收集身份服务引擎上的支持捆绑包

目录

简介

收集思科ISE上的支持捆绑包

- 步骤1.启用ISE组件的调试
- 步骤2.重新创建问题
- 步骤3.禁用调试
- 步骤4.收集支持套件

简介

本文档介绍如何通过CLI或GUI从Cisco ISE 3.x收集支持捆绑包，该捆绑包包含ISE故障排除所需的重要数据。

收集思科ISE上的支持捆绑包

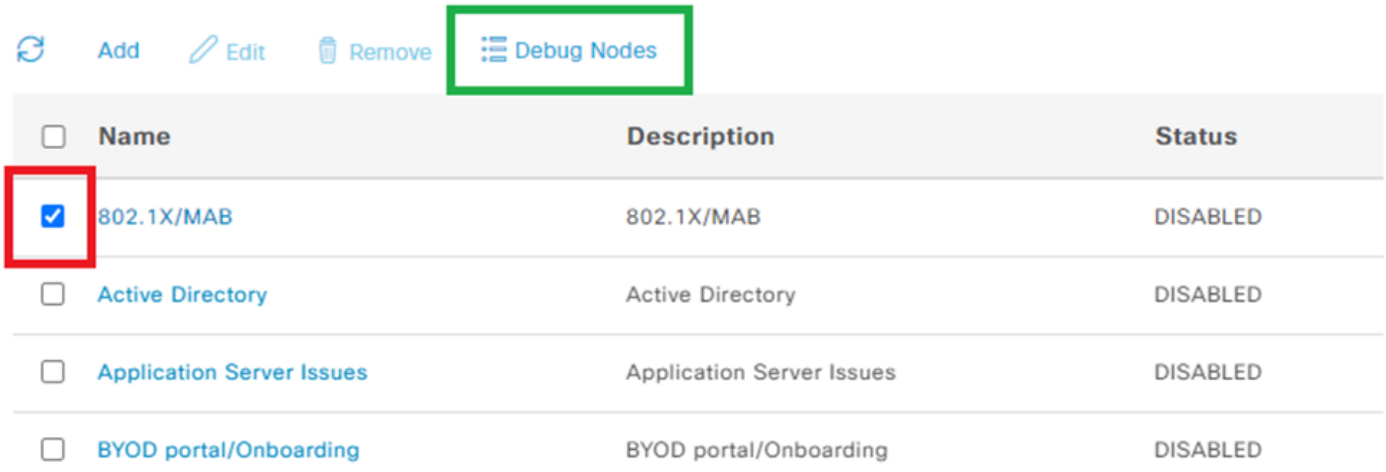
步骤1.启用ISE组件的调试

ISE上的各种问题需要不同的日志集进行故障排除。TAC工程师必须提供所需调试的完整列表。但是，ISE 3.x具有预配置的调试类别，您可以使用这些类别来收集初始徽标，以加快案例解决速度。

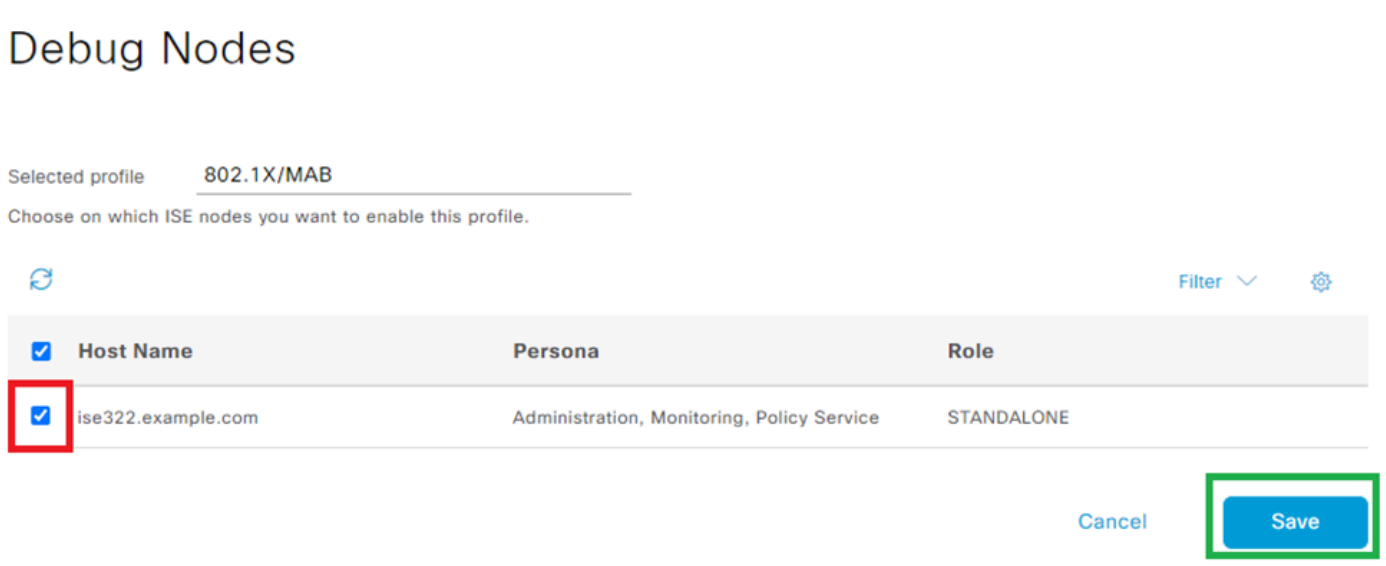
TAC工程师请求的调试列表必须始终优先于此列表。

1.要查找这些预配置的调试，请导航到操作>故障排除>调试向导>调试配置文件配置。

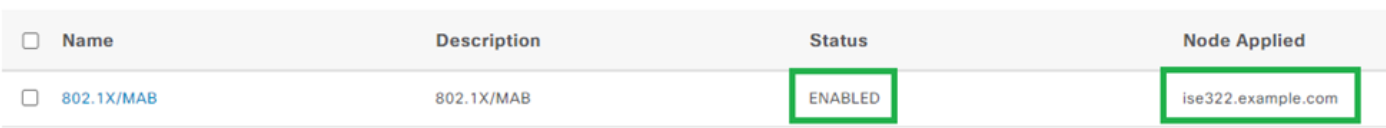
2.选择必须启用调试的功能，并在每行开头选择正确的复选框。例如，802.1x（红色），然后导航到节点选择（绿色）：



3.然后，为调试选择节点，这些节点必须通过选择每行开头处的正确复选框来启用（红色）。 然后，保存更改（绿色）：



4.页面移回“调试配置文件配置”，调试状态更改为ENABLED，显示运行这些调试的节点的相关信息。



步骤2.重新创建问题

1.启用所有必需的调试后，请重新创建问题以生成日志。

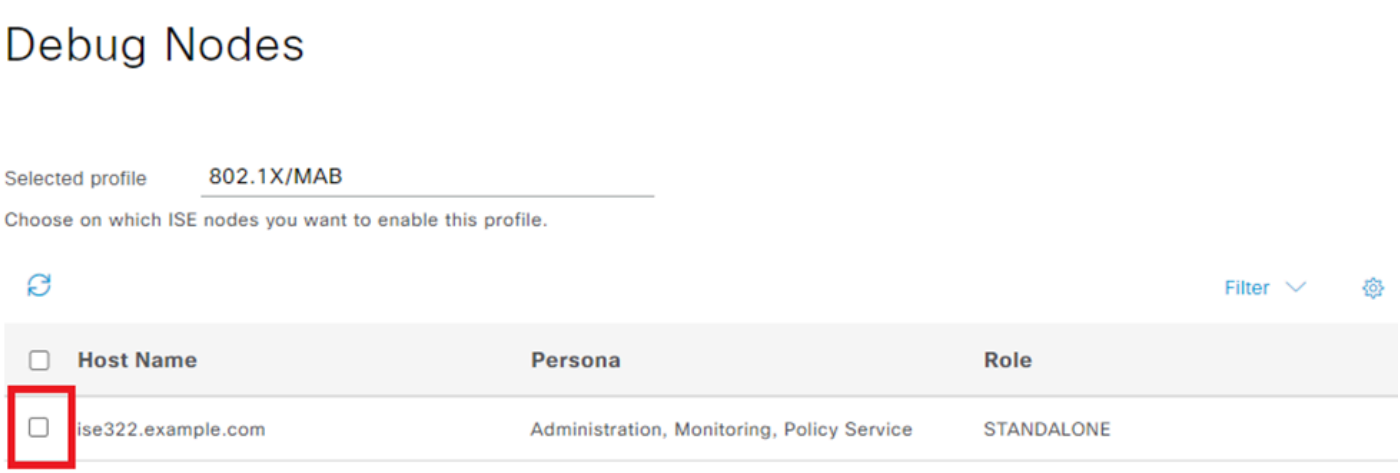
- 如果无法手动触发问题，则必须等待下次出现。
- 如果在启用调试之前出现问题，则没有足够的信息进行故障排除。
- 理想情况下，必须在问题发生后立即收集支持捆绑包。记录日志分析所需的辅助信息：

注意：日志分析所需的辅助信息：

- 娱乐的时间戳。
- 事件的任何唯一ID，例如MAC地址、IP地址、用户名或会话ID（取决于具体情况，通常为MAC/IP +用户名）。

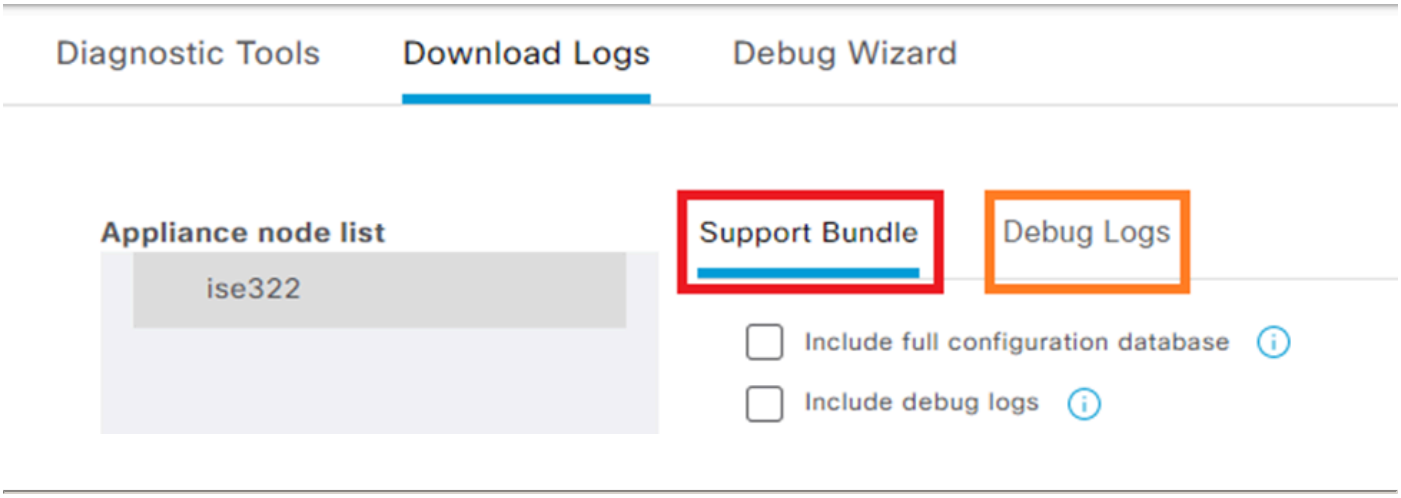
步骤3.禁用调试

重新创建问题后，请禁用调试，以防止新生成的日志被过多的日志记录覆盖。为此，请重复步骤1中的操作。但是，在节点选择页面上，取消选中适当的复选框并像以前一样进行保存。

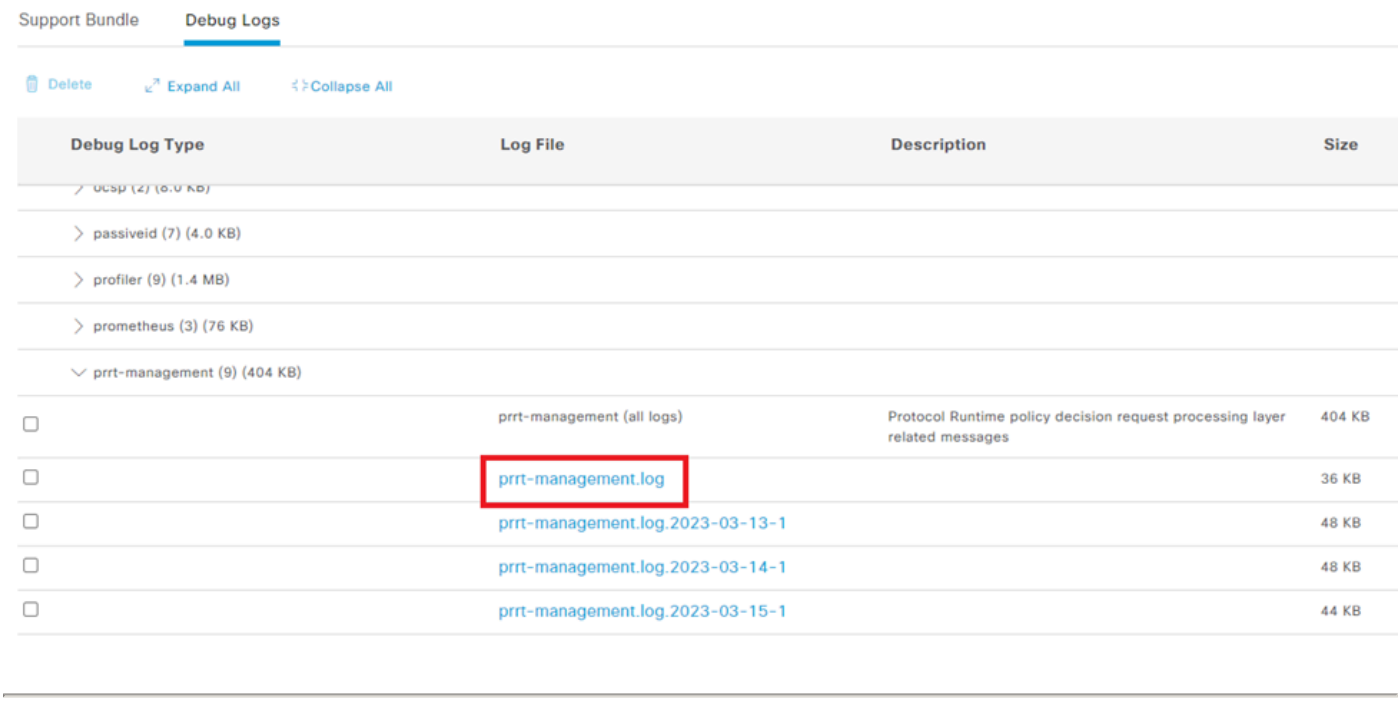


步骤4.收集支持套件

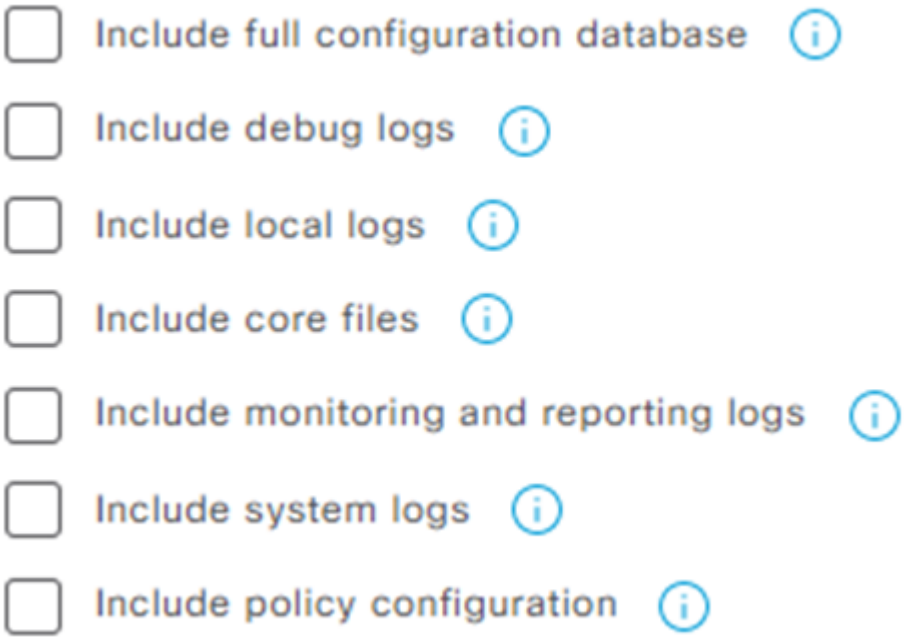
1.导航到操作>故障排除>下载日志，然后选择ISE节点（其中启用了调试）。 在每个节点的选项卡上，有两个选项：收集支持捆绑包（红色）或下载特定日志文件 — 调试日志（橙色）。



2.对于“调试日志”，将显示所有可用日志文件的完整列表。单击文件名称后，即会下载该文件。

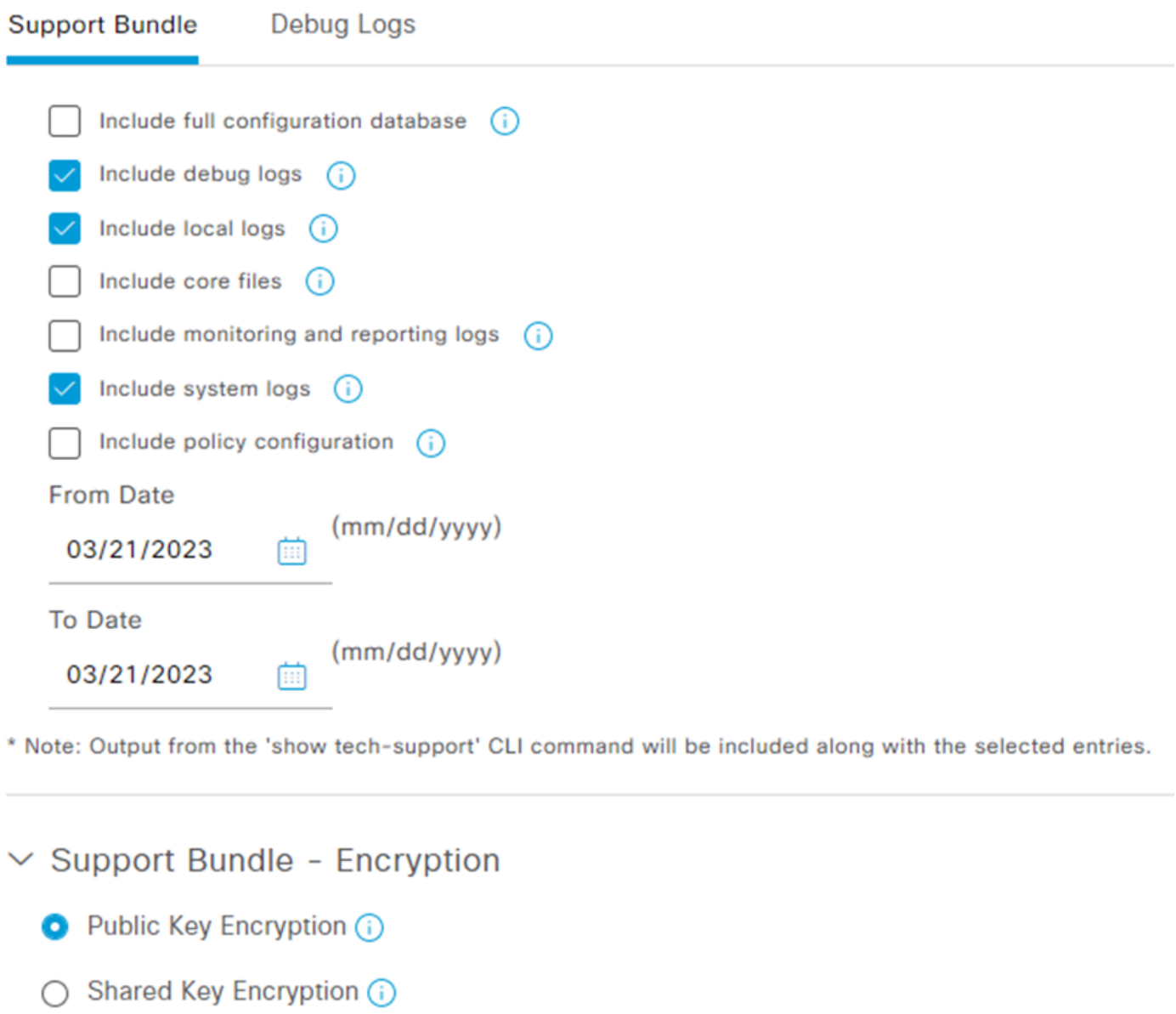


3.支持捆绑包是一个包含选定组中的所有日志的软件包。

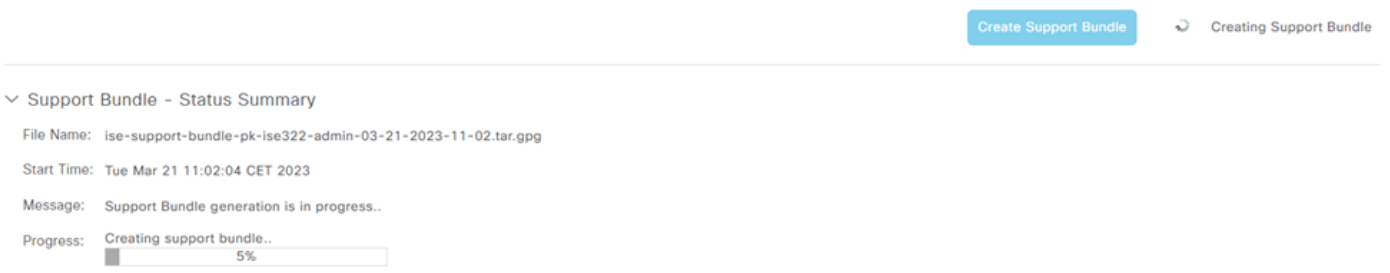


- 完整配置数据库将完整ISE配置附加到支持捆绑包。
- 调试日志最常用，因为它们包含来自所有ISE组件的所有调试。
- 本地日志包含显示部署中此节点的RADIUS身份验证的日志。
- 核心文件可能导致支持捆绑包增长，但在故障故障排除期间需要使用该捆绑包。
- 监控和报告日志包含操作数据。
- 系统日志包含系统特定日志（用于排除操作系统提供的服务故障）。
- 策略配置，即ISE上已配置策略的xml版本。

对于大多数情况，只包括调试日志和本地日志就足够了。对于稳定性和性能问题，需要核心和系统日志。如果您仅选择公钥加密，TAC可以使用思科私钥解密此捆绑包。共享密钥允许您设置解密日志所需的密码。如果它是共享密钥，请确保TAC工程师具有访问权限，以便在思科端解密捆绑包。



4.设置所有内容后，单击创建支持包按钮并等待。



完成创建支持捆绑包的流程后，即可下载该捆绑包。单击Download后，支持捆绑包将保存在PC的本地磁盘上，并且可以上传到TAC进行故障排除。

如果Web界面不可用，您可以从CLI收集支持捆绑包。为此，请使用SSH或控制台访问登录并运行以下命令：

```
backup-logs name repository ftp {encryption-key plain key | public-key}
```

---

name — 您的支持捆绑包的名称

ftp - ISE上配置的存储库的名称

key — 这是用于加密/解密支持捆绑包的密钥

上载支持捆绑包的官方工具是支持案例管理器。请勿压缩或更改支持捆绑包文件的扩展名。必须以ISE下载时完全相同的状态上传。

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

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

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