思科注册信封服务 4.5 版帐户管理员指南

2015 年 10 月 17 日

美洲总部
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
电话：408-526-4000
800 553-NETS (6387)
传真：408-527-0883

文本部件号：

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论在该手册中是否作出了其他担保，来自这些供应商的所有文档文件和软件都按“原样”提供且仍有可能存在缺陷。思科和上述供应商不承诺所有明示或暗示的担保，包括（但不限于）对特定用途的适销性、适用性、非侵权性以及因交易、使用或商业惯例所衍生的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科注册信封服务 4.5 版帐户管理员指南

目 录

第 1 章

概述 1-1

思科注册信封服务在加密方面的作用 1-1

公司帐户管理 1-3

第 2 章

管理 2-1

管理常见问题解答 2-1

思科注册信封服务公司帐户是什么？ 2-1

帐户管理员的典型任务是什么？ 2-2

本指南中包括哪些邮件管理主题？ 2-2

收件人注册是什么？ 2-2

思科注册信封服务帐户 2-3

用户 2-3

什么是用户组和角色？ 2-3

使用入门 2-4

了解公司帐户设置过程 2-4

登录 2-4

了解管理控制台中的图标 2-7

常见任务 2-8

自定义注册信封上的徽标 2-9

添加公司帐户管理员 2-11

自定义模板 2-11

监控帐户活动 2-12

管理邮件 2-13

管理密码要求 2-14
管理安全问题 2-15
管理用户 2-16
创建用户 2-16
重置用户密码 2-17
将用户添加到组 2-18
禁用用户 2-19
使用 TLS 传送 2-19
添加和测试 TLS 域 2-20
TLS 错误处理 2-22
启用发件人注册 2-23
选择身份验证方法 2-24
配置 CRES 帐户身份验证 2-25
通过 SAML 进行身份验证 2-25
配置 SAML 帐户身份验证 2-28
配置 BCE 插件或移动应用设置 2-37
禁用和启用对安全编写的访问 2-40
配置 DNS 以包括 CRES 2-41

第 3 章 **报告** 3-1
报告概述 3-1
“帐户使用情况”(Account Usage) 报告 3-2

第 4 章 **将创建密钥所需的数据从 IEA 迁移到 CRES** 4-1
有关将创建密钥所需的数据从 IEA 迁移到 CRES 的信息 4-1
如何将创建密钥所需的数据从 IEA 迁移到 CRES 4-3
迁移前提条件 4-3
在 CRES 上不受支持的功能 4-4

迁移过程 4-5
迁移完成后的功能差异 4-10
迁移错误消息 4-10
HTTP 代理配置示例 4-11
思科内容安全欢迎您发表评论 4-12
思科内容安全欢迎您发表评论 A-2

用于将创建密钥所需的数据从 IEA 迁移到 CRES 的其他参数 B-1

第 1 章

概述

思科注册信封服务 (CRES) 是一项托管服务，为思科 IronPort 加密技术提供支持。CRES 与思科 IronPort 邮件安全设备和思科 IronPort 加密设备配合使用，提供现场内容扫描、策略实施和加密功能。CRES 为加密邮件存储按邮件的加密密钥。加密邮件的收件人通过该服务进行身份验证，以便接收解密密钥。

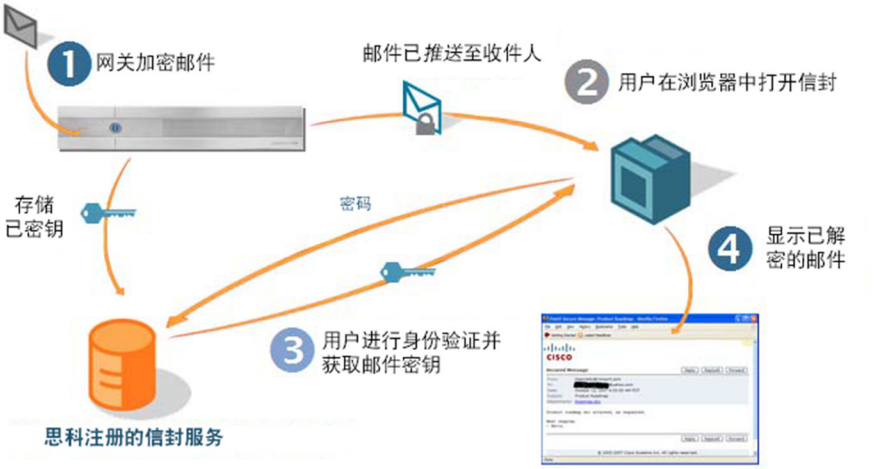
注意 该指南的最新版本以及其他 CRES 文档可在此产品页面上找到。

思科注册信封服务在加密方面的作用

该服务管理加密的以下要素：

- **收件人注册。**注册信封（加密邮件）的收件人必须在首次打开信封时注册到该服务，除非邮件以低安全性发送。注册是免费的。
- **身份验证。**已注册的用户使用单点登录 (SSO) 或提供密码来打开注册信封并阅读加密邮件。
- **加密密钥。**将为每封加密邮件创建加密密钥。当已注册的收件人在注册的信封中输入其密码时，该服务会发送用于打开该信封的解密密钥。
- **邮件到期和锁定。**已注册的用户可以为他们发送的加密邮件设置到期日期并控制邮件锁定。公司帐户管理员可以为使用公司帐户发送的所有加密邮件控制到期日期和邮件锁定。
- **安全转发和安全回复邮件。**根据公司帐户配置，收件人可以使用加密方式转发和回复加密的邮件。CRES 会为安全转发和安全回复邮件处理加密。

图中显示了 CRES 如何与 Cisco IronPort 邮件安全设备配合工作。该服务为加密邮件的注册收件人提供解密密钥。



该图描绘了以下流程：

步骤 1　Cisco IronPort 邮件安全设备使用加密功能来加密邮件并进行传送。

步骤 2　收件人在注册信封中输入其 CRES 密码。

注意　如果邮件配置为低安全性，则收件人不需要输入密码便可打开安全信封。

步骤 3　CRES 会提供打开该信封的解密密钥。

步骤 4　收件人的 Web 浏览器会显示解密的邮件。

公司帐户管理

CRES 为组织的公司帐户提供管理功能。初始 CRES 管理角色会分配给注册的技术联系人。除其他任务外，公司帐户的管理员可以执行以下任务：

- 自定义在注册信封上显示的徽标
- 管理通过该服务发送的邮件
- 生成帐户使用报告
- 管理用户（例如锁定帐户和重置密码）
- 配置 TLS 设置以实现加密的安全回复，无需信封

第 2 章

管理

本章包含以下主题：

- 管理常见问题解答（第 2-1 页）
- 使用入门（第 2-4 页）
- 常见任务（第 2-8 页）

管理常见问题解答

本部分提供对思科注册信封服务 (CRES) 公司帐户管理员角色的常见问题 (FAQ) 解答。

思科注册信封服务公司帐户是什么？

使用加密技术和 CRES 的每个组织都有一个该服务的公司帐户。此帐户可以与发送加密邮件的一个或多个思科 IronPort 邮件安全设备配合使用。

通常，一个组织有一个公司帐户，并且帐户管理员仅管理该帐户。

帐户管理员的典型任务是什么？

典型的管理任务包括：

- 配置公司帐户（例如，上传组织的徽标，将其显示于使用帐户发送的注册信封上）。
- 监控帐户使用情况（例如，查看有关用户注册和用户帐户激活的统计信息）。
- 管理使用帐户发送的邮件（例如，禁用对特定邮件的访问）。

注意　帐户管理员无法访问他们在管理控制台中管理的用户邮件中的内容。

有关管理任务的详细信息，请参阅“常见任务”部分（第 2-8 页）。

本指南中包括哪些邮件管理主题？

思科 IronPort 安全邮件解决方案的管理涉及两个不同的职责范围：

- 管理思科 IronPort 设备，例如思科邮件安全设备和思科 IronPort 加密设备
- 管理 CRES 公司帐户

本指南包含有关管理 CRES 公司帐户的信息。有关管理思科 IronPort 邮件安全设备的信息，请参阅思科客户支持门户中提供的产品文档。

收件人注册是什么？

收件人注册（也称为*用户注册*）是为首次收到注册信封的用户创建 CRES 用户帐户的过程。大多数邮件收件人必须先完成注册过程，然后才可以打开收到的加密邮件。但是，如果邮件使用低安全性，则用户无需注册便可打开该邮件。

在注册过程中，收件人提供用户配置文件信息，选择密码，然后选择安全问题和回答。

思科注册信封服务帐户

用户注册 CRES 后，该用户不与特定发件人的公司帐户关联。

发件人具有帐户，收件人也具有帐户。有了发件人 CRES 帐户之后，加密邮件的发件人就可以通过使安全邮件过期或恢复对它们进行管理。

用户

用户帐户管理由 CRES 的系统管理员处理。通常，公司帐户管理员不管理单个用户帐户。

公司管理员可以管理内部 CRES 用户以重置密码或锁定现有帐户。如果 CRES 管理员希望管理自己的用户帐户，必须提交客户支持申请单将管理的域添加到帐户。

什么是用户组和角色？

组是已注册用户的列表。角色是可以与组关联的权限集合。例如，要创建帐户管理员，具有该帐户管理权限的某个人必须将用户添加到帐户管理员组。角色不与个人关联。

注意　特定帐户管理员组中的每个用户都可以管理该帐户。

使用入门

本部分介绍了如何开始使用管理控制台来管理 CRES 公司帐户。

了解公司帐户设置过程

当某个组织将思科 IronPort 邮件安全设备配置为使用具有 CRES 的加密作为托管密钥服务时，将为该组织创建公司帐户。该组织的思科 IronPort 邮件安全设备与该公司帐户相关联。

注意　作为公司帐户管理员，您不会参与初始帐户设置过程。

默认情况下，新帐户的帐户管理员组包括组织的初始公司帐户管理员。公司帐户管理员可以通过将用户添加到“帐户管理员”(Account Administrator) 组来创建其他管理员。有关详细信息，请参阅“添加公司帐户管理员”部分（第 2-11 页）。“帐户管理员”(Account Administrator) 组还包括熟悉组织的思科 IronPort 邮件安全设备和系统配置的 IronPort 销售工程师。

登录

要管理公司帐户，请使用以下 URL 登录：

https://res.cisco.com/admin

如果您是多个帐户的管理员，则需要在登录时选择帐户。然后，可以选择是否希望：

- 计算机将记住所选的帐户。
- 在下次登录时，系统会自动选择记住的帐户。

这些选项由以下两个复选框表示：

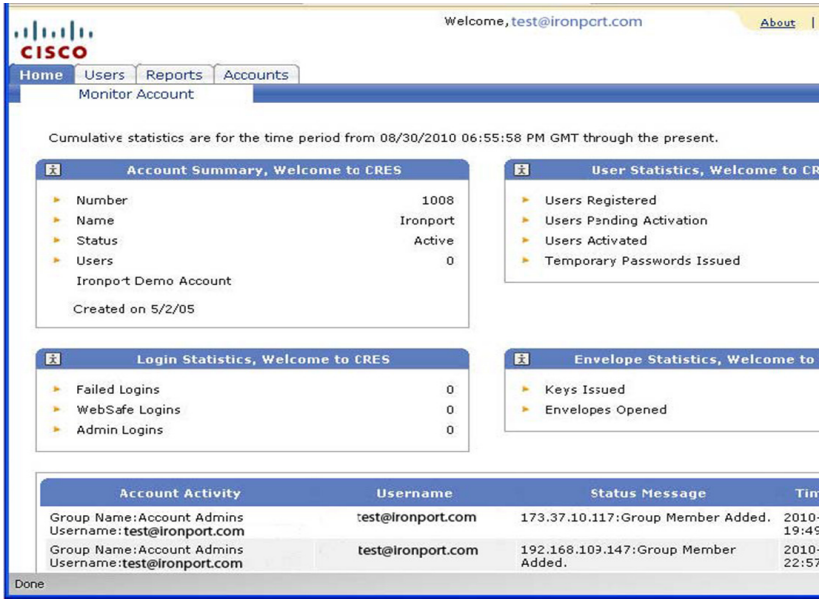
- **在此计算机上记住帐户 (Remember account on this computer)** - 如果选中该项，则下次使用同一浏览器登录时，还会在列表中选择选定的帐户。列表中仅会显示活动的帐户。
- **自动选择记住的帐户 (Automatically select remembered account)** - 如果选中该项，则不会显示帐户列表，并且在您登录时会显示记住的帐户的信息。

如果未选中**在此计算机上记住帐户 (Remember account on this computer)** 复选项，则不会启用**自动选择记住的帐户 (Automatically select remembered account)** 复选框。

要在登录后选择另一个帐户，请使用管理控制台主页底部的**选择帐户 (Select Account)** 链接。此链接还可用于取消选中**自动选择记住的帐户 (Automatically select remembered account)** 复选框。

登录公司帐户时，会显示管理控制台。

图 2-1　　公司帐户的管理控制台



主页是“监控帐户”(Monitor Account) 页面，该页面会显示帐户活动摘要。

管理控制台包含用于导航网站的以下选项卡和链接：

- **主页。**显示“监控帐户”(Monitor Account) 页面。

  使用“监控帐户”(Monitor Account) 页面可查看系统和帐户状态。点击**更新 (Update)** 按钮检索最新状态信息，或在“更新间隔”(Update Interval) 字段中输入值，然后点击**更新 (Update)** 按固定时间间隔（例如，每隔 10 秒）刷新页面。

- **用户。**显示“用户管理”(User Management) 页面。

  通常，该页面仅供思科的系统管理员使用。公司帐户管理员仅可访问分配至他们帐户的个人，并且仅在他们添加了正确的域的前提下才能访问。

- **报告。**显示“查看报告”(View Reports) 页面。

  “查看报告”(View Reports) 页面通常用于运行“帐户使用情况”(Account Usage) 报告。有关“帐户使用情况”(Account Usage) 报告的详细信息，请参阅第 3 章“报告”。

  “查看报告”(View Reports) 页面包含指向以下报告的链接：

  - **“用户信息”(User Information) 报告。**显示与帐户关联的用户列表，但是仅限于一个或多个域与该帐户关联的情况，显示的信息包括序列号 (#)、用户 ID、邮件地址、名字、姓氏、状态、创建日期、上次登录日期和上次修改日期。
  - **“用户状态”(Users Status) 报告。**显示与您的域关联的用户的状态（新、活动、已阻止）。
  - **“帐户使用情况”(Account Usage) 报告。**运行此报告可查看公司帐户的使用统计信息。有关“帐户使用情况”(Account Usage) 报告的详细信息，请参阅第 3 章“报告”。

- **帐户。**显示“帐户管理”(Account Management) 页面和“管理注册信封”(Manage Registered Envelopes) 页面的选项卡。

  点击“管理帐户”(Manage Accounts) 选项卡可查看“帐户管理”(Account Management) 页面，从中可以配置 CRES 公司帐户。有关详细信息，请参阅“自定义注册信封上的徽标”部分（第 2-9 页）、“添加公司帐户管理员”部分（第 2-11 页）和“自定义模板”部分（第 2-11 页）。

  点击“管理注册信封”(Manage Registered Envelopes) 选项卡可搜索和管理使用公司帐户发送的注册信封。有关详细信息，请参阅“管理邮件”部分（第 2-13 页）。

了解管理控制台中的图标

使用管理控制台中的图标可在系统中导航，也可以管理帐户和用户等区域。鼠标悬停文本会指示每个图标代表的功能。

表 2-1　图标列表

图标	标题	操作
	管理用户	访问“组成员身份”(Group Membership) 页面。
	管理角色	访问“组授权”(Group Authorization) 页面。
	保存令牌	将令牌保存到本地计算机。令牌是用于对思科邮件安全设备 (ESA) 和 CRES（或本地密钥服务器）之间的数据进行加密的客户特定密钥。当前仅供客户支持人员使用。
	管理规则	访问“规则”(Rules) 页面。
	关闭或删除项目	删除项目。
	预览模板	使用所选语言预览模板。

常见任务

本部分说明如何使用管理控制台执行以下管理任务：

- 自定义注册信封上的徽标
- 添加公司帐户管理员
- 自定义模板
- 监控帐户活动
- 管理邮件
- 管理密码要求
- 管理安全问题
- 管理用户
- 将 TLS 用于已加密但对用户透明的安全邮件传送
- 启用发件人注册
- 选择身份验证方法
- 配置 BCE 插件或移动应用设置
- 禁用和启用对安全编写的访问
- 配置 DNS 以包括 CRES

注意　用户可以将时间戳设置为其本地时区及其所需的格式（12 小时制或 24 小时制）。对于将时间戳设置为其本地时区的用户，包括用户时间戳的任何管理控制台屏幕都将受到该功能的影响。

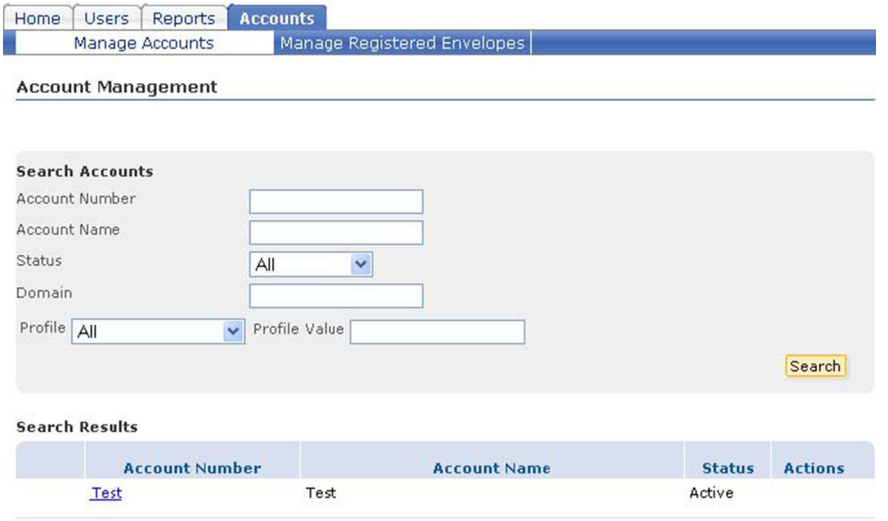
自定义注册信封上的徽标

要更改使用帐户发送的邮件中所显示的徽标，请执行以下操作：

步骤 1　登录到公司帐户的管理控制台。

步骤 2　点击**帐户 (Accouts)** 选项卡。此时系统会显示“帐户管理”(Account Management) 页面。

图 2-2　“帐户管理”(Account Management) 页面



步骤 3　点击您的帐号对应的链接。

注意　每个组织通常具有单个公司帐户。

此时系统会显示该帐户的“详细信息”(Details) 选项卡。

步骤 4　点击该帐户对应的**图像 (Images)** 选项卡。

图 2-3　“图像”(Images) 选项卡

步骤 5　浏览到要上传的徽标文件，然后点击**添加图像 (Add Image)**。

注意　文件大小不能超过 102,400 字节。思科建议徽标文件的大小也不能超过 60x160 像素。

可以为徽标使用任何类型的文件。但是，思科建议仅使用用户常用浏览器支持的文件类型（例如：GIF、JPEG 或 PNG）。

添加公司帐户管理员

要添加公司帐户管理员，请执行以下操作：

步骤 1　登录到公司帐户的管理控制台。

步骤 2　点击**帐户 (Accouts)** 选项卡。系统将显示“帐户管理”(Account Management) 页面，如图 2-2 中所示。

步骤 3　点击您的帐号对应的链接。

注意　组织通常具有单个公司帐户。

此时系统会显示您的帐户对应的**详细信息 (Details)** 选项卡。

步骤 4　点击该帐户对应的**组 (Groups)** 选项卡。

步骤 5　点击**管理用户 (Manage Users)** 图标。

有关详细信息，请参阅“了解管理控制台中的图标”部分（第 2-7 页）。

步骤 6　在“组成员身份”(Group Membership) 页面中，输入要作为一个公司帐户管理员添加的注册用户的用户 ID。

步骤 7　点击**添加到组 (Add to Group)**。

自定义模板

要自定义通知邮件模板，请执行以下操作：

步骤 1　登录到公司帐户的管理控制台。

步骤 2　点击**帐户 (Accounts)** 选项卡。此时将打开“帐户管理”(Account Management) 页面。

步骤 3　点击您的帐号对应的链接。

注意　每个组织通常具有单个公司帐户。

此时将打开帐户的**详细信息 (Details)** 选项卡。

步骤 4　点击帐户对应的**模板 (Templates)** 选项卡。

步骤 5　从**基本模板集 (Base Template Set)** 下拉列表中，选择要复制的模板，然后输入新模板集的标题。

步骤 6　点击**添加 (Add)**。

步骤 7　点击已添加模板的链接。

步骤 8　点击模板所需的区域设置。此时将打开**编辑模板 (Edit Template)** 页面。

步骤 9　根据需要，编辑 **HTML** 和**文本 (Text)** 字段中的信息。

步骤 10　点击**保存 (Save)**。

步骤 11　点击**返回到模板列表 (Back to Templates List)**。

步骤 12　点击**返回到模板集列表 (Back to Template Set List)**。

步骤 13　从**活动模板集 (Active Template Set)** 下拉列表中，选择所需的模板。

步骤 14　点击**保存 (Save)**。

监控帐户活动

IronPort 邮件安全设备提供有关加密使用情况的详细信息。例如，可以使用该设备生成有关内容过滤器的报告，这些内容过滤器会标记要进行加密的邮件。

为了补充设备生成的报告，CRES 会提供有关公司帐户活动的一般信息。可以在管理控制台中查看此信息。主页中的“监控帐户”(Monitor Accounts) 选项卡显示有关帐户活动的信息，包括用户注册、登录计数以及有关已打开和发送的加密邮件（注册信封）的统计信息。

此外，可以在“帐户”(Accounts) 选项卡上查看“帐户使用情况”(Account Usage) 报告。有关 CRES 报告的详细信息，请参阅第 3 章“报告”。

管理邮件

作为公司帐户管理员，您可以查看和管理使用该帐户发送的任何邮件的状态。

要管理邮件，请执行以下操作：

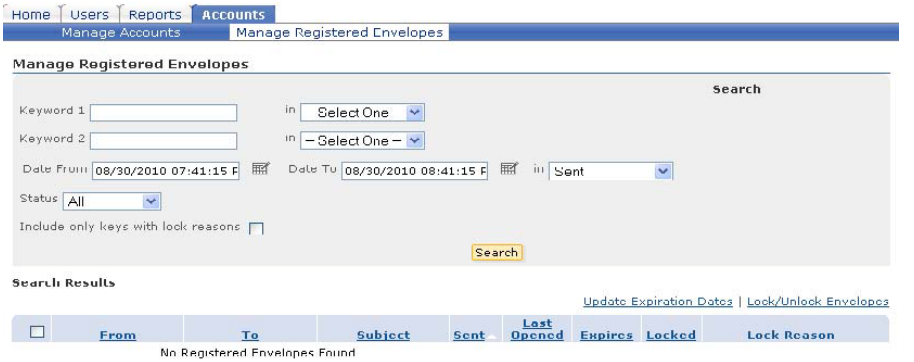
步骤 1　登录到公司帐户的管理控制台。

步骤 2　点击“帐户”(Accouts) 选项卡。系统将显示“帐户管理”(Account Management) 页面，如图 2-2 中所示。

步骤 3　点击“管理注册信封”(Manage Registered Envelopes) 选项卡

此时系统将显示“管理注册信封”(Manage Registered Envelopes) 页面。

图 2-4　“管理注册信封”(Manage Registered Envelopes) 页面



步骤 4　点击**搜索 (Search)** 可查看在过去一小时发送的所有邮件，或输入搜索条件并点击**搜索 (Search)** 查看特定邮件。

搜索结果会显示每封邮件的状态，包括发送时间、上次打开时间、邮件到期时间和邮件锁定信息。

要设置到期日期，请选择一封或多封邮件并点击**更新到期日期 (Update Expiration Dates)** 链接。

要锁定或解锁邮件，请选择一封或多封邮件并点击**锁定/解锁信封 (Lock/Unlock Envelopes)** 链接。锁定信封时，可以输入锁定原因。当接收人尝试打开信封时，会在信封上显示原因。

管理密码要求

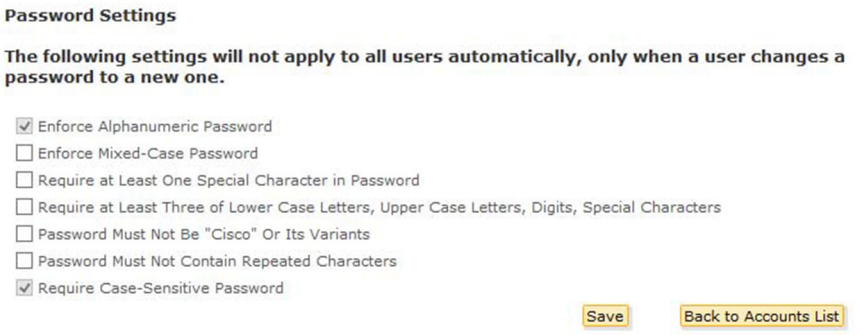
在创建或更改密码时，请确保密码满足以下要求：

- 密码必须是字母数字字符（必需）。
- 密码必须区分大小写（必需）。
- 密码必须至少以下三种可用字符类型的字符：小写字母、大写字母、数字和特殊字符。
- 密码中包含的字符不得连续重复出现三次。
- 密码不得包含用户名或逆序用户名。
- 密码不得为“Cisco”、“ocsic”或通过以下方式获得的任何相似词：更改字母大小写或将“i”替换为“1”、“l”、“！”，将“o”替换为“0”，或将“s”替换为“$”。

默认情况下，仅设置两个密码要求。可以通过选择其他选项来更改用户的密码要求。

可在**管理帐户 (Manage Accounts)** 页面的**安全 (Security)** 选项卡上管理密码要求。

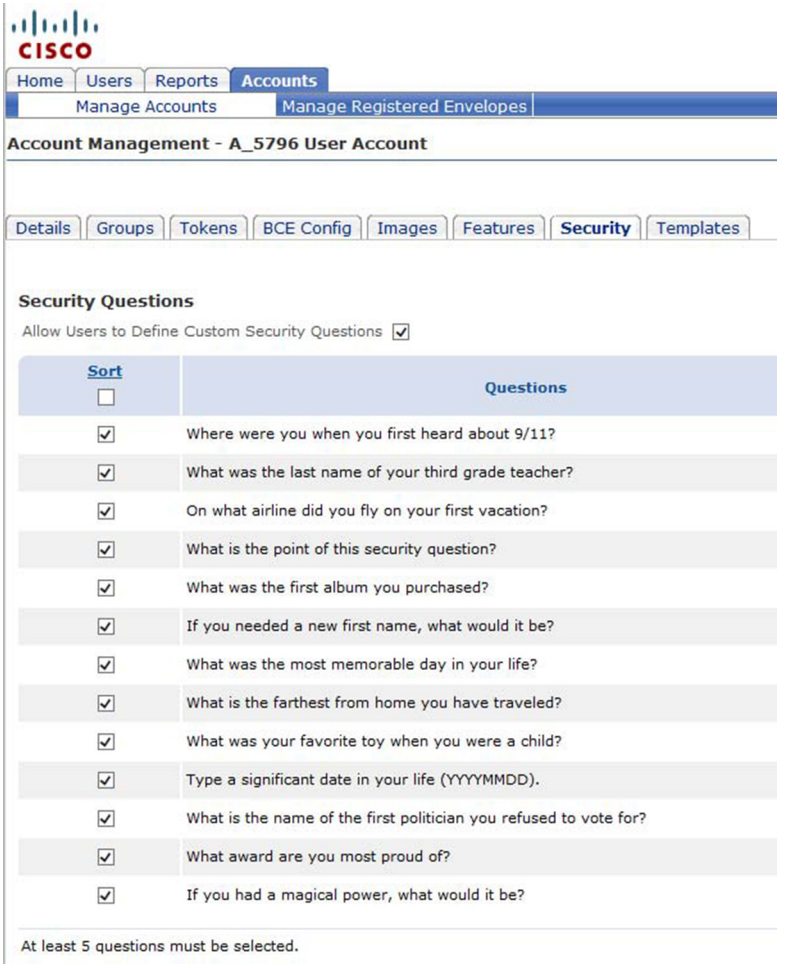
图 2-5　管理密码要求



管理安全问题

可以通过选中**管理帐户 (Manage Accounts)** 页面的**安全 (Security)** 选项卡上对应的复选框，来更改安全问题。此外，还可以允许或禁止用户定义自定义安全问题。

图 2-6　　管理安全问题



管理用户

“用户”(Users) 选项卡提供对“管理用户”(Manage Users) 功能的访问，包括创建用户、搜索用户、重置密码、将用户添加到组以及禁用用户。

仅可为与帐户关联的域管理用户。要将域与帐户管理，请与技术支持部门联系。

注意　在域与帐户关联之前即已存在于系统中的用户需要迁移到帐户。如果在请求域关联时存在现有用户，请告知技术支持人员。

创建用户

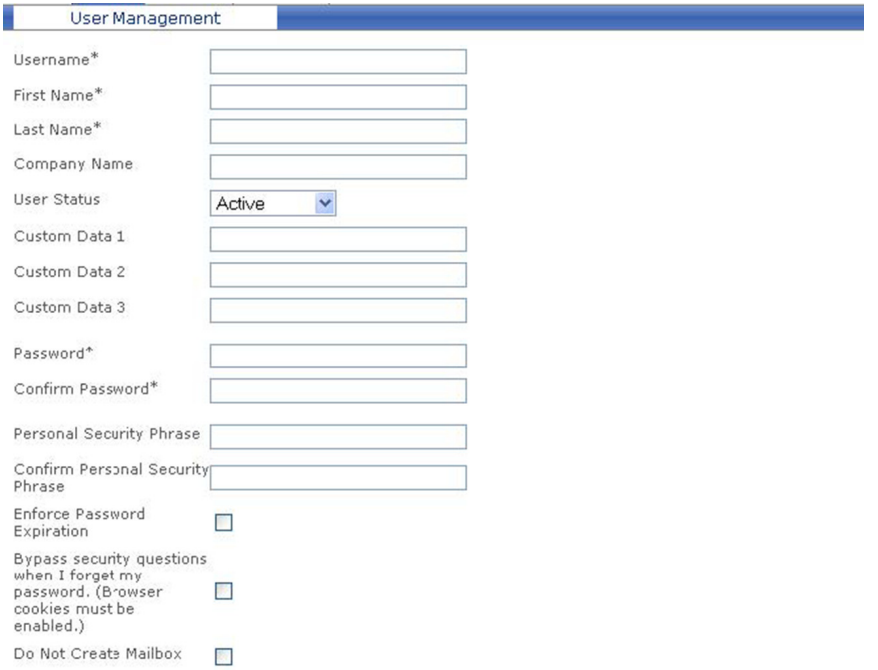
要创建用户，请执行以下操作：

步骤 1　点击“管理用户”(Manage Users) 页面上的**添加用户 (Add User)**。

步骤 2　填写表单。

注意　密码必须遵循思科密码要求。有关详细信息，请参阅“管理密码要求”部分（第 2-14 页）。

图 2-7　“创建用户”(Create User) 页面



步骤 3　可以设置自定义选项，例如实施密码到期日期、在重置密码时允许用户绕过安全问题或跳过为特定用户创建邮箱的过程。

步骤 4　点击**保存 (Save)**。

注意　创建的用户必须属于您的邮件域。

重置用户密码

用户可以使用以下链接重置其密码：

https://res.cisco.com/websafe/pswdForgot.action

如果该方法不成功（例如，如果用户记不起质询问题的答案），则可以通过管理员界面重置该用户的密码。

要重置用户的密码，请执行以下操作：

步骤 1　选择用户（点击“管理用户”(Manage Users) 页面上搜索结果中的用户名）。

步骤 2　点击**查看密码质询答案 (View Password Challenge Answers)**。

步骤 3　点击**重新进行身份验证 (Reauthenticate)**。

步骤 4　点击**下一步 (Next)**。

步骤 5　点击**重置密码 (Reset Password)**。

注意　在重置密码后，用户将收到一封邮件，其中包含用于创建新密码的链接。

将用户添加到组

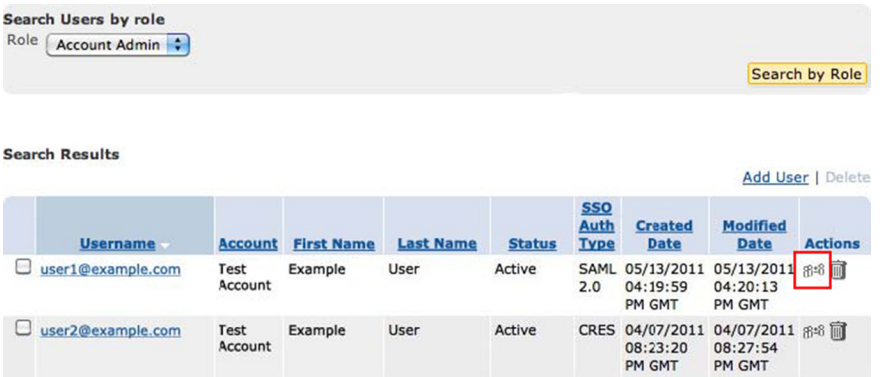
可以将用户添加到组（或从组中删除用户），从而为该用户提供更多（或更少）权限。

要管理用户的组成员身份，请执行以下操作：

步骤 1　选择用户（点击“管理用户”(Manage Users) 页面上搜索结果中的用户名）。

步骤 2　在用户对应的“操作”(Actions) 列中，点击**组 (Groups)** 图标。

图 2-8　用户列表中的组图标



步骤 3　此时系统会显示“组成员身份”(Group Membership) 页面。左侧的框会显示用户所属的组。右侧的框会显示任何其他可用的组。

步骤 4　点击某个组将其选中，然后点击向右或向左箭头在两个框之间移动该组。

步骤 5　点击**完成 (Done)**，保存更改。

禁用用户

您可能需要临时禁用某个用户的帐户，例如当用户离开公司时。要禁用用户，请执行以下操作：

步骤 1　选择用户（点击“管理用户”(Manage Users) 页面上搜索结果中的用户名）。

步骤 2　点击**修改 (Modify)**。

步骤 3　将用户状态设置为**锁定 (Locked)**。

图 2-9　　将用户的状态设置为“锁定”(Locked)

步骤 4　保存更改。

使用 TLS 传送

传输层安全 (TLS) 传送支持将源自 CRES 的邮件（如安全回复）以加密形式传送回发送域，不必使用信封。

可以启用 TLS 传送来提供一种安全的邮件传送方法，无需最终用户登录 CRES 或安装加密插件来接收或查看邮件。

TLS 按帐户启用。对于每个帐户，可指定一个或多个 TLS 域以及错误处理行为。

添加和测试 TLS 域

要为帐户启用 TLS，必须至少添加一个域。添加域会启动扫描该域以获取 TLS 支持的过程。在添加域之前，域必须通过 TLS 域测试。

TLS 域测试使用 CRES 服务器来验证信息和连接性。该检查可确保：

- 存在与域条目关联的 MX 记录，
- MX 记录可解析为 IP 地址，且每个 MX 记录具有与其关联的有效邮件服务器，
- CRES 服务器可通过端口 25 与上述邮件服务器建立 SMTP 连接，
- 上述每个邮件服务器均支持 STARTTLS 扩展，
- 最后，CRES 服务器可以成功发起到处理 MX 记录的每个邮件服务器的连接。

要将 TLS 用于安全回复，必须使用在*思科邮件加密兼容性列表*的“CRES 支持的证书颁发机构”部分中列出的其中一个证书所签名或与之关联的证书。此外，还必须使用未过期的证书。如果建立 TLS 连接的日期和时间不在证书的有效期内，则证书即已过期。

域的 TLS 测试会生成三种可能的结果之一：通过、不确定（部分通过）和失败。

- 通过：如果对 MX 记录中的所有服务器进行的测试已通过，则域被视为通过 TLS 测试。通过 TLS 测试的域将添加为 TLS 域，并且在等待客户支持人员批准期间，会收到“处理中”(Processing) 状态。
- 不确定：如果测试在至少一个关联的邮件服务器（而不是所有邮件服务器）上通过，则结果被视为不确定。默认情况下，不确定的域不会添加为 TLS 域。可以通过点击结果中显示的“请求批准”(Request Approval) 按钮添加一个不确定的域。输入有关添加该域的原因的信息，然后提交。
- 失败：如果没有与该域关联的邮件服务器支持 TLS，则域测试失败。TLS 测试失败的域不会添加为 TLS 域。

系统将为每个通过的域或针对不确定的域的审批请求建立客户支持申请单。您将收到一封邮件，指明该域已添加或请求有关该域的详细信息。

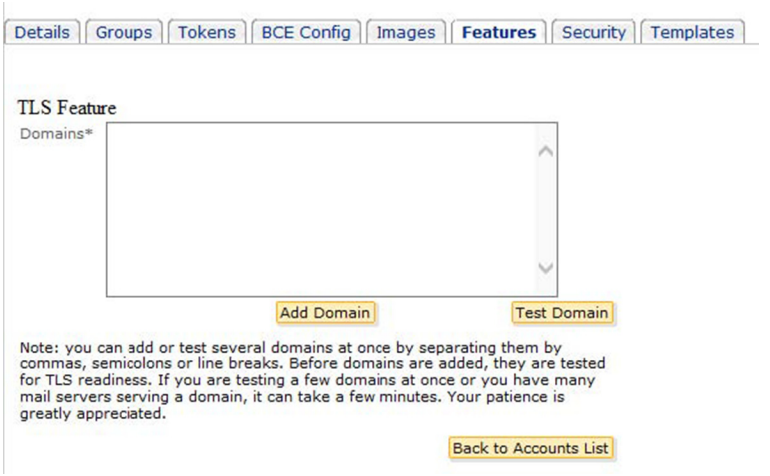
还可通过使用“测试域”(Test Domain) 按钮而不是“添加域”(Add Domain) 按钮来测试域，且无需将它们添加到 TLS 域列表。系统不会为测试的域建立支持请求。

要添加或测试 TLS 域，请执行以下操作：

步骤 1　在“帐户”(Accounts) 选项卡上，选择**管理帐户 (Manage Accounts)** 选项卡。

步骤 2　点击帐号，然后选择**功能 (Features)** 选项卡。

图 2-10　“管理帐户”(Manage Accounts) 页面，“功能”(Features) 选项卡



步骤 3　输入一个域。

a. 要测试该域，请点击**测试域 (Test Domain)**。

b. 要添加该域，请点击**添加域 (Add Domain)**。

步骤 4　屏幕将显示一条消息指示结果。

步骤 5　如果添加的域已通过，它会显示在“域”(Domain) 列表中，状态为“处理中”(Processing)。

步骤 6　通过点击垃圾桶图标删除域。

注意　不要忘记指定 TLS 错误处理行为。有关详细信息，请参阅“TLS 错误处理”（第 22 页）。

TLS 错误处理

如果 TLS 传送停止工作（例如由于证书已过期），则需要配置 TLS 错误处理。可以选择“退回邮件”(Bounce Messages) 或“回退到注册信封传送”(Fallback to Registered Envelope Delivery)。

注意　如果 TLS 失败传送首选项设置为“回退到注册信封传送”(Fallback to Registered Envelope Delivery)，请记住在内部邮件服务器上将 TLS 传送选项更改为“TLS 首选”(TLS Preferred)。

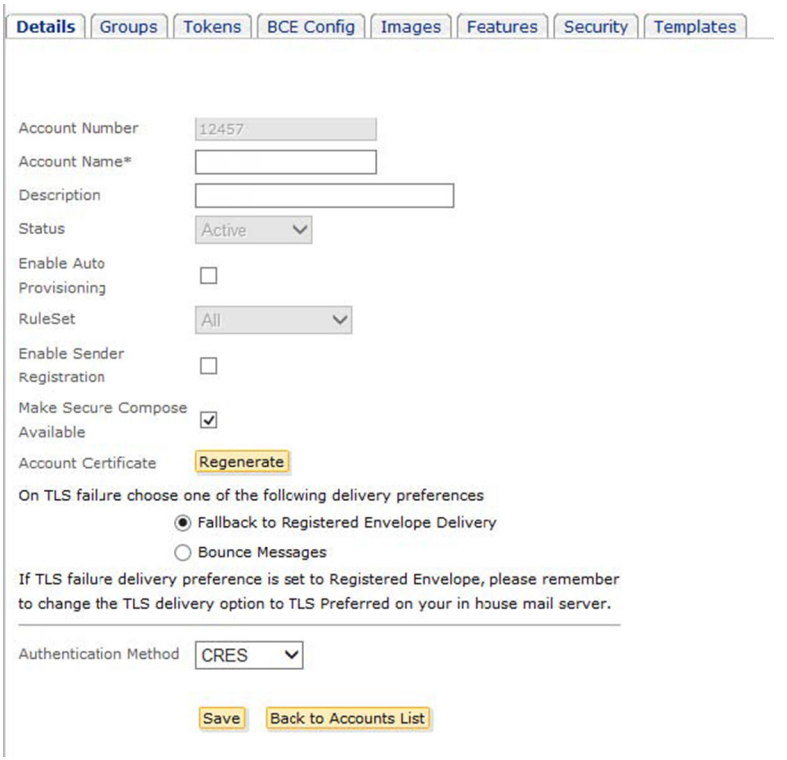
- 回退到注册信封传送：如果 TLS 传送失败（例如由于证书已到期），系统将恢复为发送注册的信封。
- 退回邮件：对于配置为在 TLS 传送失败期间退回邮件的帐户，将在 24 小时后执行退回，而在此 24 小时内则会每小时重试一次。对于配置为回退到注册信封传送的帐户，回退将在 1 小时后执行，而在此 1 小时内则会每 20 分钟重试一次。

要为帐户指定 TLS 错误处理行为，请执行以下操作：

步骤 1　在“帐户”(Accounts) 选项卡上，选择**管理帐户 (Manage Accounts)** 选项卡。

步骤 2　点击帐号并选择**详细信息 (Details)** 选项卡。

图 2-11　“帐户管理”(Account Management) 页面



步骤 3　选择 TLS 故障传送首选项。

步骤 4　点击**保存 (Save)**。

启用发件人注册

可以将系统配置为根据帐户自动提供给注册发件人。如果希望将 CRES 帐户提供给当前不使用 CRES 发送加密邮件的邮件发件人，则该功能也很有用。注册后，发件人可以详细了解有关可供他们控制其加密邮件的选项。

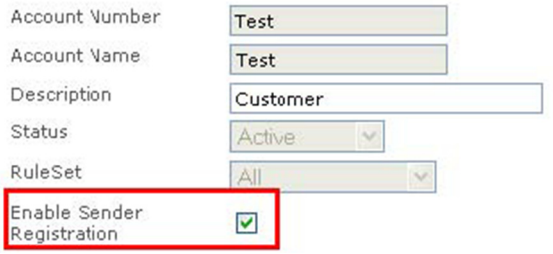
如果启用此功能，则发件人会收到邀请他们在 CRES 服务器上创建帐户的邮件。他们每隔 30 天就会收到这些邀请，而且可以按照邀请中包含的说明轻松退出。无法更改邀请频率。

要启用帐户的发件人注册，请执行以下操作：

步骤 1　在“帐户”(Accounts) 选项卡上，选择**管理帐户 (Manage Accounts)** 选项卡。

步骤 2　点击帐号并选择**详细信息 (Detail)** 选项卡。

图 2-12　启用发件人注册



步骤 3　选中**启用发件人注册 (Enable Sender Registration)** 复选框。

步骤 4　点击**保存 (Save)**。

选择身份验证方法

必须将两种身份验证方法之一分配给某个帐户，并正确配置身份验证。但是，可以根据需要更改帐户的身份验证方法。

CRES 提供其他两种方法对用户进行身份验证：

- 配置 CRES 帐户身份验证（第 2-25 页）
- 配置 SAML 帐户身份验证（第 2-28 页）

如果要保留对身份验证过程的全面控制，则可能需要使用 CRES 身份验证。

SAML 是用于单点登录 (SSO) 的一种 XML 应用。有关 CRES 如何实施 SAML 身份验证的详细信息，请参阅通过 SAML 进行身份验证（第 2-25 页）。

如果已使用思科 IronPort 网络安全设备或 PingFederate 作为用于 SSO 的 SAML 身份提供程序，则可能需要使用基于 SAML 的身份验证。有关详细信息，请参阅配置 PingFederate 注销 URL（第 2-36 页）。

配置 CRES 帐户身份验证

要为帐户配置 CRES 身份验证，请执行以下操作：

步骤 1　在“帐户”(Accounts) 选项卡上，选择**管理帐户 (Manage Accounts)** 选项卡。

步骤 2　点击帐号并选择**详细信息 (Detail)** 选项卡。

步骤 3　在“身份验证方法”(Authentication Method) 列表中，点击 **CRES**。

步骤 4　点击**保存 (Save)**。

通过 SAML 进行身份验证

SAML 是主要用于单点登录 (SSO) 的一种基于 XML 的标准，可使最终用户更加简单地通过多个 Web 服务（例如 CRES）进行身份验证。目前仅支持 SAML 2.0。

单点登录意味着用户只需登录一次进行身份验证（通过身份提供程序），以后便可使用运营商提供的一系列服务，不必重新登录。该协议还支持单点注销。

这简化了用户体验，并且提高了安全性，因为用户不必记住多个服务的登录详细信息。SAML 的 CRES 支持适用于新的和现有的 CRES 信封。必须为每个公司帐户单独启用 SAML 身份验证。完成此操作后，帐户中的所有用户必须通过 SAML 进行身份验证。不属于该帐户的任何用户将继续使用 CRES 身份验证方法。

SAML 概述

SAML 支持在不同的安全网络（有时称为安全域）之间交换身份验证和授权数据。通常，当一个域中有用户使用网络浏览器访问网络（其他域）时，会使用 SAML。

要实现单点登录，必须由每个域中的实体建立 SAML 使用以下术语定义的 SAML 对话：

- **身份提供程序 (IdP)。**身份提供程序是生成 SAML 断言的实体。身份提供程序应在生成 SAML 断言之前对其最终用户进行身份验证。CRES 可与大多数 SAML 2.0 身份提供程序配合使用。但是，它仅通过了可与思科 IronPort 网络安全设备、Active Directory 联合服务 (AD FS) 和 PingFederate 配合使用的认证。

- **运营商 (SP)。**运营商是可以使用 SAML 断言的实体。运营商依靠身份提供程序来识别最终用户，并将识别结果传送给 SAML 断言中的运营商。运营商根据断言来确定访问控制。启用了 SAML 身份验证后，CRES 将充当运营商。

SAML 断言是在身份提供程序与运营商之间所传送的信息的容器，包含在 SAML 请求和响应中。断言包含运营商用于确定访问控制的语句（例如身份验证和授权语句）。断言以 <saml:Assertion> 标记开头。

SAML 对话称为流量，流量可由任何提供程序发起：

- **运营商发起的流量。**运营商由请求访问的最终用户联系，因此，它通过联系身份提供程序以提供对该用户的身份识别，从而发起 SAML 对话。对于发起流量的运营商，最终用户可使用包含该运营商域的 URL（例如 http://www.serviceprovider.com/）来访问运营商。
- **身份提供程序发起的流量。**身份提供程序通过联系运营商发起 SAML 对话，从而请求代表最终用户进行访问。对于发起流量的身份提供程序，最终用户可使用包含本地域的 URL（例如 http://saas.example.com/）来访问运营商。

CRES 仅支持运营商发起的流量。

注意　本部分不提供有关 SAML 的综合讨论，也不介绍身份提供程序和安全提供程序如何相互通信。有关详细信息，请参阅 http://saml.xml.org/wiki/saml-wiki-knowledgebase。
有关使用网络安全设备作为身份提供程序的详细信息，请参阅思科 IronPort *AsyncOS 网络用户指南*（版本 7.0 或更高版本）中的“控制对 SaaS 应用的访问”一章。

要求

要将具有 CRES 的 SAML 身份验证作为运营商，必需满足以下要求：

- CRES 当前仅支持使用思科 IronPort 网络安全设备、Active Directory 联合服务 (AD FS) 或 PingFederate 作为身份提供程序。
- 身份提供程序的 SAML 登录机制必须能够在没有 JavaScript 的情况下工作。
- 身份提供程序必须支持 SAML 2.0。
- 在 SAML 断言中，SAML NameID 或属性必须包含邮件地址。

警告

在使用 SAML 身份验证时有一些警告：

- 必须为每个公司帐户单独启用 SAML。
- SAML 登录页面由 SAML 身份提供程序而不是 CRES 提供。这意味着 CRES 日志记录都不适用于 SAML 登录，且登录问题应报告给 SAML 身份提供程序。
- 对于具有 SAML 验证的帐户的用户，用户密码维护（如恢复已忘记的密码或更改密码）必需通过身份提供程序而不是 CRES 执行。
- 没有为管理帐户 (admin config) 启用 SAML 身份验证来防止意外锁定这些帐户。
- 与 CRES 验证的帐户不同，不能整合 SAML 验证的帐户。
- 当思科 IronPort 网络安全设备用作身份提供程序时，必须为登录页面启用 JavaScript 才能使其正常运行。
- 当思科 IronPort 网络安全设备用作身份提供程序时，系统不会缓存密码，用户必须对每次会话都进行身份验证。
- 如果身份提供程序存在问题，SAML 用户可能无法进行身份验证，即使其凭据有效也是如此。
- 如果身份提供程序变为永久不可用，则必须将身份验证方法更改为 CRES 以使用户进行身份验证。
- 如果 SMAL 服务存在问题，则管理员依靠身份提供程序来提供警报。
- 即使最终用户具有有效的凭据，如果身份提供程序存在问题，则他们仍可能无法访问服务。

用户体验

无论是否启用了 JavaScript，是否有一个或多个收件人，或者这些收件人是否为 BCC 收件人，SAML 身份验证的用户体验都基本相同。用户打开信封（或移动设备支持 [MDS] 链接），选择其用户身份或根据需要提供其邮件地址，然后通过身份提供程序进行身份验证。或者，用户可以导航到网络浏览器中的 https://res.cisco.com，输入邮件地址，然后通过身份提供程序进行身份验证。

配置 SAML 帐户身份验证

可以将 SAML 身份验证配置为使用以下身份提供程序之一：

- Active Directory 联合服务 (AD FS)
- 思科 IronPort 网络安全设备
- PingFederate

在以下部分中介绍了有关使用这些身份提供程序的配置步骤：

- 使用 AD FS 作为身份提供程序时配置 SAML 帐户身份验证（第 2-28 页）
- 在使用思科 IronPort 网络安全设备或 PingFederate 作为身份提供程序时配置 SAML 帐户身份验证（第 2-34 页）

使用 AD FS 作为身份提供程序时配置 SAML 帐户身份验证

启用 SAML 身份验证时，配置 CRES 帐户以匹配 AD FS 帐户的设置非常重要。

需要以下信息（AD FS 等同项）：

- 运营商实体 ID（SaaS 应用名称/连接 ID）
- 客户服务 URL（单点登录 URL/基本 URL）
- 身份提供程序验证证书
- （可选）备用邮件属性名称（SAML 属性/邮件地址）

在以下部分中介绍了使用 AD FS 作为身份提供程序时配置 SAML 帐户身份验证的过程：

- 配置 AD FS 的信任方信任
- 配置声明规则
- 从 ADFS 导出签名证书
- 配置 CRES
- 配置 AD FS 签名设置
- 激活 SAML 登录
- 通过 LDAP 凭据登录到网络安全

配置 AD FS 的信任方信任

步骤 1　启动 AD FS 2.0 管理工具。

步骤 2　点击“添加”(Add)。

步骤 3　在“欢迎”(Welcome) 屏幕上点击“开始”(Start)。

步骤 4　选择“手动输入有关信任方的数据”(Enter data about the relying party manually)，然后点击“下一步”(Next)。

步骤 5　为 CRES SP 输入显示名称，然后点击“下一步”(Next)。

步骤 6　选择“AD FS 2.0 配置文件”(AD FS 2.0 profile)，然后点击“下一步”(Next)。

步骤 7　选择“启用对 SAML 2.0 网络 SSO 协议的支持”(Enable support for the SAML 2.0 Web SSO protocol)。

步骤 8　对于“信任方 SAML 2.0 SSO 服务 URL”(Relying party SAML 2.0 SSO service URL)，请输入 https://res.cisco.com/websafe/ssourl，然后点击“下一步”(Next)。

步骤 9　对于“信任方信任标识符”(Relying party trust identifier)，请输入 https://res.cisco.com/，然后点击“添加”(Add)。

步骤 10　点击“下一步”(Next)。

步骤 11　选择“允许所有用户访问此信任方”(Permit all users to access this relying party)，然后点击“下一步”(Next)。

步骤 12　检查设置，然后点击“下一步”(Next)。

步骤 13　选择“向导关闭时为此信任方信任打开‘编辑声明规则’对话框”(Open the Edit Claim Rules dialog for this relying party trust when the wizard closes)，然后点击“关闭”(Close)。

配置声明规则

步骤 1　当“编辑 CRES SP 的声明规则”(Edit Claim Rules for CRES SP) 对话框打开时，选择“发布转换规则”(Issuance Transform Rules) 选项卡，然后点击“添加规则”(Add Rule)。

步骤 2　对于“声明规则模板”(Claim rule template)，选择“发送 LDAP 属性作为声明”(Send LDAP Attributes as Claims)，然后点击“下一步”(Next)。

步骤 3　在“声明规则名称”(Claim rule name) 中输入名称。

步骤 4　对于“属性存储”(Attribute store)，选择“Active Directory”。

步骤 5　在“LDAP 属性”(LDAP Attribute) 列中，选择“用户主体名称”(User-Principal-Name) 或“邮件地址”(E-Mail Addresses)。

推荐值为“用户主体名称”(User-Principal-Name)，因为它可以用于 Active Directory 目录中的任何用户。在 SAML 身份验证过程中，CRES 会将 Active Directory 中的用户名与用户的 CRES 帐户进行比较。

要使用“邮件地址”(E-Mail Addresses) 值，必须在“用户属性”(User's Properties) 配置中“常规”(General) 选项卡下的“邮件”(E-mail) 字段中输入邮件地址。由于 CRES 会获取 Active Directory 中用户帐户的邮件地址，因此如果当前没有为所有用户正确配置可选的“邮件”(E-mail) 字段，则会出现错误。

步骤 6　在“外发声明类型”(Outgoing Claim Type) 列中，选择“邮件地址”(E-Mail Addresses)。

步骤 7　点击“完成”(Finish)，然后点击“添加规则”(Add Rule)。

步骤 8　对于“声明规则模板”(Claim rule template)，选择“转换传入声明”(Transform an Incoming Claim)，然后点击“下一步”(Next)。

步骤 9　在“声明规则名称”(Claim rule name) 中输入名称。

步骤 10　对于“传入声明类型”(Incoming claim type)，选择“邮件地址”(E-mail Address)。

步骤 11　对于“外发声明类型”(Outgoing claim type)，选择“名称 ID”(Name ID)。

步骤 12　对于“外发名称 ID 格式”(Outgoing name ID format)，选择“临时标识符”(Transient Identifier)。

步骤 13　选择“通过所有声明值”(Pass through all claim values)。

步骤 14　点击“完成”(Finish)。

从 ADFS 导出签名证书

步骤 1　启动 AD FS 2.0 管理工具。

步骤 2　在左侧窗格中，选择“AD FS 2.0”>“服务”(Service) >“证书”（Certificates)。

步骤 3　选择令牌签名证书。

步骤 4　在右侧窗格中，点击“查看证书”(View Certificate)。

步骤 5　在“详细信息”(Details) 选项卡中，点击“复制到文件”(Copy to File)。

步骤 6　在“欢迎使用证书导出向导”(Welcome to the Certificate Export Wizard) 屏幕上，点击“下一步”(Next)。

步骤 7　对于导出文件格式，选择“DER 编码二进制 X .509 (.CER)”(DER excoded binary X .509 [.CER])，然后点击“下一步”(Next)。

步骤 8　输入导出文件的位置和文件名，然后点击“下一步”(Next)。

步骤 9　点击“完成”(Finish)。

配置 CRES

步骤 1　使用管理员帐户凭据登录到 CRES。

步骤 2　在“帐户”(Accounts) 选项卡上，选择“管理帐户”(Manage Accounts) 选项卡。

步骤 3　点击一个帐号，然后选择“详细信息”(Details) 选项卡。

步骤 4　对于“身份验证方法”(Authentication Method)，选择“SAML 2.0”。

步骤 5　对于“SSO 备用邮件属性名称”(SSO Alternate Email Attribute Name)，将其保留为空。

步骤 6　对于“SSO 运营商实体 ID”(SSO Service Provider Entity ID)，输入 https://*AD FS*/（其中 *AD FS* 是 AD FS 的相应值，例如 myadfs.com）。

步骤 7　对于“SSO 客户服务 URL”(SSO Customer Service URL)，输入 https://*AD FS*/adfs/ls。

步骤 8　对于“SSO 注销 URL”(SSO Logout URL)，输入 https://*AD FS*/adfs/ls。

步骤 9　对于“验证证书”(Verification Certificate)，点击“浏览”(Browse)，然后上传从 AD FS 设置导出的签名证书。

步骤 10　点击“保存”(Save)。

步骤 11　在保存页面后，点击“下载”(Download) 下载 CRES 签名证书。

配置 AD FS 签名设置

步骤 1　启动 AD FS 2.0 管理工具。

步骤 2　在左侧窗格中，选择“AD FS 2.0”>“信任关系”(Trust Relationships) >“信任方信任”(Relying Party Trusts)。

步骤 3　选择“信任方 (CRES SP)”(Relying Party [CRES SP])，然后点击右侧窗格中的“属性”(Properties)。

步骤 4　选择“签名”(Signature) 选项卡，点击“添加”(Add)，然后选择从 CRES 管理员页面下载的 CRES 签名证书。

步骤 5　选择“高级”(Advanced) 选项卡。

步骤 6　对于“安全哈希算法”(Secure hash algorith)，选择“SHA-1”，然后点击“确定”(OK)。

步骤 7　AD FS 管理工具将在互联网信息服务 (IIS) 中创建 /adfs/ls 网站。

步骤 8　启动服务器管理器工具。

步骤 9　在左侧窗格中，依次选择“服务器管理器”(Server Manager) >“角色”(Roles) >“Web 服务器 (IIS)”(Web Server [IIS]) >“互联网信息服务 (IIS) 管理器”(Internet Information Services (IIS) Manager)。

步骤 10　在“连接”(Connections) 窗格中，依次选择服务器 >“站点”(Sites) >“默认网站”(Default Web Site) >“adfs”>“ls”。

步骤 11　在 /adfs/ls 主窗格中，选择 IIS 下的“身份验证”(Authentication)。

步骤 12　启用“匿名身份验证”(Anonymous Authentication) 并禁用其他所有验证。

步骤 13　在“连接”(Connections) 树中右键点击“ls”，然后点击“浏览”(Explore)。

步骤 14　右键点击 web.config 文件，然后点击“编辑”(Edit)。

步骤 15　找到“localAuthenticationTypes”部分并删除除 <add name="Forms" page="FormsSignIn.aspx" /> 以外的所有条目。

这会仅允许身份表单验证，而不是 Windows 集成的身份验证。

步骤 16　保存并关闭文件。

激活 SAML 登录

步骤 1　通过选择“帐户”(Accounts) 选项卡下的“管理帐户”(Manage Accounts) 选项卡，返回到“CRES 帐户”(CRES Account) 页面。

步骤 2　点击一个帐号，然后选择“详细信息”(Details) 选项卡。

步骤 3　点击页面底部的“激活 SAML”(Activate SAML)。

步骤 4　点击“继续”(Continue)。

步骤 5　输入域用户名和密码，然后点击“登录”(Sign In)。

步骤 6　点击“继续”(Continue) 继续。

步骤 7　点击“继续”(Continue) 关闭该窗口。

步骤 8　确认在“CRES 帐户详细信息”(CRES Account Details) 页面顶部显示消息“已成功激活 SAML”(SAML Activated Successfully)。

步骤 9　确认“SSO 启用日期”(SSO Enable Date) 设置为当前时间。

步骤 10　检查是否为该帐户的身份验证方法选择了 SAML 2.0。

通过 LDAP 凭据登录到网络安全

步骤 1　转到网络安全 https://res.cisco.com/websafe/root

步骤 2　确认已重定向到 AD FS 身份验证页面。

步骤 3　输入 Active Directory 用户和密码。

步骤 4　点击“登录”(Sign In)。

步骤 5　确认已成功登录网络安全。

步骤 6　将邮件发送到同一域中的所有用户。

步骤 7　打开用户接收的加密邮件。

步骤 8　确认已打开一个新窗口，以便输入 Active Directory 凭证。

步骤 9　输入 Active Directory 凭证。

步骤 10　确认信封已解密。

在使用思科 IronPort 网络安全设备或 PingFederate 作为身份提供程序时配置 SAML 帐户身份验证

启用 SAML 身份验证时，配置 CRES 帐户以匹配身份提供程序帐户的设置非常重要。

您需要提供以下信息（思科 IronPort 网络安全设备或 PingFederate 等同项）：

- 运营商实体 ID（SaaS 应用名称/连接 ID）
- 客户服务 URL（单点登录 URL/基本 URL）
- 身份提供程序验证证书
- （可选）备用邮件属性名称（SAML 属性/邮件地址）

如果使用思科 IronPort 网络安全设备作为身份提供程序，则可在“SaaS 应用身份验证策略”(SaaS Application Authentication Policies) 页面上找到此信息。该证书可从“编辑 SaaS 单点登录的身份提供程序设置”(Edit Identity Provider Settings for SaaS Single Sign On) 页面进行下载。

如果使用 PingFederate 作为身份提供程序，则可在“摘要”(Summary) 区域找到此信息。

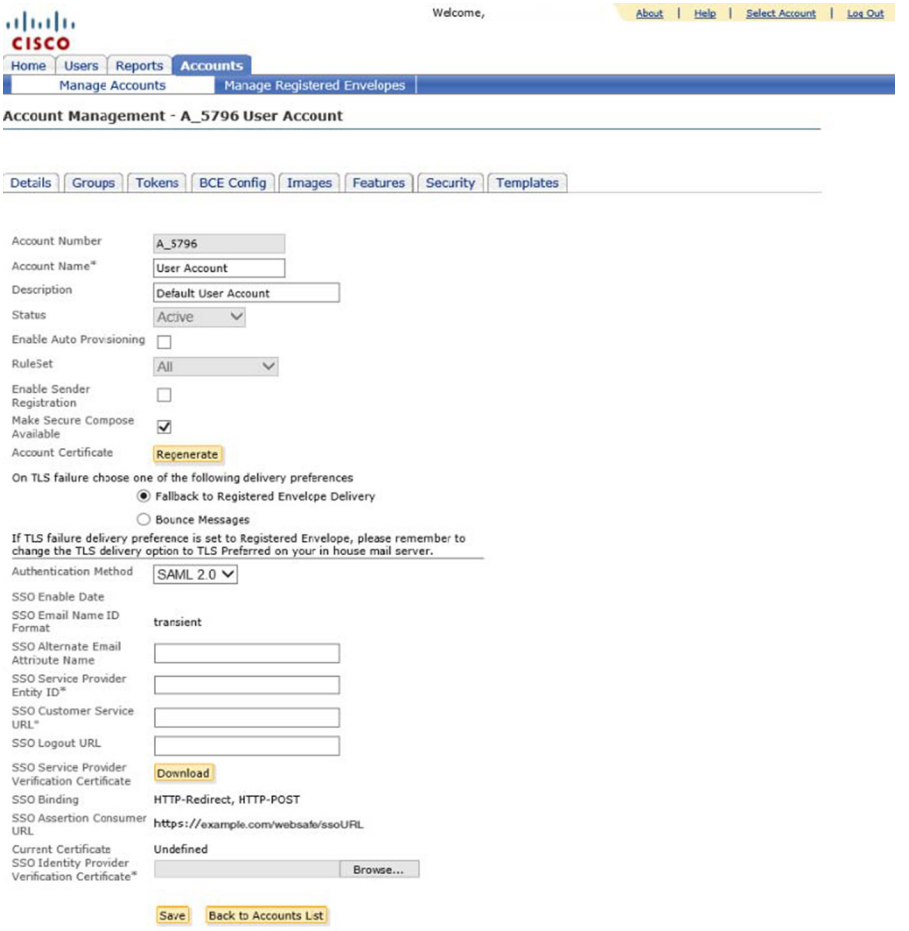
注意　当配置 PingFederate 作为 IDP 时，必须指定 CRES 断言使用者服务 URL 作为终端。此外，为了让用户可以注销，必须配置 SSO 注销 URL。有关配置此设置的说明，请参阅“配置 PingFederate 注销 URL”（第 36 页）。

要为帐户配置 SAML 身份验证，请执行以下操作：

步骤 1　在“帐户”(Accounts) 选项卡上，选择**管理帐户 (Manage Accounts)** 选项卡。

步骤 2　点击帐号并选择**详细信息 (Detail)** 选项卡。

图 2-13　选择身份验证方法



步骤 3　在“身份验证方法”(Authentication Method) 下拉列表中，选择 **SAML 2.0**。将显示 SSO 启用日期，即上次成功配置并激活 SAML 的日期。此时系统将显示 SSO 邮件名称 ID 格式。目前仅支持临时 SAML 名称格式。

步骤 4　在“SSO 备用邮件属性名称”(SSO Alternate Email Attribute Name) 中输入名称。这是包含用作名称标识符的备用邮件地址的属性名称。

步骤 5　在“SSO 运营商实体 ID”(SSO Service Provider Entity ID) 字段中，输入运营商的实体 ID。

步骤 6　输入 SSO 客户服务 URL。这是 SAML 身份提供程序单点登录 URL。

步骤 7　输入 SSO 注销 URL。这是 SAML 身份提供程序注销 URL。

单点登录绑定（通常为 HTTP 重定向或 HTTP-POST）与 SSO 断言使用者 URL 一起显示。

步骤 8　（可选）点击**下载 (Download)** 下载一份 SSO 运营商验证证书。这是您的身份提供程序 (IdP) 需要用来验证 CRES 中 SAML 注销请求签名的公共自签名证书。

步骤 9　点击**浏览 (Browse)**，然后选择并上传由 SAML 身份提供程序（思科 IronPort 网络安全设备或 PingFederate）提供的 SSO 身份提供程序验证证书。此时将显示当前证书。

步骤 10　点击**保存 (Save)**。

步骤 11　点击**激活 (Activate)**。

注意　当保存了详细信息后，必须激活 SAML 登录。这可防止在配置错误的情况下意外锁定用户。

配置 PingFederate 注销 URL

要从通过 PingFederate 配置为 IDP 的信封注销，必需在 PingFederate 中配置注销 URL。这非常关键，因为最终用户必须点击“注销”(Logout) 按钮才能完全注销 CRES。

要在 PingFederate 中配置注销 URL，请执行以下步骤：

步骤 1　从帐户的“CRES 帐户管理”(CRES Account Management) 屏幕中，下载并保存公共证书。

步骤 2　在帐户的 PingFederate 服务器上，点击**签名验证证书 (Signature Verification Certificate)**。

步骤 3　点击**管理证书 (Manage Certificates)**。

步骤 4　导入在步骤 1 中保存的证书。

步骤 5　确保导入的证书是主要证书。

注意　PingFederate 允许在验证 SAML 注销请求时有多个公共证书。因此，从 CRES 下载公共证书后，必须确保该证书是 PingFederate 中的第一个证书或主要证书。

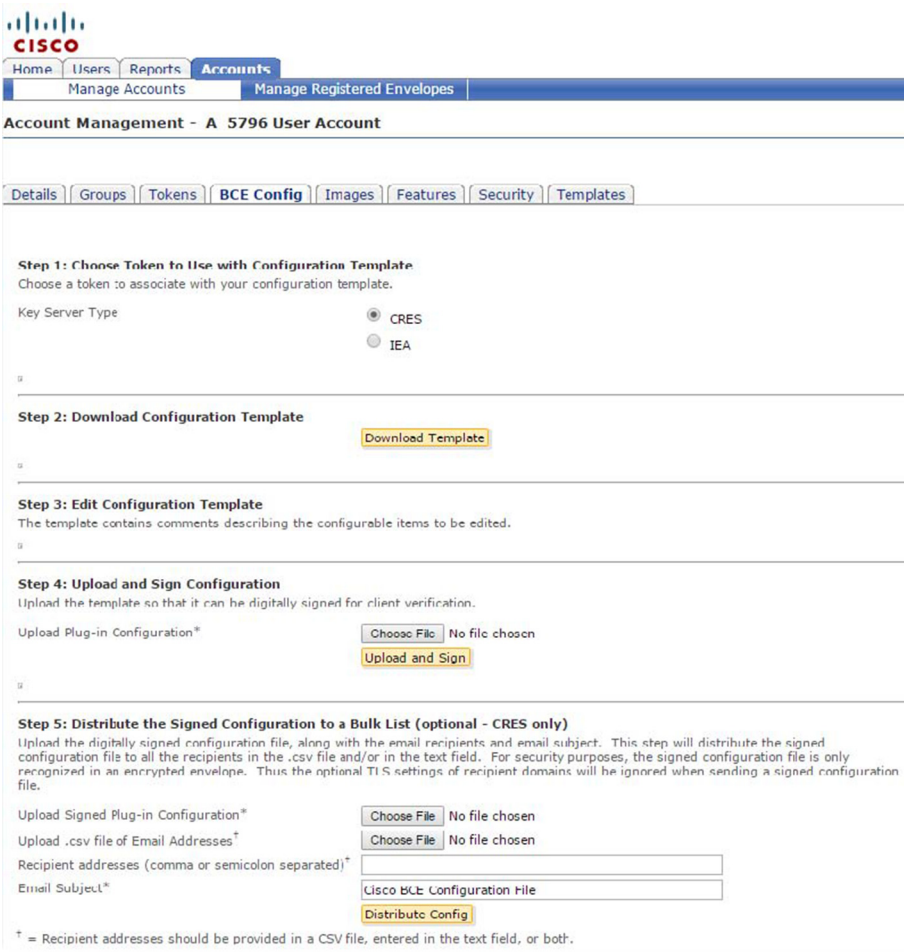
配置 BCE 插件或移动应用设置

要部署企业级邮件 (BCE) 插件或移动应用，需要向每个用户发送签名的配置文件。必须是帐户管理员才能完成这些步骤。

要签名并部署 BCE 配置文件，请转到**帐户 (Accounts)** 选项卡并选择要从中启用 BCE 插件的帐户。然后，转至 **BCE 配置 (BCE Config)** 选项卡并遵循以下说明进行操作。

注意　如果使用思科 IronPort 设备作为密钥服务器，则在开始之前，需要从思科 IronPort 加密设备下载令牌。

图 2-14　“BCE 配置”(BCE Configuration) 选项卡



步骤 1　选择要与配置模板一起使用的令牌。

如果使用 CRES 作为密钥服务器，请选择 CRES 令牌。如果使用思科 IronPort 设备，请导航至下载到本地计算机的 IEA 令牌，然后将其上传。

步骤 2　下载模板文件以对其进行编辑。

步骤 3　编辑配置文件。

BCE_Config.xml 文件包含有关根据您的特定环境需要编辑的字段的详细说明。在文本编辑器中打开文件并遵循备注中包含的说明进行必要的修改。

步骤 4　点击**浏览 (Browse)** 导航到该 BCE_Config.xml 文件，然后在找到文件后点击**上传并签名 (Upload and Sign)**。配置文件经过签名后，将显示为 BCE_Config_signed.xml。将此文件保存到本地计算机。

要将签名的配置文件部署到各个最终用户，请执行以下操作：

a. 撰写一封经过加密的邮件，并将 BCE_Config_signed.xml 文件附加到该加密邮件。

b. 然后将此邮件发送给要为其启用 BCE 的所有最终用户（企业级邮件）。

注意　邮件的发件人必须与对 BCE_Config.xml 文件签名的帐户管理员相同。请勿将 BCE_Config_signed.xml 文件发送到邮寄列表。CRES 不支持邮寄列表。

步骤 5　（可选）要将签名配置文件发送到批量列表，请执行以下操作：

注意　以下批量分发方法仅适用于 CRES 管理员。为了使 IEA 管理员可以将签名的 *BCE_Config_signed.xml* 文件正确地分发给其用户，必须将该文件附加到从 IEA 管理员邮件地址发送的加密邮件。

a. 点击**浏览 (Browse)** 导航到要发送给最终用户的 *BCE_Config_signed.xml* 文件。

b. 点击下一个**浏览 (Browse)** 按钮导航到要为其启用 BCE 的邮件地址 .csv 文件，或手动输入以逗号或分号分隔的邮件地址列表。

c. 默认情况下，邮件主题为“思科 BCE 配置文件”(Cisco BCE Configuration File)。要进行更改，请在此字段中键入新文本。

d. 点击**分发配置 (Distribute Config)** 将 BCE_Config_signed.xml 文件发送至邮件地址列表。

注意　出于安全考虑，BCE_Config_signed.xml 文件仅在加密信封中识别。因此，在发送 BCE_Config_signed.xml 文件时，收件人域的可选 TLS 设置会被忽略。

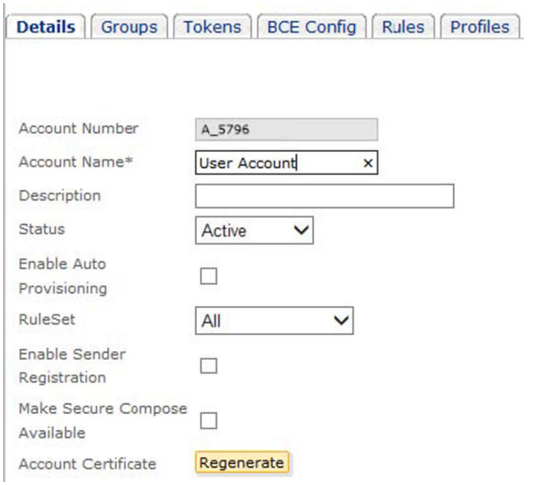
禁用和启用对安全编写的访问

此功能使您可以限制用户通过安全编写发送邮件。因此，此功能使您可以控制从无法扫描或存档并可能会导致安全问题或违反公司策略问题的安全编写发送的邮件。

禁用安全编写将针对从您帐户中的用户从最终用户门户的左侧导航菜单中删除“编写邮件”(Compose Message) 链接。

可以仅为与您帐户关联的域中的用户禁用安全编写。要将域与您的帐户相关联，请与客户支持部门联系。

图 2-15　禁用对安全编写的访问



步骤 1　在“帐户”(Accounts) 选项卡上，选择**管理帐户 (Manage Accounts)** 选项卡。

步骤 2　点击帐号并选择**详细信息 (Details)** 选项卡。

步骤 3　要启用对安全编写的访问，请选中**使安全编写变为可用 (Make Secure Compose Available)** 复选框。

步骤 4　要禁用对安全编写的访问，请取消选中**使安全编写变为可用 (Make Secure Compose Available)** 复选框。

步骤 5　点击**保存 (Save)**。

注意　帐户的“令牌”(Token) 选项卡上的任何 SecureCompose 令牌均供内部使用，且不应修改。修改或删除该令牌*不会*禁用安全编写。要禁用安全编写，请使用上述步骤。

配置 DNS 以包括 CRES

为了避免发件人策略框架 (SPF) 验证失败，必须将 mx:res.cisco.com 添加到 SPF 记录。

在何处以及如何将 CRES 添加到 SPF 记录取决于在网络拓扑中实施域名系统 (DNS) 的方式。有关详细信息，请联系 DNS 管理员。

如果未将 DNS 配置为包括 CRES，则通过托管密钥服务器生成并传送安全编写和安全回复时，外发 IP 地址不会匹配收件人端列出的 IP 地址，从而导致 SPF 验证失败。

第 3 章

报告

本章包含以下主题：

- “报告概述”，第 1 页
- “‘帐户使用情况”(Account Usage) 报告”，第 2 页

报告概述

报告功能具有易于使用的界面，只需输入搜索条件便可生成所需的报告。选择的报告可通过电子表格或 PDF 格式进行下载。要访问报告功能，请点击 **报告 (Reports)** 选项卡。

以下报告可用：

- **“用户信息”(User Information) 报告。**显示与帐户关联的用户列表，但是仅限于一个或多个域与该帐户关联的情况，显示的信息包括序列号 (#)、用户 ID、邮件地址、名字、姓氏、状态、创建日期、上次登录日期和上次修改日期。
- **“用户状态”(Users Status) 报告。**显示与您的域关联的用户的状态（新、活动、已阻止）。
- **“帐户使用情况”(Account Usage) 报告。**运行此报告可查看公司帐户的使用统计信息。有关“帐户使用情况”(Account Usage) 报告的信息，请参阅“‘帐户使用情况”(Account Usage) 报告”，第 2 页。

“用户信息”(User Information) 报告和“用户状态”(User Status) 报告通常由系统管理员使用。仅当具有与帐户关联的域（和用户）时，这些报告才可用。

“帐户使用情况”(Account Usage) 报告

“帐户使用情况”(Account Usage) 报告显示特定帐户的使用信息。数据按令牌分组，并且包含已发送的邮件的列表和邮件计数。令牌是用于对思科邮件安全设备 (ESA) 和 CRES（或本地密钥服务器）之间的数据进行加密的客户特定密钥，仅供客户支持人员使用。

注意　通常，组织的帐户管理员会管理单个公司帐户。

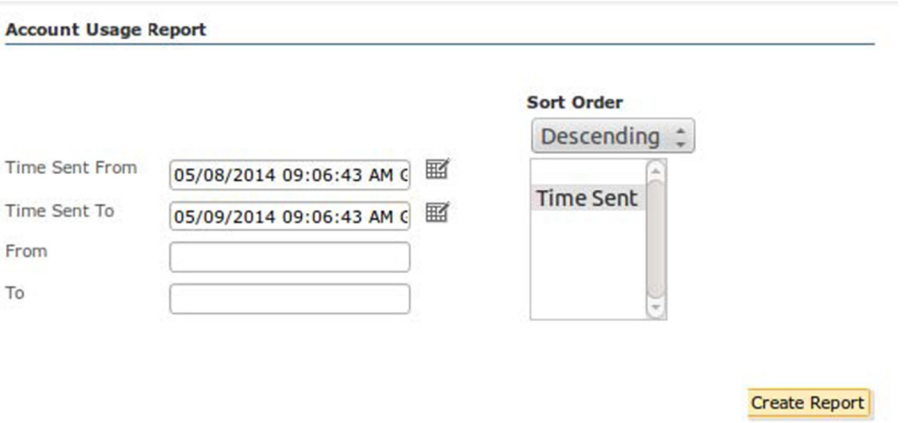
要生成“帐户使用情况”(Account Usage) 报告，请执行以下操作：

步骤 1　点击**报告 (Reports)** 选项卡以访问“查看报告”(View Reports) 页面。

步骤 2　点击**帐户使用报告 (Account Usage Report)** 链接。

此时系统会显示“帐户使用报告”(Account Usage Report) 页面。

图 3-1　“帐户使用情况”(Account Usage) 报告



步骤 3　输入或选择报告数据的时间范围。

步骤 4　输入可选搜索条件，例如发件人邮件地址或收件人邮件地址。

步骤 5　选择报告数据的排序顺序。

步骤 6　选择要包含在报告数据中的列。选择一个值，然后点击**添加到排序 (Add to sort)** 以包含该列，或点击**从排序删除 (Remove from sort)** 以排除该列。

步骤 7　点击**创建报告 (Create Report)**。

在生成报告后，可以下载 PDF 或电子表格格式的报告信息。此外，可以添加书签或打印报告的网页。

第 4 章

将创建密钥所需的数据从 IEA 迁移到 CRES

本章包含以下各节：

- 有关将创建密钥所需的数据从 IEA 迁移到 CRES 的信息（第 4-1 页）
- 如何将创建密钥所需的数据从 IEA 迁移到 CRES（第 4-3 页）
- HTTP 代理配置示例（第 4-11 页）
- 思科内容安全欢迎您发表评论（第 4-12 页）

有关将创建密钥所需的数据从 IEA 迁移到 CRES 的信息

如果当前已安装有思科 Ironport 加密设备 (IEA)，并且要将思科注册信封服务 (CRES) 用于密钥创建和管理，则不能使用 IEA 作为本地密钥服务器，而是必须执行迁移过程。

首选方法是将所有现有用户和密钥数据从 IEA 复制到 CRES 中，以便最终用户仍可打开其旧信封，不需要重新注册。为此，CRES 现在为 IEA 提供数据迁移客户端，以及用于 CRES 的数据导入服务。这些实用程序使用现有硬件，无需对基础设施进行任何更改，从而可以继续利用现有的功能，例如负载均衡和故障转移。

默认情况下，迁移客户端将在迁移数据时执行一次。可以将客户端配置为运行多次。迁移客户端会跟踪已发送的记录，而且不会重新发送 CRES 已收到的任何数据。

在迁移 IEA 后，必须完成几个步骤以确保将流量从 IEA 重定向到 CRES。在下一部分中详细介绍了这些步骤，其中包括但不限于：

1. 设置从最终用户到 HTTP 代理而不是 IEA 的 HTTP 流量重定向。
2. 将 HTTP 代理设置为将最终用户可以信任的现有或新的 SSL 证书（而不是用于 IEA 的证书）用于与代理之间的 HTTP 流量。必须使用在*思科邮件加密兼容性列表*的“CRES 支持的证书颁发机构”部分中列出的一个证书所签名或关联的证书。
3. 将代理配置为将 SSL 证书用于与 CRES 之间的可信 HTTP 通信。
4. 更新 DNS 服务器和防火墙规则，以便将计划用于 IEA 的所有 HTTP 流量重定向至 HTTP 代理。
5. 更新所有加密设备和客户端上的令牌。
6. 禁用 IEA。
7. 将邮件域与 CRES 帐户相关联。

由于切换过程不是瞬时的，一些 IEA 客户端可能会继续使用 IEA，因此有一些数据库更新可能需要镜像到 CRES。可以将数据迁移客户端配置为定期检查任何更新数据，并将任何更新的数据迁移到 CRES。

CRES 管理员可以配置允许为指定帐户导入密钥并指定何时可以导入数据的简单策略。

迁移过程将 IEA 中的用户数据和任何待处理的用户活动复制到 CRES。但是，迁移数据不包含任何用户角色或权限数据，而且迁移过程不会更改帐户管理员或属于帐户的其他用户的 CRES 权限。因此，用户的权限在 CRES 上不会升级到这些帐户管理员的权限，但是如果用户已具有帐户管理员权限，则不会删除该访问权限，无论其在 IEA 上的状态如何都是如此。在迁移后，用户可以照常升级为帐户管理员。

如何将创建密钥所需的数据从 IEA 迁移到 CRES

迁移前提条件

在迁移到 CRES 之前，必须满足以下前提条件：

- 确保不需要使用在迁移到 CRES 后将不支持的任何现有功能。有关这些功能的详细信息和示例，请参阅“在 CRES 上不受支持的功能”部分（第 4-4 页）。在与思科技术支持人员联系以开始迁移过程时，请介绍您的情况。
- 确保执行迁移的人员是数据库管理员，或者可以联系数据库管理员以获取帮助。
- 确保具有可以用作 HTTP 代理的计算机以及运行 HTTP 代理所需的软件。
- 必须将思科 IEA 软件升级到版本 6.5.6.1。
- 如果没有 CRES 帐户，请发送邮件至 stg-cres-provisioning@cisco.com 并提供以下信息：
  - 帐户名称 - 通常是公司名称。对于托管客户，帐户名称应该是“公司名称 ‹ HOSTED”
  - 将用于帐户管理员的客户邮件地址
  - 将执行加密的 ESA 设备的序列号
- 通过使用邮件地址 iea-migrations@cisco.com 与思科客户支持代表联系并提供以下信息以开始迁移过程：
  - CRES 帐号。如果没有 CRES 帐户，请联系思科以按照前面的前提条件所述创建帐户。
  - 要开始迁移的日期。至少应在计划实际执行迁移之前的 30 天联系思科。

  然后，思科客户支持代表将：
  - 配置您的帐户以启用迁移。
  - 设置迁移的开始和结束日期及时间。
  - 向您发送包含您帐户详细信息及迁移软件链接的邮件。
  - 向您发送在安全信封中包含安全密钥的邮件。

- 按照思科客户支持代表发送给您的邮件中的说明下载以下安装脚本：
  - cres-dbmigrate_install-4.4.0.xxx.sh
- 通过运行以下命令并将打印到控制台的 MD5 摘要与下载站点上显示的 MD5 摘要进行比较，验证是否正确下载了安装脚本：

  openssl dgst -MD5 cres-dbmigrate_install-4.4.0.xxx.sh
- 按照随后过程中前两个步骤的描述获取以下项目：
  - token.jar
  - 安全密钥在计划迁移后以安全信封的形式通过邮件发送给您。
- 如果使用 PostgreSQL 管理数据库，则必须安装 PL/pgSQL 才能为下面的步骤 4 运行数据库修改脚本。

在 CRES 上不受支持的功能

在迁移到 CRES 时，必须使用思科邮件安全设备而不是思科 Ironport 加密设备 (IEA)。由于 CRES 是托管服务，因此它不支持本地密钥服务器提供的一些功能，例如 IEA。因此，在迁移到 CRES 之前，必须确保不需要在 CRES 上不受支持的任何 IEA 功能。

为帮助确定是否可以迁移到 CRES，以下列表提供了当前在 CRES 上不可用的一些常用 IEA 功能示例：

- ORACLE 数据库 - 使用 Oracle 的 IEA 当前不符合进行迁移的条件。在将来的版本中会支持该功能。
- 安全邮箱
- LFS（大型文件支持）
- 语句传送
- 某些身份验证方法 - 用户在 CRES 本地数据库和 SAML（仅限客户拥有的邮件域）中注册的身份验证方法是用于 CRES 的唯一可用身份验证方法。其他 IEA 身份验证方法（如 LDAP、Kerberos 等）则不受支持。此外，不支持在多个源（也称为链查找）中进行身份验证查找。

有关 IEA 功能的详细信息，请参阅*思科 Ironport Encryption Appliance 6.5 配置手册*。

迁移过程

使用此过程可将数据从 IEA 迁移至 CRES：

步骤 1　将 token.jar 文件保存到本地驱动器：

a. 以管理员身份登录到 CRES 并选择**帐户 (Accounts)** 选项卡。

b. 选择**管理帐户 (Manage Accounts)** 选项卡。

c. 选择客户帐户管理员的帐户。

d. 选择**令牌 (Tokens)** 选项卡。

e. 点击令牌表中 SecureCompose 令牌对应的“操作”(Actions) 列下的下载图标。

步骤 2　在计划迁移后，思科技术支持人员会以安全信封的形式通过邮件将安全密钥发送给您。

步骤 3　在 IEA 上安装迁移客户端。

a. 输入以下命令以使用 SCP 将迁移客户端文件复制到 IEA。

scp cres-dbmigrate_install-4.4.0.xxx.sh admin@<IEA IP 地址>:

scp token.jar admin@<IEA IP 地址>:

b. 使用 SSH 连接到 IEA。例如，输入：

ssh admin@<IEA IP 地址>

c. 在主菜单中，输入选项 x 以退出到 UNIX 命令提示符。

注意　x 选项是一个隐藏命令，不显示在菜单选项列表中

d. 使用以下命令安装迁移客户端：

sh ./cres-dbmigrate_install-4.4.0.xxx.sh

步骤 4　运行数据库修改脚本。

- 对于 PostgreSQL，输入：

cd dbmigrate/scripts/postgres

psql -p 5432 -h localhost -d *database-name* -U *db-admin-name* -f ~/dbmigrate/scripts/postgresql/migration_table.sql

注意　必须安装 PL/pgSQL 才能执行此过程。

- 对于 MSSQL，将该脚本复制到安装了 SQL Server 管理员工具的 Windows 计算机并通过以下任一方式执行脚本：
  - 使用 SQL Server Management Studio GUI
  - 运行以下命令行命令：

    sqlcmd -H *hostname* -S *sqlserver-instance-name* -d *database-name* -U *db-admin-name* -P *db-admin-password* -i migration_table.sql

步骤 5　与思科技术支持人员合作在 dbmigrate.properties 文件中设置参数，以用于配置迁移客户端的功能。下表中介绍了这些参数。

除了在下表中显示的基本配置参数外，还可以使用多个更高级的参数，如附录 B 中所述。

可以配置的一个功能是，在迁移完成后向您以及思科技术支持人员发送通知邮件。必须为此通知配置的参数包括：*mailserver*、*mailserverport*、*notifyComplete*、*notificationRecipient* 和 *notifyCompleteForm*。

此外，还可以配置在迁移最终用户数据的过程完成后，向其发送通知邮件的功能。如果为最终用户配置通知，则思科建议向最终用户说明迁移过程，以免在其收到通知邮件时产生任何困扰。因此，此功能被视为高级功能。有关最终用户通知的可选高级参数的信息，请参阅附录 B。

可以使用 dbmigrate.properties 文件或命令行配置下表中列出的迁移客户端参数。dbmigrate.properties 文件位于具有迁移客户端安装程序的文件夹的 *conf* 子目录中：

参数	必需或可选	定义
url	必需	数据库的 JDBC 连接 URL。有关建议的值，请参阅以下说明。
driver	必需	JDBC 驱动程序名称。请参阅以下说明。
user	必需	数据库用户名。
password	必需	数据库密码。
token	必需	CRES 帐户的令牌 JAR 文件名。
securitykey	必需	用于身份验证的其他安全密钥。
importserver	可选	CRES 迁移导入服务的 URL。
passcount	可选	在完成之前创建用户和密钥表的次数。（默认值：1。最大值：无。）
passdelay	可选	迁移运行的间隔秒数。值为 0 表示无限延迟。（默认值：12 小时。最小：1 秒。）

参数	必需或可选	定义
mailserver	可选	邮件服务器的 IP 地址。
mailserverport	可选	邮件服务器的端口号。
notifyComplete	可选	启用或禁用在迁移完成后发送通知邮件的功能。有效值为 *true* 或 *false*。
notificationRecipient	可选	迁移完成后，将收到通知邮件的人员的邮件地址。
notifyCompleteFrom	可选	迁移完成后，通知邮件的发件人邮件地址。
notifyComplete Subject	可选	发送用以通知迁移已完成的邮件的主题行。

注意 如果使用与用于 IEA 的驱动程序不同的 JDBC 驱动程序，则必须为 lib 文件夹中的驱动程序复制 JAR 文件。

如果使用的是 MSSQL，请设置以下参数：

- driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
- url=jdbc:sqlserver://*database_server*;instanceName=*instance_name*;databaseName=postx;*other_options*

可在 dbmigrate.properties 文件中配置的所有参数还可使用命令行进行配置。但是，命令行有两个额外的可选参数，而且命令行仅需四个参数，如下表所示：

参数	必需或可选	定义
url	必需	数据库的 JDBC 连接 URL。
driver	必需	JDBC 驱动程序名称。
user	必需	数据库用户名。
password	必需	数据库密码。
help	可选	打印配置参数的说明。
config	可选	配置属性文件的名称。

步骤 6　输入以下命令以运行下载文件中包含的脚本来启动迁移客户端。

```
./dbmigrate_client --password=db_password
```

如果按照步骤 5 中所述配置了邮件服务器和通知参数，则迁移完成后，迁移客户端会将完成通知邮件发送给您和思科技术支持人员。然后，思科技术支持人员会检查迁移的结果，并通知您迁移是否成功。

注意　迁移过程不会处理用户帐户和域成员。现有用户记录不会移至其他帐户，而且所有新用户记录会添加到默认用户帐户 (id 1)。在迁移后，思科技术支持人员必须登录并将用户手动移动到正确的帐户。

如果 IEA 用户已存在于 CRES 上，则会保留该用户的 CRES 数据，不会生成任何错误消息。

在完成迁移并且设置了代理后，用户需要使用其 CRES 凭据来打开信封而不是其 IEA 凭据。管理员需负责通知最终用户将要执行该操作。

步骤 7　在迁移完成后，必需设置从最终用户到 HTTP 代理而不是 IEA 的 HTTP 流量重定向。需要重定向的流量包括：

- 为信封创建新密钥或者检索现有信封密钥的密钥服务器请求
- 与 Websafe 的连接
- 与安全编写的连接
- 与在线信封打开程序的连接
- 与任何其他 Web 应用的连接

要重定向此流量，应设置 HTTP/HTTPS 代理来替代 IEA。此代理的实施方式取决于现有网络。如果没有用于运行 HTTP 代理的现有 Web 服务器或代理服务器，则需要设置新的计算机来运行 HTTP 代理。有关配置示例，请参阅“HTTP 代理配置示例”部分（第 4-11 页）。

注意　在迁移过程后，将为 IEA 安全信封显示默认 CRES 徽标而不是自定义徽标。要设置自定义徽标，请配置代理以将 IEA 自定义徽标请求更改为 CRES 自定义徽标请求。
可在以下位置找到 IEA 徽标请求示例：
https://customer_domain/websafe/branding/customer-logo.gif
可在以下位置找到 CRES 自定义徽标请求示例：
https://res.cisco.com/websafe/logo/your_CRES_account_ID/branding/customer-logo.gif
要将自定义徽标添加到 CRES 帐户，请参阅“自定义注册信封上的徽标”部分（第 2-9 页）。

步骤 8　将 HTTP 代理设置为将最终用户可以信任的现有或新的 SSL 证书（而不是用于 IEA 的证书）用于与代理之间的 HTTP 流量。

注意　必须使用在*思科邮件加密兼容性列表*的“CRES 支持的证书颁发机构”部分中列出的一个证书所签名或关联的证书。

将来的版本中将不支持 SSL 版本 3。因此，应确保所使用的软件可与传输层安全 (TLS) 配合使用。

可以使用与用于 IEA 的证书（如果已由支持的证书颁发机构签署）相同的证书，也可以使用新证书。如果可能，思科建议使用现有证书。

步骤 9　将 HTTP 代理配置为将 SSL 证书用于与 CRES 之间的可信 HTTP 通信。

执行此操作的最佳方法是配置代理以参考 CA 证书可信存储。一种可管理性较低的替代方式是将代理配置为明确信任 CRES 证书，但是此方法需要在每次 CRES 证书更新时更新明确信任关系。

步骤 10　设置了 HTTP 代理后，必需更新 DNS 服务器和防火墙规则，以便将计划用于 IEA 的所有 HTTP 流量重定向至 HTTP 代理。

步骤 11　更新所有加密设备和客户端上的令牌。需要执行该操作才能实现对 keyserver 参数的加密和解密。

要更新思科邮件安全设备上的令牌，应提供 CRES 加密配置文件。要在客户端（例如 Outlook 插件、Cisco BCE Mobile App for Android 和 Cisco BCE Mobile App for iOS）上更新令牌，请下载通过 CRES 配置文件创建的新 BCE 配置文件，并通过 CRES 帐户的管理员以加密邮件的形式将其发送给这些用户。

步骤 12　停止 IEA 加密服务器，但是不要断开与 IEA 的物理连接。

步骤 13　再次运行迁移客户端以传播自首次运行以来的任何更新。或者，可以将迁移客户端保持在多次模式下运行。

成功完成第二次运行后，思科技术支持人员会为该帐户禁用进一步的迁移。

步骤 14　请联系思科技术支持人员，以将 CRES 邮件域与 CRES 帐户相关联。在此过程中，思科技术支持人员会将这些邮件域中的所有预先存在的 CRES 用户移至您的帐户。只有您拥有的邮件域可与您的 CRES 帐户关联。

迁移完成后的功能差异

CRES 具有与 IEA 不同的功能集，而且此差异可能会导致对您的用户产生一些困扰。思科建议针对两个功能集间的功能差异为用户提供培训。

有关 IEA 功能的详细信息，请参阅*思科 Ironport Encryption Appliance 6.5 配置手册*。

此外，如上面的步骤 14 所述，如果您不拥有某个邮件帐户，则该帐户不能与您的 CRES 帐户关联。因此，来自这些帐户的邮件将在邮件别名中具有不同的域名。思科建议还针对此差异为用户提供培训，以帮助他们消除此困扰。

迁移错误消息

以下错误消息是在迁移过程中将会生成的最常见消息。如果收到任何其他错误消息，请联系思科客户支持以了解有关如何解决该问题的信息。

错误消息

```
This IEA database uses a non-standard authentication system for
keys, you may continue with this migration, but when these keys
are moved to CRES they will be modified to use CRES
authentication.

Do you wish to proceed with this migration and use CRES
authentication for your keys?
```

说明　IEA 数据库使用除 PostXAuth 外的密钥服务器身份验证类型，并且 precondition.keychecker.actionOnFail 参数设置为 *prompt*。

建议的操作　解决方法方法是，回应“Yes”以继续迁移并使用 CRES 身份验证，但是我们建议先联系思科客户支持部门，然后再做出此决定。

错误消息

```
This IEA database uses non-standard key authentication, i.e.,
C_LOOKUPNAME <> 'PostXDatabase' and the Keystore checker failed
to prompt the user for resolution (console not available).
```

说明　IEA 数据库使用除 PostXAuth 外的密钥服务器身份验证类型，并且 precondition.keychecker.actionOnFail 参数设置为 *fail*。

建议的操作　联系思科客户支持部门。

错误消息

```
ERROR: language "'plpgsql'" does not exist.
```

说明　您未满足该前提条件：如果使用 PostgreSQL 管理数据库，则必须安装 PL/pgSQL 才能运行数据库修改脚本。

建议的操作　如果使用 PostgreSQL，则确保已安装 PL/pgSQL。

HTTP 代理配置示例

该示例显示了在配置 HTTP/HTTPS 代理时，如何配置其中一个最常用的产品：Apache HTTP 服务器。这并不代表唯一可能的示例或最为推荐的产品。您的基础设施会确定哪个产品最适合供您用作 HTTP/HTTPS 代理。

使用以下过程配置此情况。

步骤 1　通过在 Apache httpd.conf 文件或等同的文件中输入以下命令来启用代理和 SSL。

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule ssl_module modules/mod_ssl.so
```

步骤 2　确保 CA 证书位于适当的文件夹（例如，在 /etc/ssl/certs 中），并输入以下命令配置 Apache 服务器以在该文件夹中查找 CA 证书。

```
SSLCACertificatePath /etc/ssl/certs/
```

步骤 3　通过将证书文件复制到 Apache 安装用于证书的目录（例如，/etc/ssl/your-host-certificate.pem）来安装 IEA 证书。

步骤 4　通过输入以下命令为 HTTP 端口 80 启用代理设置：

```
<VirtualHost www.your-hostname.com:80>
    ServerName www.your-hostname.com

    ProxyPreserveHost On
     ProxyRequests off
     ProxyPass / http://res.cisco.com:80/
    ProxyPassReverse / http://res.cisco.com:80/
</VirtualHost>
```

步骤 5　通过输入以下命令为 HTTPS 端口 443 启用代理设置：

```
    <VirtualHost www.your-hostname.com:443>
        ServerName www.your-hostname.com

        ProxyPreserveHost On
        ProxyRequests off

        ProxyPass / https://res.cisco.com:443/
        ProxyPassReverse / https://res.cisco.com:443/

        SSLEngine on
        SSLProxyEngine on
        SSLCertificateFile    /etc/ssl/your-host-certificate.pem
    </VirtualHost>
```

思科内容安全欢迎您发表评论

思科内容安全技术出版物团队乐于提高产品文档的质量。我们时刻欢迎您的评论和建议。您可以将评论发送至以下电邮地址：

contentsecuritydocs@cisco.com

附 录 A

联系客户支持

要联系客户支持以获得思科注册信封服务 (CRES)，可以向以下地址发送邮件：

support@res.cisco.com

有关完整的客户支持信息，请参阅以下 URL：

https://res.cisco.com/websafe/help?topic=ContactSupport

注意 还可以通过此 URL 访问即时消息聊天支持。

此外，可以随时通过电话或在线形式请求我们的支持。可以使用以下方法之一联系思科客户支持部门：

- 思科支持门户：http://www.cisco.com/support
- 电话支持：拨打 800-553-2447 和全球电话号码联系美国和加拿大的思科技术支持中心 (TAC)

如果您是通过经销商或另一个供应商购买的支持，请直接联系该供应商咨询您的产品支持问题。

注意 对您来说，可用的支持等级取决于您的服务等级协议。Cisco IronPort 客户支持服务等级协议详细信息可从支持门户上获取。查看该页面获取有关您的支持等级详情。

联系支持人员的原因包括：

- 报告问题
- 将域添加到您的帐户
- 将用户添加到您的域
- 不直接通过 CRES 管理用户时，管理用户（例如，重置密码和锁定用户）。

思科内容安全欢迎您发表评论

思科内容安全技术出版物团队乐于提高产品文档的质量。我们时刻欢迎您的评论和建议。您可以将评论发送至以下电邮地址：

contentsecuritydocs@cisco.com

附 录 B

用于将创建密钥所需的数据从 IEA 迁移到 CRES 的其他参数

除了在第 2 章介绍的迁移客户端的 dbmigrate.properties 文件或命令行中使用的参数外，还可以使用下表中的参数。

如有没有思科技术支持人员的帮助，不可使用 dbmigrate.properties 文件或命令行更改这些参数的默认值。

max-Errors 参数指示在迁移客户端放弃当前运行之前可生成的最大错误数。max-Errors 参数的值为 0 表示对于可以生成的错误数没有限制。

某些参数用于密钥检查器进程，以指定在运行迁移之前必须满足的前提条件。密钥检查器进程会扫描数据库以了解是否存在任何非 PostXAuth 的密钥服务器身份验证类型。可以将参数配置为在不满足指定的前提条件时使密钥检查器进程执行特定操作。

有关在迁移过程中生成的错误的信息，请参阅“迁移错误消息”部分（第 4-10 页）。

参数	与命令行 / 属性文件配合使用	定义
maxUserErrors	两者皆可	在停止迁移之前，迁移用户表时可出现的最大错误数。
maxUuidErrors	两者皆可	在停止迁移之前，迁移 UUID 表时可出现的最大错误数。
maxKeyErrors	两者皆可	在停止迁移之前，迁移密钥表时可出现的最大错误数。
maxContactErrors	两者皆可	在停止迁移之前，迁移联系表时可出现的最大错误数。
precondition.key checker.database Name=*dbname*	两者皆可	指定在运行迁移之前，必须在规则文件中设置以用于密钥检查器进程的数据库名称。
precondition.key checker.class= *class*	两者皆可	指定在运行迁移之前，必须作为密钥检查器进程必须满足的前提条件调用的类名称。
precondition.key checker.actionOn Fail=*action*	两者皆可	设置不满足密钥检查器进程的前提条件时要执行的操作。 其中 *action* 的可用值为“prompt”、“pass”和“fail”。
autoNotifyUser	可选	启用或禁用在迁移完成后按用户发送通知邮件的功能。有效值为 true 和 false。
notifyUserFrom	可选	迁移完成后，用户通知邮件的发件人邮件地址。
notifyUserSubject	可选	发送给用户以通知迁移已完成的邮件的主题行。
notifyUser.params .company	可选	将收到迁移已完成通知的用户公司的名称。
notifyUser.params .cres.login	可选	将收到迁移已完成通知的用户公司的 CRES 登录 URL。
level	两者皆可	日志记录级别。可用值包括 ERROR、WARN、INFO（默认值）和 DEBUG。

参数	与命令行 / 属性文件配合使用	定义
logfile	两者皆可	日志文件名（默认：dbmigrate.log）。
tableset	两者皆可	包含要导出的表组的逗号分隔列表。可能的值包括： • users - 用于导出所有用户、用户映射和用户配置文件表。 • contacts - 用于导出所有通讯录表。 • keys - 用于导出所有密钥。 • uuids - 用于导出 UUID。
reportProcessors	两者皆可	包含要为其生成报告的表组的逗号分隔列表。可能的值包括： • users-report - 用户、用户映射和用户配置文件表的报告。 • keys-report - 密钥的报告。
maxsize	两者皆可	从 IEA 发送的 HTTP 邮件正文的最大大小（默认：2 MB。最大：10 MB）。
batchsize	两者皆可	每个请求发送的最大记录数（默认：200。最大：10000）。
batchdelay	两者皆可	批处理之间暂停的时间（默认：0.6 秒。最少：0.2 秒）。
retrycount	两者皆可	每次批处理在放弃之前重试的次数（默认：5。最大：30）。
retrydelay	两者皆可	重试之间暂停的时间（默认：20 秒。最小：1 秒）。
rules	两者皆可	规则文件的名称。
help	命令行	打印配置参数的说明。
config	命令行	配置属性文件的名称。
connectTimeout	两者皆可	HTTP 连接超时。
socketTimeout	两者皆可	HTTP 套接字超时。
sendBufferSize	两者皆可	HTTP 发送缓冲区的大小。

参数	与命令行 / 属性文件配合使用	定义
receiveBufferSize	两者皆可	HTTP 接收缓冲区的大小。
acceptSelfSigned	两者皆可	由于不能使用自签名 SSL 证书，因此必须将此参数保留为默认设置 false。
acceptUntrusted	两者皆可	由于不能使用不受信任的 SSL 证书，因此必须将此参数保留为默认设置 false。
acceptExpired	两者皆可	由于不能使用已过期的 SSL 证书，因此必须将此参数保留为默认设置 false。
requireServerTLS	两者皆可	需要使用 TLS 服务器。有效值为 true 和 false。