思科身份服务引擎版本 2.0 版本说明

修订日期：2016 年 8 月 22 日

目录

这些版本说明介绍了思科身份服务引擎 (ISE) 版本 2.0 的功能、限制和约束（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

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（本地请求方和证书调配）、访客管理和安全组访问服务，还在一个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。

思科 ISE 版本 2.0 中的新增功能

思科 ISE 版本 2.0 提供以下功能和服务。请参阅《*思科身份服务引擎版本 2.0 管理员指南*》，了解更多信息。

TACACS+ 设备管理

注意 思科 ISE 要求安装设备管理许可证，才能使用 TACACS+ 服务。设备管理许可证是一种永久许可证。如果您从较低版本升级至思科 ISE 版本 2.0，且希望启用 TACACS+ 服务，则您必须以单独的附加许可证的形式订购设备管理许可证。您需要一个设备管理许可证来完成整个 ISE 部署。

思科 ISE 支持设备管理，使用 TACACS+ 安全协议来控制和审核网络设备的配置。对网络设备进行适当配置，使其请求 ISE 对设备管理员的操作进行身份验证和授权，并发送记帐消息以便 ISE 记录这些操作。它有利于精细控制谁可以访问哪个网络设备，并更改相关的网络设置。ISE 管理员可创建策略集，从而可在设备管理访问服务的授权策略规则中选择 TACACS 结果（例如命令集和 shell 配置文件）。ISE 监控节点提供与设备管理相关的增强型报告。“设备管理工作中心”(Device Administration Work Center) 菜单包含所有设备管理页面，可用作 ISE 管理员的统一操作起点。

第三方设备支持

思科 ISE 通过使用网络设备配置文件来支持某些第三方网络访问设备 (NAD)。这些配置文件定义思科 ISE 用于支持访客、BYOD、MAB 和安全状态等流量的功能。

思科 ISE 包含适用于几家供应商的网络设备的预定义配置文件。我们已使用表 1 中列出的供应商设备对思科 ISE 2.0 进行了测试。

表 1　　在思科 ISE 2.0 测试中使用的供应商设备

		支持的/经过验证的使用案例				
	供应商	**802.1X/ MAB**	**无 CoA 的分析器**	**有 CoA 的分析器**	**安全状态**	**访客/ BYOD**
无线	Aruba 7000、InstantAP	✓	✓	✓	✓	✓
	Motorola RFS 4000	✓	✓	✓	✓	✓
	HP 830	✓	✓	✓	✓	✓
	Ruckus ZD 1200	✓	✓	✓	-	-
有线	HP 3800 (ProCurve)	✓	✓	✓	-	-
	Alcatel 6850	✓	✓	-	-	-
	Brocade ICX 6610	✓	✓	✓	-	-
对于其他第三方 NAD，您必须在思科 ISE 中确定设备属性和功能并创建自定义 NAD 配置文件。		✓	✓	需要 CoA 支持	需要 CoA 和 URL 重定向支持	需要 CoA 和 URL 重定向支持

您可以为没有预定义配置文件的其他第三方网络设备创建自定义 NAD 配置文件。对于访客、BYOD 和安全状态等流量，设备需要支持 RFC 5176“授权更改”(CoA)，以及可重定向至思科 ISE 门户的 URL 重定向机制。是否支持这些流量取决于 NAD 的功能。有关网络设备配置文件所需的很多属性的信息，可能需要参阅设备的管理指南。有关如何创建自定义 NAD 配置文件的信息，请参阅《*使用思科身份服务引擎创建的网络访问设备配置文件*》文档。

如果您在采用版本 2.0 之前已经部署非思科 NAD，并已创建使用这些 NAD 的策略规则/RADIUS 字典，则升级之后这些配置文件照常有效。

有关网络设备配置文件以及如何创建、导入和导出它们的更多信息，请参阅《*思科身份服务引擎管理指南*》中的“管理网络设备”一章。

TrustSec 控制面板

TrustSec 控制面板是 TrustSec 网络的一种集中式监控工具。“指标”(Metrics) 小面板显示有关 TrustSec 网络行为的统计信息。“活动 SGT 会话”(Active SGT Sessions) 小面板显示网络中当前活动的 SGT 会话。“警报”(Alarms) 小面板显示与 TrustSec 会话有关的警报。“快速查看”(Quick View) 小面板显示 NAD 和 SGT 的 TrustSec 相关信息。

点击“实时日志”(Live Log) 小面板中的“TrustSec 会话”(TrustSec Sessions) 链接可查看活动 TrustSec 会话。还可以查看有关 NAD 向思科 ISE 发送的 TrustSec 协议数据请求和响应的信息。

TrustSec 矩阵增强功能

您可以使用思科 ISE 创建、命名并保存自定义视图。要创建自定义视图，请选择**显示 (Display) > 创建自定义视图 (Create Custom View)**。您还可以更新视图标准或删除未使用的视图。

您可以使用“出口策略”(Egress Policy) 页面的“视图”(View) 下拉列表中的下列选项来更改矩阵视图：

- “使用 SGACL 名称压缩”(Condensed with SGACL names) - 如果选择此选项，则空白单元格隐藏，且 SGACL 名称显示在单元格中。
- “不使用 SGACL 名称压缩”(Condensed without SGACL names) - 空白单元格隐藏，且 SGACL 名称不显示在单元格中。如果您希望查看更多矩阵单元格并使用颜色、图案和图标（单元格状态）来区分单元格的内容，则此视图十分有用。
- “全屏且包含 SGACL 名称”(Full with SGACL names) - 如果选择此选项，则左侧和上部菜单隐藏，且 SGACL 名称显示在单元格中。
- “全屏且不包含 SGACL 名称”(Full without SGACL names) - 如果选择此选项，则矩阵以全屏模式显示，且 SGACL 名称不显示在单元格中。

您可以更改外观设置。以下选项可用：

- “自定义主题”(Custom theme) - 最初显示的是默认主题（有颜色但无图案）。您可以自己设置颜色和图案。
- “默认主题”(Default theme) - 预定义颜色列表但无图案（不可编辑）。
- “可访问性主题”(Accessibility theme) - 预定义颜色列表且有图案（不可编辑）。

要使矩阵更易于阅读，可根据矩阵单元格内容对单元格使用合适的颜色和图案。以下显示类型可用：

- “允许 IP/允许 IP 日志”(Permit IP/Permit IP Log) - 在单元格内配置
- “拒绝 IP/拒绝 IP 日志”(Deny IP/Deny IP Log) - 在单元格内配置
- SGACL - 适用于在单元格内配置的 SGACL
- “允许 IP/允许 IP 日志（继承）”(Permit IP/Permit IP Log (Inherited)) - 取自默认策略（适用于未配置的单元格）
- “拒绝 IP/拒绝 IP 日志（继承）”(Deny IP/Deny IP Log (Inherited)) - 取自默认策略（适用于未配置的单元格）
- “SGACL（继承）”(SGACL (Inherited)) - 取自默认策略（适用于未配置的单元格）

状态图标用于显示单元格的状态。

要配置 TrustSec 矩阵设置，请选择**工作中心 (Work Centers) > TrustSec > 设置 (Settings) > TrustSec 矩阵设置 (TrustSec Matrix Settings)**。

TrustSec 工作中心

所有 TrustSec 相关选项都整合在“TrustSec 工作中心”(TrustSec Work Center) 菜单之下（**工作中心 [Work Centers] > TrustSec**），因此管理员可在一个位置轻松访问所有 TrustSec 选项。

自动创建 SGT

您可以使用思科 ISE 自动创建 SGT，同时创建授权策略规则。自动创建的 SGT 基于规则属性进行命名。

启用此选项后，“授权策略”(Authorization Policy) 页面顶部将显示“自动安全组创建已开启”(Auto Security Group Creation is On) 消息。点击“权限”(Permissions) 字段中显示的加号 (+) 可编辑 SGT 名称和值。

默认情况下，在全新安装或升级之后此选项处于禁用状态。

对 SXP 的支持

安全组标记 (SGT) 交换协议 (SXP) 可用于跨无 TrustSec 硬件支持的网络设备传播 SGT。SXP 可用于将终端的 SGT 以及 IP 地址从一台 SGT 感知网络设备传输至另一台此类设备。

要在一个节点上启用 SXP 服务，请选中“通用节点设置”(General Node Settings) 页面中的“启用 SXP 服务”(Enable SXP Service) 复选框。您还必须指定用于 SXP 服务的接口。

在每个 SXP 连接中，一个对等体被指定为 SXP 扬声器，另一个对等体被指定为 SXP 监听器。也可将这些对等体配置为双向模式，其中每个对等体都可充当扬声器兼监听器。可从任一对等体发起连接，但是映射信息始终是从扬声器传播至监听器。

基于位置的授权

思科 ISE 与思科移动业务引擎 (MSE) 集成，以便引入基于物理位置的授权功能。思科 ISE 使用来自 MSE 的信息，根据 MSE 报告的用户实际位置来提供差异化的网络访问。

当一名用户处在合适的区域时，您可以借助此功能使用终端位置信息来提供网络访问。您也可以将终端位置作为额外属性添加至策略中，从而定义更加精细化的基于设备位置的策略授权集。在使用基于位置的属性的授权规则中，您可以配置一些条件，例如：

MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone

您可以使用 Cisco Prime 基础设施应用来定义位置层次结构（园区/楼宇/楼层结构）并配置安全和非安全区域。定义位置层次结构后，您必须将位置层次结构数据与 MSE 服务器同步。

使用从 MSE 实例检索的位置数据创建位置树。您可以使用位置树选择呈现给授权策略的位置条目。

对布尔属性的支持

思科 ISE 支持从 Active Directory 和 LDAP 身份库中检索布尔属性。您可以在配置 Active Directory 或 LDAP 的目录属性时配置布尔属性。在使用 Active Directory 或 LDAP 进行身份验证时检索这些属性。

布尔属性可用于配置策略规则的条件。

布尔属性值作为字符串类型从 Active Directory 或 LDAP 服务器获取。

如果您将布尔属性（例如 msTSAllowLogon）配置为字符串类型，那么在思科 ISE 中，Active Directory 或 LDAP 服务器中的布尔值属性将设置为字符串属性。您可以将属性类型更改为布尔型，或者手动将属性添加为布尔型。

对 EAP-TTLS 协议的支持

EAP-TTLS 是一种可扩展 EAP-TLS 协议功能的双阶段协议。第 1 阶段构建安全隧道，并生成在第 2 阶段使用的会话密钥，以便在服务器与客户端之间安全地建立属性和内部方法数据的隧道。

思科 ISE 可处理来自各种 TTLS 请求方的身份认证，包括：

- Windows 上的 AnyConnect 网络访问管理器 (NAM)
- Windows 8.1 本地请求方
- Secure W2（在 MultiOS 上也称为 JoinNow）
- MAC OS X 本地请求方
- IOS 本地请求方
- 基于 Android 的本地请求方
- Linux WPA 请求方

KVM 虚拟机监控程序支持

思科 ISE 支持 Red Hat Enterprise Linux (RHEL) 7.0 上的 KVM 虚拟机监控程序。

KVM 虚拟化需要主机处理器提供的虚拟化支持；包括 Intel 处理器的 Intel VT-x 和 AMD 处理器的 AMD-V。在主机上打开一个终端窗口，并输入 **cat /proc/cpuinfo** 命令。您会看到 vmx 或 svm 标志。

有关更多信息，请参阅《*思科身份服务引擎版本 2.0 硬件安装指南*》中的“*在 Linux KVM 上安装思科 ISE*”一章。

思科 ISE 遥感勘测

当您登录管理员门户之后，系统会立即显示思科 ISE 遥感勘测横幅。思科 ISE 安全地搜集与您的部署、网络访问设备、分析器以及您正在使用的其他服务有关的非敏感信息。收集的数据将用于在将来的版本中为您提供更好的服务和其他功能。

思科安全地收集遥感勘测信息，以便更好地了解思科 ISE 的使用情况，并改善本产品及其提供的各种服务。默认情况下，系统会启用遥感勘测功能。如果您不希望使用思科 ISE 遥感勘测功能，可从“ISE 管理员门户”(ISE Admin Portal) 禁用此功能（“管理”[Administration] > “系统”[System] > “设置”[Settings] > “遥测设置”[Telemetry Settings]）。

证书调配门户

员工可使用证书调配门户为无法通过自行激活流程的设备请求证书。例如，销售点终端等设备无法执行 BYOD 流程，需要手动发布证书。特权用户组可使用证书调配门户为此类设备上传证书请求、生成密钥对（如需要）和下载证书。员工可访问此门户，并请求单个证书或使用 CSV 文件提出批量证书请求。

证书模板扩展名

思科 ISE 内部 CA 包含一个表示用于创建终端证书的证书模板的扩展名。内部 CA 发布的所有终端证书都包含一个证书模板扩展名。您可以在授权策略条件中使用 CERTIFICATE: Template Name 属性，并根据评估结果分配合适的访问特权。

思科 ISE 内部 CA 向 ASA VPN 用户发布证书

内部 ISE CA 可向通过 ASA VPN 连接的客户端计算机发布证书。思科 ISE 使用简单证书注册协议 (SCEP) 进行注册，并向客户端计算机调配证书。

基于 GUI 的升级

思科 ISE 提供从管理员门户进行基于 GUI 的集中式升级。升级过程非常简单，且屏幕上会显示升级过程和节点状态。

注意 基于 GUI 的升级仅适用于从版本 2.0 升级至更高版本。

高级故障排除的技术支持隧道

思科 ISE 使用 Cisco IronPort Tunnel 基础设施来创建一个安全隧道，以便思科技术支持工程师可连接至您的部署环境中的 ISE 服务器，并对系统问题进行故障排除。思科 ISE 使用 SSH 在隧道中创建安全连接。作为管理员，您可以控制隧道访问。您可以选择授予支持工程师的访问时间和时长。如果没有您的干预，则思科客户支持无法建立隧道。您将收到有关服务登录的通知。您可以随时禁用隧道连接。

移动设备管理增强功能

在 ISE 网络外部的活动 MDM 服务器上注册的终端可使用思科 ISE 2.0 连接至 ISE 网络，而无需重新向 MDM 服务器注册。

当终端连接至 ISE 网络时，MDM 门户向 MDM 服务器请求该终端。如果服务器在返回结果中确认终端是合规的，则 ISE 发布一条授权更改通知，并允许终端访问网络。如果终端未向 MDM 服务器注册，则其必须执行注册流程。

对 Meraki 移动设备管理的支持

思科 ISE 支持 Meraki MDM 服务器。

pxGrid 增强功能

pxGrid 客户端可通过 ISE 2.0 创建并设置新功能，而无需更新网格中的所有其他参与者。管理员可在**管理 (Administration) > pxGrid 服务 (pxGrid Services) > 按功能查看 (View by Capabilities)** 页面启用该新功能。

访客增强功能

现在，发起人可在发起人门户中更改现有访客帐户的访客类型。

分析器增强功能

某些功能支持 IPv6 寻址。有关详细信息，请参阅 IPv6 支持（第 8 页）。

安全状态增强功能

思科 ISE 支持以下功能：

- 磁盘加密检查。用于保护写入磁盘的信息，并防止对数据存储空间的未授权访问。您仅在使用 AnyConnect ISE 安全状态代理时才可将磁盘加密条件与安全状态要求相关联。
- SHA-256 文件检查。可为管理员检查文件完整性提供一种更加安全的方式。
- 适用于 OS X 的属性列表文件检查。便于管理员检查指定文件中的指定属性值。
- 适用于 OS X 的后台守护程序检查增强功能。管理员可使用该功能来检查后台守护程序或用户代理的运行状态。
- 用于文件检查的额外变量。为用户目录提供变量，使得管理员可在用户目录中执行文件检查。

客户端调配增强功能

您只需运行一次 SPW 即可配置多个 WiFi SSID（NSP 配置文件）。第一个配置文件是活动配置文件。对于 Windows 和 Mac 而言，第一个配置文件的代理设置将会应用到全局（适用于所有后续配置文件）。自动配置代理设置时将使用代理自动配置文件 URL，支持它的操作系统包括 iOS、MAC OS、Windows 和 Android 5.0 或更高版本。如果未定义代理自动配置文件 URL，则所有操作系统都将使用代理主机/端口。但是，所有 Android 5.x 之前的版本都将使用代理主机/端口。

FIPS 模式支持

思科身份服务引擎使用经过 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。

IPv6 支持

思科 ISE 版本 2.0 支持以下 IPv6 功能：

- 支持启用 IPv6 的终端：思科 ISE 可检测、管理和保护来自终端的 IPv6 流量。您可以使用 IPv6 属性来在思科 ISE 中配置授权配置文件和策略，以处理来自启用 IPv6 的终端的请求，并确保该终端合规。
- 报告中的 IPv6 支持：版本 2.0 中的报告支持 IPv6 值。“实时会话”(Live Session) 和“实时身份验证”(Live Authentication) 页面也支持 IPv6 值。
- CLI 中的 IPv6 支持：版本 2.0 在以下 CLI 命令中支持 IPv6：
  - ipv6 address - 可对每个网络接口配置静态 IPv6 地址
  - ipv6 enable - 可在所有网络接口上启用或禁用 IPv6

- ipv6 route - 可配置 IPv6 静态路由
- ip host - 可在主机本地表中添加 IPv6 地址
- show IPv6 route - 可显示 IPv6 的路由

请参阅《*思科身份服务引擎 CLI 参考指南*》，查看有关这些命令的更多信息。

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。它以不同的软件包提供，包括 Base、Plus、Plus AC、Apex、Apex AC、设备管理、移动和移动升级。

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。

注意 思科 ISE 要求安装设备管理许可证，才能使用 TACACS+ 功能。有关更多信息，请参阅 TACACS+ 设备管理（第 3 页）的功能说明。

思科 ISE 版本 2.0 支持拥有两个 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。

有关许可证类型以及如何获取思科 ISE 许可证的详细信息，请参阅《*思科身份服务引擎版本 2.0 管理指南*》中的“思科 ISE 许可证”一章。

有关思科 ISE 版本 2.0 许可证的更多信息，请参阅《*思科身份服务引擎 (ISE) 产品手册*》。

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 2　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、策略服务和监控。
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 2.0 管理指南*》中的“为主要管理节点配置自动故障切换”部分。
  - 策略服务 - 供网络访问、安全状态分析、自带设备 (BYOD) 自行激活服务（本地请求方和证书调配）、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。

注意 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。

注意 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 对接的应用。pxGrid 服务可以在整个网络中共享情景信息，以识别策略和共享通用策略对象。这有助于扩展策略管理。

表 3　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	1	2（配置为高可用性对）
策略服务	1	• 2 - 当管理 / 监控 / 策略服务角色配置于相同的主要 / 辅助设备上时 • 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）

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 2.0 管理指南*》中的“在分布式环境中设置思科 ISE”一章。

系统要求

注意 有关思科 ISE 硬件平台和安装的更多详情，请参阅《*思科身份服务引擎版本 2.0 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 2.0。安装完成后，您可以在表 4 中列出的平台上使用指定组件角色（管理、策略服务、监控和 pxGrid）配置思科 ISE。

表 4　　支持的硬件和角色

硬件平台	角色	配置
Cisco SNS-3415-K9（小型）	任意	有关设备的硬件规格（表 3），请参阅《思科身份服务引擎 (ISE) 产品手册》。
Cisco SNS-3495-K9（大型）		
思科 ISE-VM-K9 (VMware, Linux KVM)		• 有关 CPU 和内存的建议，请参阅《*思科身份服务引擎版本 2.0 硬件安装指南*》中的“VMware 设备选型建议”部分。[1] • 有关硬盘大小的建议，请参阅《*思科身份服务引擎版本 2.0 硬件安装指南*》中的“磁盘空间要求”部分。 • NIC - 需要 1 GB NIC 接口。您最多可以安装 4 个 NIC。 • 支持的虚拟机版本包括： – ESXi 5.*x*, 6.*x* – RHEL 7.0 上的 KVM

1. 任何 VM 设备配置均不支持少于 8 GB 的内存分配。如果思科 ISE 出现行为问题，所有用户都需要将分配的内存更改为至少 8 GB，再提交支持请求。

注意 旧版 ACS 和 NAC 设备（包括思科 ISE 3300 系列）不支持思科 ISE 版本 2.0。

支持的虚拟环境

思科 ISE 支持以下虚拟环境平台：

- VMware ESXi 5.*x*、*6.x*
- RHEL 7.0 上的 KVM

支持的浏览器

管理员门户支持的浏览器包括：

- Mozilla Firefox 版本 39 及更高版本
- Google Chrome 版本 43 及更高版本
- Microsoft Internet Explorer 9.x、10.x 和 11.x

  如果使用 Internet Explorer 10.x，请启用 TLS 1.1 和 TLS 1.2，并禁用 SSL 3.0 和 TLS 1.0（“Internet 选项”[Internet Options] >“高级”[Advanced]）。

注意 必须在运行您的客户端浏览器的系统上安装 Adobe Flash Player 11.1.0.0 或更高版本。查看思科 ISE 管理员门户并实现更好的用户体验所需的最低屏幕分辨率是 1280 x 800 像素。

支持的密码套件

思科 ISE 版本 2.0 支持以下符合 FIPS 的密码：支持 TLS 版本 1.0、1.1 和 1.2。

- 对于 EAP-TLS、PEAP、EAP-FAST、EAP-TTLS：
  - DHE_RSA_WITH_AES_256_SHA256
  - DHE_RSA_WITH_AES_128_SHA256
  - RSA_WITH_AES_256_SHA256
  - RSA_WITH_AES_128_SHA256
  - DHE_RSA_WITH_AES_256_SHA
  - DHE_RSA_WITH_AES_128_SHA
  - RSA_WITH_AES_256_SHA
  - RSA_WITH_AES_128_SHA
- 对于 EAP-FAST 匿名调配：
  - ADH_WITH_AES_128_SHA

思科 ISE 版本 2.0 不支持不符合 FIPS 的密码。不支持以下密码：

- RSA_DES_192_CBC3_SHA
- EDH_RSA_DES_192_CBC3_SHA
- EDH_DSS_DES_192_CBC3_SHA
- RSA_RC4_128_SHA
- RSA_RC4_128_MD5
- EDH_RSA_DES_64_CBC_SHA

- EDH_DSS_DES_64_CBC_SHA
- RSA_RC4_128_SHA

注意 如果您拥有使用这些已弃用密码的旧版设备，请联系思科技术支持中心获取支持。

支持的设备和代理

有关支持的设备、浏览器和代理，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 4.9.5.8 是思科 NAC 设备版本 4.9(1) 4.9(3)、4.9(4)、4.9(5) 以及思科 ISE 版本 1.1.3 补丁 11、1.1.4 补丁 11、1.2.0、1.2.1、1.3、1.4 和 2.0 的一个通用代理。

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。

支持 Microsoft Active Directory

思科 ISE 版本 2.0 适用于所有功能级别的 Microsoft Active Directory 服务器 2003、2008、2008 R2、2012 和 2012 R2。

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

思科 ISE 2.0 支持与 Active Directory 基础设施进行多林/多域集成，以支持在整个大型企业网络中执行身份验证和属性收集。思科 ISE 2.0 最多支持 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 代理和思科 NAC Web 代理对具体防病毒和反间谍软件产品的支持详情，请访问以下链接：

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

思科 NAC Web 代理拥有静态合规性模块，在不升级 Web 代理的情况下无法升级这些模块。

下表列出的是 Web 代理版本和兼容的合规性模块版本。

表 5 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 2.0，请打开新设备，并配置思科集成管理控制器 (CIMC)。然后，您可以使用 CIMC 或可引导 USB 通过网络安装思科 ISE 版本 2.0。

注意 使用虚拟机 (VM) 时，在将 .ISO 映像或 OVA 文件安装到 VM 上*之前*，我们建议使用 NTP 服务器为访客 VM 设置正确的时间。

根据《*思科身份服务引擎版本 2.0 硬件安装指南*》中的说明，执行思科 ISE 初始配置。运行安装程序之前，请确保您已了解表 6 中列出的配置参数。

表 6　　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
Add/Edit another name server	（可选）允许您配置多个域名服务器。必须是其他域名服务器的有效 IPv4 地址。	输入 **y** 以添加额外域名服务器，或者输入 **n** 以配置下一个参数。
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	（可选）允许您配置多个 NTP 服务器。必须是有效的 IPv4 地址或主机名。	输入 **y** 以添加额外 NTP 服务器，或者输入 **n** 以配置下一个参数。
System Time Zone	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 2.0 CLI 参考指南*》，该文档提供思科 ISE 支持的时区列表。例如，对于太平洋标准时间 (PST)，系统时区为 PST8PDT（或协调世界时 [UTC] 减 8 小时）。 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。 **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。	UTC（默认值）

表 6　　思科 ISE 网络安装配置参数 （续）

提示	说明	示例
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

注意　有关配置和管理思科 ISE 的更多信息，请参阅适用于具体版本的文档（第 33 页）以查看思科 ISE 文档集中的其他文档。。

升级思科 ISE 软件

您可以从以下任何版本直接升级到思科 ISE 版本 2.0：

- 思科 ISE 版本 1.3
- 思科 ISE 版本 1.4

如果您的版本低于思科 ISE 版本 1.3，则必须先升级到上述版本之一，然后才能升级到版本 2.0。

按照《*思科身份服务引擎 版本 2.0 升级指南*》中的升级说明升级至思科 ISE 版本 2.0。

注意　当您升级至思科 ISE 版本 2.0 时，可能需要开启之前的思科 ISE 版本中未使用的网络端口。有关更多信息，请参阅《*思科身份服务引擎版本 2.0 硬件安装指南*》中的“*思科 ISE 端口参考*”。

升级注意事项和要求

升级至思科 ISE 版本 2.0 之前，请阅读以下部分：

- 必须开放用于通信的防火墙端口（第 16 页）
- 管理员用户在升级后无法访问 ISE 登录页面（第 16 页）
- 将思科 ISE 重新加入 Active Directory（第 16 页）
- 发起人登录失败（第 16 页）
- 为新访客类型更新授权策略（第 16 页）
- 其他已知升级注意事项和问题（第 16 页）

必须开放用于通信的防火墙端口

思科 ISE 版本 2.0 中的复制端口已更改。如果您已在主管理节点与任何其他节点之间部署防火墙，则升级至版本 2.0 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 - 用于全局集群复制。
- TCP 7800 和 7802 -（仅在节点组中包含策略服务节点时适用）用于 PSN 组集群。

如需了解思科 ISE 版本 2.0 使用的端口的完整列表，请参阅《*思科身份服务引擎版本 2.0 硬件安装指南*》中的“*思科 ISE 端口参考*”。

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 2.0 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。

为新访客类型更新授权策略

在升级至思科 ISE 2.0 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。

其他已知升级注意事项和问题

有关其他已知的升级注意事项和问题，请参阅《*思科身份服务引擎版本 2.0 升级指南*》。

从 Cisco Secure ACS 迁移至思科 ISE

您只能从 Cisco Secure ACS 版本 5.5 和 5.6 直接迁移至思科 ISE 版本 2.0。有关从 Cisco Secure ACS 版本 5.5 和 5.6 迁移至思科 ISE 版本 2.0 的信息，请参阅《*思科身份服务引擎迁移工具指南*》。

您无法从 Cisco Secure ACS 5.1、5.2、5.3、5.4、4.x 或更低版本或者从思科网络准入控制 (NAC) 设备迁移至版本 2.0。要从 Cisco Secure ACS 版本 4.x、5.1、5.2、5.3 或 5.4 迁移，您必须先升级到 ACS 版本 5.5 或 5.6，然后再迁移至思科 ISE 版本 2.0。

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，但是可以使用能充当 OCSP 服务器的 CA 来撤销证书。

思科 ISE 版本 2.0 中的已知限制

本节列出版本 2.0 中的已知限制：

- 请勿删除默认的内部思科 ISE CA 模板（第 17 页）
- 升级前请勿安装补丁（第 18 页）
- LDAP 导入的访客帐户无法从版本 1.2 升级（第 18 页）
- 从 1.2 升级时无法看到 LDAP 发起人创建的访客用户（第 18 页）
- Android 设备上的 TLS 身份验证不使用由分配的证书颁发机构颁发的证书（第 18 页）
- EKU 验证：OCSP 签名证书为根 CA 返回未知响应（第 18 页）

请勿删除默认的内部思科 ISE CA 模板

内部思科 ISE CA 配有两个默认的证书模板：

- CA_SERVICE_Certificate_Template - 当其他网络设备使用思科 ISE 作为 CA 时，思科 ISE 使用此模板发布证书。例如，该模板适用于通过 ASA VPN 连接的客户端计算机。
- EAP_Authentication_Certificate_Template - 思科 ISE 根据此模板为 EAP 身份验证发布证书。

请勿删除这些默认的证书模板。如果要自定义证书模板，您可以创建一个新的，或者复制并编辑现有模板。

升级前请勿安装补丁

在升级过程中，请勿同时在部署中的任何节点上安装补丁。应当在部署升级完成后安装补丁。

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。

从 1.2 升级时无法看到 LDAP 发起人创建的访客用户

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。

Android 设备上的 TLS 身份验证不使用由分配的证书颁发机构颁发的证书

当您执行以下配置时，会发生此问题：

- 思科 ISE 中的内部和外部证书颁发机构 (CA)。
- 分别使用内部和外部 CA 进行 TLS 身份验证的两个配置文件（SSID1 和 SSID2）。

从思科 ISE 调配的证书导入至 AnyConnect 证书存储空间中。有时候，无线网络在连接至网络时会使用众多证书的其中一个。例如，当一台 Android 设备使用 SSID 1 连接至网络时，用于身份验证的证书由内部 CA 颁发。当第二台 Android 设备使用 SSID 2 连接至网络时，用于身份验证的证书也由内部 CA 颁发，而非由外部 CA 颁发（按照 SSID2 中的配置）。

此问题只出现在 Android 设备中，并且没有解决方法。

思科建议您使用供应商提供的所有补丁包和升级包更新您的 Android 设备。

EKU 验证：OCSP 签名证书为根 CA 返回未知响应

Bouncy Castle OCSP 签名证书为根 CA 返回一个“未知”响应。如果您已经将思科 ISE 配置为当 OCSP 服务返回未知的证书状态时拒绝请求，则思科 ISE 会拒绝正在评估的证书，且用户身份验证失败。

此问题出现在 Bouncy Castle 版本 1.6.145 生成的证书中。无解决办法。

思科 ISE 版本 2.0 中不支持的功能

本节列出版本 2.0 中不支持的功能：

- 内联安全状态节点 (IPN/iPEP)（第 18 页）

内联安全状态节点 (IPN/iPEP)

思科 ISE 版本 2.0 不再支持 IPN/iPEP 配置。

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

除了安装思科 ISE 软件（第 14 页）中描述的执行思科 ISE 全新安装所需的 .ISO 安装程序包，您还可以使用软件下载网页检索其他思科 ISE 软件元素，比如 Windows 和 Mac OS X 代理安装程序和 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 依次导航至**产品 (Products) > 安全 (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
- 用于 Windows 和 Mac OS X 本地请求方的调配向导
- Windows 客户端计算机代理安装文件（包括用于执行动手调配的 MST 和 MSI 版本）
- Mac OS X 客户端计算机代理安装文件
- 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。要解决此问题，您可以将代理服务配置为允许和 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 2.0 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。

客户端调配和安全状态实时更新门户：

- **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：

  - 用于 Windows 和 Mac OS X 本地请求方的调配向导
  - 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

  有关将此门户上已可用的软件包自动下载至思科 ISE 的更多信息，请参阅《*思科身份服务引擎版本 2.0 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。

- **安全状态门户** - https://www.cisco.com/web/secure/pmbu/posture-update.xml

  此 URL 提供以下软件元素：

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

  有关将此门户上已可用的软件包自动下载至思科 ISE 的更多信息，请参阅《*思科身份服务引擎版本 2.0 管理员指南*》中“配置客户端安全状态策略”一章中的“自动下载安全状态更新”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 20 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。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，您可以使用此选项上传客户端调配和安全状态更新。

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：

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 依次导航至**产品 (Products) > 安全 (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)**。

从下列可下载的离线安装程序包中选择：

- **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)**。

有关将已下载安装版本包添加至思科 ISE 的更多信息，请参阅《*思科身份服务引擎版本 2.0 管理员指南*》中“配置客户端调配”一章的“从本地计算机添加客户端调配资源”部分。

您可以使用安全状态更新，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。

要上传离线安全状态更新：

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) > 安全状态 (Posture)**。

步骤 3 点击箭头查看安全状态的设置。

步骤 4 选择**更新 (Updates)**。系统将显示“安全状态更新”(Product Updates) 页面。

步骤 5 在“安全状态更新”(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)。

注意 “待更新文件”(File to Update) 字段是必填字段。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 7 点击**现在更新 (Update Now)** 按钮。

更新后，“安全状态更新”(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。

思科 ISE 版本 2.0 未解决的警告

未解决的警告

表 7　思科 ISE 版本 2.0 未解决的漏洞

警告	说明
CSCuy84839	ISE 2.0 中配置的默认规则从拒绝访问更改为内部用户。 **解决方法**　每次重新启动后，从 GUI 审核策略配置，如果出现问题则重新配置。
CSCus91272	由于 EAP 标识符不匹配，使用本地请求方的 EAP-TTLS 与 EAP-MSCHAPv2 身份验证失败。
CSCut18311	在 RADIUS 身份验证报告的 CVS 文件中，如果身份验证失败，则 RADIUS 状态值显示为 `0`，如果身份验证通过则显示为 `1`，而不显示 `Pass` 或 `Fail`。
CSCut33204	不能使用包含正斜杠 (\) 的字符串搜索报告。例如，`Cisco\`。它不会返回相应的结果。 **解决方法**　执行搜索时请勿使用正斜杠。
CSCut64610	操作审核报告不显示以下更改： • **身份验证策略**：所有 CRUD 操作都记录为配置更改，而不会具体地记录为创建、更新或删除。 • **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 身份验证 (Authentication) > 允许的协议 (Allowed Protocols)**：CRUD 操作无日志记录。 • **策略 (Policy) > 策略元素 (Policy Elements) > 结果 (Results) > 身份验证 (Authentication) > 样本 (Simple)**：不会记录删除操作。
CSCuv03825	系统和解决方案 (SnS)：在分布式部署中，有时所有辅助节点都处于“复制终止”(Replication Stopped) 状态（极少发生）。 **解决方法**　如果所有节点处于“复制终止”(Replication Stopped) 状态超过几分钟，请重新启动主 PAN。
CSCuv13440	在双 SSID SAML 流程中，完成证书调配后，系统会发送 CoA 断开的消息，并显示 UI 以便手动连接至 SSID。但是在 Windows 10 中，当选择 SSID 和证书时，它会请求用户名，但调配后不启动身份验证。
CSCuv14593	RBAC 管理员可从父终端组导入和查看终端。
CSCuv14605	在 Windows 10 Edge 浏览器上，访客门户中的 LAN DHCP 发布页面不启动。 **解决方法**　使用 Mozilla Firefox 浏览器。
CSCuv83774	无法使用某些允许的字符创建时间和日期策略以及可下载的 ACL 名称。支持的字符仅包括尖括号 (<>)、和号 (&) 和百分数 (%) 符号。

表 7　思科 ISE 版本 2.0 未解决的漏洞（续）

警告	说明
CSCuv88378	证书调配门户复制操作不复制授权组和模板。
CSCuv90086	在大型部署中生成思科 ISE 根 CA 时，主要管理节点 (PAN) 会重新启动。PAN 无法长期使用。
CSCuv94217	在 Mozilla Firefox 40 中，对策略集重新排序并保存新顺序后，“保存顺序” (Save Order) 按钮会消失。此问题仅出现在 Mozilla Firefox 版本 40 浏览器上。
CSCuw08701	如果授权配置文件名中包含空格，则 ACS 至 ISE 的迁移工具在导出时会产生错误。 **解决方法**　删除 ACS 授权配置文件名中的空格，然后重新导出数据。
CSCuw21758	在“我的设备”(My Devices) 门户中，将“可接受的用户策略”(Changes to the Acceptable Use Policy (AUP) 设置更改为“仅第一次登录开启”(On first login only) 或“每 *x* 天”(Every *x* days) 后，更改不生效。系统仍在每次登录时提示用户接受 AUP。
CSCuw22718	当执行大量客户端调配事务时，PAP 会耗尽堆内存并进行故障切换。
CSCuw23690	当启用或禁用 SXP 服务时，pxGrid 服务会重新启动。
CSCuw23941	在 MAC 上，在网络重置后，非广播 SSID 不会自动连接。 **解决方法**　SSID 显示在“可用网络”(Available Networks) 列表中。点击**连接 (Connect)** 以连接至 SSID。
CSCuw29997	当与 Aruba WLC 一同使用时，ISE 访客门户重定向静态 URL 包含特殊字符“?”，且系统无法正确识别 URL 中的此字符，因此重定向无法正常运行。 **解决方法**　手动配置所有 WLC 中的 URL。
CSCuw34150	当 SFTP 服务器使用 DSA 密钥时，crypto host_key add host 命令无法正常运行。 **解决方法**　建立与 SFTP 服务器的 SSH 连接，并手动将加密的主机密钥添加至思科 ISE 数据库。
CSCuw35766	即使已设置静态终端组分配，但仍然会消耗 Plus 许可证。
CSCuw38040	在 Mac OSX 中，当使用不同身份验证协议或证书模板调配有线和无线配置文件时，有线配置文件未调配。此问题出现在请求方调配向导版本 1.0.0.35 中。 **解决方法**　为有线使用案例创建单独的本地请求方配置文件。
CSCuw43915	Mac OS X 10.10 和 Mac OS X 10.11：在 PEAP 或 EAP-FAST 身份验证过程中，调配 NSP 后无法自动连接至 SSID。 **解决方法**　点击“连接”(Connect) 按钮并手动提供 PEAP 或 EAP-FAST 凭证。

表 7　思科 ISE 版本 2.0 未解决的漏洞（续）

警告	说明
CSCux31573	对于 Windows 10 build 10565，本地请求方调配 (NSP) 在 BYOD TLS 流程中失败。 症状：对于 Windows 10 版本 10565 设备，NSP 在 BYOD TLS 流程中失败。 条件：满足以下条件时会发生此问题： 1. 已安装 ISE 版本 2.0.0.306 补丁 1。 2. 将授权配置文件配置为重定向至 BYOD 门户。 3. 使用 Windows 10 配置 NSP 配置文件。 4. 使用 Windows 10 配置客户端调配策略并与 NSP 相关联。 5. 安装 Windows 10 (build 10565) 的设备通过 BYOD 流程连接。 解决方法：无。

待解决的代理警告

表 8　思科 ISE 版本 2.0 待解决的代理警告

警告	说明
CSCuw19276	思科 NAC 代理和思科 NAC Web 代理不支持 Google Chrome 版本 45 及更高版本。 Java 插件在 Google Chrome 中使用 Netscape 插件 API (NPAPI)，这是思科 NAC 代理和思科 NAC Web 代理运行的必要组件。但是，Google Chrome 版本 45 及更高版本不支持 NPAPI。 **解决方法**　要启用 Java 插件，请执行以下步骤： 1. 在 Google Chrome 窗口地址栏中，复制并粘贴以下 URL： chrome://flags/#enable-npapi 2. 点击**启用 (Enable)** 链接以便为 Mac 和 Windows 启用 NPAPI。 3. 点击页面底部的**现在重启 (Relaunch Now)** 以使更改生效。
CSCuw17919	Trend Micro Internet Security 10.x 不可用。 为 Trend Micro Internet Security 10.x 执行安全状态评估时，您必须使用 Trend Micro Titanium 10.x 配置安全状态条件，因为 Trend Micro Internet Security 10.x 使用 Trend Micro Titanium 10.x AV/AS 引擎。

思科 ISE 版本 2.0.0.306 补丁更新

思科 ISE 版本 2.0.0.306 累积型补丁 1 中已解决的问题

下表列出思科身份服务引擎版本 2.0.0.306 累积型补丁 1 (ise-patchbundle-2.0.0.306-PP1-161394.SPA.86_64.tar.gz) 中已解决的问题。

要获取将补丁应用至思科 ISE 2.0 所必需的补丁文件，请使用以下网址登录思科软件下载中心：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），依次导航至**安全 (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)**，然后保存一份补丁文件副本到本地计算机中。

补丁 1 可能不兼容旧版 SPW，因此用户需要升级 SPW。

有关如何将补丁应用至系统的说明，请参阅《*思科身份服务引擎版本 2.0 管理员指南*》中“管理思科 ISE”一章的“安装软件补丁”部分。

表 9　　思科 ISE 补丁版本 2.0.0.306 补丁 1 已解决的警告

警告	说明
CSCuw88770	ISE 2.0 PEAP TLS 1.2 无线身份验证在 Android 6 和 Win 10 中失败。 之所以出现此问题，是因为在 TLS 1.2 中，EAP-TLS、PEAP 和 EAP-TTLS 的 MPPE 密钥生成机制已经更改。EAP-FAST 不受影响。 **症状：**日志中的身份验证报告显示身份验证已成功；但是，客户端会话的 WLC 状态需要 dot1x。无线数据包的获取结果显示 EAP 成功后的 4 次握手未完成，无论是 M1 和 M2 还是仅仅 M1。 **条件：**满足以下组合条件时会发生此问题： • 思科 ISE 版本 2.0 FCS 未安装补丁。 • 为 WPA2 企业版配置了无线 LAN 和 L2 安全。 • 安装 Android 6 或 Windows 10 版本 1511 的设备尝试进行身份验证。 • 使用的协议为 PEAP、 TTLS 或 EAP-TLS。 **解决方法：** • 对于 Android，无解决方法。您无法从 Android 客户端或思科 ISE 配置 TLS 版本。 • 对于 Windows 10 客户端，您可以禁用 TLS 1.2 并启用 TLS 1.0： – 创建 DWORD HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13\TlsVersion 并将相关的 DWORD 值设为 C0。 – 重新启动 EapHost 服务。

思科 ISE 版本 2.0.0.306 累积型补丁 2 中已解决的问题

下表列出思科身份服务引擎版本 2.0.0.306 累积型补丁 2 中已解决的问题。

要获取将补丁应用至思科 ISE 2.0 所必需的补丁文件，请使用以下网址登录思科软件下载中心：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），依次导航至**安全 (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)**，然后保存一份补丁文件副本到本地计算机中。

补丁 2 可能不兼容旧版 SPW，因此用户需要升级 SPW。

有关如何将补丁应用至系统的说明，请参阅《*思科身份服务引擎版本 2.0 管理员指南*》中“管理思科 ISE”一章的“安装软件补丁”部分。

表 10　思科 ISE 补丁版本 2.0.0.306 补丁 2 的已解决警告

警告	说明
CSCuw62692	“网络设备名称”(Network Device Name) 字段不允许使用句点 (.)。
CSCuw89551	ISE XML 策略的导出不区分 TACACS+ 和 RADIUS 策略集。
CSCuw27405	应删除 ANC 的“修复”(Remediate) 和“调配”(Provisioning) 选项。
CSCuw58973	无法在 ISE 2.0 中手动取消对 EPS 终端的隔离。
CSCuw09138	如果使用 AD 连接器，将在 PSN 中看到高内存利用率。一段时间后，将生成一条关于 AD 服务重启的警告。内存使用率下降，然后再次升高。 **解决方法**　重新启动服务。
CSCuw74703	从 ISE 1.2.1 升级至 ISE 1.4 后，不正确分析 IP 电话。 **解决方法**　在启用分析器的所有节点上运行 EP_Reset_Time.sh 脚本。
CSCuw94822	ISE 2.0 与 LGPLv2.1 许可证要求不兼容。
CSCuw78737	即使清除缓存后，某些访客终端仍然在 HotSpot AUP 门户循环中卡住。 **解决方法**　将终端从 ISE 数据库中删除，并在控制器上清空该终端的所有会话。
CSCuv61017	BYOD 流失败，因为 dir: /opt/CSCOcpm/appsrv/apache-tomcat-ca/webapps/caservice-webapp/WEB-INF/lib 中缺失 PSP-Commons-1.3.0.295.jar。
CSCux30540	安装 ISE 2.0 补丁 1 后，pxGrid 控制器服务不稳定。
CSCuw45102	CIDR 格式中指定的 ID 映射过滤器（例如，10.1.100.0/24 ）无法正常工作。 **解决方法**　将各个 IP 地址指定为过滤器。
CSCuw02111	当 VPN 客户端断开连接时，ASA 发送记帐停止消息，但 ISE 中未清除该会话。
CSCuu94127	使用基于 IP 的探测功能而不启动 RADIUS 探测功能时，ISE 分析器会混淆不同会话的属性。 在应用此补丁后，请启用 RADIUS 探测功能，并将 NAD 配置为向已开启分析器的 PSN 发送 RADIUS 记帐消息。
CSCuw22718	当执行大量客户端调配事务时，PAP 会耗尽堆内存并失败。

表 10　思科 ISE 补丁版本 2.0.0.306 补丁 2 的已解决警告（续）

警告	说明
CSCuw65623	当域名中间包含数字时，系统显示无效的 FQDN 消息，例如，1portal.com 是可行的，但 portal.1test.com 或 portal.abc.1test.com 会导致错误。 **解决方法**　FQDN 中不能有数字。
CSCuu08092	升级后，读取来自数据库的网络设备出现问题。 ISE 1.3 允许在末尾使用句点 (.) 来定义网络设备。升级至 ISE 1.4 后，来自这些设备的身份验证将被丢弃，因为不允许在末尾使用句点。 **解决方法**　删除现有设备，并重新创建相同的设备。
CSCux11146	使用错误的密钥对 SXP 密码进行加密。 加密 SXP 密码所使用的密钥应当与加密 ISE Oracle DB 中存储的所有其他敏感材料所使用的相同。
CSCuv81729	升级至 ISE 1.4 后，对于任何操作系统的新补丁管理条件，都不填充供应商列表。
CSCux30578	使用 HP 设备的访客流程无法在分布式部署上正常运行。 重定向至访客门户时，系统显示 500 内部错误 (500 Internal Error) 消息。
CSCux27365	ISE 不支持使用传统密码的 EAP 客户端。 仅支持 RC4 或 DES 加密密码的传统客户端连接至 ISE 时，EAP 握手会失败。
CSCuw88244	ISE-TACACS 限期许可证在导入后显示为永久许可证。
CSCuw40899	当客户端从一个 SSID 切换为另一个时，终端 MAC 未在正确的终端身份组中更新。 **解决方法**　您必须手动将终端从之前的终端组中删除。
CSCuw59035	HTTP 状态 400 - 如果在非 443/TCP 端口上使用 PAT/NAT，登录后将显示错误请求 (Bad Request) 错误。
CSCuw51376	PSN 所有权更改后，无法正确分析终端。
CSCuw15139	生成主访客报告时，系统显示以下错误消息： `Unable to connect to the operation database.Please check the network connectivity and retry again later.`
CSCur44745	当启用“抑制重复的成功身份验证”(Suppress Repeated Successful Authentications) 选项时，CoA 事件会添加到“实时日志”(Live Log) 会话条目的“身份验证”(Auth) 详情中。 **解决方法**　在“管理”(Administration) > “系统”(System) > “设置”(Settings) > “协议” (Protocols) > RADIUS 下禁用 “抑制重复的成功身份验证” (Suppress Repeated Successful Authentications)。

思科 ISE 版本 2.0.0.306 累积型补丁 3 中已解决的问题

下表列出思科身份服务引擎版本 2.0.0.306 累积型补丁 3 中已解决的问题。

要获取将补丁应用至思科 ISE 2.0 所必需的补丁文件，请使用以下网址登录思科软件下载中心：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），依次导航至**安全 (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)**，然后保存一份补丁文件副本到本地计算机中。

补丁 3 可能不兼容旧版 SPW，因此用户需要升级 SPW。

有关如何将补丁应用至系统的说明，请参阅《*思科身份服务引擎版本 2.0 管理员指南*》中“管理思科 ISE”一章的“安装软件补丁”部分。

表 11　思科 ISE 补丁版本 2.0.0.306 补丁 3 的已解决警告

警告	说明
CSCuh80594	为自定义属性选择的“默认枚举类型”(Default Enum) 值无法正常运行。
CSCuu18124	升级至 1.3 后，LDAP 发起帐户缺失。 **解决方法**　使用 SponsorAllAccounts 组而非 Group 或 Own。
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。
CSCuv68500	MDM：请勿对未向 MDM 注册的设备执行强制重定向。 **解决方法**　通过 ISE 自行激活设备。
CSCuv71811	ISE 身份验证延迟每小时都增加。 **解决方法**　每 5 天重启一次 ISE 服务。
CSCuv77724	在“证书调配”(Certificate Provisioning) 页面，在 PQDN 字段输入内容会显示错误消息“FQDN 字段格式无效”(The FQDN field is not in a valid format)。
CSCuv88011	在 ISE 1.4 中使用分析器源送服务时，源服务更新会覆盖管理员创建的同名规则。 **解决方法**　配置“由思科提供”策略来适应自定分析器条件的需求，或者在运行源服务更新前重命名自定义策略。
CSCuv89453	在 ISE 1.3 中，访客和发起人门户会出现重复的密码更改和登录循环。
CSCuv91527	ISE 升级至 1.4 后，在补救中无 ANY AV 选项。
CSCuv94231	身份验证后，Radius 令牌上的 Acs.NormalizedUserName 为空。
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。
CSCuv99833	ISE 1.3 源安全状态安排程序服务出现 JDBC 异常的故障。 **解决方法** 1. 手动启动更新。 2. 重新启动服务。
CSCuw09627	ISE 1.3 RSA 代理在身份验证流程中引起延迟，导致身份验证在一般负载情况下失败。ISE 1.3 和 RSA/ACE 代理版本 8.1.2 上会出现此问题。 **解决方法**　请使用 RADIUS 令牌。

表 11　思科 ISE 补丁版本 2.0.0.306 补丁 3 的已解决警告（续）

警告	说明
CSCuw27263	当外部 RADIUS 服务器被用作 BYOD 流的一部分时，不支持其身份验证。 **解决方法**　请使用内部用户或 AD 用户帐户。
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。 **解决方法** 在**访客门户 (Guest Portals)** 中，取消选中“要求访客设备合规性”(Require guest device compliance) 复选框以避免嵌入式安全检查，并为安全检查设置单独的策略。 或 使用 NAC 代理或 AnyConnect ISE 安全状态模块访问网络。
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。 当使用包含 Active Directory 短名称帐户通过访客门户调配设备时，“我的设备”(My Devices) 门户中的门户用户与访客门户的门户用户名未正确映射。因此，除非使用 UPN，否则会看到设备。
CSCuw57930	在用户帐户到期之前，未发送访客帐户到期邮件。
CSCuw60028	ISE 1.x：外部 Radius 服务器不接受共享密钥中的“&”。
CSCuw67042	支持套件中缺失 ISE 文件。
CSCuw95152	向已知访客提供帐户详情时，如果取消选中“复制我”(Copy me) 复选框，则它会缓存上一个发起人的邮件地址。
CSCuw98748	访问发起人门户时，其配置中的 Javascript 输入会翻倍。
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。 **解决方法**　通过 MNT API 手动清空会话。
CSCux03119	已发起自带设备 (BYOD) 支持。
CSCux07108	ISE 1.3 补丁 4 应用在源服务复制消息后初始化。 如果用户打开分布式部署中的分析器源服务，则节点上的应用服务进入初始化状态。 **解决方法**　无。运行 **application reset-config** 命令，以便从该状态中恢复。
CSCux10424	在 ISE 中，AD 黑名单未在预期频率内刷新。 **解决方法**　重新加载表现出该行为的 PSN。
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。 **解决方法** 注册后，使用您在访客门户中创建的凭证。所有其他登录在第一个页面会正常运行。 或 请勿将“访客用户”(Guest Users) 置于 Guest_Portal_Sequence 顶部。

表 11　思科 ISE 补丁版本 2.0.0.306 补丁 3 的已解决警告（续）

警告	说明
CSCux21939	ISE 终端清除操作无法删除终端。
CSCux43787	ISE 运行时在收到超过 4 个请求后卡住。 **解决方法**　重新启动服务并重新加入节点。
CSCux46301	ISE 2.0 访客帐户到期的 SMS 通知无法正常运行。 **解决方法**　启用邮件通知。
CSCux53910	ISE 1.3 补丁 5 内存提高导致身份验证延迟。 **解决方法**　每 5 天重启一次 ISE 应用。
CSCux58966	在外部 RADIUS 服务器下显示用户密码。
CSCux61238	SNMPQUERY EventTimeout 的范围从 60 秒延长为 150 秒。
CSCux61360	ISE 2.0 访客密码经过一天就到期。 **解决方法**　为访客帐户启用 “密码永不过期” (password never expires)。
CSCux66320	ISE 2.0 身份验证策略从配置中消失。
CSCux73262	更新安全状态补救资源时，ISE 1.4 应用服务重新启动。 **解决方法**　联系 TAC。
CSCux77620	访客清除操作后显示 “由于网络错误未收到服务器响应” (Fail to receive server response due to network error)。 **解决方法** 更改安排的清除时间或频率,然后重新改回来。 或 更改 ISE 时区，然后重新改回来。
CSCux79853	HTTPS API 呼叫未到达 SMS 网关（使用 Clickatell 测试）。
CSCux91475	手动完成源服务更新后，无法进行其他源更新。
CSCux92681	对于 Clickatell 上的 GlobalDefault，通过 HTTP-POST 发送 SMS 失败。
CSCux97025	如果终端源是配置协议，则所有权更改/合并可能失败。
CSCux99204	ISE 2.0 补丁 2 使 HotSpot 门户出现故障，可在 AUP 之前执行 CoA。 **解决方法**　降级至 ISE 2.0 补丁 1 或不含补丁的 ISE 2.0。
CSCuy10037	如果网真没有 cdpCacheAddress，则 CDP 无法正常工作。
CSCuy12346	ISE 重复计数器未在 24 小时内重置。
CSCuy29028	EAP-TLS 内存泄漏。
CSCuy29124	当有足够的可用资源时，ISE 2.0.1 MR 无法纵向扩展。
CSCuy33801	ISE 2.0 管理员门户不接受带有 “-” 连字符的 FQDN。 **解决方法**　使用最后一个片段中不含 “-” 的 FQDN。

表 11　思科 ISE 补丁版本 2.0.0.306 补丁 3 的已解决警告（续）

警告	说明
CSCuy34700	更新 glibc 软件包以解决 CVE-2015-7547。
CSCuy43592	将用户标记为合规后，ISE 2.0 发送 CoA 断开连接的消息。 **解决方法**　使用 SSL VPN。
CSCuy51958	ISE 2.0 证书的自动验证操作会中断节点间通信。
CSCuy81433	ISE 2.0 CoANAK 无法找到任何会话标识属性。 **解决方法**　联系 TAC。

思科 ISE 版本 2.0 已解决的警告

下表列出此版本中已解决的警告：

表 12　思科 ISE 版本 2.0 已解决的警告

警告	说明
CSCuh12811	我的设备和发起人门户 URL 都不支持主机和 FQDN。
CSCun52844	在客户端调配下报告跨域引用方泄漏 (Cross-Domain Referer Leakage) 问题。
CSCuq22852	如果用户名或密码中使用非字母数字字符，则本地 Web 身份验证失败。
CSCuq92574	在运行 Android 4.2.2 的 LG 上，无法安装自带设备 (BYOD) 配置文件。
CSCuq96560	升级后，自助注册访客用户的访问持续时间值为 0。
CSCuq97051	在使用 3300 和 3400 系列硬件的部署中启用 SNMP 查询探测功能时，将看到缓慢复制错误。
CSCur11286	iPhone 6 在调配后不重定向至配置的 URL。
CSCur13627	监控日志收集器不显示最近 60 分钟的任何数据。
CSCur28245	“发起人组”(Sponsor Group) 和“访客类型”(Guest Type) 页面出现用户界面问题。
CSCur35764	从受信任证书存储空间中删除内部 CA 证书时，也会从证书颁发机构撤回证书。
CSCur36983	配置数据恢复进程卡在 80% 处；LD_LIB_PATH 库中缺失字段。
CSCur44557	如果各门户的语言捆绑包不同，则发起人门户通知会失败。
CSCus09940	跨站请求伪造 (CSRF) 保护在某些网页上无法正常运行。
CSCus19913	ISE AuthStatus Rest API 不支持多个 MAC 地址。
CSCus50476	监控节点 (MnT) 缓慢，尤其是在显示实时日志和报告时。
CSCus78802	在字符串中间使用变量替换会删除初始字符。
CSCus93665	从 1.2.x. 升级后，ISE 1.3 EAP-FAST 链无法通过身份验证。
CSCut04544	ISE - 传输层保护 - 不安全传输 (ISE-Transport Layer Protection- Insecure Transmission) 上有漏洞。
CSCut04556	思科 ISE 易受跨帧脚本攻击。

表 12　思科 ISE 版本 2.0 已解决的警告（续）

警告	说明
CSCut25212	在 Android 4.3 或更高版本中，本地请求方配置文件 (NSP) 不将证书存储在密钥存储库中。
CSCut25227	在 ISE 管理员页面发现跨站脚本 (XSS) 漏洞。
CSCut40042	在访客门户中升级 Apache Tomcat 后，重定向端口重新配置无法正常运行。
CSCut42520	添加第二个 Active Directory (AD) 连接点时，用户主体名称 (UPN) 身份验证失败。
CSCut58228	Samsung Android 设备无法为 BYOD EAP-TLS 安装证书。
CSCut63392	ISE GUI 的锁定/高级调整导致 AD 服务崩溃。
CSCuu03368	轻量级目录访问协议 (LDAP) 用户无法管理我的设备 (My Devices) 门户。
CSCuu04061	当 MDM 服务器关闭时，ISE 策略服务节点 (PSN) 不响应 RADIUS 请求。
CSCuu04227	后接 802.1X 的 MAB 身份验证失败。
CSCuu22410	将访客会话数据写入缓存和 DB 时出现延迟。
CSCuu43966	当交换机上的身份验证顺序为 MAB 后跟 802.1x 时出现错误。
CSCuu49759	Mac OSX 版本 10.10 无法自动连接至使用单独 SSID 的网络。
CSCuu60864	无法保存新分析的终端。
CSCuu65509	从 1.2 升级至 1.4 后，无法访问管理员门户。
CSCuu76087	连接至 IP 电话的 Windows PC 被分析为 Cisco-IP-Phone-7970。
CSCuu91928	ISE 必须发送产品名称进行定义检查，而非发送供应商名称。
CSCuu92630	修改思科 ISE 中的 CTS 策略时，触发复制失败警报。
CSCuv22443	发起访客用户在访客门户中输入凭证后，系统会提示其开启 BYOD 流程。
CSCuv22604	从 1.2 升级至 1.3 期间，并非当前所有者的 PSN 可能会获得所有权，从而导致无效的分析器分类。
CSCuv24342	CoA 重新身份验证触发 ISE 附加“会话超时”(Session Timeout) 属性。
CSCuv31567	使用对象图导航语言 (OGNL) 控制台的 Apache Struts 2 Web 应用易受远程命令执行攻击。
CSCuv51519	对于某些 AD 用户，发起人门户不会完全加载。
CSCuv52944	SWD-xxx LSQ-xxx-ISE 无法发送停止记帐消息，从而影响用户。
CSCuv53534	当 ISE 对电话或其他设备进行身份验证/授权时，从分析器 DB 查询终端非常缓慢。
CSCuv54014	使用非公开顶级域名时，CRL/OCSP URL 验证失败。
CSCuv61017	BYOD 流失败，因为 dir: /opt/CSCOcpm/appsrv/apache-tomcat-ca/webapps/caservice-webapp/WEB-INF/lib 中缺失 PSP-Commons-1.3.0.295.jar。
CSCuv71811	ISE 身份验证延迟每小时都增加。
CSCuv90268	邮件地址中包含多个点号（“.”）的管理员用户身份验证失败。

文档勘误表

思科 ISE 2.0 在线帮助包含对 3300 系列设备的参考 - CSCuw68020。

思科 ISE 版本 2.0 不支持传统的 3300 系列、ACS 或 NAC 设备。但是，在线帮助中“管理网络设备”一章的“MDM 设置中使用的组件”表格列出了 3315、3355 和 3395 系列设备。

此信息不正确，并已从 Cisco.com 上发布的《*思科身份服务引擎版本 2.0 管理指南*》中删除。

相关文档

适用于具体版本的文档

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 13　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 2.0 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 2.0 管理员指南	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 2.0 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 2.0 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 2.0 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 2.0 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 2.0 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 2.0 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

表 13　思科身份服务引擎的产品文档（续）

文档标题	位置
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
使用思科身份服务引擎创建的网络访问设备配置文件	http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-105-Network_Access_Device_Profiles_with_Cisco_ISE.pdf

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。