



## L Commands

---

This chapter describes the Cisco Nexus Cloud Services Platform commands that begin with the letter L.

### line console

To enter console configuration mode, use the **line console** command. To exit console configuration mode, use the **no** form of this command.

**line console**

**no line console**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** None

---

**Command Modes** Global configuration (config)

---

**SupportedUserRoles** network-admin

---

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

---



---

**Examples** This example shows how to enter console configuration mode:

```
n1010# configure terminal
n1010(config)# line console
n1010(config-console)#
```

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## line vty

To enter line configuration mode, use the **line vty** command. To exit line configuration mode, use the **no** form of this command.

**line vty**

**no line vty**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** None

---

**Command Modes** Global configuration (config)

---

**SupportedUserRoles** network-admin

---

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

---



---

**Examples** This example shows how to enter line configuration mode:

```
n1010# configure terminal
n1010(config)# line vty
n1010(config-line)#
```

---

Related Commands	Command	Description
	<b>exit</b>	Exits a configuration mode.
	<b>line console</b>	Enters console configuration mode.

---

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## logging console

To enable logging messages to the console session, use the **logging console** command. To disable logging messages to the console session, use the **no logging console** command.

**logging console** [*severity-level*]

**no logging console**

### Syntax Description

*severity-level* Severity level at which you want messages to be logged. When you set a severity level, such as 4, then messages at that severity level and higher (0 through 4) are logged.

Severity levels are as follows:

Level	Designation	Definition
0	Emergency	System unusable
1	Alert	Immediate action needed
2	Critical	Critical condition—default level
3	Error	Error condition
4	Warning	Warning condition
5	Notification	Normal but significant condition
6	Informational	Informational message only
7	Debugging	Condition that appears during debugging only



### Note

Level 0 is the highest severity level.

### Defaults

None

### Command Modes

Global configuration (config)

### Supported User Roles

network-admin

### Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

### Examples

This example shows how to enable logging messages with a severity level of 4 (warning) or higher to the console session:

```
n1010# configure terminal
```

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

```
n1010(config)# logging console 4
n1010(config)#
```

#### Related Commands

Command	Description
<b>logging event</b>	Logs interface events.
<b>logging level</b>	Enables the logging of messages from named facilities and for specified severity levels.
<b>logging logfile</b>	Configures the log file used to store system messages.
<b>logging module</b>	Starts logging of module messages to the log file.
<b>logging server</b>	Designate and configure a remote server for logging system messages.
<b>logging timestamp</b>	Set the unit of measure for the system messages timestamp.
<b>show logging logfile</b>	Displays the contents of the log file.

*Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).*

## logging event

To log interface events, use the **logging event** command. To disable logging of events, use the **no** version of this command.

**logging event** {link-status | trunk-status} {enable | default}

**no logging event** {link-status | trunk-status} {enable | default}

### Syntax Description

<b>link-status</b>	Logs all up/down and change status messages.
<b>trunk-status</b>	Logs all trunk status messages.
<b>default</b>	Specifies that the default logging configuration is used.
<b>enable</b>	Enables interface logging to override the port level logging configuration.

### Defaults

None

### Command Modes

Global configuration (config)

### Supported User Roles

network-admin

### Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

### Examples

This example shows how to log interface events:

```
n1010# configure terminal
n1010(config)# logging event link-status default
n1010(config)#
```

### Related Commands

Command	Description
<b>logging console</b>	Enables logging messages to the console session.
<b>logging level</b>	Enables the logging of messages from named facilities and for specified severity levels.
<b>logging logfile</b>	Configures the log file used to store system messages.
<b>logging module</b>	Starts logging of module messages to the log file.
<b>logging server</b>	Designate and configure a remote server for logging system messages.
<b>logging timestamp</b>	Set the unit of measure for the system messages timestamp.
<b>show logging logfile</b>	Displays the contents of the log file.

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

## logging level

To enable the logging of messages from a named facility and for specified severity levels, use the **logging level** command. To disable the logging of messages, use the **no** form of this command.

**logging level** *facility severity-level*

**no logging level** *facility severity-level*

Syntax Description	facility	Facility name.																											
	<i>severity-level</i>	Severity level at which you want messages to be logged. When you set a severity level, for example 4, then messages at that severity level and higher (0 through 4) are logged.  Severity levels are as follows:																											
		<table border="1"> <thead> <tr> <th>Level</th> <th>Designation</th> <th>Definition</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Emergency</td> <td>System unusable</td> </tr> <tr> <td>1</td> <td>Alert</td> <td>Immediate action needed</td> </tr> <tr> <td>2</td> <td>Critical</td> <td>Critical condition—default level</td> </tr> <tr> <td>3</td> <td>Error</td> <td>Error condition</td> </tr> <tr> <td>4</td> <td>Warning</td> <td>Warning condition</td> </tr> <tr> <td>5</td> <td>Notification</td> <td>Normal but significant condition</td> </tr> <tr> <td>6</td> <td>Informational</td> <td>Informational message only</td> </tr> <tr> <td>7</td> <td>Debugging</td> <td>Condition that appears during debugging only</td> </tr> </tbody> </table>	Level	Designation	Definition	0	Emergency	System unusable	1	Alert	Immediate action needed	2	Critical	Critical condition—default level	3	Error	Error condition	4	Warning	Warning condition	5	Notification	Normal but significant condition	6	Informational	Informational message only	7	Debugging	Condition that appears during debugging only
Level	Designation	Definition																											
0	Emergency	System unusable																											
1	Alert	Immediate action needed																											
2	Critical	Critical condition—default level																											
3	Error	Error condition																											
4	Warning	Warning condition																											
5	Notification	Normal but significant condition																											
6	Informational	Informational message only																											
7	Debugging	Condition that appears during debugging only																											



### Note

Level 0 is the highest severity level.

**Defaults** None

**Command Modes** Global configuration (config)

**Supported User Roles** network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

## Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).

### Usage Guidelines

To apply the same severity level to all facilities, use the following command:

- **logging level all** *level\_number*

To list the available facilities for which messages can be logged, use the following command:

- **logging level ?**

### Examples

This example shows how to enable logging messages from the AAA facility that have a severity level of 0 through 2:

```
n1010# configure terminal
n1010(config)# logging level aaa 2
n1010(config)#
```

This example shows how to enable logging messages from the license facility with a severity level of 0 through 4 and then display the license logging configuration:

```
n1010# configure terminal
n1010(config)# logging level license 4
n1010(config)# show logging level license
Facility           Default Severity      Current Session Severity
-----
licmgr              6                      4

0(emergencies)     1(alerts)             2(critical)
3(errors)          4(warnings)           5(notifications)
6(information)     7(debugging)
```

n1010(config)#

### Related Commands

Command	Description
<b>logging console</b>	Enables logging messages to the console session.
<b>logging event</b>	Logs interface events.
<b>logging logfile</b>	Configures the log file used to store system messages.
<b>logging module</b>	Starts logging of module messages to the log file.
<b>logging server</b>	Designate and configure a remote server for logging system messages.
<b>logging timestamp</b>	Set the unit of measure for the system messages timestamp.
<b>show logging logfile</b>	Displays the contents of the log file.

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

## logging logfile

To configure the log file used to store system messages, use the **logging logfile** command. To remove a configuration, use the **no** form of this command.

**logging logfile** *logfile-name severity-level [size bytes]*

**no logging logfile** [*logfile-name severity-level [size bytes]*]

### Syntax Description

<i>logfile-name</i>	Name of the log file that stores system messages.																											
<i>severity-level</i>	Severity level at which you want messages to be logged. When you set a severity level, for example 4, then messages at that severity level and higher (0 through 4) are logged.  Severity levels are as follows:																											
	<table border="1"> <thead> <tr> <th>Level</th> <th>Designation</th> <th>Definition</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Emergency</td> <td>System unusable</td> </tr> <tr> <td>1</td> <td>Alert</td> <td>Immediate action needed</td> </tr> <tr> <td>2</td> <td>Critical</td> <td>Critical condition—default level</td> </tr> <tr> <td>3</td> <td>Error</td> <td>Error condition</td> </tr> <tr> <td>4</td> <td>Warning</td> <td>Warning condition</td> </tr> <tr> <td>5</td> <td>Notification</td> <td>Normal but significant condition</td> </tr> <tr> <td>6</td> <td>Informational</td> <td>Informational message only</td> </tr> <tr> <td>7</td> <td>Debugging</td> <td>Condition that appears during debugging only</td> </tr> </tbody> </table>	Level	Designation	Definition	0	Emergency	System unusable	1	Alert	Immediate action needed	2	Critical	Critical condition—default level	3	Error	Error condition	4	Warning	Warning condition	5	Notification	Normal but significant condition	6	Informational	Informational message only	7	Debugging	Condition that appears during debugging only
Level	Designation	Definition																										
0	Emergency	System unusable																										
1	Alert	Immediate action needed																										
2	Critical	Critical condition—default level																										
3	Error	Error condition																										
4	Warning	Warning condition																										
5	Notification	Normal but significant condition																										
6	Informational	Informational message only																										
7	Debugging	Condition that appears during debugging only																										
<i>size bytes</i>	(Optional) Specifies the log file size in bytes, from 4096 to 10485760 bytes. The default file size is 10485760 bytes.																											



### Note

Level 0 is the highest severity level.

### Defaults

None

### Command Modes

Global configuration (config)

### Supported User Roles

network-admin

### Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.



***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).*****Examples**

This example shows how to configure a log file named LogFile to store system messages and set its severity level to 4:

```
n1010# configure terminal
n1010(config)# logging logfile LogFile 4
n1010(config)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>logging console</b>	Enables logging messages to the console session.
<b>logging event</b>	Logs interface events.
<b>logging level</b>	Enables the logging of messages from named facilities and for specified severity levels.
<b>logging module</b>	Starts logging of module messages to the log file.
<b>logging server</b>	Designate and configure a remote server for logging system messages.
<b>logging timestamp</b>	Set the unit of measure for the system messages timestamp.
<b>show logging logfile</b>	Displays the contents of the log file.

**Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).**

## logging module

To start logging of module messages to the log file, use the **logging module** command. To stop module log messages, use the **no** form of this command.

**logging module** [*severity-level*]

**no logging module** [*severity-level*]

### Syntax Description

*severity-level* Severity level at which you want messages to be logged. If you do not specify a severity level, the default is used. When you set a severity level, for example 4, then messages at that severity level and higher (0 through 4) are logged.

Severity levels are as follows:

Level	Designation	Definition
0	Emergency	System unusable
1	Alert	Immediate action needed
2	Critical	Critical condition—default level
3	Error	Error condition
4	Warning	Warning condition
5	Notification	Normal but significant condition (the default)
6	Informational	Informational message only
7	Debugging	Condition that appears during debugging only



### Note

Level 0 is the highest severity level.

### Defaults

Disabled

If you start logging of module messages, and do not specify a severity, then the default, Notification (5), is used.

### Command Modes

Global configuration (config)

### Supported User Roles

network-admin

### Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).*****Examples**

This example shows how to start logging module messages to the log file at the default severity level (severity 4):

```
n1010# configure terminal
n1010(config)# logging module
n1010(config)#
```

This example shows how to stop logging module messages to the log file:

```
n1010# configure terminal
n1010(config)# no logging module
n1010#
```

**Related Commands**

Command	Description
<b>logging console</b>	Enables logging messages to the console session.
<b>logging event</b>	Logs interface events.
<b>logging level</b>	Enables the logging of messages from named facilities and for specified severity levels.
<b>logging logfile</b>	Configures the log file used to store system messages.
<b>logging server</b>	Designate and configure a remote server for logging system messages.
<b>logging timestamp</b>	Set the unit of measure for the system messages timestamp.
<b>show logging logfile</b>	Displays the contents of the log file.

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## logging server

To designate and configure a remote server for logging system messages, use the **logging server** command. Use the **no** form of this command to remove or change the configuration.

```
logging server hostname [indicator [use-vrf name [facility {auth | authpriv | cron | daemon | ftp
| kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news |
syslog | user | uucp}]]]
```

```
no logging server hostname [indicator [use-vrf name [facility {auth | authpriv | cron | daemon |
ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news |
| syslog | user | uucp}]]]
```

Syntax Description	
<i>hostname</i>	Hostname/IPv4/IPv6 address of the remote syslog server.
<i>indicator</i>	(Optional) One of the following indicators: 0–emerg, 1–alert, 2–crit, 3–err, 4–warn, 5–notif, 6–inform, 7–debug.
<b>use-vrf</b> <i>name</i>	(Optional) Specifies the VRF name. The default is management.
<b>facility</b>	(Optional) Specifies the facility to use when forwarding to the server.
<b>auth</b>	Specifies the auth facility.
<b>authpriv</b>	Specifies the authpriv facility.
<b>cron</b>	Specifies the Cron/at facility.
<b>daemon</b>	Specifies the daemon facility.
<b>ftp</b>	Specifies the file transfer system facility.
<b>kernel</b>	Specifies the kernel facility.
<b>local0</b>	Specifies the local0 facility.
<b>local1</b>	Specifies the local1 facility.
<b>local2</b>	Specifies the local2 facility.
<b>local3</b>	Specifies the local3 facility.
<b>local4</b>	Specifies the local4 facility.
<b>local5</b>	Specifies the local5 facility.
<b>local6</b>	Specifies the local6 facility.
<b>local7</b>	Specifies the local7 facility.
<b>lpr</b>	Specifies the lpr facility.
<b>mail</b>	Specifies the mail facility.
<b>news</b>	Specifies the USENET news facility.
<b>syslog</b>	Specifies the syslog facility.
<b>user</b>	Specifies the user facility.
<b>uucp</b>	Specifies the UNIX-to-UNIX copy system facility.

**Defaults** None

**Command Modes** Global configuration (config)

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

**SupportedUserRoles** network-admin

### Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

### Examples

This example shows how to configure a remote syslog server at a specified IPv4 address using the default outgoing facility:

```
n1010# configure terminal
n1010(config)# logging server 172.28.254.253
n1010(config)#
```

This example shows how to configure a remote syslog server at a specified host name with severity level 5 or higher:

```
n1010# configure terminal
n1010(config)# logging server syslogA 5
n1010(config)#
```

### Related Commands

Command	Description
<b>logging console</b>	Enables logging messages to the console session.
<b>logging event</b>	Logs interface events.
<b>logging level</b>	Enables the logging of messages from named facilities and for specified severity levels.
<b>logging logfile</b>	Configures the log file used to store system messages.
<b>logging module</b>	Starts logging of module messages to the log file.
<b>logging timestamp</b>	Set the unit of measure for the system messages timestamp.
<b>show logging logfile</b>	Displays the contents of the log file.

*Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).*

## logging timestamp

To set the unit of measure for the system message time stamp, use the **logging timestamp** command. To restore the default unit of measure, use the **no** form of this command.

**logging timestamp** {microseconds | milliseconds | seconds}

**no logging timestamp** {microseconds | milliseconds | seconds}

Syntax Description	microseconds	Specifies the time stamp in microseconds.
	milliseconds	Specifies the time stamp in milliseconds.
	seconds	Specifies the time stamp in seconds (default).

**Defaults** Seconds

**Command Modes** Global configuration (config)

**SupportedUserRoles** network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

**Examples** This example shows how to set microseconds as the unit of measure for the system message time stamp:

```
n1010# configure terminal
n1010(config)# logging timestamp microseconds
n1010(config)#
```

Related Commands	Command	Description
	<b>logging console</b>	Enables logging messages to the console session.
	<b>logging event</b>	Logs interface events.
	<b>logging level</b>	Enables the logging of messages from named facilities and for specified severity levels.
	<b>logging logfile</b>	Configures the log file used to store system messages.
	<b>logging module</b>	Starts logging of module messages to the log file.
	<b>logging server</b>	Designate and configure a remote server for logging system messages.
	<b>show logging logfile</b>	Displays the contents of the log file.

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

## login virtual-service-blade

To log in to a Virtual Service Blade (VSB), use the **login virtual-service-blade** command.

**login virtual-service-blade** *name* [**primary** | **secondary**]

Syntax Description		
	<i>name</i>	Name of an existing virtual service blade.
	<b>primary</b>	(Optional) The Cisco Nexus 1010 that was assigned the primary role.
	<b>secondary</b>	(Optional) The Cisco Nexus 1010 that was assigned the secondary role.

**Defaults** None

**Command Modes** EXEC

**SupportedUserRoles** network-admin

Command History	Release	Modification
	4.2(1)SP1(2)	The optional <b>primary</b> and <b>secondary</b> keywords were added.
	4.0(4)SP1(1)	This command was introduced.

**Usage Guidelines** This command gives serial command access to a virtual service blade.

**Examples** This example shows how to log into the Cisco Nexus 1000V CLI for the VSB named VSB-1 which is on the primary Cisco Nexus 1010.

```
n1010# login virtual-service-blade VSB-1 primary
n1010#
```

Related Commands	Command	Description
	<b>description</b>	Adds a description to the virtual service.
	<b>enable</b>	Initiates the configuration of the virtual service and then enables it.
	<b>show virtual-service-blade</b>	Displays information about the virtual service blades.
	<b>show virtual-service-blade name</b>	Displays information about a virtual service.
	<b>show virtual-service-blade-type summary</b>	Displays a summary of all virtual service configurations by the type name.

***Send document comments to [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com).***

<b>Command</b>	<b>Description</b>
<b>virtual-service-blade</b>	Creates the named virtual service and places you into the configuration mode for that service.
<b>virtual-service-blade-type</b>	Specifies the type and name of the software image file to add to this virtual service.