

---

## Configure Systemwide Functions

 For supported software information, click [here](#).

This article describes how to configure a number of systemwide functions on Director nodes.

---

## Configure High Availability

High availability (HA) provides a fallback option in case the active Director node goes down. HA ensures a seamless bringup of the standby Director node, thus allowing network services to continue with no disruptions.

The Director node supports the following flows for HA:

- Netconf
- Fault module supports UDP and TCP channels

For a UDP channel, syslog messages are sent to the active and standby Director nodes, but only the active node processes the alarms. You configure a remote collector for the active-standby pair. For a TCP channel, only the active Director node accepts a connection, and you configure a log collector group for the active-standby pair. Data between the active and standby Director nodes is synchronized by Postgres replication.

Any settings that you configure on the active Director node automatically extend to the standby Director node. The standby node cannot perform any action until it activates.

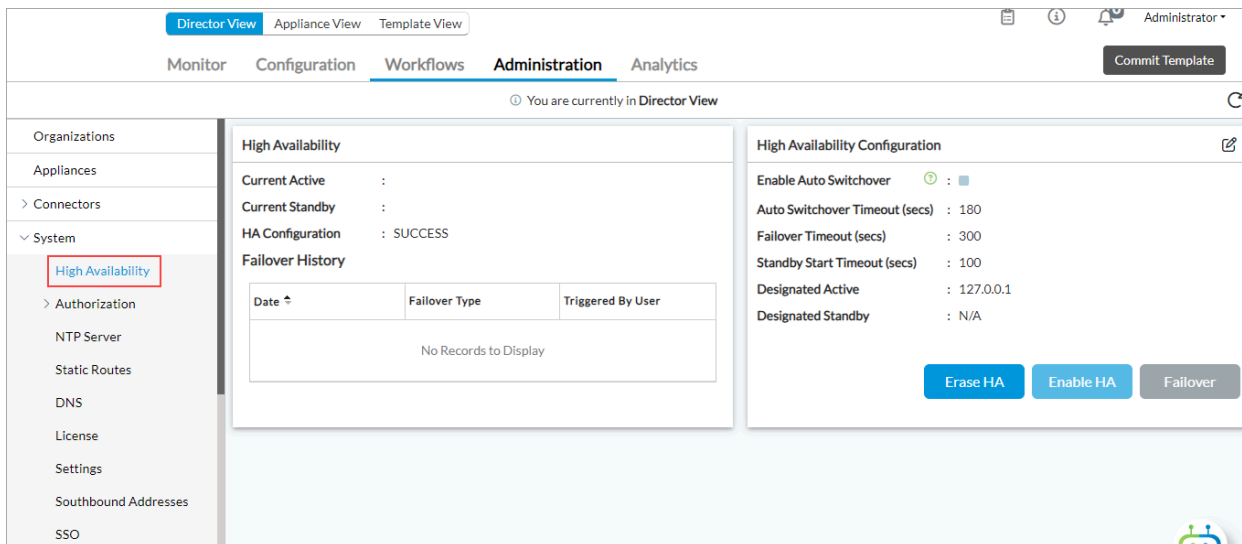
---

## View HA Settings

*For Releases 22.1.1 and later.*

To view the Director HA settings:

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > High Availability in the left menu bar. The following screen displays.



The High Availability pane displays the following read-only information about the HA components:

### High Availability

Active IP Address

: 192.168.111.232

Standby IP Address

: 192.168.111.233

HA Configuration

: SUCCESS

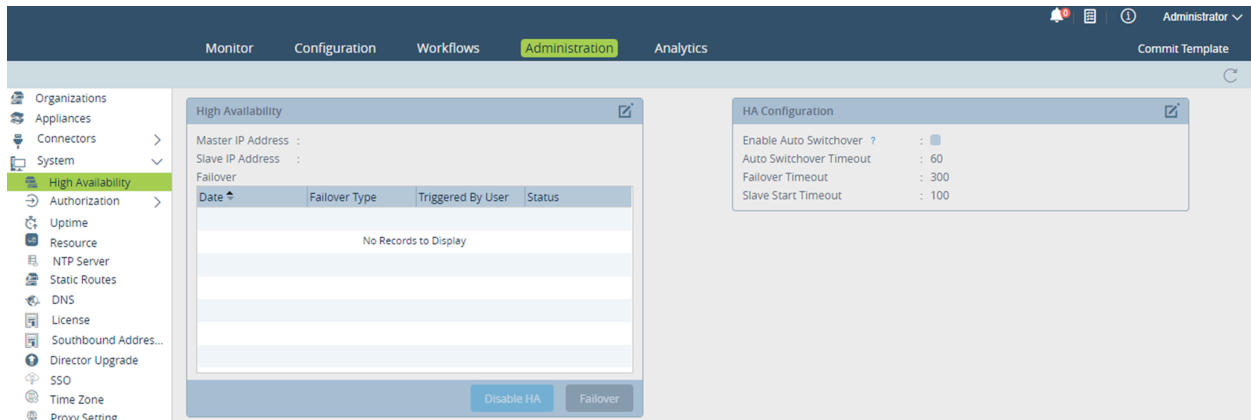
#### Failover History


Date	Failover Type	Triggered By User
No Records to Display		

## Configure HA for Director Nodes in Releases 21.2.1 and Earlier

*For Releases 21.2.1 and earlier.*

1. Install Versa Director on two hosts (virtual machines, or VMs).
2. Log in to one of the Director nodes.
3. In Director view, select the Administration tab in the top menu bar.
4. Select System > High Availability in the left menu bar.



5. In the High Availability pane, click the  Edit icon. In the High Availability popup window, enter information for the following fields.

Field	Description
Master IP Address	Enter the IP address of the active Director node.
Slave IP Address	Enter the IP address of the standby Director node.
Designated Master IP Address	Enter the IP address of the designated active Director node.
Enable Auto Switchover	Click to enable automatic switchover to the backup Director node if the active Director node goes down.

6. Click OK.

## Configure Revertive Behavior

By default, the Director HA implementation is non-revertive, which means that if the designated master is up and running after a recovery, it is not promoted to master. To change the behavior to be revertive, so that the designated master is promoted to active after a recovery, you enable automatic switchover. The designated master is then promoted to active after the automatic switchover timeout value expires.

It is recommended that you not change the HA configuration values in production deployments.

To enable revertive behavior in Releases 22.1.1 and later:

1. In the Director view, select the Administration tab in the top menu bar.
2. Select System > High Availability in the left menu bar.

The screenshot shows the Versa Director Administration interface. The top navigation bar includes tabs for Director View, Appliance View, and Template View. Below this is a secondary navigation bar with Monitor, Configuration, Workflows, Administration (selected), and Analytics. A 'Commit Template' button is visible on the right. The left sidebar shows a tree view with 'System' expanded, and 'High Availability' selected. The main content area is divided into two panels. The left panel, titled 'High Availability', shows status information: 'Current Active' (empty), 'Current Standby' (empty), 'HA Configuration' (SUCCESS), and a 'Failover History' table with columns 'Date', 'Failover Type', and 'Triggered By User'. The table is currently empty with the message 'No Records to Display'. The right panel, titled 'High Availability Configuration', contains a list of settings: 'Enable Auto Switchover' (checked), 'Auto Switchover Timeout (secs)' (180), 'Failover Timeout (secs)' (300), 'Standby Start Timeout (secs)' (100), 'Designated Active' (127.0.0.1), and 'Designated Standby' (N/A). At the bottom of this panel are three buttons: 'Erase HA', 'Enable HA', and 'Failover'.

3. In the High Availability Configuration pane, click the  Edit icon. In the Edit Configure HA popup window, enter information for the following fields.

### Edit Configure HA

☐ Enable Auto Switchover

Auto Switchover Timeout (secs)

180

Failover Timeout (secs)

300

Standby Start Timeout (secs)

100

Active IP Address \*

127.0.0.1

Standby IP Address \*

OK

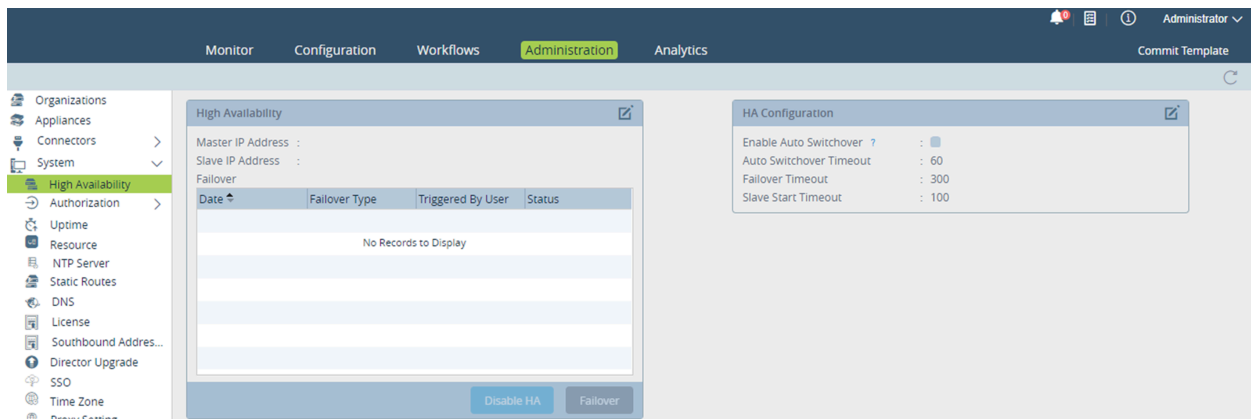
Cancel

Field	Description
Enable Auto Switchover	Click to enable the designated active Director node to promote itself to the active state after a recovery.
Auto Switchover Timeout	Enter the timeout period, in seconds, before the designated active Director node promotes itself to the active state after a recovery. <i>Range:</i> 180 through 3600 seconds (60 minutes) <i>Default:</i> 180 seconds (3 minutes)
Failover Timeout	Enter the timeout period, in seconds, before the standby Director node can promote itself to be the active Director node. <i>Range:</i> 180 through 3600 seconds (60 minutes) <i>Default:</i> 300 seconds (5 minutes)
Standby Start Timeout	Enter how long, in seconds, a non-designated standby node waits before it promotes itself to the active state. <i>Range:</i> 0 through 3600 seconds (60 minutes) <i>Default:</i> 100 seconds
Active IP Address	Enter the IP address of the active Director node. This field is disabled if HA is enabled for the Director node.
Standby IP Address	Enter the IP address of the standby Director node. This field is disabled if HA is enabled for the Director node.

4. Click OK.

To enable revertive behavior in Releases 21.2 and earlier:

1. In the Director view, select the Administration tab in the top menu bar.
2. Select System > High Availability in the left menu bar.

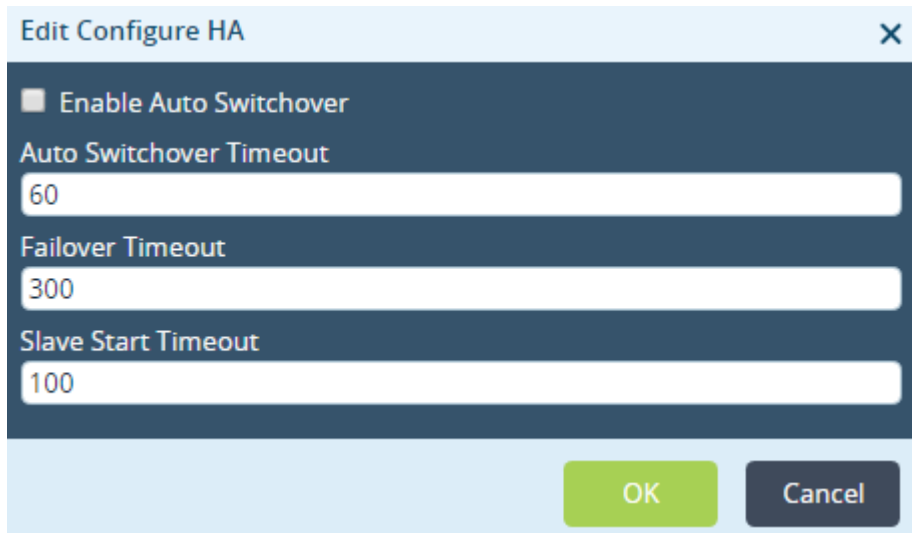


[https://docs.versa-networks.com/Management\\_and\\_Orchestration/Versa\\_Director/Configuration/Configure\\_Systemwide\\_Fun...](https://docs.versa-networks.com/Management_and_Orchestration/Versa_Director/Configuration/Configure_Systemwide_Fun...)

Updated: Thu, 24 Oct 2024 10:46:05 GMT

Copyright © 2024, Versa Networks, Inc.

3. In the HA Configuration pane, click the Edit icon. In the Edit Configure HA popup window, enter information for the following fields.



**Edit Configure HA** [X]

☐ Enable Auto Switchover

Auto Switchover Timeout  
60

Failover Timeout  
300

Slave Start Timeout  
100

OK Cancel

Field	Description
Enable Auto Switchover	Select to enable the designated active Director node to promote itself to the active state after a recovery.
Auto Switchover Timeout	Enter the timeout period, in seconds, before the designated active Director node promotes itself to the active state after a recovery. <i>Range:</i> 0 through 3600 seconds (60 minutes) <i>Default:</i> 120 seconds (2 minutes)
Failover Timeout	Enter the timeout period, in seconds, before the standby Director node can promote itself to be the active Director node. <i>Range:</i> 0 through 3600 seconds (60 minutes) <i>Default:</i> 300 seconds (5 minutes)
Standby Start Timeout	Enter how long, in seconds, a non-designated standby node waits before it promotes itself to the active state. <i>Range:</i> 0 through 3600 seconds (60 minutes) <i>Default:</i> 100 seconds
Active IP Address	Enter the IP address of the active Director node. This field is disabled if HA is enabled for the Director node.
Standby IP Address	Enter the IP address of the standby Director node. This field is disabled if HA is enabled for the Director node.

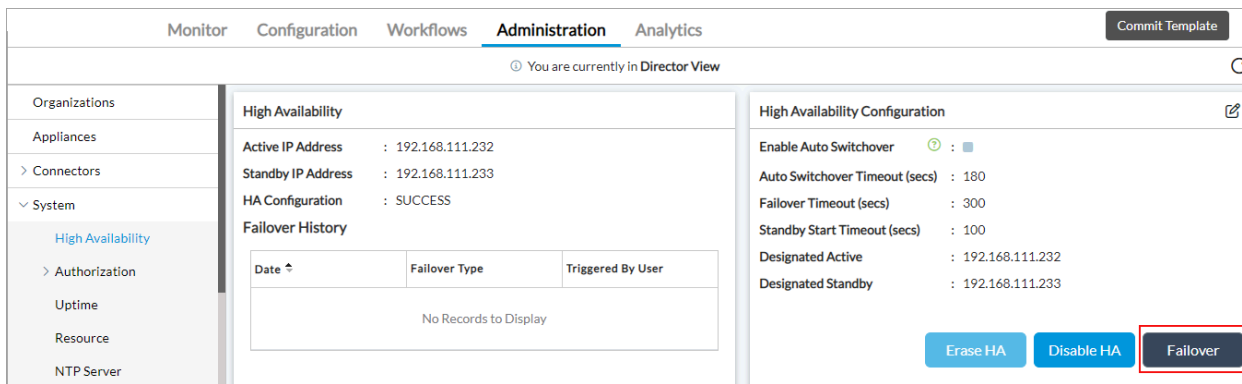
- Click OK.

## Configure HA Failover

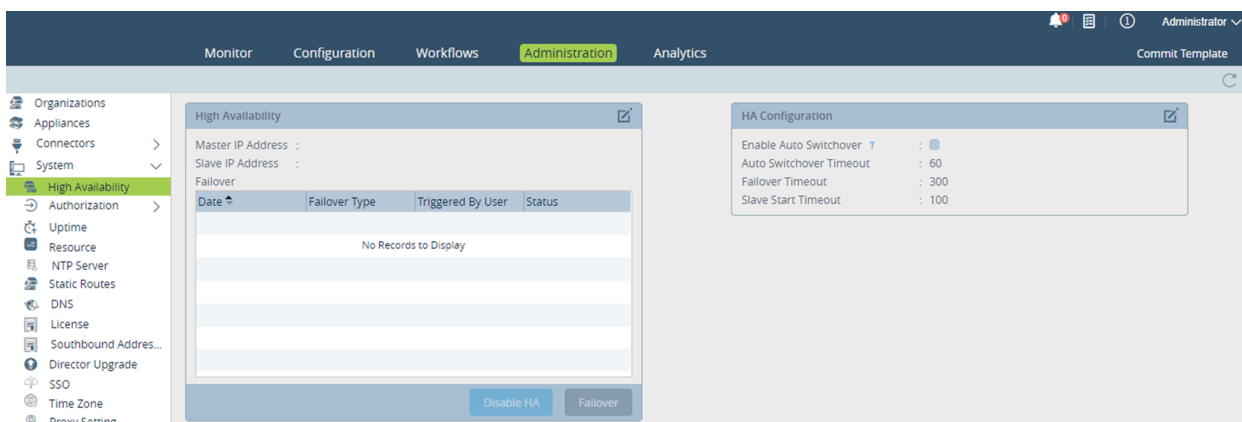
You can manually cause the Director active node to fail over. Doing this causes the active Director node to become the standby, and the standby node to become the active Director node.

For Release 22.1.1 and later, click Failover in the High Availability Configuration pane.






For 21.2 and earlier, click Failover in the High Availability pane.



For automatic failover, if the active Director node is down because of network issues or if the vnms process has stopped, the standby Director node checks the status of the active node for a maximum of 15 minutes (checking at the default interval of 300 seconds for a maximum of three times) before assuming the role as the active Director node. This behavior is not specific to the SSL certificate installation process.

In Releases 22.1.1 and later, to configure the failover timeout, click the  Edit icon in the High Availability pane, enter a value in the Failover Timeout field, and then click OK.

In Releases 21.2 and earlier, you configure the failover timeout using REST API calls or the following Director CLI commands.

To display the failover timeout, issue the following CLI command:

```
Administrator@VOAEHA2> show vnms ha-config failover-timeout
failover-timeout 300;
```

To set the failover timeout, issue the following CLI command:

Administrator @VOAEHA2% **set vnms ha-config failover-timeout seconds**

For example, to set the failover timeout to 60 seconds:

Administrator @VOAEHA2% **set vnms ha-config failover-timeout 60**  
Administrator @VOAEHA2% **commit**

---

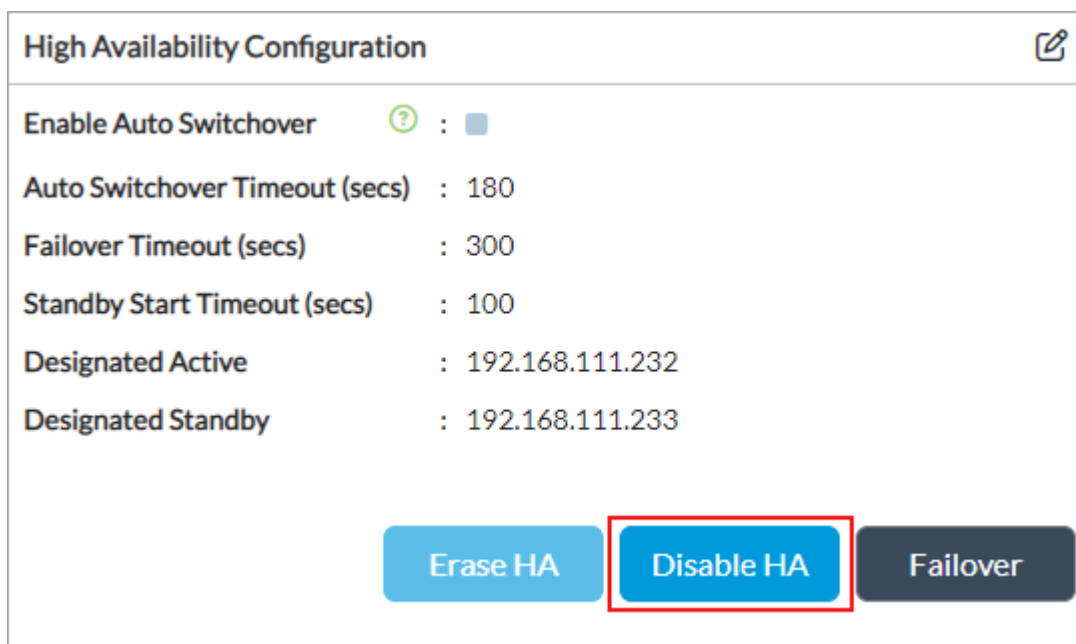
## Delete the HA Configuration

*For Releases 22.1.1 and later.*


To reconfigure the Director nodes in an HA implementation, you can delete the HA configuration.

To delete the HA configuration on a Director node on which HA is enabled:

1. In the High Availability Configuration section, click Disable HA.



The image shows a 'High Availability Configuration' pane. It has a title bar with the text 'High Availability Configuration' and an edit icon. Below the title bar, there are several configuration items: 'Enable Auto Switchover' with a green question mark icon and a checkbox; 'Auto Switchover Timeout (secs)' with a value of 180; 'Failover Timeout (secs)' with a value of 300; 'Standby Start Timeout (secs)' with a value of 100; 'Designated Active' with a value of 192.168.111.232; and 'Designated Standby' with a value of 192.168.111.233. At the bottom of the pane, there are three buttons: 'Erase HA' (light blue), 'Disable HA' (blue, highlighted with a red border), and 'Failover' (dark grey).

2. Click Erase HA.
3. To reconfigure the HA node, click the  Edit icon. The Edit Configure HA screen displays. For more information, see [Configure Revertive Behavior](#) above.

To remove the HA configuration on a Director node on which HA is not enabled, click Erase HA in the High Availability Configuration pane.

### High Availability Configuration

Enable Auto Switchover

?

:

☐

Auto Switchover Timeout (secs)

:

180

Failover Timeout (secs)

:

300

Standby Start Timeout (secs)

:

100

Designated Active

:

127.0.0.1

Designated Standby

:

N/A

Erase HA

Enable HA

Failover

---

## Configure OAuth

The Versa Director UI and Versa Analytics use the Open Authorization (OAuth) login protocol to communicate with the Director node. OAuth has two mechanisms for logging in:

- Client registration—The Director administrator registers the application client and shares the client ID and client secret with the user, who uses the information to access the application and refresh the tokens.
- Token registration—An administrator creates a client registration token and shares with the user, who uses the token to invoke a REST API call. As a result, the application self-registers and generates the client ID and secret ID to access the application and refresh the tokens.

This section describes how to register clients and tokens.

---

## Register Clients

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > Authorization > Clients in the left menu bar.

Director View
Appliance View
Template View

Administrator

Monitor
Configuration
Workflows
Administration
Analytics

Commit Template

You are currently in Director View


Organizations
Appliances
Connectors
System
High Availability
Authorization
Clients
External OAuth Ser...
NTP Server
Static Routes

Search

+ Add
Delete
Enable
Disable
Refresh Client Secret

	Name	Client ID	Expires On	Enabled	Created On	Updated On
<input type="checkbox"/>	CONCERTO	concerto		true	Tue, Aug 11 2020, 23:48	
<input type="checkbox"/>	UPGRADE-ORCHESTRAT...	upgrade-orchestrator		true	Tue, Dec 21 2021, 06:28	
<input type="checkbox"/>	VERSA-ANALYTICS	versa-analytics		true	Fri, Feb 06 2015, 23:48	
<input type="checkbox"/>	VOAE_GUI	voae_gui		true	Thu, Jan 01 2015, 23:48	
<input type="checkbox"/>	VOAE_REST	voae_rest		true	Thu, Jan 01 2015, 23:48	

Rows per page
25
Showing 1 - 5 of 5

3. Click the  Add icon. In the Add Client popup window, enter information for the following fields.

Add Client

Client

Access

Name \*

Description \*

☐ Disable

Credential

Expiry

Contacts

URL

Icon URL

Client URL

☐ Redirect URL

+

Redirect URL Not Configured

Address

☒ Any

☐

☐ Source Address

+

Source Address Not Configured

Grant Types

☐ Password

☐ Refresh Token


☐ Client Credentials

OK

Cancel

Field	Description
Name (Required)	Enter a name for the client.
Description (Required)	Enter a text description for the client.
Disable	Click to deactivate the client after you commit the configuration.

4. Select the Credential tab, and enter information for the following fields.

Field	Description
URL (Group of Fields)	
◦ Client URL	Enter the URL to invoke.
◦ Redirect URL	Enter the URL to which to redirect the user.
Address (Group of Fields)	Configure how to grant access authorization to the OAuth client.
◦ Any	Click to grant access to all IP addresses.
◦ Source Address	Click to grant access only to specific IP addresses. Click the  Add icon to add the addresses in the table.
Grant Types (Group of Fields)	Select one or more types of access to grant to an application.
◦ Client Credentials	Click to issue a client ID and secret ID.
◦ Password	Click to issue a password for access.
◦ Refresh Token	Click to issue a refresh token to generate a new token for access.

5. Select the Expiry tab, and enter information for the following fields.

Add Client

Client

Access

Name \*

Description \*

☐ Disable

Credential

Expiry

Contacts

Client Expires On

YYYY/MM/DD HH:mm:ss

Client Secret Expires On

YYYY/MM/DD HH:mm:ss

OK

Cancel

Field	Description
Client Expires On	Enter the expiration date and time for the client ID.
Client Secret Expires On	Enter the expiration date and time for the secret ID.

- Select the Contacts tab, and enter information for the following fields.

Add Client

Client

Access

Name \*

Description \*

☐ Disable

Credential

|

Expiry


|

Contacts

Client Details

<

>

Email \* 



Phone \*

+

No Contacts Added

OK

Cancel

Field	Description
Email (Required)	Enter the email address for the client contact.
Phone (Required)	Enter the telephone number for the client contact.
 Add icon	Click the  Add icon to add the contact information.

7. Select the Access tab, and enter information for the following fields.



Add Client
×

Client
Access

Max Tokens per User \*

Token Validity (seconds) \*

Max Access Tokens

Refresh Token Validity (seconds) \*

Software Identification

Software Version

OK

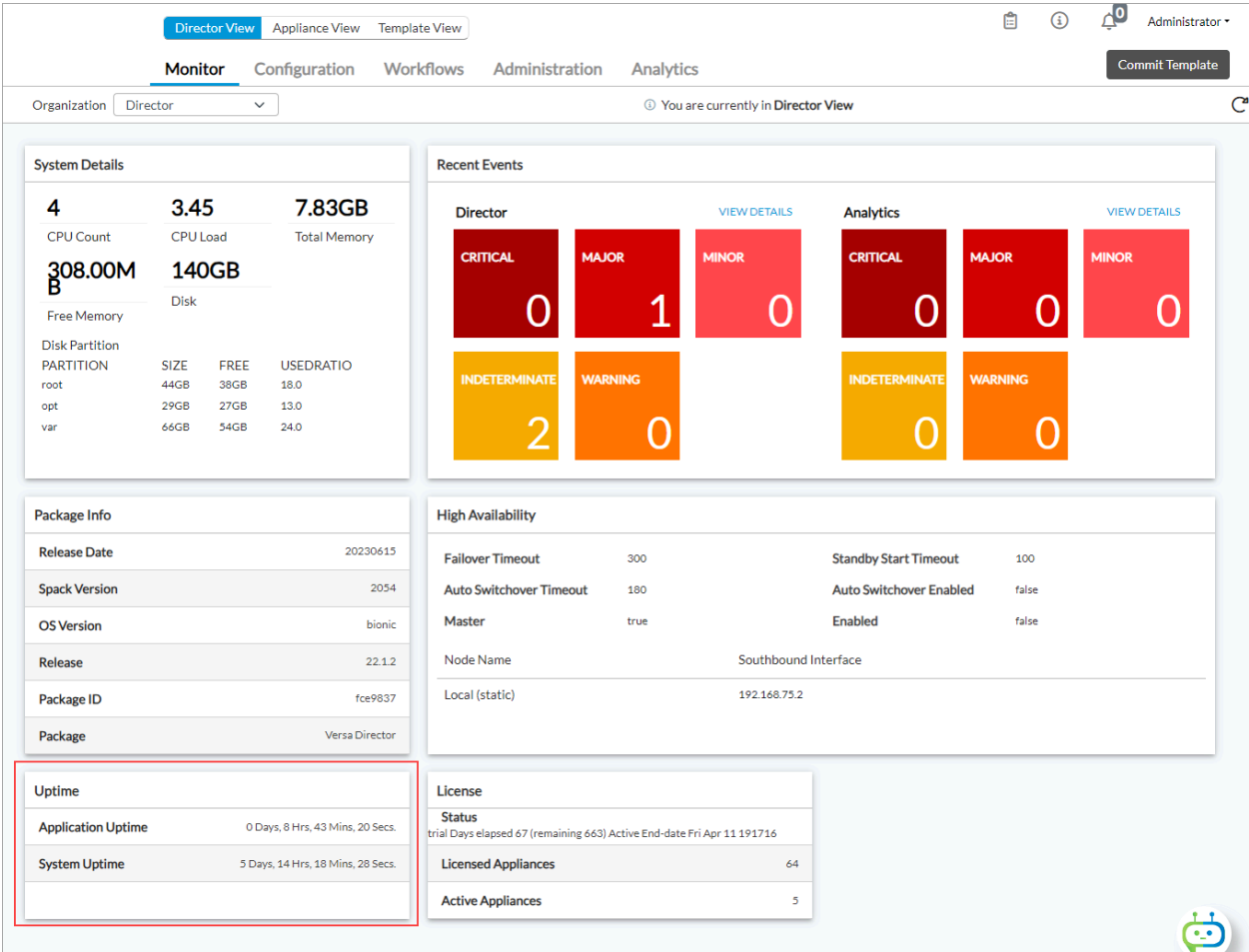
Cancel

Field	Description
Maximum Tokens per User (Required)	Enter the maximum number of tokens to allocate to each user.
Token Validity (Required)	Enter how long the token is valid, in seconds.
Maximum Access Tokens	Enter the maximum number of access tokens to allocate to a client. You can assign any number of tokens to a user to access applications or APIs. For example, for a user to access five applications, allocate five access tokens.
Refresh Token Validity (Required)	Enter how long the refresh token is valid, in seconds. When a token expires, it has to be refreshed using a refresh token, which generates a new access token for the client.
Software Identification	Enter the application identifier.
Software Version	Enter the application version.

8. Click OK.

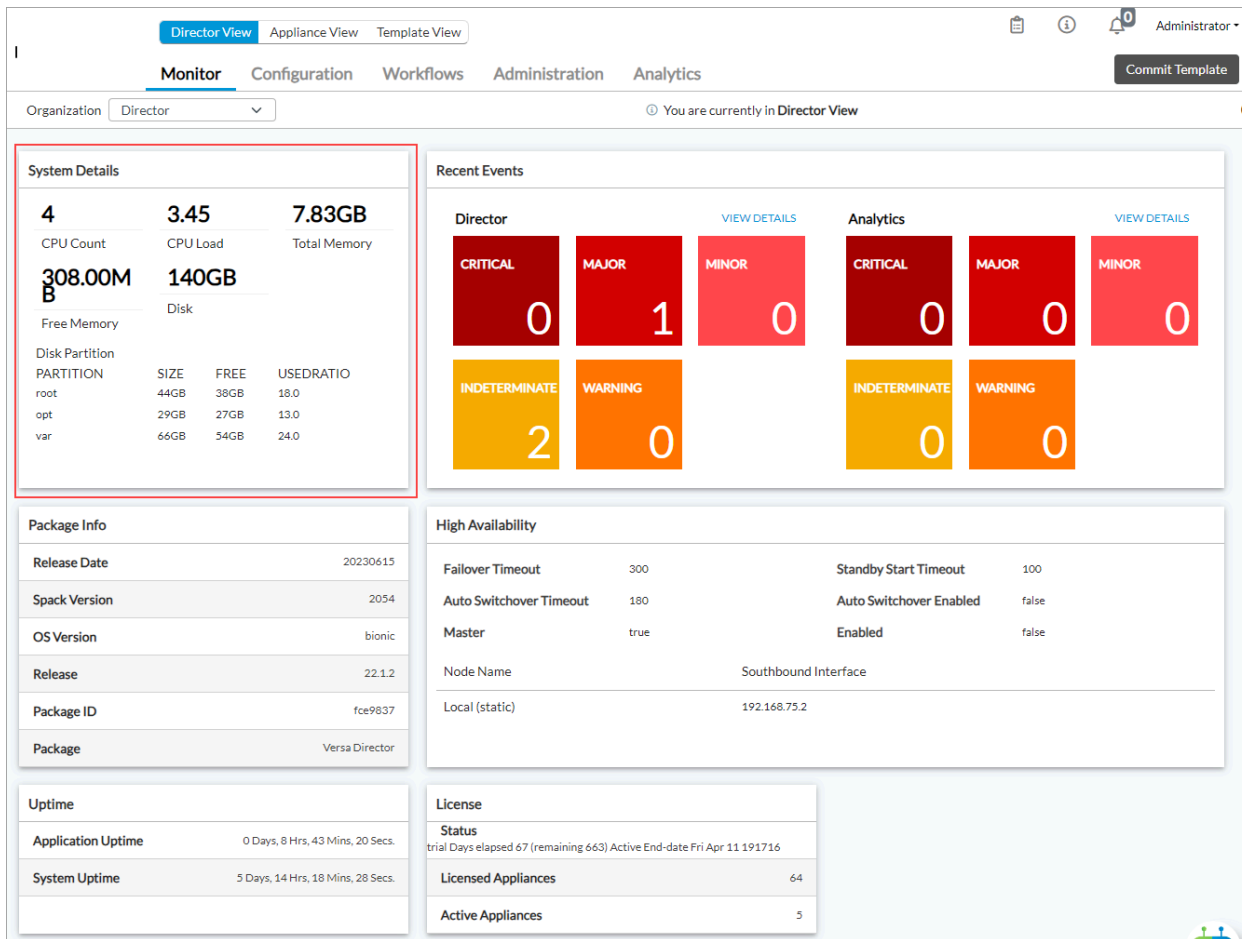
# View System Uptime

In Director view, select the Monitor tab in the top menu bar to view the system uptime and application uptime in the monitor dashboard.



# View System Resources

In Director view, select the Monitor tab in the top menu bar to view the system details usage, including memory usage, CPU load, and disk usage in the monitor dashboard.



## Configure an NTP Server

The Network Time Protocol (NTP) synchronizes clock times on the computers in a network. NTP synchronizes computer clock times to within a few milliseconds of Coordinated Universal Time (UTC). To use NTP, you configure an NTP server in a network.

For Releases 22.1.4 and later, you can configure authentication for NTP by creating an authentication key, using either MD5 or SHA1.

## Add an NTP Server

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > NTP > Server in the left menu bar.

VERSA NETWORKS

Director View | Appliance View | Template View

Monitor | Configuration | Workflows | **Administration** | Analytics

You are currently in Director View

Search

Organizations

Appliances

> Connectors

System

High Availability

> Authorization

NTP

Server

Key

Static Routes

DNS

Search

+ Add | Delete | [icon]

Servers	Version	Iburst
time.google.com	4	Disabled

Rows per page: 25 | Showing 1 - 1 of 1

- Click the **+** Add icon. In the Add NTP Server popup window, enter information for the following fields.

Add NTP Servers
✕

Server \*

Version
▼

☐ Iburst

Key
▼

OK
Cancel

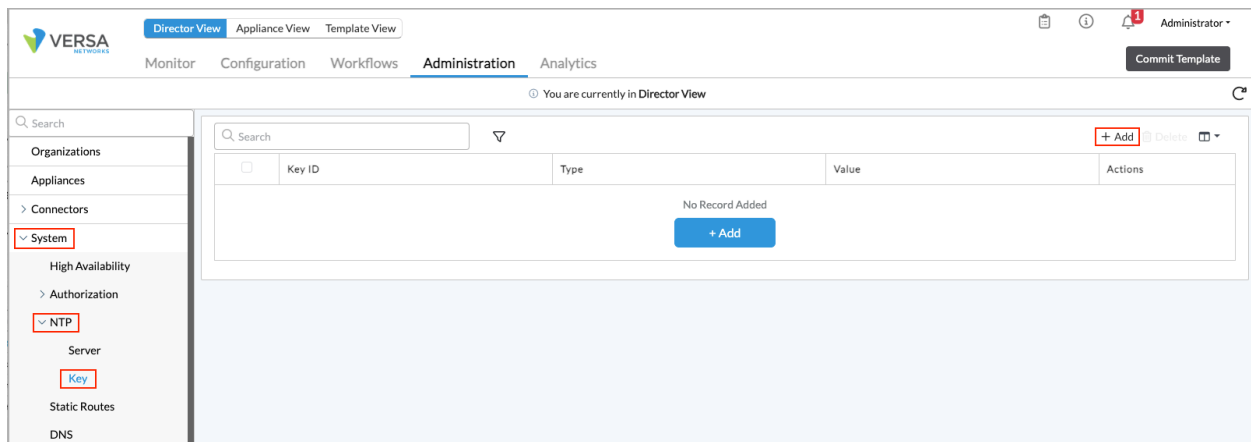
Field	Description
Server (Required)	Enter a name for the server.
Version	Enter the version NTP running on the server.
iburst	Click to enable iburst on the server. Using iburst improves the time required for initial synchronization. With iburst, when the NTP server is unreachable, a burst of eight packets is sent instead of the usual one packet.
Key	(For Release 22.1.4 and later.) Select an authentication key. For more information, see <a href="#">Create an NTP Authentication Key</a> , below.

- Click OK.

## Create an NTP Authentication Key

*For Releases 22.1.4 and later.*

- In Director view, select the Administration tab in the top menu bar.
- Select System > NTP > Key in the left menu bar. In Releases 22.1.3 and earlier, the navigation path in the left menu bar is Administration > System > NTP Server.



- Click the **+** Add icon. In the Add Create NTP Key popup window, enter information for the following fields.

Create NTP Key

Key ID \*

Type \*

---Please Select---

Value \*

OK

Cancel

Field	Description
Key ID (Required)	Enter an ID number for the NTP key. <i>Range:</i> 1 through 65535. <i>Default:</i> None
Type (Required)	Select an authentication type: <ul style="list-style-type: none"> <li>MD5</li> <li>SHA1</li> </ul>
Value (Required)	Enter a password for the NTP key.

4. Click OK.

## Configure Static Routes

Static routes are fixed and do not change, even if the network is changed or reconfigured. They are useful when dynamic routing fails.

To configure a static route:

[https://docs.versa-networks.com/Management\\_and\\_Orchestration/Versa\\_Director/Configuration/Configure\\_Systemwide\\_Fun...](https://docs.versa-networks.com/Management_and_Orchestration/Versa_Director/Configuration/Configure_Systemwide_Fun...)

Updated: Thu, 24 Oct 2024 10:46:05 GMT

Copyright © 2024, Versa Networks, Inc.

1. In the Director view, select the Administration tab in the top menu bar.
2. Select System > Static Routes in the left menu bar.

	Destination Prefix	Nexthop IP Address
<input type="checkbox"/>	10.0.30.0/24	192.168.75.1
<input type="checkbox"/>	10.0.0.0/21	192.168.75.1
<input type="checkbox"/>	10.1.30.0/24	192.168.75.1
<input type="checkbox"/>	10.0.1.0/24	192.168.75.1
<input type="checkbox"/>	10.0.33.0/24	192.168.75.1
<input type="checkbox"/>	10.0.65.0/24	192.168.75.1
<input type="checkbox"/>	10.0.62.0/24	192.168.75.1
<input type="checkbox"/>	10.1.62.0/24	192.168.75.1
<input type="checkbox"/>	10.1.64.0/24	192.168.75.1

3. For Releases 22.1.1 and later, when a standby node is available, you can add static routes to the active or standby Director node:

	Destination Prefix	Nexthop IP Address
<input type="checkbox"/>	112.0.0/24	192.168.111.236
<input type="checkbox"/>	113.0.0/24	192.168.111.236
<input type="checkbox"/>	12.1.0.0/24	192.168.111.236

4. Click the  Add icon. In the Add Static Route popup window, enter information for the following fields.

Add Static Route

Destination Prefix \*

Nexthop IP Address \*

Description

OK

Cancel

Field	Description
Destination Prefix	Enter the destination IP address of the static route.
Next-Hop IP Address	(For Releases 21.2 and earlier.) Enter the IP address of the next-hop interface to reach the destination.
Description	(For Releases 22.1.1 and later.) Enter a text description for the static route.

- Click OK.

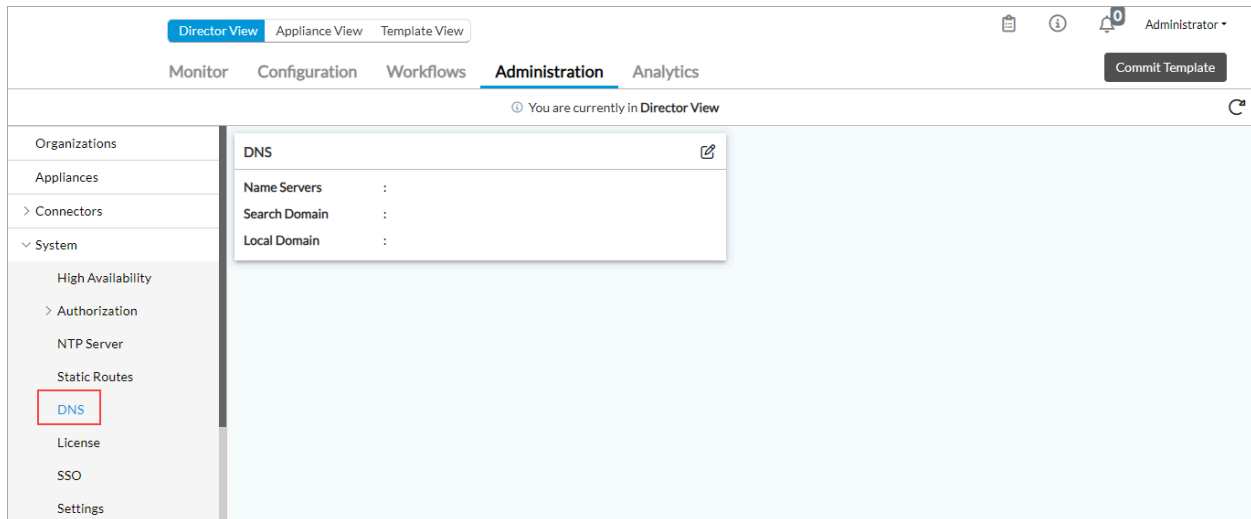
## Configure a DNS Server

A Domain Name System (DNS) server maintains a directory of domain names and translates them to Internet Protocol (IP) addresses.

To configure a DNS server:

- In Director view, select the Administration tab in the top menu bar.
- Select System > DNS in the left menu bar.





3. Click the  Edit icon. In the Edit DNS popup window, enter information for the following fields.

Edit DNS

✕

Name Servers

+

No Records to Display

Search Domain



+

No Records to Display

Local Domain

OK

Cancel

Field	Description
Name Servers	Click the  Add icon, and enter the IP address of the DNS server.
Search Domain	Click the  Add icon, and enter the IP address that the DNS service uses to resolve hostnames that are not fully qualified.
Local Domain	Enter the IP address of the local domain.

4. Click OK.

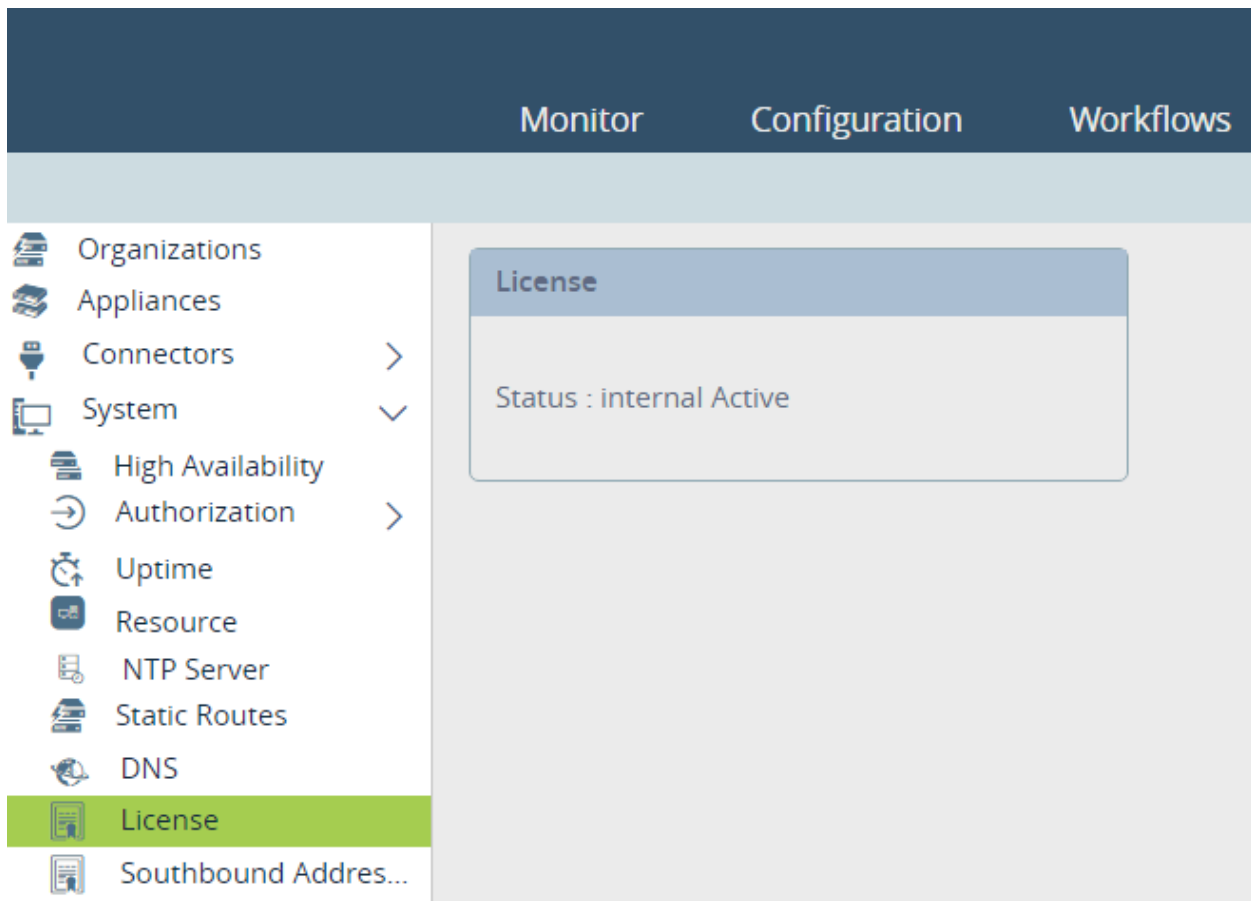
---

## Verify the Director System License Status

*For Releases 21.2 and earlier.*

To verify the license status of a Director node:

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > License in the left menu bar.

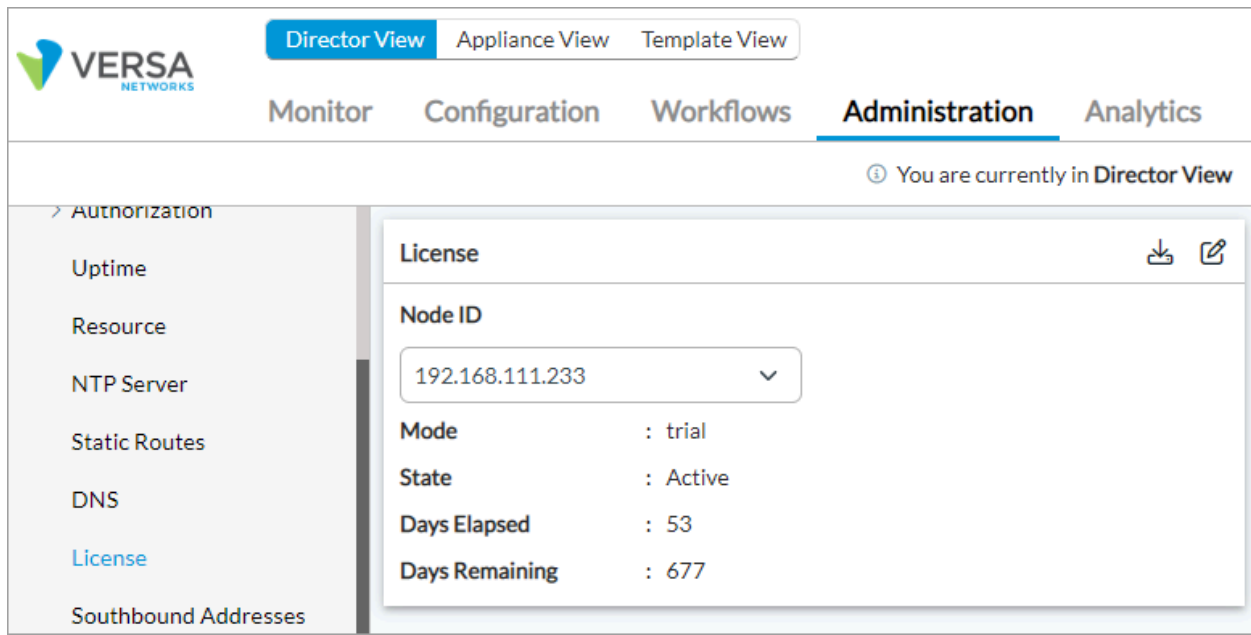




---

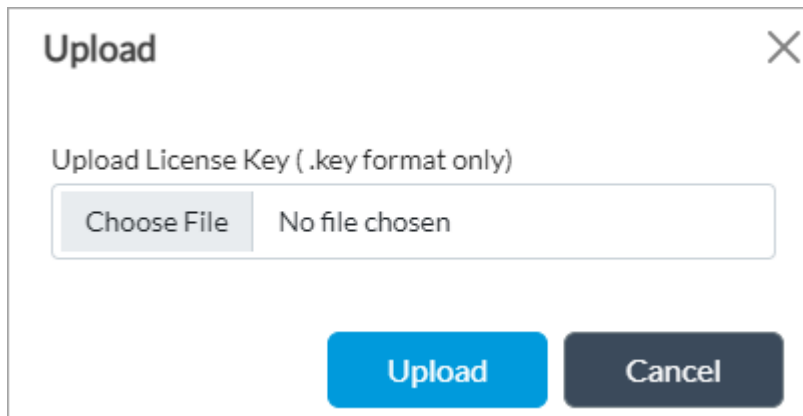
## View the Director License and Upload the License Key

*For Releases 22.1.1 and later.*

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > License in the left menu bar.
3. Select the active or standby Director node to view in the Node ID field. The License screen displays the information about the Director license. For example:



4. Click the  Download icon to download the Director node ID binary file that represents the node. You can share this file to Versa Support to request for a new license key.
5. Click the  Edit icon to upload a new license key. The license key file must be in .key format. The Upload popup window displays.



6. Click Choose File and then select the license key file from your device.
7. Click Upload.

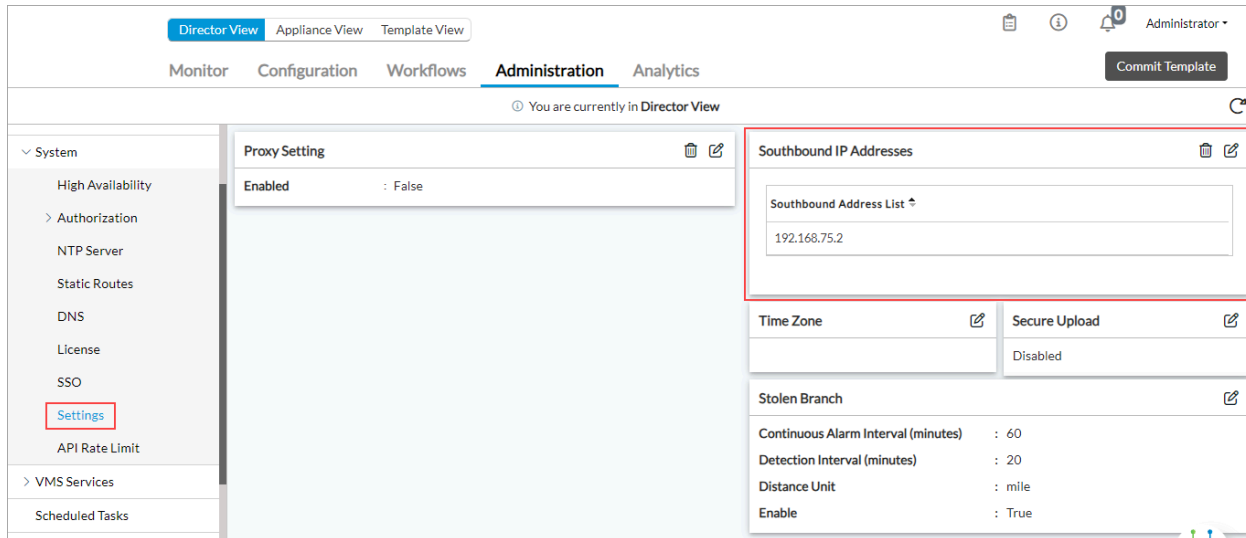
## Configure Subjugate Addresses


Subjugation allows a Director node to control selected Versa Operating System™ (VOS™) devices exclusively so that all network communication between VOS devices can happen only through that Director node. One reason to subjugate

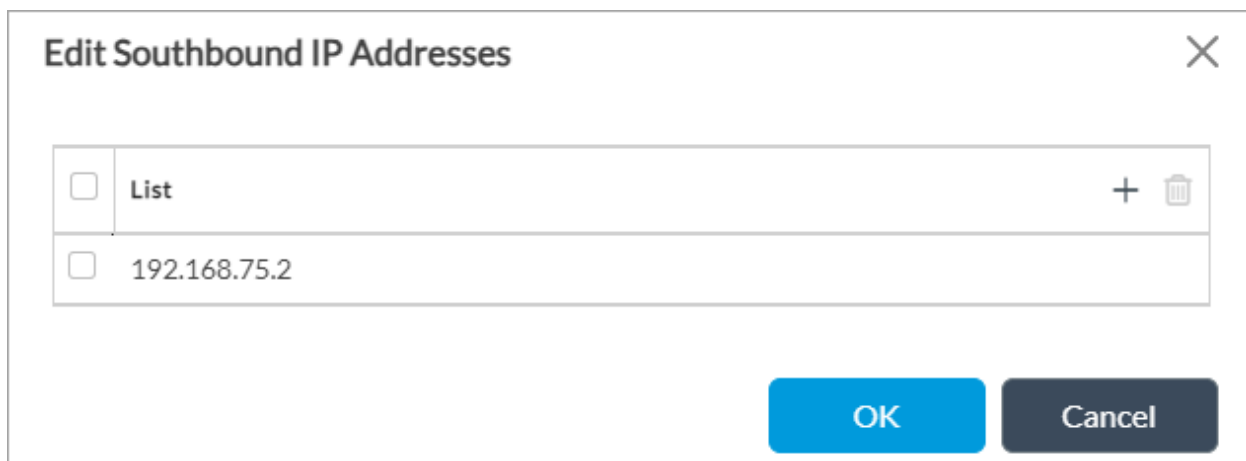
VOS devices to a particular Director node is to streamline the management of branches and network services.


To enable subjugation:

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > Settings in the left menu bar. In Releases 22.1.1 and earlier, select System > Southbound Addresses in the left menu bar.



3. In the Southbound IP Addresses pane, click the  Edit icon to add IP addresses.



4. Click the  Add icon to add an IP address.
5. Click OK.

---


## Enable the Secure Upload

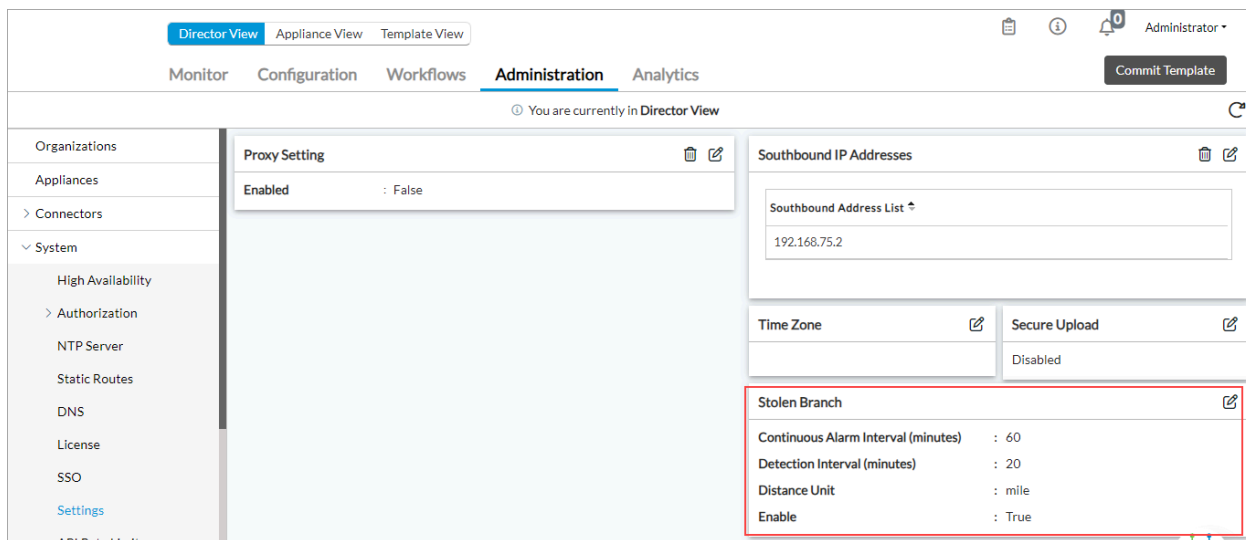
To enable signature verification for secure upload, see [Configure Signature Verification for Software Package Uploads](#).

---

## Configure Stolen Branch Settings

To edit the stolen branch settings on a Director node:

1. In Director view, select the Administration tab in the top menu bar.
2. Select System > Settings in the left menu bar. In Release 22.1.1, select System > Settings > Stolen Branch Settings in the left menu bar.
3. In the Stolen Branch pane, click the  Edit icon.



4. In the Edit Stolen Branch Setting popup window, enter information for the following fields.

Edit Stolen Branch Setting

×

Continuous Alarm Interval (minutes)

60

Detection Interval (minutes)

20

☐ Mile
☒ Kilometer

☒ Enable

OK

Cancel

Field	Description
Continuous Alarm Interval	Enter how often, in minutes, to send a continuous alarm when theft of a device is suspected.  <i>Default: 60 minutes</i>
Detection Interval	Enter how often, in minutes, to check for detect suspected stolen devices.  <i>Default: 20 minutes</i>
Distance Unit	
◦ Miles	Click to use miles for distance-based detection. This is the default.
◦ Kilometers	Click to use kilometersfor distance-based detection.
Enable	Click to enable antitheft detection.

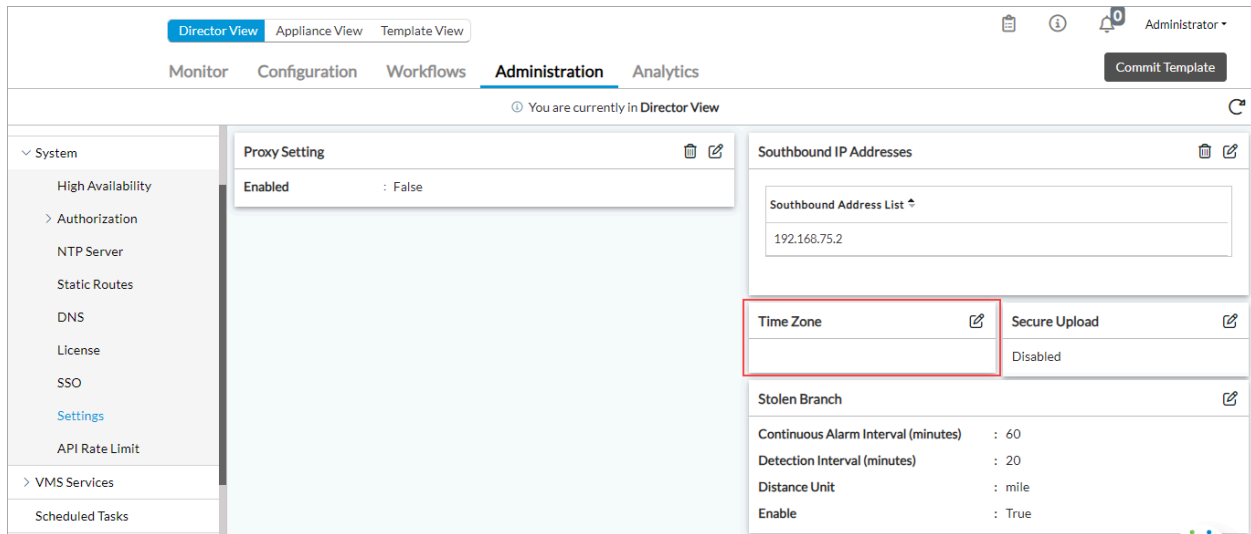
5. Click OK.


---

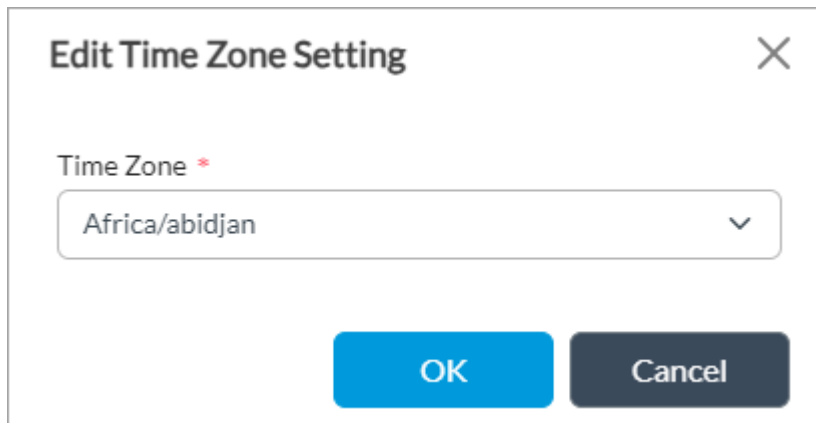
## Configure the Timezone

To configure the timezone on a Director node:

1. In the Director view, select the Administration tab in the top menu bar.
2. Select System > Settings in the left menu bar. In Releases 22.1.1 and earlier, select System > Time Zone in the left menu bar.



3. In the Timezone pane, click the  Edit icon.



4. In the Edit Time Zone Setting popup window, select the timezone in the Time Zone field.
5. Click OK.

---

## Configure Proxy Settings

*For Releases 20.2 and later.*

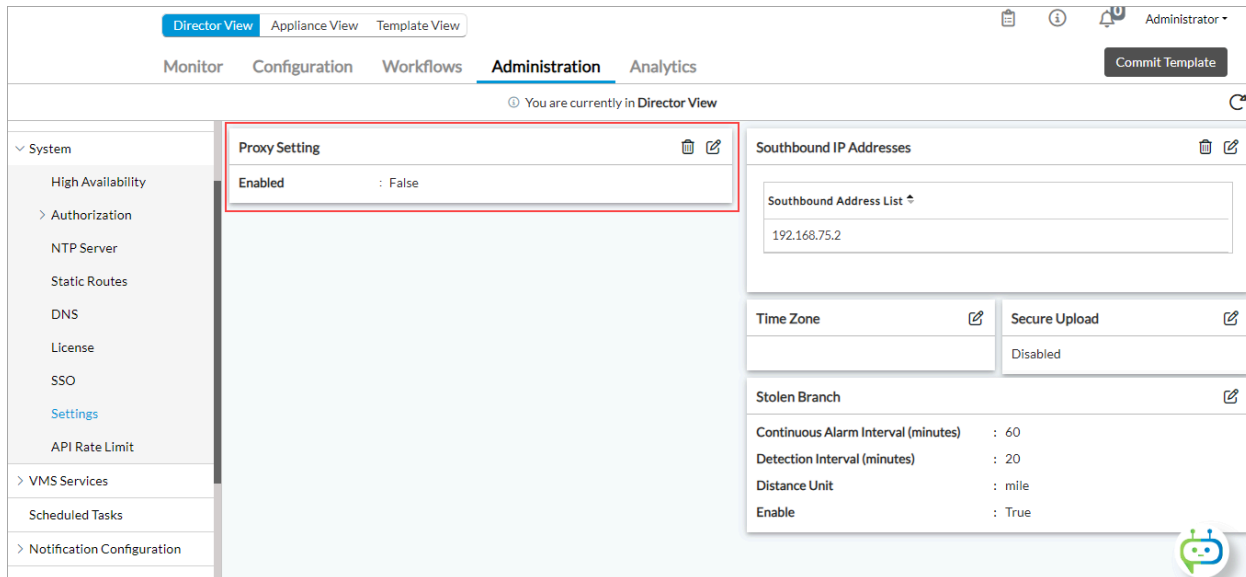
[https://docs.versa-networks.com/Management\\_and\\_Orchestration/Versa\\_Director/Configuration/Configure\\_Systemwide\\_Fun...](https://docs.versa-networks.com/Management_and_Orchestration/Versa_Director/Configuration/Configure_Systemwide_Fun...)


Updated: Thu, 24 Oct 2024 10:46:05 GMT

Copyright © 2024, Versa Networks, Inc.

To configure proxy settings for HTTP or HTTPS:

1. In the Director view, select the Administration tab in the top menu bar.
2. Select System > Settings in the left menu bar. In Releases 22.1.1 and earlier, select System > Proxy Setting in the left menu bar.



3. In the Proxy Setting pane, click the  Edit icon.
4. In the Edit Proxy Settings popup window, enter information for the following fields.

Note: For Releases 22.1.1 and later, you must add the HA IP addresses of both the active and standby Directors under Exceptions below.



Edit Proxy Setting
✕

☒ Enabled

HTTP Host

HTTP Port

HTTPS Host

HTTPS Port

Username

Password

[Change Password](#)

Exceptions

☐ Exceptions

+


🗑️

Exceptions Not Configured

OK

Cancel

Field	Description
Enabled	Click to enable proxy settings.
HTTP Host	Enter the HTTP hostname or IP address of the proxy.
HTTP Port	Enter the HTTP port number of the proxy.
HTTPS Host	Enter the HTTPS hostname or IP address of the proxy.
HTTPS Port	Enter the HTTPS port number of the proxy.
Username	Enter the login name to access the proxy.
Password	Enter the password to access the proxy.

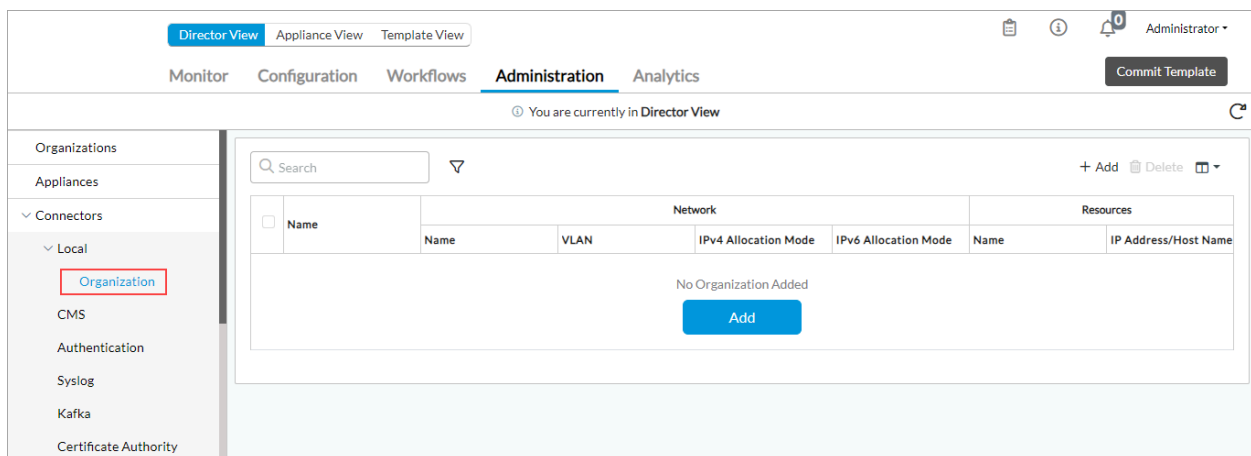
Field	Description
Exceptions	<p>Click the  Add icon to add the hostname or IP address of exceptions for the proxy.</p> <p>Note: For Releases 22.1.1 and later, you must add the HA IP addresses of both the active and standby Directors. For example:</p> <div> <div>Exceptions</div> <div> <input type="checkbox"/> Exceptions           <input type="checkbox"/> 10.40.44.199           <input type="checkbox"/> 10.40.55.195         </div> </div>

5. Click OK.

## Configure Local Organizations

To configure a local organization and associate it with a network name and VLAN IP address:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Connectors > Local > Organization in the left menu bar.



[https://docs.versa-networks.com/Management\\_and\\_Orchestration/Versa\\_Director/Configuration/Configure\\_Systemwide\\_Fun...](https://docs.versa-networks.com/Management_and_Orchestration/Versa_Director/Configuration/Configure_Systemwide_Fun...)

Updated: Thu, 24 Oct 2024 10:46:05 GMT

Copyright © 2024, Versa Networks, Inc.

3. Click the  Add icon. In the Add Organization popup window, enter information for the following fields.

Add Organization

Name \*




Description

Networks

Resources \*

Networks

<  >

Name * 	VLAN	IPv4 Allocation Mode	IPv6 Allocation Mode	
<div></div>	<div></div>	Manual 	Manual 	<div>+</div>

No network added

OK

Cancel

Field	Description
Name	Enter a name for the organization.
Description	Enter a text description for the organization.

4. Select the Networks tab, and enter information for the following fields.

Field	Description
Networks (Group of Fields)	
Name	Name of the network.
VLAN	Enter the VLAN IP address.
IPv4 Allocation Mode	Select how to allocate IPv4 addresses: <ul style="list-style-type: none"> <li>◦ DHCP</li> <li>◦ Manual</li> </ul>
IPv6 Allocation Mode	Select how to allocate IPv6 addresses: <ul style="list-style-type: none"> <li>◦ DHCP</li> <li>◦ Manual</li> </ul>

5. Select the Resources tab, and enter information for the following fields.

Add Organization

Name \*


Description

Networks

Resources \*

Resource Pool


<  >

Server Name * 	IP Address/Host Name *	
<div></div>	<div></div>	<div>+</div>

No network added

OK

Cancel

Field	Description
Resource Pool (Group of Fields)	
Server Name	Enter the names of one or more servers.
IP Address/Host Name	Displays the selected server IP address. Click  Add icon to add a server.

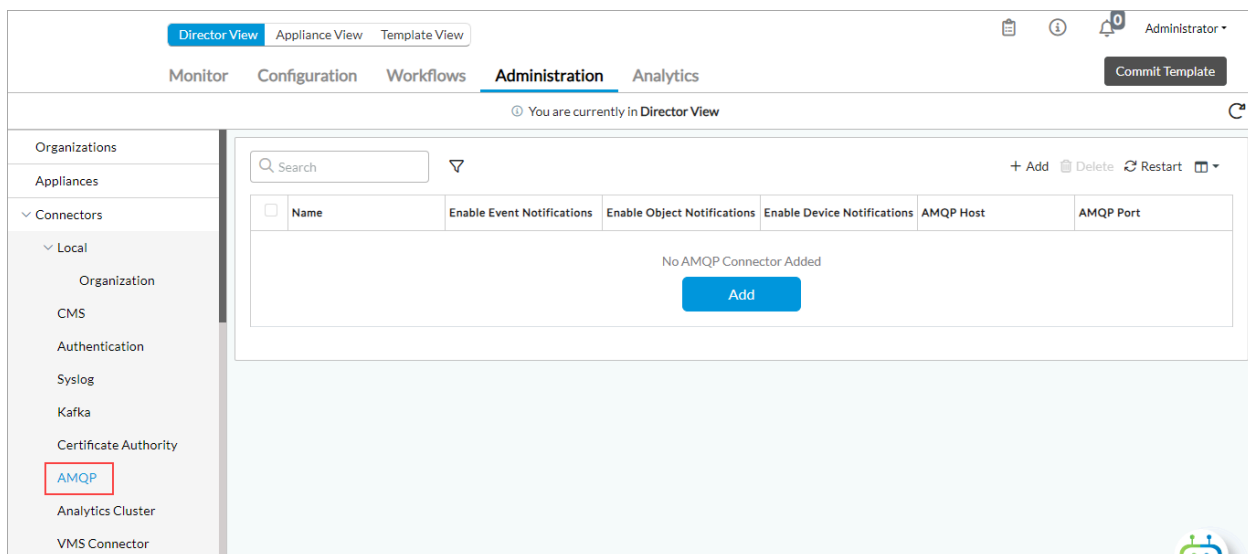
6. Click OK.


## Configure AMQP Connectors

The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for messages. The key features of AMQP are message orientation, queuing, routing, reliability, and security. The AMQP connector defines which credentials to use when connecting, and it defines all the common properties used by the inbound and outbound endpoints that use the connector.

To configure an AMQP connector:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Connectors > AMQP in the left menu bar.



3. Click the  Add icon. In the Add AMQP Connector popup window, enter information for the following fields.

Add AMQP Connector

Name \*

AMQP Host \*

AMQP Port \*

5672

Exchange \*

systemExchange

vHost \*

/

Username \*

guest

Password \*

Notification Types

☐ Enable Event Notifications

☐ Enable Object Notifications

☐ Enable Device Notifications

Email

Director Identifier Name

OK

Cancel

Field	Description
Name	Enter a name for the AMQP connector.
AMQP Host	Enter the IP address of the AMQP connector.
AMQP Port	Enter the port number that the AMQP connector uses.
Exchange	Enter the address of the exchange server.
vHost	Enter the name of the vHost server.
Username	Enter the login name to access the server.
Password	Enter the password to access the server.
Notification Types	Click to receive notifications.
Email	Enter the email ID to send AMQP server connectivity notification.
Director Identifier Name	Enter a name for the Director identifier.

4. Click OK.

---

## Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- In Release 22.1.1:
  - High Availability section in the High Availability screen is view only. Move Designated Active and Designated Standby fields to the High Availability Configuration section. Add ability to delete an HA configuration.
  - You can select the active or standby Director node to add static routes when you select Administration > Static Routes. Remove Next-Hop IP Address and Next-Hop Interface fields from the Add Static Route screen.
  - The License screen displays additional details such as mode, days elapsed, and days remaining. You can download the node ID binary file and edit the license to upload license key.
- In Release 22.1.2, add System > Settings in the left menu bar and move System > Southbound IP Addresses, System > Stolen Branch Setting, System > Secure Upload Setting, System > Timezone Setting, and System > Proxy Setting items in the left menu bar to System > Settings.
- In Release 22.1.4, you can configure authentication for NTP by creating an authentication key, using either MD5 or SHA1.

---

## Additional Information

[Configure Single Sign-On Using Director](#)

[Firewall Requirements](#)