



## **CPS UDC SNMP and Alarms Guide, Release 18.1.0 (Restricted Release)**

**First Published:** 2018-03-16

**Last Modified:** 2018-03-16

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2018 Cisco Systems, Inc. All rights reserved.

# CONTENTS

---

<b>RESTRICTED RELEASE .....</b>	<b>5</b>
<b>UDC ALARMS .....</b>	<b>6</b>
UDC/LWR ALARMS.....	7
<i>LDAP Write Alarms .....</i>	<i>7</i>
<i>SOAP Subscription Interface Alarms .....</i>	<i>7</i>
<i>LWR Broker Connection Alarms .....</i>	<i>8</i>
EXISTING ALARMS SUPPORTED ON UDC.....	9
<i>Component Notifications .....</i>	<i>9</i>
<i>Application Notifications .....</i>	<i>12</i>



# RESTRICTED RELEASE

---

**IMPORTANT:** This is a Short Term Support (STS) release with availability and use restrictions. Contact your Cisco Account or Support representatives for more information.

---

# UDC Alarms

---

A Cisco Policy Suite (CPS) deployment comprises multiple virtual machines (VMs) deployed for scaling and High Availability (HA) purposes. All VMs present in the system should have an IP address which is a routable IP to the Network Management System (NMS). The NMS can monitor each VM using this routable IP address. This guide explains the existing and new alarms supported by UDC.

## UDC/LWR Alarms

This section describes the following alarms supported on UDC and LWR:

- LDAP Write Alarms
- SOAP Subscription Interface Alarms
- LWR Broker Connection Alarms

### LDAP Write Alarms

Notification Name	Severity	Message Text	Feature
LDAPAllPeersDown	Error	1203:LDAP connection down	Application
	All LDAP Write peers are down.		
	Clear	1203:LDAP connection up	Application
	LDAP Write connection is up.		
LDAPPeerDown	Error	1204:<IP Address of the LDAP server>:LDAP connection down	Application
	LDAP Write peer identified by the IP address is down.		
	Clear	1204:<IP Address of the LDAP server>:LDAP connection up	Application
	LDAP Write peer identified by the IP address is up.		

### SOAP Subscription Interface Alarms

Notification Name	Severity	Message Text	Feature
AllSOAPSubscriptionServersDown	Error	1205: SOAP Subscription Server connection down.	Application
	All SOAP Subscription Server peers are down.		
	Clear	1205: SOAP Subscription Server connection up.	Application
	SOAP Subscription Server connection is up.		
SOAPSubscriptionServerDown	Error	1206:<IP Address of the SOAP Subscription Server>: SOAP Subscription Server	Application

		connection down	
SOAP Subscription Server peer identified by the IP address is down.			
Clear		1206: <IP Address of the SOAP Subscription Server >: SOAP Subscription Server connection up	Application
SOAP Subscription Server peer identified by the IP address is up.			

## LWR Broker Connection Alarms

**IMPORTANT:** In release 18.1, LWR is not fully qualified and is available only for testing purposes. For more information, contact your Cisco Account representative.

Notification Name	Severity	Message Text	Feature
BrokerServerDown	Error	1207: <IP Address of the LWR Broker server>:Broker Server is down	Application
	LWR Broker Server peer identified by the IP address is down.		
	Clear	1207: <IP Address of the LWR Broker server>:Broker connection up	Application
	LWR Broker Server peer identified by the IP address is up.		
AllBrokerServerDown	Error	1208: All Brokers connections down	Application
	All LWR Broker Server peers are down.		
	Clear	1208: All Brokers connections up	Application
	All LWR Broker Server connection is up.		



## Existing Alarms Supported on UDC

This section describes the following existing alarms supported on UDC:

- Component Notifications
- Application Notifications

### Component Notifications

Notification Name	Severity	Message Text	Feature
DiskFull	Warning	<p>&lt;diskPath&gt;: less than &lt;n&gt;% free (= &lt;100-n&gt;%)</p> <p>For example:</p> <p>/var: less than 10% free (= 90%)</p>	Component
<p>Current disk usage has passed a designated threshold. By default, this threshold is set to 10% of total disk space allocated for the partition. This threshold is defined in /etc/snmp/snmpd.conf on each VM.</p> <p>This situation could be a sign of logs or database files growing large.</p> <p>For new deployments, this alarm is generated for following file systems in different VMs:</p> <p>For HA System:</p> <p>perfclient/lb: /</p> <p>sessionmgr: /, /var/data/session.1</p> <p>qns: /</p> <p>udc: /</p> <p>For AIO System:</p> <p>/</p> <p>For upgrades from 7.x system, this alarm is generated for following file systems in different VMs:</p> <p>For HA System:</p> <p>perf/lb: /, /var, /boot</p> <p>sessionmgr: /, /home, /boot, /data, /var/data/session.1</p> <p>qns: /, /home, /var, /boot</p> <p>udc: /, /home, /var, /boot</p> <p>For AIO System:</p> <p>/</p>			

	/boot		
	Clear	<diskPath>: clear	Component
	<p>The disk usage has recovered from the designated threshold.</p> <p>For new deployments, this alarm is generated for following file systems in different VMs:</p> <p>For HA System:</p> <p>perfclient/lb: /</p> <p>sessionmgr: /, /var/data/session.1</p> <p>qns: /</p> <p>udc: /</p> <p>For AIO System:</p> <p>/</p> <p>For upgrades from 7.x system, this alarm is generated for following file systems in different VMs:</p> <p>For HA System:</p> <p>perf/lb: /, /var, /boot</p> <p>sessionmgr: /, /home, /boot, /data, /var/data/session.1</p> <p>qns: /, /home, /var, /boot</p> <p>udc: /, /home, /var, /boot</p> <p>For AIO System:</p> <p>/</p> <p>/boot</p>		
LowSwap	Warning	Running out of swap space	Operating System
	Current swap usage has passed a designated threshold. This is a warning.		
	Clear	Swap space recovered	Operating System
	Current swap usage has recovered a designated threshold.		
HighLoad	Warning (1, 5 minutes) Alert (15 minutes)	1 min Load Average too high (= n.nn) 5 min Load Average too high (= n.nn) 15 min Load Average too high (=n.nn)	Component
	<p>The load average of the system has exceeded the configured threshold for a period of 1/5/15 minutes.</p> <p>The default threshold value is 1.5 * Number of vCPUs (allocated to VM) for each time period as defined in/etc/snmp/snmpd.conf file.</p>		

	The value must be integer.		
	Clear	Load-1 High load recovered Load-5 High load recovered Load-15 High load recovered	Component
	The load average has recovered from more than configured threshold.		
LinkDown	Alert	IF-MIB::linkDown <Interface Name>	Operating System
	Not able to connect or ping to the interface. This alarm gets generated for all physical interface attached to the system.		
LinkUp	Clear	IF-MIB::linkUp <Interface Name>	Operating System
	Able to ping or connect to interface. This alarm gets generated for all physical interface attached to the system.		
LowMemory	Critical	Current Available Free Memory (total free memory) is less than threshold (Threshold memory) on \$HOSTNAME	Operating System
	The amount of free memory on the VM has dropped below the default threshold of 10% (as a percentage of total memory). To change the default threshold, see CPS SNMP, Alarms, and Clearing Procedures Guide		
	Clear	Current Available Free Memory (total free memory) is greater than threshold (Threshold memory) on \$HOSTNAME	Operating System
	Low memory alert has been cleared.		
HIGH CPU USAGE Alert	Critical	CPU Usage is higher than threshold on "hostname". Threshold= \$Alert_Threshold%, Current_LOAD= \$Current_load%	Component
	This trap is generated whenever CPU usage on any VM is detected to be higher than the		

	<p>alert threshold value.</p> <p>The system monitors the CPU usage at a specific instant (every 60 second by default), and not over a period of time like for the HighLoad Alert.</p> <p>To change the default threshold or the interval at which the CPU usage is checked, see <i>CPS SNMP, Alarms, and Clearing Procedures Guide</i></p>		
HIGH CPU USAGE	Clear	<p>Clear CPU Usage is below than lower threshold value on `hostname`.</p> <p>Threshold= \$Alert_Threshold%, Current_LOAD= \$Current_load%</p>	Component
<p>This trap is generated whenever CPU usage on any VM is lower than the clear threshold value. It is generated only when High CPU Usage Alert was generated earlier for the VM.</p>			

## Application Notifications

Notification Name	Severity	Message Text	Feature
MemcachedConnectError	Error Critical	<p>Memcached server is in error</p> <p>OR some exception generated message. %s is the exception that occurred.</p>	Application
	Generated if attempting to connect to or write to the memcached server causes an exception.		
	Clear	Memcached server is operational.	Application
	Generated if successfully connect to or write to the memcached server.		
ApplicationStartError	Alert	Feature %s is unable to start. Error %s	Application
	Generated if an installed feature cannot start.		
	Clear	Feature %s is Running	Application
	Generated if an installed feature successfully started.		
License Usage Threshold Exceeded	Critical, Error, Minor, Warning (Configurable)	Session Count License Usage at: xxx%, exceeding threshold:xxx%	Application

	<p>The number of sessions on the system has exceeded the configured threshold of sessions allowed by the current license.</p> <p>The threshold value and alarm severity of this alarm is configurable in Policy Builder: Click Fault List in the navigation pane, then create a new fault list or edit the existing fault list. By default, the threshold is set to 90%.</p>		
	Clear	Session Count License Usage at: xxx%, exceeding threshold:xxx%	Application
	<p>The number of sessions on the system is below the configured threshold of sessions allowed by the current license.</p>		
LicensedSessionCreation	Critical	Session creation is not allowed	Application
	<p>A predefined threshold of sessions covered by licensing has been passed. This is a warning and should be reported. License limits may need to be increased soon. This message can be generated by an invalid license, but the AdditionalInfo portion of the notification shows root cause.</p>		
	Clear	Session creation is allowed	Application
	<p>The number of sessions are below the predefined threshold of sessions covered by licensing.</p>		
InvalidLicense	Emergency	"core license is Invalid. No Core License found. Please install core license"	Application
	<p>The system license currently installed is not valid. This prevents system operation until resolved. This is possible if no license is installed or if the current license does not have core feature in it.</p>		
	Emergency	xxx license is invalid %s	Application
	<p>This alarm is generated when feature license is not installed for a particular feature.</p>		
	Critical	xxx is Expired %s	Application
	<p>License has expired.</p>		
	Error	xxx will expire soon %s	Application
	<p>License is going to expire soon.</p>		
	Critical	xxx has exceeded the allowed parameters%s	Application
	<p>License has exceeded the allowed parameters.</p>		
	Error	xxx is nearing the allowed parameters %s	Application
	<p>Proxy server is reachable.</p>		
PolicyConfiguration	Error	"Last policy configuration failed with the following message:xxx"	Application

	A change to system policy structure has failed. The AdditionalInfo portion of the notification contains more information. The system typically remains in a proper state and continues core operations. Either make note of this message or investigate more fully.		
	Clear	“Last policy configuration was successful”	Application
	A change to system policy structure has passed.		
PoliciesNotConfigured	Emergency	“Policies not configured”	Application
	The policy engine cannot find any policies to apply while starting up. This may occur on a new system, but requires immediate resolution for any system services to operate.		
	Clear	“Policies successfully configured”	Application
	The policy engine has successfully configured all the policies while starting up.		
VM Down	Critical	unable to connect %member_ip (%member) VM. It is not reachable.	Application
	The administrator is not able to ping the VM.		
VM Up	Clear	Connected %member_ip (%member) VM. It is reachable.	Application
	The administrator is able to ping the VM.		
QNS Process Down	Critical	%machinename: %server server on %vm vm is down	Application
	UDC java process is down.		
QNS Process Up	Clear	%machinename: %server server on %vm vm is up	Application
	UDC java process is up.		
VirtualInterface Down	Alert	%INTERFACE: unable to connect (lbvip01/lbvip02). Not reachable	Application
	Not able to ping the virtual Interface. This alarm gets generated for lbvip01, lbvip02.		
VirtualInterface Up	Clear	%INTERFACE: (lbvip01/lbvip02) is up	Application
	Successfully ping the virtual Interface. This alarm gets generated for lbvip01, lbvip02.		
LDAPAllPeersDown	Error	1201:LDAP connection down	Application
	All LDAP peers are down.		
	Clear	1201:LDAP connection up	Application
	LDAP connection is up.		

LDAPPeerDown	Error	1202:<IP Address of the LDAP server>:LDAP connection down	Application
	LDAP peer identified by the IP address is down.		
	Clear	1202:<IP Address of the LDAP server>:LDAP connection up	Application
LDAP peer identified by the IP address is up.			
Percentage of LDAP retry threshold Exceeded	Critical	Percentage of LDAP retries compared to total LDAP Queries exceeded to <%threshold> on <udcXX> VM.	Application
	<p>This alarm indication is generated for LDAP search queries when LDAP retries compared to total LDAP queries exceeds 10% on udcXX VM.</p> <p>Default Threshold: 10%.</p> <p><b>NOTE:</b> The LDAP server Retry Count parameter must be set to a value greater than 1 for this alarm to be generated. In Policy Builder navigate to Plugin Configuration &gt; LDAP Configuration &gt; LDAP Server Configuration &gt; Retry Count.</p>		
Percentage of LDAP retry threshold Normal	Clear	Percentage of LDAP retries compared to total LDAP Queries normal to <%threshold> on <udcXX> VM.	Application
	<p>This clear indication is generated for LDAP search queries when LDAP retries compared to total LDAP queries is normal or has fallen below the threshold value (10%) on udcXX VM.</p>		
LDAP Requests as percentage of CCR-I Dropped	Critical	LDAP Requests as percentage of CCR-I dropped to <%threshold> on udcXX VM.	Application
	<p>This alarm indication is generated for LDAP operations when LDAP requests as percentage of CCR-I (Gx messages) drops below 25% on udcXX VM.</p> <p>Default Threshold: 25%</p>		
LDAP Requests as percentage of CCR-I Normal	Clear	LDAP Requests as percentage of CCR-I normal to <%threshold> on udcXX VM.	Application
	<p>This clear indication is generated for LDAP operations when LDAP requests as a percentage of CCR-I messages is normal or above the 25% threshold on udcXX VM.</p>		
LDAP Request Dropped	Critical	LDAP Requests dropped to <threshold value> on	Application

Existing Alarms Supported on UDC

		udcXX VM.	
	This alarm indication is generated for LDAP operations when LDAP requests drop below 0 on udcXX VM. Default Threshold: 0		
LDAP Requests Normal	Clear	LDAP Requests normal to <threshold value> on udcXX VM.	Application
	This clear indication is generated for LDAP operations when LDAP requests are normal (above 0) on udcXX VM.		
LDAP Query Result Dropped	Critical	LDAP Query Result dropped to <threshold value> on udcXX VM.	Application
	This alarm indication is generated when LDAP Query Result goes to 0 on udcXX VM. Default Threshold: 0		
LDAP Query Result Normal	Clear	LDAP Query Result normal to <threshold value> on udcXX VM.	Application
	This clear indication is generated when LDAP Query Result goes above 0 (above the threshold value) on udcXX VM.		