通过点击 SGACL 列表页面中的 Push 按钮推送累积更改。	更新 RBACL 命名列表	所有 TrustSec 网络设备
	更改 SGACL 名称或 IP 版本	可以通过点击 SGACL 列表页面中的 Push 按钮或 Egress 表中的 Policy Push 按钮推送累积更改。	更新 SGT 矩阵	所有 TrustSec 网络设备
Egress Policy	用于更改 SGT 的生成 ID 的操作。	可以通过点击 Egress Policy 页面中的 Push 按钮推送累积更改。	更新 SGT 矩阵	所有 TrustSec 网络设备

## 按用户报告运行前 N 个 RBACL 丢包

可以按用户报告运行前 N 个 RBACL 丢包，以便按特定用户查看策略违规（基于丢包）。

---

**步骤 1** 从思科 ISE Admin 控制面板选择 **Operations > Reports > ISE Reports > TrustSec**。

**步骤 2** 点击 **Top N RBACL Drops by User**。

**步骤 3** 从 **Filters** 下拉菜单中添加所需的监控模式。

**步骤 4** 相应地输入选定参数的值。可以从 **Enforcement mode** 下拉列表中将模式指定为 **Enforce**、**Monitor** 或 **Both**。

**步骤 5** 从 **Time Range** 下拉菜单中选择将收集报告数据的时间段。

**步骤 6** 点击 **运行 (Run)** 在特定时间段内运行报告，以及选定的参数。

---







## 第 13 章

# 合规性

- 终端安全评估类型，第 610 页
- 安全评估管理设置，第 611 页
- 安全评估常规设置，第 616 页
- 将安全评估更新下载至思科 ISE，第 617 页
- 安全评估可接受使用政策配置设置，第 619 页
- 配置安全评估的可接受使用政策，第 621 页
- 安全评估条件，第 621 页
- Inline Posture 节点，第 625 页
- 合规性模块，第 626 页
- 检查安全评估合规性，第 628 页
- 创建补丁管理条件，第 628 页
- 创建磁盘加密条件，第 629 页
- 安全评估条件设置，第 629 页
- 配置安全评估策略，第 636 页
- 配置 AnyConnect 工作流程，第 637 页
- 客户端安全评估，第 638 页
- 终端安全状态评估选项，第 639 页
- 安全评估补救选项，第 639 页
- 安全评估的自定义条件，第 639 页
- 自定义安全评估补救措施，第 639 页
- 终端安全评估要求，第 642 页
- 重新进行安全评估配置设置，第 645 页
- 自定义安全评估权限，第 646 页
- 配置标准授权策略，第 647 页
- 安全评估故障排除工具，第 647 页
- 在思科 ISE 中配置客户端调配，第 647 页
- 客户端调配资源，第 648 页
- 创建本地请求者配置文件，第 651 页
- 思科 AnyConnect 安全移动，第 653 页

- [思科 Web 代理](#)，第 658 页
- [配置客户端调配资源策略](#)，第 674 页
- [客户端调配报告](#)，第 676 页
- [客户端调配事件日志](#)，第 676 页
- [客户端调配门户语言文件的 HTML 支持](#)，第 677 页

## 终端安全评估类型

以下终端安全评估代理可监控和实施思科 ISE 终端安全评估策略：

- **AnyConnect**：部署 AnyConnect 代理以监控和实施需要客户端交互的思科 ISE 策略。AnyConnect 代理留在客户端上。有关在思科 ISE 中使用 AnyConnect 的详细信息，请参阅 [思科 AnyConnect 安全移动](#)，第 653 页。

- **AnyConnect Stealth**：作为服务运行终端安全评估，没有用户界面。代理留在客户端上。

当在终端安全评估要求中选择 AnyConnect Stealth 终端安全评估类型时，某些条件、补救或条件中的属性会被禁用（显示为灰色）。例如，当启用 AnyConnect 要求时，手动补救类型会被禁用（显示为灰色），因为此操作需要客户端交互。

当您将姿势配置文件映射到 AnyConnect 配置，然后将 AnyConnect 配置映射到用于 AnyConnect Stealth 模式部署的客户端配置窗口时：

- AnyConnect 可以读取终端安全评估配置文件并将其设置为目标模式。
- AnyConnect 可以在初始终端安全评估请求期间将与所选模式的相关信息发送到思科 ISE。
- 思科 ISE 可以根据模式和其他因素匹配正确的策略，如身份组、操作系统和合规性模块。



---

**注释** AnyConnect Stealth 模式需要 AnyConnect 4.4 及更高版本。

---

有关在思科 ISE 中配置 AnyConnect Stealth 的详细信息，请参阅 [配置 AnyConnect 无客户端模式工作流程](#)。

- **临时代理**：当客户端尝试访问受信任网络时，思科 ISE 会打开“客户端调配” (Client Provisioning) 门户。门户会指示用户下载并安装代理，然后运行代理。临时代理会检查合规性状态，并将状态发送到思科 ISE。思科 ISE 会根据结果采取行动。在合规性处理完成后，临时代理会将自身从客户端中删除。临时代理不支持自定义补救。默认补救仅支持消息文本。

临时代理不支持以下条件：

- 服务条件 macOS - 系统后台守护程序检查
- 服务条件 macOS - 后台守护程序或用户代理检查
- PM - 最新检查
- PM - 已启用检查

- DE - 加密检查
- 使用终端安全评估类型 (Posture Types) 临时代理 (Temporal Agent) 和合规性模块 (Compliance Module) 4.x 或更高版本 (4.x or later) 配置终端安全评估策略。请勿将合规性模块配置为 3.x 或更低版本或任何版本。
- 对于临时代理，只能在要求 (Requirements) 窗口中查看包含安装 (Installation) 检查类型的补丁管理条件。
- 思科 ISE 不支持使用 macOS 临时代理的 VLAN 控制终端安全评估。当您将网络访问从现有 VLAN 更改为新 VLAN 时，用户的 IP 地址会在 VLAN 更改之前释放。当用户连接到新 VLAN 时，客户端通过 DHCP 获取新 IP 地址。识别新 IP 地址需要根权限，但临时代理作为用户进程运行。
- 思科 ISE 支持 ACL 控制的终端安全评估环境，后者不需要刷新终端 IP 地址。
- 有关在思科 ISE 中配置临时代理的详细信息，请参阅[配置思科临时代理工作流程](#)。

您可以在“客户端调配”窗口中选择终端安全评估类型 (Policy > Policy Elements > Results > Client Provisioning > Resources) and the Posture Requirements window (Policy > Policy Elements > Results > Posture > Requirements)。最佳实践是在“客户端调配” (Client Provisioning) 窗口中调配终端安全评估配置文件。

#### 相关主题

- [配置 AnyConnect 无客户端模式工作流程](#)
- [配置思科临时代理工作流程](#)

## 安全评估管理设置

您可以从全局为 Admin 门户配置安全评估服务。您可以从思科通过 Web 将更新自动下载至思科 ISE 服务器。之后您还可以离线手动更新思科 ISE。此外，如果已在客户端上安装 AnyConnect、NAC 代理或 Web 代理之类的代理，则可以为客户端提供终端安全评估和补救服务。客户端代理定期向思科 ISE 更新客户端的合规性状态。登录并成功完成安全状态要求评估之后，客户端代理显示带有一个链接的对话框，要求最终用户遵守网络使用的条款和条件。您可以使用此链接为您的企业网络定义最终用户在访问您的网络之前必须接受的网络使用信息。

## 客户端安全评估要求

要创建终端安全评估要求，请执行以下操作：

1. 依次选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture) > 要求 (Requirements)。
2. 从任何要求行末尾处的编辑 (Edit) 下拉列表中，选择插入新要求 (Insert New Requirement)。
3. 输入所需的详细信息，并点击完成 (Done)。

下表介绍客户端终端安全评估要求 (Client Posture Requirements) 窗口中的字段。

表 97: Posture Requirement

#### 相关主题

[配置安全评估的可接受使用政策](#)，第 621 页

[创建客户端安全评估要求](#)，第 644 页

## 客户端的计时器设置

您可以为用户设置计时器，用于进行补救、从一个状态过渡到另一个状态，以及控制登录成功屏幕。

但是，当没有任何配置为与客户端调配策略相匹配的代理配置文件时，您可以使用常规设置 (General Settings) 配置窗口中的设置 (管理 (Administration) > 系统 (System) > 设置 (Settings) > 终端安全评估 (Posture) > 常规设置 (General Settings))。

### 设定补救计时器，使客户端在指定时间内补救

您可以配置计时器，使客户端在指定时间内补救。在初始评估期间，客户端不符合配置的终端安全评估策略，代理将等待客户端在补救计时器中配置的时间内补救。如果客户端无法在指定时间内补救，则客户端代理将向终端安全评估运行服务发送报告，然后，客户端过渡到不合规状态。

---

**步骤 1** 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 终端安全评估 (Posture) > 常规设置 (General Settings)。

**步骤 2** 在补救计时器 (Remediation Timer) 字段中，以分钟为单位输入时间值。

默认值为 4 分钟。有效范围为 1 至 300 分钟。

**步骤 3** 点击保存 (Save)。

---

### 设置网络转换延迟计时器，使客户端实现转换

可以为客户端配置计时器，使客户端在指定的时间内，使用网络过渡延迟计时器从一种状态过渡到另一种状态，这是完成授权更改 (CoA) 所必需的操作。当客户端在终端安全评估成功和失败期间需要获得新的 VLAN IP 地址时，可能需要更长的延迟时间。终端安全评估成功时，思科 ISE 允许客户端在使用网络过渡延迟计时器指定的时间内从未知模式过渡为合规模式。终端安全评估失败时，思科 ISE 允许客户端在计时器指定的时间内从未知模式过渡为非合规模式。

---

**步骤 1** 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 终端安全评估 (Posture) > 常规设置 (General Settings)。

**步骤 2** 以秒为单位，在 Network Transition Delay 字段中输入时间值。

默认值为 3 秒。有效范围为 2 至 30 秒。

步骤 3 点击保存 (Save)。

---

## 将登录成功窗口设置为自动关闭

成功完成安全状态评估之后，客户端代理会显示一个临时网络访问屏幕。用户需要点击登录窗口中的确定 (OK) 按钮将其关闭。您可以设置计时器以在指定时间之后自动关闭此登录屏幕。

步骤 1 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 终端安全评估 (Posture) > 常规设置 (General Settings)。

步骤 2 选中 **Automatically Close Login Success Screen After** 复选框。

步骤 3 在 **Automatically Close Login Success Screen After** 复选框旁边的字段中以秒为单位输入时间值。

有效范围为 0 至 300 秒。如果时间设置为零，则 AnyConnect 不显示登录成功界面。

步骤 4 点击保存 (Save)。

---

## 设置非代理设备的终端安全评估状态

您可以配置在非代理设备上运行的终端的安全评估状态。当 Android 设备和 Apple 设备（如 iPod、iPhone 或 iPad）连接到支持思科 ISE 的网络时，这些设备采用默认安全评估状态设置。

安全评估运行期间找不到匹配的客户端调配策略时，还可以将这些设置应用到在 Windows 和 MacOS 操作系统中运行的终端，同时将终端重定向到客户端调配门户。

### 开始之前

要在一个终端上强制实施策略，必须配置相应的客户端调配策略（代理安装包）。否则，该终端的安全评估状态会自动反映默认设置。

步骤 1 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 终端安全评估 (Posture) > 常规设置 (General Settings)。

步骤 2 从默认终端安全评估 (Default Posture Status) 下拉列表中，选择合规 (Compliant) 或不合规 (Noncompliant) 选项。

步骤 3 点击保存 (Save)。

---

## 安全评估租约

您可以将思科 ISE 配置为在每次用户登录您的网络时执行安全评估或按指定的间隔执行安全评估。有效范围为 1 至 365 天。

此配置仅适用于使用 AnyConnect 代理进行安全评估的用户。

当终端安全评估租约处于活动状态时，思科 ISE 将使用上次已知的终端安全评估状态，并且不会连接到终端以检查合规性。但是，当终端安全评估租约到期时，思科 ISE 不会自动触发终端的重新身份验证或终端安全评估。因为正在使用相同的会话，所以终端将保持相同的合规性状态。当终端重新进行身份验证时，将运行终端安全评估，并重置终端安全评估租用时间。

使用案例场景示例：

- 用户登录终端，使其终端安全评估符合设置为一天的终端安全评估租约。
- 四小时后，用户从终端注销（终端安全评估租约现在还剩 20 小时）。
- 一小时后，用户再次登录。现在，终端安全评估租约还剩 19 小时。最后已知的终端安全评估状态为合规。因此为用户提供访问权限，无需在终端上运行终端安全评估。
- 四小时后，用户注销（终端安全评估租约现在还剩 15 小时）。
- 14 小时后，用户登录。终端安全评估租约还剩一个小时。最后已知的终端安全评估状态为合规。系统会为用户提供访问权限，无需在终端上运行终端安全评估。
- 一小时后，终端安全评估租约到期。用户仍连接到网络，因为正在使用同一用户会话。
- 一小时后，用户注销（会话与用户绑定，但不与计算机绑定，因此计算机可以留在网络上）。
- 一小时后，用户登录。由于终端安全评估租约已到期且已启动新的用户会话，因此计算机会执行终端安全评估，结果会发送到思科 ISE，在此使用案例中，终端安全评估租约计时器会重置为一天。

## 定期重新评估

只有成功完成合规性安全评估的客户端才可以执行定期重新评估 (PRA)。如果您网络上的客户端不合规，则不会执行 PRA。

只有在终端处于合规状态下，PRA 才有效和适用。策略服务节点检查相关策略，根据配置中定义的客户端角色编制实施 PRA 的要求。如果找到 PRA 配置匹配项，策略服务节点在发出 CoA 请求之前会用 PRA 配置中为客户端定义的 PRA 属性对客户端代理做出响应。客户端代理根据配置中指定的间隔定期发送 PRA 请求。如果 PRA 成功或继续执行 PRA 配置中配置的操作，客户端会保持合规状态。如果客户端未能满足 PRA 要求，则客户端会从合规状态变为不合规状态。

即使是安全评估状态重新评估请求，PostureStatus 属性也会在 PRA 请求中将当前安全状态显示为合规状态而不是未知状态。监控报告中也会更新 PostureStatus。

当终端安全评估租约未到期时，终端根据访问控制列表 (ACL) 变为合规，并启动 PRA。如果 PRA 失败，终端视为不合规，并重置终端安全评估租约。



**注释** 在 PSN 故障切换期间，不支持 PRA。PSN 故障切换后，您必须在客户端上启用重新扫描或启用终端安全评估。

## 配置定期重新评估

您可以配置仅定期重新评估已成功通过合规性安全状态评估的客户端。您可以为系统中定义的用户身份组配置各项 PRA。

### 开始之前

- 确保每个定期重新评估 (PRA) 配置都有分配给该配置的唯一组或用户身份组的唯一组合。
- 您可以分配 `role_test_1` 和 `role_test_2`，这是 PRA 配置独有的两个角色。您可以使用逻辑运算符组合这两个角色并将 PRA 配置分配为两个角色的唯一组合。例如，`role_test_1 OR role_test_2`。
- 确保两个 PRA 配置没有相同的用户身份组。
- 如果已有用户身份组为任何 (*Any*) 的 PRA 配置，您就无法创建其他 PRA 配置，除非您执行以下操作之一：
  - 用 Any 用户组更新现有 PRA 配置以反映 *Any* 之外的用户身份组。
  - 删除 “Any” 用户身份组的现有 PRA 配置。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 终端安全评估 (Posture) > 重新评估 (Reassessments)。

**步骤 2** 点击添加 (Add)。

**步骤 3** 修改新重新评估配置 (New Reassessment Configuration) 窗口中的值以创建新 PRA。

**步骤 4** 点击 **Submit** 以创建 PRA 配置。

## 安全评估故障排除设置

下表介绍“终端安全评估故障排除” (Posture troubleshooting) 窗口上的字段，您可以使用该窗口查找并解决网络中的终端安全评估问题。此窗口的导航路径为：操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > 终端安全状态故障排除 (Posture Troubleshooting)。

表 98: 终端安全评估故障排除设置

字段名称	使用指南
搜索并选择一个需要进行故障排除的安全评估事件	
用户名	输入要过滤的用户名。
MAC 地址	输入要过滤的 MAC 地址，请使用格式：xx-xx-xx-xx-xx-xx
Posture Status	选择要过滤的身份验证状态：

字段名称	使用指南
<b>Failure Reason</b>	输入故障原因，或者点击 <b>Select</b> 以从列表中选择故障原因。点击 <b>Clear</b> 以清除故障原因。
<b>Time Range</b>	选择时间范围。使用在此时间范围内创建的 RADIUS 身份验证记录。
<b>Start Date-Time:</b>	(仅当您选择自定义时间范围时可用) 输入开始日期和时间，或点击日历图标选择开始日期和时间。日期应为 <i>mm/dd/yyyy</i> 格式，而时间应为 <i>hh:mm</i> 格式。
<b>End Date-Time:</b>	(仅当您选择自定义时间范围时可用) 输入结束日期和时间，或点击日历图标选择结束日期和时间。日期应为 <i>mm/dd/yyyy</i> 格式，而时间应为 <i>hh:mm</i> 格式。
<b>Fetch Number of Records</b>	选择要显示的记录数：10、20、50、100、200、500
搜索结果	
时间	事件时间
状态	终端安全评估状态
用户名	与事件关联的用户名
MAC 地址	系统的 MAC 地址
<b>Failure Reason</b>	事件的失败原因

#### 相关主题

[安全评估故障排除工具](#)，第 647 页

## 安全评估常规设置

这些设置是终端安全评估的默认设置，可被终端安全评估配置文件覆盖。

#### 常规终端安全评估设置

- **补救计时器 (Remediation Timer):** 输入开始补救前等待的时间。默认值为 4 分钟。有效范围为 1 至 300 分钟。
- **网络过渡延迟 (Network Transition Delay):** 以秒为单位输入时间值。默认值为 3 秒。有效范围为 2 至 30 秒。
- **默认终端安全评估状态 (Default Posture Status):** 选择合规 (**Compliant**) 或不合规 (**Noncompliant**)。在连接到网络时，非代理设备会处于此状态。
- **自动关闭登录成功屏幕前等待 (Automatically Close Login Success Screen After):** 选中此复选框可在指定的时间过后自动关闭成功登录屏幕。可以配置计时器以自动关闭登录屏幕。有效范围为 0 至 300 秒。如果将时间设置为零，则客户端上的代理不会显示成功登录屏幕。



### 安全评估租约

- 每当用户连接到网络时执行终端安全评估 (**Perform posture assessment every time a user connects to the network**): 选择此选项可在用户每次连接网络时启动终端安全评估
- 每 **n** 天执行一次终端安全评估 (**Perform posture assessment every n days**): 选择此选项可在指定天数过后启动终端安全评估, 即使客户端的状态已评估为“合规”也是如此。

### 相关主题

[安全评估服务](#)

[安全评估管理设置](#), 第 611 页

[安全评估租约](#), 第 613 页

[在思科 ISE 中启用安全评估会话服务](#)

[设定补救计时器, 使客户端在指定时间内补救](#), 第 612 页

[设置网络转换延迟计时器, 使客户端实现转换](#), 第 612 页

[将登录成功窗口设置为自动关闭](#), 第 613 页

[设置非代理设备的终端安全评估状态](#), 第 613 页

## 将安全评估更新下载至思科 ISE

安全评估更新包括针对适用于 Windows 和 MacOS 操作系统的防病毒和反间谍软件的一系列预定义的检查、规则和支持图表, 以及思科支持的操作系统信息。您还可以从您包含最新更新档案的本地系统上的文件离线更新思科 ISE。

当您首次在您的网络上部署思科 ISE 时, 您可以从 Web 下载安全评估更新。此过程通常大约需要 20 分钟。初次下载后, 您可以将思科 ISE 配置为自动验证和下载增量更新。

在初始安全评估更新期间, 思科 ISE 仅创建一次默认安全评估策略、要求和补救。如果您删除所创建的这些内容, 在后续手动或计划更新期间思科 ISE 不会再进行创建。

### 开始之前

要确保能够访问合适的远程位置以便将安全评估资源下载至思科 ISE, 您可能需要验证您已按照“在思科 ISE 中指定代理设置”的说明为您的网络配置了正确的代理设置。

您可以使用“安全评估更新”(Posture Update) 窗口从 Web 动态下载更新。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 安全评估 (Posture) > 更新 (Updates)。

**步骤 2** 选择 Web 选项以动态地下载更新。

**步骤 3** 点击设置为默认值 (Set to Default) 为更新源 URL (Update Feed URL) 字段设置思科默认值。

如果您的网络限制 URL 重定向功能 (例如通过代理服务器) 而且您在访问上述 URL 时遇到了问题, 请尝试将您的思科 ISE 也指向相关主题中的备选 URL。

**步骤 4** 在安全评估更新 (Posture Updates) 窗口更改相应值。

**步骤 5** 点击现在更新 (Update Now) 以从思科下载更新。

更新后，“安全评估更新” (Posture Updates) 窗口显示当前思科更新版本信息，作为对“安全评估更新” (Posture Updates) 窗口“更新信息” (Update Information) 部分下的更新的验证。

步骤 6 点击 **Yes** 以继续操作。

---

## 思科 ISE 离线更新

当从思科 ISE 设备通过互联网直接访问 Cisco.com 不可用或者安全策略不允许时，您可以使用离线更新选项来下载客户端调配和安全状态安全评估更新。

要下载离线客户端调配资源：

---

步骤 1 前往：。

步骤 2 提供登录凭证。

步骤 3 导航至 Cisco 身份识别服务引擎下载窗口，然后选择版本。

以下离线安装程序包可供下载：

- **win\_spw-<version>-isebundle.zip** — 适用于 Windows 的离线 SPW 安装程序包
- **mac-spw-<version>.zip** — 适用于 Mac OS X 的离线 SPW 安装程序包
- **compliancemodule-<version>-isebundle.zip** — 离线合规性模块安装程序包
- **macagent-<version>-isebundle.zip** — 离线 Mac 代理安装程序包
- **webagent-<version>-isebundle.zip** — 离线 Web 代理安装程序包

步骤 4 单击下载 (Download) 或加入购物车 (Add to Cart)。

---

有关将下载的安装程序包添加至思科 ISE 的详细信息，请参阅《思科身份服务引擎管理员指南》中的“从本地计算机添加客户端调配资源”一节。

您可以使用安全状态安全评估更新，以离线方式通过本地系统上的存档为 Windows 和 Mac 操作系统更新检查、操作系统信息以及防病毒和反间谍软件支持图表。

要进行离线更新，请确保存档文件版本与配置文件中的版本一致。您可以在配置思科 ISE 后并且想要为状态策略服务启用动态更新时使用离线状态更新。

要下载离线安全状态安全评估更新：

---

步骤 1 转至<https://www.cisco.com/web/secure/spa/posture-offline.html>。

步骤 2 将 **posture-offline.zip** 文件保存到本地系统。此文件用于为 Windows 和 Mac 操作系统更新操作系统信息、检查、规则以及防病毒和反间谍软件支持图表。

步骤 3 启动思科 ISE 管理员用户界面，并选择 **Administration > System > Settings > Posture**。

**步骤 4** 点击箭头查看安全状态安全评估的设置。

**步骤 5** 单击更新 (Update)。

将显示终端安全评估更新 (Posture Updates) 窗口。

**步骤 6** 单击离线 (Offline) 选项。

**步骤 7** 单击浏览 (Browse) 可从您系统中的本地文件夹查找存档文件 (posture-offline.zip)。

**注释** 待更新文件 (File to Update) 字段为必填。您可以选择包含适当文件的单个存档文件 (.zip)。不支持 .zip 之外的其他存档文件，例如 .tar 和 .gz。

**步骤 8** 单击立即更新 (Update Now)。

## 自动下载安全评估更新

在初始更新后，您可以将思科 ISE 配置为检查更新并自动下载这些更新。

开始之前

- 您起初应已下载安全评估更新来将思科 ISE 配置为检查更新并自动下载这些更新。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 安全评估 (Posture) > 更新 (Updates)。

**步骤 2** 在终端安全评估更新 (Posture Updates) 窗口中，选中从初始延迟开始自动检查更新 (Automatically check for updates starting from initial delay) 复选框。

**步骤 3** 以 hh:mm:ss 格式输入初始延迟时间。

思科 ISE 在初始延迟时间结束后开始检查更新。

**步骤 4** 输入时间间隔（以小时为单位）。

思科 ISE 从初始延迟时间起按指定间隔将更新下载到部署。

**步骤 5** 单击保存 (Save)。

## 安全评估可接受使用政策配置设置

表 99: 安全评估 AUP 配置设置

字段名称	使用指南
<b>Configuration Name</b>	输入要创建的 AUP 配置的名称。
<b>Configuration Description</b>	输入要创建的 AUP 配置的说明。

字段名称	使用指南
<b>“向代理用户显示 AUP” (Show AUP to Agent users)</b> (仅适用于 Windows)	选中后，系统会在身份验证和终端安全评估成功后，向用户显示您的网络的网络使用条款和条件的链接。
<b>为 AUP 消息使用 URL (Use URL for AUP message)</b>	选中后，必须在“AUP URL”字段中输入 AUP 消息的 URL。
<b>为 AUP 消息使用文件 (Use file for AUP message)</b>	选中后，必须浏览至文件位置并以压缩格式上传文件。此文件必须在顶层包含 index.html。 除 index.html 文件以外，该 .zip 文件还可包含其他文件和子目录。这些文件可以使用 HTML 标签相互引用。
<b>AUP URL</b>	输入 AUP 的 URL，用户必须在身份验证和安全评估成功后访问该 URL。
<b>AUP File</b>	浏览至文件并将其上传到思科 ISE 服务器。它应是压缩文件，并且应在顶层包含 index.html 文件。
<b>Select User Identity Groups</b>	针对 AUP 配置选择唯一用户身份组或用户身份组的唯一组合。 创建 AUP 配置时，请注意以下事项： <ul style="list-style-type: none"> <li>• 安全评估 AUP 不适用于访客流程</li> <li>• 两个配置不会共同具有任何用户身份组</li> <li>• 如果您要使用用户身份组“Any”创建 AUP 配置，则要先删除所有其他 AUP 配置</li> <li>• 如果使用用户身份组“Any”创建 AUP 配置，则无法使用唯一用户身份组或用户身份组的唯一组合创建其他 AUP 配置。要使用除 Any 以外的用户身份组创建 AUP 配置，请先删除具有用户身份组“Any”的现有 AUP 配置，或者使用唯一用户身份组或用户身份组的唯一组合更新具有用户身份组“Any”的现有 AUP 配置。</li> </ul>
<b>Acceptable use policy configurations - Configurations list</b>	列出现有 AUP 配置以及与 AUP 配置关联的最终用户身份组。

#### 相关主题

[安全评估服务](#)

[配置安全评估的可接受使用政策](#)，第 621 页

## 配置安全评估的可接受使用政策

登录并对客户端成功完成安全状态评估之后，客户端代理会显示一个临时网络访问屏幕。此屏幕包含可接受使用政策 (AUP) 的链接。当用户点击此链接时，系统会将用户重定向至显示网络使用条款和条件的页面，用户必须阅读并理解这些条款和条件。

每个可接受使用政策配置都必须具有唯一的用户身份组或唯一的用户身份组组合。思科 ISE 找到第一个匹配的用户身份组，然后与显示 AUP 的客户端代理通信。

---

**步骤 1** 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 终端安全评估 (Posture) > 可接受使用政策 (Acceptable Use Policy)。

**步骤 2** 点击添加 (Add)。

**步骤 3** 修改新可接受使用政策配置 (New Acceptable Use Policy Configuration) 窗口中的值。

**步骤 4** 点击提交。

---

## 安全评估条件

安全评估条件可以是以下任何一个简单条件：文件、注册表、应用、服务或字典条件。这些简单条件中的一个或多个条件构成可与安全评估要求相关联的复合条件。

当您首次在您的网络上部署思科 ISE 时，您可以从 Web 下载安全评估更新。此过程称为初始安全评估更新。

在初始安全评估更新后，思科 ISE 还会创建思科定义的简单条件与复合条件。思科定义的简单条件以 `pc_` 作为前缀，复合条件以 `pr_` 作为前缀。

您也可以将思科 ISE 配置为由于通过 Web 进行动态安全评估更新而定期下载思科定义的条件。您不能删除或编辑思科定义的安全评估条件。

用户定义的条件或思科定义的条件同时包含简单条件与复合条件。

## 简单安全评估条件

您可以使用安全评估导航 (Posture Navigation) 窗格管理以下简单条件：

- 文件条件：在客户端上检查文件的存在性、文件的日期以及文件的版本的条件。
- 注册条件：在客户端上检查注册表项的存在性或注册表项的值的条件。
- 应用条件：在客户端上检查应用（进程）是否在运行的条件。



**注释** 如果进程已安装并正在运行，则用户合规。但是，应用条件的逻辑正好相反；如果应用未安装且未运行，则最终用户合规。如果应用已安装并正在运行，则最终用户不合规。

- 服务条件：检查服务是否在客户端上运行的条件。
- 词典条件：检查带某个值的词典属性的条件。
- 

## 创建简单安全评估条件

可以创建文件、注册表、应用、服务和字典简单条件，在终端安全评估策略或其他复合条件中可以使用这些条件。

### 开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 终端安全评估 (Posture)。

**步骤 2** 选择以下任意一项：文件 (File)、注册表 (Registry)、应用 (Application)、服务 (Service) 或字典简单条件 (Dictionary Simple Condition)。

**步骤 3** 点击添加 (Add)。

**步骤 4** 在字段中输入适当的值。

**步骤 5** 点击提交。

## 复合安全评估条件

复合条件由一个或多个简单条件或复合条件组成。您可以利用以下复合条件定义安全评估策略。

- 复合条件：包含一个或多个简单条件或文件、注册表、应用或服务条件类型的复合条件
- 防病毒复合条件：包含一个或多个 AV 条件或 AV 复合条件
- 反间谍软件复合条件：包含一个或多个 AS 条件或 AS 复合条件
- 字典复合条件：包含一个或多个字典简单条件或字典复合条件
- 

## 创建复合安全评估条件

您可以创建复合条件用于安全评估和验证的状态策略。

### 开始之前

要执行以下任务，您必须是超级管理员或策略管理员。

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 终端安全评估 (Posture) > 复合条件 (Compound Conditions) > 添加 (Add)。

**步骤 2** 输入适当的字段值。

**步骤 3** 点击 **Validate Expression** 验证条件。

**步骤 4** 点击提交。

## 字典复合条件设置

下表介绍字典复合条件 (Dictionary Compound Conditions) 窗口中的字段。此窗口的导航路径为：策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 终端评估状态 (Posture) > 词典复合条件 (Dictionary Compound Condition)。

表 100: 字典复合条件设置

字段名称	使用指南
<b>Name</b>	输入要创建的字典复合条件的名称。
<b>Description</b>	输入要创建的字典复合条件的说明。
<b>Select Existing Condition from Library</b>	通过从策略要素库选择预定义的条件来定义表达式，或在后续步骤中将临时属性/值对添加到表达式中。
<b>Condition Name</b>	选择已从策略要素库中创建的字典简单条件。
<b>Expression</b>	Expression 会根据从 Condition Name 下拉列表选择的选项进行更新。

字段名称	使用指南
<b>AND 或 OR 运算符</b>	<p>选择 AND 或 OR 运算符可逻辑组合可从策略要素库添加的字典简单条件。</p> <p>点击 <b>Action</b> 图标可执行以下操作：</p> <ul style="list-style-type: none"> <li>• Add Attribute/Value</li> <li>• Add Condition from Library</li> <li>• Delete</li> </ul> <p>思科 ISE 将按顺序处理复合条件中的每个 OR 条件。例如，如果复合条件检查 A OR B，思科 ISE 会首先检查 A，然后检查 B。如果条件 A 或 B 均通过，则整体结果标记为通过。</p> <p>如果条件 A 失败，条件 B 成功，则整体结果标记为通过。在这种情况下，在安全评估报告中，条件 A 标记为失败，条件 B 为通过。</p> <p>如果条件 A 成功，思科 ISE 将跳过条件 B 并将整体结果标记为通过。在安全评估报告中，条件 A 标记为通过，条件 B 标记为已跳过，总体结果为通过。</p>
<b>Create New Condition (Advance Option)</b>	<p>从各种系统或用户定义的字典中选择属性。</p> <p>还可以在后续步骤中从策略要素库中添加预定义条件。</p>
<b>Condition Name</b>	选择已创建的字典简单条件。
<b>Expression</b>	从 Expression 下拉列表可以创建字典简单条件。
<b>Operator</b>	选择要将值关联到属性的运算符。
<b>值</b>	输入要关联到字典属性的值，或者从下拉列表选择一个值。

**相关主题**

[复合安全评估条件](#)，第 622 页

[创建复合安全评估条件](#)，第 622 页

## 用于在 Windows 客户端中启用自动更新的预定义条件

pr\_AutoUpdateCheck\_Rule 是思科预定义条件，会下载至“复合条件” (Compound Conditions) 窗口。您可以通过此条件检查在 Windows 客户端上是否启用了自动更新功能。如果 Windows 客户端未满足此要求，则网络访问控制 (NAC) 代理会强制 Windows 客户端启用（补救）自动更新功能。这种补救完成后，Windows 客户端就符合安全评估。如果在 Windows 客户端上未启用自动更新功能，您在安全评估策略中关联的 Windows 更新会覆盖 Windows 管理员设置。



## 预配置的防病毒和反间谍软件条件

思科 ISE 在“AV 复合条件” (AV Compound Condition) 和“AS 复合条件” (AS Compound Condition) 窗口加载预配置的防病毒和反间谍软件复合条件（在适用于 Windows 和 MacOS 操作系统的防病毒和反间谍软件支持图表中定义）。如果指定的防病毒和反间谍软件产品存在于全部客户端，则这些复合条件则可以选中。此外，您还可以在思科 ISE 中创建新的防病毒和反间谍软件复合条件。

### 防病毒和反间谍软件支持图表

思科 ISE 使用防病毒和反间谍软件支持图表，此图表在各供应商产品的定义文件中提供最新版本和日期。用户必须定期访问防病毒和反间谍软件支持图表来查看更新。防病毒和反间谍软件供应商会经常更新防病毒和反间谍软件定义文件，请在各供应商产品的定义文件中查找最新版本和日期。

每次系统更新防病毒和反间谍软件支持图表来反映对新防病毒和反间谍软件供应商、产品及其发行版本的支持时，代理都会收到新的防病毒和反间谍软件库。这可以帮助代理支持新增的防病毒和反间谍软件。代理检索到此支持信息后，会从定期更新的 `se-checks.xml` 文件（此文件随 `se-templates.tar.gz` 档案中的 `se-rules.xml` 文件一起发布）检查最新定义信息，然后确定客户端是否符合安全评估策略。根据防病毒和反间谍软件库对于特定防病毒或反间谍软件产品的支持情况，系统会向代理发送相应的要求，在安全评估验证过程中来验证客户端上具体的防病毒和反间谍软件产品是否存在。

有关 ISE 终端安全评估代理支持的防病毒和防恶意软件产品的详细信息，请参阅思科 AnyConnect ISE 终端安全评估支持图表：[思科 ISE 兼容性指南](#)。

您可以在创建防恶意软件终端安全评估条件时验证最低合规性模块版本。更新终端安全评估源后，请选择工作中心 (Work Centers) > 终端安全评估 (Posture) > 策略元素 (Policy Elements) > 防恶意软件条件 (Anti-Malware Condition)，然后选择操作系统 (Operating System) 和供应商 (Vendor) 以查看支持图表。



**注释** 某些防恶意软件终端安全解决方案（如 FireEye、Cisco AMP、Sophos 等）需要通过网络访问各自的集中服务才能正常运行。对于此类产品，AnyConnect ISE 终端安全评估模块（或 OESIS 库）要求终端能够连接互联网。建议在这些在线代理的终端安全评估预评估期间允许此类终端访问互联网（如果未启用离线检测）。签名定义条件可能不适用于此类情况。

## Inline Posture 节点

Inline Posture 节点是守门节点，放在网络访问设备后面，例如网络上的无线 LAN 控制器 (WLC) 和 VPN 集线器。Inline Posture 节点在用户通过身份验证并被授予访问权限后实施访问策略，并且处理 WLC 或 VPN 无法满足的授权更改 (CoA) 请求。思科 ISE 允许您有两个 Inline Posture 节点，承担主要或辅助角色，提供高可用性。

Inline Posture 节点必须为专用节点。它必须仅用于内联状态服务，不能与其他思科 ISE 服务同时运行。同样，由于其服务的专业化性质，Inline Posture 节点无法承担任何角色。例如，它不能用作管理节点提供管理服务，不能用作策略服务节点提供网络访问、安全评估、配置文件和访客服务，也不能用作监控节点为思科 ISE 网络提供监控和故障排除服务。

思科 ISE 3495 平台不支持 Inline Posture 角色。确保在以下任何受支持的平台上安装 Inline Posture 角色：思科 ISE 3315、思科 ISE 3355、思科 ISE 3395 或思科 ISE 3415。

您不能访问 Inline Posture 节点的基于 Web 的用户界面，只能从 PAN 配置这些节点。

## Inline Posture 节点的安装

您必须从 Cisco.com 下载 Inline Posture ISO (IPN ISO) 映像，然后将其安装到任何支持的平台上。然后，您必须通过命令行界面 (CLI) 配置证书。接下来，您可以从管理员门户注册此节点。



**注释** 不提供版本的 Inline Posture ISO 映像。使用 1.2 IPN ISO 映像安装并设置 Inline Posture 节点。

安装和设置 Inline Posture 应用后，您必须先配置证书，然后才能注册 Inline Posture 节点。有关详细信息，请参阅《[思科身份服务引擎硬件安装指南](#)》。

## 注册 Inline Posture 节点

我们建议您在注册时确定节点的类型（思科 ISE 或 Inline Posture）。如果希望稍后更改节点类型，您必须将该节点从部署中注销，重启独立节点上的思科 ISE 并重新注册该节点。

### 开始之前

- 确保主节点的证书信任列表 (CTL) 具有适当的证书颁发机关 (CA) 证书，以验证要注册的辅助节点的 HTTPS 证书。
- 向主要节点注册辅助节点之后，如果您更改辅助节点上的 HTTPS 证书，您必须将相应的 CA 证书导入主要节点的 CTL。

**步骤 1** 登录到 PAN。

**步骤 2** 依次选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

**步骤 3** 点击左侧导航窗格中的 **Deployment**。

**步骤 4** 选择**注册 (Register)** > **注册 Inline Posture 节点 (Register an Inline Posture Node)** 以注册 Inline Posture 节点。

## 合规性模块

合规性模块包含一个字段列表，例如由支持思科 ISE 安全评估条件的 OPSWAT 提供的供应商名称、产品版本、产品名和属性。

供应商会经常更新定义文件中的产品版本和日期，因此，您必须频繁轮询合规性模块的新情况，以找到每个供应商产品的定义文件中的最新版本和日期。每次更新合规性模块以反映对新供应商、产品和版本的支持时，AnyConnect 代理都会收到一个新库。从而使 AnyConnect 代理可支持新增产品。

AnyConnect 代理检索到此支持信息后，会从定期更新的 se-checks.xml 文件（此文件随 se-templates.tar.gz 档案中的 se-rules.xml 文件一起发布）检查最新定义信息，然后确定客户端是否符合安全评估策略。根据库文件对于特定防病毒、反间谍软件、防恶意软件、磁盘加密或补丁管理产品的支持情况，系统会向 AnyConnect 代理发送相应的要求，在安全评估验证过程中验证客户端上是否存在这些产品以及它们的状态。

合规性模块可从 [Cisco.com](https://www.cisco.com) 获取。

下表列出了支持和不支持 ISE 终端安全评估策略的 OPSWAT API 版本。对于支持版本 3 和 4 的代理，存在不同的策略规则。

表 101: OPSWAT API 版本

终端安全评估条件	合规性模块版本
OPSWAT	
防病毒软件	3.x 或更低版本
反间谍软件	3.x 或更低版本
反恶意软件	4.x 或更高版本
磁盘加密	3.x 或更低版本以及 4.x 或更高版本
补丁管理	3.x 或更低版本以及 4.x 或更高版本
USB	4.x 或更高版本
非 OPSWAT	
文件	任何版本
应用	任何版本
复合	任何版本
注册表	任何版本
服务	任何版本



#### 注释

- 请务必为版本 3.x 或更低版本以及版本 4.x 或更高版本创建单独的终端安全评估策略，因为预计客户端可能已安装以上任何一个版本。
- 为合规性模块 4.x 和 Cisco AnyConnect 4.3 及更高版本提供了 OESIS 版本 4 支持。但是，AnyConnect 4.3 同时支持 OESIS 版本 3 和版本 4 策略。
- ISE 2.1 和更高版本支持第 4 版合规性模块。

## 检查安全评估合规性

**步骤 1** 登录思科 ISE 并访问控制板。

**步骤 2** 在安全评估合规性 (**Posture Compliance**) Dashlet 中，将光标悬停于堆积条形图或迷你图上。

工具提示提供详细的信息。

**步骤 3** 展开数据类别，了解更多信息。

**步骤 4** 展开 **Posture Compliance** dashlet。

系统将显示详细的实时报告。

## 创建补丁管理条件

可以创建用于检查选定供应商的补丁管理产品状态的策略。

例如，可以创建一个条件，用以检查微软系统中心配置管理器 (SCCM) 客户端版本 4.x 软件产品是否安装在终端上。



**注释** 思科 ISE 和 AnyConnect 支持的版本：

- 思科 ISE 版本 1.4
- AnyConnect 版本 4.1 及更高版本

**开始之前**

要执行以下任务，您必须是超级管理员或策略管理员。

**步骤 1** 选择策略 (**Policy**) > 策略元素 (**Policy Elements**) > 条件 (**Conditions**) > 终端安全评估 (**Posture**) > 补丁管理条件 (**Patch Management Condition**)。

**步骤 2** 点击添加 (**Add**)。

**步骤 3** 在名称 (**Name**) 和说明 (**Description**) 字段中输入条件名称和说明。

**步骤 4** 从操作系统 (**Operating System**) 下拉字段中选择适当的操作系统。

**步骤 5** 从下拉列表中选择合规性模块 (**Compliance Module**)。

**步骤 6** 从下拉列表中选择供应商名称 (**Vendor Name**)。

**步骤 7** 选择检查类型 (**Check Type**)。

**步骤 8** 从检查已安装的补丁 (**Check patches installed**) 下拉列表中选择适当的补丁。

步骤 9 点击提交。

#### 相关主题

[补丁管理条件设置](#)

[添加补丁管理补救](#)

## 创建磁盘加密条件

您可以创建一个策略以检查终端是否与指定的数据加密软件兼容。

例如，您可以创造条件检查 C 盘是否在终端加密。如果 C 盘没有加密，终端会收到一个非合规性通知，同时 ISE 会记录一条消息。

#### 开始之前

要执行以下任务，您必须是超级管理员或策略管理员。只有当您使用 AnyConnect ISE 终端安全评估代理时，您才可以将磁盘加密条件与终端安全评估需求进行关联。

步骤 1 选择策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 终端安全评估 (Posture) > 磁盘加密条件 (Disk Encryption Condition)。

步骤 2 单击添加。

步骤 3 在磁盘加密条件 (Disk Encryption Condition) 窗口中，在字段中输入适当的值。

步骤 4 点击提交。

## 安全评估条件设置

本节介绍用于安全评估的简单条件和复合条件。

### 文件条件设置

下表介绍文件条件 (File Conditions) 窗口中的字段。此窗口的导航路径为：策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 终端评估状态 (Posture) > 文件条件 (File Condition)。

#### 相关主题

[简单安全评估条件](#)，第 621 页

[复合安全评估条件](#)，第 622 页

[创建终端安全评估条件](#)

## 注册表条件设置

下表介绍了“注册表条件”(Registry Conditions)窗口中的字段。此窗口的导航路径为：**策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **注册表条件 (Registry Condition)**。

表 102: 注册表条件设置

字段名称	使用指南
<b>Name</b>	输入注册表条件的名称。
<b>Description</b>	输入对注册表条件的说明。
<b>Registry Type</b>	选择一个预定义设置作为注册表类型。
<b>Registry Root Key</b>	选择一个预定义设置作为注册表根项。
<b>Sub Key</b>	<p>输入不带反斜杠的子项 (“\”) 以检查在 Registry Root Key 中指定的路径中的注册表项。</p> <p>例如，SOFTWARE\Symantec\Norton AntiVirus\version 将检查以下路径中的注册表项： HKLM\SOFTWARE\Symantec\NortonAntiVirus\version</p>
<b>Value Name</b>	<p>(仅在选择 <b>RegistryValue</b> 或 <b>RegistryValueDefault</b> 作为 Registry Type 的情况下可用) 为 <b>RegistryValue</b> 输入要检查的注册表项名称值。</p> <p>这是 <b>RegistryValueDefault</b> 的默认字段。</p>
<b>Value Data Type</b>	<p>(仅在选择 <b>RegistryValue</b> 或 <b>RegistryValueDefault</b> 作为 Registry Type 的情况下可用) 选择一个以下设置：</p> <ul style="list-style-type: none"> <li>• <b>未指定 (Unspecified)</b>: 检查注册表项值是否存在。此选项仅可用于 <b>RegistryValue</b>。</li> <li>• <b>数值 (Number)</b>: 检查注册表项值中指定的数值</li> <li>• <b>字符串 (String)</b>: 检查注册表项值中的字符串</li> <li>• <b>版本 (Version)</b>: 检查注册表项值中的版本</li> </ul>
<b>Value Operator</b>	选择相应的设置。
<b>Value Data</b>	(仅在选择 <b>RegistryValue</b> 或 <b>RegistryValueDefault</b> 作为 Registry Type 的情况下可用) 根据您在 <b>Value Data Type</b> 中选择的数据类型输入注册表项的值。
<b>操作系统</b>	选择应该应用此注册表条件的操作系统。

### 相关主题

[简单安全评估条件](#)，第 621 页

[复合安全评估条件](#)，第 622 页

## 应用条件设置

下表说明“应用条件”窗口中的字段。此窗口的导航路径为：**策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 终端评估状态 (Posture) > 应用条件 (Application Condition)**。

相关主题

[简单安全评估条件](#)，第 621 页

[复合安全评估条件](#)，第 622 页

## 服务条件设置

下表介绍服务条件 (**File Conditions**) 窗口中的字段。此窗口的导航路径为：**策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 终端评估状态 (Posture) > 服务条件 (Service Condition)**。

相关主题

[简单安全评估条件](#)，第 621 页

[复合安全评估条件](#)，第 622 页

## 安全评估复合条件设置

下表介绍复合条件 (**Compound Conditions**) 窗口中的字段。此窗口的导航路径为：**策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 终端评估状态 (Posture) > 复合条件 (Compound Condition)**。

表 103: 安全评估复合条件设置

字段名称	使用指南
<b>Name</b>	输入您要创建的复合条件的名称。
<b>说明 (Description)</b>	输入对您要创建的复合条件的说明。
<b>操作系统</b>	选择一个或多个 Windows 操作系统。这允许关联应用该条件的 Windows 操作系统。
<b>括号 ( )</b>	点击此括号以将以下简单条件类型的两个简单条件组合起来：文件、注册表、应用和服务条件。
<b>( &amp; )：AND 运算符（用“&amp;”表示 AND 运算符，不需要加引号）</b>	您可以在复合条件中使用 AND 运算符（与号 [ & ]）。例如，输入 <b>Condition1 &amp; Condition2</b> 。

字段名称	使用指南
(   ): OR 运算符 (用“ ”表示 OR 运算符, 不需要加引号)	您可以在复合条件中使用 OR 运算符 (小竖线 [   ])。例如, 输入 <b>Condition1 &amp; Condition2</b> 。
( ! ): NOT 运算符 (用“!”表示 NOT 运算符, 不需要加引号)	您可以在复合条件中使用 NOT 运算符 (感叹号 [ ! ])。例如, 输入 <b>Condition1 &amp; Condition2</b> 。
简单条件	从以下类型的简单条件列表中选择: 文件、注册表、应用和服务条件。 您还可以从对象选择器创建文件、注册表、应用和服务条件的简单条件。 在操作 (Action) 按钮上点击快速选择器 (向下箭头) 以创建文件、注册表、应用和服务条件的简单条件。

#### 相关主题

[安全评估条件](#), 第 621 页

[创建复合安全评估条件](#), 第 622 页

## 防病毒条件设置

下表介绍了防病毒条件 (Anti-Virus Condition) 窗口中的字段。此窗口的导航路径为: **策略 (Policy) > 策略元素 (Policy Elements) > 条件 (Conditions) > 终端评估状态 (Posture) > 防病毒条件 (Anti-Virus Condition)**。

表 104: 防病毒条件设置

字段名称	使用指南
<b>Name</b>	输入要创建的防病毒条件的名称。
<b>Description</b>	输入要创建的防病毒条件的说明。
<b>操作系统</b>	选择用于检查客户端的防病毒程序安装情况, 或检查条件所适用的最新防病毒定义文件更新的操作系统。
<b>供应商 (Vendor)</b>	从下拉列表中选择供应商。通过选择供应商, 系统会检索供应商的防病毒产品和版本, 这些信息显示在 Products for Selected Vendor 表中。
<b>Check Type</b>	选择是检查客户端的防恶意软件程序安装情况, 还是检查最新定义文件更新。
<b>Installation</b>	选择此选项, 只检查客户端的防病毒程序安装情况。
<b>Definition</b>	选择此选项, 只检查客户端的防病毒产品的最新定义文件更新。



字段名称	使用指南
请针对最新防病毒定义文件版本进行检查（如适用）	（仅当选择 Definition 检查类型时可用）如果最新防病毒定义文件版本由于思科 ISE 中的终端安全评估更新变为可用，则选择此选项以针对最新防病毒定义文件版本检查客户端的防病毒定义文件版本。否则，此选项使您可以针对思科 ISE 中的最新定义文件日期检查客户端的定义文件日期。
Allow virus definition file to be (已启用)	（仅当选择 Definition 检查类型时可用）选择此选项，检查客户端的防病毒定义文件版本和最新防病毒定义文件日期。最新定义文件日期不能早于在下一个字段（days older than 字段）定义的产品的最新防病毒定义文件日期或当前系统日期。  如果未选中，则思科 ISE 使您可以使用 Check against latest AV definition file version, if available 选项，只检查防病毒定义文件的版本。
早于的天数 (Days Older Than)	定义客户端的最新防病毒定义文件日期可以早于产品的最新防病毒定义文件日期或当前系统日期的天数。默认值为零 (0)。
最新文件日期 (Latest File Date)	选择此选项，检查客户端的防病毒定义文件日期，该日期可以早于在 days older than 字段中定义的天数。  如果将天数设置为默认值 (0)，则客户端的防病毒定义文件日期不应早于产品的最新防病毒定义文件日期。
当前系统日期 (Current System Date)	选择此选项，检查客户端的防病毒定义文件日期，该日期可以早于在 days older than 字段中定义的天数。  如果将天数设置为默认值 (0)，则客户端的防病毒定义文件日期不应早于当前系统日期。
选定供应商的产品	从表中选择防病毒产品。根据在“新防病毒条件” (New Anti-virus Condition) 页面中选择的供应商，此表会检索有关供应商的防病毒产品和版本、其提供的补救支持、最新定义文件日期及其版本的信息。  通过从表中选择产品，可以检查防病毒程序的安装情况，或检查最新防病毒定义文件日期，及其最新版本。

#### 相关主题

[复合安全评估条件](#)，第 622 页

[预配置的防病毒和反间谍软件条件](#)，第 625 页

[防病毒和反间谍软件支持图表](#)，第 625 页

## 反间谍软件复合条件设置

下表介绍作为复合条件 (AS Compound Conditions) 窗口中的字段。此窗口的导航路径为：[策略 \(Policy\)](#) > [策略元素 \(Policy Elements\)](#) > [条件 \(Conditions\)](#) > [AS 复合条件 \(AS Compound Condition\)](#)。

表 105: 反间谍软件复合条件设置

字段名称	使用指南
<b>Name</b>	输入您要创建的反间谍软件复合条件的名称。
<b>Description</b>	输入对您要创建的反间谍软件复合条件的说明。
<b>Operating System</b>	选择一个操作系统，该操作系统应允许检查客户端上的反间谍软件程序的安装，或检查应用该条件的最新反间谍软件定义文件更新。
<b>供应商</b>	从下拉列表中选择供应商。选择供应商会检索其反间谍软件产品和版本，这些信息显示于 Products for Selected Vendor 表中。
<b>Check Type</b>	选择您是想要在客户端上检查安装，还是检查最新定义文件更新。
<b>Installation</b>	选择您是否只想检查客户端上的反间谍软件程序的安装。
<b>Definition</b>	选择您是否只想检查客户端上的反间谍软件软件的最新定义文件更新。
<b>允许病毒定义文件 (Allow virus definition file to be) (已启用)</b>	<p>当您创建的是反间谍软件定义检查类型时，请选中此复选框；当您创建的是反间谍软件安装检查时，请禁用此复选框。</p> <p>如果选中此复选框，系统将允许您在客户端上检查反间谍软件定义文件版本和最新反间谍软件定义文件日期。最新的定义文件日期不能早于您在 days older than 字段中定义的距离当前系统日期的天数。</p> <p>如果未选中此复选框，您就只能选择反间谍软件定义文件的版本，因为未选中 Allow virus definition file to be 复选框。</p>
<b>早于的天数 (Days Older Than)</b>	定义在客户端上最新的反间谍软件定义文件日期可以早于当前系统日期的天数。默认值为零 (0)。
<b>当前系统日期 (Current System Date)</b>	<p>选择在客户端上检查反间谍软件定义文件日期，此日期可以早您在 days older than 字段中定义的天数。</p> <p>如果您将此天数设置为默认值(0)，则客户端上的反间谍软件定义文件日期不得早于当前系统日期。</p>
<b>选定供应商的产品</b>	<p>从表中选择反间谍软件产品。根据您在 New Anti-spyware Compound Condition 页面选择的供应商，此表检索关于其反间谍软件产品及版本的信息、其所提供的补救支持、最新定义文件日期及其版本。</p> <p>您可以通过从表中选择产品，检查反间谍软件程序的安装，或检查最新反间谍软件定义文件日期，及其最新版本。</p>

#### 相关主题

[复合安全评估条件](#)，第 622 页

[预配置的防病毒和反间谍软件条件](#)，第 625 页

[防病毒和反间谍软件支持图表](#)，第 625 页

## 字典简单条件设置

下表介绍了字典简单条件 (**Dictionary Simple Conditions**) 窗口上的字段。此窗口的导航路径为：**策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **字典简单条件 (Dictionary Simple Condition)**。

表 106: 字典简单条件设置

字段名称	使用指南
<b>Name</b>	输入您要创建的字典简单条件的名称。
<b>Description</b>	输入对您要创建的字典简单条件的说明。
<b>Attribute</b>	从字典选择属性。
<b>Operator</b>	选择将值与您所选择的属性关联的运算符。
<b>Value</b>	输入您想要与字典属性关联的值，或从下拉列表选择预定义值。

### 相关主题

[简单安全评估条件](#)，第 621 页

[创建简单安全评估条件](#)，第 622 页

## 字典复合条件设置

下表介绍字典复合条件 (**Dictionary Compound Conditions**) 窗口中的字段。此窗口的导航路径为：**策略 (Policy)** > **策略元素 (Policy Elements)** > **条件 (Conditions)** > **终端评估状态 (Posture)** > **词典复合条件 (Dictionary Compound Condition)**。

表 107: 字典复合条件设置

字段名称	使用指南
<b>Name</b>	输入要创建的字典复合条件的名称。
<b>Description</b>	输入要创建的字典复合条件的说明。
<b>Select Existing Condition from Library</b>	通过从策略要素库选择预定义的条件来定义表达式，或在后续步骤中将临时属性/值对添加到表达式中。
<b>Condition Name</b>	选择已从策略要素库中创建的字典简单条件。
<b>Expression</b>	Expression 会根据从 Condition Name 下拉列表选择的选项进行更新。

字段名称	使用指南
<b>AND 或 OR 运算符</b>	<p>选择 AND 或 OR 运算符可逻辑组合可从策略要素库添加的字典简单条件。</p> <p>点击 <b>Action</b> 图标可执行以下操作：</p> <ul style="list-style-type: none"> <li>• Add Attribute/Value</li> <li>• Add Condition from Library</li> <li>• Delete</li> </ul> <p>思科 ISE 将按顺序处理复合条件中的每个 OR 条件。例如，如果复合条件检查 A OR B，思科 ISE 会首先检查 A，然后检查 B。如果条件 A 或 B 均通过，则整体结果标记为通过。</p> <p>如果条件 A 失败，条件 B 成功，则整体结果标记为通过。在这种情况下，在安全评估报告中，条件 A 标记为失败，条件 B 为通过。</p> <p>如果条件 A 成功，思科 ISE 将跳过条件 B 并将整体结果标记为通过。在安全评估报告中，条件 A 标记为通过，条件 B 标记为已跳过，总体结果为通过。</p>
<b>Create New Condition (Advance Option)</b>	<p>从各种系统或用户定义的字典中选择属性。</p> <p>还可以在后续步骤中从策略要素库中添加预定义条件。</p>
<b>Condition Name</b>	选择已创建的字典简单条件。
<b>Expression</b>	从 Expression 下拉列表可以创建字典简单条件。
<b>Operator</b>	选择要将值关联到属性的运算符。
<b>值</b>	输入要关联到字典属性的值，或者从下拉列表选择一个值。

#### 相关主题

[复合安全评估条件](#)，第 622 页

[创建复合安全评估条件](#)，第 622 页

## 配置安全评估策略

安全评估策略是与一个或多个身份组和操作系统关联的状态要求的集合。词典属性是可与身份组和操作系统一起使用以便为设备定义不同策略的可选条件。

有关详细信息，请参阅《[ISE 安全评估规范性部署指南](#)》中的“安全评估策略”一节。

#### 开始之前

- 您必须了解可接受使用政策 (AUP)。
- 您必须了解定期重新评估 (PRA)。

- 
- 步骤 1** 选择策略 (Policy) > 终端安全评估 (Posture)。
- 步骤 2** 使用下拉箭头添加新策略。
- 步骤 3** 要编辑配置文件，请双击策略或点击行末的“编辑” (Edit)。
- 步骤 4** 从规则状态 (Rule Status) 下拉列表中，选择已启用 (Enabled)或已禁用 (Disabled)。
- 步骤 5** (可选) 拖动名为延迟通知 (Delayed Notification) 的滑块延迟宽限期提示，直到宽限期消耗特定百分比后再显示给用户。例如，通知延迟期设置为 50% 且配置的宽限期为 10 分钟，则思科 ISE 将在 5 分钟后检查安全评估状态，如果发现终端不合规，则显示宽限期通知。如果终端状态为合规，则不会显示宽限期通知。如果通知延迟时间设置为 0%，系统会在宽限期开始时立即提示用户以解决问题。但在宽限期过期之前，终端会被授予访问权限。此字段的默认值为 0%。有效范围为 0 到 95%。
- 步骤 6** 在规则名称 (Rule Name) 字段中，输入策略的名称。
- 注释 最好将每项要求作为单独的规则来配置安全评估策略，以避免意外结果。
- 步骤 7** 从身份组 (Identity Groups) 列中，选择所需的身份组。
- 步骤 8** 从操作系统 (Operating Systems) 列中，选择操作系统。
- 步骤 9** 在 Other Conditions 中，您可以添加一个或多个词典属性，然后以简单或复合条件的方式将它们保存到词典中。
- 注释 您在终端安全评估策略 (Posture Policy) 窗口中创建的词典简单条件和复合条件在配置授权策略时不显示。
- 步骤 10** 在要求 (Requirements) 字段中指定要求。
- 步骤 11** 点击保存 (Save)。
- 

## 配置 AnyConnect 工作流程

要配置 AnyConnect 代理，请在思科 ISE 中执行以下步骤：

### 开始之前

在以下思科 ISE 版本中，漏洞 [CSCvs39880](#) 会导致垃圾收集进程，从而影响从主 PSN 到辅助 PSN 的内存空间和文件复制。由于此漏洞，在以下思科 ISE 版本中，在大型思科 ISE 部署中上传代理包可能需要约 7 个小时，而在小型部署中则需要约 40 分钟。

以下是受影响的思科 ISE 版本：

在更高的思科 ISE 版本中，此漏洞已得到修复，使得代理软件包上传时间约为 5 分钟。

---

- 步骤 1** 创建 AnyConnect 代理配置文件。
- 步骤 2** 为 AnyConnect 软件包创建 an AnyConnect 配置。
- 步骤 3** 创建客户端调配策略。
- 步骤 4** (可选) 创建自定义终端安全评估条件。

- 步骤 5** (可选) 创建自定义补救操作。
- 步骤 6** (可选) 创建自定义终端安全评估要求。
- 步骤 7** 创建终端安全评估策略。
- 步骤 8** 配置客户端调配策略。
- 步骤 9** 创建授权配置文件。
- 步骤 10** 配置授权策略。
- 步骤 11** 下载并启动 AnyConnect。
- a) 连接到 SSID。
  - b) 启动浏览器，您将重定向至客户端调配门户。
  - c) 点击**开始**。这样将检查 AnyConnect 代理是否已安装并正在运行。
  - d) 点击**这是我第一次访问 (This Is My First Time Here)**。
  - e) 选择 **点击此处下载并启动 AnyConnect**。
  - f) 分别保存适用于 Windows 或 macOS 的思科 Anyconnect .exe 或 .dmg 文件。对于 Windows，请运行 .exe 文件；对于 macOS，请双击 .dmg 文件并运行应用。



**注释** 思科 ISE 不支持 ARM64 版本的 AnyConnect 用于 AnyConnect 终端安全评估流程。确保不要在客户端调配策略中使用 ARM64 版本的 AnyConnect，否则可能会导致客户端故障。如果 AnyConnect 由于此问题无法正常工作，请重新启动客户端。

## 客户端安全评估

为确保已应用的网络安全措施保持相关和有效，思科 ISE 使您能够在任何可访问受保护网络的客户端计算机上验证和维护安全功能。通过应用旨在确保最新安全设置或应用在客户端计算机上可用的终端安全评估策略，思科 ISE 管理员可以确保任何访问网络的客户端都符合并且继续符合为企业网络访问定义的安全标准。终端安全评估合规性报告在用户登录时以及在周期性再评估发生时，为思科 ISE 提供客户端计算机合规性级别快照。

使用思科 ISE 中提供的下列代理类型之一，终端安全评估和合规性会发生：

- **思科 NAC Web 代理**：用户在登录时安装在系统中的临时代理，一旦登录会话终止，临时代理在客户端计算机上就不再可见。
- **思科 NAC 代理**：持久代理，安装后，依然在 Windows 或 Mac OS X 客户端计算机上执行所有安全合规性功能。
- **AnyConnect ISE 代理**：持久代理，可以安装在 Windows 或 Mac OS X 客户端计算机上执行终端安全评估合规性功能。

## 终端安全状态评估选项

### 安全评估补救选项

### 安全评估的自定义条件

安全评估条件可以是以下任何一个简单条件：文件、注册表、应用、服务或字典条件。这些简单条件中的一个或多个条件构成可与安全评估要求相关联的复合条件。

在初始安全评估更新后，思科 ISE 还会创建思科定义的简单条件与复合条件。思科定义的简单条件使用 `pc_` 作为前缀，复合条件使用 `pr_` 作为前缀。

用户定义的条件或思科定义的条件同时包含简单条件与复合条件。

安全评估服务基于防病毒和反间谍软件 (AV/AS) 复合条件利用内部检查。因此，安全评估报告不会反映您已创建的精确 AV/AS 复合条件名称。报告仅显示 AV/AS 复合条件的内部检查名称。

例如，如果您已创建名为 “MyCondition\_AV\_Check” 的 AV 复合条件来检查任何供应商与任何产品，则安全评估报告会将内部检查（即 “av\_def\_ANY”）显示为条件名称，而不是显示 “MyCondition\_AV\_Check”。

### 自定义安全评估补救措施

自定义安全评估补救措施是文件、链接、防病毒或反间谍软件定义更新、启动程序、Windows 更新或 Windows Server Update Services (WSUS) 补救类型。

### 添加反间谍程序补救

可以创建反间谍程序补救，从而在补救之后使用最新文件定义更新客户端以确保合规。

“AS 补救” (AS Remediations) 窗口显示所有防病毒软件补救以及补救的名称、说明和模式。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture)。

**步骤 2** 点击 **Remediation Actions**。

**步骤 3** 点击 **AS Remediation**。

**步骤 4** 点击 **Add**。

**步骤 5** 修改新 AS 补救 (New AS Remediations) 窗口中的值。

**步骤 6** 点击提交。

---

## 添加防病毒软件补救

您可以创建防病毒软件补救，在补救完成后，用最新的合规性文件定义更新客户端。

“AV 补救” (AV Remediations) 窗口显示所有防病毒软件补救以及补救的名称、说明和模式。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture)。

**步骤 2** 点击 **Remediation Actions**。

**步骤 3** 点击 **AV Remediation**。

**步骤 4** 点击 **Add**。

**步骤 5** 修改新 AV 补救 (New AV Remediation) 窗口中的值。

**步骤 6** 点击提交。

---

## 添加文件补救

客户端可以通过文件补救下载实现合规性所需的文件版本。客户端代理可以利用客户端或合规性要求的文件对终端进行补救。

您可以在“文件补救” (File Remediations) 窗口过滤、查看、添加或删除文件补救，但无法编辑文件补救。“文件补救” (File Remediations) 窗口显示所有文件补救及其名称与说明，还有补救所需的文件。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture)。

**步骤 2** 点击 **Remediation Actions**。

**步骤 3** 点击 **File Remediation**。

**步骤 4** 点击 **Add**。

**步骤 5** 在名称 (Name) 和说明 (Description) 字段中输入文件补救的名称和说明。

**步骤 6** 在新建文件补救 (New File Remediation) 窗口中修改值。

**步骤 7** 点击提交。

---

## 添加启动程序补救

您可以创建启动程序补救，其中客户端代理将通过启动一个或多个合规性应用来补救客户端。

Launch Program Remediations 页面显示所有启动程序补救，以及它们的名称和说明及补救模式。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture)。

**步骤 2** 点击 **Remediation Actions**。



步骤 3 点击 **Launch Program Remediation**。

步骤 4 点击添加 (**Add**)。

步骤 5 在新启动程序补救 (**New Launch Program Remediation**) 页面中修改值。

步骤 6 点击提交。

---

## 排除启动程序补救故障

### 问题

当应用作为使用启动计划修复的补救措施启动时，应用成功启动（可在 Windows 任务管理器观察到），但是应用 UI 不可见。

### 解决方案

启动计划 UI 应用在系统权限运行，并会显示在交互式服务检测 (ISD) 窗口中。要查看启动计划 UI 应用，以下操作系统应启用 ISD：

- Windows Vista: 默认情况下 ISD 处于停止状态。通过启动 services.msc 中的 ISD 服务启用 ISD。
- Windows 7: 默认情况下启用 ISD 服务。
- Windows 8/8.1: 通过在注册表中将 "NoInteractiveServices" 从 1 更改为 0 启用 ISD:  
\\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Windows。

## 添加链接补救

客户端可以通过链接补救点击 URL 以访问补救窗口或资源。客户端代理用此链接打开浏览器，并且允许客户端执行进行合规性补救。

“链接补救” (Link Remediation) 窗口显示所有链接补救及其名称与说明和补救模式。

---

步骤 1 选择策略 (**Policy**) > 策略元素 (**Policy Elements**) > 结果 (**Results**) > 终端安全评估 (**Posture**)。

步骤 2 点击 **Remediation Actions**。

步骤 3 点击 **Link Remediation**。

步骤 4 点击添加 (**Add**)。

步骤 5 在新建链接补救 (**New Link Remediation**) 窗口修改相应值。

步骤 6 点击提交。

## 添加 Windows 服务器更新服务补救

您可以将 Windows 客户端配置为从本地管理或 Microsoft 管理的 WSUS 服务器接收最新的 WSUS 更新，以实现合规性。Windows 服务器更新服务 (WSUS) 补救安装来自本地管理的 WSUS 服务器或 Microsoft 管理的 WSUS 服务器的 Windows 服务包、热补救和补丁。

在客户端代理与本地 WSUS 代理相集成的情况下，您可以创建 WSUS 补救，以检查终端是否安装最新的 WSUS 更新。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture)。

**步骤 2** 点击 **Remediation Actions**。

**步骤 3** 点击 **Windows Server Update Services Remediation**。

**步骤 4** 点击 **Add**。

**步骤 5** 修改新 Windows 服务器更新服务补救 (New Windows Server Update Services Remediation) 窗口中的值。

**步骤 6** 点击提交。

---

## 添加 Windows 更新补救

Windows Update Remediations 页面显示所有 Windows 更新补救及其名称和说明与补救模式。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > > 终端安全评估 (Posture)。

**步骤 2** 点击 **Remediation Actions**。

**步骤 3** 点击 **Windows Update Remediation**。

**步骤 4** 点击添加 (Add)。

**步骤 5** 修改新建 Windows 更新补救 (New Windows Update Remediation) 窗口中的值。

**步骤 6** 点击提交。

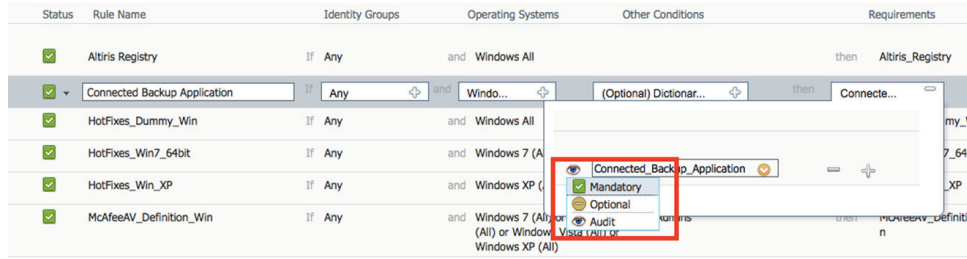
---

## 终端安全评估要求

安全评估要求是一组具有关联补救操作的复合条件，可与角色和操作系统相关联。连接到网络的所有客户端必须在安全评估过程中满足强制性要求才能在网络上达到合规状态。

安全评估策略要求可在安全评估策略中设置为强制性、可选或审核类型。如果要求为可选类型且客户端未能满足这些要求，则客户端可选择继续对终端进行安全评估。

图 38: 终端安全评估策略要求类型



### 强制性要求

在策略评估期间，代理对未能满足终端安全评估策略中定义的强制性要求的客户端提供补救选项。最终用户必须在补救计时器设置中指定的时间内进行补救以满足要求。

例如，您已通过一个用户定义条件指定强制性要求以检查绝对路径中 C:\temp\text.file 的存在。如果该文件不存在，则强制性要求未通过，用户将会被移至非合规状态。

### 可选要求

在策略评估期间，当无法满足终端安全评估策略中指定的可选要求时，代理会为客户提供一个选项继续。允许最终用户跳过指定可选要求。

例如，您通过一个用户定义条件指定一个可选要求以检查在客户端机器上运行的应用，例如 Calc.exe。虽然客户端未能满足该条件，但代理会提示一个继续后续操作的选项，以便跳过可选要求并将最终用户移至合规状态。

### 审核要求

审核要求指定用于内部目的，代理不提示任何消息或来自最终用户的四输入，无论策略评估期间状态是失败还是通过。

例如，您在创建一个强制性策略条件以检查最终用户是否拥有防病毒程序的最新版本的过程中。如果要在将其作为策略条件实际实施前找出非合规的最终用户，您可以将其指定为审核要求。

## 客户端系统处于不合规状态

如果客户机无法通过修复符合强制性要求，则安全评估状态会更改为“不合规”，且代理会话会被隔离。若要使客户机通过此“不合规”状态，则需要重启安全评估会话从而使代理再次启动客户机上的安全评估。您可以按以下方法重启安全评估会话：

- 在 802.1X 的有线和无线授权更改 (CoA) 环境下：
  - 当您在新授权策略窗口中新建授权配置文件时，您可以配置特定授权策略的重新验证计时器。此方法不支持内联安全评估部署。
  - 一旦断开并重新连接到网络时，有线用户即可离开隔离状态。在无线环境中，用户必须断开与无线局域网控制器 (WLC) 的连接并等待用户空闲超时过期后才能尝试重新连接到网络。

- 在 VPN 环境中 - 断开并重新连接 VPN 隧道。

## 创建客户端安全评估要求

可以在“要求”(Requirements)窗口创建要求，可以通过此窗口将用户定义的条件和思科定义的条件与补救操作关联起来。在“要求”(Requirements)窗口创建并保存用户定义的条件和补救操作后，可以从各自的列表窗口查看这些条件和操作。



**注释** 要创建安全评估要求以验证环境中的所有 Windows 10 补丁，您必须将“要求”的“条件”区域配置为包含 `pr_Win10_32_Hotfixes` 和 `pr_Win10_64_Hotfixes`。在条件的顶部，确保选中 **所有选定的条件成功**。如果配置成功，系统将显示 **pr\_Win10\_32\_Hotfixes & pr\_Win10\_64\_Hotfixes**。要查看终端的已验证条件的详细信息，请从主菜单选择操作 (Operations) > 报告 (Reports) > 报告 (Reports) > 终端和用户 (Endpoints and Users) > 按终端进行终端安全评估 (Posture Assessment by Endpoints)。单击终端可查看相应的终端安全评估详细信息。

图 39: 验证 Windows 10 中的安全评估要求

Requirements		Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_av_win_inst	then Message Text Only	Edit	
hotfix test	for Windows ...	using 4.x or later	using AnyConnect	met if Select C...	then Select Re...	+	
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_av_...	All selected conditions succeed	+	
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_as_...	pr_Win10_32_Hotfixes	+	
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_as_...	pr_Win10_64_Hotfixes	+	
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_av_...	AnyAVDefRemediationMac	Edit	
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_as_...	Message Text Only	Edit	
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_as_...	AnyASDefRemediationMac	Edit	
Any_AM_Installation_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_...	Message Text Only	Edit	
Any_AM_Definition_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_...	AnyAMDefRemediationWin	Edit	
Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if ANY_am_...	Message Text Only	Edit	

### 开始之前

- 必须了解适用于安全评估的可接受使用政策 (AUP)。

步骤 1 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 终端安全评估 (Posture) > 要求 (Requirements)。

步骤 2 在要求 (Requirements) 窗口中输入值。

步骤 3 点击完成 (Done)，在只读模式下保存终端安全评估要求。

步骤 4 点击保存 (Save)。

## 重新进行安全评估配置设置

表 108: 重新进行安全评估配置设置

字段名称	使用指南
<b>Configuration Name</b>	输入 PRA 配置的名称。
<b>Configuration Description</b>	输入 PRA 配置的说明。
<b>Use Reassessment Enforcement?</b>	选中此复选框，将 PRA 配置应用到用户身份组。
<b>Enforcement Type</b>	<p>选择要执行的操作：</p> <ul style="list-style-type: none"> <li>• <b>继续 (Continue)</b>: 用户继续拥有特权访问权限，无需任何用户干预即可补救客户端，无论终端安全评估要求如何都是如此。</li> <li>• <b>注销 (Logoff)</b>: 如果客户端不合规，用户将被迫从网络注销。当客户端再次登录时，合规性状态未知。</li> <li>• <b>补救 (Remediate)</b>: 如果客户端不合规，代理将在指定时间内等待补救发生。客户端一旦补救，代理将向策略服务节点发送 PRA 报告。如果在客户端忽略补救，代理程序将向策略服务节点发送注销请求，迫使客户端从网络注销。</li> </ul> <p>如果终端安全评估要求设置为强制，那么 RADIUS 会话将因为 PRA 故障操作而被清除，并且必须开始新的 RADIUS 会话，才能再次布置客户端。</p> <p>如果终端安全评估要求设置为可选，那么代理允许用户从代理点击“继续” (Continue) 选项。用户可以继续停留在当前的网络中，不受任何限制。</p>
<b>Interval</b>	<p>输入第一次成功登录后在客户端上启动 PRA 的时间间隔分钟数。</p> <p>默认值为 240 分钟。最小值为 60 分钟，最大值为 1440 分钟。</p>
<b>Grace time</b>	<p>输入允许客户端完成补救的时间间隔分钟数。宽限时间不能为零，并且应当大于 PRA 间隔。它可以介于默认最小间隔（5 分钟）和最小 PRA 间隔之间。</p> <p>最小值为 5 分钟，最大值为 60 分钟。</p> <p>注释 宽限时间仅在执行类型设置为在客户端重新进行安全评估失败后的补救操作时启用。</p>
<b>Select User Identity Groups</b>	为 PRA 配置选择唯一组或唯一组组合。
<b>PRA configurations</b>	显示现有的 PRA 配置以及关联到 PRA 配置的用户身份组。

### 相关主题

- [安全评估租约](#)，第 613 页
- [定期重新评估](#)，第 614 页
- [终端安全状态评估选项](#)，第 639 页
- [安全评估补救选项](#)，第 639 页
- [安全评估的自定义条件](#)，第 639 页
- [自定义安全评估补救措施](#)，第 639 页
- [配置定期重新评估](#)，第 615 页

## 自定义安全评估权限

自定义权限是一个在思科 ISE 中定义的标准授权配置文件。标准授权配置文件根据终端的匹配合规性状态设置访问权限。终端安全评估服务将终端安全评估广泛地划分为未知、合规和不合规的配置文件。终端安全评估策略和终端安全评估要求确定终端的合规性状态。

您必须为终端的未知、合规和不合规安全评估状态创建三种不同的授权配置文件，这些终端可以具有不同的 VLAN、DACL 和其他属性值对集合。这些配置文件可与三种不同的授权策略相关联。为了区分这些授权策略，可以使用 `Session:PostureStatus` 属性以及其他条件。

### 未知的配置文件

如果没有为终端定义匹配的终端安全评估策略，则终端的终端安全评估合规性状态可能设置为未知。未知的终端安全评估合规性状态也可适用于匹配的终端安全评估策略已启用但其终端安全评估评估尚未进行的终端，因此，客户端代理尚未提供合规性报告。



---

**注释** 我们建议您对所有思科网络接入设备使用终端安全评估和重定向。

---

### 合规的配置文件

如果已为终端定义匹配的终端安全评估策略，则终端的终端安全评估合规性状态会设置为合规。当进行终端安全评估时，终端会满足匹配的终端安全评估策略中定义的所有强制性要求。对于终端安全评估合规的终端，可以向其授予对网络的网络访问权限。

### 不合规的配置文件

当为某个终端定义匹配的终端安全评估策略，但该策略在终端安全评估过程中未能满足所有强制性要求时，该终端的终端安全评估合规性状态会设置为不合规。终端安全评估不合规的终端会将终端安全评估要求与补救操作匹配，并且应对该终端授予对补救资源的有限网络访问权限以便自行补救。

## 配置标准授权策略

您可以在 **Authorization Policy** 页面中定义两种类型的授权策略：标准和例外授权策略。特定于安全评估的标准授权策略用于根据终端的合规性状态制定策略决策。

**步骤 1** 选择策略 (**Policy**) > 授权 (**Authorization**)。

**步骤 2** 从 **Authorization Policy** 页面顶部显示的下拉列表中选择其中一个要应用的匹配规则类型。

- **应用第一个匹配的规则 (First Matched Rule Applies)** - 此选项使用标准授权策略列表中在评估过程中第一个匹配的单个授权策略设置访问权限。找到第一个匹配授权策略后，便不会评估其余标准授权策略。
- **Multiple Matched Rule Applies** - 此选项使用所有标准授权策略列表中在评估过程中匹配的多个授权策略设置访问权限。

**步骤 3** 点击默认标准授权策略行中 **编辑 (Edit)** 旁的向下箭头。

**步骤 4** 点击 **Insert New Rule Above**。

**步骤 5** 输入规则名称，选择身份组和其他条件，然后关联显示在默认标准授权策略行上方的新授权策略行中的授权配置文件。

**步骤 6** 点击 **完成 (Done)** 以在只读模式下创建新的标准授权策略。

**步骤 7** 点击 **保存 (Save)**。

## 安全评估故障排除工具

安全评估故障排除工具可帮助您查找安全状态检查失败的原因，以确定以下事项：

- 在安全评估检查中哪些终端成功，哪些终端失败。
- 如果终端在安全评估检查中失败，则确定安全评估流程中哪些步骤失败。
- 哪些强制检查和可选检查成功，哪些强制检查和可选检查失败。

您可以根据用户名、MAC 地址和安全评估状态等参数过滤请求，确定这些信息。

## 在思科 ISE 中配置客户端调配

启用客户端调配以允许用户下载客户端调配资源并配置代理配置文件。您可以配置 Windows 客户端、Mac OS X 客户端的代理配置文件，并可配置个人设备的本地请求方文件。如果禁用客户端调配，则尝试访问网络的用户会收到警告消息，表明他们无法下载客户端调配资源。

开始之前

如果使用代理并在远程系统上托管客户端调配资源，请验证代理是否允许客户端访问该远程位置。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 客户端调配 (Client Provisioning)。

**步骤 2** 从启用调配 (Enable Provisioning) 下拉列表中，选择启用 (Enable) 或禁用 (Disable)。

**步骤 3** 从 **Enable Automatic Download** 下拉列表中选择 **Enable**。

源下载包括所有可用的客户端调配资源。其中一些资源可能与您的部署并不相关。思科建议尽可能手动下载资源，而不是设置此选项。

**步骤 4** 在更新源 URL (Update Feed URL) 文本框中指定思科 ISE 搜索系统更新所在的 URL。例如，用于下载客户端调配资源的默认 URL 是 <https://www.cisco.com/web/secure/pmbu/provisioning-update.xml>。

如果您的网络限制 URL 重定向功能（例如，通过代理服务器），并且您在访问默认 URL 时遇到困难，则另请尝试将您的思科 ISE 指向以下 URL：<https://www.perfigo.com/ise/provisioning-update.xml>。

**步骤 5** 当设备没有客户端调配资源时，请选择以下选项之一：

- **允许网络访问 (Allow Network Access)**: 用户可以在网络上注册其设备，而不必安装和启动本地请求方向导。
- **应用定义的授权策略 (Apply Defined Authorization Policy)**: 用户必须尝试通过标准身份验证和授权策略应用访问思科 ISE 网络（在本地请求方配置过程之外）。如果您启用了此选项，则用户设备会根据应用于用户 ID 的任何客户端调配策略进行标准注册。如果用户的设备需要证书才能访问思科 ISE 网络，则还必须向用户提供详细说明，介绍如何使用面向用户的可自定义文本字段获取和应用有效证书。

**步骤 6** 点击保存。



**注释** 如果 ISE 证书缓存在终端的 HTTP 严格传输安全 (HSTS) 存储中，则客户端调配门户重定向可能会失败，您可能会看到以下错误消息：

您现在无法访问 `hostname.domain.com`，因为该网站使用 HSTS。网络错误和攻击是暂时的，因此此页面稍后可能会恢复正常。

要解决这个问题，请删除终端上的浏览器缓存，或者导航到 `chrome://net-internals/#hsts` 并删除自签名 ISE 证书。

下一步做什么

配置客户端调配资源策略

## 客户端调配资源

在终端连接到网络后，客户端调配资源将会下载到终端。客户端调配资源包括适用于台式电脑的合规性和终端安全评估代理，以及适用于手机和平板电脑的本地请求方配置文件。客户端调配策略将这些调配资源分配给终端，以开始网络会话。

客户端调配资源在 **策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources)** 中列出。可以通过点击添加 (Add) 按钮将以下资源类型添加到列表中：



- **思科站点中的代理资源**：选择要使其可用于客户端调配策略的 NAC、AnyConnect 和请求方调配向导。思科会定期更新该资源列表，以便添加新资源和更新现有资源。还可以将 ISE 设置为自动下载所有思科资源和资源更新，请参阅[在思科 ISE 中配置客户端调配](#)，第 647 页了解详细信息。
- **本地磁盘中的代理资源 (Agent resources from local disk)**：在 PC 中选择要上传到 ISE 的资源，请参阅[从本地计算机添加思科提供的客户端调配资源](#)，第 650 页。
- 
- **本地请求方配置文件 (Native Supplicant Profile)**：为手机和平板电脑配置一个包含网络设置的请求方配置文件。有关详细信息，请参阅[创建本地请求者配置文件](#)。
- **NAC 代理或 AnyConnect ISE 终端安全评估配置文件 (NAC Agent or AnyConnect ISE Posture Profile)**：当您不希望创建和分配代理 XML 配置文件时，请在此配置 NAC 代理和 AnyConnect ISE 终端安全评估。有关 AnyConnect ISE 终端安全评估代理和 ISE 终端安全评估配置文件编辑器的详细信息，请参阅适用于您的 AnyConnect 版本的《AnyConnect 管理员指南》<https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html>。有关 NAC 代理配置文件的详细信息，请参阅[为思科 NAC 代理创建代理自定义文件](#)，第 661 页。
- **AMP 启用程序配置文件**：创建从外部 Web 服务器下载安装程序（用于在终端上安装 AnyConnect AMP 启用程序客户端）的客户端调配配置文件。您可以通过添加另一个调配资源并选择**本地磁盘中的代理资源 (Agent resources from local disk)** 将该配置文件上传到 ISE。有关 AMP 启用程序 XML 配置文件的详细信息，请参阅适用于您的 AnyConnect 版本的《AnyConnect 管理员指南》<https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html>。

在创建客户端调配资源后，请创建客户端调配策略，以便将客户端调配资源应用于终端。请参阅[配置客户端调配资源策略](#)，第 674 页。

#### 相关主题

[在思科 ISE 中配置客户端调配](#)，第 647 页

[从思科添加客户端调配资源](#)，第 649 页

[从本地计算机添加思科提供的客户端调配资源](#)，第 650 页

[从本地计算机添加 AnyConnect 的客户创建资源](#)，第 650 页

## 从思科添加客户端调配资源

可以从 Cisco.com 添加适用于 AnyConnect 和思科 NAC 代理（Windows 和 MAC OSX 客户端）以及思科 Web 代理的客户端调配资源。根据您选择的资源和可用网络带宽，思科 ISE 会用几分钟时间，将客户端调配资源下载到思科 ISE。

#### 开始之前

- 确保已在思科 ISE 中配置正确的代理设置。
- 在思科 ISE 中启用客户端调配。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources)。

**步骤 2** 依次选择 **Add > Agent resources from Cisco site**。

**步骤 3** 从下载远程资源 (Download Remote Resources) 对话框中的可用列表选择一个或多个所需的客户端调配资源。

**步骤 4** 单击 **Save**。

---

#### 下一步做什么

在成功将客户端调配资源添加到思科 ISE 之后，您可以开始配置客户端调配资源策略。

## 从本地计算机添加思科提供的客户端调配资源

您可以从本地磁盘添加之前从思科下载的客户端调配资源。

#### 开始之前

请确保仅向思科 ISE 上传支持的最新资源。较旧且不受支持的资源可能会导致客户端访问出现严重问题。

如果要从 Cisco.com 手动下载资源文件，请参阅[思科 ISE 发行说明](#)中的“思科 ISE 离线更新”部分。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources)。

**步骤 2** 依次选择 **Add > Agent resources from local disk**。

**步骤 3** 从类别 (Category) 下拉列表中，选择思科提供的软件包 (Cisco Provided Packages)。

**步骤 4** 单击 **Browse** 以浏览要下载到思科 ISE 的资源文件所在的本地计算机上的目录。

您可以添加之前从思科下载到本地计算机的 AnyConnect、思科 NAC 代理、或思科 Web 代理资源。

**步骤 5** 单击 **Submit**。

---

#### 下一步做什么

在成功将客户端调配资源添加到思科 ISE 之后，即可开始配置客户端调配资源策略。

## 从本地计算机添加 AnyConnect 的客户创建资源

从本地计算机将 AnyConnect 自定义和本地化包及 AnyConnect 配置文件等客户创建资源添加到思科 ISE。

### 开始之前

确保 AnyConnect 的客户创建资源是压缩的文件且在您的本地磁盘中可用。A

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources)。

**步骤 2** 依次选择添加 (Add) > 来自本地磁盘的代理资源 (Agent Resources from local disk)。

**步骤 3** 从类别 (Category) 下拉列表中，选择客户创建的包 (Customer Created Packages)。

**步骤 4** 输入 AnyConnect 资源的名称和说明。

**步骤 5** 点击 **Browse** 以浏览要下载到思科 ISE 的资源文件所在的本地计算机上的目录。

**步骤 6** 选择以下要上传到思科 ISE 的 AnyConnect 资源：

- AnyConnect 自定义捆绑包
- AnyConnect 本地化捆绑包
- AnyConnect 配置文件

**步骤 7** 点击 **Submit**。

上传的 AnyConnect 表会显示您添加到思科 ISE 的 AnyConnect 资源。

### 下一步做什么

创建 AnyConnect 代理配置。

## 创建本地请求者配置文件

您可以创建本地请求者配置文件来允许用户将其自己的设备带入思科 ISE 网络。当用户登录时，思科 ISE 使用与该用户的权限要求相关的配置文件选择必要的请求者调配向导。向导运行并设置用户的个人设备以访问网络。



**注释** 调配向导仅配置活动接口。因此，除非两个接口都是活动状态，具有有线和无线连接的用户不会为两个接口进行调配。

### 开始之前

- 如果您要对远程设备注册使用 TLS 设备协议，请至少设置一个简单证书注册协议 (SCEP) 配置文件。
- 打开 TCP 端口 8909 和 UDP 端口 8909 以启用 Cisco NAC 代理、Cisco NAC Web 代理和请求者调配 (Supplicant Provisioning) 向导安装。有关端口用法的详细信息，请参阅《思科身份服务引擎硬件安装指南》中的“思科 ISE 设备端口参考”附录。

步骤 1 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources)。

步骤 2 依次选择添加 (Add) > 本地请求者配置文件 (Native Supplicant Profile)。

步骤 3 使用 [本地请求者配置文件设置](#)，第 652 页中所述的步骤来创建配置文件。

### 下一步做什么

启用自助调配功能，允许员工直接将其个人设备连接到网络，在“对多个访客门户的支持”一节中进行了介绍。

## 本地请求者配置文件设置

当您选择 策略 > 策略元素 > 结果 > 客户端调配 > 资源 > 添加 > 本地请求者配置文件时，将显示以下设置。

- **名称 (Name)**: 输入您创建的本地请求者配置文件的名称。
- **操作系统 (Operating System)**: 从下拉列表中选择此配置文件要应用于的操作系统。

每个配置文件定义思科 ISE 将应用于客户端本地请求者的网络连接的设置。

### 无线配置文件

配置一个无线配置文件，用于客户端可用的每个 SSID:

- **SSID 名称 (SSID Name)**: 输入客户端将连接到的 SSID 的名称。
- **安全 (Security)**: 选择 WPA 或 WPA2。
- **允许的协议 (Allowed Protocol)**: 选择 PEAP 或 EAP-TLS。
- **证书模板 (Certificate Template)**: 对于 TLS，选择一个证书模板证书模板在管理 (Administration) > 系统证书 (System Certificates) > 证书颁发机构 (Certificate Authority) > 证书模板 (Certificate Templates) 中定义。

### 可选设置

如果展开可选 (Optional)，则会显示以下字段。

#### Windows 设置

- **不提示用户授权新服务器或受信任的证书颁发机构 (Do not prompt user to authorize new servers or trusted certification authorities)**: 如果启用此选项，则不会提示用户授权。用户证书会被自动接受。
- **对连接使用不同的用户名 (Use a different user name for the connection)**: 这仅适用于无线配置文件。会对连接使用不同的用户名。

- 网络不广播其名称 (SSID) 时也连接 (Connect even if the network is not broadcasting its name (SSID)): 这仅适用无线配置文件。即使未广播其 SSID, 也要连接到网络。

### iOS 设置

- 目标网络隐藏时启用 (Enable if Target Network is Hidden): 仅在隐藏目标网络时选中此复选框。

### 有线配置文件

- 允许的协议 (Allowed Protocol): 选择 PEAP 或 EAP-TLS。
- 证书模板 (Certificate Template): 对于 TLS, 选择一个证书模板证书模板在管理 (Administration) > 系统证书 (System Certificates) > 证书颁发机构 (Certificate Authority) > 证书模板 (Certificate Templates) 中定义。

### 可选设置

如果展开可选 (Optional), 以下字段对 Windows 客户端可用。

- 自动使用登录名和密码 (和域, 如果有) (Automatically use logon name and password (and domain if any)): 如果选择了用于身份验证模式的用户, 若信息可用, 请使用登录名和密码, 而无需提示用户。
- 启用快速重连接 (Enable Fast Reconnect): 当 PEAP 协议选项中的会话恢复功能启用时, 允许 PEAP 会话恢复, 而不检查用户凭据, 该功能在管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > PEAP 上配置。
- 启用隔离检查 (Enable Quarantine Checks): 检查客户端是否已隔离。
- 服务器不存在加密绑定 TLV 时断开 (Disconnect if server does not present cryptobinding TLV): 网络连接不支持加密绑定 TLV 时断开。
- 不提示用户授权新服务器或受信任的证书颁发机构 (Do not prompt user to authorize new servers or trusted certification authorities): 自动接收用户证书; 不提示用户。

## 思科 AnyConnect 安全移动

思科 ISE 使用 思科 AnyConnect 中的集成模块来满足思科 ISE 终端安全评估要求。思科 AnyConnect 是与思科 ISE NAC 代理共存于同一终端上的终端安全评估代理。一次只有一个代理处于活动状态。



注释 AnyConnect 不支持 CWA 流。您无法通过访客门户使用 访客访问 > 配置 > 访客门户 > 创建、编辑或复制 > 门户行为和流设置 > 访客设备合规性设置 窗口中的 要求访客设备合规 字段来调配 AnyConnect。相反, 应在客户端调配门户上调配 AnyConnect。此方法会导致按照授权权限中的配置进行重定向。

当将思科 ISE 与 思科 AnyConnect 代理集成时，思科 ISE 会：

- 充当暂存服务器以部署 思科 AnyConnect 4.0 版本及其未来版本
- 与 AnyConnect 终端安全评估组件进行交互以满足思科 ISE 终端安全评估要求
- 支持部署 思科 AnyConnect 配置文件、自定义及语言包，以及 Windows 和 Mac OS x 操作系统的 OPSWAT 库更新
- 同时支持 思科 AnyConnect 和传统代理

## 创建 AnyConnect 配置

AnyConnect 配置包括 AnyConnect 软件及其相关的配置文件。可在允许用户下载 AnyConnect 资源并将其安装到客户端上的客户端调配策略中使用此配置。如果您使用 ISE 和 ASA 部署 AnyConnect，则两个前端上的配置必须匹配。

要在连接到 VPN 时推送 ISE 终端安全评估模块，Cisco 建议您通过使用思科自适应安全设备管理器 (ASDM) GUI 工具的思科自适应安全设备 (ASA) 安装 AnyConnect 代理。ASA 使用 VPN 下载程序执行安装。在下载后，将通过 ASA 推送 ISE 终端安全评估配置文件，并在 ISE 终端安全评估模块联系 ISE 之前提供随后调配该配置文件所需的发现主机。而对于 ISE，ISE 终端安全评估模块只会在发现 ISE 后获取该配置文件，这有可能导致错误。因此，在连接到 VPN 时，建议使用 ASA 推送 ISE 终端安全评估模块。



---

**注释** 当思科 ISE 与 ASA 集成时，请确保在 ASA 中将记帐模式设置为单一 (Single)。记帐数据在“单一” (Single) 模式下仅发送到一个记帐服务器。

---

### 开始之前

在配置 AnyConnect 配置对象之前，必须：

1. 从 [Cisco 软件下载页面](#) 下载 AnyConnect 前端部署数据包和合规性模块。
2. 将这些资源上传到思科 ISE（请参阅 [从本地计算机添加思科提供的客户端调配资源](#)，第 650 页）。
3. （可选）添加自定义和本地化捆绑包（请参阅 [从本地计算机添加 AnyConnect 的客户创建资源](#)，第 650 页）。
4. 配置 AnyConnect 终端安全评估代理配置文件（请参阅 [创建终端安全评估代理配置文件](#)，第 655 页）。

---

**步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources)。

**步骤 2** 点击 添加 创建 AnyConnect 配置。

**步骤 3** 选择 AnyConnect 配置。

- 步骤 4** 选择您之前上传的 AnyConnect 软件包。例如，AnyConnect DesktopWindows xxx.x.xxxxx.x。
- 步骤 5** 输入当前 AnyConnect 配置的名称。例如，AC Config xxx.x.xxxxx.x。
- 步骤 6** 选择您之前上传的合规性模块。例如，AnyConnect ComplianceModulewindows x.x.xxxx.x。
- 步骤 7** 选中一个或多个 AnyConnect 模块复选框。例如，从下列软件中选择一个或多个模块：ISE Posture、VPN、网络访问管理器、网络安全、ASA Posture、Start Before Log on（仅适用于 Windows OS）以及诊断和报告工具。
- 注释** 取消选中 AnyConnect 模块选择下的 VPN 模块，不会在调配的客户端禁用 VPN 磁贴。您必须配置 VPNDisable\_ServiceProfile.xml，才能在 AnyConnect GUI 上禁用 VPN 磁贴。在将 AnyConnect 安装到默认位置的系统中，可以在 C:\Program Files\Cisco 下找到此文件。如果 AnyConnect 安装到不同位置，则此文件将位于 <AnyConnect 安装的路径>\Cisco 下。
- 步骤 8** 为选定的 AnyConnect 模块选择 AnyConnect 配置文件。例如，ISE Posture、VPN、NAM 和网络安全模块。
- 步骤 9** 选择 AnyConnect 自定义和本地化捆绑包。
- 步骤 10** 点击提交。

---

## 创建终端安全评估代理配置文件

按照此程序创建 AnyConnect 或 NAC 终端安全评估代理配置文件，您可以在其中指定参数以定义终端安全评估协议的代理行为。

- 步骤 1** 选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 客户端调配 (Client Provisioning) > 资源 (Resources)。
- 步骤 2** 点击添加 (Add)。
- 步骤 3** 选择 NAC AnyConnect 代理终端安全评估配置文件 (NAC AnyConnect Agent Posture Profile)。
- 步骤 4** 在 终端代理配置文件设置下，选择 AnyConnect 或 NAC 代理。
- 步骤 5** 配置以下各项的参数：
- 思科 ISE 终端安全评估代理行为
  - 客户端 IP 地址更改
  - 思科 ISE 安全评估协议
- 步骤 6** 点击提交。

---

## 客户端 IP 地址刷新配置

下表描述 NAC AnyConnect 终端安全评估配置文件窗口中的字段，您可以通过此窗口为客户端配置在 VLAN 更改之后要更新或刷新其 IP 地址的参数。选择 Policy > Policy Elements > Results > Client Provisioning > Resources > Add > NAC or AnyConnect Posture Profile。

字段名称	默认值	模式（仅适用于思科 NAC 代理）	使用指南
“VLAN 检测时间间隔” (VLAN detection interval)	0, 5	合并	<p>此设置是代理检查 VLAN 更改的时间间隔。</p> <p>对于 Windows NAC 代理，默认值为 0。默认情况下，对 Windows 禁用访问身份验证 VLAN 更改功能。有效范围为 0 至 5 秒。</p> <p>对于 Mac OS X 代理，默认值为 5。默认情况下，已启用访问身份验证 VLAN 更改功能，对于 Mac OS X，VlanDetectInterval 为 5 秒。有效范围为 5 至 900 秒。</p> <p>0 - 禁用访问身份验证 VLAN 更改功能。</p> <p>1 至 5 - 代理每隔 5 秒发送一个互联网控制消息协议 (ICMP) 或地址解析协议 (ARP) 查询。</p> <p>6 至 900 - 每隔 x 秒发送一个 ICMP 或 ARP 查询。</p>
Enable VLAN detection without UI（不适用于 Mac OS X 客户端）	否	合并	<p>即使用户未登录，此设置仍可启用或禁用 VLAN 检测。</p> <p>“否” - 禁用 VLAN 检测功能。</p> <p>“是” - 启用 VLAN 检测功能。</p>



字段名称	默认值	模式（仅适用于思科 NAC 代理）	使用指南
“重试检测计数” (Retry detection count)	3	合并	如果互联网控制消息协议 (ICMP) 或地址解析协议 (ARP) 轮询失败，此设置将代理配置为重试 x 次再刷新客户端 IP 地址。
“Ping 命令或 ARP” (Ping 命令或 ARP)	0 有效范围为 0 至 2。	合并	此设置指定用于检测客户端 IP 地址更改的方法。 0 - 使用 ICMP 轮询 1 - 使用 ARP 轮询 2 - 首先使用 ICMP 轮询，然后（如果 ICMP 失败）使用 ARP 轮询
“ping 命令最长超时时间” (Maximum timeout for ping)	1 有效范围为 1 至 10 秒。	合并	使用 ICMP 轮询，并且如果在指定时间内没有响应，则宣布 ICMP 轮询失败。
“启用代理 IP 地址刷新” (Enable agent IP refresh)	“是”（默认值）	覆盖	指定在交换机（或 WLC）更改相应交换机端口上客户端登录会话的 VLAN 之后客户端设备是否更新或刷新其 IP 地址。
“DHCP 更新延迟” (DHCP renew delay)	0 有效范围为 0 至 60 秒。	覆盖	此设置指定客户端设备在尝试向网络 DHCP 服务器请求新 IP 地址之前等待的时间。
“DHCP 释放延迟” (DHCP release delay)	0 有效范围为 0 至 60 秒。	覆盖	此设置指定客户端设备在释放当前 IP 地址之前等待的秒数。



注释 将参数值与现有代理配置文件设置合并或覆盖这些设置，从而相应地配置 Windows 客户端和 Mac OS X 客户端以刷新 IP 地址。

## 安全评估协议设置

### 思科 Web 代理

思科 Web 代理为客户端设备提供临时安全评估。

用户可以启动思科 Web 代理可执行文件，此文件会通过 ActiveX 控件或 Java 小应用程序在客户端设备上的临时目录中安装 Web 代理文件。

用户登录思科 Web 代理后，Web 代理会从思科 ISE 服务器获取为用户角色和操作系统配置的要求，检查主机注册表、进程、应用和服务以获取所需的数据包，并向思科 ISE 服务器发回报告。如果客户端设备满足这些要求，用户就可以访问网络。如果不满足这些要求，Web 代理会向用户显示对话框，指出没有满足的各项要求。此对话框会为用户提供让客户端设备满足要求的说明和应执行的操作。或者，如未满足指定的要求，用户可以选择接受有限网络访问，同时尝试对客户端系统进行补救以满足对用户登录角色的要求。



---

**注释** 仅 32 位版本的 Internet Explorer 支持 ActiveX。无法安装在 Firefox Web 浏览器或 64 位版本的 Internet Explorer 上安装 ActiveX。

---

### 思科 NAC 代理 XML 文件安装目录

在一个将思科 NAC 代理安装在默认位置的系统中，您可以在以下目录中找到下列 .xml 文件：

- nac\_login.xml 文件位于 “C:\Program Files\Cisco\Cisco NAC Agent\UI\nac\_divs\login” 目录中。
- nacStrings\_xx.xml 文件中的 “xx” 表示区域设置。您可以在 “C:\Program Files\Cisco\Cisco NAC Agent\UI\cues\_utility” 目录中找到完整的文件列表。

如果代理安装在其他位置，则文件应位于 “<代理安装路径>\Cisco\Cisco NAC Agent\UI\nac\_divs\login” 和 “<代理安装路径>\Cisco\Cisco NAC Agent\cues\_utility”。

### 适用于 Windows 客户端的思科 NAC 代理

思科 NAC 代理为客户端设备提供安全状态评估和补救。

用户可以下载并安装思科 NAC 代理（只读客户端软件），它可以检查主机历史记录、进程、应用和服务。思科 NAC 代理可用于执行 Windows 更新或防病毒和反间谍软件定义更新，启动合格补救程序，将上传的文件分发给思科 ISE 服务器，分发网站链接以供用户下载文件来修复他们的系统，或单纯用于分发信息和说明。

思科强烈建议您确保在 Windows XP 客户端上安装最新的 Windows 修补程序和补丁，从而使思科 NAC 代理可以与思科 ISE 建立安全的加密通信（通过 SSL over TCP）。

## 从 Windows 7 及早期版本客户端中卸载思科 NAC 代理

思科 NAC 代理安装在 Windows 客户端上的 **C:\Program Files\Cisco\Cisco NAC Agent\**。

您可以用以下方式卸载代理：

- 双击 **Uninstall Cisco NAC Agent** 桌面图标。
- 前往开始菜单 > 程序 (Programs) > 思科系统 (Cisco Systems) > 思科 Clean Access (Cisco Clean Access) > 卸载思科 NAC 代理 (Uninstall Cisco NAC Agent)
- 依次选择 **Start Menu > Control Panel > Add or Remove Programs > Cisco NAC Agent** 并卸载思科 NAC 代理。

## 在 Windows 8 客户端中卸载思科 NAC 代理

可以在 Metro 模式下在 Windows 8 客户端中卸载思科 NAC 代理。

**步骤 1** 切换到 Metro 模式。

**步骤 2** 右键单击 **Cisco NAC Agent** 缩略图。

**步骤 3** 从屏幕底部的选项中选择 **Un-Install**。

**步骤 4** 系统自动切换到桌面模式，打开 **Add/Remove** 控制面板。

**步骤 5** 在 **Add/Remove** 控制面板中，执行以下操作之一：

- a) 双击 **Cisco NAC Agent**，点击 **Uninstall**。
- b) 选择 **Cisco NAC Agent**，点击 **Uninstall**。
- c) 右键单击 **Cisco NAC Agent**，选择 **Uninstall**。

## Windows 8 Metro 和 Metro 应用支持 - Toast 通知

思科 NAC 代理托盘图标上显示 **Enable Toast Notification** 选项，使用该选项可以将相关通知发送至 Windows 8 客户端上的用户。

在思科 NAC 代理场景中，如果用户没有获得网络访问权限，例如“补救失败”或“网络访问权限已到期”，代理会显示以下 Toast 通知：**Network not available, Click "OK" to continue**。

为了获取更多详细信息，您可以选择 **Toast**，系统会将您重定向至桌面模式，并显示思科 NAC 代理对话框。

对于用户需要执行才能获得网络访问权限的所有积极的建议操作，系统都会显示 **Toast** 通知。以下列出某些示例：

- 对于网络接受策略，**Toast** 通知将显示为：“**Click Accept to gain network access**”
- 对于代理/兼容模块升级，**Toast** 通知将显示为：“**Click OK to Upgrade/Update**”

- 在“用户已注销”事件中，当 Clean Access Manager (CAM) 中未启用用于注销的“Auto Close”选项时，系统会显示 Toast 通知。通过该 Toast 通知，用户知道他们已注销并且需要再次登录才能获得网络访问权限。

## 适用于 Macintosh 客户端的思科 NAC 代理

思科 NAC OS X 代理为 Macintosh 客户端计算机提供安全评估和补救。

用户可以下载并安装思科 NAC OS X 代理（只读客户端软件），该代理可检查防病毒和反间谍软件定义更新。

在用户登录到思科 NAC OS X 代理后，代理会从思科 ISE 服务器获取针对用户角色和操作系统配置的要求，检查所需软件包并向思科 ISE 服务器发回报告。如果在客户端上满足要求，则允许用户进行网络访问。如果未满足要求，则代理会针对未满足的每项要求向用户显示一个对话框。此对话框会为用户提供让客户端设备满足要求的说明和应执行的操作。或者，如果未满足指定要求，则用户可以在尝试补救客户端系统时接受受限网络访问。

## 从 Macintosh 客户端卸载思科 NAC 代理

您可以通过运行如下所示的卸载脚本，为 Mac OS X 客户端卸载思科 NAC 代理：

---

**步骤 1** 打开导航器窗格，并导航至 <本地驱动器 ID> > 应用 (Applications)。

**步骤 2** 突出显示并右键单击 CCAgent 图标，以显示选择菜单。

**步骤 3** 选择显示软件包内容 (Show Package Contents) 并双击 NacUninstall，可在 Mac OS X 上卸载思科 NAC 代理。

---

## 思科 Web 代理

思科 Web 代理为客户端设备提供临时安全评估。

用户可以启动思科 Web 代理可执行文件，此文件会通过 ActiveX 控件或 Java 小应用程序在客户端设备上的临时目录中安装 Web 代理文件。

用户登录思科 Web 代理后，Web 代理会从思科 ISE 服务器获取为用户角色和操作系统配置的要求，检查主机注册表、进程、应用和服务以获取所需的数据包，并向思科 ISE 服务器发回报告。如果客户端设备满足这些要求，用户就可以访问网络。如果不满足这些要求，Web 代理会向用户显示对话框，指出没有满足的各项要求。此对话框会为用户提供让客户端设备满足要求的说明和应执行的操作。或者，如未满足指定的要求，用户可以选择接受有限网络访问，同时尝试对客户端系统进行补救以满足对用户登录角色的要求。



---

**注释** 仅 32 位版本的 Internet Explorer 支持 ActiveX。无法安装在 Firefox Web 浏览器或 64 位版本的 Internet Explorer 上安装 ActiveX。

---

## 思科 NAC 代理日志

在适用于 Windows 的思科 NAC 代理中，右键单击代理托盘图标，然后单击 **Log Packager** 以运行支持包并收集代理日志。

在适用于 NAC OS X 的思科 NAC 代理中，点击 Tools 菜单，右键单击 Agent 图标，然后单击 **Collect Support Logs** 选项，以收集代理日志和支持信息。所收集的信息以 zip 文件形式提供。用户可以选择文件位置和文件名以保存文件。默认情况下，此文件以 *CiscoSupportReport.zip* 作为文件名，保存于桌面上。

如果代理崩溃或挂起，您可以运行 **CCAAgentLogPackager.app** 以收集日志。可于 `/Applications/CCAAgent.app` 处获得此文件。您可以右键单击 **CCAAgent.app**，选择 **Show Package Contents**，然后双击 **CCAAgentLogPackager**，以收集支持信息。

## 为思科 NAC 代理创建代理自定义文件

使用代理自定义文件，可以自定义思科 NAC 代理屏幕对话框中包含的徽标、字段和消息文本，适应特定的 Windows 客户端网络访问要求。

您可以将自定义软件包创建成一个包含 XML 描述符文件的 .zip 文件和另一个包含构成自定义选项的内容的 .zip 文件。

---

**步骤 1** 安装构成代理屏幕自定义软件包所需的文件：

- 自定义的 `nac_login.xml` 文件
- 创建为 .gif 文件的自定义公司/企业徽标
- 一个或多个自定义的 `nacStrings_xx.xml` 文件
- 自定义的 `updateFeed.xml` descriptor 文件

**步骤 2** 创建一个名为“brand-win.zip”的 zip 文件，其中包含已安装的文件。例如，在 Linux 或 UNIX 环境中，请执行以下操作：**zip -r brand-win.zip nac\_login.xml nac\_logo.gif nacStrings\_en.xml nacStrings\_cy.xml nacStrings\_el.xml**

**步骤 3** 创建一个“custom.zip”文件，其中包含适当的 `updateFeed.xml` 描述符文件和上面创建的 .zip 文件。例如，在 Linux 或 UNIX 环境中，请执行以下操作：**zip -r custom.zip updateFeed.xml brand-win.zip**

**步骤 4** 将得到的“custom.zip”文件保存到本地计算机上的某个位置，方便在将文件上传到思科 ISE 时访问。

---

## 自定义 `nac_login.xml` 文件模板

`nac_login.xml` 文件是您的代理屏幕自定义软件包中需要的文件之一，您可通过此文件自定义思科 NAC 代理对话框（例如 Properties 窗口）中包含的徽标、字段和消息文本，以满足您的特定 Windows 客户端网络接入要求。

使用以下模板构建适当的“`nac_login.xml`”文件，自定义思科 NAC 代理屏幕中包含的徽标、字段和消息文本。

以下是一个自定义文件示例。

```
<tr class="nacLoginMiddleSectionContainerInput">
<td colspan="2">
<fieldset width="100%" id="nacLoginCustomAlert" style="display:block"
class="nacLoginAlertBox">
<table width="100%">
<tr>
<td id="nacLoginCustomAlert.img" valign="top" width="32px">
</img>
</td>
<td id="nacLoginCustomAlert.content" class="nacLoginAlertText">
<cues:localize key="login.customalert"/>
</td>
</tr>
</table>
</fieldset>
</td>
</tr>
<tr id="nacLoginRememberMe" style="visibility:hidden">
<td>
<cues:localize key="cd.nbsp"/>
</td>
<td class="cuesLoginField">
<nobr>
<input type="checkbox" alt="" title="" name="rememberme" id="rememberme" checked="true"/>
<cues:localize key="login.remember_me"/>
</nobr>
</td>
</tr>
```

## 自定义 nacStrings\_xx.xml 文件模板

这是在代理屏幕自定义软件包中需要的其中一个文件，使您能够对思科NAC代理对话框（如Properties屏幕）中包含的徽标、字段和消息文本进行自定义，以满足特定 Windows 客户端网络访问要求。

使用以下模板构建一个或多个 nnacStrings\_xx.xml 文件，其中 xx 是具体语言的双字符标识符。

以下是自定义 nacStrings\_xx.xml 文件示例。

```
<cueslookup:appstrings xmlns:cueslookup="http://www.cisco.com/cues/lookup">
<cueslookup:name key="nac.brand.legal_name">Cisco Systems, Inc.</cueslookup:name>
<cueslookup:name key="nac.brand.full_name">Cisco Systems</cueslookup:name>
<cueslookup:name key="nac.brand.short_name">Cisco</cueslookup:name>
<cueslookup:name key="nac.brand.abbreviation">Cisco</cueslookup:name>
<cueslookup:name key="nac.copyright">Copyright </cueslookup:name>
<cueslookup:name key="nac.copyright.period">2009-2013</cueslookup:name>
<cueslookup:name key="nac.copyright.arr">All Rights Reserved</cueslookup:name>
<cueslookup:name key="updateagent.rqst">NAC Agent %1 is available.%br% Do you want to install
this update now?</cueslookup:name>
<cueslookup:name key="updateagent.rqst.retry">Unable to update NAC Agent. Please try
again.</cueslookup:name>
<cueslookup:name key="downloadagent.report">Downloading the update of NAC
Agent.</cueslookup:name>
<cueslookup:name key="downloadagent.packagename.label">Package Name</cueslookup:name>
<cueslookup:name key="downloadagent.completed.label">Completed</cueslookup:name>
<cueslookup:name key="downloadagent.completed.value">%1 of %2 bytes</cueslookup:name>
<cueslookup:name key="downloadagent.speed.label">Speed</cueslookup:name>
<cueslookup:name key="downloadagent.speed.value">%1 bytes/sec</cueslookup:name>
<cueslookup:name key="updateopswat.rqst">NAC Agent Posture component version %1 is
```

```

available.%br% Do you want to install this update now?</cueslookup:name>
<cueslookup:name key="updateopswat.rqst.retry">Unable to update NAC Agent Posture component.
Please try again.</cueslookup:name>
<cueslookup:name key="downloadopswat.report">Downloading the update of NAC Agent Posture
component.</cueslookup:name>
<cueslookup:name key="login.productname">Education First Compliance Check</cueslookup:name>

<cueslookup:name key="login.version">Version</cueslookup:name>
<cueslookup:name key="login.opswatversion">Posture Component Version</cueslookup:name>
<cueslookup:name key="login.username">Enter your username</cueslookup:name>
<cueslookup:name key="login.password">Enter your PIN</cueslookup:name>
<cueslookup:name key="login.remember_me">Remember Me</cueslookup:name>
<cueslookup:name key="login.server">Server</cueslookup:name>
<cueslookup:name key="login.customalert">Custom EF package version 2.1.1.1 with EF
Logo</cueslookup:name>
<cueslookup:name key="login.Too many users using this account">This account is already
active on another device</cueslookup:name>
<cueslookup:name key="login.differentuser">Login as Different User</cueslookup:name>
<cueslookup:name key="login.removeoldest">Remove Oldest Login Session</cueslookup:name>
<cueslookup:name key="menu_devtools">Dev Tools</cueslookup:name>
<cueslookup:name key="c.sso.ad">Performing Windows Domain automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.generic">Unknown authentication type</cueslookup:name>
<cueslookup:name key="c.sso.macauth">Performing device filter automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.vpn">Performing automatic login into NAC environment for remote
user</cueslookup:name>
<cueslookup:name key="c.title.status.authenticating">Authenticating User</cueslookup:name>

<cueslookup:name key="c.title.status.answeringchallenge">Sending Response</cueslookup:name>

<cueslookup:name key="c.title.status.checking">Checking Requirements</cueslookup:name>
<cueslookup:name key="c.title.status.checkcomplete">System Check Complete</cueslookup:name>

<cueslookup:name key="c.title.status.loggedin">NAC Process Completed</cueslookup:name>
<cueslookup:name key="c.title.status.netaccess.none">NAC Process Completed</cueslookup:name>

<cueslookup:name key="c.title.status.netpolicy">Network Usage Policy</cueslookup:name>
<cueslookup:name key="c.title.status.properties">Agent Properties &
Information</cueslookup:name>
<cueslookup:name key="c.title.status.remediating">Remediating System</cueslookup:name>
<cueslookup:name key="c.title.status.session.expired">Session has Expired</cueslookup:name>

<cueslookup:name key="c.title.status.update.available">Update Agent</cueslookup:name>
<cueslookup:name key="c.title.status.update.downloading">Downloading Agent</cueslookup:name>

<cueslookup:name key="c.title.status.update.opswat.available">Update Posture
Component</cueslookup:name>
<cueslookup:name key="c.title.status.update.opswat.downloading">Downloading Posture
Component</cueslookup:name>
<cueslookup:name key="scanning">Checking</cueslookup:name>
<!-- <cueslookup:name key="scanningitemcomplete">Finished Checking</cueslookup:name> -->
<cueslookup:name key="ph.about">About</cueslookup:name>
<cueslookup:name key="ph.cancel">Cancel</cueslookup:name>
<!-- <cueslookup:name key="ph.details">Details</cueslookup:name> -->
<cueslookup:name key="ph.logout">Logout</cueslookup:name>
<cueslookup:name key="title_remediating">Remediating System</cueslookup:name>
<cueslookup:name key="title_check_complete">System Check Complete</cueslookup:name>
<cueslookup:name key="title_full_access_granted">Logged In</cueslookup:name>
<cueslookup:name key="title_access_denied">Network Access Denied</cueslookup:name>
<cueslookup:name key="tempNetAccess">Temporary Network Access</cueslookup:name>
<cueslookup:name key="announcePleaseBePatient">Please be patient while your system is checked
against the network security policy
</cueslookup:name>

```

```

<cueslookup:name key="btn.accept">Accept</cueslookup:name>
<cueslookup:name key="btn.apply">Apply</cueslookup:name>
<cueslookup:name key="btn.cancel">Cancel</cueslookup:name>
<cueslookup:name key="btn.continue">Update Later</cueslookup:name>
<cueslookup:name key="btn.close">Close</cueslookup:name>
<cueslookup:name key="btn.detailshide">Hide Compliance</cueslookup:name>
<cueslookup:name key="btn.detailsshow">Show Compliance</cueslookup:name>
<cueslookup:name key="btn.download">Download</cueslookup:name>
<cueslookup:name key="btn.guestAccess">Guest Access</cueslookup:name>
<cueslookup:name key="btn.go2link">Go To Link</cueslookup:name>
<cueslookup:name key="btn.launch">Launch</cueslookup:name>
<cueslookup:name key="btn.login">Log In</cueslookup:name>
<cueslookup:name key="btn.next">Re-Scan</cueslookup:name>
<cueslookup:name key="btn.ok">OK</cueslookup:name>
<cueslookup:name key="btn.propertieshide">Hide Properties</cueslookup:name>
<cueslookup:name key="btn.reject">Reject</cueslookup:name>
<cueslookup:name key="btn.remediate">Repair</cueslookup:name>
<cueslookup:name key="btn.rescan">Rescan</cueslookup:name>
<cueslookup:name key="btn.reset">Reset</cueslookup:name>
<cueslookup:name key="btn.restrictedNet">Get Restricted NET access This one comes down
from the network</cueslookup:name>
<cueslookup:name key="btn.saverreport">Save Report</cueslookup:name>
<cueslookup:name key="btn.skip">Skip</cueslookup:name>
<cueslookup:name key="btn.skipao">Skip All Optional</cueslookup:name>
<cueslookup:name key="btn.submit">Submit</cueslookup:name>
<cueslookup:name key="btn.update">Update</cueslookup:name>
<cueslookup:name key="cd.days">
days
</cueslookup:name>
<cueslookup:name key="cd.nbsp">

</cueslookup:name>
<cueslookup:name key="cd.tempNetAccess.counting">
There is approximately %1 left until your temporary network access expires
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccess.expired">
Your Temporary Network Access has Expired!
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccessShort.counting">
%1 left
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccessShort.expired">
Expired!
</cueslookup:name>
<cueslookup:name key="cd.window.counting">
This window will close in %1 secs
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess">
Full Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">
Your device conforms with all the security policies for this protected
network
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">
Only optional requirements are failing.
It is recommended that you update your system at
your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">
Refreshing IP address. Please Wait...
</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">
Refreshing IP address succeeded.

```



```
</cueslookup:name>
<cueslookup:name key="dp.status.vlanchange.progress.verbose">
Connecting to protected Network. Please Wait...
</cueslookup:name>
<cueslookup:name key="dp.status.guestNetAccess">
Guest Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess">
Network Access Denied
</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess.verbose">
There is at least one mandatory requirement failing.
You are required to update your system before
you can access the network.
</cueslookup:name>
<cueslookup:name key="dp.status.rejectNetPolicy.verbose">
Network Usage Terms and Conditions are rejected. You will not be
allowed to access the network.
</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">
Restricted Network Access granted.
</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">
You have been granted restricted network access because your device
did not conform with all the security policies for this protected
network and you have opted to defer updating your system. It is recommended
that you update your system at your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">
Temporary Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">
Please be patient while your system is checked against the network security policy.
</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">
Performing Re-assessment
</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">
There is at least one mandatory requirement failing.
You are required to update your system otherwise
your network access will be restricted.
</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">
Performing Re-assessment
</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">
Only optional requirements are failing.
It is recommended that you update your system at
your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">
Logged out
</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">
Temporary Access to the network has expired.
</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">
Logged out
</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose">

</cueslookup:name>
<cueslookup:name key="ia.status.checkcomplete">
Finished Checking Requirements
```

```
</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress">
Please be patient while we determine if your system is compliant with the security policy
</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress.01">
Checking %1 out of %2
</cueslookup:name>
<cueslookup:name key="ia.status.netpolicy">
Access to the network requires that you view and accept the following
Network Usage Policy
</cueslookup:name>
<cueslookup:name key="ia.status.netpolicylinktxt">
Network Usage Policy Terms and Conditions
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.inprogress">
Remediating
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.start">
Please Remediate
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.checkinprogress">
Checking for compliance with Requirement
</cueslookup:name>
<cueslookup:name key="ia.table.name">
Name
</cueslookup:name>
<cueslookup:name key="ia.table.location">
Location
</cueslookup:name>
<cueslookup:name key="ia.table.software">
Software
</cueslookup:name>
<cueslookup:name key="ia.table.software.programs">
program(s)
</cueslookup:name>
<cueslookup:name key="ia.table.update">
Update
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.nochange">
Do not change current setting
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforedownload">
Notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforeinstall">
Notify before install
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.scheduledinstallation">
Download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforedownload">
Change to notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforeinstall">
Change to notify before installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcescheduledinstall">
Change to download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.description">
Description
</cueslookup:name>
<cueslookup:name key="scs.table.title">
Security Compliance Summary
```

```
</cueslookup:name>
<cueslookup:name key="scs.table.header1.scan_rslt">
Scan Result
</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_name">
Requirement Name
</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_details">
Requirement Description - Remediation Suggestion
</cueslookup:name>
<cueslookup:name key="scs.table.data.mandatory">
Mandatory
</cueslookup:name>
<cueslookup:name key="scs.table.data.optional">
Optional
</cueslookup:name>
<cueslookup:name key="scs.table.data.pass">
Passed
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_download">
Please download and install the optional software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_download">
Please download and install the required software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_launch">
Please launch the optional remediation program(s) before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_launch">
Please launch the required remediation program(s) before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_av">
Please update the virus definition file of the specified antivirus software before accessing
the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_av">
Please update the virus definition file of the specified antivirus software before accessing
the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_as">
Please update the spyware definition file of the specified anti-spyware software before
accessing the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_as">
Please update the spyware definition file of the specified anti-spyware software before
accessing the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_win_update">
Please download and install the optional windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_win_update">
Please download and install the required windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_prog">
Launching Remediation Program(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_url">
Launching Remediation URL...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_av">
Updating Virus Definition...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_as">
Updating Spyware Definition...
```

```

</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_win_update">
Launching Windows auto Update(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_launch_downloaded_file">
Downloaded at %1. %br% Please open this folder & double-click executable file to install
the required software.
</cueslookup:name>
<cueslookup:name key="discoveryhost.label">
Discovery Host
</cueslookup:name>
<cueslookup:name key="properties.table.title">
List of Antivirus & Anti-Spyware Products Detected by the Agent
</cueslookup:name>
<cueslookup:name key="properties.table.header1.index">
No.
</cueslookup:name>
<cueslookup:name key="properties.table.header1.description">
Description
</cueslookup:name>
<cueslookup:name key="properties.table.header1.value">
Value
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_type">
Product Type
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_name">
Product Name
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_version">
Product Version
</cueslookup:name>
<cueslookup:name key="properties.table.data.def_version">
Definition Version
</cueslookup:name>
<cueslookup:name key="properties.table.data.def_date">
Definition Date
</cueslookup:name>
<cueslookup:name key="reboot.mandatory.001">
Mandatory System Reboot Required
</cueslookup:name>
<cueslookup:name key="reboot.optional.001">
You need to reboot your system in order for the changes to take effect.
</cueslookup:name>
<cueslookup:name key="rem.error.001">
Unable to remediate particular requirement
</cueslookup:name>
<cueslookup:name key="rem.error.av_access_denied">
The remediation you are attempting is reporting an access denied error. This is usually due
to a privilege issue. Please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_buffer_too_small">
The remediation you are attempting has failed with an internal error. Please contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_elevation_required">
The remediation you are attempting requires elevation. Please contact your system
administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_failed">
The remediation you are attempting had a failure. If the problem persists contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_internal_error">

```

```
The remediation you are attempting has reported an internal error. If this problem persists
  please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_not_implemented">
The remediation you are attempting is not implemented for this product. Please contact your
  system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_not_supported">
The remediation you are attempting is not supported for this product. Please contact your
  system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_update_faile">
The AV/AS update has failed. Please try again and if this message continues to display
  contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_update_failed_due_to_network">
The AV/AS update failed due to a networking issue. Please try again and if this message
  continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_timeout">
The remediation you are attempting has timed out waiting for the operation to finish. If
  this continues please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_dist_size_error">
The size of the downloaded file does not match the package! Please discard downloaded file
  and check with your administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_is_not_signed">
The file that has been requested was not digitally signed. Please try again and if this
  message continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_save_location_error">
The location for the file to be saved to can not be written. Please choose a different
  location.
</cueslookup:name>
<cueslookup:name key="rem.error.http_file_not_found">
The requested file is not found. Please try again and if this problem persists, contact
  your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.launch_file_not_found">
The file that has been requested could not be launched either because it could not be found
  or there was a problem launching it. Please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.malformed_URL">
The file that is trying to be downloaded has an incorrect URL. Please contact your system
  administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.network_error">
There has been a network error, please try the remediation again. If this message continues
  to be seen contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.update_fail_for_non_admin">
The remediation you are trying to do can not be accomplished at your user level. Please
  contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.wsus_search_failure">
The WSUS search failed. This is probably due to a network issue. Please try again and if
  this message continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="server.error.generic">
Agent encountered problems logging user
</cueslookup:name>
<cueslookup:name key="server.error.255">
Network Error: NAC Server could not establish a secure connection to NAC Manager.
```

This could be due to one or more of the following reasons:

- 1) NAC Manager certificate has expired or
- 2) NAC Manager certificate cannot be trusted or
- 3) NAC Manager cannot be reached or
- 4) NAC Manager is not responding

Please report this to your network administrator.

</cueslookup:name>

<cueslookup:name key="server.error.5000">

Invalid provider name

</cueslookup:name>

<cueslookup:name key="server.error.5001">

Failed to add user to online list

</cueslookup:name>

<cueslookup:name key="server.error.5002">

Server communication error

</cueslookup:name>

<cueslookup:name key="server.error.5003">

Invalid username or password

</cueslookup:name>

<cueslookup:name key="server.error.5004">

Unknown user

</cueslookup:name>

<cueslookup:name key="server.error.5005">

Account expired

</cueslookup:name>

<cueslookup:name key="server.error.5006">

Account currently disabled

</cueslookup:name>

<cueslookup:name key="server.error.5007">

Exceed quota limit

</cueslookup:name>

<cueslookup:name key="server.error.5008">

Insufficient Clean Access packages installed

</cueslookup:name>

<cueslookup:name key="server.error.5009">

Access to network is blocked by the administrator

</cueslookup:name>

<cueslookup:name key="server.error.5010">

Vulnerabilities not fixed

</cueslookup:name>

<cueslookup:name key="server.error.5011">

This client version is old and not compatible. Please login from web browser to see the download link for the new version.

</cueslookup:name>

<cueslookup:name key="server.error.5012">

Network policy is not accepted

</cueslookup:name>

<cueslookup:name key="server.error.5013">

Invalid switch configuration

</cueslookup:name>

<cueslookup:name key="server.error.5014">

Too many users using this account

</cueslookup:name>

<cueslookup:name key="server.error.5015">

Invalid session

</cueslookup:name>

<cueslookup:name key="server.error.5016">

Null session

</cueslookup:name>

<cueslookup:name key="server.error.5017">

Invalid user role

</cueslookup:name>

<cueslookup:name key="server.error.5018">

Invalid login page

```
</cueslookup:name>
<cueslookup:name key="server.error.5019">
Encoding failure
</cueslookup:name>
<cueslookup:name key="server.error.5020">
A security enhancement is required for your Agent. Please upgrade your Agent or contact
your network administrator.
</cueslookup:name>
<cueslookup:name key="server.error.5021">
Can not find server reference
</cueslookup:name>
<cueslookup:name key="server.error.5022">
User role currently disabled
</cueslookup:name>
<cueslookup:name key="server.error.5023">
Authentication server is not reachable
</cueslookup:name>
<cueslookup:name key="server.error.5024">
Agent user operating system is not supported
</cueslookup:name>
<cueslookup:name key="server.error.generic_emergency">
The Agent has encountered an unexpected error and is restarting.
</cueslookup:name>
<cueslookup:name key="server.error.http_error">
Clean Access Server is not available on the network.
</cueslookup:name>
<cueslookup:name key="server.error.nw_interface_chg">
Authentication interrupted due to network status change. Press OK to retry.
</cueslookup:name>
<cueslookup:name key="server.error.svr_misconfigured">
Clean Access Server is not properly configured.
</cueslookup:name>
<cueslookup:name key="server.clarification.generic_emergency">
Please contact your administrator if the problem persists.
</cueslookup:name>
<cueslookup:name key="announce.savingreport">
Saving Report
</cueslookup:name>
<cueslookup:name key="announce.savingreport.failed">
Unable to save report
</cueslookup:name>
<cueslookup:name key="announce.cancelremediationack">
Clicking Cancel may change your network connectivity and interrupt download or required
updates.<p> Do you want to continue?</p>
</cueslookup:name>
<cueslookup:name key="announce.dismiss.default">
Dismiss to continue
</cueslookup:name>
<cueslookup:name key="announce.logoutconfirm">
Successfully logged out from the network!
</cueslookup:name>
</cueslookup:appstrings>
```



**注释** 可用于自定义文本的字符没有数量限制。但是，思科建议限制字符长度，确保在所产生的自定义登录屏幕显示于客户端上时，这些字段不会占用太多空间。

## 扩展的 nacStrings\_xx.xml 文件示例

```

<cueslookup:name key="dp.status.fullNetAccess">Full Network Access</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">Your device conforms with all the
security policies for this protected network</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">Only optional requirements are
failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">Refreshing IP address. Please
Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">Refreshing IP address
succeeded.</cueslookup:name>
<cueslookup:name key="dp.status.vlanchange.progress.verbose">Connecting to protected Network.
Please Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.guestNetAccess">Guest Network Access</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess">Network Access Denied</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess.verbose">There is at least one mandatory
requirement failing. You are required to update your system before you can access the
network.
</cueslookup:name><cueslookup:name key="dp.status.rejectNetPolicy.verbose">Network Usage
Terms and Conditions are rejected. You will not be allowed to access the
network.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">Restricted Network Access
granted.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">You have been granted restricted
network access because your device did not conform with all the security policies for this
protected network and you have opted to defer updating your system. It is recommended that
you update your system at your earliest convenience.</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">Temporary Network Access</cueslookup:name>

<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">Please be patient
while your system is checked against the network security policy.</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">There is at least one mandatory
requirement failing. You are required to update your system otherwise your network access
will be restricted.</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">Only optional requirements are
failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">Temporary Access to the network has
expired.</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose"> </cueslookup:name>

```

## UpdateFeed.xml 描述符文件模板

这是在代理屏幕自定义软件包中需要的其中一个文件，使您能够对思科NAC代理对话框（如Properties屏幕）中包含的徽标、字段和消息文本进行自定义，以满足特定 Windows 客户端网络访问要求。

必须先构建合适的 updateFeed.xml 描述符文件，才能完成代理屏幕自定义软件包。使用以下示例作为模板，以设置自定义软件包所需的 updateFeed.xml 描述符文件。

```

<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:update="http://www.cisco.com/cpm/update/1.0">

<title>Provisioning Update</title>
<updated>2011-12-21T12:00:00Z</updated>
<id>https://www.cisco.com/web/secure/pmbu/provisioning-update.xml</id>

```



```

<author>
<name>Cisco Support</name>
<email>support@cisco.com</email>
</author>
<!-- Custom Branding -->
<entry>
<id>http://foo.foo.com/foo/AgentCustomizationPackage/1/1/1/7</id>
<title>Agent Customization Package</title>
<updated>2010-06-07T12:00:00Z</updated>
<summary>This is EF Agent Customization Package 1.1.1.7</summary>
<link rel="enclosure" type="application/zip" href="brand-win.zip" length="18884" />
<update:type>AgentCustomizationPackage</update:type>
<update:version>1.1.1.7</update:version>
<update:os>WINDOWS_ALL</update:os>
</entry>
</feed>

```

在创建 updateFeed.xml 描述符文件时，请注意以下几点：

- <update:os> - 必须始终将此属性设置为“WINDOWS\_ALL”，才能包含思科 NAC 代理支持的所有 Windows 操作系统版本。有关思科 NAC 代理支持的 Windows 操作系统版本列表，请参阅 [Cisco NAC 设备代理的支持信息](#)。
- <update:version> - 这是指要升级到的代理自定义软件包版本。此值应为四位数 <n.n.n.n>，且应大于当前安装的自定义软件包版本。
- <id> - 此 ID 可以是任何内容，但对于每个代理自定义软件包都应唯一。

## 使用创建配置文件功能生成的 XML 文件示例

```

<?xml version="1.0" ?>
<cfg>
  <VlanDetectInterval>0</VlanDetectInterval>
  <RetryDetection>3</RetryDetection>
  <PingArp>0</PingArp>
  <PingMaxTimeout>1</PingMaxTimeout>
  <EnableVlanDetectWithoutUI>0</EnableVlanDetectWithoutUI>
  <SignatureCheck>0</SignatureCheck>
  <DisableExit>0</DisableExit>
  <PostureReportFilter>displayFailed</PostureReportFilter>
  <BypassSummaryScreen>1</BypassSummaryScreen>
  <LogFileSize>5</LogFileSize>
  <DiscoveryHost></DiscoveryHost>
  <DiscoveryHostEditable>1</DiscoveryHostEditable>
  <Locale>default</Locale>
  <AccessibilityMode>0</AccessibilityMode>
  <SwissTimeout>1</SwissTimeout>
  <HttpDiscoveryTimeout>30</HttpDiscoveryTimeout>
  <HttpTimeout>120</HttpTimeout>
  <ExceptionMACList></ExceptionMACList>
  <GeneratedMAC></GeneratedMAC>
  <AllowCRLChecks>1</AllowCRLChecks>
  <DisableL3SwissDelay>0</DisableL3SwissDelay>
  <ServerNameRules></ServerNameRules>
</cfg>

```



**注释** 此文件还包含两个静态（即，不可由用户或思科 ISE 管理员编辑）参数“AgentCfgVersion”和“AgentBrandVersion”，分别用于标识客户端上的当前版本的代理配置文件和代理自定义文件。

## 配置客户端调配资源策略

对于客户端，客户端调配资源策略确定在登录和用户会话启动时哪些用户会从思科 ISE 收到哪个版本的资源（代理、代理合规性模块和代理自定义包或配置文件）。

对于 AnyConnect，可以从 **客户端调配资源** 窗口选择资源，创建可在 **客户端调配策略** 窗口中使用的 AnyConnect 配置。AnyConnect 配置指定了 AnyConnect 软件及其与不同配置文件的关联，其中包括 Windows 和 Mac OS X 客户端的 AnyConnect 二进制包、合规性模块、模块配置文件以及 AnyConnect 的自定义包和语言包。

对于思科 ISE NAC 代理，可以从 **客户端调配 (Client Provisioning)** 窗口选择资源。

### 开始之前

- 请确保您已将资源添加到思科 ISE，然后才能创建有效的客户端调配资源策略。当您下载代理合规性模块时，它始终会覆盖系统中可用的现有模块（如果有）。
- 检查客户端配置中使用的原生 Supplicant 客户端配置文件，并确保无线 SSID 是正确的。对于 iOS 设备，如果您尝试连接到的网络已隐藏，请从 **iOS 设置 (iOS Settings)** 区域中，选中 **目标网络隐藏时启用 (Enable if target network is hidden)** 复选框。

**步骤 1** 选择策略 (Policy) > 客户端调配 (Client Provisioning)。

**步骤 2** 从行为 (Behavior) 下拉列表中，选择以下选项之一：

- **启用 (Enable)**：确保思科 ISE 使用此策略，以在用户登录到网络时帮助实现客户端调配功能，并帮助遵守客户端调配策略规定。
- **禁用 (Disable)**：思科 ISE 不使用指定的资源策略来实现客户端调配功能。
- **监控 (Monitor)**：禁用策略并“观察”客户端调配会话请求，以查看思科 ISE 尝试根据“受监控”策略进行调用的次数。

**步骤 3** 在规则名称 (Rule Name) 文本框中输入新资源策略的名称。

**步骤 4** 指定登录到思科 ISE 的用户可能所属的一个或多个身份组。

您可以选择指定任何 (Any) 身份组类型，或者从已配置的现有身份组列表选择一个或多个组。

**步骤 5** 使用操作系统 (Operating Systems) 字段指定可能在用户登录到思科 ISE 所通过的客户端计算机或设备上运行的一个或多个操作系统。

您可以选择指定单个操作系统，例如 Android、Mac iOS 和 macOS，或者指定用于处理多个客户端计算机操作系统的伞操作系统，例如“Windows XP (All)”或“Windows 7 (All)”。

**步骤 6** 在**其他条件 (Other Conditions)** 字段中，指定要为此特定资源策略创建的新表达式。

**步骤 7** 对于客户端计算机，使用**代理配置 (Agent Configuration)** 选项指定将在客户端计算机上供使用和进行调配的代理类型、合规性模块、代理自定义包和配置文件。

必须在授权策略中包含客户端调配 URL，以使代理能够在客户端计算机中弹出。这会阻止来自任何随机客户端的请求，并且确保只有具有正确重定向 URL 的客户端可以请求安全状态评估。

**步骤 8** 点击保存。

---

### 下一步做什么

在您已成功配置一个或多个客户端调配资源策略后，即可开始配置思科 ISE，以在登录过程中在客户端计算机上执行安全评估。

## 在客户端调配策略中配置思科 ISE 安全评估代理

对于客户端计算机，请配置代理类型、合规性模块、代理自定义包和/或配置文件，使之可供使用和调配，以使用户下载和安装到客户端计算机。

### 开始之前

您必须在思科 ISE 中为 AnyConnect 和思科 ISE NAC 添加客户端调配资源。

---

**步骤 1** 从 **Agent** 下拉列表中选择可用代理，并根据需要启用或禁用 **Is Upgrade Mandatory** 选项来指定此处定义的代理升级（下载）对于客户端设备而言是否为强制性的。

**Is Upgrade Mandatory** 设置仅适用于代理下载。代理配置文件、合规性模块和代理自定义包更新始终为强制性的。

**步骤 2** 从 **Profile** 下拉列表中选择现有的代理配置文件。

**步骤 3** 使用 **Compliance Module** 下拉列表选择要下载到客户端设备的可用合规性模块。

**步骤 4** 从 **Agent Customization Package** 下拉列表中选择用于客户端设备的可用代理自定义包。

---

## 为个人设备配置本地请求方

员工可以直接使用本地请求方将个人设备连接至网络，本地请求方可用于 Windows、Mac OS、iOS 和 Android 设备。对于个人设备，请指定在所注册的个人设备上提供和调配哪个本地请求方配置。

### 开始之前

创建本地请求方配置文件，使思科 ISE 在用户登录时根据您为用户授权要求关联的配置文件提供必要的请求方调配向导，以将用户个人设备设置为接入网络。

---

**步骤 1** 选择策略 (Policy) > 客户端调配 (Client Provisioning)。

**步骤 2** 从行为下拉列表中选择 **Enable**、**Disable** 或 **Monitor**。

**步骤 3** 在 **Rule Name** 文本框中输入新资源策略的名称。

**步骤 4** 指定以下项：

- 使用 **Identity Groups** 字段指定登录思科 ISE 的用户可能隶属的一个或多个身份组。
- 使用 **Operating System** 字段指定用户个人设备上可能运行的、用户借以登录思科 ISE 的一个或多个操作系统。
- 使用 **Other Conditions** 字段指定想要为此特定资源策略创建的新表达式。

**步骤 5** 对于个人设备，请使用 **本地请求方配置 (Native Supplicant Configuration)** 以选择向这些个人设备分发的具体 **Configuration Wizard**。

**步骤 6** 为特定个人设备类型指定适用的 **Wizard Profile**。

**步骤 7** 点击保存 (**Save**)。

---

## 客户端调配报告

可以访问思科 ISE 监控和故障排除功能，以检查成功或失败的用户登录会话的整体趋势，收集有关在指定时间段登录网络的客户端计算机的数量和类型的统计信息，或检查客户端调配资源中的所有最新配置更改。

### 客户端调配请求

**操作 (Operations) > 报告 (Reports) > ISE 报告 (ISE Reports) > 终端和用户 (Endpoints and Users) > 客户端调配 (Client Provisioning)** 报告显示有关成功和失败的客户端调配请求的统计信息。当选择 **Run** 并指定其中一个预设时间段时，思科 ISE 会梳理数据库并显示产生的客户端调配数据。

### 请求方调配请求

**Operations > Reports > ISE Reports > Endpoints and Users > Supplicant Provisioning** 窗口显示有关最新成功和失败的用户设备注册和请求方调配请求的信息。当选择 **Run** 并指定其中一个预设时间段时，思科 ISE 会梳理数据库并显示产生的请求方调配数据。

**Supplicant Provisioning** 报告提供有关特定时间段内通过设备注册门户注册的终端列表的信息，包括登录日期和时间、身份（用户 ID）、IP 地址、MAC 地址（终端 ID）、服务器、配置文件、终端操作系统、SPW 版本、故障原因（如有）和注册状态等数据。

## 客户端调配事件日志

您可以搜索事件日志条目，帮助诊断客户端登录行为可能存在的问题。例如，您网络上的客户端设备在登录后无法获取客户端调配资源更新，您可能需要确定问题的原因。您可以将日志条目用于安全评估和客户端调配审核以及安全评估和客户端调配诊断。

## 客户端调配门户语言文件的 HTML 支持

此门户的说明 (**Instructional Text**)、内容 (**Content**)、可选内容 1 (**Optional Content 1**) 和可选内容 2 (**Optional Content 2**) 文本框的导航路径为 **管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **客户端调配门户 (Client Provisioning Portals)** > **编辑 (Edit)** > **门户页面定制 (Portal Page Customization)** > **页面 (Pages)**。您可以使用小型编辑器中的**查看 HTML 源代码 (View HTML Source)** 图标，并在内容中添加 HTML 代码。

门户语言属性文件中的以下字典键支持在其文本中使用 HTML。



注释 以下是文件中字典键的不完整列表。

- key.guest.ui\_client\_provision\_agent\_installed\_instructions\_without\_java\_message
- key.guest.ui\_contact\_instruction\_message
- key.guest.ui\_success\_message
- key.guest.ui\_client\_provision\_unable\_to\_detect\_message
- key.guest.ui\_client\_provision\_instruction\_message
- key.guest.ui\_client\_provision\_agent\_installation\_message
- key.guest.ui\_client\_provision\_posture\_agent\_check\_message
- key.guest.ui\_vlan\_instruction\_message
- key.guest.ui\_client\_provision\_agent\_installation\_instructions\_with\_no\_java\_message
- key.guest.ui\_success\_instruction\_message
- key.guest.ui\_vlan\_optional\_content\_1
- key.guest.ui\_vlan\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_client\_provision\_posture\_check\_compliant\_message
- key.guest.ui\_client\_provision\_optional\_content\_2
- key.guest.ui\_client\_provision\_optional\_content\_1
- key.guest.ui\_error\_optional\_content\_2
- key.guest.ui\_error\_optional\_content\_1

- key.guest.ui\_client\_provision\_posture\_check\_non\_compliant\_message
- key.guest.ui\_vlan\_install\_message
- key.guest.ui\_success\_optional\_content\_1
- key.guest.ui\_success\_optional\_content\_2
- key.guest.ui\_client\_provision\_posture\_agent\_scan\_message



## 第 14 章

# 威胁控制

- 以威胁防护为中心的 NAC 服务，第 679 页
- 部署和节点设置，第 689 页
- 受信任证书设置，第 695 页
- 证书存储设置，第 697 页
- 日志记录设置，第 711 页
- 维护设置，第 713 页
- 管理员访问设置，第 715 页
- TrustSec 设置，第 718 页
- 设置，第 720 页
- 身份管理，第 728 页
- 网络资源，第 739 页
- 设备门户管理，第 753 页

## 以威胁防护为中心的 NAC 服务

凭借以威胁防护为中心的网络访问控制 (TC-NAC) 功能，您可依据接收自威胁和漏洞适配器的威胁和漏洞属性创建授权策略。

威胁严重级别和漏洞评估结果可用于动态控制终端或用户的访问级别。

您可以配置漏洞和威胁适配器来向思科 ISE 发送高保真危害表现 (IoC)、检测到威胁事件和 CVSS 分数，以便创建以威胁防护为中心的访问策略来相应地更改终端的授权和情景。

思科 ISE 支持以下适配器：

- SourceFire FireAMP
- Qualys



---

注释 TC-NAC 流目前仅支持 Qualys 企业版。

---

当检测到终端威胁事件时，可以在**受到危害的终端 (Compromised Endpoints)** 窗口选择该终端的 MAC 地址并应用一个 ANC 策略，例如隔离。思科 ISE 对该终端触发 CoA 并应用相应的 ANC 策略。如果 ANC 策略不可用，则思科 ISE 对该终端触发 CoA 并应用原始的授权策略。可以使用**受到危害的终端 (Compromised Endpoints)** 窗口上的**清除威胁和漏洞 (Clear Threat and Vulnerabilities)** 选项来（从思科 ISE 系统数据库）清除与某终端关联的威胁和漏洞。

以下属性列在威胁 (Threat) 字典下：

- Qualys-CVSS\_Base\_Score
- Qualys-CVSS\_Temporal\_Score

基础评分 (Base Score) 和临时分数 (Temporal Score) 属性的有效范围均为 0 至 10。

当收到某个终端的漏洞事件时，思科 ISE 对该终端触发 CoA。但是，在收到威胁事件时不会触发 CoA。

您可以通过使用漏洞属性来创建授权策略，从而基于属性值自动隔离易受攻击的终端。例如：

```
Any Identity Group & Threat:Qualys-CVSS_Base_Score > 7.0 -> Quarantine
```

要查看在 CoA 事件期间自动隔离的终端的日志，请选择操作 **(Operations)** > **以威胁防护为中心的 NAC 实时日志 (Threat-Centric NAC Live Logs)**。要查看手动隔离的终端的日志，请选择操作 **(Operations)** > **报告 (Reports)** > **审核 (Audit)** > **更改配置审核 (Change Configuration Audit)**。

启用以威胁防护为中心的 NAC 服务时，请注意以下几点：

- 以威胁防护为中心的 NAC 服务需要思科 ISE Apex 许可证。
- 在一个部署中，只能在一个节点上启用以威胁防护为中心的 NAC 服务。
- 对于漏洞评估服务，每个供应商只能添加一个适配器实例。但是，您可以添加多个 FireAMP 适配器实例。

您可以在以下页面上查看终端的威胁信息：

- **主页 (Home page)** > **威胁控制面板 (Threat dashboard)**
- **情景可视性 (Context Visibility)** > **终端 (Endpoints)** > **受到危害的终端 (Compromised Endpoints)**

以下警报由以威胁防护为中心的 NAC 服务触发：

- 无法访问适配器（系统日志 ID：91002）：表示适配器无法访问。
- 适配器连接失败（系统日志 ID：91018）：表示适配器可访问，但是适配器和源服务器之间的连接已中断。
- 适配器因出错而停止工作（系统日志 ID：91006）：如果适配器未处于所需状态，则触发此警报。如果显示此警报，请检查适配器配置和服务器连接。有关详细信息，请参阅适配器日志。
- 适配器错误（系统日志 ID：91009）：表示 Qualys 适配器无法与 Qualys 站点建立连接或通过其下载信息。

以下报告可用于以威胁防护为中心的 NAC 服务：



- **适配器状态 (Adapter Status):** 适配器状态报告显示威胁和漏洞适配器的状态。
- **COA 事件 (COA Events):** 当收到某个终端的漏洞事件时, 思科 ISE 对该终端触发 CoA。CoA 事件报告显示这些 CoA 事件的状态。同时显示这些终端的新旧授权规则和配置文件详细信息。
- **漏洞评估 (Vulnerability Assessment):** 漏洞评估报告提供您的终端正在进行的评估的信息。您可以查看此报告以确认评估是否以配置策略为基础正在进行。
- 收到事件的总数
- 威胁事件的总数
- 漏洞事件的总数
- 发出 (到 PSN) 的 CoA 的总数

威胁 (Threat) 控制面板包含以下 Dashlet:

- **受到危害的终端总数 (Total Compromised Endpoints) Dashlet** 显示当前网络中受影响的终端总数 (包括连接和断开连接的终端)。
- **特定时段受危害的终端 (Compromised Endpoints Over Time) Dashlet** 显示特定时间段内对终端影响的历史视图。
- **首要威胁 (Top Threats) Dashlet** 显示基于受影响的终端数量和威胁的严重程度的首要威胁。
- 可以使用**威胁关注列表 (Threats Watchlist) Dashlet** 分析所选事件的趋势。

**首要威胁 (Top Threats) Dashlet** 中的气泡大小表示受影响终端的数量, 而浅色面积表示断开连接终端的数量。颜色和垂直刻度表示威胁的严重程度。威胁分为两类 - 指标和事故。指标的严重程度属性是 “Likely\_Impact”, 而事故的严重程度属性是 “Impact\_Qualification”。

“受到危害的终端” (Compromised Endpoint) 窗口会显示受影响终端的矩阵视图以及各个威胁类别的影响严重性。您可以点击设备链接以查看某终端的详细威胁信息。

在主页 (Home) 上的漏洞 (Vulnerability) 控制面板包含以下 Dashlet:

- **易受攻击的终端总数 (Total Vulnerable Endpoints) Dashlet** 显示 CVSS 分数大于指定值的终端总数。此外, 还显示 CVSS 分数大于指定值的连接和断开连接的终端总数。
- **首要漏洞 (Top Vulnerability) Dashlet** 显示基于受影响的终端数量或漏洞的严重程度的首要漏洞。首要漏洞 (Top Vulnerability) Dashlet 中的气泡大小表示受影响终端的数量, 而浅色面积表示断开连接终端的数量。颜色和垂直刻度表示漏洞的严重程度。
- 可以使用**漏洞关注列表 (Vulnerability Watchlist) Dashlet** 分析一段时间内所选漏洞的趋势。点击 Dashlet 中的搜索图标并输入供应商特定 ID (Qualys ID 号码为 “qid”) 以选择和查看该特定 ID 号码的趋势。
- **特定时段易受攻击终端 (Vulnerable Endpoints Over Time) Dashlet** 显示一段时间内对终端影响的历史视图。

易受攻击的终端 (**Vulnerable Endpoints**) 窗口上的“按 CVSS 排序的终端数” (Endpoint Count By CVSS) 图表显示受影响终端的数量及其 CVSS 分数。在易受攻击的终端 (**Vulnerable Endpoints**) 窗口，还可以查看受影响的终端列表。可以点击设备链接以查看各个终端的详细漏洞信息。

支持捆绑包中包含以威胁防护为中心的 NAC 服务日志。以威胁防护为中心的 NAC 服务日志位于 <support/logs/TC-NAC/>

## 启用威胁中心 NAC 服务

要配置漏洞和威胁适配器，您必须首先启用威胁中心 NAC 服务。此服务只可在您部署中的一个策略服务节点上启用。

### 步骤 1

步骤 2 选中要启用威胁中心 NAC 服务的 PSN 旁边的复选框，然后点击编辑 (**Edit**)。

步骤 3 选中启用威胁中心 NAC 服务 (**Enable Threat Centric NAC Service**) 复选框。

步骤 4 点击保存 (**Save**)。

### 相关主题

[添加 Sourcefire FireAMP 适配器](#)，第 682 页

[配置感知威胁分析适配器](#)

[为 CTA 适配器配置授权配置文件](#)

[使用操作过程属性配置授权策略](#)

[以威胁防护为中心的 NAC 服务](#)，第 679 页

## 添加 Sourcefire FireAMP 适配器

### 开始之前

- 您必须有一个配有 SourceFire FireAMP 的账户。
- 您需要在所有终端部署 FireAMP 客户端。
- 您需要在部署节点上启用以威胁防护为中心的 NAC 服务（请参阅[启用威胁中心 NAC 服务](#)，第 682 页）。
- FireAMP 适配器使用 SSL 进行 REST API 调用（对于 AMP 云），并使用 AMQP 接收事件。它还支持使用代理。FireAMP 适配器使用端口 443 进行通信。

### 步骤 1

步骤 2 点击添加 (**Add**)。

步骤 3 从提供商 (**Vendor**) 下拉列表中选择 **AMP: 威胁防护 (AMP : Threat)**。

步骤 4 输入适配器实例的名称。

- 步骤 5** 点击**保存 (Save)**。
- 步骤 6** 刷新“供应商实例列表” (Vendor Instances listing) 窗口。在“供应商实例列表” (Vendor Instances listing) 窗口中，仅在适配器状态变为**配置就绪 (Ready to Configure)**之后，您才可配置适配器。
- 步骤 7** 点击**准备配置 (Ready to Configure)** 链接。
- 步骤 8** (可选) 如果您配置了 SOCKS 代理服务器用于路由所有流量，请输入主机名和该代理服务器的端口号。
- 步骤 9** 选择您想要连接的云。您可以选择 US 云或 EU 云。
- 步骤 10** 点击 FireAMP 链路并以管理员的身份登录 FireAMP。点击**应用 (Applications)** 窗格中的**允许 (Allow)**，以授权流事件导出请求。  
您将被重定向回到思科 ISE。
- 步骤 11** 选择您要监控的事件（例如，可疑下载、连接到可疑域、已执行恶意软件、Java 威胁）。  
适配器实例配置摘要将在**配置摘要 (Configuration Summary)** 页面中显示。

## 思科 ISE 中的漏洞评估支持

来自生态系统合作伙伴的结果被转换为结构化威胁信息表达式 (STIX) 表示，然后基于该值根据需要触发授权更改 (CoA)，并授予终端相应的访问权限级别。

评估终端漏洞所需的时间取决于多种因素，因此无法实时执行 VA。影响评估终端漏洞所需时间的因素包括：

- 漏洞评估生态系统
- 扫描的漏洞类型
- 启用的扫描类型
- 生态系统为扫描设备分配的网络和系统资源

在此版本的思科 ISE 中，仅对采用 IPv4 地址的终端进行漏洞评估。

### 支持的漏洞评估生态系统合作伙伴

思科 ISE 支持 Qualys，Qualys 是一种基于云的评估系统，其在网络中部署有扫描设备。

思科 ISE 允许您配置与 Qualys 通信并获取 VA 结果的适配器。您可以从管理门户配置适配器。您需要具有超级管理员权限的思科 ISE 管理员帐户来配置适配器。

Qualys 适配器使用 REST API 与 Qualys 云服务进行通信。您需要 Qualys 中具有管理器权限的用户帐户来访问 REST API。思科 ISE 使用以下 Qualys REST API：

- 托管检测列表 API - 检查终端的最后一次扫描结果
- 扫描 API - 触发终端的按需扫描

Qualys 对已订阅用户可进行的 API 调用数量实施限制。默认速率限制数为每 24 小时 300 次。

思科 ISE 使用 Qualys API 版本 2.0 连接到 Qualys。请参阅 Qualys API V2 用户指南，以了解这些 API 功能的详细信息。

## Qualys 漏洞评估流程

1. 终端发送请求到 NAD
2. NAD 向思科 ISE 发送身份验证请求。
3. 终端会得到身份验证，并获得网络访问权限。
4. 在思科 ISE 上运行的 VA 服务发送请求到 Qualys，以扫描终端。基于思科 ISE 中的 Qualys 适配器实例配置，Qualys 执行以下操作之一：
  - 扫描终端。
  - 根据终端 IP 地址从数据库获取最后一次扫描的结果。或者，您可以在使用最后一次扫描结果时，使用终端的 MAC 地址。
5. Qualys 将 CVSS 得分返回到思科 ISE。
6. 根据 Qualys 返回的 CVSS 得分和您在思科 ISE 中配置的策略，TC-NAC 核心引擎容器（在思科 ISE 上运行的进程）可以发出授权变更 (CoA) 以授予对终端的完全、有限或无访问权限。

## 启用并配置漏洞评估服务

要启用和配置思科 ISE 的漏洞评估服务，请执行以下任务：

### 开始之前

请在启用以威胁防护为中心的 NAC 服务时注意以下问题：

- 在一个部署中，只能在一个节点上启用以威胁防护为中心的 NAC 服务
- 您只能每供应商添加一个适配器实例

---

**步骤 1** [启用威胁中心 NAC 服务，第 682 页。](#)

**步骤 2** [配置 Qualys 适配器，第 685 页。](#)

**步骤 3** [配置授权配置文件，第 688 页。](#)

**步骤 4** [配置隔离易受攻击的终端的例外规则，第 688 页。](#)

---

## 启用威胁中心 NAC 服务

要配置漏洞和威胁适配器，您必须首先启用威胁中心 NAC 服务。此服务只可在您部署中的一个策略服务节点上启用。

---

**步骤 1**

**步骤 2** 选中要启用威胁中心 NAC 服务的 PSN 旁边的复选框，然后点击**编辑 (Edit)**。

**步骤 3** 选中启用威胁中心 NAC 服务 (**Enable Threat Centric NAC Service**) 复选框。

**步骤 4** 点击保存 (**Save**)。

---

**相关主题**

[添加 Sourcefire FireAMP 适配器](#)，第 682 页

[配置感知威胁分析适配器](#)

[为 CTA 适配器配置授权配置文件](#)

[使用操作过程属性配置授权策略](#)

[以威胁防护为中心的 NAC 服务](#)，第 679 页

## 配置 Qualys 适配器

思科 ISE 支持 Qualys 漏洞评估生态系统。您必须创建一个 Qualys 适配器供思科 ISE 与 Qualys 通信和获取 VA 结果。此思科 ISE 版本仅支持每个供应商一个适配器。

**开始之前**

- 您必须拥有以下用户帐户：
    - 带可配置供应商适配器的超级管理员权限的思科 ISE 的管理员用户帐户。
    - 带管理器权限的 Qualys 用户帐户
  - 确保您拥有适当的 Qualys 许可证订阅。您需要 Qualys 报告中心、知识库 (KBX) 和 API 的访问权限。有关详细信息，请联系您的 Qualys 客户经理。
  - 将 Qualys 服务器证书导入思科 ISE 的受信任证书库（**管理 (Administration) > 证书 (Certificates) > 证书管理 (Certificate Management) > 受信任证书 (Trusted Certificates) > 导入 (Import)**）。确保适当的根证书和中间证书导入（或存在于）思科 ISE 受信任证书库中。
  - 请参阅《Qualys API 指南》以了解以下配置：
    - 确保已启用 Qualys CVSS 评分（**报告 (Reports) > 设置 (Setup) > CVSS 评分 (CVSS Scoring) > 启用 CVSS 评分 (Enable CVSS Scoring)**）。
    - 确保添加了 IP 地址和 Qualys 终端子网掩码（**资产 (Assets) > 主机资产 (Host Assets)**）。
    - 确保拥有 Qualys 选项配置文件的名称。选项配置文件是 Qualys 用于扫描的扫描器模板。我们建议您使用包括身份验证扫描的选项配置文件（此选项也检查终端的 MAC 地址）。
  - 思科 ISE 通过 HTTPS/SSL（端口 443）与 Qualys 通信。
- 

**步骤 1**

**步骤 2** 点击添加 (Add)。

**步骤 3** 从供应商 (Vendor) 下拉列表中选择 **Qualys:VA**。

**步骤 4** 输入适配器实例的名称。例如, Qualys\_Instance。

系统会显示一个列表窗口, 其中包含配置的适配器实例列表。

**步骤 5** 刷新“供应商实例列表”(Vendor Instances listing) 窗口。新添加的 Qualys\_Instance 适配器的状态应更改为 **准备配置 (Ready to Configure)**。

**步骤 6** 点击 **准备配置 (Ready to Configure)** 链接。

**步骤 7** 在 Qualys 配置屏幕输入以下值并点击下一步 (Next)。

字段名称	说明
<b>REST API 主机</b>	托管 Qualys 云的服务器的主机名。请联系 Qualys 代表以获得此信息。
<b>REST API 端口</b>	443
<b>用户名</b>	具有管理器权限的 Qualys 用户帐户。
<b>密码</b>	Qualys 帐户的密码。
<b>HTTP 代理主机 (HTTP Proxy Host)</b>	如果您拥有配置为路由所有 Internet 流量的代理服务器, 输入该代理服务器的主机名。
<b>HTTP 代理端口 (HTTP Proxy Port)</b>	输入代理服务器使用的端口号。

如果与 Qualys 服务器建立了连接, 将显示“扫描仪映射”(Scanner Mappings) 窗口, 其中包含 Qualys 扫描仪列表。您网络中的 Qualys 扫描仪将显示在此窗口中。

**步骤 8** 选择思科 ISE 用于按需扫描的默认扫描仪。

**步骤 9** 在 **PSN 到扫描仪映射 (PSN to Scanner Mapping)** 区域中, 选择一个或多个到 PSN 节点的 Qualys 扫描仪设备, 然后点击下一步 (Next)。

系统将显示高级设置 (Advanced Settings) 窗口。

**步骤 10** 在高级设置 (Advanced Settings) 窗口中输入以下值。此窗口中的设置确定按需扫描是否会触发或最后扫描结果将用于 VA。

字段名称	说明
<b>选项配置文件</b>	选择要 Qualys 用于端口的选项配置文件。您可以选择默认选项配置文件初始选项。
<b>最后扫描结果 - 检查设置</b>	
<b>最后扫描结果检查间隔 (按分钟计)</b>	(影响主机检测列表 API 的接入速率) 时间间隔 (按分钟计), 该时间后会再次检查最后扫描结果。有效范围为 1 到 2880。

字段名称	说明
检查最后扫描结果之前的最大结果数	(影响主机检测列表API的接入速率) 如果队列扫描请求数超过此处指定的最大数量, 最后扫描结果会在 <b>最后扫描结果检查间隔 (按分钟计) (Last scan results check interval in minutes)</b> 之前接受检查。有效范围为 1 到 1000。
验证 MAC 地址	正确还是错误? 当设置为 true 时, Qualys 的最后扫描结果只会在春包括终端的 MAC 地址时使用。
扫描设置	
扫描触发间隔 (按分钟计)	(影响扫描API接入速率) 时间间隔 (按分钟计), 该时间后按需扫描会触发。有效范围为 1 到 2880。
在扫描触发之前的最大请求数	(影响扫描API的接入速率) 如果队列扫描请求数超过此处指定的最大数量, 按需扫描会在 <b>扫描触发间隔 (按分钟计) (Scan trigger interval in minutes)</b> 字段中的指定时间间隔之前被触发。有效范围为 1 到 1000。
扫描状态检查间隔 (按分钟计)	思科 ISE 与 Qualys 通信以检查扫描状态的时间间隔 (按分钟计)。有效范围为 1 到 60。
可同时触发的扫描数量	(此选项取决于您映射到在扫描仪映射屏幕的每个节点的扫描仪数量) 每个扫描仪每次只能处理一个请求。如果映射了一个以上扫描仪到 PSN, 则可以根据选定的扫描仪数量增加此值。有效范围为 1 到 200。
扫描超时 (按分钟计)	时间 (按分钟计), 该时间后扫描请求将超时。如果扫描请求超时, 将生成警报。有效范围为 20 到 1440。
每个扫描仪将提交的 IP 地址最大数量	指示可排列为一个请求以发送到 Qualys 进行处理的请求数。有效范围为 1 到 1000。
选择适配器日志文件的日志级别	选择适配器的日志级别。可用选项为“错误”(ERROR)、“信息”(INFO)、“调试”(DEBUG)和“跟踪”(TRACE)。

步骤 11 点击下一步 (Next) 以审核配置设置。

步骤 12 点击完成。

Qualys 适配器实例的状态更改为“活动”。有关如何在授权配置文件中启用 VA 服务的信息, 请参阅[配置授权配置文件, 第 688 页](#)。

## 配置授权配置文件

思科 ISE 中的授权配置文件现在包括扫描漏洞终端的选项。您可以选择定期运行扫描，并指定这些扫描的时间间隔。定义授权配置文件后，可以将其应用于现有授权策略规则，或创建新的授权策略规则。

### 开始之前

您必须已启用以威胁防护为中心的 NAC 服务，并且已配置供应商适配器。

#### 步骤 1

**步骤 2** 创建新授权配置文件或编辑现有配置文件。

**步骤 3** 从常见任务 (Common Tasks) 区域中，选中评估漏洞 (Assess Vulnerabilities) 复选框。

**步骤 4** 从适配器实例 (Adapter Instance) 下拉列表中，选择已配置的供应商适配器。例如，Qualys\_Instance。

**步骤 5** 如果上一次扫描的时间大于文本框中的时间，请在触发扫描字段中输入以小时为单位的扫描间隔。有效范围为 1 到 9999。

**步骤 6** 勾选按上述间隔定期评估 (Assess periodically using above interval) 复选框。

**步骤 7** 点击提交。

## 配置隔离易受攻击的终端的例外规则

您可以使用以下漏洞评估 (Vulnerability Assessment) 属性来配置一个例外规则，并提供对以下易受攻击终端的有限访问权限：

- Threat:Qualys-CVSS\_Base\_Score
- Threat:Qualys-CVSS\_Temporal\_Score

这些属性在威胁目录下可用。有效值范围为 0 到 10。

您可以选择隔离终端，提供有限访问权限（重定向至不同的门户）或拒绝请求。

**步骤 1** 系统会显示授权策略页面。您可以编辑现有策略规则或创建新例外规则，以检查 VA 属性。

**步骤 2** 创造条件检查 Qualys 评分并分配正确的授权配置文件。例如：

任何身份组和 Threat:Qualys-CVSS\_Base\_Score (Any Identity Group & Threat:Qualys-CVSS\_Base\_Score) > 5 -> 隔离 (授权配置文件) (Quarantine (authorization profile))

**步骤 3** 点击保存 (Save)。

## 漏洞评估日志

思科 ISE 为故障排除 VA 服务提供以下日志。



- vaservice.log - 包含 VA 核心信息，在运行 TC-NAC 服务的节点上可用。
- varuntime.log - 包含终端和 VA 流程的信息；在监控节点和运行 TC-NAC 服务的节点上可用。
- vaaggregation.log - 包含终端漏洞的每小时汇聚详细信息，在主管理节点上可用。

## 部署和节点设置

您可以通过**部署节点 (Deployment Nodes)** 窗口配置思科 ISE (PAN、PSN 和 MnT) 节点和内联终端安全评估节点并设置部署。

### 部署节点列表窗口

表 109: 部署节点列表

字段名称	使用指南
主机名	显示节点的主机名。
<b>Node Type</b>	显示节点类型。 它可以是下列类型之一： <ul style="list-style-type: none"> <li>• 思科 ISE (PAN、PSN、Mnt) 节点</li> <li>• Inline Posture 节点</li> </ul>
相关角色	(只有在节点类型为思科 ISE 时才显示) 列出思科 ISE 节点承担的角色，例如管理 (Administration)、策略服务 (Policy Service)、监控 (Monitoring) 或 pxGrid。 例如，管理 (Administration)、策略服务 (Policy Service)、监控 (Monitoring) 或 pxGrid。
角色	如果在此节点上启用了管理和监控角色，则指示管理和监控角色承担的职责 (主要、辅助或独立职责)。职责可以是以下一项或多项： <ul style="list-style-type: none"> <li>• <b>PRI(A)</b>: 指主 PAN。</li> <li>• <b>SEC(A)</b>: 指辅助 PAN。</li> <li>• <b>PRI(M)</b>: 指主 MnT。</li> <li>• <b>SEC(M)</b>: 指辅助 MnT。</li> </ul>

字段名称	使用指南
服务	<p>(只有在启用策略服务角色时才显示) 列出此思科 ISE 节点上运行的服务。服务可包括以下任意一项:</p> <ul style="list-style-type: none"> <li>• 身份映射</li> <li>• 会话</li> <li>• 剖析</li> <li>• 全部</li> </ul>
Node Status	<p>指示部署中每个思科 ISE 节点的数据复制状态:</p> <ul style="list-style-type: none"> <li>• 绿色 (已连接): 表示部署中已注册的思科 ISE 节点与主 PAN 处于同步状态。</li> <li>• 红色 (断开): 表示思科 ISE 节点无法到达、已断开或未进行数据复制。</li> <li>• 橙色 (处理中): 表示向主 PAN 新注册了新思科 ISE 节点、您已执行手动同步操作或思科 ISE 节点与主 PAN 不同步。</li> </ul> <p>有关详细信息, 请点击节点状态 (Node Status) 列中每个思科 ISE 节点的快速查看图标。</p>

#### 相关主题

[思科 ISE 分布式部署](#), 第 35 页

[思科 ISE 部署术语](#), 第 32 页

[配置思科 ISE 节点](#), 第 32 页

[注册辅助思科 ISE 节点](#), 第 33 页

## 常规节点设置

下表说明思科 ISE 节点的常规设置 (General Settings) 窗口中的字段。在此窗口中, 可以将角色分配给节点并配置要在其上运行的服务。此窗口的导航路径为: **管理 (Administration) > 系统 (System) > 部署 (Deployment) > 部署节点 (Deployment Node) > 编辑 (Edit) > 常规设置 (General Settings)**。

表 110: 常规节点设置

字段名称	使用指南
主机名	显示思科 ISE 节点的主机名。
FQDN	显示思科 ISE 节点的完全限定域名, 例如 isel.cisco.com。
IP 地址	显示思科 ISE 节点的 IP 地址。
Node Type	显示节点类型。可以为以下任一项: 身份服务引擎 (ISE)、Inline Posture 节点
相关角色	

字段名称	使用指南
管理	<p>如果思科 ISE 节点承担管理角色，请选中此复选框。只有在受许可提供管理服务的节点上才可以启用 Administration 角色。</p> <p><b>角色 (Role)</b> - 显示管理角色在部署中承担的职责任务。个人可以选择其中一种值 - <b>独立 (Standalone)</b>、<b>主要 (Primary)</b> 或 <b>辅助 (Secondary)</b>。</p> <p><b>设为主要 (Make Primary)</b> - 选择它可使该节点成为主思科 ISE 节点。在部署中您只能有一个主要思科 ISE 节点。当您将此节点设置为主要节点之后，此窗口中的其他选项将进入活动状态。在部署中您只能有两个 Administration 节点。如果节点具有 <b>独立 (Standalone)</b> 角色，则旁边会显示 <b>设为主要 (Make Primary)</b> 按钮。如果节点具有 <b>辅助 (Secondary)</b> 角色，则旁边会显示 <b>升级为主要 (Promote to Primary)</b> 按钮。如果节点具有 <b>主要 (Primary)</b> 角色，并且没有其他节点注册到该节点，则旁边会显示 <b>设为独立 (Make Standalone)</b> 按钮。点击 <b>设为独立 (Make Standalone)</b> 按钮以使您的主要节点成为独立节点。</p>
Monitoring	<p>如果要思科 ISE 节点承担监控角色并充当日志收集器，请选中此复选框。分布式部署中必须至少有一个监控节点。配置主 PAN 时，必须启用监控角色。在部署中注册辅助监控节点之后，如有必要，可以编辑主 PAN 和禁用监控角色。</p> <p>要在 VMware 平台上将思科 ISE 节点配置为您的日志收集器，请使用以下规定确定您所需要的最低磁盘空间：您的网络中每天每个终端 180KB，您的网络中每天每个思科 ISE 节点 2.5 MB。</p> <p>您可以根据您想要将多少个月的数据至于监控模式下，计算您所需的最大磁盘空间。如果您的部署中只有一个监控节点，则该节点会承担独立职责。如果在部署中有两个监控节点，思科 ISE 还会显示另一个监控节点的名称以供您配置主要/辅助角色。要配置这些职责，请选择以下选项之一：</p> <ul style="list-style-type: none"> <li>• <b>主 (Primary)</b>：使当前节点成为主监控节点。</li> <li>• <b>辅助 (Secondary)</b>：使当前节点成为辅助监控节点。</li> <li>• <b>无 (None)</b> - 如果要使监控节点不承担主要-辅助角色。</li> </ul> <p>如果您将您的一个监控节点配置为主要或辅助节点，另一个监控节点相应地自动成为辅助或主要节点。主要监控节点和辅助监控节点都接收管理和策略服务日志。如果将一个监控节点的角色改为 <b>无 (None)</b>，则另一个监控节点的角色也会成为 <b>无 (None)</b>，从而会在您将某个节点指定为监控节点之后取消高可用性。您会在 <b>远程日志记录目标 (Remote Logging Targets)</b> 窗口中发现此节点被列为系统日志目标：<b>管理 (Administration) &gt; 系统 (System) &gt; 日志记录 (Logging) &gt; 远程日志记录目标 (Remote Logging Targets)</b>。</p>

字段名称	使用指南
策略服务	<p>选中此复选框可启用以下任一或所有服务：</p> <ul style="list-style-type: none"> <li>• <b>启用会话服务 (Enable Session Services)</b>：选中此复选框可启用网络访问、终端安全评估、访客和客户端调配服务。从在节点组中包含节点 (<b>Include Node in Node Group</b>) 下拉列表中选择此策略服务节点所属的组。请注意，证书颁发机构 (CA) 和安全传输注册 (EST) 服务只能在已启用会话服务的策略服务节点上运行。</li> </ul> <p>对于在节点组中包含节点 (<b>Include Node in Node Group</b>)，如果不希望此策略服务节点加入某个组，请选择无 (<b>None</b>)。</p> <p>同一个节点组中的所有节点都应在网络接入设备上配置为 RADIUS 客户端，并获 CoA 授权，因为这些节点中的任何一个节点均可为通过节点组中的任何节点建立的会话发出 CoA 请求。如果您未使用负载均衡器，则节点组中的节点应与在 NAD 上配置的 RADIUS 服务器和客户端相同，或作为 RADIUS 服务器和客户端的子集。这些节点还将配置为 RADIUS 服务器。</p> <p>虽然单个 NAD 可以配置多个思科 ISE 节点以作为 RADIUS 服务器和动态授权客户端，但节点不必全部位于同一个节点组。</p> <p>一个节点组中的所有成员应通过高速 LAN 连接（例如，千兆以太网）互相建立连接。虽然节点组成员不需要在第二层相邻，但是我们依然建议节点组成员在第 2 层相邻，以确保足够的宽带和可达性。有关详细信息，请参阅<a href="#">创建策略服务节点组</a>，第 63 页。</p> <ul style="list-style-type: none"> <li>• <b>启用分析服务 (Enable Profiling Service)</b>：选中此复选框可启用分析服务。如果启用分析服务，必须点击<b>分析配置 (Profiling Configuration)</b> 选项卡并根据要求输入详细信息。当您启用或禁用策略服务节点上运行的任意服务或对此节点做任何更改时，您将重新启动运行这些服务的应用服务器进程。这些服务重新启动时，预计会有延迟。您可以从 CLI 使用 <b>show application status ise</b> 命令，确定何时在节点上重新启动了应用服务器。</li> </ul>
pxGrid	<p>选中此复选框可启用 pxGrid 角色。思科 pxGrid 用于将来自思科 ISE 会话目录区分上下文的信息共享给其他策略网络系统，如思科自适应安全设备 (ASA)。此 pxGrid 框架还可用于在节点之间交换策略和配置数据，例如在思科 ISE 和第三方供应商之间共享标签和策略对象，以及交换威胁信息等非思科 ISE 相关信息。</p>

#### 相关主题

[分布式思科 ISE 部署中的角色](#)，第 32 页

[管理节点](#)，第 48 页

[策略服务节点](#)，第 49 页

[监控节点](#)，第 50 页

[思科 pxGrid 节点](#)，第 54 页

[同步主要和辅助思科 ISE 节点](#)，第 61 页

[创建策略服务节点组](#)，第 63 页

[部署思科 pxGrid 节点，第 56 页](#)

[更改节点角色和服务，第 62 页](#)

[配置用于自动故障切换的监控节点，第 54 页](#)

## 分析节点的设置

下表介绍分析配置 (**Profiling Configuration**) 窗口上的字段，您可以使用此窗口为分析器服务配置探测功能。此窗口的导航路径为：**管理 (Administration) > 系统 (System) > 部署 (Deployment) > ISE 节点 (ISE Node) > 编辑 (Edit) > 分析配置 (Profiling Configuration)**。

表 111: 分析节点的设置

字段名称	使用指南
<b>NetFlow</b>	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 NetFlow，以便接收从路由器发送的 NetFlow 数据包。为以下选项输入所需的值： <ul style="list-style-type: none"> <li>• <b>接口 (Interface)</b>: 选择思科 ISE 节点上的接口。</li> <li>• <b>端口 (Port)</b>: 输入从路由器接收 NetFlow 导出数据的 NetFlow 侦听器端口号。默认端口为 9996。</li> </ul>
<b>DHCP</b>	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 DHCP，以便侦听来自 IP 帮助程序的 DHCP 数据包。为以下选项提供值： <ul style="list-style-type: none"> <li>• <b>接口 (Interface)</b>: 选择思科 ISE 节点上的接口。</li> <li>• <b>端口 (Port)</b>: 输入 DHCP 服务器 UDP 端口号。默认端口为 67。</li> </ul>
<b>DHCP SPAN</b>	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 DHCP，以便收集 DHCP 数据包。 <ul style="list-style-type: none"> <li>• <b>接口 (Interface)</b>: 选择思科 ISE 节点上的接口。</li> </ul>
<b>HTTP</b>	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 HTTP，以便接收并解析 HTTP 数据包。 <ul style="list-style-type: none"> <li>• <b>接口 (Interface)</b>: 选择思科 ISE 节点上的接口。</li> </ul>
<b>RADIUS</b>	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 RADIUS 服务器，以便收集 RADIUS 会话属性，以及来自自己启用思科 IOS 传感器的设备的思科设备协议 (CDP) 和链路层发现协议 (LLDP) 属性。
<b>Network Scan (NMAP)</b>	选中此复选框可启用 NMAP 探测。

字段名称	使用指南
<b>DNS</b>	<p>选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 DNS，以便对 FQDN 执行 DNS 查找。以秒为单位输入<b>超时 (Timeout)</b> 期间。</p> <p><b>注释</b> 要使 DNS 探测功能在分布式部署中特定思科 ISE 节点上运行，您必须启用这些探测功能 - DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP。对于 DNS 查找，必须连同 DNS 探测功能一起启用这些探测功能之一。</p>
<b>SNMP Query</b>	<p>选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 SNMP 查询，以便按照指定的间隔轮询网络设备。在<b>重试 (Retries)</b>、<b>超时 (Timeout)</b>、<b>事件超时 (Event Timeout)</b>（必填）和<b>说明 (Description)</b>（可选）字段中输入值。</p> <p><b>注释</b> 除配置 SNMP 查询探测功能之外，还必须在<b>管理 (Administration) &gt; 网络资源 (Network Resources) &gt; 网络设备 (Network Devices)</b> 中配置其他 SNMP 设置。当在网络设备上配置 SNMP 设置时，请确保在网络设备上全局启用 CDP 和 LLDP。</p>
<b>SNMP 陷阱</b>	<p>选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 SNMP 陷阱探测，以便从网络设备接收链路接通、链路断开和 MAC 通知陷阱。提供或启用以下信息：</p> <ul style="list-style-type: none"> <li>• <b>链接陷阱查询 (Link Trap Query)</b>：选中此复选框可接收和解释通过 SNMP 陷阱接收的通知。</li> <li>• <b>MAC 陷阱查询 (MAC Trap Query)</b>：选中此复选框可接收和解释通过 SNMP 陷阱接收的 MAC 通知。</li> <li>• <b>接口 (Interface)</b>：选择思科 ISE 节点上的接口。</li> <li>• <b>端口 (Port)</b>：输入要使用的主机 UDP 端口。默认端口为 162。</li> </ul>
<b>Active Directory</b>	<p>选中此复选框可扫描所定义的 Active Directory 服务器，以获取有关 Windows 用户的信息。</p> <ul style="list-style-type: none"> <li>• <b>重新扫描前的天数 (Days before rescan)</b>：选择您希望经过多少天后再次运行扫描。</li> </ul>

#### 相关主题

[思科 ISE 分析服务](#)，第 396 页

[分析服务使用的网络探测功能](#)，第 398 页

[在思科 ISE 节点中配置分析服务](#)，第 397 页

## Inline Posture 节点设置

### 受信任证书设置

表 112: 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)	从下拉列表中选择启用 (Enabled) 或禁用 (Disabled)。如果证书被禁用，则思科 ISE 将不使用此证书建立信任。
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>
信任基于证书的管理人员身份验证	仅当选择信任客户端身份验证和系统日志 (Trust for client authentication and Syslog) 时，才能选中此复选框。  选中此复选框可启用基于证书的身份验证用于管理员访问。将所需的证书链导入受信任证书存储区。
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
<b>证书状态验证 (Certificate Status Validation)</b>	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。
<b>验证 OCSP 服务 (Validate Against OCSP Service)</b>	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。
<b>如果 OCSP 返回未知状态则拒绝请求 (Reject the request if OCSP returns UNKNOWN status)</b>	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。
<b>下载 CRL (Download CRL)</b>	选中此复选框以使思科 ISE 下载 CRL。
<b>CRL 分类的 URL (CRL Distribution URL)</b>	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。
<b>检索 (Retrieve CRL)</b>	可以自动或定期下载 CRL。请配置下载时间间隔。
<b>如果下载失败，请稍候 (If download failed, wait)</b>	配置在思科 ISE 再次尝试下载 CRL 之前等待的时间间隔。
<b>如果 CRL 没有收到，绕过此 CRL 验证 (Bypass CRL Verification if CRL is not Received)</b>	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。
<b>忽略 CRL 无效或已过期 (Ignore that CRL is not yet valid or expired)</b>	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。 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。

#### 相关主题

[受信任证书库](#)，第 101 页

[编辑受信任证书](#)，第 105 页



## 证书存储设置

通过“证书存储区”(Certificate Store)窗口，您可以在思科 ISE 中配置可用于身份验证的证书。

### 自签证书设置

表 113: 自签证书设置

字段名称	使用指南
<b>Select Node</b>	(必填) 从下拉列表中选择您要为其生成系统证书的节点。
<b>Common Name (CN)</b>	(如果您不指定 SAN, 则此字段必填) 默认情况下, Common Name 为您要生成自签证书的思科 ISE 节点的 FQDN。
<b>组织单位 (OU) (Organizational Unit [OU])</b>	组织单位名称。例如, Engineering。
<b>Organization (O)</b>	组织名称。例如, Cisco。
<b>City (L)</b>	(请勿缩写) 城市名称。例如, 圣何塞。
<b>省/自治区/直辖市 (ST) (State [ST])</b>	(请勿缩写) 省/自治区/直辖市名称。例如, 加州。
<b>国家/地区 (C) (Country [C])</b>	国家/地区名称。输入两个字母 ISO 国家/地区代码。例如, US。
<b>主体可选名称 (SAN) (Subject Alternative Name [SAN])</b>	与该证书关联的。

字段名称	使用指南
密钥长度	<p>公共密钥的位大小。从 RSA 的下拉列表中选择以下选项之一：</p> <ul style="list-style-type: none"> <li>• 512</li> <li>• 1024</li> <li>• 2048</li> <li>• 4096</li> </ul> <p>从 ECDSA 的下拉列表中选择以下选项之一：</p> <ul style="list-style-type: none"> <li>• 256</li> <li>• 384</li> </ul> <p>如果您计划获得公共 CA 签名的证书，请选择 2048。</p>
Digest to Sign With	<p>从下拉列表中选择以下散列算法之一：</p> <ul style="list-style-type: none"> <li>• SHA-1</li> <li>• SHA-256</li> </ul>
Expiration TTL	指定证书到期之前的天数。从下拉列表中选择值。
友好名称 (Friendly Name)	输入证书的友好名称。如果未指定名称，思科 ISE 会自动创建以下格式的名称： <common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是唯一的五位数数字。
使用情况	<p>选择必须使用此系统证书的服务：</p> <ul style="list-style-type: none"> <li>• <b>管理员 (Admin)</b>：用于确保与部署中的管理门户和思科 ISE 节点之间安全通信的服务器证书。</li> <li>• <b>EAP 身份验证 (EAP Authentication)</b>：用于使用 EAP 协议建立 SSL 或 TLS 隧道的身份验证的服务器证书。</li> <li>• <b>pxGrid</b>：用于确保 pxGrid 客户端和服务器之间的安全通信的客户端和服务端证书。</li> <li>• <b>门户 (Portal)</b>：用于确保与所有思科 ISE Web 门户的安全通信的服务器证书。</li> </ul>

#### 相关主题

[系统证书](#)，第 94 页

[查看系统证书](#)，第 95 页

[生成自签证书](#)，第 97 页

## 证书签名请求设置

通过思科 ISE，只需一个请求即可从管理门户为部署中的所有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多个两个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)。如果在 CN 字段中输入的域名不是节点的 FQDN，思科 ISE 将拒绝使用该证书进行身份验证。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 节点的 FQDN。如有必要，您还可以在 SAN 字段中添加其他 FQDN。如果选择为部署中的所有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 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 (\*)，可以在部署中的多个两个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 节点分配唯一服务器证书的安全性低。

表 114: 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>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 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>EAP 身份验证 (EAP Authentication)</b>: 用于服务器身份验证。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)</li> </ul> </li> </ul> <p><b>注释</b>           EAP-TLS 客户端证书需要使用数字签名密钥。</p> <ul style="list-style-type: none"> <li>• <b>门户 (Portal)</b>: 用于服务器身份验证（以确保与所有 ISE Web 门户之间的安全通信）。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)</li> </ul> </li> <li>• <b>pxGrid</b> - 同时用于客户端和服务端身份验证（以确保 pxGrid 客户端与服务端之间的安全通信）。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> </ul> <p><b>注释</b>           建议您不要将包含值 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。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 style="margin-left: 40px;">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>

字段	使用指南
	<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 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 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 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 节点的 FQDN。\$FQDN\$ 表示 ISE 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 Common Name 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。
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。

字段	使用指南
主体可选名称 (SAN) (Subject Alternative Name [SAN])	<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 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 节点的 IP 地址。</li> </ul>
密钥长度 (Key Length)	如果计划获取公共的 CA 签名证书或将思科 ISE 部署为符合 FIPS 标准的策略管理系统, 请选择 2048 或更大长度。
签名摘要 (Digest to Sign With)	选择下列散列算法之一: SHA-1 或 SHA-256。

#### 相关主题

[证书签名请求](#), 第 113 页

[创建证书签名请求并将其提交给证书颁发机构](#), 第 113 页

[将 CA 签名的证书绑定到证书签名请求](#), 第 114 页

## 终端证书概述窗口 (Endpoint Certificate Overview Window)

表 115: 证书管理概述 (Certificate Management Overview)

字段名称	使用指南
Node name	发出证书的策略服务节点 (PSN) 的名称。
Endpoint Certificates Issued	PSN 节点发出的终端证书的数量。
Endpoint Certificates Revoked	已吊销的证书的数量 (已由 PSN 节点发出的证书)。
Endpoint Certificates Requests	PSN 节点处理的基于证书的身份验证请求数量。
Endpoint Certificates Failed	PSN 节点处理的失败身份验证请求数量。



注释 已过期或已撤销的证书将在 30 天后自动删除。

#### 相关主题

[终端证书](#), 第 124 页

[用户和终端证书续订](#), 第 119 页

[配置思科 ISE 以使用证书对个人设备进行身份验证](#)，第 128 页

[将思科 ISE 配置为允许用户续订证书](#)，第 120 页

[吊销终端证书](#)，第 138 页

## 系统证书导入设置

表 116: 系统证书导入设置

字段名称	说明
<b>Select Node</b>	(必填) 从下拉列表中选择您要导入系统证书的思科 ISE 节点。
<b>Certificate File</b>	(必填) 单击浏览 ( <b>Browse</b> )，从本地系统中选择证书文件。
<b>Private Key File</b>	(必需) 单击浏览 ( <b>Browse</b> )，从本地系统中选择私钥文件。
密码	(必填) 输入密码以解密私钥文件。
<b>友好名称 (Friendly Name)</b>	输入证书的友好名称。如果未指定名称，思科 ISE 会自动创建以下格式的名称：  <common name> # <issuer> # <nnnnn>，其中 <nnnnn> 是一个唯一的五位数。
<b>Allow Wildcard Certificates</b>	如果要导入通配符证书，请选中此复选框。通配符证书使用通配符号（在域名前带一个星号和一个句点）。通配符证书会在组织中的多个主机之间共享。  如果选中此复选框，思科 ISE 会将此证书导入到部署中的所有其他节点。
	如果希望思科 ISE 验证证书扩展，请选中此复选框。如果选中此复选框，并且要导入的证书包含 CA 标志设为 true 的基本限制扩展，请确保密钥用法扩展存在。还必须设置 keyEncipherment 位和/或 keyAgreement 位。



字段名称	说明
使用情况	<p>选择必须使用此系统证书的服务：</p> <ul style="list-style-type: none"> <li>• <b>管理员 (Admin)</b>：用于确保与部署中的管理门户和思科 ISE 节点之间安全通信的服务器证书。</li> </ul> <p>注释        在主 PAN 上更改管理员角色证书的证书将在所有其他思科 ISE 节点上重新启动服务。</p> <ul style="list-style-type: none"> <li>• <b>EAP 身份验证 (EAP Authentication)</b>：用于使用 EAP 协议建立 SSL 或 TLS 隧道的身份验证的服务器证书。</li> <li>• <b>pxGrid</b>：用于确保 pxGrid 客户端和服务器的安全通信的客户端和服务器的证书。</li> <li>• <b>：</b>用于经思科 ISE 消息传递的系统日志 (<b>Syslog Over Cisco ISE Messaging</b>) 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。</li> <li>• <b>门户 (Portal)</b>：用于确保与所有思科 ISE Web 门户的安全通信的服务器证书。</li> </ul>



注释    如果证书是由其他第三方工具而不是思科 ISE 生成的，则无法将证书或其私钥导入思科 ISE。

#### 相关主题

[系统证书](#)，第 94 页

[查看系统证书](#)，第 95 页

[导入系统证书](#)，第 95 页

## 受信任证书列表

表 117: 受信任证书窗口列

字段名称	使用指南
<b>Friendly Name</b>	显示证书的名称。
状态	此列会显示已启用 ( <b>Enabled</b> ) 或已禁用 ( <b>Disabled</b> )。如果证书被禁用，则思科 ISE 将不使用此证书建立信任。

字段名称	使用指南
<b>Trusted for</b>	显示以下一项或多项使用此证书的服务。 <ul style="list-style-type: none"> <li>• 基础设施</li> <li>• 思科服务</li> <li>• 终端</li> </ul>
<b>Issued To</b>	显示证书持有者的通用名称。
<b>颁发者</b>	显示证书颁发机构的通用名称。
<b>Valid From</b>	显示证书的颁发日期和时间。该值也称为“不早于”(Not Before)证书属性。
<b>到期日期</b>	显示证书到期的日期和时间。该值也称为“不迟于”(Not After)证书属性。
<b>Expiration Status</b>	提供有关证书到期状态的信息。此列会显示五个图标和提示消息类别： <ul style="list-style-type: none"> <li>• 绿色：距到期还有 90 天以上</li> <li>• 蓝色：距到期还有 90 天或更短</li> <li>• 黄色：距到期还有 60 天或更短</li> <li>• 橙色：距到期还有 30 天或更短</li> <li>• 红色：已到期</li> </ul>

#### 相关主题

[受信任证书库](#)，第 101 页

[查看受信任的证书](#)，第 104 页

[更改受信任证书库中的证书状态](#)，第 105 页

[在受信任的证书库中添加证书](#)，第 105 页

## 受信任证书导入设置

表 118: 受信任证书导入设置

字段名称	说明
	点击浏览 ( <b>Browse</b> ) 从运行浏览器的计算机选择证书文件。
<b>友好名称 (Friendly Name)</b>	输入证书的友好名称。如果您不指定名称，思科ISE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。

字段名称	说明
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 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 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。
	（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 101 页

[证书链导入](#)，第 109 页

[将根证书导入受信任证书库](#)，第 108 页

## OCSP 客户端配置文件设置

表 119: OCSP 客户端配置文件设置

字段名称	使用指南
Name	OCSP 客户端配置文件的名称。
说明	输入可选的说明。
启用辅助服务器	选中此复选框来以启用高可用性辅助 OCSP 服务器。
总是先访问主服务器	使用此选项以在尝试移至辅助服务器之前先检查主要服务器。即使之前已检查主要服务器并且发现主服务器无响应，思科 ISE 在移至辅助服务器之前仍会尝试向主要服务器发送请求。

字段名称	使用指南
在 $n$ 分钟后回退至主服务器	当您希望思科 ISE 移至辅助服务器，然后再回到主服务器时，请使用此选项。在这种情况下，系统将跳过所有其他请求，并按照该文本框中配置的时间使用辅助服务器。允许的时间范围是 1 至 999 分钟。
URL	输入主要和/或辅助 OCSP 服务器的 URL。
启用 Nonce 扩展支持	您可以配置一个作为 OCSP 请求的一部分发送的 Nonce。Nonce 会在 OCSP 请求中包含一个伪随机数。系统会验证在响应中接收的数值是否与请求中包含的此数相同。此选项可确保重放攻击无法利用旧通信数据。
验证响应签名	<p>OCSP 响应器用以下一个证书为响应签名：</p> <ul style="list-style-type: none"> <li>• CA 证书</li> <li>• 与 CA 证书不同的证书</li> </ul> <p>为了使思科 ISE 验证响应签名，OCSP 响应器需要连同该证书一起发送响应，否则响应验证会失败，而且证书状态不可靠。根据 RFC，OCSP 可以使用不同的证书给响应签名。只要 OCSP 发送给响应签名的证书以供思科 ISE 进行验证，就会如此。如果 OCSP 使用思科 ISE 中未配置的其他证书给响应签名，响应验证将失败。</p>
缓存条目生存时间 $n$ 分钟 (Cache Entry Time To Live $n$ Minutes)	<p>以分钟为单位输入缓存项目在多长时间之后过期。来自 OCSP 服务器的每个响应都有一个 nextUpdate 值。此值显示服务器上接下来将于何时更新证书的状态。缓存 OCSP 响应时，系统会比较两个值（一个是来自配置的值，另一个是来自响应的值），系统会按照这两个值中最低的值将响应缓存相应的时间。如果 nextUpdate 值为 0，则根本不缓存响应。思科 ISE 将 OCSP 响应缓存所配置的时间。缓存不复制，也不是持久性的，所以当思科 ISE 重新启动时，系统会清除缓存。使用 OCSP 缓存是为了保持 OCSP 响应以及出于以下原因：</p> <ul style="list-style-type: none"> <li>• 减少网络流量和降低 OCSP 服务器对已知证书带来的负载</li> <li>• 通过缓存已知证书状态提高思科 ISE 性能</li> </ul>

字段名称	使用指南
清除缓存	<p>点击 <a href="#">清除缓存</a> 以清除连接至 OCSP 服务的所有证书颁发机构的条目。</p> <p>在部署中，<a href="#">清楚缓存</a>与所有节点交互并执行此操作。此机制可更新部署中的每个节点。</p>

#### 相关主题

- [OCSP 服务](#)，第 138 页
- [思科 ISE CA 服务在线证书状态协议响应器](#)，第 139 页
- [OCSP 证书状态值](#)，第 139 页
- [OCSP 高可用性](#)，第 140 页
- [OCSP 故障](#)，第 140 页
- [OCSP 统计计数器](#)，第 143 页
- [添加 OCSP 客户端配置文件](#)，第 140 页

## 内部 CA 设置

表 120: 内部 CA 设置

字段名称	使用指南
<b>Disable Certificate Authority</b>	点击此按钮以禁用内部 CA 服务。
主机名	运行 CA 服务的思科 ISE 节点的主机名。
相关角色	在运行 CA 服务的节点上启用的思科 ISE 节点角色。例如管理角色、策略服务角色等。
<b>Role(s)</b>	运行 CA 服务的思科 ISE 节点承担的职责。例如，独立、主要或辅助职责。
<b>CA &amp; OCSP Responder Status</b>	启用或禁用
<b>OCSP Responder URL</b>	思科 ISE 节点用于访问 OCSP 服务器的 URL。

#### 相关主题

- [思科 ISE CA 服务](#)，第 123 页
- [配置思科 ISE 以使用证书对个人设备进行身份验证](#)，第 128 页

## 证书模板设置



**注释** 在证书模板字段（“组织单位” [Organizational Unit]、“企业” [Organization]、“城市” [City]、“省” [State] 和“国家/地区” [Country]）中不支持 UTF-8 字符。如果在证书模板中使用 UTF-8 字符，则证书调配将会失败。

字段名称	使用指南
<b>Name</b>	（必填）输入证书模板的名称。例如，Internal_CA_Template。
<b>Description</b>	（可选）输入说明。
<b>Common Name (CN)</b>	（仅显示）公用名自动填充为用户名。
<b>Organizational Unit (OU)</b>	组织单位名称。例如，Engineering。
<b>Organization (O)</b>	组织名称。例如，Cisco。
<b>城市 (L) (City [L])</b>	（请勿缩写）城市名称。例如，圣何塞。
<b>省/自治区/直辖市 (ST) (State [ST])</b>	（请勿缩写）省/自治区/直辖市名称。例如，加州。
<b>Country (C)</b>	国家/地区名称。必须输入两个字母 ISO 国家/地区代码。例如，US。
<b>Subject Alternative Name (SAN)</b>	（仅显示）终端的 MAC 地址。
<b>Key Size</b>	指定密钥大小为 1024 或更大数字。
<b>SCEP RA Profile</b>	选择 ISE Internal CA 或您已创建的外部 SCEP RA 配置文件。
<b>Valid Period</b>	输入证书的到期天数。

### 相关主题

[证书模板](#)

[证书模板扩展名](#)

[配置思科 ISE 以使用证书对个人设备进行身份验证](#)，第 128 页

[为 pxGrid 控制器部署思科 ISE CA 证书](#)

[在授权策略条件中使用证书模板](#)

## 日志记录设置

下面的小节解释了如何配置调试日志的严重性、创建外部日志目标，并使思科 ISE 能够将日志消息发送到这些外部日志目标。

### 远程日志记录目标设置

下表介绍远程日志记录目标 (**Remote Logging Targets**) 窗口中的字段，您可以使用此窗口创建外部位置（系统日志服务器）来存储日志记录消息。此页面的导航路径为**管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 远程日志记录目标 (Remote Logging Targets)**。单击添加 (**Add**)。

表 121: 远程日志记录目标设置

字段名称	使用指南
<b>Name</b>	为新的系统日志目标输入名称。
<b>Target Type</b>	从下拉列表中选择目标类型。默认值为 <b>UDP 系统日志 (UDP Syslog)</b> 。
<b>Description</b>	输入新目标的简短说明。
<b>IP 地址</b>	输入将存储日志的目标计算机的 IP 地址或主机名。
<b>端口</b>	输入目标计算机的端口号。
<b>Facility Code</b>	从下拉列表中选择必须用于记录的系统日志设备代码。有效选项为 Local0 至 Local7。
<b>Maximum Length</b>	输入远程日志目标消息的最大长度。有效值为 200 至 1024 字节。
<b>包括此目标的警报 (Include Alarms For This Target)</b>	选中此复选框时，警报消息也会发送到远程服务器。
<b>符合 RFC 3164 (Comply to RFC 3164)</b>	选中此复选框时，即使使用了反斜线 (\)，发送到远程服务器的系统日志消息中的分隔符 ( ; { } \ ) 也不会转义。
<b>Buffer Message When Server Down</b>	当您从目标类型 ( <b>Target Type</b> ) 下拉列表中选择 <b>TCP 系统日志 (TCP Syslog)</b> 或 <b>安全系统日志 (Secure Syslog)</b> 时，系统会显示此复选框。如果希望思科 ISE 在 TCP 系统日志目标或安全系统日志目标不可用时缓冲系统日志消息，请选中此复选框。思科 ISE 会在与目标的连接恢复时重新尝试将消息发送到目标。连接恢复后，将按从最旧到最新的顺序发送消息。缓冲消息会始终在新消息之前发送。如果缓冲区已满，则会丢弃旧消息。
<b>Buffer Size (MB)</b>	设置每个目标的缓冲区大小。默认情况下设置为 100 MB。更改缓冲区大小会清除缓冲区，并且特定目标的所有现有缓冲消息都会丢失。

字段名称	使用指南
<b>Reconnect Timeout (Sec)</b>	输入时间（以秒为单位），以便配置在服务器关闭的情况下，TCP 和安全系统日志在被丢弃之前将会保留多长时间。
<b>Select CA Certificate</b>	当您从目标类型 ( <b>Target Type</b> ) 下拉列表中选择 <b>安全系统日志 (Secure Syslog)</b> 时，系统会显示此下拉列表。从下拉列表中选择一个客户端证书。
<b>Ignore Server Certificate Validation</b>	当您从目标类型 ( <b>Target Type</b> ) 下拉列表中选择 <b>安全系统日志 (Secure Syslog)</b> 时，系统会显示此复选框。选中此复选框，以便让思科 ISE 忽略服务器证书身份验证并接受任何系统日志服务器。默认情况下，除非在禁用此复选框时系统处于 FIPS 模式，否则此选项设置为关闭。

#### 相关主题

[思科 日志记录机制](#)，第 175 页

[思科 ISE 系统日志](#)，第 176 页

[思科 ISE 消息目录](#)，第 179 页

[集合过滤器](#)，第 181 页

[事件抑制绕行过滤器](#)，第 182 页

[配置远程系统日志收集位置](#)，第 177 页

[配置集合过滤器](#)，第 181 页

## 配置日志记录类别

下表介绍了可用于配置日志记录类别的字段。设置日志严重性级别，然后为日志记录类别的日志选择日志记录目标。此窗口的导航路径为**管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)**。

单击想要查看的日志记录类别旁边的单选按钮，单击**编辑 (Edit)**。下表对日志记录类别的编辑窗口中显示的字段进行了说明。

表 122: 日志记录类别设置

字段名称	使用指南
<b>Name</b>	显示日志记录类别的名称。



字段名称	使用指南
<b>Log Severity Level</b>	<p>对于某些日志记录类别，默认情况下会设置此值，并且您无法对其进行编辑。对于某些日志记录类别，您可以从下拉列表中选择以下严重性级别之一：</p> <ul style="list-style-type: none"> <li>• <b>严重 (FATAL)</b>: 紧急级别。此级别意味着您无法使用思科 ISE，并且必须立即采取必要的操作。</li> <li>• <b>错误 (ERROR)</b>: 此级别表示严重错误情况。</li> <li>• <b>警告 (WARN)</b>: 此级别表示正常但值得注意的情况。这是会为很多日志记录类别设置的默认级别。</li> <li>• <b>信息 (Info)</b>: 此级别表示供参考的消息。</li> <li>• <b>调试 (DEBUG)</b>: 此级别表示诊断错误消息。</li> </ul>
<b>Local Logging</b>	选中此复选框可为本地节点上的类别启用日志记录事件。
<b>目标</b>	<p>该区域允许您使用左侧和右侧图标在可用 (<b>Available</b>) 和所选 (<b>Selected</b>) 区域之间转移目标，从而更改类别的目标。</p> <p><b>可用 (Available)</b> 区域包含本地（预定义）和外部（用户定义）的现有日志记录目标。</p> <p><b>选定 (Selected)</b> 区域最初为空，然后会显示为该类别选择的目标。</p>

#### 相关主题

[思科 ISE 消息代码](#)，第 178 页

[配置远程系统日志收集位置](#)，第 177 页

[设置消息代码的严重性级别](#)，第 178 页

## 维护设置

使用备份、恢复和数据清除功能，这些窗口可帮助您管理数据。

## 存储库设置

表 123: 存储库设置

字段	使用指南
<b>Repository</b>	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。
<b>协议 (Protocol)</b>	从可用协议中选择一个您想要使用的协议。

字段	使用指南
服务器名称 (Server Name)	（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 IPv4 地址。  注释 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。
路径 (Path)	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。  此值可以用双前斜杠 (//) 或单前斜杠 (/) 开头，表示服务器的根目录。但是，对于 FTP 协议，单前斜杠 (/) 表示 FTP 的本地设备主目录，而不是根目录。
用户名	（对于 FTP、SFTP 和 NFS 为必填字段）输入对指定服务器拥有写入权限的用户名。用户名可以包含字母数字和 _、/、@、\$ 字符。
密码 (Password)	（对于 FTP、SFTP 和 NFS 为必填字段）输入用于访问指定服务器的密码。密码可以包含以下字符：0-9、a-z、A-Z、-、.、 、@、#、\$、^、&、*、(、)、+、和 =。

#### 相关主题

[备份和恢复存储库](#)，第 158 页

[创建存储库](#)，第 159 页

## 按需备份设置

下表介绍**按需备份 (On-Demand Backup)** 窗口上的字段，您可以随时使用此窗口获取备份。此窗口的导航路径为：**管理 (Administration) > 系统 (System) > 备份和恢复 (Backup & Restore)**。

表 124: 按需备份设置

字段名称	使用指南
<b>Backup Name</b>	输入备份文件的名称。
<b>Repository Name</b>	应该保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
<b>Encryption Key</b>	此密钥用于加密和解密备份文件。

#### 相关主题

[备份数据类型](#)，第 158 页

[按需备份和计划备份](#)，第 160 页

[备份历史记录](#)，第 164 页

[备份失败](#)，第 165 页

[思科 ISE 恢复操作](#)，第 165 页

[导出身份验证和授权策略配置](#)，第 171 页

[在分布式环境中同步主节点和辅助节点](#)，第 171 页  
[执行按需备份](#)，第 161 页

## 计划备份设置

下表介绍“定期备份”(Scheduled Backup)窗口上的字段，您可以使用此窗口恢复完整备份或增量备份。此窗口的导航路径为：**管理 (Administration) > 系统 (System) > 备份和恢复(Backup and Restore)**。

表 125: 计划备份设置

字段名称	使用指南
<b>Name</b>	输入备份文件的名称。您可以输入您所选的描述性名称。思科 ISE 会将时间戳附加到备份文件名之后并将其存储在存储库中。即使您配置了一系列备份，也要有唯一的备份文件名。在“定期备份”(Scheduled Backup)列表窗口上，备份文件名前面将附加“backup_occur”，表示文件是一次 <b>kron</b> 作业。
<b>Description</b>	输入对备份的说明。
<b>Repository Name</b>	选择保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
<b>Encryption Key</b>	输入用于加密和解密备份文件的密钥。
<b>Schedule Options</b>	选择计划备份的频率并相应地填写其他选项。

### 相关主题

[备份数据类型](#)，第 158 页  
[按需备份和计划备份](#)，第 160 页  
[备份历史记录](#)，第 164 页  
[备份失败](#)，第 165 页  
[思科 ISE 恢复操作](#)，第 165 页  
[导出身份验证和授权策略配置](#)，第 171 页  
[在分布式环境中同步主节点和辅助节点](#)，第 171 页  
[使用 CLI 备份](#)，第 164 页  
[计划备份](#)，第 162 页

## 管理员访问设置

您可以通过这些部分来为管理员配置访问设置。

## 管理员密码策略设置

下表介绍了密码策略 (**Password Policy**) 选项卡中的字段，可以使用此选项卡来定义管理员密码应满足的条件。此窗口的导航路径为：**管理 (Administration) > 系统 (System) > 管理员访问权限 (Admin Access) > 身份验证 (Authentication) > 密码策略 (Password Policy)**。。

表 126: 管理员密码策略设置

字段名称	使用指南
最小长度 (Minimum Length)	指定密码的最小长度（以字符数为单位）。默认值为 6 个字符。
密码不可包含管理员姓名或其反向顺序的字符	选中此复选框可限制使用管理员用户名或其反向顺序的字符。
密码不可包含“cisco”或其反向顺序的字符	选中此复选框可限制使用字词“cisco”或其反向顺序的字符。
密码不可包含_____或其反向顺序的字符	选中此复选框可限制使用您定义的任何字词或其反向顺序的字符。
密码不可包含连续重复四次或以上的字符	选中此复选框可限制使用连续重复四次或以上的字符。
必用字符	指定管理员密码必须包含从以下选项中选择的地类型的至少一个字符： <ul style="list-style-type: none"> <li>• 小写字母字符</li> <li>• 大写字母字符</li> <li>• 数字字符</li> <li>• 非字母数字字符</li> </ul>
密码历史记录 (Password History)	指定必须与新密码不同的先前密码的数量，以防止重复使用同一密码。 此外，指定必须与先前密码不同的字符的数量。 输入在其之前不能重复使用密码的天数。

字段名称	使用指南
“密码有效期” (Password Lifetime)	指定以下选项来强制用户在经过指定时间段后更改密码： <ul style="list-style-type: none"> <li>“如果此时间（按天计）过后未更改密码，则禁用管理员帐户。” (Time (in days) before the administrator account is disabled if the password is not changed.) （允许的范围是 0 至 2147483647 天。）</li> <li>“禁用管理员帐户之前的提醒时间（按天计）。” (Reminder (in days) before the administrator account is disabled.)</li> </ul>
“不正确的登录尝试之后锁定或暂停帐户” (Lock or Suspend Account with Incorrect Login Attempts)	指定思科 ISE 在将管理员锁定以及暂停或禁用帐户凭证之前记录错误管理员密码的次数。 系统会向其帐户已锁定的管理员发送邮件。您可以输入自定义邮件补救消息。

#### 相关主题

[思科 ISE 管理员](#)，第 9 页

[创建新管理员](#)，第 10 页

## 会话超时和会话信息设置

下表介绍会话 (Session) 窗口中的字段，您可以使用此窗口定义会话超时和终止活动管理会话。此窗口的导航路径为：**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **会话 (Session)**。

表 127: 会话超时和会话信息设置

字段名称	使用指南
会话超时	
会话空闲超时 (Session Idle Timeout)	输入思科 ISE 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。
会话信息	
失效 (Invalidate)	选中要终止的会话 ID 旁边的复选框，然后单击失效 (Invalidate)。

#### 相关主题

[管理员访问设置](#)，第 145 页

[配置管理员会话超时](#)，第 147 页

[终止活动管理会话](#)，第 147 页

# TrustSec 设置

## 验证 Trustsec 部署 (Verify Trustsec Deployment)

此选项可帮助验证所有网络设备是否部署了最新的 TrustSec 策略。如果在思科 ISE 和网络设备上配置的策略之间存在任何差异，“警报”(Alarms) Dashlet 中会显示警报，该 Dashlet 位于工作中心 (Work Centers) > TrustSec > 控制板和主页 (Dashboard and Home) > 摘要 (Summary) 下。TrustSec 控制板中会显示以下警报：

- 每当验证过程开始或完成时，系统都会显示带有信息 (Info) 图标的警报。
- 如果由于新的部署请求而取消验证过程，则会显示带有信息 (Info) 图标的警报。
- 如果验证过程因错误而失败，则会显示带有警告 (Warning) 图标的警报。例如，无法打开与网络设备的 SSH 连接，或当网络设备不可用，或当思科 ISE 和网络设备上配置的策略之间存在任何差异。

验证部署 (Verify Deployment) 选项也可从以下窗口选择。

- 工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 (Security Groups)
- 工作中心 (Work Centers) > TrustSec > 组件 (Components) > 安全组 ACL (Security Group ACLs)
- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 矩阵 (Matrix)
- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 源树 (Source Tree)
- 工作中心 (Work Centers) > TrustSec > TrustSec 策略 (TrustSec Policy) > 出口策略 (Egress Policy) > 目标树 (Destination Tree)

**每次部署后自动验证 (Automatic Verification After Every Deploy)：** 如果希望思科 ISE 在每次部署后验证所有网络设备上的更新，请选中此复选框。部署过程完成后，经过您在部署过程后的时间 (Time after Deploy Process) 字段中指定的时间后，验证过程开始。

**部署过程后的时间 (Time After Deploy Process)：** 指定您希望思科 ISE 在部署过程完成后等待多长时间，然后再开始验证过程。有效范围为 10 - 60 分钟。

如果在等待期间收到新的部署请求或正在进行其他验证，则会取消当前验证过程。

**立即验证 (Verify Now)：** 点击此选项可立即开始验证过程。

## 受保护的访问凭证 (PAC)

- **隧道 PAC 生存时间 (Tunnel PAC Time to Live)：**

指定 PAC 的到期时间。隧道 PAC 为 EAP-FAST 协议生成隧道。您可以秒、分钟、小时、天或周为单位指定时间。默认值为 90 天。以下是有效范围：

- 1 - 157680000 秒

- 1 - 2628000 分钟
  - 1 - 43800 小时
  - 1 - 1825 天
  - 1 - 260 周
- **进行主动 PAC 更新前所经历的时间 (Proactive PAC Update Will Occur After):** 当剩余的隧道 PAC TTL 百分比达到设定值时, 思科 ISE 会在成功身份验证后主动向客户端提供新 PAC。如果第一次成功身份验证发生在 PAC 到期之前, 则服务器会启动隧道 PAC 更新。此机制会为客户端更新有效的 PAC。默认值为 10%。

### 安全组标签编号

#### APIC EPG 的安全组标签编号 (Security Group Tag Numbering for APIC EPGs)

**APIC EPG 的安全组标签编号 (Security Group Tag Numbering for APIC EPGs):** 选中此复选框, 指定编号范围以用于根据从 APIC 获取的 EPG 创建的 SGT。

#### 自动创建安全组

**创建授权规则时自动创建安全组 (Auto Create Security Groups When Creating Authorization Rules):** 选中此复选框可在创建授权策略规则时自动创建 SGT。

如果选中此选项, **授权策略 (Authorization Policy)** 窗口顶部会显示以下消息: 开启自动安全组创建 (Auto Security Group Creation is On)。

系统会根据规则属性命名自动创建的 SGT。点击权限 (**Permissions**) 字段中显示的加号 (+) 标志可编辑 SGT 名称和值。



---

**注释** 当删除相应的授权策略规则时, 不会删除自动创建的 SGT。

---

默认情况下, 此选项在全新安装或升级后会被禁用。

#### IP SGT 主机名静态映射

**IP SGT 主机名静态映射 (IP SGT Static Mapping of Hostnames):** 如果使用 FQDN 和主机名, 则思科 ISE 会在部署映射和检查部署状态的同时在 PAN 和 PSN 节点中查找对应的 IP 地址。您可以使用此选项指定为 DNS 查询返回的 IP 地址创建的映射数。您可以选择以下其中一个选项:

- 为 DNS 查询返回的所有 IP 地址创建映射 (**Create mappings for all IP addresses returned by a DNS query**)
- 仅为 DNS 查询返回的第一个 IPv4 地址和第一个 IPv6 地址创建映射 (**Create mappings only for the first IPv4 address and the first IPv6 address that is returned by a DNS query**)

### 相关主题

[TrustSec 架构](#)，第 578 页

[TrustSec 组件](#)，第 579 页

[配置 TrustSec 全局设置](#)，第 581 页

## 设置

通过这些窗口，您可以配置各种服务的常规设置。

## 安全评估常规设置

这些设置是终端安全评估的默认设置，可被终端安全评估配置文件覆盖。

### 常规终端安全评估设置

- **补救计时器 (Remediation Timer)**: 输入开始补救前等待的时间。默认值为 4 分钟。有效范围为 1 至 300 分钟。
- **网络过渡延迟 (Network Transition Delay)**: 以秒为单位输入时间值。默认值为 3 秒。有效范围为 2 至 30 秒。
- **默认终端安全评估状态 (Default Posture Status)**: 选择**合规 (Compliant)**或**不合规 (Noncompliant)**。在连接到网络时，非代理设备会处于此状态。
- **自动关闭登录成功屏幕前等待 (Automatically Close Login Success Screen After)**: 选中此复选框可在指定的时间过后自动关闭成功登录屏幕。可以配置计时器以自动关闭登录屏幕。有效范围为 0 至 300 秒。如果将时间设置为零，则客户端上的代理不会显示成功登录屏幕。

### 安全评估租约

- **每当用户连接到网络时执行终端安全评估 (Perform posture assessment every time a user connects to the network)**: 选择此选项可在用户每次连接网络时启动终端安全评估
- **每 n 天执行一次终端安全评估 (Perform posture assessment every n days)**: 选择此选项可在指定天数过后启动终端安全评估，即使客户端的状态已评估为“合规”也是如此。

### 相关主题

[安全评估服务](#)

[安全评估管理设置](#)，第 611 页

[安全评估租约](#)，第 613 页

[在思科 ISE 中启用安全评估会话服务](#)

[设定补救计时器，使客户端在指定时间内补救](#)，第 612 页

[设置网络转换延迟计时器，使客户端实现转换](#)，第 612 页

[将登录成功窗口设置为自动关闭](#)，第 613 页



设置非代理设备的终端安全评估状态，第 613 页

## 重新进行安全评估配置设置

表 128: 重新进行安全评估配置设置

字段名称	使用指南
<b>Configuration Name</b>	输入 PRA 配置的名称。
<b>Configuration Description</b>	输入 PRA 配置的说明。
<b>Use Reassessment Enforcement?</b>	选中此复选框，将 PRA 配置应用到用户身份组。
<b>Enforcement Type</b>	<p>选择要执行的操作：</p> <ul style="list-style-type: none"> <li>• <b>继续 (Continue)</b>: 用户继续拥有特权访问权限，无需任何用户干预即可补救客户端，无论终端安全评估要求如何都是如此。</li> <li>• <b>注销 (Logoff)</b>: 如果客户端不合规，用户将被迫从网络注销。当客户端再次登录时，合规性状态未知。</li> <li>• <b>补救 (Remediate)</b>: 如果客户端不合规，代理将在指定时间内等待补救发生。客户端一旦补救，代理将向策略服务节点发送 PRA 报告。如果在客户端忽略补救，代理程序将向策略服务节点发送注销请求，迫使客户端从网络注销。</li> </ul> <p>如果终端安全评估要求设置为强制，那么 RADIUS 会话将因为 PRA 故障操作而被清除，并且必须开始新的 RADIUS 会话，才能再次布置客户端。</p> <p>如果终端安全评估要求设置为可选，那么代理允许用户从代理点击“继续” (Continue) 选项。用户可以继续停留在当前的网络中，不受任何限制。</p>
<b>Interval</b>	<p>输入第一次成功登录后在客户端上启动 PRA 的时间间隔分钟数。</p> <p>默认值为 240 分钟。最小值为 60 分钟，最大值为 1440 分钟。</p>
<b>Grace time</b>	<p>输入允许客户端完成补救的时间间隔分钟数。宽限时间不能为零，并且应当大于 PRA 间隔。它可以介于默认最小间隔（5 分钟）和最小 PRA 间隔之间。</p> <p>最小值为 5 分钟，最大值为 60 分钟。</p> <p>注释 宽限时间仅在执行类型设置为在客户端重新进行安全评估失败后的补救操作时启用。</p>
<b>Select User Identity Groups</b>	为 PRA 配置选择唯一组或唯一组组合。

字段名称	使用指南
<b>PRA configurations</b>	显示现有的 PRA 配置以及关联到 PRA 配置的用户身份组。

#### 相关主题

- [安全评估租约](#)，第 613 页
- [定期重新评估](#)，第 614 页
- [终端安全状态评估选项](#)，第 639 页
- [安全评估补救选项](#)，第 639 页
- [安全评估的自定义条件](#)，第 639 页
- [自定义安全评估补救措施](#)，第 639 页
- [配置定期重新评估](#)，第 615 页

## 安全评估可接受使用政策配置设置

表 129: 安全评估 AUP 配置设置

字段名称	使用指南
<b>Configuration Name</b>	输入要创建的 AUP 配置的名称。
<b>Configuration Description</b>	输入要创建的 AUP 配置的说明。
<b>“向代理用户显示 AUP” (Show AUP to Agent users)</b> (仅适用于 Windows)	选中后，系统会在身份验证和终端安全评估成功后，向用户显示您的网络的网络使用条款和条件的链接。
<b>为 AUP 消息使用 URL (Use URL for AUP message)</b>	选中后，必须在“AUP URL”字段中输入 AUP 消息的 URL。
<b>为 AUP 消息使用文件 (Use file for AUP message)</b>	选中后，必须浏览至文件位置并以压缩格式上传文件。此文件必须在顶层包含 index.html。 除 index.html 文件以外，该 .zip 文件还可包含其他文件和子目录。这些文件可以使用 HTML 标签相互引用。
<b>AUP URL</b>	输入 AUP 的 URL，用户必须在身份验证和安全评估成功后访问该 URL。
<b>AUP File</b>	浏览至文件并将其上传到思科 ISE 服务器。它应是压缩文件，并且应在顶层包含 index.html 文件。

字段名称	使用指南
<b>Select User Identity Groups</b>	<p>针对 AUP 配置选择唯一用户身份组或用户身份组的唯一组合。</p> <p>创建 AUP 配置时，请注意以下事项：</p> <ul style="list-style-type: none"> <li>• 安全评估 AUP 不适用于访客流程</li> <li>• 两个配置不会共同具有任何用户身份组</li> <li>• 如果您要使用用户身份组 “Any” 创建 AUP 配置，则要先删除所有其他 AUP 配置</li> <li>• 如果使用用户身份组 “Any” 创建 AUP 配置，则无法使用唯一用户身份组或用户身份组的唯一组合创建其他 AUP 配置。要使用除 Any 以外的用户身份组创建 AUP 配置，请先删除具有用户身份组 “Any” 的现有 AUP 配置，或者使用唯一用户身份组或用户身份组的唯一组合更新具有用户身份组 “Any” 的现有 AUP 配置。</li> </ul>
<b>Acceptable use policy configurations - Configurations list</b>	列出现有 AUP 配置以及与 AUP 配置关联的最终用户身份组。

#### 相关主题

[安全评估服务](#)

[配置安全评估的可接受使用政策](#)，第 621 页

## EAP-FAST 设置

表 130: 配置 EAP-FAST 设置

字段名称	使用指南
<b>Authority Identity Info Description</b>	输入用于说明向客户端发送凭证的思科 ISE 节点的用户友好字符串。客户端可以在类型、长度和价值 (TLV) 的受保护访问凭证 (PAC) 信息中发现此字符串。默认值为 Identity Services Engine。
<b>Master Key Generation Period</b>	指定主键生成期（以秒、分钟、小时、天或周为单位）。值必须是范围在 1 至 2147040000 秒内的正整数。默认值为 604800 秒，相当于一周。
<b>Revoke all master keys and PACs</b>	点击“撤销” (Revoke) 可撤销所有主键和 PAC。
<b>Enable PAC-less Session Resume</b>	如果您要在没有 PAC 文件的情况下使用 EAP-FAST，请选中此复选框。

字段名称	使用指南
<b>PAC-less Session Timeout</b>	指定无 PAC 会话恢复超时的时间（以秒为单位）。默认值为 7200 秒。

#### 相关主题

[用于身份验证的协议设置](#)，第 549 页

[将 EAP-FAST 用作身份验证协议的指南](#)，第 549 页

[EAP-FAST 的优势](#)，第 576 页

[配置 EAP-FAST 设置](#)，第 550 页

## PAC 设置

下表介绍“生成 PAC” (Generate PAC) 窗口上的字段，您可以使用此窗口为 EAP-FAST 身份验证配置受保护的访问凭证。此页面的导航路径为：要查看此处窗口，请单击菜单图标(☰)，然后选择管理 (Administration) > 系统 (System) > 设置 (Settings) > 协议 (Protocols) > EAP-FAST > 生成 (Generate PAC)。

表 131: 为 EAP-FAST 设置生成 PAC

字段名称	使用指南
<b>Tunnel PAC</b>	点击此单选按钮生成隧道 PAC。
<b>Machine PAC</b>	点击此单选按钮生成设备 PAC。
<b>Trustsec PAC</b>	点击此单选按钮生成 Trustsec PAC。
<b>Identity</b>	<p>（针对 Tunnel 和 Machine PAC）指定 EAP-FAST 协议显示为“内部用户名”的用户名或设备名称。如果身份字符串与该用户名不匹配，则身份验证失败。</p> <p>这是主机定义在自适应安全设备 (ASA) 上定义的主机名。身份字符串必须与 ASA 主机名匹配，否则 ASA 无法导入生成的 PAC 文件。</p> <p>如果生成的是 Trustsec PAC，则 Identity 字段指定 Trustsec 网络设备的设备 ID 并且由 EAP-FAST 协议提供发起方 ID。如果在此处输入的 Identity 字符串与该设备 ID 不匹配，则身份验证失败。</p>
<b>PAC Time to Live</b>	<p>（对于隧道和设备 PAC）请以秒为单位输入 PAC 的到期时间。默认值为 604800 秒，相当于一周。该值必须是介于 1 和 157680000 秒之间的正整数。对于 Trustsec PAC，请以天、周、月或年为输入一个值。默认情况下，该值为一年。最小值为一天，最大值为 10 年。</p>

字段名称	使用指南
<b>Encryption Key</b>	输入加密密钥。密钥的长度必须介于 8 和 256 个字符之间。密钥可以包含大写或小写字母或数字，或字母数字字符的组合。
<b>Expiration Data</b>	（仅对于 Trustsec PAC）到期日期根据 PAC Time to Live 计算。

#### 相关主题

[用于身份验证的协议设置](#)，第 549 页

[将 EAP-FAST 用作身份验证协议的指南](#)，第 549 页

[为 EAP-FAST 生成 PAC](#)，第 550 页

## EAP-TLS 设置

#### 相关主题

[用于身份验证的协议设置](#)，第 549 页

[配置 EAP-TLS 设置](#)，第 552 页

## PEAP 设置

#### 相关主题

[用于身份验证的协议设置](#)，第 549 页

[配置 PEAP 设置](#)，第 553 页

[使用 PEAP 的优势](#)，第 574 页

[PEAP 协议支持的请求方](#)，第 575 页

[PEAP 协议流程](#)，第 575 页

## RADIUS 设置

当您启用异常客户端抑制并且在配置的检测间隔内终端身份验证失败两次时，思科 ISE 会将请求方标识为配置错误并抑制由于相同失败原因导致的失败身份验证。您可以通过在 Live Authentications 页面点击 **Misconfigured Supplicant Counter** 链接，找到关于此抑制功能的更多详细信息。如果从受抑制的终端成功完成身份验证，则会清除此抑制，而且会降低 Live Authentications 页面上 Misconfigured Supplicant Counter 的值。此外，如果在六小时的时间内受抑制终端没有任何身份验证活动，系统会自动清除抑制。

思科 ISE 允许通过启用 **Reject Requests After Detection** 选项，实施强抑制。如果您选中 **Reject Requests After Detection** 复选框，并且终端身份验证因同一失败原因失败五次，思科 ISE 就会激活强抑制。所有后续的身份验证，无论成功与否，都会被抑制，所以不会进行身份验证。经过所配置的 **Request Rejection Interval** 间隔或终端无身份验证活动达六小时后，系统会清除“强”抑制。



**注释** 如果配置 RADIUS 失败抑制，则在配置 RADIUS 日志抑制后，仍可能会收到错误“5440 终端已放弃会话并启动了新会话”(5440 Endpoint Abandoned EAP Session and started a new one)。有关详细信息，请参阅以下思科 ISE 社区帖子：

<https://community.cisco.com/t5/network-access-control/authentication-failed-quot-5440-endpoint-abandoned-eap-session/td-p/3191944>

表 132: RADIUS 设置

字段名称	使用指南
<b>Suppress Anomalous Clients</b>	选中此复选框以检查身份验证重复失败的客户端。每经过一个 Reporting Interval 间隔，系统会报告失败身份验证摘要。
<b>Detection Interval</b>	以分钟为单位输入检测客户端的时间间隔。
<b>Reporting Interval</b>	以分钟为单位输入报告失败身份验证的时间间隔。
<b>Reject Requests After Detection</b>	选中此复选框以拒绝来自被识别为异常或配置错误的客户端的请求。在请求拒绝间隔期间，系统会拒绝来自异常客户端的请求。
<b>Request Rejection Interval</b>	以分钟为单位输入拒绝请求的时间间隔。此选项仅在已选择在检测后拒绝请求 ( <b>Reject Requests After Detection</b> ) 复选框时可用。
<b>Suppress Repeated Successful Authentications</b>	选中此复选框以防重复报告前 24 小时内身份验证场景、网络设备和授权方面没有变更的成功身份验证。
<b>Accounting Suppression Interval</b>	以秒为单位输入抑制记帐请求报告的时间间隔。
<b>Long Processing Step Threshold Interval</b>	以毫秒为单位输入时间间隔。身份验证详细信息报告中会显示这些步骤。如果单个步骤的执行超出指定阈值，则在身份验证详细报告中会突出显示此步骤。
<b>RADIUS UDP 端口</b>	

#### 相关主题

[用于身份验证的协议设置](#)，第 549 页

[思科 ISE 中的 RADIUS 协议支持](#)，第 558 页

[配置 RADIUS 设置](#)，第 553 页

## SMS 网关设置

这些设置的导航路径为 **Guest Access > Settings > SMS Gateway**。

这些设置的导航路径为 **管理 (Administration) > 设置 (Settings) > SMS 网关 (SMS Gateway)**。

使用以下设置配置通过邮件服务器向访客和发起人发送 SMS 消息。

表 133: SMS 邮件网关的 SMS 网关设置

字段	使用指南
SMS Gateway Provider Domain	输入作为用于向提供商 SMS/MMS 网关发送消息的邮件地址主机部分的提供商域和作为此地址用户部分的访客帐户移动号码。
Provider account address	(可选) 输入作为电子邮件发件人地址 (通常是帐户地址) 的帐户地址, 并在 <b>访客访问 (Guest Access) &gt; 设置 (Settings)</b> 中覆盖默认电子邮件地址 ( <b>Default Email Address</b> ) 全局设置。
SMTP API destination address	(可选) 如果您使用的是需要具体帐户收件人地址的 SMTP SMS API (例如 Clickatell SMTP API), 请输入 SMTP API 目标地址。 此地址用作邮件的 TO 地址并且系统会将访客帐户的移动号码代入消息的正文模板中。
SMTP API body template	(可选) 如果您使用的是需要使用特定邮件正文模板来发送 SMS 的 SMTP SMS API (例如 SMTP API), 请输入 SMTP API 正文模板。 支持的动态替换为 \$mobilenumber\$、和 \$message\$。

这些设置的导航路径为 **Guest Access > Settings > SMS Gateway**。

使用以下设置配置通过 HTTP API（GET 或 POST 方法）向访客和发起人发送 SMS 消息。

表 134: SMS HTTP API 的 SMS 网关设置

字段	使用指南
URL	<p>输入 API 的 URL。</p> <p>此字段不是 URL 编码的。系统将访客帐户的手机号码代入 URL 中。支持的动态替换为 \$mobilenumber\$ and \$message\$。</p> <p>如果您将 HTTPS 用于 HTTP API，请在 URL 字符串中包含 HTTPS 并将您的提供商的受信任证书上传至思科 ISE。依次选择 <b>Administration &gt; System &gt; Certificates &gt; Trusted Certificates</b>。</p>
Data (Url encoded portion)	<p>输入 GET 或 POST 请求的数据（Url 编码部分）。</p> <p>此字段是 URL 编码的。如果使用默认 GET 方法，此数据附加于上述指定 URL 后面。</p>
Use HTTP POST method for data portion	<p>如果使用 POST 方法，请选中此选项。</p> <p>上述指定数据用作 POST 请求的内容。</p>
HTTP POST data content type	<p>如果使用 POST 方法，请指定内容类型，例如 “plain/text” 或 “application/xml”。</p>
HTTPS Username HTTPS Password HTTPS Host name HTTPS Port number	<p>输入此信息。</p>

#### 相关主题

[SMS 运营商和服务](#)，第 222 页

[配置 SMS 网关以向访客发送 SMS 通知](#)，第 222 页

## 身份管理

您可以使用这些窗口在思科 ISE 中配置和管理身份。

## 终端

通过这些窗口，您可以配置和管理连接到您的网络的终端。



## 终端设置

表 135: 终端设置

字段名称	使用指南
<b>MAC 地址</b>	<p>输入十六进制格式的 MAC 地址以静态创建终端。</p> <p>MAC 地址是连接到启用思科 ISE 的网络的接口设备标识符。</p>
<b>Static Assignment</b>	<p>如果您想要在“终端”(Endpoints) 窗口静态地创建终端并且已将静态分配的状态设置为静态，请选中此复选框。</p> <p>您可以将终端静态分配的状态从静态切换至动态或从动态切换至静态。</p>
<b>Policy Assignment</b>	<p>(除非选中<b>静态分配 (Static Assignment)</b> 复选框，否则会默认禁用此字段) 从<b>策略分配 (Policy Assignment)</b> 下拉列表选择匹配的终端策略。</p> <p>您可以执行以下操作之一：</p> <ul style="list-style-type: none"> <li>如果您不选择匹配的终端策略，而是使用默认终端策略 Unknown，则对于允许对终端进行动态分析的终端，其静态分配状态要设置为动态。</li> <li>如果您选择“未知”(Unknown) 之外的匹配终端策略，则对该终端，静态分配状态应设置为静态并且系统会自动选中<b>静态分配 (Static Assignment)</b> 复选框。</li> </ul>
<b>Static Group Assignment</b>	<p>当您想要向身份组静态分配终端时，请选中此复选框。</p> <p>如果您选中此复选框，下一次为之前动态分配至其他终端身份组的这些终端评估终端策略期间，分析服务不会更改终端身份组。</p> <p>如果您取消选中此复选框，则像 ISE 分析器根据策略配置所分配的一样，终端身份组处于动态状态。如果不选择 Static Group Assignment 选项，下一次评估终端策略期间，系统会自动将终端分配至匹配的身份组。</p>

字段名称	使用指南
<b>Identity Group Assignment</b>	<p>选择您要将终端分配至哪个终端身份组。</p> <p>当您静态创建终端，或在为某个终端评估终端策略期间不想使用<b>创建匹配身份组 (Create Matching Identity Group)</b> 选项时，可将终端分配至身份组。</p> <p>思科 ISE 包括以下系统创建的终端身份组：</p> <ul style="list-style-type: none"> <li>• 黑名单</li> <li>• GuestEndpoints</li> <li>• Profiled <ul style="list-style-type: none"> <li>• Cisco IP-Phone</li> <li>• Workstation</li> </ul> </li> <li>• RegisteredDevices</li> <li>• Unknown</li> </ul>

#### 相关主题

[已识别的终端](#)，第 438 页

[使用策略和身份的静态分配创建终端](#)，第 434 页

## 从 LDAP 设置导入终端

表 136: 从 LDAP 设置导入终端

字段名称	使用指南
<b>连接设置</b>	
<b>主机</b>	输入 LDAP 服务器的主机名或 IP 地址。
<b>Port</b>	<p>输入 LDAP 服务器的端口号。您可以使用默认端口 389 从 LDAP 服务器导入，并使用默认端口 636 通过 SSL 从 LDAP 服务器导入。</p> <p><b>注释</b> 思科 ISE 支持配置的任何端口号。配置值应与 LDAP 服务器连接的详细信息匹配。</p>
<b>Enable Secure Connection</b>	选中启用安全连接 ( <b>Enable Secure Connection</b> ) 复选框，通过 SSL 从 LDAP 服务器导入。
<b>Root CA Certificate Name</b>	<p>点击下拉箭头，查看受信任的 CA 证书。</p> <p>根 CA 证书名称指连接 LDAP 服务器所需的受信任 CA 证书。您可以在思科 ISE 中添加（导入）、编辑、删除并导出受信任的 CA 证书。</p>

字段名称	使用指南
<b>Anonymous Bind</b>	您必须选中 <b>匿名绑定 (Anonymous Bind)</b> 复选框，或输入 slapd.conf 配置文件中的 LDAP 管理员凭证。
<b>Admin DN</b>	输入 slapd.conf 配置文件中为 LDAP 管理员配置的可分辨名称 (DN)。 管理员 DN 格式示例：cn=Admin、dc=cisco.com、dc=com
<b>密码 (Password)</b>	输入 slapd.conf 配置文件中为 LDAP 管理员配置的密码。
<b>Base DN</b>	输入父项的可分辨名称。 基本 DN 格式示例：dc=cisco.com、dc=com。
<b>查询设置</b>	
<b>MAC Address objectClass</b>	输入用于导入 MAC 地址的查询过滤器，例如，ieee802Device。
<b>MAC Address Attribute Name</b>	输入导入操作返回的属性名称，例如，macAddress。
<b>Profile Attribute Name</b>	输入 LDAP 属性的名称。此属性为 LDAP 服务器中定义的每个终端条目保留策略名称。 当配置 <b>分析属性名称 (Profile Attribute Name)</b> 字段时，请考虑以下事项： <ul style="list-style-type: none"> <li>• 如果未在<b>分析属性名称 (Profile Attribute Name)</b> 字段中指定此 LDAP 属性或错误地配置此属性，则执行导入操作期间系统会将终端标记为“未知” (Unknown)，并且会根据匹配的终端分析策略单独分析这些终端。</li> <li>• 如果您在<b>分析属性名称 (Profile Attribute Name)</b> 字段中配置此 LDAP 属性，系统会验证属性值，以确保终端策略与思科 ISE 中的现有策略相匹配，然后导入终端。如果终端策略与现有策略不匹配，则不会导入这些终端。</li> </ul>
<b>超时</b>	输入时间值（以秒为单位）。有效范围是从 1 到 60 秒。

**相关主题**

[已识别的终端](#)，第 438 页

[从 LDAP 服务器导入终端](#)，第 437 页

**终端身份组设置**

表 137: 终端身份组设置

字段名称	使用指南
<b>Name</b>	输入您要创建的终端身份组的名称。

字段名称	使用指南
<b>Description</b>	输入对您要创建的终端身份组的说明。
<b>Parent Group</b>	<p>从父级组 (<b>Parent Group</b>) 下拉列表选择您要关联新创建的终端身份组的终端身份组。</p> <p>思科 ISE 包括以下终端身份组：</p> <ul style="list-style-type: none"> <li>• Blacklist</li> <li>• GuestEndpoints</li> <li>• Profiled</li> <li>• RegisteredDevices</li> <li>• Unknown</li> </ul> <p>此外，它还会再创建两个身份组：Cisco-IP-Phone 和 Workstation，这两个身份组与 Profiled（父）身份组关联。</p>

#### 相关主题

[已识别终端划分为终端身份组](#)，第 440 页  
[创建终端身份组](#)，第 440 页

## 外部身份源

您可以通过这些窗口配置和管理包含思科 ISE 用于身份验证和授权的用户数据的外部身份源。

### LDAP 身份源设置

#### LDAP 常规设置

下表介绍常规 (**General**) 选项卡上的字段。

表 138: LDAP 常规设置

字段名称	使用指南
<b>Name</b>	输入 LDAP 实例的名称。此值在搜索中用于获取主题 DN 和属性。此值为字符串类型，最大长度为 64 个字符。
<b>Description</b>	输入对 LDAP 实例的说明。此值为字符串类型，最大长度为 1024 个字符。

字段名称	使用指南
架构 (Schema)	<p>您可以选择以下任一内置架构类型或创建自定义架构：</p> <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Sun 目录服务器 (Sun Directory Server)</li> <li>• Novell eDirectory</li> </ul> <p>您可以点击 Schema 旁边的箭头以查看架构详细信息。</p> <p>如果您编辑该预定义架构的属性，思科 ISE 会自动创建自定义架构。</p>
注释	仅在您选择定制架构时，可以编辑以下字段。
<b>Subject Objectclass</b>	输入在搜索中用于获取主题 DN 和属性的值。此值为字符串类型，最大长度为 256 个字符。
<b>主题名称属性 (Subject Name Attribute)</b>	输入包含请求中用户名的属性的名称。此值为字符串类型，最大长度为 256 个字符。
<b>证书属性 (Certificate Attribute)</b>	输入包含证书定义的属性。对于基于证书的身份验证，这些定义用于验证由客户端提供的证书。
<b>Group Objectclass</b>	输入在搜索中用于指定识别为组的对象的值。此值为字符串类型，最大长度为 256 个字符。
<b>组映射属性 (Group Map Attribute)</b>	指定包含映射信息的属性。根据选择的参考方向，此属性可以是用户或组属性。
<b>主题对象包含对组的引用 (Subject Objects Contain Reference To Groups)</b>	如果使用者对象包含指定这些对象所属组的属性，请点击此选项。
<b>组对象包含对主题的引用 (Group Objects Contain Reference To Subjects)</b>	如果组对象包含指定使用者的属性，请点击此选项。此值为默认值。
<b>组对象作为...存储于成员属性中 (Subjects in Groups Are Stored in Member Attribute As)</b>	(仅适用于启用组对象包含对使用者的引用 (Group Objects Contain Reference To Subjects) 选项时) 指定在组成员属性中如何搜索成员，其默认值为 DN。



注释 配置的主题名称属性应在外部 ID 存储区中编入索引。

### LDAP 连接设置

下表介绍连接设置 (Connection Settings) 选项卡中的字段。

表 139: LDAP 连接设置

字段名称	使用指南
启用辅助服务器	选中此选项以在主要 LDAP 服务器出现故障的时候启用辅助 LDAP 服务器作为备份。如果选中此复选框，则必须输入辅助 LDAP 服务器的配置参数。
<b>主服务器和辅助服务器</b>	
Hostname/IP	输入运行 LDAP 软件的设备的 IP 地址或 DNS 名称。此主机可以包含 1 至 256 个字符或以字符串表示的有效 IP 地址。对于主机名，仅字母数字字符 (a 至 z; A 至 Z; 0 至 9)、点 (.) 和连字符 (-) 为有效字符。
端口	输入 LDAP 服务器侦听的 TCP/IP 端口号。有效值为 1 至 65535。默认值为 389，如 LDAP 规范中所述。如果您不知道端口号，可以向 LDAP 服务器管理员查询此信息。
访问	<p><b>匿名访问 (Anonymous Access):</b> 点击此选项可确保在 LDAP 目录中进行匿名搜索。服务器不识别客户端身份并且会允许客户端读取配置为允许任何未经身份验证的客户端访问的任何数据。在缺少要向服务器发送的具体策略许可身份验证信息的情况下，客户端应该使用匿名连接。</p> <p><b>身份验证访问 (Authenticated Access):</b> 点击此选项可确保使用管理凭证在 LDAP 目录上进行搜索。如果选择此选项，请为“管理员 DN” (Admin DN) 字段和“密码” (Password) 字段输入信息。</p>
管理员 DN (Admin DN)	输入管理员的 DN。管理员 DN 是有权限搜索“用户目录子树” (User Directory Subtree) 下所有必要用户和有权限搜索组的 LDAP 帐户。如果指定的管理员没有权限在搜索中查看组名称属性，对于由该 LDAP 服务器进行身份验证的用户，组映射将失败。
密码	输入 LDAP 管理员帐户密码。
安全身份验证 (Secure Authentication)	点击此字段以对思科 ISE 和主 LDAP 服务器之间的通信进行加密。验证“端口” (Port) 字段是否包含用于 LDAP 服务器上的 SSL 的端口号。如果启用此选项，则必须选择一个根 CA。
“LDAP 服务器根 CA” (LDAP Server Root CA)	从下拉列表中选择受信任根证书颁发机构，以启用使用证书的安全身份验证。

字段名称	使用指南
<b>服务器超时 (Server Timeout)</b>	以秒为单位输入思科 ISE 在确定与主要 LDAP 服务器的连接或身份验证失败之前等待该服务器响应的的时间。有效值为 1 至 99。默认值为 10。
<b>最大管理员连接数 (Max. Admin Connections)</b>	输入利用 LDAP 管理员帐户权限对于特定 LDAP 配置可以运行的并发连接的最大数量（大于 0）。这些连接用于在“用户目录子树” (User Directory Subtree) 和“组目录子树” (Group Directory Subtree) 下搜索目录中的用户和组。有效值为 1 至 99。默认值为 20。
<b>测试与服务器的绑定 (Test Bind to Server)</b>	点击此选项以测试并确保可以成功绑定 LDAP 服务器详细信息和凭证。如果测试失败，请编辑您的 LDAP 服务器详细信息并重新测试。
<b>Failover</b>	
<b>Always Access Primary Server First</b>	如果您希望思科 ISE 在进行身份验证和授权时始终先访问主 LDAP 服务器，请选中该选项。
<b>...后故障恢复到主服务器 (Failback to Primary Server after)</b>	如果思科 ISE 尝试连接的主 LDAP 服务器无法访问，思科 ISE 会尝试连接辅助 LDAP 服务器。如果您希望思科 ISE 再次使用主 LDAP 服务器，请点击此选项并在文本框中输入值。

### LDAP 目录组织设置

下表介绍目录组织 (Directory Organization) 选项卡上的字段。

表 140: LDAP 目录组织设置

字段名称	使用指南
<b>主题搜索库 (Subject Search Base)</b>	<p>输入包含所有主题的子树的 DN。例如：</p> <p>o=corporation.com</p> <p>如果包含主题的树是基本 DN，请输入：</p> <p>o=corporation.com</p> <p>或</p> <p>dc=corporation,dc=com</p> <p>根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。</p>

字段名称	使用指南
组搜索库 (Group Search Base)	<p>输入包含所有组的子树的 DN。例如： ou=organizational unit, ou=next organizational unit, o=corporation.com</p> <p>如果包含组的树是基本 DN，请键入： o=corporation.com</p> <p>或 dc=corporation,dc=com</p> <p>根据适用于您的 LDAP 配置而定。有关更多信息，请参阅您的 LDAP 数据库文档。</p>
搜索该格式的 MAC 地址 (Search for MAC Address in Format)	<p>输入一个 MAC 地址格式供思科 ISE 用于在 LDAP 数据库中进行搜索。在内部身份源中的 MAC 地址按照 xx-xx-xx-xx-xx-xx 格式进行搜索。LDAP 数据库中的 MAC 地址可以按照不同格式进行搜索。但是，当思科 ISE 收到主机查找请求时，思科 ISE 会将 MAC 地址从内部格式转换为此字段指定的格式。</p> <p>使用下拉列表以启用按照指定的格式搜索 MAC 地址，其中 <i>&lt;format&gt;</i> 可以是以下任何一种格式：</p> <ul style="list-style-type: none"> <li>• xxxx.xxxx.xxxx</li> <li>• xxxxxxxxxxxxxx</li> <li>• xx-xx-xx-xx-xx-xx</li> <li>• xx:xx:xx:xx:xx:xx</li> </ul> <p>您选择的格式必须与在 LDAP 服务器中搜索的 MAC 地址的格式一致。</p>
主题名称条开始直到最后一次出现分隔符 (Strip Start of Subject Name Up To the Last Occurrence of the Separator)	<p>输入适当的文本以删除用户名的域前缀。</p> <p>如果思科 ISE 在用户名中找到此字段中指定的分隔符，则会删除从用户名的开头一直到该分隔符的所有字符。如果用户名包含 <i>&lt;start_string&gt;</i> 框中指定的多个字符，思科 ISE 会删除从用户名的开头一直到该分隔符之前的最后一个匹配字符之间的所有字符。例如，如果分隔符为反斜线 (\)，用户名为 DOMAINuser1，则思科 ISE 会向 LDAP 服务器提交 user1。</p> <p>注释 <i>&lt;start_string&gt;</i> 不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (&gt;) 和左尖括号 (&lt;)。思科 ISE 不允许在用户名中使用这些字符。</p>



字段名称	使用指南
从第一次出现分隔符时主题名称条结束 (Strip End of Subject Name from the First Occurrence of the Separator)	<p>输入适当的文本以删除用户名的域后缀。</p> <p>如果思科 ISE 在用户名中找到此字段中指定的分隔符，则会删除从该分隔符一直到用户名结尾的所有字符。如果用户名包含此字段中指定的多个字符，思科 ISE 会删除从该分隔符之后的第一个匹配字符开始的所有字符。例如，如果分隔符为 @，用户名为 <i>user1@domain</i>，则思科 ISE 会向 LDAP 服务器提交 <i>user1</i>。</p> <p>注释 &lt;end_string&gt; 框不能包含以下特殊字符：井号 (#)、问号 (?)、引号 (“)、星号 (*)、右尖括号 (&gt;) 和左尖括号 (&lt;)。思科 ISE 不允许在用户名中使用这些字符。</p>

## LDAP 组设置

表 141: LDAP 组设置

字段名称	使用指南
添加	<p>选择 <b>Add</b>; 添加组添加新组或从目录中选择 <b>Add</b>; 选择 Group 选择组从 LDAP 目录。</p> <p>如果您选择添加组，请输入新组的名称。如果您正在从目录中选择，请输入过滤器条件，然后点击<b>检索组 (Retrieve Groups)</b>。点击要选择的组旁边的复选框，然后点击<b>确定 (OK)</b>。选中的组将显示在<b>组 (Groups)</b> 窗口中。</p>

## LDAP 属性设置

表 142: LDAP 属性设置

字段名称	使用指南
添加	<p>选择 <b>Add</b>; 添加属性添加新属性或从目录中选择 <b>Add</b>; 选择属性从 LDAP 服务器的属性。</p> <p>如果选择添加属性，则为新属性输入名称。如果从目录中选择，请输入用户名，然后点击<b>检索属性 (Retrieve Attributes)</b>以检索属性。选中想要选择的属性旁边的复选框，然后点击“确定”。</p>

## 相关主题

[LDAP 目录服务](#)，第 370 页

[LDAP 用户身份验证](#)，第 371 页

[LDAP 用户查找](#)，第 374 页

[添加 LDAP 身份源](#)，第 374 页

## RADIUS 令牌身份源设置

### 相关主题

[RADIUS 令牌身份源](#)，第 382 页

[添加 RADIUS 令牌服务器](#)，第 386 页

## RSA SecurID 身份源设置

### RSA 提示设置

下表介绍 **RSA 提示 (RSA Prompts)** 选项卡上的字段。

表 143: RSA 提示设置

字段名称	使用指南
<b>Enter Passcode Prompt</b>	输入文本字符串以获取密码。
<b>Enter Next Token Code</b>	输入文本字符串以请求下一个令牌。
<b>Choose PIN Type</b>	输入文本字符串以请求 PIN 类型。
<b>Accept System PIN</b>	输入文本字符串以接受系统生成的 PIN。
<b>Enter Alphanumeric PIN</b>	输入文本字符串以请求字母数字 PIN。
<b>Enter Numeric PIN</b>	输入文本字符串以请求数字 PIN。
<b>Re-enter PIN</b>	输入文本字符串以请求用户重新输入 PIN。

### RSA 消息设置

下表介绍 **RSA 消息 (RSA Messages)** 选项卡上的字段。

表 144: RSA 消息设置

字段名称	使用指南
<b>Display System PIN Message</b>	输入文本字符串以编辑系统 PIN 消息。
<b>Display System PIN Reminder</b>	输入文本字符串以通知用户记住新 PIN。
<b>Must Enter Numeric Error</b>	输入一条消息，指导用户仅输入数字作为 PIN。

字段名称	使用指南
<b>Must Enter Alpha Error</b>	输入一条消息，指导用户仅输入字母数字字符作为 PIN。
<b>PIN Accepted Message</b>	输入在系统接受用户的 PIN 时用户所看到的消息。
<b>PIN Rejected Message</b>	输入在系统拒绝用户的 PIN 时用户所看到的消息。
<b>User Pins Differ Error</b>	输入在用户输入错误 PIN 时所看到的消息。
<b>System PIN Accepted Message</b>	输入在系统接受用户的 PIN 时用户所看到的消息。
<b>Bad Password Length Error</b>	输入用户指定的 PIN 不属于在 PIN 长度策略中指定的范围时用户所看到的消息。

#### 相关主题

[RSA 身份源](#)，第 387 页

[思科 ISE 和 RSA SecurID 服务器集成](#)，第 388 页

[添加 RSA 身份源](#)，第 390 页

## 网络资源

### 对话感知网络 (SAnet) 的支持

思科 ISE 为对话感知网络 (SAnet) 提供有限支持。SAnet 是在许多思科交换机上运行的会话管理框架。SAnet 管理访问会话，包括可视性、身份验证和授权。SAnet 使用服务模板，其中包含 RADIUS 授权属性。思科 ISE 在授权配置文件中包含服务模板。思科 ISE 在授权配置文件中 使用标志来标识服务模板，该标志会将配置文件标识为兼容“服务模板”。

思科 ISE 授权配置文件包含转换为属性列表的 RADIUS 授权属性。SAnet 服务模板还包含 RADIUS 授权属性，但这些属性不会转换为列表。

对于 SAnet 设备，思科 ISE 会发送服务模板的名称。设备会下载服务模板的内容，除非该内容已存在于缓存或静态定义的配置中。当服务模板更改 RADIUS 属性时，思科 ISE 会向设备发送 CoA 通知。

## 网络设备

下列会话所描述的窗口可使您在思科 ISE 中添加和管理网络设备。

## 网络设备定义设置

下表介绍网络设备 (Network Devices) 窗口上的字段，您可以使用该窗口配置思科 ISE 中的网络访问设备。此页面的导航路径为：**管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices)**，然后单击**添加 (Add)**。

### 网络设备设置

下表介绍网络设备设置 (Network Device Settings) 窗口中的字段。

表 145: 网络设备设置

字段名称	Description
名称	<p>输入网络设备的名称。</p> <p>您可以为网络设备提供一个不同于设备主机名的描述性名称。设备名称是一个逻辑标识符。</p> <p>注释 如果需要，可以在配置后更改设备的名称。</p>
说明	输入设备的说明。
IP 地址或 IP 掩码	<p>输入单一 IP 地址和子网掩码。</p> <p>以下是定义 IP 地址和子网掩码时必须遵守的准则：</p> <ul style="list-style-type: none"> <li>您可以使用子网掩码定义一个特定 IP 地址或 IP 地址范围。如果设备 A 定义了 IP 地址范围，则可以使用在设备 A 中定义的 IP 地址范围的某个地址配置另一设备 B。</li> <li>您不能使用相同的特定 IP 地址定义两台设备。</li> <li>您不能使用同一 IP 地址范围定义两台设备。IP 地址范围不得部分或全部重叠。</li> </ul>
Model Name	<p>从下拉列表中选择设备型号。</p> <p>在基于规则的策略中查找条件时，可以将型号名称用作其中一个参数。此属性存在于设备字典中。</p>
软件版本	<p>从下拉列表中选择在网络设备上运行的软件版本。</p> <p>在基于规则的策略中查找条件时，您可以将软件版本用作其中一个参数。此属性存在于设备字典中。</p>
网络设备组 (Network Device Group)	<p>在网络设备组 (Network Device Group) 区域中，从位置 (Location)、和设备类型 (Device Type) 下拉列表中选择所需的值。</p> <p>如果未将设备专门分配到组，则设备将加入默认设备组（根网络设备组），位置为所有位置 (All Locations)，设备类型为所有设备类型 (All Device Types)。</p>



**注释** 使用过滤器从思科 ISE 部署中选择和删除网络访问设备 (NAD) 时，请清除浏览器缓存，以确保仅删除选定的 NAD。

### RADIUS 身份验证设置

下表介绍 **RADIUS 身份验证设置 (RADIUS Authentication Settings)** 区域中的字段。

表 146: RADIUS 身份验证设置

字段名称	使用指南
协议	显示 <b>RADIUS</b> 作为所选协议。
共享密钥	输入最大长度为 127 个字符的共享密钥。 共享密钥是您使用 <b>radius-host</b> 命令和 <b>pac</b> 关键词在网络设备上配置的密钥。
启用 KeyWrap (Enable KeyWrap)	仅当网络设备支持 KeyWrap 算法时，选中启用 <b>KeyWrap (Enable KeyWrap)</b> 复选框。网络设备必须与 AES KeyWrap RFC (RFC 3394) 兼容。 此选项用于通过 AES KeyWrap 算法提高 RADIUS 安全性。
密钥加密密钥 (Key Encryption Key)	(仅在启用 KeyWrap 时显示) 输入用于会话加密 (保密) 的加密密钥。 <b>注释</b> 当您在 FIPS 模式下运行思科 ISE 时，您必须在网络设备上启用 KeyWrap。
消息身份验证器代码密钥 (Message Authenticator Code Key)	(仅在启用 KeyWrap 时显示) 输入用于通过 RADIUS 消息传输的加密散列消息验证码 (HMAC) 计算的密钥。
密钥输入格式 (Key Input Format)	<p>点击以下格式之一对应的单选按钮：</p> <ul style="list-style-type: none"> <li>• <b>ASCII</b>：“密钥加密密钥” (Key Encryption Key) 长度必须为 16 个字符 (字节)，“消息身份验证器代码密钥” (Message Authenticator Code Key) 长度必须为 20 个字符 (字节)。</li> <li>• <b>十六进制 (Hexadecimal)</b>：“密钥加密密钥” (Key Encryption Key) 长度必须为 32 个字节，“消息身份验证器代码密钥” (Message Authenticator Code Key) 长度必须为 40 个字节。</li> </ul> <p>您可以指定要用于输入密钥加密密钥和消息身份验证器代码密钥的密钥输入格式，以便与网络设备上的配置相匹配。您指定的值必须是密钥的正确 (完整) 长度。不允许使用较短的值。</p>

## SNMP 设置

下表介绍 **SNMP 设置 (SNMP Settings)** 部分中的字段。

表 147: **SNMP** 设置区域中的字段

字段名称	使用指南
<b>SNMP 版本 (SNMP Version)</b>	<p>从 <b>SNMP (SNMP 版本)</b> 下拉列表中，选择以下选项之一：</p> <ul style="list-style-type: none"> <li>• <b>1</b>: SNMPv1 不支持通知。</li> <li>• <b>2c</b></li> <li>• <b>3</b>: SNMPv3 是最安全的型号，因为它允许您在选择 <b>安全级别</b> 字段中 <b>Priv</b> 时加密数据包。</li> </ul> <p>注释 如果已使用 SNMPv3 参数配置网络设备，则无法生成监控服务提供的网络设备会话状态 (<b>Network Device Session Status</b>) 摘要报告 (操作 (<b>Operations</b>) &gt; 报告 (<b>Reports</b>) &gt; 目录 (<b>Catalog</b>) &gt; 网络设备 (<b>Network Device</b>) &gt; 会话状态摘要 (<b>Session Status Summary</b>)。如果网络设备使用 SNMPv1 或 SNMPv2c 参数配置，则可以成功生成此报告。</p>
<b>SNMP 只读社区 (SNMP RO Community)</b>	(仅适用于 SNMP 版本 1 和 2c) 输入只读社区字符串，为思科 ISE 提供特殊类型的设备访问权限。
<b>SNMP 用户名 (SNMP Username)</b>	(仅适用于 SNMP 版本 3) 输入 SNMP 用户名。
<b>安全级别 (Security Level)</b>	<p>(仅适用于 SNMP 版本 3) 从安全级别 (<b>Security Level</b>) 下拉列表中选择以下选项之一：</p> <ul style="list-style-type: none"> <li>• <b>身份验证 (Auth)</b>: 启用 MD5 或安全散列算法 (SHA) 数据包身份验证。</li> <li>• <b>无身份验证 (No Auth)</b>: 无身份验证，无隐私安全级别。</li> <li>• <b>隐私 (Priv)</b>: 启用数据加密标准 (DES) 数据包加密。</li> </ul>
<b>身份验证协议 (Auth Protocol)</b>	<p>(选择安全级别身份验证 [<b>Auth</b>] 和隐私 [<b>Priv</b>] 时，仅适用于 SNMP 版本 3) 从身份验证协议 (<b>Auth Protocol</b>) 下拉列表中，选择希望网络设备使用的身份验证协议。</p> <ul style="list-style-type: none"> <li>• <b>MD5</b></li> <li>• <b>SHA</b></li> </ul>
<b>身份验证密码 (Auth Password)</b>	<p>(选择安全级别身份验证 [<b>Auth</b>] 和隐私 [<b>Priv</b>] 时，仅适用于 SNMP 版本 3) 输入身份验证密钥。密码的长度应至少为 8 个字符。</p> <p>点击<b>显示 (Show)</b>，显示已为设备配置的身份验证密码。</p>

字段名称	使用指南
隐私协议 (Privacy Protocol)	<p>(选择安全级别隐私 [Priv] 时, 仅适用于 SNMP 版本 3) 从隐私协议 (Privacy Protocol) 下拉列表中, 选择以下选项之一:</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• AES128</li> <li>• AES192</li> <li>• AES256</li> <li>• 3DES</li> </ul>
隐私密码 (Privacy Password)	<p>(选择安全级别隐私 [Priv] 时, 仅适用于 SNMP 版本 3) 输入隐私密码。 点击显示 (Show), 显示已为设备配置的隐私密码。</p>
轮询间隔 (Polling Interval)	<p>输入轮询间隔 (秒)。默认值为 3600。</p>
链路陷阱查询 (Link Trap Query)	<p>选中链路陷阱查询 (Link Trap Query) 复选框, 可接收和解析通过 SNMP 陷阱接收的链路接通和链路断开通知。</p>
MAC 陷阱查询 (Mac Trap Query)	<p>选中链路陷阱查询 (Link Trap Query) 复选框, 可接收和解析通过 SNMP 陷阱接收的 MAC 通知。</p>
Originating Policy Services Node (原始策略服务节点)	<p>从原始策略服务节点 (Originating Policy Services Node) 下拉列表中, 选择要用于轮询 SNMP 数据的思科 ISE 服务器。此字段的默认值为自动 (Auto)。从下拉列表中选择特定值以覆盖设置。</p>

### 高级 Trustsec 设置 (Advanced TrustSec Settings)

下表介绍高级 Trustsec 设置 (Advanced Trustsec Settings) 部分中的字段。

表 148: 高级 TrustSec 设置区域中的字段

字段名称	使用指南
将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)	<p>如果希望在设备 ID (Device ID) 字段中将设备名称作为设备标识符列出, 请选择中将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification) 复选框。</p>
设备 ID	<p>仅当未选中 将设备 ID 用于 Trustsec 标识 复选框时, 才能使用此字段。</p>

字段名称	使用指南
密码	<p>输入在思科 TrustSec 设备 CLI 中配置的密码，用于对思科 TrustSec 设备进行身份验证。</p> <p>点击<b>显示 (Show)</b> 可显示密码。</p>
<b>HTTP REST API 设置</b>	
<b>Trustsec 设备通知和更新设置</b>	
将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification)	<p>如果希望在设备 ID (Device ID) 字段中将设备名称作为设备标识符列出，请选中将设备 ID 用于 Trustsec 标识 (Use Device ID for TrustSec Identification) 复选框。</p>
设备 ID	<p>仅当未选中 将设备 ID 用于 Trustsec 标识 复选框时，才能使用此字段。</p>
密码	<p>输入在思科 TrustSec 设备 CLI 中配置的密码，用于对思科 TrustSec 设备进行身份验证。</p> <p>点击<b>显示 (Show)</b> 可显示密码。</p>
每<...>下载一次环境数据 (Download Environment Data Every <...>)	<p>通过从此区域的下拉列表中选择所需的值，指定设备从思科 ISE 下载其环境数据时必须遵守的时间间隔。您可以选择秒、分钟、小时、天或周为单位的时间间隔。默认值为一天。</p>
每<...>下载一次对等授权策略 (Download Peer Authorization Policy Every <...>)	<p>通过从此区域的下拉列表中选择所需的值，指定设备从思科 ISE 下载对等授权策略时必须遵守的时间间隔。您可以指定单位为秒、分钟、小时、天或周的时间间隔。默认值为一天。</p>
每<...>重新进行身份验证 (Reauthentication Every <...>)	<p>通过从此区域的下拉列表中选择所需的值，指定在初始身份验证后设备对照思科 ISE 重新进行身份验证的时间间隔。您可以配置秒、分钟、小时、天或周为单位的时间间隔。例如，如果输入 1000 秒，则设备会每 1000 秒对照思科 ISE 对自身重新进行身份验证。默认值为一天。</p>
每<...>下载 SGACL 列表 (Download SGACL Lists Every <...>)	<p>通过从此区域的下拉列表中选择所需的值，指定设备从思科 ISE 下载 SGACL 列表时遵守的时间间隔。您可以配置秒、分钟、小时、天或周为单位的时间间隔。默认值为一天。</p>



字段名称	使用指南
其他 TrustSec 设备信任该设备 (Trustsec 信任) (Other TrustSec Devices to Trust This Device [TrustSec Trusted])	选中其他 TrustSec 设备信任该设备 ( <b>Other TrustSec Devices to Trust This Device</b> ) 复选框，可允许所有对等设备信任此思科 TrustSec 设备。如果取消选中此复选框，则对等设备不信任此设备，所有从此设备到达的数据包都会相应地标注颜色或进行标记。
向此设备通知 Trustsec 配置更改 (Notify this device about TrustSec configuration changes)	如果希望思科 ISE 向此 TrustSec 设备发送 TrustSec CoA 通知，请选中此复选框。
<b>设备配置部署设置</b>	
当部署安全组标签映射更新时纳入该设备 (Include this device when deploying Security Group Tag Mapping Updates)	如果希望思科 TrustSec 设备使用设备接口凭据获取 IP-SGT 映射，请选中 <b>当部署安全组标记映射更新时包含此设备</b> 复选框。
EXEC 模式用户名 (EXEC Mode Username)	输入用于登录思科 TrustSec 设备的用户名。
EXEC 模式密码 (EXEC Mode Password)	输入设备密码。 点击 <b>显示 (Show)</b> 可查看密码。  注释 我们建议您避免在密码（包括 EXEC 模式和启用模式密码）中使用 % 字符，以避免安全漏洞。
启用模式密码 (Enable Mode Password)	（可选）输入用于在特权 EXEC 模式下编辑思科 TrustSec 设备配置的启用密码。 点击 <b>显示 (Show)</b> 可查看密码。
<b>带外 (OOB) Trustsec PAC 显示</b>	
颁发日期 (Issue Date)	显示思科 ISE 为思科 Trustsec 设备生成的最后一个思科 Trustsec PAC 的颁发日期。
到期日期	显示思科 ISE 为思科 Trustsec 设备生成的最后一个思科 Trustsec PAC 的到期日期。

字段名称	使用指南
颁发者	显示思科 ISE 为思科 Trustsec 设备生成的最后一个思科 Trustsec PAC 的颁发者（思科 TrustSec 管理员）名称。
生成 PAC (Generate PAC)	点击生成 PAC (Generate PAC) 按钮，为思科 TrustSec 设备生成带外思科 TrustSec PAC。

#### 相关主题

[在思科 ISE 中定义网络设备](#)

[思科 ISE 中的第三方网络设备支持](#)

[网络设备组，第 491 页](#)

[在思科 ISE 中添加网络设备](#)

[在思科 ISE 中配置第三方网络设备](#)

## 默认网络设备定义设置

下表介绍默认网络设备 (Default Network Device) 窗口中的字段，该窗口用于配置思科 ISE 可用于 RADIUS 和 TACACS+ 身份验证的默认网络设备。选择以下导航路径之一：

- 管理 (Administration) > 网络资源 (Network Resources) > 网络设备 (Network Devices) > 默认设备 (Default Device)
- 工作中心 (Work Centers) > 设备管理 (Device Administration) > 网络资源 (Network Resources) > 默认设备 (Default Devices)

表 149: “默认网络设备”窗口中的字段

字段名称	使用指南
Default Network Device Status	从默认网络设备状态 (Default Network Device Status) 下拉列表中选择启用 (Enable)，以启用默认网络设备定义。  注释 如果默认设备已启用，则必须通过选中窗口中的复选框启用 RADIUS 或 TACACS+ 身份验证设置。
设备配置文件	显示思科 (Cisco) 为默认的设备供应商。
<b>RADIUS 身份验证设置</b>	
启用 RADIUS	选中启用 RADIUS (Enable RADIUS) 复选框，启用设备的 RADIUS 身份验证。
共享密钥	输入共享密钥。共享密钥最大长度为 127 个字符。  共享密钥是您使用 <code>radius-host</code> 命令和 <code>pac</code> 关键词在网络设备上配置的密钥。
启用 KeyWrap (Enable KeyWrap)	(可选) 仅在网络设备支持 KeyWrap 算法时选中启用 KeyWrap (Enable KeyWrap) 复选框，这可以通过 AES KeyWrap 算法提高 RADIUS 安全性。

字段名称	使用指南
密钥加密密钥 (Key Encryption Key)	启用 KeyWrap 时，输入用于会话加密（保密）的加密密钥。
Message Authenticator Code Key	启用 KeyWrap 时，输入对 RADIUS 消息进行键控散列消息身份验证代码 (HMAC) 计算的密钥。
Key Input Format	<p>通过点击相应的单选按钮选择以下格式之一，并在密钥加密密钥 (Key Encryption Key) 和消息身份验证器代码密钥 (Message Authenticator Code Key) 字段中输入值：</p> <ul style="list-style-type: none"> <li>• <b>ASCII</b>：密钥加密密钥 (Key Encryption Key) 长度必须为 16 个字符（字节），而消息身份验证器代码密钥 (Message Authenticator Code Key) 长度必须为 20 个字符（字节）。</li> <li>• <b>十六进制 (Hexadecimal)</b>：密钥加密密钥 (Key Encryption Key) 长度必须为 32 个字节，而消息身份验证器代码密钥 (Message Authenticator Code Key) 长度必须为 40 个字节。</li> </ul> <p>指定要用于输入密钥加密密钥和消息身份验证器代码密钥的密钥输入格式，以便与网络设备上的配置相匹配。您指定的值必须是密钥的正确（完整）长度。不允许使用较短的值。</p>
<b>TACACS 身份验证设置</b>	
共享密钥	当 TACACS+ 协议启用时，输入文本字符串以分配给网络设备。请注意，在网络设备验证用户名和密码之前，用户必须输入文本。在用户提供共享密钥之前，连接始终被拒绝。
停用共享密钥处于启用状态 (Retired Shared Secret is Active)	当停用期处于启用状态时显示。
淘汰	停用现有的共享密钥而不是结束它。当您点击 <b>停用</b> 时，系统会显示一个对话框。点击是 (Yes) 或否 (No)。
剩余停用期 (Remaining Retired Period)	<p>（可选）仅当您在 <b>停用</b> 对话框中点击 <b>是</b> 时可用。显示在 <b>工作中心 &gt; 设备管理 &gt; 设置 &gt; 连接设置 &gt; 默认共享密钥失效期窗口</b> 中指定的默认值。您可以更改默认值。</p> <p>这允许输入新的共享密钥。旧共享密钥将在指定天数内保持有效。</p>
结束	（可选）仅当您在 <b>剩余停用期间</b> 对话框中选择 <b>是</b> 时可用。结束停用期并终止旧的共享密钥。

字段名称	使用指南
启用单连接模式 (Enable Single Connect Mode)	<p>选中启用单连接模式 (<b>Enable Single Connect Mode</b>) 复选框，将单一 TCP 连接用于与网络设备之间的所有 TACACS+ 通信。点击以下单选按钮之一：</p> <ul style="list-style-type: none"> <li>• 传统思科设备 (<b>Legacy Cisco Devices</b>)</li> <li>• TACACS 草案合规性单连接支持 (<b>TACACS Draft Compliance Single Connect Support</b>)。</li> </ul> <p>注释 如果禁用此字段，思科 ISE 会为每个 TACACS+ 请求使用新的 TCP 连接。</p>

## 设备安全设置

指定 RADIUS 共享密钥的最小长度。默认情况下，对于新安装和升级的部署，此值为 4 个字符。对于 RADIUS 服务器而言，长度最好为 22 个字符。



注释 在“网络设备” (Network Devices) 页面输入的共享密钥长度必须等于或大于在“设备安全设置” (Device Security Settings) 页面的“RADIUS 共享密钥最小长度” (Minimum RADIUS Shared Secret Length) 字段中配置的值。

### 相关主题

[网络设备定义设置](#)，第 740 页

## 网络设备导入设置

表 150: 导入网络设备设置

字段名称	使用指南
生成模板 (Generate a Template)	<p>点击创建模板 (<b>Generate a Template</b>) 可创建逗号分隔值 (CSV) 模板文件。</p> <p>使用 CSV 格式的网络设备信息更新模板，并将其保存在本地。然后，使用编辑的模板将网络设备导入任何思科 ISE 部署。</p>
文件	<p>点击 <b>浏览</b>，选择您可能最近创建的或以前从思科 ISE 部署导出的 CSV 文件。</p> <p>您可以使用 <b>导入</b> 选项将包含新的和更新后的网络设备信息的网络设备导入其他思科 ISE 部署中。</p>
用新数据覆盖现有数据 (Overwrite Existing Data with New Data)	<p>选中 <b>用新数据覆盖现有数据</b> 复选框可用您的导入文件中的设备取代现有网络设备。</p> <p>如不选中此复选框，则导入文件中可用的新网络设备定义将添加到网络设备存储库。系统会忽略重复条目。</p>

字段名称	使用指南
<b>Stop Import on First Error</b>	<p>如果您希望思科 ISE 在导入过程中遇到错误时停止导入，请选中<b>遇到第一个错误时停止导入 (Stop Import on First Error)</b> 复选框。思科 ISE 会导入网络设备，直至出现错误。</p> <p>如未选中此复选框并且遇到错误，系统会报错并且思科 ISE 会继续导入剩余设备。</p>

#### 相关主题

[在思科 ISE 中定义网络设备](#)

[思科 ISE 中的第三方网络设备支持](#)

[将网络设备导入思科 ISE](#)

## 管理网络设备组

通过以下窗口，您可以配置和管理网络设备组。

### 网络设备组设置

表 151: “网络设备组” (*Network Device Group*) 窗口中的字段

字段名称	使用指南
<b>Name</b>	<p>为根网络设备组输入一个名称。对于添加到该根网络设备组的所有后续子网络设备组，请输入这个新建网络设备组的名称。</p> <p>网络设备组的全称最多可以包含 100 个字符。例如，如果在父组<b>全球 (Global)</b> &gt; <b>亚洲 (Asia)</b> 下创建一个名为<b>印度 (India)</b> 的子组，则您创建的网络设备组的全称将为<b>全球 (Global)</b> &gt; <b>亚洲 (Asia)</b> &gt; <b>印度 (India)</b>。全称不能超过 100 个字符。如果网络设备组的全称超过 100 个字符，则网络设备组创建失败。</p>
<b>Description</b>	为根网络设备组或子网络设备组输入一段说明。
<b>Parent Group</b>	要将所创建的组添加到现有父组，请从下拉列表中选择一个父组。要将此新组添加为根组，请从下拉列表中选择 <b>添加为根组 (Add as root group)</b> 。
<b>Type</b>	<p>输入根网络设备组 (NDG) 的类型。</p> <p>所有添加到根网络设备组的子网络设备组都将继承组类型。</p> <p>如果此网络设备组是根网络设备组，则其类型可作为设备字典中的属性使用。您可以基于此属性定义条件。网络设备组的名称是此属性可以采用的值之一。</p>

#### 相关主题

[网络设备组](#)，第 491 页

[思科 ISE 在策略评估中使用的网络设备属性](#)，第 492 页

[在思科 ISE 中添加网络设备](#)

## 网络设备组导入设置

表 152: 网络设备组导入窗口中的字段

字段名称	使用指南
生成模板 (Generate a Template)	<p>点击此链接下载 CSV 模板文件。</p> <p>使用相同格式的网络设备组信息更新模板。将模板保存在本地，以便将网络设备组导入任何思科 ISE 部署中。</p>
文件	<p>点击 <b>浏览</b>，导航至您要上传的 CSV 文件的位置。该文件可能是新文件，也可能是从另一个思科 ISE 部署中导出的文件。</p> <p>可以将包含新的和更新后的网络设备组信息的网络设备组从一个思科 ISE 部署导入另一部署。</p>
用新数据覆盖现有数据 (Overwrite Existing Data with New Data)	<p>如果您希望思科 ISE 用您的导入文件中的设备组替换现有网络设备组，请选中此复选框。</p> <p>如果未选中此复选框，则只会将导入文件中的新网络设备组添加到网络设备组存储库。系统会忽略重复条目。</p>
Stop Import on First Error	<p>选中此复选框，可在导入期间遇到错误的第一个实例时停止导入。</p> <p>如果未选中此复选框并且遇到错误，思科 ISE 将报告错误，并继续导入剩余设备组。</p>

### 相关主题

[网络设备组](#)，第 491 页

[思科 ISE 在策略评估中使用的网络设备属性](#)，第 492 页

[将网络设备组导入到思科 ISE](#)，第 492 页

## 外部 RADIUS 服务器设置

表 153: 外部 RADIUS 服务器设置

字段名称	使用指南
Name	输入外部 RADIUS 服务器的名称。
Description	输入外部 RADIUS 服务器的说明。
Host IP	输入外部 RADIUS 服务器的 IP 地址。
Shared Secret	<p>输入思科 ISE 和外部 RADIUS 服务器之间用于对外部 RADIUS 服务器进行身份验证的共享密钥。共享密钥是用户必须提供的预期文本字符串，使网络设备能够验证用户名和密码。在用户提供共享密钥之前，连接始终被拒绝。共享密钥最大长度为 128 个字符。</p>

字段名称	使用指南
<b>Enable KeyWrap</b>	启用此选项，通过 AES KeyWrap 算法增加 RADIUS 协议安全性，帮助在思科 ISE 中实现 FIPS 140 合规性。
<b>Key Encryption Key</b>	（仅当选中启用密钥封装 ( <b>Enable Key Wrap</b> ) 复选框时）输入要用于会话加密（保密）的密钥。
<b>Message Authenticator Code Key</b>	（仅当选中启用密钥封装 ( <b>Enable Key Wrap</b> ) 复选框时）输入用于基于 RADIUS 消息的键控 HMAC 计算的密钥。
<b>Key Input Format</b>	<p>指定要在输入思科 ISE 加密密钥时使用的格式，使其匹配 WLAN 控制器上可用的配置。您指定的值必须是密钥的正确（完整）长度，符合下方的定义（不允许使用短于此长度的值）。</p> <ul style="list-style-type: none"> <li>• ASCII: “密钥加密密钥” (Key Encryption Key) 长度必须为 16 个字符（字节），“消息身份验证器代码密钥” (Message Authenticator Code Key) 长度必须为 20 个字符（字节）。</li> <li>• 十六进制 (Hexadecimal): “密钥加密密钥” (Key Encryption Key) 长度必须为 32 个字节，“消息身份验证器代码密钥” (Message Authenticator Code Key) 长度必须为 40 个字节。</li> </ul>
身份验证端口	输入 RADIUS 身份验证端口号。有效范围为 1 至 65535。默认值为 1812。
计费端口	输入 RADIUS 记账端口号。有效范围为 1 至 65535。默认值为 1813。
<b>Server Timeout</b>	输入思科 ISE 等待外部 RADIUS 服务器响应的秒数。默认值为 5 秒。有效值为 5 至 120。
<b>Connection Attempts</b>	输入思科 ISE 尝试连接到外部 RADIUS 服务器的次数。默认值为 3 次。有效值为 1 至 9。

#### 相关主题

[将思科 ISE 用作 RADIUS 代理服务器](#)，第 568 页

[配置外部 RADIUS 服务器](#)，第 569 页

## RADIUS 服务器序列

表 154: RADIUS 服务器序列

字段名称	使用指南
<b>Name</b>	输入 RADIUS 服务器序列的名称。
<b>说明 (Description)</b>	输入可选的说明。

字段名称	使用指南
<b>Host IP</b>	输入外部 RADIUS 服务器的 IP 地址。
<b>User Selected Service Type</b>	从 Available 列表框选择您要用作策略服务器的外部 RADIUS 服务器，并将其移入 Selected 列表框。
<b>Remote Accounting</b>	选中此复选框以在远程策略服务器上启用记账功能。
<b>Local Accounting</b>	选中此复选框以在思科 ISE 上启用记账功能。
高级属性设置	
<b>Strip Start of Subject Name up to the First Occurrence of the Separator</b>	选中此复选框以删除用户名的前缀。例如，如果主题名称是 acme\userA，分隔符为 \，则用户名成为 userA。
<b>Strip End of Subject Name from the Last Occurrence of the Separator</b>	选中此复选框以删除用户名的后缀。例如，如果主题名称是 userA@abc.com，分隔符为 @，则用户名成为 userA。  <ul style="list-style-type: none"> <li>• 您必须启用这些删除选项以从 NetBIOS 或用户主体名称 (UPN) 格式用户名 (user@domain.com 或 /domain/user) 提取用户名，因为系统向 RADIUS 服务器仅传递用户名以对用户进行身份验证。</li> <li>• 如果您同时激活 \ 和 @ 删除功能，而且您使用的是 AnyConnect，则思科 ISE 会从字符串中准确地删除第一个 \。但是，每个单独使用的剥离功能都按照设计与 AnyConnect 配合运行。</li> </ul>
<b>Modify Attributes in the Request to the External RADIUS Server</b>	选中此复选框以允许思科 ISE 修改往来于经过身份验证的 RADIUS 服务器的属性。  属性修改操作包括以下选项： <ul style="list-style-type: none"> <li>• 添加 (<b>Add</b>) - 向整体 RADIUS 请求/响应添加其他属性。</li> <li>• 更新 (<b>Update</b>) - 更改属性值（固定或静态）或将一个属性值替换为另一个属性值（动态）。</li> <li>• 删除 (<b>Remove</b>) - 删除属性或属性-值对。</li> <li>• 删除所有 (<b>RemoveAny</b>) - 删除所有出现的属性。</li> </ul>
<b>Continue to Authorization Policy</b>	选中此复选框以将代理流程转为运行授权策略，从而根据身份库组和属性检索结果执行进一步决策。如果启用此选项，来自外部 RADIUS 服务器的响应的属性将适用于身份验证策略选择。上下文中已有的属性将根据 AAA 服务器 accept response 属性的相应值进行更新。
<b>Modify Attributes before send an Access-Accept</b>	选中此复选框以在快要向设备发回响应之前修改属性。



## 相关主题

[将思科 ISE 用作 RADIUS 代理服务器](#)，第 568 页

[定义 RADIUS 服务器序列](#)，第 569 页

## NAC 管理器设置

表 155: NAC 管理器设置

字段	使用指南
名称	输入思科接入管理器 (CAM) 的名称。
Status	点击 Status 复选框，启用从验证连接的思科 ISE 分析器到 CAM 的 REST API 通信。
Description	输入 CAM 的说明。
IP Address	<p>输入 CAM 的 IP 地址。在思科 ISE 中创建和保存 CAM 后，无法编辑 CAM 的 IP 地址。</p> <p>您不能使用 0.0.0.0 和 255.255.255.255，因为在思科 ISE 中验证 CAM 的 IP 地址时，这些 IP 地址被排除在外。因此，它们不是您可以在 CAM 的 IP Address 字段中使用的有效 IP 地址。</p> <p><b>注释</b> 您可以使用一对 CAM 在高可用性配置中共享的虚拟服务 IP 地址。这允许在高可用性配置中支持 CAM 故障切换。</p>
Username	输入允许您登录 CAM 用户界面的 CAM 管理员的用户名。
Password	输入允许您登录 CAM 用户界面的 CAM 管理员的密码。

## 设备门户管理

### 配置设备门户设置

#### 设备门户的全局设置

选择 **工作中心 (Work Centers) > BYOD > 设置 (Settings) > 员工注册的设备 (Employee Registered Devices)** 或 **管理 (Administration) > 设备门户管理 (Device Portal Management) > 设置 (Settings)**。

您可以为 BYOD 门户和 My Devices 门户配置以下常规设置：

- **员工注册的设备 (Employee Registered Devices)**：在将员工限制为 (**Restrict employees to**) 中输入员工可注册的最大设备数量。默认情况下，此值设置为 **5** 台设备。

- **重试 URL (Retry URL):** 在**重试激活 URL (Retry URL for onboarding)** 中输入可用于将设备重定向至思科 ISE 的 URL。

当您配置这些常规设置后，它们适用于为您的公司设置的所有 BYOD 门户和 My Devices 门户。

#### 相关主题

- [限制员工注册的个人设备的数量](#)，第 471 页
- [提供用于重新连接 BYOD 注册流程的 URL](#)，第 472 页
- [分布式环境中的最终用户设备门户](#)，第 465 页

## 设备门户的门户标识设置

这些设置的导航路径为：**管理 (Administration) > 设备门户管理 (Device Portal Management) > 黑名单门户 (Blacklist Portal)、客户端调配门户 (Client Provisioning Portals)、BYOD 门户 (BYOD Portals)、MDM 门户 (MDM Portals) 或我的设备门户 (My Devices Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户设置和自定义 (Portals Settings and Customization)。**

- **门户名称 (Portal Name):** 输入用于访问此门户的唯一门户名称。请勿将此门户名称用于任何其他发起人门户、访客门户或非访客门户，如黑名单门户、自带设备 (BYOD) 门户、客户端调配门户、移动设备管理 (MDM) 门户或我的设备门户。

此名称显示在用于重定向选择的授权配置文件门户选择中。它应用于门户列表，以便在其他门户中轻松识别。

- **描述 (Description):** 可选。
- **门户测试 URL (Portal test URL):** 点击**保存 (Save)** 后，系统生成的 URL 会显示为链接。使用此连接来测试门户。

点击该链接可打开新的浏览器标签页，其中显示此门户的 URL。必须打开具有策略服务的策略服务节点 (PSN)。如果禁用策略服务，则 PSN 仅显示管理员门户。



**注释** 测试门户不支持 RADIUS 会话，因此您将无法看到所有门户的完整门户流程。BYOD 和客户端调配是取决于 RADIUS 会话的门户的示例。例如，重定向到外部 URL 时不起作用。如果有多个 PSN，思科 ISE 会选择第一个活动 PSN。

- **语言文件 (Language File):** 默认情况下，每个门户类型支持 15 种语言，这些语言可作为在单个压缩语言文件中捆绑在一起的单独属性文件使用。导出或导入要用于门户的压缩语言文件。压缩语言文件包含可用于显示门户的文本的所有单独语言文件。

语言文件包含到特定浏览器区域设置的映射，以及该语言下整个门户的所有字符串设置。单个语言文件包含所有受支持的语言，因此它可轻松用于实现翻译和本地化目的。

如果您更改一种语言的浏览器区域设置，则更改会应用于所有其他最终用户 Web 门户。例如，如果在热点访客门户中将 `French.properties` 浏览器区域设置从 `fr,fr-fr,fr-ca` 更改为 `fr,fr-fr`，则更改还会应用于我的设备门户。

在门户页面自定义 (**Portal Page Customizations**) 选项卡中自定义任何文本时，系统都会显示警报图标。警报消息会提醒您在自定义门户时对一种语言所做的任何更改必须同时添加到所有受支持的语言属性文件。您可以使用下拉列表选项手动关闭警报图标；或者它会在您导入更新后的压缩语言文件后自动关闭。

#### 相关主题

[创建授权策略规则](#)，第 484 页

[创建授权配置文件](#)，第 484 页

[个人设备门户](#)，第 466 页

## 黑名单门户的门户设置

此窗口的导航路径为：**管理 (Administration) > 设备门户管理 (Device Portal Management) > 黑名单门户 (Blacklist Portal) > 编辑 (Edit) > 门户行为和流设置 (Portal Behavior and Flow Settings) > 门户设置 (Portal Settings)**。

使用这些设置指定值，或者定义适用于整体门户而不仅是向用户（适用情况下的访客、发起人或员工）显示的特定门户页面的行为。

- **HTTPS 端口 (HTTPS Port)**: 输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此窗口之前会遵循这些设置。如果修改此窗口，应更新端口设置以遵守此限制。

如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。



**注释** 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 `ip host` 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces):** 选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

- 以太网接口必须使用不同子网上的 IP 地址。
- 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
- 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
- 在思科 ISE CLI 中配置 `ip host x.x.x.x x.yyy.domain.com` 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
- **证书组标签 (Certificate Group tag):** 选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **显示语言**
  - **使用浏览器区域设置 (Use Browser Locale):** 使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language):** 选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use):** 选择要用于门户的显示语言。此设置会覆盖用户浏览器区域 (**User Browser Locale**) 选项。

#### 相关主题

[编辑黑名单门户](#)，第 476 页

[黑名单门户](#)，第 467 页

[黑名单门户语言文件的 HTML 支持](#)，第 315 页

## BYOD 和 MDM 门户的门户设置

配置这些设置以定义门户页面操作。

- **HTTPS 端口 (HTTPS Port):** 输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此窗口之前会遵循这些设置。如果修改此窗口，应更新端口设置以遵守此限制。

如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。



**注释** 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 `ip host` 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces):** 选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

- 以太网接口必须使用不同子网上的 IP 地址。
- 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
- 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。

- 在思科 ISE CLI 中配置 `ip host x.x.x.x x.yyy.domain.com` 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
- **证书组标签 (Certificate Group tag)**: 选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **终端身份组 (Endpoint Identity Group)**: 选择用于跟踪访客设备的终端身份组。思科 ISE 提供 **GuestEndpoints** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。  
选择用于跟踪员工设备的终端身份组。思科 ISE 提供 **RegisteredDevices** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。
- **显示语言**
  - **使用浏览器区域设置 (Use Browser Locale)**: 使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language)**: 选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use)**: 选择要用于门户的显示语言。此设置会覆盖用户浏览器区域 (**User Browser Locale**) 选项。

#### 相关主题

[自带设备门户](#)，第 467 页

[创建 BYOD 门户](#)，第 478 页

[移动设备管理门户](#)，第 468 页

[创建 MDM 门户](#)，第 481 页

[自带设备门户语言文件的 HTML 支持](#)，第 315 页

[对移动设备管理门户语言文件的 HTML 支持](#)，第 321 页

## BYOD 门户的 BYOD 设置

字段名称	使用指南
包含一个 AUP (在页面上/作为链接) (Include an AUP [on page/as link])	将公司的网络使用条款和条件显示为当前为用户显示的窗口上的文本或者显示为用于打开包含 AUP 文本的新选项卡或窗口的链接。
要求接受 (Require Acceptance)	要求用户在其帐户完全启用之前接受 AUP。除非用户接受 AUP，否则不会启用登录 (Login) 按钮。如果用户不接受 AUP，将不会获取网络访问权限。

字段名称	使用指南
要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)	仅在启用在页面上包含一个 AUP (Include an AUP on page) 的情况下，才会显示此选项。 确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用接受 (Accept) 按钮。
在注册期间显示设备 ID 字段 (Display Device ID Field During Registration)	在注册过程中向用户显示设备 ID，即使设备 ID 已预配置并在使用 BYOD 门户时无法更改也如此。
原始 URL (Originating URL)	成功对网络进行身份验证后，将用户的浏览器重定向到用户正在尝试访问的原始网站（如果适用）。如果不适用，则系统会显示“身份验证成功” (Authentication Success) 窗口。请确保允许重定向 URL 通过 NAD 上的访问控制列表和在该 NAD 的思科 ISE 中配置的授权配置文件，在 PSN 的端口 8443 上工作。  对于 Windows、MAC 和 Android 设备，控制权交给自助调配向导应用，后者负责调配。因此，这些设备不会被重定向到原始 URL。但是，iOS (dot1X) 和不受支持的设备（允许进行网络访问）会重定向到此 URL。
注册成功页面	显示设备注册成功的页面。
URL	成功对网络进行身份验证后，将用户的浏览器重定向到指定的 URL，例如贵公司的网站。



**注释** 如果您在身份验证后将一个访客重定向到外部 URL，可能会在解析 URL 地址和重定向会话时有延迟。

#### 相关主题

[自带设备门户](#)，第 467 页

[创建 BYOD 门户](#)，第 478 页

[自带设备门户语言文件的 HTML 支持](#)，第 315 页

## 客户端调配门户的门户设置

这些设置的导航路径为 **管理 (Administration) > 设备门户管理 (Device Portal Management) > 客户端调配门户 (Client Provisioning Portals) > 创建、编辑或复制 (Create, Edit or Duplicate) > 门户行为和流量设置 (Portal Behavior and Flow Settings) > 门户设置 (Portal Settings)**。

- **HTTPS 端口 (HTTPS Port):** 输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此窗口之前会遵循这些设置。如果修改此窗口，应更新端口设置以遵守此限制。

如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。




---

**注释** 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

---

- **允许的接口 (Allowed interfaces)**: 选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

- 以太网接口必须使用不同子网上的 IP 地址。
- 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
- 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
- 在思科 ISE CLI 中配置 **ip host x.x.x.x, x.yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。



- **证书组标签 (Certificate Group tag)**: 选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **身份源序列 (Identity Source Sequence)**: 选择将哪个身份源序列用于用户身份验证。身份源序列是验证用户凭证时，按顺序搜索的身份存储区列表。

思科 ISE 包含适用于发起人门户的默认身份源序列: Sponsor\_Portal\_Sequence。

要配置身份源序列，请依次选择**管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences)**。

- **显示语言**
  - **使用浏览器区域设置 (Use Browser Locale)**: 使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。
  - **回退语言 (Fallback Language)**: 选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
  - **始终使用 (Always Use)**: 选择要用于门户的显示语言。此设置会覆盖用户浏览器区域 (**User Browser Locale**) 选项。

#### 相关主题

[客户端调配门户](#)，第 468 页

[创建客户端调配门户](#)，第 480 页

[客户端调配门户语言文件的 HTML 支持](#)，第 316 页

## MDM 门户的员工移动设备管理设置

字段名称	使用指南
包含一个 AUP (在页面上/作为链接) (Include an AUP [on page/as link])	将公司的网络使用条款和条件显示为当前为用户显示的窗口上的文本或者显示为用于打开包含 AUP 文本的新选项卡或窗口的链接。
要求接受 (Require Acceptance)	要求用户在其帐户完全启用之前接受 AUP。除非用户接受 AUP，否则不会启用 <b>登录 (Login)</b> 按钮。如果用户不接受 AUP，将不会获取网络访问权限。
要求滚动至 AUP 的末尾 (Require scrolling to end of AUP)	仅在启用在页面上包含一个 AUP (Include an AUP on page) 的情况下，才会显示此选项。 确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用 <b>接受 (Accept)</b> 按钮。

#### 相关主题

[移动设备管理门户](#)，第 468 页

[创建 MDM 门户](#)，第 481 页

## 移动设备管理器与思科 ISE 的互操作性

### 我的设备门户的门户设置

- **HTTPS 端口 (HTTPS Port):** 输入 8000 至 8999 之间的端口值；对于所有默认门户，默认值为 8443（黑名单门户除外，其端口值为 8444）。如果已使用此范围外的端口值进行升级，则在您修改此窗口之前会遵循这些设置。如果修改此窗口，应更新端口设置以遵守此限制。

如果向访客门户分配由非访客（例如“我的设备”）门户使用的端口，系统会显示错误消息。

仅针对安全评估和补救，客户端调配门户还使用 8905 和 8909 端口。否则，它使用分配给访客门户的相同端口。

分配给同一 HTTPS 端口的门户可以使用同一千兆以太网接口或其他接口。如果它们使用相同的端口和接口组合，则必须使用同一证书组标签。例如：

- 有效的组合包括（以发起人门户为例）：
  - 发起人门户：端口 **8443**，接口 **0**，证书标签 **A** 和我的设备门户：端口 **8443**，接口 **0**，证书组 **A**。
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：端口 **8445**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **1**，证书组 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **B**。
- 无效组合包括：
  - 发起人门户：端口 **8443**，接口 **0**，证书组 **A** 和我的设备门户：**8443**，接口 **0**，证书组 **B**。
  - 发起人门户：端口 **8444**，接口 **0**，证书标签 **A** 和黑名单门户：端口 **8444**，接口 **0**，证书组 **A**。



**注释** 我们建议为访客服务使用接口 0，以获得最佳性能。您可以在**门户设置 (Portal Settings)** 中仅配置接口 0，也可以使用 CLI 命令 **ip host** 将主机名或 FQDN 映射到接口 0 的 IP 地址。

- **允许的接口 (Allowed interfaces):** 选择 PAN 可用来运行门户的 PSN 接口。当 PAN 发送开启门户的请求时，PAN 查找 PSN 上的可用允许端口。您必须使用不同子网上的 IP 地址配置以太网接口。

这些接口必须在所有 PSN 上都可用，包括已开启策略服务的基于 VM 的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。

- 以太网接口必须使用不同子网上的 IP 地址。

- 您此处启用的接口必须在所有 PSN 上可用，包括策略服务打开时基于虚拟机的 PSN。由于其中任何 PSN 都可用于在访客会话的开头重定向，因此要求如此。
  - 门户证书使用者名称/备用使用者名称必须解析为接口 IP 地址。
  - 在思科 ISE CLI 中配置 **ip host x.x.x、x.yyy.domain.com** 以将辅助接口 IP 地址映射到 FQDN，用于匹配证书使用者名称/备用使用者名称。
- **证书组标签 (Certificate Group tag)**: 选取一个证书组标签，指定要用于门户的 HTTPS 流量的证书。
- **完全限定域名 (FQDN) (Fully Qualified Domain Name [FQDN])**: 为发起人门户或我的设备门户输入至少一个唯一 FQDN 或主机名。例如，可以输入 **sponsorportal.yourcompany.com, sponsor**，以便在用户将其中任一名称输入到浏览器中时，发起人门户会打开。以逗号分隔名称，但条目之间不包含空格。
- 如果更改默认 FQDN，还需执行以下操作：
- 更新 DNS，以便新 URL 的 FQDN 解析为有效的策略服务节点 (PSN) IP 地址。或者，此地址可能指向提供 PSN 池的负载均衡器虚拟 IP 地址。
  - 要避免由于名称不匹配而出现证书警告消息，请在思科 ISE PSN 的本地服务器证书的使用者备选名称 (SAN) 属性中加入自定义 URL 的 FQDN 或通配符。
- **身份源序列 (Identity Source Sequence)**: 选择将哪个身份源序列用于用户身份验证。身份源序列是验证用户凭证时，按顺序搜索的身份存储区列表。
- 思科 ISE 包含适用于发起人门户的默认身份源序列：Sponsor\_Portal\_Sequence。
- 要配置身份源序列，请依次选择**管理 (Administration) > 身份管理 (Identity Management) > 身份源序列 (Identity Source Sequences)**。
- **终端身份组 (Endpoint Identity Group)**: 选择用于跟踪访客设备的终端身份组。思科 ISE 提供 **GuestEndpoints** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。
- 选择用于跟踪员工设备的终端身份组。思科 ISE 提供 **RegisteredDevices** 终端身份组用作默认值。如果您选择不使用默认值，则还可以创建其他终端身份组。
- **当此身份组中的终端达到 \_\_ 天时将其清除 (Purge Endpoints in this Identity Group when they Reach \_\_ Days)**: 指定从思科 ISE 数据库中清除设备之前应经历的天数。每天都会进行清除，并且清除活动与整体清除时间同步。更改全局应用于此终端身份组。
- 如果根据其他策略条件对终端清除策略进行更改，则此设置不可再使用。
- **空闲超时 (Idle Timeout)**: 输入思科 ISE 在门户中没有活动的情况下注销用户之前要等待的时间（以分钟为单位）。有效范围为 1 至 30 分钟。
- **显示语言**
- **使用浏览器区域设置 (Use Browser Locale)**: 使用在客户端浏览器的区域设置中指定的语言作为门户的显示语言。如果思科 ISE 不支持浏览器区域设置的语言，则使用**回退语言 (Fallback Language)** 作为语言门户。

- **回退语言 (Fallback Language):** 选择当无法从浏览器区域设置获取语言或思科 ISE 不支持浏览器区域设置语言时使用的语言。
- **始终使用 (Always Use):** 选择要用于门户的显示语言。此设置会覆盖用户浏览器区域 (**User Browser Locale**) 选项。

#### 相关主题

- [我的设备门户](#)，第 468 页
- [创建我的设备门户](#)，第 482 页

## 我的设备门户的登录页面设置

- **速率限制之前最大失败登录尝试次数 (Maximum Failed Login Attempts Before Rate Limiting):** 指定思科 ISE 开始限制该帐户之前从单个浏览器会话尝试登录时的失败次数。这不会导致帐户锁定。限制的速率在限制速率时登录尝试之间的间隔时间 (**Time Between Login Attempts When Rate Limiting**) 中进行配置。
- **速率限制之前最大失败登录尝试次数 (Maximum Failed Login Attempts Before Rate Limiting):** 指定思科 ISE 开始限制该帐户之前从单个浏览器会话尝试登录时的失败次数。这不会导致帐户锁定。限制的速率在限制速率时登录尝试之间的间隔时间 (**Time Between Login Attempts When Rate Limiting**) 中进行配置。
- **包含 AUP (Include an AUP):** 将可接受使用策略窗口添加到流。可以将 AUP 添加到窗口，或链接到另一个窗口。

#### 相关主题

- [我的设备门户](#)，第 468 页
- [创建我的设备门户](#)，第 482 页
- [监控我的设备门户和终端活动](#)，第 486 页

## 我的设备门户的可接受使用策略页面设置

字段	使用指南
包含 AUP 页面 ( <b>Include AUP page</b> )	在单独的页面上向用户显示公司的网络使用条款和条件。
要求滚动至 AUP 的末尾 ( <b>Require scrolling to end of AUP</b> )	确保用户已完整阅读 AUP。仅在用户已滚动至 AUP 末尾时，才会启用接受 ( <b>Accept</b> ) 按钮。
仅首次登录时 ( <b>On First Login only</b> )	仅在用户首次登录到网络或门户时显示 AUP。
每次登录时 ( <b>On Every Login</b> )	每次用户登录到网络或门户时显示 AUP。

字段	使用指南
每__天（从首次登录算起）(Every __ Days [starting at first login])	在用户首次登录到网络或门户时定期显示 AUP。

#### 相关主题

[我的设备门户](#)，第 468 页

[创建我的设备门户](#)，第 482 页

## 我的设备门户的登录后横幅页面设置

字段名称	使用指南
包含登录后横幅页面 (Include a Post-Login Banner page)	在用户成功登录后并在向其授予网络访问权限之前显示其他信息。

#### 相关主题

[我的设备门户](#)，第 468 页

[创建我的设备门户](#)，第 482 页

## 我的设备门户的员工更改密码设置

要设置员工密码策略，请依次选择 **Administration > Identity Management > Settings > Username Password Policy**。

字段名称	使用指南
<b>Allow internal users to change password</b>	在员工登录 My Devices 门户后，允许员工更改其密码。 这仅适用于帐户存储于思科 ISE 数据库中的员工，不适用于帐户存储于外部数据库（例如 Active Directory 或 LDAP）的员工。

#### 相关主题

[创建我的设备门户](#)，第 482 页

[门户中的 UTF-8 字符支持](#)，第 81 页

## 管理我的设备门户的设备设置

表 156: 管理我的设备门户的设备设置

字段名称	使用指南
<b>Lost</b>	使员工可以指示其设备已丢失。此操作会将“我的设备” (My Devices) 门户中的设备状态更新为“丢失” (Lost) 并将该设备添加至黑名单终端身份组。

字段名称	使用指南
<b>Reinstate</b>	<p>此操作可恢复列入黑名单、已丢失或被盗的设备并将其状态重置为上一次的已知值。此操作会将被盗设备的状态重置为 <b>Not Registered</b>，因为它要经过额外调配才能连接网络。</p> <p>如果您要阻止员工恢复您已列入黑名单的设备，请勿在“我的设备” (My Devices) 门户中启用此选项。</p>
<b>删除</b>	<p>使员工在已注册设备达到最大数量时，可以从“我的设备” (My Devices) 门户删除已注册设备或删除未使用的设备和添加新设备。此操作会将设备从 My Devices 门户中显示的设备列表上删除，但是设备仍保留在思科 ISE 数据库中并继续列于 Endpoints 列表上。</p> <p>要定义员工可以使用 BYOD 门户或“我的设备” (My Devices) 门户注册的个人设备最大数量，请选择 <b>管理 (Administration) &gt; 设备门户管理 (Device Portal Management) &gt; 设置 (Settings) &gt; 员工注册的设备 (Employee Registered Devices)</b>。</p> <p>要从思科 ISE 永久删除设备，选择 <b>管理 (Administration) &gt; 身份管理 (Identity Management) &gt; 身份 (Identities) &gt; 终端 (Endpoints)</b>。</p>
<b>Stolen</b>	<p>使员工可以指示其设备已被盗。此操作会将“我的设备” (My Devices) 门户中的设备状态更新为 <b>Stolen</b> 并将该设备添加至黑名单终端身份组，然后删除其证书。</p>
<b>Device lock</b>	<p>仅适用于已向 MDM 注册的设备。</p> <p>在员工设备丢失或被盗的情况下，使员工可以立即从 My Devices 门户远程锁定其设备。此操作可防止他人未经授权而使用设备。</p> <p>但是，在 My Devices 门户中无法设置 PIN 而且员工应已提前在其移动设备上配置 PIN。</p>
<b>Unenroll</b>	<p>仅适用于已向 MDM 注册的设备。</p> <p>如果员工在工作中不再需要使用其设备，则可以选择此选项。此操作仅删除您公司安装的那些应用和设置，其他应用和数据仍会保留在员工的移动设备上。</p>
<b>Full wipe</b>	<p>仅适用于已向 MDM 注册的设备。</p> <p>使员工丢失其设备或换成使用新设备的情况下可以选择此选项。此操作会将员工的移动设备重置为其默认出厂设置，删除所安装的应用和数据。</p>

#### 相关主题

[管理员工添加的个人设备](#)，第 485 页

[我的设备门户](#)，第 468 页

## 为我的设备门户自定义添加、编辑和定位设备

在 **Page Customizations** 下，您可以自定义显示在我的设备门户的添加、编辑和定位选项卡中的消息、标题、内容、说明以及字段和按钮标签。

### 相关主题

[我的设备门户](#)，第 468 页

[创建我的设备门户](#)，第 482 页

## 设备门户的支持信息页面设置

字段名称	使用指南
包含支持信息页面 (Include a Support Information Page)	在门户的所有已启用窗口上显示指向信息窗口（例如联系我们 [Contact Us]）的链接。
MAC 地址	在支持信息 (Support Information) 窗口上包含设备的 MAC 地址。
IP 地址	在支持信息 (Support Information) 窗口上包含设备的 IP 地址。
浏览器用户代理	在支持信息 (Support Information) 窗口上包含浏览器详细信息，如产品名称和版本、布局引擎，以及发起请求的用户代理的版本。
策略服务器 (Policy Server)	在支持信息 (Support Information) 窗口上包含服务此门户的 ISE 策略服务节点 (PSN) 的 IP 地址。
故障代码	如果适用，请包含日志消息目录中的对应编号。要查看消息目录，选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 消息目录 (Message Catalog)。
隐藏字段 (Hide Field)	如果字段标签将会包含的信息不存在，请勿在支持信息 (Support Information) 窗口上显示任何字段标签。例如，如果故障代码未知并因此为空白，请勿显示故障代码 (Failure code)，即使已选择故障代码也如此。
显示不含任何值的标签 (Display Label with no Value)	在支持信息 (Support Information) 窗口上显示所有选定字段标签，即使其将会包含的信息不存在也如此。例如，如果故障代码未知，请显示故障代码 (Failure code)，即使其为空白也如此。
显示含默认值的标签 (Display Label with Default Value)	如果标签将会包含的信息不存在，请在支持信息 (Support Information) 窗口上的任何选定字段中显示此文本。例如，如果在此字段中输入“不可用” (Not Available)，并且故障代码未知，则故障代码 (Failure Code) 将显示不可用 (Not Available)。

### 相关主题

[监控我的设备门户和终端活动](#)，第 486 页

[访问设备门户](#)，第 467 页







# 第 15 章

## Cisco pxGrid

- 思科 pxGrid 节点，第 769 页

### 思科 pxGrid 节点

可以使用思科 pxGrid 与其他网络系统（例如思科 ISE 生态系统合作伙伴系统）和其他思科平台共享思科 ISE 会话目录中的情景相关信息。pxGrid 框架也可用来在思科 ISE 与第三方供应商之间、在节点（例如共享标记）与策略对象之间交换策略和配置数据，还能进行其他信息的交换。思科 pxGrid 还允许第三方系统调通过自适应网络控制操作来隔离用户和/或设备以应对网络或安全事件。可通过思科 TrustSec 主题将标签定义、值和说明等思科 TrustSec 信息从思科 ISE 传输到其他网络。可通过终端配置文件元主题，将具有完全限定名称 (FQN) 的终端配置文件从思科 ISE 传输到其他网络。思科 pxGrid 还支持标签和终端配置文件的批量下载。

在高可用性配置中，思科 pxGrid 服务器通过 PAN 在节点之间复制信息。当 PAN 关闭时，思科 pxGrid 服务器会停止处理客户端注册和订用。需要手动升级 PAN，以激活思科 pxGrid 服务器。

在具有 pxGrid 角色的活动思科节点上，这些进程会显示为正在运行 (**Running**)。在备用思科 pxGrid 节点上，它们会显示为备用 (**Standby**)。如果活动 pxGrid 节点关闭，备用 pxGrid 节点会检测到此情况，并启动四个 pxGrid 进程。在几分钟内，这些进程显示为正在运行 (**Running**)，备用节点成为活动节点。可以运行 CLI 命令 `show logging application pxgrid/pxgrid.state` 来验证思科 pxGrid 服务在此节点上是否处于备用状态。

启动面向辅助思科 pxGrid 节点的自动故障切换后，如果原始主思科 pxGrid 节点重新接入网络，则除非当前主节点关闭，否则原始主思科 pxGrid 节点将继续具有辅助角色，并且不会重新升级到主角色。



---

**注释** 有时，原始主思科 pxGrid 节点可能会自动重新升级回主角色。

---

在高可用性部署中，当主 pxGrid 节点关闭时，可能需要大约 3 到 5 分钟来切换到辅助 pxGrid 节点。我们建议客户端等待故障切换完成，然后再清除缓存数据，以防主思科 pxGrid 节点发生故障。

以下日志可用于思科 pxGrid 节点：

- pxgrid.log：通过状态变更通知。

- pxgrid-cm.log: 显示有关客户端与服务器之间的发布者和/或用户以及数据交换活动的更新。
- pxgrid-controller.log: 显示客户端功能、组和客户端授权的详细信息。
- pxgrid-jabberd.log: 显示与系统状态和身份验证相关的所有日志。
- pxgrid-pubsub.log: 显示与发布者和用户事件相关的所有信息。



注释



注释 可以使用 Base 许可证启用思科 pxGrid，但必须使用 Plus 许可证才能启用思科 pxGrid 角色。



注释

## 思科 pxGrid 客户端和功能管理

使用 Cisco pxGrid 服务之前，连接到思科 ISE 的客户端必须注册并获得帐户审批。Cisco pxGrid 客户端使用 Cisco pxGrid SDK 中提供的 Cisco pxGrid 客户端库成为客户端。思科 ISE 同时支持自动和手动批准。客户端可以使用唯一名称和基于证书的相互身份验证登录 Cisco pxGrid。类似于交换机上的 AAA 设置，客户端可以连接已配置的 Cisco pxGrid 服务器主机名或 IP 地址。

Cisco pxGrid 功能是指 Cisco pxGrid 上供客户端发布和订用的信息主题或信道。在思科 ISE 中，仅支持身份、自适应网络控制 (ANC) 和安全组访问 (SGA) 等功能。您可以启用或禁用功能。如果禁用这些功能，客户端就被取消订用。可通过发布、定向查询或批量下载查询，从发布方获取功能信息。

### 相关主题

[生成思科 pxGrid 证书](#)

## 启用 pxGrid 服务

### 开始之前

- 至少在一个节点上启用 pxGrid 角色，以查看思科 pxGrid 客户端发送的请求。
- 启用身份映射。有关详细信息，请参阅[配置身份映射](#)，第 58 页。

**步骤 1** 选择管理 (Administration) > pxGrid 服务 (pxGrid Services)。

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

**步骤 3** 要查看功能，请点击右上角的根据功能查看 (View by Capabilities)。

步骤 4 点击刷新 (Refresh) 查看最新的状态。

步骤 5 选择要启用的功能，并点击启用 (Enable)。

步骤 6 单击刷新 (Refresh) 查看最新的状态。

---

## 部署思科 pxGrid 节点

在独立节点和分布式部署节点上都可以启用思科 pxGrid 角色。

### 开始之前

- 所有节点都将 CA 证书用于思科 pxGrid 服务用途。如果在升级之前对思科 pxGrid 服务使用默认证书，则升级时会将该证书替换为内部 CA 证书。
- 如果您使用的是分布式部署或从思科 ISE 1.2 升级，则需要为证书启用 pxGrid 用途选项。您可以在系统证书 (System Certificates) 窗口中启用 pxGrid 用途选项。此窗口的导航路径为管理 (Administration) > 证书 (Certificates) > 系统证书 (System Certificates)。选择用于部署的证书，然后点击编辑 (Edit) 选中 **pxGrid: 使用 pxGrid 控制器证书 (pxGrid: use certificate for the pxGrid Controller)** 复选框。
- 必须为 Websocket (pxGrid 2.0) 打开端口 8910，并为 XMPP (pxGrid V1.0) 打开端口 5222。如果在节点上禁用思科 pxGrid 服务，则端口 5222 将关闭，但是端口 8910 仍正常工作，并继续响应请求。

---

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

步骤 2 在部署节点 (Deployment Nodes) 窗口中，选中要为其启用思科 pxGrid 服务的节点旁的复选框，然后点击编辑 (Edit)。

步骤 3 点击常规设置 (General Settings) 选项卡，选中 **pxGrid** 复选框。

步骤 4 点击 Save。

注释 当从以前的版本升级时，系统可能会禁用保存 (Save) 选项。当浏览器缓存引用以前版本的思科 ISE 中的旧文件时，就会发生这种情况。清除浏览器缓存以启用保存 (Save) 选项。

---

## 思科 pxGrid 实时日志

“实时日志” (Live Logs) 窗口会显示所有 pxGrid 管理事件。事件信息包括客户端和功能名称，以及事件类型和时间戳。

此窗口的导航路径为管理 (Administration) > pxGrid 服务 (pxGrid Services) > 实时日志 (Live Log)。您还可以清除日志并重新同步或刷新列表。





## 第 16 章

# 集成

以下各节介绍思科 ISE 上的无线设置配置以及交换机和无线控制器上支持思科 ISE 功能所需的配置。

- 使交换机能够支持标准 Web 身份验证，第 773 页
- 为综合 RADIUS 事务定义本地用户名和密码，第 774 页
- 配置 NTP 服务器以获得准确的日志和记账时间戳，第 774 页
- 启用 AAA 功能的命令，第 774 页
- 交换机上的 RADIUS 服务器配置，第 775 页
- 将交换机配置为向 Inline Posture 节点发送 RADIUS 记帐开始/停止消息，第 775 页
- 启用交换机处理 RADIUS 更改授权 (CoA)，第 776 页
- 在交换机端口上启用设备跟踪和 DHCP 监听，第 776 页
- 为交换机端口启用 802.1X 基于端口的身份验证，第 776 页
- 为关键身份验证启用 EAP，第 777 页
- 使用恢复延迟来限制 AAA 请求，第 777 页
- 根据实施状态定义 VLAN，第 777 页
- 交换机上的本地（默认）访问列表 (ACL) 定义，第 778 页
- 对 802.1X 和 MAB 启用交换机端口，第 779 页
- 启用 EPM 日志记录，第 781 页
- 启用交换机以接收 SNMP 陷阱，第 781 页
- 在交换机上启用 SNMP v3 查询以进行分析，第 781 页
- 启用 MAC 通知陷阱以使分析器进行收集，第 781 页
- 在交换机上配置 RADIUS 空闲超时，第 782 页
- 用于 iOS 请求方调配的无线控制器配置，第 782 页
- Apple 设备的无线 LAN 控制器支持，第 782 页
- 在无线控制器上配置 ACL 以实现 MDM 互操作性，第 783 页

## 使交换机能够支持标准 Web 身份验证

请确保在交换机配置中包含以下命令，以为思科 ISE 启用标准 Web 身份验证功能，包括身份验证后的 URL 重定向调配：

```
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.2.3

ip http server
! Must enable HTTP/HTTPS for URL-redirection on port 80/443

ip http secure-server
```

## 为综合 RADIUS 事务定义本地用户名和密码

输入以下命令以使交换机像该网络的 RADIUS 一样与思科 ISE 节点通信：

```
username test-radius password 0 abcde123
```

## 配置 NTP 服务器以获得准确的日志和记账时间戳

输入以下命令，确保在交换机上指定的 NTP 服务器与思科 ISE 中的设置相同：

```
ntp server <IP_address>|<domain_name>
```

## 启用 AAA 功能的命令

在交换机上输入以下命令可启用交换机与思科 ISE 之间的各种 AAA 功能，包括 802.1X 和 MAB 身份验证功能：

```
aaa new-model

! Creates an 802.1X port-based authentication method list

aaa authentication dot1x default group radius

! Required for VLAN/ACL assignment

aaa authorization network default group radius

! Authentication & authorization for webauth transactions

aaa authorization auth-proxy default group radius

! Enables accounting for 802.1X and MAB authentications

aaa accounting dot1x default start-stop group radius

!

aaa session-id common
```

```
!  
aaa accounting update periodic 1440  
  
! Update AAA accounting information periodically every 1440 minutes  
  
aaa accounting system default start-stop group radius  
  
!
```

## 交换机上的 RADIUS 服务器配置

输入以下命令，将交换机配置为与用作 RADIUS 源服务器的思科 ISE 进行互操作：

```
!  
radius-server <ISE Name>  
  
! ISE Name is the name of the ISE PSN  
  
address ipv4 <ip address> auth-port 1812 acct-port 1813  
  
! IP address is the address of the PSN. This example uses the standard RADIUS ports.  
  
key <passwd>  
  
! passwd is the secret password configured in Cisco ISE  
  
exit
```



**注释** 我们建议将死亡标准时间配置为 30 秒，期间允许 3 次重试，为使用 Active Directory 进行身份验证的 RADIUS 请求提供更长的响应时间。

## 将交换机配置为向 Inline Posture 节点发送 RADIUS 记帐开始/停止消息

将网络接入设备配置为在会话开始和结束时发送 RADIUS 记账“开始”和“停止”消息。发送到内联安全评估节点的消息包含远程设备的 IP 地址。内联安全评估节点将设备 IP 地址与在会话持续期间下载的任何相关授权配置文件关联。例如，某个远程设备在初始登录时可能会有一个“合规性状态未知”授权配置文件，然后在 CoA 之后（假设设备安全评估成功）会改为“合规”授权配置文件。

## 启用交换机处理 RADIUS 更改授权 (CoA)

请通过输入以下命令，指定设置以确保交换机能够相应地处理 RADIUS CoA 和相关的思科 ISE 的安全状态功能：

```
aaa server radius dynamic-author client <ISE-IP> server-key 0 abcde123
```



注释

- 思科 ISE 将端口 1700（思科 IOS 软件默认端口）与 RFC 默认端口 3799 用于 CoA。现有 Cisco Secure ACS 5.x 客户如果将 CoA 作为现有 ACS 实施的环节，则可能已将此端口设置为端口 3799。
- 密钥应与添加网络设备时在思科 ISE 上配置的密钥相同，并且 IP 地址应为 PSN IP 地址。

## 在交换机端口上启用设备跟踪和 DHCP 监听

要帮助提供思科 ISE 面向安全的可选功能，请在交换机端口动态 ACL 中针对 IP 替代启用设备跟踪和 DHCP 监听，您可输入以下命令：

```
! Optional
ip dhcp snooping

! Required!

! Configure Device Tracking Policy!device-tracking policy <DT_POLICY_NAME>no protocol
ndp tracking enable

! Bind it to interface!interface <interface_id>device-tracking
attach-policy<DT_POLICY_NAME>
```

在 RADIUS 记帐中，即便已启用 DHCP 监听，DHCP 属性也不会通过 IOS 传感器发送到思科 ISE。在这种情况下，则应启用 VLAN 的 DHCP 监听使 DHCP 成为活动状态。

使用以下命令启用 VLAN 的 DHCP 监听：

```
ip dhcp snooping
ip dhcp snooping vlan 1-100
```

## 为交换机端口启用 802.1X 基于端口的身份验证

输入以下命令在全局范围内开启交换机端口的 802.1X 身份验证：

```
dot1x system-auth-control
```



## 为关键身份验证启用 EAP

要支持局域网上的请求方身份验证请求，请输入以下命令，为临界身份验证（不可访问的身份验证绕行）启用 EAP：

```
dot1x critical eapol
```

## 使用恢复延迟来限制 AAA 请求

在关键身份验证恢复的情况下，配置交换机以自动引入身份验证延迟（以毫秒为单位），确保思科 ISE 可以在恢复后再次启动服务。使用以下命令：

```
authentication critical recovery delay 1000
```

## 根据实施状态定义 VLAN

输入以下命令，根据网络中已知的实施状态，定义 VLAN 名称、编号和虚拟交换机接口 (SVI)。创建单独的 VLAN 接口，实现网络间路由。对于处理来自终端（如 PC、笔记本电脑）和终端通过其连接到网络的 IP 电话等在同一网段上传递的多个流量源，这特别有帮助。



**注释** 第一个 IP 助手进入 DHCP 服务器，第二个 IP 助手将 DHCP 请求副本发送至 Inline Posture 节点进行分析。

```
vlan <VLAN_number>
name ACCESS!
vlan <VLAN_number>
name VOICE

!
interface <VLAN_number>
description ACCESS
ip address 10.1.2.3 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
ip helper-address <Cisco_ISE_IP_address>

!
interface <VLAN_number>
description VOICE
ip address 10.2.3.4 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
```

## 交换机上的本地（默认）访问列表 (ACL) 定义

通过输入以下命令，在较低版本的交换机（使用低于 12.2(55)SE 版本的思科 IOS 软件的交换机）上启用这些功能，确保思科 ISE 能够执行进行身份验证和授权所需的动态 ACL 更新。

```
ip access-list extended ACL-ALLOW

  permit ip any any

!

ip access-list extended ACL-DEFAULT

  remark DHCP

  permit udp any eq bootpc any eq bootps

  remark DNS

  permit udp any any eq domain

  remark Ping

  permit icmp any any

  remark Ping

  permit icmp any any

  remark PXE / TFTP

  permit udp any any eq tftp

  remark Allow HTTP/S to ISE and WebAuth portal
  permit tcp any host <Cisco_ISE_IP_address> eq www

  permit tcp any host <Cisco_ISE_IP_address> eq 443

  permit tcp any host <Cisco_ISE_IP_address> eq 8443

  permit tcp any host <Cisco_ISE_IP_address> eq 8905

  permit udp any host <Cisco_ISE_IP_address> eq 8905

  permit udp any host <Cisco_ISE_IP_address> eq 8906

  permit tcp any host <Cisco_ISE_IP_address> eq 8080

  permit udp any host <Cisco_ISE_IP_address> eq 9996
```

```
remark Drop all the rest

deny ip any any log

!

! The ACL to allow URL-redirection for WebAuth
ip access-list extended ACL-WEBAUTH-REDIRECT

permit tcp any any eq www

permit tcp any any eq 443
```



**注释** 无线控制器上的这种配置可以提高 CPU 使用率，但是也会提高系统不稳定的风险。这是 IOS 问题，不会对思科 ISE 产生不利影响。

## 对 802.1X 和 MAB 启用交换机端口

要为 802.1X 和 MAB 启用交换机端口，请执行以下操作：

**步骤 1** 使所有接入交换机端口进入接口配置模式：

```
interface range FastEthernet0/1-8
```

**步骤 2** 启用交换机端口的接入模式（而不是中继模式）：

```
switchport mode access
```

**步骤 3** 静态配置接入 VLAN。这样，即可在本地调配接入 VLAN，这也是开放模式身份验证所要求的：

```
switchport access vlan <VLAN_number>
```

**步骤 4** 静态配置语音 VLAN：

```
switchport voice vlan <VLAN_number>
```

**步骤 5** 启用开放模式身份验证。身份验证完成之前，开放模式允许将流量桥接至数据和语音 VLAN。我们强烈建议您在生产环境中使用基于端口的 ACL，以防止进行未经授权的访问。

启用开放模式身份验证还会在 AAA 服务器响应之前允许预身份验证访问，具体取决于端口 ACL。

```
authentication open
```

**步骤 6** 应用基于端口的 ACL，确定默认情况下应将哪些流量从未经授权的终端桥接至接入 VLAN。由于您应首先允许所有访问，然后再实施策略，因此您应当应用 ACL-ALLOW，以允许所有流量都流经交换机端口。您已创建默认的思科 ISE 授权，允许到目前为止的所有流量，这是因为我们希望实现完全可见性，并且不希望影响到现有最终用户的体验。

必须配置 ACL 才能从 AAA 服务器预设定动态 ACL。

```
ip access-group ACL-ALLOW in
```

**注释** 在 DSBU 交换机上使用思科 IOS 软件版本 12.2(55)SE 之前，需提供端口 ACL 才能从要应用的 RADIUS AAA 服务器获取动态 ACL。如果未能设置默认 ACL，交换机将忽略分配的动态 ACL。使用思科 IOS 软件版本 12.2(55)SE 时，系统会自动生成并应用默认 ACL。

**注释** 我们之所以在实验室中使用 ACL-ALLOW，是因为我们希望启用基于 802.1X 端口的身份验证，但对现有网络造成任何影响。在稍后的练习中，我们将应用不同的 ACL-DEFAULT，以阻止生产环境中产生不需要的流量。

**步骤 7** 启用多身份验证主机模式。多身份验证可以说是多域身份验证 (MDA) 的超集。MDA 只允许数据域中有一个终端。当配置多身份验证时，语音域中只允许有一个身份验证电话（和 MDA 一样），但在数据域中却可以对不限数量的数据设备进行身份验证。

允许在同一个物理接入端口上使用语音和多个终端

**authentication host-mode multi-auth**

**注释** IP 电话背后的多台数据设备（无论是虚拟设备还是连接到集线器的物理设备）都可以增强接入端口的物理链路状态感知能力。

**步骤 8** 通过以下命令启用各种身份验证方式的选项：

启用重新进行身份验证：

**authentication periodic**

通过 RADIUS 会话超时启用重新进行身份验证：

**authentication timer reauthenticate server**

**authentication event fail action next-method**

配置服务器故障情况下的关键身份验证 VLAN 方法：

**authentication event server dead action reinitialize vlan <VLAN\_number>**

**authentication event server alive action reinitialize**

配置 802.1X 和 MAB 的 IOS Flex-Auth 身份验证：

**authentication order dot1x mab**

**authentication priority dot1x mab**

**步骤 9** 在交换机端口上启用 802.1X 端口控制：

**authentication port-control auto**

**authentication violation restrict**

**步骤 10** 启用 MAC 身份验证绕行 (MAB)：

**mab**

**步骤 11** 在交换机端口上启用 802.1X：

**dot1x pae authenticator**

**步骤 12** 将重传时间设置为 10 秒：

**dot1x timeout tx-period 10**

**注释** 应将 802.1X 传输超时时间设置为 10 秒。除非您了解影响，否则请勿更改此值。

**步骤 13** 启用 portfast 功能：

spanning-tree portfast

## 启用 EPM 日志记录

在交换机上设置标准日志记录功能，以支持对思科 ISE 功能进行可能的故障排除和记录：

```
epm logging
```

## 启用交换机以接收 SNMP 陷阱

确保交换机能够通过网段中的适当 VLAN，从思科 ISE 接收 SNMP 陷阱传输：

```
snmp-server community public RO
snmp-server trap-source <VLAN_number>
```

## 在交换机上启用 SNMP v3 查询以进行分析

使用以下命令来配置交换机，确保按预期执行 SNMP v3 轮询以支持思科 ISE 分析服务。在此之前，请在 **SNMP 设置 (SNMP Settings)** 窗口的思科 ISE GUI 中配置 SNMP 设置。此窗口的导航路径为：**管理 (Administration)** **网络资源 (Network Resources)** **网络设备 (Network Devices)** **添加 (Add)** | **编辑 (Edit)** **SNMP 设置 (SNMP Settings)**。

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>
snmp-server group <group> v3 priv
snmp-server group <group> v3 priv contextvlan-1
```



**注释** 必须为每个情景配置 `snmp-server group <group> v3 priv context vlan-1` 命令。`snmp show context` 命令会列出所有上下文信息。

如果 SNMP 请求超时并且不存在连接问题，则可以提高超时值。

## 启用 MAC 通知陷阱以使分析器进行收集

配置您的交换机以传送适当的 MAC 通知陷阱，这样思科 ISE 分析器功能就可以收集网络终端上的信息：

```
mac address-table notification change
mac address-table notification mac-move
snmp trap mac-notification change added
snmp trap mac-notification change removed
```

## 在交换机上配置 RADIUS 空闲超时

要在交换机上配置 RADIUS 空闲超时，请使用以下命令：

```
Switch(config-if)# authentication timer inactivity
```

其中 *inactivity* 是以秒为单位的非活动时间间隔，这个时间之后，客户端活动将被视为未授权。

在思科 ISE 中，可以为这类会话非活动计时器应用到的任何授权策略启用此选项。依次选择策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 授权 (Authorization) > 授权配置文件 (Authorization Profiles)。

## 用于 iOS 请求方调配的无线控制器配置

### 对于单 SSID

要支持基于 Apple iOS 的设备 (iPhone 或 iPad) 从一个 SSID 切换至同一无线接入点的另一个 SSID，请将无线控制器配置为启用 **FAST SSID change** 功能。此功能有助于确保基于 IOS 的设备能够在 SSID 之间快速切换。

### 对于双 SSID BYOD

必须启用快速 SSID 以支持双 SSID BYOD。启用快速 SSID 更改后，无线控制器允许客户端在 SSID 间更快速移动。启用快速 SSID 时，不会清除客户端条目，也不会强制执行延迟。有关在思科无线控制器上配置快速 SSID 的详细信息，请参阅 [《Cisco Wireless Controller 配置指南》](#)。

### 无线控制器配置示例

```
WLC (config)# FAST SSID change
```

当您尝试在某些基于 Apple iOS 的设备中连接无线网络时，您可以会看到以下错误信息：

```
Could not scan for Wireless Networks.
```

您可以忽略该错误消息，因为这不会影响设备的身份验证。

## Apple 设备的无线 LAN 控制器支持

Apple 设备包括 Apple Captive Network Assistant (CNA) 功能，此功能可检查强制网络（例如思科 ISE WebAuth 页面），但是会干扰支持访客和个人设备所需的门户重定向。

您可以通过在无线 LAN 控制器 (WLC) 上启用 **web-auth captive-bypass enable** 命令绕过此功能：

```
WLC > config network web-auth captive-bypass enable
```

```
Web-auth support for Captive-Bypass will be enabled.
```

```
You must reset system for this setting to take effect.
```

```
WLC > save config
Are you sure you want to save? (y/n) y
Configuration Saved!
WLC >
```

## 在无线控制器上配置 ACL 以实现 MDM 互操作性

在无线控制器上配置 ACL 以用于授权策略，从而重定向未注册的设备证书调配。ACL 必须采用以下顺序。

- 
- 步骤 1 允许所有从服务器到客户端的出站流量。
  - 步骤 2 （可选）允许从客户端到服务器的 ICMP 入站流量以进行故障排除。
  - 步骤 3 允许未注册和不合规设备访问 MDM 服务器，以下载 MDM 代理和执行合规检查。
  - 步骤 4 允许从客户端到服务器再到 ISE 的所有入站流量以执行 Web 门户和请求方以及证书调配流程。
  - 步骤 5 允许从客户端到服务器的入站域名系统 (DNS) 流量以进行名称解析。
  - 步骤 6 允许从客户端到服务器的入站 DHCP 流量以获取 IP 地址。
  - 步骤 7 拒绝所有从客户端到服务器再到企业资源的入站流量，以重定向至思科 ISE（根据公司策略）。
  - 步骤 8 （可选）允许其余流量。
- 

### 示例

以下示例显示的 ACL 用于将未注册的设备重定向至 BYOD 流程。在本例中，思科 ISE IP 地址为 10.35.50.165，内部企业网络 IP 地址为 192.168.0.0 和 172.16.0.0（重定向），MDM 服务器子网为 204.8.168.0。

图 40: 用于重定向未注册设备的 ACL

General										
Access List Name		NSP-ACL								
Deny Counters		0								
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720	<input type="checkbox"/>
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227	<input type="checkbox"/>
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626	<input type="checkbox"/>
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505	<input type="checkbox"/>
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864	<input type="checkbox"/>
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0	<input type="checkbox"/>
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0	<input type="checkbox"/>
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4	<input type="checkbox"/>
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457	<input type="checkbox"/>
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256	<input type="checkbox"/>
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310	<input type="checkbox"/>
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0	<input type="checkbox"/>
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819	<input type="checkbox"/>





## 第 17 章

# 故障排除

- [思科 ISE 中的监控和故障排除服务，第 785 页](#)
- [网络处理状态，第 787 页](#)
- [网络身份验证，第 787 页](#)
- [Smart Call Home，第 788 页](#)
- [日志收集，第 789 页](#)
- [RADIUS 实时日志，第 790 页](#)
- [实时身份验证，第 792 页](#)
- [RADIUS 实时会话，第 794 页](#)
- [导出摘要，第 796 页](#)
- [身份验证摘要报告，第 798 页](#)
- [故障排除诊断工具，第 798 页](#)
- [用于验证传入流量的 TCP Dump 实用工具，第 801 页](#)
- [获取其他故障排除信息，第 804 页](#)

## 思科 ISE 中的监控和故障排除服务

监控和故障排除 (MnT) 服务是所有思科 ISE 运行时服务的综合身份解决方案，并使用以下组件：

- **监控：**实时呈现代表网络上的访问活动状态的有意义数据。通过查看展示，您可以轻松地解释并监控操作条件。
- **故障排除：**提供用来解决网络上的访问问题的上下文指导。然后，您可以解决用户的问题并及时提供解决方案。
- **报告：**提供标准报告的目录，这些报告可用于分析趋势和监控系统性能以及网络活动。您可以使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。

## 网络权限框架

控制面板显示网络权限框架 (NPF) 上的活动并提供关于各个组件的详细信息。

NPF 由下表所述的三个层级组成：

表 157: NPF 层级

层	规范
1	使用 802.1x、MAC 身份验证绕行 (MAB)、思科 ISE 分析器服务，根据身份进行访问控制
2	利用 802.1x、MAB、分析器、对网络准入控制 (NAC) 管理器的访客调配、集中式 Web 身份验证，根据身份进行访问控制
3	利用 802.1x、MAB、分析器、对 NAC 管理器的访客调配、集中式 Web 身份验证，根据身份和安全评估进行访问控制

NPF 身份验证和授权生成事件流。然后，思科 ISE 监控和故障排除工具会收集不同来源的事件并进行汇总。您可以在控制面板上查看身份验证和授权结果，或选择运行任意数量的报告。

## 网络权限框架事件流程

网络权限框架 (NPF) 身份验证和授权事件流程使用下表列出的过程：

流程阶段	说明
1	网络访问设备 (NAD) 执行正常授权或 Flex 授权。
2	使用 Web 授权分析无代理的未知身份。
3	RADIUS 服务器进行身份验证和授权。
4	在端口配置身份的授权。
5	丢弃未经授权的终端通信。

## 用于监控和故障排除功能的用户角色和权限

监控和故障排除功能与默认用户角色相关联。允许您执行的任务与分配给您的用户角色直接相关。

有关为每个用户角色设置的权限和限制的信息，请参阅[思科 ISE 管理员组](#)，第 10 页。



**注释** 不支持在没有思科 TAC 监管的情况下使用根 shell 访问思科 ISE，并且思科不对由此导致的任何服务中断负责。

## 监控数据库中存储的数据

思科 ISE 监控服务会收集数据并将所收集的数据存储于专用监控数据库中。根据用于监控网络功能的数据速率和数据量，可能需要将某个节点专用于监控。如果思科 ISE 网络以高速率从策略服务节点或网络设备收集日志数据，则我们建议将某个思科 ISE 节点专用于监控。

要管理监控数据库中存储的信息，需要对数据库执行完整备份和增量备份。这包括清除不需要的数据，然后还原数据库。

## 网络处理状态

您可以使用 **System Summary dashlet** 从思科 ISE 控制面板查看网络的处理状态。例如，当应用服务器或数据库等进程失败时，会生成警报，您可以使用 **System Summary dashlet** 查看结果。

系统状态图标的颜色指示系统的运行状况。

- 绿色 = 正常
- 黄色 = 警告
- 红色 = 严重问题
- 灰色 = 无信息

## 监控网络处理状态

**步骤 1** 转至思科 ISE **Dashboard**。

**步骤 2** 展开 **System Summary dashlet**。系统将显示详细的实时报告。

**步骤 3** 查看网络上正在运行的进程的以下信息：

- 进程的名称
- CPU 和内存使用情况
- 进程开始运行的时间

## 网络身份验证

您可以从 **Authentications** 面板中查看成功和失败的网络身份验证。此面板会提供有关用户或设备类型、位置和用户或设备所属身份组的数据。面板顶部的迷你图显示过去 24 小时和过去 60 分钟的分布。

## 监控网络身份验证

**步骤 1** 转至思科 ISE Dashboard。

**步骤 2** 展开身份验证 (Authentications) Dashlet。

系统将显示详细的实时报告。

**步骤 3** 查看网络上经过身份验证的用户或设备的信息。

**步骤 4** 展开数据类别，了解更多信息。

## Smart Call Home

Smart Call Home (SCH) 监控您的网络中的思科设备，并将关键事件通过电子邮件方式通知您。电子邮件包含实时告警，其中提供环境信息和补救建议。

如果您从思科 ISE 激活智能许可，则默认情况下将启用 SCH 功能。否则，要启用 SCH，您必须为 SCH 服务注册思科 ISE。有关如何启用 SCH 功能的信息，请参阅[Smart Call Home 服务进行注册](#)，第 789 页。

在激活智能许可或注册 SCH 服务后，您可以选择执行以下操作之一：

- 仅启用匿名报告。SCH 的匿名报告功能只提供少量的有关您的网络中的思科 ISE 设备运行状况的信息。
- 启用 SCH 提供的完整功能集。

## Smart Call Home 配置文件

Smart Call Home 配置文件决定了您的设备所监控的事件类型。思科包括以下默认配置文件：

- ciscotac-1 - 用于匿名报告
- isesch-1 - 用于 Smart Call Home 功能

您无法编辑用于 Anonymous Reporting 的默认配置文件 (ciscotac-1)。

## Anonymous Reporting

思科可以安全地收集有关部署、网络接入设备、分析器和正在使用的其他服务的非敏感信息。收集此数据有助于更好地了解思科的使用情况，并改进该产品以及它提供的各种服务。

默认情况下，会启用匿名报告。如果要禁用匿名报告，可以通过 管理员门户（管理 (Administration) > 系统 (System) > 设置 (Settings) > Smart Call Home）来禁用。

## 为 Smart Call Home 服务进行注册



**注释** 如果已从思科 ISE 激活智能许可，则无需注册 Smart Call Home (SCH) 服务。使用智能许可，默认情况下启用 SCH 功能。Smart Call Home 页面中的注册状态为活动。您可以选择仅启用匿名报告或启用 SCH 提供的完整功能集。

要在没有智能许可的情况下启用 SCH 服务，您必须先注册用于 SCH 服务的思科 ISE。您只能从独立节点或主要管理节点执行此操作。

**步骤 1** 选择管理 (Administration) > 系统 (System) > 设置 (Settings) > Smart Call Home。

**步骤 2** 选择以下其中一个选项：

- 打开全部 SCH 功能
- 保留默认 SCH 遥测设置并只发送匿名数据
- 禁用一切

**步骤 3** （仅当您选择打开全部 SCH 功能 [Turn on full SCH Capability] 选项时）在注册状态 (Registration Status) 区域输入您的邮箱地址。

**步骤 4** 点击保存 (Save)。

如果已选择打开全部 SCH 功能，您将收到一封包含激活链接的邮件。点击激活链接并按照提供的说明完成注册。

## 日志收集

监控服务收集日志和配置数据，存储数据，然后处理数据，以生成报告和警报。您可以查看从部署中的任何服务器收集的日志详情。

## 警报系统日志收集位置

如果将监控功能配置为将警报通知作为系统日志消息发送，您需要提供一个接收通知的系统日志目标。警报系统目标即发送警报系统日志消息的目标位置。



**注释** 思科 ISE 监控要求日志记录源接口配置使用网络接入服务器 (NAS) IP 地址。您必须为思科 ISE 监控配置交换机。

您还必须有一个配置为系统日志服务器的系统，才能接受系统日志消息。您可以创建、编辑和删除警报系统日志目标。

要将远程日志记录目标配置为警报目标，请执行此程序。

步骤 1 选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 远程日志记录目标 (Remote Logging Targets)。

步骤 2 点击添加 (Add)。

步骤 3 在新建日志记录目标 (New Logging Target) 窗口中，提交日志记录目标所需的详细信息，并选中包括此目标的警报 (Include Alarms for this Target) 复选框。

## RADIUS 实时日志

下表介绍“实时日志” (Live logs) 窗口中的字段，其中显示最近的 RADIUS 身份验证。此页面的访问路径为：操作 (Operations) > RADIUS > 实时日志 (Live Logs)。请注意，只能在主 PAN 中查看 RADIUS 实时日志。

表 158: RADIUS 实时日志

字段名称	Description
时间	显示监控和故障排除收集代理接收日志的时间。此列为必选项，无法取消选择。
状态	显示身份验证成功还是失败。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。
详细信息	<p>单击详细信息 (Details) 列下的图标可在新浏览器窗口中打开身份验证详细报告 (Authentication Detail Report)。此报告提供有关身份验证和相关属性以及身份验证流程的信息。</p> <p>如果已为该会话处理审计事件，则单击详细信息 (Details) 列下的图标可打开审计详细信息 (Accounting Detail) 报告。如果会话处于已验证状态，当您单击详细信息 (Details) 列下的图标时，会显示身份验证详细信息 (Authentication Detail) 报告。</p> <p>身份验证详细信息 (Authentication Detail) 报告中的响应时间 (Response Time) 是思科 ISE 处理身份验证流程所需的总时间。例如，如果身份验证包含三个往返消息，初始消息花费 300 毫秒，下一条消息花费 150 毫秒，最后一条消息花费 100 毫秒，则响应时间为 <math>300 + 150 + 100 = 550</math> 毫秒。</p> <p>注释 您无法查看活动时间超过 48 小时的终端的详细信息。当单击活动时间超过 48 小时的终端的详细信息 (Details) 图标时，您会看到一个包含以下消息的窗口：此记录无可用数据。(No Data available for this record.) 数据可能已清除或此会话记录的身份验证发生在一周之前。(Either the data is purged or authentication for this session record happened a week ago.) 或者，如果这是“PassiveID”或“PassiveID 可视性” (PassiveID Visibility) 会话，则不会有 ISE 身份验证详细信息，只有会话。(Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.)</p>

字段名称	Description
<b>重复次数 (Repeat Count)</b>	显示过去 24 小时内身份验证请求的重复次数，它们在身份、网络设备和授权方面没有任何变化。
<b>Identity</b>	显示与身份验证关联的已登录用户名。
<b>终端 ID (Endpoint ID)</b>	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
<b>终端配置文件</b>	显示所分析的终端的类型，例如分析为 iPhone、Android、MacBook、Xbox 等。
<b>身份验证策略 (Authentication Policy)</b>	显示为特定身份验证选择的策略的名称。
<b>授权策略</b>	显示为特定授权选择的策略的名称。
<b>授权配置文件 (Authorization Profiles)</b>	显示用于身份验证的授权配置文件。
<b>IP 地址</b>	显示终端设备的 IP 地址。
<b>Network Device</b>	显示网络访问设备的 IP 地址。
<b>Device Port</b>	显示终端连接的端口号。
<b>Identity Group</b>	显示分配给生成了日志的用户或终端的身份组。
<b>终端安全评估状态 (Posture Status)</b>	显示安全评估验证的状态和身份验证的详细信息。
<b>服务器</b>	指明从其生成日志的策略服务。
<b>MDM 服务器名称 (MDM Server Name)</b>	显示 MDM 服务器的名称。
<b>事件</b>	显示事件状态。
<b>Failure Reason</b>	如果身份验证失败，显示失败的详细原因。
<b>身份验证方法 (Auth Method)</b>	显示 RADIUS 协议（例如 Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)、IEEE 802.1x 或 dot1X 等）使用的身份验证方法。
<b>身份验证协议</b>	显示所使用的身份验证协议，例如受保护的可扩展身份验证协议 (PEAP) 和可扩展身份验证协议 (EAP) 等等。
<b>Security Group</b>	显示由身份验证日志标识的组。
<b>Session ID</b>	显示会话 ID。



---

**注释** 在 **RADIUS 实时日志 (RADIUS Live Logs)** 和 **TACACS+ 实时日志 (TACACS+ Live Logs)** 窗口中，系统会为每个策略授权规则的第一个属性显示一个“已查询 PIP” (Queried PIP) 条目。如果授权规则中的所有属性都与已为之前的规则查询的字典相关，则不会显示其他“已查询 PIP” (Queried PIP) 条目。

---

您可以在 **RADIUS 实时日志 (Live Logs)** 窗口中执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。
- 对列值排序。



---

**注释** 所有用户自定义将存储为用户首选项。

---

## 实时身份验证

您可以在 **实时身份验证 (Live Authentications)** 窗口实时监控最近发生的 RADIUS 身份验证。此窗口显示最近 24 小时内发生的前 10 项 RADIUS 身份验证。此节说明 **实时身份验证 (Live Authentications)** 窗口的功能。

**实时身份验证 (Live Authentications)** 窗口显示与所发生的身份验证事件对应的实时身份验证条目。除了身份验证条目之外，此窗口还显示与这些事件对应的实时会话条目。您还可以向下钻取会话，查看与该会话对应的详细报告。

此 **实时身份验证 (Live Authentications)** 窗口提供一个按所发生时间排序的最近 RADIUS 身份验证的表格说明。**实时身份验证 (Live Authentications)** 窗口底部显示的最近更新会显示服务器日期、时间和时区。



---

**注释** 如果 Access-Request 数据包中的密码属性为空，则会触发错误消息，访问请求将失败。

---

一个终端成功通过身份验证时，**实时身份验证 (Live Authentications)** 窗口会显示两个条目——一个条目对应身份验证记录，另一个条目对应会话记录（从会话实时视图下拉）。随后，当设备进行其他身份验证成功时，与会话记录对应的重复次数计数器会递增其次数。在 **实时身份验证 (Live Authentications)** 窗口显示的重复次数计数器会显示所抑制的重复 RADIUS 身份验证成功消息的数量。



请参阅默认情况下显示的实时身份验证数据类别。“最近的 RADIUS 身份验证” (Recent RADIUS Authentications) 部分中说明了这些类别。

您可以选择查看所有列，也可以只显示所选择的数据列。在选择您想要显示的列之后，您可以保存您的选择。

## 监控实时身份验证

**步骤 1** 选择操作 (Operations) > 身份验证 (Authentications)。

**步骤 2** 从刷新 (Refresh) 下拉列表中，选择更改数据刷新率的间隔。

**步骤 3** 点击刷新 (Refresh) 图标手动更新数据。

**步骤 4** 从显示 (Show) 下拉列表中，选择一个选项以更改显示的记录数量。

**步骤 5** 从时间范围 (Within) 下拉列表中，选择一个选项以指定时间间隔。

**步骤 6** 点击添加或删除列 (Add or Remove Columns) 并从下拉列表中选择选项以更改所显示的列。

**步骤 7** 单击窗口底部的保存 (Save) 以保存您的修改。

**步骤 8** 点击显示实时会话 (Show Live Sessions) 以查看实时 RADIUS 会话。

您可以使用实时会话的动态授权更改 (CoA) 功能，使您可以动态控制活动的 RADIUS 会话。您可以向网络接入设备 (NAD) 发送重新身份验证或断开连接请求。

## 在“实时身份验证” (Live Authentications) 页面过滤数据

使用实时身份验证 (Live Authentications) 窗口中的过滤器，可以过滤出您需要的信息，快速排除网络身份验证问题。您可以在身份验证实时日志 (Live Logs) 窗口筛选记录，只查看那些您感兴趣的记录。身份验证日志包含许多详细信息，过滤特定用户或位置的身份验证信息有助于您快速扫描数据。您可以使用实时身份验证 (Live Authentications) 窗口中可用的若干运算符，根据搜索条件筛选记录。

- “abc”：包含“abc”
- “!abc”：不包含“abc”
- “{}”：为空
- “!{}”：不为空
- “abc\*”：以“abc”开头
- “\*abc”：以“abc”结束
- “\!”、“\\*”、“\{”、“\”：转义

通过 Escape 选项，您可以筛选包含特殊字符的文本（包括用作过滤器的特殊字符）。您必须将反斜线 (\) 放在特殊字符的前面。例如，如果您要查看身份为“Employee!”的用户的身份验证记录，请在身份过滤器 (Identity Filter) 文本框中输入“Employee\!”。在此例中，思科 ISE 考虑将感叹号 (!) 作为文字字符，而不是作为特殊字符。

此外，使用状态 (**Status**) 字段您可以筛选出仅成功的身份验证记录、失败的身份验证、实时会话，等等。绿色复选标记会筛选过去发生的所有成功身份验证。红色十字标记会筛选所有失败身份验证。蓝色 *i* 图标会筛选所有实时会话。您还可以选择查看这些选项的组合。

**步骤 1** 选择操作 (**Operations**) > 身份验证 (**Authentications**)。

**步骤 2** 根据显示实时身份验证 (**Show Live Authentications**) 窗口中的任意字段筛选数据。

您可以根据成功或失败身份验证，或实时会话筛选结果。

## RADIUS 实时会话

下表说明了 RADIUS 实时会话 (**Live Sessions**) 窗口中的字段，此窗口显示实时身份验证。此页面的导航路径为：操作 (**Operations**) > RADIUS > 实时会话 (**Live Sessions**)。您仅可在主 PAN 上查看 RADIUS 实时会话。

表 159: RADIUS 实时会话

字段名称	说明
启动时间 ( <b>Initiated</b> )	显示启动会话时的时间戳。
已更新 ( <b>Updated</b> )	显示会话上次由于更改而更新时的时间戳。
帐户会话时间 ( <b>Account Session Time</b> )	显示用户会话的时间跨度 (秒)。
会话状态 ( <b>Session Status</b> )	显示终端设备的当前状态。
CoA 操作 ( <b>Action</b> )	点击操作 ( <b>Actions</b> ) 图标可对活动 RADIUS 会话重新进行身份验证或断开活动 RADIUS 会话连接。
重复次数 (Repeat Count)	显示用户或终端重新进行身份验证的次数。
终端 ID ( <b>Endpoint ID</b> )	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
身份 ( <b>Identity</b> )	显示终端设备的用户名。
IP 地址 ( <b>IP Address</b> )	显示终端设备的 IP 地址。

字段名称	说明
审核会话 ID (Audit Session ID)	显示唯一会话标识符。
帐户会话 ID (Account Session ID)	显示网络设备提供的唯一 ID。
终端配置文件 (Endpoint Profile)	显示设备的终端配置文件。
安全评估状态 (Posture Status)	显示安全评估验证的状态和身份验证的详细信息。
安全组 (Security Group)	显示由身份验证日志标识的组。
服务器 (Server)	指示已从中生成日志的策略服务节点。
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 (PAP)、质询握手身份验证协议 (CHAP)、IEE 802.1x 或 dot1x 等等。
身份验证协议 (Authentication Protocol)	显示所使用的身份验证协议，例如受保护的可扩展身份验证协议 (PEAP) 和可扩展身份验证协议 (EAP) 等等。
身份验证策略 (Authentication Policy)	显示为特定身份验证选择的策略的名称。
授权策略 (Authorization Policy)	显示为特定授权选择的策略的名称。
授权配置文件 (Authorization Profiles)	显示用于身份验证的授权配置文件。
NAS IP 地址 (NAS IP Address)	显示网络设备的 IP 地址。
设备端口 (Device Port)	显示网络设备的连接端口。
PRA 操作 (PRA Action)	显示客户端在网络上成功通过合规性验证后，在客户端上采取的定期重评估操作。
ANC 状态 (ANC Status)	设备的自适应网络控制状态，如隔离 (Quarantine)、取消隔离 (Unquarantine) 或关闭 (Shutdown)。

字段名称	说明
<b>WLC 漫游 (WLC Roam)</b>	显示用于跟踪是否已在漫游期间从一个无线局域网控制器 (WLC) 传递到另一个 WLC 的终端的布尔值 (Y/N)。它的值为 <code>cisco-av-pair=nas-update=Y</code> 或 N。  注释 思科 ISE 依靠 WLC 中的 <code>nas-update=true</code> 属性识别会话是否处于漫游状态。当原始 WLC 在 <code>nas-update=true</code> 时发送记账停止属性时，不会在 ISE 中删除会话，以避免重新进行身份验证。如果漫游失败，ISE 将在会话处于非活动状态五天后清除该会话。
<b>接收的数据包 (Packets In)</b>	显示接收的数据包数量。
<b>发送的数据包 (Packets Out)</b>	显示发送的数据包数量。
<b>接收的字节 (Bytes In)</b>	显示接收的字节数。
<b>发送的字节 (Bytes Out)</b>	显示发送的字节数。
<b>会话源 (Session Source)</b>	显示终端通过 RADIUS 或是身份映射进行身份验证。
<b>用户域名 (User Domain Name)</b>	显示用户的注册 DNS 名称。
<b>主机域名 (Host Domain Name)</b>	显示主机的注册 DNS 名称。
<b>用户 NetBIOS 名称 (User NetBIOS Name)</b>	显示用户的 NetBIOS 名称。
<b>主机 NetBIOS 名称 (Host NetBIOS Name)</b>	显示主机的 NetBIOS 名称。

## 导出摘要

您可以查看过去 7 天内所有用户导出的报告的详细信息以及状态。导出摘要包括手动报告和已计划的报告。导出摘要 (**Export Summary**) 窗口每 2 分钟自动刷新一次。单击刷新图标可手动刷新导出摘要 (**Export Summary**) 窗口。

超级管理员可以取消正在进行 (**In-Progress**) 或处于排队 (**Queued**) 状态的导出进程。其他用户只能取消他们发起的导出进程。

默认情况下，在给定的时间点只能运行 3 次报告手动导出，其余触发的报告手动导出会排队。计划导出的报告没有此类限制。

下表列出导出摘要 (**Export Summary**) 窗口中的字段。此页面的导航路径为：**操作 (Operations) > 报告 (Reports) > 导出摘要 (Export Summary)**。

表 160: 导出摘要

字段名称	说明
报告已导出	显示报告的名称。
导出依据	显示发起导出进程的用户的角色。
已计划	显示报告导出是否为计划性导出。
触发于	显示在系统中触发导出进程的时间。
<b>Repository</b>	显示将存储导出数据的存储库的名称。
过滤器参数	显示导出报告时选择的过滤器参数。
状态	<p>显示导出的报告的状态。它可以是下列类型之一：</p> <ul style="list-style-type: none"> <li>• 已排队</li> <li>• 正在进行</li> <li>• 已完成</li> <li>• 正在取消</li> <li>• 已取消</li> <li>• 失败</li> <li>• 已跳过</li> </ul> <p><b>注释</b>      失败状态指示失败的原因。已跳过状态指示当主 MnT 节点关闭时，跳过了计划的报告导出。</p>

您可以在导出摘要 (**Export Summary**) 窗口中执行以下操作：

- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。

## 身份验证摘要报告

您可以根据与身份验证请求相关的属性，针对具体用户、设备或搜索条件对网络接入进行故障排除。您可以通过运行“身份验证摘要”(Authentication Summary) 报告实现此目标。



注释 您只能生成最近 30 天的“身份验证摘要”报告。

## 网络接入问题故障排除

**步骤 1** 选择操作 (Operations) > 报告 (Reports) > 身份验证摘要报告 (Authentication Summary Report)。

**步骤 2** 过滤报告以了解故障原因。

**步骤 3** 查看报告中身份验证失败原因 (Authentication by Failure Reasons) 部分的数据以对您的网络访问问题进行故障排除。

注释 由于身份验证摘要报告会收集和显示与失败或成功的身份验证对应的最新数据，所以报告内容会延迟几分钟后显示。

## 故障排除诊断工具

诊断工具可帮助您诊断思科 ISE 网络上的问题并进行故障排除，同时提供关于如何解决问题的详细说明。您可以使用这些工具对身份验证进行故障排除并评估您网络上包括 TrustSec 设备在内的任何网络设备的配置。

## RADIUS 身份验证故障排除工具

当身份验证结果不是预期结果时，可使用此工具搜索并选择 RADIUS 身份验证或与 RADIUS 身份验证相关的 Active Directory，以进行故障排除。如果希望通过身份验证但却未通过，或者希望用户或计算机具有特定级别的权限但用户或计算机没有这些权限，请使用此工具。

- 根据用户名、终端 ID、网络访问服务 (NAS) IP 地址和身份验证失败原因搜索 RADIUS 身份验证以排除故障时，思科 ISE 只显示系统（当前）日期的身份验证。
- 根据 NAS 端口搜索 RADIUS 身份验证以排除故障时，思科 ISE 显示自上个月初至当前日期的所有 NAS 端口值。



**注释** 根据 NAS IP 地址和终端 ID 字段搜索 RADIUS 身份验证时，先在操作数据库中执行搜索，然后在配置数据库中执行搜索。

## 对意外 RADIUS 身份验证结果进行故障排除

**步骤 1** 选择 **操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > > 常规工具 (General Tools) > RADIUS 身份验证故障排除 (RADIUS Authentication Troubleshooting)**。

**步骤 2** 根据需要在字段中指定搜索条件。

**步骤 3** 点击 **Search** 以显示与您的搜索条件匹配的 RADIUS 身份验证。

如果要搜索 Active Directory 相关的身份验证，但在部署中未配置 Active Directory 服务器，则系统将显示未配置 AD” (*AD not configured*) 消息。

**步骤 4** 从表格中选择 RADIUS 身份验证记录，并单击**故障排除 (Troubleshoot)**。

要对 Active Directory 相关的身份验证进行故障排除，请访问**管理 (Administration) > 身份管理 (Identity Management) > 外部身份源 (External Identity Sources) > Active Directory > AD 节点 (AD node)** 下的“诊断工具” (Diagnostics Tool)。

**步骤 5** 点击**需要用户输入 (User Input Required)**，根据需要修改字段，然后点击**提交 (Submit)**。

**步骤 6** 点击 **Done**。

**步骤 7** 故障排除完成后，点击 **Show Results Summary**。

**步骤 8** (可选) 若要查看诊断、为解决问题而采取的步骤以及故障排除摘要，请单击**完成 (Done)**。

## 执行网络设备命令诊断工具

执行网络设备命令诊断工具允许您在任何网络设备上运行 **show** 命令。

显示的结果与您应在控制台上看到的结果相同。通过此工具，您可以发现设备配置中的任何问题。

使用此工具可验证任何网络设备的配置，也可以使用此工具了解网络设备的配置方式。

要访问执行网络设备命令诊断工具，请选择以下导航路径之一：

1. 选择 **操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 执行网络设备命令 (Execute Network Device Command)**。选择 **工作中心 (Work Centers) > 解析器 (Profiler) > 故障排除 (Troubleshoot) > 执行网络设备命令 (Execute Network Device Command)**。
2. 在显示的 **执行网络设备命令** 窗口中，在相应字段中输入网络设备的 IP 地址和您想要运行的 **显示** 命令。
3. 点击**运行 (Run)**。

## 执行思科 IOS show 命令以检查配置

---

- 步骤 1 选择操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > 执行网络设备命令 (Execute Network Device Command)。
  - 步骤 2 在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 选择操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > 执行网络设备命令 (Execute Network Device Command)。
  - 步骤 3 在相应字段中输入信息。
  - 步骤 4 点击 **Run** 以在指定网络设备上执行此命令。
  - 步骤 5 点击需要用户输入 (User Input Required)，必要时修改字段。
  - 步骤 6 点击 **Submit** 以在网络设备上运行命令，然后查看输出。
- 

## 评估配置验证程序工具

可以使用此诊断工具评估网络设备的配置并确定配置问题（如果有）。**Expert Troubleshooter** 会将设备的配置与标准配置进行比较。

## 解决网络设备配置问题

---

- 步骤 1 选择 操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > 评估配置验证器 (Evaluate Configuration Validator)。
  - 步骤 2 在网络设备 IP (Network Device IP) 字段中输入您想要评估网络设备的 IP 地址。
  - 步骤 3 选中相应复选框，然后点击要与建议模板进行比较的配置选项旁边的单选按钮。
  - 步骤 4 点击 **Run**。
  - 步骤 5 点击需要用户输入 (User Input Required)，必要时修改字段。
  - 步骤 6 （可选）选中想要分析的接口旁边的复选框，然后单击提交 (Submit)。
  - 步骤 7 （可选）单击显示结果摘要 (Show Results Summary) 以查看配置评估的详细信息。
- 

## 排除终端安全评估故障

---

- 步骤 1 选择操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > 终端安全评估故障排除 (Posture Troubleshooting)。
- 步骤 2 在相应字段中输入信息。
- 步骤 3 点击 **Search**。



步骤 4 要查找说明和确定事件的解决方法，请在列表中选择事件，点击 **Troubleshoot**。

## 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。



**注意** 如果启动 TCP Dump，系统会自动删除之前的转储文件。要保存之前的转储文件，请执行“保存 TCP Dump 文件”一节描述的任务，再开始新的 TCP Dump 会话。

## 使用 TCP Dump 监控网络流量

### 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 选择操作 (**Operations**) > 故障排除 (**Troubleshoot**) > 诊断工具 (**Diagnostic Tools**) > 常规工具 (**General Tools**) > **TCP 转储 (TCP Dump)**。

步骤 2 在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择操作 (**Operations**) > 故障排除 (**Troubleshoot**) > 诊断工具 (**Diagnostic Tools**) > 常规工具 (**General Tools**) > **TCP 转储 (TCP Dump)**。

步骤 3 从主机名称 (**Host Name**) 下拉列表中选择 TCP Dump 实用工具的源。不支持 Inline Posture 节点。

步骤 4 从**网络接口 (Network Interface)** 下拉列表中选择要监控的接口。

步骤 5 点击混合模式 (**Promiscuous Mode**) 切换按钮以设置为“On” (开) 或“关” (Off)。默认值为 On。

混合模式为默认数据包嗅探模式，在此模式下，网络接口将所有流量都传输到系统的 CPU。建议将该选项保留为“开” (On)。

步骤 6 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 7 点击开始 (Start)，开始监控网络。

步骤 8 收集足够数据后，点击停止 (Stop)，或者等进程在累计到最大数据包数量 500,000 后自动结束。



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 选择操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > TCP 转储 (TCP Dump)。

步骤 2 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 3 点击下载 (Download)，导航至所需位置，并点击保存 (Save)。

步骤 4 （可选）若要清除以前的转储文件而无需保存，请点击删除 (Delete)。

## 比较终端或用户的意外 SGACL

步骤 1 选择操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > TrustSec 工具 (TrustSec Tools) > 出口 (SGACL) 策略 (Egress [SGACL] Policy)。

步骤 2 在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > TrustSec 工具 (TrustSec Tools) > 出口 (SGACL) 策略 (Egress [SGACL] Policy)。

步骤 3 输入想要比较其 SGACL 策略的 TrustSec 设备的网络设备 IP 地址。

步骤 4 点击运行 (Run)。

步骤 5 单击需要用户输入 (User Input Required)，必要时修改字段。

步骤 6 点击 Submit。

步骤 7 点击 Show Results Summary，查看诊断和建议的解决步骤。

## 出口策略诊断流程

出口策略诊断工具会使用下表中介绍的流程：

流程阶段	说明
1	使用您所提供的 IP 地址连接设备，然后获取每个源和目标 SGT 对的访问控制列表 (ACL)。
2	检查并确保已在思科 ISE 中配置出口策略并为每个源和目标 SGT 对获取 ACL。
3	将从网络设备获取的 SGACL 策略与从思科 ISE 获取的 SGACL 策略进行比较。
4	如果存在不匹配情况，则显示源和目标 SGT 对。此外，作为额外的信息，系统会显示匹配的条目。

## 使用 SXP-IP 映射排除支持 TrustSec 的网络中的连接问题

**步骤 1** 选择操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > Trustsec 工具 (Trustsec Tools) > SXP-IP 映射 (SXP-IP Mappings)。

**步骤 2** 输入网络设备的 IP 地址。

**步骤 3** 点击选择。

**步骤 4** 单击运行 (Run)。

专业的故障排除人员从网络设备检索 TrustSec SXP 连接，并提示您再次选择 SXP 对等设备。

**步骤 5** 单击需要用户输入 (User Input Required)，然后在字段中输入必要信息。

**步骤 6** 选中您要用于对比 SXP 映射的 SXP 对等设备的复选框，然后输入通用连接参数。

**步骤 7** 点击 Submit。

**步骤 8** 点击 Show Results Summary 查看诊断和解决步骤。

## 通过 IP-SGT 映射解决支持 TrustSec 的网络中的连接问题

**步骤 1** 选择操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > Trustsec Tools (Trustsec 工具) > IP 用户 SGT (IP User SGT)。

**步骤 2** 根据需要在字段中输入信息。

**步骤 3** 点击 Run。

系统会提示您输入其他信息。

**步骤 4** 单击需要用户输入 (User Input Required)，必要时修改字段。

步骤 5 点击 **Submit**。

步骤 6 点击 **Show Results Summary** 查看诊断和解决步骤。

---

## 设备 SGT 工具

对于启用 TrustSec 解决方案的设备，每个网络设备都会通过 RADIUS 身份验证分配到一个 SGT 值。设备 SGT 诊断工具连接至网络设备（使用您提供的 IP 地址）并获取网络设备 SGT 值，然后检查 RADIUS 身份验证记录以确定最近分配的 SGT 值。最后，它会用表格格式显示设备-SGT 对，并确定 SGT 值为相同还是不同。

---

## 通过对比设备 SGT 映射排除启用 TrustSec 的网络中的连接故障

步骤 1 选择操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > Trustsec 工具 (Trustsec Tools) > 设备 SGT (Device SGT)。

步骤 2 根据需要在字段中输入信息。

Telnet 的默认端口号为 23，SSH 的默认端口号为 22。

步骤 3 点击 **Run**。

步骤 4 点击 **Show Results Summary** 查看设备 SGT 的比较结果。

---

## 获取其他故障排除信息

通过思科，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 调试日志，第 806 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*。



---

**注释** 对于内嵌式状态节点，您不能从管理员门户下载支持捆绑包。必须从思科 ISE CLI 使用 **backup-logs** 命令。

---

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 [下载思科日志文件](#)，第 805 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 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 日志文件，以查找更多信息。

### 开始之前

- 您必须具有超级管理员或系统管理员权限才能执行以下任务。
- 应已配置调试日志和调试日志级别。

---

**步骤 1** 选择 **操作 (Operations) > 故障排除 (Troubleshoot) > 下载日志 (Download Logs) > 设备节点列表 (Appliance Node List)**。

**步骤 2** 点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** 输入支持捆绑包的加密密钥，并重新输入加以确认。

**步骤 6** 点击 **创建支持捆绑包 (Create Support Bundle)**。

**步骤 7** 点击下载 (**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 调试日志

调试日志为各种思科 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。请参阅 [思科 组件和相应的调试日志](#)，第 807 页。

**步骤 2** [下载调试日志](#)。

---

## 思科 组件和相应的调试日志

表 161: 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
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
	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
ipsec-api	api-service.log

组件	调试日志
ipsec-ui	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
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

### 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** 选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)** > **设备节点列表 (Appliance Node List)**。

**步骤 2** 在“设备节点” (Appliance node) 列表中，点击您希望下载调试日志的节点。

**步骤 3** 点击调试日志 (**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** 点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
  - iseLocalStore.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
-



## 当地语言翻译版本说明

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