Monitoring and Reporting Change Logs, Workflows, and Jobs

CDO effectively monitors configuration change logs, bulk device operations, and the process that runs when communicating with devices. This helps you understand how your network's existing policies influence its security posture.

Manage Change Logs in CDO

The Change Log captures configuration changes made in CDO, providing a single view that includes changes in all supported devices and services. These are some of the features of the change log:

- Side-by-side comparison of changes made to device configuration.
- Plain-English labels for all change log entries.
- Records on-boarding and removal of devices.
- Detection of policy change conflicts occurring outside of CDO.
- Answers who, what, and when during an incident investigation or troubleshooting.
- The full change log, or only a portion, can be downloaded as a CSV file.

Manage Change Log Capacity

CDO retains the change log information for one year and deletes data older than a year.

There is a difference between the change log information stored in CDO's database and what you see in an exported change log. See Export the Change Log, on page 4 for more information.

Change Log Entries

A change log entry reflects changes to a single device configuration, an action performed on a device, or if a change was made to the device outside of CDO.

- For change log entries that contain a change to configuration, you can expand the change by clicking anywhere in the row.
- For out-of-band changes made outside of CDO that are detected as a conflict, **System User** is reported as the Last User.
- CDO closes a change log entry after the device's configuration on CDO is synced with the configuration on the device or when a device is removed from CDO. Configurations are in sync after "reading" the configuration from the device to CDO or by deploying the configuration from CDO to the device.
- CDO creates a new change log entry immediately after closing an existing entry. Additional configuration changes are added to the open change log entry.
- Events are displayed for read, deploy, and delete actions against a device. These actions close a device's change log.
- A change log is closed once CDO is in sync with the configuration on the device (either by reading or deploying), or when CDO no longer manages the device.
- If a change is made to the device outside of CDO, a "conflict detected" entry is written to the change log.

Pending and Completed Change Log Entries

Change logs have a status of either **pending**or **completed**. As you make changes to a device's configuration using CDO, those changes are recorded in an **pending** change log entry. Reading a configuration from a device to CDO, deploying changes from CDO to a device, deleting a device from CDO completes, or running a CLI command that updates the running configuration file completes the pending change log and creates a new one for future changes.

Search and Filter Change Log Entries

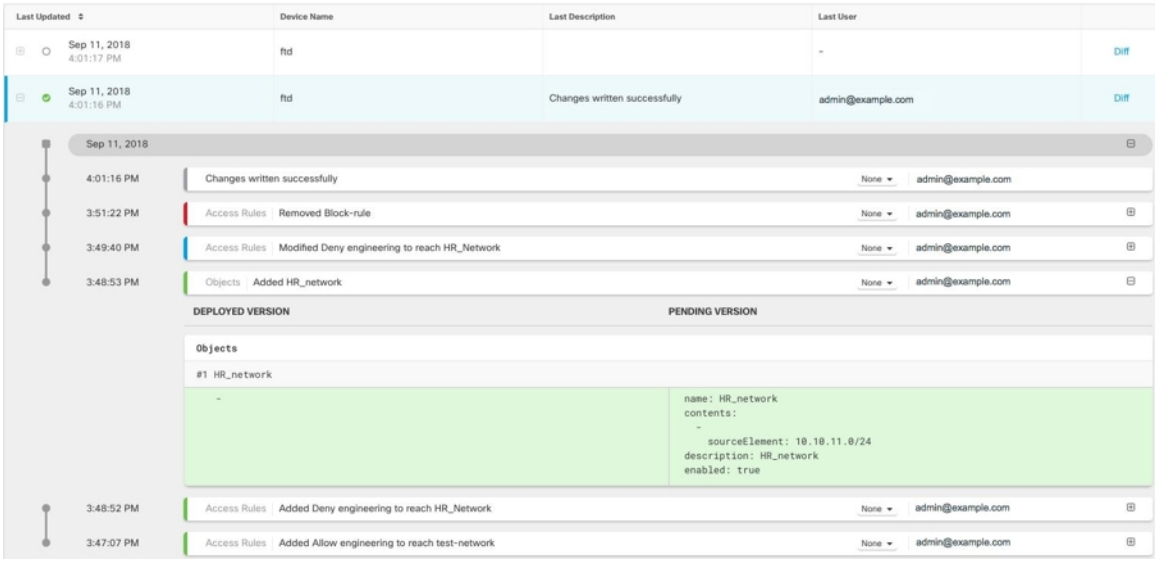
You can search and filter Change log entries. Use the search bar to find events that match your keywords. Use the filter to find the entries that meet all the criteria you specify. You can also combine the operations by filtering the change log and adding a keyword to the search field to find an entry within the filtered results.

Change Log Entries after Deploying to FDM-Managed Device

The changes in change log entries for FDM-managed devices are summarized in plain English. Clicking on a change in the change log entry expands it so you can see exactly what changed. After writing changes from CDO to your FDM-managed device, the change log entry is completed and Defense Orchestrator creates a new entry for future changes. Clicking the blue View Change Log Differences link in the change log entry row displays a side by side comparison of the changes in the context of the running configuration file.

Changes in red are deletions, changes in blue are modifications, changes in green are additions to the device configuration and changes in grey are messages.

Look at the expanded change for **Added HR_network** in the illustration below. This is the addition of the network object HR_network. The Deployed Version column is empty because there was no HR_network object on the device before the change. The Pending Version column shows that HR_network object was creatd with the value 10.10.11.0/24.



Change Log Entries after Reading Changes from an FDM-Managed Device

When CDO detects a change on a FDM-managed device, it registers a "Conflict Detected" state on the **Inventory** page in the Configuration Status column for the device. It does not record that Configuration Status in the change log.

When you accept configuration changes made outside of CDO, CDO creates a job and displays the job's processing status in the lower right corner of the interface. We do not recommend making additional until the job completes. If you do, the changes may be lost.

when the job successfully completes, click the "View Change Log Differences" link for the change log entry.

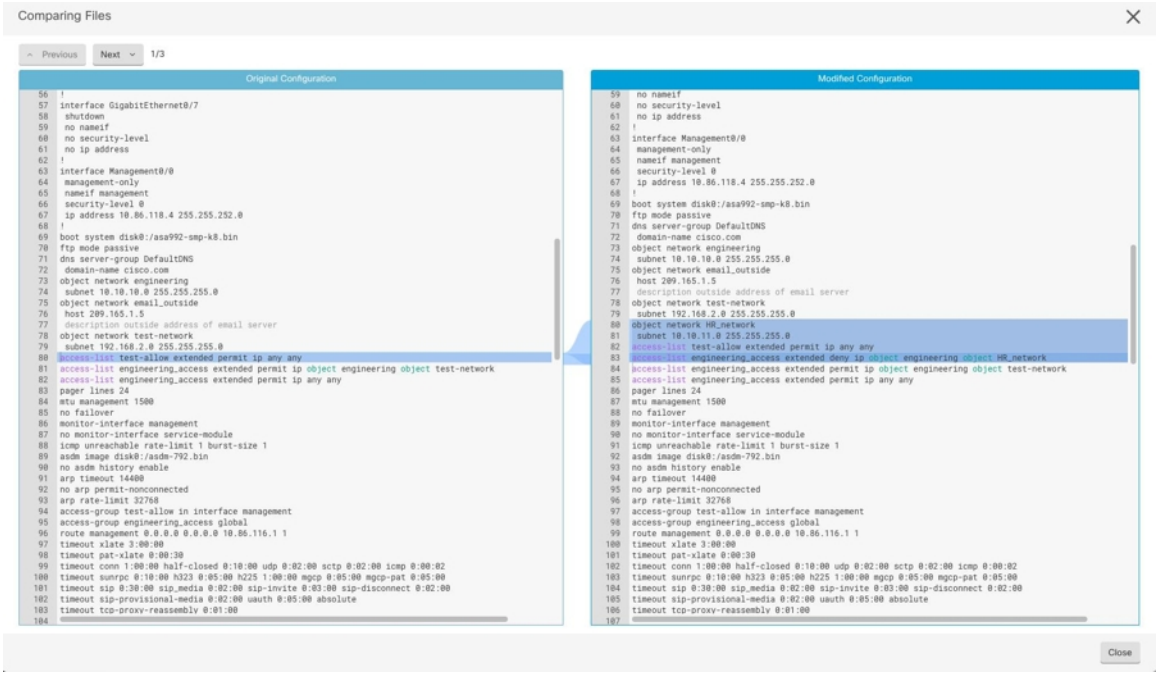
Related Information:

- About Device Configuration Changes

View Change Log Differences

Clicking the blue "Diff" link in the change log opens up a side-by-side comparison of the changes in the running configuration file of the device. You see the differences in the two versions.

In the illustration below, the "Original Configuration" is the running configuration file before a change was written to the ASA and the "Modified Configuration" column shows the running configuration file after the change was written. In this case, the Original Configuration column highlights a row in the running configuration file that actually didn't change but gives you a point of reference in the Modified Configuration column. Follow the lines across from the left to the right column and you see the addition of the HR_network object and the access rule preventing addresses in the "engineering" network to reach addresses in the "HR_network" network. Use the **Previous** and **Next** buttons to click through the changes in the file.



Related Topics

- Manage Change Logs in CDO, on page 1

Export the Change Log

You can export all or a subset of the CDO change log to a comma separated value (.csv) file so you can filter and sort the information in it however you like.

To export the change log to a .csv file, follow this procedure:

Procedure

Step 1 In the navigation pane, click **Change Log**.

Step 2 Find the changes you want to export by taking one of these actions:

- Use the filter field and the search field to find exactly what you want to export. For example, filter by device to see only the changes for your selected device or devices.
- Clear all the filters and search criteria in the change log. This allows you to export the entire change log.

Note Keep in mind, CDO stores 1 year of change log data. It may be better to filter the change log contents and download the results ot a .csv file rather than downloading up to a year of change log history.

Step 3 Click the blue export button in the top right of the change log .

Step 4 Give the .csv file a descriptive name and save the file to your local file system.

Differences Between the Change Log Capacity in CDO and the Size of an Exported Change Log

The information that you export from CDO's change log page is different from the change log information CDO stores in its database.

For every change log, CDO stores two copies of the device's configuration, the "starting" configuration and either the "ending" configuration in the case of a closed change log; or the "current" configuration, in the case of an open change log. This allows CDO to display configuration differences side by side. In addition, CDO tracks and stores every step "change event", with the username that made the change, the time the change was made, and other details.

When you export the change log, however, the export does not include the two complete copies of the configuration. It only includes the "change events," which makes the export file much smaller than the change log CDO stores.

CDO stores up to 1 year of change log information, this includes the two copies of the configuration.

Change Request Management

Change request management allows you to associate a change request and its business justification, opened in a third-party ticketing system, with an event in the Change Log. Use change request management to create a change request in CDO, identify it with a unique name, enter a description of the change, and associate the change request with change log events. You can later search the Change Log for the change request name.

Note You may also see references to Change Request Tracking in CDO. Change Request Tracking and Change Request Management refer to the same functionality.

Enable Change Request Management

Enabling change request tracking affects all users of your tenant. To enable Change Request Tracking, follow this procedure:

Procedure

Step 1 From the user menu, select Settings.

Step 2 From the user menu, click **General Settings**.

Step 3 Click the slider under "Change Request Tracking".

Once confirmed, you see the Change Request toolbar appear in the lower left corner of the Defense Orchestrator interface and the Change Request drop-down menu in the Change Log.

Create a Change Request

Procedure

Step 1 On any page within CDO, click the +on the change request toolbar at the lower-left side of the page.

Step 2 Enter a change request name and description. The change request name must reflect a change request identifier your organization wants to implement. Use the description field to describe the purpose of change.

Note You can't change the name of a change request once you create it.

Step 3 Save the change request.

Note CDO saves the change request and associates all new changes with that change request name until you disable change requests or clear the change request information in the change request toolbar.

Associate a Change Request with a Change Log Event

Procedure

Step 1 In the navigation pane, click **Change Log**.

Step 2 Expand the change log to show the events you want to associate with a change request.

Step 3 In the Change Request column, click the drop-down menu for the event. Note that the newest change requests are listed at the top of the change request list.

Step 4 Click the name of a change request and click **Select**.

Search for Change Log Events with Change Requests

Procedure

Step 1 From the navigation pane, choose **Change Log**.

Step 2 In the Change Log search field, enter the exact name of the change request to find the change log events associated with that change request. CDO highlights change log events with exact matches.

Search for a Change Request

Procedure

Step 1 Click the change request menu in the change request toolbar.

Step 2 Start entering the name of the change request or a relevant keyword in the search field. As you type, you see results that partially match your input, appearing in both the name and description fields within the list of change requests.

Filter Change Requests

Procedure

Step 1 From the navigation pane, choose **Change Log**.

Step 2 Click the filter icon to expand it, start typing the change request name in the search field. As you type, results that partially match your entry begin to appear.

Step 3 Select the change request and check the corresponding check box. The matches appear in the **Change Log** table. CDO highlights change log events with exact matches.

Clear the Change Request Toolbar

Clear the change request toolbar to prevent change log events from being automatically associated with an existing change request.

Procedure

Step 1 Select the change request menu in the change request toolbar.

Step 2 Click **Clear**. The change request menu changes to **None**.

Clear a Change Request Associated with a Change Log Event

Procedure

Step 1 From the navigation pane, choose **Change Log**.
Step 2 Expand the change log to view the events that you want to disassociate from change requests.
Step 3 Click the change request drop-down list for the event.
Step 4 Click **Clear**.

Delete a Change Request

When you delete a change request, you delete it from the change request list not from the change log.

Procedure

Step 1 Click the change request menu in the change request toolbar.
Step 2 Click the bin icon to delete a change request.
Step 3 Click the check mark to confirm.

Disable Change Request Management

Disabling change request management affects all users of your account. To disable Change Request Management, follow this procedure:

Procedure

Step 1 From the navigation pane, choose **Settings**.
Step 2 Disable the **Change Request Tracking** toggle button.

Change Request Management Use Cases

These use cases assume that you have previously enabled Change Request Management following the above instructions.

Track Firewall Changes Made to Resolve a Ticket Maintained in an External System

In this use case, you are making firewall changes to resolve a ticket maintained in an external system. You want to associate change log events resulting from those firewall changes with a change request. Follow this procedure to create a change request and associate change log events with it.

1. Create a Change Request, on page 6. Use the ticket name or number from the external system as the name of the change request. Use the description field to add the justification for the change or other relevant information.
2. Ensure that the new change request is visible in the change request toolbar.
3. Make the firewall changes.
4. In the navigation pane, choose **Change Log** and find change log events that are associated with your new change request.
5. Clear the Change Request Toolbar, on page 7 when done.

Manually Update Individual Change Log Events After Firewall Changes Are Made

In this use case, you made firewall changes to resolve a ticket that is maintained in an external system but forgot to use the change request management feature to associate change requests with the change log events. You want to update the change log events with the ticket number. Follow this procedure to associate change requests with change log events.

1. Create a Change Request, on page 6. Use the ticket name or number from the external system as the name of the change request. Use the description field to add the justification for the change or other relevant information.
2. In the navigation pane, choose **Change Log** and search for the change log events that are associated with the firewall changes.
3. Associate a Change Request with a Change Log Event, on page 6.
4. Clear the Change Request Toolbar, on page 7 when done.

Search for Change Log Events Associated with a Change Request

In this use case, your requirement is to find out what change log events were recorded in the Change Log due to the work that is done to resolve a ticket maintained in an external system. Follow this procedure to search for change log events that are associated with a change request:

1. In the navigation pane, choose **Change Log.**
2. Search for change log events that are associated with change requests using one of these methods.
   - In the Change Log search field, enter the exact name of the change request to find change log events associated with that change request. CDO highlights change log events with exact matches.
   - Filter Change Requests, on page 7 to find the change log events.
3. View each change log to find the highlighted change log events showing the associated change request.

FDM-Managed Device Executive Summary Report

The Executive Summary Report offers a collection of operational statistics for all FDM-managed devices. Once a device is onboarded, Cisco Defense Orchestrator may take up to two hours to collect this information from Firewall device manager; after the initial report generation, data is compiled hourly. Note that report information is not part of the request for events, so events and reports are not available at the same cadence.

Data in the reports is generated when network traffic triggers an access rule or policy on an FDM-managed device. We strongly recommend enabling malware defense and IPS licenses, as well as enabling file logging for access rules, to allow a device to generate the events that are reflected in the reports.

Note that all of the information displayed in the report is dependent on the **Time Range** toggle located at the top of the page. Policies may experience varying traffic or triggers during the time range you select.

If you experience issues with the Executive Summary Report, or see an unexpected amount of traffic, see Troubleshoot the Executive Summary Report for more information.

Generate Network Operation Data

Once a device is onboarded to CDO, event data is automatically collected. The data that is collected is dependent on the device configuration. The license that is delivered with all FDM-managed devices does not support all the options within the network operations report. We recommend the following configurations for devices you want to collect data from:

- **Logging** - enable file logging on applicable access control rules. See Logging Settings in an FDM Access Control Rule for more information.
- **Malware Events** - enable the malware smart license.
- **Security Intelligence** - enable the smart license.
- **IPS Threats** - enable the smart license.
- **Web Categories** - enable the URL smart license.
- **Files Detected** - enable the smart license.

See FDM-Managed Device Licensing Types for more information on smart licenses and the capabilities these licenses provide.

Note The executive summary does not inherently include traffic experienced over VPN.

Overview

The overview tab displays visuals from triggered rules, threats, and file types. These items are displayed numerically, with the largest or most frequently hit rules, events, or files listed first.

Malware events represent detected or blocked malware files only. Note that the disposition of a file can change, for example, from clean to malware or from malware to clean. We recommend that you Schedule a Security Database Update to keep your devices up to date with the latest intrusion rules (SRUs).

Top Ten Access Rule Hits offers three different tabs you can toggle between to view the top ten rule transfers, connections, or rules that blocked packets.

Network Assessment

The Network Assessment tab addresses web site categories and detected file types. This display captures only the top ten most frequently encountered categories and file types. Other than by the selected time range, you cannot use this tab to determine when a specific web category or file type was detected.

Threats

The Threats tab displays statistics generated by intrusion events: **Top Attacker** captures the originating IP address of an event, **Top Target** captures the destination IP address of an event, and **Top Threats** captures the type of events that have been categorized as a threat.

This tab also details the threats and malware types that were detected.

Generate a Report

Once you have configured the report to your preference, feel free to generate a PDF of the report. See Generating FDM-Managed Device Executive Summary Reports for more information.

Generating FDM-Managed Device Executive Summary Reports

CDO provides several reports that you can use to analyze the impact of your security policies on the traffic going through your FDM-managed devices. An executive summary report summarizes the most impactful malware, threats, and impacted security intelligence. CDO polls devices every hour to collect events. To learn more about what the executive summary offers, see FDM-Managed Device Executive Summary Report for more information.

Important The FDM-managed device reports are available only on the FDM-managed device that is currently onboarded to your tenant. These reports are generated hourly and are not part of the request for events, so events and reports are not available at the same cadence. After initially onboarding your FDM-managed device, CDO may take up to two hours to generate reports. Until there are reports to display, the **Reports** tab under the **Monitoring** option may not be visible.

If you are a Security Analytics and Logging subscriber, Network Reports do not reflect the events forwarded to the Secure Event Connector (SEC).

Note The data used in traffic-related reports is collected from events triggered by the access control rules, and other security policies. The generated report does not reflect traffic for rules where logging is not enabled, or rules that have not been triggered. Ensure that you configure your rules with the information that matters to you.

Use the following procedure to generate an Executive Summary Report:

Procedure

Step 1 In the navigation pane, click **Monitoring > Executive Summary Report**.

Step 2 Select the time range for the reports: **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, or **Last 90 Days**.

Step 3 (Optional) Click the filter icon to generate a report on a custom list of devices.

Step 4 Click **Generate Report (PDF)**.

Step 5 Click **Save** to save the report as a PDF. Browse for the save location and click **Save**. If you decide not to save the report, click **Cancel** at any time.

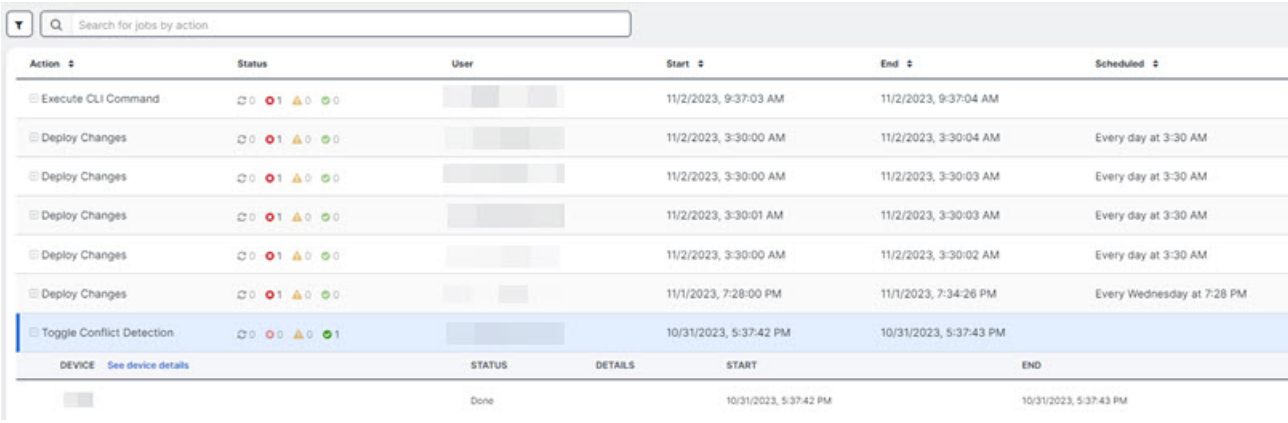
Related Information:

- FDM-Managed Device Executive Summary Report
- Troubleshoot the Executive Summary Report

Monitor Jobs in CDO

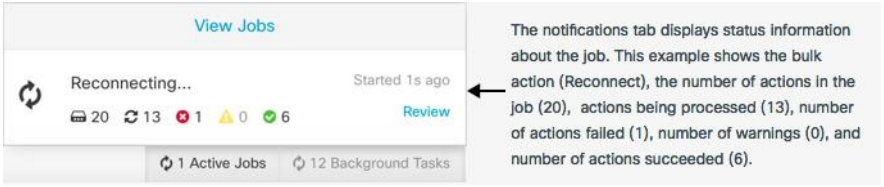
The Jobs page provides an overview of the progress of bulk operations, such as reconnecting multiple devices, reading configurations from multiple devices, or upgrading multiple devices simultaneously. The Jobs table uses color-coded rows to indicate the status of individual actions, whether they have succeeded or failed.

One row in the table represents a single bulk operation. That one bulk operation may have been, for example, an attempt to reconnect 20 devices. Expanding a row in the Jobs page displays the results for each of the devices affected by the bulk operation.



You can reach the Jobs page two different ways:

- In the notifications tab when there is new Jobs notification, click the **Review** link. You will be redirected to the Jobs page and see the specific job represented by the notification.



- From CDO's menu, select **Jobs**. This table shows a complete list of the bulk actions performed in CDO.

Search Jobs in CDO

When you're on the Jobs page, you can filter and search by different actions, the users who performed them, and the action status.

Reinitiate a Bulk Action

After reviewing the **Jobs** page, if one or more actions in a bulk action fail, you can retry the bulk action after making necessary corrections. CDO will re-run the job only for the failed actions. To re-run a bulk action:

Procedure

Step 1 Select the row in the jobs page that indicates a failed action.

Step 2 Click **Retry**.

Cancel a Bulk Action

You now have the ability to cancel any bulk actions that are currently in progress on multiple devices. For example, if you have tried to reconnect four managed devices and three of them have successfully reconnected, but the fourth device is still neither connected nor disconnected, you can cancel the bulk action.

To cancel a bulk action:

Procedure

Step 1 On the CDO navigation menu, click **Jobs**.

Step 2 Identify the running bulk action and click the **Cancel** link on the right side.

If any part of the bulk action is successful, it cannot be undone. Any ongoing action will be cancelled.

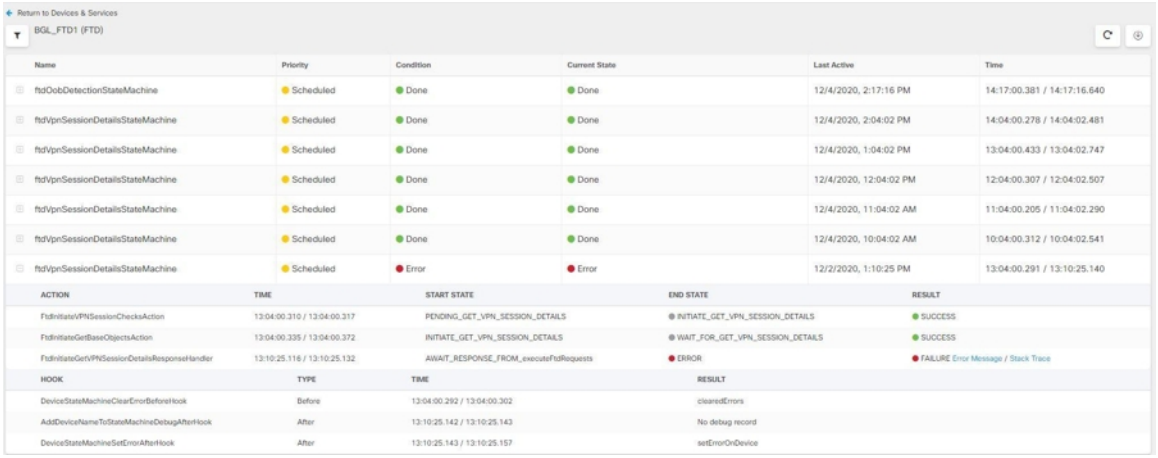
Monitor Workflows in CDO

The Workflow page allows you to monitor every process that CDO runs when communicating with devices, Secure Device Connector (SDC), or Secure Event Connector (SEC), and when applying ruleset changes to devices. CDO creates an entry in the workflow table for every step and displays its outcome on this page. The entry contains information pertaining only to the action performed by CDO and not the device it is interacting with.

CDO reports an error when it fails to perform a task on a device, and you can navigate to the Workflows page to see the step where the error occurred for more details.

You can visit this page to determine and troubleshoot errors or share information with TAC when they insist.

To navigate to the Workflows page, on the **Inventory** page, click the **Devices** tab. Click the appropriate device type tab to locate the device and select the device you want. In the **Devices and Actions** in the right pane, click **Workflows**. The following picture shows the Workflow page with entries in the Workflow table.



Export Device Workflows

You can download the complete workflow information to a JSON file and provide it when the TAC team asks for further analysis. To export this information, you can select the device and navigate to its Workflows page and click the export button appearing on the top right corner.

Copy Stack Trace

If you have an error you cannot resolve, TAC may ask you for a copy of the stack trace. To collect the stack trace for the error, click the **Stack Trace** link and click **Copy Stacktrace** to copy the stacks appearing on the screen to a clipboard.