



# System Director System Log Messages

Controller Management System Log Messages.....	1
AP System Log Messages.....	7
802.11 System Log Messages.....	10
Security System Log Messages.....	10
Captive Portal System Log Messages .....	12
QoS System Log Messages.....	13
Rogue AP System Log Messages .....	15
Licensing System Log Messages.....	15
N+1 Redundancy System Log Messages .....	15

This document lists and describes system messages for System Director.

The following information is provided for each message:

- Event: Event for which system log message is triggered.
- System Log Example: Example of a system log message.
- Description: Description of the system log message.
- Action: Action that can be taken. If no action is mentioned, no action is required.

## Controller Management System Log Messages

[Table 1](#) lists messages generated for configuration changes, user management, and other administrative events on the controller.

**Table 1: Controller Management System Log Messages**

Event	System Log Example	Description	Action
CONTROLLER REBOOT	Oct 13 11:11:32 172.18.37.201 ALARM: 1255432836l   system   notice   NOT   Controller administrative reboot requested	A controller reboot is requested.	
CONTROLLER BOOT  PROCESS START	<p>Oct 13 11:12:55 172.18.37.201 syslog: syslogd startup succeeded</p> <p>Oct 13 11:12:55 172.18.37.201 syslog: klogd startup succeeded</p> <p>Oct 13 11:12:58 172.18.37.201 sysctl: net.ipv4.ip_forward = 1</p> <p>Oct 13 11:12:58 172.18.37.201 sysctl: net.ipv4.conf.default.rp_filter = 1</p> <p>Oct 13 11:12:58 172.18.37.201 sysctl: kernel.sysrq = 0</p> <p>Oct 13 11:12:58 172.18.37.201 sysctl: kernel.core_uses_pid = 1</p> <p>Oct 13 11:12:58 172.18.37.201 network: Setting network parameters: succeeded</p> <p>Oct 13 11:12:58 172.18.37.201 network: Bringing up loopback interface: succeeded</p> <p>Oct 13 11:12:58 172.18.37.201 crond: crond startup succeeded</p> <p>Oct 13 11:12:58 172.18.37.201 sshd: succeeded</p> <p>Oct 13 11:12:58 172.18.37.201 sshd[303]: Server listening on 0.0.0.0 port 22.</p> <p>Oct 13 11:12:58 172.18.37.201 network: Bringing up interface eth0: succeeded</p> <p>Oct 13 11:12:59 172.18.37.201 xinetd: xinetd startup succeeded</p> <p>Oct 13 11:12:59 172.18.37.201 root: Start WLAN Services ...</p> <p>Oct 13 11:13:01 172.18.37.201 meru: /etc/init.d/ceflog: /opt/meru/var/run/running-db/ceflog.conf: No such file or directory</p> <p>Oct 13 11:13:01 172.18.37.201 meru: Setting up swap space version 0, size = 43446272 bytes</p> <p>Oct 13 11:13:01 172.18.37.201 meru: Using /lib/modules/2.4.18-3-meruenabled/kernel/drivers/dump/dump.o</p> <p>Oct 13 11:13:01 172.18.37.201 meru: Kernel data gathering phase complete</p> <p>Oct 13 11:13:05 172.18.37.201 meru: Warning: loading /opt/meru/kernel/ipt_vlan_routing.mod will taint the kernel: non-GPL license - Proprietary</p> <p>Oct 13 11:13:37 172.18.37.201 meru: Process RemoteUpgrade did not come up. Will retry again</p> <p>Oct 13 11:13:37 172.18.37.201 root: Controller Up on Tue Oct 13 11:22:42 UTC 2009</p>	Controller boot sequence showing different processes and WLAN services getting started.	

Event	System Log Example	Description	Action
	<p>Oct 13 11:13:37 172.18.37.201 root: WLAN Services started</p> <p>Oct 13 11:13:37 172.18.37.201 rc: Starting meru: succeeded</p>		
<p>CONTROLLER SHUTDOWN</p> <p>PROCESS STOP</p>	<p>Oct 13 11:11:33 172.18.37.201 root: Stop WLAN Services ...</p> <p>Oct 13 11:11:33 172.18.37.201 meru: icrd stopped.</p> <p>Oct 13 11:11:33 172.18.37.201 meru: Rlos stopped.</p> <p>Oct 13 11:11:37 172.18.37.201 meru: discovery stopped.</p> <p>Oct 13 11:11:37 172.18.37.201 meru: WncDhcpRelay stopped.</p> <p>Oct 13 11:11:37 172.18.37.201 meru: nmsagent stopped.</p> <p>Oct 13 11:11:38 172.18.37.201 meru: melfd stopped.</p> <p>Oct 13 11:11:38 172.18.37.201 meru: igmp-snoop-daemon stopped.</p> <p>Oct 13 11:11:44 172.18.37.201 meru: dfsd stopped.</p> <p>Oct 13 11:11:45 172.18.37.201 meru: aeroscoutd stopped.</p> <p>Oct 13 11:11:45 172.18.37.201 meru: snmp stopped.</p> <p>Oct 13 11:11:46 172.18.37.201 meru: cmdd stopped.</p> <p>Oct 13 11:11:47 172.18.37.201 meru: rfsmgr stopped.</p> <p>Oct 13 11:11:49 172.18.37.201 meru: wncclid stopped.</p> <p>Oct 13 11:11:50 172.18.37.201 meru: sipfd stopped.</p> <p>Oct 13 11:11:51 172.18.37.201 meru: rulefd stopped.</p> <p>Oct 13 11:11:52 172.18.37.201 meru: watchdog stopped.</p> <p>Oct 13 11:11:52 172.18.37.201 meru: oct_watchdog stopped.</p> <p>Oct 13 11:11:52 172.18.37.201 meru: h323fd stopped.</p> <p>Oct 13 11:11:53 172.18.37.201 meru: sccpfd stopped.</p> <p>Oct 13 11:11:54 172.18.37.201 meru: coordinator stopped.</p> <p>Oct 13 11:11:54 172.18.37.201 meru: security-mm stopped.</p> <p>Oct 13 11:11:56 172.18.37.201 meru: hostapd stopped.</p> <p>Oct 13 11:11:57 172.18.37.201 meru: rogueapd stopped.</p> <p>Oct 13 11:11:58 172.18.37.201 meru: xems stopped.</p> <p>Oct 13 11:11:58 172.18.37.201 meru: apache stopped.</p>	<p>Controller shutdown sequence, showing different processes and WLAN services getting stopped.</p>	

Event	System Log Example	Description	Action
	<p>Oct 13 11:12:01 172.18.37.201 meru: xclid stopped.</p> <p>Oct 13 11:12:07 172.18.37.201 meru: wncagent stopped.</p> <p>Oct 13 11:12:07 172.18.37.201 meru: Removed VLAN -:vlan133:-</p> <p>Oct 13 11:12:08 172.18.37.201 meru: vlan stopped.</p> <p>Oct 13 11:12:10 172.18.37.201 meru: rsync stopped.</p> <p>Oct 13 11:12:12 172.18.37.201 meru: lmgrd stopped.</p> <p>Oct 13 11:12:15 172.18.37.201 meru: kdi stopped.</p> <p>Oct 13 11:12:15 172.18.37.201 meru:</p> <p>Oct 13 11:12:18 172.18.37.201 root: WLAN Services stopped</p> <p>Oct 13 11:12:18 172.18.37.201 rc: Stopping meru: succeeded</p> <p>Oct 13 11:12:18 172.18.37.201 sshd[317]: Received signal 15; terminating.</p> <p>Oct 13 11:12:18 172.18.37.201 sshd: sshd - TERM succeeded</p> <p>Oct 13 11:12:18 172.18.37.201 xinetd: xinetd shutdown succeeded</p> <p>Oct 13 11:12:18 172.18.37.201 crond: crond shutdown succeeded</p> <p>Oct 13 11:12:19 172.18.37.201 syslog: klogd shutdown succeeded</p>		
SSH LOGIN SESSION	<p>Oct 13 11:13:58 172.18.37.201 sshd[4874]: PAM _pam_init_handlers: no default config /etc/pam.d/other</p> <p>Oct 13 11:14:00 172.18.37.201 sshd[4874]: PAM _pam_init_handlers: no default config /etc/pam.d/other</p> <p>Oct 13 11:14:00 172.18.37.201 sshd[4874]: Accepted password for admin from 172.18.37.12 port 1891 ssh2</p> <p>Oct 13 11:14:00 172.18.37.201 sshd(pam_unix)[4876]: session opened for user admin by (uid=0)</p> <p>Oct 13 11:14:00 172.18.37.201 PAM-env[4876]: Unable to open config file: No such file or directory</p> <p>Oct 13 11:14:00 172.18.37.201 sshd[4876]: lastlog_perform_login: Couldn't stat /var/log/lastlog: No such file or directory</p> <p>Oct 13 11:14:00 172.18.37.201 sshd[4876]: lastlog_openseek: /var/log/lastlog is not a file or directory!</p> <p>Apr 09 12:00:22 172.18.49.14 -- admin[19814]: LOGIN ON pts/3 BY admin FROM xp.merunetworks.com</p> <p>Apr 09 15:23:07 172.18.37.203 sshd(pam_unix)[23750]: session closed for user admin</p>	A controller user logged in, using an SSH connection.	

Event	System Log Example	Description	Action
	Apr 09 15:07:53 172.18.37.203 su(pam_unix)[28060]: session opened for user root by admin(uid=0) Apr 09 15:08:09 172.18.37.203 su(pam_unix)[28060]: session closed for user root Apr 09 17:48:48 172.18.37.203 sshd[28588]: Received disconnect from 172.18.37.15: 11: Disconnect requested by Windows SSH Client.		
WEB ADMIN LOGIN	Oct 13 11:15:07 172.18.37.201 xems: 1255433051   security   info   WAU   Controller Access User admin@172.18.37.12 login to controller at time Tue Oct 13 11:24:11 2009 is OK	Admin logged in to controller GUI.	
NTP SERVER NOT ACCESSIBLE	Apr 12 18:01:10 172.18.49.14 root: NTP server time.windows.com did not respond.	NTP server is not accessible.	Check to see if NTP server is down, or verify that the NTP server is correctly configured on the controller. If the configuration is wrong, use the "Setup" command to correct the configuration.
User Management: RADIUS request sent	Mar 29 13:43:40 172.18.86.229 SecurityMM: 1269866620   security   info   RBAC   Sending Radius Access-Request message for user : pat	For RADIUS-based controller user management, RADIUS access request is being sent to RADIUS server.	
User Management: Group ID not available	Mar 29 13:46:32 172.18.86.229 xems: 1269866791   security   info   RBAC   Group Id not available for Group Num 700 and User Id pat	Group ID configured for controller user is not available.	Create group with this group ID, or change the group ID for this user.
User Management: RADIUS Success	Mar 29 13:49:18 172.18.86.229 SecurityMM: 1269866959   security   info   RBAC   Radius Access succeed for user <pat>	For RADIUS-based controller user management, RADIUS authentication succeeded.	
User Management: Group Number received from RADIUS	Mar 29 13:49:18 172.18.86.229 SecurityMM: 1269866959   security   info   RBAC   Group Num <700> received from Radius server for user <pat>	RADIUS server returned group number for user logged in.	
User Management: User Login Success	Mar 29 13:49:18 172.18.86.229 xems: 1269866959   security   info   WAU   Controller Access User pat@172.18.45.17 login to controller at time Mon Mar 29 18:19:19 2010 is OK	Controller user logged in.	
User Management: RADIUS Failure	Mar 29 13:50:42 172.18.86.229 SecurityMM: 1269867043   security   info   RBAC   Radius Access failed for user <local1234>	RADIUS authentication for controller user failed.	

Event	System Log Example	Description	Action
User Management: User Login Failure	Mar 29 13:50:43 172.18.86.229 xems: 1269867043l   security   info   WAU   Controller Access User local1234@172.18.45.17 login to controller at time Mon Mar 29 18:20:43 2010 is FAILED	Controller user login failed.	
DUAL ETHERNET	info NOT 10/08/2009 00:12:42 <00:90:0b:0a:81:b0> 1st interface link up.	Controller's first interface link is up.	
DUAL ETHERNET	info NOT 10/08/2009 00:16:14 <00:90:0b:0a:81:b0> 1st interface link down.	Controller's first interface link is down.	
DUAL ETHERNET	info NOT 10/08/2009 00:25:55 <00:90:0b:0a:81:af> 2nd interface link up.	Controller's second interface link is up.	
DUAL ETHERNET	info NOT 10/08/2009 00:26:16 <00:90:0b:0a:81:af> 2nd interface link down.	Controller's second interface link is down.	
DUAL ETHERNET	info NOT 10/08/2009 00:25:56 <00:90:0b:0a:81:af> switch to 2nd interface done.	Controller is configured in redundant mode for dual Ethernet. The first interface went down, so the second interface has taken over.	
DUAL ETHERNET	info NOT 10/08/2009 00:26:19 <00:90:0b:0a:81:af> switch to 1st interface done.	Controller is configured in redundant mode for dual Ethernet. The second interface went down, so the first interface has taken over.	
DUAL ETHERNET: STANDALONE MODE EXAMPLE	info NOT 10/08/2009 00:12:42 <00:90:0b:0a:81:b0> 1st interface link up. info NOT 10/08/2009 00:16:14 <00:90:0b:0a:81:b0> 1st interface link down.	Sequence shown when the controller is configured in standalone mode and the first interface goes down.	If first interface link down message is seen, check the connectivity to first interface.
DUAL ETHERNET: REDUNDANT MODE EXAMPLE	info NOT 10/08/2009 00:24:26 <00:90:0b:0a:81:af> 1st interface link up. info NOT 10/08/2009 00:25:52 <00:90:0b:0a:81:af> 1st interface link down. info NOT 10/08/2009 00:25:55 <00:90:0b:0a:81:af> 2nd interface link up. info NOT 10/08/2009 00:25:56 <00:90:0b:0a:81:af> switch to 2nd interface done. info NOT 10/08/2009 00:26:16 <00:90:0b:0a:81:af> 2nd interface link down. info NOT 10/08/2009 00:26:19 <00:90:0b:0a:81:af> 1st interface link up. info NOT 10/08/2009 00:26:19 <00:90:0b:0a:81:af> switch to 1st interface done.	Sequence shown when the controller is configured in redundant mode. When the first interface goes down, the second interface takes over.	Check the connectivity on the interface that has gone down.

Event	System Log Example	Description	Action
DUAL ETHERNET: ACTIVE MODE EXAMPLE	info NOT 10/08/2009 00:37:29 <00:90:0b:0a:81:b0> 1st interface link up. info NOT 10/08/2009 00:37:29 <00:90:0b:0a:81:af> 2nd interface link up. info NOT 10/08/2009 00:38:34 <00:90:0b:0a:81:af> 2nd interface link down. info NOT 10/08/2009 00:38:39 <00:90:0b:0a:81:b0> 1st interface link down. info NOT 10/08/2009 00:38:43 <00:90:0b:0a:81:b0> 1st interface link up. info NOT 10/08/2009 00:38:45 <00:90:0b:0a:81:af> 2nd interface link up.	Sequence shown when the controller is configured in active mode.	Check the connectivity on the interface that has gone down.

## AP System Log Messages

[Table 2](#) lists messages generated for AP discovery, AP redirection, AP replacement, and AP and interface up/down events.

**Table 2: AP System Log Messages**

Event	System Log Example	Description	Action
AP Down	Mar 21 12:56:51 172.18.65.202 ALARM: 1206084411   system   info   ALR   AP DOWN CRITICAL Access Point Pat-AP300 (2) at time Fri Mar 21 07:26:51 2008	This message is generated when the controller detects an AP Down event. An AP Down event can be reported for many reasons: AP upgrading Power failure Network failure, AP not accessible. AP crash	If an AP crash is occurring due to an unknown issue, contact Meru Customer Support.
AP Up	Mar 21 12:57:20 172.18.65.202 ALARM: 1206084440   system   info   ALR   AP UP Access Point Pat-AP300 (2) is up at time Fri Mar 21 07:27:20 2008	This message is generated when the controller detects an AP Up event.	
AP Software Version Mismatch	Mar 21 15:19:05 172.18.65.202 ALARM: 1206092945   system   info   ALR   AP SOFTWARE VERSION MISMATCH CRITICAL AP Pat-AP300 (2) - Software Version Mismatch : AP version is 3.4.SR3m-10 and Controller version is 3.6-40	This message is generated when the AP software version does not match the controller software version.	If Auto-AP-Upgrade is enabled, the controller will automatically upgrade AP software to the same version. Otherwise, manually upgrade the AP to the version same as the controller.
AP Upgrade	Apr 09 12:41:18 172.18.37.203 ALARM: 1270817859   system   notice   NOT   Software version of AP 4 is being changed from 4.0-86 to 4.0-89	The AP software is being upgraded.	

Event	System Log Example	Description	Action
Boot Image Version Mismatch	Apr 28 14:03:35 172.18.65.202 ALARM: 1209371615I   system   info   ALR   AP BOOTIMAGE VERSION MISMATCH CRITICAL BootImage_Version_MisMatch_for_AP1	This message is generated when the AP has an incompatible boot image.	
Boot Image Match	Apr 28 14:03:51 172.18.65.202 ALARM: 1209371631I   system   info   ALR   AP BOOTIMAGE VERSION MISMATCH CLEAR BootImage_Version_Match_for_AP1	The message is generated when the AP's incompatible boot image has been replaced by a compatible boot image.	
AP Neighbor Loss	Apr 28 14:01:12 172.18.65.202 ALARM: 1209371472I   system   info   ALR   AP NEIGHBOR LOSS CRITICAL Neighbor_Loss_for_AP1	This message is generated when an AP has lost its neighbor AP.	
AP Neighbor Loss Cleared	Apr 28 14:01:18 172.18.65.202 ALARM: 1209371478I   system   info   ALR   AP NEIGHBOR LOSS CLEAR Neighbor_Loss_for_AP1	This message is generated when then the AP Neighbor loss alarm is cleared.	
Hardware Diagnostics Error	Mar 21 13:49:53 172.18.65.202 ALARM: 1206087593I   system   info   ALR   AP HARDWARE DIAGNOSTIC ERROR CRITICAL HardwareDiagnostics	This message is generated when an AP has an incompatible FPGA version.	
Hardware Diagnostics Error Cleared	Mar 21 13:49:47 172.18.65.202 ALARM: 1206087587I   system   info   ALR   AP HARDWARE DIAGNOSTIC ERROR CLEAR HardwareDiagnostics	This message is generated when an AP's incompatible FPGA version is replaced with a compatible version.	
Handoff Fail	Apr 28 14:02:04 172.18.65.202 ALARM: 1209371524I   system   info   ALR   HAND OFF FAIL CRITICAL HandOff_Fail_for_AP1	This message is generated when handoff fails.	
Handoff Fail Cleared	Apr 28 14:02:21 172.18.65.202 ALARM: 1209371541I   system   info   ALR   HAND OFF FAIL CLEAR HandOff_Fail_Cleared_for_AP1	This message is generated when the handoff fail alarm is cleared.	
Resource Threshold Exceeded	Mar 21 13:56:27 172.18.65.202 ALARM: 1206087987I   system   info   ALR   RESOURCE THRESHOLD EXCEED CRITICAL ResourceThreshold	This message is generated when the resource (CPU & Memory) threshold is exceeded.	
Resource Threshold Exceed Cleared	Mar 21 13:57:17 172.18.65.202 ALARM: 1206088037I   system   info   ALR   RESOURCE THRESHOLD EXCEED CLEAR ResourceThreshold	This message is generated when the resource threshold exceed alarm is cleared.	
System Failure	Mar 21 14:18:29 172.18.65.202 ALARM: 1206089309I   system   info   ALR   SYSTEM FAILURE CRITICAL SystemFailure	This message is generated when the system.	
System Failure Cleared	Mar 21 14:19:04 172.18.65.202 ALARM: 1206089344I   system   info   ALR   SYSTEM FAILURE CLEAR SystemFailure	This message is generated when the system failure alarm is cleared.	



Event	System Log Example	Description	Action
Watchdog Failure	Mar 21 14:27:28 172.18.65.202 ALARM: 1206089848  system   info   ALR   WATCHDOG FAILURE CRITICAL WatchDog_Failure	This message is generated when the Watchdog process is terminated.	
Watchdog Failure Cleared	Mar 21 14:27:59 172.18.65.202 ALARM: 1206089879  system   info   ALR   WATCHDOG FAILURE CLEAR WatchDog_Failure	This message is generated when the Watchdog process resumes.	
Certificate Error	Mar 21 15:04:10 172.18.65.202 ALARM: 1206092050  system   info   ALR   CERTIFICATE ERROR CRITICAL Certificare_Error	This message is generated when a certificate error occurs.	
Certificate Error Cleared	Mar 21 15:04:38 172.18.65.202 ALARM: 1206092078  system   info   ALR   CERTIFICATE ERROR CLEAR Certificate_Error	This message is generated when the certificate error alarm is cleared.	
AP Init Failure	Apr 28 12:55:58 172.18.65.202 ALARM: 1209367557  system   info   ALR   AP INIT FAILURE CRITICAL Init_Failure_for_AP1	This message is generated when an AP initialization fails.	
AP Init Failure Cleared	Apr 28 12:55:45 172.18.65.202 ALARM: 1209367545  system   info   ALR   AP INIT FAILURE CLEAR Init_Failure_for_AP1	This message is generated when the AP initialization failure alarm is cleared.	
AP Radio Card Failure	Apr 28 13:01:00 172.18.65.202 ALARM: 1209367860  system   info   ALR   AP RADIO CARD FAILURE CRITICAL Radio_Card_Failure_for_AP1	This message is generated when an AP radio card stops working.	
AP Radio Card Failure Cleared	Apr 28 13:01:08 172.18.65.202 ALARM: 1209367868  system   info   ALR   AP RADIO CARD FAILURE CLEAR Radio_Card_Failure_for_AP1	This message is generated when an AP radio card failure alarm is cleared.	
Primary RADIUS Server Restored	Mar 21 15:50:53 172.18.65.202 ALARM: 1206094852  system   info   ALR   PRIMARY RADIUS SERVER RESTORED CRITICAL Radius_Server_Restored	This message is generated when the primary RADIUS server that was down is restored.	
RADAR Detected	Mar 21 15:12:08 172.18.65.202 ALARM: 1206092528  system   info   ALR   RADAR DETECTED CRITICAL Radar Detected	This message is generated when DFS Manager detects RADAR.	
MIC Counter Measure Activation	Apr 28 13:57:36 172.18.65.202 ALARM: 1209371256  system   info   ALR   MIC COUNTERMEASURE ACTIVATION CRITICAL MIC_CounterMeasure_Activation_for_AP1	This message is generated when there are two subsequent MIC failures.	
AP MIC Failure	Apr 28 13:13:12 172.18.65.202 ALARM: 1209368592  system   info   ALR   AP MIC FAILURE CRITICAL MIC_Failure_for_AP1	This message is generated when there is a MIC failure.	

## 802.11 System Log Messages

[Table 3](#) lists messages generated for 802.11 protocol events.

**Table 3: 802.11 System Log Messages**

Event	System Log Example	Description	Action
Station Unassociated	Apr 09 13:25:28 172.18.37.203 coordinator: Wireless Associations, Unassociated for STA 00:1f:3b:6c:62:e7 in BSSID 00:0c:e6:56:dd:3b ESS 4088clear AP_ID 1 at Time Fri Apr 9 13:41:49 2010	802.11 station disassociation.	
Station Associated	Apr 09 14:05:04 172.18.37.203 coordinator: Wireless Associations, Associated for STA 00:1f:3b:6c:62:e7 in BSSID 00:0c:e6:56:dd:3b ESS 4088clear AP_ID 1 at Time Fri Apr 9 14:21:25 2010  Mar 22 13:23:34 172.18.65.202 ALARM: 1206127090I   system   info   ALR   Station Info Update : MacAddress : 00:40:96:ae:20:7a, UserName : pat, AP-Id : 1, AP-Name : AP-1, BSSID : 00:0c:e6:8f:01:01, ESSID : pat, Ip-Type : dynamic dhcp, Ip-Address : 172.18.65.11, L2mode : clear, L3-mode : clear, Vlan-Name : VLAN-111, Vlan-Tag : 111  Apr 06 11:59:24 172.18.65.202 ALARM: 1270535364I   system   info   ALR   Station Disconnected : MacAddress : 00:40:96:ae:20:7a	802.11 station association.  Station connection.  Station disconnected.	

## Security System Log Messages

[Table 4](#) lists messages generated for 802.1X authentication events.

**Table 4: Security System Log Messages**

Event	System Log Example	Description	Action
RADIUS ACCESS REQUEST	Mar 29 13:14:06 172.18.98.221 RadiusInfo: RADIUS Access-Request Message sent for Client (00:1e:37:0e:98:3e).	RADIUS request message has been sent to RADIUS server.	
RADIUS ACCESS ACCEPT	Mar 29 13:14:06 172.18.98.221 RadiusInfo: RADIUS Access-Accept message received for Client (00:1e:37:0e:98:3e).	RADIUS server responded with Access-Accept message for RADIUS request (success scenario).	

Event	System Log Example	Description	Action
802.1X RADIUS ACCESS REQUEST	Apr 09 15:05:58 172.18.37.203 ALARM: 1270826539I   system   info   ALR   802.1x Authentication Attempt INFO Radius Access Attempt by station with MAC address 00:1f:3b:6c:62:e7 and user is NULL , AP Id: <1>	As part of 802.1X authentication, RADIUS request message has been sent to RADIUS server from controller.	
802.1X RADIUS ACCESS REJECT WITH BAD USERNAME	Apr 13 19:48:23 172.18.48.151 ALARM: 1271169441I   system   info   ALR   802.1X AUTHENTICATION FAILURE INFO Access Request rejected for User: <harsh>, NAS IP: <172.18.48.151>, SSID: <wpa2h>, Calling Station ID: <00:1f:3b:83:21:13>, Called Station ID: <00:90:0b:0a:82:48>, Authentication Type: <802.1X>, Reason: <Bad Username or Password>, AP Id: <1>	As part of 802.1X authentication, RADIUS server has responded with Access-Reject message, with the reason "Username or password is not correct." (Failure scenario).	Check for correct username or password.
802.1X RADIUS ACCESS REJECT WITH FOUR WAY HANDSHAKE TIMEOUT	Apr 12 17:26:24 172.18.49.14 ALARM: 1271073384I   system   info   ALR   802.1X AUTHENTICATION FAILURE MINOR Access Request rejected for Calling Station ID: <00:26:82:43:02:24>, Authentication Type: <802.1X>, Reason: <Four Way Handshake Timeout>, AP Id: <3>	802.1x authentication failure due to "Four Way Handshake Timeout" reason.	
RADIUS SWITCHOVER FAILURE	Apr 09 15:07:54 172.18.37.203 ALARM: 1270826655I   system   info   ALR   RADIUS SERVER SWITCHOVER FAILED MAJOR Primary Radius Server <172.18.1.3> failed. No valid Secondary Radius Server present. Switchover FAILED for Profile <4089wpa2>	During RADIUS authentication, primary RADIUS server was not accessible, and secondary RADIUS server is not configured.	Check for connectivity to primary RADIUS server from controller. If another RADIUS server is available, configure it as secondary server.
ACCOUNTING RADIUS SWITCHOVER	Mar 22 16:38:19 172.18.65.202 ALARM: 1206061018I   system   info   ALR   ACCOUNT RADIUS SERVER SWITCHOVER MAJOR Accounting Radius Server switches over from Primary <1.1.1.1> to Secondary <2.2.2.2> for Profile <WPA2>	For accounting, primary RADIUS server is not accessible, and switchover to secondary RADIUS server is attempted.	Check for connectivity between primary RADIUS server and controller.
ACCOUNTING RADIUS SWITCHOVER FAILURE	Mar 22 16:41:51 172.18.65.202 ALARM: 1206061230I   system   info   ALR   ACCOUNT RADIUS SERVER SWITCHOVER FAILED MAJOR Primary Accounting Radius Server <1.1.1.1> failed. No valid Secondary Accounting Radius Server present. Switchover FAILED for Profile <WPA2>	For accounting, primary RADIUS server is not accessible, and switchover secondary RADIUS server is not configured.	Check for connectivity to primary RADIUS server from controller. If another RADIUS server is available, configure it as secondary server.
MAC FILTERING: RADIUS SWITCHOVER	Mar 21 16:38:57 172.18.65.202 ALARM: 1206097736I   system   info   ALR   RADIUS SERVER SWITCHOVER MAJOR Radius Server switched over from Primary < 1.1.1.1 > to Secondary < 172.18.1.7 > for Mac Filtering	For MAC filtering, primary RADIUS server is not accessible, and switchover to secondary RADIUS is attempted.	Check for connectivity between configured primary RADIUS server and controller.

# Captive Portal System Log Messages

[Table 5](#) lists messages generated for Captive Portal events.

**Table 5: Captive Portal System Log Messages**

Event	System Log Example	Description	Action
Captive Portal Login Request	Mar 29 14:11:53 172.18.98.221 xems: 1269867812l   security   info   CAP   Captive Portal User(pat@172.18.98.41) login Request Received.	Login request for Captive Portal User has been received.	
Captive Portal: Radius Login Success	Mar 29 14:11:53 172.18.98.221 SecurityMM: 1269867812l   security   info   CAP   pat@172.18.98.41 StationMac[00:1b:77:af:dc:6e] Radius User logged in OK	Captive Portal RADIUS user has successfully logged in.	
Captive Portal: Redirection	Mar 29 13:39:16 172.18.86.229 xems: 1269866356l   security   info   CAP   Captive Portal User(172.18.86.14) Redirected. Sending login (https://secsol:8081/vpn/loginformWebAuth.html)	Complete Captive Portal login.	
Captive Portal: Login Sequence	Mar 22 13:23:47 172.18.65.202 httpd: 1206127103l   802.mobility   info   CAP   172.18.111.11:8080 1 http://www.google.com/webhp?complete=1&hl=en Mar 22 13:23:47 172.18.65.202 xems: 1206127103l   802.mobility   info   RED   172.18.111.11:8080 1 Mar 22 13:23:47 172.18.65.202 xems: 1206127103l   802.mobility   info   RED   172.18.111.11:8080 2 Mar 22 13:23:47 172.18.65.202 httpd: 1206127103l   802.mobility   info   CAP   172.18.111.11:8080 2 Mar 22 13:23:49 172.18.65.202 httpd: 1206127105l   802.mobility   info   CAP   172.18.111.11:8081 1 http://172.18.111.211:8081/vpn/loginformWebAuth.html Mar 22 13:23:49 172.18.65.202 xems: 1206127105l   802.mobility   info   CNT   172.18.111.11:8081 1 Mar 22 13:23:49 172.18.65.202 xems: 1206127105l   802.mobility   info   CNT   172.18.111.11:8081 2 Mar 22 13:23:49 172.18.65.202 httpd: 1206127105l   802.mobility   info   CAP   172.18.111.11:8081 2 Mar 22 13:23:49 172.18.65.202 httpd: 1206127105l   802.mobility   info   CAP   172.18.111.11:8081 1 http://172.18.111.211:8081/vpn/Images.vpn/newlogo.gif Mar 22 13:23:49 172.18.65.202 xems: 1206127105l   802.mobility   info   CNT		

Event	System Log Example	Description	Action
	<pre> 172.18.111.11:8081 1 Mar 22 13:23:49 172.18.65.202 xems: 1206127105l   802.mobility   info   CNT   172.18.111.11:8081 2 Mar 22 13:23:49 172.18.65.202 httpd: 1206127105l   802.mobility   info   CAP   172.18.111.11:8081 2 Mar 22 13:23:49 172.18.65.202 httpd: 1206127105l   802.mobility   info   CAP   172.18.111.11:8081 1 http://172.18.111.211:8081/favicon.ico Mar 22 13:23:49 172.18.65.202 httpd: 1206127105l   802.mobility   info   CAP   172.18.111.11:8081 2 Mar 22 13:23:49 172.18.65.202 httpd: 1206127105l   802.mobility   info   CAP   172.18.111.11:8081 1 http://172.18.111.211:8081/favicon.ico Mar 22 13:23:49 172.18.65.202 httpd: 1206127105l   802.mobility   info   CAP   172.18.111.11:8081 2 Mar 22 13:23:55 172.18.65.202 httpd: 1206127110l   802.mobility   info   CAP   172.18.111.11:8081 1 http://172.18.111.211:8081/vpn/loginUser Mar 22 13:23:55 172.18.65.202 xems: 1206127110l   802.mobility   info   LOG   172.18.111.11:8081 1 Mar 22 13:23:55 172.18.65.202 xems: 1206127110l   security   info   CAP   ramesh@172.18.111.11 logged in OK Mar 22 13:23:55 172.18.65.202 xems: 1206127110l   802.mobility   info   LOG   172.18.111.11:8081 2 Mar 22 13:23:55 172.18.65.202 httpd: 1206127110l   802.mobility   info   CAP   172.18.111.11:8081 2 </pre>		

## QoS System Log Messages

[Table 6](#) lists messages generated for QoS events.

**Table 6: QoS System Log Messages**

Event	System Log Example	Description	Action
QoS: Action Drop	Apr 13 18:14:23 172.18.117.217 kernel: 1271193480   system   info   ALR   Network Traffic, Flow of Traffic MAC: 00:40:96:ad:49:b0->MAC: 00:90:0b:0a:81:ae src_ip:172.18.117.27-> dst_ip:69.147.125.65:[dst_port:0], rule id: 23, action: Drop. AP MAC Address : 00:0c:e6:05:c5:14	This message is generated when packets match the QoS rule based on the configured parameters. Packets are dropped.	
QoS: Action Forward	Apr 13 18:21:54 172.18.117.217 kernel: 1271193932   system   info   ALR   Network Traffic, Flow of Traffic MAC: 00:14:a8:59:c8:80->MAC: 00:90:0b:0a:81:ae src_ip:172.18.117.1-> dst_ip:172.18.117.217:[dst_port:0], rule id: 23, action: Forward. AP MAC Address : 00:00:00:00:00:00	This message is generated when packets match the QoS rule based on the configured parameters. The packets that match the configured QoS rules are forwarded for further processing.	
QoS: Action Capture	Apr 13 18:30:47 172.18.117.217 kernel: 1271194465   system   info   ALR   Network Traffic, Flow of Traffic MAC: 00:40:96:ad:49:b0->MAC: 00:90:0b:0a:81:ae src_ip:172.18.117.27-> dst_ip:172.18.122.122:[dst_port:5060], rule id: 3, action: Capture. AP MAC Address : 00:0c:e6:07:5d:71	This message is generated when packets match the QoS rule based on the configured parameters. The packets are captured and sent to respective Flow Detector for further processing.	
CAC Per BSSID > CAC Per AP	info ALR 05/04/2010 13:39:20 CAC LIMIT REACHED MAJOR CAC/Global Bssid Limit Reached (1): call Rejected for STA [00:03:2a:00:d8:55] on AP [00:0c:e6:07:5d:7e] in BSSID [00:0c:e6:de:a2:ef]	This message is generated when the CAC limit is reached (based on BSSID). Calls will not go through.	
CAC Per AP > CAC Per BSSID	info ALR 05/04/2010 14:42:39 CAC LIMIT REACHED MAJOR CAC/AP Limit Reached (1): call Rejected for STA [00:03:2a:00:d8:55] on AP [00:0c:e6:07:5d:7e]	This message is generated when the CAC limit is reached (based on AP). Calls will not go through.	
CAC Per AP = CAC Per BSSID	info ALR 05/04/2010 15:03:22 CAC LIMIT REACHED MAJOR CAC/AP Limit Reached (1): call Rejected for STA [00:03:2a:00:d8:55] on AP [00:0c:e6:07:5d:7e]	This message is generated when the CAC limit is reached (based on AP=BSSID). Calls will not go through.	
CAC PER Interference	info ALR 05/04/2010 15:09:01 CAC LIMIT REACHED MAJOR CAC/Interference Limit Reached (1): call Rejected for STA [00:03:2a:00:d8:55] on AP [00:0c:e6:07:5d:7e]	This message is generated when the CAC limit is reached (based on CAC per interference region). Calls will not go through.	

## Rogue AP System Log Messages

[Table 7](#) lists messages generated for rogue AP events.

**Table 7: Rogue AP System Log Messages**

Event	System Log Example	Description	Action
ROGUE AP DETECTED	Oct 13 11:11:31 172.18.37.201 ALARM: 1255432835  system   info   ALR   ROGUE AP DETECTED CRITICAL CONTROLLER (1:13) ROGUE AP DETECTED. AP mac=00:1f:28:57:fa:b7 bss=00:1f:28:57:fa:b7 cch= 6 ess=Integral by AP AP-204 (204)	A rogue AP has been detected.	
ROGUE AP REMOVED	Mar 29 13:12:43 172.18.86.229 ALARM: 1269864763  system   info   ALR   ROGUE AP REMOVED CONTROLLER (1:24490) ROGUE AP DETECTED. AP mac=00:12:f2:00:17:63 bss=00:12:f2:00:17:63 cch=161 ess=rogue-35	A rogue AP has been removed.	

## Licensing System Log Messages

[Table 8](#) lists messages generated for licensing events.

**Table 8: Licensing System Log Messages**

Event	System Log Example	Description	Action
LICENSE EXPIRE WARNING	Mar 22 15:27:42 172.18.65.202 ALARM: 1205970893  system   notice   NOT   controller license expires in 1 day	Notification that license expires in one day.	Install a license for the software.
LICENSE EXPIRE WARNING	Mar 22 15:33:46 172.18.65.202 ALARM: 1205971257  system   notice   NOT   controller license expires tonight at midnight.	Notification that license expires by midnight.	Install a license for the software.
LICENSE EXPIRED	Mar 22 15:42:17 172.18.65.202 ALARM: 1206057655  system   info   ALR   SOFTWARE LICENSE EXPIRED MAJOR controller license has already expired.	License has expired.	Install a license for the software.
LICENSE EXPIRED ALARM CLEAR	Mar 22 15:52:23 172.18.65.202 ALARM: 1206058262  system   info   ALR   SOFTWARE LICENSE EXPIRED CLEAR controller	License alarm cleared.	

## N+1 Redundancy System Log Messages

[Table 9](#) lists messages generated for N+1 redundancy events.

**Table 9: N+1 Redundancy System Log Messages**

Event	System Log Example	Description	Action
MASTER CONTROLLER DOWN	Apr 19 14:24:26 172.18.253.203 nplus1_Slave: ALERT: Master Controller has timed out: Regression1 172.18.253.201	Slave detects that master controller is not reachable. Slave moves to active state.	Diagnose the master controller.
PASSIVE TO ACTIVE SLAVE STATE TRANSITION	Apr 19 14:24:26 172.18.253.203 nplus1_Slave: Slave State: Passive->Active	Passive slave in transition to becoming active slave.	
ACTIVE SLAVE	May 15 16:07:49 172.18.32.201 nplus1_Slave: Slave State: Active	Slave in active state.	
ACTIVE TO PASSIVE SLAVE TRANSITION	May 15 16:07:59 172.18.32.201 nplus1_Slave: Slave State: Active->Passive	Slave detected that master controller is reachable, so slave becomes passive again.	
ACTIVE TO PASSIVE SLAVE TRANSITION	Apr 19 14:40:21 172.18.253.203 nplus1_Slave: NOTICE: Active Slave Controller (Regression1 172.18.253.201) -> Passive Slave (RegressionSlave 172.18.253.203)	Slave detected that master controller is reachable, so slave becomes passive again.	
PASSIVE SLAVE	Apr 19 14:40:21 172.18.253.203 nplus1_Slave: Slave State: Passive	Slave in passive state.	
MASTER CONTROLLER DOWN ALARM	May 15 16:07:49 172.18.32.201 ALARM: 1210847902   system   info   ALR   MASTER CONTROLER DOWN INFO	Master controller down alarm.	
MASTER CONTROLLER UP ALARM	May 15 16:07:59 172.18.32.201 ALARM: 1210847912   system   info   ALR   MASTER CONTROLER UP INFO	Master controller up alarm.	
SLAVE CONFIG SYNC	Apr 19 14:51:07 172.18.253.201 sshd[7465]: PAM_pam_init_handlers: no default config /etc/pam.d/other Apr 19 14:51:07 172.18.253.201 sshd[7465]: PAM_pam_init_handlers: no default config /etc/pam.d/other Apr 19 14:51:07 172.18.253.201 sshd[7465]: Accepted publickey for root from 172.18.253.203 port 34674 ssh2 Apr 19 14:51:07 172.18.253.201 PAM-env[7465]: Unable to open config file: No such file or directory	SSH system log messages are shown while slave is syncing certain configuration files with the master controller using scp.	