

思科IQ虚拟设备版本说明v1.2.4

简介

Cisco IQTM为客户提供的功能旨在提高资产可视性，并在整个环境中提供更智能的见解。此外，AI Assistant等AI功能通过提供情景理解来优化运营成果和思科IQ用户体验，使用户能够主动做出明智的决策，并简化客户参与和成功的流程。

Cisco IQ On-Prem Air-Gapped是Cisco IQ的部署模式，专为无法连接到云的环境而构建。它作为独立的虚拟机(VM)(称为Cisco IQ Virtual Appliance(VA))提供，完全在客户现场运行，与外部网络完全隔离，软件更新和维护包从Cisco IQ SaaS获得，并通过经过批准的手动流程传输到VA。

对于在受监管、高度安全和主权环境中运营的组织，VA消除了见解和控制之间的权衡。客户在自己的网络内部署思科智能资产与评估功能，并保留对数据的完全所有权，同时仍可获得期望从思科智能获得的见解和建议。气隙部署模式将Cisco IQ SaaS的功能扩展到隔离环境，使任务关键型团队能够以云连接企业的速度和诊断智能进行操作。

本文档概述了Cisco IQ VA v1.2.4的新功能、模块支持和已知问题。

主要亮点

资产模块

资产模块为思科资产提供全面的可视性和管理功能，是思科IQ的基础，可提供组织内所有设备的集中列表。通过从多个来源收集信息，它可以作为设备资产的一个单一数据源。它是下载安装程序的一部分，安装VA后即可使用。主要亮点包括：

资产重要程度见解

资产重要程度分析使资产模块能够预测网络设备的功能角色和业务重要性。通过分析设备配置和启用的功能，Asset Criticality Insights可帮助您确定哪些资产对网络的影响最大，从而让您能够针对安全补救、软件升级、寿命终止/支持终止规划和覆盖范围决策确定资产的优先级。

服务合同

Service Contracts页面对支持合同进行集中监督。关键功能包括：

- 服务合同监督:通过全面的合同摘要和详细数据简化续约规划和覆盖战略
- 特定资产见解:通过直接链接到您的资产的清晰、可操作的数据，更快地发现并缓解漏洞

LDOS控制面板

最后支持日期(LDOS)控制面板提供LDOS里程碑的集中视图，并允许在硬件或软件达到寿命终止之前改进资产规划和预算预测，从而显著降低运营风险。

资产标记

资产标记提供了一种使用自定义标签灵活地组织、过滤资产并对其执行操作的方法。标签可以创建、修改并分配到资产，帐户管理员可以集中管理标签。您可以将标签分配给个别资产或批量分配，也可以按标签过滤资产以快速找到所需的资产。

评估模块

“评估”模块通过评估贵组织的资产提供对资产的可视性，并提供一个框架，使您能够主动调查并降低与安全性、稳定性、容量、合规性和老化相关的风险，帮助保持网络安全。主要亮点包括：

Security Advisories

集成安全建议使您能够防患于未然。系统主动发现相关漏洞，确保您及时了解关键更新，并立即采取措施保护您的网络。

安全强化

安全强化可根据Cisco OS强化指南持续评估您的资产，从而自动实时了解网络基础设施的安全状态。每个安全强化规则都会在您覆盖的资产中进行评估，以检测配置偏差，并将结果按严重性进行优先排序，以帮助您解决安全差距、增强恢复能力并降低运营风险

配置

根据思科久经考验的专业知识，根据建议的最佳实践来评估您的资产，以检测您的整个基础设施中可能影响可用性、安全性或性能的配置偏差。系统跨所覆盖的资产评估每个最佳实践规则，按严重程度排列发现结果的优先级，以帮助您确保配置一致性、增强可复原性并降低运营风险。

Field Notices

现场通知提供有关硬件和软件更新的及时、主动通知。通过直接在“评估”控制面板中展示相关的现场通知，此功能使您能够在潜在问题影响操作之前解决它们。

AI支持的功能

思科IQ VA提供AI支持的功能，将SaaS级AI见解直接融入您的空调环境中。它通过将原始数据转化为切实可行的见解、建议和指导性行动，提升思科的智商。AI支持的功能需要配备支持的图形处理单元的节点。这些功能不能在仅CPU部署上启用。功能包括：

- 询问AI界面：直接在资产和资产模块中访问AI驱动的交互式见解。
- LDOS：可以浏览预定义提示列表，以获取摘要、识别关键资产或分析LDOS资产的产品系列
- 主要见解:将资产和评估数据转化为切实可行的见解和建议。集成到工作流程中，提供实时见解和报告

软件生命周期管理

您可以管理VA内运行模块、规则、授权和专门的AI支持的功能的软件生命周期（安装和配置）。您可以通过导航到系统设置>软件包目录从Cisco IQ(SaaS)下载最新版本来安装它们。

Cisco IQ连接器

Cisco IQ VA配备全面的Cisco IQ连接器，支持从直接连接设备和通过Cisco Catalyst Center管理的设备进行灵活的遥测数据收集，从而增强网络可视性和管理。主要亮点包括：

定义设备

Cisco IQ VA提供灵活的选项来定义您的设备范围。您可以通过上传CSV文件、手动输入逗号分隔列表、使用IP范围或利用CDP（思科发现协议）或LLDP（链路层发现协议）来指定设备。可随时更新此列表以添加或删除设备，确保设备组保持最新状态。

安排发现和收集

Cisco IQ VA支持发现和收集过程的独立调度，支持特定日期、时间和重复模式。您可以单独配置这些任务，使其与运营工作流程保持一致。此外，您可以随时对单个设备执行按需重新发现，从而更好地控制数据刷新周期，加快故障排除响应时间。

支持的虚拟机监控程序

Cisco IQ VA支持在以下虚拟机监控程序平台上部署。在开始部署之前，请确保您的基础设施满足特定虚拟机监控程序的最低版本要求。

- VMware ESXi:标准虚拟化环境支持
- Microsoft Hyper-V Server：支持基于Windows的虚拟化堆栈
- 基于Red Hat内核的虚拟机：支持开源虚拟化环境

非HA多节点支持

Cisco IQ VA支持非高可用性(HA)多节点架构，为您的部署环境提供更高的可扩展性和灵活性。多节点提供分布式架构，将管理和员工功能分开，让您能够定制和扩展基础设施，使其超越单个虚拟资产，以满足更大、更复杂的工作负载的需求。管理节点用作群集注册、平台安装和安装后监控的主要接口。

用户管理

以下功能旨在简化用户管理流程，为系统中的用户提供更好的控制和安全性。

本地用户管理

用户可以安全地加入并管理具有不同访问权限的多个用户。管理员创建的本地用户可以在首次登录时使用Sign Up选项，并使用管理员配置的电子邮件地址安全地设置自己的密码。

自助服务安全管理

现在，您可以独立管理本地安全设置，从而控制帐户访问和恢复。自助服务功能包括重置忘记的密码和配置安全问题的功能，无需外部支持即可提供更精简的安全用户体验。

安全SSO的SAML配置

Cisco IQ VA通过集成安全断言标记语言(SAML)v2.0身份验证支持安全单点登录(SSO)功能。此集成可实现与第三方身份提供程序(IDP)的无缝身份联合，允许您使用现有企业凭证进行身份验证。通过利用SAML v2.0，组织可以在其环境中增强安全性、简化用户访问并简化身份管理。在任何给定时间只能有一(1)个IDP处于活动状态。当前支持以下IDP:

- Okta IDP
- ADFS IDP
- Entra IDP

活动日志

所有操作日志都存储在本地，并且帐户管理员可以查看这些日志，从而轻松监控用户活动并确保透明度。

支持安全和标准NTP

Cisco IQ VA同时支持安全和标准网络时间协议(NTP)。安全NTP在Cisco IQ VA和可信NTP服务器之间启用经过身份验证和加密的时间同步，而标准NTP为加密NTP交换不要求或不支持身份验证的环境提供同步。

自定义SSL证书支持

Cisco IQ VA支持自定义SSL证书的安装和管理。此功能允许帐户管理员使用其组织的证书颁发机构(CA)颁发的证书替换默认证书。通过使用自定义证书，您可以确保安全、可信的通信，并完全遵守组织的内部安全策略。目前，在任何给定时间只能安装并激活一(1)个SSL证书。

支持外部系统日志服务器

Cisco IQ VA支持与外部系统日志服务器集成，使帐户管理员能够将系统日志转发到集中日志记录平台。此增强功能提供跨整个基础设施的系统事件和安全日志的持续、整合视图，从而简化监控、审计和故障排除。在任何指定时间最多可以配置两(2)台系统日志服务器。

登录和自定义横幅

Cisco IQ VA现在提供可配置的横幅功能。帐户管理员可以在登录屏幕上配置并显示强制性系统通知和安全警告。此外，帐户管理员可以配置和显示思科IQ VA上的自定义横幅。此功能支持直接向Cisco IQ VA内的用户传达重要信息（例如，通知、免责声明或警报）。

系统管理

您可以通过System Management选项卡查看和安装最新的Cisco IQ VA更新，从而轻松访问最新的功能、改进和增强功能。Cisco IQ VA支持从Cisco IQ推送的自动软件更新和手动软件更新。对于手

动更新，您可以通过导航到系统设置>软件包目录，直接从Cisco IQ(SaaS)下载软件包。

已知问题

Cisco IQ VA积极解决以下问题。

Recurring Schedule字段显示UNIX Cron语法

目前，用于网络扫描文件上传的周期性计划输入需要一个包含五(5)个字段的UNIX cron表达式（例如，"0 2 * * *"）。不熟悉cron语法的用户可能会发现此输入格式不明确。但是，用户可以在线获得有关cron语法和示例的详细信息。

大规模部署中少数设备的间歇性资产收集故障

目前，在超过10,000台设备的部署中，尽管发现过程成功，但一小部分设备可能无法执行资产收集。对此的解决方法是，从系统中删除故障设备，然后重新添加。如需其他帮助，请联系思科技术支持中心(TAC)。

授权上传状态在收集期间不可见

目前，上传授权文件后，UI中没有任何明确指示已成功加载和处理授权。在权利得到完全处理之前开始收集可能会导致覆盖失败。解决方法是，在上传后至少等待一(1)小时，然后运行收集。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。