变更管理

如果您的组织需要实施更加正式的配置更改流程，包括在部署更改之前进行审核跟踪和正式审批，则可以启用“更改管理”。

关于变更管理

一些组织需要实施正式的方法来部署配置更改。这可能包括更多审核，以及在对设备进行配置更改之前必须进行的正式审批流程。

如果您的组织使用更正式的配置更改流程，您可以启用更改管理来实施该流程。使用变更管理时，管理员必须先创建故障单，然后才能进行配置更改。然后，更改完成后，他们必须提交故障单进行审批，然后才能部署建议的更改。这使您可以执行正式的审批流程，并确保由合适的员工做出最终决策。

使用“更改管理”时，管理员可以在故障单中查看自己的更改，但无法查看其他人在故障单中所做的更改。由于一旦用户在故障单中进行更改，策略就会被锁定，因此用户应该无法进行干扰性更改。但是，当其他用户进行了等待审批的更改时，用户将无法进行更改。

管理员可以创建多个故障单，以便单个故障单仅包含逻辑相关的策略更改。范围更有限的故障单也更容易快速评估和批准。

以下主题介绍变更管理工作流程以及哪些策略和对象需要提交故障单和审批流程。

如何在变更管理工作流程中配置设备

当您启用更改管理时，配置设备的用户需要稍微更改其方法。对支持的策略和对象进行配置更改时，配置专家需要采用以下方法。

过程

步骤 1 创建故障单。

步骤 2 打开故障单。

步骤 3 对配置进行更改。

请注意，在线帮助和用户指南中介绍的程序假定“变更管理”处于非活动状态，并省略创建、打开或提交故障单的任何步骤。

步骤 4 或者，预览并验证故障单，以确保更改完整且正确。

步骤 5 提交故障单。此时，审批人可以批准或拒绝故障单。

- 如果故障单获得批准，请部署更改。
- 如果故障单被拒绝，请解决问题，然后重新提交故障单。

创建单独的审批人和配置角色

某些系统定义的角色具有修改（创建/打开/丢弃）和审核（批准/拒绝）故障单的权限：

- 要修改和查看故障单，请执行以下操作：
  - 管理员
  - 网络管理员
- 仅修改故障单：
  - 访问管理员
  - 入侵管理员
- 仅查看故障单：
  - 安全审批人

如果您的组织要求需要更精细的角色来分隔这些活动，则可以创建单独的角色，以确保仅将故障单审批分配给具有审批更改的组织权限的用户。要创建新的用户角色，请转至 **系统** > **用户**，然后选择 **用户角色** 选项卡。。

以下是 **系统** > **更改管理** 文件夹中与故障单使用和审批相关的权限。请注意，这些权限仅在启用更改管理后可用。

- 修改故障单 - 创建故障单（为自己）、使用配置更改故障单，以及丢弃故障单。
- 审核故障单 - 批准或拒绝故障单。

- 修改和查看通知单 - 要为自己和他人创建通知单，请使用通知单，并批准/拒绝通知单。您还可以接管分配给其他用户的通知单。

您所采取的方法取决于精细的要求。例如：

- 如果还应允许您的审批人进行配置更改，您只需为他们分配系统定义的角色，例如管理员。然后，创建包含相同权限但不包含“审核故障单”权限的自定义仅配置角色。
- 如果您需要完全分离审批者和进行配置更改的人员，请为两者创建自定义角色，将角色限制为“修改故障单”或“审核故障单”权限，以及查看或更改支持的策略和对象所需的所有其他权限。

支持变更管理的策略和对象

如果策略或对象支持更改管理工作流程，则必须在未解决的故障单中创建、编辑或删除策略或对象，包括将策略分配给设备。

可以创建、编辑或删除不支持更改管理工作流程的任何操作、策略或对象，而无需打开故障单。即使故障单处于未决状态，对不受支持的策略所做的更改也不会包含在已发出故障单的更改中，并且可以立即进行部署。

以下列表包括支持的策略和对象。未列出的任何内容均不受支持。

支持的策略

- 访问控制，包括规则、对其他策略的引用和继承设置。故障单中不包含克隆访问控制策略。该克隆将被立即接受并提供给所有用户。
- 设备配置策略：
  - 接口
  - 内联集
  - DHCP
  - VTEP
  - 所有路由
- 解密策略
- DNS 策略
- FlexConfig
- 入侵策略和网络分析策略 (NAP)，仅限 Snort 3。
- 恶意软件和文件策略
- 网络地址转换 (NAT)
- 网络发现策略

- 平台设置
- 预过滤器
- QoS
- Umbrella SASE 拓扑
- VPN 策略，站点间和远程访问
- Zero Trust 访问

支持的对象

- AAA 服务器
- 访问列表
- 地址池
- AS 路径
- 密码套件列表
- 社区列表
- 可分辨名称对象
- DHCP IPv6 池
- DNS 服务器组
- FlexConfig 对象
- 组策略
- 接口
- 密钥链
- 网络
- PKI 证书，所有对象
- 策略列表
- 端口
- 前缀列表
- 路由映射
- Sinkhole
- SLA 监控器
- 时间范围

- 时区
- 隧道区域
- URL
- 变量集
- VLAN 标记
- VPN 对象（IKEv1、IKEv2 IPSec 和策略、PKI 注册、证书映射）

变更管理的要求和前提条件

型号支持

管理中心

支持的域

任意

用户角色

- 要启用或禁用变更管理： 管理员。
- 要修改和查看故障单，请执行以下操作：
  - 管理员
  - 网络管理员
- 仅修改故障单：
  - 访问管理员
  - 入侵管理员
- 仅查看故障单：
  - 安全审批人

变更管理的准则和限制

- 在更改管理模式下运行时，用户可以对支持的策略进行更改，但无法保存更改。例如，您可以在没有打开故障单的情况下通过对话框创建新的平台设置策略，但是当您点击确定实际创建策略时，您将收到错误消息，并且不会创建策略。

- 以下活动要求所有故障单都处于终止状态，即已批准或已丢弃：备份/恢复、在域之间移动设备、升级 防火墙管理中心。
- 从资产中删除设备需要批准或丢弃涉及该设备的所有故障单。
- 某些进程（例如部署和备份/恢复）会阻止您更改更改管理模式。等待该过程完成以更改模式。
- 根据更改管理是否支持功能和对象，您在配置功能时创建对象的能力受到限制。例如，更改管理不支持导入配置。因此，在导入期间无法创建受支持的安全区域对象。另一方面，您可以在配置访问控制规则时创建新对象，因为这两种规则都受支持。
- 使用 云交付的防火墙管理中心时，只有在 思科安全云控制 中定义的用户至少交叉启动一次 cdFMC 后，才能为其分配故障单。在第一次交叉启动之前，用户不存在于 cdFMC中。

启用或禁用更改管理

默认情况下，更改管理工作流程处于禁用状态。用户在进行配置更改时不需要打开故障单并获得批准。如果要实施更改管理工作流程，则必须为系统全局启用它。

开始之前

有几个系统进程会阻止您启用/禁用更改管理。如果正在执行以下任何操作，则需要等待它们完成后才能更改这些设置：备份/恢复；导入/导出；域移动；升级； Flexconfig迁移；设备注册；高可用性注册、创建、中断或切换；集群创建、注册、中断、编辑、添加或删除节点； EPM 中断或加入。

更改这些设置时，无法锁定访问控制策略。如果策略已锁定，则必须等待锁定被释放，然后才能启用/禁用此功能。

过程

步骤 1 选择**系统 (⚙) > 配置**。

步骤 2 点击 **变更管理**。

步骤 3 选择 **启用变更管理**。

要禁用该功能，请取消选择该选项。要禁用变更管理，必须批准或丢弃所有故障单。无法禁用变更管理，如果任何故障单处于“进行中”、“暂时搁置”、“已拒绝”或“待审批”状态。

步骤 4 选择 **需要审批的数量**，即要批准和部署故障单，必须有多少管理员批准更改。默认值为 1，但每个故障单最多可以有 5 个审批人。用户可以在创建故障单时覆盖此编号。

步骤 5 选择 **故障单清除持续时间**，即保留已批准的故障单的天数，范围为 1-100 天。默认值为 5 天。

步骤 6 （可选。）输入**回复地址**和**审批者列表地址**的邮件地址。您还必须配置邮件通知系统设置，邮件才能正常工作。

步骤 7 点击**保存**。

系统将 **工单** (▣) 快捷方式添加到菜单栏，并添加 **系统** (⚙) > **更改管理流程** 命令。用户可以使用这些方法来管理故障单。

管理故障单

启用更改管理时，必须在故障单的上下文中完成受支持策略的配置更改。您可以打开故障单，进行更改，然后提交故障单进行审批。

您可以在“更改管理”页面上或通过“故障单”快速访问菜单查看故障单列表并创建新故障单。所有故障单更改都在每个菜单中同步，因此您可以在方便时来回切换，并使用您喜欢的任何方法。

注释 当您打开故障单并对受支持的策略进行更改时，该策略将被其他用户或通过其他故障单锁定。策略保持锁定，直到故障单被批准或丢弃。

过程

步骤 1 执行以下任一操作：

- 选择 **系统** (⚙) > **更改管理流程** 打开显示现有故障单的页面。
- 点击 **工单** (▣) 快速访问菜单。图标可以命名为“选择故障单”（如果未打开故障单）、故障单名称（如果已打开故障单）或未命名（如果不存在故障单）。

两个页面的组织方式相同。**故障单** 选项卡列出所有故障单，而 **审核** 选项卡列出已提交审批的故障单。默认视图仅显示您的故障单。

步骤 2 在 **故障单** 选项卡上，执行以下任何操作：

- 要创建新故障单，请点击 **添加故障单**。
- 要查看故障单的详细信息，请点击故障单名称旁边的>。“详细信息”页面包括UUID、名称、说明、用户、上次修改日期和注释。历史记录页面包括故障单的状态更改。顶部的图像显示了故障单在整个工作流程中的位置。
- 要预览未解决的故障单的配置更改，请点击 **预览** (🔍)。
- 要验证未解决的故障单中的配置更改，请点击 **验证** (✓) 或 **更多** (⋮) > **验证** 。如果存在任何验证错误，系统将打开一个对话框，显示错误、警告和参考消息。
- 要创建故障单，请点击 **打开** (📂) 或 **更多** (⋮) > **打开** 。
- 要关闭未解决的故障单，请点击 **暂停故障单 (X)** 或 **更多** (⋮) > **暂停故障单**。关闭故障单不会将其提交进行审核，也不会解除对已编辑策略的任何锁定。

- 要提交未解决的故障单以供审核和批准，请点击 **提交供审批** () 或 **更多** () > **提交以供批准** 。故障单必须处于打开状态才能提交。
- 要丢弃故障单，请点击 **丢弃** () 或 **更多** () > **丢弃** 。
- 要接管或重新分配故障单，请 **更多** () > **在查看系统中的所有故障单时点击接管故障单** 。
- 要搜索故障单，请在搜索框中键入字符串。搜索将查看故障单名称、描述和负责用户。
- 要按故障单状态过滤列表（在“更改管理工作流程”页面上）， **请**点击列表 **上方**的状态： **新建** 、未解决、待审核（故障单已关闭）、已 **拒绝**、 **待批准**、 **已批准**。每个状态都有该状态的故障单数量的计数。点击 **我的故障单** 下的 **全部** 可恢复显示所有故障单的默认设置，或点击 **系统** 故障单下的 **全部** 以查看每个人的故障单。

步骤 3 在 **审核**选项卡上，对已提交的故障单执行以下任何操作。如果没有已提交的故障单，则列表为空。此外，只有具有审核故障单权限的用户才能看到此选项卡。

- 要预览故障单的配置更改，请点击 **预览** ()。
- 要验证未解决的故障单中的配置更改，请点击 **验证** () 或 **更多** () > **验证** 。
- 要批准故障单，请点击 **批准** () 或 **更多** () > **批准**。
- 要拒绝请求，请点击 **拒绝** () 或 **更多** () > **拒绝**。

创建变更管理故障单

使用更改管理工作流程时，必须在未解决的故障单的上下文中执行所有配置更改。如果您还没有故障单，则必须创建一个新的故障单。

过程

步骤 1 选择 **系统** () > **更改管理流程**或点击 **工单** () 快捷菜单。

步骤 2 点击 **添加故障单**。

步骤 3 配置故障单选项：

- **名称**- 故障单的名称。名称可以包含字母、数字、空格和以下特殊字符：#-_!
- **说明**-您打算使用此故障单进行配置的可选说明。例如，如果您有一个与您打算使用此故障单修复的问题相关的案例编号，这将是说明中的有用信息。
- **审批的数量**-要批准和部署故障单，必须有多少管理员批准更改。您可以指定 1-5。
- **分配到** -选择将拥有故障单并负责实施更改的用户。选择 **自己** 将其分配给自己。

步骤 4 点击以下选项之一：。

- **创建**-故障单已添加到故障单列表，但未打开。您需要先打开它，然后才能在故障单的上下文中工作。
- **创建并打开** - 通知单将添加到通知单列表并打开。

提交配置更改请求

必须先打开故障单，然后才能在故障单中进行更改。

如果您有另一个待处理的故障单，系统会在打开新的故障单之前为您搁置（关闭）该故障单。

过程

步骤 1 选择 **系统** (⚙) > **更改管理流程**或点击 **工单** (📋) 快捷菜单。

步骤 2 在 **故障单** 选项卡上，点击 **打开** (📂) 或 **更多** (⋮) > **打开** 故障单。

步骤 3 或者，输入操作的注释。

步骤 4 点击**打开 (Open)**。

现在，您可以开始部署配置更改。故障单图标的名称将更改为待处理故障单的名称。

预览故障单

您可以在更改配置时或在批准故障单之前预览故障单。预览显示在故障单上下文中进行的所有配置更改。

过程

步骤 1 选择 **系统** (⚙) > **更改管理流程**或点击 **工单** (📋) 快捷菜单。

步骤 2 点击 **预览** (🔍) 获取故障单。

系统会显示“预览”对话框。更改根据对话框顶部的图例进行颜色编码。

步骤 3 在已更改的策略列表中选择要查看其更改的策略。

您将看到 Cisco Secure Firewall Management Center 中定义的当前策略版本（位于左侧）以及故障单中定义的建议更改。

对于包含“平台设置”等页面的策略，您可以在“已更改的策略”列表中选择整体策略以查看所有更改，或选择策略中的特定页面。

您无法在预览中更改更改。如果您需要更改某些内容，则必须关闭预览并返回到要更改的策略。

步骤 4 或者，点击 **下载为 PDF** 将预览保存为 PDF 文件，以供离线查看或存档。

步骤 5 点击**确定**。

提交故障单

完成故障单所需的更改后，您可以预览并验证更改。然后，当您对更改感到满意时，请提交故障单以供审核和批准。

在您提交故障单并且故障单获得批准之前，不会应用在故障单中所做的更改。在获得批准之前，故障单中修改的所有策略都将锁定到该故障单，其他任何人都无法更改。

过程

步骤 1 选择 **系统** (⚙) > **更改管理流程**或点击 **工单** (🖥) 快捷菜单。

步骤 2 点击 **提交供审批** (📤) 或 **更多** (⋮) > **提交待批准** 请求。

步骤 3 或者，为您的操作输入注释。

步骤 4 点击**提交 (Submit)**。

丢弃故障单

如果您不再需要对其创建故障单的更改，则可以丢弃该故障单。当您丢弃故障单时，您在故障单中所做的任何更改都将被删除。

您无法撤消此操作并检索故障单及其更改。如果需要，您必须创建一个新的故障单并重新开始。

您无法在提交故障单后将其丢弃。但是，如果审批人拒绝了该故障单，您可以将其丢弃。

注释 如果您有权修改故障单，则可以丢弃属于其他用户的故障单。这样就可以处理管理员正在休假或无法管理处理中的故障单的情况。 如果您有“审核故障单”权限，则可以重新分配或接管故障单，而不是将其丢弃。

过程

步骤 1 选择 **系统** (⚙) > **更改管理流程**或点击 **工单** (🖥) 快捷菜单。

步骤 2 点击 **丢弃** (🗑) 或 **更多** (⋮) > **丢弃** 该故障单。

步骤 3 或者，为您的操作输入注释。

步骤 4 点击 **丢弃**。

批准或拒绝故障单

当用户提交故障单时，必须批准该故障单中所做的更改才能变为活动状态并可供部署。

您是否可以批准自己的故障单，还是有单独的审批人，取决于您的工作场所策略和用户角色的分配方式，而不是管理软件。

详细信息视图包括故障单所需的审批人数量以及故障单的审批人。

如果更改不充分或不需要，您可以拒绝故障单。被拒绝的故障单返回给提交者，然后提交者可以进行其他更改并重新提交故障单，或者直接丢弃故障单及其包含的配置更改。

过程

步骤 1 选择 **系统** (⚙) > **更改管理流程**或点击 **工单** (📋) 快捷菜单。

步骤 2 在 **审核** 选项卡上，点击故障单的 **预览** (📄) 并评估建议的更改。

您还可以点击 **验证** (☐) 或 **更多** (⋮) > **验证** 来检查错误。

步骤 3 完成评估后，请执行以下操作之一：

- 要批准故障单，请点击 **批准** (✓) 或 **更多** (⋮) > **批准**。
- 要拒绝请求，请点击 **拒绝** (✕) 或 **更多** (⋮) > **拒绝**。

步骤 4 或者，为您的操作输入注释。

步骤 5 根据需要点击 **批准** 或 **拒绝**。

接管或重新分配故障单

有时可能需要接管其他人创建的故障单。例如，故障单所有者可能正在休假或不可用，并且故障单阻止了需要部署的更新。

您也可以使用此程序将您自己的故障单重新分配给其他人。

开始之前

以下是接管通知单所需的权限：

- 管理员用户 - 您可以将通知单分配给自己或其他用户。
- 修改或查看通知单 + 系统 > 用户管理 > 用户（自定义角色）- 您可以将通知单分配给自己或其他用户。

但是，仅当用户具有与当前故障单所有者或管理员角色相同的角色时，才能分配用户。这可确保新用户具有配置故障单中当前修改的功能所需的权限。

您无法重新分配已提交审批的故障单。

过程

步骤 1 选择**系统 (⚙) > 更改管理流程**。

步骤 2 点击 **系统中故障单下的 全部**。

步骤 3 点击 **更多** (⋮) > **接管故障单**。

步骤 4 选择现在应拥有该故障单的用户。

用户列表仅限于具有编辑故障单中已更改策略所需权限的用户。例如，如果故障单包含对访问控制策略的更改，则用户列表仅包含允许修改访问控制策略的用户。

步骤 5 输入可选注释，然后点击 **接管**。

变更管理的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
接管故障单并为变更管理提供额外支持。	7.6.0	任意	您可以接管其他用户的故障单。如果故障单阻止了策略的其他更新，并且用户不可用，这将非常有用。此外，变更管理审批工作流程现在包括以下功能：解密策略、DNS 策略、文件和恶意软件策略、网络发现、证书和证书组、密码套件列表、可分辨名称对象、Sinkhole 对象。
变更管理。	7.4.1	任意	如果您的组织需要实施更加正式的配置变更流程，包括在部署变更之前进行审核跟踪和正式审批，则可以启用变更管理。 我们添加了**系统**（⚙）> **配置 (Configuration)** > **更改管理 (Change Management)** 页面来启用此功能。启用后，将在菜单中显示**系统**（⚙）> **更改管理工作流程 (Change Management Workflow)** 页面和新的**故障单**（📄）快速访问图标。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。