思科安全 **ACS** 至思科 **ISE** 迁移工具版本 **2.4** 用户指南

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录

序言：

前言 vii

简介 vii

目标读者 vii

文档结构 viii

文档约定 viii

相关文档 ix

获取文档和提交服务请求 x

第 1 章

使用入门 1

迁移概述 1

将数据从思科安全 ACS 迁移至 1

支持的数据迁移路径 2

思科安全 ACS 至思科 ISE 迁移工具 2

系统要求 3

迁移工具增强功能 3

第 2 章

安装迁移工具 5

迁移工具安装指南 5

安全注意事项 5

迁移工具初始化 6

第 3 章

制定迁移计划 7

必备条件 7

启用迁移接口 7

启用在迁移工具中可信证书 8
数据迁移时间估算 8
从思科安全 ACS 版本 5.5 或 5.6进行迁移之前的准备工作 9
策略服务迁移指南 9
思科安全 ACS 策略规则迁移指南 10

第 4 章 持续数据传输程序 11
从思科安全 ACS 导出数据 11
分析思科 ISE 与思科安全 ACS 之间的策略差异 14
将数据导入到思科 ISE 16
思科 ISE 中迁移的数据验证 19

第 5 章 报告 21
导出报告 21
策略差异分析报告 22
导入报告 23

第 6 章 从更早版本的思科安全 ACS 迁移至思科 ISE 25
从更早版本的思科安全 ACS 迁移至思科 ISE 25
从思科安全 ACS 版本 3.x 迁移 25
从思科安全 ACS 版本 4.x 迁移 25
从思科安全 ACS 版本 5.x 迁移 26

第 7 章 策略元素 27
思科 ISE 与思科安全 ACS 的奇偶校验 27
策略模式 28
思科安全 ACS 服务选择策略和思科 ISE 策略集 28
思科安全 ACS 策略访问服务与思科 ISE 策略集 28
UTF-8 支持 29
网络访问用户配置 29
RSA 29

RADIUS 令牌 29
策略 30
ISE 802.1X 服务的 FIPS 支持 30

第 8 章 思科安全 ACS 到思科 ISE 迁移工具故障排除 31
无法启动迁移工具 31
日志中显示错误消息 31
连接错误 31
I/O 异常错误 32
内存不足错误 32
未创建默认文件夹、文件和报告 32
迁移导出阶段非常缓慢 33
报告向思科 TAC 问题 33

第 9 章 常见问题解答 35
常见问题解答 35

附录 A： 数据结构映射 37
数据结构映射 37
已迁移的数据对象 37
部分迁移的数据对象 39
未迁移的数据对象 39
不支持的规则元素 40
支持的属性和数据类型 42
可以从思科安全 ACS 版本 5.5 或 5.6迁移至思科 ISE 的用户属性 42
用户属性：与用户的关联 42
从思科安全 ACS 版本 5.5 或 5.6 迁移至思科 ISE 版本 的主机属性 43
主机属性：与主机的关联 43
从思科安全 ACS 版本 5.5 或 5.6 迁移至思科 ISE 版本 的 RADIUS 属性 43
RADIUS 属性：与 RADIUS 服务器的关联 44
数据信息映射 44

网络设备映射 44
NDG 类型映射 45
NDG 层次结构映射 46
默认网络设备映射 46
身份组映射 46
用户映射 47
主机（终端）映射 47
LDAP 映射 48
Active Directory 映射 49
证书身份验证配置文件映射 50
身份库序列映射 50
授权配置文件映射 51
可下载 ACL 映射 51
RADIUS 字典（供应商）映射 51
RADIUS 字典（属性）映射 52
身份字典映射 52
身份属性字典映射 53
外部 RADIUS 服务器映射 53
RADIUS 令牌映射 54
RSA 映射 55
RSA 提示符映射 55

前言

本指南介绍使用思科安全 ACS 到思科 ISE 迁移工具，将数据从思科安全访问控制服务器 (ACS) 版本 5.5 或 5.6 迁移至思科身份服务引擎 (ISE) 版本 2.4 的过程。

注释 由于各个版本的思科安全 ACS 或思科 ISE 在功能上不尽相同，所以并非所有思科安全 ACS 数据都可以迁移到思科 ISE。此迁移工具为您提供关于不支持的对象的完整列表。

- 简介， 第 vii 页
- 目标读者， 第 vii 页
- 文档结构， 第 viii 页
- 文档约定， 第 viii 页
- 相关文档， 第 ix 页
- 获取文档和提交服务请求， 第 x 页

简介

本文档介绍将数据从思科安全访问控制系统 (ACS) 版本 5.5 或更高版本迁移至思科 ISE 2.4 的过程。思科安全 ACS 平台与思科 ISE 平台之间有若干不同点。在尝试迁移至思科 ISE 2.4 之前，您应清楚地了解这些不同点。本文档重点介绍这些不同点，并提供关于如何将您的 ACS 5.5 或更高版本配置迁移至思科 ISE 2.4 的指导。思科建议您除了掌握本文档中的信息外，还应对思科安全 ACS 5.5 或更高版本以及思科 ISE 平台进行全面的评估。

目标读者

本迁移指南的目标受众是负责使用思科安全 ACS 至思科 ISE 迁移工具将现有思科安全 ACS（版本 5.5/5.6）的数据库信息迁移至思科 ISE（版本 ）设备的网络管理员。

文档结构

本指南包含以下章节：

章标题	说明
第 1 章 - 入门指南	概括介绍迁移工具及源设备和目标设备，并说明系统要求。
第 2 章 - 安装迁移工具	提供迁移工具安装指南，并叙述安装过程。
第 3 章 - 制定迁移计划	说明执行迁移过程之前的必要准备。
第 4 章 - 数据传输程序	针对迁移工具数据迁移过程的各个阶段提供分步指导。
第 5 章 - 报告	提供与使用迁移工具时生成的报告相关的信息。
第 6 章 - 数据结构映射	列出可以迁移和无法迁移的思科安全 ACS 数据对象，并说明思科安全 ACS 与思科 ISE 之间的数据结构映射。
附录 A - 思科安全 ACS 至思科 ISE 数据迁移	介绍将数据从思科安全 ACS 迁移至思科 ISE 的相关信息。
附录 B - 数据迁移原则	说明各种数据迁移和部署场景。
附录 C - 故障排除	提供与迁移工具相关的故障排除信息。
附录 D - 常见问题解答	列出有关迁移工具和迁移过程的常见问题及解答。

文档约定

本文档使用下列约定：

约定	说明
粗体	命令和关键字及用户输入的文本以**粗体**显示。
斜体字体	文档标题、新出现或强调的术语，以及要为其提供数值的参数以斜体显示。
[x]	方括号中的关键字或参数是可选的。
[ ]	系统提示的默认响应括在方括号中。
|	竖线，称为管道，表示一组关键字或参数中的一个选项。
[x | y]	可选的备选关键字集中在方括号内，以竖线分隔。

约定	说明
{x | y}	必需的备选关键字集中在大括号内，以竖线分隔。
[x {y | z}]	嵌套方括号组或大括号组表示可选或必填元素中的可选或必填选项。方括号中的大括号和竖线指示可选元素中的必需选项。
Courier 字体	固定宽度字体形式的屏幕显示、提示和脚本示例。
Bold Courier 字体	您输入的信息示例。
< >	非打印字符（如密码）括在尖括号中。
! #	以感叹号 (!) 或井字号 (#) 开头的代码行为注释行。

读者提示约定

本文档使用以下读者提示约定：

注释 表示读者需要注意的地方。“注”中包含有用的建议或本文档未涵盖材料的引用信息。

提示 表示以下信息将帮助您解决问题或者可能是一些有用信息。

注意 表示读者应当小心处理。在这种情况下，您的操作可能会导致设备损坏或数据丢失。

便捷程序 表示所述操作可以节省时间。按照该段落中的说明执行操作，有助于节省时间。

警告 **表示读者需要注意。在这种情况下，操作可能会造成人身伤害。**

相关文档

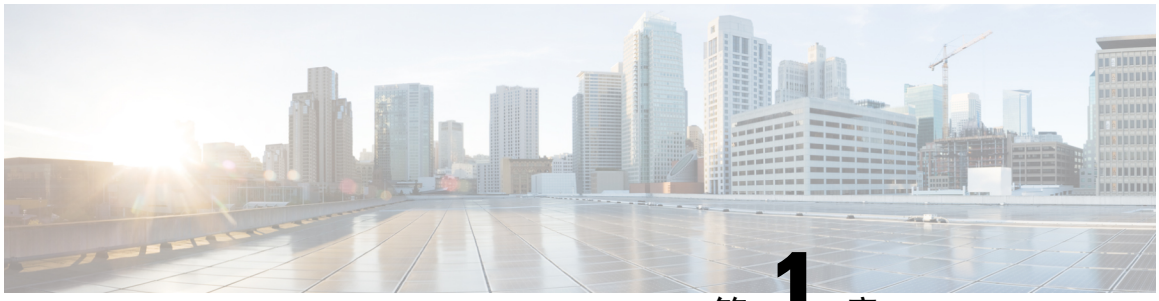
下表列出 Cisco.com 上提供的相关配套技术文档。

文档标题	位置
思科安全 ACS 至思科 ISE 迁移工具 2.1.0 版本说明	https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html
《思科身份服务引擎管理员指南》版本 2.1	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 2.1 版本说明	http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html

获取文档和提交服务请求

有关获取文档、使用思科缺陷搜索工具 (BST)、提交服务请求和收集其他信息的说明，请参阅思科产品文档更新。

要将新的和经过修订的思科技术内容直接接收到您的桌面，您可以订阅。RSS 源是一项免费服务。



第 1 章

使用入门

本章详细介绍用于将数据从思科安全 ACS（版本 5.5 或更高版本）迁移至思科 ISE（版本 2.4）系统的思科安全 ACS 到思科 ISE 迁移工具。

- 迁移概述， 第 1 页
- 将数据从思科安全 ACS 迁移至， 第 1 页
- 思科安全 ACS 至思科 ISE 迁移工具， 第 2 页
- 系统要求， 第 3 页
- 迁移工具增强功能， 第 3 页

迁移概述

由于思科安全 ACS 5.x 与思科 ISE 平台在操作系统、数据库和信息模式方面有所不同，所以需要使用迁移应用来读取思科安全 ACS 中的数据，并在思科 ISE 中创建相应的数据。您可以在安装思科 ISE 后运行迁移应用。迁移应用是思科提供的一个实用程序，用于从思科安全 ACS 提取配置信息，并导入到思科 ISE 中。迁移管理员可以在整个迁移过程中查看当前的进度以及与 ACS 配置相关的详细日志，以进行故障排除。对于不迁移的对象、属性和策略，迁移工具会显示警告消息。迁移后，我们强烈建议您验证迁移的配置（尤其是策略集）是否适当。

将数据从思科安全 ACS 迁移至

在将现有的思科安全 ACS 版本 5.5 或 5.6 的数据迁移至思科 ISE 版本 2.4 的虚拟机或设备之前，请确保您已阅读并理解所有设置、备份和安装说明。

我们建议您在充分理解思科安全 ACS 版本 5.5 或 5.6 与思科 ISE 版本 2.4 系统之间的相关数据结构和方案差别之后，再尝试迁移现有的思科安全 ACS 版本 5.5 或 5.6 的数据。

在从思科安全 ACS 版本 5.5 或 5.6数据库迁移至思科 ISE 版本 时，数据迁移可实现以下功能：

- 在思科 ISE 版本 中支持思科安全 ACS 版本 5.5 或 5.6的功能。
- 在从思科安全 ACS 版本 5.5 或 5.6 迁移数据后，可支持思科 ISE 版本 中的新功能。

注释 由于每个思科安全 ACS 或思科 ISE 版本的功能差异是动态变化的，所以并非所有思科安全 ACS 数据都可以迁移到思科 ISE。从思科安全 ACS 版本 5.5 或 5.6 迁移至思科 ISE 版本 可以最大限度减少配置差异（即可在思科 ISE 中支持以前不支持的思科安全 ACS 功能）。

注释 由于思科 ISE 的数据和思科安全 ACS 的数据在命名约定、策略层次结构、预定义对象等方面有所不同，所以迁移工具可能无法支持所有对象。但是对于无法迁移的对象，迁移工具会显示警告和错误消息，以帮助您采取更正措施。

支持的数据迁移路径

您无法将数据从 3.x、4.x 和 5.x 版本思科安全 ACS 迁移至 1.0 版本思科 ISE，但是之前数据迁移仅支持从 5.1 版本思科安全 ACS 至 1.0 版本思科 ISE；从 5.1/5.2 版本思科安全 ACS 至 1.1 版本思科 ISE；或从 5.3 版本思科安全 ACS 至 1.2 版本思科 ISE。

现在支持使用思科安全 ACS 到思科 ISE 迁移工具，执行从思科安全 ACS 版本 5.5 或 5.6 到思科 ISE 版本 的数据迁移。您还可以将思科安全 ACS 版本 3.x 升级至思科安全 ACS 版本 4.x，然后升级至思科安全 ACS 版本 5.5 或 5.6 。

思科安全 **ACS** 至思科 **ISE** 迁移工具

运行迁移工具之前，请确保您已升级至思科 ISE 版本，并且已安装思科安全 ACS 版本 5.5、5.6 的最新补丁。

此迁移工具可帮助您将数据从思科安全 ACS 版本 5.5 或 5.6 迁移至思科 ISE 版本 2.4 系统。此工具的设计解决了由于基本硬件平台和系统、数据库以及数据架构之间的差异而固有的一些迁移问题。

此迁移工具可在 Linux 系统和 Windows 系统上运行，其工作方式为：导出思科安全 ACS 数据文件，分析数据，并根据需要进行必要的数据修改，以便将数据转换为可供思科 ISE 版本 2.4 系统使用的格式加以导入。

- 此迁移工具最大程度地减少了所需的用户交互，而且可以迁移完整的配置数据集。
- 此迁移工具为您提供关于不支持的对象的完整列表。

思科安全 ACS 版本 5.5 或 5.6 和思科 ISE 版本 2.4 应用可以在相同类型的物理硬件上运行，也可以在不同类型的物理硬件上运行。此迁移工具使用思科安全 ACS 编程接口 (PI) 和思科 ISE 具象状态传输 (REST) 应用程序编程接口 (API)。思科安全 ACS PI 和思科 ISE REST API 允许思科安全 ACS 和思科 ISE 应用在支持的硬件平台或 VMware 服务器上运行。由于思科安全 ACS 被视为封闭设备，所以不允许直接在思科 ACS 设备上运行此迁移工具。反之，思科安全 ACS PI 以规范化格式读取和返回配置数据。思科 ISE REST API 执行验证并将导出的思科安全 ACS 数据规范化，将其保留为适用于思科 ISE 软件的形式。

系统要求

表 *1:* 迁移工具的系统要求

操作系统	迁移工具可在 Windows 和 Linux 计算机上运行。该计算机上应安装 1.7 或更高版本的 Java。
最小磁盘空间	所需的最小磁盘空间为 1 GB。 此所需空间不仅用于安装迁移工具，也用于存储迁移数据以及生成报告和日志。
最小 RAM	所需的最小 RAM 为 2 GB。 如果您有大约 300,000 个用户、50,000 台主机、50,000 台网络设备，我们建议您至少要有 2 GB 的 RAM。

表 *2:* 源和目标迁移计算机的系统要求

平台	要求
思科安全 ACS 版本 5.5 或更高版本	确保已将思科安全 ACS 源计算机配置为具有同一 IP 地址。
思科 ISE 版本 2.4	确保思科 ISE 目标计算机至少有 2GB 的 RAM。
迁移计算机 - 确保迁移计算机至少有 2GB 的 RAM。	
64 位 Windows 和 Linux	安装 1.7 或更高版本的 64 位 Java JRE。如果迁移计算机上未安装 Java JRE，迁移工具将无法运行。
32 位 Windows 和 Linux	安装 1.7 或更高版本的 32 位 Java JRE。如果迁移计算机上未安装 Java JRE，迁移工具将无法运行。

迁移工具增强功能

迁移工具支持以下功能：

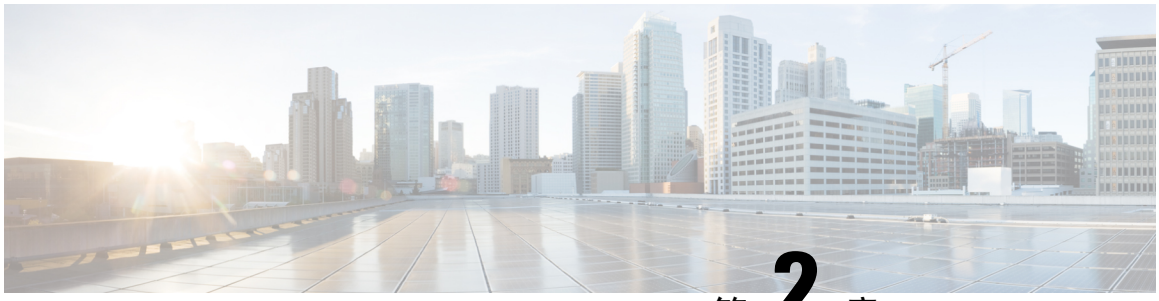
- 迁移基于 RADIUS 或 TACACS 的配置 - 迁移工具允许您选择迁移对象是特定于 RADIUS 还是 TACACS。如果您的思科安全 ACS 部署仅包括 TACACS 或 RADIUS 配置，您可以选择相应的选项。
    - RADIUS 配置 - 迁移除 TACACS 特定配置（例如 Shell 配置文件、命令集和接入服务 [设备管理]）之外的所有配置。

- TACACS 配置 - 迁移除 RADIUS 特定配置（例如授权配置文件和接入服务 [网络访问]）之外的所有配置。

在现有思科 ISE 安装中执行迁移，或从不同的思科安全 ACS 部署迁移到同一个思科 ISE 服务器时：

- 如果思科 ISE 中不存在同名的对象，迁移工具会创建该对象。
- 如果思科 ISE 中已存在同名的数据对象，迁移工具会显示警告消息“对象已经存在/资源已经存在”(object already exists/resource already exists) 以及对象名称的详细信息。
- 在执行基于 TACACS 或 RADIUS 的迁移时，如果思科 ISE 中已存在同名的网络设备，协议设置将自动更新。

- 选择对象迁移 - 迁移工具还支持选择要从思科安全 ACS 迁移到思科 ISE 的高级配置组件，例如预定义的参考数据、、字典、外部服务器、用户和身份库、设备、策略元素和访问策略。建议在执行选择对象迁移之前仔细参考对象级依赖关系列表。您可以根据需要，选择迁移所有受支持的配置组件，或仅从配置组件列表中选择一部分高级配置组件。您可以根据“导出和策略差异分析报告”来执行此选择对象迁移功能。
- 对象名称中的特殊字符 - 如果思科安全 ACS 中的数据对象的名称包含任何不受思科 ISE 支持的特殊字符，迁移工具会将不受支持的特殊字符转换为下划线 (_)，再将数据对象迁移至思科 ISE。在导出报告中，经过自动转换处理的数据对象会带有警告提示。但是，如果 LDAP 和 AD 属性、RSA、RSA 域提示符、内部用户和任何预定义的参考数据中包含不受思科 ISE 支持的特殊字符，导出过程将会失败。
- 迁移 IP 地址范围在最后一个八位组的网络设备 - 迁移工具通过将 IP 地址范围转换为对应的子网或单一 IP 地址，支持迁移配置的 IP 地址范围在最后一个八位组的网络设备。例如：10.197.64.40-50 将被转换为 10.197.64.40/29、10.197.64.48/32、10.197.64.49/32 和 10.197.64.50/32。
- 增强帮助 - 在迁移工具的用户界面中，您可以导航至**帮助 > 迁移工具的使用**，以查看迁移工具中的可用选项的详细信息。



第 2 章

安装迁移工具

本章提供关于如何安装思科安全 ACS 至思科 ISE 迁移工具的指南。

- 迁移工具安装指南， 第 5 页
- 安全注意事项， 第 5 页
- 迁移工具初始化， 第 6 页

迁移工具安装指南

- 确保您的环境已做好迁移准备。除了思科安全 ACS 版本 5.5 或 5.6 Windows 或 Linux 源计算机之外，您还必须部署一个安全外部系统（该系统具有一个用于执行双设备迁移（迁移分布式部署中的数据）的数据库），并拥有一个思科 ISE 版本 2.4 设备作为目标系统。
- 确保您已为思科安全 ACS 版本 5.5 或 5.6 源计算机配置了单一 IP 地址。如果每个接口都有多个 IP 地址别名，则在迁移期间迁移工具可能会出现故障。
- 如果是在同一设备上执行从思科安全 ACS 至思科 ISE 的迁移，请确保备份 ACS 配置数据。
- 确保您已完成以下任务：
  - 如果这是双设备迁移，您已在目标计算机上安装思科 ISE 版本 2.4 软件。
  - 如果这是单设备迁移，您可使用思科 ISE 版本 2.4 软件对设备或虚拟机进行重新映像。
  - 拥有所有相应的思科安全 ACS 版本 5.5 或 5.6 和思科 ISE 版本 2.4 的凭证和密码。
- 确保您可以在源计算机和安全外部系统之间建立网络连接。

安全注意事项

迁移过程的导出阶段创建用作导入过程输入的数据文件。此数据文件的内容会加密，无法直接读取。

您需要知道思科安全 ACS 版本 5.5 或 5.6 和思科 ISE 版本 2.4 的管理员用户名和密码，才能导出思科安全 ACS 数据，并将其成功导入到思科 ISE 设备。您应该使用专用用户名，确保导入实用程序所创建的记录在审核日志中可以被识别。

您必须输入主要思科安全ACS服务器和思科ISE服务器的IP地址（或主机名），以及管理员凭证。当您通过身份验证后，迁移工具会继续以类似于升级的形式迁移全套已配置的数据项目。运行迁移工具之前，请确保您已在 ACS 服务器上启用 IP 接口，并在 ISE 服务器上启用 ACS 迁移接口。

迁移工具初始化

开始之前

您只能在满足以下条件时运行迁移工具：刚刚完成思科 ISE 安装；使用 **application reset-config** 命令重置思科 ISE 应用配置并清空思科 ISE 数据库。因此，迁移过程完成之前，不得启用思科 ISE FIPS 模式。

迁移工具完成初始化后会弹出一个消息框，您可以在其中选择所要迁移的配置类型，包括：所有受支持的对象、RADIUS 配置（例如身份验证配置文件、接入服务 [网络访问] 等）或 TACACS 配置（例如命令集、Shell配置文件、接入服务 [设备管理] 等）。迁移工具会针对其无法迁移的不受支持（或部分支持）的对象提供一个列表，以及一个对象级依赖关系列表。您也可以在思科安全ACS至思科 ISE 迁移工具的用户界面中选择**帮助 > 不受支持对象的详细信息和对象级依赖关系列表**，以查看不支持的对象的列表。

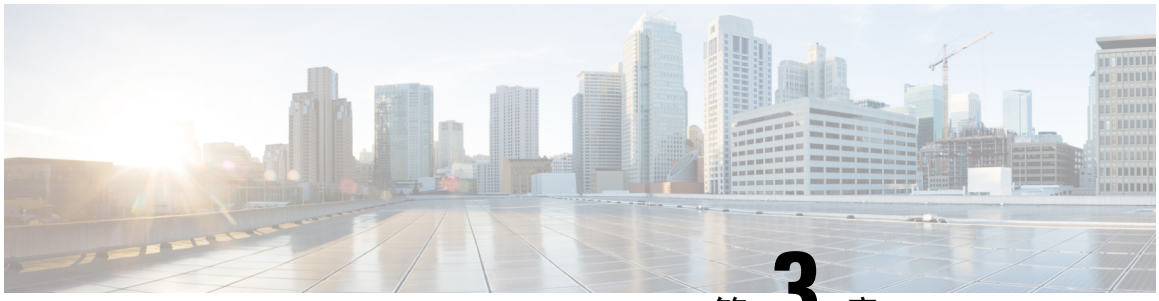
注释 您可以在全新安装的思科 ISE 上执行迁移，也可以在现有思科 ISE 系统中执行迁移。如果要迁移的对象已存在于思科 ISE 中，您会收到一条警告消息，迁移工具将忽略该对象；如果要迁移的对象在思科 ISE 中不存在，迁移工具将在思科 ISE 中创建该对象。

步骤 1 点击 **migration.bat** 批处理文件启动迁移工具。
屏幕上将显示“迁移选择选项”窗口。

步骤 2 在迁移选项列表中，点击与您想要选择的迁移选项对应的单选按钮。

- 所有受支持对象的配置 - 显示所有受支持的对象。
- RADIUS 配置（例如身份验证配置文件、接入服务 [网络访问] 等）- 仅显示 RADIUS 相关对象和通用对象。
- TACACS 配置（例如命令集、Shell 配置文件、接入服务 [设备管理] 等）- 仅显示 TACACS 相关对象和通用对象。

步骤 3 在弹出窗口中，点击**是**显示不受支持和部分支持的对象列表，以及对象级迁移依赖关系列表。



第 3 章

制定迁移计划

本章提供必要的信息来帮助您制定迁移计划。仔细制定迁移计划可确保迁移过程顺利进行，并降低迁移失败的风险。

- 必备条件， 第 7 页
- 数据迁移时间估算， 第 8 页
- 从思科安全 ACS 版本 5.5 或 5.6进行迁移之前的准备工作， 第 9 页
- 策略服务迁移指南， 第 9 页
- 思科安全 ACS 策略规则迁移指南， 第 10 页

必备条件

本节说明执行迁移过程的必备条件。

启用迁移接口

您必须在思科安全 ACS 和思科 ISE 服务器上启用数据迁移接口，才能开始执行迁移过程。建议在迁移过程完成后禁用思科安全 ACS 和思科 ISE 服务器的迁移接口。

步骤 1 在思科安全 ACS CLI 中输入以下命令，以在思科安全 ACS 计算机上启用迁移接口：

acs config-web-interface migration enable

步骤 2 执行以下任务，在思科 ISE 服务器上启用迁移接口：

a) 在思科 ISE CLI 中，输入 **application configure ise**。

b) 输入 **11**，以启用/禁用 ACS 迁移。

c) 输入 **Y**。

注释 在迁移过程完成后，使用以下命令禁用思科安全ACS计算机上的迁移界面：**acs config-web-interface migration disable**。

注释 迁移过程完成后，在思科安全 ISE 服务器上禁用迁移接口。

启用在迁移工具中可信证书

开始之前

从思科 ISE 将迁移工具下载到客户端计算机。要允许从思科安全 ACS 服务器向（客户端计算机上的）迁移工具导出数据，您可以选择信任思科安全 ACS CA 证书或思科安全 ACS 管理证书。

要允许从迁移工具向思科 ISE 服务器导入数据，您可以选择信任思科 ISE CA 证书或思科 ISE 管理证书。

要在迁移工具中启用可信证书，请执行以下操作：

- 在思科安全 ACS 中，确保服务器证书在**系统管理** > **配置** > **本地服务器证书** > **本地证书**页面中。在“ACS5 证书”对话框中，输入证书的公用名称（“使用者”字段中的 CN 属性）或 DNS 名称（“使用者替代名称”字段中），以便与思科安全 ACS 建立连接并从中导出数据。
- 在思科 ISE 中，确保服务器证书在**管理** > **系统** > **证书** > **证书管理** > **系统证书**页面中。在“ISE 证书”对话框中，输入公用名称（“使用者”字段中的 CN 属性）或 DNS 名称（“使用者替代名称”字段中），以便与思科 ISE 建立连接并从迁移工具导入数据。

步骤 1 在思科安全 ACS 至思科 ISE 迁移工具窗口中，点击**设置** > **可信证书** > **添加**，添加思科安全 ACS 和思科 ISE 证书，以启用可信通信。

您可以在迁移工具中查看或删除证书。

步骤 2 在**打开**对话框中，选择包含可信 root 证书的文件夹，然后点击**打开**将所选思科 ISE 证书添加到迁移工具。

步骤 3 重复上一步，添加思科安全 ACS 证书。

数据迁移时间估算

思科安全 ACS 至思科 ISE 迁移工具可能会需要大约 20 小时来迁移 10,000 台设备、25,000 个用户、100,000 台主机、100 个身份组、420 个可下载访问控制列表 (DACLs)、320 份授权配置文件、6 个设备分级和 20 个网络设备组 (NDG)。

对于下列配置，迁移工具所需的迁移时间约为 52 小时：

- 4 个 LDAP
- 1,000 个身份组
- 500 个用户身份组
- 20 个网络设备位置
- 100 个网络设备组
- 25 个接入服务
- 50 个 SSP
- 600 个可下载访问控制列表 (DACL)
- 320 条授权规则
- 600 个授权配置文件（无论是否包含策略集）
- 20 个命令集和 Shell 配置文件（每个命令集包含 100 条命令）
- 40 个策略集（受最大规则数限制）
- 20 个自定义用户字典
- 100,000 个网络设备
- 300,000 个用户
- 150,000 台主机

从思科安全 ACS 版本 5.5 或 5.6进行迁移之前的准备工作

我们建议您在从思科安全 ACS 成功迁移之后不要更改为 Simple 模式。否则，您可能会丢失思科 ISE 中的所有已迁移的策略。您无法恢复这些已迁移的策略，但是您可以从 Simple 模式切换至 Policy Set 模式。

在您开始将思科安全 ACS 数据迁移至思科 ISE 之前，必须考虑以下事项：

- 仅在思科 ISE 版本 2.4 的策略集模式下迁移思科安全 ACS 版本 5.5 或 5.6 的数据。
- 在全新安装的思科 ISE 版本 上执行迁移。在思科 ISE 中，选择**管理 > 系统 > 设置 > 策略集**，以启用策略集。
- 在服务选择策略 (SSP) 中每启用一条规则，都会生成一个策略集，并按照 SSP 规则的顺序进行排列。

注释 SSP 默认规则生成的服务将成为思科 ISE 版本 2.4 中的默认策略集。对于在迁移过程创建的所有策略集，第一个匹配的策略集就是匹配的类型。

策略服务迁移指南

您必须执行以下检查，确保策略服务从思科安全 ACS 迁移至思科 ISE：

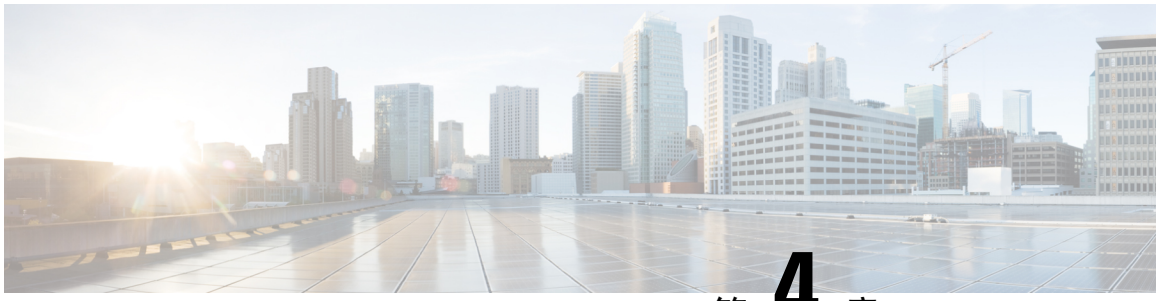
- 如果服务选择策略 (SSP) 中包含在思科安全 ACS 版本 5.5 或 5.6中禁用或监控的 SSP 规则，这些规则不会迁移到思科 ISE。
- 如果服务选择策略 (SSP) 中包含在思科安全 ACS 版本 5.5 或 5.6中启用的 SSP 规则，
  - 如果请求设备管理服务，则无法迁移至思科 ISE。（思科 ISE 不支持设备管理。）
  - 若这些规则用于请求包含“组映射”策略的服务，则无法迁移至思科 ISE。（思科 ISE 不支持组映射策略。）
  - 如果请求服务而且其身份策略包含规则，这些规则导致使用 RADIUS 身份服务器，则无法迁移至思科 ISE。（思科 ISE 与之不同，其使用 RADIUS 身份服务器进行身份验证。）
  - 如果请求服务而且此服务具有使用思科 ISE 不支持的属性或策略元素的策略，则无法迁移至思科 ISE。

思科安全 ACS 策略规则迁移指南

鉴于安全因素以及数据完整性，当无法迁移规则时，无法整体迁移策略模型。您可以在 Policy Gap Analysis Report 中查看有问题的规则的详细信息。如果您不修改或删除不支持的规则，则策略无法迁移至思科 ISE。

一般而言，在将数据从思科安全 ACS 版本 5.5 或 5.6 迁移至思科 ISE 版本 2.4 时必须考虑以下规则：

- 不迁移包含特殊字符的对象。
- 枚举类型的属性（RADIUS、VSA、身份和主机）按照采用允许值的整数迁移。
- 所有终端属性（无论属性数据类型如何）都按照字符串数据类型迁移。
- RADIUS 属性和 VSA 值无法过滤并添加至思科 ISE 日志。



第 4 章

持续数据传输程序

本章介绍如何使用迁移工具导出思科安全 ACS 版本 5.5 或 5.6 的数据并将其导入到思科 ISE 版本 2.4 系统。

- 从思科安全 ACS 导出数据，第 11 页
- 分析思科 ISE 与思科安全 ACS 之间的策略差异，第 14 页
- 将数据导入到思科 ISE，第 16 页
- 思科 ISE 中迁移的数据验证，第 19 页

从思科安全 ACS 导出数据

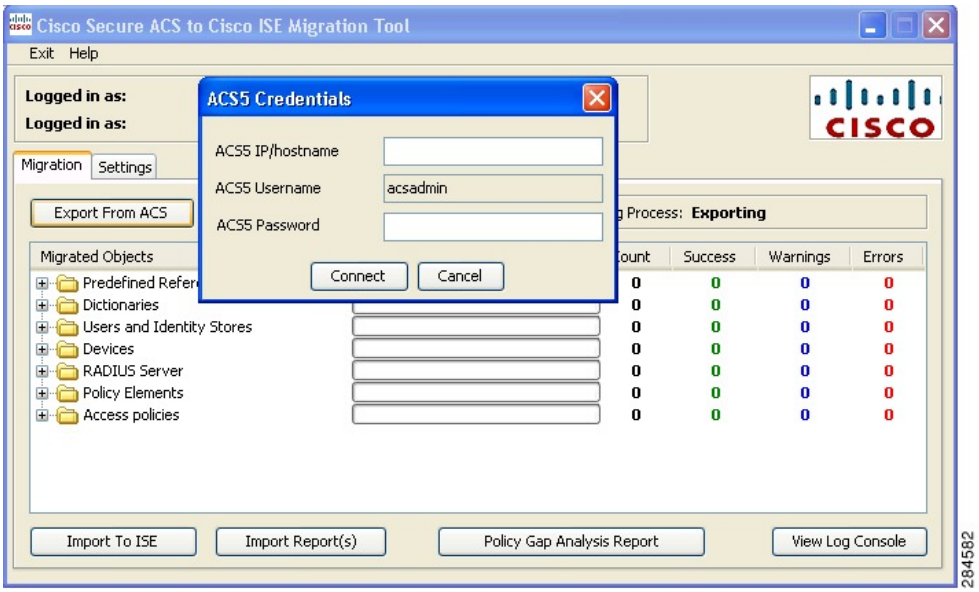
启动迁移工具后，完成下列步骤，将数据从思科安全 ACS 导出至迁移工具。

步骤 1 在思科安全 ACS 至思科 ISE 迁移工具窗口中，点击**设置**显示可以迁移的数据对象的列表。

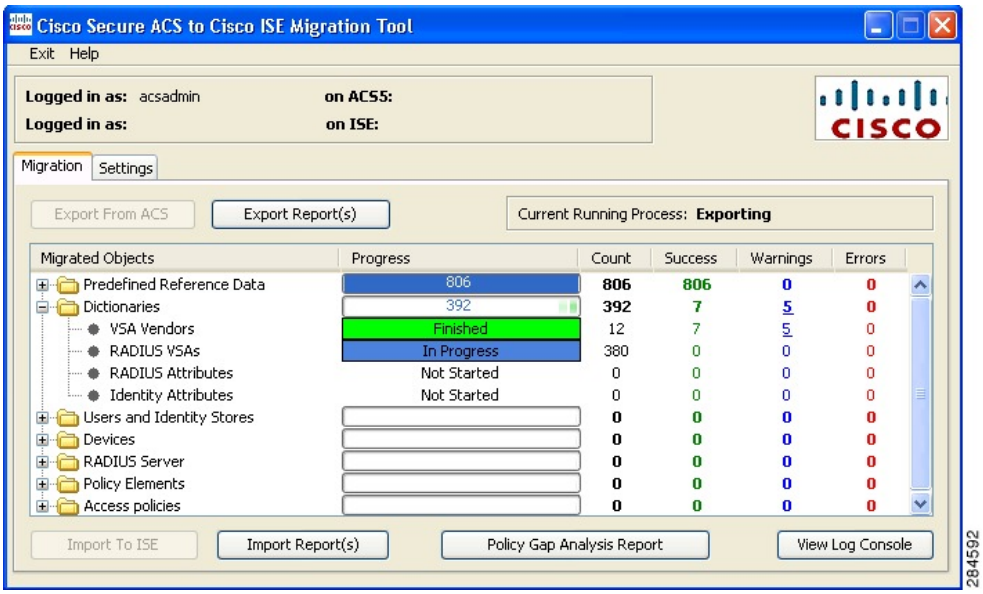
步骤 2 （可选）要执行迁移，不一定必须配置处理依赖关系。选中您想要导出的数据对象的复选框，以防其依赖关系数据丢失，然后点击 **Save**。

步骤 3 在 Cisco Secure ACS to Cisco ISE Migration Tool 窗口，点击 **Migration**，然后点击 **Export From ACS**。

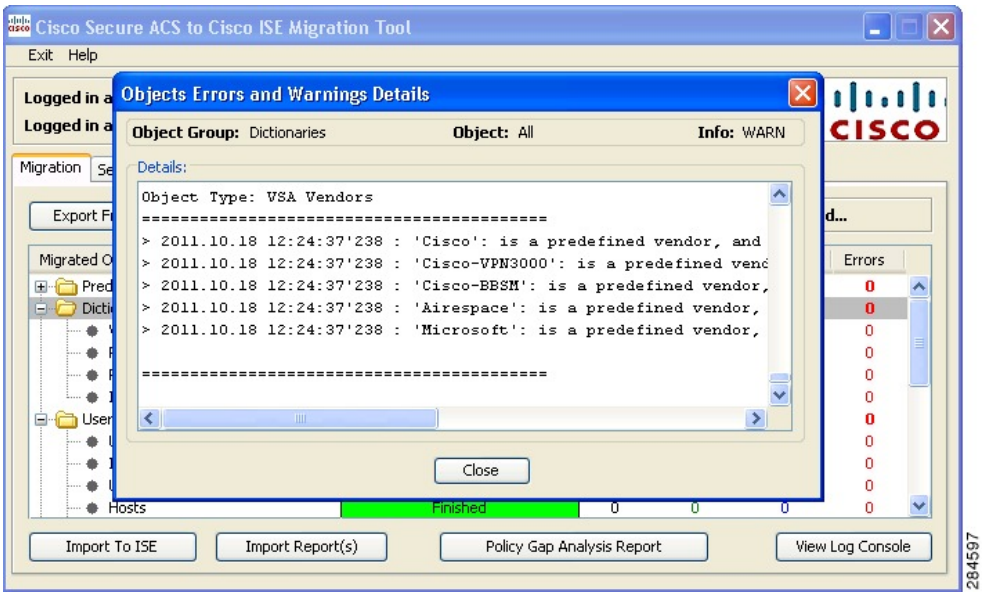
步骤 4 对于思科安全 ACS 版本 5.5 或 5.6 系统，密码，然后点击“ACS5 凭证”窗口中的**连接**。



步骤 5 监控 Cisco Secure ACS to Cisco ISE Migration Tool 窗口中的迁移过程，此窗口显示当前成功导出的对象数量并列出触发警告或错误的所有对象。

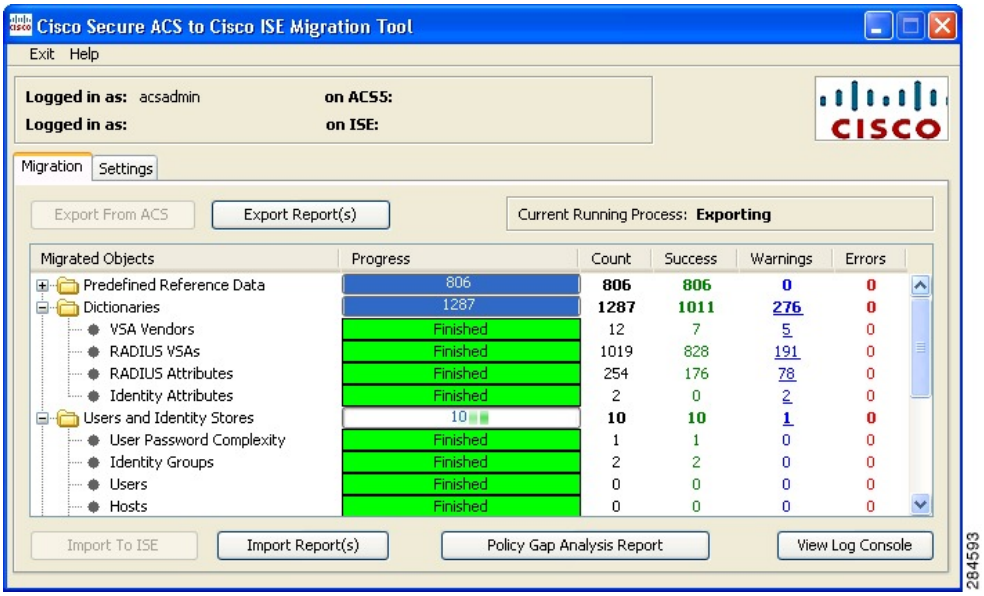


步骤 6 要获取关于在导出过程中发生的警告或错误的详细信息，请在 Migrations 选项卡上点击 Warnings 或 Errors 栏中带下划线的任意数字。Object Errors and Warnings Details 窗口显示导出期间发生的警告或错误的结果。其提供发生警告或错误的对象组、类型以及日期和时间。

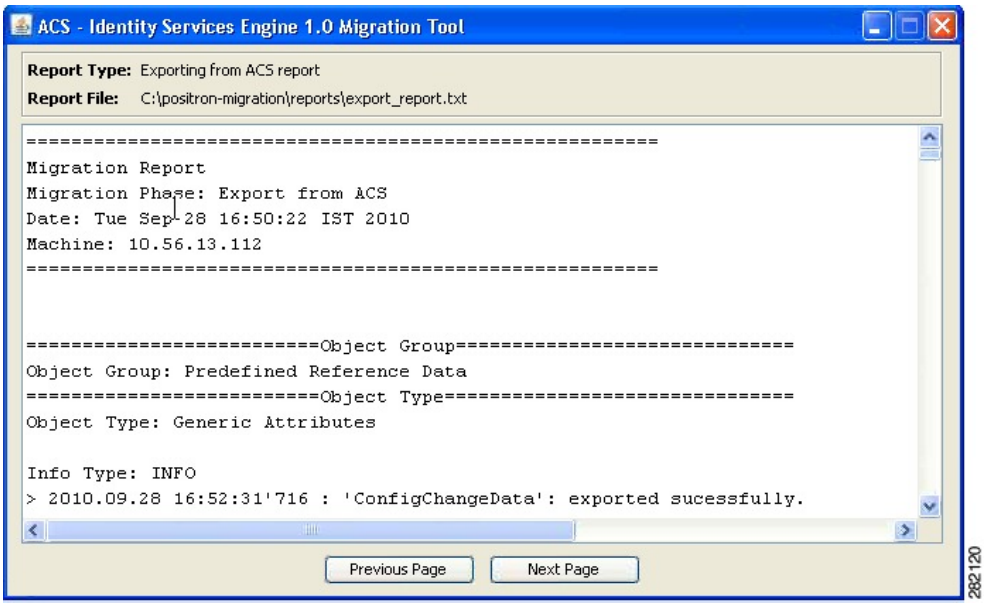


步骤 7 滚动显示所选对象错误的详细信息，然后点击 **Close**。

步骤 8 数据导出过程完成后，思科安全 ACS 至思科 ISE 迁移工具窗口将显示导出状态：“导出完成”。



步骤 9 点击 **Export Report(s)** 可查看导出报告的内容。每个导出报告都包含标题信息，包括操作类型、日期和时间、以及系统 IP 地址或主机名。每个对象组都会详细说明类型和相关信息。报告结尾为操作的开始和结束日期、时间以及持续的时间。



步骤 10 要分析思科安全 ACS 和思科 ISE 之间的策略差异，请点击 **Policy Gap Analysis Report**。

分析思科 ISE 与思科安全 ACS 之间的策略差异

导出数据后，管理员应分析导出报告和策略差异报告，修复报告中列出的ACS配置错误，并解决出现的警告和其他问题。

根据目前的观察，从思科安全 ACS 迁移至思科 ISE 会导致配置集出现以下差异。您可以对其中的一些差异进行校正。

- **身份组**
  - 内部用户问题
    - 思科安全 ACS 与思科 ISE 之间的奇偶校验差异
      - 密码类型
      - 下次登录时更改密码
      - 更改密码
      - 命名约束
  - 外部身份库会顺利完成迁移。但是您必须检查名称。
- **网络设备或网络设备组**
  - 网络设备迁移警告（思科 ISE 2.1）

- 思科 ISE 中不支持的 IP 范围
  - 排除仅适用于重叠的 IP
- 仅 IPV4
- 默认设备必须启用 RADIUS

- 迁移工具校正流程
  - 如果设备在思科 ISE 中不存在（即 IP 配置不重叠），在迁移过程中，迁移工具会自动添加该设备。
  - 如果设备已存在（IP 或子网完全匹配且名称也完全匹配），迁移工具将添加 TACACS+ 元素
  - 如果设备已存在（IP/子网完全匹配或名称完全匹配），迁移工具将报错

- **授权结果**

  命令集和 Shell 配置文件会顺利完成迁移。对象名称会出现不一致。
  - 思科 ISE 会严格地以名称为准
  - 策略结果名称空间将与网络访问用户共享
    - 建议对设备管理授权结果使用前缀

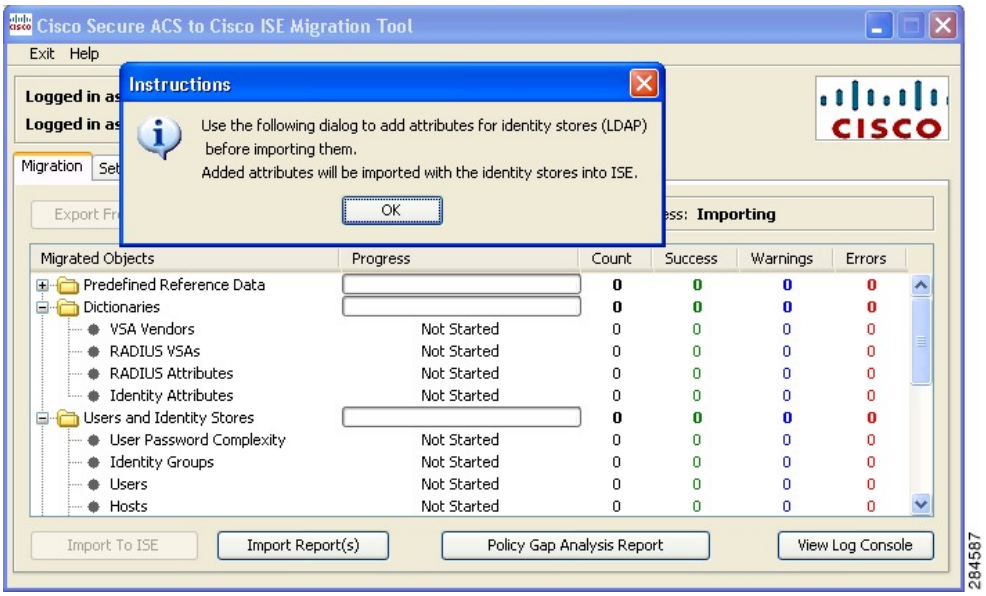
- **Policies**
  - “思科安全 ACS 5.x 接入服务”将从“服务选择策略”分离
    - 可以包含未购买使用的服务
    - 可以包含由不同的服务选择规则选择的服务
  - 思科安全 ACS 5.x 组映射
    - 可以从思科安全 ACS 4.x 传输组映射
    - 组映射的内容必须迁移到思科 ISE 的授权策略
  - 可以使用协议进行身份验证
    - 思科安全 ACS 5.x 中的部分服务配置
    - 思科 ISE 中的部分策略结果

解决出现的错误或警告后，请重新执行导出过程。有关从思科安全 ACS 导出数据的过程，请参阅从思科安全 ACS 导出数据，第 11 页。

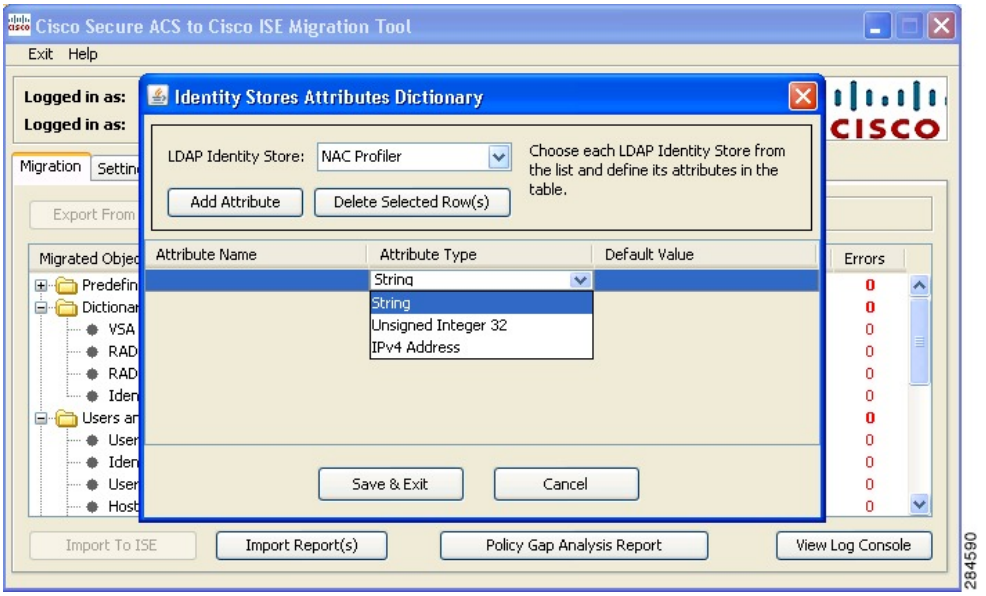
将数据导入到思科 ISE

步骤 1 在思科安全 ACS 至思科 ISE 迁移工具窗口中，点击**导入至 ISE**。

步骤 2 当系统提示您在导入思科 ISE 之前向 LDAP 身份库添加属性时，请点击 **OK**。

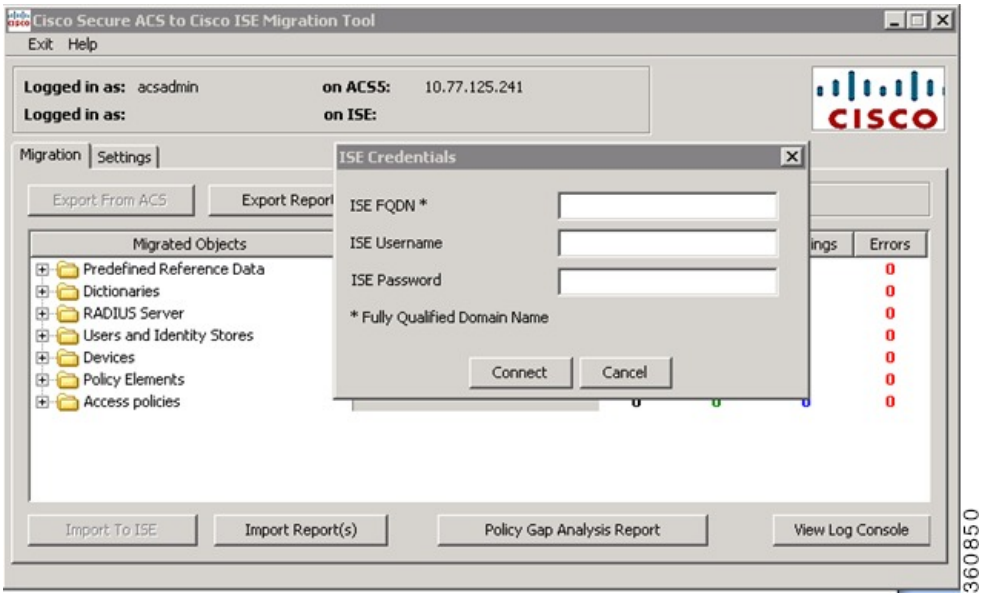


步骤 3 在 **LDAP 身份库**下拉列表中，选择您要向其添加属性的身份库，然后点击**添加属性**。



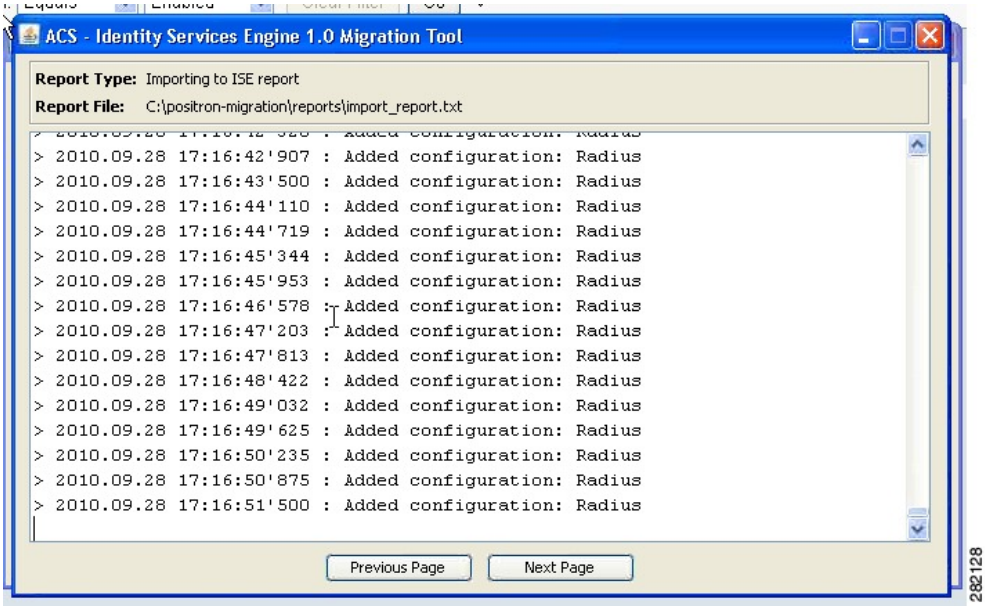
步骤 4 在**属性名称**字段输入名称，然后从**属性类型**下拉列表选择属性类型，在**默认值**字段输入值，然后点击**保存并退出**。

步骤 5 完成属性添加后，点击**导入至 ISE**，在“ISE 证书”窗口中输入思科 ISE 的完全限定域名 (FQDN)、用户名和密码，然后点击**连接**。迁移工具会通过检查确保此处输入的信息与 SSL 证书中的 FQDN 完全匹配。



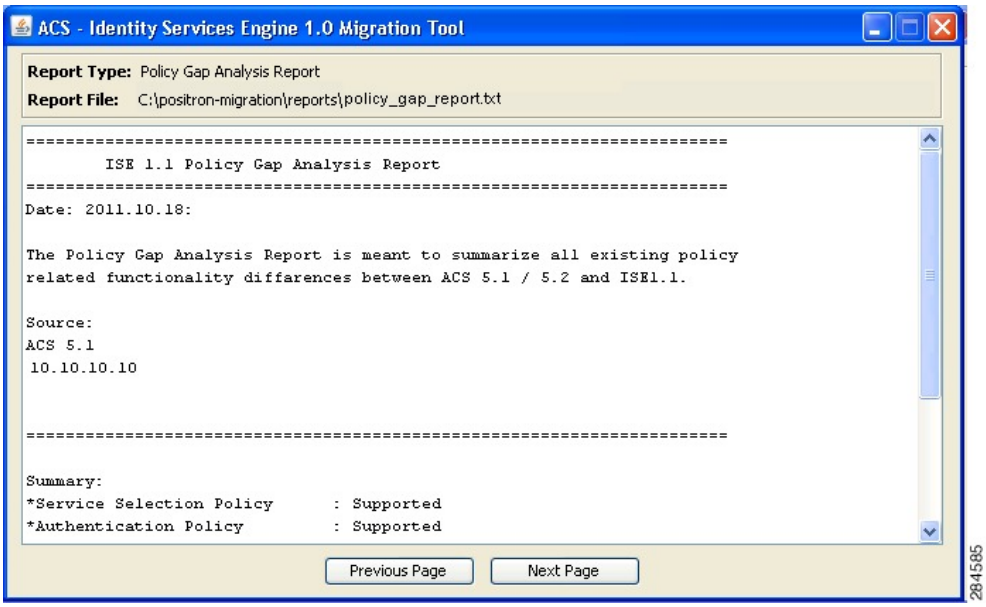
步骤 6 数据导入过程完成后，思科安全 ACS 至思科 ISE 迁移工具窗口将显示导入状态：**导入完成**。

步骤 7 要查看已导入的数据的完整报告，请点击 **Import Report(s)**。

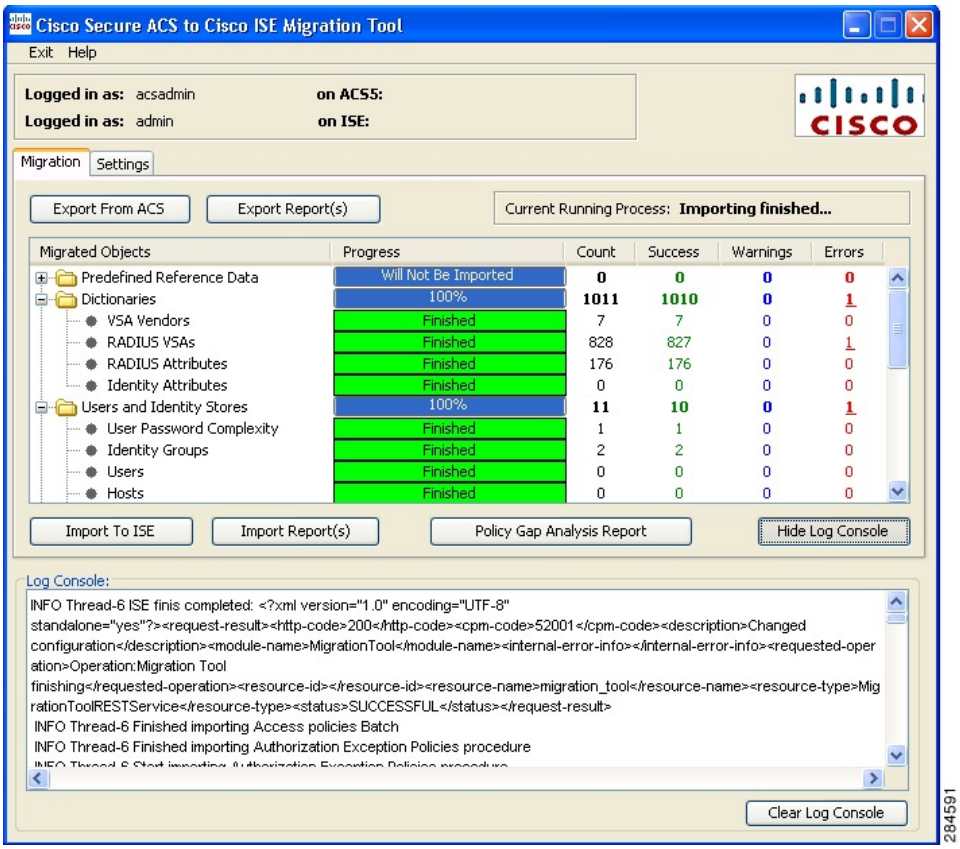


步骤 8 要获取关于在导入过程中发生的警告或错误的详细信息，在**迁移**选项卡上点击“警告”或“错误”栏中带下划线的任意数字。

步骤 9 要分析思科安全 ACS 和思科 ISE 之间的策略差异，请点击 **Policy Gap Analysis Report**。

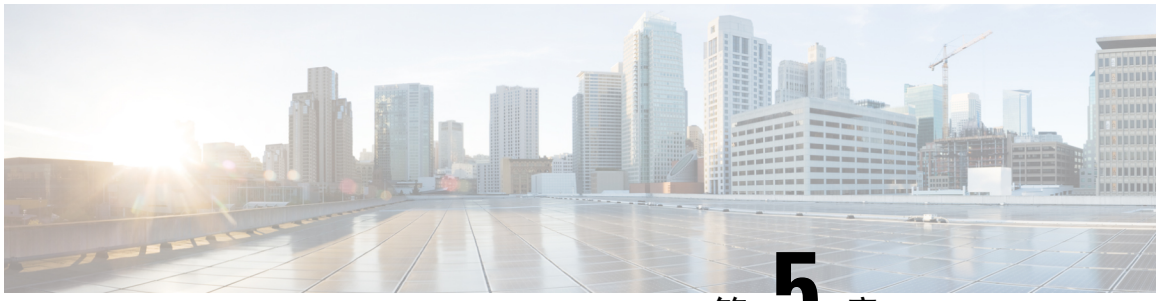


步骤 10 点击**查看日志控制台**可显示导出或导入操作的实时视图。



思科 ISE 中迁移的数据验证

要验证思科安全 ACS 数据已迁移至思科 ISE，请登录思科 ISE 并检查是否可以查看各个思科安全 ACS 对象。



第 5 章

报告

在数据迁移过程中，迁移工具会生成下列报告：导出报告、导入报告和策略差异分析报告。

如果您决定与任何人分享报告文件，或想要将其保存至其他位置，则可以在迁移工具的 Reports 文件夹中查找以下文件：

- import_report.txt
- export_report.txt
- policy_gap_report.txt

- 导出报告， 第 21 页
- 策略差异分析报告， 第 22 页
- 导入报告， 第 23 页

导出报告

此报告显示具体信息或从思科安全 ACS 数据库导出数据期间遇到的错误。报告结尾包含一个数据分析部分，此部分说明思科安全 ACS 和思科 ISE 之间的功能差异。导出报告还包含无法导入的已导出对象的错误信息。

表 *3:* 思科安全 *ACS* 至思科 *ISE* 迁移工具导出报告

报告类型	消息类型	消息说明
导出	信息	列出已成功导出的数据对象的名称。
	警告	列出由于数据对象不受思科 ISE 版本 而失败或未尝试的导出操作。

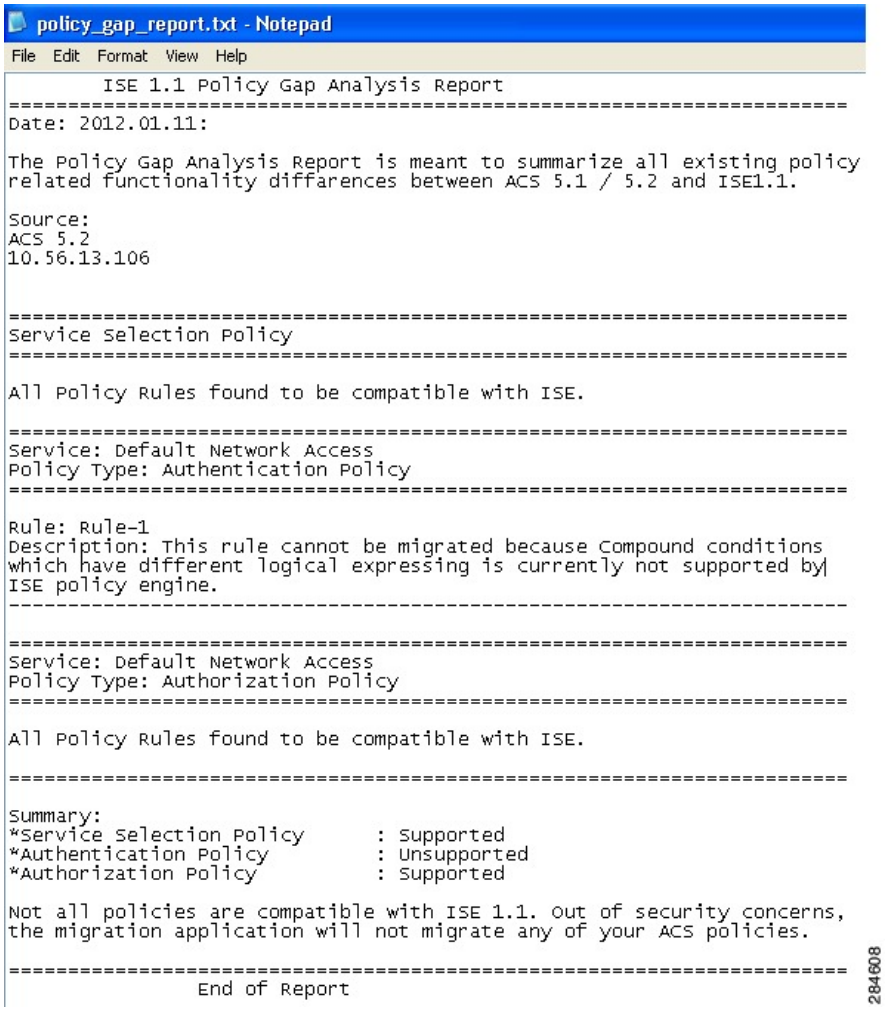
策略差异分析报告

此报告会列出有关思科安全 ACS 与思科 ISE 之间的策略差异的具体信息。在导出完成后，可以点击迁移工具用户界面上的“策略差异分析报告”按钮访问此报告。

在导出阶段，迁移工具会确定身份验证和授权策略中的差异。如有任何策略未被迁移，则会列入策略差异分析报告中。此报告列出与策略相关的不兼容规则和条件。其说明无法迁移的数据及其原因以及手动解决方案。

有些条件可以使用相应的思科 ISE 术语自动迁移，例如名称为 Device Type In 的条件被迁移为 Device Type Equals。如果条件受支持或可以自动转换，则不会显示在报告中。如果条件被发现为“Not Supported”或“Partially supported”，则不会导入此策略并且此条件会显示在报告中。执行迁移的管理员负责修改或删除这类条件。如果不修改或删除这类条件，则策略无法迁移至思科 ISE。

图 *1:* 策略差异分析报告示例

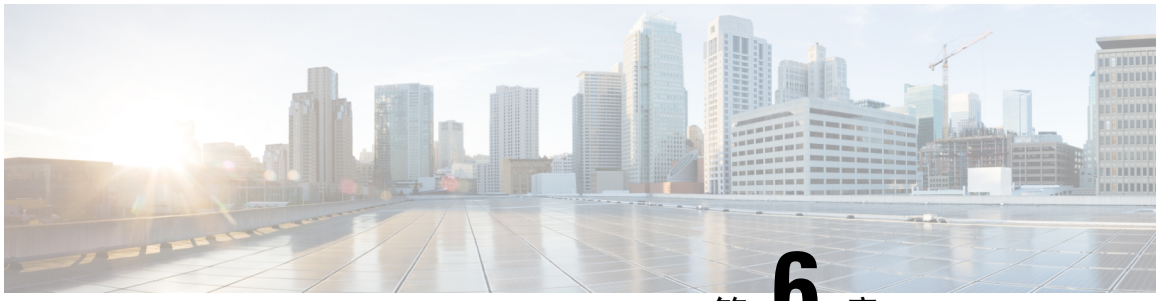


导入报告

此报告显示具体信息或在将数据导入思科 ISE 设备期间遇到的错误。

表 *4:* 思科安全 *ACS* 至思科 *ISE* 迁移工具导入报告

报告类型	消息类型	消息说明
导入	信息	列出已成功导入的数据对象的名称。
	错误	确定由于以下原因导致的数据对象错误： • 对象已存在 • 对象名称超出字符限制 • 对象名称包含不支持的特殊字符 • 对象包含不支持的数据字符



第 6 章

从更早版本的思科安全 ACS 迁移至思科 ISE

本章提供有关从更早版本的思科安全 ACS 将数据迁移至思科 ISE 的详细信息。

- 从更早版本的思科安全 ACS 迁移至思科 ISE，第 25 页

从更早版本的思科安全 ACS 迁移至思科 ISE

您可以将较早版本的思科安全 ACS 数据迁移至思科安全 ACS 版本 5.5 或 5.6 状态，以便使用迁移工具将其迁移至思科 ISE 版本 2.4 设备。

从思科安全 ACS 版本 3.x 迁移

如果您的环境中运行的是思科安全 ACS 版本 3.x，您必须升级至思科安全 ACS 版本 4.x 中支持迁移的某一个版本，然后再升级至思科安全 ACS 版本 5.5 或 5.6。

步骤 1 请参阅《思科安全 ACS 解决方案引擎 4.1 安装指南》或《思科安全 ACS 解决方案引擎 4.2 安装指南》，了解思科安全 ACS 版本 3.x 的升级路径。

步骤 2 将 3.x 版本思科安全 ACS 升级至 4.x 版本思科安全 ACS 支持迁移的版本。例如，升级至以下某个版本：思科安全 ACS 4.1.1.24、思科安全 ACS 4.1.4、思科安全 ACS 4.2.0.124 或思科安全 ACS 4.2.1。

步骤 3 完成升级之后，执行从思科安全 ACS 版本 4.x 到思科安全 ACS 版本 5.5 或 5.6 的迁移步骤。

从思科安全 ACS 版本 4.x 迁移

如果您的环境中运行的不是思科安全 ACS 版本 4.x 中支持迁移的某一个版本，请升级至能够从思科安全 ACS 版本 4.x 迁移至思科安全 ACS 版本 5.5 或 5.6的版本。

步骤 1 如果您的 4.x 版本思科安全 ACS 服务器当前运行的不是支持迁移的某个版本，请将 4.x 版本思科安全 ACS 升级至支持迁移的某个版本。

步骤 2 在迁移计算机，即 Windows 服务器上安装同一支持迁移的版本的思科安全 ACS。

步骤 3 备份 4.x 版本思科安全 ACS 数据并将其存储在迁移计算机上。

步骤 4 将 Migration 实用程序放在迁移计算机上。您可从 Installation and Recovery DVD 获取 Migration 实用程序。

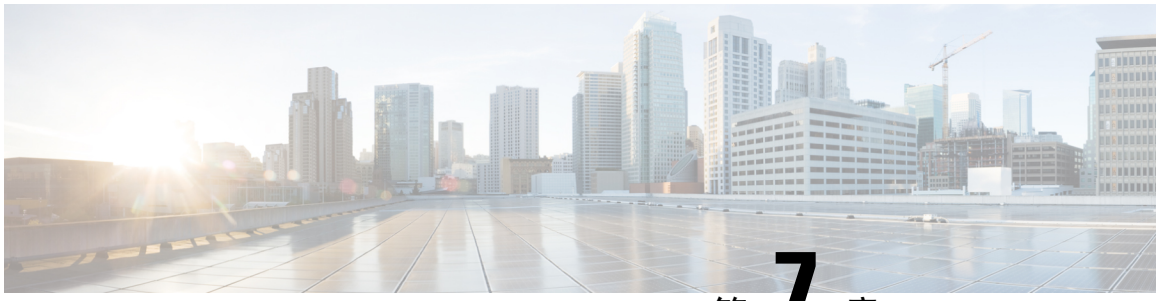
步骤 5 在迁移计算机上运行 Migration 实用程序的分析和导出阶段。

步骤 6 解决分析和导出阶段的所有问题。

步骤 7 在迁移计算机上运行迁移实用程序的导入阶段，在此阶段，迁移实用程序会将数据导入到思科安全 ACS 版本 5.5 或 5.6 服务器。

从思科安全 ACS 版本 5.x 迁移

如果您的环境中运行的是思科安全 ACS 版本 5.x，您必须升级至思科安全 ACS 版本 5.5 或 5.6。



第 7 章

策略元素

本章介绍思科 ISE 和思科安全 ACS 中的策略元素。

- 思科 ISE 与思科安全 ACS 的奇偶校验，第 27 页
- 策略模式，第 28 页
- UTF-8 支持，第 29 页
- ISE 802.1X 服务的 FIPS 支持，第 30 页

思科 ISE 与思科安全 ACS 的奇偶校验

为了与思科安全 ACS 进行奇偶校验，思科 ISE 引入了下列功能。在从思科安全 ACS 迁移到思科 ISE 时，思科 ISE 将迁移所有这些功能。

- 如果用户帐户的配置日期超过为单个用户设置的特定时间段，则禁用该用户帐户
- 如果用户帐户的配置日期超过为所有用户设置的全局特定时间段，则禁用该用户帐户
- 如果用户帐户的全局配置时间超过 n 天，则禁用该用户帐户
- 如果用户帐户处于非活动状态超过 n 天，则禁用该用户帐户
- Active Directory 中的 MAR 配置
- 使用动态属性配置的授权配置文件
- 对服务类型 RADIUS 属性使用两个新值
- 支持的内部用户数量增加到 30 万人
- 根据外部身份库密码对内部用户进行身份验证
- 在对终端无线局域网单元 (TWLU) 客户端执行 EAP-TLS 身份验证时，使用包含长度的标记
- 支持对 LDAP 身份库的组名属性使用通用名称和识别名

有关思科 ISE 和思科安全 ACS 奇偶校验功能的更多信息，请参阅《思科身份服务引擎 2.1 管理指南》。

策略模式

思科安全 ACS 和思科 ISE 都具有简单的基于规则的身份验证模式，但是思科安全 ACS 和思科 ISE 是基于不同的策略模型，这使得从思科安全 ACS 将策略迁移至思科 ISE 有点复杂。

思科安全ACS策略的层次结构以“服务选择规则”作为开始，服务选择规则可将身份验证请求重定向到接入服务。接入服务由身份策略和授权策略组成，用于根据内部或外部身份库对用户进行身份验证，然后根据定义的条件对用户进行授权。

身份验证和授权策略已从思科安全 ACS 版本 5.5 或 5.6 迁移至思科 ISE 版本 2.4。思科 ISE 版本 支持新的策略模式，即“策略集”。策略集类似于思科安全 ACS 版本 5.5/5.6 中的服务选择策略 (SSP)，因此有助于简化策略迁移过程。

思科安全 ACS 服务选择策略和思科 ISE 策略集

思科安全 ACS 版本 5.5/5.6 服务选择策略 (SSP) 根据 SSP 规则向相应的服务分配请求，其中思科 ISE 策略集保留一条规则，此规则包含策略集的输入条件。策略集的顺序与此准入规则顺序相同，类似于 SSP 规则的顺序。

多个SSP规则可能会请求思科安全ACS中相同的服务或重新使用服务。但是，每个策略集都带有自己的输入条件，因此您无法在思科 ISE 中重新使用策略集。如果您想要迁移多个 SSP 规则请求的一个服务，则必须创建属于该服务副本的多个策略集，这意味着您必须在思科 ISE 中为请求思科安全 ACS 中相同服务的每个 SSP 规则创建一个策略集。

在思科安全ACS中，您可以将SSP规则定义为被禁用或监控，而在思科ISE中策略集的同等准入规则始终处于启用状态。如果在思科安全 ACS 中 SSP 规则被禁用或监控，则 SSP 所请求的策略服务无法迁移至思科 ISE。

思科安全 ACS 策略访问服务与思科 ISE 策略集

您无需请求某个策略服务即可定义该服务，这意味着您可以在思科安全ACS中按照SSP中的规则将策略服务定义为非活动状态。思科安全 ACS 版本 5.5 或 5.6具有一项开箱即用的 DenyAccess 服务。对于思科安全ACS中的默认SSP规则，此服务既无适用策略，也无允许的协议，这样就会自动拒绝所有请求。思科 ISE 没有同等的策略集。但是，您不能使用没有准入规则的策略集，即思科 ISE 中的策略集。

允许的协议与思科安全ACS版本5.5或5.6中未设置条件（SSP中指向整个服务的条件除外）的整个服务（而不是具体策略）关联。由于思科 ISE 中设置的具有条件的外部规则，允许的协议仅指身份验证策略。

身份策略是在思科安全 ACS 版本 5.5 或 5.6中产生身份源（身份源和身份库序列）的规则的简单列表。身份验证策略有两个级别的规则：外部策略规则和内部策略规则。外部策略规则会产生允许的协议，是内部策略规则集的准入条件。内部策略规则产生身份源。

思科安全ACS版本5.5或5.6 和思科ISE版本2.4均包括一条附加到各条授权策略的可选例外策略。除了该例外策略之外，思科 ISE 版本 2.4 还提供了一条可选的影响所有授权策略的全局例外策略。

在思科安全ACS版本5.5或5.6中，则没有等同于全局例外策略的策略。在授权时，系统会首先执行本地例外策略，再执行全局例外策略和授权策略。

UTF-8 支持

思科 ISE 版本 的某些管理配置支持 8 位 Unicode 转换格式 (UTF-8)。以下配置项目使用 UTF-8 编码导出和导入：

- 网络访问用户配置
- RSA
- RADIUS 令牌
- 策略
- 身份组映射

网络访问用户配置

- 用户名
- 密码和重新输入密码
- 名字
- 姓氏
- 电子邮件

RSA

RSA 提示和消息由请求方向最终用户显示。

- 消息
- 提示

RADIUS 令牌

RADIUS令牌提示在最终用户请求方上显示。

- 身份验证选项卡 > 提示
- 管理员配置
- 管理管理员用户名和密码
- 使用 UTF-8 配置管理员

策略

- 身份验证 > 适用于 AV 表达式的值
- 授权 > 其他条件 > 适用于 AV 表达式的值
- 属性值条件
- 身份验证 > 简单条件/复合条件 > 适用于 AV 表达式的值
- 授权 > 简单条件/复合条件 > 适用于 AV 表达式的值

ISE 802.1X 服务的 FIPS 支持

迁移过程完成之前，不得启用思科 ISE FIPS 模式。

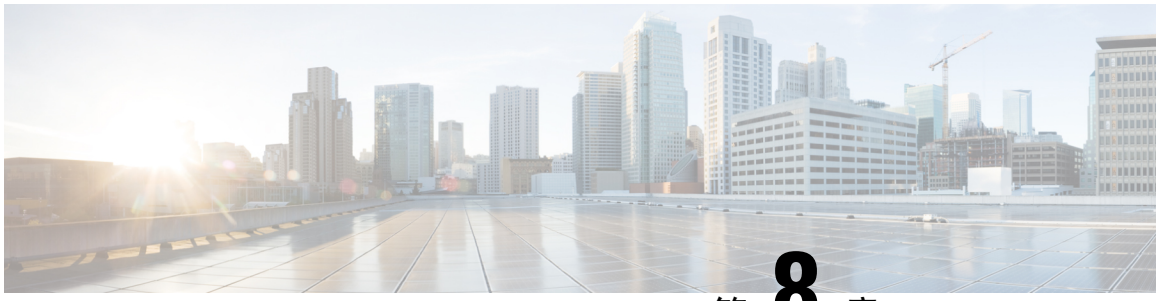
为了支持联邦信息处理标准 (FIPS)，迁移工具会迁移默认网络设备 Keywrap 数据。

兼容和支持 FIPS 的协议：

- 流程主机查询
- 可扩展身份验证协议-传输层安全 (EAP-TLS)
- 受保护的可扩展身份验证协议 (PEAP)
- EAP-通过安全隧道的灵活身份验证 (FAST)

不兼容和不支持 FIPS 的协议：

- EAP-消息摘要 5 (MD5)
- 密码身份验证协议和 ASCII
- 质询握手身份验证协议 (CHAP)
- Microsoft 质询握手身份验证协议版本 1 (MS-CHAPv1)
- Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)
- 轻量级可扩展身份验证协议 (LEAP)



第 8 章

思科安全 ACS 到思科 ISE 迁移工具故障排除

- 无法启动迁移工具， 第 31 页
- 日志中显示错误消息， 第 31 页
- 未创建默认文件夹、文件和报告， 第 32 页
- 迁移导出阶段非常缓慢， 第 33 页
- 报告向思科 TAC 问题， 第 33 页

无法启动迁移工具

情况

无法启动迁移工具。

操作

确认已在迁移计算机上安装 Java JRE 版本 1.6 或更高版本，而且已在系统路径和类路径中正确完成配置。

日志中显示错误消息

连接错误

情况

日志中显示以下错误消息：“Hosts: Connection to https://hostname-or-ip refused: null”。此外，在迁移至思科 ISE 时会报告此对象。

操作

- 确保迁移应用计算机已连接至网络并且配置正确。

- 确保思科 ISE 设备连接至网络上并且配置正确。
- 确保思科 ISE 设备和迁移计算机在网络上可以相互连接。
- 确保迁移工具与思科 ISE 连接时，思科 ISE 主要节点中使用的主机名（如有）在 DNS 内可解析。
- 确保思科 ISE 设备正常运行。
- 确保思科 ISE 应用服务器服务正常运行。

I/O 异常错误

情况

日志中显示以下错误消息：

“I/O exception (org.apache.http.NoHttpResponseException) caught when processing request: The target server failed to respond”。

操作

- 确保思科 ISE 应用服务器服务正常运行。
- 确保未超过思科 ISE Web 服务器阈值并且没有内存异常。
- 确保思科 ISE 设备 CPU 使用率不是 100% 而且 CPU 处于活动状态。

内存不足错误

情况

日志中显示以下错误消息：

“OutofMemory”。

操作

将 Java 堆大小增至至少 1 GB。

未创建默认文件夹、文件和报告

情况

迁移工具无法创建默认文件夹、日志文件、报告和持久性数据文件。

操作

确定用户有文件系统写入权限，而且有足够的磁盘空间。

迁移导出阶段非常缓慢

情况

迁移过程的导出阶段非常缓慢。

操作

开始执行迁移过程之前先重启思科安全 ACS 设备，以便释放内存空间。

报告向思科 TAC 问题

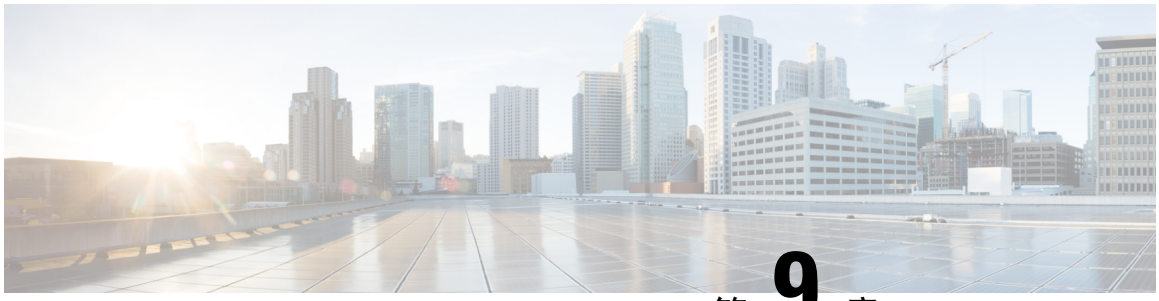
如果您无法找到某个技术问题的根源和潜在解决方案，可以联系思科客户服务代表，获取关于如何解决该问题的信息。有关思科技术支持中心 (TAC) 的信息，请参阅随您的设备一起提供的 Cisco Information Packet 出版物或访问以下网站：

http://www.cisco.com/cisco/web/support/index.html

在联系思科 TAC 之前，请确保您已准备好以下信息：

- 设备机箱类型和序列号。
- 维护协议或保修信息（请参阅 Cisco Information Packet）。
- 软件的名称、类型和版本或版本号（如果适用）。
- 您收到新设备的日期。
- 对您遇到的问题的简要说明、您为诊断或再现问题而采取的措施，以及对您为解决此问题已采取的所有措施的说明。
- 迁移日志文件 (...migration/bin/migration.log)。
- config 文件夹中的所有报告 (...migration/config)。
- 思科安全 ACS 版本 5.5 或 5.6的日志文件。
- 思科安全 ACS 版本 5.5 或 5.6 内部版本号。

注释 确保向客户服务代表提供关于在您完成初始安装之后，对思科 ISE 3300 系列设备执行的任何操作或维护的信息。



第 9 章

常见问题解答

- 常见问题解答，第 35 页

常见问题解答

如果不迁移会怎么样？

思科安全 ACS 已针对 5.7 及更早版本发布 EOL 公告。同时，思科对思科 ISE 进行了升级，以确保今后的思科 ISE 版本可以更好地与思科安全 ACS 进行奇偶校验。当思科 ISE 能够与思科安全 ACS 实现完整奇偶校验时，思科将发布思科 ACS 5.8 的 EOL 公告。思科未来的所有开发工作都将重点围绕思科 ISE 展开。思科 ISE 今后将作为面向 TACACS+ 和 RADIUS 的平台。如果您想要使用支持高级 TACACS+ 和 RADIUS 协议的安全产品，则必须迁移到思科 ISE。

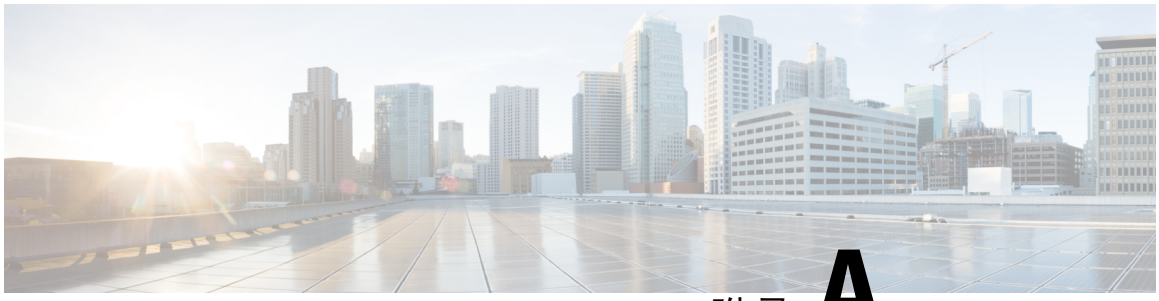
在迁移过程中，思科会提供哪些支持？

您可以参阅《迁移工具指南》，了解迁移过程的相关信息。如果需要我们协助您执行迁移，可以联系高级服务部门及思科合作伙伴。如果在迁移过程中遇到任何问题，您可以联系思科技术支持中心 (TAC) 团队。

在迁移过程中，思科 ISE 如何提供安全保护？

思科安全 ACS 至思科 ISE 迁移工具会在思科 ISE 与思科安全 ACS 之间建立安全连接；而且在将导出的数据导入思科 ISE 之前，迁移工具会以加密格式存储这些数据。

常见问题解答



附录 A

数据结构映射

此附录提供关于从思科安全 ACS 版本 5.5 或 5.6 迁移、部分迁移或未迁移至思科 ISE 版本 2.4 的数据对象的信息。

- 数据结构映射， 第 37 页
- 已迁移的数据对象， 第 37 页
- 部分迁移的数据对象， 第 39 页
- 未迁移的数据对象， 第 39 页
- 不支持的规则元素， 第 40 页
- 支持的属性和数据类型， 第 42 页
- 数据信息映射， 第 44 页

数据结构映射

从思科安全 ACS 版本 5.5 或 5.6 到思科 ISE 版本 的数据结构映射，是在导出阶段利用迁移工具分析和验证数据对象的过程。

已迁移的数据对象

以下数据对象从思科安全 ACS 迁移至思科 ISE：

- 网络设备组 (NDG) 类型和分级
- 的网络设备
- 默认网络设备
- 外部 RADIUS 服务器
- 身份组
- 内部用户
- 内部终端（主机）

数据结构映射

- 轻量级目录访问协议 (LDAP)
- Microsoft Active Directory (AD)
- RSA（部分支持，请参阅表 A-19）
- RADIUS 令牌（请参阅表 A-18）
- 证书身份验证配置文件
- 日期和时间条件（部分支持，请参阅“不支持的规则元素”）
- RADIUS 属性和供应商特定属性 (VSA) 值（请参阅表 A-5 和表 A-6）
- RADIUS 供应商字典（请参阅表 A-5 和表 A-6 的备注）
- 内部用户属性（请参阅表 A-1 和表 A-2）
- 内部终端属性
- 授权配置文件
- 可下载访问控制列表 (DACLs)
- 身份（身份验证）策略
- 授权策略（针对网络访问）
- TACACS+ 身份验证、授权和授权例外策略（针对策略对象）
- 授权异常策略（针对网络访问）
- 服务选择策略（针对网络访问）
- RADIUS 代理服务
- 用户密码复杂性
- 身份序列和 RSA 提示
- UTF-8 数据（请参阅“UTF-8 支持”页面）
- EAP 身份验证协议 - PEAP-TLS
- 用户检查属性
- 身份序列高级选项
- 策略条件中可用的其他属性 - AuthenticationIdentityStore
- 其他字符串运算符 - Start with、Ends with、Contains、Not contains
- RADIUS 身份服务器属性

部分迁移的数据对象

以下数据对象已部分从思科安全 ACS 版本 5.5 或 5.6 迁移至思科 ISE 版本 2.4：

- 属于日期类型的身份和主机属性未迁移。
- RSA sdopts.rec 文件和辅助信息未迁移。
- 多 Active Directory 域（仅限加入主要域的 Active Directory 域）可以迁移。
- 迁移针对主要 ACS 实例定义的 LDAP 配置。

未迁移的数据对象

以下数据对象没有从思科安全 ACS迁移至思科 ISE 版本 2.4：

- 监控报告
- 计划的备份
- 存储库
- 管理员、角色和管理员设置
- 客户/调试日志配置
- 部署信息（辅助节点）
- 证书（证书颁发机构和本地证书）
- 安全组访问控制列表 (SGACL)
- 安全组 (SG)
- 适用于受支持的安全组访问 (SGA) 设备的 AAA 服务器
- 安全组映射
- 网络设备准入控制 (NDAC) 策略
- SGA 出口矩阵
- 网络设备内的 SGA 数据
- SGA 授权策略结果中的安全组标记 (SGT)
- 网络条件（终端站过滤器、设备过滤器、设备端口过滤器）
- 设备 AAA 策略
- 拨号属性支持
- TACACS+ 代理

- TACACS+ CHAP 和 MSCHAP 身份验证
- 适用于 TACACS+ shell 配置文件的属性替换
- 显示 RSA 节点缺失密钥
- 最大用户会话数
- 帐号禁用情况
- 用户密码类型
- “密码类型”配置为“外部身份库”的内部用户
- 策略条件中可用的其他属性 - NumberOfHoursSinceUserCreation
- 适用于主机的通配符
- 网络设备范围
- OCSP 服务
- 基于 SSL/TCP 的系统日志消息
- 可配置的版权横幅
- 内部用户有效期限
- IP 地址排除

不支持的规则元素

思科安全 ACS 和思科 ISE 是基于不同的策略模型，而且在将其迁移至思科 ISE 时，思科安全 ACS 数据块之间也有差异。当思科安全 ACS 和思科 ISE 版本改变时，由于以下原因，并非所有思科安全 ACS 策略和规则都可以迁移：

- 策略所使用的属性不受支持
- AND/OR 条件结构不受支持（主要是在配置了复杂条件的情况下）
- 运算符不受支持

表 *5:* 不支持的规则元素

规则元素	支持状态	说明
日期和时间	不支持	具有按周循环设置的授权策略中的日期和时间条件无法迁移至思科 ISE。这样，其规则也无法迁移。

规则元素	支持状态	说明
日期和时间	不支持	身份验证策略中的日期和时间条件无法迁移至思科 ISE。这样，其规则也无法迁移。
In	部分支持	“In”操作符用于层次结构，而“Is”仅用于字符串类型。这可以使用“Matches”进行转换。
Not In	部分支持	“Not In”操作符用于层次结构，而“Is”仅用于字符串类型。这可以使用“Matches”进行转换。
Contains Any	不支持	“Contains Any”操作符仅适用于外部组，例如 Active Directory 和轻量级目录访问协议。
Contains All	不支持	“Contains All”操作符仅适用于外部组，例如 Active Directory 和轻量级目录访问协议。
逻辑表达式的组合	不支持	在条件中使用以下操作符的规则都无法迁移： • 包含复合条件的身份验证策略，其中复合条件具有除 a || b || c || 和/或 a && b && c && 之外的其他逻辑表达式，例如 (a || b) && c。 • 包含复合条件的授权策略，其中复合条件具有除 a && b && c && 之外的不同局部表达式，这些授权策略无法作为规则条件的一部分迁移。作为一个解决方法，您可以对某些高级逻辑表达式手动使用库复合条件。
网络条件	不支持	仅包括网络条件的规则无法迁移。如果条件包含网络条件和其他支持的条件，则网络条件会被忽略并且无法作为规则条件的一部分迁移。

规则元素	支持状态	说明
用户属性	部分支持	如果规则所带的条件包含除“字符串”数据类型之外的数据类型的用户属性，则无法迁移这些规则。
主机属性	不支持	规则引用主机属性时身份验证会失败。 如果授权策略包含具有主机（终端）属性的条件，则无法迁移至思科 ISE 授权策略。
TACACS 属性	不支持	思科 ISE 不支持终端访问控制器访问控制系统 (TACACS)。使用 TACACS 属性的思科安全 ACS 服务选择策略规则无法迁移。

支持的属性和数据类型

可以从思科安全 **ACS** 版本 **5.5** 或 **5.6**迁移至思科 **ISE** 的用户属性

思科安全 **ACS** 版本 **5.5** 或 **5.6** 中支持的用户属性	思科 **ISE** 版本 中的目标数据类型
字符串	字符串
UI32	不支持
IPv4	不支持
布尔值	不支持
日期	不支持
枚举	不支持

用户属性：与用户的关联

思科安全 **ACS** 版本 **5.5** 或 **5.6** 中与用户关联的属性	思科 **ISE** 版本
字符串	支持
UI32	不支持

思科安全 ACS 版本 5.5 或 5.6 中与用户关联的属性	思科 ISE 版本
IPv4	不支持
布尔值	不支持
日期	不支持

从思科安全 ACS 版本 5.5 或 5.6 迁移至思科 ISE 版本 的主机属性

思科安全 ACS 版本 5.5 或 5.6 中支持的主机属性	思科 ISE 版本 中的目标数据类型
字符串	字符串
UI32	UI32
IPv4	IPv4
布尔值	布尔值
日期	不支持
枚举	带允许的值的整数

主机属性：与主机的关联

思科安全 ACS 版本 5.5 或 5.6 中与主机关联的属性	思科 ISE 版本
字符串	支持
UI32	支持（值被转换为字符串）
IPv4	支持（值被转换为字符串）
布尔值	支持（值被转换为字符串）
日期	支持（值被转换为字符串）
枚举	支持（值被转换为字符串）

从思科安全 ACS 版本 5.5 或 5.6 迁移至思科 ISE 版本 的 RADIUS 属性

思科安全 ACS 版本 5.5 或 5.6 中支持的 RADIUS 属性	思科 ISE 版本 中的目标数据类型
UI32	UI32

思科安全 ACS 版本 5.5 或 5.6 中支持的 RADIUS 属性	思科 ISE 版本 中的目标数据类型
UI64	UI64
IPv4	IPv4
十六进制字符串	八进制字符串
字符串	字符串
枚举	带允许的值的整数

RADIUS 属性：与 RADIUS 服务器的关联

思科安全 ACS 版本 5.5 或 5.6 中与 RADIUS 服务器关联的属性	思科 ISE 版本
UI32	支持
UI64	支持
IPv4	支持
十六进制字符串	支持（十六进制字符串被转换为八进制字符串）
字符串	支持
枚举	支持（枚举为带允许的值的整数）

数据信息映射

本节提供列出导出过程中映射的数据信息的表。这些表包括了思科安全 ACS 版本 5.5 或 5.6 中的对象类别，及其在思科 ISE 版本 2.4 中的同等对象类别。本节中的数据映射表列出在迁移过程的导出阶段迁移数据时映射的有效或无效数据对象的状态。

网络设备映射

思科安全 ACS 属性	思科 ISE 属性
名称	按原样迁移
说明	按原样迁移
网络设备组	按原样迁移

思科安全 ACS 属性	思科 ISE 属性
单一 IP 地址	按原样迁移
单一 IP 和子网地址	按原样迁移
IP 和子网地址集合	不支持
排除 IP 地址	不支持
TACACS 信息	未迁移，因为在思科 ISE 版本 中不支持 TACACS。
RADIUS 共享密码	按原样迁移
CTS	按原样迁移
SNMP	SNMP 数据仅在 ISE 中可用；因此没有适用于已迁移设备的 SNMP 信息。
型号名称	此属性仅在思科 ISE 中可用（而且其值为默认值“Unknown”）。
软件版本	此属性仅在思科 ISE 中可用（而且其值为默认值“Unknown”）。

注释 仅设置为 TACACS 的任何网络设备都不支持迁移而且被列为非迁移设备。

NDG 类型映射

思科安全 ACS 属性	思科 ISE 属性
名称	名称
说明	说明

注释 思科安全 ACS 版本 5.5 或 5.6允许多个网络设备组 (NDG) 使用相同的名称。思科 ISE 版本 2.4 不支持此命名方案。因此，仅迁移使用任何已定义名称的第一个 NDG 类型。

NDG 层次结构映射

思科安全 ACS 属性	思科 ISE 属性
名称	名称
说明	说明
父级	无特定属性与此属性关联，因为此值仅作为NDG层次结构名称的一部分输入。（此外，NDG类型是此对象名称的前缀）。

注释 由于思科 ISE 版本 无法将冒号 (:) 识别为有效字符，所以任何在 root 名称中包含冒号的 NDG 均未迁移。

默认网络设备映射

思科安全 ACS 属性	思科 ISE 属性
默认网络设备状态	默认网络设备状态
网络设备组	未迁移
身份验证选项 - TACACS+	未迁移
RADIUS - 共享密钥	共享密钥
RADIUS - CoA 端口	未迁移
RADIUS - 启用 Keywrap	启用 Keywrap
RADIUS - 密钥加密密钥	密钥加密密钥
RADIUS - 消息验证器代码密钥	消息验证器代码密钥
RADIUS - 密钥输入格式	密钥输入格式

身份组映射

思科安全 ACS 属性	思科 ISE 属性
名称	名称
说明	说明

思科安全 ACS 属性	思科 ISE 属性
父级	此属性作为层次结构详细信息的一部分迁移。

注释 思科 ISE 版本 2.4 中包含用户和终端身份组。思科安全 ACS 版本 5.5 或 5.6 中的身份组以用户和终端身份组的方式迁移至思科 ISE 版本 2.4，因为用户需要被分配到用户身份组，并且终端需要被分配到终端身份组。

用户映射

思科安全 ACS 属性	思科 ISE 属性
名称	名称
说明	说明
状态	无需迁移此属性。（此属性在思科 ISE 中不存在）
身份组	迁移至思科 ISE 中的身份组
密码	密码
启用密码	无需迁移此属性。（此属性在思科 ISE 中不存在）
下一次登录时更改密码	此属性无需迁移
用户属性列表	用户属性从思科 ISE 导入，并且与用户关联
有效期限（天）	不支持

主机（终端）映射

思科安全 ACS 属性	思科 ISE 属性
MAC 地址	按原样迁移
状态	未迁移
说明	按原样迁移
身份组	迁移与终端组的关联。
属性	已迁移终端属性。
身份验证状态	此属性仅在思科 ISE 中可用（而且其值为固定值“Authenticated”）。

思科安全 ACS 属性	思科 ISE 属性
类名	此属性仅在思科 ISE 中可用（而且其值为固定值“TBD”）。
终端策略	此属性仅在思科 ISE 中可用（而且其值为固定值“Unknown”）。
匹配的策略	此属性仅在思科 ISE 中可用（而且其值为固定值“Unknown”）。
匹配的值	此属性仅在思科 ISE 中可用（而且其值为固定值“0”）。
NAS IP 地址	此属性仅在思科 ISE 中可用（而且其值为固定值“0.0.0.0”）。
OUI	此属性仅在思科 ISE 中可用（而且其值为固定值“TBD”）。
状态	此属性仅在思科 ISE 中可用（而且其值为固定值“Unknown”）。
静态分配	此属性仅在思科 ISE 中可用（而且其值为固定值“False”）。

LDAP 映射

思科安全 ACS 属性	思科 ISE 属性
名称	名称
说明	说明
服务器连接信息	按原样迁移。(Server Connection 选项卡；请参阅第 A-10 页图 A-1。）
目录组织信息	按原样迁移。(Directory Organization 选项卡；请参阅第 A-10 页图 A-2。）
目录组	按原样迁移
目录属性	手动执行迁移（使用思科安全 ACS 至思科 ISE 迁移工具）。

注释 仅迁移针对主要 ACS 实例定义的 LDAP 配置。

图 *2: Server Connection* 选项卡

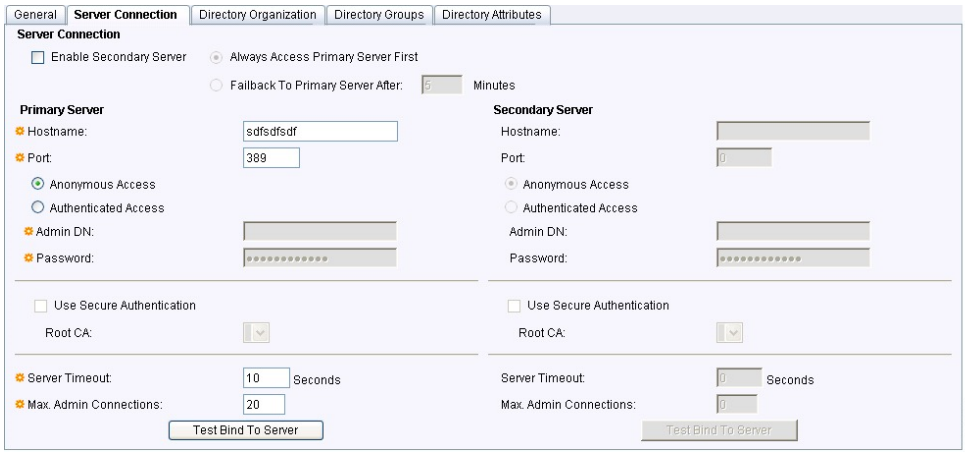
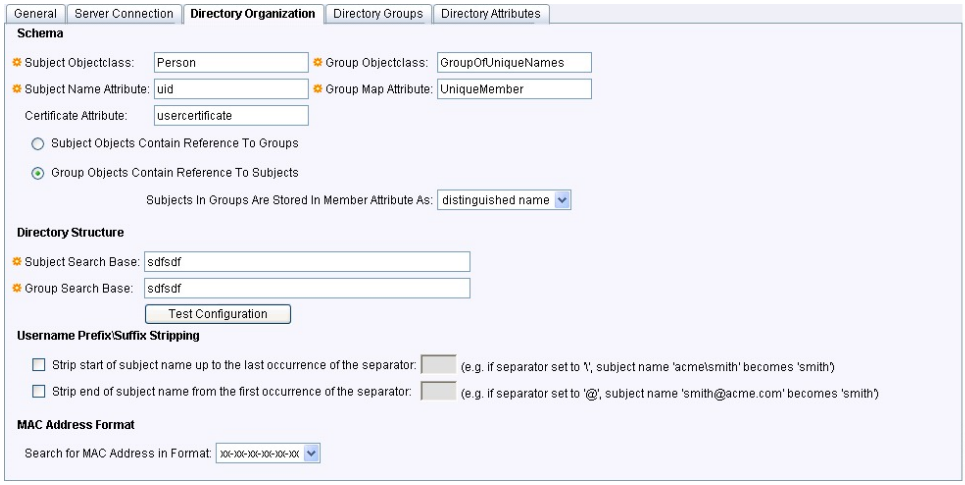


图 *3: Directory Organization* 选项卡



Active Directory 映射

思科安全 ACS 属性	思科 ISE 属性
域名	按原样迁移
用户名	按原样迁移
密码	按原样迁移
允许更改密码	按原样迁移
允许限制计算机访问	按原样迁移
老化时间	按原样迁移

思科安全 ACS 属性	思科 ISE 属性
用户属性	按原样迁移
组	按原样迁移
多域支持	仅迁移联接主要 ACS 实例的域

证书身份验证配置文件映射

思科安全 ACS 属性	思科 ISE 属性
名称	名称
说明	说明
主体用户名（X.509 属性）	主体用户名（X.509 属性）。
二进制证书与 LDAP 或 AD 证书的比较	二进制证书与 LDAP 或 AD 证书的比较。
用于获取证书的 AD 或 LDAP 名称	用于获取证书的 AD 或 LDAP 名称。

身份库序列映射

思科安全 ACS 属性	思科 ISE 属性
名称	名称
说明	说明
基于证书，证书身份验证配置文件	基于证书，证书身份验证配置文件
基于密码	身份验证搜索列表
高级选项 > 如果当前身份库上访问失败，则打破序列	请勿访问序列中的其他库并将“AuthenticationStatus”属性设置为“ProcessError”。
高级选项 > 如果当前身份库上访问失败，则继续进入下一个库	视为“User Not Found”并继续进入序列中的下一个库。
仅检索属性 > 退出序列并视为“User Not Found”	不支持（应忽略）

授权配置文件映射

思科安全 **ACS** 属性	思科 **ISE** 属性
名称	名称
说明	说明
DACLID（可下载的 ACL ID）	按原样迁移
属性类型（静态和动态）	• 如果是静态属性，则按原样迁移。 • 如果是除动态VLAN之外的动态属性，则按原样迁移。
属性（仅针对静态类型过滤）	RADIUS 属性。

可下载 **ACL** 映射

思科安全 **ACS** 属性	思科 **ISE** 属性
名称	名称
说明	说明
DACL 内容	DACL 内容

RADIUS 字典（供应商）映射

思科安全 **ACS** 属性	思科 **ISE** 属性
名称	名称
说明	说明
供应商 ID	供应商 ID
属性前缀	无需迁移此属性。
供应商长度字段大小	供应商属性类型字段长度。
供应商类型字段大小	供应商属性大小字段长度。

注释 只有思科安全 ACS 版本 5.5 或 5.6安装中不包括的 RADIUS 供应商需要迁移。这只涉及用户定义的供应商。

RADIUS 字典（属性）映射

思科安全 ACS 属性	思科 ISE 属性
名称	名称
说明	说明
属性 ID	无特定属性与此关联，因为此值仅作为 NDG 层次结构名称（NDG类型是此对象名称的前缀）的一部分输入。
方向	思科 ISE 中不支持
允许多项	思科 ISE 中不支持
属性类型	按原样迁移
添加策略条件	思科 ISE 中不支持
策略条件显示名称	思科 ISE 中不支持

注释 只有思科安全 ACS 版本 5.5 或 5.6安装中不包括的用户定义 RADIUS 属性需要迁移（即只有用户定义的属性需要迁移）。

身份字典映射

思科安全 ACS 属性	思科 ISE 属性
属性	属性名称
说明	说明
内部名称	内部名称
属性类型	数据类型
最大长度	未迁移
默认值	未迁移
必填字段	未迁移
用户	字典属性接受此值（“user”）。

身份属性字典映射

思科安全 **ACS** 属性	思科 **ISE** 属性
属性	属性名称
说明	内部名称
名称	按原样迁移
属性类型	数据类型
没有此类属性	字典（如果是用户身份属性，其值设置为“InternalUser”；如果是主机身份属性，其值设置为“InternalEndpoint”。）
尚未从思科安全 ACS 导出或提取	允许的值 = 显示名称
尚未从思科安全 ACS 导出或提取	允许的值 = 内部名称
尚未从思科安全 ACS 导出或提取	允许的值为默认值
最大长度	无
默认值	无
必填字段	无
添加策略条件	无
策略条件显示名称	无

外部 **RADIUS** 服务器映射

思科安全 **ACS** 属性	思科 **ISE** 属性
名称	名称
说明	说明
服务器 IP 地址	主机名
共享密钥	共享密钥
身份验证端口	身份验证端口
计帐端口	计帐端口
服务器超时	服务器超时

思科安全 ACS 属性	思科 ISE 属性
连接尝试	连接尝试

RADIUS 令牌映射

思科安全 ACS 属性	思科 ISE 属性
名称	名称
说明	说明
SafeWord 服务器	SafeWord 服务器
启用辅助设备	启用辅助设备
始终先访问主要设备	始终先访问主要设备
在几分钟内回退至主要设备	在几分钟内回退至主要设备
主要设备 IP 地址	主要设备 IP 地址
主要共享密钥	主要共享密钥
主要身份验证端口	主要身份验证端口
主要设备 TO（超时）	主要设备 TO
主要连接尝试	主要连接尝试
辅助设备 IP 地址	辅助设备 IP 地址
辅助共享密钥	辅助共享密钥
辅助身份验证端口	辅助身份验证端口
辅助设备 TO	辅助设备 TO
辅助连接尝试	辅助连接尝试
高级 > 将拒绝视为身份验证失败标志	高级 > 将拒绝视为身份验证失败标志。
高级 > 将拒绝视为未找到用户标志	高级 > 将拒绝视为未找到用户标志。
高级 > 启用身份缓存和老化值	高级 > 启用身份缓存和老化值。
Shell > 提示	身份验证 > 提示

思科安全 ACS 属性	思科 ISE 属性
目录属性	授权 > 属性名称（如果思科安全 ACS 中的字典属性列表包含属性“CiscoSecure-Group-Id”，则会迁移至此属性；否则，默认值为“CiscoSecure-Group-Id”。）

RSA 映射

思科安全 ACS 属性	思科 ISE 属性
名称	名称始终是 RSA
说明	未迁移
领域配置文件	领域配置文件
服务器超时	服务器超时
改为 PIN 之后重新验证	改为 PIN 之后重新验证
RSA 实例文件	未迁移
将拒绝视为身份验证失败	将拒绝视为身份验证失败
将拒绝视为未找到用户	将拒绝视为未找到用户
启用身份缓存	启用身份缓存
身份缓存老化时间	身份缓存老化时间

RSA 提示符映射

思科安全 ACS 属性	思科 ISE 属性
密码提示	密码提示
下一个令牌提示	下一个令牌提示
PIN 类型提示	PIN 类型提示
接受系统 PIN 提示	接受系统 PIN 提示
字母数字 PIN 提示	字母数字 PIN 提示
数字 PIN 提示	数字 PIN 提示