



# Monitoring Multiple Prime Infrastructure Instances

---

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

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

If multiple Prime Infrastructure 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:

- Viewing the Operations Center dashboards
- Configuring devices using Prime Infrastructure templates
- Monitoring your network
- Running reports

See Related Topics for details on these and related tasks.

## Related Topics

- [Setting Up Operations Center](#)
- [Viewing the Operations Center Dashboards](#)
- [Configuring Devices Using Operations Center](#)
- [Monitoring Your Network Using Operations Center](#)
- [Running Reports With Operations Center](#)
- [Operations Center FAQs](#)

## Viewing the Operations Center Dashboards

The Operations Center provides additional, Operations Center-specific dashboards that you can use to quickly determine the status of your network and identify any issues that require further attention. The Operations Center dashlets display aggregated data. The following types of dashboards are available:

- Overview dashboards, which summarize the current status of key areas in your network.
- Incident dashboards, which report on all alarms and events recorded across your network.

To access a particular dashboard and the dashlets that comprise it, either click the appropriate tabs on the main Operations Center page or select the dashboard from the Dashboard menu.

For general information about using and customizing dashboards and dashlets, see “Prime Infrastructure User Interface Reference” in Related Topics.

### Related Topics

- [Setting Up Operations Center](#)
- [Monitoring Your Network Using Operations Center](#)
- [Appendix A, “Prime Infrastructure User Interface Reference.”](#)
- [Operations Center FAQs](#)

## Configuring Devices 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 Prime Infrastructure server instances it manages. You can use Operations Center to:

- View the configuration templates on any of the Prime Infrastructure 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 Prime Infrastructure servers. You simply need to log into the Operations Center instance first, and then select the Prime Infrastructure server instance whose templates you want to work on.

See the following Related Topics for more details.

### Related Topics

- [Viewing Configuration Templates Using Operations Center](#)
- [Distributing Configuration Templates Across Managed Servers](#)
- [Monitoring Your Network Using Operations Center](#)

## Viewing Configuration Templates Using Operations Center

You can view configuration templates on any managed Prime Infrastructure 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 displays a list of the managed Prime Infrastructure 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.
- 

#### Related Topics

- [Distributing Configuration Templates Across Managed Servers](#)
- [Configuring Devices Using Operations Center](#)
- [Creating Feature-Level Configuration Templates](#)
- [Deploying Templates](#)

## Distributing Configuration Templates Across Managed Servers

You can copy any user-defined configuration template on any managed Prime Infrastructure instance to another managed instance by selecting that template and clicking **Distribute**.

Distributing a template to another Prime Infrastructure 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 Prime Infrastructure 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** When you see the template you want to distribute, click on it to select it. Operations Center displays details for the selected template.
- Step 5** Click **Distribute**. Operations Center displays a list of all the Prime Infrastructure server instances that it manages and that are currently reachable.
- Step 6** Select the checkbox next to each Prime Infrastructure server instance to which you want to distribute the template, then click **OK**.

If the template already exists on the other server, Operations Center will prompt you to either cancel the distribution or confirm that you want to overwrite the existing template.

---

#### Related Topics

- [Viewing Configuration Templates Using Operations Center](#)
- [Configuring Devices Using Operations Center](#)

# Monitoring Your Network Using Operations Center

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 Prime Infrastructure 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

- [Monitoring Devices Using Operations Center](#)
- [Using Virtual Domains With Operations Center](#)
- [Managing and Monitoring Prime Infrastructure Servers Using Operations Center](#)
- [Viewing the Prime Infrastructure Server Status Summary in Operations Center](#)
- [Viewing Prime Infrastructure Server Software Updates in Operations Center](#)
- [Viewing Prime Infrastructure Server Reachability History in Operations Center](#)
- [Viewing Alarms and Events Using Operations Center](#)
- [Viewing Clients and Users Using Operations Center](#)
- [Cross-Launching Prime Infrastructure Using Operations Center](#)
- [Viewing the Operations Center Dashboards](#)

## Monitoring Devices 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 Prime Infrastructure 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.

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.
- 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 "Performing a Quick Filter".
- Search for a particular device. For details, see the related topic "Search Methods".

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

## Related Topics

- [Performing a Quick Filter](#)

- [Search Methods](#)
- [Monitoring Your Network Using Operations Center](#)
- [Using Virtual Domains With Operations Center](#)

## Using Virtual Domains With Operations Center

As explained in “Controlling User Access” in Related Topics, this feature provides an Operations Center administrator the ability to define a virtual domain on managed Prime Infrastructure instances. The Virtual Domains page will be modified to give Operations Center administrators visibility to each virtual domain defined under a managed Prime Infrastructure 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 Prime Infrastructure 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 Prime Infrastructure 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 Prime Infrastructure 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 Prime Infrastructure , since the Virtual Domain shows only managed network elements.

Note that any virtual domain you create using Operations Center will be replicated across all the instances of Prime Infrastructure that Operations Center manages, and if selected network elements are not present in particular instances, an empty virtual domain will be created.

Creating and editing virtual domains from within Operations Center works the same way as creating and editing virtual domains in a single instance of Prime Infrastructure . For details on adding, editing and viewing virtual domains, see “Using Virtual Domains to Control Access” in Related Topics.

### Related Topics

- [Controlling User Access](#)
- [Using Virtual Domains to Control Access](#)
- [Monitoring Your Network Using Operations Center](#)
- [Monitoring Devices Using Operations Center](#)
- [Managing and Monitoring Prime Infrastructure Servers Using Operations Center](#)
- [Creating Existing Virtual Domain in New Instances](#)
- [Maximum Virtual Domains Supported in Operations Center](#)

## Maximum Virtual Domains Supported in Operations Center

We recommend you use Express OVA for Operations Center. For Express OVA, the maximum number of Virtual Domains supported in Operations Center is 100 (Including Virtual Domains in Prime Infrastructure instances). Also you have an option to increase CPU and Memory of Operations Center server to higher configuration based on number of Virtual Domains supported. For more understanding, please refer *Cisco Prime Infrastructure 3.1 Quick Start Guide*, for metrics of hardware profiles and the respective number of Virtual Domains supported.

**Related Topics**

- [Using Virtual Domains With Operations Center](#)
- [Creating Existing Virtual Domain in New Instances](#)

## Creating Existing Virtual Domain in New Instances

In Operations Center, if you want to create the existing virtual domain in new 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 **Distribute to All Servers**.
  - Step 5** Click **Submit**.
- 

**Related Topics**

- [Controlling User Access](#)
- [Using Virtual Domains With Operations Center](#)
- [Maximum Virtual Domains Supported in Operations Center](#)

## Role Based Access Control Support in Operations Center

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 providing Nbi privilege to generate reports and populate certain dashlets, to a specific user.

Follow these steps to enable RBAC in the Operations Center:

- 
- Step 1** Log in to Prime Infrastructure 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**
    - **Nbi Security Exception**.

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

**Step 6** Click **Save**.

---

#### Related Topics

- [Controlling User Access](#)
- [Using Virtual Domains With Operations Center](#)
- [Maximum Virtual Domains Supported in Operations Center](#)

## Managing and Monitoring Prime Infrastructure 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 Prime Infrastructure servers (up to the license limit).
- Edit, delete, activate, and deactivate current Prime Infrastructure servers.
- View each servers' reachability, network latency, CPU utilization, memory utilization, software update status and secondary server details (if it is configured), license count, and alarms generated for the Prime Infrastructure instances.
- Determine whether any servers are down.
- View alarms and events.
- Cross-launch into individual Prime Infrastructure instances.
- See if any backup servers are running. Administrators can use the Prime Infrastructure High Availability (HA) framework to configure a backup Prime Infrastructure server to automatically come online and take over operations for the associated primary server when it goes down. For more information on Prime Infrastructure's HA framework, see "Configuring 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:

- Network latency
- 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

- [Configuring High Availability](#)
- [Before You Begin Setting Up High Availability](#)
- [Monitoring Your Network Using Operations Center](#)

- [Using Virtual Domains With Operations Center](#)
- [Viewing the Prime Infrastructure Server Status Summary in Operations Center](#)

## Viewing the Prime Infrastructure Server Status Summary in Operations Center

Use the Server Status Summary to view the current status of your Prime Infrastructure 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 Prime Infrastructure instance for the selected server.

### Related Topics

- [Monitoring Your Network Using Operations Center](#)
- [Cross-Launching Prime Infrastructure Using Operations Center](#)



## Viewing Prime Infrastructure Server Software Updates in Operations Center

You can quickly view the list of software updates that have been applied to any Prime Infrastructure server managed by Operations Center.

- 
- Step 1** Select **Monitor > Monitoring Tools > Manage and Monitor Servers**. Operations Center displays the list of Prime Infrastructure servers it manages.
- Step 2** Select one of the managed servers. The page displays summary status for that server.
- Step 3** Click the **Software Updates** tab at the bottom of the page. Operations Center displays the list of software updates applied to the selected Prime Infrastructure server.
- 

### Related Topics

- [Monitoring Your Network Using Operations Center](#)
- [Cross-Launching Prime Infrastructure Using Operations Center](#)

## Viewing Prime Infrastructure Server Reachability History in Operations Center

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

- 
- Step 1** Select **Monitor > Monitoring Tools > Manage and Monitor Servers**. Operations Center displays the list of Prime Infrastructure 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 Prime Infrastructure server.
- 

### Related Topics

- [Monitoring Your Network Using Operations Center](#)
- [Cross-Launching Prime Infrastructure Using Operations Center](#)

## Viewing Alarms and Events 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 Prime Infrastructure 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 “Performing a Quick Filter”.
- 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 Prime Infrastructure instances. You can also acknowledge, annotate, and delete alarms; that action is duplicated on the respective Prime Infrastructure instance.

### Related Topics

- [Performing a Quick Filter](#)
- [Search Methods](#)
- [Monitoring Your Network Using Operations Center](#)
- [Viewing Clients and Users Using Operations Center](#)

## Viewing Clients and Users 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 Prime Infrastructure 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. By clicking a client's corresponding radio button, you can access even more detailed information for that client at the bottom of the Clients and Users page. 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 “Performing a Quick Filter”.
- Search for a particular client. For details, see the related topic “Search Methods”.

### Related Topics

- [Performing a Quick Filter](#)
- [Search Methods](#)
- [Monitoring Your Network Using Operations Center](#)

## Cross-Launching Prime Infrastructure Using Operations Center

A common element in the Operations Center's four Monitor pages is the Prime Server column, which indicates the Prime Infrastructure server associated with any given device, alarm, event, client, or user. By clicking the corresponding link in any of the Monitor pages or the Server Status summary, you can launch a separate Prime Infrastructure instance to perform the necessary management tasks without closing the Operations Center.

### Related Topics

- [Monitoring Your Network Using Operations Center](#)

## Running Reports With Operations Center

In addition to the Operations Center dashboards and monitor pages, Operations Center provides a subset of Prime Infrastructure reports that combine network management and performance data across all the managed instances of Prime Infrastructure. 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 Prime Infrastructure 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 Prime Infrastructure 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 “Using Virtual Domains With Operations Center” in Related Topics.

Except for aggregating data across managed instances, Operations Center reports generation works the same way as in Prime Infrastructure. For more information about Prime Infrastructure reports and how to generate them, see “Managing Reports” in Related Topics.

#### Related Topics

- [Generating Reports](#)
- [Viewing the Operations Center Dashboards](#)
- [Monitoring Your Network Using Operations Center](#)
- [Using Virtual Domains With Operations Center](#)
- [Viewing Alarms and Events Using Operations Center](#)
- [Viewing Clients and Users Using Operations Center](#)
- [Operations Center FAQs](#)

## Operations Center FAQs

- Q.** What are the system requirements for Operations Center, and what OVA size should I use?
- A.** Operations Center requires the Standard OVA to manage up to 100 virtual domains. To manage more virtual domains, you must use a bigger OVA. See the full list of system requirements in the [Scaling for Operations Center](#) section in the [Cisco Prime Infrastructure 3.1 Quick Start Guide](#).
- Q.** How does the licensing work in Operations Center?
- A.** Prior to release 3.1, there were two license files that had to be applied in Operations Center (a *base* license and an *incremental* license). Starting with version 3.1, you apply a single license file to transform the Prime Infrastructure instance to an Operations Center instance and to indicate how many instances you can manage in Operations Center.
- After applying the license, log out and log back in for the changes to take affect.
- Q.** What communication ports must be opened between Operations Center and its managed instances?
- A.** You must enable Single Sign On (SSO) when you set up Operations Center. The SSO server and its managed instances are configured as the SSO client. SSO requires two ports to be open:
- 443 (HTTPS)
  - 8082 (used for setting up SSL certificate).
- Q.** Why does the number of alarms in the Alarm Summary and the total alarm count differ in Operations Center and the managed instances?
- A.** You might have customized settings differently for the Operations Center and the managed instances. Check the following on both Operations Center and the managed instances to ensure they have the same settings:
- User Preferences—Click your login name in the top right-hand corner, then click **My Preferences**. Make sure the settings under Alarms are the same in Operations Center and the managed instances.

- System Settings—Choose **Administration > Settings > System Settings**, then click **Alarms and Events**. Make sure that all the settings under Alarm Display Options are the same in Operations Center and the managed instances. By default, Prime Infrastructure and Operations Center hide acknowledged and cleared alarms, but you can choose to display them.

For more information, see [Customizing the Alarm Summary](#) in the *Cisco Prime Infrastructure 3.1 User Guide*.

- Q.** Why does the number of aggregated events and syslogs differ in Operations Center and managed instances?
- A.** Events and syslogs are constantly changing on managed instances. (If you click the **Refresh** button every 5 seconds, you can see the constant changes.) Because of the time it takes to update the corresponding information in Operations Center, these two numbers might not always be in sync. You should not compare the number displayed in the individual managed instances with the number displayed in Operations Center. The information displayed in the managed instances is more current than that displayed in the Operations Center.
- Q.** Why can't I go directly to the Events page?
- A.** We will fix this issue in a future release. (See [CSCui47865](#) for details.) To workaround this issue, on the Alarms page that is displayed, click the **Events** tab, then click **Refresh** to view the events data.
- Q.** Why does cross launching from Network Devices page, in some cases, display multiple devices instead of filtering on the selected device?
- A.** This is known limitation within Operations Center and is likely due to the similarity of device names on your managed instances.
- Q.** Why are there discrepancies in the report values generated between Operations Center and Prime Infrastructure ?
- A.** Because of the differences in how the values are generated for Operations Center and Prime Infrastructure , minor discrepancies are expected. Prime Infrastructure generates values using fractional values. Operations Center aggregates these values using a set of rounded numbers. See [CSCui29279](#) for details.
- Q.** Does Operations Center support third-party devices?
- A.** No. Because third-party devices are queried directly, there is not a corresponding NBI API to retrieve the data.
- Q.** From the Network Device Summary dashlet, why can't I cross-launch to my third party APs?
- A.** This is a known issue. None of the third party APs are displayed.
- Q.** How do you enable GZip compression for reports?
- A.** To enable GZip compression in Operations Center go to **Administration > Settings > System Settings > General > Report**, click **Enable Compression**, then click **Save**.
- Q.** In Operations Center, why am I unable to cross-launch a managed instance and filter on my syslogs from the **Monitor > Monitoring Tools > Alarms and Events > Syslogs** tab?
- A.** Prime Infrastructure does not support filtering by instanceId for Syslogs. Therefore, Operations Center does not support filtering on Syslogs when cross launching to a managed instance.

- Q.** Why do Virtual Domains work incorrectly in Firefox version ESR 17.0.6?
- A.** You need to change the default character encoding scheme to Western(ISO-8859-1). By default, the character encoding is set to UTF8 in Firefox ESR 17.0.6. After you change the setting, refresh the browser.
- Q.** Why does the Current Associated Wired Clients table look different in Operations Center and Prime Infrastructure ?
- A.** The Operations Center table has fixed columns, while Prime Infrastructure has customizable columns.
- Q.** Why is there a discrepancy in the VLAN ID and Association ID on the Clients and Users page between Operations Center and the managed instances?
- A.** This data changes frequently. As a result, the managed instances data may have already changed before the Operations Center was updated.
- Q.** Why is there a discrepancy in CPU Utilization and Memory Utilization fields for Autonomous AP on the device details page between Operations Center and the managed instances?
- A.** These fields change very quickly. Operations Center collects, aggregates, and then displays the data from the managed instances. Because of the time it takes to update this information in Operations Center, the data might not always be in sync. The information displayed in the managed instances is more current than that displayed in the Operations Center.
- Q.** Why does the network devices count (between Operations Center and managed instances) shown in the Network Devices table not match when someone tries to add them to a virtual domain?
- A.** In Prime Infrastructure , when you are adding a device to a virtual domain, you see all devices, even devices that cannot be added due to an incomplete inventory collection. In Operations Center, devices that cannot be added to a virtual domain are not displayed. See [CSCuu41360](#) for details.
- Q.** Why do some managed instances keep going into *Unreachable* state?
- A.** This might occur if you initiate multiple concurrent cross-launches to the managed instances. This creates many SSO sessions for the managed instances, which might cause a session limit error and make the managed instance unreachable in Operations Center.
- Q.** Does Operations Center support High Availability (HA)?
- A.** HA is supported in both aspects:
- HA on managed instances of Prime Infrastructure : Any and all of the Prime Infrastructure instances that you manage using Operations Center can have HA set up. Operations Center automatically detects the secondary server for each Prime Infrastructure instance that has HA set up. If the primary server in such setups goes down, Operations Center will automatically re-route all calls to the secondary server. It will also indicate the status of these instances by marking them as “Backup” on the Operations Center Manage & Monitor Servers page.
  - HA on the Operations Center instance: This is supported starting with version 3.1. You can specify a secondary server for Operations Center, which will be automatically activated when the primary instance goes down. Follow these steps to enable HA on Operations Center (for more details on each of these steps, see the [Setting Up Operations Center](#)):
    1. Set up two servers. These will serve as the primary and secondary HA Operations Center servers.

2. Enable Operations Center on the primary server and configure a Virtual IP on the primary server.
3. Log out from the primary Operations Center server and then log back in using the Virtual IP you configured.
4. Configure the primary Operations Center server as the primary SSO server, using the Virtual IP.
5. On each of your managed Prime Infrastructure instances, specify the primary Operations Center server as the primary SSO server, using the Virtual IP.
6. Add each of your managed Prime Infrastructure instances to the Operations Center server. Operations Center will fetch all data from the instances.
7. Shut down the primary Operations Center server and log in to the secondary server. The secondary server will operate as an Operations Center server and will fetch all data from the managed instances.

**Q.** What are the system requirements for Operations Center? Which size OVA should I use?

**A.** As of version 3.1, Operations Center requires (at a minimum) the Express OVA size with at least the following system specifications: 4 CPUs, 12GB Memory, 300GB Hard Disk. With this setup, Operations Center can manage up to 100 Virtual Domains, and up to 10 managed instances. You must choose a larger OVA to manage more virtual domains. For Operations Center to work properly, your network must support at least 250 kbps of bandwidth and latency of no more than 5 milliseconds between the Operations Center server and the managed instances.

**A.** How do you disable auto-logout in Operations Center?

**A.** To disable auto log out:

1. Click your login name in the top right-hand corner, then click **My Preferences**.
2. Under User Idle Timeout, uncheck **Logout idle user**, then click **Save**.
3. Choose **Administration > Settings > System Settings > Server**, then under Global Idle Timeout, uncheck **Logout all idle users**, then click **Save**.

**Q.** How do you set up Single-Sign-On (SSO) in Operations Center?

**A.** You must set up Single-Sign-On (SSO) so that Operations Center acts as the SSO server and the managed instances act as the SSO clients.

As of version 3.1, SSO can be configured automatically. Once you have configured SSO on the Operations Center server and applied the Operations Center license file, you can choose to configure SSO automatically on each managed instance as you add it using the Manage & Monitor Servers page, by checking the “Enable Single-Sign-On Automatically” checkbox.

If need be, you can also set up SSO manually, as explained in the following steps:

**In Operations Center:**

1. Select **Administration > Users > Users, Roles & AAA**, then select **SSO Servers**.
2. Choose **Select a command > Add SSO Server**, then click **Go**.
3. Complete the required fields, then click **OK**.
4. From the left-hand menu, select **AAA Mode Settings**.
5. Click **SSO**, then click **Save**.
6. Logout of Operations Center.

**In each managed instance:**

1. Select **Administration > Users > Users, Roles & AAA**, then select **SSO Servers**.
2. Choose **Select a command > Add SSO Server**, then click **Go**.
3. Enter the IP address of the Operations Center server, then click **OK**.
4. From the left-hand menu, select **AAA Mode Settings**.
5. Click **SSO**, then click **Save**.
6. Log out of the managed instance.

To ensure that SSO is working properly, log in to Operations Center, open a new browser tab and access one of your managed instances. If you are automatically logged into your Prime Infrastructure instance without having to re-authenticate, then SSO is working as expected.

**Q.** Does Operations Center support TACACS?

**A.** Yes. To set up TACACS or another central authentication server in Operations Center, follow these steps:

1. Select **Administration > Users > Users, Roles & AAA**, then select **TACACS+ Servers** from left-hand menu
2. From the Select a command dropdown menu, select **Add TACACS+ Server**, then click **Go**.
3. Complete the required fields, then click **OK**.
4. From the left-hand menu, select **SSO Server Settings**.
5. Click **TACACS+**, then click **Save**.

**Q.** How do I avoid a single point of failure with Operations Center?

**A.** You can do this by configuring a second Prime Infrastructure instance as an SSO server. Ensure that it contains all the TACACS details (if applicable). Specify this sever as the second SSO server for all your managed instances. If your Operations Center server goes down, the Prime Infrastructure instances will reroute to this instance to authenticate users. Also, starting with version 3.1, you can set up High Availability (HA) for Operations Center itself, by specifying primary and secondary HA servers.

**Q.** What is the maximum number of supported instances in Operations Center?

**A.** Operations Center currently supports up to 10 managed instances. This is a not a hard limit. You can add more managed instances as long as your license allows for them. However, Cisco recommends that you observe the 10-instance limit for performance reasons. Operations Center must wait for responses from all its managed instances before aggregating and displaying their data. The more instances you add to Operations Center, the more data it needs to process and the slower it becomes. Adding more instances also increases the likelihood that one or more of the managed instances will serve as a bottleneck.

**Q.** How does Operations Center's license count work with respect to Prime Infrastructure instances that have a secondary High Availability (HA) server setup?

**A.** Secondary HA servers are not accounted for as part of your license count when adding your managed instances to Operations Center. In other words if your Operations Center license allows for management of three instances, that means three instances with or without HA. Hence, you will need to specify a count of "3" for your L-PI2X-OPRCTR-1 license.



- Q.** When Operations Center is managing multiple Prime Infrastructure instances, do we lose GUI or CLI access to those individual instances?
- A.** No, but remember that Operations Center acts as the Single-Sign-On (SSO) server and its managed Prime Infrastructure instances act as SSO clients. So you will only be able to login to the GUI of your Prime Infrastructure instances with credentials defined in Operations Center. You will not be able to login to any of the Prime Infrastructure instances with credentials defined locally on that instance. Operations Center does not affect CLI access to your Prime Infrastructure instances in any way.
- Q.** What is the impact to managed Prime Infrastructure instances if an Operations Center server without High Availability (HA) goes down?
- A.** If you don not have HA set up with Operations Center and your Operations Center server goes down, the individual Prime Infrastructure instances will fallback to “Local Authentication” mode and will allow you to login using their local credentials. Starting with version 3.1, Prime Infrastructure instances can also fallback to a centralized authentication server (such as TACACS) if one is specified.

