监控和报告

CDO 的监控和报告功能可帮助您深入了解现有策略的影响以及由此产生的安全状况。

变更日志

关于更改日志

更改日志 会持续捕获在 CDO 中进行的配置更改。此单一视图包括所有受支持设备和服务的更改。以下是更改日志的一些功能：

- 并排比较对设备配置所做的更改。
- 所有更改日志条目的纯英文标签。
- 记录设备的载入和删除。
- 检测在 CDO 之外发生的策略更改冲突。
- 回答事件调查或故障排除期间的人员、内容和时间。
- 可以将完整更改日志或仅一部分下载为 CSV 文件。

更改日志容量

CDO 会将更改日志中的信息保留一年。超过一年的信息将被删除。

CDO 在其数据库中存储的更改日志信息与导出更改日志时看到的信息之间存在差异。有关详细信息，请参阅将更改日志导出到 CSV 文件, on page 5。

“更改日志”(Change Log) 页面上的更改日志条目

更改日志条目反映对单个设备配置的更改、在设备上执行的操作，或者是否在CDO之外对设备进行了更改。

- 对于包含配置更改的更改日志条目，您可以通过点击行中的任意位置来展开更改。
- 对于在 CDO 之外进行的被检测为冲突的带外更改，**系统用户**将被报告为最后一个用户。
- 在CDO上的设备配置与设备上的配置同步后，或从CDO中删除设备时，CDO会关闭更改日志条目。将配置从设备“读取”到 CDO 或通过将配置从 CDO 部署到设备后，配置会同步。
- CDO在关闭现有条目后立即创建新的更改日志条目。其他配置更改将添加到打开的更改日志条目中。
- 显示针对设备的读取、部署和删除操作的事件。这些操作会关闭设备的更改日志。
- 一旦 CDO 与设备上的配置同步（通过读取或部署），或者当 CDO 不再管理设备时，更改日志就会关闭。
- 如果在 CDO 之外对设备进行了更改，则会在更改日志中写入“检测到冲突”的条目。

活动和已完成的更改日志条目

更改日志的状态为 **活动**或**已完成**。当您使用 CDO 更改设备的配置时，这些更改会记录在**活动**更改日志条目中。将配置从设备读取到CDO、将更改从CDO部署到设备、从CDO删除设备或运行更新运行配置文件的 CLI 命令都会完成活动更改日志，并为未来的更改创建新的更改日志。

下图显示的是 ASA 中的**活动**更改日志条目。请注意左侧时间戳旁边的空心圆圈。

在更改日志中查找条目

更改日志事件可搜索和过滤。使用搜索栏查找与关键字匹配的事件。使用过滤器 以查找符合您指定的所有条件的条目。您还可以通过过滤更改日志并将关键字添加到搜索字段来组合操作，以在过滤后的结果中查找条目。

ASA 更改日志详细信息

有关 ASA 更改日志条目的说明，请参阅以下文章：

部署到 ASA 后的更改日志条目

以下是对更改日志条目的说明。条目左上角带有复选标记的绿色圆圈表示更改日志已完成。更改日志会按从新到旧的顺序显示条目，并对条目内的更改进行排序。

如果点击更改日志条目行中的蓝色查看更改日志差异 链接，则会在运行配置文件的上下文中并排对比显示更改。

请参阅下面对不同更改的说明。

图中的数字	说明
1	这是 admin@example.com 在 2018 年 9 月 11 日上午 10:03:59 所做的更改。 **1.** 添加了“HR_network”对象。 **2.** 将初始网络地址 (10.10.11.0) 和子网掩码 (255.255.255.0) 添加到了 HR_network 对象。 **3.** 在“engineering_access”网络策略中添加了一条规则，拒绝“engineering”网络中的地“HR_network”
2	运行配置文件的校验和已由 ASA 重新计算并更改。旧值已被删除，而新值已被添加。

图中的数字	说明
3	ASA 会将对象移至运行配置文件中的其他位置，而不是 Defense Orchestrator 放置该对象的位 **Note** 您不会始终看到这种条目。
4	上次更新运行配置文件的记录。旧时间戳被删除，新时间戳被添加。此更改由 ASA 进行。
5	这些是由防御协调器送到 ASA 进行配置更改的命令。

从 ASA 读取更改后的更改日志条目

当 Cisco Defense Orchestrator (CDO) 在其管理的 ASA 上检测到更改时，它会打开一个更改日志条目并记录检测到配置冲突的时间。当 CDO 检测到冲突时，您可以看到以下更改日志条目：

如果您接受更改，或查看并接受更改，则该更改将添加到更改日志条目中，并且该条目已完成。

此条目显示检测到的冲突 (Conflict Detected) 更改以及阻止工程网络中的地址到达 HR_network 的规则的删除。更改日志条目还显示带有消息“已成功导入带外更改”的更改。如果管理员已选择拒绝带外更改，则更改日志将显示消息“已成功拒绝设备上的带外更改”以及被拒绝的内容。带外更改是指在不使用 CDO 的情况下直接在 ASA 设备上进行的更改。

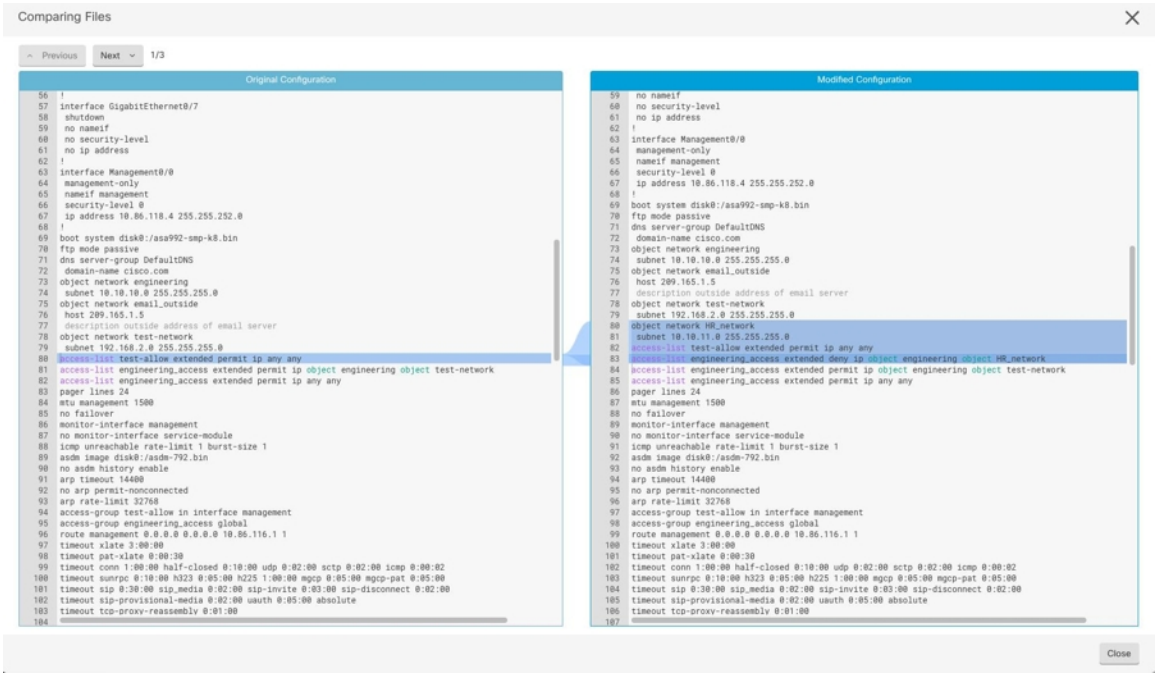
相关主题

- 变更日志, on page 1
- 部署到 ASA 后的更改日志条目, on page 3
- 查看更改日志差异, on page 5
- 读取、丢弃、检查和部署配置更改

查看更改日志差异

点击更改日志中的蓝色“差异”(Diff)链接，可以并排比较设备的运行配置文件中的更改。您会看到两个版本的差异。

在下图中，“原始配置”(Original Configuration) 是更改写入之前的运行配置文件，“修改后的配置”(Modified Configuration) 列显示更改写入 ASA 后的运行配置文件。在这种情况下，原始配置列会突出显示运行配置文件中实际未更改的行，但会在修改后的配置列中提供参考点。按照从左到右列的行，您会看到添加了 HR_network 对象和访问规则，以防止“工程”网络中的地址访问“HR_network”网络中的地址。点击**上一个 (Previous)** 和**下一个 (Next)** 按钮浏览文件中的更改。



相关主题

- 变更日志, on page 1

将更改日志导出到 CSV 文件

您可以将 CDO 更改日志的全部或子集导出到逗号分隔值 (.csv) 文件，以便您可以随意过滤和排序其中的信息。

要将更改日志导出到 .csv 文件，请执行以下程序：

步骤 1 在导航窗格中，点击 **更改日志**。

步骤 2 通过执行以下操作之一查找要导出的更改：

- 使用过滤器 字段和搜索字段准确查找要导出的内容。例如，按设备过滤以仅查看所选设备的更改。
- 清除更改日志中的所有过滤器和搜索条件。这允许您导出整个更改日志。

Note 请记住，CDO 会存储 1 年的更改日志数据。最好是过滤更改日志内容并将结果下载到 .csv 文件，而不是下载长达一年的更改日志历史记录。

步骤 3 点击更改日志右上角的蓝色导出按钮  。

步骤 4 为 .csv 文件指定一个描述性名称，并将文件保存到本地文件系统。

CDO 中的更改日志容量与导出的更改日志大小之间的差异

您从 CDO 的更改日志页面导出的信息与 CDO 存储在其数据库中的更改日志信息不同。

对于每个更改日志，CDO 会存储设备配置的两个副本，即“开始”配置和“结束”配置（如果更改日志已关闭）；或“当前”配置（如果是打开的更改日志）。这允许 CDO 并排显示配置差异。此外，CDO 会跟踪并存储每个步骤的“更改事件”，包括进行更改的用户名、更改时间以及其他详细信息。

但是，导出更改日志时，导出的内容不包括配置的两个完整副本。它仅包括“更改事件”，这使得导出文件比 CDO 存储的更改日志小得多。

CDO 最多可存储 1 年的更改日志信息，其中包括配置的两个副本。

更改请求管理

变更请求管理 允许您将在第三方故障单系统中打开的变更请求及其业务理由与变更日志中的事件相关联。使用更改请求管理在 CDO 中创建更改请求，使用唯一名称进行标识，输入更改说明，并将更改请求与更改日志事件相关联。您可以稍后在更改日志中搜索更改请求名称。

Note 您可能还会在 CDO 中看到对变更请求跟踪的引用。变更请求跟踪和变更请求管理指的是相同的功能。

启用更改请求管理

启用更改请求跟踪会影响租户的所有用户。要启用更改请求跟踪，请执行以下程序：

步骤 1 从用户菜单中，选择“设置”(Settings)。

步骤 2 从用户菜单中，点击常规设置。

步骤 3 点击“更改请求跟踪”下的滑块。

确认后，您会在 Defense Orchestrator 界面的左下角看到 Change Request 工具栏，并在 Change Log 中看到 Change Request 下拉菜单。

创建更改请求

步骤 1 在任何 CDO 页面中，点击页面左下角的更改请求工具栏中的蓝色 + 按钮。

步骤 2 为更改请求指定名称和说明。让变更请求名称反映您的组织想要实施的变更请求标识符。使用说明字段描述更改的目的。

Note 更改请求的名称一旦创建便无法更改。

步骤 3 保存更改请求。

Note CDO 保存更改请求并将所有新更改与该更改请求名称关联，直到您禁用更改请求或清除更改请求工具栏中的更改请求信息。

将更改请求与更改日志事件关联

步骤 1 在导航窗格中，点击**更改日志 (Change Log)**。

步骤 2 展开更改日志以显示要与更改请求关联的事件。

步骤 3 在“更改请求”列中，点击事件的下拉菜单。请注意，最新的更改请求列在更改请求列表的顶部。

步骤 4 点击更改请求的名称，然后点击选择。

使用更改请求搜索更改日志事件

步骤 1 在导航窗格中，点击**更改日志 (Change Log)**。

步骤 2 在更改日志搜索字段中，输入更改请求的确切名称，以便查找与该更改请求关联的更改日志事件。CDO 突出显示具有完全匹配项的更改日志事件。

搜索更改请求

步骤 1 点击更改请求工具栏中的更改请求菜单。

步骤 2 开始键入您要搜索的更改请求名称或关键字。您将开始在更改请求列表的名称字段和说明字段中看到部分匹配的结果。

过滤器更改请求

过滤器托盘中有一个“更改请求”过滤器，可用于查找更改日志事件。

步骤 1 在“更改日志”页面左侧的过滤器托盘中，找到“更改请求”区域。

步骤 2 展开过滤器并开始在搜索字段中键入更改请求的名称。部分匹配开始显示在搜索字段下方。

步骤 3 选择更改请求名称，选中相应的复选框，然后在“更改日志”表中显示匹配项。CDO 突出显示具有完全匹配项的更改日志事件。

清除更改请求工具栏

清除更改请求工具栏可防止更改日志事件与现有更改请求自动关联。

步骤 1 选择更改请求工具栏中的更改请求菜单。

步骤 2 点击**清除**。更改请求菜单更改为“无”。

清除与更改日志事件关联的更改请求

步骤 1 在导航窗格中，点击 **更改日志**。

步骤 2 展开更改日志以显示要与更改请求取消关联的事件。

步骤 3 在“更改请求”列中，点击事件的下拉菜单。

步骤 4 点击**清除**。

删除更改请求

删除更改请求时，是将其从更改请求列表中删除，而不是从更改日志中删除。

步骤 1 点击更改请求工具栏中的更改请求菜单。

步骤 2 点击更改请求名称。

步骤 3 点击该行中的删除图标。

步骤 4 点击绿色复选标记以确认您要删除更改请求。

禁用更改请求管理

禁用更改请求管理会影响您账户的所有用户。要禁用变更请求管理，请执行以下程序：

步骤 1 从用户名菜单中，选择设置。

步骤 2 滑动更改请求跟踪下的按钮以显示灰色 X。

使用案例

这些使用案例假定您之前已按照上述说明启用了变更请求管理。

跟踪为解决外部系统中维护的故障单所做的防火墙更改

在此使用案例中，用户正在更改防火墙以解决在外部系统中维护的故障单。用户希望将这些防火墙更改导致的更改日志事件与更改请求相关联。请按照以下程序创建更改请求，并将更改日志事件与其关联。

1. 创建更改请求, on page 7。使用外部系统中的故障单名称或编号作为更改请求的名称。使用说明字段添加更改理由或其他相关信息。
2. 确保新的更改请求在更改请求工具栏中可见。
3. 进行防火墙更改。
4. 在导航窗格中，点击更改日志并查找与新更改请求关联的更改日志事件。
5. 清除更改请求工具栏, on page 8 完成后。

更改防火墙后手动更新单个更改日志事件

在此使用案例中，用户进行了防火墙更改以解决在外部系统中维护的故障单，但忘记使用更改请求管理功能将更改请求与更改日志事件相关联。用户希望返回更改日志，以使用故障单编号更新更改日志事件。请按照以下程序将更改请求与更改日志事件相关联。

1. 创建更改请求, on page 7。使用外部系统中的故障单名称或编号作为更改请求的名称。使用说明字段添加更改理由或其他相关信息。
2. 在导航窗格中，点击更改日志并搜索与防火墙更改关联的更改日志事件。
3. 将更改请求与更改日志事件关联, on page 7。
4. 完成后，清除更改请求工具栏。

搜索与更改请求关联的更改日志事件

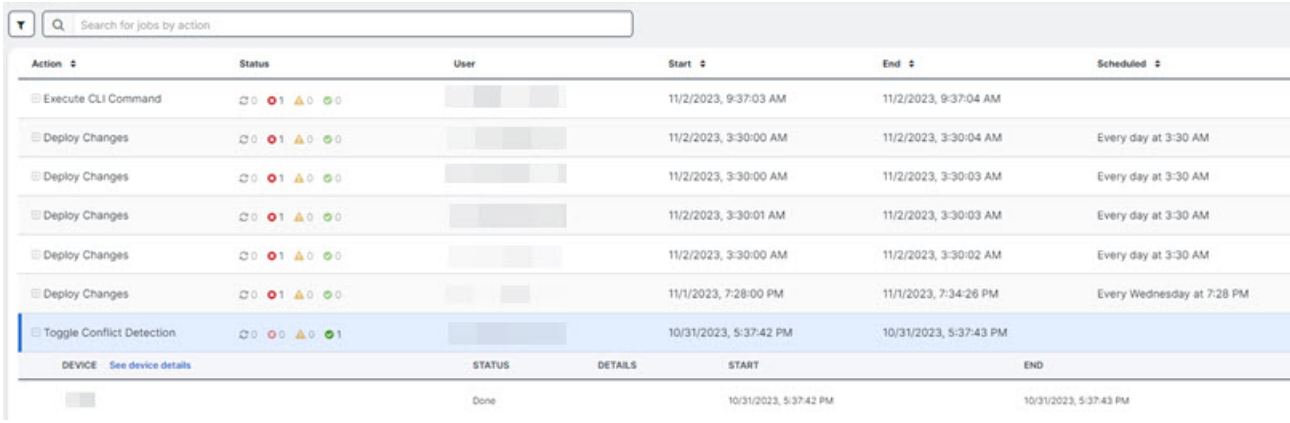
在此使用案例中，用户希望了解由于解决外部系统中维护的故障单而导致的更改日志中记录了哪些更改日志事件。请按照以下程序搜索与更改请求关联的更改日志事件：

1. 在导航窗格中，点击**更改日志 (Change Log)**。
2. 使用以下方法之一搜索与更改请求关联的更改日志事件。
   - 在更改日志搜索字段中，输入更改请求的确切名称，以便查找与该更改请求关联的更改日志事件。CDO 突出显示具有完全匹配项的更改日志事件。
   - 过滤器更改请求, on page 8 查找更改日志事件。
3. 查看每个更改日志，查找显示相关更改请求的突出显示的更改日志事件。

作业页面

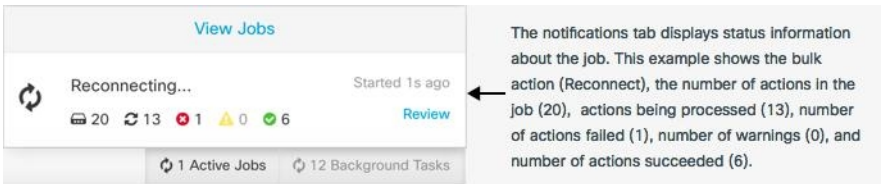
“作业”(Jobs)会页面显示有关批量操作状态的信息。批量操作可能是重新连接多个设备、从多个设备读取配置或同时升级多个设备。作业表中用颜色标记的行表示成功或失败的各个操作。

表中的一行代表一个批量操作。例如，该批量操作可能是尝试重新连接20台设备。展开“作业”(Jobs)页面中的一行，将显示受批量操作影响的每个设备的结果。



您可以通过两种不同的方式访问“作业”(Jobs) 页面：

- 在当通知选项卡有新作业中，点击通知行中的**查看 (Review)** 链接。您将被重定向到“作业”(Jobs)页面，并查看该通知所代表的特定作业。



- 从 CDO 的菜单中，选择**作业 (Jobs)**。此表显示了在 CDO 中执行的批量操作的完整列表。

搜索和过滤

进入“作业”(Jobs) 页面后，您可以按操作类型、执行这些操作的用户以及操作状态进行过滤和搜索。

重新启动导致操作失败的批量操作

查看“作业”(Jobs) 页面时，如果发现批量操作中的一个或多个操作失败，则可以在进行任何必要的更正后重新运行批量操作。CDO将仅对失败的操作重新运行作业。要重新运行批量操作，请执行以下操作：

步骤 1 选择作业页面中指示失败操作的行。

步骤 2 点击“作业”(Job) 行上的重新启动 **重试**图标。

取消批量操作

现在，您可以取消在多台设备上执行的任何活动批量操作。例如，假设您已尝试重新连接四台受管设备，其中三台设备已成功重新连接，但第四台设备既未成功重新连接，也无法重新连接。

要取消批量操作，请执行以下操作：

步骤 1 在 CDO 导航菜单上，点击作业。

步骤 2 找到仍在运行的批量操作，然后点击作业行右侧的取消链接。

如果批量操作的任何部分成功，这些操作将不会被撤销。任何仍在运行的操作都将被取消。

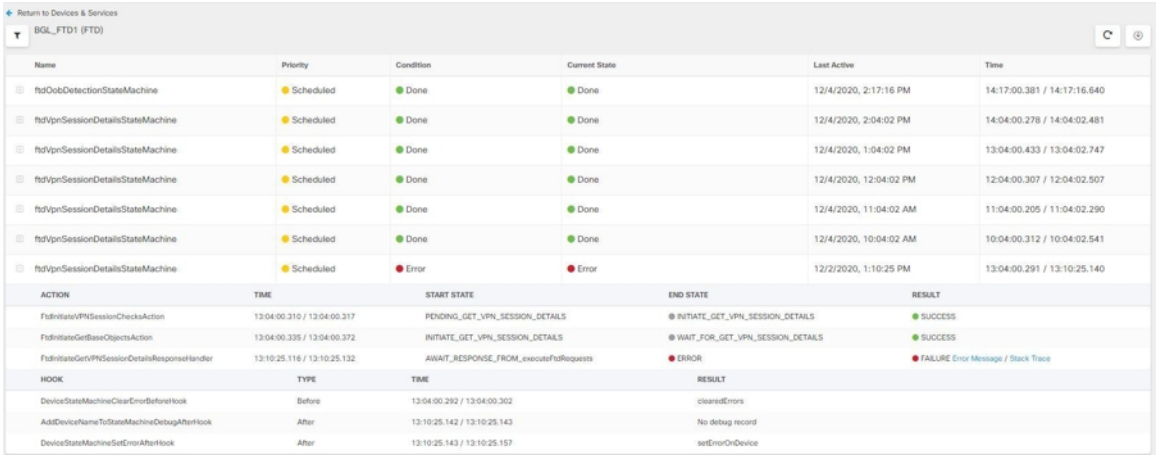
工作流程页面

通过“工作流程”(Workflow) 页面，您可以监控 CDO 在与设备、安全设备连接器 (SDC) 或安全事件连接器 (SEC) 通信时以及在对设备应用规则集更改时运行的每个进程。CDO 会在工作流程表中为每个步骤创建一个条目，并在此页面上显示其结果。该条目只会包含与 CDO 执行的操作相关的信息，而不是与其交互的设备相关的信息。

当 CDO 无法在设备上执行任务时，它会报告错误，您可以导航至“工作流程”(Workflows) 页面查看发生错误的步骤以了解更多详细信息。

您可以访问此页面来确定错误并进行故障排除，或者在 TAC 坚持时与他们共享信息。

要导航至“工作流程”(Workflows) 页面，请在**清单 (Inventory)** 页面上点击**设备 (Devices)** 选项卡。点击相应的设备类型选项卡，以便查找设备并选择所需的设备。在右侧窗格的**设备和操作 (Devices and Actions)** 中，点击**工作流程 (Workflows)**。下图显示了“工作流程”(Workflow) 页面，其中包含“工作流程”(Workflow) 表中的条目。



下载工作流程信息

您可以将完整的工作流程信息下载到 JSON 文件，并在 TAC 团队要求进行进一步分析时提供。要下载这些信息，您可以选择设备并导航至其工作流程页面，然后点击右上角显示的导出按钮 。

生成堆栈跟踪

如果您遇到无法解决的错误，TAC 可能会要求您提供堆栈跟踪的副本。要收集错误的堆栈跟踪，请点击**堆栈跟踪 (Stack Trace)** 链接，然后点击**复制堆栈跟踪 (Copy Stacktrace)**，以便将屏幕上显示的堆栈复制到剪贴板。

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。