Use Operations Center to Monitor Multiple Prime Infrastructure Instances

- How to Monitor Multiple Instances, on page 1
- Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 2
- Run Reports on Deployments with Multiple Servers Using Operations Center, on page 16

How to Monitor Multiple Instances

There are three situations in which you will want to use multiple server instances to manage your network:

- You want to categorize the devices in your network into logical groups, with a different instance managing each of those groups. For example, you could have one instance managing all of your network's wired devices and another managing all of its wireless devices.
- The one instance you have running is sufficient to manage your network, but the addition of one or more instances would improve performance by spreading the CPU and memory load among multiple instances.
- Your network has sites located throughout the world, and you want a different instance to manage each of those sites in order to keep their data separate.

If multiple instances are running in your network, you can monitor those instances from the Operations Center. In this chapter, we will cover a typical workflow you might employ when using the Operations Center. This workflow consists of the following tasks:

- Use the Operations Center Config Dashboard to Manage Multiple Servers
- Run Reports on Deployments with Multiple Servers Using Operations Center

See Related Topics for more details:

Related Topics

Run Reports on Deployments with Multiple Servers Using Operations Center, on page 16

Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 2

Operations Center FAQ

Use the Operations Center Config Dashboard to Manage Multiple Servers

After viewing the various dashboards available in the Operations Center, you can then take a closer look at what is going on in your network. Specifically, you can monitor:

- The devices that belong to your network.
- The servers that manage those devices.
- The alarms, events and other incidents that have taken place in your network.
- The clients and users configured to use your network.

The following related topics cover these items in more detail.

Related Topics

View Devices Managed by All Servers Using Operations Center, on page 9
Use Virtual Domains on Deployments with Multiple Servers Using Operations Center, on page 10
Manage Servers using Operations Center, on page 13
View the Status of Multiple Servers using Operations Center, on page 14
View Software Updates on Multiple Prime Infrastructure Servers Using Operations Center
View Alarms on Devices Managed by Multiple Servers Using Operations Center, on page 15
View Clients and Users Managed by Multiple Servers Using Operations Center, on page 16

Supported Reports in Operations Center

The list of supported reports in operation center are:

- Autonomous AP
  - Autonomous AP Summary
  - Autonomous AP Uptime
- CleanAir
  - Air Quality vs Time
  - Security Risk Interferers
  - Worst Air Quality APs
  - Worst Interferers
- Client
  - Busiest Clients
  - CCX Client Statistics
  - Client Count
  - Client Sessions

    - Client Summary
    - Client Traffic
    - Client Traffic Stream Metrics
    - Mobility Client Summary
    - Throughput
    - Unique Clients
    - Unique Clients and Users Summary

- Compliance
    - Change Audit
    - Network Discrepancy
    - PCI DSS Detailed
    - Wireless Configuration Audit

- Device
    - AP Ethernet Port Utilization
    - AP Profile Status
    - AP Radio Downtime Summary
    - AP Summary
    - AP Utilization
    - Busiest APs
    - CPU Utilization
    - Detailed Hardware
    - Detailed Software
    - Device Credential Verification
    - Device Health
    - Interface Availability
    - Interface Detail
    - Interface Utilization
    - Interface Utilization Trend
    - Inventory
    - Memory Utilization
    - Non-Primary Controller APs

  - Port Capacity
  - Port Reclaim Report
  - Top AP by Client Count
  - Unified AP Ping Availability
  - Vlan
  - Wired Device Availability
  - Wired Module Detail
  - Wired Port Attribute
  - Wireless Up Time
  - Wireless Utilization

- Guest
  - Guest Accounts Status
  - Guest Association
  - Guest Count
  - Guest Operations
  - Guest User Sessions

- Mesh
  - Link Stats

- Network Summary
  - 802.11n Summary
  - Wireless Network Executive Summary

- Performance
  - 802.11 Counters
  - AP RF Quality
  - AP RF Quality History
  - Application Summary
  - Conversations
  - Coverage Hole
  - Environmental Temperature
  - Interface Errors and Discards
  - Interface Summary

    - Threshold Violation
    - VoIP Calls Graph
    - VoIP Calls Table
    - Voice Statistics
    - Wireless Network Utilization
    - Wireless Traffic Stream Metrics
    - Wireless Tx Power and Channel
    - Worst RF APs

- Raw NetFlow
    - Netflow V5

- Security
    - Adaptive wIPS Alarm
    - Adaptive wIPS Top 10 AP
    - Adhoc Rogues
    - New Rogue AP Count Summary
    - New Rogue APs
    - Rogue AP Count Summary
    - Rogue AP Events
    - Rogue APs(Updated)
    - Security Alarm Trending Summary
    - Wired Rogue APs via SPT(New)

- System Monitoring
    - CPU Threshold Breach Reports

Supported Dashlet in Operations Center

The list of supported dashlets in the operation center are:

- Network Summary
    - Overview
        - Interface Availability Summary
        - Interface Utilization Summary
        - Top N CPU Utilization

        - Top N Environmental Temperature
        - Top N Interface Utilization
        - Top N Memory Utilization
        - Top N WAN Interfaces by Utilization
    - Incidents
        - Alarms
        - Device Reachability Status
        - Syslog Summary
        - Syslog Watch
        - Top N Syslog Sender
        - Top N Alarms Types
        - Top N Event Types
    - Client Summary
        - Client Count By Association/Authentication
        - Client Count By Wireless/Wired
        - Client Distribution
        - Client Posture Status
        - Client Traffic
        - Coverage Area
        - Top 5 SSIDs by Client Count
        - Top 5 Switches by Client Count
    - Site Summary
        - Top N Applications
        - Top N Clients
        - Top N Devices With Most Alarms
        - Top N Servers
    - Network Health
- Overview
    - Incidents
        - Top N Sites with Most Alarms

        - Top N Alarm Types
        - Alarm Summary
        - Device Reachability Status
    - Client
        - Client Count By Association/Authentication
        - Client Count By Wireless/Wired
        - Client Distribution
        - Client Posture Status
        - User Auth Failure Count
        - Guest Users Count
        - Most Recent Client Alarms
    - Network Devices
        - Coverage Area
        - Recent Alarms
        - Top N CPU Utilization
        - Top N Memory Utilization
        - Device Availability Summary
        - Interface Availability Summary
    - Network Interface
- Wireless
    - Security
        - AP Threats/Attacks
        - Attacks Detected
        - Cisco Wired IPS Events
        - CleanAir Security
        - MFP Attacks
        - Security Index
    - Mesh
        - Mesh Top Over Subscribed AP
    - Clean Air

        - 802.11a/n/ac/ax Interferer Count
        - 802.11b/g/n/ax Interferer Count
        - Recent Security-risk Interferers
        - Worst 802.11a/n/ac/ax Interferers
        - Worst 802.11b/g/n/ax Interferers
    - Context Aware
        - Rouge Element Detected by CAS
- Performance
    - Device
        - Device Memory Utilization Trend
        - Device Port Summary
        - Device CPU Utilization Trend
        - Device Health Information

Add Devices Using Operations Center

Operations Center allows you to add the devices to one or more of managed instances from the Operations Center user interface. In addition to manually adding devices, you can also choose to import devices using the Bulk Import option.

Step 1 Choose Monitor > Managed Elements > Network Devices.

Step 2 To add devices manually, do the following:

a) Click the + icon above the Network Devices table, then choose Add Device.
b) In the Add Device dialog box, choose the server to which you want to add the devices.
c) Complete the required fields. Click the "?" next to a field for a description of that field.

Note Telnet/SSH information is mandatory for devices such as most Cisco NCS devices.

d) (Optional) Click Verify Credentials to validate the credentials before adding the device.

supports HTTP credentials-verification for NAM devices only.

e) Click Add to add the device with the settings you specified.

Note User Defined Field (UDF) parameters will be available for the new device only if you first choose Administration > Settings > System Settings > Inventory > User Defined Fields and then add these UDF parameters. Do not use the special characters : ; and # for UDF field parameters.

Step 3 To import devices from another source using CSV file, do the following:

a) Click the + icon above the Network Devices table, then choose Bulk Import.
b) In the Bulk Device Import dialog box, choose the server to which you want to import the devices.
c) Click Choose File and select the CSV file containing the device details for bulk import.

For details on creating a CSV file, see Create Device Import CSV Files

d) Click Import.

Move Device from One Prime Infrastructure Instance to Another Prime Infrastructure Instance

You can move the device that is managed in one instance to another instance for load balancing among different managed instances.

Step 1 Choose Monitor > Managed Elements > Network Devices.

Step 2 In the Network Devices table, choose the device and click Move Device.

Step 3 In the Moving Devices Dialog box, choose the server to which you want the device to be moved.

Step 4 Check the Remove device from source server check box and click OK.

If you uncheck the Remove device from source server check box, the device will be managed by more than one instance which is not a recommended practice.

View Devices Managed by All Servers Using Operations Center

Select Monitor > Managed Elements > Network Devices to open the Network Devices page in Operations Center. From here, you can view information for every device that belongs to your network that a instance is managing. This information includes the device’s hostname/IP address, its current reachability status, and the last time inventory data was successfully collected from that device. You can also launch the Device 360° view and perfom Telnet, Ping, and Traceroute actions.

When you first open the Network Devices page, every network device is displayed. To refine the devices displayed, do one of the following:

- From the Device Group pane, select the desired device type, location, or user-defined group.

  Note Cisco Prime Infrastructure Operations Center now supports the Meraki group of devices which includes Meraki Access Point, Meraki Dashboard, Meraki Security Appliances, and Meraki Switches. Click on any one of the Meraki device groups to view the list of devices associated with that particular group.

- Apply a custom filter or select one of the predefined filters from the Show drop-down list. Operations Center provides a custom filter that allows you to view duplicate devices across your managed instances. For details on how to use filters, see the related topic "Quick Filter”.

- Search for a particular device. For details, see the related topic “Search Methods”.
- If you want to hide the empty device groups, do the following:
  - Choose Administration > System Settings > Inventory > Grouping.
  - Uncheck the Display groups with no members check box.
  - Click Save.

If you delete a device from the Operations Center Network Devices page, the device is also deleted from all the managed instances monitoring that device.

Related Topics

Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 2
Use Virtual Domains on Deployments with Multiple Servers Using Operations Center, on page 10
Quick Filters
Search Methods

Synchronize Devices Using Operations Center

To synchronize the Prime Infrastructure Operation Center database with the configuration running on Prime Infrastructure devices, you can force an inventory collection.

To synchronize devices, follow these steps:

Step 1 Choose Monitor > Managed Elements > Network Devices.

Step 2 Select the device(s) whose configuration you want synchronized with the configuration stored in the Prime Infrastructure Operation Center database.

Step 3 Click Sync.

Note If the synchronized device is a default/Admin VDC, then all the configuration of all the child VDCs are synchronized automatically and the configuration is updated in the Prime Infrastructure Operation Center database. Admin VDC sync will also add the newly added VDC in hardware to the user interface or delete the deleted VDC in hardware from the user interface.

Use Virtual Domains on Deployments with Multiple Servers Using Operations Center

As explained in Control User Access, this feature provides an Operations Center administrator the ability to define a virtual domain on managed instances. The Virtual Domains page will be modified to give Operations Center administrators visibility to each virtual domain defined under a managed instance. The list of domains will be consolidated and displayed in the Operations Center.

From the Operations Center, you can view all the virtual domains available in all of the instances that Operations Center is managing.

You can also create or edit virtual domains from Operations Center itself. If the same virtual domain is active in multiple instances, Operations Center displays the virtual domain once, with data aggregated from all the active virtual domains with the same name on all the managed instances.

You can create virtual domain only if an instance is present or it is in reachable state. The Number of network elements in Virtual Domains is limited when compared to that of , since the Virtual Domain shows only managed network elements. You can assign device groups to virtual domain and also choose the instances to which you want to distribute the virtual domain using Operations Center.

Creating, editing, importing, and exporting virtual domains from within Operations Center works the same way as creating, editing, importing, and exporting virtual domains in a single instance of . For more details, see Using Virtual Domains to Control Access

Related Topics

Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 2
View Devices Managed by All Servers Using Operations Center, on page 9
Manage Servers using Operations Center, on page 13
Distribute Virtual Domains to Servers, on page 11

Distribute Virtual Domains to Servers

In Operations Center, if you want to distribute the existing virtual domain to instances, follow these steps:

Step 1 Choose Administration > Users > Virtual Domains.

Step 2 From the Virtual Domains sidebar menu, click an existing virtual domain which you want to create in new instance.

Step 3 Click Managed Servers tab.

Step 4 Click Add and choose the manage instances for which you want to distribute the virtual domain.

Step 5 Click OK.

Step 6 Click Submit.

For more information see the chapter User Permissions and Device Access in Cisco Prime Infrastructure Administrator Guide.

Related Topics

Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 2

Enable Operations Center RBAC Support

The Role Based Access Control (RBAC) support in Operations Center allows a collection of devices from multiple managed instances to be associated with a user via virtual domains. This feature enables to assign privileges such as accessing Monitor and Manage server page, adding, modifying or deleting managed instances, and populate certain dashlets, to a specific user.

Follow these steps to enable RBAC in the Operations Center:

Step 1 Log in to as an administrator.

Step 2 Choose Administration > Users > Users, Roles & AAA > User Groups.

Step 3 Click a group name to which RBAC is to be provided.

Step 4 Click Task Permissions tab.

Step 5 Check the following check boxes under Operations Center Tasks:

- Monitor and Manage Servers Page Access.
- Administrative Privileges under Manage and Monitor Server Pages.

These options are enabled by default for admin and super users.

Step 6 Click Save.

For more information refer the chapter User Access and Device Permisssions in Cisco Prime Infrastructure Administrator Guide.

Related Topics

Use Virtual Domains on Deployments with Multiple Servers Using Operations Center, on page 10

Share Device Configuration Templates Across Prime Infrastructure Servers Using Operations Center

Although it does not directly manage or configure any device in your network, Operations Center gives you access to the configuration templates stored on the server instances it manages. You can use Operations Center to:

- View the configuration templates on any of the servers.
- Distribute templates that exist on one server to any of the other servers Operations Center manages. Template distribution like this is required if (for example) you want to deploy a template across your entire network.

The steps for doing these tasks are identical to the ones you follow when you perform the same tasks on standalone servers. You simply need to log into the Operations Center instance first, and then select the server instance whose templates you want to work on.

View Configuration Templates Using Operations Center

You can view configuration templates on any managed instance by selecting the Configuration menu option in Operations Center and expanding the listing until you find the templates you want.

Step 1 Log in to Operations Center and choose Configuration > Templates > Features & Technologies.

Step 2 Expand the template category you want to view (for example, My Templates). Operations Center display a list of the managed instances with templates in that category.

Step 3 Expand the managed instance whose templates you want to view. Expand the template sub-categories as needed.

Deploy Configuration Templates Using Operations Center

Step 1 After you create a configuration template, click Deploy.
The Deployment wizard appears.

Step 2 Select the devices on which you want to deploy the template, then click Next to choose the input values.

Step 3 In the Input Values tab, you can toggle between Form and CLI view.

Step 4 After entering the necessary configuration values, click CLI to confirm the device and template configuration values.

Step 5 Click Next to view the job deployment summary.

Step 6 On the Deployment Summary tab, you can see the CLI view for each of the devices.

Step 7 Click Finish to deploy the template.

Distribute Configuration Templates Across Managed Servers

You can distribute any user-defined configuration template from one managed instance to another managed instance.

Distributing a template to another server instance occurs automatically when you deploy a template to a device on another such instance without first copying (distributing) that template to the other instance.

Step 1 Log in to Operations Center and choose Configuration > Templates > Features & Technologies.

Step 2 Expand the template category you want to view (for example, My Templates). Operations Center displays a list of the managed instances with templates in that category.

Step 3 Expand the managed instance whose templates you want to view. Expand the template sub-categories as needed.

Step 4 (optional) If you want to edit the template before distribution, do the following:

a) Click Add Variable and choose the template variable.
b) Click the edit icon and make the necessary changes.
c) Click Save.

Step 5 When you see the template you want to distribute, click on it to select it. Operations Center displays details for the selected template.

Step 6 Click Distribute. Operations Center displays a list of all the server instances that it manages and that are currently reachable.

Step 7 Select the checkbox next to each server instance to which you want to distribute the template.

Step 8 Check the Overwrite template with the same name check box and then click OK.

If you uncheck the Overwrite template with the same name check box and if the template already exists on the other server, Operations Center will not distribute the template and will alert you to check the Overwrite template with the same name check box.

Manage Servers using Operations Center

Select Monitor > Monitoring Tools > Manage and Monitor Servers to open the Manage and Monitor Servers page. From here, you can:

- Add new servers (up to the license limit).
- Edit, delete, activate, and deactivate current servers.
- View each servers reachability, CPU utilization, memory utilization, software update status and secondary server details (if it is configured), summary of purchased licenses and utilized licenses, and alarms generated for the instances.
- Determine whether any servers are down.
- View alarms and events.
- Cross-launch into individual instances.

- See if any backup servers are running. Administrators can use the High Availability (HA) framework to configure a backup server to automatically come online and take over operations for the associated primary server when it goes down. For more information on HA framework, see “Configure High Availability” in Related Topics. Administrators should be sure to follow the restrictions on use of HA with Operations Center given in “Before You Begin Setting Up High Availability”.

Aside from a server’s reachability status, there are three server metrics you should focus on:

- CPU utilization
- Memory utilization.

If a server has a network latency figure that exceeds one second, or it has a CPU or memory utilization percentage greater than 80%, the chances are good that an issue exists with that server.

If a server’s status is listed as “unreachable”, a “?” icon will appear next to the reachability status message. Hover your mouse cursor over the icon to see a popup message giving possible causes for the server’s status (for example, server cannot be pinged, API response (latency) is too slow and SSO is not setup properly).

Related Topics

Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 2

Use Virtual Domains on Deployments with Multiple Servers Using Operations Center, on page 10

View the Status of Multiple Servers using Operations Center, on page 14

View the Status of Multiple Servers using Operations Center

Use the Server Status Summary to view the current status of your servers without leaving the dashboard or page you have open. To open it, place your cursor over any portion of the Server Status area at the top of the Operations Center’s main page. From here, you can quickly determine if any of your servers are currently down. You can also launch a separate instance for the selected server.

You can also quickly view the reachability history for any server managed by Operations Center.

Step 1 Select Monitor > Monitoring Tools > Manage and Monitor Servers. Operations Center displays the list of servers it manages.

Step 2 Select one of the managed servers. The page displays summary status for that server.

Step 3 Click the Reachability History tab at the bottom of the page. Operations Center displays a list of recent changes in reachability for the selected server.

Step 4 If want to clear the reachability history, click Clear History and click Yes in the pop-up window.

Related Topics

Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 2

Activate Operation Center using Smart Licensing

Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks. The solution allows you to easily track the status of your license and software usage trends.

Smart Licensing helps simplify three core functions:

- Purchasing: The software that you have installed in your network can automatically self-register themselves, without Product Activation Keys (PAKs).
- Management: You can automatically track activations against your license entitlements. Additionally, there is no need to install the license file on every node.
- Reporting: Through the portal, Smart Licensing offers an integrated view of the licenses you have purchased and what has been actually deployed in your network. You can use this data to make better purchase decisions, based on your consumption.

To select smart software licenses, see Choose Smart Software Licenses section in Cisco Prime Infrastructure Administrator Guide.

Distribute Software Updates to Prime Infrastructure Instances Managed by Operations Center

Operation Center allows you to distribute software updates to multiple Prime Infrastructure instances.

To distribute a software update:

Step 1 Go to Administration > Licenses and Software Updates > Software Update.

Step 2 Click Prime Infrastructure tab and click upload link. In the Upload Update dialog, click the Upload from local computer or Copy from server's local disk radio button as required.

Step 3 Click Browse to choose the dowloaded patch file from the save location and click Ok.

Step 4 Click Distribute to distribute the patch file to Prime Infrastructure servers.

Note You may now choose to distribute the patch file from Prime Infrastructure Operations Center to Prime Infrastructure's Secondary Server. Please note that installing patches on paired High Availability servers is not allowed. For more information, refer How to Patch Paired HA Servers section in the Cisco Prime Infrastructure Administrator Guide.

Step 5 Choose the required Prime Infrastructure servers from the list of servers and click Ok. Update success popup message appears.

Step 6 Select the Prime infrastructure tab and click the Install button to install the updates in Prime Infrastructure instances.

Step 7 You can view the status of the updates in Status of Updates section.

Note You can distribute the software update to any number of available Prime Infrastructure servers using Distribute button in Prime Infrastructure tab. To know more on Software Updates, see Licensens and Software Updates chapter in Cisco Prime Infrastructure Administrator Guide.

View Alarms on Devices Managed by Multiple Servers Using Operations Center

Select Monitor > Monitoring Tools > Alarms and Events to open the Alarms and Events page. From here, you can view a comprehensive listing of your network's alarms, events, and syslog messages. With one or multiple alarms selected, you can also determine whether those alarms have been acknowledged, add a note that describes them in more detail, or delete them from the page.

The Alarm Summary displays an aggregated count of critical, major, and minor alarms from the managed instances.

To refine the alarms, events, and syslog messages displayed here, do one of the following:

- From the Device Group pane, select the desired device type, location, or user-defined group.
- Apply a custom filter or select one of the predefined filters from the Show drop-down list. For details on how to use filters, see the related topic “Quick Filters”.
- Search for a particular alarm or event. For details, see the related topic “Search Methods”.
- Hover your cursor on the Alarm Browser screen to display the aggregated count of alarms for the managed instances. You can also acknowledge, annotate, and delete alarms; that action is duplicated on the respective instance.

Related Topics

Quick Filters
Search Methods
Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 2
View Clients and Users Managed by Multiple Servers Using Operations Center, on page 16

View Clients and Users Managed by Multiple Servers Using Operations Center

Select Monitor > Monitoring Tools > Clients and Users to open the Clients and Users page, which contains the aggregated clients of all managed instances. From here, you can view information for the clients configured on your network, such as a client’s MAC address, the user associated with the client, and the name of the device that hosts the client. You can choose a client or user and view the client association history and the statistical information. You can also launch the 360° Degree View to get more information about the device and the associated clients.

To refine the list of clients displayed here, do one of the following:

- Apply a custom filter or select one of the predefined filters from the Show drop-down list. For details on how to use filters, see the related topic “Quick Filters”.
- Search for a particular client. For details, see the related topic “Search Methods”.

Related Topics

Quick Filters
Search Methods
Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 2

Run Reports on Deployments with Multiple Servers Using Operations Center

In addition to the Operations Center dashboards and monitor pages, Operations Center provides a subset of reports that combine network management and performance data across all the managed instances of . If you are using Operations Center to segment and rationalize your management of a global network, these specialized versions of the standard reports can help get a closer look at your network as a whole, help you monitor health across the globe, and troubleshoot emergent issues.

The Operations Center reports contain aggregated data from all of the managed instances. If you want to restrict this aggregation to a subset of the managed instances, the best ways to do this are to:

- Temporarily deactivate those managed instances whose data you do not want included in the aggregated Operations Center report data. You can do this by selecting Monitor > Monitoring Tools > Manage and Monitor Servers and choosing to deactivate the servers you want to ignore.
- Use virtual domains to restrict the data the instances in which you are interested. For details, see “Use Virtual Domains on Deployments with Multiple Prime Infrastructure Servers Using Operations Center” in Related Topics.

Except for aggregating data across managed instances, Operations Center reports generation works the same way as in . For more information about reports and how to generate them, see "Create, Schedule, and Run a New Report" in Related Topics.

Related Topics

Create, Schedule, and Run a New Report
Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 2
Use Virtual Domains on Deployments with Multiple Servers Using Operations Center, on page 10
View Alarms on Devices Managed by Multiple Servers Using Operations Center, on page 15
View Clients and Users Managed by Multiple Servers Using Operations Center, on page 16
Operations Center FAQ