



思科身份服务引擎版本 1.4 版本说明

修订日期：2016 年 7 月 15 日

目录

这些版本说明介绍了思科身份服务引擎 (ISE) 版本 1.4 的功能、局限性和限制（警告）以及相关信息，是对产品硬件和软件版本附带的思科 ISE 文档的补充，涵盖以下主题：

- [简介（第 2 页）](#)
- [部署术语、节点类型和角色（第 2 页）](#)
- [系统要求（第 4 页）](#)
- [安装思科 ISE 软件（第 7 页）](#)
- [升级思科 ISE 软件（第 8 页）](#)
- [从 Cisco Secure ACS 迁移至思科 ISE（第 12 页）](#)
- [思科 ISE 许可证信息（第 12 页）](#)
- [CA 与思科 ISE 实现互通性的要求（第 12 页）](#)
- [思科 ISE 版本 1.4 的新增功能（第 13 页）](#)
- [思科 ISE 版本 1.4 的已知问题（第 15 页）](#)
- [思科 ISE 安装文件、更新和客户端资源（第 15 页）](#)
- [尚未解决和已解决的缺陷（第 18 页）](#)
- [文档更新（第 21 页）](#)
- [相关文档（第 22 页）](#)



简介

思科 ISE 平台是一款基于情景的下一代综合访问控制解决方案。它不仅提供经过身份验证的网络访问、分析、安全状态、自带设备 (BYOD) 自行激活服务 (原生请求方和证书调配)、访客管理和安全组访问服务，还在一个统一物理或虚拟设备上提供监控、报告和故障排除功能。思科 ISE 可以在两款具有不同性能特征的物理设备上提供，也可以作为软件在 VMware 服务器上运行。您可以向部署中添加更多设备，以增强性能、可扩展性和恢复能力。

思科 ISE 具有支持独立式和分布式部署的可扩展架构，该架构同时提供集中配置和管理。它还允许配置和管理不同角色和服务。通过这一功能，您可以根据网络中的具体需求创建并应用服务，但是仍然作为一个完整且协调的系统来运行思科 ISE 部署。

部署术语、节点类型和角色

思科 ISE 提供支持独立式和分布式部署的可扩展架构。

表 1 思科 ISE 部署术语

| 术语 | 说明 |
|------|---|
| 服务 | 角色提供的特定功能，例如网络访问、分析器、安全状态、安全组访问和监控。 |
| 节点 | 运行思科 ISE 软件的单个实例。思科 ISE 可作为设备提供，也可以作为软件在 VMware 服务器上运行。运行思科 ISE 软件的各个实例都叫作节点，不管这些实例是在思科 ISE 设备上还是在 VMware 服务器上运行。 |
| 角色 | 确定节点提供的服务。思科 ISE 节点可以承担以下任意或所有角色：管理、策略服务、监控和内联状态。 |
| 部署模式 | 决定您的部署是独立式、高可用性独立式（基本双节点部署）还是分布式部署。 |

节点类型和角色

思科 ISE 网络具有以下类型的节点：

- 可承担以下任意角色的思科 ISE 节点：
 - 管理 - 允许您为思科 ISE 执行所有管理操作。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，您可以有一个节点，或者最多两个运行管理角色且配置为一主一辅的节点。如果主要管理节点出现故障，您可以手动升级辅助管理节点，也可以为管理角色配置自动故障切换。
有关配置自动故障切换的更多信息，请参阅《[思科身份服务引擎版本 1.4 管理员指南](#)》中的“为主要管理节点配置自动故障切换”部分。
 - 策略服务 - 提供网络访问、安全状态、自带设备 (BYOD) 自行激活服务 (原生请求方和证书调配)、访客接入以及分析服务。此角色评估策略并作出所有决策。您可以让多个节点承担此角色。通常，在分布式部署中会有多个策略服务角色。驻留在负载均衡器后面的所有策略服务角色可以组合在一起，形成一个节点组。如果节点组中的一个节点发生故障，组中的其他节点会处理故障节点收到的请求，从而实现高可用性。



注 分布式设置中至少有一个节点应当承担策略服务角色。

- 监控 - 使思科 ISE 能够充当日志收集器，并存储网络中思科 ISE 节点上的所有管理和策略服务角色产生的日志消息。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将其收集的数据汇聚并关联，以提供有意义的报告。思科 ISE 最多允许存在一主一辅两个承担此角色的节点，以实现高可用性。主要和辅助监控角色均会收集日志消息。如果主要监控角色出现故障，辅助监控角色会自动承担起主要监控角色的职责。



注 在分布式设置中，至少应有一个节点承担监控角色。建议在独立的专用节点上配置监控角色，以便提高数据收集和报告的性能。

- pxGrid - 通过 Cisco pxGrid 方法，网络和安全设备可使用安全发布和订用机制与其他设备共享数据。这些服务适用于在 ISE 外部使用以及与 pxGrid 连接的应用。pxGrid 服务可在网络中共享情景信息，以便识别策略并共享公共策略对象。这有助于扩展策略管理。
- 内联状态节点是位于网络上的无线局域网控制器 (WLC) 和 VPN 集中器等网络接入设备后方的网守节点。内联状态节点在用户通过身份验证并获得访问权限后实施访问策略，还会处理 WLC 或 VPN 无法应对的授权变更 (CoA) 请求。思科 ISE 允许在一个部署中配置最多 10,000 个内联状态节点。您可以将两个内联状态节点配置为故障切换对，以实现高可用性。



注 内联状态节点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，内联状态节点无法承担任何角色。VMware 服务器系统不支持内联状态节点。



注

部署中的每个思科 ISE 节点都可以同时承担多个角色：管理、策略服务、监控或 pxGrid，而每个内联状态节点仅可作为专用网守角色运行。

表 2 分布式部署中的建议节点和角色数量

| 节点/角色 | 部署中的最小数量 | 部署中的最大数量 |
|--------|----------|--|
| 管理 | 1 | 2（配置为高可用性对） |
| 监控器 | 1 | 2（配置为高可用性对） |
| 策略服务 | 1 | <ul style="list-style-type: none"> • 2 - 当管理/监控/策略服务角色配置于相同的主要/辅助设备时 • 5 - 当管理和监控角色配置于相同的设备上时 • 40 - 当每个角色配置于专用设备上时 |
| pxGrid | 0 | 2（配置为高可用性对） |
| 内联状态 | 0 | 10000 个，以便每个部署支持尽可能多的网络接入设备 (NAD) |

您可以更改节点的角色。有关如何在思科 ISE 节点上配置角色的信息，请参阅《[思科身份服务引擎版本 1.4 管理员指南](#)》中的“在分布式环境中设置思科 ISE”一章。

系统要求

- 支持的硬件（第 4 页）
- 支持的虚拟环境（第 6 页）
- 支持的浏览器（第 6 页）
- 支持的硬件和代理（第 6 页）
- 支持的防病毒和反间谍软件产品（第 7 页）



注

有关思科 ISE 硬件平台和安装的更多信息，请参阅《[思科身份服务引擎版本 1.4 硬件安装指南](#)》。

支持的硬件

思科 ISE 软件与设备或安装映像文件一同提供。以下平台附带思科 ISE 版本 1.4。安装后，您可以为思科 ISE 配置指定的组件角色（管理、策略服务、监控以及 pxGrid），或者在表 3 所列平台中将其配置为内联状态节点。

表 3 支持的硬件和角色

| 硬件平台 | 角色 | 配置 |
|--|-----------------------------|--|
| Cisco SNS-3415-K9 (小型) | 任意 | <ul style="list-style-type: none"> • Cisco UCS¹ C220 M3 • 单插槽英特尔 E5-2609 2.4-GHz CPU，共 4 个内核，4 个线程 • 16-GB RAM • 1 个 600-GB 磁盘 • 嵌入式软件 RAID 0 • 4 GE 网络接口 |
| Cisco SNS-3495-K9 ² (大型) | 管理 策略服务 监控器 pxGrid | <ul style="list-style-type: none"> • Cisco UCS C220 M3 • 双插槽英特尔 E5-2609 2.4-GHz CPU，共 8 个内核，8 个线程 • 32-GB RAM • 2 个 600-GB 磁盘 • RAID 0+1 • 4 GE 网络接口 |
| 思科 ISE-3315-K9 (小型) ³ | 任意 | <ul style="list-style-type: none"> • 1 个至强 2.66-GHz 四核处理器 • 4 GB RAM • 2 个 250 GB SATA⁴ HDD⁵ • 4 个 1 GB NIC⁶ |

表3 支持的硬件和角色 (续)

| 硬件平台 | 角色 | 配置 |
|--------------------------|----------------------------------|--|
| 思科 ISE-3355-K9 (中型) | 任意 | <ul style="list-style-type: none"> • 1 个 Nehalem 2.0-GHz 四核处理器 • 4 GB RAM • 2 个 300 GB 2.5 英寸 SATA HDD • RAID⁷ (禁用) • 4 个 1 GB NIC • 冗余交流电源 |
| 思科 ISE-3395-K9 (大型) | 任意 | <ul style="list-style-type: none"> • 2 个 Nehalem 2.0-GHz 四核处理器 • 4 GB RAM • 4 个 300 GB 2.5 英寸 SAS II HDD • RAID 1 • 4 个 1 GB NIC • 冗余交流电源 |
| 思科 ISE-VM-K9 (VMware) | 独立式管理、监控、策略服务和 pxGrid 服务 (无内联状态) | <ul style="list-style-type: none"> • 有关 CPU 和内存建议, 请参阅《思科身份服务引擎版本 1.4 硬件安装指南》中的“关于确定 VMware 设备规格的建议”部分。⁸ • 有关硬盘大小的建议, 请参阅《思科身份服务引擎版本 1.4 硬件安装指南》中的“硬盘空间要求”部分。 • NIC - 需要 1 GB NIC 接口卡 (最多可安装 4 个 NIC)。 • 支持的 VMware 版本包括: <ul style="list-style-type: none"> - ESXi 5.x |

1. Cisco Unified Computing System (UCS)
2. 内联状态是 32 位系统, 不支持对称多处理 (SMP)。因此, 其不适用于 SNS-3495 平台。
3. 在思科 ISE 3315 中, 在启用内部 CA 时运行自带设备 (BYOD) 可能导致节点不同步。
4. SATA = 串行高级技术附件
5. HDD = 硬盘驱动器
6. NIC = 网络接口卡
7. RAID = 独立磁盘冗余阵列
8. 任何 VMware 设备配置均不支持分配小于 4GB 的内存。如果出现思科 ISE 行为问题, 请所有用户首先尝试分配至少 4GB 的内存, 然后再向思科技术支持中心提交支持请求。

如果您是从思科安全访问控制系统 (ACS) 或思科 NAC 设备迁移至思科 ISE, 请注意思科 NAC 3315 设备支持小型部署, 思科 NAC 3355 设备支持中型部署, 而思科 NAC 3395 设备支持大型部署。Cisco Secure ACS 34xx 以及思科 NAC 34xx 系列设备也支持思科 ISE。

支持的虚拟环境

思科 ISE 支持以下 VMware 服务器和客户端：

- 适用于 ESXi 5.x 的 VMware 版本 8（标配）
- 适用于 ESXi 6.0 的 VMware 版本 11（标配，需要安装思科 ISE 1.4 补丁 3）

支持的浏览器

思科 ISE 版本 1.4 的管理用户界面支持通过以下支持 HTTPS 的浏览器使用 Web 界面：

- Mozilla Firefox 版本 31.x ESR、36.x 和 37.x
- Microsoft Internet Explorer 10.x 和 11.x

运行客户端浏览器的系统必须安装 Adobe Flash Player 11.1.0.0 或更高版本。查看管理门户及实现更佳用户体验所需的最低屏幕分辨率为 1280 x 800 像素。

支持的硬件和代理

有关支持的设备、浏览器及代理的信息，请参阅 *思科身份服务引擎网络组件兼容性*。

思科 NAC 代理互通性

思科 NAC 代理版本 4.9.4.3 及更高版本可用于思科网络准入控制设备版本 4.9(1)、4.9(3)、4.9(4) 和思科 ISE 版本 1.1.3 补丁 11、1.1.4 补丁 11、1.2.0、1.2.1、1.3 以及 1.4。在用户需要在 ISE 和 NAC 部署之间漫游的环境中部署 NAC 代理时，建议使用上述型号。



注

思科 NAC 代理版本 4.9.5.8 和 Web 代理版本 4.9.5.4 支持 Windows 10。合规性模块版本 3.6.10120.2 支持 Windows 10。支持 Microsoft Internet Explorer 11。不支持适用于 Windows 10 的 Microsoft Edge 浏览器。思科网络准入控制设备和思科 NAC 代理软件已宣布终止销售 (EoS)/寿命终止 (EoL)。有关详细信息，请访问以下链接参阅 EoS/EoL 通知：
<http://www.cisco.com/c/en/us/products/security/nac-appliance-clean-access/eos-eol-notice-listing.html>

支持 Microsoft Active Directory

思科 ISE 版本 1.4 在所有功能级别均支持 Microsoft Active Directory 服务器 2003、2008、2008 R2、2012 以及 2012 R2。

思科 ISE 不支持 Microsoft Active Directory 版本 2000 或其功能级别。

此外，思科 ISE 1.4 支持与 Active Directory 基础设施的多林/多域集成，以在大型企业网中支持身份验证和属性集合。思科 ISE 1.4 支持最多 50 个域连接点。

支持的防病毒和反间谍软件产品

有关思科 NAC 代理及思科 NAC Web 代理支持的特定防病毒和反间谍软件产品的详细信息，请参阅以下链接：

<http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html>

思科 NAC Web 代理还具有静态合规性模块，这些模块在升级 Web 代理后方可升级。

下表列出的是 Web 代理版本和兼容的合规性模块版本。

表 4 Web 代理及合规性模块版本

| 思科 NAC Web 代理版本 | 合规性模块版本 |
|-----------------|------------|
| 4.9.5.3 | 3.6.9845.2 |
| 4.9.5.2 | 3.6.9186.2 |
| 4.9.4.3 | 3.6.8194.2 |
| 4.9.0.1007 | 3.5.5980.2 |
| 4.9.0.1005 | 3.5.5980.2 |

安装思科 ISE 软件

要在思科 SNS-3415 和 SNS-3495 硬件平台上安装思科 ISE 版本 1.4 软件，请启动新设备，并配置思科集成管理控制器 (CIMC)。随后，您即可使用 CIMC 或可引导 USB 通过网络安装思科 ISE 版本 1.4。



注

若使用虚拟机 (VM)，我们建议先使用 NTP 服务器正确设置访客 VM 的时间，然后在 VM 上安装 .ISO 映像。

根据《[思科身份服务引擎版本 1.4 硬件安装指南](#)》中的相关说明，对思科 ISE 进行初始配置。运行安装程序之前，请确保您已了解[表 5](#)中列出的配置参数。

表 5 思科 ISE 网络安装配置参数

| 提示 | 说明 | 示例 |
|--|---|---------------|
| Hostname | 不得超过 19 个字符。有效字符包括字母数字 (A-Z、a-z、0-9) 和连字符 (-)。第一个字符必须是字母。 | isebeta1 |
| (eth0) Ethernet interface address | 必须是千兆以太网 0 (eth0) 接口的有效 IPv4 地址。 | 10.12.13.14 |
| Netmask | 必须是有效的 IPv4 网络掩码。 | 255.255.255.0 |
| Default gateway | 必须是默认网关的有效 IPv4 地址。 | 10.12.13.1 |
| DNS domain name | 不能是 IP 地址。有效字符包括 ASCII 字符、任意数字、连字符 (-) 和句点 (.)。 | mycompany.com |
| Primary name server | 必须是主要域名服务器的有效 IPv4 地址。 | 10.15.20.25 |

表 5 思科 ISE 网络安装配置参数 (续)

| 提示 | 说明 | 示例 |
|------------------------------|--|--|
| Add/Edit another name server | 必须是其他域名服务器的有效 IPv4 地址。 | (可选) 允许您配置多个域名服务器。为此, 请输入 y 以继续。 |
| Primary NTP server | 必须是网络时间协议 (NTP) 服务器的有效 IPv4 地址或主机名。 | clock.nist.gov |
| Add/Edit another NTP server | 必须是有效的 NTP 域。 | (可选) 允许您配置多个 NTP 服务器。为此, 请输入 y 以继续。 |
| System Time Zone | <p>必须是有效时区。有关详细信息, 请参阅《思科身份服务引擎版本 1.4 CLI 参考指南》, 该指南中提供有思科 ISE 支持的时区列表。例如, 对于太平洋夏令时间 (PST), 系统时区为 PST8PDT (或协调世界时 [UTC] 减 8 小时)。</p> <p>参照的时区均为最常用的时区。您可以从思科 ISE CLI 运行 show timezones 命令, 获取受支持时区的完整列表。</p> <p>注 我们建议您将所有思科 ISE 节点都设置为 UTC 时区。此设置可确保来自部署中各种节点的报告、日志和安全状态代理日志文件始终与时间戳同步。</p> | UTC (默认值) |
| Username | 标识用于对思科 ISE 系统进行 CLI 访问的管理用户名。如果选择不使用默认值 (admin), 则必须创建新用户名。用户名的长度必须为三至八个字符, 并且由有效的字母数字字符 (A-Z、a-z 或 0-9) 组成。 | admin (默认值) |
| Password | 标识用于对思科 ISE 系统进行 CLI 访问的管理密码。您必须创建此密码 (无默认值)。密码长度必须至少为六个字符, 并且至少包含一个小写字母 (a-z)、一个大写字母 (A-Z) 和一个数字 (0-9)。 | MyIseYPass2 |



注

有关配置和管理思科 ISE 的更多信息, 请参阅[版本特定文档 \(第 22 页\)](#), 以查看思科 ISE 文档集中的其他文档。

升级思科 ISE 软件

思科身份服务引擎 (ISE) 仅支持从 CLI 升级。支持的升级路径包括:

- 思科 ISE 版本 1.2 补丁 14 或更高版本
- 思科 ISE 版本 1.2.1 补丁 5 或更高版本
- 思科 ISE 版本 1.3 或更高版本

下表列出的是思科 ISE 版本, 以及您需要执行什么操作才能从相应版本升级至思科 ISE 版本 1.4:

表 6 思科 ISE 1.4 升级路线图

| 思科 ISE 版本 | 升级路径 |
|-----------------------|---|
| 思科 ISE 版本 1.0 或 1.0.x | <ol style="list-style-type: none"> 1. 升级至思科 ISE 版本 1.1.0。 2. 应用最新的思科 ISE 版本 1.1.0 补丁。 3. 升级至思科 ISE 版本 1.2。 4. 升级至思科 ISE 版本 1.3。 5. 升级至思科 ISE 版本 1.4。 |
| 思科 ISE 版本 1.1 | <ol style="list-style-type: none"> 1. 应用最新的思科 ISE 版本 1.1.0 补丁。 2. 升级至思科 ISE 版本 1.2。 3. 升级至思科 ISE 版本 1.3。 4. 升级至思科 ISE 版本 1.4。 |
| 思科 ISE 版本 1.1.x | <ol style="list-style-type: none"> 1. 应用最新的思科 ISE 版本 1.1.x 补丁。 2. 升级至思科 ISE 版本 1.2。 3. 升级至思科 ISE 版本 1.3。 4. 升级至思科 ISE 版本 1.4。 |
| 思科 ISE 版本 1.2 | <ol style="list-style-type: none"> 1. 应用最新的思科 ISE 版本 1.2 补丁。 2. 升级至思科 ISE 版本 1.4。 |
| 思科 ISE 版本 1.2.1 | <ol style="list-style-type: none"> 1. 应用最新的思科 ISE 版本 1.2.1 补丁。 2. 升级至思科 ISE 版本 1.4。 |
| 思科 ISE 版本 1.3 | 升级至思科 ISE 版本 1.4。 |

遵循《[思科身份服务引擎版本 1.4 升级指南](#)》中的升级说明，将产品升级至思科 ISE 版本 1.4。



注

升级至思科 ISE 版本 1.4 后，您可能需要打开之前版本的思科 ISE 中未使用的网络端口。有关详细信息，请参阅[思科身份服务引擎硬件安装指南，版本 1.4](#)中的“思科 SNS-3400 系列设备端口参考”部分。

升级注意事项和要求

在升级至思科 ISE 版本 1.4 之前，请阅读以下部分：

- [ISE 控制面板中关于补丁安装的冲突警报（第 10 页）](#)
- [思科 ISE 1.4 中的 iPEP 支持（第 10 页）](#)
- [必须开放用于通信的防火墙端口（第 10 页）](#)
- [VMware 操作系统将更换为 RHEL 6（64 位）（第 10 页）](#)
- [管理员用户在升级后无法访问 ISE 登录页面（第 11 页）](#)
- [将思科 ISE 重新加入 Active Directory（第 11 页）](#)

- 发起人登录失败（第 11 页）
- 为新的访客类型更新授权策略（第 11 页）
- 对 UCS 和 IBM 设备的网络接口卡 (NIC) 进行排序（第 11 页）
- 其他已知升级注意事项和问题（第 11 页）

ISE 控制面板中关于补丁安装的冲突警报

在向若干辅助 PSN 节点应用补丁时，PSN 可能显示补丁应用失败，但随后很快又应用成功。PAN 应用补丁后，会将补丁传播给辅助节点。如果出现网络延迟或服务器问题，PAN 可能会认为 PSN 未成功应用补丁，并报告错误，即便 PSN 当时仍在应用补丁。若发生此现象，请再等待 15 分钟，然后再次检查“补丁管理” (Patch Management) 页面。

思科 ISE 1.4 中的 iPEP 支持

使用随版本 1.4 一同提供的思科 ISE 1.2.1 版 IPN，可将思科 ISE 版本 1.4 安装在 iPEP 节点上。

必须开放用于通信的防火墙端口

思科 ISE 版本 1.4 中的复制端口已发生变化。如果您在主要管理节点与任何其他节点之间部署了防火墙，则在升级至版本 1.4 之前必须开放以下端口：

- TCP 1521 - 用于主管理节点与监控节点之间的通信。
- TCP 443 - 用于主管理节点与所有其他辅助节点之间的通信。
- TCP 12001 - 用于全球群集复制。
- TCP 7800 和 7802 - （仅在节点组中包含策略服务节点时适用）用于 PSN 组群集。

有关思科 ISE 版本 1.4 使用的端口的完整列表，请参阅 [思科 SNS-3400 系列设备端口参考](#)。

VMware 操作系统将更换为 RHEL 6（64 位）

思科 ISE 版本 1.4 具有 64 位架构。若思科 ISE 节点在虚拟机上运行，请确保虚拟机的硬件与 64 位系统兼容：



注

在进行相应更改前，您必须关闭虚拟机，并在完成更改后再启动虚拟机。

确保选择 Linux 作为访客操作系统，而版本则应选择 Red Hat Enterprise Linux 6（64 位）。有关更多信息，请参阅 http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005870。

管理员用户在升级后无法访问 ISE 登录页面

如果在升级前为思科 ISE 的管理访问启用了基于证书的身份验证（管理 [Administration] > 管理员访问 [Admin Access]），并使用 Active Directory 作为您的身份源，则升级后您将无法启动 ISE 登录页面，这是因为升级期间会丢失与 Active Directory 的连接。

解决方法

从思科 ISE CLI 使用下列命令以安全模式启动 ISE 应用：

```
application start ise safe
```

该命令可在安全模式下启动思科 ISE 节点，并且您可以使用内部管理员用户凭证登录 ISE GUI。

登录后，您可以将 ISE 连接至 Active Directory。

将思科 ISE 重新加入 Active Directory

如果使用 Active Directory 作为外部身份源，请确保您拥有 Active Directory 凭证。升级后，可能会丢失 Active Directory 连接。如果发生此问题，您必须将思科 ISE 重新加入 Active Directory。重新加入后，请执行外部身份源调用流程以确保连接。

发起人登录失败

升级流程并不会迁移所有发起人组。在访客角色的创建中未使用的发起人组不会被迁移。由于此变更，升级到版本 1.4 后，部分发起人（内部数据库或 Active Directory 用户）可能无法登录。

请检查发起人组映射，查看哪些发起人无法登录发起人门户，然后将他们映射到适当的发起人组。

为新的访客类型更新授权策略

升级至思科 ISE 1.4 后，创建的新访客类型与升级后的授权策略不匹配。您需确保根据新的访客类型更新授权策略。

对 UCS 和 IBM 设备的网络接口卡 (NIC) 进行排序

网络接口卡 (NIC) 与思科 UCS SNS 3415 和思科 UCS SNS 3495 以及 IBM 思科 ISE 3315 设备连接的顺序可能会对升级到 ISE 1.4 有所影响。您应确保执行升级前的检查，然后再对 NIC 进行排序。对 UCS 和 IBM 设备的 NIC 进行升级前检查，确保 UCS 设备上的英特尔 NIC 使用端口 eth0 和 eth1，以及 IBM 设备上的 Broadcom NIC 使用端口 eth2 和 eth3。请参阅《[思科身份服务引擎版本 1.4 升级指南](#)》中的“对 UCS 和 IBM 设备的网络接口卡 (NIC) 进行排序”部分。

其他已知升级注意事项和问题

有关其他已知升级注意事项和问题，请参阅《[思科身份服务引擎版本 1.4 升级指南](#)》。

从 Cisco Secure ACS 迁移至思科 ISE

您仅可以从 Cisco Secure ACS 版本 5.5 和 5.6 迁移至思科 ISE 版本 1.4。在尝试迁移至思科 ISE 版本 1.4 之前，您必须将 Cisco Secure ACS 部署升级至版本 5.5 或 5.6。

思科 ISE 并不对 ACS 5.5/5.6 中可用的所有功能提供全奇偶校验，特别是策略。迁移后，您可能会发现现有数据类型和元素在新思科 ISE 环境中的显示方式有所不同。我们建议您使用迁移工具从 ACS 迁移特定对象（例如网络设备、内部用户和身份存储区定义）。迁移完成后，您可以手动定义适用于思科 ISE 的相关功能的策略。

有关从 Cisco Secure ACS 5.5/5.6 数据库迁移至思科 ISE 版本 1.4 的完整说明，请参阅《[思科身份服务引擎版本 1.4 迁移工具指南](#)》。

思科 ISE 许可证信息

思科 ISE 许可提供管理应用功能和访问权限的功能，例如，可以使用思科 ISE 网络资源的并发终端的数量。

许可证仅适用于无线及 VPN，或在 LAN 部署中仅适用于有线。许可证通过各种软件包提供，例如 Base、Plus、Plus AC、Apex、Apex AC、Mobility 以及 Mobility Upgrade。

所有思科 ISE 设备均附带一个 90 天的 Evaluation 许可证。要在 90 天的 Evaluation 许可证到期后继续使用思科 ISE 服务，并且要在网络上支持超过 100 个并发终端，必须根据系统上的并发用户数量获取和注册 Base 许可证。如果需要附加功能，则需要 Plus 和/或 Apex 许可证才能启用该功能。

有关思科 ISE 许可证类型以及如何获取许可证的信息，请参阅《[思科身份服务引擎版本 1.4 管理员指南](#)》中的“思科 ISE 许可证”部分。

思科 ISE 版本 1.4 支持带两个 UID 的许可证。您可以根据主要和辅助管理节点的 UID 获取许可证。有关思科 ISE 版本 1.4 许可证的更多信息，请参阅[思科身份服务引擎许可说明](#)。

CA 与思科 ISE 实现互通性的要求

配合思科 ISE 使用 CA 服务器时，请确保满足以下要求：

- 密钥大小应为 1024、2048 或更高。在 CA 服务器中，密钥大小使用证书模板定义。您可以使用请求方配置文件在思科 ISE 上定义密钥大小。
- 密钥使用应允许在扩展中应用签名和加密。
- 通过 SCEP 协议使用 GetCACapabilities 时，应支持加密算法和请求散列。建议使用 RSA + SHA1。
- 支持在线证书状态协议 (OCSP)。虽然这在自带设备 (BYOD) 中并不会直接使用，但是可以启用能充当 OCSP 服务器的 CA 来撤销证书。

思科 ISE 版本 1.4 的新增功能

思科 ISE 版本 1.4 提供以下功能和服务。有关更多信息，请参阅《[思科身份服务引擎版本 1.4 管理员指南](#)》。

- [访客](#) (第 13 页)
- [证书管理](#) (第 13 页)
- [分析器](#) (第 13 页)
- [将 SAMLv2 身份提供程序作为外部身份源](#) (第 14 页)
- [管理](#) (第 14 页)
- [MDM](#) (第 14 页)
- [FIPS](#) (第 14 页)
- [补丁](#) (第 14 页)
- [终端和 AnyConnect](#) (第 15 页)

访客

- 访客定期接受 AUP - 您可以创建授权规则，要求访客用户在经过特定小时数后接受 AUP，以让会话保持打开。
- 访客最大会话数 - 限制一名访客用户可打开的并发会话数，这可在“访客类型” (Guest Type) 中配置。
- SAML - 可使用 SAML 服务器对访客用户进行身份验证。
- 发起人门户 - 发起人现在可以在编辑现有访客用户帐户时更改访客类型。
- 访客类型 - 对访客类型的更改（自定义字段除外）现在将应用至现有访客帐户。

证书管理

这一版本的思科 ISE 提供以下与证书相关的增强功能：

- 您现在可以创建通用证书签名请求，并指定在稍后使用。您可以通过编辑证书，指定在绑定时使用或者稍后使用。
- 从管理员门户编辑通配符证书时，更改将被复制到部署中的所有节点上。
- 您现在可以从管理员门户删除不再需要的系统证书。
- 您现在可以将默认门户证书组标签重新分配至 CA 签名的证书。您还可以通过“系统证书” (System Certificates) 页面查看使用该标签的门户列表。

分析器

“分析器源” (Profiler Feed) 按钮 - “分析器源” (Profiler Feed) 页面已添加了一个测试按钮，用于测试与思科源服务器的连接。

将 SAMLv2 身份提供程序作为外部身份源

思科 ISE 支持以下门户的 SAML 单点登录 (SSO):

- 访客门户（发起人管理或自助注册）
- 发起人门户
- 我的设备门户

身份提供者存储并验证用户凭证，并生成 SAML 响应以允许用户访问门户。无需输入不同的用户名和密码组合，降低了密码管理难度。



注

在 ISE 1.4 中，只有 Oracle 访问管理器 (OAM) 和 Oracle 身份联合 (OIF) 支持 SAML SSO 功能。

管理

思科 ISE 支持管理角色的自动故障切换。要启用自动故障切换功能，分布式设置中至少有两个节点应承担管理角色，一个节点应承担非管理角色。如果主管理节点 (PAN) 关闭，则会启动辅助管理节点的自动升级。为此，系统将非管理辅助节点指定为每个管理节点的运行状况检查节点。运行状况检查节点按配置的时间间隔检查 PAN 的运行状况。如果收到的关于 PAN 运行状况的运行状况检查响应由于 PAN 关闭或无法访问而不理想，则运行状况检查节点会启动辅助管理节点升级，从而在等待已配置的阈值对应的时间后接管主角色。在辅助管理节点进行自动故障切换后，有些功能不可用。思科 ISE 不支持回退到原始 PAN。

MDM

- 思科 ISE 1.4 允许您在网络上运行多个活动 MDM 服务器，包括来自不同供应商的 MDM 服务器。您可以根据位置或设备类型等设备因素，将不同的终端路由到不同的 MDM 服务器。您可以为网络上的每个 MDM 服务器设置一个 MDM 门户。
- 思科 ISE 1.4 还支持通过 MDM 让设备通过 VPN 访问网络，但需要借助 AnyConnect 和思科 ASA 9.3.2 或更高版本。
- 思科 ISE 1.4 现在支持 Meraki 提供的 MDM 服务器。

FIPS

FIPS 模式支持 - 这一版本的思科 ISE 兼容 FIPS。思科身份服务引擎产品使用经过 FIPS 140-2 验证的嵌入式加密模块 - 思科通用加密模块（证书编号 1643 和 2100）。有关 FIPS 合规性要求的详细信息，请参阅 [FIPS 合规性证书](#)。

补丁

思科 ISE 支持状态补丁管理和补丁修复功能，以便您主动管理软件补丁。您可以使用 Opswat OESIS 库来检测和修复补丁管理应用，从而为 Windows OS 和 Mac OSX 添加补丁管理合规性检查和修复支持。您可以为供应商支持的各种产品选择安装、“启用” (Enabled) 和“最新” (Up to Date) 属性。通过状态补丁管理修复功能，您可以启用补丁管理软件、安装缺失补丁或在终端上激活补丁管理软件 GUI。补丁管理和补丁修复功能受众多供应商支持，包括 Microsoft Windows Server Update Services (WSUS)、System Management Server (SMS) 和 System Center Configuration Manager (SCCM) 服务器。

终端和 AnyConnect

SOURCEfire 的高级恶意软件防护 (AMP) 可在发生攻击事件之前、之中以及之后为终端软件提供全方位的保护。它可提供您所需的可视性与可控性，帮助阻止未被其他安全层发现的高级威胁。您应从 SOURCEfire 门户下载此软件，以便将 AMP Enabler 配置文件添加到思科 ISE 的客户端调配资源中。您必须下载两个映像，即，为 Windows OS 的终端软件下载 AMP 的可再分发版本，为 Mac OSX 的终端软件下载 AMP。已下载的软件托管在一台可从企业网络访问的服务器上。AnyConnect AMP Enabler 模块使用 URL 将文件下载到终端上。

思科 ISE 版本 1.4 的已知问题

[LDAP 导入的访客帐户无法从版本 1.2 升级（第 15 页）](#)

[LDAP 发起人创建的访客用户在从版本 1.2 升级后不可见（第 15 页）](#)

LDAP 导入的访客帐户无法从版本 1.2 升级

在升级到 1.3、1.4、2.0 或 2.1 期间，无法迁移由通过 LDAP 身份验证的发起人在版本 1.2 中导入的访客。

LDAP 发起人创建的访客用户在从版本 1.2 升级后不可见

从版本 1.2 升级到 1.3、1.4、2.0 或 2.1 时，由通过 LDAP 身份验证的发起人创建的访客仅对直接发起人可见。相同发起人组中的其他发起人将看不到这些访客。

思科 ISE 安装文件、更新和客户端资源

您可以使用以下三种资源下载文件，为思科 ISE 调配和提供策略服务：

- [从“下载软件” \(Download Software\) 中心获取思科 ISE 下载文件（第 15 页）](#)
- [思科 ISE 实时更新（第 16 页）](#)
- [思科 ISE 离线更新（第 17 页）](#)

从“下载软件” (Download Software) 中心获取思科 ISE 下载文件

除新装思科 ISE 所需的 .ISO 安装软件包之外（请参阅[安装思科 ISE 软件（第 7 页）](#)的说明），您还可以通过“下载软件” (Download Software) 网页获取其他思科 ISE 软件元素，例如 Windows 和 Mac OS X 代理安装程序以及 AV/AS 合规性模块。

下载的代理文件可用于在支持的终端中执行手动安装，也可通过第三方软件分发软件包进行大规模部署。

要访问思科“下载软件” (Download Software) 中心并下载必要的软件:

-
- 步骤 1** 转到“下载软件” (Download Software) 网页：
<http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm>。您可能需要提供登录凭证。
- 步骤 2** 依次转到产品 (Products) > 安全性 (Security) > 访问控制和策略 (Access Control and Policy) > 思科身份服务引擎 (Cisco Identity Services Engine) > 思科身份服务引擎软件 (Cisco Identity Services Engine Software)。
- 从以下思科 ISE 安装程序和可供下载的软件包中进行选择：
- 思科 ISE 安装程序 .ISO 映像
 - 适用于 Windows 和 Mac OS X 原生请求方的请求方调配向导
 - Windows 客户机代理安装文件（包括用于执行动手调配的 MST 和 MSI 版本）
 - Mac OS X 客户机代理安装文件
 - AnyConnect 代理安装文件
 - AV/AS 合规性模块
- 步骤 3** 点击下载(Download) 或加入购物车 (Add to Cart)。
-

思科 ISE 实时更新

通过思科 ISE 实时更新位置，您能够让系统自动下载请求方调配向导、适用于 Windows 和 Mac OS X 的思科 NAC 代理、AV/AS 支持（合规性模块）以及支持客户端调配和状态策略服务的代理安装程序包。您应于初次部署时在思科 ISE 中配置这些实时更新门户，以便直接从 Cisco.com 为思科 ISE 设备获取最新的客户端调配和状态软件。

前提条件：

如果无法访问默认的更新源 URL，且您的网络要求使用代理服务器，您可能需要在**管理 (Administration) > 系统 (System) > 设置 (Settings) > 代理 (Proxy)** 中配置代理设置，然后才能访问实时更新位置。如果启用了代理设置以便访问分析器和状态/客户端调配源，则与 MDM 服务器的连接可能被中断，因为思科 ISE 无法为 MDM 通信绕过代理服务。为解决此问题，您可以将代理服务配置为允许与 MDM 服务器通信。有关代理设置的更多信息，请参阅《[思科身份服务引擎版本 1.4 管理员指南](#)》中“管理思科 ISE”一章的“在思科 ISE 中指定代理设置”部分。

客户端调配和状态实时更新门户：

- 客户端调配门户 - <https://www.cisco.com/web/secure/pmbu/provisioning-update.xml>

此 URL 提供以下软件元素：

- 适用于 Windows 和 Mac OS X 原生请求方的请求方调配向导
- Windows 版最新思科 ISE 永久代理和临时代理
- Mac OS X 版最新思科 ISE 永久代理
- ActiveX 和 Java 小应用程序的安装程序帮助工具
- AV/AS 合规性模块文件

有关自动为思科 ISE 下载此门户提供的软件包的更多信息，请参阅《[思科身份服务引擎版本 1.4 管理员指南](#)》中“配置客户端调配”一章的“自动下载客户端调配资源”部分。

- 状态门户 - <https://www.cisco.com/web/secure/pmbu/posture-update.xml>

此 URL 提供以下软件元素：

- 思科预定义的检查 and 规则
- Windows 和 Mac OS X AV/AS 支持图表
- 思科 ISE 操作系统支持

有关自动为思科 ISE 下载此门户提供的软件包的更多信息，请参阅《[思科身份服务引擎版本 1.4 管理员指南](#)》中“配置客户端状态策略”一章的“自动下载状态更新”部分。

如果不启用上述自动下载功能，您可以选择离线下载更新。请参阅[思科 ISE 离线更新（第 17 页）](#)。

思科 ISE 离线更新

通过思科 ISE 离线更新，您可以手动下载请求方调配向导、代理、AV/AS 支持、合规性模块以及支持客户端调配和状态策略服务的代理安装程序包。通过这一选项，您可以在无法从思科 ISE 设备通过互联网直接访问 Cisco.com 或者安全性策略不允许通过互联网直接访问该网站时，上传客户端调配和状态更新。

离线更新不适用于分析器源服务。

要上传离线客户端调配资源，请完成以下步骤：

-
- 步骤 1** 转到“下载软件” (Download Software) 网页：
<http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm>。您可能需要提供登录凭证。
- 步骤 2** 依次转到产品 (Products) > 安全性 (Security) > 访问控制和策略 (Access Control and Policy) > 思科身份服务引擎 (Cisco Identity Services Engine) > 思科身份服务引擎软件 (Cisco Identity Services Engine Software)。
- 从以下可供下载的离线安装程序包中进行选择：
- **win_spw-[<版本>-isebundle.zip](#)** - 适用于 Windows 的离线 SPW 安装程序包
 - **mac-spw-[<版本>.zip](#)** - 适用于 Mac OS X 的离线 SPW 安装程序包
 - **compliancemodule-[<版本>-isebundle.zip](#)** - 离线合规性模块安装程序包
 - **macagent-[<版本>-isebundle.zip](#)** - 离线 Mac 代理安装程序包
 - **nacagent-[<版本>-isebundle.zip](#)** - 离线 NAC 代理安装程序包
 - **webagent-[<版本>-isebundle.zip](#)** - 离线 Web 代理安装程序包
- 步骤 3** 点击下载 (Download) 或加入购物车 (Add to Cart)。
-

有关向思科 ISE 添加已下载的安装程序包的更多信息，请参阅《[思科身份服务引擎版本 1.4 管理员指南](#)》中“配置客户端调配”一章的“从本地机器添加客户端调配资源”部分。

您可以使用状态更新，以离线方式通过本地系统上的存档为 Windows 和 Macintosh 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，您需要确保存档文件版本与配置文件中的版本一致。您可以在已配置思科 ISE 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。

要上传离线状态更新，请完成以下步骤：

- 步骤 1** 转至 <https://www.cisco.com/web/secure/pmbu/posture-offline.html>。
将 **posture-offline.zip** 文件保存到本地系统。此文件用于为 Windows 和 Macintosh 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 2** 访问思科 ISE 管理员用户界面，然后依次选择**管理 (Administration) > 系统 (System) > 设置 (Settings) > 状态 (Posture)**。
- 步骤 3** 点击箭头以查看状态设置。
- 步骤 4** 选择**更新 (Updates)**。系统将显示“状态更新” (Posture Updates) 页面。
- 步骤 5** 从“状态更新” (Posture Updates) 页面，选择**离线 (Offline)** 选项。
- 步骤 6** 从“待更新文件” (File to update) 字段，点击**浏览 (Browse)**，以从您的系统的本地文件夹中找到单个存档文件 (posture-offline.zip)。



注 “待更新文件” (File to update) 字段是必填字段。您仅可选择包含相应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 7** 点击**现在更新 (Update Now)** 按钮。
更新后，“状态更新” (Posture Updates) 页面的“更新信息” (Update Information) 下将显示当前思科更新版本的信息。

尚未解决和已解决的缺陷

可通过思科缺陷搜索工具查看这一版本中尚未解决和已解决的缺陷。通过这一基于 Web 的工具，您可以访问思科缺陷追踪系统，其中记录了关于此本产品和其他思科硬件及软件产品的缺陷和漏洞信息。



注 您必须拥有 Cisco.com 帐户才能登录并访问思科缺陷搜索工具。如果您还没有此帐户，请[注册一个帐户](#)。

有关思科缺陷搜索工具的更多信息，请参阅“缺陷搜索工具帮助和常见问题解答” (Bug Search Tool Help & FAQ)。

思科 ISE 版本 1.4.0.253 - 累积性补丁 7 中已解决的问题

表 7 中列出的是思科身份服务引擎版本 1.4.0.253 累积性补丁 7 中已解决的问题。要为思科 ISE 版本 1.4 获取必要的补丁文件以应用补丁，请登录思科“下载软件” (Download Software) 网站 (<http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm>) (您可能需要提供 Cisco.com 登录凭证)，依次转到**安全性 (Security) > 访问控制和策略 (Access Control and Policy) > 思科身份服务引擎 (Cisco Identity Services Engine) > 思科身份服务引擎软件 (Cisco Identity Services Engine Software)**，然后将一份补丁文件副本保存到本地计算机中。

补丁 7 可能不兼容较低版本的 SPW，用户需要升级 SPW。

然后参阅《思科身份服务引擎版本 1.4 管理员指南》中“管理思科 ISE”一章的“安装软件补丁”部分，了解如何为系统应用补丁。



注

该补丁不适用于使用 FIPS 模式的客户。

表 7 思科 ISE 补丁版本 1.4.0.253 补丁 7 的已解决警告

| 警告 | 说明 |
|----------------------------|--|
| CSCuy34700 | 更新 glibc 软件包以解决 CVE-2015-7547。 |
| CSCuy53020 | 在访客相关门户的首份 Appscan 报告中发现了 SQL 盲注攻击。 |
| CSCut77541 | 2015 年 4 月，NTPd 版本已针对 CVE ID CVE-2015-1798 和 CVE-2015-1799 更新至 4.2.6p5-3.el6.x86_64。 |
| CSCuy20317 | ISE 1.3/4 补丁 5 中发现“已达到分析器队列限制” (Profiler Queue limit reached) 错误。 |
| CSCux41407 | 对 OpenSSL 2015 年 12 月的漏洞进行状态评估。 |

思科 ISE 版本 1.4.0.253 - 累积性补丁 6 中已解决的问题

表 8 中列出的是思科身份服务引擎版本 1.4.0.253 累积性补丁 6 中已解决的问题。要为思科 ISE 版本 1.4 获取必要的补丁文件以应用补丁，请登录思科“下载软件” (Download Software) 网站 (<http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm>) (您可能需要提供 Cisco.com 登录凭证)，依次转到安全性 (Security) > 访问控制和策略 (Access Control and Policy) > 思科身份服务引擎 (Cisco Identity Services Engine) > 思科身份服务引擎软件 (Cisco Identity Services Engine Software)，然后将一份补丁文件副本保存到本地计算机中。

补丁 6 可能不兼容较低版本的 SPW，用户需要升级 SPW。

然后参阅《思科身份服务引擎版本 1.4 管理员指南》中“管理思科 ISE”一章的“安装软件补丁”部分，了解如何为系统应用补丁。

表 8 思科 ISE 补丁版本 1.4.0.253 补丁 6 的已解决警告

| 警告 | 说明 |
|----------------------------|--|
| CSCur40082 | 自助注册门户无法隐藏访问者及其用户名和密码。 |
| CSCus54412 | 当密码不符合密码策略时，ISE 1.3 不提示远程客户端。 |
| CSCus79596 | 网络接入：IdentityAccessRestricted 未能正确授权。 |
| CSCut56171 | 在发起人门户中添加的自定义字段无法删除。 |
| CSCut95631 | 新的发起人用户无法通过邮件获得访客凭证摘要。 |
| CSCuu11893 | ISE 1.3 中显示复制缓慢的警报。 |
| CSCuu12335 | ISE 1.3 补丁 2：无法为活动终端重置 InactiveDays 属性。 |
| CSCuu30079 | 在 AMP Enabler 配置文件中执行添加、编辑和复制操作时存在问题。 |
| CSCuu32547 | 发起人用户无法管理 ISE 1.3 中的所有帐户。 |
| CSCuu39225 | 偶发性身份验证故障 - 与域控制器的通信失败。 |
| CSCuu45021 | 在实时验证页面中点击 DACL 条目的身份验证详情时会发生 HTTP 500 错误。 |

表 8 思科 ISE 补丁版本 1.4.0.253 补丁 6 的已解决警告

| 警告 | 说明 |
|------------|--|
| CSCUu52655 | 在 NSP 配置文件中同时为 PEAP 和 TLS 指定 MAC OSX 时，MAC 自带设备 (BYOD) 流会发生问题。 |
| CSCUu85800 | 身份验证域 - 许多域缺失林。 |
| CSCUu92630 | ISE 1.2 在修改策略后 SGT 复制失败。 |
| CSCUv52944 | SWD-xxx LSQ-xxx ISE 无法发送停止记帐命令；这会影响 Lancope 用户。 |
| CSCUv53534 | 在分析器数据库中查找终端速度慢。 |
| CSCUv54014 | 非公共顶级域的 CRL/OCSP URL 验证失败。 |
| CSCUv71811 | ISE 1.3 身份验证延迟每小时均会增加。 |
| CSCUv88011 | 在 ISE 1.4 使用分析器源服务时，源服务更新会覆盖管理员创建的同名规则。 |
| CSCUv97343 | 创建新的访客帐户时，ISE 1.3 会缓存上一个发起人的邮件地址。 |
| CSCUw02111 | ISE 1.4 补丁 3：收到 ASA 发出的记帐停止命令后，会话不清除。 |
| CSCUw09138 | 在 ISE 1.3 补丁 3 中，在 PSN 上观察到较高的内存利用率。 |
| CSCUw15139 | ISE 报告发生错误：无法连接到操作数据库。 |
| CSCUw21758 | 对 MyDevices AUP 页面设置的更改无法生效。 |
| CSCUw29108 | ISE 1.3 访客门户访问的嵌入式状态检查和 Web 代理流失败。 |
| CSCUw31016 | “我的设备” (My Devices) 门户无法从访客流正确映射门户用户名称。 |
| CSCUw31568 | 当状态策略设置为 MAC 10.11 时，CP 策略失败。 |
| CSCUw32233 | ISE 1.3 补丁 4 中“显示实时会话” (Show Live Sessions) 页面为空白。 |
| CSCUw34448 | ISE 1.4 补丁 3：SMS 网关配置要求填写可选字段。 |
| CSCUw40899 | 在更改 SSID 后，ISE 1.4 终端身份组无法更新。 |
| CSCUw51376 | DHCP 属性无法在 PSN 所有权发生变更后获得确认。 |
| CSCUw74703 | 并发错误。无法在从 1.2.1 升级到 1.4 期间更新终端。 |
| CSCUw78737 | 即便执行了清除操作，GuestEndpoint 仍卡在 HotSpot AUP 门户循环中。 |
| CSCUw99899 | ISE 1.3 补丁 5：即便在收到记帐停止命令后，MNT 会话也未清空。 |
| CSCUx03119 | 已发起自带设备 (BYOD) 支持。 |
| CSCUx10424 | ISE 中的 Active Directory 黑名单未按预期频率刷新。 |
| CSCUx18771 | 在自助注册后，因为发生内部错误而无法成功使用其他用户登录。 |
| CSCUx24703 | 管理会话 ID 不应记录在系统日志审核记录中。 |
| CSCUx26799 | 从身份组中删除热点访客终端后，无法再次连接至热点。 |
| CSCUx53910 | 在 ISE 1.3 补丁 5 中增加系统内存会导致身份验证延迟。 |
| CSCUx91475 | 在 ISE 1.4 补丁 6 中执行手动更新后，无法更新源服务。 |

思科 ISE 版本 1.4.0.253 - 累积性补丁 5

思科 ISE 版本 1.4(0.253)- 累积性补丁 5 中已解决的问题

以下搜索中包含 ISE 1.4(0.905) 的所有已解决缺陷：

[1.4\(0.905\) 的已解决缺陷搜索](#)

以下搜索中包含 ISE 1.4(0.905) 中所有尚未解决的缺陷：

[1.4\(0.905\) 中尚未解决的缺陷搜索](#)

思科 ISE 版本 1.4.0.253 - 累积性补丁 3

新功能和已解决问题

思科 ISE 版本 1.4.0.253 累积性补丁 3 提供以下新功能：

- [支持 Windows 10 操作系统（第 21 页）](#)
- [支持 VMware ESXi 6.0（第 21 页）](#)

支持 Windows 10 操作系统

思科 ISE 版本 1.4.0.253 累积性补丁 3 支持运行 Windows 10 操作系统的客户机和个人设备。

支持 VMware ESXi 6.0

思科 ISE 版本 1.4.0.253 累积性补丁 3 支持 ESXi 6.0 的 VMware 版本 11（默认）。

思科 ISE 版本 1.4(0.253)- 累积性补丁 3 中已解决的问题

以下搜索中包含 ISE 1.4(0.903) 的所有已解决缺陷：

[1.4\(0.903\) 的已解决缺陷搜索](#)

以下搜索中包含 ISE 1.4(0.903) 中所有尚未解决的缺陷：

[1.4\(0.903\) 中尚未解决的缺陷搜索](#)

思科 ISE 版本 1.4

以下搜索中包含 ISE 1.4(0.253) 的所有已解决缺陷：

[1.4\(0.253\) 的已解决缺陷搜索](#)

以下搜索中包含思科 ISE 1.4(0.253) 中所有尚未解决的严重性为 3 或更高的缺陷：

[1.4\(0.253\) 中尚未解决的缺陷搜索](#)

文档更新

表 9 *更新至思科身份服务引擎版本 1.4 版本说明*

| 日期 | 说明 |
|----------------|-----------------|
| 2015 年 5 月 1 日 | 思科身份服务引擎，版本 1.4 |

相关文档

版本特定文档

思科 ISE 的一般产品信息位于 <http://www.cisco.com/go/ise>。最终用户文档位于 Cisco.com 上的 http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html。

表 10 思科身份服务引擎的产品文档

| 文档标题 | 位置 |
|---|---|
| 思科身份服务引擎版本 1.4 版本说明 | http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html |
| 思科身份服务引擎版本 1.4 管理指南 | http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html |
| 思科身份服务引擎版本 1.4 硬件安装指南 | http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html |
| 思科身份服务引擎版本 1.4 升级指南 | http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html |
| 思科身份服务引擎版本 1.4 迁移工具指南 | http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html |
| 思科身份服务引擎版本 1.4 发起人门户用户指南 | http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-user-guide-list.html |
| 思科身份服务引擎版本 1.4 CLI 参考指南 | http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-command-reference-list.html |
| 思科身份服务引擎版本 1.4 API 参考指南 | http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-command-reference-list.html |
| 思科 ISE 与 Active Directory 的集成 | http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html |
| 思科身份服务引擎 3300 系列设备、思科安全访问控制系统 1121 设备、思科网络准入控制设备、Cisco NAC Guest Server 以及思科 NAC 分析器的监管合规性和安全信息 | http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html |
| 思科 ISE 设备内文档和中国 RoHS 指针卡 | http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-documentation-roadmaps-list.html |

平台特定文档

其他平台特定文档的链接位于以下位置：

- 思科 ISE
<http://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html>
- 思科 UCS C 系列服务器
http://www.cisco.com/en/US/docs/unified_computing/ucs/overview/guide/UCS_rack_roadmap.html
- Cisco Secure ACS
<http://www.cisco.com/c/en/us/support/security/secure-access-control-system/tsd-products-support-series-home.html>
- 思科 NAC 设备
<http://www.cisco.com/c/en/us/support/security/nac-appliance-clean-access/tsd-products-support-series-home.html>
- 思科 NAC 分析器
<http://www.cisco.com/c/en/us/support/security/nac-profiler/tsd-products-support-series-home.html>
- 思科 NAC 访客服务器
<http://www.cisco.com/c/en/us/support/security/nac-guest-server/tsd-products-support-series-home.html>

获取文档和提交服务请求

关于如何获取文档、提交服务请求和收集详情，请参阅每月的 *思科产品文档更新*（其中还含有所有最新及修订的思科技术文档）。要查看文档，请前往：

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

通过 Really Simple Syndication (RSS) 源的方式订阅 *思科产品文档更新*，相关内容将通过阅读器应用程序直接发送至您的桌面。RSS 源是一项免费服务，思科目前支持 RSS 2.0 版本。

本文档需结合“[相关文档](#)”部分中列出的文档一起使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请转至此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

© 2015 年思科系统公司。保留所有权利。

