



Alcatel-Lucent 7705

SERVICE AGGREGATION ROUTER OS | RELEASE 4.0
SYSTEM MANAGEMENT GUIDE

Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

Copyright 2010 Alcatel-Lucent.
All rights reserved.

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent tries to ensure that this information accurately reflects information provided by the supplier, please refer to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

Table of Contents

Preface	27
Getting Started	31
Alcatel-Lucent 7705 SAR System Management Configuration Process	31
Notes on 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F	32
Security	35
Authentication, Authorization, and Accounting	36
Authentication	37
Local Authentication	38
RADIUS Authentication	39
TACACS+ Authentication	39
Authorization	40
Local Authorization	41
RADIUS Authorization	41
TACACS+ Authorization	41
Accounting	42
RADIUS Accounting	42
TACACS+ Accounting	42
Security Controls	44
When a Server Does Not Respond	44
Access Request Flow	44
Vendor-Specific Attributes (VSAs)	46
Sample User (VSA) Configuration	48
Alcatel-Lucent Dictionary	49
Other Security Features	50
Secure Shell (SSH)	50
CSM Filters and CSM Security	51
Exponential Login Backoff	53
Encryption	53
802.1x Network Access Control	53
Configuration Notes	54
Reference Sources	54
Configuring Security with CLI	55
Setting Up Security Attributes	56
Configuring Authentication	56
Configuring Authorization	57
Configuring Accounting	58
Security Configurations	59
Security Configuration Procedures	61
Configuring IPv4 or IPv6 Management Access Filters	61
Configuring IPv4 or IPv6 CPM (CSM) Filters	64
Configuring Password Management Parameters	65
Configuring Profiles	66
Configuring Users	68
Copying and Overwriting Users and Profiles	69

Table of Contents

Copying a User	69
Copying a Profile	71
Configuring SSH	73
Configuring Login Controls	73
RADIUS Configurations	75
Configuring RADIUS Authentication	75
Configuring RADIUS Authorization	76
Configuring RADIUS Accounting	77
Configuring 802.1x RADIUS Policies	78
TACACS+ Configurations	79
Enabling TACACS+ Authentication	79
Configuring TACACS+ Authorization	80
Configuring TACACS+ Accounting	81
Security Command Reference	83
Command Hierarchies	83
Command Descriptions	95
Configuration Commands	96
Show Commands	158
Clear Commands	179
Debug Commands	180
SNMP	181
SNMP Overview	182
SNMP Architecture	182
Management Information Base	183
SNMP Versions	183
Management Information Access Control	183
User-Based Security Model Community Strings	184
Views	184
Access Groups	185
Users	185
Which SNMP Version to Use?	186
Configuration Notes	187
Reference Sources	187
Configuring SNMP with CLI	189
SNMP Configuration Overview	190
Configuring SNMPv1 and SNMPv2c	190
Configuring SNMPv3	190
Basic SNMP Security Configuration	191
Configuring SNMP Components	192
Configuring a Community String	192
Configuring View Options	193
Configuring Access Options	194
Configuring USM Community Options	195
Configuring Other SNMP Parameters	196
SNMP Command Reference	197
Command Hierarchies	197
Command Descriptions	200
Configuration Commands	201
Show Commands	211

Event and Accounting Logs	223
Logging Overview	224
Log Destinations	226
Console	226
Session	226
Memory Logs	226
Log Files	227
SNMP Trap Group	228
Syslog	229
Event Logs	230
Event Sources	230
Event Control	232
Log Manager and Event Logs	234
Event Filter Policies	234
Event Log Entries	235
Simple Logger Event Throttling	237
Default System Log	238
Accounting Logs	239
Accounting Records	239
Accounting Files	242
Design Considerations	242
Configuration Notes	243
Reference Sources	243
Configuring Logging with CLI	245
Log Configuration Overview	246
Log Type	247
Basic Event Log Configuration	248
Common Configuration Tasks	249
Configuring an Event Log	249
Configuring a File ID	250
Configuring an Accounting Policy	251
Configuring Event Control	252
Configuring Throttle Rate	253
Configuring a Log Filter	254
Configuring an SNMP Trap Group	256
Configuring a Syslog Target	257
Log Management Tasks	258
Modifying a Log File	258
Deleting a Log File	260
Modifying a File ID	261
Deleting a File ID	262
Modifying a Syslog ID	262
Deleting a Syslog ID	263
Modifying an SNMP Trap Group	263
Deleting an SNMP Trap Group	264
Modifying a Log Filter	265
Deleting a Log Filter	266
Modifying Event Control Parameters	267
Returning to the Default Event Control Configuration	268

Table of Contents

Log Command Reference	269
Command Hierarchies	269
Command Descriptions	274
Configuration Commands	275
Show Commands	310
Clear Commands	329
Standards and Protocol Support	331

List of Tables

Getting Started	31
Table 1: Management Configuration Process	31
Table 2: 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F Comparison	32
Security	35
Table 3: Supported Authorization Configurations	40
Table 4: Security Configuration Requirements	56
Table 5: 16-bit Mask Formats	104
Table 6: IP Protocol IDs and Descriptions	112
Table 7: IP Option Formats	118
Table 8: Show System Security Access Group Output Fields	159
Table 9: Show System Security Authentication Output Fields	162
Table 10: Show Communities Output Fields	163
Table 11: Show CPM Filter Output Fields	165
Table 12: Show Management Access Filter Output Fields	168
Table 13: Show Password Options Output Fields	169
Table 14: Show User Profile Output Fields	171
Table 15: Show Source Address Output Fields	172
Table 16: Show SSH Output Fields	173
Table 17: Show User Output Fields	175
Table 18: Show View Output Fields	177
Table 19: Show Users Output Fields	178
SNMP	181
Table 20: Show SNMP Counters Output Fields	212
Table 21: Show System Information Output Fields	214
Table 22: Show System Access Group Fields	218
Table 23: Show Communities Output Fields	219
Table 24: Show User Output Fields	220
Table 25: Show System Security View Output Fields	222
Event and Accounting Logs	223
Table 26: Event Severity Levels	225
Table 27: 7705 SAR to Syslog Severity Level Mappings	229
Table 28: Valid Filter Policy Operators	235
Table 29: Log Entry Field Descriptions	236
Table 30: Accounting Record Name and Collection Periods	239
Table 31: Accounting Record Name Details	240

List of Tables

Table 32:	Accounting Record Names	280
Table 33:	Valid Facility Codes	297
Table 34:	Threshold Severity Level Values	299
Table 35:	Accounting Policy Output Fields	311
Table 36:	Accounting Records Output Fields	312
Table 37:	Event Control Output Fields	316
Table 38:	Log File Summary Output Fields	318
Table 39:	Filter ID Summary Output Fields	319
Table 40:	Filter ID Match Criteria Output Fields	320
Table 41:	Log Collector Output Fields	322
Table 42:	Log ID Output Fields	324
Table 43:	SNMP Trap Group Output Fields	327
Table 44:	Syslog Output Fields	328

List of Figures

Security	35
Figure 1: RADIUS Requests and Responses	37
Figure 2: Security Flow	45
Event and Accounting Logs	223
Figure 3: Event Logging Block Diagram	230

List of Acronyms

Acronym	Expansion
2G	second generation wireless telephone technology
3DES	triple DES (data encryption standard)
3G	third generation mobile telephone technology
5620 SAM	5620 Service Aware Manager
7705 SAR	7705 Service Aggregation Router
7710 SR	7710 Service Router
7750 SR	7750 Service Router
9500 MPR	9500 Microwave Packet Radio
ABR	available bit rate area border router
AC	alternating current attachment circuit
ACK	acknowledge
ACL	access control list
ACR	adaptive clock recovery
ADP	automatic discovery protocol
AFI	authority and format identifier
AIS	alarm indication signal
ANSI	American National Standards Institute
Apipe	ATM VLL
APS	automatic protection switching
ARP	address resolution protocol
A/S	active/standby
AS	autonomous system

Acronym	Expansion
ASAP	any service, any port
ASBR	autonomous system boundary router
ASN	autonomous system number
ATM	asynchronous transfer mode
ATM PVC	ATM permanent virtual circuit
B3ZS	bipolar with three-zero substitution
Batt A	battery A
B-bit	beginning bit (first packet of a fragment)
Bellcore	Bell Communications Research
BFD	bidirectional forwarding detection
BGP	border gateway protocol
BITS	building integrated timing supply
BMCA	best master clock algorithm
BMU	<p>broadcast, multicast, and unknown traffic</p> <p>Traffic that is not unicast. Any nature of multipoint traffic:</p> <ul style="list-style-type: none"> • broadcast (that is, all 1s as the destination IP to represent all destinations within the subnet) • multicast (that is, traffic typically identified by the destination address, uses special destination address); for IP, the destination must be 224.0.0.0 to 239.255.255.255 • unknown (that is, the destination is typically a valid unicast address but the destination port/interface is not yet known; therefore, traffic needs to be forwarded to all destinations; unknown traffic is treated as broadcast)
BOF	boot options file
BPDU	bridge protocol data unit
BRAS	Broadband Remote Access Server
BSC	Base Station Controller
BSTA	Broadband Service Termination Architecture

Acronym	Expansion
BTS	base transceiver station
CAS	channel associated signaling
CBN	common bonding networks
CBS	committed buffer space
CC	control channel continuity check
CCM	continuity check message
CE	customer edge circuit emulation
CEM	circuit emulation
CES	circuit emulation services
CESoPSN	circuit emulation services over packet switched network
CFM	connectivity fault management
CIDR	classless inter-domain routing
CIR	committed information rate
CLI	command line interface
CLP	cell loss priority
CoS	class of service
CPE	customer premises equipment
Cpipe	circuit emulation (or TDM) VLL
CPM	Control and Processing Module (CPM is used instead of CSM when referring to CSM filtering to align with CLI syntax used with other SR products). CSM management ports are referred to as CPM management ports in the CLI.
CPU	central processing unit
CRC	cyclic redundancy check
CRON	a time-based scheduling service (from chronos = time)

Acronym	Expansion
CSM	Control and Switching Module
CSNP	complete sequence number PDU
CSPF	constrained shortest path first
C-TAG	customer VLAN tag
CV	connection verification customer VLAN (tag)
CW	control word
DC	direct current
DC-C	DC return - common
DCE	data communications equipment
DC-I	DC return - isolated
DCO	digitally controlled oscillator
DDoS	distributed DoS
DES	data encryption standard
DF	do not fragment
DHB	decimal, hexadecimal, or binary
DHCP	dynamic host configuration protocol
DHCPv6	dynamic host configuration protocol for IPv6
DIS	designated intermediate system
DM	delay measurement
DNS	domain name server
DoS	denial of service
dot1p	IEEE 802.1p bits, found in Ethernet or VLAN ingress packet headers and used to map traffic to up to eight forwarding classes
dot1q	IEEE 802.1q encapsulation for Ethernet interfaces
DPI	deep packet inspection

Acronym	Expansion
DPLL	digital phase locked loop
DSCP	differentiated services code point
DSL	digital subscriber line
DSLAM	digital subscriber line access multiplexer
DTE	data termination equipment
DU	downstream unsolicited
DUID	DHCP unique identifier
DV	delay variation
e911	enhanced 911 service
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
E-bit	ending bit (last packet of a fragment)
ECMP	equal cost multi-path
EFM	Ethernet in the first mile
EGP	exterior gateway protocol
EIA/TIA-232	Electronic Industries Alliance/Telecommunications Industry Association Standard 232 (also known as RS-232)
ELER	egress label edge router
E&M	ear and mouth earth and magneto exchange and multiplexer
Epipe	Ethernet VLL
EPL	Ethernet private line
ERO	explicit route object
ESD	electrostatic discharge
ESMC	Ethernet synchronization message channel
ETE	end-to-end

Acronym	Expansion
ETH-CFM	Ethernet connectivity fault management (IEEE 802.1ag)
EVDO	evolution - data optimized
EVPL	Ethernet virtual private link
EXP bits	experimental bits (currently known as TC)
FC	forwarding class
FCS	frame check sequence
FDB	forwarding database
FDL	facilities data link
FEAC	far-end alarm and control
FEC	forwarding equivalence class
FF	fixed filter
FIB	forwarding information base
FIFO	first in, first out
FNG	fault notification generator
FOM	figure of merit
FRR	fast reroute
FTN	FEC-to-NHLFE
FTP	file transfer protocol
GFP	generic framing procedure
GigE	Gigabit Ethernet
GRE	generic routing encapsulation
GSM	Global System for Mobile Communications (2G)
HCM	high capacity multiplexing
HDB3	high density bipolar of order 3
HEC	header error control
HMAC	hash message authentication code

Acronym	Expansion
HSDPA	high-speed downlink packet access
HSPA	high-speed packet access
HVPLS	hierarchical virtual private line service
IANA	internet assigned numbers authority
IBN	isolated bonding networks
ICMP	Internet control message protocol
ICMPv6	Internet control message protocol for IPv6
ICP	IMA control protocol cells
IEEE	Institute of Electrical and Electronics Engineers
IEEE 1588v2	Institute of Electrical and Electronics Engineers standard 1588-2008
IES	Internet Enhanced Service
IETF	Internet Engineering Task Force
IGP	interior gateway protocol
ILER	ingress label edge router
ILM	incoming label map
IMA	inverse multiplexing over ATM
IOM	input/output module
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPIP	IP in IP
Ipipe	IP interworking VLL
IPoATM	IP over ATM
IS-IS	Intermediate System-to-Intermediate System
IS-IS-TE	IS-IS-traffic engineering (extensions)
ISO	International Organization for Standardization

Acronym	Expansion
LB	loopback
lbf-in	pound force inch
LBM	loopback message
LBO	line buildout
LBR	loopback reply
LCP	link control protocol
LDP	label distribution protocol
LER	label edge router
LFIB	label forwarding information base
LIB	label information base
LLDP	link layer discovery protocol
LLDPDU	link layer discovery protocol data unit
LLF	link loss forwarding
LLID	loopback location ID
LM	loss measurement
LSA	link-state advertisement
LSDB	link-state database
LSP	label switched path link-state PDU (for IS-IS)
LSR	label switch router link-state request
LSU	link-state update
LT	linktrace
LTE	line termination equipment
LTM	linktrace message
LTN	LSP ID to NHLFE

Acronym	Expansion
LTR	linktrace reply
MA	maintenance association
MAC	media access control
MA-ID	maintenance association identifier
MBB	make-before-break
MBS	maximum buffer space maximum burst size media buffer space
MBSP	mobile backhaul service provider
MC-MLPPP	multi-class multilink point-to-point protocol
MD	maintenance domain
MD5	message digest version 5 (algorithm)
MDA	media dependent adapter
MDDDB	multidrop data bridge
MDL	maintenance data link
ME	maintenance entity
MED	multi-exit discriminator
MEF	Metro Ethernet Forum
MEG	maintenance entity group
MEG-ID	maintenance entity group identifier
MEN	Metro Ethernet network
MEP	maintenance association end point
MFC	multi-field classification
MHF	MIP half function
MIB	management information base
MIP	maintenance association intermediate point

Acronym	Expansion
MIR	minimum information rate
MLPPP	multilink point-to-point protocol
MP	merge point multilink protocol
MP-BGP	multiprotocol border gateway protocol
MPLS	multiprotocol label switching
MPR	see 9500 MPR
MRRU	maximum received reconstructed unit
MRU	maximum receive unit
MSDU	MAC Service Data Unit
MS-PW	multi-segment pseudowire
MTIE	maximum time interval error
MTSO	mobile trunk switching office
MTU	maximum transmission unit multi-tenant unit
M-VPLS	management virtual private line service
MW	microwave
N·m	newton meter
NBMA	non-broadcast multiple access (network)
NE	network element
NET	network entity title
NHLFE	next hop label forwarding entry
NHOP	next-hop
NLRI	network layer reachability information
NNHOP	next next-hop
NNI	network-to-network interface

Acronym	Expansion
Node B	similar to BTS but used in 3G networks — term is used in UMTS (3G systems) while BTS is used in GSM (2G systems)
NSAP	network service access point
NSSA	not-so-stubby area
NTP	network time protocol
OAM	operations, administration, and maintenance
OAMPDU	OAM protocol data units
OC3	optical carrier, level 3
ORF	outbound route filtering
OS	operating system
OSI	Open Systems Interconnection (reference model)
OSINLCP	OSI Network Layer Control Protocol
OSPF	Open Shortest Path First
OSPF-TE	OSPF-traffic engineering (extensions)
OSS	operations support system
OSSP	Organization Specific Slow Protocol
OTP	one time password
PADI	PPPoE active discovery initiation
PADR	PPPoE active discovery request
PAE	port authentication entities
PCP	priority point code
PDU	protocol data units
PDV	packet delay variation
PDVT	packet delay variation tolerance
PE	provider edge router
PHB	per-hop behavior

Acronym	Expansion
PHY	physical layer
PID	protocol ID
PIR	peak information rate
PLCP	Physical Layer Convergence Protocol
PLR	point of local repair
POP	point of presence
POS	packet over SONET
PPP	point-to-point protocol
PPPoE	point-to-point protocol over Ethernet
PRC	primary reference clock
PSN	packet switched network
PSNP	partial sequence number PDU
PTP	precision time protocol performance transparency protocol
PVC	permanent virtual circuit
PVCC	permanent virtual channel connection
PW	pseudowire
PWE	pseudowire emulation
PWE3	pseudowire emulation edge-to-edge
QL	quality level
QoS	quality of service
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RBS	robbed bit signaling
RD	route distinguisher
RDI	remote defect indication

Acronym	Expansion
RED	random early discard
RESV	reservation
RIB	routing information base
RJ-45	registered jack 45
RNC	Radio Network Controller
RRO	record route object
RS-232	Recommended Standard 232 (also known as EIA/TIA-232)
RSHG	residential split horizon group
RSTP	Rapid Spanning Tree Protocol
RSVP-TE	resource reservation protocol - traffic engineering
RT	receive/transmit
RTM	routing table manager
RTN	battery return
RTP	real-time protocol
R&TTE	Radio and Telecommunications Terminal Equipment
RTU	remote terminal unit
RU	rack unit
SAA	service assurance agent
SAP	service access point
SAR-8	7705 Service Aggregation Router - 8-slot chassis
SAR-18	7705 Service Aggregation Router - 18-slot chassis
SAR-F	7705 Service Aggregation Router - fixed form-factor chassis
SAToP	structure-agnostic TDM over packet
SCADA	surveillance, control and data acquisition
SCP	secure copy
SD	signal degrade

Acronym	Expansion
SDH	synchronous digital hierarchy
SDI	serial data interface
SDP	service destination point
SE	shared explicit
SF	signal fail
SFP	small form-factor pluggable (transceiver)
SGT	self-generated traffic
SHA-1	secure hash algorithm
SHG	split horizon group
SIR	sustained information rate
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNPA	subnetwork point of attachment
SNTP	simple network time protocol
SONET	synchronous optical networking
S-PE	switching provider edge router
SPF	shortest path first
SPT	shortest path tree
SR	service router (includes 7710 SR, 7750 SR)
SRLG	shared risk link group
SSH	secure shell
SSM	synchronization status messaging
SSU	system synchronization unit
S-TAG	service VLAN tag
STM1	synchronous transport module, level 1
SVC	switched virtual circuit

Acronym	Expansion
SYN	synchronize
TACACS+	Terminal Access Controller Access-Control System Plus
TC	traffic class (formerly known as EXP bits)
TCP	transmission control protocol
TDEV	time deviation
TDM	time division multiplexing
TE	traffic engineering
TFTP	trivial file transfer protocol
TLDP	targeted LDP
TLV	type length value
ToS	type of service
T-PE	terminating provider edge router
TPID	tag protocol identifier
TPMR	two-port MAC relay
TTL	time to live
TTM	tunnel table manager
U-APS	unidirectional automatic protection switching
UBR	unspecified bit rate
UDP	user datagram protocol
UMTS	Universal Mobile Telecommunications System (3G)
UNI	user-to-network interface
V.35	V-series Recommendation 35
VC	virtual circuit
VCC	virtual channel connection
VCCV	virtual circuit connectivity verification
VCI	virtual circuit identifier

Acronym	Expansion
VID	VLAN ID
VLAN	virtual LAN
VLL	virtual leased line
VoIP	voice over IP
Vp	peak voltage
VP	virtual path
VPC	virtual path connection
VPI	virtual path identifier
VPLS	virtual private LAN service
VPN	virtual private network
VPRN	virtual private routed network
VRF	virtual routing and forwarding table
VSE	vendor-specific extension
VSO	vendor-specific option
WCDMA	wideband code division multiple access (transmission protocol used in UMTS networks)
WRED	weighted random early discard
WTR	wait to restore

Preface

About This Guide

This guide describes general information you will need to configure router security, SNMP features, and event and accounting logs. It covers basic tasks such as configuring management access filters that control traffic in and out of the CSM, passwords, user profiles, security such as RADIUS, TACACS+, and SSH servers, the router clock, and virtual routers.

This guide is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

Audience

This guide is intended for network administrators who are responsible for configuring the 7705 SAR. It is assumed that the network administrators have an understanding of networking principles and configurations. Protocols, standards, and processes described in this guide include the following:

- CLI concepts
- system and user access and security
- SNMP
- event and accounting logs

List of Technical Publications

The 7705 SAR OS documentation set is composed of the following guides:

- 7705 SAR OS Basic System Configuration Guide
This guide describes basic system configurations and operations.
- 7705 SAR OS System Management Guide
This guide describes system security and access configurations as well as event logging and accounting logs.
- 7705 SAR OS Interface Configuration Guide
This guide describes card and port provisioning.
- 7705 SAR OS Router Configuration Guide
This guide describes logical IP routing interfaces, IP-based filtering, and routing policies.
- 7705 SAR OS MPLS Guide
This guide describes how to configure Multiprotocol Label Switching (MPLS), Resource Reservation Protocol for Traffic Engineering (RSVP-TE), and Label Distribution Protocol (LDP).
- 7705 SAR OS Services Guide
This guide describes how to configure service parameters such as service access points (SAPs), service destination points (SDPs), customer information, and user services.
- 7705 SAR OS Quality of Service Guide
This guide describes how to configure Quality of Service (QoS) policy management.
- 7705 SAR OS Routing Protocols Guide
This guide provides an overview of dynamic routing concepts and describes how to configure them.
- 7705 SAR OS OAM and Diagnostics Guide
This guide provides information on Operations, Administration and Maintenance (OAM) tools.

Multiple PDF File Search

You can use Adobe Reader, Release 6.0 or later, to search multiple PDF files for a term. Adobe Reader displays the results in a display panel. The results are grouped by PDF file. You can expand the entry for each file.



Note: The PDF files in which you search must be in the same folder.

To search multiple PDF files for a term:

Step 1. Open Adobe Reader.

Step 2. Choose Edit – Search from the Adobe Reader main menu. The Search panel appears.

Step 3. Enter the term to search for.

Step 4. Select the All PDF Documents in radio button.

Step 5. Choose the folder in which to search using the drop-down menu.

Step 6. Select the following criteria if required:

- Whole words only
- Case-Sensitive
- Include Bookmarks
- Include Comments

Step 7. Click on the Search button.

Adobe Reader displays the search results. You can expand the entries for each file by clicking on the + symbol.

Step 8. Click on a search result to go directly to that location in the selected file.

Technical Support

If you purchased a service agreement for your 7705 SAR router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, check this link for instructions to contact Support personnel:

Web: <http://support.alcatel-lucent.com>

Getting Started

In This Chapter

This chapter provides process flow information to configure system security and access functions as well as event and accounting logs.

Alcatel-Lucent 7705 SAR System Management Configuration Process

[Table 1](#) lists the tasks necessary to configure system security and access functions and logging features.

Each chapter in this book is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 1: Management Configuration Process

Area	Task	Chapter
System security	Configure system security parameters, such as authentication, authorization, and accounting	Security
Network management	Configure SNMP elements	SNMP
Operational functions	Configure event and accounting logs	Event and Accounting Logs
Reference	List of IEEE, IETF, and other proprietary entities	Standards and Protocol Support

Notes on 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F

The 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F run the same operating system software. The main difference between the products is their hardware platforms.

The 7705 SAR-8 is an 8-slot chassis that supports 2 CSMs, a Fan module, and 6 adapter cards. The 7705 SAR-18 chassis has 18 slots; in Release 4.0, it supports 2 CSMs, a Fan module, an Alarm module, and 12 adapter cards.

The 7705 SAR-F chassis has a fixed hardware configuration. The 7705 SAR-F replaces the CSM, Fan module, and the 16-port T1/E1 ASAP Adapter card and 8-port Ethernet Adapter card with an all-in-one unit that provides comparable functional blocks, as detailed in [Table 2](#).

The fixed configuration of the 7705 SAR-F means that provisioning the router at the “card slot” and “type” levels is preset and is not user-configurable. Operators begin configurations at the port level.



Note: Unless stated otherwise, references to the terms “Adapter card” and “CSM” throughout the 7705 SAR OS documentation set include the equivalent functional blocks on the 7705 SAR-F.

Table 2: 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F Comparison

7705 SAR-8, 7705 SAR-18	7705 SAR-F	Notes
CSM	Control and switching functions	The control and switching functions include the console and management interfaces, the alarm and fan functions, the synchronization interfaces, system LEDs, and so on.
Fan module	Integrated with the control and switching functions	

Table 2: 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F Comparison (Continued)

7705 SAR-8, 7705 SAR-18	7705 SAR-F	Notes
16-port T1/E1 ASAP Adapter card	16 individual T1/E1 ports on the faceplate	<p>The T1/E1 ports on the 7705 SAR-F are equivalent to the T1/E1 ports on the 16-port T1/E1 ASAP Adapter card, version 1, except that the 16 T1/E1 ports on the 7705 SAR-F support multiple synchronization sources to support two timing references. The 16-port T1/E1 ASAP Adapter card, version 2, also supports two timing references.</p> <p>On the 7705 SAR-8 and 7705 SAR-18, the CLI indicates the MDA type for the 16-port T1/E1 ASAP Adapter card as <code>a16-chds1</code> for version 1 and <code>a16-chds1v2</code> for version 2.</p> <p>On the 7705 SAR-F, the CLI indicates the MDA type for the 7705 SAR-F ports as <code>i16-chds1</code>.</p>
8-port Ethernet Adapter card	8 individual Ethernet ports on the faceplate	<p>The –48 VDC versions of the 7705 SAR-8 support two versions of the 8-port Ethernet Adapter card, with version 2 having additional support for Synchronous Ethernet. The +24 VDC version of the 7705 SAR-8 supports only version 2 of the 8-port Ethernet Adapter card.</p> <p>The 7705 SAR-18 supports only version 2 of the card.</p> <p>The Ethernet ports on the 7705 SAR-F are functionally equivalent to the Ethernet ports on version 2 of the 8-port Ethernet Adapter card and support multiple synchronization sources to support two timing references.</p> <p>On the 7705 SAR-8, the CLI indicates the MDA type for the 8-port Ethernet Adapter card as <code>a8-eth</code> or <code>a8-ethv2</code>. On the 7705 SAR-18, the CLI indicates the MDA type as <code>a8-ethv2</code>. On the 7705 SAR-F, the CLI indicates the MDA type for the 7705 SAR-F Ethernet ports as <code>i8-eth</code>.</p>
Requires user configuration at card (IOM) and MDA (adapter card) levels	Configuration at card (IOM) and MDA (adapter card) levels is preset and users cannot change these types	

In This Chapter

This chapter provides information to configure security parameters. Topics in this chapter include:

- [Authentication, Authorization, and Accounting on page 36](#)
 - [Authentication on page 37](#)
 - [Authorization on page 40](#)
 - [Accounting on page 42](#)
- [Security Controls on page 44](#)
 - [When a Server Does Not Respond on page 44](#)
 - [Access Request Flow on page 44](#)
- [Vendor-Specific Attributes \(VSAs\) on page 46](#)
 - [Sample User \(VSA\) Configuration on page 48](#)
- [Other Security Features on page 50](#)
 - [Secure Shell \(SSH\) on page 50](#)
 - [CSM Filters and CSM Security on page 51](#)
 - [Exponential Login Backoff on page 53](#)
 - [Encryption on page 53](#)
 - [802.1x Network Access Control on page 53](#)
- [Configuration Notes on page 54](#)
- [Configuring Security with CLI on page 55](#)
- [Security Command Reference on page 83](#)

Authentication, Authorization, and Accounting

This chapter describes authentication, authorization, and accounting (AAA) used to monitor and control network access on the 7705 SAR. Network security is based on a multi-step process. The first step, authentication, validates a user's name and password. The second step is authorization, which allows the user to access and execute commands at various command levels based on profiles assigned to the user.

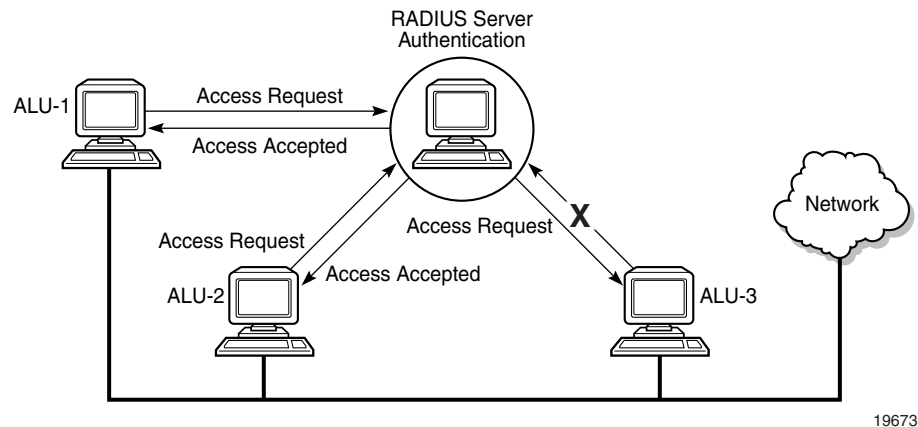
The third step, accounting, keeps track of the activity of a user who has accessed the network. The type of accounting information recorded can include a history of the commands executed, the amount of time spent in the session, the services accessed, and the data transfer size during the session. The accounting data can then be used to analyze trends, and also for billing and auditing purposes.

You can configure the 7705 SAR to use local, Remote Authentication Dial In User Service (RADIUS), or Terminal Access Controller Access Control System Plus (TACACS+) security to validate users who attempt to access the router by console, Telnet, or FTP. You can select the authentication order that determines the authentication method to try first, second, and third.

The 7705 SAR supports the following security features:

- RADIUS can be used for authentication, authorization, and accounting
- TACACS+ can be used for authentication, authorization, and accounting
- local security can be implemented for authentication and authorization

[Figure 1](#) depicts end-user access requests sent to a RADIUS server. After validating the user names and passwords, the RADIUS server returns an access accept message to the users on ALU-1 and ALU-2. The user name and password from ALU-3 could not be authenticated, thus access was denied.

Figure 1: RADIUS Requests and Responses

19673

Authentication

Authentication validates a user name and password combination when a user attempts to log in.

When a user attempts to log in through the console, Telnet, SSH, SCP, or FTP, the 7705 SAR client sends an access request to a RADIUS, TACACS+, or local database.

Transactions between the client and a RADIUS server are authenticated through the use of a shared secret. The secret is never transmitted over the network. User passwords are sent encrypted between the client and RADIUS server, which prevents someone snooping on an insecure network to learn password information.

If the RADIUS server does not respond within a specified time, the router issues the access request to the next configured servers. Each RADIUS server must be configured identically to guarantee consistent results. Up to five RADIUS servers can be configured.

If a server is unreachable, it will not be used again by the RADIUS application until 30 seconds have elapsed, to give the server time to recover from its unreachable state. After 30 seconds, the unreachable server becomes available again for the RADIUS application.

If, within the 30 seconds, the RADIUS server receives a valid response to a previously sent RADIUS packet on that unreachable server, the server immediately becomes available again.

If any RADIUS server rejects the authentication request, it sends an access reject message to the router. In this case, no access request is issued to any other RADIUS servers. However, if other authentication methods such as TACACS+ and/or local are configured, then these methods are attempted. If no other authentication methods are configured, or all methods reject the authentication request, then access is denied.

The user login is successful when the RADIUS server accepts the authentication request and responds to the router with an access accept message.

Implementing authentication without authorization for the 7705 SAR does not require the configuration of VSAs (Vendor Specific Attributes) on the RADIUS server. However, users, user access permissions, and command authorization profiles must be configured on each router.

Any combination of these authentication methods can be configured to control network access from a 7705 SAR router:

- [Local Authentication](#)
- [RADIUS Authentication](#)
- [TACACS+ Authentication](#)

Local Authentication

Local authentication uses user names and passwords configured on the router to authenticate login attempts. The user names and passwords are local to each router, not to user profiles.

By default, local authentication is enabled. When one or more of the other security methods are enabled, local authentication is disabled. Local authentication is restored when the other authentication methods are disabled. Local authentication is attempted if the other authentication methods fail and local is included in the authentication order password parameters.

Locally, you can configure user names and password management information. This is referred to as local authentication. Remote security servers such as RADIUS or TACACS+ are not enabled.

RADIUS Authentication

Remote Authentication Dial-In User Service (RADIUS) is a client/server security protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize access to the requested system or service.

RADIUS allows you to maintain user profiles in a shared central database and provides better security, allowing a company to set up a policy that can be applied at a single administered network point.

RADIUS Server Selection

Up to five RADIUS servers can be configured. They can be selected to authenticate user requests in two ways, using either the direct method or the round-robin method. The default method is direct.

Direct

In direct mode, the first server, as defined by the `server-index` command, is the primary server. This server is always used first when authenticating a request.

Round-robin

In round-robin mode, the server used to authenticate a request is the next server in the list, following the last authentication request. For example, if server 1 is used to authenticate the first request, server 2 is used to authenticate the second request, and so on.

TACACS+ Authentication

Terminal Access Controller Access Control System, commonly referred to as TACACS, is an authentication protocol that allows a remote access server to forward a user's login password to an authentication server to determine whether access can be allowed to a given system. TACACS is an encryption protocol and therefore less secure than the later Terminal Access Controller Access Control System Plus (TACACS+) and RADIUS protocols.

TACACS+ and RADIUS have largely replaced earlier protocols in the newer or recently updated networks. TACACS+ uses Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). TACACS+ is popular as TCP is thought to be a more reliable protocol. RADIUS combines authentication and authorization. TACACS+ separates these operations.

Authorization

The 7705 SAR supports local, RADIUS, and TACACS+ authorization to control the actions of specific users by applying a profile based on user name and password configurations once network access is granted. The profiles are configured locally as well as on the RADIUS server as VSAs. See [Vendor-Specific Attributes \(VSAs\)](#).

Once a user has been authenticated using RADIUS (or another method), the 7705 SAR router can be configured to perform authorization. The RADIUS server can be used to:

- download the user profile to the 7705 SAR router
- send the profile name that the node should apply to the 7705 SAR router

Profiles consist of a suite of commands that the user is allowed or not allowed to execute. When a user issues a command, the authorization server looks at the command and the user information and compares it with the commands in the profile. If the user is authorized to issue the command, the command is executed. If the user is not authorized to issue the command, then the command is not executed.

Profiles must be created on each 7705 SAR router and should be identical for consistent results. If the profile is not present, then access is denied.

[Table 3](#) displays the following scenarios.

- If the user is authenticated locally (on the 7705 SAR router), local authorization is supported and remote (RADIUS) authorization cannot be performed.
- If the user is authenticated by the RADIUS server, both local authorization and remote (RADIUS) authorization are supported.
- If the user is TACACS+ authenticated, local authorization is supported and remote (RADIUS) authorization cannot be performed.

When authorization is configured and profiles are downloaded to the router from the RADIUS server, the profiles are considered temporary configurations and are not saved when the user session terminates.

Table 3: Supported Authorization Configurations

	Local Authorization	RADIUS Authorization
7705 SAR configured user	Supported	Not Supported
RADIUS server configured user	Supported	Supported
TACACS+ server configured user	Supported	Not Supported

When using authorization, maintaining a user database on the router is not required. User names can be configured on the RADIUS server. User names and their associated passwords are temporary and are not saved in the configuration database when the user session terminates.

- [Local Authorization](#)
- [RADIUS Authorization](#)
- [TACACS+ Authorization](#)

Local Authorization

Local authorization uses user profiles and user access information after a user is authenticated. The profiles and user access information specify the actions the user can and cannot perform.

By default, local authorization is enabled. Local authorization is disabled only when a different remote authorization method is configured (RADIUS authorization or TACACS+). Local authorization is restored when RADIUS authorization is disabled.

You must configure profile and user access information locally.

RADIUS Authorization

RADIUS authorization grants or denies access permissions for a 7705 SAR router. Permissions include the use of FTP, Telnet, SSH (SCP), and console access. When granting Telnet, SSH (SCP) and console access to the 7705 SAR router, authorization can be used to limit what CLI commands the user is allowed to issue and which file systems the user is allowed or denied access to.

TACACS+ Authorization

Like RADIUS authorization, TACACS+ grants or denies access permissions for a 7705 SAR router. The TACACS+ server sends a response based on the user name and password.

TACACS+ separates the authentication and authorization functions. RADIUS combines the authentication and authorization functions.

Accounting

Accounting tracks user activity to a specific host. The 7705 SAR supports RADIUS and TACACS+ accounting.

RADIUS Accounting

When enabled, RADIUS accounting sends command line accounting from the 7705 SAR router to the RADIUS server. The router sends accounting records using UDP packets at port 1813 (decimal).

The router issues an accounting request packet for each event requiring the activity to be recorded by the RADIUS server. The RADIUS server acknowledges each accounting request by sending an accounting response after it has processed the accounting request. If no response is received in the time defined in the timeout parameter, the accounting request must be retransmitted until the configured retry count is exhausted. A trap is issued to alert the NMS (or trap receiver) that the server is unresponsive. The router issues the accounting request to the next configured RADIUS server (up to 5).

User passwords and authentication keys of any type are never transmitted as part of the accounting request.

When RADIUS accounting is enabled, the server is responsible for receiving accounting requests and returning a response to the client indicating that it has successfully received the request. Each command issued on the 7705 SAR router generates a record sent to the RADIUS server. The record identifies the user who issued the command and the timestamp.

Accounting can be configured independently from RADIUS authorization and RADIUS authentication.

TACACS+ Accounting

The 7705 SAR allows you to configure the type of accounting record packet that is to be sent to the TACACS+ server when specified events occur on the device. The accounting **record-type** parameter indicates whether TACACS+ accounting start and stop packets will be sent or just stop packets will be sent. A start packet is sent to a TACACS+ server when an authenticated user establishes a Telnet or SSH session and a stop packet is sent when the user logs out.

When a user logs in to request access to the network using Telnet or SSH, or a user enters a command for which accounting parameters are configured, or a system event occurs, such as a reboot or a configuration file reload, the 7705 SAR checks the configuration to see if TACACS+ accounting is required for the particular event.

If TACACS+ accounting is required, then, depending on the accounting record type specified, the device sends a start packet to the TACACS+ accounting server that contains information about the event.

The TACACS+ accounting server acknowledges the start packet and records information about the event. When the event ends, the device sends a stop packet. The stop packet is acknowledged by the TACACS+ accounting server.

Security Controls

You can configure the 7705 SAR to use RADIUS, TACACS+, and local authentication to validate users requesting access to the network. The order in which password authentication is processed among RADIUS, TACACS+ and local passwords can be specifically configured. For example, the authentication order can be configured to process authorization via TACACS+ first, then RADIUS for authentication and accounting. Local access can be specified next in the authentication order in the event that the RADIUS and TACACS+ servers are not operational.

When a Server Does Not Respond

A trap is issued if a RADIUS server is unresponsive. An alarm is raised if RADIUS is enabled with at least one RADIUS server and no response is received to either accounting or user access requests from any server.

Periodic checks to determine if the primary server is responsive again are performed. If a server is down, it will not be contacted for 5 minutes. If a login is attempted after 5 minutes, then the server is contacted again. If a server has the health check feature enabled and is unresponsive, the server's status is checked every 30 seconds. Health check is enabled by default. When a service response is restored from at least one server, the alarm condition is cleared. Alarms are raised and cleared on the Alcatel-Lucent Fault Manager or other third party fault management servers.

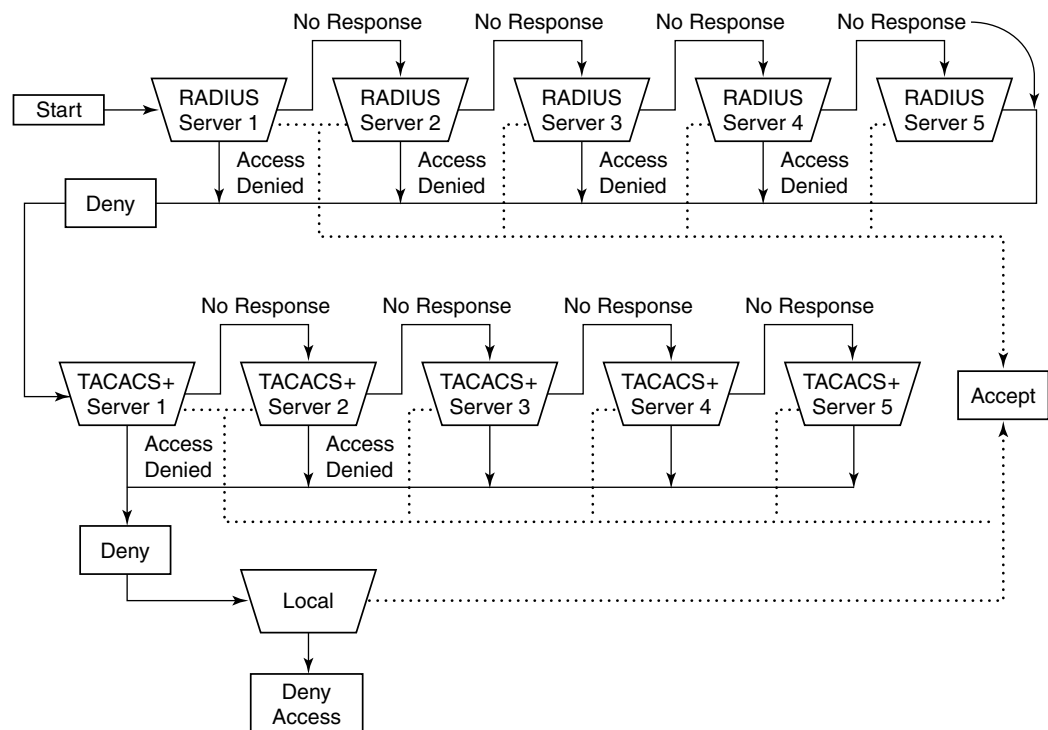
The servers are accessed in order from lowest to highest specified index (from 1 to 5) for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server. If a response from the server is received, no other server is queried.

Access Request Flow

In [Figure 2](#), the authentication process is defined in the `config>system>security>password` context. The authentication order is determined by specifying the sequence in which password authentication is attempted among RADIUS, TACACS+, and local servers. This example uses the authentication order of RADIUS, then TACACS+, and finally, local. An access request is sent to RADIUS server 1. One of two scenarios can occur. If there is no response from the server, the request is passed to the next RADIUS server with the next lowest index (RADIUS server 2) and so on, until the last RADIUS server is attempted (RADIUS server 5). If server 5 does not respond, the request is passed to the TACACS+ server 1. If there is no response from that server, the request is passed to the next TACACS+ server with the next lowest index (TACACS+ server 2) and so on.

If a request is sent to an active RADIUS server and the user name and password are not recognized, access is denied and passed on to the next authentication option, in this case, the TACACS+ server. The process continues until the request is either accepted, denied, or each server is queried. Finally, if the request is denied by the active TACACS+ server, the local parameters are checked for user name and password verification. This is the last chance for the access request to be accepted.

Figure 2: Security Flow



19672

Vendor-Specific Attributes (VSAs)

The 7705 SAR software supports the configuration of Alcatel-Lucent-specific RADIUS attributes. These attributes are known as vendor-specific attributes (VSAs) and are discussed in RFC 2138. VSAs must be configured when RADIUS authorization is enabled. It is up to the vendor to specify the format of their VSA. The attribute-specific field is dependent on the vendor's definition of that attribute. The Alcatel-Lucent-defined attributes are encapsulated in a RADIUS vendor-specific attribute with the vendor ID field set to 6527, the vendor ID number.

Note that “PE-Record” should be added as a new standard attribute in the standard RADIUS dictionary file.

The following RADIUS VSAs are supported by Alcatel-Lucent:

- `timetra-access <ftp> <console> <both>` — this is a mandatory command that must be configured. This command specifies whether the user has FTP and /or console (serial port, Telnet, and SSH) access.
- `timetra-profile <profile-name>` — when configuring this VSA for a user, it is assumed that the user profiles are configured on the local 7705 SAR router and the following applies for local and remote authentication:
 - a. The `authentication-order` parameters configured on the router must include the `local` keyword.
- 9. The user name may or may not be configured on the 7705 SAR router.
- 10. The user must be authenticated by the RADIUS server.
- 11. Up to eight valid profiles can exist on the router for a user. The sequence in which the profiles are specified is relevant. The most explicit matching criteria must be ordered first. The process stops when the first complete match is found.

If all the above-mentioned conditions are not met, then access to the router is denied and a failed login event/trap is written to the security log.

- `timetra-default-action <permit-all | deny-all | none>` — this is a mandatory command that must be configured even if the `timetra-cmd` VSA is not used. This command specifies the default action when the user has entered a command and no entry configured in the `timetra-cmd` VSA for the user resulted in a match condition.
- `timetra-cmd <match-string>` — configures a command or command subtree as the scope for the match condition

The command and all subordinate commands in subordinate command levels are specified.

Configure from most specific to least specific. The 7705 SAR exits on the first match; subordinate levels cannot be modified with subsequent action commands. Subordinate level VSAs must be entered prior to this entry to be effective.

All commands at and below the hierarchy level of the matched command are subject to the `timetra-action` VSA.

Multiple match-strings can be entered in a single `timetra-cmd` VSA. Match strings must be semicolon (;) separated (maximum string length is 254 characters).

One or more `timetra-cmd` VSAs can be entered followed by a single `timetra-action` VSA:

- `timetra-action <deny | permit>` — causes the permit or deny action to be applied to all match strings specified since the last `timetra-action` VSA
- `timetra-home-directory <home-directory string>` — specifies the home directory that applies for the FTP and CLI user. If this VSA is not configured, the home directory is Compact Flash slot 1 (*cf3*: on all platforms).
- `timetra-restrict-to-home-directory <true | false>` — specifies if user access is limited to their home directory (and directories and files subordinate to their home directory). If this VSA is not configured, the user is allowed to access the entire file system.
- `timetra-login-exec <login-exec-string>` — specifies the login exec file that is executed when the user login is successful. If this VSA is not configured, no login exec file is applied.

If no VSAs are configured for a user, then the following applies.

- The password authentication-order command on the 7705 SAR router *must* include `local`.
- The user name must be configured on the 7705 SAR router.
- The user must be successfully authenticated by the RADIUS server.
- A valid profile must exist on the 7705 SAR router for this user.

If all conditions listed above are not met, then access to the 7705 SAR router is denied and a failed login event/trap is written to the security log.

For receiving data from the RADIUS server, the following are supported:

- Juniper (vendor-id 4874) attributes 4 (Primary DNS server) and 5 (Secondary DNS server)
- Redback (vendor-id 2352) attributes 1 (Primary DNS) and 2 (Secondary DNS)
- sending authentication requests: (from the DSL Forum) (vendor-id 3561), attributes 1 (Circuit ID) and 2 (Remote ID)

Sample User (VSA) Configuration

The following example displays a user-specific VSA configuration. This configuration shows attributes for users named `ruser1` and `ruser2`.

The following example shows that user `ruser1` is granted console access. `ruser1`'s home directory is in compact flash slot 3 and is limited to the home directory. The default action permits all packets when matching conditions are not met. The `timetra-cmd` parameters allow the user to use the `tools;telnet;configure system security` commands. Matching strings specified in the `timetra-action` command are denied for this user.

The user `ruser2` is granted FTP access. The default action denies all packets when matching conditions are not met. The `timetra-cmd` parameters allow the user to use the `configure, show, and debug` commands. Matching strings specified in the `timetra-action` command are permitted for this user.

```
users.timetra

ruser1  Auth-Type := System, Password == "ruser1"
        Service-Type = Login-User,
        Idle-Timeout = 600,
        Timetra-Access = console,
        Timetra-Home-Directory = cf3:
        Timetra-Restrict-To-Home = true
        Timetra-Default-Action = permit-all,
        Timetra-Cmd = "tools;telnet;configure system security",
        Timetra-Action = deny

ruser2 Auth-Type := System, Password == "ruser2"
        Service-Type = Login-User,
        Idle-Timeout = 600,
        Timetra-Access = ftp
        Timetra-Default-Action = deny-all,
        Timetra-Cmd = "configure",
        Timetra-Cmd = "show",
        Timetra-Action = permit,
        Timetra-Cmd = "debug",
        Timetra-Action = permit,
```


Alcatel-Lucent Dictionary

```
# Version: 20061003-1

VENDORAlcatel-IPD6527

# User management VSAs
ATTRIBUTE Timetra-Access1integerAlcatel-IPD
ATTRIBUTE Timetra-Home-Directory2stringAlcatel-IPD
ATTRIBUTE Timetra-Restrict-To-Home3integerAlcatel-IPD
ATTRIBUTE Timetra-Profile4stringAlcatel-IPD
ATTRIBUTE Timetra-Default-Action5integer Alcatel-IPD
ATTRIBUTE Timetra-Cmd6stringAlcatel-IPD
ATTRIBUTE Timetra-Action7integerAlcatel-IPD
ATTRIBUTE Timetra-Exec-File8stringAlcatel-IPD

# RADIUS authorization and CoA VSAs
ATTRIBUTE Alc-Primary-Dns9ipaddrAlcatel-IPD
ATTRIBUTE Alc-Secondary-Dns10ipaddrAlcatel-IPD
ATTRIBUTE Alc-Subsc-ID-Str11stringAlcatel-IPD
ATTRIBUTE Alc-Subsc-Prof-Str12stringAlcatel-IPD
ATTRIBUTE Alc-SLA-Prof-Str13stringAlcatel-IPD
ATTRIBUTE Alc-Force-Renew14stringAlcatel-IPD
# CoA
ATTRIBUTE Alc-Create-Host15stringAlcatel-IPD
# CoA
ATTRIBUTE Alc-ANCP-Str16stringAlcatel-IPD
ATTRIBUTE Alc-Retail-Serv-Id17integerAlcatel-IPD
ATTRIBUTE Alc-Default-Router18ipaddrAlcatel-IPD

# RADIUS accounting VSAs
ATTRIBUTE Alc-Acct-I-Inprof-Octets-6419octetsAlcatel-IPD
ATTRIBUTE Alc-Acct-I-Outprof-Octets-6420octetsAlcatel-IPD
ATTRIBUTE Alc-Acct-O-Inprof-Octets-6421octetsAlcatel-IPD
ATTRIBUTE Alc-Acct-O-Outprof-Octets-6422octetsAlcatel-IPD
ATTRIBUTE Alc-Acct-I-Inprof-Pkts-6423octetsAlcatel-IPD
ATTRIBUTE Alc-Acct-I-Outprof-Pkts-6424octetsAlcatel-IPD
ATTRIBUTE Alc-Acct-O-Inprof-Pkts-6425octetsAlcatel-IPD
ATTRIBUTE Alc-Acct-O-Outprof-Pkts-6426octetsAlcatel-IPD

ATTRIBUTE Alc-Client-Hardware-Addr27stringAlcatel-IPD
# CoA

VALUE      Timetra-Restrict-To-Hometrue1
VALUE      Timetra-Restrict-To-Homefalse2

VALUE      Timetra-Accessftp1
VALUE      Timetra-Accessconsole2
VALUE      Timetra-Accessboth3

VALUE      Timetra-Default-Actionpermit-all1
VALUE      Timetra-Default-Actiondeny-all2
VALUE      Timetra-Default-Actionnone3

VALUE      Timetra-Actionpermit1
VALUE      Timetra-Actiondeny2
```

Other Security Features

Secure Shell (SSH)

Secure Shell Version 1 (SSH1) is a protocol that provides a secure, encrypted Telnet-like connection to a router. A connection is always initiated by the client (the user). Authentication takes place by one of the configured authentication methods (local, RADIUS, or TACACS+). With authentication and encryption, SSH allows for a secure connection over an insecure network.

The 7705 SAR allows you to configure SSH1 or Secure Shell Version 2 (SSH2). SSH1 and SSH2 are different protocols and encrypt at different parts of the packets. SSH1 uses the server as well as host keys to authenticate systems, whereas SSH2 only uses host keys. SSH2 does not use the same networking implementation that SSH1 does and is considered a more secure, efficient, and portable version of SSH that includes Secure FTP (SFTP). SFTP is functionally similar to FTP but is SSH2-encrypted. Rather than validating identities via passwords, SSH2 can also use public key encryption to authenticate remote hosts. For example, if you were to connect to a remote host also running SSH2, the secure shell would use this system to verify that the remote system is the host and not a computer set up to imitate it.

SSH runs on top of a transport layer (like TCP or IP), and provides authentication and encryption capabilities. SSH supports remote login to another computer over a network, remote command execution, and file relocation from one host to another.

The 7705 SAR has a global SSH server process to support inbound SSH and SCP sessions initiated by external SSH or SCP client applications. The SSH server supports SSH1. Note that this server process is separate from the SSH and SCP client commands on the 7705 SAR, which initiate outbound SSH and SCP sessions.

Inbound SSH sessions are counted as inbound Telnet sessions for the purposes of the maximum number of inbound sessions specified by Login Control. Inbound SCP sessions are counted as inbound FTP sessions by Login Control.

When the SSH server is enabled, an SSH security key is generated. The key is only valid until either the node is restarted or the SSH server is stopped and restarted. The key size is non-configurable and set at 1024 bits. When the server is enabled, both inbound SSH and SCP sessions will be accepted provided the session is properly authenticated.

When the global SSH server process is disabled, no inbound SSH or SCP sessions will be accepted.

When using SCP to copy files from an external device to the file system, the 7705 SAR SCP server will accept either forward slash (“/”) or backslash (“\”) characters to delimit directory and/or filenames. Similarly, the 7705 SAR SCP client application can use either slash or backslash characters, but not all SCP clients treat backslash characters as equivalent to slash characters. In particular, UNIX systems will often interpret the backslash character as an “escape” character, which does not get transmitted to the 7705 SAR SCP server. For example, a destination directory specified as “cf3:\dir1\file1” will be transmitted to the 7705 SAR SCP server as “cf3:dir1file1” where the backslash escape characters are stripped by the SCP client system before transmission. On systems where the client treats the backslash like an “escape” character, a double backslash “\\” or the forward slash “/” can typically be used to properly delimit directories and the filename.

CSM Filters and CSM Security

In previous releases of the 7705 SAR, all traffic received by the router was destined for the router itself. All received IP packets were extracted to the CSM for processing. Rather than using CSM filters, basic IP filters were used to protect the control plane from DoS attacks, unauthorized access to the node, and similar security breaches.

With the introduction of IP forwarding on the 7705 SAR, IP filters applied to network interfaces have been enhanced, and CSM filters have been introduced that apply to IP packets extracted to the control plane.

IP filters scan all traffic and take the appropriate (configured) action against matching packets. Packets that are not filtered by the IP filters and are destined for the SAR are scanned by the configured CSM filter.

For information on IP filters, refer to the 7705 SAR OS Router Configuration Guide.



Note: Although the Control and Switching module on the 7705 SAR is called a CSM, the CSM filters are referred to as CPM filters in the CLI in order to maintain consistency with other SR routers.

Both IPv4 and IPv6 CSM filters are supported.

IPv4 CSM filters drop or accept incoming packets based on the following match criteria:

- DSCP name
- destination IP address
- destination port
- fragmentation
- ICMP code

- ICMP type
- IP option value
- multiple options
- option present
- source IP address
- source port
- TCP ACK
- TCP SYN

IPv6 CSM filters drop or accept incoming packets based on the following match criteria:

- DSCP name
- destination IP address
- destination port
- ICMP code
- ICMP type
- source IP address
- source port
- TCP ACK
- TCP SYN

To avoid DoS-like attacks overwhelming the control plane while ensuring that critical control traffic such as signaling is always serviced in a timely manner, the 7705 SAR has three queues (High, Low, and Ftp) for handling packets addressed to the CSM:

- High – handles all important messaging, such as network management and signaling links
- Low – handles lower-importance messages, such as pings
- Ftp – handles bulk file transfers, such as new software image downloads

These queues are fixed use (each queue handles a certain type of traffic, which is not user-configurable) and fixed configuration (each queue is configured for particular rates and buffering capacity and is not user-configurable).

Exponential Login Backoff

A malicious user can gain CLI access via a dictionary attack: using a script to try "admin" with any password.

The 7705 SAR increases the delay between login attempts exponentially to mitigate attacks. It is applied to the console login. SSH and Telnet sessions terminate after four attempts.

Encryption

Data Encryption Standard (DES) and Triple DES (3DES) are supported for encryption.

- DES is a widely used method of data encryption using a private (secret) key. Both the sender and the receiver must know and use the same private key.
- 3DES is a more secure version of the DES protocol.

802.1x Network Access Control

The 7705 SAR supports network access control of client devices (PCs, STBs, etc.) on an Ethernet network using the IEEE 802.1x standard. 802.1x is known as Extensible Authentication Protocol (EAP) over a LAN network or EAPOL.

Refer to the 7705 SAR OS Interface Configuration Guide for more information about IEEE 802.1x.

Configuration Notes

This section describes security configuration caveats.

- If a RADIUS or a TACACS+ server is not configured, then password, profiles, and user access information must be configured on each router in the domain.
- If RADIUS authorization is enabled, then VSAs must be configured on the RADIUS server.

Reference Sources

For information on supported IEEE standards, IETF drafts and standards as well as standard and proprietary MIBs, refer to [Standards and Protocol Support](#).

Configuring Security with CLI

This section provides information to configure security using the command line interface. Topics in this section include:

- [Setting Up Security Attributes on page 56](#)
 - [Configuring Authentication on page 56](#)
 - [Configuring Authorization on page 57](#)
 - [Configuring Accounting on page 58](#)
- [Security Configurations on page 59](#)
- [Security Configuration Procedures on page 61](#)
 - [Configuring IPv4 or IPv6 Management Access Filters on page 61](#)
 - [Configuring IPv4 or IPv6 CPM \(CSM\) Filters on page 64](#)
 - [Configuring Password Management Parameters on page 65](#)
 - [Configuring Profiles on page 66](#)
 - [Configuring Users on page 68](#)
 - [Copying and Overwriting Users and Profiles on page 69](#)
 - [Configuring SSH on page 73](#)
 - [Configuring Login Controls on page 73](#)
- [RADIUS Configurations on page 75](#)
 - [Configuring RADIUS Authentication on page 75](#)
 - [Configuring RADIUS Authorization on page 76](#)
 - [Configuring RADIUS Accounting on page 77](#)
 - [Configuring 802.1x RADIUS Policies on page 78](#)
- [TACACS+ Configurations on page 79](#)
 - [Enabling TACACS+ Authentication on page 79](#)
 - [Configuring TACACS+ Authorization on page 80](#)
 - [Configuring TACACS+ Accounting on page 81](#)

Setting Up Security Attributes

[Table 4](#) depicts the capabilities of authentication, authorization, and accounting configurations. For example, authentication can be enabled locally and on RADIUS and TACACS+ servers. Authorization can be executed locally, on a RADIUS server, or on a TACACS+ server. Accounting can be performed on a RADIUS or TACACS+ server.

Table 4: Security Configuration Requirements

Authentication	Authorization	Accounting
Local	Local	None
RADIUS	Local and RADIUS	RADIUS
TACACS+	Local and TACACS+	TACACS+

Configuring Authentication

Refer to the following sections to configure authentication:

- Local authentication
 - [Configuring Password Management Parameters](#)
 - [Configuring Profiles](#)
 - [Configuring Users](#)
- RADIUS authentication (with local authorization)

By default, authentication is enabled locally. Perform the following tasks to configure security on each participating 7705 SAR router:

 - [Configuring Profiles](#)
 - [Configuring RADIUS Authentication](#)
 - [Configuring Users](#)
- RADIUS authentication (with RADIUS authorization)

To implement RADIUS authentication with authorization, perform the following tasks on each participating 7705 SAR router:

 - [Configuring RADIUS Authentication](#)
 - [Configuring RADIUS Authorization](#)

- TACACS+ authentication

To implement TACACS+ authentication, perform the following tasks on each participating 7705 SAR router:

- [Configuring Profiles](#)
- [Configuring Users](#)
- [Enabling TACACS+ Authentication](#)

Configuring Authorization

Refer to the following sections to configure authorization:

- Local authorization

For local authorization, configure these tasks on each participating 7705 SAR router:

- [Configuring Profiles](#)
- [Configuring Users](#)

- RADIUS authorization with authentication

For RADIUS authorization with authentication, configure these tasks on each participating 7705 SAR router:

- [Configuring RADIUS Authorization](#)

For RADIUS authorization, VSAs must be configured on the RADIUS server. See [Vendor-Specific Attributes \(VSAs\)](#).

- [Configuring RADIUS Authentication](#)
- [Configuring Profiles](#)

- TACACS+ authorization (only)

For TACACS+ authorization without authentication, configure these tasks on each participating 7705 SAR router:

- [Configuring TACACS+ Authorization](#)

- TACACS+ authorization

For TACACS+ authorization with authentication, configure these tasks on each participating 7705 SAR router:

- [Enabling TACACS+ Authentication](#)
- [Configuring TACACS+ Authorization](#)

Configuring Accounting

Refer to the following sections to configure accounting.

- Local accounting is not implemented. For information about configuring accounting policies, refer to [Configuring Logging with CLI](#).
 - [Configuring RADIUS Accounting](#)
 - [Configuring TACACS+ Accounting](#)
-

Security Configurations

This section provides information on configuring security and examples of configuration tasks.

To implement security features, configure the following components:

- management access filters
- CPM (CSM) filters
- profiles
- user access parameters
- password management parameters
- RADIUS and/or TACACS+
 - enable one to five RADIUS and/or TACACS+ servers
 - configure RADIUS and/or TACACS+ parameters

The following example displays default values for security parameters.

```
ALU-1>config>system>security# info detail
-----
management-access-filter
  ip-filter
    default-action permit
    entry 1
      action permit
      src-ip 10.10.10.xx/32
    exit
    entry 2
      action permit
      src-ip 10.10.0.xx/32
    exit
  exit
cpm-filter
  ip-filter
    shutdown
    entry 2 create
      action drop
    exit
  exit
profile "default"
  default-action none
  entry 10
    no description
    match "exec"
    action permit
  exit
...
  entry 70
    no description
    match "show"
    action permit
```

```
        exit
    exit
    profile "administrative"
        default-action permit-all
        entry 10
            no description
            match "configure system security"
            action permit
        exit
    ...
    password
        authentication-order radius tacplus local
        no aging
        minimum-length 6
        attempts 3 time 5 logout 10
        complexity
    exit
    user "admin"
        password "./3kQWERTYn0Q6w" hash
        access console
    no home-directory
    no restricted-to-home
        console
            no login-exec
            no cannot-change-password
            no new-password-at-login
            member "administrative"
        exit
    exit
    snmp
        view iso subtree 1
            mask ff type included
        exit
    ...
    access group snmp-ro security-model snmpv1 security-level no-auth-no-privacy read no-
security notify no-security
    access group snmp-ro security-model snmpv2c security-level no-auth-no-privacy read
no-security notify no-security
    access group snmp-rw security-model snmpv1 security-level no-auth-no-privacy read no-
security write no-security notify no-security
    access group snmp-rw security-model snmpv2c security-level no-auth-no-privacy read
no-security write no-security notify no-security
    access group snmp-rwa security-model snmpv1 security-level no-auth-no-privacy read
iso write iso notify iso
    access group snmp-rwa security-model snmpv2c security-level no-auth-no-privacy read
iso write iso notify iso
    access group snmp-trap security-model snmpv1 security-level no-auth-no-privacy notify
iso
    access group snmp-trap security-model snmpv2c security-level no-auth-no-privacy
notify iso
    access group cli-readonly security-model snmpv2c security-level
no-auth-no-privacy read iso notify iso
    access group cli-readwrite security-model snmpv2c security-level
no-auth-no-privacy read iso write iso notify iso
        attempts 20 time 5 logout 10
    exit
    no ssh
    exit
```

Security Configuration Procedures

- [Configuring IPv4 or IPv6 Management Access Filters](#)
- [Configuring IPv4 or IPv6 CPM \(CSM\) Filters](#)
- [Configuring Password Management Parameters](#)
- [Configuring Profiles](#)
- [Configuring Users](#)
- [Copying and Overwriting Users and Profiles](#)
- [Configuring SSH](#)
- [Configuring Login Controls](#)
- [RADIUS Configurations](#)
- [TACACS+ Configurations](#)

Configuring IPv4 or IPv6 Management Access Filters

Creating and implementing management access filters is optional. Management access filters control all traffic going in to the CSM, including all routing protocols. They apply to packets from all ports. The filters can be used to restrict management of the 7705 SAR router by other nodes outside either specific (sub)networks or through designated ports. By default, there are no filters associated with security options. The management access filter and entries must be explicitly created on each router. These filters apply to the management Ethernet port.

The management Ethernet port supports both IPv4 and IPv6 filters.

The 7705 SAR exits the filter when the first match is found and executes the actions according to the specified action. For this reason, entries must be sequenced correctly from most to least explicit.

An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword `action` to be considered complete. Entries without the `action` keyword are considered incomplete and will be rendered inactive.

Use the following CLI commands to configure an IPv4 management access filter. This example only accepts packets matching the criteria specified in entries 1 and 2. Non-matching packets are denied.

CLI Syntax:

```
config>system
      security
        management-access-filter
          ip-filter
            default-action {permit | deny |
                          deny-host-unreachable}
            entry entry-id
              action {permit | deny |
                    deny-host-unreachable}
              description description-string
              dst-port port [mask]
              log
              protocol protocol-id
              router router-instance
              src-ip {ip-prefix/mask |
                    ip-prefix netmask}
              src-port {port-id | cpm}
              renum old-entry-number new-entry-number
              no shutdown
```

Use the following CLI commands to configure an IPv6 management access filter. This example only accepts packets matching the criteria specified in entries 1 and 2. Non-matching packets are denied.

CLI Syntax:

```
config>system
      security
        management-access-filter
          ipv6-filter
            default-action {permit | deny |
                          deny-host-unreachable}
            entry entry-id
              action {permit | deny |
                    deny-host-unreachable}
              description description-string
              dst-port port [mask]
              flow-label value
              log
              next-header next-header
              router router-instance
              src-ip ipv6-address/prefix-length
              src-port {port-id | cpm}
              renum old-entry-number new-entry-number
              no shutdown
```

The following displays an example of an IPv4 management access filter command usage.

Example:

```

config>system>security# management-access-filter
security>mgmt-access-filter# ip-filter default-action
deny
security>mgmt-access-filter# ip-filter entry 1
security>mgmt-access-filter>entry# mgmt-access-
    filter>ip-filter>entry# src-ip 10.10.10.104/32
security>mgmt-access-filter>ip-filter>entry# exit
security>mgmt-access-filter>ip-filter# entry 2
security>mgmt-access-filter>ip-filter>entry# mgmt-access-
    filter>entry# src-ip 10.10.10.1/32
security>mgmt-access-filter>ip-filter>entry# exit
  
```

The following example displays the management access filter configuration.

```

ALU-1>config>system>security# info
-----
    management-access-filter
        ip-filter
        default-action deny
        entry 1
            action permit
            src-ip 10.10.10.104/32
        exit
        entry 2
            action permit
            src-ip 10.10.0.1/32
        exit
    exit
    snmp
        community "private" rwa version both
    exit
-----
ALU-1>config>system>security#
  
```

Configuring IPv4 or IPv6 CPM (CSM) Filters

CPM filters control all traffic going in to the CSM, including all routing protocols. They apply to packets from all network and access ports, but not to packets from a management Ethernet port. CPM packet filtering is performed by network processor hardware using no resources on the main CPUs.

Use the following CLI commands to configure an IPv4 CPM filter.

CLI Syntax:

```
config>system>security
  cpm-filter
    default-action {accept | drop}
  ip-filter
    entry entry-id [create]
      action {accept | drop}
      description description-string
      log log-id
      match [protocol protocol-id]
        dscp dscp-name
        dst-ip {ip-address/mask|ip-address netmask}
        dst-port [tcp/udp port-number] [mask]
        fragment {true | false}
        icmp-code icmp-code
        icmp-type icmp-type
        ip-option ip-option-value [ip-option-mask]
        multiple-option {true | false}
        option-present {true | false}
        src-ip {ip-address/mask|ip-address netmask}
        src-port src-port-number [mask]
        tcp-ack {true | false}
        tcp-syn {true | false}
      renum old-entry-id new-entry-id
```

Use the following CLI commands to configure an IPv6 CPM filter.

CLI Syntax:

```
config>system>security
  cpm-filter
    default-action {accept | drop}
  ipv6-filter
    entry entry-id [create]
      action {accept | drop}
      description description-string
      log log-id
      match [next-header next-header]
        dscp dscp-name
        dst-ip ipv6-address/prefix-length
        dst-port [tcp/udp port-number] [mask]
        icmp-code icmp-code
        icmp-type icmp-type
```



```

src-ip ipv6-address/prefix-length
src-port src-port-number [mask]
tcp-ack {true | false}
tcp-syn {true | false}
renum old-entry-id new-entry-id

```

The following displays an IPv4 CPM filter configuration example:

```

A:ALU-49>config>sys>sec>cpm>ip-filter# info
-----
entry 10 create
  action drop
  description "CPM-Filter 10.4.101.2 #101"
  log 101
exit
entry 20 create
  no action
  description "CPM-Filter 10.4.101.2 #201"
  log 101
exit
no shutdown
-----
A:ALU-49>config>sys>sec>cpm>ip-filter#

```

Configuring Password Management Parameters

Configuring password management parameters consists of defining aging, the authentication order and authentication methods, password length and complexity, as well as the number of attempts a user can make to enter a password.

Depending on the authentication requirements, password parameters are configured locally or on the RADIUS or TACACS+ server.

Use the following CLI commands to configure password support:

CLI Syntax: `config>system>security`

```

password
  admin-password password [hash | hash2]
  aging days
  attempts count [time minutes1] [lockout minutes2]
  authentication-order [method-1] [method-2]
    [method-3] [exit-on-reject]
  complexity [numeric] [special-character]
    [mixed-case]
  health-check
  minimum-length value

```

The following displays an example of the password command usage.

Example:

```
config>system>security#password
security>password# aging 365
security>password# minimum-length 8
security>password# attempts 5 time 5 lockout 20
security>password# authentication-order radius tacplus
local
```

The following example displays the password configuration:

```
ALU-1>config>system>security# info
-----
password
authentication-order radius tacplus local
aging 365
minimum-length 8
attempts 5 time 5 lockout 20
exit
-----
ALU-1>config>system>security#
```

Configuring Profiles

Profiles are used to deny or permit access to a hierarchical branch or specific commands. Profiles are referenced in a user configuration. A maximum of 16 user profiles can be defined. A user can participate in up to 16 profiles. Depending on the the authorization requirements, passwords are configured locally or on the RADIUS server.

Use the following CLI commands to configure user profiles:

CLI Syntax:

```
config>system>security
  profile user-profile-name
  default-action {deny-all | permit-all | none}
  renum old-entry-number new-entry-number
  entry entry-id
    description description-string
    match command-string
    action {permit | deny}
```

The following displays an example of the user profile command usage.

Example:

```

config>system>security# profile ghost
config>system>security>profile$ default-action permit-all
config>system>security>profile# entry 1
config>system>security>profile>entry$ action permit
config>system>security>profile>entry# match "configure"
config>system>security>profile>entry# exit
config>system>security>profile# entry 2
config>system>security>profile>entry$ match "show"
config>system>security>profile>entry# exit
config>system>security>profile# entry 3
config>system>security>profile>entry$ match "exit"

```

The following example displays the user profile output:

```

ALU-1>config>system>security# info
-----
...
    profile "ghost"
        default-action permit-all
        entry 1
            match "configure"
            action permit
        exit
        entry 2
            match "show"
        exit
        entry 3
            match "exit"
        exit
...
-----
ALU-1>config>system>security#

```

Configuring Users

Access parameters are configured for individual users. For each user, the login name and, optionally, information that identifies the user is defined. Use the following CLI commands to configure access parameters for users:

CLI Syntax:

```
config>system>security
  user-template template-name
  user user-name
    access [ftp] [snmp] [console]
    console
      cannot-change-password
      login-exec url-prefix:source-url
      member user-profile-name [user-profile-name... (up to 8 max)]
      new-password-at-login
      home-directory url-prefix [directory]
      [directory/directory ..]
      password [password] [hash | hash2]
      restricted-to-home
      snmp
        authentication {[none] | [[hash] {md5 key-1 | sha key-1} privacy {none | des-key key-2}]}
```

The following displays an example of the command usage.

Example:

```
config>system>security
config>system>security# user 49ers
config>system>security>user$ access ftp snmp console
config>system>security>user$ console
config>system>security>user>console# member default ghost
config>system>security>user>console# new-password-at-login
config>system>security>user>console# exit
config>system>security>user# password testuser1
config>system>security>user# restricted-to-home
config>system>security>user# exit
```

The following example displays the user configuration:

```
ALU-1>config>system>security# info
-----
...
    user "49ers"
        password "qQbnuzLd7H/VxGdUqdh7bE" hash2
        access console ftp snmp
        restricted-to-home
        console
            member "default"
            member "ghost"
        exit
    exit
...
-----
ALU-1>config>system>security#
```

Copying and Overwriting Users and Profiles

You can copy a profile or user or overwrite an existing profile or user. The `overwrite` option must be specified; otherwise, an error occurs if the destination profile or user name already exists.

Copying a User

CLI Syntax: `config>system>security# copy {user source-user | profile source-profile} to destination [overwrite]`

Example:

```
config>system>security# copy user "testuser" to
"testuserA"
MINOR: CLI User "testuserA" already exists - use overwrite
flag.
config>system>security#
config>system>security# copy user "testuser" to
"testuserA" overwrite
config>system>security#
```

The following output displays the copied user configurations:

```
ALU-12>config>system>security# info
-----
...
        user "testuser"
            password "F6XjryaATzM" hash
            access snmp
            snmp
                authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy
none
            group "testgroup"
            exit
        exit
        user "testuserA"
            password "" hash2
            access snmp
            console
                new-password-at-login
            exit
            snmp
                authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy
none
            group "testgroup"
            exit
        exit
...
-----
ALU-12>config>system>security# info
```



Note: The `cannot-change-password` flag is not replicated when a copy user command is performed. A `new-password-at-login` flag is created instead.

```
ALU-12>config>system>security>user# info
-----
        password "F6XjryaATzM" hash
        access snmp
        console
            cannot-change-password
        exit
        snmp
            authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
        group "testgroup"
        exit
-----
ALU-12>config>system>security>user# exit
ALU-12>config>system>security# user testuserA
ALU-12>config>system>security>user# info
-----
        password "" hash2
        access snmp
        console
            new-password-at-login
        exit
        snmp
            authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
        group "testgroup"
```

```

        exit
-----
ALU-12>config>system>security>user#

```

Copying a Profile

CLI Syntax: config>system>security# copy {user *source-user* | profile *source-profile*} to *destination* [overwrite]

Example: config>system>security# copy profile default to testuser

The following output displays the copied profiles:

```

A:ALU-49>config>system>security# info
-----
...
A:ALU-49>config>system>security# info detail
-----
...
        profile "default"
            default-action none
            entry 10
                no description
                match "exec"
                action permit
            exit
            entry 20
                no description
                match "exit"
                action permit
            exit
            entry 30
                no description
                match "help"
                action permit
            exit
            entry 40
                no description
                match "logout"
                action permit
            exit
            entry 50
                no description
                match "password"
                action permit
            exit
            entry 60
                no description
                match "show config"
                action deny
            exit
            entry 70
                no description
                match "show"
                action permit

```

```
exit
entry 80
    no description
    match "enable-admin"
    action permit
exit
exit
profile "testuser"
    default-action none
    entry 10
        no description
        match "exec"
        action permit
    exit
    entry 20
        no description
        match "exit"
        action permit
    exit
    entry 30
        no description
        match "help"
        action permit
    exit
    entry 40
        no description
        match "logout"
        action permit
    exit
    entry 50
        no description
        match "password"
        action permit
    exit
    entry 60
        no description
        match "show config"
        action deny
    exit
    entry 70
        no description
        match "show"
        action permit
    exit
    entry 80
        no description
        match "enable-admin"
        action permit
    exit
exit
profile "administrative"
    default-action permit-all exit
...
```


Configuring SSH

Use the SSH command to configure the SSH server as SSH1, SSH2 or both. The default is SSH2. This command should only be enabled or disabled when the SSH server is disabled. This setting cannot be changed while the SSH server is running.

CLI Syntax:

```
config>system>security
ssh
  preserve-key
  no server-shutdown
  version ssh-version
```

Example:

```
config>system>security# ssh
config>system>security>ssh# preserve-key
config>system>security>ssh# version 1-2
```

The following example displays the SSH server configuration as both SSH1 and SSH2 using a host-key:

```
A:ALU-1>config>system>security>ssh# info
-----
                preserve-key
                version 1-2
-----
A:ALU-1>config>system>security>ssh#
```

Configuring Login Controls

Use the `login-control` context to configure parameters for console, Telnet, and FTP sessions.

CLI Syntax:

```
config>system
login-control
  exponential-backoff
  ftp
    inbound-max-sessions value
  telnet
    inbound-max-sessions value
    outbound-max-sessions value
  idle-timeout {minutes | disable}
  pre-login-message login-text-string [name]
  login-banner
  motd {url url-prefix:source-url | text motd-text-string}
```

The following example displays the login control configuration:

Example:

```
config>system>login-control# ftp inbound-max-sessions 5
config>system>login-control# telnet inbound-max-sessions
7
config>system>login-control# telnet outbound-max-sessions
2
config>system>login-control# idle-timeout 1440
config>system>login-control# pre-login-message "Property
of Service Routing Inc. Unauthorized access prohibited."
config>system>login-control# motd text "Notice to all
users: Software upgrade scheduled 3/2 1:00 AM"
```

The following example displays the login control configuration:

```
ALU-1>config>system# info
-----
...
    login-control
        ftp
            inbound-max-sessions 5
        exit
        telnet
            inbound-max-sessions 7
            outbound-max-sessions 2
        exit
        idle-timeout 1440
        pre-login-message "Property of Service Routing Inc. Unauthorized access
prohibited."
        motd text "Notice to all users: Software upgrade scheduled 3/2 1:00 AM"
        exit
        no exponential-backoff
    ...
-----
ALU-1>config>system#
```

RADIUS Configurations

- [Configuring RADIUS Authentication](#)
- [Configuring RADIUS Authorization](#)
- [Configuring RADIUS Accounting](#)

Configuring RADIUS Authentication

RADIUS is disabled by default and must be explicitly enabled. The mandatory commands to enable RADIUS on the local router are `radius` and `server server-index address ip-address secret key`. The `server` command adds a RADIUS server and configures the RADIUS server's IP address, index, and key values. The index determines the sequence in which the servers are queried for authentication requests.

Also, the system IP address must be configured in order for the RADIUS client to work. See "Configuring a System Interface" in the 7705 SAR OS Router Configuration Guide.

The other commands are optional.

On the local router, use the following CLI commands to configure RADIUS authentication:

CLI Syntax:

```
config>system>security
      radius
      port port
      retry count
      server server-index address ip-address secret key
          [hash1 | hash2]
      timeout seconds
      no shutdown
```

The following example displays the CLI syntax usage:

Example:

```
config>system>security>
security# radius
security# no shutdown
security>radius# server 1 address 10.10.10.103 secret
test11
security>radius# server 2 address 10.10.0.1 secret test2
security>radius# server 3 address 10.10.0.2 secret test3
security>radius# server 4 address 10.10.0.3 secret test4
security>radius# retry 5
security>radius# timeout 5
config>system>security>radius# exit
```

The following example displays the RADIUS authentication configuration:

```
ALU-1>config>system>security# info
-----
        retry 5
        timeout 5
        server 1 address 10.10.10.103 secret "test1"
        server 2 address 10.10.0.1 secret "test2"
        server 3 address 10.10.0.2 secret "test3"
        server 4 address 10.10.0.3 secret "test4"
        ...
-----
ALU-1>config>system>security#
```

Configuring RADIUS Authorization

In order for RADIUS authorization to function, RADIUS authentication must be enabled first. See [Configuring RADIUS Authentication](#).

In addition to the local configuration requirements, VSAs must be configured on the RADIUS server. See [Vendor-Specific Attributes \(VSAs\)](#).

On the local router, use the following CLI commands to configure RADIUS authorization:

CLI Syntax:

```
config>system>security
        radius
        authorization
```

The following example displays the CLI syntax usage:

Example:

```
config>system>security>
config>system>security# radius
config>system>security>radius# authorization
```

The following example displays the RADIUS authorization configuration:

```
ALU-1>config>system>security# info
-----
        ...
        radius
        authorization
        retry 5
        timeout 5
        server 1 address 10.10.10.103 secret "test1"
        server 2 address 10.10.0.1 secret "test2"
        server 3 address 10.10.0.2 secret "test3"
        server 4 address 10.10.0.3 secret "test4"
        exit
        ...
-----
ALU-1>config>system>security#
```

Configuring RADIUS Accounting

On the local router, use the following CLI commands to configure RADIUS accounting:

CLI Syntax: `config>system>security
 radius
 accounting`

The following example displays the CLI syntax usage:

Example: `config>system>security>
config>system>security# radius
config>system>security>radius# accounting`

The following example displays the RADIUS accounting configuration:

```
ALU-1>config>system>security# info
-----
...
      radius
      shutdown
      authorization
      accounting
      retry 5
      timeout 5
      server 1 address 10.10.10.103 secret "test1"
      server 2 address 10.10.0.1 secret "test2"
      server 3 address 10.10.0.2 secret "test3"
      server 4 address 10.10.0.3 secret "test4"
      exit
...
-----
ALU-1>config>system>security#
```

Configuring 802.1x RADIUS Policies

Use the following CLI commands to configure generic authentication parameters for clients using 802.1x EAPOL. Additional parameters are configured on Ethernet ports. Refer to the 7705 SAR OS Interface Configuration Guide, “Card, Adapter Card, and Port Command Reference”, for more information on configuring 802.1x parameters on Ethernet ports.

To configure generic parameters for 802.1x authentication, enter the following CLI syntax:

CLI Syntax:

```
config>system>security
dot1x
    radius-plcy name [create]
        retry count
        server server-index address ip-address secret
        key [hash | hash2] [auth-port auth-port]
        [acct-port acct-port] [type server-type]
        no shutdown
        source-address ip-address
        timeout seconds
    no shutdown
```

The following example displays the CLI syntax usage:

Example:

```
config>system>security>
config>system>security# dot1x
config>system>security>dot1x# radius-plcy dot1x_plcy
create
config>system>security>dot1x>radius-plcy# server 1
address 1.1.1.1 secret abc auth-port 65000
config>system>security>dot1x>radius-plcy# server 2
address 1.1.1.3 secret xyz auth-port 862
config>system>security>dot1x>radius-plcy# source-address
1.1.1.255
```

The following example displays an 802.1x configuration:

```
*A:7705_custDoc>config>system>security>dot1x# info
-----
radius-plcy "dot1x_plcy" create
server 1 address 1.1.1.1 auth-port 65000 acct-port 1813 secret
"WDoQz6DJf4.0M5dlpwjHbk" hash2 type authorization
server 2 address 1.1.1.3 auth-port 862 acct-port 1813 secret
"WDoQz6DJf4.jlWcCeHZwz." hash2 type authorization
source-address 1.1.1.255
shutdown
exit
...
-----
A:ALU-1>config>system#
```

TACACS+ Configurations

- [Enabling TACACS+ Authentication](#)
- [Configuring TACACS+ Authorization](#)
- [Configuring TACACS+ Accounting](#)

Enabling TACACS+ Authentication

To use TACACS+ authentication on the router, configure one or more TACACS+ servers on the network.

Use the following CLI commands to configure TACACS+ authentication:

CLI Syntax:

```
config>system>security
tacplus
    server server-index address ip-address secret key
    [hash1 | hash2]
    single-connection
    timeout seconds
    no shutdown
```

The following example is configured in the config>system context:

Example:

```
security# tacplus
security>tacplus# server 1 address 10.10.0.5 secret test1
security>tacplus# server 2 address 10.10.0.6 secret test2
security>tacplus# server 3 address 10.10.0.7 secret test3
security>tacplus# server 4 address 10.10.0.8 secret test4
security>tacplus# server 5 address 10.10.0.9 secret test5
config>system>security>tacplus# single-connection
config>system>security>tacplus# timeout 5
config>system>security>tacplus# no shutdown
```

The following example displays the TACACS+ authentication configuration:

```
ALU-1>config>system>security>tacplus# info
-----
    timeout 5
    single-connection
    server 1 address 10.10.0.5 secret "h6.TeL7YPohbmhlvz0gob." hash2
    server 2 address 10.10.0.6 secret "h6.TeL7YPog7WbLsR3QRd." hash2
    server 3 address 10.10.0.7 secret "h6.TeL7YPojGJqbYt85LVk" hash2
    server 4 address 10.10.0.8 secret "h6.TeL7YPoiCfWKUFHARvk" hash2
    server 5 address 10.10.0.9 secret "h6.TeL7YPojuCyTFvTNGBU" hash2
-----
ALU-1>config>system>security>tacplus#
```

Configuring TACACS+ Authorization

In order for TACACS+ authorization to function, TACACS+ authentication must be enabled first. See [Enabling TACACS+ Authentication](#).

On the local router, use the following CLI commands to configure TACACS+ authorization:

CLI Syntax:

```
config>system>security
      tacplus
      authorization
      no shutdown
```

The following example displays the CLI syntax usage:

Example:

```
config>system>security>
config>system>security# tacplus
config>system>security>tacplus# authorization
config>system>security>tacplus# no shutdown
```

The following example displays the TACACS+ authorization configuration:

```
ALU-1>config>system>security>tacplus# info
-----
      authorization
      timeout 5
      single-connection
      server 1 address 10.10.0.5 secret "h6.TeL7YPohbmhlvz0gob." hash2
      server 2 address 10.10.0.6 secret "h6.TeL7YPog7WbLsR3QRd." hash2
      server 3 address 10.10.0.7 secret "h6.TeL7YPojGJqbYt85LVk" hash2
      server 4 address 10.10.0.8 secret "h6.TeL7YPoiCfWKUFHARvk" hash2
      server 5 address 10.10.0.9 secret "h6.TeL7YPojuCyTFvTNGBU" hash2
-----
ALU-1>config>system>security>tacplus#
```


Configuring TACACS+ Accounting

On the local router, use the following CLI commands to configure TACACS+ accounting:

CLI Syntax: `config>system>security
tacplus
accounting`

The following example displays the CLI syntax usage:

Example: `config>system>security>
config>system>security# tacplus
config>system>security>tacplus# accounting`

The following example displays the TACACS+ accounting configuration:

```
ALU-1>config>system>security>tacplus# info
-----
accounting
authorization
timeout 5
single-connection
server 1 address 10.10.0.5 secret "h6.TeL7YPohbmhlvz0gob." hash2
server 2 address 10.10.0.6 secret "h6.TeL7YPog7WbLsR3QRd." hash2
server 3 address 10.10.0.7 secret "h6.TeL7YPojGJqbYt85LVk" hash2
server 4 address 10.10.0.8 secret "h6.TeL7YPoiCfWKUFHARvk" hash2
server 5 address 10.10.0.9 secret "h6.TeL7YPojuCyTFvTNGBU" hash2
-----
ALU-1>config>system>security>tacplus#
```

Security Command Reference

Command Hierarchies

- [Configuration Commands](#)
 - [Security Configuration Commands](#)
 - [Management Access Filter Commands](#)
 - [IPv6 Management Access Filter Commands](#)
 - [CPM Filter Commands](#)
 - [IPv6 CPM Filter Commands](#)
 - [Password Commands](#)
 - [Profile Commands](#)
 - [User Commands](#)
 - [RADIUS Commands](#)
 - [TACACS+ Commands](#)
 - [802.1x Commands](#)
 - [SSH Commands](#)
- [Login Control Commands](#)
- [Show Commands](#)
 - [Security](#)
 - [Login Control](#)
- [Clear Commands](#)
 - [Authentication](#)
- [Debug Commands](#)

Configuration Commands

Security Configuration Commands

```

config
  — system
    — security
      — copy {user source-user | profile source-profile} to destination [overwrite]
      — ftp-server
      — no ftp-server
      — hash-control [read-version {1 | 2 | all}] [write-version {1 | 2}]
      — no hash-control
      — source-address
        — application app [ip-int-name | ip-address]
        — no application app
      — [no] telnet-server
      — [no] telnet6-server

```

Management Access Filter Commands

```

config
  — system
    — security
      — [no] management-access-filter
        — ip-filter
          — default-action {permit | deny | deny-host-unreachable}
          — [no] entry entry-id
            — action {permit | deny | deny-host-unreachable}
            — no action
            — description description-string
            — no description
            — dst-port port [mask]
            — no dst-port
            — [no] log
            — [no] protocol protocol-id
            — router router-instance
            — no router
            — src-ip {ip-prefix/mask | ip-prefix netmask}
            — no src-ip
            — src-port {port-id | cpm}
            — no src-port
          — renum old-entry-number new-entry-number
          — [no] shutdown

```

IPv6 Management Access Filter Commands

```

config
  — system
    — security
      — [no] management-access-filter
        — ipv6-filter
          — default-action {permit | deny | deny-host-unreachable}
          — [no] entry entry-id
            — action {permit | deny | deny-host-unreachable}
            — no action
            — description description-string
            — no description
            — dst-port port [mask]
            — no dst-port
            — flow-label value
            — no flow-label
            — [no] log
            — [no] next-header next-header
            — router router-instance
            — no router
            — src-ip ipv6-address/prefix-length
            — no src-ip
            — src-port {port-id | cpm}
            — no src-port
          — renum old-entry-number new-entry-number
          — [no] shutdown

```

CPM Filter Commands

```

config
  — system
    — security
      — [no] cpm-filter
        — default-action {accept | drop}
        — ip-filter
          — entry entry-id [create]
          — no entry entry-id
            — action {accept | drop}
            — no action
            — description description-string
            — no description
            — log log-id
            — no log
            — match [protocol protocol-id]
            — no match
              — dscp dscp-name
              — no dscp
              — dst-ip {ip-address/mask | ip-address netmask}
              — no dst-ip
              — dst-port tcp/udp port-number [mask]
              — no dst-port
              — fragment {true | false}
              — no fragment
              — icmp-code icmp-code
              — no icmp-code
              — icmp-type icmp-type
              — no icmp-type
              — ip-option ip-option-value [ip-option-mask]
              — no ip-option
              — multiple-option {true | false}
              — no multiple-option
              — option-present {true | false}
              — no option-present
              — src-ip {ip-address/mask | ip-address netmask}
              — no src-ip
              — src-port src-port-number [mask]
              — no src-port
              — tcp-ack {true | false}
              — no tcp-ack
              — tcp-syn {true | false}
              — no tcp-syn
          — renum old-entry-id new-entry-id
          — [no] shutdown

```

IPv6 CPM Filter Commands

```

config
  — system
    — security
      — [no] cpm-filter
        — default-action {accept | drop}
        — ipv6-filter
          — entry entry-id [create]
          — no entry entry-id
            — action {accept | drop}
            — no action
            — description description-string
            — no description
            — log log-id
            — no log
            — match [next-header next-header]
            — no match
              — dscp dscp-name
              — no dscp
              — dst-ip ipv6-address/prefix-length
              — no dst-ip
              — dst-port tcp/udp port-number [mask]
              — no dst-port
              — icmp-code icmp-code
              — no icmp-code
              — icmp-type icmp-type
              — no icmp-type
              — src-ip ipv6-address/prefix-length
              — no src-ip
              — src-port src-port-number [mask]
              — no src-port
              — tcp-ack {true | false}
              — no tcp-ack
              — tcp-syn {true | false}
              — no tcp-syn
          — renum old-entry-id new-entry-id
        — [no] shutdown

```

Password Commands

```

config
  — system
    — security
      — password
        — admin-password password [hash | hash2]
        — no admin-password
        — aging days
        — no aging
        — attempts count [time minutes1] [lockout minutes2]
        — no attempts
        — authentication-order [method-1] [method-2] [method-3] [exit-on-reject]
        — no authentication-order
        — [no] complexity [numeric] [special-character] [mixed-case]
        — [no] health-check
        — minimum-length value
        — no minimum-length

```

Profile Commands

```

config
  — system
    — security
      — [no] profile user-profile-name
        — default-action {deny-all | permit-all | none}
        — renum old-entry-number new-entry-number
        — [no] entry entry-id
          — action {permit | deny}
          — description description-string
          — no description
          — match command-string
          — no match

```


User Commands

```

config
  — system
    — security
      — [no] user user-name
        — [no] access [ftp] [snmp] [console]
        — console
          — [no] cannot-change-password
          — login-exec url-prefix:source-url
          — no login-exec
          — member user-profile-name [user-profile-name...(up to 8
            max)]
          — no member user-profile-name
          — [no] new-password-at-login
        — home-directory url-prefix [directory] [directory/directory...]
        — no home-directory
        — password [password] [hash | hash2]
        — [no] restricted-to-home
        — snmp
          — authentication {[none] | [[hash] {md5 key-1 | sha key-1}
            privacy {privacy-level key-2}]}
          — group group-name
          — no group
      — user-template {tacplus_default | radius_default}
        — [no] access [ftp] [console]
        — console
          — login-exec url-prefix:source-url
          — no login-exec
        — home-directory url-prefix [directory][directory/directory ..]
        — no home-directory
        — [no] restricted-to-home

```

RADIUS Commands

```
config
  — system
    — security
      — [no] radius
        — access-algorithm {direct | round-robin}
        — [no] access-algorithm
        — [no] accounting
        — accounting-port port
        — no accounting-port
        — [no] authorization
        — port port
        — no port
        — retry count
        — no retry
        — server server-index address ip-address secret key [hash | hash2]
        — no server server-index
        — [no] shutdown
        — timeout seconds
        — no timeout
        — use-default-template
```

TACACS+ Commands

```
config
  — system
    — security
      — [no] tacplus
        — accounting [record-type {start-stop | stop-only}]
        — no accounting
        — [no] authorization
        — server server-index address ip-address secret key [hash | hash2]
        — no server server-index
        — [no] single-connection
        — timeout seconds
        — no timeout
        — [no] shutdown
        — [no] use-default-template
```

802.1x Commands

```

config
  — system
    — security
      — [no] dot1x
        — [no] radius-pley name [create]
          — retry count
          — no retry
          — server server-index address ip-address secret key [hash |
            hash2] [auth-port auth-port] [acct-port acct-port]
            [type server-type]
          — no server server-index
          — source-address ip-address
          — no source-address
          — [no] shutdown
          — timeout seconds
          — no timeout
        — [no] shutdown
  
```

SSH Commands

```

config
  — system
    — security
      — ssh
        — [no] preserve-key
        — [no] server-shutdown
        — [no] version SSH-version
  
```

Login Control Commands

```

config
  — system
    — login-control
      — [no] exponential-backoff
      — ftp
        — inbound-max-sessions value
        — no inbound-max-sessions
      — telnet
        — inbound-max-sessions value
        — no inbound-max-sessions
        — outbound-max-sessions value
        — no outbound-max-sessions
      — idle-timeout {minutes | disable}
      — no idle-timeout
      — [no] login-banner
      — motd {url url-prefix: source-url | text motd-text-string}
      — no motd
      — pre-login-message login-text-string [name]
      — no pre-login-message
  
```

Show Commands

Security

```
show
  — system
    — security
      — access-group [group-name]
      — authentication [statistics]
      — communities
      — cpm-filter
        — ip-filter [entry entry-id]
        — ipv6-filter [entry entry-id]
      — management-access-filter
        — ip-filter [entry entry-id]
        — ipv6-filter [entry entry-id]
      — password-options
      — profile user-profile-name
      — source-address
      — ssh
      — user [user-id] [detail]
      — view [view-name] [detail]
```

Login Control

```
show
  — users
```

Clear Commands

Authentication

```
clear
  — router
    — authentication
      — statistics [interface ip-int-name | ip-address]
```

Debug Commands

```
debug
  — radius [detail] [hex]
  — no radius
```

Command Descriptions

- [Configuration Commands on page 96](#)
- [Show Commands on page 158](#)
- [Clear Commands on page 179](#)
- [Debug Commands on page 180](#)

Configuration Commands

- [Generic Security Commands on page 97](#)
- [Security Commands on page 98](#)
- [Management Access Filter Commands on page 101](#)
 - [Management Access Filter Entry Commands on page 103](#)
- [CPM Filter Commands on page 109](#)
- [Global Password Commands on page 123](#)
- [Password Commands on page 124](#)
- [Profile Management Commands on page 129](#)
 - [Profile Management Entry Commands on page 130](#)
- [User Management Commands on page 132](#)
 - [User Management Console Commands on page 136](#)
 - [User Management SNMP Commands on page 137](#)
- [RADIUS Client Commands on page 140](#)
- [TACACS+ Client Commands on page 144](#)
- [802.1x Commands on page 147](#)
- [SSH Commands on page 151](#)
- [Login Control Commands on page 153](#)
 - [FTP Login Control Commands on page 155](#)
 - [Telnet Login Control Commands on page 156](#)

Generic Security Commands

description

Syntax	description <i>description-string</i> no description
Context	config>system>security>management-access-filter>ip-filter>entry <i>entry-id</i> config>system>security>management-access-filter>ipv6-filter>entry <i>entry-id</i> config>system>security>cpm-filter>ip-filter>entry> <i>entry-id</i> config>system>security>cpm-filter>ipv6-filter>entry> <i>entry-id</i> config>system>security>profile <i>user-profile-name</i> >entry <i>entry-id</i>
Description	This command creates a text description stored in the configuration file for a configuration context. The no form of the command removes the string.
Default	n/a
Parameters	<i>description-string</i> — the description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax	[no] shutdown
Context	config>system>security>management-access-filter>ip-filter config>system>security>management-access-filter>ipv6-filter config>system>security>cpm-filter>ip-filter config>system>security>cpm-filter>ipv6-filter config>system>security>radius config>system>security>tacplus
Description	This command administratively disables the entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. When disabled, an entity does not change, reset, or remove any configuration settings or statistics, other than the administrative state. Many objects must be shut down before they can be deleted. The no form of the command puts an entity into the administratively enabled state. Many entities must be explicitly enabled using the no shutdown command.
Default	no shutdown

Security Commands

security

Syntax	security
Context	config>system
Description	<p>This command creates the context to configure security settings.</p> <p>Security commands manage user profiles and user membership. Security commands also manage user login registrations.</p>

copy

Syntax	copy {user <i>source-user</i> profile <i>source-profile</i>} to <i>destination</i> [overwrite]
Context	config>system>security
Description	<p>This command copies the specified user or profile configuration parameters to another (destination) user or profile.</p> <p>The password is set to the return key and a new password at login must be selected.</p>
Parameters	<p><i>source-user</i> — the user to copy from. The user must already exist.</p> <p><i>source-profile</i> — the profile to copy from. The profile must already exist.</p> <p><i>destination</i> — the destination user or profile</p> <p>overwrite — specifies that the destination user or profile configuration will be overwritten with the copied source user or profile configuration. A configuration will not be overwritten if the overwrite command is not specified.</p>

ftp-server

Syntax	[no] ftp-server
Context	config>system>security
Description	<p>This command enables FTP servers running on the system.</p> <p>FTP servers are disabled by default. At system startup, only SSH servers are enabled.</p> <p>The no form of the command disables FTP servers running on the system.</p>
Default	no ftp-server

hash-control

Syntax	hash-control [read-version {1 2 all}] [write-version {1 2}] no hash-control
Context	config>system>security
Description	<p>Whenever the user executes a save or info command, the system will encrypt all passwords and keys, and so on for security reasons. At present, two algorithms exist.</p> <p>The first algorithm is a simple, short key that can be copied and pasted in a different location when the user wants to configure the same password. However, because it is the same password and the hash key is limited to the password/key, it is obvious that it is the same key.</p> <p>The second algorithm is a more complex key, and cannot be copied and pasted in different locations in the configuration file. In this case, if the same key or password is used repeatedly in different contexts, each encrypted (hashed) version will be different.</p>
Default	all — read-version set to accept both versions 1 and 2
Parameters	<p>read-version {1 2 all} — when the read-version is configured as “all,” both versions 1 and 2 will be accepted by the system. Otherwise, only the selected version will be accepted when reading configuration or exec files. The presence of incorrect hash versions will abort the script/startup.</p> <p>write-version {1 2} — selects the hash version that will be used the next time the configuration file is saved (or an info command is executed). Be careful to save the read and write version correctly, so that the file can be properly processed after the next reboot or exec.</p>

source-address

Syntax	source-address
Context	config>system>security
Description	This command specifies the source address that should be used in all unsolicited packets sent by the application.

application

Syntax	application <i>app</i> [<i>ip-int-name</i> <i>ip-address</i>] no application <i>app</i>
Context	config>system>security>source-address
Description	<p>This command specifies the application to use the source IP address specified by the source-address command.</p> <p>The no form of the command removes the specified source address from the application, causing the application to use the system IP address as the source address.</p>

Parameters *app* — specifies the application name

Values telnet, ftp, ssh, radius, tacplus, snmptrap, syslog, ping, traceroute, dns, sntp, ntp

ip-int-name | *ip-address* — specifies the name of the IP interface or IP address. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

telnet-server

Syntax [no] telnet-server

Context config>system>security

Description This command enables Telnet servers running on the system.

Telnet servers are off by default. At system startup, only SSH servers are enabled.

Telnet servers in 7705 SAR networks limit a Telnet client to three retries to log in. The Telnet server disconnects the Telnet client session after three retries.

The **no** form of the command disables Telnet servers running on the system.

Default no telnet-server

telnet6-server

Syntax [no] telnet6-server

Context config>system>security

Description This command enables Telnet IPv6 servers running on the system.

Telnet servers are off by default. At system startup, only SSH servers are enabled.

Telnet servers in 7705 SAR networks limit a Telnet client to three retries to log in. The Telnet server disconnects the Telnet client session after three retries.

The **no** form of the command disables Telnet servers running on the system.

Default no telnet6-server

Management Access Filter Commands

management-access-filter

Syntax	[no] management-access-filter
Context	config>system>security
Description	<p>This command creates the context to edit management access filters and to reset match criteria.</p> <p>Management access filters control all traffic in and out of the CSM. They can be used to restrict management of the 7705 SAR by other nodes outside either specific (sub)networks or through designated ports.</p> <p>Management filters, as opposed to other traffic filters, are enforced by system software.</p> <p>The no form of the command removes management access filters from the configuration.</p>
Default	n/a

ip-filter

Syntax	ip-filter
Context	config>system>security>management-access-filter
Description	This command creates the context to configure IP filter commands.

ipv6-filter

Syntax	ipv6-filter
Context	config>system>security>management-access-filter
Description	This command creates the context to configure IPv6 filter commands.

default-action

Syntax	default-action { permit deny deny-host-unreachable }
Context	config>system>security>management-access-filter>ip-filter config>system>security>management-access-filter>ipv6-filter
Description	<p>This command creates the default action for management access in the absence of a specific management access filter match.</p> <p>The default-action is applied to a packet that does not satisfy any match criteria in any of the management access filters. Whenever management access filters are configured, the default-action must be defined.</p>
Default	n/a
Parameters	<p>permit — specifies that packets not matching the configured selection criteria in any of the filter entries will be permitted</p> <p>deny — specifies that packets not matching the selection criteria will be denied</p> <p>deny-host-unreachable — specifies that packets not matching the selection criteria will be denied and a host unreachable message will be issued</p>

renum

Syntax	renum <i>old-entry-number new-entry-number</i>
Context	config>system>security>management-access-filter>ip-filter config>system>security>management-access-filter>ipv6-filter
Description	<p>This command renumbers existing management access filter entries to resequence filter entries.</p> <p>The 7705 SAR exits on the first match found and executes the actions in accordance with the accompanying action command. This may require some entries to be renumbered from most to least explicit.</p>
Parameters	<p><i>old-entry-number</i> — the entry number of the existing entry</p> <p>Values 1 to 9999</p> <p><i>new-entry-number</i> — the new entry number that will replace the old entry number</p> <p>Values 1 to 9999</p>

Management Access Filter Entry Commands

entry

Syntax	[no] entry <i>entry-id</i>
Context	config>system>security>management-access-filter>ip-filter config>system>security>management-access-filter>ipv6-filter
Description	<p>This command is used to create or edit a management access filter entry. Multiple entries can be created with unique <i>entry-id</i> numbers. The 7705 SAR exits the filter upon the first match found and executes the actions according to the respective action command. For this reason, entries must be sequenced correctly from most to least explicit.</p> <p>An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword action defined to be considered complete. Entries without the action keyword are considered incomplete and inactive.</p> <p>The no form of the command removes the specified entry from the management access filter.</p>
Default	n/a
Parameters	<p><i>entry-id</i> — an entry ID uniquely identifies a match criteria and the corresponding action. It is recommended that entries be numbered in staggered increments. This allows users to insert a new entry in an existing policy without having to renumber the existing entries.</p> <p>Values 1 to 9999</p>

action

Syntax	action {permit deny deny-host-unreachable} no action
Context	config>system>security>management-access-filter>ip-filter>entry config>system>security>management-access-filter>ipv6-filter>entry
Description	<p>This command creates the action associated with the management access filter match criteria entry.</p> <p>The action keyword is required. If no action is defined, the filter is ignored. If multiple action statements are configured, the last one overwrites previous configured actions.</p> <p>If the packet does not meet any of the match criteria, the configured default action is applied.</p>
Default	n/a

- Parameters**
- permit** — specifies that packets matching the configured criteria will be permitted
 - deny** — specifies that packets not matching the selection criteria will be denied
 - deny-host-unreachable** — specifies that packets not matching the selection criteria will be denied and a host unreachable message will be issued

dst-port

- Syntax** **dst-port** *port* [*mask*]
no dst-port
- Context** config>system>security>management-access-filter>ip-filter>entry
config>system>security>management-access-filter>ipv6-filter>entry
- Description** This command configures a destination TCP or UDP port number or port range for a management access filter match criterion.
- The **no** form of the command removes the destination port match criterion.
- Default** n/a
- Parameters** *port* — the source TCP or UDP port number as match criteria
- Values** 1 to 65535 (decimal)
- mask* — mask used to specify a range of destination port numbers as the match criterion
- This 16-bit mask can be configured using the following formats:

Table 5: 16-bit Mask Formats

Format Style	Format Syntax	Example
Decimal	DDDDD	63488
Hexadecimal	0xHHHH	0xF800
Binary	0bBBBBBBBBBBBBBBBB	0b1111100000000000

For example, to select a range from 1024 up to 2047, specify 1024 0xFC00 for value and mask.

Default 65535 (exact match)

Values 1 to 65535 (decimal)

flow-label

Syntax	flow-label <i>value</i> no flow-label
Context	config>system>security>management-access-filter>ipv6-filter>entry
Description	This command configures flow label match conditions for a management access filter match criterion. Flow labeling enables the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non-default QoS or real-time service. This command applies to IPv6 filters only.
Parameters	<i>value</i> — the flow identifier in an IPv6 packet header that can be used to discriminate traffic flows (see RFC 3595, <i>Textual Conventions for IPv6 Flow Label</i>) Values 0 to 1048575

log

Syntax	[no] log
Context	config>system>security>management-access-filter>ip-filter>entry config>system>security>management-access-filter>ipv6-filter>entry
Description	This command enables match logging. The no form of this command disables match logging.
Default	no log

next-header

Syntax	[no] next-header <i>next-header</i>
Context	config>system>security>management-access-filter>ipv6-filter>entry
Description	This command specifies the next header to match as a management access filter match criterion. This command applies to IPv6 filters only.

Parameters	<i>next-header</i> — the IPv6 next header to match. This parameter is similar to the protocol parameter used in IPv4 filter match criteria.
Values	[1 to 42 45 to 49 52 to 59 61 to 255] — (values can be expressed in decimal, hexadecimal, or binary - DHB) keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp * — udp/tcp wildcard

protocol

Syntax	[no] protocol <i>protocol-id</i>
Context	config>system>security>management-access-filter>ip-filter>entry
Description	<p>This command configures an IP protocol type to be used as a management access filter match criterion.</p> <p>The protocol type is identified by its respective protocol number. Well-known protocol numbers include ICMP (1), TCP (6), and UDP (17).</p> <p>This command applies to IPv4 filters only.</p> <p>The no form of the command removes the protocol from the match criteria.</p>
Default	n/a
Parameters	<i>protocol-id</i> — the protocol number for the match criterion
Values	1 to 255 (decimal)

router

Syntax	router <i>router-instance</i> no router
Context	config>system>security>management-access-filter>ip-filter>entry config>system>security>management-access-filter>ipv6-filter>entry
Description	<p>This command configures a router name or service ID to be used as a management access filter match criterion.</p> <p>The no form of the command removes the router name or service ID from the match criteria.</p>

Parameters *router-instance* — specifies one of the following parameters for the router instance:

- router-name* — specifies a router name up to 32 characters to be used in the match criteria
- service-id* — specifies an existing service ID to be used in the match criteria

Values 1 to 2147483647

src-ip

Syntax **src-ip** {*ip-prefix/mask* | *ip-prefix netmask*}
no src-ip

Context config>system>security>management-access-filter>ip-filter>entry

Description This command configures a source IPv4 address range to be used as a management access filter match criterion.

To match on the source IP address, specify the address and the associated mask (for example, 10.1.0.0/16). The conventional notation of 10.1.0.0 255.255.0.0 can also be used.

The **no** form of the command removes the source IP address match criterion.

Default n/a

Parameters *ip-prefix* — the IP prefix for the IP match criterion in dotted-decimal notation
mask — specifies the subnet mask length expressed as a decimal integer

Values 0.0.0.0 to 255.255.255.255 (IP prefix), 1 to 32 (mask length)

netmask — the subnet mask in dotted-decimal notation

Values a.b.c.d (network bits all 1 and host bits all 0)

src-ip

Syntax **src-ip** *ipv6-address/prefix-length*
no src-ip

Context config>system>security>management-access-filter>ipv6-filter>entry

Description This command configures a source IPv6 address range to be used as an management access filter match criterion.

To match on the source IP address, specify the address and prefix length; for example, 11::12/128.

The **no** form of the command removes the source IP address match criterion.

Default n/a

Parameters	<i>ipv6-address/prefix-length</i> — the IPv6 address on the interface		
Values	<i>ipv6-address</i>	x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D	
	<i>prefix-length</i>	1 to 128	

src-port

Syntax	src-port {port-id cpm} no src-port		
Context	config>system>security>management-access-filter>ip-filter>entry config>system>security>management-access-filter>ipv6-filter>entry		
Description	<p>This command restricts ingress management traffic to either the CSM Ethernet port or any other logical port (port or channel) on the device.</p> <p>When the source interface is configured, only management traffic arriving on those ports satisfy the match criteria.</p> <p>The no form of the command reverts to the default value.</p>		
Default	any interface		
Parameters	<p>port-id — the port ID in the following format: slot/mda/port (the slot ID is always 1)</p> <p>For example: port 3 on MDA 2 on card 1 would be specified as 1/2/3.</p>		
Syntax:	port-id		
Values	port-id	slot/mda/port[.channel] bundle-id - bundle-<type>-slot/mda.<bundle-num> bundle - keyword type - ima ppp bundle-num - [1..10]	
	cpm — specifies that ingress management traffic is restricted to the CSM Ethernet port		

CPM Filter Commands

cpm-filter

Syntax	[no] cpm-filter
Context	config>system>security
Description	<p>This command enables the context to configure a CPM filter. A CPM filter is a hardware filter on the CSM that applies to all the traffic going to the CSM CPU. It can be used to drop or accept packets, as well as allocate dedicated hardware queues for the traffic. The hardware queues are not user-configurable.</p> <p>The no form of the command disables the CPM filter.</p>

default-action

Syntax	default-action {accept drop}
Context	config>system>security>cpm-filter
Description	<p>This command specifies the action to be applied to packets when the packets do not match the specified criteria in all of the IP filter entries of the filter. If there are no filter entries defined, the packets received will either be accepted or dropped based on that default action.</p>
Default	accept
Parameters	<p>accept — packets are accepted unless there is a specific filter entry that causes the packet to be dropped</p> <p>drop — packets are dropped unless there is a specific filter entry that causes the packet to be accepted</p>

ip-filter

Syntax	ip-filter
Context	config>system>security>cpm-filter
Description	<p>This command enables the context to configure IPv4 CPM filter parameters.</p>

ipv6-filter

Syntax	ipv6-filter
Context	config>system>security>cpm-filter
Description	This command enables the context to configure IPv6 CPM filter parameters.

entry

Syntax	entry <i>entry-id</i> [create] no entry <i>entry-id</i>
Context	config>system>security>cpm-filter>ip-filter config>system>security>cpm-filter>ipv6-filter
Description	<p>This command specifies a particular CPM filter match entry. Every CPM filter must have at least one filter match entry. A filter entry with no match criteria set will match every packet, and the entry action will be taken.</p> <p>The create keyword must be used with every new entry configured. Once the entry has been created, you can navigate to the entry context without using the create keyword.</p> <p>For filter entries 1 to 29, the match parameters can be any combination of source IP address/range, destination IP address/range, source port/range, and destination port/range as long as the accumulated total of the number of unique records does not exceed 256 combinations.</p> <p>For filter entries 30 to 64 (extended filter entries), there are no range-based restrictions. As few or as many match parameters can be specified as required.</p>
Parameters	<p><i>entry-id</i> — identifies a CPM filter entry as configured on this system.</p> <p>Values 1 to 64</p> <p> where: 1 to 29 are filter entries 30 to 64 are extended filter entries</p>

action

Syntax	action {accept drop} no action
Context	config>system>security>cpm-filter>ip-filter>entry config>system>security>cpm-filter>ipv6-filter>entry
Description	This command specifies the action to take for packets that match this filter entry.
Default	drop
Parameters	accept — packets matching the entry criteria will be forwarded drop — packets matching the entry criteria will be dropped

log

Syntax	log log-id no log
Context	config>system>security>cpm-filter>ip-filter>entry config>system>security>cpm-filter>ipv6-filter>entry
Description	This command specifies the log in which packets matching this entry should be entered. The value 0 indicates that logging is disabled. The no form of the command deletes the log ID.
Parameters	<i>log-id</i> — the log ID where packets matching this entry should be entered Values 101 to 199

match

Syntax	match [protocol protocol-id] no match
Context	config>system>security>cpm-filter>ip-filter>entry
Description	This command enables the context to enter match criteria for the IPv4 filter entry. When the match criteria have been satisfied, the action associated with the match criteria is executed. If more than one match criterion (within one match statement) is configured, all criteria must be satisfied (AND function) before the action associated with the match is executed. A match context may consist of multiple match criteria, but multiple match statements cannot be entered per entry. The no form of the command removes the match criteria for the <i>entry-id</i> .

- Parameters**
- protocol** — configures an IP protocol to be used as an IP filter match criterion. The protocol type such as TCP or UDP is identified by its respective protocol number.
- protocol-id** — configures the decimal value representing the IP protocol to be used as an IP filter match criterion. Common protocol numbers include ICMP(1), TCP(6), UDP(17). The **no** form the command removes the protocol from the match criteria. See [Table 6](#) for the protocol IDs and descriptions for the IP protocols.
- Values** 0 to 255 (values can be expressed in decimal, hexadecimal, or binary – DHB)
- keywords - none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp
- * — udp/tcp wildcard

Table 6: IP Protocol IDs and Descriptions

Protocol ID	Protocol	Description
1	icmp	Internet Control Message
2	igmp	Internet Group Management
4	ip	IP in IP (encapsulation)
6	tcp	Transmission Control
8	egp	Exterior Gateway Protocol
9	igp	Any private interior gateway
17	udp	User Datagram
27	rdp	Reliable Data Protocol
41	ipv6	IPv6
43	ipv6-route	Routing Header for IPv6
44	ipv6-frag	Fragment Header for IPv6
45	idrp	Inter-Domain Routing Protocol
46	rsvp	Reservation Protocol
47	gre	General Routing Encapsulation
58	ipv6-icmp	ICMP for IPv6
59	ipv6-no-nxt	No Next Header for IPv6
60	ipv6-opts	Destination Options for IPv6
80	iso-ip	ISO Internet Protocol
88	eigrp	EIGRP

Table 6: IP Protocol IDs and Descriptions (Continued)

Protocol ID	Protocol	Description
89	ospf-igp	OSPFIGP
97	ether-ip	Ethernet-within-IP Encapsulation
98	encap	Encapsulation Header
102	pnni	PNNI over IP
103	pim	Protocol Independent Multicast
112	vrrp	Virtual Router Redundancy Protocol
115	l2tp	Layer Two Tunneling Protocol
118	stp	Schedule Transfer Protocol
123	ptp	Performance Transparency Protocol
124	isis	ISIS over IPv4
126	crtip	Combat Radio Transport Protocol
127	crudp	Combat Radio User Datagram

match

Syntax **match** [**next-header** *next-header*]
no match

Context config>system>security>cpm-filter>ipv6-filter>entry

Description This command enables the context to enter match criteria for the IPv6 filter entry. When the match criteria have been satisfied, the action associated with the match criteria is executed.

If more than one match criterion (within one match statement) is configured, all criteria must be satisfied (AND function) before the action associated with the match is executed.

A **match** context may consist of multiple match criteria, but multiple **match** statements cannot be entered per entry.

The **no** form of the command removes the match criteria for the *entry-id*.

Parameters	<i>next-header</i> — the IPv6 next header to match. This parameter is similar to the protocol parameter used in IPv4 filter match criteria.
Values	[1 to 42 45 to 49 52 to 59 61 to 255] — (values can be expressed in decimal, hexadecimal, or binary - DHB) keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp * — udp/tcp wildcard

dscp

Syntax	dscp <i>dscp-name</i> no dscp
Context	config>system>security>cpm-filter>ip-filter>entry>match config>system>security>cpm-filter>ipv6-filter>entry>match
Description	This command configures a DiffServ Code Point (DSCP) name to be used as an IP filter match criterion. The no form of the command removes the DSCP match criterion.
Default	no dscp
Parameters	<i>dscp-name</i> — a DSCP name that has been previously mapped to a value using the dscp-name command. The DiffServ Code Point may only be specified by its name. Values be cp1 cp2 cp3 cp4 cp5 cp6 cp7 cs1 cp9 af11 cp11 af12 cp13 af13 cp15 cs2 cp17 af21 cp19 af22 cp21 af23 cp23 cs3 cp25 af31 cp27 af32 cp29 af33 cp31 cs4 cp33 af41 cp35 af42 cp37 af43 cp39 cs5 cp41 cp42 cp43 cp44 cp45 ef cp47 nc1 cp49 cp50 cp51 cp52 cp53 cp54 cp55 nc2 cp57 cp58 cp59 cp60 cp61 cp62 cp63

dst-ip

Syntax	dst-ip <i>{ip-address/mask ip-address netmask}</i> no dst-ip
Context	config>system>security>cpm-filter>ip-filter>entry>match
Description	<p>This command configures a destination IPv4 address range to be used as an IP filter match criterion.</p> <p>To match on the destination IP address, specify the address and its associated mask; for example, 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.</p> <p>The no form of the command removes the destination IP address match criterion.</p>
Default	no dst-ip
Parameters	<p><i>ip-address</i> — the IP prefix for the IP match criterion in dotted-decimal notation</p> <p>Values 0.0.0.0 to 255.255.255.255</p> <p><i>mask</i> — the subnet mask length expressed as a decimal integer</p> <p>Values 1 to 32</p> <p><i>netmask</i> — the dotted-decimal equivalent of the mask length</p> <p>Values 0.0.0.0 to 255.255.255.255</p>

dst-ip

Syntax	dst-ip <i>ipv6-address/prefix-length</i> no dst-ip										
Context	config>system>security>cpm-filter>ipv6-filter>entry>match										
Description	<p>This command configures a destination IPv6 address range to be used as an IP filter match criterion.</p> <p>To match on the destination IP address, specify the address and prefix length; for example, 11::12/128.</p> <p>The no form of the command removes the destination IP address match criterion.</p>										
Default	n/a										
Parameters	<p><i>ipv6-address/prefix-length</i> — the IPv6 address on the interface</p> <p>Values</p> <table> <tr> <td><i>ipv6-address</i></td><td>x:x:x:x:x:x:x (eight 16-bit pieces)</td></tr> <tr> <td></td><td>x:x:x:x:x:d.d.d</td></tr> <tr> <td></td><td>x: [0 to FFFF]H</td></tr> <tr> <td></td><td>d: [0 to 255]D</td></tr> <tr> <td><i>prefix-length</i></td><td>1 to 128</td></tr> </table>	<i>ipv6-address</i>	x:x:x:x:x:x:x (eight 16-bit pieces)		x:x:x:x:x:d.d.d		x: [0 to FFFF]H		d: [0 to 255]D	<i>prefix-length</i>	1 to 128
<i>ipv6-address</i>	x:x:x:x:x:x:x (eight 16-bit pieces)										
	x:x:x:x:x:d.d.d										
	x: [0 to FFFF]H										
	d: [0 to 255]D										
<i>prefix-length</i>	1 to 128										

dst-port

Syntax	dst-port <i>tcp/udp port-number</i> [<i>mask</i>] no dst-port
Context	config>system>security>cpm-filter>ip-filter>entry>match config>system>security>cpm-filter>ipv6-filter>entry>match
Description	<p>This command specifies the TCP/UDP port to match the destination port of the packet.</p> <p>The no form of the command removes the destination port match criterion.</p> <p>The TCP or UDP protocol must be configured using the match command before this filter can be configured.</p>
Parameters	<p><i>tcp/udp port-number</i> — the destination port number to be used as a match criterion</p> <p>Values 0 to 65535 (accepted in decimal, hexadecimal, or binary format)</p> <p><i>mask</i> — the 16-bit mask to be applied when matching the destination port</p>

fragment

Syntax	fragment { true false } no fragment
Context	config>system>security>cpm-filter>ip-filter>entry>match
Description	<p>This command configures fragmented or non-fragmented IP packets as an IP filter match criterion.</p> <p>The no form of the command removes the match criterion.</p> <p>This command applies to IPv4 filters only.</p>
Default	false
Parameters	<p>true — configures a match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set or have the Fragment Offset field of the IP header set to a non-zero value.</p> <p>false — configures a match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero.</p>

icmp-code

Syntax	icmp-code <i>icmp-code</i> no icmp-code
Context	config>system>security>cpm-filter>ip-filter>entry>match config>system>security>cpm-filter>ipv6-filter>entry>match
Description	<p>This command configures matching on an ICMP code field in the ICMP header of an IP packet as an IP filter match criterion.</p> <p>The ICMP protocol must be configured using the match command before this filter can be configured.</p> <p>The no form of the command removes the criterion from the match entry.</p>
Default	no icmp-code
Parameters	<p><i>icmp-code</i> — specifies the ICMP code values that must be present to match</p> <p>Values 0 to 255 (values can be expressed in decimal, hexadecimal, or binary – DHB) keywords - none network-unreachable host-unreachable protocol-unreachable port-unreachable fragmentation-needed dest-network-unknown dest-host-unknown</p>

icmp-type

Syntax	icmp-type <i>icmp-type</i> no icmp-type
Context	config>system>security>cpm-filter>ip-filter>entry>match config>system>security>cpm-filter>ipv6-filter>entry>match
Description	<p>This command configures matching on an ICMP type field in the ICMP header of an IP packet as an IP filter match criterion.</p> <p>The ICMP protocol must be configured using the match command before this filter can be configured.</p> <p>The no form of the command removes the criterion from the match entry.</p>
Default	no icmp-type
Parameters	<p><i>icmp-type</i> — specifies the ICMP type values that must be present to match</p> <p>Values 0 to 255 (values can be expressed in decimal, hexadecimal, or binary – DHB) keywords - none echo-reply dest-unreachable echo-request time-exceeded parameter-problem</p>

ip-option

Syntax	ip-option <i>ip-option-value</i> [<i>ip-option-mask</i>] no ip-option
Context	config>system>security>cpm-filter>ip-filter>entry>match
Description	This command configures matching packets with a specific IP option or a range of IP options in the IP header as an IP filter match criterion.

The option type octet contains 3 fields:

- 1 bit copied flag (copy options in all fragments)
- 2 bits option class
- 5 bits option number

The **no** form of the command removes the match criterion.

This command applies to IPv4 filters only.

Default	no ip-option
Parameters	<p><i>ip-option-value</i> — the 8-bit option type (can be entered using decimal, hexadecimal, or binary formats). The mask is applied as an AND to the option byte and the result is compared with the option value.</p> <p>The decimal value entered for the match should be a combined value of the 8-bit option type field and not just the option number. Therefore, to match on IP packets that contain the Router Alert option (option number = 20), enter the option type of 148 (10010100).</p> <p>Values 0 to 255</p>

ip-option-mask — specifies a range of option numbers to use as the match criteria

This 8-bit mask can be entered using decimal, hexadecimal, or binary formats as shown in [Table 7](#).

Table 7: IP Option Formats

Format Style	Format Syntax	Example
Decimal	DDD	20
Hexadecimal	0xHH	0x14
Binary	0BBBBBBBBB	0b0010100

Default 255 (decimal) (exact match)

Values 0 to 255

multiple-option

Syntax	multiple-option {true false} no multiple-option
Context	config>system>security>cpm-filter>ip-filter>entry>match
Description	<p>This command configures matching packets that contain more than one option field in the IP header as an IP filter match criterion.</p> <p>The no form of the command removes the checking of the number of option fields in the IP header as a match criterion.</p> <p>This command applies to IPv4 filters only.</p>
Default	no multiple-option
Parameters	<p>true — specifies matching on IP packets that contain more than one option field in the header</p> <p>false — specifies matching on IP packets that do not contain multiple option fields in the header</p>

option-present

Syntax	option-present {true false} no option-present
Context	config>system>security>cpm-filter>ip-filter>entry>match
Description	<p>This command configures matching packets that contain the option field or have an option field of 0 in the IP header as an IP filter match criterion.</p> <p>The no form of the command removes the checking of the option field in the IP header as a match criterion.</p> <p>This command applies to IPv4 filters only.</p>
Parameters	<p>true — specifies matching on all IP packets that contain the option field in the header. A match will occur for all packets that have the option field present. An option field of 0 is considered as no option present.</p> <p>false — specifies matching on IP packets that do not have any option field present in the IP header (an option field of 0)</p>

src-ip

Syntax	src-ip <i>{ip-address/mask ip-address netmask}</i> no src-ip
Context	config>system>security>cpm-filter>ip-filter>entry>match
Description	<p>This command specifies the IPv4 address to match the source IP address of the packet.</p> <p>To match on the source IP address, specify the address and its associated mask; for example, 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 may also be used.</p> <p>The no form of the command removes the source IP address match criterion.</p>
Default	no src-ip
Parameters	<p><i>ip-address</i> — the IP prefix for the IP match criterion in dotted-decimal notation</p> <p>Values 0.0.0.0 to 255.255.255.255</p> <p><i>mask</i> — the subnet mask length expressed as a decimal integer</p> <p>Values 1 to 32</p> <p><i>netmask</i> — the dotted-decimal equivalent of the mask length</p> <p>Values 0.0.0.0 to 255.255.255.255</p>

src-ip

Syntax	src-ip <i>ipv6-address/prefix-length</i> no src-ip				
Context	config>system>security>cpm-filter>ipv6-filter>entry>match				
Description	<p>This command configures a source IPv6 address range to be used as an IP filter match criterion.</p> <p>To match on the source IP address, specify the address and prefix length; for example, 11::12/128.</p> <p>The no form of the command removes the source IP address match criterion.</p>				
Default	n/a				
Parameters	<p><i>ipv6-address/prefix-length</i> — the IPv6 address on the interface</p> <p>Values</p> <table> <tr> <td><i>ipv6-address</i></td><td> x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D </td></tr> <tr> <td><i>prefix-length</i></td><td>1 to 128</td></tr> </table>	<i>ipv6-address</i>	x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D	<i>prefix-length</i>	1 to 128
<i>ipv6-address</i>	x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D				
<i>prefix-length</i>	1 to 128				

src-port

Syntax	src-port <i>src-port-number</i> [<i>mask</i>] no src-port
Context	config>system>security>cpm-filter>ip-filter>entry>match config>system>security>cpm-filter>ipv6-filter>entry>match
Description	This command specifies the TCP/UDP port to match the source port of the packet.
Default	no src-port
Parameters	<i>src-port-number</i> — the source port number to be used as a match criterion Values 0 to 65535 (accepted in decimal, hexadecimal, or binary format) <i>mask</i> — the 16-bit mask to be applied when matching the destination port

tcp-ack

Syntax	tcp-ack { true false } no tcp-ack
Context	config>system>security>cpm-filter>ip-filter>entry>match config>system>security>cpm-filter>ipv6-filter>entry>match
Description	This command configures matching on the ACK bit being set or reset in the control bits of the TCP header of an IP packet as an IP filter match criterion. The no form of the command removes the criterion from the match entry.
Default	no tcp-ack
Parameters	true — specifies matching on IP packets that have the ACK bit set in the control bits of the TCP header of an IP packet false — specifies matching on IP packets that do not have the ACK bit set in the control bits of the TCP header of the IP packet

tcp-syn

Syntax	tcp-syn {true false} no tcp-syn
Context	config>system>security>cpm-filter>ip-filter>entry>match config>system>security>cpm-filter>ipv6-filter>entry>match
Description	<p>This command configures matching on the SYN bit being set or reset in the control bits of the TCP header of an IP packet as an IP filter match criterion.</p> <p>The SYN bit is normally set when the source of the packet wants to initiate a TCP session with the specified destination IP address.</p> <p>The no form of the command removes the criterion from the match entry.</p>
Default	no tcp-syn
Parameters	<p>true — specifies matching on IP packets that have the SYN bit set in the control bits of the TCP header</p> <p>false — specifies matching on IP packets that do not have the SYN bit set in the control bits of the TCP header</p>

renum

Syntax	renum <i>old-entry-id new-entry-id</i>
Context	config>system>security>cpm-filter>ip-filter config>system>security>cpm-filter>ipv6-filter
Description	<p>This command renumbers existing IP filter entries in order to resequence filter entries.</p> <p>Resequencing may be required in some cases because the OS exits when the first match is found and executes the actions according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.</p>
Parameters	<p><i>old-entry-id</i> — the entry number of an existing entry</p> <p>Values 1 to 64</p> <p>where: 1 to 29 are filter entries 30 to 64 are extended filter entries</p> <p><i>new-entry-id</i> — the new entry number to be assigned to the old entry</p> <p>Values 1 to 64</p> <p>where: 1 to 29 are filter entries 30 to 64 are extended filter entries</p>

Global Password Commands

enable-admin

Syntax	enable-admin
Context	<global>
Description	



Note: See the description for the [admin-password](#) command. If the **admin-password** is configured in the **config>system>security>password** context, then any user can enter the special administrative mode by entering the **enable-admin** command.

The **enable-admin** command is in the default profile. By default, all users are given access to this command.

Once the **enable-admin** command is entered, the user is prompted for a password. If the password matches, the user is given unrestricted access to all the commands.

There are two ways to verify that a user is in the enable-admin mode:

- Enter the `show users` command – Administrator can know which users are in this mode
- Enter the `enable-admin` command again at the root prompt and an error message will be returned

```
A:ALU-1# show users
=====
User          Type    Login time                               Idle time
  From
=====
admin         Console 10AUG2006 13:55:24                       0d 19:42:22
--
admin         Telnet  09AUG2006 08:35:23                       0d 00:00:00 A
10.20.30.93
-----
Number of users : 2
'A' indicates user is in admin mode
=====
A:ALU-1#
A:ALU-1# enable-admin
MINOR: CLI Already in admin mode.
A:ALU-1#
```

Password Commands

password

Syntax	password
Context	config>system>security
Description	This command creates the context to configure password management parameters.

admin-password

Syntax	admin-password <i>password</i> [<i>hash</i> <i>hash2</i>] no admin-password
Context	config>system>security>password
Description	This command allows a user (with admin permissions) to configure a password which enables a user to become an administrator.



Note: See the description for the [enable-admin](#) command. If the **admin-password** is configured in the **config>system>security>password** context, then any user can enter the admin mode by entering the **enable-admin** command and the correct admin password.

The minimum length of the password is determined by the **minimum-length** command. The complexity requirements for the password are determined by the **complexity** command.



Note: The *password* argument of this command is not sent to the servers. This is consistent with other commands that configure secrets. User names and passwords in the FTP and TFTP URLs will not be sent to the authorization or accounting servers when the **file>copy** *source-url dest-url* command is executed.

For example:

```
file copy ftp://test:secret@131.12.31.79/test/srcfile cf3:\destfile
```

In this example, the user name “test” and password “secret” will not be sent to the AAA servers (or to any logs). They will be replaced with “*****”.

The **no** form of the command removes the admin password from the configuration.

Default	no admin-password
Parameters	<p><i>password</i> — configures the password that enables a user to become a system administrator. The maximum length can be up to 20 characters if unhashed, 32 characters if hashed, and 54 characters if the hash2 keyword is specified.</p> <p>hash — specifies that the key is entered and stored on the node in encrypted form</p> <p>hash2 — specifies that the key is entered and stored on the node in a more complex encrypted form</p>



Note: If neither the hash nor hash2 keyword is specified, the key is entered in clear text. However, for security purposes, the key is stored on the node using hash encryption.

aging

Syntax	aging days no aging
Context	config>system>security>password
Description	<p>This command configures the number of days a user password is valid before the user must change their password.</p> <p>The no form of the command reverts to the default value.</p>
Default	No aging is enforced.
Parameters	<p><i>days</i> — the maximum number of days the password is valid</p> <p>Values 1 to 500</p>

attempts

Syntax	attempts count [time minutes1] [lockout minutes2] no attempts
Context	config>system>security>password
Description	<p>This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame.</p> <p>If the threshold is exceeded, the user is locked out for a specified time period.</p> <p>If multiple attempts commands are entered, each command overwrites the previously entered command.</p> <p>The no attempts command resets all values to default.</p>

Default	count: 3 time minutes: 5 lockout minutes: 10
Parameters	<p>count — the number of unsuccessful login attempts allowed for the specified time. This is a mandatory value that must be explicitly entered.</p> <p>Values 1 to 64</p> <p>time minutes — the period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out</p> <p>Values 0 to 60</p> <p>lockout minutes — the lockout period, in minutes, where the user is not allowed to log in. Values are minutes.</p> <p>Values 0 to 1440</p> <p>When the user exceeds the attempted count times in the specified time, then that user is locked out from any further login attempts for the configured time period.</p>

authentication-order

Syntax	authentication-order [<i>method-1</i>] [<i>method-2</i>] [<i>method-3</i>] [exit-on-reject] no authentication-order
Context	config>system>security>password
Description	<p>This command configures the sequence in which password authentication, authorization, and accounting is attempted among RADIUS, TACACS+, and local passwords.</p> <p>The order should be from the most preferred authentication method to the least preferred. The presence of all methods in the command line does not guarantee that they are all operational. Specifying options that are not available delays user authentication.</p> <p>If all (operational) methods are attempted and no authentication for a particular login has been granted, then an entry in the security log registers the failed attempt. Both the attempted login identification and originating IP address are logged with a timestamp.</p> <p>The no form of the command reverts to the default authentication sequence.</p>
Default	authentication-order radius tacplus local
Parameters	<p><i>method-1</i> — the first password authentication method to attempt</p> <p>Default radius</p> <p>Values radius, tacplus, local</p> <p><i>method-2</i> — the second password authentication method to attempt</p> <p>Default tacplus</p> <p>Values radius, tacplus, local</p>

method-3 — the third password authentication method to attempt

Default local

Values radius, tacplus, local

radius — RADIUS authentication

tacplus — TACACS+ authentication

local — password authentication based on the local password database

exit-on-reject — when enabled, and if one of the AAA methods configured in the authentication order sends a reject, then the next method in the order will not be tried. If the **exit-on-reject** keyword is not specified and one AAA method sends a reject, the next AAA method will be attempted. If in this process all the AAA methods are exhausted, it will be considered a reject.

Note that a rejection is distinct from an unreachable authentication server. When the **exit-on-reject** keyword is specified, authorization and accounting will only use the method that provided an affirmation authentication; only if that method is no longer readable or is removed from the configuration will other configured methods be attempted. If the local keyword is the first authentication and:

- **exit-on-reject** is configured and the user does not exist, the user will not be authenticated
- the user is authenticated locally, then other methods, if configured, will be used for authorization and accounting
- the user is configured locally but without console access, login will be denied

complexity

Syntax	[no] complexity [numeric] [special-character] [mixed-case]
Context	config>system>security>password
Description	<p>This command configures the complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96, and des-keys configured in the config>system>security>user <i>user-name</i> >snmp>authentication context.</p> <p>If more than one complexity command is entered, each command overwrites the previous command.</p> <p>The no form of the command cancels all requirements. To remove a single requirement, enter the no form of the command followed by the requirement that needs to be removed (for example, no complexity numeric).</p>
Default	No complexity requirements are configured.
Parameters	<p>mixed-case — specifies that at least one uppercase and one lowercase character must be present in the password. This keyword can be used in conjunction with the numeric and special-character parameters. However, if this command is used with the authentication none command, the complexity command is rejected.</p>

numeric — specifies that at least one numeric character must be present in the password. This keyword can be used in conjunction with the **mixed-case** and **special-character** parameters. However, if this command is used with the **authentication none** command, the **complexity** command is rejected.

special-character — specifies that at least one special character must be present in the password. This keyword can be used in conjunction with the **numeric** and **mixed-case** parameters. However, if this command is used with the **authentication none** command, the **complexity** command is rejected.

Special characters include: ~!@#\$\$%^&*()_+|{}:”<>?’-=\[];’,./.

health-check

Syntax	[no] health-check
Context	config>system>security>password
Description	<p>This command specifies that RADIUS and TACACS+ servers are monitored for 3 seconds each at 30-second intervals. Servers that are not configured will have 3 seconds of idle time. If in this process a server is found to be unreachable, or a previously unreachable server starts responding, depending on the type of server, a trap will be sent.</p> <p>The no form of the command disables the periodic monitoring of the RADIUS and TACACS+ servers. In this case, the operational status for the active server will be up if the last access was successful.</p>
Default	health-check

minimum-length

Syntax	minimum-length <i>value</i> no minimum-length
Context	config>system>security>password
Description	<p>This command configures the minimum number of characters required for locally administered passwords, HMAC-MD5-96, HMAC-SHA-96, and des-keys configured in the config>system>security context.</p> <p>If multiple minimum-length commands are entered, each command overwrites the previously entered command.</p> <p>The no form of the command reverts to the default value.</p>
Default	minimum-length 6
Parameters	<p><i>value</i> — the minimum number of characters required for a password</p> <p>Values 1 to 8</p>

Profile Management Commands

profile

Syntax	[no] profile <i>user-profile-name</i>
Context	config>system>security
Description	<p>This command creates a context to create user profiles for CLI command tree permissions.</p> <p>Profiles are used to either deny or permit user console access to a hierarchical branch or to specific commands.</p> <p>Once the profiles are created, the user command assigns users to one or more profiles. You can define up to 16 user profiles, but a maximum of 8 profiles can be assigned to a user.</p> <p>The no form of the command deletes a user profile.</p>
Default	user-profile default
Parameters	<i>user-profile-name</i> — the user profile name entered as a character string. The string is case-sensitive and limited to 32 ASCII 7-bit printable characters with no spaces.

default-action

Syntax	default-action { deny-all permit-all none }
Context	config>system>security>profile <i>user-profile-name</i>
Description	This command specifies the default action to be applied when no match conditions are met.
Default	none
Parameters	<p>deny-all — sets the default of the profile to deny access to all commands</p> <p>permit-all — sets the default of the profile to permit access to all commands</p>



Note: **permit-all** does not change access to security commands. Security commands are only and always available to members of the admin-user profile.

none — sets the default of the profile to no-action. This option is useful to assign multiple profiles to a user.

For example, if a user is a member of two profiles and the default action of the first profile is **permit-all**, then the second profile will never be evaluated because **permit-all** is executed first. If the first profile default action is set to **none** and if no match conditions are met in the first profile, then the second profile will be evaluated. If the default action of the last profile is **none** and no explicit match is found, then the default-action **deny-all** takes effect.

renum

Syntax	renum <i>old-entry-number new-entry-number</i>
Context	config>system>security>profile <i>user-profile-name</i>
Description	<p>This command renumbers profile entries to resequence the entries.</p> <p>Since the 7705 SAR exits when the first match is found and executes the actions according to the accompanying action command, renumbering is useful to rearrange the entries from most explicit to least explicit.</p>
Parameters	<p><i>old-entry-number</i> — the entry number of an existing entry</p> <p>Values 1 to 9999</p> <p><i>new-entry-number</i> — the new entry number</p> <p>Values 1 to 9999</p>

Profile Management Entry Commands

entry

Syntax	[no] entry <i>entry-id</i>
Context	config>system>security>profile <i>user-profile-name</i>
Description	<p>This command is used to create a user profile entry.</p> <p>More than one entry can be created with unique <i>entry-id</i> numbers. The 7705 SAR exits when the first match is found and executes the actions according to the accompanying action command. Entries should be sequenced from most explicit to least explicit.</p> <p>An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword action for it to be considered complete.</p> <p>The no form of the command removes the specified entry from the user profile.</p>
Default	No entry IDs are defined.

Parameters	<i>entry-id</i> — an entry-id uniquely identifies a user profile command match criteria and a corresponding action. If more than one entry is configured, the <i>entry-ids</i> should be numbered in staggered increments to allow users to insert a new entry without requiring renumbering of the existing entries.
Values	1 to 9999

action

Syntax	action {deny permit}
Context	config>system>security>profile <i>user-profile-name</i> >entry <i>entry-id</i>
Description	This command configures the action associated with the profile entry.
Parameters	deny — specifies that commands matching the entry command match criteria will be denied permit — specifies that commands matching the entry command match criteria will be permitted

match

Syntax	match <i>command-string</i> no match
Context	config>system>security>profile <i>user-profile-name</i> >entry <i>entry-id</i>
Description	<p>This command configures a command or command subtree.</p> <p>Because the 7705 SAR exits when the first match is found, subordinate levels cannot be modified with subsequent action commands. More specific action commands should be entered with a lower entry number or in a profile that is evaluated prior to this profile.</p> <p>All commands below the hierarchy level of the matched command are denied.</p> <p>The no form of this command removes a match condition.</p>
Default	No match command string is specified.
Parameters	<i>command-string</i> — the CLI command or CLI tree level that is the scope of the profile entry

User Management Commands

user

Syntax	[no] user <i>user-name</i>
Context	config>system>security
Description	<p>This command creates a local user and a context to edit the user configuration.</p> <p>If a new <i>user-name</i> is entered, the user is created. When an existing <i>user-name</i> is specified, the user parameters can be edited.</p> <p>When a new user is created and the info command is entered, the system displays a password with has2 encryption in the output screen. However, when using that user name, there will be no password required. The user can log in to the system by entering their user name and then pressing ↵ at the password prompt.</p> <p>Unless an administrator explicitly changes the password, it will be null. The hashed value displayed uses the user name and null password field, so when the user name is changed, the displayed hashed value will change.</p> <p>The no form of the command deletes the user and all configuration data. Users cannot delete themselves.</p>
Default	none
Parameters	<i>user-name</i> — the name of the user, up to 16 characters


user-template

Syntax	user-template { tacplus_default radius_default }
Context	config>system>security
Description	This command configures default security user template parameters.
Parameters	tacplus_default — specifies that the default template is used for the configuration

access

Syntax	[no] access [ftp] [snmp] [console] [no] access [ftp] [console]
Context	config>system>security>user <i>user-name</i> config>system>security>user-template
Description	<p>This command grants a user permission for FTP, SNMP, or console access.</p> <p>If a user requires access to more than one application, then multiple applications can be specified in a single command. Multiple commands are treated sequentially.</p> <p>The no form of command removes access for a specific application.</p> <p>The no access command denies permission for all management access methods. To deny a single access method, enter the no form of the command followed by the method to be denied; for example, no access FTP denies FTP access.</p>
Default	no access
Parameters	<p>ftp — specifies FTP permission</p> <p>snmp — specifies SNMP permission. This keyword is only configurable in the config>system>security>user context.</p> <p>console — specifies console access (serial port or Telnet) permission</p>

home-directory

Syntax	home-directory url-prefix [directory] [directory/directory...] no home-directory
Context	config>system>security>user <i>user-name</i> config>system>security>user-template
Description	<p>This command configures the local home directory for the user for both console and FTP access.</p> <p>If the URL or the specified URL/directory structure is not present, then a warning message is issued and the default is assumed.</p> <p>The no form of the command removes the configured home directory.</p>
Default	no home-directory
	<p> Note: If restrict-to-home has been configured, no file access is granted and no home-directory is created; if restricted-to-home is not applied, root becomes the user's home-directory.</p>

Parameters *url-prefix* [*directory*] [*directory/directory...*] — the user's local home directory URL prefix and directory structure, up to 190 characters in length

password

Syntax **password** [*password*] [**hash** | **hash2**]

Context config>system>security>user *user-name*

Description This command configures the user password for console and FTP access.

The use of the **hash** keyword sets the initial password when the user is created or modifies the password of an existing user and specifies that the given password was hashed using hashing algorithm version 1.

The use of the **hash2** keyword specifies that the given password is already hashed using hashing algorithm version 2. A semantic check is performed on the given password field to verify that it is a valid hash 2 key to store in the database.

The password is stored in an encrypted format in the configuration file when specified. Passwords must be encased in double quotes (" ") at the time of the password creation if they contain any special characters. The double quote character (") is not accepted inside a password. It is interpreted as the start or stop delimiter of a string.

For example:

```
config>system>security# user testuser1
config>system>security>user$ password "zx/Uhcn6ReMOZ3BVrWcvk." hash2
config>system>security>user# exit

config>system>security# info
-----
...
        user "testuser1"
            password "zx/Uhcn6ReMOZ3BVrWcvk." hash2
        exit
...
-----
config>system>security#
```

Parameters *password* — the password for the user that must be entered by this user during the login procedure. The minimum length of the password is determined by the **minimum-length** command. The maximum length can be up to 20 characters if unhashed and 32 characters if hashed or 54 characters if hash2. The complexity requirements for the password are determined by the **complexity** command.

Passwords that contain special characters (#, \$, spaces, etc.) must be enclosed within double quotes.

For example: config>system>security>user# password "south#bay?"

The question mark character (?) cannot be directly inserted as input during a Telnet connection because the character is bound to the **help** command during a normal Telnet/console connection.

To insert # or ? characters, they must be entered inside a notepad or clipboard program and then cut and pasted into the Telnet session in the password field that is encased in the double quotes as delimiters for the password.

If a password is entered without any parameters, a password length of zero is implied (return key).

hash — specifies that the given password is already hashed using hashing algorithm version 1. A semantic check is performed on the given password field to verify that it is a valid hash 1 key to store in the database.

hash2 — specifies that the given password is already hashed using hashing algorithm version 2. A semantic check is performed on the given password field to verify that it is a valid hash 2 key to store in the database.

restricted-to-home

Syntax	[no] restricted-to-home
Context	config>system>security>user <i>user-name</i> config>system>security>user-template
Description	<p>This command prevents users from navigating above their home directories for file access. A user is not allowed to navigate to a directory higher in the directory tree on the home directory device. The user is allowed to create and access subdirectories below their home directory.</p> <p>If a home directory is not configured or the home directory is not available, then the user has no file access.</p> <p>The no form of the command allows the user access to navigate to directories above their home directory.</p>
Default	no restricted-to-home

User Management Console Commands

console

Syntax	console
Context	config>system>security>user <i>user-name</i> config>system>security>user-template
Description	This command creates the context to configure user profile membership for the console.

cannot-change-password

Syntax	[no] cannot-change-password
Context	config>system>security>user <i>user-name</i> >console
Description	<p>This command allows a user to change their password for both FTP and console login.</p> <p>To disable a user's privilege to change their password, use the cannot-change-password form of the command.</p> <p>Note that the cannot-change-password flag is not replicated when a user copy is performed. A new-password-at-login flag is created instead.</p>
Default	no cannot-change-password

login-exec

Syntax	[no] login-exec <i>url-prefix:source-url</i>
Context	config>system>security>user <i>user-name</i> >console config>system>security>user-template>console
Description	<p>This command configures a user's login exec file, which executes whenever the user successfully logs in to a console session.</p> <p>Only one exec file can be configured. If multiple login-exec commands are entered for the same user, each subsequent entry overwrites the previous entry.</p> <p>The no form of the command disables the login exec file for the user.</p>
Default	No login exec file is defined.
Parameters	<i>url-prefix: source-url</i> — enter either a local or remote URL, up to 200 characters in length, that identifies the exec file that will be executed after the user successfully logs in

member

Syntax	member <i>user-profile-name</i> [<i>user-profile-name...</i>] no member <i>user-profile-name</i>
Context	config>system>security>user <i>user-name</i> >console
Description	This command allows the user access to a profile. A user can participate in up to eight profiles. The no form of this command deletes access user access to a profile.
Default	default
Parameters	<i>user-profile-name</i> — the user profile name

new-password-at-login

Syntax	[no] new-password-at-login
Context	config>system>security>user <i>user-name</i> >console
Description	This command forces the user to change passwords at the next console or FTP login. If the user is limited to FTP access, the administrator must create the new password. The no form of the command does not force the user to change passwords.
Default	no new-password-at-login

User Management SNMP Commands

snmp

Syntax	snmp
Context	config>system>security>user <i>user-name</i>
Description	This command creates the context to configure SNMP group membership for a specific user and defines encryption and authentication parameters. All SNMPv3 users must be configured with the commands available in this CLI context. The 7705 SAR always uses the configured SNMPv3 user name as the security user name.

authentication

Syntax	authentication {[none] [[hash] {md5 <i>key-1</i> sha <i>key-1</i> } privacy {none des-key <i>key-2</i> }]}
Context	config>system>security>user <i>user-name</i> >snmp
Description	<p>This command configures the authentication and encryption method the user must use in order to be validated by the 7705 SAR. SNMP authentication allows the device to validate the managing node that issued the SNMP message and determine if the message has been tampered with. The authentication protocol can either be HMAC-MD5-96 or HMAC-SHA-96.</p> <p>The user password is encrypted first by the MD5/SHA/DES algorithm. The output of the algorithm is always a fixed-length string (key). Copy the password key and paste the output in the appropriate authentication command <i>key</i> parameter.</p>
Default	authentication none - No authentication is configured and privacy cannot be configured.
Parameters	<p>none — do not use authentication. If none is specified, then privacy cannot be configured.</p> <p>hash — when hash is not specified, unencrypted characters can be entered. When hash is configured, all specified keys are stored in an encrypted format in the configuration file. The password must be entered in encrypted form when the hash parameter is used.</p> <p>md5 <i>key-1</i> — the MD5 authentication key is stored in an encrypted format. The minimum key length is determined by the config>system>security>password>minimum-length value. The maximum length is 16 octets (32 printable characters).</p> <p>The complexity of the key is determined by the complexity command.</p> <p>sha <i>key-1</i> — the sha authentication key is stored in an encrypted format. The minimum key length is determined by the config>system>security>password>minimum-length value. The maximum length is 20 octets (40 printable characters).</p> <p>The complexity of the key is determined by the complexity command.</p> <p>privacy none — do not perform SNMP packet encryption</p> <p>privacy des-key <i>key-2</i> — configure the des-key for SNMP packet encryption. This key is stored in an encrypted format . The minimum key length is determined by the config>system>security>password>minimum-length value. The maximum length is 16 octets (32 printable characters). If privacy is configured, then authentication must be enabled.</p> <p>To remove a previously configured des-key, enter privacy none.</p> <p>The complexity of the key is determined by the complexity command.</p> <p>Default privacy none</p>

group

Syntax	group <i>group-name</i> no group
Context	config>system>security>user <i>user-name</i> >snmp
Description	This command associates (or links) a user to a group name. The access command links the group with one or more views, security model(s), security level(s), and read, write, and notify permissions.
Default	No group name is associated with a user.
Parameters	<i>group-name</i> — enter the group name (between 1 and 32 alphanumeric characters) that is associated with this user. A user can be associated with one group name per security model.

RADIUS Client Commands

radius

Syntax	[no] radius
Context	config>system>security
Description	<p>This command creates the context to configure RADIUS authentication on the 7705 SAR.</p> <p>Implement redundancy by configuring multiple server addresses for each 7705 SAR.</p> <p>The no form of the command removes the RADIUS configuration.</p>

access-algorithm

Syntax	access-algorithm {direct round-robin} [no] access-algorithm
Context	config>system>security>radius
Description	<p>This command configures the algorithm used to access the set of RADIUS servers. Up to five servers can be configured.</p> <p>In direct mode, the first server, as defined by the server command, is the primary server. This server is always used first when authenticating a request. In round-robin mode, the server used to authenticate a request is the next server in the list, following the last authentication request. For example, if server 1 is used to authenticate the first request, server 2 is used to authenticate the second request, and so on.</p>
Default	direct
Parameters	<p>direct — first server is always used to authenticate a request</p> <p>round-robin — server used to authenticate a request is the next server in the list, following the last authentication request</p>

accounting

Syntax	[no] accounting
Context	config>system>security>radius
Description	<p>This command enables RADIUS accounting. The no form of this command disables RADIUS accounting.</p>
Default	no accounting

accounting-port

Syntax	accounting-port <i>port</i> no accounting-port
Context	config>system>security>radius
Description	This command specifies a UDP port number on which to contact the RADIUS server for accounting requests.
Parameters	<i>port</i> — specifies the UDP port number
Values	1 to 65535
Default	1813

authorization

Syntax	[no] authorization
Context	config>system>security>radius
Description	This command configures RADIUS authorization parameters for the system. The no form of this command disables RADIUS authorization for the system.
Default	no authorization

port

Syntax	port <i>port</i> no port
Context	config>system>security>radius
Description	This command configures the TCP port number to contact the RADIUS server. The no form of the command reverts to the default value.
Default	1812 (as specified in RFC 2865, <i>Remote Authentication Dial In User Service (RADIUS)</i>)
Parameters	<i>port</i> — the TCP port number to contact the RADIUS server
Values	1 to 65535

retry

Syntax	retry <i>count</i> no retry
Context	config>system>security>radius
Description	This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server. The no form of the command reverts to the default value.
Default	3
Parameters	<i>count</i> — the retry count Values 1 to 10

server

Syntax	server <i>server-index</i> address <i>ip-address</i> secret <i>key</i> [hash hash2] no server <i>server-index</i>
Context	config>system>security>radius
Description	This command adds a RADIUS server and configures the RADIUS server IP address, index, and key values. Up to five RADIUS servers can be configured at any one time. RADIUS servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher-indexed server is only queried if no response is received from a lower-indexed server (which implies that the server is not available). If a response from a server is received, no other RADIUS servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data. The no form of the command removes the server from the configuration.
Default	No RADIUS servers are configured.
Parameters	<i>index</i> — the index for the RADIUS server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from lowest to highest index. Values 1 to 5 address <i>ip-address</i> — the IP address of the RADIUS server. Two RADIUS servers cannot have the same IP address. An error message is generated if the server address is a duplicate. Values ipv4-address a.b.c.d (host bits must be 0) secret <i>key</i> — the secret key to access the RADIUS server. This secret key must match the password on the RADIUS server. Values Up to 20 characters in length

hash — specifies that the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — specifies that the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

timeout

Syntax	timeout <i>seconds</i> no timeout
Context	config>system>security>radius
Description	This command configures the number of seconds the router waits for a response from a RADIUS server. The no form of the command reverts to the default value.
Default	3
Parameters	<i>seconds</i> — the number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer Values 1 to 90

use-default-template

Syntax	[no] use-default-template
Context	config>system>security>radius
Description	This command specifies whether or not the user template defined by this entry is to be actively applied to the RADIUS user.
Default	no use-default-template

TACACS+ Client Commands

tacplus

Syntax	[no] tacplus
Context	config>system>security
Description	<p>This command creates the context to configure TACACS+ authentication on the 7705 SAR.</p> <p>Configure multiple server addresses for each 7705 SAR for redundancy.</p> <p>The no form of the command removes the TACACS+ configuration.</p>

accounting

Syntax	accounting [record-type {start-stop stop-only}] no accounting
Context	config>system>security>tacplus
Description	<p>This command enables TACACS+ accounting and configures the type of accounting record packet that is to be sent to the TACACS+ server. The record-type parameter indicates whether TACACS+ accounting start and stop packets will be sent or just stop packets will be sent.</p>
Default	record-type stop-only
Parameters	<p>record-type start-stop — specifies that a TACACS+ start packet is sent whenever the user executes a command and a stop packet is sent when the command is complete</p> <p>record-type stop-only — specifies that a stop packet is sent when the command execution is complete</p>

authorization

Syntax	[no] authorization
Context	config>system>security>tacplus
Description	<p>This command configures TACACS+ authorization parameters for the system.</p>
Default	no authorization

server

Syntax	server <i>index</i> address <i>ip-address</i> secret <i>key</i> [hash hash2] no server <i>index</i>
Context	config>system>security>tacplus
Description	<p>This command adds a TACACS+ server and configures the TACACS+ server IP address, index, and key values.</p> <p>Up to five TACACS+ servers can be configured at any one time. TACACS+ servers are accessed in order from the lowest index to the highest index for authentication requests.</p> <p>The no form of the command removes the server from the configuration.</p>
Default	No TACACS+ servers are configured.
Parameters	<p><i>index</i> — the index for the TACACS+ server. The index determines the sequence in which the servers are queried for authentication requests. Servers are queried in order from the lowest index to the highest index.</p> <p>Values 1 to 5</p> <p>address <i>ip-address</i> — the IP address of the TACACS+ server. Two TACACS+ servers cannot have the same IP address. An error message is generated if the server address is a duplicate.</p> <p>Values ipv4-address a.b.c.d (host bits must be 0)</p> <p>secret <i>key</i> — the secret key to access the RADIUS server. This secret key must match the password on the TACACS+ server.</p> <p>Values Up to 20 characters in length</p> <p>hash — specifies that the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.</p> <p>hash2 — specifies that the key is entered in a more complex encrypted form. If the hash2 parameter is not used, the less encrypted hash form is assumed.</p>

single-connection

Syntax	[no] single-connection
Context	config>system>security>tacplus
Description	<p>This command sets up a single connection to the TACACS+ server and validates everything via that connection. Normally, each authentication event sets up a connection to validate that particular event.</p> <p>The no form of the command disables TACACS+ single connection configuration.</p>
Default	no single-connection

timeout

Syntax	timeout <i>seconds</i> no timeout
Context	config>system>security>tacplus
Description	<p>This command configures the number of seconds the router waits for a response from a TACACS+ server.</p> <p>The no form of the command reverts to the default value.</p>
Default	3
Parameters	<i>seconds</i> — the number of seconds the router waits for a response from a TACACS+ server, expressed as a decimal integer
Values	1 to 90

use-default-template

Syntax	[no] use-default-template
Context	config>system>security>tacplus
Description	This command specifies whether or not the user template defined by this entry is to be actively applied to the TACACS+ user.

802.1x Commands

dot1x

Syntax	[no] dot1x
Context	config>system>security
Description	This command creates the context to configure 802.1x network access control on the 7705 SAR. The no form of the command removes the 802.1x configuration.

radius-plcy

Syntax	[no] radius-plcy <i>name</i> [create]
Context	config>system>security>dot1x
Description	This command creates the context to configure RADIUS server parameters for 802.1x network access control on the 7705 SAR. The RADIUS server configured under the config>system>security>dot1x>radius-plcy context authenticates clients who get access to the data plane of the 7705 SAR. This configuration differs to the RADIUS server configured under the config>system>security>radius context that authenticates CLI login users who get access to the management plane of the 7705 SAR. The no form of the command removes the RADIUS server configuration for 802.1x. <i>name</i> — the RADIUS policy name, up to 32 characters create — keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the create keyword.

retry

Syntax	retry <i>count</i> no retry
Context	config>system>security>dot1x
Description	This command configures the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server. The no form of the command reverts to the default value.
Default	3

Parameters *count* — the retry count
Values 1 to 10

server

Syntax **server** *server-index* **address** *ip-address* **secret** *key* [**hash** | **hash2**] [**auth-port** *auth-port*]
 [**acct-port** *acct-port*] [**type** *server-type*]
no server *server-index*

Context config>system>security>dot1x>radius-plcy

Description This command adds an 802.1x server and configures the IP address, index, and key values.

Up to five 802.1x servers can be configured at any one time. These servers are accessed in order from lowest to highest index for authentication requests until a response from a server is received. A higher indexed server is only queried if no response is received from a lower indexed server (which implies that the server is not available). If a response from a server is received, no other 802.1x servers are queried. It is assumed that there are multiple identical servers configured as backups and that the servers do not have redundant data.

The **no** form of the command removes the server from the configuration.

Default n/a

Parameters *server-index* — the index for the 802.1x server
Values 1 to 5

ip-address — the IP address of the 802.1x server. Each 802.1x server must have a unique IP address. An error message is generated if the server address is a duplicate.

Values a.b.c.d

key — the secret key to access the 802.1x server. This secret key must match the password on the 802.1x server.

Values up to 20 alphanumeric characters

hash — specifies that the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.

hash2 — specifies that the key is entered in a more complex encrypted form that involves more variables than the key value alone. This means that the hash2 encrypted variable cannot be copied and pasted. If the hash or hash2 parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.

auth-port — the UDP port number used to contact the RADIUS server for authentication

Values 1 to 65535

acct-port — the UDP port number used to contact the RADIUS server for accounting requests

Values 1 to 65535

server-type — the server type

Values authorization, accounting, or combined

source-address

Syntax	source-address <i>ip-address</i> no source-address
Context	config>system>security>dot1x>radius-plcy
Description	This command configures the NAS IP address to be sent in the RADIUS packet. The no form of the command reverts to the default value.
Default	system IP address
Parameters	<i>ip-address</i> — the source address of the RADIUS packet in dotted-decimal notation Values 0.0.0.0 to 255.255.255.255

shutdown

Syntax	[no] shutdown
Context	config>system>security>dot1x config>system>security>dot1x>radius-plcy
Description	This command administratively disables the 802.1x protocol operation. Shutting down the protocol does not remove or change the configuration other than the administrative state. The operational state of the entity is disabled as well as the operational state of any entities contained within. The no form of the command administratively enables the protocol.
Default	shutdown

timeout

Syntax	timeout <i>seconds</i> no timeout
Context	config>system>security>dot1x>radius-plcy
Description	<p>This command configures the number of seconds the router waits for a response from a RADIUS server.</p> <p>The no form of the command reverts to the default value.</p>
Default	5
Parameters	<p><i>seconds</i> — the number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer</p> <p>Values 1 to 90</p>

SSH Commands

ssh

Syntax	ssh
Context	config>system>security
Description	<p>This command enables the context to configure the SSH server on the system. This command should only be enabled or disabled no SSH session is running.</p> <p>When the command is executed, an SSH security key is generated. This key is valid until either the node is restarted or the SSH server is stopped with the no ssh command and restarted. The key size is non-configurable and set at 1024 bits.</p> <p>Quitting SSH while in the process of authentication is accomplished by either executing a ctrl-c or "~." (tilde and dot), assuming the "~" is the default escape character for the SSH session.</p>
Default	ssh — The SSH server is enabled.

preserve-key

Syntax	[no] preserve-key
Context	config>system>security>ssh
Description	<p>This command specifies the persistence of the SSH server host key. When enabled, the host key will be saved by the server and restored following a system reboot. This command can only be enabled or disabled when no SSH session is running.</p> <p>The no form of the command specifies that the host key will be held in memory by the SSH server and not be restored following a system reboot.</p>
Default	no preserve-key

server-shutdown

Syntax	[no] server-shutdown
Context	config>system>security>ssh
Description	This command enables the SSH servers running on the system.
Default	At system startup, only the SSH server is enabled.

version

Syntax	version <i>ssh-version</i> no version
Context	config>system>security>ssh
Description	This command specifies the SSH protocol version that will be supported by the SSH server. The server may be configured as Secure Shell Version 1 (SSH1), Version 2 (SSH2) or both. SSH1 and SSH2 are different protocols and encrypt at different parts of the packets. SSH1 uses the server as well as host keys to authenticate systems, whereas SSH2 only uses host keys. SSH2 does not use the same networking implementation that SSH1 does and is considered a more secure, efficient, and portable version of SSH that includes Secure FTP (SFTP).
Parameters	<i>ssh-version</i> — specifies the SSH version
Values	1 — specifies that the SSH server will only accept connections from clients supporting SSH protocol version 1 2 — specifies that the SSH server will only accept connections from clients supporting SSH protocol version 2 1-2 — specifies that the SSH server will accept connections from clients supporting either SSH protocol version 1, or SSH protocol version 2, or both
Default	2

Login Control Commands

login-control

Syntax	login-control
Context	config>system
Description	This command creates the context to configure the session control for console, Telnet and FTP.

exponential-backoff

Syntax	[no] exponential-backoff
Context	config>system>login-control
Description	<p>This command enables the exponential-backoff of the login prompt. The exponential-backoff command is used to deter dictionary attacks, when a malicious user can gain access to the CLI by using a script to try admin with any conceivable password.</p> <p>The no form of the command disables exponential-backoff.</p>
Default	no exponential-backoff

idle-timeout

Syntax	idle-timeout {minutes disable} no idle-timeout
Context	config>system>login-control
Description	<p>This command configures the idle timeout for FTP, console, or Telnet sessions before the session is terminated by the system.</p> <p>By default, an idle FTP, console, or Telnet session times out after 30 minutes of inactivity. This timer can be set per session.</p> <p>The no form of the command reverts to the default value.</p>
Default	30
Parameters	<p><i>minutes</i> — the idle timeout in minutes. Allowed values are 1 to 1440.</p> <p>Values 1 to 1440</p> <p>disable — when the disable option is specified, a session will never time out. To re-enable idle timeout, enter the command without the disable option.</p>

login-banner

Syntax	[no] login-banner
Context	config>system>login-control
Description	<p>This command enables or disables the display of a login banner. The login banner contains the 7705 SAR copyright and build date information for a console login attempt.</p> <p>The no form of the command causes only the configured pre-login-message and a generic login prompt to display.</p>

motd

Syntax	motd {url url-prefix:source-url text motd-text-string} no motd
Context	config>system>login-control
Description	<p>This command creates the message of the day that is displayed after a successful console login.</p> <p>Only one message can be configured.</p> <p>The no form of the command removes the message.</p>
Default	no motd
Parameters	<p>url url-prefix: source-url — when the message of the day is present as a text file, provide both url-prefix and the source-url of the file containing the message of the day. The URL prefix can be local or remote.</p> <p>text motd-text-string — the text of the message of the day. The <i>motd-text-string</i> must be enclosed in double quotes. Multiple text strings are not appended to one another.</p> <p>Some special characters can be used to format the message text. The “\n” character creates multi-line MOTDs and the “\r” character restarts at the beginning of the new line. For example, entering “\n\r” will start the string at the beginning of the new line, while entering “\n” will start the second line below the last character from the first line.</p>

pre-login-message

Syntax	pre-login-message <i>login-text-string</i> [name] no pre-login-message
Context	config>system>login-control
Description	<p>This command creates a message displayed prior to console login attempts on the console via Telnet.</p> <p>Only one message can be configured. If multiple pre-login-messages are configured, the last message entered overwrites the previous entry.</p> <p>The system name can be added to an existing message without affecting the current pre-login-message.</p> <p>The no form of the command removes the message.</p>
Default	no pre-login-message
Parameters	<p><i>login-text-string</i> — a text string, up to 900 characters. Any printable, 7-bit ASCII characters can be used. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.</p> <p>name — when the keyword name is defined, the configured system name is always displayed first in the login message. To remove the name from the login message, the message must be cleared and a new message entered without the name.</p>

FTP Login Control Commands

ftp

Syntax	ftp
Context	config>system>login-control
Description	This command creates the context to configure FTP login control parameters.

inbound-max-sessions

Syntax	inbound-max-sessions <i>value</i> no inbound-max-sessions
Context	config>system>login-control>ftp
Description	<p>This command configures the maximum number of concurrent inbound FTP sessions.</p> <p>This value is the combined total of inbound and outbound sessions.</p> <p>The no form of the command reverts to the default value.</p>

Default 3

Parameters *value* — the maximum number of concurrent FTP sessions on the node

Values 0 to 5

Telnet Login Control Commands

telnet

Syntax telnet

Context config>system>login-control

Description This command creates the context to configure the Telnet login control parameters.

inbound-max-sessions

Syntax inbound-max-sessions *value*
no inbound-max-sessions

Context config>system>login-control>telnet

Description This parameter limits the number of inbound Telnet sessions. Each 7705 SAR router is limited to a total of 15 Telnet or SSH sessions.

The value controls inbound Telnet sessions only. Console sessions through the local serial (console) port cannot be disabled.

The **no** form of the command reverts to the default value.

Default 5

Parameters *value* — the maximum number of concurrent inbound Telnet sessions, expressed as an integer

Values 0 to 15

outbound-max-sessions

Syntax	outbound-max-sessions <i>value</i> no outbound-max-sessions
Context	config>system>login-control>telnet
Description	<p>This parameter limits the number of outbound Telnet sessions. Each 7705 SAR router is limited to a total of 15 Telnet or SSH sessions.</p> <p>The value controls Telnet outbound sessions only. The local serial port cannot be disabled.</p> <p>The no form of the command reverts to the default value.</p>
Default	5
Parameters	<i>value</i> — the maximum number of concurrent outbound Telnet sessions, expressed as an integer
	Values 0 to 15

Show Commands

- [Security Show Commands on page 159](#)
- [Login Control Show Commands on page 178](#)

Security Show Commands

access-group

Syntax	access-group [<i>group-name</i>]
Context	show>system>security
Description	This command displays SNMP access group information.
Parameters	<i>group-name</i> — displays information for the specified access group
Output	The following output is an examples of system security access group information, and Table 8 describes the fields.

Sample Output

```
A:ALU-4# show system security access-group
=====
Access Groups
=====
group name      security  security  read      write      notify
                model    level    view      view      view
-----
snmp-ro         snmpv1   none     no-security
snmp-ro         snmpv2c  none     no-security
snmp-rw         snmpv1   none     no-security  no-security
snmp-rw         snmpv2c  none     no-security  no-security
snmp-rwa        snmpv1   none     iso          iso         iso
snmp-rwa        snmpv2c  none     iso          iso         iso
snmp-trap       snmpv1   none
snmp-trap       snmpv2c  none
=====
A:ALU-7#
```

Table 8: Show System Security Access Group Output Fields

Label	Description
Group name	The access group name
Security model	The security model required to access the views configured in this node
Security level	Specifies the required authentication and privacy levels to access the views configured in this node
Read view	Specifies the variable of the view to read the MIB objects
Write view	Specifies the variable of the view to configure the contents of the agent
Notify view	Specifies the variable of the view to send a trap about MIB objects

authentication

Syntax	authentication [statistics]
Context	show>system>security
Description	This command displays system login authentication configuration and statistics.
Parameters	statistics — appends login and accounting statistics to the display
Output	The following output is an examples of system security authentication information, and Table 9 describes the fields.

Sample Output

```

A:ALU-4# show system security authentication
=====
Authentication                      sequence : radius tacplus local
=====
type      server address      status  timeout  single  retry
          (secs)              conn     count
-----
radius
  10.10.10.103                up      5        n/a     5
radius
  10.10.0.1                   up      5        n/a     5
radius
  10.10.0.2                   up      5        n/a     5
tacplus
  10.10.0.9(49)               down    5        true    n/a
-----
radius admin status   : up
tacplus admin status  : down
health check          : enabled (interval 30)
-----
No. of Servers: 4
=====
A:ALU-4#

```



```

A:ALU-7>show>system>security# authentication statistics
=====
Authentication                               sequence : radius tacplus local
=====
type      status  timeout  single  retry
server address      (secs)   conn    count
-----
radius
  10.10.10.103      up       5       n/a     5
radius
  10.10.0.1         up       5       n/a     5
radius
  10.10.0.2         up       5       n/a     5
tacplus
  10.10.0.9(49)     down     5       true    n/a
-----
radius admin status : up
tacplus admin status : down
health check       : enabled (interval 30)
-----
No. of Servers: 4
=====
Login Statistics
=====
server address      conn  accepted  rejected
                    errors logins   logins
-----
10.10.10.103       0      0          0
10.10.0.1          0      0          0
10.10.0.2          0      0          0
10.10.0.9          0      0          0
local              n/a     1          0
=====
Authorization Statistics (TACACS+)
=====
server address      conn  sent  rejected
                    errors pkts   pkts
-----
10.10.0.9           0      0      0
=====
Accounting Statistics
=====
server address      conn  sent  rejected
                    errors pkts   pkts
-----
10.10.10.103       0      0      0
10.10.0.1          0      0      0
10.10.0.2          0      0      0
=====
A:ALU-7#

```

Table 9: Show System Security Authentication Output Fields

Label	Description
Sequence	The sequence in which authentication is processed
Server address	The IP address of the RADIUS server
Status	The current status of the RADIUS server
Type	The authentication type
Timeout (secs)	The number of seconds the router waits for a response from a RADIUS server
Single connection	Enabled — Specifies a single connection to the TACACS+ server and validates everything via that connection
	Disabled — The TACACS+ protocol operation is disabled
Retry count	Displays the number of times the router attempts to contact the RADIUS server for authentication if there are problems communicating with the server
Connection errors	The number of times a user has attempted to log in irrespective of whether the login succeeded or failed
Accepted logins	The number of times the user has successfully logged in
Rejected logins	The number of unsuccessful login attempts
Sent packets	The number of packets sent
Rejected packets	The number of packets rejected

communities

Syntax	communities
Context	show>system>security
Description	This command displays SNMP communities and characteristics.
Output	The following output is an examples of community information, and Table 10 describes the fields.

Sample Output

```

A:ALU-48# show system security communities
=====
Communities
=====
community          access  view          version  group name
-----
cli-readonly        r       iso           v2c      cli-readonly
cli-readwrite       rw      iso           v2c      cli-readwrite
public              r       no-security   v1 v2c   snmp-ro
-----
No. of Communities: 3
=====
A:ALU-48#

```

Table 10: Show Communities Output Fields

Label	Description
Community	The community string name for SNMPv1 and SNMPv2c access only
Access	r — The community string allows read-only access
	rw — The community string allows read-write access
	rwa — The community string allows read-write access
	mgmt — The unique SNMP community string assigned to the management router
View	The view name
Version	The SNMP version
Group Name	The access group name
No of Communities	The total number of configured community strings

cpm-filter

Syntax	cpm-filter ip-filter [entry <i>entry-id</i>] cpm-filter ipv6-filter [entry <i>entry-id</i>]				
Context	show>system>security				
Description	This command displays information on CPM (CSM) filters. If an entry number is not specified, all entries are displayed.				
Parameters	<i>entry-id</i> — displays information about the specified CPM filter entry <table> <tr> <td>Default</td><td>All filter entries</td></tr> <tr> <td>Values</td><td>1 to 9999</td></tr> </table>	Default	All filter entries	Values	1 to 9999
Default	All filter entries				
Values	1 to 9999				
Output	The following output is an examples of CPM filter information, and Table 11 describes the fields.				

Sample Output

```
A:ALU-35# show system security cpm-filter ip-filter
=====
CPM IP Filters
=====
Entry-Id  Dropped   Forwarded Description
-----
2          0          0          CPM filter #2
3        25880          0          CPM filter #3
4        25880          0          CPM filter #4
5        25882          0          CPM filter #5
6        25926          0          CPM filter #6
7        25926          0          CPM filter #7
8        25944          0          CPM filter #8
9        25950          0          CPM filter #9
10       25968          0          CPM filter #10
11       25984          0          CPM filter #11
12       26000          0          CPM filter #12
13       26018          0          CPM filter #13
14       26034          0          CPM filter #14
15       26050          0          CPM filter #15
=====
A:ALU-35#

A:ALU-35# show system security cpm-filter ip-filter entry 2
=====
CPM IP Filter Entry
=====
Entry Id      : 2
Description   : CPM filter #2
-----
Filter Entry Match Criteria :
-----
Log Id        : 101
Src. IP       : 10.4.101.2/32      Src. Port     : 0
Dest. IP      : 10.4.101.1/32     Dest. Port    : 0
Protocol      : tcp               Dscp          : ef
```

```

ICMP Type      : Undefined      ICMP Code       : Undefined
Fragment       : True           Option-present  : Off
IP-Option      : n/a           Multiple Option : True
TCP-syn        : Off           TCP-ack         : True
Match action   : Drop
Dropped pkts   : 0             Forwarded pkts   : 0
=====
A:ALU-35#

A:ALU-35# show system security cpm-filter ipv6-filter entry 101
=====
CPM IPv6 Filter Entry
=====
Entry Id : 1
Description : CPM-Filter 11::101:2 #101
-----
Filter Entry Match Criteria :
-----
Log Id : n/a
Src. IP : 11::101:2      Src. Port : 0
Dest. IP : 11::101:1     Dest. Port : 0
next-header : none Dscp : Undefined
ICMP Type : Undefined    ICMP Code : Undefined
TCP-syn : Off            TCP-ack : Off
Match action : Drop
Dropped pkts : 25880      Forwarded pkts : 0
=====

```

Table 11: Show CPM Filter Output Fields

Label	Description
CPM IP (or IPv6) Filter Entry	
Entry-id	Displays information about the specified CPM filter entry
Dropped	The number of dropped events
Forwarded	The number of forwarded events
Description	The CPM filter description
Filter Entry Match Criteria	
Log Id	The log ID where matched packets will be logged
Src. IP	The source IP address
Dest. IP	The destination IP address
Protocol	The Protocol field in the IP header (IPv4 filters only)
next-header	The next header ID. Undefined indicates no next header is specified. (IPv6 filters only)
ICMP Type	The ICMP type field in the ICMP header

Table 11: Show CPM Filter Output Fields (Continued)

Label	Description
Fragment	The 3-bit fragment flags or 13-bit fragment offset field (IPv4 filters only)
IP-Option	The IP option setting (IPv4 filters only)
TCP-syn	The SYN flag in the TCP header
Match action	When the criteria matches, displays drop or forward packet
Dropped pkts	The number of matched dropped packets
Src. Port	The source port number (range)
Dest. Port	The destination port number (range)
Dscp	The DSCP field in the IP header
ICMP Code	The ICMP code field in the ICMP header
Option-present	The option present setting (IPv4 filters only)
Multiple Option	The multiple option setting (IPv4 filters only)
TCP-ack	The ACK flag in the TCP header
Match action	When the criteria matches, displays drop or forward packet
Next Hop	If match action is forward, indicates destination of the matched packet
Forwarded pkts	Indicates number of matched forwarded packets

management-access-filter

Syntax	management-access-filter ip-filter [entry <i>entry-id</i>] management-access-filter ipv6-filter [entry <i>entry-id</i>]
Context	show>system>security
Description	This command displays management access control filter information. If no specific entry number is specified, all entries are displayed.
Parameters	<i>entry-id</i> — displays information about the specified management access filter entry <div> Default All filter entries </div> <div> Values 1 to 9999 </div>
Output	The following output is an examples of management access filter information, and Table 12 describes the fields.

Sample Output

```

A:ALU-7# show system security management-access-filter ip-filter entry 1
=====
IPv4 Management Access Filters
=====

filter type:      : ip
Def. Action       : permit
Admin Status      : enabled (no shutdown)
-----

Entry             : 1
Description        : test description
Src IP             : 10.10.10.104
Src interface      : undefined
Dest port          : 10.10.10.103
Protocol           : 6
Router             : undefined
Action             : permit
Log                : disabled
Matches            : 0
=====

A:ALU-7#

A:ALU-7# show system security management-access-filter ipv6-filter entry 2
=====
IPv6 Management Access Filter
=====

filter type       : ipv6
Def. Action        : permit
Admin Status       : enabled (no shutdown)
-----

Entry             : 1
Src IP             : 2001::1/128
Flow label         : undefined
Src interface      : undefined
Dest port          : undefined
Next-header        : undefined
Router             : undefined
Action             : permit
Log                : enabled
Matches            : 0
=====

A:ALU-7#

```

Table 12: Show Management Access Filter Output Fields

Label	Description
IPv4 (or IPv6) Management Access Filters	
filter type	The management access filter type
Def. Action	Permit — Specifies that packets not matching the configured selection criteria in any of the filter entries are permitted
	Deny — Specifies that packets not matching the configured selection criteria in any of the filter entries are denied and that a ICMP host unreachable message will be issued
	Deny-host-unreachable — Specifies that packets not matching the configured selection criteria in the filter entries are denied
Admin Status	Up — indicates that the management access filter is administratively enabled
	Down — indicates that the management access filter is administratively disabled
Entry	The entry ID in a policy or filter table
Description	A text string describing the filter
Src IP	The source IP address used for management access filter match criteria
Flow label	The flow label to match (IPv6 filters only)
Src interface	The interface name for the next hop to which the packet should be forwarded if it hits this filter entry
Dest port	The destination port
Protocol	The IP protocol to match (IPv4 filters only)
Next-header	The next header ID to match. Undefined indicates no next header is specified. (IPv6 filters only)
Action	The action to take for packets that match this filter entry
Matches	The number of times a management packet has matched this filter entry

password-options

Syntax	password-options
Context	show>system>security
Description	This command displays configured password options.
Output	The following output is an examples of password options information, and Table 13 describes the fields.

Sample Output

```

A:ALU-7# show system security password-options
=====
Password Options
=====
Password aging in days                : none
Number of invalid attempts permitted per login : 3
Time in minutes per login attempt      : 5
Lockout period (when threshold breached) : 10
Authentication order                  : radius tacplus local
Configured complexity options         :
Minimum password length                : 6
=====
A:ALU-7#

```

Table 13: Show Password Options Output Fields

Label	Description
Password aging in days	The number of days a user password is valid before the user must change their password
Number of invalid attempts permitted per login	The number of unsuccessful login attempts allowed for the specified time
Time in minutes per login attempt	The period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out
Lockout period (when threshold breached)	The lockout period, in minutes, where the user is not allowed to log in
Authentication order	The sequence in which password authentication is attempted among RADIUS, TACACS+, and local passwords

Table 13: Show Password Options Output Fields (Continued)

Label	Description
Configured complexity options	The complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96 and DES-keys configured in the authentication section
Minimum password length	The minimum number of characters required for locally administered passwords, HMAC-MD5-96, HMAC-SHA-96, and DES-keys configured in the system security section

profile

- Syntax** `profile user-profile-name`
- Context** `show>system>security`
- Description** This command displays user profile information.
- If the *profile-name* is not specified, then information for all profiles is displayed.
- Parameters** *profile-name* — displays information for the specified user profile
- Output** The following output is an examples of user profile information, and [Table 14](#) describes the fields.

Sample Output

```
A:ALU-7# show system security profile administrative
=====
User Profile
=====
User Profile : administrative
Def. Action  : permit-all
LI           : no
-----
Entry        : 10
Description   :
Match Command: configure system security
Action       : permit
-----
Entry        : 20
Description   :
Match Command: show system security
Action       : permit
-----
No. of profiles: 1
=====
A:ALU-7#
```

Table 14: Show User Profile Output Fields

Label	Description
User Profile	The profile name used to deny or permit user console access to a hierarchical branch or to specific commands
Def. action	Permit all — Permits access to all commands
	Deny — Denies access to all commands
	None — No action is taken
Entry	The entry ID in a policy or filter table
Description	Displays the text string describing the entry
Match Command	Displays the command or subtree commands in subordinate command levels
Action	Permit all — Commands matching the entry command match criteria are permitted
	Deny — Commands not matching the entry command match criteria are not permitted
No. of profiles	The total number of profiles listed

source-address

Syntax **source-address**

Context show>system>security

Description This command displays the source address configured for applications.

Output The following output is an examples of source address information, and [Table 15](#) describes the fields.

Sample Output

```
A:ALU-1# show system security source-address
=====
Source-Address applications
=====
Application          IP address/Interface Name          Oper status
-----
telnet                10.20.1.7                          Up
radius                loopback1                          Up
=====
A:ALU-1#
```

Table 15: Show Source Address Output Fields

Label	Description
Application	The source-address application
IP address Interface Name	The source address IP address or interface name
Oper status	Up — The source address is operationally up
	Down — The source address is operationally down

ssh

Syntax ssh**Context** show>system>security**Description** This command displays all the SSH sessions as well as the SSH status and fingerprint.**Output** The following output is an examples of SSH information, and [Table 16](#) describes the fields.**Sample Output**

```

ALU-7# show system security ssh
SSH is enabled
SSH preserve key: Enabled
SSH protocol version 1: Enabled
RSA host key finger print:c6:a9:57:cb:ee:ec:df:33:1a:cd:d2:ef:3f:b5:46:34

SSH protocol version 2: Enabled
DSA host key finger print:c0:be:4a:da:55:87:e0:92:da:33:b8:55:fb:42:71:58
RSA host key finger print:79:28:68:61:d8:8b:c0:f0:5c:f5:bc:0b:fa:02:24:d8
=====
Connection          Username           Version
=====
192.168.5.218       admin             1-2
-----
Number of SSH sessions : 1
=====
ALU-7#

```

Table 16: Show SSH Output Fields

Label	Description
SSH status	SSH is enabled — Displays that SSH server is enabled SSH is disabled — Displays that SSH server is disabled
SSH Preserve Key	Enabled — Displays that preserve-key is enabled Disabled — Displays that preserve-key is disabled
SSH protocol version 1	Enabled — Displays that SSH1 is enabled Disabled — Displays that SSH1 is disabled
SSH protocol version 2	Enabled — Displays that SSH2 is enabled Disabled — Displays that SSH2 is disabled
Key fingerprint	The key fingerprint is the server's identity. Clients trying to connect to the server verify the server's fingerprint. If the server fingerprint is not known, the client may not continue with the SSH session since the server might be spoofed.
Connection	The IP address of the connected router(s) (remote client)
User name	The name of the user
Version	The SSH version
Number of SSH sessions	The total number of SSH sessions

user

Syntax `user [user-id] [detail]`

Context `show>system>security`

Description This command displays user registration information.

If no command line options are specified, summary information for all users displays.

Parameters *user-id* — displays information for the specified user

Default All users

detail — displays detailed user information to the summary output

Output The following output is an examples of user information, and [Table 17](#) describes the fields.

Sample Output

```
ALU-7# show system security user
```

```
=====
Users
=====
```

user id	New Pwd	User Console	Permissions ftp	snmp	Password Expires	Login Attempts	Failed Logins	Local Conf
admin	n	y	n	n	never	21	0	y
testuser	n	n	n	n	never	0	0	y

```
-----
Number of users: 2
=====
ALU-7#
```

```
ALU-7# show system security user detail
```

```
=====
Users
=====
```

user id	New Pwd	User Console	Permissions ftp	snmp	Password Expires	Login Attempts	Failed Logins	Local Conf
admin	n	y	n	n	never	21	0	y
testuser	n	n	n	n	never	0	0	y

```
-----
Number of users: 2
=====

=====
User Configuration Detail
=====
=====
```

```
user id          : admin
-----
console parameters
-----
new pw required   : no                cannot change pw : no
home directory    : cf3:\
restricted to home : no
login exec file   :
profile           : administrative
-----
snmp parameters
-----
=====
ALU-7#
```

Table 17: Show User Output Fields

Label	Description
User ID	The name of a system user
Need new pwd	Y — The user must change their password at the next login
	N — The user is not forced to change their password at the next login
Cannot change pw	Y — The user has the ability to change the login password
	N — The user does not have the ability to change the login password
User permissions	Console — Y - The user is authorized for console access N- The user is not authorized for console access
	FTP — Y - The user is authorized for FTP access N - The user is not authorized for FTP access
	SNMP — Y - The user is authorized for SNMP access N - The user is not authorized for SNMP access
Password expires	The number of days the user has left before they must change their login password
Attempted logins	The number of times the user has attempted to log in irrespective of whether the login succeeded or failed
Failed logins	The number of unsuccessful login attempts
Local conf	Y — Password authentication is based on the local password database
	N — Password authentication is not based on the local password database
Home directory	Specifies the local home directory for the user for both console and FTP access
Restricted to home	Yes — The user is not allowed to navigate to a directory higher in the directory tree on the home directory device
	No — The user is allowed to navigate to a directory higher in the directory tree on the home directory device
Login exec file	Displays the user's login exec file which executes whenever the user successfully logs in to a console session

view

Syntax	view [<i>view-name</i>] [detail] [capabilities]
Context	show>system>security
Description	This command displays one or all views and permissions in the MIB-OID tree.
Parameters	<p><i>view-name</i> — specifies the name of the view to display. If no view name is specified, the complete list of views displays.</p> <p>detail — displays detailed view information</p>
Output	The following output is an examples of view information, and Table 18 describes the fields.

Sample Output

```
A:ALU-48# show system security view
=====
Views
=====
```

view name	oid tree	mask	permission
iso	1		included
read1	1.1.1.1	11111111	included
writel	2.2.2.2	11111111	included
testview	1	11111111	included
testview	1.3.6.1.2	11111111	excluded
mgmt-view	1.3.6.1.2.1.2		included
mgmt-view	1.3.6.1.2.1.4		included
mgmt-view	1.3.6.1.2.1.5		included
mgmt-view	1.3.6.1.2.1.6		included
mgmt-view	1.3.6.1.2.1.7		included
mgmt-view	1.3.6.1.2.1.31		included
mgmt-view	1.3.6.1.2.1.77		included
mgmt-view	1.3.6.1.4.1.6527.3.1.2.3.7		included
mgmt-view	1.3.6.1.4.1.6527.3.1.2.3.11		included
vprn-view	1.3.6.1.2.1.2		included
vprn-view	1.3.6.1.2.1.4		included
vprn-view	1.3.6.1.2.1.5		included
vprn-view	1.3.6.1.2.1.6		included
vprn-view	1.3.6.1.2.1.7		included
vprn-view	1.3.6.1.2.1.15		included
vprn-view	1.3.6.1.2.1.23		included
vprn-view	1.3.6.1.2.1.31		included
vprn-view	1.3.6.1.2.1.68		included
vprn-view	1.3.6.1.2.1.77		included
vprn-view	1.3.6.1.4.1.6527.3.1.2.3.7		included
vprn-view	1.3.6.1.4.1.6527.3.1.2.3.11		included
vprn-view	1.3.6.1.4.1.6527.3.1.2.20.1		included
no-security	1		included
no-security	1.3.6.1.6.3		excluded
no-security	1.3.6.1.6.3.10.2.1		included
no-security	1.3.6.1.6.3.11.2.1		included
no-security	1.3.6.1.6.3.15.1.1		included
on-security	2	00000000	included

```
-----
```


No. of Views: 33

=====

A:ALU-48#

Table 18: Show View Output Fields

Label	Description
view name	The name of the view. Views control the accessibility of a MIB object within the configured MIB view and subtree
oid tree	The object identifier of the ASN.1 subtree
mask	The bit mask that defines a family of view subtrees
permission	Indicates whether each view is included or excluded
No. of Views	The total number of views

Login Control Show Commands

users

Syntax	users
Context	show
Description	This command displays console user login and connection information.
Output	The following output is an examples of view information, and Table 19 describes the fields.

Sample Output

```
A:ALU-7# show users
=====
User           Type      Login time                Idle time
  From
=====
testuser       Console  21FEB2007 04:58:55        0d 00:00:00  A
  --
-----
Number of users : 1
'A' indicates user is in admin mode
=====
A:ALU-7#
```

Table 19: Show Users Output Fields

Label	Description
User	The user name
Type	The user is authorized for this access type
From	The originating IP address
Login time	The time the user logged in
Idle time	The amount of idle time for a specific login
Number of users	The total number of users logged in

Clear Commands

statistics

Syntax	statistics [interface <i>ip-int-name</i> <i>ip-address</i>]
Context	clear>router>authentication
Description	This command clears authentication statistics.
Parameters	<i>ip-int-name</i> — clears the authentication statistics for the specified interface name. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes <i>ip-address</i> — clears the authentication statistics for the specified IP address

Debug Commands

radius

Syntax	radius [detail] [hex] no radius
Context	debug
Description	This command enables debugging for RADIUS connections. The no form of the command disables the debugging.
Parameters	detail — displays detailed output hex — displays the packet dump in hexadecimal format

In This Chapter

This chapter provides information to configure SNMP. Topics in this chapter include:

- [SNMP Overview on page 182](#)
 - [SNMP Architecture on page 182](#)
 - [Management Information Base on page 183](#)
 - [SNMP Versions on page 183](#)
 - [Management Information Access Control on page 183](#)
 - [User-Based Security Model Community Strings on page 184](#)
 - [Views on page 184](#)
 - [Access Groups on page 185](#)
 - [Users on page 185](#)
- [Which SNMP Version to Use? on page 186](#)
- [Configuration Notes on page 187](#)
- [Configuring SNMP with CLI on page 189](#)
- [SNMP Command Reference on page 197](#)

SNMP Overview

SNMP Architecture

The Service Assurance Manager (SAM) consists of two elements: managers and agents. The manager is the entity through which network management tasks are facilitated. An agent is a software module integrated into the operating system of the managed device that communicates with the network manager. Managed devices, such as bridges, hubs, routers, and network servers can contain managed objects. A managed object can be a configuration attribute, performance statistic, or control action that is directly related to the operation of a device.

Managed devices collect and store management information and use Simple Network Management Protocol (SNMP). SNMP is an application-layer protocol that provides a message format to facilitate communication between SNMP managers and agents. SNMP provides a standard framework to monitor and manage devices in a network from a central location.

An SNMP manager controls and monitors the activities of network hosts that use SNMP. An SNMP manager can obtain (get) a value from an SNMP agent or store (set) a value in the agent. The manager uses definitions in the management information base (MIB) to perform operations on the managed device such as retrieving values from variables or blocks of data, replying to requests, and processing traps.

Between the SNMP agent and the SNMP manager, the following actions can occur:

- The manager can get information from the agent.
- The manager can set the value of a MIB object that is controlled by an agent.
- The agent can send traps to notify the manager of significant events that occur on the managed device (for example, the 7705 SAR router).

SNMP is supported on network hosts using the IPv4 and IPv6 protocols.

Management Information Base

A MIB is a formal specifications document with definitions of management information used to remotely monitor, configure, and control a managed device or network system. The agent's management information consists of a set of network objects that can be managed with SNMP. Object identifiers are unique object names that are organized in a hierarchical tree structure. The main branches are defined by the Internet Engineering Task Force (IETF). When requested, the Internet Assigned Numbers Authority (IANA) assigns a unique branch for use by a private organization or company. The branch assigned to the Alcatel-Lucent 7705 SAR is 1.3.6.1.4.1.6527.

The SNMP agent provides management information to support a collection of IETF specified MIBs and a number of MIBs defined to manage device parameters and network data unique to the 7705 SAR.

SNMP Versions

The agent supports multiple versions of the SNMP protocol.

- SNMP Version 1 (SNMPv1) is the original Internet-standard network management framework.
SNMPv1 provides access control for communities and uses a community string match for authentication.
- SNMPv2c uses a community string match for authentication.
- SNMP Version 3 (SNMPv3) provides access control for users. In SNMPv3, User-based Security Model (USM) defines the user authentication and encryption features. The View Access Control MIB (VACM) defines the user access control features. The SNMP-COMMUNITY-MIB is used to associate SNMPv1/SNMPv2c community strings with SNMPv3 VACM access control.
SNMPv3 uses a user name match for authentication.

Management Information Access Control

By default, the 7705 SAR implementation of SNMP uses SNMPv3. SNMPv3 incorporates security model and security level features. A security model is the authentication type for the group and the security level is the permitted level of security within a security model. The combination of the security level and security model determines which security mechanism handles an SNMP packet.

To implement SNMPv1 and SNMPv2c configurations, several access groups are predefined. These access groups are standard read-only, read-write, and read-write-all access groups and views that can simply be assigned community strings. In order to implement SNMP with security features, security models, security levels, and USM communities must be explicitly configured. Optionally, additional views that specify more specific OIDs (MIB objects in the subtree) can be configured.

Access to the management information in an SNMPv1/SNMPv2c agent is controlled by the inclusion of a community name string in the SNMP request. The community defines the subset of the agent's managed objects that can be accessed by the requester. It also defines what type of access is allowed: read-only or read-write.

The use of community strings provide minimal security and context checking for both agents and managers that receive requests and initiate trap operations. A community string is a text string that acts like a password to permit access to the agent on the 7705 SAR router.

The Alcatel-Lucent implementation of SNMP has defined three levels of community-named access:

- read-only permission — grants only read access to objects in the MIB, except security objects
- read-write permission — grants read and write access to all objects in the MIB, except security objects
- read-write-all permission — grants read and write access to all objects in the MIB, including security objects

User-Based Security Model Community Strings

User-based security model (USM) community strings associate a community string with an SNMPv3 access group and its view. The access granted with a community string is restricted to the scope of the configured group.

Views

Views control the access to a managed object. The total MIB of a 7705 SAR router can be viewed as a hierarchical tree. When a view is created, either the entire tree or a portion of the tree can be specified and made available to a user to manage the objects contained in the subtree. Object identifiers (OIDs) uniquely identify managed objects. A view defines the type of operations allowed, such as read, write, or notify.

OIDs are organized in a hierarchical tree with specific values assigned to different organizations. A view defines a subset of the agent's managed objects controlled by the access rules associated with that view.

Predefined views are available that are particularly useful when configuring SNMPv1 and SNMPv2c.

The Alcatel-Lucent SNMP agent associates SNMPv1 and SNMPv2c community strings with an SNMPv3 view.

Access Groups

Access groups associate a user group and a security model with the views the group can access. An access group is defined by a unique combination of a group name, security model (SNMPv1, SNMPv2c, or SNMPv3), and security level (no-authorization-no privacy, authorization-no-privacy, or privacy).

An access group, is a template that defines a combination of access privileges and views. A group can be associated with one or more network users to control their access privileges and views.

Additional access parameters must be explicitly configured if the preconfigured access groups and views for SNMPv1 and SNMPv2c do not meet your security requirements.

Users

By default, authentication and encryption parameters are not configured. Authentication parameters that a user must use in order to be validated by the 7705 SAR can be modified. SNMP authentication allows the device to validate the managing node that issued the SNMP message and determine if the message has been tampered with.

User access and authentication privileges must be explicitly configured. In a user configuration, a user is associated with an access group, which is a collection of users who have common access privileges and views.

Which SNMP Version to Use?

SNMPv1 and SNMPv2c do not provide security, authentication, or encryption. Without authentication, an unauthorized user could perform SNMP network management functions and eavesdrop on management information as it passes from system to system. Many SNMPv1 and SNMPv2c implementations are restricted read-only access, which, in turn, reduces the effectiveness of a network monitor in which network control applications cannot be supported.

To implement SNMPv3, an authentication and encryption method must be assigned to a user in order to be validated by the 7705 SAR. SNMP authentication allows the router to validate the managing node that issued the SNMP message and determine if the message was tampered with.

Configuration Notes

This section describes SNMP configuration caveats.

- To avoid management systems attempting to manage a partially booted system, SNMP will remain in a shutdown state if the configuration file fails to complete during system startup. While shut down, SNMP gets and sets are not processed. However, notifications are issued if an SNMP trap group has been configured.
In order to enable SNMP, the portions of the configuration that failed to load must be initialized properly. Start SNMP with the `config>system>snmp>no shutdown` command.
- Use caution when changing the SNMP engine ID. If the SNMP engine ID is changed in the `config>system>snmp>engineID engine-id` context, the current configuration must be saved and a reboot must be executed. If the configuration is not saved and the system is not rebooted, the previously configured SNMP communities and logger trap-target notify communities will not be valid for the new engine ID.

Reference Sources

For information on supported IETF drafts and standards as well as standard and proprietary MIBS, refer to [Standards and Protocol Support](#).

Configuring SNMP with CLI

This section provides information about configuring SNMP with CLI.

Topics in this chapter include:

- [SNMP Configuration Overview on page 190](#)
 - [Configuring SNMPv1 and SNMPv2c on page 190](#)
 - [Configuring SNMPv3 on page 190](#)
- [Basic SNMP Security Configuration on page 191](#)
- [Configuring SNMP Components on page 192](#)
 - [Configuring a Community String on page 192](#)
 - [Configuring View Options on page 193](#)
 - [Configuring Access Options on page 194](#)
 - [Configuring USM Community Options on page 195](#)
 - [Configuring Other SNMP Parameters on page 196](#)

SNMP Configuration Overview

This section describes how to configure SNMP components that apply to SNMPv1, SNMPv2c, and SNMPv3 on the 7705 SAR.

- [Configuring SNMPv1 and SNMPv2c](#)
- [Configuring SNMPv3](#)

Configuring SNMPv1 and SNMPv2c

The 7705 SAR router is based on SNMPv3. To use 7705 SAR routers with SNMPv1 and/or SNMPv2c, SNMP community strings must be configured. Three predefined access methods are available when SNMPv1 or SNMPv2c access is required. Each access method (`r`, `rw`, or `rwa`) is associated with an SNMPv3 access group that determines the access privileges and the scope of managed objects available. The `community` command is used to associate a community string with a specific access method and the required SNMP version (SNMPv1 or SNMPv2c). The access methods are:

- read-only — grants read-only access to the entire management structure with the exception of the security area
- read-write — grants read and write access to the entire management structure with the exception of the security area
- read-write-all — grants read and write access to the entire management structure, including security

If the predefined access groups do not meet your access requirements, then additional access groups and views can be configured. The `usm-community` command is used to associate an access group with an SNMPv1 or SNMPv2c community string.

SNMP trap destinations are configured in the `config>log>snmp-trap-group` context.

Configuring SNMPv3

The 7705 SAR implements SNMPv3. If security features other than the default views are required, the following parameters must be configured:

- views
 - access groups
 - SNMP users
-

Basic SNMP Security Configuration

This section provides information to configure SNMP parameters and provides examples of common configuration tasks. The minimal SNMP parameters are:

For SNMPv1 and SNMPv2c:

- Configure community string parameters

For SNMPv3:

- Configure view parameters
- Configure SNMP group
- Configure access parameters
- Configure user with SNMP parameters

The following displays SNMP default views, access groups, and attempts parameters.

```
ALU-1>config>system>security>snmp# info detail
-----
view iso subtree 1
  mask ff type included
exit
view "mgmt-view" subtree 1.3.6.1.2.1.2
  mask ff type excluded
exit
view "mgmt-view" subtree 1.3.6.1.2.1.4
  mask ff type included
exit
view no-security subtree 1.3.6.1.6.3.11.2.1
  mask ff type included
exit
view no-security subtree 1.3.6.1.6.3.15.1.1
  mask ff type included
exit
access group snmp-ro security-model snmpv1 security-level no-auth-no-
privacy read no-security notify no-security
access group snmp-ro security-model snmpv2c security-level no-auth-no-
privacy read no-security notify no-security
access group snmp-rw security-model snmpv1 security-level no-auth-no-
privacy read no-security write no-security notify no-security
access group snmp-rw security-model snmpv2c security-level no-auth-no-
privacy read no-security write no-security notify no-security
access group snmp-rwa security-model snmpv1 security-level no-auth-no-
privacy read iso write iso notify iso
access group snmp-rwa security-model snmpv2c security-level no-auth-
no-privacy read iso write iso notify iso
access group snmp-trap security-model snmpv1 security-level no-auth-
no-privacy notify iso
access group snmp-trap security-model snmpv2c security-level no-auth-
no-privacy notify iso
attempts 20 time 5 lockout 10
```

Configuring SNMP Components

Use the CLI syntax displayed below to configure the following SNMP scenarios:

- [Configuring a Community String](#)
- [Configuring View Options](#)
- [Configuring Access Options](#)
- [Configuring USM Community Options](#)
- [Configuring Other SNMP Parameters](#)

CLI Syntax: `config>system>security>snmp`
`attempts [count] [time minutes1] [lockout minutes2]`
`community community-string [hash | hash2] access-`
`permissions [version SNMP version]`
`usm-community community-string [hash | hash2] group`
`group-name`
`view view-name subtree oid-value`
`mask mask-value [type {included | excluded}]`
`access group group-name security-model security-model`
`security-level security-level [context context-`
`name [prefix-match]] [read view-name-1] [write`
`view-name-2] [notify view-name-3]`

Configuring a Community String

SNMPv1 and SNMPv2c community strings are used to define the relationship between an SNMP manager and agent. The community string acts like a password to permit access to the agent. The access granted with a community string is restricted to the scope of the configured group.

One or more of the following characteristics associated with the string can be specified:

- read-only, read-write, and read-write-all permission for the MIB objects accessible to the community
- the SNMP version, SNMPv1 or SNMPv2c

Default access features are preconfigured by the agent for SNMPv1 and SNMPv2c.

Use the following CLI syntax to configure community options:

CLI Syntax: `config>system>security>snmp`
`community community-string [hash | hash2] access-`
`permissions [version SNMP version]`

The following example displays community string command usage:

Example:

```
config>system>security# snmp
config>system>security>snmp# community private hash2 rwa
version both
config>system>security>snmp# community public hash r
version v2c
```

The following example displays the SNMP community configuration:

```
ALU-1>config>system>security>snmp# info
-----
community "uTdc9j48PBRkxn5DcSjchk" hash2 rwa version both
community "Lla.RtAyRW2" hash2 r version v2c
-----
ALU-1>config>system>security>snmp#
```

Configuring View Options

Use the following CLI syntax to configure view options:

CLI Syntax:

```
config>system>security>snmp
view view-name subtree oid-value
mask mask-value [type {included | excluded}]
```

The following example displays view command usage:

Example:

```
config>system>security>snmp# view testview subtree 1
config>system>security>snmp>view$ mask ff type included
config>system>security>snmp>view$ exit
config>system>security>snmp# view testview subtree
1.3.6.1.2
config>system>security>snmp>view$ mask ff type excluded
config>system>security>snmp>view$ exit
```

The following example displays the view configuration:

```
ALU-1>config>system>security>snmp# info
-----
view "testview" subtree 1
mask ff
exit
view testview subtree 1.3.6.1.2
mask ff type excluded
exit
community "private" rwa version both
community "public" r version v2c
-----
ALU-1>config>system>security>snmp#
```

Configuring Access Options

The `access` command creates an association between a user group, a security model, and the views that the user group can access. Access must be configured unless security is limited to the preconfigured access groups and views for SNMPv1 and SNMPv2c. An access group is defined by a unique combination of the group name, security model, and security level.

Use the following CLI syntax to configure access features:

CLI Syntax: `config>system>security>snmp`
 `access group group-name security-model security-model`
 `security-level security-level [context context-name`
 `[prefix-match]] [read view-name-1] [write view-name-2]`
 `[notify view-name-3]`

The following example displays access command usage:

Example: `ALU-1>config>system>security>snmp# access group`
 `testgroup security-model usm security-level auth-no-`
 `privacy read testview write testview notify testview`

The following example displays the access configuration with the view configurations.

```
ALU-1>config>system>security>snmp# info
-----
view "testview" subtree 1
    mask ff
    exit
view "testview" subtree 1.3.6.1.2
    mask ff type excluded
    exit
access group "testgroup" security-model usm security-level auth-no-
-privacy read "testview" write "testview" notify "testview"
community "public" r version both
-----
ALU->config>system>security>snmp#
```

Use the following CLI syntax to configure user group and authentication parameters:

CLI Syntax: `config>system>security# user user-name`
 `access [ftp] [snmp] [console]`
 `snmp`
 `authentication [none] | [[hash]{md5 key | sha key }`
 `privacy {none | des-key key}}`
 `group group-name`

The following example displays user security command usage:

Example: ALU-1>config>system>security# user **testuser**
 config>system>security>user\$ access **snmp**
 config>system>security>user# snmp
 config>system>security>user>snmp# authentication **hash** md5
e14672e71d3e96e7a1e19472527ee969 privacy **none**
 config>system>security>user>snmp# group **testgroup**
 config>system>security>user>snmp# exit
 config>system>security>user# exit

The following example displays the user's SNMP configuration.

```
ALU-1>config>system>security# info
-----
    user "testuser"
      access snmp
      snmp
        authentication hash md5 e14672e71d3e96e7a1e19472527ee969 privacy none
        group testgroup
      exit
    exit
  ...
-----
ALU-1>config>system>security#
```

Configuring USM Community Options

User-based security model (USM) community strings associate a community string with an SNMPv3 access group and its view. The access granted with a community string is restricted to the scope of the configured group.

By default, the 7705 SAR OS implementation of SNMP uses SNMPv3. To implement SNMPv1 and SNMPv2c, USM community strings must be explicitly configured.

Use the following CLI syntax to configure USM community options:

CLI Syntax: config>system>security>snmp
 usm-community *community-string* [hash | hash2] group
 group-name

The following example displays USM community string command usage. Note that the group `testgroup` was configured in the `config>system>security>snmp>access` CLI context.

Example: config>system>security>snmp# usm-community "test" **hash2**
 group "testgroup"

The following example displays the SNMP community configuration:

```
ALU-1>config>system>security>snmp# info
-----
view testview subtree 1
    mask ff
exit
view testview subtree 1.3.6.1.2
    mask ff type excluded
exit
access group testgroup security-model usm security-level auth-no
-privacy read testview write testview notify testview
community "private" hash2 rwa version both
community "public" hash r version v2c
usm-community "test" group "testgroup"
-----
ALU-1>config>system>security>snmp#
```

Configuring Other SNMP Parameters

Use the following CLI syntax to modify the system SNMP options:

CLI Syntax: config>system>snmp
engineID *engine-id*
general-port *port*
packet-size *bytes*
no shutdown

The following example displays the system SNMP default values:

```
ALU-104>config>system>snmp# info detail
-----
shutdown
engineID "0000xxxx000000000xxxxx00"
packet-size 1500
general-port 161
-----
ALU-104>config>system>snmp#
```

SNMP Command Reference

Command Hierarchies

- [Configuration Commands](#)
 - [SNMP System Commands](#)
 - [SNMP Security Commands](#)
- [Show Commands](#)

Configuration Commands

SNMP System Commands

```

config
  — system
    — snmp
      — snmp engine-id
      — no snmp
      — general-port port
      — no general-port
      — packet-size bytes
      — no packet-size
      — [no] shutdown

```

SNMP Security Commands

```

config
  — system
    — security
      — usm-community
        — snmp group-name security-model security-model security-level
           security-level [context context-name [prefix-match]]
           [read view-name-1] [write view-name-2] [notify view-name-3]
        — no snmp group-name [security-model security-model] [security-level
           security-level] [context context-name [prefix-match]]
           [read view-name-1] [write view-name-2] [notify view-name-3]
        — attempts [count] [time minutes1] [lockout minutes2]
        — no attempts
        — community community-string [hash | hash2] group group-name
        — no community community-string
        — usm-community community-string group group-name
        — no usm-community community-string
        — view view-name subtree oid-value
        — no view view-name [subtree oid-value]
           — usm-community mask-value [type {included | excluded}]
           — no usm-community

```

The following commands configure user-specific SNMP features. Refer to the **Security** section for CLI syntax and command descriptions.

```

config
  — system
    — security
      — [no] access user-name
      — [no] snmp
        — authentication {[none] | [[hash] {md5 key-1 | sha key-1}
           privacy {privacy-level | key-2}]
        — group group-name
        — [no] group

```

Show Commands

```
show
  — snmp
    — counters
  — system
    — information
    — security
      — access-group [group-name]
      — communities [statistics]
      — communities
      — user [profile-name]
      — user [user-id] [detail]
      — view [view-name] [capabilities] [detail]
```

Command Descriptions

- [Configuration Commands on page 201](#)
- [Show Commands on page 211](#)

Configuration Commands

- [SNMP System Commands on page 202](#)
- [SNMP Security Commands on page 205](#)

SNMP System Commands

snmp

Syntax	snmp
Context	config>system
Description	This command creates the context to configure SNMP parameters.

engineID

Syntax	[no] engineID <i>engine-id</i>
Context	config>system>snmp
Description	This command sets the SNMP engine ID to uniquely identify the SNMPv3 node. By default, the engine ID is generated using information from the system backplane.

If the SNMP engine ID is changed in the **config>system>snmp>engineID** *engine-id* context, the current configuration must be saved and a reboot must be executed. If the configuration is not saved and the system is not rebooted, the previously configured SNMP communities and logger trap-destination notify communities will not be valid for the new engine ID.



Caution: In conformance with IETF standard RFC 2274, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, hashing algorithms that generate SNMPv3 MD5 or SHA security digest keys use the engine ID. Changing the SNMP engine ID invalidates all SNMPv3 MD5 and SHA security digest keys and may render the node unmanageable. If the SNMP engine ID is changed, the SNMP hash keys must be reconfigured.

This command could be used, for example, when a chassis is replaced. Use the engine ID of the first system and configure it in the new system to preserve SNMPv3 security keys. This allows management stations to use their existing authentication keys for the new system.

Ensure that the engine IDs are not used on multiple systems. A management domain can only have one instance of each engine ID.

The **no** form of the command reverts to the default setting.

Default	The engine ID is system-generated.
Parameters	<i>engine-id</i> — an identifier from 10 to 64 hexadecimal digits (5 to 32 octet number), uniquely identifying this SNMPv3 node. This string is used to access this node from a remote host with SNMPv3.

general-port

Syntax	general-port <i>port-number</i> no general-port
Context	config>system>snmp
Description	<p>This command configures the port number used by this node to receive SNMP request messages and to send replies. Note that SNMP notifications generated by the agent are sent from the port specified in the <code>config>log>snmp-trap-group>trap-target</code> command.</p> <p>The no form of the command reverts to the default value.</p>
Default	161
Parameters	<i>port-number</i> — the port number used to send SNMP traffic other than traps
	Values 1 to 65535 (decimal)

packet-size

Syntax	packet-size <i>bytes</i> no packet-size
Context	config>system>snmp
Description	<p>This command configures the maximum SNMP packet size generated by this node. If the packet size exceeds the MTU size of the egress interface, the packet will be fragmented.</p> <p>The no form of the command reverts to the default value.</p>
Default	1500 bytes
Parameters	<i>bytes</i> — the SNMP packet size in bytes
	Values 484 to 9216

shutdown

Syntax	[no] shutdown
Context	config>system>snmp
Description	<p>This command administratively disables SNMP agent operations. System management can then only be performed using the CLI. Shutting down SNMP does not remove or change configuration parameters other than the administrative state. This command does not prevent the agent from sending SNMP notifications to any configured SNMP trap destinations. SNMP trap destinations are configured under the <code>config>log>snmp-trap-group</code> context.</p> <p>This command is automatically invoked in the event of a reboot when the processing of the configuration file fails to complete or when an SNMP persistent index file fails while the bof persist on command is enabled.</p> <p>The no form of the command administratively enables SNMP.</p>
Default	no shutdown

SNMP Security Commands

snmp

Syntax	snmp
Context	config>system>security
Description	This command creates the context to configure SNMPv1, SNMPv2c, and SNMPv3 parameters.

access group

Syntax	[no] access group <i>group-name</i> security-model {snmpv1 snmpv2c usm} security-level {no-auth-no-privacy auth-no-privacy privacy} [context <i>context-name</i> [prefix-match {exact prefix}]] [read <i>view-name-1</i>] [write <i>view-name-2</i>] [notify <i>view-name-3</i>]
Context	config>system>security>snmp
Description	<p>This command creates an association between a user group, a security model, and the views that the user group can access. Access parameters must be configured unless security is limited to the preconfigured access groups and views for SNMPv1 and SNMPv2c. An access group is defined by a unique combination of the group name, security model, and security level.</p> <p>Access must be configured unless security is limited to SNMPv1/SNMPv2c with community strings (see community).</p> <p>Default access group configurations cannot be modified or deleted.</p> <p>To remove the user group with associated security model(s) and security level(s), use the command, no access group <i>group name</i>.</p> <p>To remove a security model and security level combination from a group, use the command, no access group <i>group-name</i> security-model {snmpv1 snmpv2c usm} security-level {no-auth-no-privacy auth-no-privacy privacy}.</p>
Default	none
Parameters	<p><i>group-name</i> — specifies a unique group name up to 32 characters</p> <p>security-model {snmpv1 snmpv2c usm} — specifies the security model required to access the views configured in this node. A group can have multiple security models. For example, one view may only require SNMPv1/ SNMPv2c access while another view may require USM (SNMPv3) access rights.</p> <p>security-level {no-auth-no-priv auth-no-priv privacy} — specifies the required authentication and privacy levels to access the views configured in this node</p> <p>security-level no-auth-no-privacy — specifies that no authentication and no privacy (encryption) is required. When configuring the user's authentication, select the none option.</p>

security-level auth-no-privacy — specifies that authentication is required but privacy (encryption) is not required. When this option is configured, both the **group** and the **user** must be configured for authentication.

security-level privacy — specifies that both authentication and privacy (encryption) is required. When this option is configured, both the **group** and the **user** must be configured for authentication. The user must also be configured for privacy.

context context-name — specifies a set of SNMP objects that are associated with the context-name

The *context-name* is treated as either a full context-name string or a context-name prefix depending on the keyword specified (**exact** or **prefix**).

prefix-match — specifies the context-name **prefix-match** keywords, **exact** or **prefix**

Default exact

read view-name-1 — specifies the keyword and variable of the view to read the MIB objects. This command must be configured for each view to which the group has read access.

Values up to 32 characters

write view-name-2 — specifies the keyword and variable of the view to configure the contents of the agent. This command must be configured for each view to which the group has write access.

Values up to 32 characters

notify view-name-3 — specifies the keyword and variable of the view to send a trap about MIB objects. This command must be configured for each view to which the group has notify access.

Values up to 32 characters

attempts

Syntax	attempts [<i>count</i>] [time <i>minutes1</i>] [lockout <i>minutes2</i>] no attempts
Context	config>system>security>snmp
Description	<p>This command configures a threshold value for the number of unsuccessful SNMP connection attempts allowed in a specified time frame. The command parameters are used to counter denial of service (DOS) attacks through SNMP.</p> <p>If the threshold is exceeded, the host is locked out for the lockout time period.</p> <p>If multiple attempts commands are entered, each command overwrites the previously entered command.</p> <p>The no form of the command resets the parameters to the default values.</p>
Default	attempts 20 time 5 lockout 10

Parameters	<p><i>count</i> — the number of unsuccessful SNMP attempts allowed for the specified time</p> <p>Default 20</p> <p>Values 1 to 64</p> <p><i>time minutes1</i> — the period of time, in minutes, that a specified number of unsuccessful attempts can be made before the host is locked out</p> <p>Default 5</p> <p>Values 0 to 60</p> <p><i>lockout minutes2</i> — the lockout period, in minutes, during which the host is not allowed to log in. When the host exceeds the attempted count times in the specified time, then that host is locked out from any further login attempts for the configured time period.</p> <p>Default 10</p> <p>Values 0 to 1440</p>
-------------------	---

community

Syntax	community <i>community-string</i> [hash hash2] <i>access-permissions</i> group <i>group-name</i> no community <i>community-string</i>
Context	config>system>security>snmp
Description	<p>This command creates SNMP community strings for SNMPv1 and SNMPv2c access. This command is used in combination with the predefined access groups and views. To create custom access groups and views and associate them with SNMPv1 or SNMPv2c access, use the usm-community command.</p> <p>When configured, community implies a security model for SNMPv1 and SNMPv2c only. For SNMPv3 security, the snmp command must be configured.</p> <p>The no form of the command removes a community string.</p>
Default	none
Parameters	<p><i>community-string</i> — configures the SNMPv1/SNMPv2c community string</p> <p>hash1 hash2 — configures the hashing scheme for the community-string</p> <p><i>access-permissions</i> —</p> <ul style="list-style-type: none"> r — grants only read access to objects in the MIB, except security objects rw — grants read and write access to all objects in the MIB, except security objects rwa — grants read and write access to all objects in the MIB, including security objects mgmt — assigns a unique SNMP community string to the management router <p>group — specifies the group that governs the access rights of this community string. This group must be configured first in the config>system>security>snmp>access group context.</p> <p><i>group-name</i> — specifies the group name.</p>

usm-community

Syntax	usm-community <i>community-string</i> [hash hash2] group <i>group-name</i> no usm-community <i>community-string</i>
Context	config>system>security>snmp
Description	<p>This command is used to associate a community string with an SNMPv3 access group and its view. The access granted with a community string is restricted to the scope of the configured group.</p> <p>The 7705 SAR OS implementation of SNMP uses SNMPv3. In order to implement SNMPv1 and SNMPv2c configurations, several access groups are predefined. In order to implement SNMP with security features (version 3), security models, security levels, and USM communities must be explicitly configured. Optionally, additional views that specify more specific OIDs (MIB objects in the subtree) can be configured.</p> <p>The no form of this command removes a community string.</p>
Default	none
Parameters	<p><i>community-string</i> — configures the SNMPv1/SNMPv2c community string to determine the SNMPv3 access permissions to be used</p> <p>group — specifies the group that governs the access rights of this community string. This group must be configured first in the config>system>security>snmp>access group context.</p> <p><i>group-name</i> — specifies the group name.</p> <p>hash1 hash2 — configures hashing scheme for the community-string</p>

view

Syntax	view <i>view-name</i> subtree <i>oid-value</i> no view <i>view-name</i> [subtree <i>oid-value</i>]
Context	config>system>security>snmp
Description	<p>This command configures a view. Views control the accessibility of a MIB object within the configured MIB view and subtree. Object identifiers (OIDs) uniquely identify MIB objects in the subtree. OIDs are organized hierarchically with specific values assigned by different organizations.</p> <p>Once the subtree (OID) is identified, a mask can be created to select the portions of the subtree to be included or excluded for access using this particular view. See the mask command. The view(s) configured with this command can subsequently be used in read, write, and notify commands that are used to assign specific access group permissions to created views and assigned to particular access groups.</p> <p>Multiple subtrees can be added or removed from a view name to tailor a view to the requirements of the user access group.</p> <p>The no view <i>view-name</i> command removes a view and all subtrees.</p>

The **no view** *view-name* **subtree** *oid-value* command removes a sub-tree from the view name.

Default No views are defined

Parameters *view-name* — the 1 to 32 character view name

Default none

oid-value — the object identifier (OID) value for the *view-name*. This value, for example, 1.3.6.1.6.3.11.2.1, combined with the mask and include and exclude statements, configures the access available in the view.

It is possible to have a view with different subtrees with their own masks and include and exclude statements. This allows you to customize visibility and write capabilities for specific user requirements.

mask

Syntax **mask** *mask-value* [**type** {**included** | **excluded**}]
no mask

Context config>system>security>snmp>view *view-name*

Description The mask value and the mask type, along with the *oid-value* configured in the **view** command, determines the access of each sub-identifier of an object identifier (MIB subtree) in the view.

Each bit in the mask corresponds to a sub-identifier position; for example, the most significant bit for the first sub-identifier, the next most significant bit for the second sub-identifier, and so on. If the bit position on the sub-identifier is available, it can be included or excluded.

For example, the MIB subtree that represents MIB-II is 1.3.6.1.2.1. The mask that catches all MIB-II is 0xfc or 0b11111100.

Only a single mask may be configured per view and OID value combination. If more than one entry is configured, each subsequent entry overwrites the previous entry.

Per RFC 2575, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*, each MIB view is defined by two sets of view subtrees, the included view subtrees, and the excluded view subtrees. Every view subtree, both the included and the excluded ones, are defined in this table. To determine if a particular object instance is in a particular MIB view, compare the object instance's object identifier (OID) with each of the MIB view's active entries in this table. If none match, then the object instance is not in the MIB view. If one or more match, then the object instance is included in, or excluded from, the MIB view according to the value of vacmViewTreeFamilyType in the entry whose value of vacmViewTreeFamilySubtree has the most sub-identifiers.

The **no** form of this command removes the mask from the configuration.

Default no mask

Parameters *mask-value* — the mask value associated with the OID value determines whether the sub-identifiers are included or excluded from the view

The mask can be entered either:

- In hexadecimal format (for example, 0xfc)
- In binary format (for example, 0b11111100)



Note: If the number of bits in the bit mask is less than the number of sub-identifiers in the MIB subtree, then the mask is extended with ones until the mask length matches the number of sub-identifiers in the MIB subtree.

Default All 1s

type {included | excluded} — specifies whether to include or exclude MIB subtree objects

included - all MIB subtree objects that are identified with a 1 in the mask are available in the view

excluded - all MIB subtree objects that are identified with a 1 in the mask are denied access in the view

Default Included

Show Commands

counters

Syntax	counters
Context	show>snmp
Description	This command displays SNMP counter information. SNMP counters will continue to increase even when SNMP is shut down. Some internal modules communicate using SNMP packets.
Output	The following output is an example of SNMP counters information, and Table 20 describes the fields.

Sample Output

```
A:ALU-1# show snmp counters
=====
SNMP counters:
=====
    in packets : 463
-----
    in gets      : 93
    in getnexts  : 0
    in sets      : 370
    out packets: 463
-----
    out get responses : 463
    out traps         : 0
    variables requested: 33
    variables set      : 497
=====
A:ALU-1#
```

Table 20: Show SNMP Counters Output Fields

Label	Description
in packets	The total number of messages delivered to SNMP from the transport service
in gets	The number of SNMP get request PDUs accepted and processed by SNMP
in getnexts	The number of SNMP get next PDUs accepted and processed by SNMP
in sets	The number of SNMP set request PDUs accepted and processed by SNMP
out packets	The total number of SNMP messages passed from SNMP to the transport service
out get responses	The number of SNMP get response PDUs generated by SNMP
out traps	The number of SNMP Trap PDUs generated by SNMP
variables requested	The number of MIB objects requested by SNMP
variables set	The number of MIB objects set by SNMP as the result of receiving valid SNMP set request PDUs

information

Syntax	information
Context	show>system
Description	This command lists the SNMP configuration and statistics.
Output	The following output is an example of system information, and Table 21 describes the fields.

Sample Output

```

A:ALU-1# show system information
=====
System Information
=====
System Name           : ALU-1
System Type           : 7710 SAR-8
System Version        : B-0.0.I1204
System Contact        :
System Location       :
System Coordinates    :
System Active Slot    : A
System Up Time        : 1 days, 02:12:57.84 (hr:min:sec)

SNMP Port             : 161
SNMP Engine ID        : 0000197f00000479ff000000
SNMP Max Message Size : 1500
SNMP Admin State      : Enabled
SNMP Oper State       : Enabled
SNMP Index Boot Status : Not Persistent
SNMP Sync State       : OK

Telnet/SSH/FTP Admin  : Enabled/Enabled/Disabled
Telnet/SSH/FTP Oper   : Up/Up/Down

BOF Source            : cf3:
Image Source          : primary
Config Source         : primary
Last Booted Config File: ftp://172.22.184.249/./debby-sim1/debby-sim1-config.cfg
Last Boot Cfg Version : THU MAR 11 16:58:20 2009 UTC
Last Boot Config Header: # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SAR 7705
                        Copyright (c) 2000-2009 Alcatel-Lucent. # All rights
                        reserved. All use subject to applicable license
                        agreements. # Built on Tue Mar 11 01:26:23 PST 2009 by
                        builder in /rel0.0/I1042/panos/main # Generated TUE
                        MAR 11 16:58:20 2009 UTC

Last Boot Index Version: N/A
Last Boot Index Header : # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SAR 7705
                        Copyright (c) 2000-2009 Alcatel-Lucent. # All rights
                        reserved. All use subject to applicable license
                        agreements. # Built on Tue Mar 11 01:26:23 PST 2009 by
                        builder in /rel0.0/I1042/panos/main # Generated TUE
                        MAR 11 16:58:20 2009 UTC

Last Saved Config     : N/A
Time Last Saved       : N/A
Changes Since Last Save: No

```

```

Time Last Modified      : 2009/04/07 18:34:18
Max Cfg/BOF Backup Rev : 5
Cfg-OK Script           : N/A
Cfg-OK Script Status    : not used
Cfg-Fail Script         : N/A
Cfg-Fail Script Status  : not used

Management IP Addr     : 192.168.2.121/20
Primary DNS Server     : 192.168.1.246
Secondary DNS server   : N/A
DNS Domain             : ca.alcatel.com
BOF Static Routes      :
  To                    Next Hop
  128.251.10.0/23      192.168.1.251
  172.22.184.0/22      192.168.1.251
ATM Location ID        : 01:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
=====
A:ALU-1#

```

Table 21: Show System Information Output Fields

Label	Description
System Name	The name configured for the device
System Contact	The text string that identifies the contact name for the device
System Location	The text string that identifies the location of the device
System Coordinates	The text string that identifies the system coordinates for the device location. For example, "37.390 -122.0550" is read as latitude 37.390 north and longitude 122.0550 west.
System Up Time	The time since the last reboot
SNMP Port	The port that SNMP sends responses to management requests
SNMP Engine ID	The ID for either the local or remote SNMP engine to uniquely identify the SNMPv3 node
SNMP Max Message Size	The maximum size SNMP packet generated by this node
SNMP Admin State	Enabled — SNMP is administratively enabled
	Disabled — SNMP is administratively disabled
SNMP Oper State	Enabled — SNMP is operationally enabled
	Disabled — SNMP is operationally disabled
SNMP Index Boot Status	Persistent — Persistent indexes was enabled at the last system reboot
	Disabled — Persistent indexes was disabled at the last system reboot

Table 21: Show System Information Output Fields (Continued)

Label	Description
SNMP Sync State	The state when the synchronization of configuration files between the primary and secondary CSMs finish
Telnet/SSH/FTP Admin	The administrative state of the Telnet, SSH, and FTP sessions
Telnet/SSH/FTP Oper	The operational state of the Telnet, SSH, and FTP sessions
BOF Source	The boot location of the BOF
Image Source	primary — specifies whether the image was loaded from the primary location specified in the BOF
	secondary — specifies whether the image was loaded from the secondary location specified in the BOF
	tertiary — specifies whether the image was loaded from the tertiary location specified in the BOF
Config Source	primary — specifies whether the configuration was loaded from the primary location specified in the BOF
	secondary — specifies whether the configuration was loaded from the secondary location specified in the BOF
	tertiary — specifies whether the configuration was loaded from the tertiary location specified in the BOF
Last Booted Config File	The URL and filename of the configuration file used for the most recent boot
Last Boot Cfg Version	The version of the configuration file used for the most recent boot
Last Boot Config Header	The header information of the configuration file used for the most recent boot
Last Boot Index Version	The index version used in the most recent boot
Last Boot Index Header	The header information of the index used in the most recent boot
Last Saved Config	The filename of the last saved configuration
Time Last Saved	The time the configuration was most recently saved
Changes Since Last Save	Yes — the configuration has changed since the last save
	No — the configuration has not changed since the last save
Time Last Modified	The time of the last modification

Table 21: Show System Information Output Fields (Continued)

Label	Description
Max Cfg/BOF Backup Rev	The maximum number of backup revisions maintained for a configuration file. This value also applies to the number of revisions maintained for the BOF file.
Cfg-OK Script	URL — the location and name of the CLI script file executed following successful completion of the boot-up configuration file execution
	N/A — no CLI script file is executed
Cfg-OK Script Status	Successful/Failed — the results from the execution of the CLI script file specified in the Cfg-OK Script location
	Not used — no CLI script file was executed
Cfg-Fail Script	URL — the location and name of the CLI script file executed following a failed boot-up configuration file execution
	Not used — no CLI script file was executed
Cfg-Fail Script Status	Successful/Failed — the results from the execution of the CLI script file specified in the Cfg-Fail Script location
	Not used — no CLI script file was executed
Management IP address	The Management IP address of the node
DNS Server	The DNS address of the node
DNS Domain	The DNS domain name of the node
BOF Static Routes	To — the static route destination
	Next Hop — the next hop IP address used to reach the destination
	Metric — displays the priority of this static route versus other static routes
	None — no static routes are configured
ATM location ID	For ATM OAM loopbacks - the address of the network device referenced in the loopback request

access-group

Syntax	access-group <i>group-name</i>
Context	show>system>security
Description	This command displays access group information.
Parameters	<i>group-name</i> — the access group name
Output	The following output is an example of access group information, and Table 22 describes the fields.

Sample Output

```
A:ALU-1# show system security access-group
=====
Access Groups
=====
```

group name	security model	security level	read view	write view	notify view
snmp-ro	snmpv1	none	no-security		no-security
snmp-ro	snmpv2c	none	no-security		no-security
snmp-rw	snmpv1	none	no-security	no-security	no-security
snmp-rw	snmpv2c	none	no-security	no-security	no-security
snmp-rwa	snmpv1	none	iso	iso	iso
snmp-rwa	snmpv2c	none	iso	iso	iso
snmp-trap	snmpv1	none			iso
snmp-trap	snmpv2c	none			iso

```
-----
No. of Access Groups: 8
=====
A:ALU-1#

A:ALU-1# show system security access-group snmp-ro
=====
Access Groups
=====
```

group name	security model	security level	read view	write view	notify view
snmp-ro	snmpv1	none	no-security		no-security

```
-----
No. of Access Groups: 1
...
=====
A:ALU-1#
```

Table 22: Show System Access Group Fields

Label	Description
Group name	The access group name
Security model	The security model required to access the views configured in this node
Security level	The required authentication and privacy levels to access the views configured in this node
Read view	The view to read the MIB objects
Write view	The view to configure the contents of the agent
Notify view	The view to send a trap about MIB objects
No. of access groups	The total number of configured access groups

communities

Syntax **communities**

Context show>system>security

Description This command lists SNMP communities and characteristics.

Output The following output is an example of communities information, and [Table 23](#) describes the fields.

Sample Output

```
A:ALU-1# show system security communities
=====
Communities
=====
community      access  view      version    group name
-----
private         rw      iso       v1 v2c     snmp-rwa
cli-readonly    r       iso       v2c        cli-readonly
cli-readwrite   rw      iso       v2c        cli-readwrite
-----
No. of Communities: 3
=====
A:ALU-1#
```

Table 23: Show Communities Output Fields

Label	Description
Community	The community string name for SNMPv1 and SNMPv2c access only
Access	<code>rw</code> — The community string allows read-only access to all objects in the MIB except security objects
	<code>rw</code> — The community string allows read-write access to all objects in the MIB except security objects
	<code>rwa</code> — The community string allows read-write access to all objects in the MIB including security objects
	<code>mgmt</code> — The unique SNMP community string assigned to the management router
View	The view name
Version	The SNMP version
Group Name	The access group name
No of Communities	The total number of configured community strings

user

Syntax `user [user-id] [detail]`

Context `show>system>security`

Description This command displays user information.

Parameters *user-id* — the name of the user

detail — displays all information associated with the specified use

Output The following output is an example of user information, and [Table 24](#) describes the fields.

Sample Output

```

A:ALU-1# show system security user
=====
Users
=====
user id          New   User Permissions Password   Login   Failed   Local
                  Pwd   console ftp snmp  Expires Attempts Logins  Conf
-----
admin            n     y     n   n   never      2         0       y
testuser         n     n     n   y   never      0         0       y
-----
Number of users : 2
=====
A:ALU-1#

```

Table 24: Show User Output Fields

Label	Description
User ID	The name of a system user
Need New PWD	Yes — the user must change their password at the next login
	No — the user is not forced to change their password at the next login
User Permissions	Console — specifies whether the user is permitted console/Telnet access
	FTP — specifies whether the user is permitted FTP access
	SNMP — specifies whether the user is permitted SNMP access
Password expires	The date on which the current password expires
Attempted logins	The number of times the user has attempted to log in, irrespective of whether the login succeeded or failed
Failed logins	The number of unsuccessful login attempts
Local Conf.	Y — password authentication is based on the local password database
	N — password authentication is not based on the local password database

view

Syntax	view [<i>view-name</i>] [detail capabilities]
Context	show>system>security
Description	This command lists one or all views and permissions in the MIB-OID tree.
Parameters	<p><i>view-name</i> — the name of the view</p> <p>detail — displays all groups associated with the view</p> <p>capabilities — displays all views, including excluded MIB-OID trees from unsupported features</p>
Output	The following output is an example of system security view information, and Table 25 describes the fields.

Sample Output

```
A:ALU-1# show system security view
=====
Views
=====
view name      oid tree      mask      permission
-----
iso            1             included
no-security    1             included
no-security    1.3.6.1.6.3   excluded
no-security    1.3.6.1.6.3.10.2.1 included
no-security    1.3.6.1.6.3.11.2.1 included
no-security    1.3.6.1.6.3.15.1.1 included
-----
No. of Views: 6
=====
A:ALU-1#

A:ALU-1# show system security view no-security detail
=====
Views
=====
view name      oid tree      mask      permission
-----
no-security    1             included
no-security    1.3.6.1.6.3   excluded
no-security    1.3.6.1.6.3.10.2.1 included
no-security    1.3.6.1.6.3.11.2.1 included
no-security    1.3.6.1.6.3.15.1.1 included
-----
No. of Views: 5
=====
=====
no-security used in
```

```

=====
group name
-----
snmp-ro
snmp-rw
=====
A:ALU-1#
A:ATM1M1>config# show system security view capabilities

=====
Views
=====
view name          oid tree          mask          permission
-----
iso                1                included
iso                1.0.8802         no-support
iso                1.3.6.1.3.37     no-support
iso                1.3.6.1.3.92     no-support
iso                1.3.6.1.3.95     no-support
iso                1.3.6.1.2.1.14   no-support
iso                1.3.6.1.2.1.15   no-support
iso                1.3.6.1.2.1.23   no-support
iso                1.3.6.1.2.1.51   no-support
iso                1.3.6.1.2.1.68   no-support
iso                1.3.6.1.2.1.85   no-support
iso                1.3.6.1.2.1.100  no-support
iso                1.3.6.1.2.1.4.39 no-support
iso                1.3.6.1.2.1.5.20 no-support
=====
A:ALU-1#

```

Table 25: Show System Security View Output Fields

Label	Description
View name	The name of the view. Views control the accessibility of a MIB object within the configured MIB view and subtree.
OID tree	The Object Identifier (OID) value. OIDs uniquely identify MIB objects in the subtree.
Mask	The mask value and the mask type, along with the <i>oid-value</i> configured in the view command, determines the access of each sub-identifier of an object identifier (MIB subtree) in the view
Permission	Included — specifies to include MIB subtree objects
	Excluded — specifies to exclude MIB subtree objects
	No-support — specifies not to support MIB subtree objects
No. of Views	The total number of configured views
Group name	The access group name

Event and Accounting Logs

In This Chapter

This chapter provides information about configuring event and accounting logs in the 7705 SAR. Topics in this chapter include:

- [Logging Overview on page 224](#)
- [Log Destinations on page 226](#)
 - [Console on page 226](#)
 - [Session on page 226](#)
 - [Memory Logs on page 226](#)
 - [Log Files on page 227](#)
 - [SNMP Trap Group on page 228](#)
 - [Syslog on page 229](#)
- [Event Logs on page 230](#)
 - [Event Sources on page 230](#)
 - [Event Control on page 232](#)
 - [Log Manager and Event Logs on page 234](#)
 - [Event Filter Policies on page 234](#)
 - [Event Log Entries on page 235](#)
 - [Simple Logger Event Throttling on page 237](#)
 - [Default System Log on page 238](#)
- [Accounting Logs on page 239](#)
 - [Accounting Records on page 239](#)
 - [Accounting Files on page 242](#)
 - [Design Considerations on page 242](#)
- [Configuration Notes on page 243](#)
- [Configuring Logging with CLI on page 245](#)
- [Log Command Reference on page 269](#)

Logging Overview

The two primary types of logging supported on the 7705 SAR are event logging and accounting logs.

Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system. Events are messages generated by the system by applications or processes within the 7705 SAR. The 7705 SAR groups events into four major categories or event sources:

- Security events — security events are generated by the SECURITY application and pertain to attempts to breach system security
- Change events — change events are generated by the USER application and pertain to the configuration and operation of the node
- Debug events — debug events are generated by the DEBUG application and pertain to trace or other debugging information
- Main events — events that pertain to 7705 SAR applications that are not assigned to other event categories/sources

The applications listed above have the following properties:

- a timestamp in UTC or local time
- the generating application
- a unique event ID within the application
- the VRF-ID
- a subject identifying the affected object
- a short text description

Event control assigns the severity for each application event and determines whether the event should be generated or suppressed. The severity numbers and severity names supported in the 7705 SAR conform to ITU standards M.3100 X.733 and X.21 and are listed in [Table 26](#).

Table 26: Event Severity Levels

Severity Number	Severity Name
1	Cleared
2	Indeterminate (info)
3	Critical
4	Major
5	Minor
6	Warning

Event control maintains a count of the number of events generated (logged) and dropped (suppressed) for each application event. The severity of an application event can be configured in event control.

An event log within the 7705 SAR associates the event sources with logging destinations. Examples of logging destinations include: the console session, memory logs, file destinations, SNMP trap groups, and syslog destinations. A log filter policy can be associated with the event log to control which events will be logged in the event log based on combinations of application, severity, event ID range, and the subject of the event.

The 7705 SAR accounting logs collect comprehensive accounting statistics to support a variety of billing models. The 7705 SAR collects accounting data on services on a per-service class basis. In addition to gathering information critical for service billing, accounting records can be analyzed to provide insight about customer service trends for potential service revenue opportunities.

Accounting statistics are collected according to the parameters defined within the context of an accounting policy. Accounting policies are applied to customer Service Access Points (SAPs). Accounting statistics are collected by counters for individual service queues defined on the customer's SAPs.

The type of record defined within the accounting policy determines where a policy is applied, what statistics are collected and the time interval at which to collect statistics.

The only supported destination for an accounting log is a compact flash system device (*cf3*: on all platforms; *cf1*: or *cf2*: on the 7705 SAR-18). Accounting data is stored within a standard directory structure on the device in compressed XML format.

Log Destinations

Both event logs and accounting logs use a common mechanism for referencing a log destination. 7705 SAR routers support the following log destinations:

- [Console](#)
- [Session](#)
- [Memory Logs](#)
- [Log Files](#)
- [SNMP Trap Group](#)
- [Syslog](#)

An event log can be associated with multiple event sources, but it can only have a single log destination.

A file destination is the only type of log destination that can be configured for an accounting log.

Console

Sending events to a console destination means the message will be sent to the system console. The console device can be used as an event log destination.

Session

A session destination is a temporary log destination that directs entries to the active Telnet or SSH session for the duration of the session. When the session is terminated, for example, when the user logs out, the event log is removed. Event logs configured with a session destination are not stored in the configuration file. Event logs can direct log entries to the session destination.

Memory Logs

A memory log is a circular buffer. When the log is full, the oldest entry in the log is replaced with the new entry. When a memory log is created, the specific number of entries it can hold can be specified; otherwise, it will assume a default size. An event log can send entries to a memory log destination.

Log Files

Log files can be used by both event logs and accounting logs and are stored on the compact flash device (*cf3*: on all platforms; *cf1*: or *cf2*: on the 7705 SAR-18) in the file system.

A log file is identified by a single log file ID, but a log file will generally be composed of a number of individual files in the file system. A log file is configured with a rollover parameter, expressed in minutes, which represents the length of time an individual log file should be written to before a new file is created for the relevant log file ID. The rollover time is checked only when an update to the log is performed. Thus, this rule is subject to the incoming rate of the data being logged. For example, if the rate is very low, the actual rollover time may be longer than the configured value.

The retention time for a log file specifies the amount of time the file should be retained on the system based on the creation date and time of the file. The retention time is used as a factor to determine which files should be deleted first if the file system device nears 100% usage.

When a log file is created, only the compact flash device for the log file is specified. Log files are created in specific subdirectories with standardized names depending on the type of information stored in the log file.

Event log files are always created in the `\log` directory on the compact flash device. The naming convention for event log files is:

`logeeff-timestamp`

where:

ee is the event log ID

ff is the log file destination ID

timestamp is the timestamp when the file is created in the form of *yyyymmdd-hhmmss* where:

yyyy is the four-digit year (for example, 2008)

mm is the two-digit number representing the month (for example, 12 for December)

dd is the two-digit number representing the day of the month (for example, 03 for the 3rd of the month)

hh is the two-digit hour in a 24-hour clock (for example, 04 for 4 a.m.)

mm is the two-digit minute (for example, 30 for 30 minutes past the hour)

ss is the two-digit second (for example, 14 for 14 seconds)

Accounting log files are created in the `\act-collect` directory on the compact flash device. The naming convention for accounting logs is:

`actaa \overline{ff} -timestamp.xml.gz`

where:

aa is the accounting policy ID

ff is the log file destination ID

timestamp is the timestamp when the file is created, in the same form as for event logs.

Accounting logs are `.xml` files created in a compressed format and have a `.gz` extension.

The `\act-collect` directory is where active accounting logs are written. When an accounting log is rolled over, the active file is closed and archived in the `\act` directory before a new active accounting log file is created in `\act-collect`.

SNMP Trap Group

An event log can be configured to send events to SNMP trap receivers by specifying an SNMP trap group destination.

An SNMP trap group can have multiple trap targets. Each trap target can have different operational parameters.

A trap destination has the following properties:

- the IP address of the trap receiver (IPv4 or IPv6)
- the UDP port used to send the SNMP trap
- SNMP version (v1, v2c, or v3) used to format the SNMP notification
- SNMP community name for SNMPv1 and SNMPv2c receivers
- security name and level for SNMPv3 trap receivers

For SNMP traps that will be sent out-of-band through the Management Ethernet port on the CSM, the source IP address of the trap is the IP interface address defined on the Management Ethernet port. For SNMP traps that will be sent in-band, the source IP address of the trap is the system IP address of the 7705 SAR.

Each trap target destination of a trap group receives the identical sequence of events as defined by the log ID and the associated sources and log filter applied.

Syslog

An event log can be configured to send events to one syslog destination. Syslog destinations have the following properties:

- syslog server IP address (IPv4 or IPv6)
- the UDP port used to send the syslog message
- the Syslog Facility Code
- the Syslog Severity Threshold (0 to 7) (events exceeding the configured level will be sent)

Because syslog uses eight severity levels whereas the 7705 SAR uses six internal severity levels, the severity levels are mapped to syslog severities. [Table 27](#) displays the severity level mappings to syslog severities.

Table 27: 7705 SAR to Syslog Severity Level Mappings

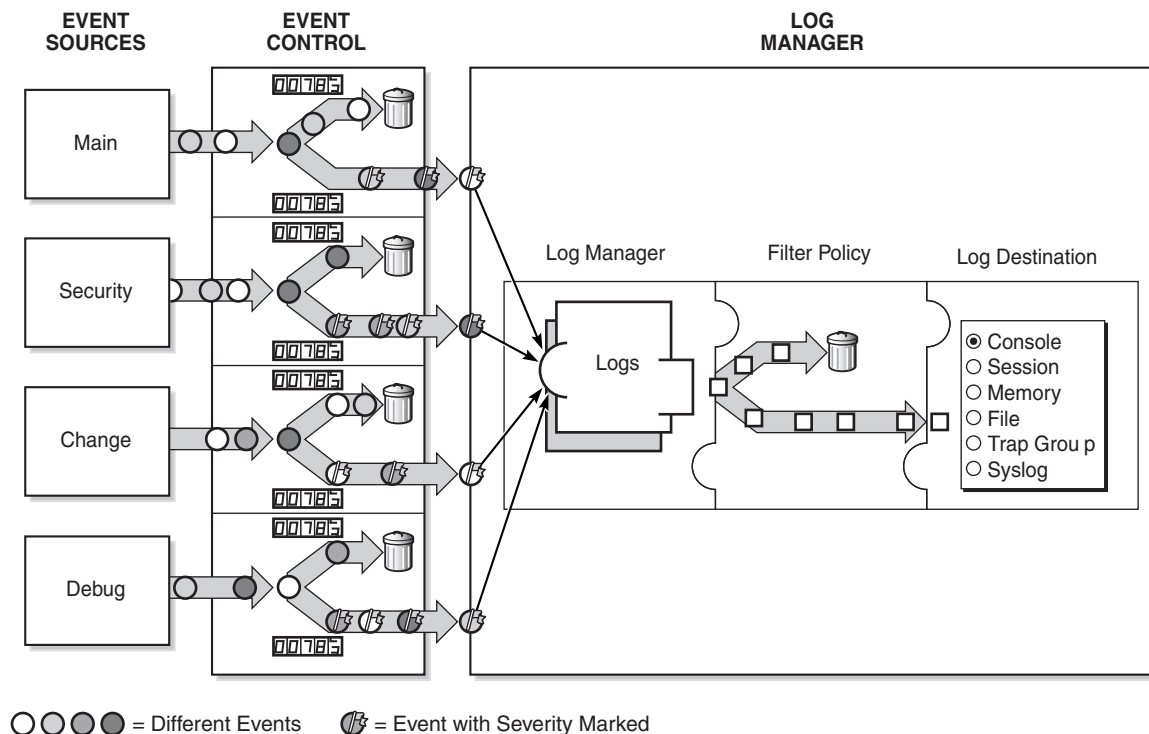
7705 SAR Severity Level	Syslog Severity Level (highest to lowest)	Syslog Configured Severity	Definition
3 critical	0	emergency	System is unusable
	1	alert	Action must be taken immediately
4 major	2	critical	Critical conditions
5 minor	3	error	Error conditions
6 warning	4	warning	Warning conditions
	5	notice	Normal but significant condition
1 cleared 2 indeterminate	6	info	Informational messages
	7	debug	Debug-level messages

Event Logs

Event logs are the means of recording-system generated events for later analysis. Events are messages generated by the system by applications or processes within the 7705 SAR.

Figure 3 depicts a functional block diagram of event logging.

Figure 3: Event Logging Block Diagram



No1025

Event Sources

In Figure 3, the event sources are the main categories of events that feed the log manager.

- **Security** — The security event source is all events that affect attempts to breach system security, such as failed login attempts, attempts to access MIB tables to which the user is not granted access, or attempts to enter a branch of the CLI to which access has not been granted. Security events are generated by the SECURITY application.

- **Change** — The change activity event source is all events that directly affect the configuration or operation of the node. Change events are generated by the USER application.
- **Debug** — The debug event source is the debugging configuration that has been enabled on the system. Debug events are generated by the DEBUG application.
- **Main** — The main event source receives events from all other applications within the 7705 SAR.

Examples of applications within the 7705 SAR include MPLS and services. The following is an example of the `show log applications` command output that displays all applications:

```
*A:ALU-48# show log applications
=====
Log Event Application Names
=====
Application Name
-----
APS
ATM
BGP
CHASSIS
CPMHWFILTER
DEBUG
DHCP
EFM_OAM
ETH-CFM
FILTER
IP
ISIS
LDP
LOGGER
MPLS
NTP
OAM
OSPF
PORT
PPP
PTP
QOS
ROUTE_POLICY
SECURITY
SNMP
STP
SVCNMR
SYSTEM
TIP
USER
VRTR
=====
*A:ALU-48#
```

Event Control

Event control pre-processes the events generated by applications before the event is passed into the main event stream. Event control assigns a severity to application events and can either forward the event to the main event source or suppress the event. Suppressed events are counted in event control, but these events will not generate log entries as they never reach the log manager.

Simple event throttling is another method of event control and is configured in the same way as the generation and suppression options. See [Simple Logger Event Throttling](#).

Events are assigned a default severity level in the system, but the application event severities can be changed by the user.

Application events contain an event number and description that explains why the event is generated. The event number is unique within an application, but the number can be duplicated in other applications.

The following example, generated by querying event control for application-generated events, displays a partial list of event numbers and names.

```
router# show log event-control
=====
Log Events
=====
Application
ID#      Event Name                               P   g/s    Logged    Dropped
-----
ATM:
  2011 tAtmPlcpSubLayerClear                   MI  gen      0          0
  2012 tAtmEpOutOfPeerVpiOrVciRange            WA  gen      0          0
  2013 tAtmMaxPeerVccsExceeded                 WA  gen      0          0
...
CHASSIS:
  2001 cardFailure                             MA  gen      0          0
  2002 cardInserted                           MI  gen      7          0
  2003 cardRemoved                             MI  gen      0          0
...
DEBUG:
L 2001 traceEvent                             MI  gen      0          0
EFM_OAM:
  2001 tmnxDot3OamPeerChanged                 MI  gen      0          0
  2002 tmnxDot3OamLoopDetected                MI  gen      0          0
FILTER:
  2001 tIPFilterPBRPacketsDrop                WA  gen      0          0
  2002 tFilterEntryActivationFailed            WA  gen      0          0
  2003 tFilterEntryActivationRestored          WA  gen      0          0
GSMP:
  2001 tmnxAncpIngRateMonitorEvent            WA  gen      0          0
L 2002 tmnxAncpIngRateMonitorEventL           WA  gen      0          0
  2003 tmnxAncpEgrRateMonitorEvent            WA  gen      0          0
...
IP:
L 2001 clearRTMError                          MI  gen      0          0
```



```

L 2002 ipEtherBroadcast          MI  gen      0      0
L 2003 ipDuplicateAddress        MI  gen      0      0
...
LDP:
    2001 vRtrLdpStateChange      MI  gen      0      0
    2002 vRtrLdpInstanceStateChange MI  gen      0      0
    2003 vRtrLdpIfStateChange    MI  gen      0      0
...
LOGGER:
L 2001 STARTED                  MI  gen      5      0
    2002 tmnxLogTraceError       CR  gen      0      0
    2005 tmnxLogSpaceContention  MA  gen      0      0
...
MPLS:
    2001 mplsXCUp                WA  gen      0      0
    2002 mplsXCDown              WA  gen      0      0
    2003 mplsTunnelUp            WA  gen      0      0
...
NTP:
    2001 tmnxNtpAuthMismatch     WA  gen      0      0
    2002 tmnxNtpNoServersAvail   MA  gen      0      0
    2003 tmnxNtpServersAvail     MI  gen      0      0
...
SYSTEM:
    2001 stiDateAndTimeChanged    WA  gen      0      0
    2002 ssiSaveConfigSucceeded   MA  gen      0      0
    2003 ssiSaveConfigFailed      CR  gen      0      0
...
USER:
L 2001 cli_user_login            MI  gen      4      0
L 2002 cli_user_logout           MI  gen      3      0
L 2003 cli_user_login_failed     MI  gen      0      0
...
VRTR:
    2001 tmnxVRtrMidRouteTCA      MI  gen      0      0
    2002 tmnxVRtrHighRouteTCA     MI  gen      0      0
    2003 tmnxVRtrHighRouteCleared MI  gen      0      0
...
=====
router#

```

Log Manager and Event Logs

Events that are forwarded by event control are sent to the log manager. The log manager manages the event logs in the system and the relationships between the log sources, event logs and log destinations, and log filter policies.

An event log has the following properties:

- a unique log ID
The log ID is a short, numeric identifier for the event log. A maximum of 10 logs can be configured at a time.
- one or more log sources
The source stream or streams to be sent to log destinations can be specified. The source must be identified before the destination can be specified. The events can be from the main event stream, events in the security event stream, or events in the user activity stream.
- one event log destination
A log can only have a single destination. The destination for the log ID destination can be one of console, session, syslog, snmp-trap-group, memory, or a file on the local file system.
- an optional event filter policy
An event filter policy defines whether to forward or drop an event or trap based on match criteria.

Event Filter Policies

The log manager uses event filter policies to control which events are forwarded or dropped based on various criteria. Like other policies with the 7705 SAR, filter policies have a default action. The default actions are either:

- forward
- drop

Filter policies also include a number of filter policy entries that are identified with an entry ID and define specific match criteria and a forward or drop action for the match criteria.

Each entry contains a combination of matching criteria that define the application, event number, router, severity, and subject conditions. The entry's action determines how the packets should be treated if they have met the match criteria.

Entries are evaluated in order from the lowest to the highest entry ID. The first matching event is subject to the forward or drop action for that entry.

Valid operators are displayed in [Table 28](#).

Table 28: Valid Filter Policy Operators

Operator	Description
eq	Equal to
neq	Not equal to
lt	Less than
lte	Less than or equal to
gt	Greater than
gte	Greater than or equal to

A match criteria entry can include combinations of:

- equal to or not equal to a given system application
- equal to, not equal to, less than, less than or equal to, greater than, or greater than or equal to an event number within the application
- equal to, not equal to, less than, less than or equal to, greater than, or greater than or equal to a severity level
- equal to or not equal to a router name string or regular expression match
- equal to or not equal to an event subject string or regular expression match

Event Log Entries

Log entries that are forwarded to a destination are formatted in a way that is appropriate for the specific destination; for example, whether it is to be recorded to a file or sent as an SNMP trap, but log event entries also have common elements or properties. All application-generated events have the following properties:

- a timestamp in UTC or local time
- the generating application
- a unique event ID within the application
- a router name identifying the VRF-ID that generated the event
- a subject identifying the affected object
- a short text description

The general format for an event in an event log with either a memory, console or file destination is as follows:

```
nnnn YYYY/MM/DD HH:MM:SS.SS <severity>:<application> # <event_id> <router-name>
<subject> description
```

The following is an event log example:

```
475 2007/11/27 00:19:40.38 WARNING: SNMP #2008 Base 1/1/1
"interface 1/1/1 came up"
```

The specific elements that make up the general format are described in [Table 29](#).

Table 29: Log Entry Field Descriptions

Label	Description
nnnn	The log entry sequence number
YYYY/MM/DD	The UTC date stamp for the log entry <i>YYYY</i> — Year <i>MM</i> — Month <i>DD</i> — Day
HH:MM:SS.SS	The UTC timestamp for the event <i>HH</i> — Hours (24-hour format) <i>MM</i> — Minutes <i>SS.SS</i> — Seconds
<severity>	The severity level name of the event CLEARED — a cleared event (severity number 1) INFO — an indeterminate/informational severity event (severity level 2) CRITICAL — a critical severity event (severity level 3) MAJOR — a major severity event (severity level 4) MINOR — a minor severity event (severity level 5) WARNING — a warning severity event (severity 6)
<application>	The application generating the log message
<event_id>	The application's event ID number for the event
<router>	The router name representing the VRF-ID that generated the event
<subject>	The subject/affected object for the event
<description>	A text description of the event

Simple Logger Event Throttling

Simple event throttling provides a mechanism to protect event receivers from being overloaded when a scenario causes many events to be generated in a very short period of time. A throttling rate (events/seconds), can be configured. Specific application events can be configured to be throttled. Once the throttling event limit is exceeded in a throttling interval, any further events of that type are dropped and the dropped events counter is incremented. Dropped events counts are displayed with the **show>log>event-control** command. Events are dropped before being sent to one of the logger event collector tasks. There is no record of the details of the dropped events and therefore no way to retrieve event history data lost by this throttling method.

A particular event type can be generated by multiple managed objects within the system. At the point that this throttling method is applied, the logger application has no information about the managed object that generated the event and cannot distinguish between events generated by object "A" from events generated by object "B". If the events have the same event-id, they are throttled regardless of the managed object that generated them. The logger application also cannot distinguish between events that will be logged to destination log-id <n> from events that will be logged to destination log-id <m>.

Throttle rate applies commonly to all event types. It is not configurable for a specific event type.

A timer task checks for events dropped by throttling when the throttle interval expires. If any events have been dropped, a TIMETRA-SYSTEM-MIB::tmnxTrapDropped notification is sent.

By default, event throttling is set to off for each specific event type. It must be explicitly enabled for each event type where throttling is desired. This makes backwards compatibility of configuration files easier to manage.

Default System Log

Log 99 is a preconfigured memory-based log that logs events from the main event source (not security, debug, or change). Log 99 exists by default.

The following example displays the log 99 configuration.

```
ALU-1>config>log# info detail
#-----
echo "Log Configuration "
#-----
...
    log-id 99
        description "Default system log"
        no filter
        time-format utc
        from main
        to memory 500
        no shutdown
    exit
-----
```

Accounting Logs

Before an accounting policy can be created, a target log file must be created to collect the accounting records. The files are stored in system memory on a compact flash (*cf3*: on all platforms; *cf1*: or *cf2*: on the 7705 SAR-18) in a compressed (tar) XML format and can be retrieved using FTP or SCP.

Accounting Records

An accounting policy must define a record name and collection interval. Only one record name can be configured per accounting policy. Also, a record name can only be used in one accounting policy.

[Table 30](#) lists the record name, sub-record types, and default collection period for service and network accounting policies.

Table 30: Accounting Record Name and Collection Periods

Record Name	Sub-Record Types	Accounting Object	Default Collection Period (minutes)
service-ingress-octets	sio	SAP	5
service-egress-octets	seo	SAP	5
service-ingress-packets	sip	SAP	5
service-egress-packets	sep	SAP	5

When creating accounting policies, one service accounting policy can be defined as the default. If statistics collection is enabled on a SAP and no accounting policy is applied, then the respective default policy is used. If no default policy is defined, then no statistics are collected unless a specifically defined accounting policy is applied.

Each accounting record name is composed of one or more sub-records, which are in turn composed of multiple fields. [Table 31](#) lists the accounting policy record names and the statistics that are collected with each.

Table 31: Accounting Record Name Details

Record Name	Sub-Record	Field	Field Description
Service-ingress-octets	sio	svc	SvcId
		sap	SapId
		qid	QueueId
		hoo	OfferedHiPrioOctets
		hod	DroppedHiPrioOctets
		loo	LowOctetsOffered
		lod	LowOctetsDropped
		uco	UncoloredOctetsOffered
		iof	InProfileOctetsForwarded
		oof	OutOfProfileOctetsForwarded
Service-egress-octets	seo	svc	SvcId
		sap	SapId
		qid	QueueId
		iof	InProfileOctetsForwarded
		iod	InProfileOctetsDropped
		oof	OutOfProfileOctetsForwarded
		ood	OutOfProfileOctetsDropped

Table 31: Accounting Record Name Details (Continued)

Record Name	Sub-Record	Field	Field Description
Service-ingress-packets	sip	svc	SvcId
		sap	SapId
		qid	QueueId
		hpo	HighPktsOffered
		hpd	HighPktsDropped
		lpo	LowPktsOffered
		lpd	LowPktsDropped
		ucp	UncoloredPacketsOffered
		ipf	InProfilePktsForwarded
		opf	OutOfProfilePktsForwarded
Service-egress-packets	sep	svc	SvcId
		sap	SapId
		qid	QueueId
		ipf	InProfilePktsForwarded
		ipd	InProfilePktsDropped
		opf	OutOfProfilePktsForwarded
		opd	OutOfProfilePktsDropped
		sap	SapId
		slaProfile	SlaProfile

Accounting Files

When a policy has been created and applied to a service, the accounting file is stored on the compact flash in a compressed XML file format. The 7705 SAR creates two directories on the compact flash to store the files. The following output displays a directory named `act-collect` that holds accounting files that are open and actively collecting statistics, and a directory named `act` that stores the files that have been closed and are awaiting retrieval.

```
ALU-1>file cf3:\# dir act*
12/19/2006 06:08a      <DIR>          act-collect
12/19/2006 06:08a      <DIR>          act

ALU-1>file cf3:\act-collect\ # dir
Directory of cf3:\act-collect#

12/23/2006 01:46a      <DIR>          .
12/23/2006 12:47a      <DIR>          ..
12/23/2006 01:46a                      112 act1111-20031223-014658.xml.gz
12/23/2006 01:38a                      197 act1212-20031223-013800.xml.gz
```

Accounting files always have the prefix `act` followed by the accounting policy ID, log ID and timestamp. The accounting log file naming and log file destination properties (such as rollover and retention) are discussed in more detail in [Log Files](#).

A file ID can only be assigned to either one event log ID or one accounting log.

Design Considerations

The 7705 SAR has ample resources to support large-scale accounting policy deployments. When preparing for an accounting policy deployment, verify that data collection, file rollover, and file retention intervals are properly tuned for the amount of statistics to be collected.

If the accounting policy collection interval is too brief, there may be insufficient time to store the data from all the services within the specified interval. If that is the case, some records may be lost or incomplete. Interval time, record types, and number of services using an accounting policy are all factors that should be considered when implementing accounting policies.

The rollover and retention intervals on the log files and the frequency of file retrieval must also be considered when designing accounting policy deployments. The amount of data stored depends on the type of record collected, the number of services that are collecting statistics, and the collection interval that is used.

Configuration Notes

This section describes logging configuration caveats.

- A file or filter cannot be deleted if it has been applied to a log.
- File IDs, syslog IDs, or SNMP trap groups must be configured before they can be applied to a log ID.
- A file ID can only be assigned to either one log ID or one accounting policy.
- Accounting policies must be configured in the `config>log` context before they can be applied to a service SAP or service interface.
- The `snmp-trap-id` must be the same as the `log-id`.

Reference Sources

For information on supported IETF drafts and standards as well as standard and proprietary MIBS, refer to [Standards and Protocol Support](#).

Configuring Logging with CLI

This section provides information to configure logging using the command line interface.

Topics in this section include:

- [Log Configuration Overview on page 246](#)
- [Log Type on page 247](#)
- [Basic Event Log Configuration on page 248](#)
- [Common Configuration Tasks on page 249](#)
 - [Configuring an Event Log on page 249](#)
 - [Configuring a File ID on page 250](#)
 - [Configuring an Accounting Policy on page 251](#)
 - [Configuring Event Control on page 252](#)
 - [Configuring Throttle Rate on page 253](#)
 - [Configuring a Log Filter on page 254](#)
 - [Configuring an SNMP Trap Group on page 256](#)
 - [Configuring a Syslog Target on page 257](#)
- [Log Management Tasks on page 258](#)
 - [Modifying a Log File on page 258](#)
 - [Deleting a Log File on page 260](#)
 - [Modifying a File ID on page 261](#)
 - [Deleting a File ID on page 262](#)
 - [Modifying a Syslog ID on page 262](#)
 - [Deleting a Syslog ID on page 263](#)
 - [Modifying an SNMP Trap Group on page 263](#)
 - [Deleting an SNMP Trap Group on page 264](#)
 - [Modifying a Log Filter on page 265](#)
 - [Deleting a Log Filter on page 266](#)
 - [Modifying Event Control Parameters on page 267](#)
 - [Returning to the Default Event Control Configuration on page 268](#)

Log Configuration Overview

Logging on the 7705 SAR is used to provide the operator with logging information for monitoring and troubleshooting. You can configure logging parameters to save information in a log file or direct the messages to other devices. Logging commands allow you to:

- select the types of logging information to be recorded
 - assign a severity to the log messages
 - select the source and target of logging information
-

Log Type

Logs can be configured in the following contexts:

- Log file — log files can contain log event message streams or accounting/billing information. Log file IDs are used to direct events, alarms/traps, and debug information to their respective targets.
 - SNMP trap groups — SNMP trap groups contain an IP address and community names that identify targets to send traps following specified events
 - Syslog — information can be sent to a syslog host that is capable of receiving selected syslog messages from a network element
 - Event control — configures a particular event, or all events associated with an application, to be generated or suppressed
 - Event filters — an event filter defines whether to forward or drop an event or trap based on match criteria
 - Accounting policies — an accounting policy defines the accounting records that will be created. Accounting policies can be applied to one or more service access points (SAPs).
 - Event logs — an event log defines the types of events to be delivered to an associated destination
 - Event throttling rate — defines the rate of throttling events
-

Basic Event Log Configuration

The most basic log configuration must have the following:

- a log ID or an accounting policy ID
- a log source
- a log destination

The following displays a log configuration example.

```
ALU-12>config>log# info
#-----
echo "Log Configuration "
#-----
    file-id 1
        description "This is a test file-id."
        location cf3:
    exit
    file-id 2
        description "This is a test log."
        location cf3:
    exit
    snmp-trap-group 7
        trap-target 11.22.33.44 "snmpv2c" notify-community "public"
    exit
    log-id 2
        from main
        to file 2
    exit
#-----
ALU-12>config>log#
```

Common Configuration Tasks

The following sections describe basic system tasks that must be performed.

- [Configuring an Event Log](#)
- [Configuring a File ID](#)
- [Configuring an Accounting Policy](#)
- [Configuring Event Control](#)
- [Configuring Throttle Rate](#)
- [Configuring a Log Filter](#)
- [Configuring an SNMP Trap Group](#)
- [Configuring a Syslog Target](#)

Configuring an Event Log

An event log file contains information used to direct events, alarms, traps, and debug information to their respective destinations. One or more event sources can be specified. File IDs, SNMP trap groups, or syslog IDs must be configured before they can be applied to an event log ID.

Use the following CLI syntax to configure a log file:

CLI Syntax: `config>log`
 `log-id log-id`
 `description description-string`
 `filter filter-id`
 `from {[main] [security] [change] [debug-trace]}`
 `to console`
 `to file file-id`
 `to memory [size]`
 `to session`
 `to snmp [size]`
 `to syslog syslog-id`
 `time-format {local | utc}`
 `no shutdown`

The following displays an example of the log file configuration command syntax:

Example:

```
config# log
config>log# log-id 2
config>log>log-id$ description "This is a test log file."
config>log>log-id# filter 1
config>log>log-id# from main security
config>log>log-id# to file 1
config>log>log-id# no shutdown
config>log>log-id# exit
```

The following displays a log file configuration:

```
ALU-12>config>log>log-id# info
-----
...
    log-id 2
        description "This is a test log file."
        filter 1
        from main security
        to file 1
    exit
...
-----
ALU-12>config>log>log-id#
```

Configuring a File ID

To create a log file, a file ID is defined that specifies the target compact flash drive and the rollover and retention interval period for the file. The rollover interval is defined in minutes and determines how long a file will be used before it is closed and a new log file is created. The retention interval determines how long the file will be stored on the compact flash drive before it is deleted.

Use the following CLI syntax to configure a log file ID:

CLI Syntax:

```
config>log
    file-id log-file-id
    description description-string
    location cflash-id
    rollover minutes [retention hours]
```

The following displays an example of the log file ID configuration command syntax:

Example:

```
config# log
config>log# file-id 1
config>log>file-id# description "This is a log file."
config>log>file-id# location cf3:
config>log>file-id# rollover 600 retention 24
```

The following displays the file ID configuration:

```
ALU-12>config>log# info
-----
      file-id 1
      description "This is a log file."
      location cf3:
      rollover 600 retention 24
      exit
-----
ALU-12>config>log#
```

Configuring an Accounting Policy

Before an accounting policy can be created, a target log file must be created to collect the accounting records. The files are stored in system memory on the compact flash drive in a compressed (tar) XML format and can be retrieved using FTP or SCP. See [Configuring an Event Log](#) and [Configuring a File ID](#).

Accounting policies must be configured in the `config>log` context before they can be applied to a SAP or service interface. For information on associating an accounting policy with a SAP, see the 7705 SAR OS Services Guide.

An accounting policy must define a record type and collection interval. Only one record type can be configured per accounting policy.

When creating accounting policies, one service accounting policy can be defined as default. If statistics collection is enabled on a SAP and no accounting policy is applied, then the respective default policy is used. If no default policy is defined, then no statistics are collected unless a specifically defined accounting policy is applied.

Use the following CLI syntax to configure an accounting policy:

CLI Syntax:

```
config>log>
  accounting-policy acct-policy-id interval minutes
  description description-string
  default
  record record-name
  to file log-file-id
  no shutdown
```

The following displays an example of the accounting policy configuration command syntax:

Example:

```
config>log# accounting-policy 4
config>log>acct-policy# description "This is the default
accounting policy."
config>log>acct-policy# record service-ingress-packets
config>log>acct-policy# default
config>log>acct-policy# to file 1
config>log>acct-policy# exit
config>log# accounting-policy 5
config>log>acct-policy# description "This is a test
accounting policy."
config>log>acct-policy# record service-ingress-packets
config>log>acct-policy# to file 2
config>log>acct-policy#
```

The following displays the accounting policy configuration:

```
ALU-12>config>log# info
-----
    accounting-policy 4
        description "This is the default accounting policy."
        record service-ingress-packets
        default
        to file 1
    exit
    accounting-policy 5
        description "This is a test accounting policy."
        record service-ingress-packets
        to file 2
    exit
-----
ALU-12>config>log#
```

Configuring Event Control

Use the following CLI syntax to configure event control. Note that the **throttle** parameter used in the **event-control** command syntax enables throttling for a specific event type. The **config>log>throttle-rate** command configures the number of events and interval length to be applied to all event types that have throttling enabled by this **event-control** command.

CLI Syntax:

```
config>log
    event-control application-id [event-name |
        event-number] generate[severity-level] [throttle]
    event-control application-id [event-name |
        event-number] suppress
    throttle-rate events [interval seconds]
```

The following displays an example of an event control configuration command syntax:

Example: Config# log
 config>log# event-control atm 2014 generate critical
 config>log# event-control oam 2001 suppress
 config>log# throttle-rate 500 interval 10

The following displays the event control configuration:

```
ALU-12>config>log# info
#-----
echo "Log Configuration"
#-----
      throttle-rate 500 interval 10
      event-control "atm" 2014 generate critical
      event-control "oam" 2001 suppress
..
#-----
ALU-12>config>log>filter#
```

Configuring Throttle Rate

This command configures the number of events and interval length to be applied to all event types that have throttling enabled by the **event-control** command.

Use the following CLI syntax to configure the throttle rate.

CLI Syntax: config>log#
 throttle-rate events [interval *seconds*]

The following displays an example of the configuration command syntax:

Example: config>log# throttle-rate 500 interval 10
 config>log# event-control mpls 2001 generate throttle

The following displays the configuration:

```
*A:gal171>config>log# info
#-----
      throttle-rate 500 interval 10
      event-control "mpls" 2001 generate throttle
#-----
*A:gal171>config>log#
```

Configuring a Log Filter

Use the following CLI syntax to configure a log filter:

CLI Syntax:

```
config>log
    filter filter-id
    default-action {drop | forward}
    description description-string
    entry entry-id
        action {drop | forward}
        description description-string
        match
            application {eq | neq} application-id
            number {eq | neq | lt | lte | gt | gte} event-id
            router {eq | neq} router-instance [regex]
            severity {eq | neq | lt | lte | gt | gte}
            severity-level
            subject {eq | neq} subject [regex]
```

The following displays an example of the log filter configuration command syntax:

Example:

```
Config# log
config>log# filter 1
config>log>filter# description "This is a sample filter."
config>log>filter# default-action drop
config>log>filter# entry 1
config>log>filter>entry$ action forward
config>log>filter>entry# match application eq atm
config>log>filter>entry# match severity eq critical
config>log>filter>entry# exit
```

The following displays the log filter configuration:

```

ALU-12>config>log# info
#-----
echo "Log Configuration "
#-----
    file-id 1
        description "This is our log file."
        location cf3:
        rollover 600 retention 24
    exit
    filter 1
        default-action drop
        description "This is a sample filter."
        entry 1
            action forward
            match
                application eq "atm"
                severity eq critical
            exit
        exit
    exit
...
    log-id 2
        shutdown
        description "This is a test log file."
        filter 1
        from main security
        to file 1
    exit
...
#-----
ALU-12>config>log#

```

Configuring an SNMP Trap Group

The associated *log-id* does not have to be configured before a **snmp-trap-group** can be created; however, the **snmp-trap-group** must exist before the *log-id* can be configured to use it.

Use the following CLI syntax to configure an SNMP trap group:

CLI Syntax:

```
config>log
    snmp-trap-group log-id
    trap-target name [address ip-address] [port port]
    [snmpv1 | snmpv2c | snmpv3] notify-community
    communityName | snmpv3SecurityName [security-level
    {no-auth-no-privacy | auth-no-privacy | privacy}]
```

The following displays an example of the SNMP trap group configuration command syntax:

Example:

```
Config# log
config>log# snmp-trap-group 2
config>log>snmp-trap-group# trap-target "target name"
address 10.10.10.104 notify-community
"communitystring" security-level no-auth-no-privacy
config>log>snmp-trap-group# exit
```

The following displays the SNMP trap group configuration:

```
ALU-12>config>log# info
-----
...
    snmp-trap-group 2
        trap-target "target name" address 10.10.10.104:5 "snmpv3" notify-community
        "communitystring"
        exit
...
    log-id 2
        description "This is a test log file."
        filter 1
        from main security
        to file 1
    exit
...
-----
ALU-12>config>log#
```


Configuring a Syslog Target

Log events cannot be sent to a syslog target host until a valid syslog ID exists.

Use the following CLI syntax to configure a syslog file:

CLI Syntax:

```
config>log
        syslog syslog-id
        description description-string
        address ip-address
        log-prefix log-prefix-string
        port port
        level {emergency | alert | critical | error |
              warning | notice | info | debug}
        facility syslog-facility
```

The following displays an example of the syslog file configuration command syntax:

Example:

```
config# log
config>log# syslog 1
config>log>syslog$ description "This is a syslog file."
config>log>syslog# address 10.10.10.104
config>log>syslog# facility user
config>log>syslog# level warning
```

The following displays the syslog configuration:

```
ALU-12>config>log# info
-----
...
    syslog 1
        description "This is a syslog file."
        address 10.10.10.104
        facility user
        level warning
    exit
...
-----
ALU-12>config>log#
```

Log Management Tasks

This section discusses the following logging tasks:

- [Modifying a Log File](#)
- [Deleting a Log File](#)
- [Modifying a File ID](#)
- [Deleting a File ID](#)
- [Modifying a Syslog ID](#)
- [Deleting a Syslog ID](#)
- [Modifying an SNMP Trap Group](#)
- [Deleting an SNMP Trap Group](#)
- [Modifying a Log Filter](#)
- [Deleting a Log Filter](#)
- [Modifying Event Control Parameters](#)
- [Returning to the Default Event Control Configuration](#)

Modifying a Log File

Use the following CLI syntax to modify a log file:

CLI Syntax: `config>log`
 `log-id log-id`
 `description description-string`
 `filter filter-id`
 `from {[main] [security] [change] [debug-trace]}`
 `to console`
 `to file file-id`
 `to memory [size]`
 `to session`
 `to snmp [size]`
 `to syslog syslog-id}`

The following displays the current log configuration:

```
ALU-12>config>log>log-id# info
-----
...
    log-id 2
        description "This is a test log file."
        filter 1
        from main security
        to file 1
    exit
...
-----
ALU-12>config>log>log-id#
```

The following displays an example of modifying log file parameters:

Example:

```
Config# log
config>log# log-id 2
config>log>log-id# description "Chassis log file."
config>log>log-id# filter 2
config>log>log-id# from security
config>log>log-id# exit
```

The following displays the modified log file configuration:

```
ALU-12>config>log# info
-----
...
    log-id 2
        description "Chassis log file."
        filter 2
        from security
        to file 1
    exit
...
-----
ALU-12>config>log#
```

Deleting a Log File

The log ID must be shut down first before it can be deleted. In a previous example, file 1 is associated with log-id 2.

```
ALU-12>config>log# info
-----
    file-id 1
        description "LocationTest."
        location cf3:
        rollover 600 retention 24
    exit
...
    log-id 2
        description "Chassis log file."
        filter 2
        from security
        to file 1
    exit
...
-----
ALU-12>config>log#
```

Use the following CLI syntax to delete a log file:

CLI Syntax:

```
config>log
    no log-id log-id
    shutdown
```

The following displays an example of deleting a log file:

Example:

```
Config# log
config>log# log-id 2
config>log>log-id# shutdown
config>log>log-id# exit
config>log# no log-id 2
```

Modifying a File ID



Note: When the file-id location parameter is modified, log files are not written to the new location until a rollover occurs or the log is manually cleared. A rollover can be forced by using the **clear>log** command. Subsequent log entries are then written to the new location. If a rollover does not occur or the log is not cleared, the old location remains in effect.

Use the following CLI syntax to modify a file ID :

CLI Syntax:

```
config>log
      file-id log-file-id
      description description-string
      location [cflash-id]
      rollover minutes [retention hours]
```

The following displays the current file ID configuration:

```
ALU-12>config>log# info
-----
      file-id 1
      description "This is a log file."
      location cf3:
      rollover 600 retention 24
      exit
-----
ALU-12>config>log#
```

The following displays an example of modifying file ID parameters:

Example:

```
config# log
config>log# file-id 1
config>log>file-id# description "LocationTest."
config>log>file-id# location cf3:
config>log>file-id# rollover 2880 retention 500
config>log>file-id# exit
```

The following displays the file ID modifications:

```
ALU-12>config>log# info
-----
...
      file-id 1
      description "LocationTest."
      location cf3:
      rollover 2880 retention 500
      exit
...
-----
ALU-12>config>log#
```

Deleting a File ID



Note: All references to the file ID must be deleted before the file ID can be removed.

Use the following CLI syntax to delete a file ID:

CLI Syntax: `config>log`
`no file-id log-file-id`

The following displays an example of deleting a file ID:

Example: `config>log# no file-id 1`

Modifying a Syslog ID

Use the following CLI syntax to modify syslog ID parameters:

CLI Syntax: `config>log`
`syslog syslog-id`
`description description-string`
`address ip-address`
`log-prefix log-prefix-string`
`port port`
`level {emergency | alert | critical | error |`
`warning | notice | info | debug}`
`facility syslog-facility`

The following displays an example of the syslog ID modifications:

Example: `config# log`
`config>log# syslog 1`
`config>log>syslog$ description "Test syslog."`
`config>log>syslog# address 10.10.0.91`
`config>log>syslog# facility mail`
`config>log>syslog# level info`

The following displays the syslog configuration:

```
ALU-12>config>log# info
-----
...
    syslog 1
        description "Test syslog."
        address 10.10.10.91
        facility mail
        level info
    exit
...
-----
ALU-12>config>log#
```

Deleting a Syslog ID



Note: All references to the syslog ID must be deleted before the syslog ID can be removed.

Use the following CLI syntax to delete a syslog ID:

CLI Syntax: `config>log`
 `no syslog syslog-id`

The following displays an example of deleting a syslog ID:

Example: `config# log`
 `config>log# no syslog 1`

Modifying an SNMP Trap Group

Use the following CLI syntax to modify an SNMP trap group:

CLI Syntax: `config>log`
 `snmp-trap-group log-id`
 `trap-target name [address ip-address] [port port]`
 `[snmpv1 | snmpv2c | snmpv3] notify-community`
 `communityName | snmpv3SecurityName [security-level`
 `{no-auth-no-privacy | auth-no-privacy | privacy}]`

The following displays the current SNMP trap group configuration:

```
ALU-12>config>log# info
-----
...
    snmp-trap-group 10
        trap-target 10.10.10.104:5 "snmpv3" notify-community "communitystring"
    exit
...
-----
ALU-12>config>log#
```

The following displays an example of the command usage to modify an SNMP trap group:

Example:

```
Config# log
config>log# snmp-trap-group 10
config>log>snmp-trap-group# no trap-target 10.10.10.104:5
config>log>snmp-trap-group# snmp-trap-group#
trap-target 10.10.0.91:1 snmpv2c notify-community "com1"
```

The following displays the SNMP trap group configuration:

```
ALU-12>config>log# info
-----
...
    snmp-trap-group 10
        trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
    exit
...
-----
ALU-12>config>log#
```

Deleting an SNMP Trap Group

Use the following CLI syntax to delete a trap target and SNMP trap group:

CLI Syntax:

```
config>log
    no snmp-trap-group log-id
    no trap-target name
```

The following displays the SNMP trap group configuration:

```
ALU-12>config>log# info
-----
...
    snmp-trap-group 10
        trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
    exit
...
-----
ALU-12>config>log#
```


The following displays an example of deleting a trap target and an SNMP trap group.

Example:

```
config>log# snmp-trap-group 10
config>log>snmp-trap-group# no trap-target 10.10.0.91:1
config>log>snmp-trap-group# exit
config>log# no snmp-trap-group 10
```

Modifying a Log Filter

Use the following CLI syntax to modify a log filter:

CLI Syntax:

```
config>log
    filter filter-id
    default-action {drop | forward}
    description description-string
    entry entry-id
        action {drop | forward}
        description description-string
        match
            application {eq | neq} application-id
            number {eq | neq | lt | lte | gt | gte} event-id
            router {eq | neq} router-instance [regex]
            severity {eq | neq | lt | lte | gt | gte}
            severity-level
            subject {eq | neq} subject [regex]
```

The following output displays the current log filter configuration:

```
ALU-12>config>log# info
#-----
echo "Log Configuration"
#-----
...
    filter 1
        default-action drop
        description "This is a sample filter."
        entry 1
            action forward
            match
                application eq "atm"
                severity eq critical
            exit
        exit
    exit
...
#-----
ALU-12>config>log#
```

The following displays an example of the log filter modifications:

Example:

```
config# log
config>log# filter 1
config>log>filter# description "This allows <n>."
config>log>filter# default-action forward
config>log>filter# entry 1
config>log>filter>entry$ action drop
config>log>filter>entry# match
config>log>filter>entry>match# application eq user
config>log>filter>entry>match# number eq 2001
config>log>filter>entry>match# no severity
config>log>filter>entry>match# exit
```

The following displays the log filter configuration:

```
ALU-12>config>log>filter# info
-----
...
      description "This allows <n>."
      entry 1
        action drop
        match
          application eq "user"
          number eq 2001
        exit
      exit
    exit
  ...
-----
ALU-12>config>log>filter#
```

Deleting a Log Filter

Use the following CLI syntax to delete a log filter:

CLI Syntax:

```
config>log
      no filter filter-id
```

The following output displays the current log filter configuration:

The following displays an example of the command to delete a log filter:

Example:

```
config>log# no filter 1
```

Modifying Event Control Parameters

Use the following CLI syntax to modify event control parameters:

CLI Syntax: `config>log`
 `event-control application-id [event-name |`
 `event-number] generate[severity-level] [throttle]`
 `event-control application-id [event-name |`
 `event-number] suppress`

The following displays the current event control configuration:

```
ALU-12>config>log# info
-----
...
    event-control "atm" 2014 generate critical
...
-----
ALU-12>config>log#
```

The following displays an example of event control modifications:

Example: `Config# log`
 `config>log# event-control atm 2014 suppress`

The following displays the log filter configuration:

```
ALU-12>config>log# info
-----
...
    event-control "atm" 2014 suppress
...
-----
ALU-12>config>log#
```

Returning to the Default Event Control Configuration

The **no** form of the **event-control** command returns modified values back to the default values.

Use the following CLI syntax to return to the default event control configuration:

CLI Syntax: `config>log`
 `no event-control application [event-name |`
 `event-number]`

The following displays an example of the command usage to return to the default values:

Example: `Config# log`
 `config>log# no event-control "atm" 2014`
 `config>log# no event-control "filter" 2001`
 `config>log# no event-control "mpls" 2001`

```
ALU-12>config>log# info detail
-----
#-----
echo "Log Configuration"
#-----
...
event-control "atm" 2004 generate minor
event-control "atm" 2005 generate warning
event-control "atm" 2006 generate warning
event-control "atm" 2007 generate critical
event-control "atm" 2008 generate warning
event-control "atm" 2009 generate warning
event-control "atm" 2010 generate warning
event-control "atm" 2011 generate warning
event-control "atm" 2012 generate warning
event-control "atm" 2013 generate warning
event-control "atm" 2014 generate warning
event-control "atm" 2015 generate warning
event-control "atm" 2016 generate warning
event-control "atm" 2017 generate warning
...
-----
ALU-12>config>log#
```

Log Command Reference

Command Hierarchies

- Configuration Commands
 - Accounting Policy Commands
 - Event Control Commands
 - Log File Commands
 - Log Filter Commands
 - Log Filter Entry Commands
 - Log Filter Entry Match Commands
 - Syslog Commands
 - Logging Destination Commands
 - SNMP Trap Groups
- Show Commands
- Clear Commands

Configuration Commands

Accounting Policy Commands

```

config
  — log
    — accounting-policy acct-policy-id [interval minutes]
    — no accounting-policy acct-policy-id
      — [no] default
      — description description-string
      — no description
      — record record-name
      — no record
      — [no] shutdown
      — to file file log-file-id

```

Event Control Commands

```

config
  — log
    — event-control application-id [event-name | event-number] generate [severity-level]
      [throttle]
    — event-control application-id [event-name | event-number] suppress
    — no event-control application-id [event-name | event-number]
    — throttle-rate events [interval seconds]
    — no throttle-rate

```

Log File Commands

```

config
  — log
    — [no] file-id log-file-id
      — description description-string
      — no description
      — location cflash-id
      — rollover minutes [retention hours]
      — no rollover

```

Log Filter Commands

```

config
  — log
    — [no] filter filter-id
      — default-action {drop | forward}
      — no default-action
      — description description-string
      — no description

```

Log Filter Entry Commands

```

config
  — log
    — [no] filter filter-id
      — [no] entry entry-id
        — action {drop | forward}
        — no action
        — description description-string
        — no description

```

Log Filter Entry Match Commands

```

config
  — log
    — [no] filter filter-id
      — [no] entry entry-id
        — [no] match
          — application {eq | neq} application-id
          — no application
          — number {eq | neq | lt | lte | gt | gte} event-id
          — no number
          — router {eq | neq} router-instance [regexp]
          — no router
          — severity {eq | neq | lt | lte | gt | gte} severity-level
          — no severity
          — subject {eq | neq} subject [regexp]
          — no subject

```

Syslog Commands

```

config
  — log
    — [no] syslog syslog-id
      — address ip-address
      — no address
      — description description-string
      — no description
      — facility syslog-facility
      — no facility
      — level syslog-level
      — no level
      — log-prefix log-prefix-string
      — no log-prefix
      — port port
      — no port

```

Logging Destination Commands

```

config
  — log
    — log-id
      — [no] to console log-id
      — description description-string
      — no description
      — log-id filter-id
      — no log-id
      — from {[main] [security] [change] [debug-trace]}
      — no from
      — [no] shutdown
      — time-format {local | utc}
      — to console
      — to file log-file-id
      — to memory [size]
      — to session
      — to snmp [size]
      — to syslog syslog-id

```

SNMP Trap Groups

```

config
  — log
    — [no] snmp-trap-group log-id
      — description description-string
      — no description
      — trap-target name [address ip-address] [port port] [snmpv1 | snmpv2c | snmpv3]
      — notify-community {communityName | snmpv3SecurityName} [security-level {no-auth-no-privacy | auth-no-privacy | privacy}]
      — no trap-target name

```

Show Commands

```

show
  — log
    — accounting-policy [acct-policy-id] access
    — accounting-records
    — applications
    — event-control [application-id] [event-name | event-number]
    — file-id [log-file-id]
    — filter-id [filter-id]
    — log-collector
    — log-id [log-id] [severity severity-level] [application application] [sequence from-seq [to-seq]] [count count] [subject subject] [ascending | descending]
    — snmp-trap-group [log-id]
    — syslog [syslog-id]

```


Clear Commands

`clear`
— `log log-id`

Command Descriptions

- [Configuration Commands on page 275](#)
- [Show Commands on page 310](#)
- [Clear Commands on page 329](#)

Configuration Commands

- [Generic Commands on page 276](#)
- [Accounting Policy Commands on page 278](#)
- [Event Control on page 281](#)
- [Log File Commands on page 284](#)
- [Log Filter Commands on page 288](#)
- [Log Filter Entry Commands on page 289](#)
- [Log Filter Entry Match Commands on page 291](#)
- [Syslog Commands on page 296](#)
- [Logging Destination Commands on page 301](#)
- [SNMP Trap Groups on page 307](#)

Generic Commands

description

Syntax	description <i>string</i> no description
Context	config>log>filter <i>filter-id</i> config>log>filter <i>filter-id</i> >entry <i>entry-id</i> config>log>log-id <i>log-id</i> config>log>accounting-policy <i>policy-id</i> config>log>file-id <i>file-id</i> config>log>syslog <i>syslog-id</i> config>log>snmp-trap-group
Description	<p>This command creates a text description stored in the configuration file for a configuration context.</p> <p>The command associates a text string with a configuration context to help identify the content in the configuration file.</p> <p>The no form of the command removes the string from the configuration.</p>
Default	No text description is associated with this configuration.
Parameters	<i>string</i> — The description can contain a string of up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax	[no] shutdown
Context	config>log>log-id <i>log-id</i> config>log>accounting-policy <i>policy-id</i>
Description	<p>This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.</p> <p>The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they can be deleted.</p> <p>The no form of this command administratively enables an entity.</p>
Default	no shutdown

- Special Cases**
- log-id* — When a *log-id* is shut down, no events are collected for the entity. This leads to the loss of event data.
 - policy-id* — When an accounting policy is shut down, no accounting data is written to the destination log ID. Counters in the billing data reflect totals, not increments, so when the policy is re-enabled (**no shutdown**) the counters include the data collected during the period the policy was shut down.

Accounting Policy Commands

accounting-policy

Syntax	accounting-policy <i>policy-id</i> [interval <i>minutes</i>] no accounting-policy <i>policy-id</i>
Context	config>log
Description	<p>This command creates an access accounting policy.</p> <p>An accounting policy defines the accounting records that are created.</p> <p>Access accounting policies are policies that can be applied to one or more service access points (SAPs). Changes made to an existing policy, using any of the sub-commands, are applied immediately to all SAPs where this policy is applied.</p> <p>If an accounting policy is not specified on a SAP, then accounting records are produced in accordance with the access policy designated as the default. For more information, see the default command.</p> <p>The no form of the command deletes the policy from the configuration. The accounting policy cannot be removed unless it is removed from all the SAPs or channels where the policy is applied.</p>
Default	No default accounting policy is defined.
Parameters	<p><i>policy-id</i> — the policy ID that uniquely identifies the accounting policy, expressed as a decimal integer</p> <p>Values 1 to 99</p> <p>interval <i>minutes</i> — the interval, in minutes, in which statistics are collected and written to their destination</p> <p>The default interval for each record type is defined in the record <i>record-name</i> description.</p> <p>Default As defined in the record name description.</p> <p>Values 5 to 120</p>

default

Syntax [no] default

Context config>log>accounting-policy *policy-id*

This command adds the designation that the accounting policy ID is the default access accounting policy to be used with all SAPs without a specified accounting policy.

If no access accounting policy is defined on a SAP, accounting records are produced in accordance with the default access policy. If no default access policy is created, no accounting records will be collected other than the records for the accounting policies that are explicitly configured.

Only one access accounting policy ID can be designated as the default access policy.

The record name must be specified prior to assigning an accounting policy as default.

If a policy is configured as the default policy, then a **no default** command must be issued before a new default policy can be configured.

The **no** form of the command removes the default policy designation from the policy ID. The accounting policy will be removed from all SAPs that do not have this policy explicitly defined.

record

Syntax [no] record *record-name*

Context config>log>accounting-policy *policy-id*

Description This command adds the accounting record type to the accounting policy to be forwarded to the configured accounting file. Each accounting policy can only contain one record name. To obtain a list of all record types that can be configured, use the **show log accounting-records** command.

```
ALU-12>config>log# show log accounting-records
=====
Accounting Policy Records
=====
Record # Record Name                               Def. Interval
-----
1      service-ingress-octets                        5
2      service-egress-octets                         5
3      service-ingress-packets                       5
4      service-egress-packets                        5
=====
ALU-12>config>log#
```

To configure an accounting policy for access ports, select a service record (for example, service-ingress-octets). To change the record name to another service record, re-enter the **record** command with the new record name and it will replace the old record name.

Only one record may be configured in a single accounting policy.



Note: Collecting excessive statistics can adversely affect the CPU utilization and take up large amounts of storage space.

The **no** form of the command removes the record type from the policy.

Default No accounting record is defined.

Parameters *record-name* — the accounting record name

[Table 32](#) lists the accounting record names available and the default collection interval.

Table 32: Accounting Record Names

Record Type	Accounting Record Name	Default Interval
1	service-ingress-octets	5 minutes
2	service-egress-octets	5 minutes
3	service-ingress-packets	5 minutes
4	service-egress-packets	5 minutes

to file

Syntax **to file** *file-id*

Context config>log>accounting-policy *policy-id*

This command specifies the destination for the accounting records selected for the accounting policy.

Default No destination is specified.

Parameters *file-id* — the *file-id* option specifies the destination for the accounting records associated with this accounting policy. The characteristics of the *file-id*, such as rollover and retention intervals, must have already been defined in the **config>log>file-id** context. A *file-id* can only be used once.

The file is generated when the file ID is referenced. This command identifies the type of accounting file to be created. If the **to** command is executed while the accounting policy is in operation, then it becomes active during the next collection interval.

Values 1 to 99

Event Control

event-control

Syntax	event-control <i>application-id</i> [event-name <i>event-number</i>] generate [<i>severity-level</i>] [throttle] event-control <i>application-id</i> [event-name <i>event-number</i>] suppress no event-control <i>application-id</i> [event-name <i>event-number</i>]
Context	config>log
Description	<p>This command is used to specify that a particular event, or all events associated with an application, are either generated or suppressed.</p> <p>Events are generated by an application and contain an event number and description explaining the cause of the event. Each event has a default designation that directs it to be generated or suppressed.</p> <p>Events are generated with a default severity level that can be modified by using the <i>severity-level</i> option.</p> <p>For example, to change event reporting for an external alarm output on the chassis:</p> <ul style="list-style-type: none"> • specify the application: config>log>event-control>chassis • specify the event name or number (to display a list of events, use the show>log>event-control command): config>log>event-control>chassis>extAlarmInput1Detected • specify whether the event is generated or suppressed: config>log>event-control>chassis>extAlarmInput1Detected>generate • change the severity level (for this event, the default is critical): config>log>event-control>chassis>extAlarmInput1Detected>generate>major <p>Events that are suppressed by default are typically used for debugging purposes. Events are suppressed at the time the application requests the event's generation. No event log entry is generated regardless of the destination. While this feature can save processor resources, there may be a negative effect on the ability to troubleshoot problems if the logging entries are not generated. In reverse, the generation of too many events may cause excessive overhead.</p> <p>The rate is set with the throttle-rate command. The throttle parameter enables event throttling for these events.</p> <p>The no form of the command reverts the parameters to the default setting for events for the application or a specific event within the application. The severity, generate, and suppress options will also be reset to the initial values.</p>
Default	Each event has a default suppress or generate state. To display a list of all events and the current configuration use the event control command.

- Parameters** *application-id* — the application whose events are affected by this event control filter
- Default** None, this parameter must be explicitly specified.
- Values** A valid application name. To display a list of valid application names, use the [applications](#) command. Valid applications are:
 aps, atm, bgp, chassis, debug, dhcp, dot1ag, efm_oam, eth-cfm, filter, ip, isis, ldp, logger, mpls, ntp, oam, ospf, port, ppp, ptp, qos, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, vtrr
- event-name* | *event-number* — to generate, suppress, or revert to default for a single event, enter the specific number or event short name. If no event number or name is specified, the command applies to all events in the application. To display a list of all event short names use the **show>log>event-control** command.
- Default** none
- Values** A valid event name or event number.
- generate** — specifies that logger event is created when this event occurs. The generate keyword can be used with two optional parameters, *severity-level* and **throttle**.
- Default** generate
- severity-level* — An ASCII string representing the severity level to associate with the specified generated events
- Default** The system assigned severity level
- Values** One of: cleared, indeterminate, critical, major, minor, warning
- throttle** — specifies whether events of this type will be throttled.
By default, event throttling is off for each specific event type. It must be explicitly enabled for each event type where throttling is desired. This makes backwards compatibility easier to manage.
- suppress** — indicates that the specified events will not be logged. If the **suppress** keyword is not specified, then the events are generated by default.
- Default** generate

throttle-rate

Syntax	throttle-rate <i>events</i> [<i>interval seconds</i>] no throttle-rate
Context	config>log
Description	This command configures an event throttling rate.
Parameters	<p><i>events</i> — specifies the number of log events that can be logged within the specified interval for a specific event. Once the limit has been reached, any additional events of that type will be dropped, and the event drop count will be incremented. At the end of the throttle interval, if any events have been dropped, a trap notification will be sent.</p> <p>Values 10 to 20000</p> <p>Default 500</p> <p><i>interval seconds</i> — specifies the number of seconds that an event throttling interval lasts</p> <p>Values 1 to 60</p> <p>Default 1</p>

Log File Commands

file-id

Syntax	[no] file-id <i>file-id</i>
Context	config>log
Description	This command creates the context to configure a file ID template to be used as a destination for an event log or billing file.

This command defines the file location and characteristics that are to be used as the destination for a log event message stream or accounting and billing information. The file defined in this context is subsequently specified in the **to** command under **log-id** or **accounting-policy** to direct specific logging or billing source streams to the file destination.

A file ID can only be assigned to either one **log-id** or one **accounting-policy**. It cannot be reused for multiple instances. A file ID and associated file definition must exist for each log and billing file that must be stored in the file system.

A file is created when the file ID defined by this command is selected as the destination type for a specific log or accounting record. Log files are collected in a “log” directory. Accounting files are collected in an “act” directory.

The file names for a log are created by the system as summarized in the table below:

File Type	File Name
Log File	<i>logllff-timestamp</i>
Accounting File	<i>actaaff-timestamp</i>

where:

- *ll* is the *log-id*
- *aa* is the accounting *policy-id*
- *ff* is the *file-id*
- the *timestamp* is the actual timestamp when the file is created. The format for the timestamp is *yyyymmdd-hhmmss* where:
 - *yyyy* is the year (for example, 2007)
 - *mm* is the month number (for example, 12 for December)
 - *dd* is the day of the month (for example, 03 for the 3rd of the month)
 - *hh* is the hour of the day in 24-hour format (for example, 04 for 4 a.m.)
 - *mm* is the minutes (for example, 30 for 30 minutes past the hour)
 - *ss* is the number of seconds (for example, 14 for 14 seconds)

- the accounting file is compressed and has a gz extension

When initialized, each file will contain:

- the *log-id* description
- the time the file was opened
- the reason the file was created
- the sequence number of the last event stored on the log (if the event log file was closed properly)

If the process of writing to a log file fails (for example, the compact flash card is full), the log file will not become operational even if the compact flash card is replaced. Enter a **clear log** command or a **shutdown/no shutdown** command to reinitialize the file.

If the location fails (for example, the compact flash card fills up during the write process), a trap is sent.

The **no** form of the command removes the *file-id* from the configuration. A *file-id* can only be removed from the configuration if the file is not the designated output for a log destination. The actual file remains on the file system.

Default	No default file IDs are defined.
Parameters	<i>file-id</i> — the file identification number for the file, expressed as a decimal integer
Values	1 to 99

location

Syntax	location <i>cflash-id</i> no location
Context	config>log>file <i>file-id</i>
Description	This command specifies the location where the log or billing file will be created.

The **location** command is optional. If the location command is not explicitly configured, log and accounting files will be created on cf3: for the 7705 SAR-F and 7705 SAR-8. For the 7705 SAR-18, log files are created by default on cf1: and accounting files are created by default on cf2:. There are no overflows onto other devices.

When multiple location commands are entered in a single file ID context, the last command overwrites the previous command.

When the location of a file ID that is associated with an active log ID is changed, the log events are not immediately written to the new location. The new location does not take effect until the log is rolled over, either because the rollover period has expired or a **clear log log-id** command is entered to manually roll over the log file.

When creating files, the designated location is used as long as there is available space. If no space is available, an attempt is made to delete unnecessary files that are past their retention date.

If sufficient space is not available, an attempt is made to remove the oldest to newest closed log or accounting files. After each file is deleted, the system attempts to create the new file.

A medium severity trap is issued to indicate that the compact flash is either not available or that no space is available on the specified flash.

A high-priority alarm condition is raised if the compact flash device for this file ID is not present or if there is insufficient space available. If space does become available, then the alarm condition will be cleared.

Use the **no** form of this command to revert to default settings.

Default For 7705 SAR-8 and 7705 SAR-F, log and accounting files are created on cf3:
For 7705 SAR-18, log files are created on cf1: and accounting files are created on cf2:

Parameters *cf-flash-id* — specifies the location of the flash

Values cf-flash-id: cf3: for all platforms; cf1: or cf2: for the 7705 SAR-18

rollover

Syntax **rollover** *minutes* [**retention** *hours*]
no rollover

Context config>log>file *file-id*

Description This command configures how often an event or accounting log is rolled over or partitioned into a new file.

An event or accounting log is actually composed of multiple individual files. The system creates a new file for the log based on the **rollover** time, expressed in minutes.

The **retention** option, expressed in hours, allows you to modify the default time to keep the file in the system. The retention time is based on the rollover time of the file. The retention time is used as a factor to determine which files should be deleted first as the file space becomes full.

When multiple **rollover** commands for a *file-id* are entered, the last command overwrites the previous command.

Default **rollover 1440 retention 12**

Parameters **rollover** *minutes* — the rollover time, in minutes

Values 5 to 10080

retention *hours* — the retention period in hours, expressed as a decimal integer. The retention time is based on the creation time of the file. The file becomes a candidate for removal once the creation timestamp + rollover time + retention time is less than the current timestamp.

Values 1 to 500

Log Filter Commands

filter

Syntax	[no] filter <i>filter-id</i>
Context	config>log
Description	<p>This command creates a context for an event filter. An event filter specifies whether to forward or drop an event or trap based on the match criteria.</p> <p>Filters are configured in the filter <i>filter-id</i> context and then applied to a log in the log-id <i>log-id</i> context. Only events for the configured log source streams destined for the log ID where the filter is applied are filtered.</p> <p>Any changes made to an existing filter, using any of the sub-commands, are immediately applied to the destinations where the filter is applied.</p> <p>The no form of the command removes the filter association from log IDs, which causes those logs to forward all events.</p>
Default	No event filters are defined.
Parameters	<i>filter-id</i> — uniquely identifies the filter
Values	1 to 1000

default-action

Syntax	default-action {drop forward} no default-action
Context	config>log>filter <i>filter-id</i>
Description	<p>The default action specifies the action that is applied to events when no action is specified in the event filter entries or when an event does not match the specified criteria.</p> <p>When multiple default-action commands are entered, the last command overwrites the previous command.</p> <p>The no form of the command reverts the default action to the default value.</p>
Default	default-action forward
Parameters	<p>drop — the events that are not explicitly forwarded by an event filter match are dropped</p> <p>forward — the events that are not explicitly dropped by an event filter match are forwarded</p>

Log Filter Entry Commands

action

Syntax	action { drop forward } no action
Context	config>log>filter <i>filter-id</i> >entry <i>entry-id</i>
Description	<p>This command specifies a drop or forward action associated with the filter entry.</p> <p>If neither drop nor forward is specified, the default-action will be used for traffic that conforms to the match criteria. This could be considered a No-Op filter entry used to explicitly exit a set of filter entries without modifying previous actions.</p> <p>When multiple action commands are entered, the last command will overwrite the previous command.</p> <p>The no form of the command removes the specified action statement.</p>
Default	no action
Parameters	<p>drop — specifies that packets matching the entry criteria will be dropped</p> <p>forward — specifies that packets matching the entry criteria will be forwarded</p>

entry

Syntax	[no] entry <i>entry-id</i>
Context	config>log>filter <i>filter-id</i>
Description	<p>This command is used to create or edit an event filter entry. Multiple entries may be created using unique <i>entry-id</i> numbers. The TiMOS implementation exits the filter on the first match found and executes the action in accordance with the action command.</p> <p>Comparisons are performed in an ascending entry ID order. When entries are created, they should be arranged sequentially from the most explicit entry to the least explicit. Matching ceases when a packet matches an entry. The entry action is performed on the packet, either drop or forward. To be considered a match, the packet must meet all the conditions defined in the entry.</p> <p>An entry may have no match criteria defined (in which case, everything matches) but must have at least the action keyword for it to be considered complete. Entries without the action keyword will be considered incomplete and are rendered inactive.</p> <p>The no form of the command removes the specified entry from the event filter. Entries removed from the event filter are immediately removed from all log IDs where the filter is applied.</p>
Default	No event filter entries are defined. An entry must be explicitly configured.

Parameters *entry-id* — uniquely identifies a set of match criteria corresponding action within a filter. Entry ID values should be configured in staggered increments so you can insert a new entry in an existing policy without renumbering the existing entries.

Values 1 to 999

Log Filter Entry Match Commands

match

Syntax	[no] match
Context	config>log>filter <i>filter-id</i> >entry <i>entry-id</i>
Description	<p>This command creates the context to enter or edit match criteria for a filter entry. When the match criteria is satisfied, the action associated with the entry is executed.</p> <p>If more than one match parameter (within one match statement) is specified, then all the criteria must be satisfied and functional before the action associated with the match is executed.</p> <p>Use the applications command to display a list of the valid applications.</p> <p>Match context can consist of multiple match parameters (application, event-number, severity, subject), but multiple match statements cannot be entered per entry.</p> <p>The no form of the command removes the match criteria for the <i>entry-id</i>.</p>
Default	No match context is defined.

application

Syntax	application {eq neq} application-id no application
Context	config>log>filter <i>filter-id</i> >entry <i>entry-id</i> >match
Description	<p>This command adds a TiMOS application as an event filter match criterion.</p> <p>A TiMOS application is the software entity that reports the event. Examples of applications include: IP, MPLS, CLI, and SERVICES. Only one application can be specified per entry.</p> <p>When multiple application commands are entered, the last command will overwrite the previous command.</p> <p>The no form of the command removes the application as a match criterion.</p>
Default	no application

Parameters **eq | neq** — the operator specifying the type of match. Valid operators are listed in the table below.

Operator	Notes
eq	Equal to
neq	Not equal to

application-id — the application name string

Values aps, atm, bgp, chassis, debug, dhcp, dot1ag, efm_oam, eth-cfm, filter, ip, isis, ldp, logger, mpls, ntp, oam, ospf, port, ppp, ptp, qos, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, vtrr

number

Syntax **number {eq | neq | lt | lte | gt | gte} event-id**
no number

Context config>log>filter *filter-id*>entry *entry-id*>match

Description This command adds a TiMOS application event number as a match criterion.

TiMOS event numbers uniquely identify a specific logging event within an application.

Only one **number** command can be entered per event filter entry. If multiple **number** commands are entered, the last command overwrites the previous command.

The **no** form of the command removes the event number as a match criterion.

Default **no event-number**

Parameters **eq | neq | lt | lte | gt | gte** — this operator specifies the type of match. Valid operators are listed in the table below.

Operator	Notes
eq	Equal to
neq	Not equal to
lt	Less than
lte	Less than or equal to
gt	Greater than
gte	Greater than or equal to

event-id — the event ID, expressed as a decimal integer

Values 1 to 4294967295

router

Syntax	router { eq neq } <i>router-instance</i> [regex] no router
Context	config>log>filter>entry>match
Description	This command specifies the log event matches for the router.
Parameters	<p>eq — determines if the matching criteria should be equal to the specified value</p> <p>neq — determines if the matching criteria should not be equal to the specified value</p> <p><i>router-instance</i> — specifies a router name up to 32 characters to be used in the match criteria</p> <p>regex — specifies the type of string comparison to use to determine if the log event matches the value of router command parameters. When the regex keyword is specified, the string in the router command is a regular expression string that will be matched against the subject string in the log event being filtered.</p> <p>When regex keyword is not specified, the subject command string is matched exactly by the event filter.</p>

severity

Syntax	severity { eq neq lt lte gt gte } <i>severity-level</i> no severity
Context	config>log>filter>entry>match
Description	<p>This command adds an event severity level as a match criterion.</p> <p>Only one severity command can be entered per event filter entry. When multiple severity commands are entered, the last command overwrites the previous command.</p> <p>The no form of the command removes the severity match criterion.</p>
Default	no severity

Parameters **eq** | **neq** | **lt** | **lte** | **gt** | **gte** — this operator specifies the type of match. Valid operators are listed in the table below.

Operator	Notes
eq	Equal to
neq	Not equal to
lt	Less than
lte	Less than or equal to
gt	Greater than
gte	Greater than or equal to

severity-level — the ITU severity level number. The following table lists severity levels and corresponding numbers per ITU standards M.3100 X.733 & X.21 severity levels.

Severity Number	Severity Level
1	cleared
2	indeterminate (info)
3	critical
4	major
5	minor
6	warning

subject

Syntax **subject** {**eq** | **neq**} *subject* [**regexp**]
no subject

Context config>log>filter *filter-id*>entry *entry-id*>match

Description This command adds an event subject as a match criterion.

The subject is the entity for which the event is reported, such as a port. In this case, the port-id string would be the subject.

Only one **subject** command can be entered per event filter entry. When multiple **subject** commands are entered, the last command overwrites the previous command.

The **no** form of the command removes the subject match criterion.

Default **no subject**

Parameters **eq | neq** — this operator specifies the type of match. Valid operators are listed in the following table:

Operator	Notes
eq	Equal to
neq	Not equal to

subject — a string used as the subject match criterion.

regex — specifies the type of string comparison to use to determine if the log event matches the value of subject command parameters. When the **regex** keyword is specified, the string in the subject command is a regular expression string that will be matched against the subject string in the log event being filtered.

When **regex** keyword is not specified, the subject command string is matched exactly by the event filter.

Syslog Commands

syslog

Syntax	[no] syslog <i>syslog-id</i>
Context	config>log
Description	<p>This command creates the context to configure a syslog target host that is capable of receiving selected syslog messages from the 7705 SAR.</p> <p>A valid <i>syslog-id</i> must have the target syslog host address configured.</p> <p>A maximum of 10 syslog IDs can be configured.</p> <p>No log events are sent to a syslog target address until the syslog-id has been configured as the log destination (to) in the log-id node.</p>
Default	No syslog IDs are defined.
Parameters	<i>syslog-id</i> — the syslog ID number for the syslog destination, expressed as a decimal integer
Values	1 to 10

address

Syntax	address <i>ip-address</i> no address
Context	config>log>syslog <i>syslog-id</i>
Description	<p>This command associates the syslog target host IP address with the syslog ID.</p> <p>This parameter is mandatory. If no address is configured, syslog data cannot be forwarded to the syslog target host.</p> <p>Only one address can be associated with a <i>syslog-id</i>. If multiple addresses are entered, the last address entered overwrites the previous address.</p> <p>The same syslog target host can be used by multiple log IDs.</p> <p>The no form of the command removes the syslog target host IP address.</p>
Default	no address

Parameters	<i>ip-address</i> — the IP address of the syslog target host		
	Values	<i>ipv4-address</i>	a.b.c.d (host bits must be 0)
		<i>ipv6-address</i>	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0 to FFFF]H d: [0 to 255]D

facility

Syntax	facility <i>syslog-facility</i> no facility
Context	config>log>syslog <i>syslog-id</i>
Description	<p>This command configures the facility code for messages sent to the syslog target host.</p> <p>Multiple syslog IDs can be created with the same target host but each syslog ID can only have one facility code. If multiple facility codes are entered, the last facility code entered overwrites the previous facility code.</p> <p>If multiple facilities need to be generated for a single syslog target host, then multiple log-id entries must be created, each with its own filter criteria to select the events to be sent to the syslog target host with a given facility code.</p> <p>The no form of the command reverts to the default value.</p>
Default	local7
Parameters	<p><i>syslog-facility</i> — the syslog facility name represents a specific numeric facility code. The code should be entered in accordance with the syslog RFC. However, the software will not confirm whether the facility code is valid or invalid for the event type being sent to the syslog target host.</p> <p>Values kernel user mail systemd auth syslogd printer netnews uucp cron authpriv ftp ntp logaudit logalert cron2 local0 local1 local2 local3 local4 local5 local6 local7</p> <p>Valid codes per RFC 3164, <i>The BSD syslog Protocol</i>, are listed in the Table 33.</p>

Table 33: Valid Facility Codes

Numerical Code	Facility Code
0	kernel
1	user
2	mail
3	systemd
4	auth

Table 33: Valid Facility Codes (Continued)

Numerical Code	Facility Code
5	syslogd
6	printer
7	net-news
8	uucp
9	cron
10	auth-priv
11	ftp
12	ntp
13	log-audit
14	log-alert
15	cron2
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

Values 0 to 23

level

- Syntax** **level** syslog-level
no level
- Context** config>log>syslog *syslog-id*
- Description** This command configures the syslog message severity level threshold. All messages with severity level equal to or higher than the threshold are sent to the syslog target host.
- Only a single threshold level can be specified. If multiple **level** commands are entered, the last command will overwrite the previous command.
- The **no** form of the command reverts to the default value.
- Parameters** *syslog-level* — the threshold severity level name. Values are described in [Table 34](#).
- Values** emergency, alert, critical, error, warning, notice, info, debug

Table 34: Threshold Severity Level Values

7705 SAR Severity Level	Syslog Severity Level (highest to lowest)	Configured Severity	Definition
3 critical	0	emergency	System is unusable
	1	alert	Action must be taken immediately
4 major	2	critical	Critical condition
5 minor	3	error	Error condition
6 warning	4	warning	Warning condition
	5	notice	Normal but significant condition
1 cleared 2 indeterminate	6	info	Informational messages
	7	debug	Debug-level messages

Values 0 to 7

log-prefix

Syntax	log-prefix <i>log-prefix-string</i> no log-prefix
Context	config>log>syslog <i>syslog-id</i>
Description	<p>This command adds the string prepended to every syslog message sent to the syslog host.</p> <p>RFC 3164, <i>The BSD syslog Protocol</i>, allows an alphanumeric string (tag) to be prepended to the content of every log message sent to the syslog host. This alphanumeric string can, for example, be used to identify the node that generates the log entry. The software appends a colon (:) and a space to the string and it is inserted in the syslog message after the date stamp and before the syslog message content.</p> <p>Only one string can be entered. If multiple strings are entered, the last string overwrites the previous string. The alphanumeric string can contain lowercase (a-z), uppercase (A-Z) and numeric (0-9) characters.</p> <p>The no form of the command removes the log prefix string.</p>
Default	no log-prefix
Parameters	<i>log-prefix-string</i> — an alphanumeric string of up to 32 characters. Special characters (#, \$, spaces, etc.) cannot be used in the string.

port

Syntax	port <i>value</i> no port
Context	config>log>syslog <i>syslog-id</i>
Description	<p>This command configures the UDP port that will be used to send syslog messages to the syslog target host.</p> <p>The port configuration is needed if the syslog target host uses a port other than the standard UDP syslog port 514.</p> <p>Only one port can be configured. If multiple port commands are entered, the last entered port overwrites the previously entered ports.</p> <p>The no form of the command reverts to default value.</p>
Default	no port
Parameters	<i>value</i> — the configured UDP port number used when sending syslog messages
Values	1 to 65535

Logging Destination Commands

log-id

Syntax	[no] log-id <i>log-id</i>
Context	config>log
Description	<p>This command creates a context to configure destinations for event streams.</p> <p>The log-id context is used to direct events, alarms/traps, and debug information to respective destinations.</p> <p>A maximum of 10 logs can be configured.</p> <p>Before an event can be associated with this <i>log-id</i>, the from command identifying the source of the event must be configured.</p> <p>Only one destination can be specified for a <i>log-id</i>. The destination of an event stream can be an in-memory buffer, console, session, snmp-trap-group, syslog, or file.</p> <p>Use the event-control command to suppress the generation of events, alarms, and traps for all log destinations.</p> <p>An event filter policy can be applied in the <i>log-id</i> context to limit which events, alarms, and traps are sent to the specified <i>log-id</i>.</p> <p>Log-IDs 99 and 100 are created by the agent. Log-ID 99 captures all log messages. Log-ID 100 captures log messages with a severity level of major and above.</p> <p>The no form of the command deletes the log destination ID from the configuration.</p>
Default	No log destinations are defined.
Parameters	<i>log-id</i> — the log ID number, expressed as a decimal integer
Values	1 to 100

filter

Syntax	filter <i>filter-id</i> no filter
Context	config>log>log-id <i>log-id</i>
Description	<p>This command associates an event filter policy with the log destination.</p> <p>The filter command is optional. If no event filter is configured, all events, alarms and traps generated by the source stream will be forwarded to the destination.</p> <p>An event filter policy defines (limits) the events that are forwarded to the destination configured in the <i>log-id</i>. The event filter policy can also be used to select the alarms and traps to be forwarded to a destination snmp-trap-group.</p> <p>The application of filters for debug messages is limited to application and subject only.</p> <p>Accounting records cannot be filtered using the filter command.</p> <p>Only one <i>filter-id</i> can be configured per log destination.</p> <p>The no form of the command removes the specified event filter from the <i>log-id</i>.</p>
Default	no filter
Parameters	<p><i>filter-id</i> — the event filter policy ID is used to associate the filter with the <i>log-id</i> configuration. The event filter policy ID must already be defined in config>log>filter <i>filter-id</i>.</p> <p>Values 1 to 1000</p>

from

Syntax	from {[main] [security] [change] [debug-trace]} no from
Context	config>log>log-id <i>log-id</i>
Description	<p>This command selects the source stream to be sent to a log destination.</p> <p>One or more source streams must be specified. The source of the data stream must be identified using the from command before you can configure the destination using the to command. The from command can identify multiple source streams in a single statement (for example: from main change debug-trace).</p> <p>Only one from command may be entered for a single <i>log-id</i>. If multiple from commands are entered, then the last command entered overwrites the previous command.</p> <p>The no form of the command removes all previously configured source streams.</p>
Default	no from

Parameters	<p>main — instructs all events in the main event stream to be sent to the destination defined in the to command for this destination <i>log-id</i>. The main event stream contains the events that are not explicitly directed to any other event stream. To limit the events forwarded to the destination, configure filters using the filter (log destination) command.</p> <p>security — instructs all events in the security event stream to be sent to the destination defined in the to command for this destination <i>log-id</i>. The security stream contains all events that affect attempts to breach system security such as failed login attempts, attempts to access MIB tables to which the user is not granted access, or attempts to enter a branch of the CLI to which access has not been granted. To limit the events forwarded to the destination, configure filters using the filter (log destination) command.</p> <p>change — instructs all events in the user activity stream to be sent to the destination configured in the to command for this destination <i>log-id</i>. The change event stream contains all events that directly affect the configuration or operation of this node. To limit the events forwarded to the change stream destination, configure filters using the filter (log destination) command.</p> <p>debug-trace — instructs all debug-trace messages in the debug stream to be sent to the destination configured in the to command for this destination <i>log-id</i>. Filters applied to debug messages are limited to application and subject.</p>
-------------------	--

to console

Syntax	to console
Context	config>log>log-id <i>log-id</i>
Description	<p>This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination.</p> <p>This command instructs the events selected for the log ID to be directed to the console. If the console is not connected, then all entries are dropped.</p> <p>The source of the data stream must be specified in the from command prior to configuring the destination with the to command.</p> <p>The to command cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed then recreated.</p>
Default	No destination is specified.

to file

Syntax	to file <i>log-file-id</i>
Context	config>log>log-id <i>log-id</i>
Description	<p>This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination.</p> <p>This command instructs the events selected for the log ID to be directed to a specified file.</p> <p>The source of the data stream must be specified in the from command prior to configuring the destination with the to command.</p> <p>The to command cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed then recreated.</p>
Default	No destination is specified.
Parameters	<i>log-file-id</i> — instructs the events selected for the log ID to be directed to the <i>log-file-id</i> . The characteristics of the <i>log-file-id</i> referenced here must have already been defined in the config>log>file <i>log-file-id</i> context.
Values	1 to 99

to memory

Syntax	to memory [<i>size</i>]
Context	config>log>log-id <i>log-id</i>
Description	<p>This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination.</p> <p>This command instructs the events selected for the log ID to be directed to a memory log. A memory file is a circular buffer. Once the file is full, each new entry replaces the oldest entry in the log.</p> <p>The source of the data stream must be specified in the from command prior to configuring the destination with the to command.</p> <p>The to command cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed then recreated.</p>
Default	No destination is specified.
Parameters	<i>size</i> — indicates the number of events that can be stored in the memory
Default	100
Values	50 to 1024

to session

Syntax	to session
Context	config>log>log-id <i>log-id</i>
Description	<p>This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination.</p> <p>This command instructs the events selected for the log ID to be directed to the current console or telnet session. This command is only valid for the duration of the session. When the session is terminated, the log ID is removed. A log ID with a <i>session</i> destination is not saved in the configuration file.</p> <p>The source of the data stream must be specified in the from command prior to configuring the destination with the to command.</p> <p>The to command cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed then recreated.</p>
Default	No destination is specified.

to snmp

Syntax	to snmp [<i>size</i>]
Context	config>log>log-id <i>log-id</i>
Description	<p>This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination.</p> <p>This command instructs the alarms and traps to be directed to the snmp-trap-group associated with <i>log-id</i>.</p> <p>A local circular memory log is always maintained for SNMP notifications sent to the specified snmp-trap-group for the <i>log-id</i>.</p> <p>The source of the data stream must be specified in the from command prior to configuring the destination with the to command.</p> <p>The to command cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed then recreated.</p>
Default	No destination is specified.

Parameters	<i>size</i> — defines the number of events stored in this memory log
Default	100
Values	50 to 1024

to syslog

Syntax	to syslog <i>syslog-id</i>
Context	config>log>log-id
Description	<p>This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination.</p> <p>This command instructs the alarms and traps to be directed to a specified syslog. To remain consistent with the standards governing syslog, messages to syslog are truncated to 1 kbytes.</p> <p>The source of the data stream must be specified in the from command prior to configuring the destination with the to command.</p> <p>The to command cannot be modified or re-entered. If the log destination needs to be changed or if the maximum size of an SNMP log or memory log needs to be modified, the log ID must be removed then recreated.</p>
Default	No destination is specified.
Parameters	<p><i>syslog-id</i> — instructs the events selected for the log ID to be directed to the <i>syslog-id</i>. The characteristics of the <i>syslog-id</i> referenced here must have been defined in the config>log>syslog <i>syslog-id</i> context.</p> <p>Values 1 to 10</p>

time-format

Syntax	time-format { local utc }
Context	config>log>log-id
Description	This command specifies whether the time should be displayed in local or Coordinated Universal Time (UTC) format.
Default	utc
Parameters	<p>local — specifies that timestamps are written in the system's local time</p> <p>utc — specifies that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.</p>

SNMP Trap Groups

snmp-trap-group

Syntax	[no] snmp-trap-group <i>log-id</i>
Context	config>log
Description	<p>This command creates the context to configure a group of SNMP trap receivers and their operational parameters for a given <i>log-id</i>.</p> <p>A trap group specifies the types of SNMP traps and specifies the log ID that will receive the group of SNMP traps. A trap group must be configured in order for SNMP traps to be sent.</p> <p>To suppress the generation of all alarms and traps, see the event-control command. To suppress alarms and traps that are sent to this <i>log-id</i>, see the filter (log destination) command. Once alarms and traps are generated, they can be directed to one or more SNMP trap groups. Logger events that can be forwarded as SNMP traps are always defined on the main event source.</p> <p>The no form of the command deletes the SNMP trap group.</p>
Default	There are no default SNMP trap groups.
Parameters	<p><i>log-id</i> — the log ID value of a log configured in the to snmp context. Alarms and traps cannot be sent to the trap receivers until a valid <i>log-id</i> exists.</p> <p>Values 1 to 99</p>

trap-target

Syntax	trap-target name [address ip-address] [port port] [snmpv1 snmpv2c snmpv3] notify-community { <i>communityName</i> <i>snmpv3SecurityName</i> } [security-level { no-auth-no-privacy auth-no-privacy privacy }] no trap-target name
Context	config>log>snmp-trap-group <i>log-id</i>
Description	<p>This command adds or modifies a trap receiver and configures the operational parameters for the trap receiver.</p> <p>Before an SNMP trap can be issued to a trap receiver, the to console, snmp-trap-group, and at least one trap-target must be configured.</p>

The `trap-target` command is used to add or remove a trap receiver from an `snmp-trap-group`. The operational parameters specified in the command include:

- the IP address of the trap receiver
- the UDP port used to send the SNMP trap
- SNMP version
- SNMP community name for SNMPv1 and SNMPv2c receivers
- security name and level for SNMPv3 trap receivers

A single **snmp-trap-group** *log-id* can have multiple trap receivers. Each trap receiver can have different operational parameters.

An address can be configured as a trap receiver more than once as long as a different port is used for each instance.

To prevent resource limitations, only configure a maximum of 10 trap receivers.



Note: If the same **trap-target** *name* **port** *port* parameter value is specified in more than one SNMP trap group, each trap destination should be configured with a different **notify-community** value. This allows a trap receiving an application, such as NMS, to reconcile a separate event sequence number stream for each 7705 SAR event log when multiple event logs are directed to the same IP address and port destination.

The **no** form of the command removes the SNMP trap receiver from the SNMP trap group.

Default

No SNMP trap targets are defined.

Parameters

name — specifies the name of the trap target, up to 28 characters in length

address *ip-address* — the IP address of the trap receiver. Only one IP address destination can be specified per trap destination group.

Values	<i>ipv4-address</i>	a.b.c.d (host bits must be 0)
	<i>ipv6-address</i>	x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:d.d.d.d
		x: [0 to FFFF]H
		d: [0 to 255]D

port *port* — the destination UDP port used for sending traps to the destination, expressed as a decimal integer. Only one port can be specified per **trap-target** statement. If multiple traps need to be issued to the same address, multiple ports must be configured.

Default 162

Values 1 to 65535

snmpv1 | **snmpv2c** | **snmpv3** — specifies the SNMP version format to use for traps sent to the trap receiver

The keyword **snmpv1** selects the SNMP version 1 format. When specifying **snmpv1**, the **notify-community** parameter must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv1**, then the **notify-community** parameter must be changed to reflect the community string rather than the *snmpv3securityName* that is used by **snmpv3**.

The keyword **snmpv2c** selects the SNMP version 2c format. When specifying **snmpv2c**, the **notify-community** parameter must be configured for the proper SNMP community string that the trap receiver expects to be present in alarms and traps messages. If the SNMP version is changed from **snmpv3** to **snmpv2c**, then the **notify-community** parameter must be changed to reflect the community string rather than the *security-name* that is used by **snmpv3**.

The keyword **snmpv3** selects the SNMP version 3 format. When specifying **snmpv3**, the **notify-community** parameter must be configured for the SNMP *security-name*. If the SNMP version is changed from **snmpv1** or **snmpv2c** to **snmpv3**, then the **notify-community** parameter must be changed to reflect the *security-name* rather than the community string used by **snmpv1** or **snmpv2c**.

Default snmpv3

Values snmpv1, snmpv2c, snmpv3

notify-community *communityName* | *snmpv3SecurityName* — specifies the community string for **snmpv1** or **snmpv2c**, or the **snmpv3** *security-name*. If no **notify-community** is configured, then no alarms or traps will be issued for the trap destination. If the SNMP version is modified, the **notify-community** must be changed to the proper form for the SNMP version.

community — the community string as required by the **snmpv1** or **snmpv2c** trap receiver. The community string can be an ASCII string up to 32 characters in length.

security-name — the *security-name* as defined in the **config>system>security>user** context for SNMP v3. The *security-name* can be an ASCII string up to 32 characters in length.

security-level {**no-auth-no-privacy** | **auth-no-privacy** | **privacy**} — specifies the required authentication and privacy levels required to access the views configured on this node when configuring an **snmpv3** trap receiver.

The keyword **no-auth-no-privacy** specifies that no authentication and no privacy (encryption) are required.

The keyword **auth-no-privacy** specifies that authentication is required but no privacy (encryption) is required. When this option is configured, the *security-name* must be configured for **authentication**.

The keyword **privacy** specifies that both authentication and privacy (encryption) are required. When this option is configured, the *security-name* must be configured for **authentication** and **privacy**.

Default No default. The security level must be specified when configuring an SNMPv3 trap receiver.

Values no-auth-no-privacy, auth-no-privacy, privacy

Show Commands

accounting-policy

Syntax	<code>accounting-policy [acct-policy-id] access</code>
Context	<code>show>log</code>
Description	This command displays accounting policy information.
Parameters	<p><i>acct-policy-id</i> — the policy ID that uniquely identifies the accounting policy, expressed as a decimal integer</p> <p>Values 1 to 99</p> <p>access — only displays access accounting policies</p>
Output	The following output is an example of accounting policy information, and Table 35 describes the fields.

Sample Output

```
A:ALU-1# show log accounting-policy
=====
Accounting Policies
=====
Policy Type   Def Admin Oper  Intvl   File Record Name
Id           State State
-----
1      access  No  Up    Up    15      1      service-ingress-packets
2      access  Yes Up    Up    15      2      service-ingress-octets
=====
A:ALU-1#

A:ALU-1# show log accounting-policy 10
=====
Accounting Policies
=====
Policy Type   Def Admin Oper  Intvl   File Record Name
Id           State State
-----
10      access  Yes Up    Up    5       3      service-ingress-packets

Description : (Not Specified)

This policy is applied to:
  Svc Id: 100  SAP : 1/1/8:0      Collect-Stats
  Svc Id: 101  SAP : 1/1/8:1      Collect-Stats
  Svc Id: 102  SAP : 1/1/8:2      Collect-Stats
  Svc Id: 106  SAP : 1/1/8:6      Collect-Stats
  Svc Id: 107  SAP : 1/1/8:7      Collect-Stats
  Svc Id: 108  SAP : 1/1/8:8      Collect-Stats
```

```

Svc Id: 109  SAP : 1/1/8:9      Collect-Stats
...
=====
A:ALU-1#

A:ALU-1# show log accounting-policy access
=====
Accounting Policies
=====
Policy Type      Def Admin Oper  Intvl      File Record Name
Id              State State      Id
-----
10      access  Yes Up      Up      5          3      service-ingress-packets
=====
A:ALU-1#

```

Table 35: Accounting Policy Output Fields

Label	Description
Policy ID	The identifying value assigned to a specific policy
Type	Identifies the accounting record type forwarded to the configured accounting file
	access — indicates that the policy is an access accounting policy
	none — indicates no accounting record types assigned
Def	Yes — indicates that the policy is a default access policy
	No — indicates that the policy is not a default access policy
Admin State	Displays the administrative state of the policy
	Up — indicates that the policy is administratively enabled
	Down — indicates that the policy is administratively disabled
Oper State	Displays the operational state of the policy
	Up — indicates that the policy is operationally up
	Down — indicates that the policy is operationally down
Intvl	Displays the interval, in minutes, in which statistics are collected and written to their destination. The default depends on the record name type.
File ID	The log destination
Record Name	The accounting record name that represents the configured record type
This policy is applied to	Specifies the entities that the accounting policy is applied to

accounting-records

- Syntax** accounting-records
- Context** show>log
- Description** This command displays accounting policy record names.
- Output** The following output is an example of accounting policy record information, and [Table 36](#) describes the fields.

Sample Output

```
A: ALU-1# show log accounting-records
=====
Accounting Policy Records
=====
Record # Record Name                               Def. Interval
-----
1         service-ingress-octets                     5
2         service-egress-octets                       5
3         service-ingress-packets                     5
4         service-egress-packets                     5
=====
A:ALU-1#
```

Table 36: Accounting Records Output Fields

Label	Description
Record #	The record ID that uniquely identifies the accounting policy, expressed as a decimal integer
Record Name	The accounting record name
Def. Interval	The default interval, in minutes, in which statistics are collected and written to their destination

applications

Syntax	applications
Context	show>log
Description	This command displays a list of all application names that can be used in event-control and filter commands.

Output Sample Output

```

A:ALU-1# show log applications
=====
Log Event Application Names
=====
Application Name
-----
APS
ATM
BGP
CHASSIS
CPMHWFILTER
DEBUG
DHCP
EFM_OAM
ETH-CFM
FILTER
IP
ISIS
LDP
LOGGER
MPLS
NTP
OAM
OSPF
PORT
PPP
PTP
QOS
ROUTE_POLICY
SECURITY
SNMP
STP
SVCMMGR
SYSTEM
TIP
USER
VRTR

=====
A:ALU-1#

```

event-control

Syntax	event-control [<i>application-id</i>] [<i>event-name</i> <i>event-number</i>]
Context	show>log
Description	This command displays event control settings for events, including whether the event is suppressed or generated and the severity level for the event. If no options are specified, all events, alarms and traps are listed.
Parameters	<p><i>application-id</i> — displays event control for the specified application only</p> <p>Default All applications</p> <p>Values aps, atm, bgp, chassis, debug, dhcp, dot1ag, efm_oam, eth-cfm, filter, ip, isis, ldp, logger, mpls, ntp, oam, ospf, port, ppp, ptp, qos, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, vtrr</p> <p><i>event-name</i> — displays event control for the named application event only</p> <p>Default All events for the application</p> <p><i>event-number</i> — displays event control for the specified application event number only</p> <p>Default All events for the application</p>
Output	The following output is an example of event control information, and Table 37 describes the fields. Because the output is very large, only a sample of the events are shown here.

Sample Output

```
A:gal171# show log event-control
=====
Log Events
=====
Application
ID#      Event Name                               P   g/s      Logged      Dropped
-----
ATM:
  2004  tAtmTcSubLayerDown                     MI   gen        0           0
  2005  tAtmTcSubLayerClear                     MI   gen        0           0
L  2006  atmVclStatusChange                       WA   gen        0           0
...
CHASSIS:
  2001  cardFailure                             MA   gen        4           0
  2002  cardInserted                           MI   gen        3           0
  2003  cardRemoved                             MI   gen        8           0
  2004  cardWrong                             MI   gen        0           0
  2005  EnvTemperatureTooHigh                   MA   gen        0           0
  2007  powerSupplyOverTemp                     CR   gen        0           0
  2008  powerSupplyAcFailure                     CR   gen        0           0
  2009  powerSupplyDcFailure                     CR   gen        0           0
  2010  powerSupplyInserted                       MA   gen        0           0
  2011  powerSupplyRemoved                       MA   gen        0           0
  2012  redPrimaryCPMFail                       CR   gen        0           0
  2016  clearNotification                       MA   gen        0           0
```

2017	syncIfTimingHoldover	CR	gen	0	0	
2018	syncIfTimingHoldoverClear	CR	gen	0	0	
2019	syncIfTimingRef1Alarm	MI	gen	0	0	
2020	syncIfTimingRef1AlarmClear	MI	gen	0	0	
2021	syncIfTimingRef2Alarm	MI	gen	0	0	
2022	syncIfTimingRef2AlarmClear	MI	gen	0	0	
2023	flashDataLoss	MA	gen	0	0	
2024	flashDiskFull	MA	gen	0	0	
2025	softwareMismatch	MA	gen	0	0	
2026	softwareLoadFailed	MA	gen	0	0	
2027	bootloaderMismatch	MA	gen	0	0	
2028	bootromMismatch	MA	gen	0	0	
2029	fpgaMismatch	MA	gen	0	0	
2030	syncIfTimingBITSAlarm	MI	gen	0	0	
2031	syncIfTimingBITSAlarmClear	MI	gen	0	0	
2032	cardUpgraded	MA	gen	0	0	
2033	cardUpgradeInProgress	MA	gen	0	0	
2034	cardUpgradeComplete	MA	gen	0	0	
2050	powerSupplyInputFailure	CR	gen	0	0	
2051	powerSupplyOutputFailure	CR	gen	0	0	
2052	mdaHiBwMulticastAlarm	MI	gen	0	0	
2056	mdaCfgNotCompatible	MA	gen	0	0	
2057	extAlarmInput1Detected	CR	gen	0	0	
2058	extAlarmInput2Detected	MA	gen	0	0	
2059	extAlarmInput3Detected	MA	gen	0	0	
2060	extAlarmInput4Detected	MI	gen	0	0	
2061	extAlarmCleared	MA	gen	0	0	
2062	syncIfTimingExternAlarm	MI	gen	0	0	
2063	syncIfTimingExternAlarmClear	MI	gen	0	0	
2064	cardBgDiagsFault	MI	gen	0	0	
2065	fanCriticalFailure	CR	gen	0	0	
2066	fanMinorFailure	MI	gen	0	0	
2067	cardSyncFileNotPresent	MI	gen	0	0	
2058	tmnxEqMdaXplError	MI	sup	0	0	
...						
DEBUG:						
L	2001	traceEvent	MI	gen	0	0
DOTLAG:						
	2001	dotlagCfmFaultAlarm	MI	gen	0	0
EFM_OAM:						
	2001	tmnxDot3OamPeerChanged	MI	gen	0	0
	2002	tmnxDot3OamLoopDetected	MI	gen	0	0
	2003	tmnxDot3OamLoopCleared	MI	gen	0	0
FILTER:						
	2001	tIPFilterPBRPacketsDrop	WA	gen	0	0
	2002	tFilterEntryActivationFailed	WA	gen	0	0
	2003	tFilterEntryActivationRestored	WA	gen	0	0
IP:						
L	2001	clearRTMError	MI	gen	0	0
L	2002	ipEtherBroadcast	MI	gen	0	0
L	2003	ipDuplicateAddress	MI	gen	0	0
L	2004	ipArpInfoOverwritten	MI	gen	0	0
L	2005	fibAddFailed	MA	gen	0	0
L	2006	qosNetworkPolicyMallocFailed	MA	gen	0	0
L	2007	ipArpBadInterface	MI	gen	0	0
L	2008	ipArpDuplicateIpAddress	MI	gen	0	0
L	2009	ipArpDuplicateMacAddress	MI	gen	0	0
....						

```

USER:
L 2001 cli_user_login          MI  gen      2      0
L 2002 cli_user_logout        MI  gen      1      0
L 2003 cli_user_login_failed   MI  gen      0      0
L 2004 cli_user_login_max_attempts MI  gen      0      0
L 2005 ftp_user_login          MI  gen      0      0
L 2006 ftp_user_logout         MI  gen      0      0
L 2007 ftp_user_login_failed   MI  gen      0      0
L 2008 ftp_user_login_max_attempts MI  gen      0      0
L 2009 cli_user_io             MI  sup      0     48
L 2010 snmp_user_set           MI  sup      0      0
L 2011 cli_config_io           MI  gen     4357      0
=====
A:ALU-1#

```

Table 37: Event Control Output Fields

Label	Description
Application	The application name
ID#	The event ID number within the application L ID# — an “L” in front of an ID represents event types that do not generate an associated SNMP notification. Most events do generate a notification; only the exceptions are marked with a preceding “L”.
Event Name	The event name
P	CL — the event has a cleared severity/priority
	CR — the event has critical severity/priority
	IN — the event has indeterminate severity/priority
	MA — the event has major severity/priority
	MI — the event has minor severity/priority
	WA — the event has warning severity/priority
g/s	gen — the event will be generated/logged by event control
	sup — the event will be suppressed/dropped by event control
	thr — specifies that throttling is enabled
Logged	The number of events logged/generated
Dropped	The number of events dropped/suppressed

file-id

Syntax	file-id [<i>log-file-id</i>]
Context	show>log
Description	<p>This command displays event log file information.</p> <p>If no command line parameters are specified, a summary output of all event log files is displayed.</p> <p>Specifying a file ID displays detailed information on the event log file.</p>
Parameters	<i>log-file-id</i> — displays detailed information on the specified event log file.
Output	The following output is an example of event log file information, and Table 38 describes the fields.

Sample Output

```

A:ALU-1# show log file-id
=====
File Id List
=====
file-id  rollover  retention  admin      backup      oper
         location  location  location
-----
1         60         4         cf3:       none       none
2         60         3         cf3:       none       none
3         1440        12        cf3:       none       none
10        1440        12        cf3:       none       none
11        1440        12        cf3:       none       none
15        1440        12        cf3:       none       none
20        1440        12        cf3:       none       none
=====

A:ALU-1#

A:ALU-1# show log file-id 10
=====
File Id List
=====
file-id  rollover  retention  admin      backup      oper
         location  location  location
-----
10        1440        12        cf3:       none       none
Description : Main
=====

=====
File Id 10 Location cf3:
=====
file name                                expired  state
-----
cf3:\log\log0302-20060501-012205        yes     complete
cf3:\log\log0302-20060501-014049        yes     complete
cf3:\log\log0302-20060501-015344        yes     complete
cf3:\log\log0302-20060501-015547        yes     in progress
=====

```

Table 38: Log File Summary Output Fields

Label	Description
<code>file-id</code>	The log file ID
<code>rollover</code>	The rollover time for the log file, which is the amount of time before the file is partitioned into a new file.
<code>retention</code>	The retention time for the file in the system, which is how long the file should be retained in the file system
<code>admin location</code>	The flash device specified for the file location
	<code>none</code> — indicates no specific flash device was specified
<code>oper location</code>	The actual flash device on which the log file exists
<code>file name</code>	The complete pathname of the file associated with the log ID
<code>expired</code>	Indicates whether or not the retention period for this file has passed
<code>state</code>	<code>in progress</code> — indicates the current open log file
	<code>complete</code> — indicates the old log file

filter-id

Syntax `filter-id [filter-id]`

Context `show>log`

Description This command displays event log filter policy information. If you specify a filter ID, the command also displays the filter match criteria.

Parameters *filter-id* — displays detailed information on the specified event filter policy ID

Output The following outputs are examples of event log filter policy information:

- filter ID summary information ([Sample Output, Table 39](#))
- filter ID information with match criteria specified ([Sample Output, Table 40](#))

Sample Output

```

*A:ALU-48>config>log# show log filter-id
=====
Log Filters
=====
Filter Applied Default Description
Id             Action
-----
1             no      forward
5             no      forward
10            no      forward
1001          yes      drop    Collect events for Serious Errors Log
=====
*A:ALU-48>config>log#

```

Table 39: Filter ID Summary Output Fields

Label	Description
Filter Id	The event log filter ID
Applied	no — the event log filter is not currently in use by a log ID
	yes — the event log filter is currently in use by a log ID
Default Action	drop — the default action for the event log filter is to drop events not matching filter entries
	forward — the default action for the event log filter is to forward events not matching filter entries
Description	The description string for the filter ID

Sample Output

```

*A:ALU-48>config>log# show log filter-id 1001
=====
Log Filter
=====
Filter-id      : 1001      Applied      : yes      Default Action: drop
Description    : Collect events for Serious Errors Log
-----
Log Filter Match Criteria
-----
Entry-id      : 10              Action      : forward
Application   :                  Operator     : off
Event Number  : 0              Operator     : off
Severity      : major          Operator     : greaterThanOrEqual
Subject       :                  Operator     : off
Match Type    : exact string    :
Router        :                  Operator     : off
Match Type    : exact string    :
Description   : Collect only events of major severity or higher
-----
*A:ALU-48>config>log#

```

Table 40: Filter ID Match Criteria Output Fields

Label	Description
Entry-id	The event log filter entry ID
Action	default — there is no explicit action for the event log filter entry and the filter's default action is used on matching events
	drop — the action for the event log filter entry is to drop matching events
	forward — the action for the event log filter entry is to forward matching events
Description (Entry-id)	The description string for the event log filter entry
Application	The event log filter entry application match criterion
Event Number	The event log filter event ID match criterion
Severity	cleared — the event log filter severity match is cleared
	indeterminate — the event log filter entry application event severity indeterminate match criterion
	critical — the event log filter entry application event severity critical match criterion
	major — the event log filter entry application event severity cleared match criterion
	minor — the event log filter entry application event severity minor match criterion
	warning — the event log filter entry application event severity warning match criterion
Subject	Displays the event log filter entry subject string match criterion
Router	Displays the event log filter entry router <i>router-instance</i> string match criterion
Operator	There is an operator field for each match criteria: application, event number, severity, and subject
	equal — matches when equal to the match criterion

Table 40: Filter ID Match Criteria Output Fields (Continued)

Label	Description
	<code>greaterThan</code> — matches when greater than the match criterion
	<code>greaterThanOrEqualTo</code> — matches when greater than or equal to the match criterion
	<code>lessThan</code> — matches when less than the match criterion
	<code>lessThanOrEqualTo</code> — matches when less than or equal to the match criterion
	<code>notEqual</code> — matches when not equal to the match criterion
	<code>off</code> — no operator specified for the match criterion

log-collector

Syntax	log-collector
Context	show>log
Description	This command displays log collector statistics for the main, security, change and debug log collectors.
Output	The following output is an example of log collector statistics, and Table 41 describes the fields.

Sample Output

```

A:ALU-1# show log log-collector
=====
Log Collectors
=====
Main          Logged   : 1224          Dropped   : 0
  Dest Log Id: 99   Filter Id: 0      Status: enabled   Dest Type: memory
  Dest Log Id: 100  Filter Id: 1001   Status: enabled   Dest Type: memory

Security      Logged   : 3          Dropped   : 0

Change        Logged   : 3896       Dropped   : 0

Debug         Logged   : 0          Dropped   : 0

=====
A:ALU-1#

```

Table 41: Log Collector Output Fields

Label	Description
<Collector Name>	Main — the main event stream contains the events that are not explicitly directed to any other event stream
	Security — the security stream contains all events that affect attempts to breach system security, such as failed login attempts, attempts to access MIB tables to which the user is not granted access or attempts to enter a branch of the CLI to which access has not been granted
	Change — the change event stream contains all events that directly affect the configuration or operation of this node
	Debug — the debug-trace stream contains all messages in the debug stream
Dest. Log ID	Specifies the event log stream destination
Filter ID	The value is the index to the entry that defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.
Status	Enabled — logging is enabled
	Disabled — logging is disabled
Dest. Type	Console — a log created with the console type destination displays events to the physical console device Events are displayed to the console screen whether a user is logged in to the console or not. A user logged in to the console device or connected to the CLI via a remote telnet or SSH session can also create a log with a destination type of 'session'. Events are displayed to the session device until the user logs off. When the user logs off, the 'session' type log is deleted.
	Syslog — all selected log events are sent to the syslog address
	SNMP traps — events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables
	File — all selected log events are directed to a file on the CSM's compact flash disk
	Memory — all selected log events are directed to an in-memory storage area

log-id

Syntax	log-id [<i>log-id</i>] [severity <i>severity-level</i>] [application <i>application</i>] [sequence <i>from-seq</i> [<i>to-seq</i>]] [count <i>count</i>] [router router-instance [<i>expression</i>]] [subject <i>subject</i> [<i>regexp</i>]] [ascending descending]
Context	show>log
Description	<p>This command displays an event log summary with settings and statistics or the contents of a specific log file, SNMP log, or memory log.</p> <p>If the command is specified with no command line options, a summary of the defined system logs is displayed. The summary includes log settings and statistics.</p> <p>If the log ID of a memory, SNMP, or file event log is specified, the command displays the contents of the log. Additional command line options control what and how the contents are displayed.</p> <p>Contents of logs with console, session or syslog destinations cannot be displayed. The actual events can only be viewed on the receiving syslog or console device.</p>
Parameters	<p><i>log-id</i> — displays the contents of the specified log file or memory log ID. The log ID must have a destination of an SNMP or log file or a memory log for this parameter to be used.</p> <p>Default Displays the event log summary</p> <p>Values 1 to 99</p> <p><i>severity severity-level</i> — displays only events with the specified and higher severity</p> <p>Default All severity levels</p> <p>Values cleared, indeterminate, critical, major, minor, and warning</p> <p><i>application application</i> — displays only events generated by the specified application</p> <p>Default All applications</p> <p>Values aps, atm, bgp, chassis, debug, dhcp, dot1ag, efm_oam, eth-cfm, filter, ip, isis, ldp, logger, mpls, ntp, oam, ospf, port, ppp, ptp, qos, route_policy, rsvp, security, snmp, stp, svcmgr, system, user, vrrtr</p> <p><i>sequence from-seq [to-seq]</i> — displays the log entry numbers from a particular entry sequence number (<i>from-seq</i>) to another sequence number (<i>to-seq</i>). The <i>to-seq</i> value must be larger than the <i>from-seq</i> value.</p> <p>If the <i>to-seq</i> number is not provided, the log contents to the end of the log are displayed unless the count parameter is present, in which case the number of entries displayed is limited by the count.</p> <p>Default All sequence numbers</p> <p>Values 1 to 4294967295</p> <p>count count — limits the number of log entries displayed to the number specified</p> <p>Default All log entries</p> <p>Values 1 to 4294967295</p>

router-instance — specifies a router name up to 32 characters to be used in the display criteria

expression — specifies to use a regular expression as match criteria for the router instance string

subject *subject* — displays only log entries matching the specified text *subject* string. The subject is the object affected by the event; for example, the port-id would be the subject for a link-up or link-down event.

regexp — specifies to use a regular expression as parameters with the specified *subject* string

ascending | **descending** — specifies the log sort direction. Logs are normally shown from the newest entry to the oldest in **descending** sequence number order on the screen. When using the **ascending** parameter, the log will be shown from the oldest to the newest entry.

Default Descending

Output The following output is an example of event log summary information, and [Table 42](#) describes the fields.

Sample Output

```
A:ALU-1# show log log-id
=====
Event Logs
=====
Log Source      Filter Admin Oper  Logged  Dropped Dest      Dest  Size
Id             Id       State State                Type      Id
-----
1   none       none    up    down    52      0      file      10    N/A
2   C          none    up    up      41      0      syslog    1     N/A
99  M          none    up    up      2135    0      memory    500
=====
A:ALU-1#
```

Table 42: Log ID Output Fields

Label	Description
Log Id	An event log destination
Source	no — the event log filter is not currently in use by a log ID
	yes — the event log filter is currently in use by a log ID
Filter ID	The value is the index to the entry that defines the filter to be applied to this log's source event stream to limit the events output to this log's destination. If the value is 0, then all events in the source log are forwarded to the destination.
Admin State	Up — indicates that the administrative state is up
	Down — indicates that the administrative state is down

Table 42: Log ID Output Fields (Continued)

Label	Description
Oper State	Up — indicates that the operational state is up
	Down — indicates that the operational state is down
Logged	The number of events that have been sent to the log source(s) that were forwarded to the log destination
Dropped	The number of events that have been sent to the log source(s) that were not forwarded to the log destination because they were filtered out by the log filter
Dest. Type	Console — all selected log events are directed to the system console. If the console is not connected, then all entries are dropped.
	Syslog — all selected log events are sent to the syslog address
	SNMP traps — events defined as SNMP traps are sent to the configured SNMP trap destinations and are logged in NOTIFICATION-LOG-MIB tables
	File — all selected log events are directed to a file on the CSM's compact flash disk
	Memory — all selected log events are directed to an in-memory storage area
Dest ID	The event log stream destination
Size	The allocated memory size for the log
Time format	<p>The time format specifies the type of timestamp format for events sent to logs where the log ID destination is either syslog or file.</p> <p>When the time format is UTC, timestamps are written using the Coordinated Universal Time value.</p> <p>When the time format is local, timestamps are written in the system's local time.</p>

Sample Memory or File Event Log Contents Output

```
A:gal171# show log log-id 99
=====
Event Log 99
=====
Description : Default System Log
Memory Log contents [size=500 next event=3722 (wrapped)]

3721 2008/02/07 09:14:06.69 UTC WARNING: SYSTEM #2006 Base LOGGER
"Log File Id 2 configuration modified"

3720 2008/02/07 09:13:18.86 UTC WARNING: SYSTEM #2006 Base LOGGER
"Log File Id 2 configuration modified"

3719 2008/02/01 11:54:15.67 UTC MINOR: IP #2004 management PIP MANAGEMENT
"ARP information overwritten for 138.120.52.253 by 00:e0:52:d4:a5:00"

3718 2008/02/01 11:54:15.40 UTC MINOR: IP #2004 management PIP MANAGEMENT
"ARP information overwritten for 138.120.52.253 by 00:e0:5e:00:a5:00"

...
=====
A:gal171
```

snmp-trap-group

Syntax	snmp-trap-group [<i>log-id</i>]
Context	show>log
Description	This command displays SNMP trap group configuration information.
Parameters	<i>log-id</i> — displays only SNMP trap group information for the specified trap group log ID
	Values 1 to 99
Output	The following output is an example of SNMP trap group information, and Table 43 describes the fields.

Sample Output

```
*A:ALU-48>config>log# show log snmp-trap-group
=====
SNMP Trap Groups
=====
id      name
port    address
-----
29      name
162     10.20.30.10
=====
*A:ALU-48>config>log#
```

Table 43: SNMP Trap Group Output Fields

Label	Description
Log-ID	The log destination ID for an event stream
Address	The IP address of the trap receiver
Port	The destination UDP port used for sending traps to the destination, expressed as a decimal integer
Version	Specifies the SNMP version format to use for traps sent to the trap receiver. Valid values are <code>snmpv1</code> , <code>snmpv2c</code> , <code>snmpv3</code> .
Community	The community string required by snmpv1 or snmpv2c trap receivers
Security-Level	The required authentication and privacy levels required to access the views on this node

syslog

Syntax **syslog** [*syslog-id*]

Context `show>log`

Description This command displays syslog event log destination summary information or detailed information on a specific syslog destination.

Parameters *syslog-id* — displays detailed information on the specified syslog event log destination

Values 1 to 10

Output The following output is an example of syslog event log destination summary information, and [Table 44](#) describes the fields.

Sample Output

```
*A:ALU-48>config>log# show log syslog
=====
Syslog Target Hosts
=====
```

Id	Ip Address	Port	Sev Level
	Below Level Drop	Facility	Pfx Level
2	unknown	514	info
	0	local7	yes
3	unknown	514	info
	0	mail	yes

```
=====
*A:ALU-48>config>log#
```

```

*A:ALU-48>config>log# show log syslog 1
=====
Syslog Target 1
=====
IP Address       : 192.168.15.22
Port             : 514
Log-ids          : none
Prefix           : Sr12
Facility         : mail
Severity Level   : info
Prefix Level     : yes
Below Level Drop : 0
Description      : Linux Station Springsteen
=====
*A:ALU-48>config>log#

```

Table 44: Syslog Output Fields

Label	Description
Syslog ID	The syslog ID number for the syslog destination
IP Address	The IP address of the syslog target host
Port	The configured UDP port number used when sending syslog messages
Facility	The facility code for messages sent to the syslog target host
Severity Level	The syslog message severity level threshold
Below Level Dropped	A count of messages not sent to the syslog collector target because the severity level of the message was above the configured severity. The higher the level, the lower the severity.
Prefix Present	Yes — a log prefix was prepended to the syslog message sent to the syslog host
	No — a log prefix was not prepended to the syslog message sent to the syslog host
Description	A text description stored in the configuration file for a configuration context
LogPrefix	The prefix string prepended to the syslog message
Log-id	Events are directed to this destination

Clear Commands

log

Syntax	log <i>log-id</i>
Context	clear
Description	<p>This command reinitializes/rolls over the specified memory log or log file. Memory logs are reinitialized and cleared of contents. Log files are manually rolled over by this command.</p> <p>This command is only applicable to event logs that are directed to file destinations and memory destinations.</p> <p>SNMP, syslog and console/session logs are not affected by this command.</p>
Parameters	<i>log-id</i> — the event log ID to be initialized/rolled over
Values	1 to 100

Standards and Protocol Support

Standards Compliance

IEEE 802.1ag	Service Layer OAM
IEEE 802.1p/q	VLAN Tagging
IEEE 802.3	10BaseT
IEEE 802.3ah	Ethernet OAM
IEEE 802.3u	100BaseTX
IEEE 802.3x	Flow Control
IEEE 802.3z	1000BaseSX/LX
IEEE 802.3-2008	Revised base standard
ITU-T Y.1731	OAM functions and mechanisms for Ethernet-based networks

Telecom Compliance

IC CS-03 Issue 9	Spectrum Management and Telecommunications
ACTA TIA-968-A	
AS/ACIF S016 (Australia/New Zealand)	Requirements for Customer Equipment for connection to hierarchical digital interfaces
ITU-T G.703	Physical/electrical characteristics of hierarchical digital interfaces
ITU-T G.707	Network node interface for the Synchronous Digital Hierarchy (SDH)
ITU-T G.712-2001	Transmission performance characteristics of pulse code modulation channels
ITU-T G.957	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy
ITU-T V.24	List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit- terminating equipment (DCE)
ITU-T V.36	Modems for synchronous data transmission using 60-108 kHz group band circuits
ITU-T X.21	Interface between Data Terminal Equipment and Data Circuit- Terminating Equipment for Synchronous Operation on Public Data Networks

Protocol Support

ATM

RFC 2514	Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management, February 1999
RFC 2515	Definition of Managed Objects for ATM Management, February 1999
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
af-tm-0121.000	Traffic Management Specification Version 4.1, March 1999
ITU-T Recommendation I.610	B-ISDN Operation and Maintenance Principles and Functions version 11/95
ITU-T Recommendation I.432.1	B-ISDN user- network interface - Physical layer specification: General characteristics
GR-1248-CORE	Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3 June 1996
GR-1113-CORE	Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994
AF-PHY-0086.001	Inverse Multiplexing for ATM (IMA)

BFD

draft-ietf-bfd-mib-00.txt	Bidirectional Forwarding Detection Management Information Base
draft-ietf-bfd-base-o5.txt	Bidirectional Forwarding Detection
draft-ietf-bfd-v4v6-1hop-06.txt	BFD IPv4 and IPv6 (Single Hop)
draft-ietf-bfd-multihop-06.txt	BFD for Multi-hop Paths

BGP

- RFC 1397 BGP Default Route Advertisement
- RFC 1997 BGP Communities Attribute
- RFC 2385 Protection of BGP Sessions via MDS
- RFC 2439 BGP Route Flap Dampening
- RFC 2547bis BGP/MPLS VPNs
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3392 Capabilities Advertisement with BGP-4
- RFC 4271 BGP-4 (previously RFC 1771)
- RFC 4360 BGP Extended Communities Attribute
- RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2574bis BGP/MPLS VPNs)
- RFC 4456 BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 and RFC 2796)
- RFC 4724 Graceful Restart Mechanism for BGP - GR Helper
- RFC 4760 Multi-protocol Extensions for BGP (previously RFC 2858)
- RFC 4893 BGP Support for Four-octet AS Number Space

DHCP/DHCPv6

- RFC 1534 Interoperation between DHCP and BOOTP
- RFC 2131 Dynamic Host Configuration Protocol (REV)
- RFC 3046 DHCP Relay Agent Information Option (Option 82)
- RFC 3315 Dynamic Host Configuration Protocol for IPv6

DIFFERENTIATED SERVICES

- RFC 2474 Definition of the DS Field in the IPv4 and IPv6 Headers
- RFC 2597 Assured Forwarding PHB Group
- RFC 2598 An Expedited Forwarding PHB
- RFC 3140 Per-Hop Behavior Identification Codes

DIGITAL DATA NETWORK MANAGEMENT V.35

RS-232 (also known as EIA/TIA-232)

GRE

- RFC 2784 Generic Routing Encapsulation (GRE)

IPv6

- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2462 IPv6 Stateless Address Autoconfiguration
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4291 IPv6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
- RFC 4649 DHCPv6 Relay Agent Remote-ID Option
- RFC 4861 Neighbor Discovery for IP version 6 (IPv6)

LDP

- RFC 5036 LDP Specification

IS-IS

- RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
- RFC 1195 Use of OSI IS-IS for routing in TCP/IP & dual environments
- RFC 2763 Dynamic Hostname Exchange for IS-IS
- RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
- RFC 3719 Recommendations for Interoperable Networks using IS-IS
- RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
- RFC 3787 Recommendations for Interoperable IP Networks
- RFC 4205 for Shared Risk Link Group (SRLG) TLV draft-ietf-isis-igp-p2p-over-lan-05.txt
- RFC 5309 Point-to-Point Operation over LAN in Link State Routing Protocols

MPLS

- RFC 3031 MPLS Architecture
- RFC 3032 MPLS Label Stack Encoding
- RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
- RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

NETWORK MANAGEMENT

- ITU-T X.721: Information technology- OSI-Structure of Management Information
- ITU-T X.734: Information technology- OSI-Systems Management: Event Report Management Function
- M.3100/3120 Equipment and Connection Models
- TMF 509/613 Network Connectivity Model
- RFC 1157 SNMPv1
- RFC 1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis
- RFC 1850 OSPF-MIB
- RFC 1907 SNMPv2-MIB
- RFC 2011 IP-MIB
- RFC 2012 TCP-MIB
- RFC 2013 UDP-MIB
- RFC 2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- RFC 2096 IP-FORWARD-MIB
- RFC 2138 RADIUS
- RFC 2206 RSVP-MIB
- RFC 2571 SNMP-FRAMEWORKMIB
- RFC 2572 SNMP-MPD-MIB
- RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
- RFC 2574 SNMP-USER-BASED-SMMIB
- RFC 2575 SNMP-VIEW-BASED ACM-MIB
- RFC 2576 SNMP-COMMUNITY-MIB
- RFC 2588 SONET-MIB
- RFC 2665 EtherLike-MIB
- RFC 2819 RMON-MIB
- RFC 2863 IF-MIB
- RFC 2864 INVERTED-STACK-MIB
- RFC 3014 NOTIFICATION-LOG MIB
- RFC 3164 The BSD Syslog Protocol
- RFC 3273 HCRMON-MIB
- RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

- RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413 Simple Network Management Protocol (SNMP) Applications
- RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3418 SNMP MIB
- draft-ietf-disman-alarm-mib-04.txt
- draft-ietf-mpls-ldp-mib-07.txt
- draft-ietf-ospf-mib-update-04.txt
- draft-ietf-mpls-lsr-mib-06.txt
- draft-ietf-mpls-te-mib-04.txt
- IANA-IFType-MIB

OSPF

- RFC 1765 OSPF Database Overflow
- RFC 2328 OSPF Version 2
- RFC 2370 Opaque LSA Support
- RFC 3101 OSPF NSSA Option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3630 Traffic Engineering (TE) Extensions to OSPF
- RFC 4203 Shared Risk Link Group (SRLG) sub-TLV

PPP

- RFC 1332 PPP Internet Protocol Control Protocol (IPCP)
- RFC 1570 PPP LCP Extensions
- RFC 1619 PPP over SONET/SDH
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1662 PPP in HDLC-like Framing
- RFC 1989 PPP Link Quality Monitoring
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 2686 The Multi-Class Extension to Multi-Link PPP

PSEUDOWIRES

- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
- RFC 4385 Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- RFC 4446 IANA Allocation for PWE3
- RFC 4447 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)

RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
RFC 4717 Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
draft-ietf-pwe3-redundancy-02 Pseudowire (PW) Redundancy

RADIUS

RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

RSVP-TE and FRR

RFC 2430 A Provider Architecture for DiffServ & TE
RFC 2961 RSVP Refresh Overhead Reduction Extensions
RFC 2702 Requirements for Traffic Engineering over MPLS
RFC 2747 RSVP Cryptographic Authentication
RFC 3097 RSVP Cryptographic Authentication - Updated Message Type Value
RFC 3209 Extensions to RSVP for LSP Tunnels
RFC 3210 Applicability Statement for Extensions to RSVP for LSP Tunnels
RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels

SONET/SDH

GR-253-CORE SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000
ITU-T Recommendation G.841 Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

SSH

draft-ietf-secsh-architecture.txt SSH Protocol Architecture
draft-ietf-secsh-userauth.txt SSH Authentication Protocol
draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
draft-ietf-secsh-connection.txt SSH Connection Protocol
draft-ietf-secsh-newmodes.txt SSH Transport Layer Encryption Modes

SYNCHRONIZATION

G.813 Timing characteristics of SDH equipment slave clocks (SEC)
G.8261 Timing and synchronization aspects in packet networks
G.8262 Timing characteristics of synchronous Ethernet equipment slave clock
GR 1244 CORE Clocks for the Synchronized Network: Common Generic Criteria
IEEE 1588v2 1588 PTP 2008

TACACS+

IETF draft-grant-tacacs-02.txt The TACACS+ Protocol

TCP/IP

RFC 768 User Datagram Protocol
RFC 791 Internet Protocol
RFC 792 Internet Control Message Protocol
RFC 793 Transmission Control Protocol
RFC 826 Ethernet Address Resolution Protocol
RFC 854 Telnet Protocol Specification
RFC 1350 The TFTP Protocol (Rev. 2)
RFC 1812 Requirements for IPv4 Routers

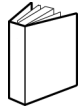
VPLS

RFC 4762 Virtual Private LAN Services Using LDP

Proprietary MIBs

TIMETRA-ATM-MIB.mib
TIMETRA-CAPABILITY-7705-V1.mib
TIMETRA-CFLOWD-MIB.mib
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-LDP-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MPLS-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-PPP-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-ROUTE-POLICY-MIB.mib
TIMETRA-RSVP-MIB.mib
TIMETRA-SAP-MIB.mib
TIMETRA-SDP-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib

Customer documentation and product support



Customer documentation

<http://www.alcatel-lucent.com/myaccess>

Product manuals and documentation updates are available at [alcatel-lucent.com](http://www.alcatel-lucent.com). If you are a new user and require access to this service, please contact your Alcatel-Lucent sales representative.



Technical Support

<http://support.alcatel-lucent.com>



Documentation feedback

documentation.feedback@alcatel-lucent.com

