思科安全访问控制系统 5.6 版本说明

修订日期：7 15, 2016

这些版本说明涉及思科安全访问控制系统 (ACS) 版本 5.6（以下简称 ACS 5.6）。此版本说明介绍 Cisco Secure ACS 的功能、限制和约束（警告）以及相关文档，是对产品硬件和软件版本附带的 Cisco Secure ACS 文档的补充。

本文档包括以下内容：

简介

ACS 是一款策略驱动型访问控制系统，是网络访问控制和身份管理的集成点。

ACS 5.6 软件可在专用的思科 SNS-3495 设备、思科 SNS-3415 设备、思科 1121 安全访问控制系统 (CSACS-1121) 或 VMware 服务器上运行。思科 SNS-3495 和思科 SNS-3415 设备附带 ACS 5.6。但是，ACS 5.6 仍支持 CSACS-1121 设备。您可从在 CSACS-1121 设备上运行的任何较早的 ACS 版本升级到 ACS 5.6。有关升级路径的更多信息，请参阅升级 Cisco Secure ACS 软件（第 8 页）。

此 ACS 版本提供新增和增强的功能。在本文档中，思科 SNS-3495、思科 SNS-3415 和 CSACS-1121 是指设备硬件，而 ACS 服务器是指 ACS 软件。

注 在每个主要版本中，思科都会对 ACS 应用运行安全扫描。我们不建议您在 ACS 生产环境下运行漏洞扫描，因为这样操作可能会带来影响 ACS 应用的风险。您可以在预生产环境下执行漏洞扫描操作。

系统要求

注 有关 Cisco Secure ACS 硬件平台和安装的更多详细信息，请参阅《思科安全访问控制系统 5.6 的安装和升级指南》。

支持的硬件

Cisco Secure ACS 封装在您的设备或映像中以便于安装。以下平台附带 Cisco Secure ACS 5.6：

表 1　　支持的硬件平台

硬件平台	配置
思科 SNS-3495-K9 （大型 UCS）	• 思科 UCS C220 M3 • 双插槽 Intel E5-2609 2.4Ghz 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 SNS-3415-K9 （小型 UCS）	• 思科 UCS C220 M3 • 单插槽 Intel E5-2609 2.4Ghz 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
思科 1121 安全访问控制系统硬件 (CSACS-1121)	• Intel Core 2 Duo 2.4 GHz 处理器，带 800 MHz 前端总线 (FSB) 和 2 MB 第 2 层缓存 • 4 GB SDRAM • 2 个 250 GB SATA 硬盘 • 4 个 1 GB 网络接口
Cisco Secure ACS-VM-K9 (VMware)	• 2 个 CPU（双 CPU、Xeon、Core2 Duo 或 2 个单 CPU） • 4 GB RAM • NIC - 需要 1 GB NIC 接口（最多可以安装 4 个 NIC。） • 有关支持的 VMware 版本，请参阅支持的虚拟环境 有关 VMware 要求的信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》。

支持的虚拟环境

ACS 5.6 支持以下 VMware 版本：

- VMware ESXi 5.0
- VMware ESXi 5.0 更新 2
- VMware ESXi 5.1
- VMware ESXi 5.1 更新 2
- VMware ESXi 5.5
- VMware ESXi 5.5 更新 1

有关 VMware 计算机的要求和安装流程的信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》中“在 VMware 虚拟机中安装 ACS”一章。

支持的浏览器

您可以使用以下浏览器访问 ACS 5.6 管理员用户界面：

- Mac 操作系统
  - Mozilla Firefox 版本 28.*x*
  - Mozilla Firefox 版本 29.*x*
  - Mozilla Firefox 版本 24.4 ESR
- Windows 7 32 位和 Windows 7 64 位
  - Internet Explorer 版本 10.*x*
  - Internet Explorer 版本 11.*x*
  - Mozilla Firefox 版本 17.*x*
  - Mozilla Firefox 版本 21.*x*
  - Mozilla Firefox 版本 22.*x*
  - Mozilla Firefox 版本 25.*x*
  - Mozilla Firefox 版本 26.*x*
  - Mozilla Firefox 版本 28.*x*
  - Mozilla Firefox 版本 29.*x*
  - Mozilla Firefox 版本 31.*x*
  - Mozilla Firefox 版本 17.0.6 ESR
  - Mozilla Firefox 版本 24.1.1 ESR
  - Mozilla Firefox 版本 24.4 ESR
  - Mozilla Firefox 版本 24.5 ESR
  - Mozilla Firefox 版本 24.7.0 ESR
  - Mozilla Firefox 版本 31.0 ESR

- Windows 8.*x*
  - Internet Explorer 版本 11.*x*
  - Mozilla Firefox 版本 31.*x*
  - Mozilla Firefox 版本 24.7.0 ESR
  - Mozilla Firefox 版本 31.0 ESR

仅以下密码套件支持上述浏览器：

- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

  如果在 Windows XP 操作系统中使用 Internet Explorer 版本 8 *x* 以兼容模式访问 ACS Web 界面，则不支持上述密码套件。

必须在运行客户端浏览器的系统上安装 Adobe Flash Player 11.2.0.0 或更高版本。

注

- 当从 ACS 5.*x* 导入或导出 .csv 文件时，必须关闭弹出窗口拦截器。

注

- 仅可在 Internet Explorer 7.*x* 或更高版本以及 Mozilla Firefox 3.*x* 版本中使用 IPv6 地址启动 ACS Web 界面。

支持的设备和用户存储库

有关支持的设备、802.1X 客户端和用户存储库的信息，请参阅《*思科安全访问控制系统 5.6 支持的互操作设备和软件*》。

ACS 5.6 版本的新功能

以下部分简要介绍 5.6 版本的新功能：

增强的报告

Cisco Secure ACS 版本 5.6 中的报告经过改进后，界面焕然一新，更加简洁且易于使用。报告划分为不同的逻辑类别，提供有关身份验证、会话流量、设备管理、ACS 服务器配置和管理以及故障排除的信息。增强的动态导出选项可以将选定的报告以逗号分隔值 (.csv) 文件的形式导出到 Excel 电子表格。增强的计划服务还允许您将报告加入队列并在报告可用时接收通知。

报告名称及其过滤器在左侧窗格上显示，而报告在“报告”(Reports) Web 界面的右侧窗格上显示。增强的 Web 界面可帮助您轻松导航报告并从左侧窗格更好地控制不同类型的报告。ACS 5.6 报告可提供增强性能并且易于使用，但不支持全局交互式查看器功能；不过，支持“显示或隐藏列”(show or hide columns) 和“固定列”(fixing columns)（交互式查看器功能的组成部分）。您可以将报告导出至 CSV 文件，使用 Microsoft Excel 电子表格或任何其他支持的工具打开该文件，并使用 Excel 选项来执行操作。ACS 5.6 中缺失的某些交互式查看器自定义选项将在未来的 ACS 版本或 ACS 5.6 补丁中向客户提供。

注 ACS 5.6 补丁 2 引入了两种新的交互式查看器功能：排序和过滤报告数据。安装 ACS 5.6 补丁 2 后，您可以从“报告”(Reports) Web 界面生成报告，然后对数据项进行过滤和排序。

ACS 5.6 Flex 报告的优点

- 根据观察，性能方面的一项重大改进表现在缩短了生成报告所需的时间。
- 基于 Flex 的报告提高了应用开发人员控制代码库的能力。这样，开发人员就可以缓解安全问题，尤其是在基于 Web 服务器的应用中。
- 如果您需要新的功能或修复 Actuate 报告当前版本中的任何现有问题，则需将 Actuate 升级到最新版本。将 Actuate 当前版本升级到最新版本需要耗费大量的精力和资本。Flex 报告极少出现这些问题，并且可以长期保持可持续性。
- Actuate 需要可重新分发的许可证，而 Flex 仅需开发人员许可证。
- 在不同类型的报告之间进行导航时，现在可以从左侧窗格更好地控制，而不必转至右侧窗格再选择报告及其过滤器值。此左侧窗格导航改善了用户体验。
- Flex 报告的外观和风格以及布局均远远优于 Actuate 报告。
- 思科身份服务引擎 (ISE) 使用 Flex 框架生成报告，而且 ISE 报告与 ACS 5.6 报告相似。这种相似性将帮助您在今后更加顺利地执行从 ACS 到 ISE 的迁移。

ACS 5.6 Flex 报告的限制

表 2 列出的是 ACS 5.5 和 5.6 “报告”(Reports) Web 界面的功能实施之间的限制和差异。

表 2　　ACS 5.6 报告与 ACS 5.5 报告相比所具有的限制

ACS 5.5 的功能	ACS 5.6 中实施的功能	解决方法
在“查询及运行”(Query & Run) 页面，您可以搜索用户、ACS 节点和身份组并生成自定义报告，并可从所有用户或组列表中选择一个用户或组。	在 ACS 5.6 中，此功能经过专门设计，因此您不必记住用户或组。在输入字段中输入前三个字符时，系统会自动填充用户或组。	无
ACS 5.4 中的“计划”(Scheduled) 报告和“收藏”(Favorite) 报告可以在 ACS 5.5 中重新使用。但是，这些报告不可以在 ACS 5.6 中重新使用，因为 Flex 框架无法识别存储在磁盘中的基于 Actuate 的“计划”(Scheduled) 报告和“收藏”(Favorite) 报告的格式。	ACS 5.4 或 5.5 中生成的“计划”(Scheduled) 报告和“收藏”(Favorite) 报告可以在 ACS 5.6 中重新使用。ACS 5.4 或 5.5 的“计划”(Scheduled) 报告和“收藏”(Favorite) 报告存储在 ACS 5.6 的“已保存”(Saved) 报告下。	无
列排序 - 在交互式查看器中，您可以对列进行升序或降序排列。	不可用	您可以将报告导出至 CSV 文件，使用 Microsoft Excel 电子表格打开该文件，并使用 Excel 选项对数据排序。
在交互式查看器中，您可以汇总数字列中的值。例如，可以汇总已通过的身份验证的数量并查看已通过的身份验证的总数。同样，您可以搜索并查找最小值、最大值、第一个值、最后一个值等等。	不可用	您可以将报告导出至 CSV 文件，使用 Microsoft Excel 电子表格或任何其他支持的工具打开该文件，并使用 Excel 选项来执行操作。
在交互式查看器中，您可以通过合并两列的值添加新的一列。您还可以使用表达式合并列中的值。	不可用	您可以将报告导出至 CSV 文件，使用 Microsoft Excel 电子表格或任何其他支持的工具打开该文件，并使用 Excel 选项来执行操作。
在交互式查看器中，您可以根据等于、小于、大于、在...之间、非空值等条件来过滤列值。	不可用	您可以将报告导出至 CSV 文件，使用 Microsoft Excel 电子表格或任何其他支持的工具打开该文件，并使用 Excel 选项来执行操作。
在交互式查看器中，您可以通过应用分页符、更改对齐方式、更改字体、样式、颜色、大小写（大写/小写）等来编辑报告。	不可用	您可以将报告导出至 CSV 文件，使用 Microsoft Excel 电子表格或任何其他支持的工具打开该文件，并使用 Excel 选项来执行操作。
在交互式查看器中，您可以根据特定列的值重新整理报告或划分整个报告。例如，按照失败尝试次数均超过三次的所有用户重新整理报告。	不可用	您可以将报告导出至 CSV 文件，使用 Microsoft Excel 电子表格或任何其他支持的工具打开该文件，并使用 Excel 选项来执行操作。

升级 Cisco Secure ACS 软件

思科安全访问控制系统 (ACS) 支持从不同的 ACS 5.*x* 版本升级至 ACS 5.6。支持的升级路径包括：

- Cisco Secure ACS 5.4 版本，建议应用最新补丁
- Cisco Secure ACS 5.5 版本，建议应用最新补丁

请遵循《*思科安全访问控制系统 5.6 安装和升级指南*》中的升级说明升级到 Cisco Secure ACS 5.6 版本。

监控和报告数据导出兼容性

如果远程数据库为 Oracle 数据库且已在集群设置中配置，则不能将监控和故障排除记录导出至远程数据库。

安装和升级说明

本部分提供关于 ACS 5.6 的安装任务和配置流程的信息。

此部分包含以下内容：

安装、设置和配置 CSACS-1121

本部分介绍如何安装、设置和配置 CSACS-1121 系列设备。CSACS-1121 系列设备已预安装软件。

要设置和配置 CSACS-1121，请执行以下步骤：

步骤 1 打开包含 CSACS-1121 系列设备的箱子并确认其包含以下各项：

- CSACS-1121 系列设备
- 电源线
- 机架安装套件
- 思科信息包
- 保修卡
- *思科安全访问控制系统 5.6 的合规性与安全信息*

步骤 2 浏览 CSACS-1121 系列设备的规格。

有关详细信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》。

步骤 3 安装 CSACS-1121 系列设备之前，请阅读必须遵循的一般注意事项和安全说明。

有关详细信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》并特别注意所有安全警告。

步骤 4 将设备安装在4 柱式机架中，并完成其余硬件安装步骤。

有关安装 CSACS-1121 系列设备的更多详细信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》。

步骤 5 将 CSACS-1121 系列设备连接至网络，然后将 USB 键盘和视频图形阵列 (VGA) 显示器或串行控制台连接至串行端口。

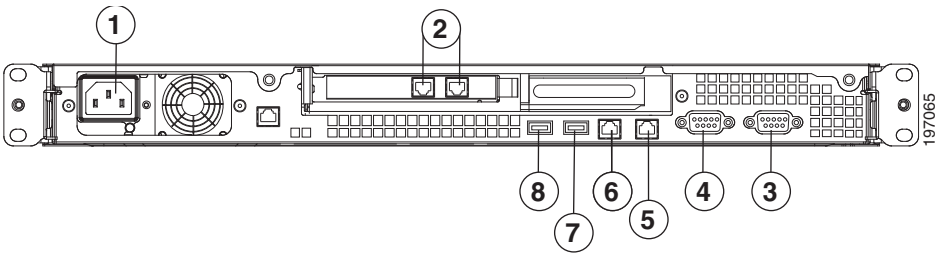
图 1 显示的是 CSACS-1121 系列设备的后面板以及各种电缆连接器。

注 对于初始设置，您必须有 USB 键盘和 VGA 显示器或运行终端仿真软件的串行控制台。

有关详细信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》。

有关在 VMware 中安装 ACS 5.6 的信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》中的“在 VMware 虚拟机中安装 ACS”一章。

图 1 CSACS 1121 系列设备后视图



下表介绍的是图 1 中的标注。

1	交流电源插座	5	千兆以太网 1
2	千兆以太网	6	千兆以太网 0
3	串行连接器	7	USB 3 连接器
4	视频连接器	8	USB 4 连接器

步骤 6 完成硬件安装后，请启动设备。

首次启动设备后，您必须运行安装程序以配置设备。有关详细信息，请参阅运行设置程序（第 11 页）。

安装、设置和配置思科 SNS-3495 或思科 SNS-3415

思科 SNS-3495 和思科 SNS-3415 设备没有 DVD 驱动器。您必须使用设备上的 CIMC 或可引导 USB 在此设备中安装、设置和配置 ACS 5.6。有关详细信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》。

本部分介绍如何安装、设置和配置思科 SNS-3495 和思科 SNS-3415 设备。思科 SNS-3495 和思科 SNS-3415 设备已预安装软件。

要设置和配置思科 SNS-3495 和思科 SNS-3415，请执行以下步骤：

步骤 1 打开包含思科 SNS-3495 和思科 SNS-3415 设备的箱子并确认其包含以下各项：

- 思科 SNS-3495 和思科 SNS-3415 设备
- 电源线
- KVM 电缆
- 思科信息包
- 保修卡
- *思科安全访问控制系统 5.6 的合规性与安全信息*

步骤 2 浏览思科 SNS-3495 或思科 SNS-3415 设备的规格。

有关详细信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》。

步骤 3 安装思科 SNS-3495 或思科 SNS-3415 设备之前，请阅读必须遵循的一般注意事项和安全说明。

有关详细信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》并特别注意所有安全警告。

步骤 4 将设备安装在4 柱式机架中，并完成其余硬件安装步骤。

有关安装思科 SNS-3495 或思科 SNS-3415 设备的更多详细信息，请参阅

《思科安全访问控制系统 5.6 的安装和升级指南》。

步骤 5 将思科 SNS-3495 或思科 SNS-3415 系列设备连接至网络，然后将 USB 键盘和视频图形阵列 (VGA) 显示器或串行控制台连接至串行端口。

有关思科 SNS-3495 和思科 SNS-3415 设备以及各种电缆连接器的说明，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》。

注 对于初始设置，您必须有 USB 键盘和 VGA 显示器或运行终端仿真软件的串行控制台。

有关详细信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》。

有关在 VMware 中安装 ACS 5.6 的信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》的“在 VMware 虚拟机中安装 ACS”一章。

步骤 6 完成硬件安装后，请启动设备。

首次启动设备后，您必须运行安装程序以配置设备。有关详细信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》。

运行设置程序

设置程序会运行交互式 CLI，提示输入必需的参数。管理员可以使用控制台或哑终端配置初始网络设置并输入使用该设置程序的 ACS 5.6 服务器的初始管理员凭证。设置流程是一种一次性配置任务。

要配置 ACS 服务器，请执行以下步骤：

步骤 1 启动设备。

系统将显示以下设置提示：

```
Please type 'setup' to configure the appliance
localhost login:
```

在登录提示符下，输入 **setup**，然后按下 **Enter**。

控制台会显示一组参数。必须如表 3 中所述输入参数。

注 您可以在输入最后一个设置值之前，键入 **Ctrl-C** 随时中断设置流程。

表 3 网络配置提示符

提示符	默认	条件	说明
主机名	*localhost*	第一个字母必须为 ASCII 字符。 长度必须介于 3 到 15 个字符之间。 有效字符为字母数字（A-Z、a-z、0-9）和连字符 (-)，且第一个字符必须为字母。 **注** 要使用 AD ID 存储区并设置具有相同名称前缀的多个 ACS 实例时，请使用最多 15 个字符作为主机名以免影响 AD 功能。	输入主机名。
IPv4 IP 地址	无，特定于网络	必须是介于 0.0.0.0 和 255.255.255.255 之间的有效 IPv4 地址。	输入 IP 地址。
IPv4 网络掩码	无，特定于网络	必须是介于 0.0.0.0 和 255.255.255.255 之间的有效 IPv4 网络掩码。	输入有效的网络掩码。
IPV4 网关	无，特定于网络	必须是介于 0.0.0.0 和 255.255.255.255 之间的有效 IPv4 地址。	输入默认网关的有效 IP 地址。
域名	无，特定于网络	不能是 IP 地址。 有效字符为 ASCII 字符、任意数字、连字符 (-) 和句点 (.)。	输入域名。
IPv4 主名称服务器地址	无，特定于网络	必须是介于 0.0.0.0 和 255.255.255.255 之间的有效 IPv4 地址。	输入一个有效名称服务器地址。
添加另一个名称服务器	无，特定于网络	必须是介于 0.0.0.0 和 255.255.255.255 之间的有效 IPv4 地址。 **注** 最多可以从 ACS CLI 配置三个名称服务器。	要配置多个名称服务器，请输入 **y**。
NTP 服务器	time.nist.gov	必须是介于 0.0.0.0 和 255.255.255.255 之间的有效 IPv4 地址或域名服务器。 **注** 最多可以从 ACS CLI 配置三个 NTP 服务器。	输入一个有效域名服务器或 IPv4 地址。

表 3　　网络配置提示符（续）

提示符	默认	条件	说明
时区	UTC	必须是有效的当地时区。	输入有效的系统时区。
SSH 服务	无，特定于网络	无。	要启用SSH服务，请输入 **y**。
用户名	*admin*	第一个管理员用户的名称。您可以接受默认用户名或输入新的用户名。 必须介于 3 到 8个字符之间，且必须是字母数字（A-Z、a-z、0-9）。	输入用户名。
管理员密码	无	无默认密码。输入密码。 密码长度必须至少为 6 个字符且包含至少一个小写字母、一个大写字母和一个数字。 此外： • 保存初始配置时所设置帐户的用户和密码信息。 • 这些信息允许对 ACS 硬件、CLI 及应用执行完全的管理员控制，因此请记住并保护好这些凭证。 • 如果丢失管理员凭证，可以使用 ACS 5.6 安装光盘重置密码。	输入密码。

输入参数后，控制台会显示：

```
localhost login: setup
Enter hostname[]: acs54-server-1
Enter IP address[]: 192.0.2.177
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 192.0.2.1
Enter default DNS domain[]: mycompany.com
Enter primary nameserver[]: 192.0.2.6
Add secondary nameserver?Y/N : n
Add primary NTP server [time.nist.gov]: 192.0.2.2
Add secondary NTP server?Y/N : n
Enter system timezone[UTC]:
Enable SSH Service?Y/N [N] : y
Enter username [admin]: admin
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Virtual machine detected, configuring VMware tools...
File descriptor 4 (/opt/system/etc/debugd-fifo) leaked on lvm.static invocation
Parent PID 3036: /bin/bash
Do not use `Ctrl-C' from this point on...
debugd[2455]: [2809]: config:network: main.c[252] [setup]: Setup is complete.
Appliance is configured
Installing applications...
Installing acs...
Generating configuration...
Rebooting...
```

安装 ACS 服务器后，系统会自动重启。现在，您可以使用在设置流程中配置的 CLI 用户名和密码登录 ACS。

仅可使用此用户名和密码通过 CLI 登录到 ACS。要登录到 Web 界面，必须使用默认的预定义用户名 *ACSAdmin* 和密码 *default*。

首次访问 Web 界面时，系统会提示更改预定义的管理员密码。您还可以定义要访问 Web 界面的其他管理员的访问权限。

ACS 5.6 中的许可

要运行 ACS，必须安装有效的许可证。首次访问 Web 界面时，ACS 会提示您安装有效的许可证。

分布式部署中的每个 ACS 实例（无论是主实例还是辅助实例）均要求安装唯一基础许可证。

此部分包含以下内容：

许可证类型

表 4 列出的是 ACS 5.6 中可用的许可证类型。

表 4　　ACS 许可证支持

许可证	说明
基础许可证	所有已部署软件实例和所有设备均需要基础许可证。基础许可证允许您使用许可证控制功能之外的所有 ACS 功能，并支持标准的集中报告功能。 基础许可证： • 对于所有主辅 ACS 实例都是必需的。 • 对于所有设备是必需的。 • 支持最多 500 个 NAD 的部署。 以下是基础许可证的类型： • 永久型 - 没有到期日期。支持最多 500 个 NAD 的部署。 • 评估型 - 自许可证发布之日起 90 天到期。支持最多 50 个 NAD 的部署。 设备的数量由您所配置的唯一 IP 地址数量决定。这包括您配置的子网掩码： 例如，255.255.255.0 子网掩码表示 256 个唯一 IP 地址；因此设备数量是 256。
附加许可证	附加许可证只能安装在具有永久型基础许可证的 ACS 服务器中。大型部署要求安装永久型基础许可证。 安全组访问功能许可证包括两种类型：永久型和 NFR 型。但是，永久型安全组访问功能许可证仅可与永久型基础许可证配合使用。

ACS 5.6 不支持自动安装评估型许可证。因此，如果需要 ACS 5.6 评估版本，则必须从 Cisco.com 获取评估型许可证并手动安装 ACS 5.6。

如果您没有任何 ACS 产品的有效 SAS 服务合同，则无法从 Cisco.com 下载 ISO 映像。在这种情况下，您需要联系当地的合作伙伴或思科代表获取 ISO 映像。

升级 ACS 服务器

如果已在计算机中安装 ACS 5.4 或 ACS 5.5，可以使用以下方法之一升级到 ACS 5.6：

- 使用应用升级捆绑包升级 ACS 服务器
- 重新映像和升级 ACS 服务器

只有在磁盘大于或等于 500 GB 时，才可以在思科设备或虚拟机中执行应用升级。如果磁盘小于 500 GB，则必须重新映像至 ACS 5.6，然后恢复在 ACS 5.4 或 ACS 5.5 中所执行的备份，从而迁移至 ACS 5.6 版本。

有关升级 ACS 服务器的信息，请参阅《*思科安全访问控制系统 5.6 的安装和升级指南*》。

注 如果任何 LDAP 身份存储空间中未配置组或属性且未配置 AD 身份存储空间，则升级到 ACS 5.6 可能会失败。要避免此问题，在升级到 ACS 5.6 之前，需要向 LDAP 身份存储空间添加组或属性，或配置 AD 身份存储空间。

注 使用 **backup-staging-url** 命令在 ACS 5.6 中配置 NFS 位置时，必须提供完全的 NFS 目录权限才能成功执行按需备份。

应用累积型补丁

我们将在 Cisco.com 上定期发布补丁，为 ACS 5.6 提供修复。这些补丁为累积型。每个补丁包括此版本之前补丁中所包含的所有修复。

您可以从以下位置下载 ACS 5.6 累积型补丁：

http://software.cisco.com/download/navigator.html

要下载和应用补丁，请执行以下步骤：

步骤 1 登录 Cisco.com 并依次导航到**产品 (Products) > 安全 (Security) > 访问控制和策略 (Access Control and Policy) > 策略和访问管理 (Policy and Access Management) > 思科安全访问控制系统 (Cisco Secure Access Control System) > 思科安全访问控制系统 5.6 (Cisco Secure Access Control System 5.6)**。

步骤 2 下载补丁。

步骤 3 安装 ACS 5.6 累积型补丁。安装操作如下所述：

在 EXEC 模式下输入以下 **acs patch** 命令安装 ACS 补丁：

acs patch install *patch-name*.**tar.gpg repository** *repository-name*

ACS 会显示以下确认消息：

```
Installing an ACS patch requires a restart of ACS services.
Would you like to continue? yes/no
```

步骤 4 输入 **yes**。

ACS 会显示以下消息：

```
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Getting bundle to local machine...
  md5: aa45b77465147028301622e4c590cb84
```

```
  sha256: 3b7f30d572433c2ad0c4733a1d1fb55cceb62dc1419b03b1b7ca354feb8bbcfa
% Please confirm above crypto hash with what is posted on download site.
% Continue?Y/N [Y]?
```

步骤 5 ACS 5.6 升级捆绑包会显示 md5 和 sha256 校验和。请将其与 Cisco.com 下载站点所显示的值进行比较。执行以下其中一项操作：

- 如果加密散列匹配，请输入 **Y**。如果输入 Y，ACS 会继续执行安装步骤。

  ```
  % Installing an ACS patch requires a restart of ACS services.
  Would you like to continue? yes/no
  ```

- 如果加密散列不匹配，请输入 **N**。如果输入 N，ACS 会终止安装步骤。

步骤 6 输入 **yes**。

ACS 版本即已升级到所应用的补丁。在 EXEC 模式下，使用 **show application status acs** 命令，检查所有服务是否正常运行。

步骤 7 在 EXEC 模式下，输入 **show application version acs** 命令，验证补丁是否已正确安装。

ACS 会显示类似于以下内容的消息：

```
acs/admin# show application version acs
CISCO ACS VERSION INFORMATION
-----------------------------
Version: 5.6.0.22
Internal Build ID: B.225
acs/admin #
```

注 安装补丁时，如果补丁大小超过允许的磁盘配额，则会在 ACS CLI 中显示警告消息，并在“ACS 监控和报告”(ACS Monitoring and Reports) 页面显示警告。

已解决的 ACS 问题

表 5 列出 ACS 5.6 中已解决的问题。

表 5　　ACS 5.6 中已解决的问题

漏洞 ID	说明
CSCuj91631	如果主机名无法解析，则无法从主 ACS 实例启动辅助实例的 Web 界面。
CSCuj53935	证书授权编辑页面易受 XSS 的攻击。
CSCuj80866	如果 ACS 实例不是日志收集服务器，则无法从 Web 界面收集支持的捆绑包。
CSCul09022	以分段数据包发送 TACACS 请求时，ACS 无响应。
CSCth35755	如果组名包含“/”字符，将无法在 Active Directory 中进行组映射。
CSCul29675	新创建的授权规则无法保留自定义状态。
CSCul32497	ACS 中的清除过滤器选项无法显示 200 个以上的授权规则。
CSCul64484	ACS View NBAPI 不具有详细的调试日志。
CSCuh63873	ACS View 应通过 TLS 或 TCP 协议实施系统日志消息。
CSCum03625	ACS 中存在脚本漏洞。

表 5　　ACS 5.6 中已解决的问题 （续）

漏洞 ID	说明
CSCum13044	Active Directory 会在更改密码后丢失与 ACS 的连接。
CSCuj94585	当同一用户位于两个不同的组织单位时，无法在 ACS 中执行 Active Directory 身份验证。
CSCum26584	升级到 ACS 5.5 后，当 ACS 5.4 中存在多个 CLI 管理员时，ACS Web 界面中的某些功能无法正常工作。
CSCuj01135	与 LDAP 服务器通信时，Active Directory 客户端在频繁重启，出现异常错误。
CSCum68228	在 ACS 5.5 中使用 CSV 文件导入用户详细信息时，无法更改内部用户密码。
CSCum86948	在 ACS 5.5 中，最小密码长度更改为 4。
CSCum86626	升级到 ACS 5.5 后，无法通过广域网向主 ACS 实例注册辅助 ACS 实例注册。
CSCum51180	在 ACS 5.4 中，当配置数据库大小超过 1GB 时不出现警告。
CSCty13296	使用相同密码导入用户不显示错误消息。
CSCum67932	由于未知的加密算法，ACS 5.5 在从 ACS 5.4 升级后无法启动。
CSCun37608	当原来的主实例恢复在线状态时，辅助 ACS 实例忽略新的主 ACS 实例。
CSCun85949	配置 RADIUS 属性 150、151 和 152 后，ACS 5.5 无法启动其服务。
CSCun71995	点击“NDG 位置”(NDG:Location) 选项时，ACS Web 界面无法显示网络设备组的位置。
CSCun67769	属性长度较大时，无法创建或编辑“收藏”(Favorites) 选项。
CSCun81726	无法在 ACS 5.5 中从 Active Directory 检索用户属性“userAccountControl”。
CSCun92213	ACS 5.x 一次打开过多与远程 DB 的 TCP 连接。
CSCun98622	从终端站过滤器导出 MAC 地址会导致从 ACS Web 界面注销用户。
CSCtx99385	ACS 显示未配置增量备份的错误警告报告。
CSCun84823	在 ACS 中，未经身份验证的用户可以看到输入验证码。
CSCuo54517	在 ACS 中，无法覆盖全局日志配置选项。
CSCuo88797	使用不支持的浏览器访问 ACS Web 界面时，ACS 5.*x* 无法显示相应的错误信息。
CSCuj41395	重启 ACS 服务后，您会发现在 ACS CLI 中运行 **show running configuration** 命令时会添加两次计划备份。
CSCuo93378	使用 Chrome 和 Safari 浏览器通过 ACS Web 界面更改配置时，会损坏 ACS 数据库。
CSCuo82841	添加 AAA 客户端进行 TACACS+ 身份验证时，必须具有共享密钥。
CSCuo60270	由于具有大量的域控制器，ACS 无法加入 Active Directory 域。
CSCum60476	ACS 5.4 无法获取内部组。
CSCun05712	如果负载过大，ACS 中的 RSA 代理会被耗尽。
CSCuo68704	需要在 ACS 5.*x* 中改进检查状态监控的功能。
CSCuo78625	ACS 5.5 不允许 TACACS+ 和 RADIUS 身份验证的共享密钥中包含特殊字符。
CSCuo88163	在 ACS 5.5 中无法使用编程界面获取用户信息。
CSCuo63302	如果使用复制选项创建用户，则无法通过 REST 服务更改用户密码。

表 5　　ACS 5.6 中已解决的问题 （续）

漏洞 ID	说明
CSCuo19733	基于 ACS 5.5 View 开始和结束日期的自定义报告会显示结束日期之前的最后 500 页记录。
CSCuo89864	在 ACS 5.5 中，URL 的跨帧脚本和会话令牌中存在问题。
CSCuo89889	在 ACS 5.5 中，会话相关的 Cookie 不使用 HTTP-only 或安全关键字。
CSCuo89946	在 ACS 5.5 中，未经批准的散列算法被用于存储敏感数据。
CSCuo93378	使用 Chrome 和 Safari Web 浏览器会导致数据库损坏。
CSCup00818	执行 **show application status acs** 命令时，ACS 5.5 CLI 界面显示错误。
CSCup10509	在 ACS 5.5.中安全管理员可将其角色更改为超级管理员。
CSCup32287	在 ACS 5.5 中，默认情况下系统日志消息的 TCP 端口 6514 处于打开状态。
CSCup34695	在 ACS 5.5 中，由于 ACS 服务器与远程数据库之间的数据类型不匹配，将数据导出至远程数据库时因出现错误而失败。
CSCup77077	将 userAccountControl 作为授权规则中的条件时，ACS 不会从 Active Directory 检索 userAccountControl 属性。
CSCuq00890	在 ACS 命令行界面执行 **halt** 命令时，在部署中发现意外行为。
CSCtx65471	在部署中多次重启日志收集服务器时，ACS 无法将系统日志消息发送至远程数据库。
CSCup75144	使用 Internet Explorer 11.*x* 版本时，无法正确显示 ACS Web 界面中的授权策略页。
CSCuq64564	使用 Internet Explorer 11.*x* 打开 ACS 5.5 Web 界面时，会发生配置问题。这些问题现已解决。
CSCul06939	在 ACS 5.x 中使用 DNS 服务器名称时 LDAP 身份验证失败，且第一个 DNS 服务器会出现当机。
CSCum05372	升级至 ACS 5.5 后，ACS 活动日志不显示任何信息。
CSCum28910	在 Active Directory 组中缺失条目时，无法启动 ACS 运行时服务。
CSCum93359	将 ACS 5.*x* 升级至 ACS 5.5 版本后，SFTP 服务器无法工作。
CSCun45555	用于将 ACS 加入 Active Directory 的 Active Directory 用户密码在日志中以明文显示。
CSCun89799	选择外部身份存储空间时，REST API 服务会提示输入密码。
CSCuo45648	ACS 5.*x* 将系统日志消息发送至远程日志目标位置时，在夏令时期间使用错误的时区条目。
CSCup40317	ACS View 工作管理器进程在磁盘空间计算过程中意外终止。
CSCup79536	ACS 在重新加载后会忽略日志记录配置。
CSCup79591	ACS 在重新加载后会忽略 **no cdp run** 命令。
CSCup90014	系统会复制 /CSCOacs/view/decap/data/ 中的条目并将其存储在 /opt 中，导致 /opt 中的磁盘使用量增加。
CSCuq36829	/var 中的文件占用全部磁盘空间并使 ACS 不稳定。
CSCuq26876	无法在 ACS 5.5 中将远程数据库导出至 Microsoft SQL。
CSCul38172	在 ACS 5.x 中配置 NIC 绑定后，SNMP 无法正常工作。

累积型补丁 ACS 5.6.0.22.1 中已解决的问题

表 6 列出 ACS 5.6.0.22.1 累积型补丁中已解决的问题。

您可以从以下位置下载 ACS 5.6.0.22.1 累积型补丁：

http://software.cisco.com/download/navigator.html?a=a&i=rpm

有关如何将补丁应用至系统的说明，请参考“应用累积型补丁”部分（第 14 页）。

表 6　　累积型补丁 ACS 5.6.0.22.1 中已解决的问题

漏洞 ID	说明
CSCur00511	CVE-2014-6271 和 CVE-2014-7169 的 ACS 评估。 通过升级至要求的系统库，此修复解决了 bash shell 中已发现的漏洞。此补丁修复包括安全修复，因此 ACS 服务器会提示重启。为了成功安装补丁，强烈建议重启。

累积型补丁 ACS 5.6.0.22.2 中已解决的问题

表 7 列出 ACS 5.6.0.22.2 累积型补丁中已解决的问题。

您可以从以下位置下载 ACS 5.6.0.22.2 累积型补丁：

http://software.cisco.com/download/navigator.html?a=a&i=rpm

有关如何将补丁应用至系统的说明，请参考“应用累积型补丁”部分（第 14 页）。

表 7　　累积型补丁 ACS 5.6.0.22.2 中已解决的问题

漏洞 ID	说明
CSCur10264	ACS 5.6 已在“报告”(Reports) Web 界面中引入“排序”(Sorting) 功能和“过滤”(Filtering) 功能。
CSCuq67241	“过期后禁用帐户”(Disable account if date exceeds) 功能在 ACS 5.6 中不可用。
CSCuq13294	当在 ACS 5.6 独立节点中检索已从 ACS 5.3 部署执行的数据库备份时，会在 ACS 5.6 独立节点中自动注册 ACS 5.3 节点。
CSCuq35410	无法搜索包含“’ ”字符的用户名。
CSCuq11378	第一、第二和第三八位组相同时，ACS 5.6 显示 IP 地址或 IP 范围重叠错误消息。
CSCuq06377	从“报告”(Reports) Web 界面创建“已保存报告”(Saved Reports) 时，如果禁用某些过滤器，则在“已保存报告”(Saved Reports) 中会显示所有默认过滤器。
CSCuq21543	SGT 分配报告中不显示“全天身份验证”(Day-wise Authentication) 详细信息。
CSCuq21559	从“报告”(Reports) Web 界面交叉运行报告时，无法显示选定的时间范围。
CSCuq22094	ACS“报告”(Reports) Web 界面中的计划报告详细信息显示最后一次查看的报告。
CSCuq46862	ACS“报告”(Reports) Web 界面中的计划报告无法显示自定义的时间范围。
CSCuq56757	生成会话目录报告时，无法正确显示开始时间和结束时间范围。
CSCur30345	在 ACS 中发现 SSLv3 Poodle 漏洞评估。
CSCur27402	无法在 ACS 5.6“报告”(Reports) Web 界面安排报告计划。

累积型补丁 ACS 5.6.0.22.3 中已解决的问题

表 8 列出 ACS 5.6.0.22.3 累积型补丁中已解决的问题。

您可以从以下位置下载 5.6.0.22.3 累积型补丁：

http://software.cisco.com/download/navigator.html?a=a&i=rpm

有关如何将补丁应用至系统的说明，请参考“应用累积型补丁”部分（第 14 页）。

表 8　　累积型补丁 ACS 5.6.0.22.3 中已解决的问题

漏洞 ID	说明
CSCuq62466	数据中含有垃圾字符时，无法将远程数据库导出至 Microsoft SQL 数据库。
CSCur42721	ACS 5.*x* TACACS+ 线程需要改进。
CSCur59417	ACS 5.*x* Web 界面不允许出现单引号、省略号以及加号字符。
CSCur68196	配置远程数据库一两天之后，ACS 5.*x* 工作自动停止运行。
CSCur98716	ACS 5.4 显示“超过 GC 开销限制”(GC overhead limit exceeded) 异常且无法加载“监控和报告”(Monitoring and Reports) Web 界面。
CSCus17482	从主实例删除一个对象后，主实例向辅助实例发送不正确的参照。
CSCus38676	提交 AAA 运行状况警告中的更改后，ACS 5.6 显示内部错误。
CSCus42056	ACS View 中存在增量备份问题。
CSCus42060	日志不运行时，主动清除日志收集器漏洞。
CSCus55169	由于加密问题，无法运行 ACS 5.4 到 5.6 的应用升级。
CSCus68826	ACS 5.*x* 容易遭受 CVE-2015-0235 攻击。
CSCut55144	ACS 5.*x* 中存在特殊字符问题。
CSCut05442	ACS 不正确显示 IP 子网重叠错误消息。
CSCut20508	在 ACS 中配置网络设备的排除 IP 范围可能导致与其他子网重叠。
CSCut01441	如果 ACS 接收到 SIGPIPE（损坏的管道）信号，则会出现运行时崩溃。
CSCus52928	计划备份会同时在 FTP 服务器上创建许多相同名称的文件。
CSCus80750	如果第一个 TACACS+ ASCII 请求不含有用户名，则无法匹配服务选择规则。

累积型补丁 ACS 5.6.0.22.4 中已解决的问题

表 9 列出 ACS 5.6.0.22.4 累积型补丁中已解决的问题。

您可以从以下位置下载 5.6.0.22.4 累积型补丁：

http://software.cisco.com/download/navigator.html?a=a&i=rpm

有关如何将补丁应用至系统的说明，请参考“应用累积型补丁”部分（第 14 页）。

表 9　　累积型补丁 ACS 5.6.0.22.4 中已解决的问题

漏洞 ID	说明
CSCuu94829	ACS 识别到重叠 IP 范围时，ACS 5.x 显示不正确的设备名称。
CSCuu93287	无法在 ACS 中打开邮件通知警告中提供的报告链接。
CSCuu57091	应用 ACS 5.6 补丁 3 后，ACS 运行时进程停滞且未处于监控状态。
CSCuu43343	ACS 不允许网络设备的 KEK 和 MACK 密钥中包含特殊字符。
CSCuu30320	ACS 服务器无法识别从 ACS Web 界面配置的密码缓存超时选项。
CSCuu59807	由于 ACS 5.x 中的管理员帐户密码变更，发现存在复制问题。
CSCus63338	添加新布局时，ACS View 控制面板显示错误。
CSCuv88723	在更改 ACS 管理员密码时，如果密码含有 <字符或 > 字符，则会出现问题。
CSCuu81221	安装新的 CA 证书后，无法删除原来的从属 CA。
CSCuc16427	使用时间戳选项将记录导出至 .csv 文件功能无法正常运行。
CSCuv99693	ACS 5.6 不允许命令集中包含特殊字符。
CSCuw09481	ACS 5.*x* 容易遭受 CVE2015-5600 攻击。
CSCuv39328	当存在大量 AAA 客户端时，如果您在 ACS 中搜索具有网络设备名称的报告，ACS 管理流程将无法响应。
CSCuw21552	对于在配置“审计计划报告”(Audit Scheduled Report) 中所使用的所有过滤器，ACS 5.*x* 显示不正确的结果。
CSCuw70238	时钟时区设置为 ETC/GMT+/-7 时，无法在 ACS 5.*x* 中保存计划报告。
CSCuv95363	重新加载 ACS 服务器后，无法在 ACS 5.*x* 中运行计划报告。
CSCuv63197	最后一个 EAP 分段的长度大于 EAP 分段总长度时，发生 ACS 运行时崩溃。
CSCuv42038	高级丢弃选项未丢弃 ACS 5.x 中的 TACACS+ 请求。
CSCus42781	2015 年 1 月期间在 ACS 中发现了 OpenSSL 漏洞。
CSCus43434	如果 ACS 在数据包处理过程中接收到重置请求，则会达到情景限制。
CSCut94394	重启 ACS 服务时，无法启动临时数据库。
CSCuu11002	在 ACS 5.x 中发现反射型 XSS 漏洞。
CSCuu11005	在 ACS 5.x 中发现本地文件包含漏洞。
CSCus64212	ACS 5.6 中的计划报告无法显示所有列。
CSCut87378	身份验证过程中频繁发生 ACS 运行时崩溃。
CSCus97002	ACS 5.6 中的收藏报告不显示任何数据。
CSCto56190	如果 Active Directory 未启用 LDAP SSL，Active Directory 界面操作会需要很长时间。
CSCut75184	ACS 将括号视为无效字符。
CSCut46073	2015 年 3 月期间在 ACS 中发现了 OpenSSL 漏洞。
CSCuu82493	2015 年 6 月期间在 ACS 中发现了 OpenSSL 漏洞。
CSCuu67914	安装 ACS 5.6 补丁 3 后，在 ACS 中无法执行清除。
CSCuu42929	需要放宽 ACS 5.x 中的终端站过滤器限制。
CSCuv20514	恢复 ACS 5.5 View 数据库时发现问题。
CSCuv03303	从 ACS Web 界面导出报告时，ACS 无法正确发送邮件。
CSCuu75750	无法在 ACS 中使用 .csv 文件更新终端站过滤器。

ACS 部署中的限制

表 10 介绍 ACS 部署中的限制。

表 10　　ACS 部署中的限制

对象类型	ACS 系统限制
ACS 实例	22
主机数	150,000
用户	300,000
身份组	1,000
Active Directory 组检索	1,500
网络设备	100,000
网络设备组	12
设备分层	6
所有地点	10,000
所有设备类型	350
服务	25
授权规则	320
条件	8
授权配置文件	600
服务选择策略 (SSP)	50
网络条件(NAR)	3,000
ACS 管理员	50
	9 个静态角色
dACL	600 个 dACL，每个具有 100 个 ACE

已知的 ACS 问题

表 11 列出 ACS 5.6 中的已知问题。您还可以在 Cisco.com 上使用漏洞搜索工具 (Bug Toolkit) 查找此表中未列出的任何公开漏洞。

表 11　　ACS 5.6 中的已知问题

漏洞 ID	说明
CSCuo38291 未删除 ACS“报告”(Reports) Web 界面错误消息中显示的额外信息。	在“报告”(Reports) Web 界面中生成报告时，如果注销 ACS 会话，会显示错误消息。应删除此错误消息中的额外信息。 当从主 ACS 窗口注销且在另一个窗口中打开报告查看器时，会发生此问题。 **解决方法：** 1. 关闭 “报告” (Reports) Web 界面。 2. 登录 ACS Web 界面，然后点击**运行监控和报告查看器 (Launch Monitoring and Report Viewer)**。“监控和报告” (Monitoring and Reports) Web 界面在新窗口中打开。 3. 点击**报告 (Report)**，在新窗口中打开 “报告” (Reports) Web 界面。
CSCuq61449 已保存报告中不显示开始时间和结束时间过滤器。	运行任何已保存报告时，必须输入开始时间和结束时间过滤器值。 运行并保存具有开始时间和结束时间过滤器的报告时，会发生此问题。 **解决方法：** 手动输入开始时间和结束时间过滤器值。
CSCuq24311 将用户报告设置为收藏报告时，会自动更改收藏报告的过滤器选项。	在 ACS 5.6 中，将用户报告设置为收藏报告时，无法正确显示在收藏报告中自定义的过滤器值。 使用自定义过滤器生成收藏报告，并在使用 ACS“报告”(Reports) 部分的默认过滤器生成同一报告后选择此收藏报告查看其详细信息，会发生此问题。 **解决方法：** 刷新“报告”(Reports) Web 界面。
CSCuq24409 “已保存报告”(Saved Reports) 中显示的过滤器值不正确。	无法正确显示已保存报告、ACS 报告和收藏报告的滤值。 运行具有自定义过滤器值的已保存报告、ACS 报告和收藏报告时，会发生此问题。 **解决方法：** 关闭“报告”(Reports) Web 界面，然后从 ACS Web 界面重新打开。 “报告”(Reports) Web 界面中的过滤器值显示不正确，但是，当 ACS 从数据库中获取过滤器数据时，生成的报告会显示正确的信息。
CSCuo87567 ACS 5.6 “报告”(Reports) Web 界面不支持某些交互式查看器功能。	ACS 5.6 “报告”(Reports) Web 界面不支持全局交互式查看器功能；但是支持“显示或隐藏列”(show or hide columns) 和“固定列”(fixing columns)（交互式查看器功能的组成部分）。 将 ACS 升级到 ACS 5.6 版本后，会发生此问题。 **解决方法：** 将生成的报告导出至 CSV 文件。使用 Microsoft Excel 电子表格打开此 CSV 文件，并使用 Excel 选项获取缺失的交互式查看器功能。
CSCuq06377 ACS 会为已保存报告显示所有过滤器，即使保存报告时某些过滤器已禁用。	ACS 会为已保存报告显示所有过滤器，即使在“报告”(Reports) Web 界面中保存报告时某些过滤器已禁用。而一般情况下，对于所有已保存报告，ACS 仅显示自定义过滤器。 使用自定义过滤器保存报告，并在使用 ACS 报告部分的默认过滤器生成同一报告后选择此已保存报告查看其详细信息时，会发生此问题。 **解决方法：** 刷新“报告”(Reports) Web 界面。

表 11　　ACS 5.6 中的已知问题（续）

漏洞 ID	说明
CSCuq21543 SGT 分配报告中不显示全天身份验证信息。	ACS 无法为 SGT 分配报告显示全天身份验证信息。 生成 SGT 分配报告时，会发生此问题。 **解决方法：** 生成具有开始日期和结束日期过滤器的 SGT 分配报告。
CSCuq21559 从 ACS“报告”(Reports) Web 界面交叉运行报告时，会显示不正确的时间范围。	在 ACS“报告”(Reports) Web 界面交叉运行 RADIUS 和 TACACS+ 报告时，会显示不正确的时间范围。 从 ACS“报告”(Reports) Web 界面交叉运行 RADIUS 和 TACACS 报告时，会发生此问题。 **解决方法：** “报告”(Reports) Web 界面中的时间范围显示不正确，但是，当 ACS 从数据库中获取过滤器数据时，生成的报告会显示正确的信息。
CSCuq22094 查看另一个计划报告的详细信息时，会显示之前生成的计划报告的过滤器。	从“保存和计划报告”(Saved and Scheduled Report) 部分选择任何计划报告并在右窗格中查看其详细信息时，会在右窗格显示之前生成的计划报告的过滤器。 当存在多个计划报告时，如果在生成另一个计划报告后立即选择一个计划报告并在右窗格中查看其详细信息，则会发生此问题。 **解决方法：** 刷新“报告”(Reports) Web 界面。
CSCuq46862 从“报告”(Reports) Web 界面点击计划报告时，右窗格中不显示开始和结束日期。	从“保存和计划报告”(Saved and Scheduled Report) 部分选择一个计划报告并在右窗格中查看其详细信息时，右窗格中不显示开始和结束日期。 安排任何具有自定义时间范围的 ACS 报告计划时，会发生此问题。 **解决方法：** 无 此问题不会影响计划报告。
CSCuq51480 ACS 会为已保存报告显示其他过滤器，即使保存报告时某些过滤器已禁用。	ACS 会为已保存报告显示其他过滤器，即使在“报告”(Reports) Web 界面中保存报告时某些过滤器已禁用。而一般情况下，对于所有已保存报告，ACS 仅显示自定义过滤器。 使用自定义过滤器保存报告，并在使用 ACS 报告部分的默认过滤器生成同一报告后选择此已保存报告查看其详细信息时，会发生此问题。 **解决方法：** 刷新“报告”(Reports) Web 界面，然后从已保存报告部分打开已保存的报告。
CSCuq56757 在“报告”(Reports) Web 界面中无法正确显示开始日期和结束日期。	生成报告后，当使用时间范围过滤器时，在“报告”(Reports) Web 界面中会显示开始日期和结束日期。但是在 ACS 5.6 中，生成具有时间范围过滤器的会话目录报告时，无法正确显示开始日期和结束日期值。 生成具有应用时间范围过滤器的会话目录报告时，会发生此问题。 **解决方法：** “报告”(Reports) Web 界面中的时间范围显示不正确，但是，当 ACS 从数据库中获取过滤器数据时，生成的报告会显示正确的信息。

文档更新

表 12 列出《*思科安全访问控制系统 5.6 版本说明*》。

表 12　　思科安全访问控制系统 5.6 版本说明更新

日期	说明
2015 年 11 月 19 日	添加累积型补丁 ACS 5.6.0.22.4 中已解决的问题（第 19 页）
2015 年 4 月 27 日	添加累积型补丁 ACS 5.6.0.22.3 中已解决的问题（第 19 页）
2014 年 11 月 27 日	添加累积型补丁 ACS 5.6.0.22.2 中已解决的问题（第 18 页）
2014 年 10 月 8 日	添加累积型补丁 ACS 5.6.0.22.1 中已解决的问题（第 18 页）
2014 年 9 月 26 日	思科安全访问控制系统版本 5.6

产品文档

注　原始出版物发布之后，思科可能会更新打印文档和电子文档。因此，您应该从 http://www.cisco.com 查看所有更新信息。

表 13 列出 ACS 5.6 可用的产品文档。要在 Cisco.com 上查找所有产品的最终用户文档，请转至：http://www.cisco.com/go/techdocs。

依次选择**产品 (Products) > 安全 (Security) > 访问控制和策略 (Access Control and Policy) > 策略和访问管理 (Policy and Access Management) > 思科安全访问控制系统 (Cisco Secure Access Control System)**。

表 13　　产品文档

文档标题	可用的格式
思科安全访问控制系统设备内文档和中国 RoHS 指针卡	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-documentation-roadmaps-list.html
思科安全访问控制系统 5.6 迁移指南	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-installation-guides-list.html
思科安全访问控制系统 5.6 用户指南	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-user-guide-list.html
思科安全访问控制系统 5.6 CLI 参考指南	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-command-reference-list.html
思科安全访问控制系统 5.6 支持的互通设备和软件	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-device-support-tables-list.html
思科安全访问控制系统 5.6 安装和升级指南	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-installation-guides-list.html
思科安全访问控制系统 5.6 软件开发者指南	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-programming-reference-guides-list.html
思科安全访问控制系统的合规性与安全信息	http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/ 5 - 6 /regulatory/compliance/csacsrcsi.html

通知

以下通知与此软件许可证有关。

OpenSSL/OpenSSL 项目

此产品包括 OpenSSL 项目开发的、可在 OpenSSL 工具包中使用的软件 (http://www.openssl.org/)。

此产品包括 Eric Young (eay@cryptsoft.com) 编写的加密软件。

此产品包括 Tim Hudson (tjh@cryptsoft.com) 编写的软件。

许可问题

OpenSSL 工具包使用双重许可模式，即 OpenSSL 许可证和原有的 SSLeay 许可证同时适用于该工具包。实际许可证文本详见下文。事实上，两个许可证都是 BSD 样式的开放源许可证。有关 OpenSSL 的任何许可证问题，请联系 openssl-core@openssl.org。

OpenSSL License

版权所有 © 1998-2007 OpenSSL Project。保留所有权利。

对源代码或二进制形式代码的重新发行和使用（包含或不含修改）需要符合下列条件：

1. 源代码的再次分发必须保留版权通知、该条件列表和以下免责声明。
2. 以二进制形式重新发行时，必须通过文档和/或在发行时一并提供的其它材料复制上述版权声明、此条件清单和下面的免责声明。
3. 所有提及此软件的功能或用途的宣传材料必须显示以下声明“此产品包括 OpenSSL 项目开发的、可在 OpenSSL 工具包中使用的软件 (http://www.openssl.org/)”。
4. 不经事先书面许可，不得将名称“OpenSSL 工具包”和“OpenSSL Project”用于促销和宣传从该软件衍生的产品。有关书面许可，请联系 openssl-core@openssl.org。
5. 未经 OpenSSL Project 事先书面许可，从该软件衍生的产品不得称为“OpenSSL”，也不得在其名称中显示“OpenSSL”。
6. 无论何种形式的再分发都必须保留以下内容：

   “此产品包括 OpenSSL 项目开发的、可在 OpenSSL 工具包中使用的软件 (http://www.openssl.org/)”。

该软件由 OpenSSL PROJECT 按“原样”提供，对于明示或暗含的担保，包括但不限于特定目的的适销性和适用性的暗含担保，均不负任何责任。在任何情况下，OpenSSL PROJECT 或其参与者对于由使用该软件造成的任何直接、间接、意外、特殊、惩罚性或后果性损失（包括但不限于获得替换的货物或服务；用途、数据或利益损失；或业务中断），无论其原因及理论上的责任，包括是否在合同中、严格赔偿责任或侵权行为（包括疏忽或其他），均不负有任何责任，即使已被告知此类损失的可能性也是如此。

此产品包括 Eric Young (eay@cryptsoft.com) 编写的加密软件。此产品包括 Tim Hudson (tjh@cryptsoft.com) 编写的软件。

原有的 SSLeay 许可

版权所有 © 1995-1998 Eric Young (eay@cryptsoft.com)保留所有权利。

该数据包是由 Eric Young (eay@cryptsoft.com) 编写的 SSL 实施。

* 该应用 与 Netscapes SSL 兼容。

只要符合以下条件，则该库可免费用于商业和非商业用途。以下条件适用于在该分发中出现的所有代码，可以是 RC4、RSA、lhash、DES 等代码，而不仅是 SSL 代码。包括在该分发中的 SSL 文档受相同版权条款限制，但其版权持有人是 Tim Hudson (tjh@cryptsoft.com)。

版权仍然属于 Eric Young，因此不会删除代码中的任何版权通知。如果在产品中使用该数据包，则应在所用库的部分的作者中署名 Eric Young。此内容可以在程序启动时以文本消息的形式，也可以包括在随数据包提供的文档（在线或文本）中。

对源代码或二进制形式代码的重新发行和使用（包含或不含修改）需要符合下列条件：

1. 源代码的再次分发必须保留版权通知、该条件列表和以下免责声明。
2. 以二进制形式重新发行时，必须通过文档和/或在发行时一并提供的其它材料复制上述版权声明、此条件清单和下面的免责声明。
3. 所有提及该软件功能或使用的广告资料都必须显示以下内容：

   “该产品包括由 Eric Young (eay@cryptsoft.com) 编写的密码软件”

   如果使用的库的惯例不与密码相关，则可省去“密码”一词。
4. 如果您包括来自任何 Windows 专用代码（或其衍生目录（应用程序代码）必须包含以下声明“本产品包括由 Tim Hudson (tjh@cryptsoft.com) 编写的软件”。

该软件由 ERIC YOUNG 按“原样”提供，对于明示或暗含的担保，包括但不限于特定目的的适销性和适用性的暗含担保，均不负任何责任。在任何情况下，作者或参与者对于由使用该软件造成的任何直接、间接、意外、特殊、惩罚性或后果性损失（包括 [但不限于] 获得替换的货物或服务；用途、数据或利益损失；或业务中断），无论其原因及理论上的责任，包括是否在合同中、严格赔偿责任或侵权行为（包括疏忽或其他），均不负有任何责任，即使已被告知此类损失的可能性也是如此。

此代码的任何公开发行版本或衍生代码的许可和分发条款不可更改，即，此代码不能复制并置于其他分发许可 [包含 GNU 公共许可证] 下。

许可协议补充协议

思科系统访问控制系统软件的最终用户许可协议补充协议：

重要信息：请仔细阅读

本最终用户许可协议补充协议（“补充协议”）包含您与思科之间的最终用户许可协议（“EULA”，统称为“协议”)下许可的软件产品的其他条款和条件。本补充协议中使用但未定义的加粗术语采用 EULA 中规定的含义。如果 EULA 和本补充协议的条款和条件冲突，以本补充协议的条款和条件为准。

除遵守 EULA 中有关访问和使用本软件的其他限制之外，您还同意始终遵循本补充协议的条款和条件。下载、安装或使用本软件即表示接受本协议，并且您同意您本人和您代表的业务实体（统称为“客户”）受本协议的约束。若您不同意本协议全部条款，则思科不愿意授予您本软件许可，因此 (a) 您不得下载、安装或使用本软件；和 (b) 您可退还本软件（包括未启封的 CD 包和所有书面资料）并获得全额退款。或者，如果本软件与书面材料构成其他产品的组成部分，您可退还全部产品并获得全额退款。只有原始最终用户购买者才享有退货与退款权利，该等权利自从思科或授权的思科的经销商购买产品 30 天后失效。

1. 产品名称

对于本补充协议，可作为访问控制系统软件组成部分订购的产品名称和产品说明如下：

A. 高级报告和故障排除许可证

支持自定义报告、警告以及其他监控和故障排除功能。

B. 大型部署许可证

允许部署支持 500 台以上的网络设备（AAA 客户端以所配置的 IP 地址数量计算）也就是说，大型部署许可证允许在企业 ACS 部署中支持无限数量的网络设备。

C. 高级访问许可证（不适用于访问控制系统软件 5.0，将与未来的访问控制系统软件版本一起发行）

支持安全组访问策略控制功能以及其他高级访问功能。

2. 其他许可证限制

- 安装和使用。思科 SNS 3495、SNS 3415 和 CSACS 1121 硬件平台已预安装思科安全访问控制系统 (ACS) 软件组件。包含用于为 SNS 3495、SNS 3415 和 CSACS 1121 硬件恢复此软件的工具的光盘仅限客户用于重新安装用途。客户仅可在思科 SNS 3495、SNS 3415 和 CSACS 1121 硬件平台上运行支持的专用思科安全访问控制系统软件产品。请勿在思科 SNS 3495、SNS 3415 和 CSACS 1121 硬件平台上安装任何不支持的软件产品或组件。
- 软件升级、主要和次要版本。思科可能将思科 SNS 3495、SNS 3415 和 CSACS 1121 硬件平台的思科安全访问控制系统软件升级作为主要升级或次要升级提供。如果可通过思科或其认可的合作伙伴或经销商进行购买软件主要升级或次要升级，客户应为每个 SNS 3495、SNS 3415 和 CSACS 1121 硬件平台购买一个主要升级或次要升级。如果客户有资格通过思科扩展服务计划接收软件版本，每个有效服务合同仅限申请接收一个软件升级或新发行版本。
- 复制和分发。客户不得复制或分发软件。

3. 定义

主要升级指提供附加软件功能的软件版本。思科通过更改软件版本号的个位数字 [(x).x.x] 来对主要升级进行命名。

次要升级指提供维护修复和附加软件功能的增量软件版本。思科通过更改软件版本号的十分位数字 [x.(x).x] 来对次要升级进行命名。

4. 其他权利和限制说明。

请参阅思科系统公司的最终用户许可协议。

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 *What's New in Cisco Product Documentation*（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。

思科安全访问控制系统 5.6 版本说明