思科身份服务引擎 (ISE)

产品概述

思科® 身份服务引擎 (ISE) 可帮助 IT 专业人员应对企业移动性挑战，并为不断发展的网络提供涵盖整个攻击过程的保护。Cisco ISE 是市场领先的安全策略管理平台，它能以统一且自动化的方式实现高度安全的访问控制，帮助实施基于角色的网络访问及网络资源访问。它提供出色的用户可视性和设备可视性，可实现简化的企业移动性体验。它采用基于思科平台交换网格 (pxGrid) 技术的集成生态系统合作伙伴解决方案共享至关重要的情景数据，可更快地识别和缓解威胁，并采取补救措施。

移动性企业环境中的安全性

企业网络已不再局限于安全防火墙所保护的范围内。当今的员工需要使用比以往更多的媒介（包括个人笔记本电脑、平板电脑和智能手机），从家庭网络和移动网络访问企业资源。显然，移动性可能使网络遭受极具破坏性的攻击和数据泄露，并由此给组织造成巨大的经济损失。但是当今的移动员工需要随时随地工作，以保持竞争力和工作效率。在这种扩展网络的复杂性不断增加的同时，“物联网”逐渐兴起，各种支持网络功能的设备连接至私有和公共网络，导致无法识别网络安全威胁并采取补救措施的潜在影响急剧增加。

此外，IT 专业人员必须在更紧张的预算内支持企业移动性计划，同时遵守政府、行业和其他合规性要求。要满足这些要求乃至更多要求，就必须清楚地了解网络访问并严格实施访问控制。安全点解决方案通常被大量分布并部署在整个企业网络中。这类解决方案侧重于在威胁出现时识别威胁，或在发生泄露或攻击后协助进行取证调查。将防止受影响的设备或用户访问网络放在首位的安全解决方案通常涉及复杂、耗时且昂贵的部署。随着您的网络不断发展和扩展，这些互无联系的安全点解决方案无法足够快地进行相应的扩展。必须对不断发展的移动性企业环境采用一种兼顾管理性和安全性的新方法。这种方法便是思科身份服务引擎 (ISE)。

功能和优势

Cisco ISE 为实现网络访问安全提供了一种更全面的方法，它具有以下特性：

- 可准确识别每一位用户和每一台设备
- 使所有设备的自注册和调配变得简单
- 提供集中的情景感知型策略管理来控制用户访问 - 覆盖任何人、任何时间，以及任何设备
- 提供有关已连接用户和设备的更深入的情景数据，以便更快地识别和缓解威胁，并采取补救措施

在网络中运营时，客户可通过部署 Cisco ISE 获得表 1 所示的优势。

表 1. 客户可以获得的主要优势

Cisco ISE 的优势	
强大的设备分类	Cisco ISE 提供业内首款集成的设备分析器，该分析器不仅能够识别每个终端，将终端与其用户或功能及其他属性（包括时间、位置和网络）相匹配，而且能创建情景身份，从而使 IT 能够精确控制允许访问网络的人员和允许访问的内容。自动设备馈送服务会实时更新 Cisco ISE，以确保新设备在上市后能够尽快得到识别。
广泛的策略实施	Cisco ISE 使组织能够轻松且非常灵活地定义访问策略规则，以满足企业不断变化的业务要求。例如，在 Cisco ISE 中，IT 管理员可以定义策略来区别对待访客用户和访客设备与注册用户和注册设备。访客用户可能会获得整个网络的有限访问权限，注册用户则能获得其相应策略指定的访问权限。此外，Cisco ISE 中的策略可保证只有注册用户的受信任设备或合规设备才能访问网络。Cisco ISE 会根据用户或设备的情景身份向网络进入点发送高度安全的访问规则，这样，IT 人员就可以在用户或设备尝试访问网络的任何位置确保策略实施的一致性。

Cisco ISE 的优势	
简化的访客体验	Cisco ISE 提供开箱即用的访客管理和自注册功能，十分方便。管理员可使用动态的可视化工具在几分钟内自定义访客门户，该工具可实时预览访客所看到的门户屏幕和所要经历的步骤，以便准确展示设置的变化会如何影响到用户。Cisco ISE 支持完全自定义访客页面（包括广告、横幅、主题和品牌）、全面管理访客帐户和到期日期，以及全面审核整个网络中的访客帐户和活动。Cisco ISE 支持所有可能的访客工作流程类型（从热点接入，到员工发起的采用短信确认方式的访客接入），使访客接入变得十分轻松。
自助式设备自注册	Cisco ISE 使 IT 人员可以灵活决定如何实施企业的自带设备 (BYOD) 或访客策略。Cisco ISE 为用户提供自助式注册门户，以便根据 IT 自动定义的业务策略注册和调配新设备。这样一来，IT 能够实现自动化的设备调配、分析和安全评估来满足符合安全策略的需要，同时确保极致简化，让员工可在无需 IT 帮助的情况下将设备接入网络。
安全合规性	单一管理控制台简化了所有公司网络中的策略创建、可视性和报告，对审计要求、监管要求，以及 IEEE 802.1X 标准的联邦政府强制性准则的合规性验证将变得简单轻松。
自动化的设备合规性检查	Cisco ISE 使用 Cisco AnyConnect® 4.0 Unified Agent 提供设备安全状态检查和补救选项。Cisco AnyConnect® 4.0 Unified Agent 还提供用于检查台式机和笔记本电脑的高级 VPN 服务，并支持与市场领先的面向移动设备的企业移动性管理 (EMM) 解决方案相集成。此功能有助于确保用户的设备既安全又符合策略要求。
可靠的随时随地访问	Cisco ISE 可实时调配有关网络接入设备的策略，使移动用户或远程用户能够通过无线连接获得与有线连接一致的服务访问体验。
运营效率	Cisco ISE 可提供自注册和安全自动化、集中策略控制、可视性、故障排除以及与 Cisco Prime™ 解决方案集成，有助于大幅减少 IT 和服务中心在解决用户和网络安全问题上所需的时间。
嵌入式实施	大多数思科交换机和无线控制器中都内置设备传感功能，可在进入点将分析信息扩展到整个网络，而无需购买和管理重叠设备或更换基础设施。
使用 Cisco TrustSec® 策略网络功能将策略从接入扩展到数据中心	Cisco ISE 是适合独特的 Cisco TrustSec 网络技术的策略管理点，它提供策略定义的网络分段，以消除网络安全的复杂性。借助 Cisco TrustSec 技术，用户可以使用基于角色的访问策略，根据业务规则轻松地以符合逻辑的动态方式对其网络进行分段，而不是管理多个 VLAN 或不断变化的网络架构，从而在不断变化的扩展网络上轻松实现高度安全的访问。
多供应商基础设施支持	Cisco ISE 可与符合 RADIUS 和 IEEE 802.1X 标准的多供应商基础设施互通。思科及其合作伙伴可提供最佳实践指导以及详细的实际设计指南。企业客户可结合使用 Cisco ISE 与思科设计的网络基础设施及 Cisco TrustSec 技术，以便从其网络中获取更丰富的情报，并获得更强的网络可视性。
Cisco pxGrid 情景共享	Cisco ISE 可从整个网络中收集动态的情景数据，并利用 Cisco pxGrid 技术（一个强大的情景共享平台）与外部和内部生态系统合作伙伴解决方案共享有关已连接用户和设备的更深层次的情景数据。Cisco ISE 网络和安全合作伙伴通过使用单个 API 来利用这些数据，以改善其各自的网络接入功能，并使其解决方案能够更快地识别和缓解网络威胁，并采取补救措施。
广泛、集成的合作伙伴生态系统	Cisco ISE 拥有最广泛的合作伙伴生态系统。合作伙伴使用 Cisco pxGrid 改善其终端设备漏洞补救、网络取证调查和网络单点登录 (SSO)。EMM、安全信息和事件管理 (SIEM) 以及威胁防御 (TD) 的集成技术合作伙伴均利用 Cisco ISE 提供的深入情景身份感知功能，来应对比他们可以单独应对的使用案例更多的使用案例，从而更有效地履行其职责。利用 Cisco ISE，合作伙伴平台可深入挖掘思科网络基础设施，并对用户和设备执行网络操作（例如隔离智能手机或笔记本电脑，以及阻止网络访问）。

Cisco ISE 通过提供全面的策略管理、简化的设备自注册过程、可与合作伙伴共享的丰富情景数据以及动态的策略实施，来帮助确保高度安全的有线、无线和 VPN 接入，从而增强企业的能力。Cisco ISE 的功能和优势如表 2 所示。

表 2. 功能和优势

功能	优势
业务策略实施	提供一个基于规则的、属性驱动的策略模型，用以创建具有业务相关性的灵活访问控制策略。通过从预定义字典（包括用户和端点身份、安全状态验证、身份验证协议、分析身份或其他外部属性来源的信息）中提取属性，从而创建精细策略。也可动态创建属性，并保存属性以备日后使用。 可与多种外部身份库（例如 Active Directory、LDAP、RADIUS、RSA OTP 以及用于身份验证和授权的证书授权）集成。
访问控制	使用 Cisco TrustSec 技术支持的网络设备的高级功能提供各种访问控制选项，包括可下载访问控制列表 (dACL)、VLAN 分配、URL 重定向、指定的 ACL 和安全组标签 (SGT)。

功能	优势
访客生命周期管理	提供简化的全新体验，以支持和自定义访客网络接入。凭借对热点接入、终端发起的接入、自助式接入及其他许多接入工作流程提供的内置支持，ISE 使用户可以轻松地在几分钟内创建公司品牌（带有广告和促销信息）的访客体验。新的访客管理工作中心提供实时的可视化流程，将您的设计效果展现在您的眼前。时间限制、帐户到期日期和短信验证提供额外的安全控制，全面的访客审计可以在您的网络中跟踪访问，以满足安全和合规性要求。
简化的设备自注册过程	使用主题提供可完全自定义的品牌用户体验。提供开箱即用的工作流程，这些工作流程可引导用户完成自注册过程，并向最终用户提供其各自的自助服务门户，用于添加和管理其设备。为标准的 PC 和移动计算平台提供自动化的 Supplicant 调配和证书注册。通过精简设备自注册过程减少 IT 服务中心支持请求，并为用户提供更安全的访问和更轻松、更透明的体验。
AAA 协议	使用标准的 RADIUS 协议进行身份验证、授权和记账 (AAA)。支持多种身份验证协议，包括（但不限于）PAP、MS-CHAP、可扩展身份验证协议 (EAP)-MD5、受保护的 EAP (PEAP)、通过安全隧道的 EAP 灵活身份验证 (FAST) 以及 EAP 传输层安全 (TLS)。Cisco ISE 是唯一支持机器与用户凭证的 EAP 链路的 RADIUS 服务器。
内部证书授权	在 Cisco ISE 内为组织提供易于部署的内部证书授权，以简化个人设备的证书管理，而不会显著增加外部证书授权申请的复杂性。Cisco ISE 提供用于管理终端设备及其证书的单一控制台，能够通过基于标准的在线证书状态协议 (OCSP) 检查证书状态，并且可在设备失窃时自动吊销证书。内部证书授权支持独立和从属（即与您现有的企业 PKI 一起）部署。
设备分析	附带了适用于各种终端（如 IP 电话、打印机、IP 摄像机、智能手机和平板电脑）的预定义设备模板。此外，管理员还可以创建属于自己的设备模板。端点连接至网络时，这些模板可用于自动检测、分类和关联管理员定义的身份。管理员还可以根据设备类型关联端点特定的授权策略。 Cisco ISE 通过被动网络监控和遥感勘测来收集终端属性数据，具体方式包括直接查询实际终端，或者通过 Cisco Catalyst® 交换机上的设备传感器从思科基础设施进行查询。 Cisco ISE 传感技术包含 Cisco Catalyst 交换机具有的由基础设施驱动的终端传感功能。利用这项功能，交换机能够快速收集终端属性信息，然后使用标准 RADIUS 将此信息传送至 Cisco ISE，以便执行终端分类和基于策略的实施。这种基于交换机的传感功能可更有效地分发终端信息，从而改善可扩展性、可部署性和分类时间。
设备配置文件馈送服务	Cisco ISE 提供的业内首个设备配置文件馈送服务支持开箱即用的分析技术，方法是为来自多家供应商的各种支持 IP 的设备自动更新思科已验证的设备配置文件。馈送服务还提供了一种机制，合作伙伴和客户可通过该机制共享各自的自定义配置文件信息，以便思科审核和重新分发。由于这些自动更新功能，企业可在用户尝试连接到网络时检测所有最新的设备。这不仅使紧跟不断出现的大量新设备变得更加简单，而且能大幅减少 IT 管理员的支持任务。
终端状态	验证连接网络的 PC 和移动设备的终端状态评估。通过基于客户端的永久代理或临时网络代理进行操作，以验证终端是否符合企业的状态策略。可创建强大的策略，包括（但不限于）使用当前的定义文件变量（版本、日期等）、注册表（项、值等）和应用来检查是否有最新的操作系统补丁、防病毒软件包和反间谍软件包。此外，Cisco ISE 还支持自动补救 PC 客户端和定期重新评估，以确保终端未违反公司策略。
Cisco pxGrid 和 ISE 生态系统	Cisco pxGrid 是 Cisco ISE 内的一个强大的情景共享平台，它将 Cisco ISE 收集的更深层次的情景数据提供给外部和内部的生态系统合作伙伴解决方案，以便这些解决方案在在整个网络中更快地执行其功能。从终端漏洞评估到网络单点登录，利用简单的统一框架的 Cisco ISE 生态系统合作伙伴的名单不断扩大。
ISE 生态系统：EMM 集成	EMM 集成使 Cisco ISE 能够与 Cisco EMM 技术合作伙伴解决方案连接，从而帮助确保正在尝试连接至网络的移动设备之前已经向 EMM 注册，并且符合企业策略。它还有助于用户对其设备采取补救措施。合规性检查包括（但不限于）检查设备加密、PIN 锁和越狱状态。
ISE 生态系统：SIEM 和 TD	通过与 Cisco ISE 集成，SIEM 和 TD 合作伙伴可获悉有关用户及设备身份、网络授权级别以及安全状态的 Cisco ISE 情景信息，进一步增加他们对整个网络的安全事件的可视性。出现这种变革后，合作伙伴能够从数月的取证事件追查到异常设备，从中获得实时可视性，并制定可直接从管理员面板内部执行的安全措施。
ISE 生态系统：控制/SCADA 运营和安全策略集成	实现高度安全地访问和管理控制以及监控与数据收集 (SCADA) 网络设备。Cisco ISE 为控制和 SCADA 策略管理器提供情景和控制，
ISE 生态系统：简化的网络故障排除和取证调查	允许数据包捕获系统使用 Cisco ISE 收集的情景数据将用户、设备和用户角色与捕获的数据包数据关联。由于数据包捕获对于调查威胁和网络问题至关重要，因此将情景数据与数据包捕获相关联可简化网络故障排除和加快取证调查。
ISE 生态系统：终端漏洞补救集成	了解如何在网络漏洞报告上确定优先顺序以及确定优先顺序的对象非常困难。将来自 Cisco ISE 的情景数据与漏洞报告共享可更好地识别和优先处理需要调查的终端漏洞，并帮助用户采取措施以便快速补救。
ISE 生态系统：基于风险的自适应身份验证和单点登录	启用情景驱动的用户身份验证和网络应用授权。可根据 Cisco ISE 提供的联合身份、身份验证风险因素和情景数据组合来精细策略，减少甚至完全消除身份验证挑战。随着员工用来访问企业资产的移动设备数量激增，用户身份验证（虽然对安全至关重要）变得极其繁琐。此集成使用户能够对企业资产透明地进行身份验证，而无需重复挑战，同时根据风险级别阻止对云资产的访问。

功能	优势
广泛的多林 Active Directory 支持	Cisco ISE 提供对多林 Microsoft Active Directory (AD) 域的全面身份验证和授权。它可以将多个分散的域分组到逻辑组，以简化配置复杂的 AD 拓扑，从而支持不断变化的业务环境。Cisco ISE 还支持灵活的身份改写规则，以便实现顺利过渡和集成。 支持 Microsoft AD 2003、2008、2008R2、2012、2012R2。
终端保护服务	使管理员能够对网络中存在入侵风险的终端快速采取纠正操作（隔离、解除隔离或关机）。这样有助于减少网络危险，增强安全性。
集中管理	允许管理员在一个基于网络的 GUI 控制台上集中配置和管理分析器、状态、访客、身份验证和授权服务，并从单一虚拟管理平台提供集成管理服务，从而大大简化了管理。
监控和故障排除	包括具有监控、报告和故障排除功能的内置网络控制台，用于帮助服务中心和网络操作人员快速识别和解决问题。提供所有服务的全面历史和实时报告、所有活动的记录以及连接至网络的所有用户和终端的实时控制面板指标。
平台选择	可作为物理或虚拟设备使用。具体包括两个物理平台以及一个基于 VMware ESX 或 ESXi 的设备。物理和虚拟设备都可用来构建 Cisco ISE 集群，以便为较大型的组织服务，并提供关键企业业务系统所需的必要扩展、冗余以及故障转移能力。

产品规格

表 3 中列出了两个适用于 ISE 的硬件选项。

表 3. Cisco ISE 硬件规格

	思科安全网络服务器 3415（小）	思科安全网络服务器 3495（大）
处理器	1 个 Intel® Xeon® 四核 2.4 GHz E5-2609	2 个 Intel Xenon 四核 2.4 GHz E5-2609
内存	16 GB	32 GB
硬盘	1 个 600 GB 6 Gb SAS 10K RPM	2 个 600 GB 6 Gb SAS 10K RPM
RAID	否	有 (RAID 1)
CD/DVD-ROM 驱动器	否	否
网络连接		
以太网卡	4 个集成的千兆网卡	4 个集成的千兆网卡
10/100/1000BASE-TX 电缆支持	5 类 UTP，最长 328 英尺 （100 米）	5 类 UTP，最长 328 英尺 （100 米）
安全套接层 (SSL) 加速卡	无	Cavium CN1620-400-NHB-G
接口		
前面板连接器	1 个 KVM 控制台连接器（提供 2 个 USB、1 个 VGA、1 个串行连接器）	1 个 KVM 控制台连接器（提供 2 个 USB、1 个 VGA、1 个串行连接器）
额外的后面连接器	额外接口包括一个 VGA 视频端口、两个 USB 2.0 端口、一个 RJ45 串行端口、1 GB 以太网管理端口以及双 1 GB 以太网端口	额外接口包括一个 VGA 视频端口、两个 USB 2.0 端口、一个 RJ45 串行端口、1 GB 以太网管理端口以及双 1 GB 以太网端口
系统部件		
外形	机架式安装，1 机架单元 (1RU)	机架式安装，1 RU
重量	35.6 磅 （16.2 千克） 26.8 磅 （12.1 千克）	35 磅 （15.87 千克）完全配置
尺寸（高 x 宽 x 长）	1.7 x 16.9 x 28.5 英寸 （4.32 x 43 x 72.4 厘米）	1.7 x 16.9 x 28.5 英寸 （4.32 x 43 x 72.4 厘米）
电源	650W	双 650W（冗余）
散热风扇	5	5
温度：工作	32 至 104°F (0 至 40°C)（运行中、海平面、无风扇故障、没有 CPU 限制、加速模式）	32 至 104°F (0 至 40°C)（运行中、海平面、无风扇故障、没有 CPU 限制、加速模式）
温度：非工作	-40°C 至 70°C（-40°F 至 158°F）	-40°C 至 70°C（-40°F 至 158°F）

平台支持和兼容性

VMware ESX/ESXi 4.x 和 5.x 支持 Cisco ISE 虚拟设备，运行该设备的硬件配置不得低于表 3 中所列的物理平台配置。Cisco ISE 要求虚拟目标提供至少 4 GB 的内存和至少 200 GB 的可用硬盘空间。

安全状态评估系统要求

以下是用于状况评估的 Cisco AnyConnect 4.0 Agent 的系统要求：

- Microsoft Windows 7、8 或 8.1（32 位或 64 位）
- Mac OS X 10.7、10.8 或 10.9

订购信息

如需下订单，请访问思科订购主页。要下载 Cisco ISE 软件，请访问思科软件中心。

服务与支持

思科提供各种服务计划。这些创新型计划通过将人员、流程、工具及合作伙伴
巧妙结合来实现，可大幅提升客户的满意度。思科服务有助于保护您在网络上的投资，优化网络运营，并合理地配置您的网络，通过使用新的应用来增强网络智能并拓展您的业务能力。有关思科服务的更多信息，请参阅思科技术支持服务或思科安全服务。

如需了解保修信息，请访问：http://www.cisco.com/go/warranty。有关许可信息，请访问：http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-licensing-information-listing.html。

更多详情

如需了解有关 Cisco ISE 和 Cisco TrustSec 解决方案的详情，请访问 http://www.cisco.com/go/ise 或与您当地的客户代表联系。

美洲总部
思科系统公司
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。

美国印刷 C78-656174-09 10/14