

思科身份服务引擎

简介

传统企业网络边界和孤岛式服务已经是过去的事情了。今天的网络在提供以用户为中心的策略并支持全球协作的同时，还必须适应日益增多的消费 IT 设备。思科 TrustSec® 架构通过使用基于身份的访问策略来应对这种转变，让您知道连接至您网络的用户和设备，使 IT 部门能够启用相应的服务而又不失控制。

Cisco® 身份服务引擎 (ISE) 侧重于对思科 TrustSec（无边界网络整体方案的一部分）提供全面服务支持。身份辨认服务引擎在一个通用平台上提供了企业网络所需的所有必要服务：AAA、分析、状态和访客管理。作为 SecureX 框架的核心组件，思科身份服务引擎提供了一个统一策略平台。该平台将组织安全策略与安全和网络基础设施、用户身份、资源和 IT 操作流程等业务组成部分关联在一起。思科 ISE 允许客户创建和管理集中策略，而思科 TrustSec 可通过网络提供策略和实施。

概述

思科 ISE 是一个基于身份的情景感知平台，可从网络、用户和设备收集实时信息。然后，ISE 通过利用基于标准的内置控件在网络基础设施内实施策略，使用这些信息来做出主动的监管决策。思科 ISE 可提供：

- 安全：通过实时查看和控制网络中的用户和设备确保网络安全。

- 合规性：通过在基础设施内创建一致的策略进行有效的企业监管。
- 效率：通过使传统的劳动密集型任务实现自动化并简化服务交付来帮助提高 IT 和网络员工的工作效率。
- 推动：允许 IT 部门通过启用策略的服务支持一系列新业务计划，例如自带设备 (BYOD)。

解决方案优势

- 与业务相关的策略：支持从总部到分公司在整个公司基础设施内进行集中化、协作式的策略创建和一致的策略实施。
- 系统范围内的运营可视性：发现、评估和监控用户和端点并利用高级故障排除功能，使 IT 团队能够全面查看接入公司网络的用户和设备。

图 1. ISE 的主要优势





- **情景感知实施**：从用户、设备、基础设施和网络服务收集信息，使各个组织在整个网络内实施基于情景的业务策略。思科身份服务引擎用作情景丰富的身份属性（包括连接状态、用户和设备身份、位置、时间和端点运行状况）的“唯一信息来源”。
- **最高精确度的设备分析**：将基于 ISE 的被动网络探测和策略驱动的主动端点扫描工作以及基于思科基础设施的设备传感器功能相结合，可以为 IT 部门提供所需的端点保真度以及完整网络感知和基于设备类型的自动网络支持所需的简化分析功能。
- **灵活的服务架构**：将 AAA、状态、分析和访客管理功能整合在一个设备平台中。思科身份服务引擎可以在整个企业基础设施内进行部署，从而应用支持 802.1x 有线、无线和 VPN 网络的适当服务。
- **通过 IT 自动化提高了运营效率**：使用户能够按照 IT 部门定义的策略进行自助注册和调配，从而自己负责登记他们的设备。提供发起人驱动的访客接入、自动设备分类、自动化端点登记和门户驱动的设备注册等功能，使 IT 部门可以将更多的时间用在其他任务上，并使用户能更灵活地选择他们的工作方式。
- **MDM 集成**：思科与领先的 MDM 供应商合作，使 IT 组织能够根据用户和设备来启用相应的应用程序和服务，并能根据公司定义的策略更清楚地查看以及更好地控制端点访问。在 2012 日历年的后半年可用。

部署组件

身份服务引擎是使用思科网络设备将访问实施延伸到整个网络的基于基础设施的思科 TrustSec 部署的一部分。其他部署组件包括端点上的思科 NAC Agent 和思科 AnyConnect™（或本地 802.1X Supplicant 客户端）；充当局域网策略实施点的思科 Catalyst® 交换机和思科无线局域网控制器；以及用于安全远程访问的思科自适应安全设备。

思科身份服务引擎还与 Microsoft Active Directory 和 Sun ONE Directory Server 等目录服务相集成来作为策略信息点。将来，思科 ISE 还将与作为外部策略信息点、业界领先的 MDM 供应商相集成。

图 2. 思科 TrustSec 解决方案架构的组件



包装和许可

思科身份服务引擎可用作物理设备或虚拟设备。许可选项允许客户根据网络中的活动端点数选择他们需要的功能。

根据环境和策略，现有 ACS 和 NAC 客户可以考虑迁移至 ISE。ISE 是 ACS 和 NAC 产品组合当前提供的端点访问服务的自然发展，因此，思科已经相应地将 ISE CAPEX 迁移成本降至最低。



许可

基础许可证适用于想要在其网络（有线、无线和 VPN）中对用户和设备进行身份验证和授权的组织。基础许可证支持 AAA 服务、访客生命周期管理、合规性报告以及端到端监控和故障排除。

高级许可证扩展了基础许可证的功能，使组织能够根据更丰富的用户和设备情景信息，做出更超前的策略决策。高级许可证功能包括自动化端点登记、设备分析、终端安全评估以及安全组访问 (SGA) 实施功能。

无线许可证适用于只想为无线端点启动身份服务引擎部署的组织。无线许可证可说是基础许可证和高级许可证的预定义捆绑包。无线升级许可证允许开始仅采用无线端点的客户将其部署扩展到有线和 VPN 端点。

图 3. 思科 ISE 许可和包装选项



为什么选择思科身份服务引擎?

市场领先地位:

- 就客户部署而言，市场份额最大。
- 被行业领先的分析公司连续评为行业第一，包括在 2011 年 12 月发布的 Gartner NAC Magic Quadrant 报告中被评选为领导者。
- 由开创了原始网络访问控制技术并开发出众多行业标准的公司创建而成。
- 当今独有的综合性单供应商解决方案。

技术和解决方案领先:

- 以独特的方式将 AAA、状态、分析和访客管理功能整合在一个统一设备中，从而实现简化的部署和集成式管理。
- 依靠用于简化咨询台和支持团队操作的一流监控和故障排除功能，可大大降低拥有成本。
- 通过与 SGA 等嵌入式基础设施功能集成在一起的方法提供了全面的安全功能。

更多详情

有关思科身份服务引擎的详情，请访问 <http://www.cisco.com/go/ise>。有关思科 TrustSec 以及构成思科 TrustSec 解决方案的全部产品的详情，请访问 <http://www.cisco.com/go/trustsec>。