Feature Highlights of 2018

November 2018

November 22, 2018

Auto-Accept Out-of-Band Changes

You can now make configuration changes directly on your managed devices and set Defense Orchestrator to accept them automatically when it detects them. You will not have to monitor Defense Orchestrator and accept out-of-band changes manually.

For more information, see "Automatically Accept Out-of-Band Changes from your Device" in *Managing ASA with Cisco Defense Orchestrator*.

November 8, 2018

System Objects Filter

The system object filter lets you see the objects in the object table that are most important to you.

Some devices come with pre-defined objects for common services. These system objects are convenient because they are already made for you and you can use them in your rules and policies. There can be many system objects in the objects table. System objects cannot be edited or deleted.

Show System Objects is "off" by default. To display system objects in the object table, check Show System Objects in the filter bar. To hide system objects in the object table, leave Show System Objects unchecked in the filter bar.

For more information, see "Object Filters" in *Managing ASA with Cisco Defense Orchestrator*.

September 2018

September 20, 2018

Improvements to Policy Exports

When you export an ASA policy with a specified time range, the time range object name is now included in the .CSV file. This gives you a better sense of when rules in the policy are active.

Improvements to CLI Handling

Defense Orchestrator no longer trims trailing spaces on ASA CLI commands it executes.

Documentation Updates

ASA change log and "Diff" documentation added to give you a clear understanding of the contents of a change log entry and the "Diff" page. See before-and-after side-by-side comparisons of configuration changes. For more information, see "Change Log" in *Managing ASA with Cisco Defense Orchestrator*.

September 13, 2018

Export Only The Change Log Entries You Are Interested In

Previously you could only export the entire Defense Orchestrator's change log. Now you can apply filter and search criteria to the change log and export only the entries you are interested in.

For more information, see "Exporting the Change Log to a CSV file" in *Managing FTD with Cisco Defense Orchestrator*.

September 6, 2018

New Super Admin Role Can Create New User Records and Change User Roles

Defense Orchestrator added support for the Super Admin role. This new role has all of the permissions of the Admin role and has additional permissions of being able to manage user records. The Defense Orchestrator support team can upgrade your existing Admin accounts to Super Admins. Having a user with a Super Admin role gives you the ability to create and manage additional user records without opening a support ticket.

If your company integrated its SAML Identity Provider (IdP) with Defense Orchestrator, you are now be able to fully manage user access to your Defense Orchestrator account.

If you are a Managed Service Provider with multiple Defense Orchestrator accounts, you are now able to grant and revoke account access for your existing users without opening a support ticket with Defense Orchestrator.

If your company uses Defense Orchestrator's default identity provider (OneLogin), you'll continue to need to open support tickets to create new user accounts but will be able to revoke access to your Defense Orchestrator account without opening a support ticket.

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

August 16, 2018

Improvements to Change Log

When you make a change to an ASA through CDO and the configuration change succeeds, the change log now shows the CLI commands used to make the change.

If you make a change to an ASA through CDO and the configuration change fails, the Change Log shows the CLI commands that failed and surrounds them with asterisks so you can locate them easily.

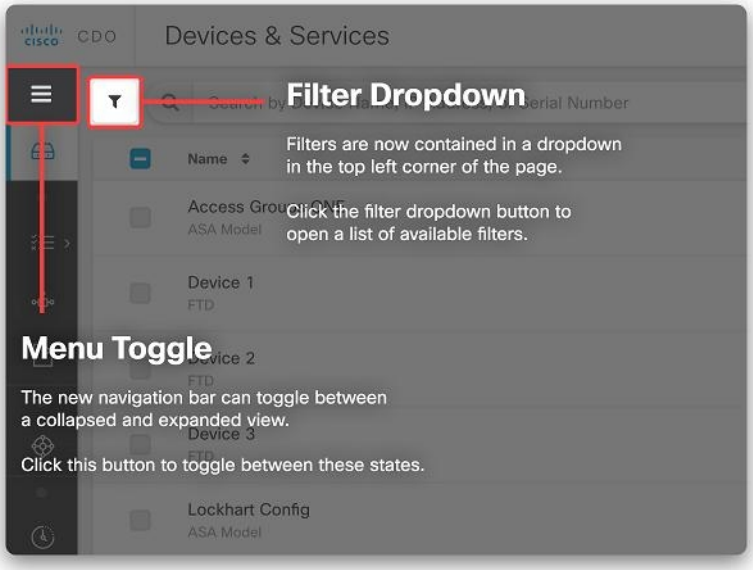
To see the commands that succeeded or failed, open the Change Log for the device on which the change was made, locate the entry for your action and expand it by clicking the + button at the end of the log entry.

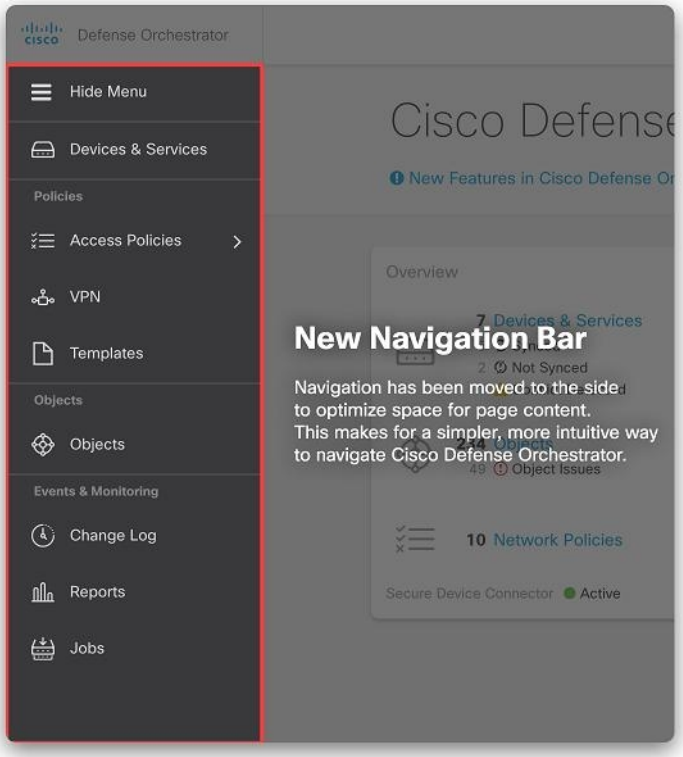
July 2018

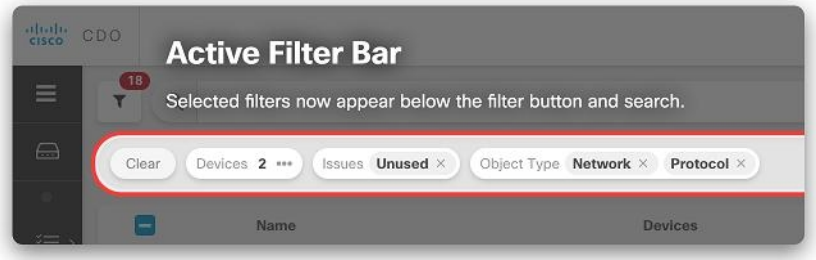
July 26, 2018

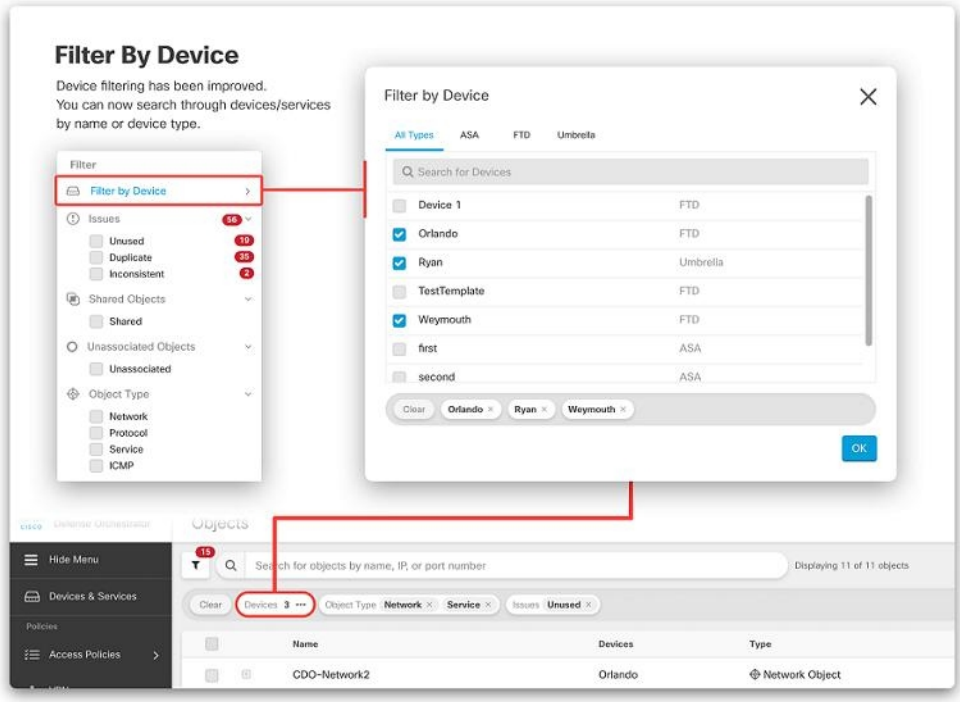
New CDO UI

We redesigned the navigation and filtering to be more intuitive and help you manage your environment more efficiently.


CDO
Devices & Services
Filter Dropdown
Filters are now contained in a dropdown in the top left corner of the page.
Click the filter dropdown button to open a list of available filters.
Name
Device 1
FTD
Lockhart Config
ASA Model
Menu Toggle
The new navigation bar can toggle between a collapsed and expanded view.
Click this button to toggle between these states.

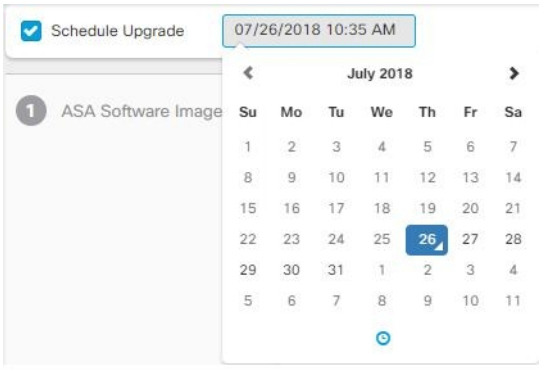

Defense Orchestrator
Hide Menu
Devices & Services
Policies
Access Policies
VPN
Templates
Objects
Objects
Events & Monitoring
Change Log
Reports
Jobs
Cisco Defense
New Features in Cisco Defense Or
Overview
7 Devices & Services
2 Not Synced
49 Object Issues
10 Network Policies
Secure Device Connector Active
New Navigation Bar
Navigation has been moved to the side to optimize space for page content.
This makes for a simpler, more intuitive way to navigate Cisco Defense Orchestrator.





Schedule Device Upgrade

You can now schedule software upgrades to your devices. On the Device Upgrade page, select the Schedule Upgrade check box, and configure a later date and time. For more information, see "Upgrade Devices and Services" in in *Managing ASA with Cisco Defense Orchestrator*.



Bulk Update Credentials

You can now update the credentials that CDO uses to connect to your ASA on multiple ASA devices at once. On the **Inventory** page, select multiple ASA devices, and click Update Credentials. For more information, see "Update ASA Connection Credentials" in *Managing ASA with Cisco Defense Orchestrator*.

Update Device Location

You can now update the device location of an onboarded ASA by clicking the edit button next to its IP address.

July 20, 2018

Update Credentials

You can now update the credentials that CDO uses to connect to your ASA. In the process of onboarding an ASA, you entered the username and password CDO must use to connect to the ASA. In the past, if you wanted to change those credentials or change the password, you needed to remove the ASA from CDO and onboard it again with the new credentials. Now you can change the credentials without having to re-onboard the ASA.

For more information, see "Updating ASA Connection Credentials" in *Managing ASA with Cisco Defense Orchestrator*.

July 12, 2018

New ASA Default Rule Behavior

When a new rule is added to an ASA network policy, it is assigned the "Permit" action by default.

Exported Device Lists Include the Tenant Name

When you export the device list of a particular tenant, the name of the tenant is now incorporated in the exported file name.

For more information, see "Export List of Devices and Services" in Managing ASA with Cisco Defense Orchestrator

Bulk Entry of Network Groups

When creating or editing an ASA network object group, you can now add IP addresses in bulk rather than one at a time.

For more information, see "Create or Edit ASA Network Objects and Network Groups" in Managing ASA with Cisco Defense Orchestrator.

May 2018

May 24, 2018

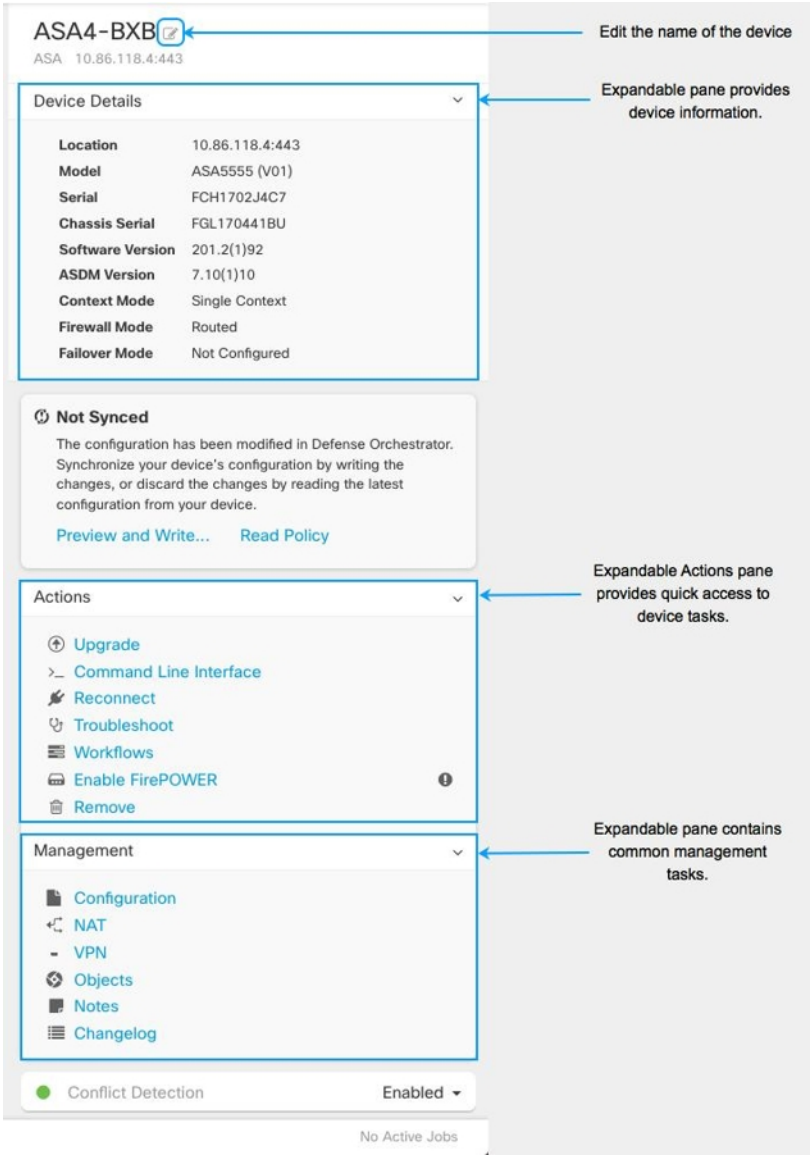
Support for Time-based ASA Network Policies

Time-based ASA Network policies allow access to networks and resources based on time of day. The time of day is defined by a time range object. Time range objects have a start time and an end time and can also be defined as a recurring event. For more information, see "Define a Time Range for a Policy" in *Managing ASA with Cisco Defense Orchestrator*.

May 17, 2018

New Device Details Panel Layout

We reorganized our device details panel to make device information and commonly used command buttons easier to find.



Support for ASA Global Access Policies

Now you can create a global access policy for your ASAs using CDO. A global access policy is a network policy applied to all the interfaces on an ASA. It is applied to inbound network traffic.With CDO, you can also copy a global access policy from one ASA to another to maintain consistency across devices. For more information, see " Configure an ASA Global Access Policy" in *Managing ASA with Cisco Defense Orchestrator*.

Network Address Translation Rule Wizard for ASA Devices

There is a new Network Address Translation (NAT) rule wizard to help you create NAT rules on your ASA devices for these use cases:

- Enable Internet Access for Internal Users
- Expose an Internal Server to the Internet

For more information, see "Network Address Translation Rule Wizard" in *Managing ASA with Cisco Defense Orchestrator*.

April 2018

April 26, 2018

New troubleshooting documentation

If Cisco Defense Orchestrator (CDO) and your ASA do not connect after an ASA reboot, it may be because the ASA has fallen back to using an OpenSSL cipher suite that is not supported by CDO's Secure Device Connector. The "ASA Fails to Reconnect to CDO After Reboot" troubleshooting topic tests for that case, provides a list of supported cipher suites, and remediation steps.

April 5, 2018

Access Control Entry (ACE) Limit Calculation

CDO displays the number of access control entries (ACEs) in individual rules, network policies, and the total number running on an ASA. Though there is no hard-coded limit to the number of ACEs that an ASA can process, an ASA's performance will degrade when the number of access control entries becomes too large. For more information, see "Access Control Entries (ACEs)" in *Managing ASA with Cisco Defense Orchestrator*.

March 2018

March 22, 2018

Unsuported Device

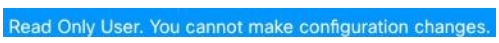
CDO does support the **ASA Service Module** (ASASM) at this time.

March 15, 2018

Read-only Users

We have created a read-only user role. Read-only users can view everything in CDO but they cannot create, update, configure, or delete anything on any page. Neither can they onboard devices.

Read-only users see a blue banner that reads, "Read Only User. You cannot make configuration pages." on every page



and they are identified by their role in the User Management table. For more information, see "User Roles" in *Managing ASA with Cisco Defense Orchestrator*.

Update Connection Credentials

When you onboard a device, you specify a username and password for that device. Cisco Defense Orchestrator connects to the device using those credentials and acts as that user when sending commands to the device. If users or passwords change on the device, you can update the device credentials to reflect those changes.

For more information, see the following topics:

- Updating ASA Connection Credentials—*Managing ASA with Cisco Defense Orchestrator*
- Updating AWS Connection Credentials—*Managing AWS with Cisco Defense Orchestrator*
- Updating Meraki MX Connection Credentials—*Managing Meraki with Cisco Defense Orchestrator*

Improved Network Policy Filtering

You can now filter network policies by hit count without first knowing which ASA the policy runs on. This allows you to find network policies with zero hit counts anywhere in your deployment. For more information, see "Filtering Use Cases" in *Managing ASA with Cisco Defense Orchestrator*.

Export Network Policy Rules

You can export the contents of each Access-Group or Crypto-Map to a .csv file. This .csv displays each Access Control List (ACL) and the data that CDO has for each ACL. For more information, see "Export Network Policy Rules" in *Managing ASA with Cisco Defense Orchestrator*.

March 7, 2018

New CDO Portal

We redesigned the portal to quickly communicate what you need to know, what you need to do, and where you go to do it.

Custom URL Upgrade

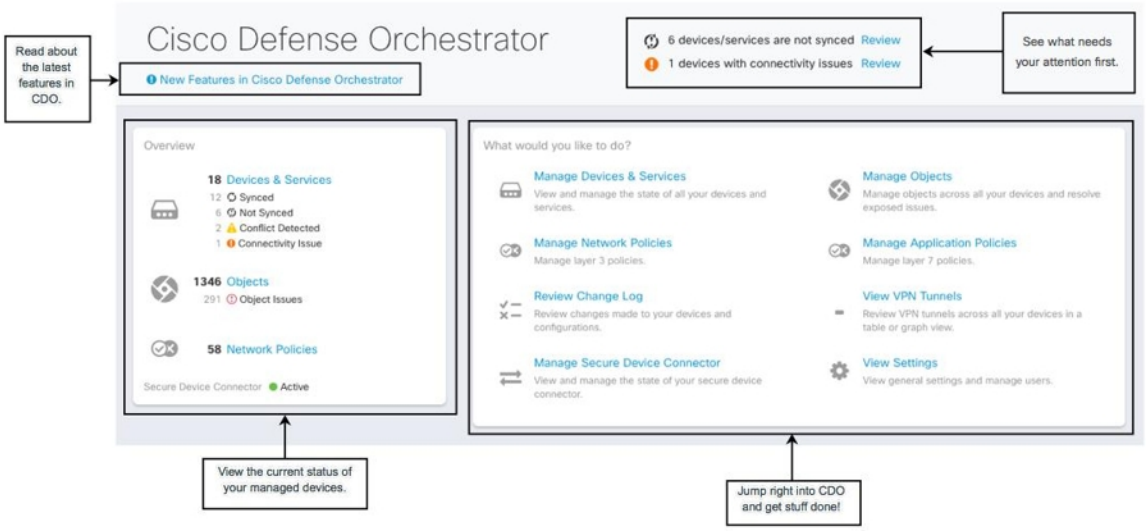
You can now upgrade your ASA device with ASA software and ASDM images you maintain in your own image repository. If your ASA does not have outbound access to the internet or you want an image that is not yet in CDO's image repository, this is the best way to upgrade your ASA. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB.

For more information, see "Custom URL Upgrade" in *Managing ASA with Cisco Defense Orchestrator*.

Device Notes

Now you can save notes about a specific ASA in a single, plain-text, file without leaving CDO. For more information, see "Device Notes" in *Managing ASA with Cisco Defense Orchestrator*.

February 2018



February 29, 2018

See All the Accounts Associated with your Tenant

You will now be able to see all the users associated with your tenant on the **User Management** screen. This includes any Cisco support engineer temporarily associated with your account to resolve a support ticket.

To view the users associated with your tenant:

1. From the user menu, select **Settings**.
2. Click **User Management**.

Manage Cisco Access to Your Tenant

Cisco support will associate its users with your tenant to resolve support tickets or proactively fix issues that affect more than one customer. However, if you prefer, you can prevent Cisco support from accessing your account by changing your account settings. For more information, see "General Settings" in *Managing FTD with Cisco Defense Orchestrator*.

See All the Accounts Associated with your Tenant

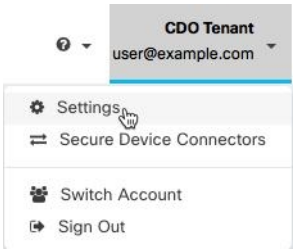
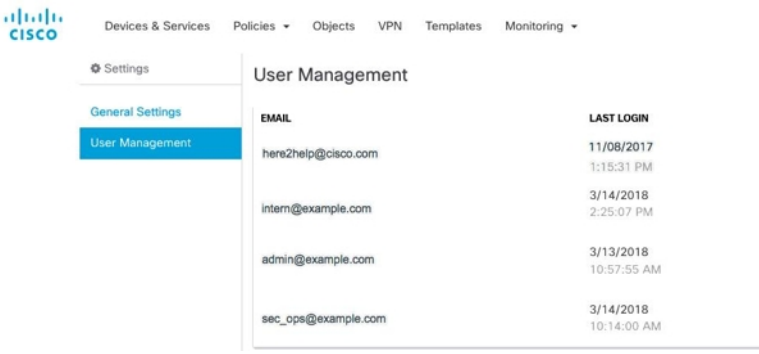
You will now be able to see all the users associated with your tenant on the **User Management** screen. This includes any Cisco support engineer temporarily associated with your account to resolve a support ticket.

To view the users associated with your tenant:

SUMMARY STEPS

1. From the user menu, select **Settings**
2. Click **User Management**

DETAILED STEPS

	Command or Action	Purpose
Step 1	From the user menu, select **Settings**	
Step 2	Click **User Management**	

Manage Cisco Access to Your Tenant

Cisco support will associate its users with your tenant to resolve support tickets or proactively fix issues that affect more than one customer. However, if you prefer, you can prevent Cisco support from accessing your account by changing your account settings. See for more information.

February 15, 2018

Manage ASAs Using CLI Macros

CDO provides a list of complete CLI-based commands and command templates that are ready for you to customize and run on your ASAs. These CLI macros can be run on a single ASA or ASAs in bulk. Do you have a regular monitoring or maintenance task you perform? You can create and store your own CLI-based commands on CDO and reuse them when you need them.

Manage ASAs Using CLI Macros

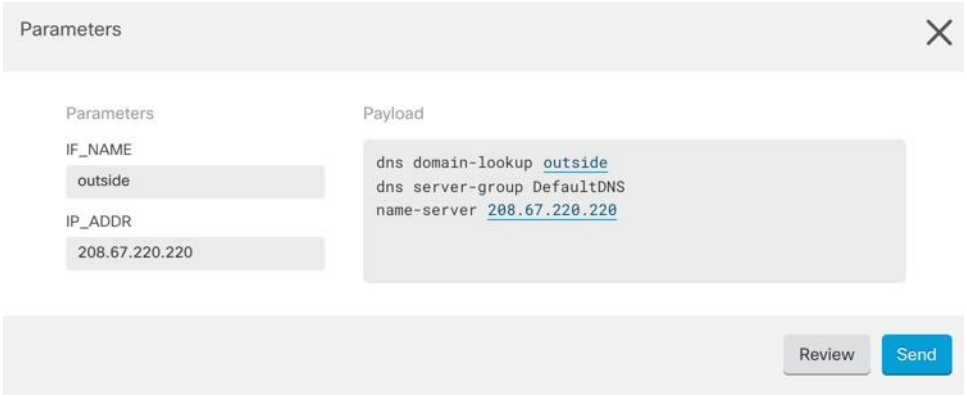
CDO provides a list of complete CLI-based commands and command templates that are ready for you to customize and run on your ASAs. These CLI macros can be run on a single ASA or ASAs in bulk. Do you have a regular monitoring or maintenance task you perform? You can create and store your own CLI-based commands on CDO and reuse them when you need them.

Here's an example of using a CLI macro to configure a DNS server on your ASAs:

Step 1 Select the devices you need to configure.

Step 2 Select the Configure DNS macro.

Step 3 Fill in the parameter fields with your information:

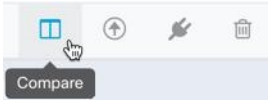


Step 4 Send it to all of your ASAs.

February 11, 2018

Compare ASA Configurations

You can now easily compare two ASA configurations. Select two ASAs in the **Inventory** page and click the compare button. CDO provides a side-by-side comparison of the devices' configurations. For more information, see "Compare ASA Configurations" in *Managing ASA with Cisco Defense Orchestrator*.



January 2018

January 31, 2018

Use CDO to Mitigate the Risks of Recent Cisco ASA Security Advisory

On January 29, 2018, the Cisco Product Security Incident Response Team (PSIRT) published the security advisory cisco-sa-20180129-asa1 describing an ASA and Firepower security vulnerability. Read our article, Using *CDO to Respond to Cisco ASA Advisory cisco-sa-20180129-asa1* to learn how to find the ASAs in your enterprise that are affected by the advisory and upgrade them to a patched version of ASA.

CDO Allows Long CLI Sequences

If you enter a long list of commands in the command box of the CLI, CDO attempts to break up your command into multiple commands so that they can be run against the ASA API at once. If CDO is unable to determine a proper separation in your command, it will prompt you for a hint. For example:

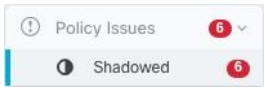
Error: CDO attempted to execute a portion of this command with a length that exceeded 600 characters. You can give a hint to CDO at where a proper command separation point is by breaking up your list of commands with an additional empty line between them.

For more information, see "ASA Command Line Interface" in *Managing ASA with Cisco Defense Orchestrator*.

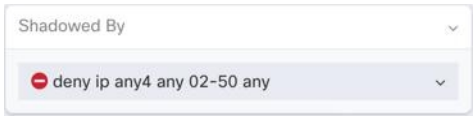
January 18, 2018

Enhancements to Help You Manage Shadow Rule Issues

- The ASA network policy issues filter indicate if there are any shadowed rules in a policy.



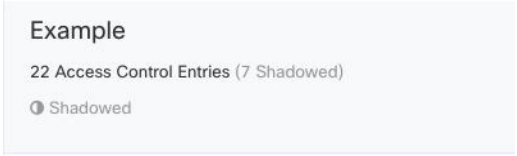
- A new badge ⚠ next to a rule in an ASA network policy indicates that it is shadowing another rule in the policy.
- For a shadowed rule, the network policy details pane identifies which rule in the policy is shadowing it.



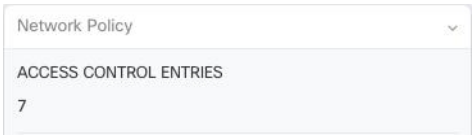
- New documentation on Resolving Shadow Rule Issues.

CDO Calculates Access Control Entries in your ASA Network Policies

Cisco Defense Orchestrator (CDO) calculates the number of access control entries (ACEs) derived from all the rules in an ASA network policy and displays that total at the top of the network policy details pane. If any of the rules in the network policy are shadowed, it lists that number as well.



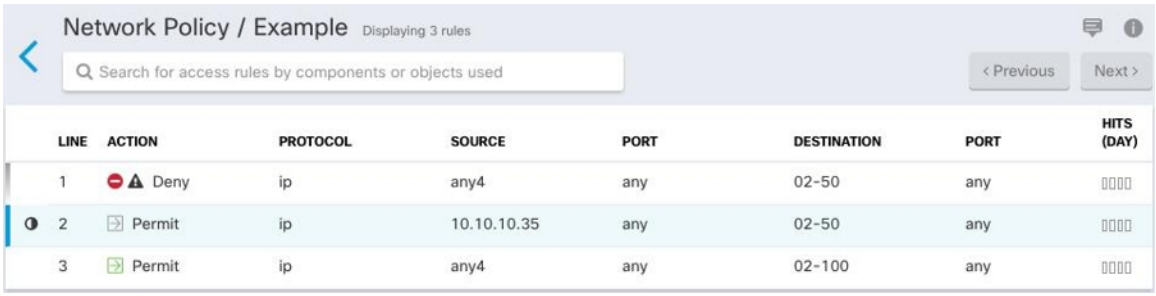
CDO also displays the number of ACEs derived from a single rule in a network policy and displays that information in the network policy details pane. Here is an example of that listing:



ASAs have recommended limits on the number of ACEs created on a device. Following those recommendations allows the ASA to process network traffic at an optimal speed. Deleting unused rules or shadowed rules helps keep your ACE count down.

Numbered Lines in Network Policies

CDO numbers rules in network policies for easy reading. Lines are renumbered as you add and delete rules or reorder them in a policy.



January 4, 2018

Enhanced ASA Network Policy Management

You can now perform these tasks with your ASA network policies!

- **Copy and paste policies between ASA devices**. Copy a policy from one ASA to another and assign it to a specific interface.
- **Cut and paste rules within policies**. Change the prioritization of rules within a policy by cutting and pasting them in the rule table.
- **Copy and paste rules between policies**. Promote policy consistency by copying a rule from one policy to another. These policies can be on the same device or on different devices.

These enhancements compliment existing functions like creating ASA network policies, activating or deactivating rules in a policy, and logging activity generated by rules in a policy.

For more information, see "Create or Edit ASA Network Objects and Network Groups" and "ASA Network Policies" in *Managing ASA with Cisco Defense Orchestrator* and navigate through the ASA network policy documentation using the topic arrows at the bottom of a page: