Feature Highlights of 2021

This article describes some of the features that were added to Cisco Defense Orchestrator in 2021.

- December 2021, on page 1
- November 2021, on page 2
- October 2021, on page 2
- September 2021, on page 3
- August 2021, on page 4
- July 2021, on page 4
- June 2021, on page 6
- May 2021, on page 8
- March 2021, on page 8
- February 2021, on page 9
- January 2021, on page 10

December 2021

December 9, 2021

CDO Support for Firepower Threat Defense, Version 7.1

CDO now supports Firepower Threat Defense (FTD), version 7.1 devices. These are the aspects of support CDO provides:

- Onboard a supported physical or virtual device running Firepower Threat Defense version 7.1.
- Upgrade from Firepower Threat Defense versions 6.4+ to version 7.1.
- Support for existing Firepower Threat Defense features.

These caveats apply to Firepower Threat Defense, version 7.1 support:

- CDO currently does not support backing up Firepower Threat Defense devices running version 7.1. Support for this functionality is planned for the first maintenance release of Firepower Threat Defense, version 7.1.
- CDO does not support features introduced in the Firepower Threat Defense, version 7.1 release.

For more information about the FTD features CDO currently supports, see *Managing FTD with Cisco Defense Orchestrator*.

New CDO Documentation Platform

Online Help

- Content describing all your devices in a single place.
- Context-sensitivity.
- Content matches found as you search.
- Search results highlighted in a table of contents puts information in a larger context.

Content Maintained on Cisco.com

- Availability on Cisco.com places all your Cisco documentation on one site.
- Device-specific configuration guides makes finding information easier.
- What's New for Cisco Defense Orchestrator continues to describe the latest features available in CDO.

November 2021

November 11, 2021

New SASE Tunnel Functionality

You can now edit SASE tunnels that have been read into or created through the CDO UI. Note that this function only supports tunnels between an Umbrella organization and an ASA peer device that is already onboarded to CDO.

For more information see "Edit a SASE Tunnel" in *Managing an ASA with Cisco Defense Orchestrator* for more information.

October 2021

October 21, 2021

Improved SecureX Integration

For users who have not already linked SecureX with their CDO tenant, CDO now offers a streamlined integration with SecureX. This process allows you to quickly and securely connect your CDO tenant to your SecureX Organization and add a CDO module to the SecureX dashboard with a single click. If you do not have a SecureX Organization, you can create one during this process.

For more information, see "Integrating CDO with SecureX" in *Managing FTD with Cisco Defense Orchestrator*.

Upload an AnyConnect Package from CDO Repository

CDO now supports uploading the AnyConnect package to ASA and FTD devices from the CDO repository.

The Remote Access VPN Configuration wizard presents AnyConnect packages per operating system, which you can select and upload to a device.

For more information, see "Upload an AnyConnect Package from CDO Repository" in *Managing FTD with Cisco Defense Orchestrator* and "Manage AnyConnect Software Packages on ASA Devices" in *Managing ASA with Cisco Defense Orchestrator*.

September 2021

September 16, 2021

CDO Notifications with Service Integrations

CDO notifications now integrate with webhooks. The notifications selected in the Notification Settings page will be sent to the application or service integration of your choice.

For more information, see "Enable Service Integrations for CDO Notifications" in *Managing FTD with Cisco Defense Orchestrator*.

Cisco Secure Firewall Cloud Native Support for Cisco Security Analytics and Logging

Cisco Security Analytics and Logging has been greatly expanded to support logging events from Secure Firewall Cloud Native.

Secure Firewall Cloud Native logging: Security Analytics and Logging (SAL SaaS) now supports logging from any Secure Firewall Cloud Native device. Users can choose to store Secure Firewall Cloud Native events in syslog format, NetFlow Security Event Logs (NSEL) format, or both in the Cisco Cloud and use Cisco Secure Cloud Analytics to analyze them. Customers that want to enable logging analytics will be required to enable NSEL logs to provide the necessary telemetry for the higher-tier SAL licenses.

- Traffic Analysis—Secure Firewall Cloud Native logs can be run through SAL's traffic analysis and observations and alerts can be reviewed by cross-launching Cisco Secure Cloud Analytics from CDO. Cloud Native customers only logging syslog events must switch to NSEL logs to enable traffic analytics.
- Logging Analytics and Detection and Total Network Analytics Detection—Customers acquiring Logging Analytics and Detection and Total Network Analytics Detection licenses can provision and use a Secure Cloud Analytics portal for analysis. Secure Cloud Analytics detections include observations and alerts specifically enabled using firewall logging data, in addition to the other detections available to SAL users as part of Secure Cloud Analytics core capability. Existing Logging and Troubleshooting license holders can test the detection capabilities of higher licenses with no commitment for 30 days.
- Free Trials—You can start a no-commitment 30-day SAL trial for all licenses by filling out this form. This trial requires only a minimal set of on-premises connectors for exporting data to the cloud. You can use this trial to evaluate SAL capabilities, and estimate the data volume required to support production environments, as a precursor to purchasing the appropriate daily volume for SAL licenses. To this end, the SAL trial will not throttle data for most user volumes. In addition, an estimator tool helps you estimate SAL daily volume.

For information, see "Cisco Security Analytics and Logging" in *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*.

August 2021

August 26, 2021

CDO and Umbrella Integration

CDO now supports Umbrella integration. You can onboard Umbrella organizations and view, manage, and create SASE tunnels that exist between Umbrella and ASA devices. ASA devices utilize Umbrella's SIG tunnel and inspection which provides centralized management for easy-to-use security.

When you onboard an Umbrella organization, we recommend onboarding the ASA devices associated with that organization as well.

For more information about what Umbrella is and how CDO communicates with it, see *Managing ASA with Cisco Defense Orchestrator*.

August 13, 2021

Duo Configuration Support using LDAP for FTD RA VPN

You can now configure Duo two-factor authentication using LDAP for an FTD Remote Access VPN connection.

Use the Duo LDAP server as the secondary authentication source along with a Microsoft Active Directory (AD) or RADIUS server as the primary authentication source. With Duo LDAP, the secondary authentication validates the primary authentication with a Duo passcode, push notification, phone call, or SMS.

For more information, see "Duo Two-Factor Authentication using LDAP" in *Managing FTD with Cisco Defense Orchestrator*.

July 2021

July 08, 2021

Digital Certificate Management Support for ASA

CDO now manages digital certificates on ASA devices. You can add a digital certificate such as identity certificates and trusted CA certificates as trustpoint objects and install them on one or more managed ASA devices. You can also export an installed identity certificate to duplicate a trustpoint configuration on a different ASA manually.

You can upload or create an identity certificate in the following formats:

- PKCS12 file with a passphrase
- Self-signed certificate

- Certificate Signing Request (CSR) signed by a certificate authority

The Remote Access VPN uses digital certificates for authenticating ASA and AnyConnect clients to establish a secure VPN connection.

For more information, see "ASA Certificate Management" in *Managing ASA with Cisco Defense Orchestrator*.

AnyConnect Module Support for RA VPN ASA and FTD

CDO now supports managing AnyConnect modules on ASA and FTD devices.

Note This feature is supported on FTD running software version 6.7 or later versions.

As part of your RA VPN group policy creation, you can now configure a variety of optional modules to be downloaded and installed when a user downloads the Cisco AnyConnect VPN client. These modules can provide services such as web security, malware protection, off-network roaming protection, and so on.

You can associate each module with a profile containing your custom configurations, created in the AnyConnect Profile Editor and uploaded to the CDO as an AnyConnect File object.

For more information on how to upload the profiles and assign them to group policies, see "Upload RA VPN AnyConnect Client Profile" and "Create New FTD RA VPN Group Policies" in *Managing FTD with Cisco Defense Orchestrator*.

July 01, 2021

Snort 3 Support

CDO now supports the Snort 3 processing engine for FTD devices running Version 6.7 and later. The Snort engine automatically updates new snort rules to keep your device compliant with the latest vulnerabilities. You can perform a standalone upgrade from Snort 2 to Snort 3 or upgrade the device system and the Snort engine simultaneously for an abridged upgrade experience.

For more information, see "Upgrade to Snort 3.0" in *Managing FTD with Cisco Defense Orchestrator*.

Custom Intrusion Prevention System Policy

CDO now supports Snort 3 and customized Intrusion Prevention System (IPS) policies for FTD devices running Version 6.7 and later. The improved Snort 3 processing engine allows you to create and customize IPS policies using rules provided by the Cisco Talos Intelligence Group (Talos). The best practice is to create your own policy based on the provided Talos policy templates and change that if you need to adjust rule actions.

Note Be aware of the differences and limitations when you upgrade to or from Snort 3, as the upgrade may change how your rules are configured.

For more information, see "Custom Firepower Intrusion Prevention System Policy" in *Managing FTD with Cisco Defense Orchestrator*.

June 2021

June 17, 2021

CDO Support for Firepower Threat Defense, Version 7.0

CDO now supports Firepower Threat Defense (FTD), 7.0. You can onboard an FTD device running FTD 7.0, or use CDO to upgrade the device to that version. CDO continues to support existing FTD features in addition to the new Reputation Enforcement on DNS Traffic feature. This feature is an access control policy setting. Enable this option to apply your URL filtering category and reputation rules to DNS lookup requests.

For more information, see "Configuring Access Policy Settings" in *Managing FTD with Cisco Defense Orchestrator*.

CDO has limited support for these features:

- FTDv Tiered License Support—Version 7.0 supports performance-tiered Smart Licensing for FTDv devices based on throughput requirements and RA VPN session limits. CDO does not fully support tiered smart licensing at this time. You can onboard an FTDv device that uses a tiered license but you cannot update the license using CDO. Use the device's Firepower Device Manager to install and manage licenses on the FTDv.

  For more information, see "FTD Licensing" in *Managing FTD with Cisco Defense Orchestrator*.

- Scan Interface Support—If an interface is added to a Firepower device by using the Firepower eXtensible Operating System (FXOS) Chassis Manager, on the Firepower 4100 series or 9300 series devices, you will need to configure that interface on FDM and then have CDO "check for changes" to the device to read in the configuration.

  For more information, see "Synchronizing Interfaces Added to a Firepower Device using FXOS" in *Managing FTD with Cisco Defense Orchestrator*

- Virtual Router Support—VRF routes are not seen in CDO. You can onboard a device with virtual route support but you will not be able to see the virtual route in CDO's static routing page.

  For more information, see "About Virtual Routing and Forwarding" in *Managing FTD with Cisco Defense Orchestrator*

- Equal Cost Multi Path Routing (ECMP)—CDO can onboard a device that uses ECMP and read the configuration but doesn't allow you to modify them. You can create and change the ECMP configuration through FDM and then read it into CDO.

- Rulesets—You cannot apply rulesets to an FTD 7.0 device.

Note For information about the FTD features that CDO currently supports, see Managing FTD with Cisco Defense Orchestrator.

June 10, 2021

Cisco Secure Firewall Cloud Native Support

CDO now supports Cisco Secure Firewall Cloud Native. The Cisco Secure Firewall Cloud Native seamlessly extends Cisco's industry-leading security to a cloud-native form factor (CNFW) using Kubernetes (K8s) orchestration to achieve scalability and manageability. Amazon Elastic Kubernetes Service (Amazon EKS) gives you the flexibility to start, run, and scale Kubernetes applications in the AWS cloud. Amazon EKS helps you provide highly-available and secure clusters and automates key tasks such as patching, node provisioning, and updates.

CDO allows onboarding of this firewall and provides complete firewall management:

- View real-time and historical data from AnyConnect RA VPN sessions.
- Create and manage objects and use them in different policies that handle ingress and egress traffic in your network.
- Recognizes and reconciles changes made to the firewall outside of CDO, using the Kubernetes command-line tool.

For more information, see *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*.

You can also read *Cisco Secure Firewall Cloud Native At-a-Glance* for additional information.

Enhanced Remote Access VPN Monitoring

In addition to monitoring the live AnyConnect Remote Access VPN session, CDO now allows monitoring the historical data from AnyConnect Remote Access VPN sessions recorded over the last three months.

You can monitor VPN sessions across all Adaptive Security Appliance (ASA), Firepower Threat Defense (FTD), and Cisco Secure Firewall Cloud Native (SFCN) VPN head-ends in your tenant.

These are some of the salient enhancements made to the current release:

- Displays intuitive graphical visuals to provide at-a-glance views from all active VPN head-ends managed by CDO.
- The live session screen shows the most used operating system and VPN connection profile in the CDO tenant. It also shows the average session duration and data uploaded and downloaded.
- The historical session screen plots a bar graph to show data recorded for all devices in the last 24 hours, 7 days, and 30 days.
- Provides new filtering capabilities to narrow down your search based on criteria such as device type, session length, and upload and download data range.

Open the Remote Access VPN Monitoring screen from the navigation bar by clicking **VPN** > **Remote Access VPN Monitoring**.

New User Role

CDO now provides a new user role, the VPN Sessions Manager user role, that allows specific users the ability to terminate VPN sessions per tenant. Note that terminating VPN sessions is the only action this role allows; users designated with this role are otherwise limited with read-only capabilities.

May 2021

May 27, 2021

Improved Device Notifications in CDO

You can now subscribe to CDO email alerts and view recent notifications within the CDO UI.

Receive email alerts for when a device associated with your tenant experiences a wokflow or event change. Workflow changes include deployments, upgrades, or backups; event changes include devices going online or offline, conflict detection, HA or failover state, and site-to-site VPN connection status.

Note These customizable notifications and alerts are applied to all devices associated with your tenant and are not device-specific.

For more information, see "Notifcations Settings" in *Managing FTD with Cisco Defense Orchestrator*.

March 2021

March 25, 2021

Cisco Security Analytics and Logging Availability in APJC

Cisco Security Analytics and Logging is now available in the Asia (APJC) region through the newly commissioned Tokyo data store. Security Analytics-enabled accounts will have access to the Cisco Secure Cloud Analytics service in Sydney, Austraila for security-related alerting. With this, the Asia region has been brought up to par with capabilities available in the Americas and EU regions.

For more information, see "Cisco Security Analytics and Logging" at *Managing Cisco Secure Firewall Cloud Native with Cisco Defense Orchestrator*

March 18, 2021

EtherChannel Interface Support

CDO now supports EtherChannel interface configuration on supported models running Firepower Version 6.5 and later, such as the Firepower 1010, 1120,1140,1150, 2110, 2120, 2130, 2140. EtherChannel is a port link aggregation technology or port-channel architecture that allows the grouping of several physical Ethernet links to create one logical Ethernet link for the purpose of providing links between switches, routers and servers.

Note that the configuration that you apply to the physical ports affects only the LAN port where you apply the configuration.

For more information about device support and configuration limitations, see "Guidelines and Limitations for Firepower Interface Configuration" in *Managing FTD with Cisco Defense Orchestrator*.

March 15, 2021

ASA Remote Access VPN Support

CDO now allows creating Remote Access Virtual Private Network (RA VPN) configuration on Adaptive Security Appliance (ASA) devices to enable remote users to connect to the ASA and securely access the remote network. It also allows managing the RA VPN settings that have already been configured using other ASA management tools, such as the Adaptive Security Defense Manager (ASDM) or Cisco Security Manager (CSM).

AnyConnect is the only client that is supported on endpoint devices for RA VPN connectivity.

CDO supports the following aspects of RA VPN functionality on ASA devices:

- SSL client-based remote access
- IPv4 and IPv6 addressing
- Shared RA VPN configuration across multiple ASA devices

For more information, see "Configuring Remote Access VPN for an ASA" in *Managing ASA with Cisco Defense Orchestrator*.

ASA File Management Support

CDO provides the File Management tool for performing basic file management tasks such as viewing, uploading, or deleting files present on the ASA device's flash (disk0) space. Using this tool, you can upload any files such as the AnyConnect software images, DAP.xml, data.xml, host scan image files to a single or multiple ASA device using URL-based file upload from the remote server.

This tool helps you to upload the newly released AnyConnect image to multiple ASA devices simultaneously.

For more information, see "ASA File Management" in *Managing ASA with Cisco Defense Orchestrator*.

February 2021

February 11, 2021

Multiple Secure Device Connector Support

You can now deploy more than one on-premises Secure Device Connector (SDC) for your tenant. This allows you to manage more devices with CDO and maintain communication performance between CDO, your SDCs, and your managed devices.

You can move managed ASA, AWS VPC, and Meraki MX devices from one SDC to another.

Having multiple SDCs also allows you to use one CDO tenant to manage devices in isolated network segments. Do this by assigning all managed devices in the isolated network segment to a single SDC.

For more information, see "Using Multiple SDCs on a Single CDO Tenant" in *Managing ASA with Cisco Defense Orchestrator*.

January 2021

January 21, 2021

FMC Object Reading

Now when you onboard an FMC to CDO, CDO imports the objects from the FMC-managed FTD devices. Once imported to CDO, the objects are read-only. Though the FMC objects are read-only, CDO allows you to apply a copy of the objects to other devices on your tenant that are not managed by the FMC. The copy is disassociated from the original object so you can edit the copy without changing the value of the object that was imported from the FMC. FMC objects can be used on any device you manage that support that object type.

For more information, see "FMC Objects" in Managing FMC with Cisco Defense Orchestrator

January 14, 2021

Exporting CLI Command Results

You can export the results of CLI commands issued to a standalone device, or several devices, to a comma separated value (.csv) file so you can filter and sort the information in it however you like. You can export the CLI results of a single device, or many devices at once.

For more information, see "Export CLI Command Results" in *Managing FTD with Cisco Defense Orchestrator*.

Configuring Cloud Services for your FTD Devices

Connecting to the Cisco Success Network and configuring which events are sent to the Cisco cloud are features that can be configured on FTD devices running software version 6.6 or higher.

Cisco Success Network

By enabling Cisco Success Network, you are providing usage information and statistics to Cisco to improve the FTD and to make you aware of unused or additional features that will help you maximize the value of Cisco products in your network. When you enable the Cisco Success Network, your device establishes a secure connection to the Cisco Cloud and maintains this secure connection at all times.

For more information, see "Connecting to the Cisco Success Network" in *Managing FTD with Cisco Defense Orchestrator*.

Send Events Directly to Cisco Cloud

You can now specify which types of events you send from your FTD directly to the Cisco cloud. Once stored in the Cisco cloud, you can use cloud applications, such as Cisco Threat Response, to analyze the events and to evaluate threats that the device might have encountered.

For more information, see "Sending Events to the Cisco Cloud" in *Managing FTD with Cisco Defense Orchestrator*.

Web Analytics

Enabling web analytics provides anonymous product usage information to Cisco based on page hits. The information includes pages viewed, the time spent on a page, browser versions, product version, device hostname, and so forth. This information can help Cisco determine feature usage patterns and improve the product. All usage data is anonymous and no sensitive data is transmitted. You can use CDO to configure this feature on all versions of FTD.

For more information, see "Enabling or Disabling Web Analytics" in *Managing FTD with Cisco Defense Orchestrator*.

January 7, 2021

FTD HA Pair Onboarding

CDO has enhanced the process of onboarding an FTD HA pair. Once you onboard one of the HA peers with either the registration token method or the login credentials method, CDO automatically detects that the corresponding peer is not onboarded yet and prompts you to take action. The improvement minimizes the effort required to onboard both devices, shortens how long it takes to onboard the peer device, and reuses any registration keys or smart license tokens you may have used to onboard the first device.

You can onboard either the active or the standby device, and once synced, CDO will always detect that the device is part of an HA pair.

Note We strongly recommend onboarding your FTD devices using the registration key method.

For more information on FTD HA Pair Onboarding, see "Onboard an FTD HA Pair with a Registration Key" or "Onboard an FTD HA Pair using Username Password and IP Address"in *Managing FTD with Cisco Defense Orchestrator*.