# Table of Contents

Configuring Password Management Parameters .................................................. 55  
Configuring Profiles ......................................................................................... 56  
Configuring Users .............................................................................................. 57  
Configuring Keychains ...................................................................................... 58  
Copying and Overwriting Users and Profiles ....................................................... 59  
  User .................................................................................................................. 59  
  Profile ................................................................................................ .......... 61  
RADIUS Configurations ...................................................................................... 63  
  Configuring RADIUS Authentication ............................................................. 63  
  Configuring RADIUS Authorization ............................................................... 64  
  Configuring RADIUS Accounting ................................................................. 65  
Configuring 802.1x RADIUS Policies ................................................................. 66  
TACACS+ Configurations .................................................................................... 67  
  Enabling TACACS+ Authentication ............................................................... 67  
  Configuring TACACS+ Authorization ............................................................ 68  
  Configuring TACACS+ Accounting ............................................................... 69  
  Enabling SSH ................................................................................................. 70  
Configuring Login Controls .............................................................................. 71  
Security Command Reference ......................................................................... 73  
  Command Hierarchies ....................................................................................... 73  
  Configuration Commands ................................................................................ 73  

## SNMP

SNMP Overview .................................................................................................. 150  
  SNMP Architecture ....................................................................................... 150  
  Management Information Base ..................................................................... 150  
  SNMP Protocol Operations .......................................................................... 151  
  SNMP Versions .............................................................................................. 151  
  Management Information Access Control ..................................................... 152  
  User-Based Security Model Community Strings .......................................... 153  
  Views .............................................................................................................. 153  
  Access Groups .............................................................................................. 153  
  Users .............................................................................................................. 154  
Which SNMP Version to Use? .......................................................................... 155  
Configuration Notes ......................................................................................... 157  
  General ...................................................................................................... 157  
Configuring SNMP with CLI ........................................................................... 159  
  SNMP Configuration Overview .................................................................... 160  
  Configuring SNMPv1 and SNMPv2c ............................................................ 160  
  Configuring SNMPv3 .................................................................................... 160  
Basic SNMP Security Configuration .................................................................. 161  
Configuring SNMP Components ..................................................................... 162  
  Configuring a Community String ................................................................. 163  
  Configuring View Options ............................................................................ 164  
  Configuring Access Options ........................................................................ 165  
  Configuring USM Community Options ......................................................... 167  
  Configuring Other SNMP Parameters .......................................................... 168
# Table of Contents

SNMP Command Reference .................................................. 169  
Command Hierarchies ......................................................... 169  
Configuration Commands .................................................. 169  

## Event and Accounting Logs

Logging Overview .............................................................. 196  
Log Destinations .............................................................. 198  
Console ............................................................................. 198  
Session .............................................................................. 198  
Memory Logs ....................................................................... 198  
Log Files ............................................................................ 199  
SNMP Trap Group ............................................................... 201  
Syslog .............................................................................. 201  

## Event Logs

Event Sources ........................................................................ 204  
Event Control ....................................................................... 206  
Log Manager and Event Logs .................................................. 208  
Event Filter Policies .............................................................. 209  
Event Log Entries ................................................................ 210  
Simple Logger Event Throttling ................................................ 212  
Default System Log ............................................................... 213  

## Accounting Logs

Accounting Records ............................................................... 214  
Reporting and Time-Based Accounting ................................... 217  

Configuration Notes ............................................................. 218  
Configuring Logging with CLI ............................................... 219  

Log Configuration Overview .................................................. 220  
Log Types .......................................................................... 220  

## Basic Event Log Configuration

Common Configuration Tasks .................................................. 221  
Configuring an Event Log ..................................................... 222  
Configuring a File ID ............................................................ 224  
Configuring an Accounting Policy ........................................... 225  
Configuring Event Control .................................................... 226  
Configuring Throttle Rate ..................................................... 227  
Configuring a Log Filter ....................................................... 228  
Configuring an SNMP Trap Group ......................................... 229  
Configuring a Syslog Target .................................................. 230  

## Log Management Tasks

Modifying a Log File ............................................................. 231  
Deleting a Log File .............................................................. 232  
Modifying a File ID .............................................................. 234  
Deleting a File ID ............................................................... 235  
Modifying a Syslog ID .......................................................... 236  
Deleting a Syslog ............................................................... 237  
Modifying an SNMP Trap Group ............................................ 238  
Deleting an SNMP Trap Group .............................................. 239  
Modifying a Log Filter .......................................................... 240  
Modifying a Log Filter .......................................................... 241  

---

7210 SAS-E OS System Management Guide  Page 5
## LIST OF TABLES

### Getting Started
Table 1: Configuration Process ................................................................. 13

### Security
Table 2: Supported Authorization Configurations ........................................ 22
Table 3: Security Methods Capabilities ....................................................... 26
Table 4: Keychain Mapping .................................................................. 42
Table 5: Security Configuration Requirements ........................................... 52
Table 6: Show System Security Access Group Output Fields ......................... 131
Table 7: Show System Security Authentication Output Fields ....................... 132
Table 8: Show Communities Output Fields .................................................. 134
Table 9: Show Management Access Filter Output Fields ............................. 136
Table 10: Show Management Access Filter Output Fields ............................ 137
Table 11: Show User Profile Output Fields ................................................... 139
Table 12: Show Source Address Output Fields ............................................. 140
Table 13: Show View Output Fields ............................................................ 144
Table 14: Show Users Output Fields ............................................................ 146

### SNMP
Table 15: Counters Output Fields ............................................................ 179
Table 16: Show System Information Output Fields ........................................ 180
Table 17: Show System Information Output Fields ........................................ 184
Table 18: Show Communities Output Fields ................................................ 187
Table 19: Show SSH Output Fields ............................................................. 191
Table 20: Show User Output Fields ............................................................. 192
Table 21: Show System Security View Output Fields ................................... 193

### Event and Accounting Logs
Table 22: Event Severity Levels ............................................................... 196
Table 23: 7210 SAS-Series to Syslog Severity Level Mappings ...................... 202
Table 24: Valid Filter Policy Operators ....................................................... 209
Table 25: Log Entry Field Descriptions ....................................................... 210
Table 26: Accounting Record Name and Collection Periods .......................... 214
Table 27: Accounting Record Name Details ................................................ 215
Table 28: Show Accounting Policy Output Fields ......................................... 285
Table 29: Accounting Policy Output Fields .................................................. 287
Table 30: Event Log Filter Summary Output Fields ...................................... 293
Table 31: Event Log Filter Detail Output Fields .......................................... 294
Table 32: Log Filter Match Criteria Output Fields ....................................... 294
Table 33: Show Log-Collector Output Fields ............................................... 296
Table 34: SNMP Trap Group Output Fields .................................................. 301
Table 35: Show Log Syslog Output Fields .................................................... 303
# List of Figures

## Security
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RADIUS Requests and Responses</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>Security Flow</td>
<td>27</td>
</tr>
</tbody>
</table>

## SNMP
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>SNMPv1 and SNMPv2c Configuration and Implementation Flow</td>
<td>156</td>
</tr>
</tbody>
</table>

## Event and Accounting Logs
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Event Logging Block Diagram</td>
<td>203</td>
</tr>
<tr>
<td>5</td>
<td>Show Log Applications Command Output</td>
<td>205</td>
</tr>
</tbody>
</table>
Preface

About This Guide

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

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

- CLI concepts
- System and user access and security
- SNMP
- Event and accounting logs

List of Technical Publications

The 7210 SAS E OS documentation set is composed of the following books:

- 7210 SAS E OS Basic System Configuration Guide
  This guide describes basic system configurations and operations.
- 7210 SAS E OS System Management Guide
This guide describes system security and access configurations as well as event logging and accounting logs.

- 7210 SAS E OS Interface Configuration Guide
  This guide describes card, Media Dependent Adapter (MDA), and port provisioning.

- 7210 SAS E OS Router Configuration Guide

This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, link

- 7210 SAS E OS Routing Protocols Guide
  This guide provides an overview of routing concepts and provides configuration examples for protocols and route policies.

- 7210 SAS E OS Services Guide
  This guide describes how to configure service parameters such as customer information, and user services.

- 7210 SAS E OS OAM and Diagnostic Guide
  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.

- 7210 SAS E OS Quality of Service Guide
  This guide describes how to configure Quality of Service (QoS) policy management.

**Technical Support**

If you purchased a service agreement for your 7210 SAS device 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, contact your welcome center:

Web: http://www1.alcatel-lucent.com/comps/pages/carrier_support.jhtml
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 7210 SAS Router 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: Configuration Process

<table>
<thead>
<tr>
<th>Area</th>
<th>Task</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>System security</td>
<td>Configure system security parameters, such as authentication, authorization, and accounting.</td>
<td>Security on page 15</td>
</tr>
<tr>
<td>Network management</td>
<td>Configure SNMP elements.</td>
<td>SNMP on page 149</td>
</tr>
<tr>
<td>Operational functions</td>
<td>Configure event and accounting logs.</td>
<td>Event and Accounting Logs on page 195</td>
</tr>
<tr>
<td>Reference</td>
<td>List of IEEE, IETF, and other proprietary entities.</td>
<td></td>
</tr>
</tbody>
</table>
In This Chapter

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

- Authentication, Authorization, and Accounting on page 16
  → Authentication on page 17
  → Authorization on page 22
  → Accounting on page 24
- Security Controls on page 26
  → When a Server Does Not Respond on page 26
  → Access Request Flow on page 27
- Vendor-Specific Attributes (VSAs) on page 29
- Other Security Features on page 35
  – Secure Shell (SSH) on page 35
  – Encryption on page 39
- Configuration Notes on page 43
This chapter describes authentication, authorization, and accounting (AAA) used to monitor and control network access on 7210 SAS routers. 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.

Another 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 7210 SAS routers 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 which determines the authentication method to try first, second, and third.

7210 SAS 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 ALA-1 and ALA-2. The user name and password from ALA-3 could not be authenticated, thus access was denied.
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 7210 SAS-Series 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.

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.

For the RADIUS server selection, round-robin is used if multiple RADIUS servers are configured. Although, if the first alive server in the list cannot find a user-name, the router does not re-query the next server in the RADIUS server list and denies the access request. It may get authenticated on the next login attempt if the next selected RADIUS server has the appropriate user-name. It is recommended that the same user databases are maintained for RADIUS servers in order to avoid inconsistent behavior.

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 7210 SAS-Series routers 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 7210 SAS-Series router:

- Local Authentication on page 18
- RADIUS Authentication on page 18
- TACACS+ Authentication on page 21
Local Authentication

Local authentication uses user names and passwords 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

The RADIUS server selection algorithm is used by different applications:

- RADIUS operator management
- RADIUS authentication for Enhanced Subscriber Management
- RADIUS accounting for Enhanced Subscriber Management
- RADIUS PE-discovery

In all these applications, up to 5 RADIUS servers pools (per RADIUS policy, if used) can be configured.

The RADIUS server selection algorithm can work in 2 modes, either Direct mode or Round-robin mode.
Direct Mode

The first server is used as the primary server. If this server is unreachable, the next server, based on the server index, of the server pool is used. This continues until either all servers in the pool have been tried or an answer is received.

If a server is unreachable, it will not be used again by the RADIUS application for the next 30 seconds to allow the server to recover from its unreachable state. After 30 seconds the unreachable server is available again for the RADIUS application. If in these 30 seconds the RADIUS application receives a valid response for a previously sent RADIUS packet on that unreachable server, the server will be available for the RADIUS application again, immediately after reception of that response.

Round-Robin Mode

The RADIUS application sends the next RADIUS packet to the next server in the server pool. The same server non-reachability behavior is valid as in the Direct mode.

Server Reachability Detection

A server is reachable, when the operational state UP, when a valid response is received within a timeout period which is configurable by the retry parameter on the RADIUS policy level.

A server is treated as not-reachable, when the operational state down, when the following occurs:

- A timeout — If a number of consecutive timeouts are encountered for a specific server. This number is configurable by the retry parameter on RADIUS policy level.
- A send failed — If a packet cannot be sent to the RADIUS server because the forwarding path towards the RADIUS server is broken (for example, the route is not available, the is interface shutdown, etc.), then, no retry mechanism is invoked and immediately, the next server in line is used.

A server that is down can only be used again by the RADIUS algorithm after 30 seconds, unless, during these 30 seconds a valid RADIUS reply is received for that server. Then, the server is immediately marked UP again.

The operational state of a server can also be “unknown” if the RADIUS application is not aware of the state of the RADIUS server (for example, if the server was previously down but no requests had been sent to the server, thus, it is not certain yet whether the server is actually reachable).
Application Specific Behavior

Operator Management

The server access mode is fixed to Round-Robin (Direct cannot be configured for operator management). A health-check function is available for operator management, which can optionally be disabled. The health-check polls the server once every 10 seconds with an improbable user name. If the server does not respond to this health-check, it will be marked down.

If the first server in the list cannot find a user, the next server in the RADIUS server list is not queried and access is denied. If multiple RADIUS servers are used, it is assumed they all have the same user database.

RADIUS Authentication

If the first server in the list cannot find a user, the next server in the RADIUS server list is not queried and access is denied. If multiple RADIUS servers are used, it is assumed they all have the same user database.

RADIUS Accounting

The RADIUS accounting application will try to send all the concerned packets of a subscriber host to the same server. If that server is down, then the packet is sent to the next server and, from that moment on, the RADIUS application uses that server to send its packets for that subscriber host.

RADIUS PE-Discovery

If the first server in the list cannot find a user, the next server in the RADIUS server list is not queried and access is denied. If multiple RADIUS servers are used, it is assumed they all have the same user database.

The RADIUS PE-discovery application makes use of a 10 second time period instead of the generic 30 seconds and uses a fixed consecutive timeout value of 2 (see Server Reachability Detection on page 19).

As long as the Session-Timeout (attribute in the RADIUS user file) is specified, it is used for the polling interval. Otherwise, the configured polling interval will be used (60 seconds by default).


**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 logon 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

routers support 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 VSAs on the RADIUS server. See Vendor-Specific Attributes (VSAs) on page 29.

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

- Download the user profile to the router
- Send the profile name that the node should apply to the 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 router and should be identical for consistent results. If the profile is not present, then access is denied.

Table 2 displays the following scenarios:

- Remote (RADIUS) authorization cannot be performed if authentication is done locally (on the router).
- The reverse scenario is supported if RADIUS authentication is successful and no authorization is configured for the user on the RADIUS server, then local (router) authorization is attempted, if configured in the authorization order.

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 2: Supported Authorization Configurations

<table>
<thead>
<tr>
<th>RADIUS Supplied Profile</th>
<th>configured user</th>
<th>RADIUS server configured user</th>
<th>TACACS+ server configured user</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>Not Supported</td>
<td></td>
<td>Not Supported</td>
</tr>
</tbody>
</table>
When using authorization, maintaining a user database on the router is not required. User names can be configured on the RADIUS server. User names are temporary and are not saved in the configuration when the user session terminates. Temporary user login names and their associated passwords are not saved as part of the configuration.

- Local Authorization on page 23
- RADIUS Authorization on page 23
- TACACS+ Authorization on page 23

Local Authorization

Local authorization uses user profiles and user access information after a user is authenticated. The profiles and user access information specifies 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). 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 router. Permissions include the use of FTP, Telnet, SSH (SCP), and console access. When granting Telnet, SSH (SCP) and console access to the 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.

TACACS+ Authorization

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

TACACS+ separates the authentication, authorization, and accounting function. RADIUS combines the authentication and authorization functions.
Accounting

When enabled, RADIUS accounting sends command line accounting from the 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.

RADIUS Accounting

Accounting tracks user activity to a specified host. 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 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

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 be sent or just stop packets be sent. Start/stop messages are only sent for individual commands, not for the session.

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 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, sends a start packet to the TACACS+ accounting server which 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 routers 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. In other words, 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.

<table>
<thead>
<tr>
<th>Method</th>
<th>Authentication</th>
<th>Authorization</th>
<th>Accounting*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

* Local commands always perform account logging using the `config log` command.

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 not 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. When a server does not respond with the health check feature enabled, 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 Alcatel-Lucent’s 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, implying a lower indexed server is not available. 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 passwords. 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 is 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]

---

7210 SAS-E OS System Management Guide   Page 27
Vendor-Specific Attributes (VSAs)

The 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 the PE-record entry is required in order to support the RADIUS Discovery for Layer 2 VPN feature. Note that a PE-record is only relevant if the RADIUS Discovery feature is used, not for the standard RADIUS setup.

The following RADIUS vendor-specific attributes (VSAs) are supported by Alcatel-Lucent.

- **timetra-access <ftp> <console> <both>** — This is a mandatory command that must be configured. This command specifies if 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 router and the following applies for local and remote authentication:
  1. The authentication-order parameters configured on the router must include the local keyword.
  2. The user name may or may not be configured on the router.
  3. The user must be authenticated by the RADIUS server.
  4. Up to 8 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.
Vendor-Specific Attributes (VSAs)

Configure from most specific to least specific. The implementation 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 (`cf1:`).
- `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:

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

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

The complete list of TiMetra VSAs is available on a file included on the compact flash shipped with the image.
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 = cf1:
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,
```
Vendor-Specific Attributes (VSAs)

Alcatel-Lucent Dictionary

# Revision: 1.29.6.2

VENDOR Alcatel-IPD 6527

# User management VSAs
ATTRIBUTE Timetra-Access 1 integer Alcatel-IPD
VALUE Timetra-Access ftp 1
VALUE Timetra-Access console 2
VALUE Timetra-Access both 3
ATTRIBUTE Timetra-Home-Directory 2 string Alcatel-IPD
ATTRIBUTE Timetra-Restrict-To-Home 3 integer Alcatel-IPD
VALUE Timetra-Restrict-To-Home true 1
VALUE Timetra-Restrict-To-Home false 2
ATTRIBUTE Timetra-Profile 4 string Alcatel-IPD
ATTRIBUTE Timetra-Default-Action 5 integer Alcatel-IPD
VALUE Timetra-Default-Action permit-all 1
VALUE Timetra-Default-Action deny-all 2
VALUE Timetra-Default-Action none 3
ATTRIBUTE Timetra-Cmd 6 string Alcatel-IPD
ATTRIBUTE Timetra-Action 7 integer Alcatel-IPD
VALUE Timetra-Action permit 1
VALUE Timetra-Action deny 2
ATTRIBUTE Timetra-Exec-File 8 string Alcatel-IPD

# RADIUS subscriber authorization and CoA VSAs
ATTRIBUTE Alc-Primary-Dns 9 ipaddr Alcatel-IPD
ATTRIBUTE Alc-Secondary-Dns 10 ipaddr Alcatel-IPD
ATTRIBUTE Alc-Subsc-ID-Str 11 string Alcatel-IPD
ATTRIBUTE Alc-Subsc-Prof-Str 12 string Alcatel-IPD
ATTRIBUTE Alc-SLA-Prof-Str 13 string Alcatel-IPD
ATTRIBUTE Alc-Force-Renew 14 string Alcatel-IPD # CoA
ATTRIBUTE Alc-Create-Host 15 string Alcatel-IPD # CoA
ATTRIBUTE Alc-ANCP-Str 16 string Alcatel-IPD
ATTRIBUTE Alc-Retail-Serv-Id 17 integer Alcatel-IPD
ATTRIBUTE Alc-Default-Router 18 ipaddr Alcatel-IPD

# RADIUS subscriber accounting VSAs
ATTRIBUTE Alc-Acct-I-Inprof-Octets-64 19 octets Alcatel-IPD
ATTRIBUTE Alc-Acct-I-Outprof-Octets-64 20 octets Alcatel-IPD
ATTRIBUTE Alc-Acct-O-Inprof-Octets-64 21 octets Alcatel-IPD
ATTRIBUTE Alc-Acct-O-Outprof-Octets-64 22 octets Alcatel-IPD
ATTRIBUTE Alc-Acct-I-Inprof-Pkts-64 23 octets Alcatel-IPD
ATTRIBUTE Alc-Acct-O-Outprof-Pkts-64 24 octets Alcatel-IPD
ATTRIBUTE Alc-Acct-O-Inprof-Pkts-64 25 octets Alcatel-IPD
ATTRIBUTE Alc-Acct-O-Outprof-Pkts-64 26 octets Alcatel-IPD
ATTRIBUTE Alc-Client-Hardware-Addr 27 string Alcatel-IPD
ATTRIBUTE Alc-Int-Dest-Id-Str              28      string  Alcatel-IPD
ATTRIBUTE Alc-Primary-Nbns                 29      ipaddr  Alcatel-IPD
ATTRIBUTE Alc-Secondary-Nbns               30      ipaddr  Alcatel-IPD
ATTRIBUTE Alc-MSAP-Serv-Id                 31      integer Alcatel-IPD
ATTRIBUTE Alc-MSAP-Policy                  32      string  Alcatel-IPD
ATTRIBUTE Alc-MSAP-Interface               33      string  Alcatel-IPD
ATTRIBUTE Alc-PPPoE-PADO-Delay             34      integer Alcatel-IPD
ATTRIBUTE Alc-PPPoE-Service-Name           35      string  Alcatel-IPD
ATTRIBUTE Alc-DHCP-Vendor-Class-Id         36      string  Alcatel-IPD

# RADIUS subscriber accounting VSAs (HSMDA override counters)
ATTRIBUTE Alc-Acct-OC-I-Inprof-Octets-64   37      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-I-Outprof-Octets-64  38      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-O-Inprof-Octets-64   39      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-O-Outprof-Octets-64  40      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-I-Inprof-Pkts-64     41      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-I-Outprof-Pkts-64    42      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-O-Inprof-Pkts-64     43      octets  Alcatel-IPD
ATTRIBUTE Alc-Acct-OC-O-Outprof-Pkts-64    44      octets  Alcatel-IPD

ATTRIBUTE Alc-App-Prof-Str                 45      string  Alcatel-IPD
ATTRIBUTE Alc-Tunnel-Group                 46      string  Alcatel-IPD
ATTRIBUTE Alc-Tunnel-Algorithm             47      integer Alcatel-IPD

VALUE     Alc-Tunnel-Algorithm            weighted-access 1
VALUE     Alc-Tunnel-Algorithm            existing-first  2

ATTRIBUTE Alc-BGP-Policy                   55      string  Alcatel-IPD
ATTRIBUTE Alc-BGP-Auth-Keychain            56      string  Alcatel-IPD
ATTRIBUTE Alc-BGP-Auth-Key                 57      octets  Alcatel-IPD
ATTRIBUTE Alc-BGP-Export-Policy            58      string  Alcatel-IPD
ATTRIBUTE Alc-BGP-Import-Policy            59      string  Alcatel-IPD
ATTRIBUTE Alc-BGP-PeerAS                   60      integer Alcatel-IPD
ATTRIBUTE Alc-IPsec-Serv-Id                61      integer Alcatel-IPD
ATTRIBUTE Alc-IPsec-Interface              62      string  Alcatel-IPD
ATTRIBUTE Alc-IPsec-Tunnel-Template-Id     63      integer Alcatel-IPD
ATTRIBUTE Alc-IPsec-SA-Lifetime            64      integer Alcatel-IPD
ATTRIBUTE Alc-IPsec-SA-PFS-Group           65      integer Alcatel-IPD

# Match TC TmnxIkePolicyDHGroup in TIMETRA-IPSEC-MIB
VALUE     Alc-IPsec-SA-PFS-Group          group1          1
VALUE     Alc-IPsec-SA-PFS-Group          group2          2
VALUE     Alc-IPsec-SA-PFS-Group          group5          5

ATTRIBUTE Alc-IPsec-SA-Encr-Algorithm      66      integer Alcatel-IPD

# Match TC TmnxEncrAlgorithm in TIMETRA-IPSEC-MIB
VALUE     Alc-IPsec-SA-Encr-Algorithm     null            1
VALUE     Alc-IPsec-SA-Encr-Algorithm     des             2
VALUE     Alc-IPsec-SA-Encr-Algorithm     des3            3
VALUE     Alc-IPsec-SA-Encr-Algorithm     aes128          4
VALUE     Alc-IPsec-SA-Encr-Algorithm     aes192          5
VALUE     Alc-IPsec-SA-Encr-Algorithm     aes256          6

ATTRIBUTE Alc-IPsec-SA-Auth-Algorithm      67      integer Alcatel-IPD

# Match TC TmnxAuthAlgorithm in TIMETRA-IPSEC-MIB
VALUE     Alc-IPsec-SA-Auth-Algorithm     null            1
VALUE     Alc-IPsec-SA-Auth-Algorithm     md5             2
Vendor-Specific Attributes (VSAs)

<table>
<thead>
<tr>
<th>VALUE</th>
<th>Alc-IPsec-SA-Auth-Algorithm</th>
<th>shal</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTRIBUTE</td>
<td>Alc-IPsec-SA-Replay-Window</td>
<td>68</td>
<td>integer</td>
</tr>
</tbody>
</table>

# RADIUS subscriber accounting VSAs (custom records)

| ATTRIBUTE | Alc-Acct-I-High-Octets-Drop_64 | 69 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-I-Low-Octets-Drop_64 | 70 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-I-High-Pack-Drop_64 | 71 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-I-Low-Pack-Drop_64 | 72 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-I-High-Octets-Offer_64 | 73 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-I-Low-Octets-Offer_64 | 74 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-I-High-Pack-Offer_64 | 75 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-I-Low-Pack-Offer_64 | 76 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-I-Unc-Octets-Offer_64 | 77 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-I-Unc-Pack-Offer_64 | 78 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-I-All-Octets-Offer_64 | 79 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-I-All-Pack-Offer_64 | 80 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-O-Inprof-Pack-Drop_64 | 81 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-O-Outprof-Pack-Drop_64 | 82 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-O-Inprof-Octs-Drop_64 | 83 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-O-Outprof-Octs-Drop_64 | 84 | octets | Alcatel-IPD |

# RADIUS subscriber accounting VSAs (custom records, HSMDA)

| ATTRIBUTE | Alc-Acct-OC-I-All-Octs-Offer_64 | 85 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-OC-I-All-Pack-Offer_64 | 86 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-OC-I-Inpr-Octs-Drop_64 | 87 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-OC-I-Outpr-Octs-Drop_64 | 88 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-OC-I-Inpr-Pack-Drop_64 | 89 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-OC-I-Outpr-Pack-Drop_64 | 90 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-OC-O-Inpr-Pack-Drop_64 | 91 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-OC-O-Outpr-Pack-Drop_64 | 92 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-OC-O-Inpr-Octs-Drop_64 | 93 | octets | Alcatel-IPD |
| ATTRIBUTE | Alc-Acct-OC-O-Outpr-Octs-Drop_64 | 94 | octets | Alcatel-IPD |

# credit control VSAs

| ATTRIBUTE | Alc-Credit-Control-CategoryMap | 95 | string | Alcatel-IPD |
| ATTRIBUTE | Alc-Credit-Control-Quota | 96 | string | Alcatel-IPD |

| ATTRIBUTE | Alc-Force-Nak | 98 | string | Alcatel-IPD |

# CoA
Other Security Features

Secure Shell (SSH)

Secure Shell Version 1 (SSH) 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 places 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.

7210 SAS-Series allows you to configure Secure Shell (SSH) Version 2 (SSH2). SSH1 and SSH2 are different protocols and encrypt at different parts of the packets. SSH1 uses 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. 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.

7210 SAS-Series 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 SSHv1. Note that this server process is separate from the SSH and SCP client commands on the 7210 SAS-Series 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 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 7210 SAS-Series SCP server will accept either forward slash (“/”) or backslash (“\”) characters to delimit directory and/or filenames. Similarly, the 7210 SAS-Series 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 times interpret the backslash character as an “escape” character which does not get transmitted to the 7210 SASSCP server. For example, a destination directory specified as “cf1:dir1\file1” will be transmitted to the 7210 SAS SCP server as “cf1: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.
Exponential Login Backoff

A malicious user may attempt to gain CLI access by means of a dictionary attack using a script to automatically attempt to login as an “admin” user and using a dictionary list to test all possible passwords. Using the exponential-backoff feature in the `config>system>login-control` context the 7210 SAS increases the delay between login attempts exponentially to mitigate attacks.

When trying to access the router, the user is only allowed three attempts per session, by default, to login to the system before the connectivity session is terminated. It is during that single connectivity session that the exponential backoff is utilized. Each time an invalid password is entered for a login account name, a delay is inserted before the next display of the login/password prompt. The first delay is 1 second, and each subsequent delay is 2 times the last delay (for example, 1 second, 2 seconds, 4 seconds). Once the connectivity session is terminated after the third failed login attempt, the exponential backoff timer is reset to 1 second.

Note that the `config>system>login-control>[no] exponential-backoff` command works in conjunction with the `config>system>security>password>attempts` command which is also a system wide configuration.

For example:

*A:ALA-48>config>system# security password attempts*
- `attempts <count> [time <minutes1>] [lockout <minutes2>]`
- `no attempts`

< count > : [1..64]
< minutes1 > : [0..60]
< minutes2 > : [0..1440]

Exponential backoff applies to any user and by any login method such as console, SSH and Telnet.

Refer to Configuring Login Controls on page 71. The commands are described in Login, Telnet, SSH and FTP Commands on page 86.
User Lockout

When a user exceeds the maximum number of attempts allowed (the default is 3 attempts) during a certain period of time (the default is 5 minutes) the account used during those attempts will be locked out for a pre-configured lock-out period (the default is 10 minutes).

An security event log will be generated as soon as a user account has exceeded the number of allowed attempts and the `show>system>security>user` command can be used to display the total number of failed attempts per user.

The account will be automatically re-enabled as soon as the lock-out period has expired.
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 Alcatel-Lucent 7210 SAS 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.

TCP Enhanced Authentication Option

The TCP Enhanced Authentication Option, currently covered in draft-bonica-tcp-auth-05.txt, Authentication for TCP-based Routing and Management Protocols, extends the previous MD5 authentication option to include the ability to change keys without tearing down the session, and allows for stronger authentication algorithms to be used.
The TCP Enhanced Authentication Option is a TCP extension that enhances security for BGP, LDP and other TCP-based protocols. This includes the ability to change keys in a BGP or LDP session seamlessly without tearing down the session. It is intended for applications where secure administrative access to both the end-points of the TCP connection is normally available.

TCP peers can use this extension to authenticate messages passed between one another. This strategy improves upon current practice, which is described in RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*. Using this new strategy, TCP peers can update authentication keys during the lifetime of a TCP connection. TCP peers can also use stronger authentication algorithms to authenticate routing messages.
Packet Formats

```
+---+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Kind | Length |T|K| Alg ID|Res| Key ID |
+---+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Authentication Data |
+---+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option Syntax

- **Kind**: 8 bits
  The Kind field identifies the TCP Enhanced Authentication Option. This value will be assigned by IANA.

- **Length**: 8 bits
  The Length field specifies the length of the TCP Enhanced Authentication Option, in octets. This count includes two octets representing the Kind and Length fields.
  The valid range for this field is from 4 to 40 octets, inclusive.
  For all algorithms specified in this memo the value will be 16 octets.

- **T-Bit**: 1 bit
  The T-bit specifies whether TCP Options were omitted from the TCP header for the purpose of MAC calculation. A value of 1 indicates that all TCP options other than the Extended Authentication Option were omitted. A value of 0 indicates that TCP options were included.
  The default value is 0.

- **K-Bit**: 1 bit
  This bit is reserved for future enhancement. Its value MUST be equal to zero.

- **Alg ID**: 6 bits
  The Alg ID field identifies the MAC algorithm.

- **Res**: 2 bits
  These bits are reserved. They MUST be set to zero.

- **Key ID**: 6 bits
  The Key ID field identifies the key that was used to generate the message digest.

- **Authentication Data**: Variable length
  The Authentication Data field contains data that is used to authenticate the TCP segment. This data includes, but need not be restricted to, a MAC. The length and format of the Authentication Data Field can be derived from the Alg ID.

- The Authentication for TCP-based Routing and Management Protocols draft provides and overview of the TCP Enhanced Authentication Option. The details of this feature are described in draft-bonica-tcp-auth-04.txt.
Keychain

A keychain is a set of up to 64 keys, where each key is \{A[i], K[i], V[i], S[i], T[i], S'[i], T'[i]\} as described in draft-bonica-tcp-auth-05.txt, *Authentication for TCP-based Routing and Management Protocols*. They keys can be assigned to both sides of a BGP or LDP peer. The individual keys in a keychain have a begin- and end-time indicating when to use this key. These fields map to the CLI tree as:

**Table 4: Keychain Mapping**

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>The key identifier expressed as an integer (0...63)</td>
<td>config&gt;system&gt;security&gt;keychain&gt;direction&gt;bi&gt;entry&lt;br&gt;config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;receive&gt;entry&lt;br&gt;config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;send&gt;entry</td>
</tr>
<tr>
<td>A[i]</td>
<td>Authentication algorithm to use with key[i]</td>
<td>config&gt;system&gt;security&gt;keychain&gt;direction&gt;bi&gt;entry with algorithm parameter&lt;br&gt;config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;receive&gt;entry with algorithm parameter&lt;br&gt;config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;send&gt;entry with algorithm parameter</td>
</tr>
<tr>
<td>K[i]</td>
<td>Shared secret to use with key[i].</td>
<td>config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;receive&gt;entry with shared secret parameter&lt;br&gt;config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;send&gt;entry with shared secret parameter&lt;br&gt;config&gt;system&gt;security&gt;keychain&gt;direction&gt;bi&gt;entry with shared secret parameter</td>
</tr>
<tr>
<td>V[i]</td>
<td>A vector that determines whether the key[i] is to be used to generate MACs for inbound segments, outbound segments, or both.</td>
<td>config&gt;system&gt;security&gt;keychain&gt;direction</td>
</tr>
<tr>
<td>S[i]</td>
<td>Start time from which key[i] can be used by sending TCPs.</td>
<td>config&gt;system&gt;security&gt;keychain&gt;direction&gt;bi&gt;entry&gt;begin-time&lt;br&gt;config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;send&gt;entry&gt;begin-time</td>
</tr>
<tr>
<td>T[i]</td>
<td>End time after which key[i] cannot be used by sending TCPs.</td>
<td>Inferred by the begin-time of the next key (youngest key rule).</td>
</tr>
<tr>
<td>S'[i]</td>
<td>Start time from which key[i] can be used by receiving TCPs.</td>
<td>config&gt;system&gt;security&gt;keychain&gt;direction&gt;bi&gt;entry&gt;begin-time&lt;br&gt;config&gt;system&gt;security&gt;keychain&gt;direction&gt;bi&gt;entry&gt;tolerance&lt;br&gt;config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;receive&gt;entry&gt;begin-time&lt;br&gt;config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;receive&gt;entry&gt;tolerance</td>
</tr>
<tr>
<td>T'[i]</td>
<td>End time after which key[i] cannot be used by receiving TCPs</td>
<td>config&gt;system&gt;security&gt;keychain&gt;direction&gt;uni&gt;receive&gt;entry&gt;end-time</td>
</tr>
</tbody>
</table>
Configuration Notes

This section describes security configuration caveats.

General

- 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 a RADIUS authorization is enabled, then VSAs must be configured on the RADIUS server.
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 46
  - Configuring Authorization on page 47
  - Configuring Authorization on page 47
  - Configuring Accounting on page 49
- Configuration Tasks on page 52
- Security Configuration Procedures on page 53
  - Configuring Management Access Filters on page 53
  - Configuring Password Management Parameters on page 55
  - Configuring Profiles on page 56
  - Configuring Users on page 57
  - Copying and Overwriting Users and Profiles on page 59
  - Enabling SSH on page 70
  - Configuring Login Controls on page 71
  - RADIUS Configurations on page 63
    - Configuring RADIUS Authentication on page 63
    - Configuring RADIUS Authorization on page 64
    - Configuring RADIUS Accounting on page 65
  - TACACS+ Configurations on page 67
    - Enabling TACACS+ Authentication on page 67
    - Configuring TACACS+ Authorization on page 68
    - Configuring TACACS+ Accounting on page 69
Configuring Authentication

Refer to the following sections to configure authentication:

- Local authentication
  → Configuring Password Management Parameters on page 55
  → Configuring Profiles on page 56
  → Configuring Users on page 57

- RADIUS authentication (only)
  By default, authentication is enabled locally. Perform the following tasks to configure security on each participating router:
  → Configuring Profiles on page 56
  → Configuring RADIUS Authentication on page 63
  → Configuring Users on page 57

- RADIUS authentication
  To implement only RADIUS authentication, with authorization, perform the following tasks on each participating router:
  → Configuring RADIUS Authentication on page 63
  → Configuring RADIUS Authorization on page 64

- TACACS+ authentication
  To implement only TACACS+ authentication, perform the following tasks on each participating router:
  → Configuring Profiles on page 56
  → Configuring Users on page 57
  → Enabling TACACS+ Authentication on page 67
Configuring Authorization

Refer to the following sections to configure authorization.

• Local authorization
  For local authorization, configure these tasks on each participating router:
  → Configuring Profiles on page 56
  → Configuring Users on page 57

• RADIUS authorization (only)
  For RADIUS authorization (without authentication), configure these tasks on each participating router:
  → Configuring RADIUS Authorization on page 64
  → Configuring Profiles on page 56
  For RADIUS authorization, VSAs must be configured on the RADIUS server. See Vendor-Specific Attributes (VSAs) on page 29.

• RADIUS authorization
  For RADIUS authorization (with authentication), configure these tasks on each participating router:
  → Configuring RADIUS Authorization on page 64
    For RADIUS authorization, VSAs must be configured on the RADIUS server. See Vendor-Specific Attributes (VSAs) on page 29.
  → Configuring RADIUS Authentication on page 63
  → Configuring Profiles on page 56

• TACACS+ authorization (only)
  For TACACS+ authorization (without authentication), configure these tasks on each participating router:
  → Configuring TACACS+ Authorization on page 68

• TACACS+ authorization
For TACACS+ authorization (with authentication), configure these tasks on each participating router:

→ Enabling TACACS+ Authentication on page 67
→ Configuring TACACS+ Authorization on page 68
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 on page 219
- Configuring RADIUS Accounting on page 65
- Configuring TACACS+ Accounting on page 69
Security Configurations

This section provides information to configure security and configuration examples of configuration tasks.

To implement security features, configure the following components:

- Management access filters
- Profiles
- User access parameters
- Password management parameters
- Enable RADIUS and/or TACACS+
  → One to five RADIUS and/or TACACS+ servers
  → RADIUS and/or TACACS+ parameters

The following example displays default values for security parameters.

```
A:ALA-1>config>system>security# info detail
----------------------------------------------
  no hash-control
telnet-server
no telnet6-server
no ftp-server
management-access-filter
exit
profile "default"
  default-action none
  no li
  entry 10
  no description
  match "exec"
  action permit

... password
  authentication-order radius tacplus local
  no aging
  minimum-length 6
  attempts 3 time 5 lockout 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 lockout 10
exit

no ssh
This section provides a brief overview of the tasks that must be performed to configure security and provides the CLI commands. Table 5 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 5: Security Configuration Requirements

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Authorization</th>
<th>Accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Local</td>
<td>None</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Local and RADIUS</td>
<td>RADIUS</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Local</td>
<td>TACACS+</td>
</tr>
</tbody>
</table>
Security Configuration Procedures

- Configuring Management Access Filters on page 53
- Configuring Password Management Parameters on page 55
- Configuring Profiles on page 56
- Configuring Users on page 57
- Copying and Overwriting Users and Profiles on page 59
- Enabling SSH on page 70

Configuring Management Access Filters

Creating and implementing management access filters is optional. Management access filters control all traffic going in to the node, including all routing protocols. They apply to packets from all ports. The filters can be used to restrict management of the 7210 SAS 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 also apply to the management Ethernet port.

The 7210 SAS implementation exits the filter when the first match is found and execute 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 one keyword to be considered complete. Entries without the action keyword are considered incomplete and will be rendered inactive.

Use the following CLI commands to configure a 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
  default-action {permit|deny|deny-host-unreachable}
  renum old-entry-number new-entry-number
  no shutdown
  entry entry-id
    description description-string
    src-port {port-id cpm|lag|lag-id}
    src-ip {ip-prefix/mask|ip-prefix netmask}
    protocol protocol-id
    dst-port port [mask]
The following displays a management access filter configuration example:

```
A:ALA-1>config>system>security# info
--------------------------------------------
no hash-control
telnet-server
no telnet6-server
no ftp-server
management-access-filter
exit
profile "default"
    default-action none
    no li
    entry 10
        no description
        match "exec"
        action permit
exit
entry 20
    no description
snmp
    community "private" rwa version both
exit
--------------------------------------------
A:ALA-1>config>system>security#
```
Configuring Password Management Parameters

Password management parameters consist of defining aging, the authentication order and authentication methods, password length and complexity, as well as the number of attempts a user can enter a password.

Depending on your authentication requirements, password parameters are configured locally.

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 example displays a password configuration:

```
A:ALA-1>config>system>security# info
----------------------------------------------
    password
    authentication-order radius tacplus local
        aging 365
        minimum-length 8
        attempts 5 time 5 lockout 20
    exit
----------------------------------------------
A:ALA-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 sixteen user profiles can be defined. A user can participate in up to sixteen 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 example displays a user profile output:

```
A:ALA-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
... exit

----------------------------------------------
A:ALA-1>config>system>security#
```
Configuring Users

Configure access parameters for individual users. For user, define the login name for the user and, optionally, information that identifies the user. Use the following CLI commands to configure RADIUS support:

**CLI Syntax:**
```
cfg>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]}
group group-name
```

The following displays a user configuration example:

```
A:ALA-1>config>system>security# info
----------------------------------------------
...                                           
user "49ers"
  password "gQbnuzLd7H/VxGdUqdh7bE" hash2
  access console ftp snmp
  restricted-to-home
  console
  member "default"
  member "ghost"
  exit
  exit
...

----------------------------------------------
A:ALA-1>config>system>security#
```
Configuring Keychains

The following displays a keychain configuration.

```
A:ALA-1>config>system>security# info
----------------------------------------------
... keychain "abc"
direction bi
    entry 1 key "ZcvSElJzJx/wBZ9biCToVQj9YZQVvU.S" hash2 alg
orithm aes-128-cmac-96
    begin-time 2006/12/18 22:55:20
    exit
    exit
    exit
    exit
keychain "basasd"
direction uni
    receive
        entry 1 key "Ee7xdK1YO2DOm7v3Ijv/84LIu96R2fZh" hash2
orithm aes-128-cmac-96
    tolerance forever
    exit
    exit
    exit
    exit
... ----------------------------------------------
A:ALA-1>config>system>security#
```
Copying and Overwriting Users and Profiles

You can copy a profile or user. You can copy a profile or user or overwrite an existing profile or user. The **overwrite** option must be specified or an error occurs if the destination profile or username already exists.

---

**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.`

```bash  
config>system>security#  
config>system>security# copy user testuser to testuserA  
overwrite  
config>system>security#  
```

The following output displays the copied user configurations:

```bash  
A:ALA-12>config>system>security# info  
----------------------------------------------  
...  
user "testuser"  
password "F6XjryaATzM" hash  
access snmp  
    snmp  
        authentication hash md5 e14672e71d3e96e7ale19472527ee969 privacy none  
        group "testgroup"  
    exit  
    exit  
user "testuserA"  
password "" hash2  
access snmp  
    console  
        new-password-at-login  
        exit  
    snmp  
        authentication hash md5 e14672e71d3e96e7ale19472527ee969 privacy none  
        group "testgroup"  
    exit  
    exit  
...  
----------------------------------------------  
A:ALA-12>config>system>security# info  
```

---

Security
Note that the cannot-change-password flag is not replicated when a copy user command is performed. A new-password-at-login flag is created instead.

A:ALA-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
----------------------------------------------
A:ALA-12>config>system>security>user# exit
A:ALA-12>config>system>security# user testuserA
A:ALA-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
----------------------------------------------
A:ALA-12>config>system>security>user#
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:ALA-49>config>system>security# info
--------------
... 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

A:ALA-12>config>system>security#
RADIUS Configurations

- Configuring RADIUS Authentication on page 63
- Configuring RADIUS Authorization on page 64
- Configuring RADIUS Accounting on page 65
- Configuring 802.1x RADIUS Policies on page 66

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`.

Also, the system IP address must be configured in order for the RADIUS client to work. See Configuring a System Interface of the .

The other commands are optional. 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.

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
    timeout seconds
    no shutdown
```

The following displays a RADIUS authentication configuration example:

```
A:ALA-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"
...```

A:ALA-1>config>system>security#
Configuring RADIUS Authorization

In order for RADIUS authorization to function, RADIUS authentication must be enabled first. See Configuring RADIUS Authentication on page 63.

In addition to the local configuration requirements, VSAs must be configured on the RADIUS server. See Vendor-Specific Attributes (VSAs) on page 29.

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

**CLI Syntax:**
```
config>system>security
radius
authorization
```

The following displays a RADIUS authorization configuration example:

```
A:ALA-1>config>system>security# info
----------------------------------------------
...radius
authorization
retry 5
timeout 5
server 1 address 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
...----------------------------------------------
A:ALA-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 displays RADIUS accounting configuration example:

```
A:ALA-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
...-
----------------------------------------------
A:ALA-1>config>system>security#
```
Use the following CLI commands to configure generic authentication parameters for clients using 802.1x EAPOL. Additional parameters are configured per Ethernet port. Refer to the

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

**CLI Syntax:**
```
config>system>security
  dot1x
    radius-plcy policy-name
      server server-index address ip-address secret key [port
      port]
      source-address ip-address
      no shutdown
```

The following displays a 802.1x configuration example:

```
A:ALA-1>config>system>security# info
----------------------------------------------
dot1x
  radius-plcy policy-name
    server server-index address ip-address secret key [port
    port]
    source-address ip-address
    no shutdown
----------------------------------------------
A:ALA-1>config>system#
```
TACACS+ Configurations

- Enabling TACACS+ Authentication on page 67
- Configuring TACACS+ Authorization on page 68
- Configuring TACACS+ Accounting on page 69

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 profiles:

**CLI Syntax:**
```
config>system>security
tacplus
server server-index address ip-address secret key
timeout seconds
no shutdown
```

The following displays a TACACS+ authentication configuration example:

```
A:ALA-1>config>system>security>tacplus# info
----------------------------------------------
timeout 5
server 1 address 10.10.0.5 secret "test1"
server 2 address 10.10.0.6 secret "test2"
server 3 address 10.10.0.7 secret "test3"
server 4 address 10.10.0.8 secret "test4"
server 5 address 10.10.0.9 secret "test5"
----------------------------------------------
A:ALA-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 page 67.

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

**CLI Syntax:**
```
config>system>security
tacplus
   authorization
   no shutdown
```

The following displays a TACACS+ authorization configuration example:

```
A:ALA-1>config>system>security>tacplus# info
----------------------------------------------
   authorization
   timeout 5
   server 1 address 10.10.0.5 secret "test1"
   server 2 address 10.10.0.6 secret "test2"
   server 3 address 10.10.0.7 secret "test3"
   server 4 address 10.10.0.8 secret "test4"
   server 5 address 10.10.0.9 secret "test5"
----------------------------------------------
A:ALA-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 displays a TACACS+ accounting configuration example:

```
A:ALA-1>config>system>security>tacplus# info
----------------------------------------------
accounting
authorization
timeout 5
server 1 address 10.10.0.5 secret "test1"
server 2 address 10.10.0.6 secret "test2"
server 3 address 10.10.0.7 secret "test3"
server 4 address 10.10.0.8 secret "test4"
server 5 address 10.10.0.9 secret "test5"
----------------------------------------------
A:ALA-1>config>system>security>tacplus#
```
Enabling SSH

Use the SSH command to configure the SSH server as SSH1, SSH2 or both. The default is SSH2 (SSH version 2). This command should only be enabled or disabled when the SSH server is disabled. This setting should not be changed while the SSH server is running since the actual change only takes place after SSH is disabled or enabled.

**CLI Syntax:**
```plaintext
config>system>security
  ssh
    preserve-key
    no server-shutdown
    version ssh-version
```

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

```
A:sim1>config>system>security>ssh# info
----------------------------------------------
preserve-key
version 1-2
----------------------------------------------
A:sim1>config>system>security>ssh#
```
Configuring Login Controls

Configure login control parameters for console, Telnet, and FTP sessions.

To configure login controls, enter the following CLI syntax.

**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 displays a login control configuration example:

```
A:ALA-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
...----------------------------------------------
A:ALA-1>config>system#
```
Security Command Reference

Command Hierarchies

Configuration Commands

- Security Commands
  - Password Commands on page 76
  - Profile Commands on page 76
  - RADIUS Commands on page 76
  - SSH Commands on page 77
  - TACACS+ Commands on page 77
  - User Commands on page 77
  - Dot1x Commands on page 78
  - Keychain Commands on page 78
  - TCP Enhanced Authentication Commands on page 78
- Login Control Commands on page 80
- Show Commands on page 81
- Clear Commands on page 81
- Debug Commands on page 81
Security Command Reference

Security Commands

```
config
  system
    security
      copy {user source-user | profile source-profile} to destination [overwrite]
      [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|ipv6-address]
        [no] application app
      [no] telnet-server
```
Management Access Filter Commands

    config
    ├── system
    │   └── security
    │       └── [no] management-access-filter
    │           └── default-action {permit | deny | deny-host-unreachable}
    │           └── [no] entry entry-id
    │               └── action {permit | deny | deny-host-unreachable}
    │               └── description description-string
    │               └── no description
    │               └── dst-port value [mask]
    │               └── no dst-port
    │               └── protocol protocol-id
    │               └── no protocol
    │               └── src-ip {ip-prefix/mask | ip-prefix netmask}
    │               └── no src-ip
    │               └── src-port {port-id | cpm | lag lag-id}
    │               └── no src-port
    │               └── renum old-entry-number new-entry-number
    │               └── [no] shutdown
Security Password Commands

```
config
  — system
  — security
  — password
    — admin-password  password [hash | hash2]
    — no admin-password
    — aging  days
    — no aging
    — attempts  count [time minutes] [lockout minutes]
    — 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}
    — [no] entry  entry-id
      — action  {deny | permit}
      — description  description-string
      — no description
      — match  command-string
      — no match
    — renum  old-entry-number new-entry-number
```

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
```
SSH Commands

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

TACPLUS 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] shutdown
    -- timeout seconds
    -- [no] timeout
    -- [no] use-default-template

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
    {none | des-key key-2}}]
    -- group group-name
    -- [no] group

User Template Commands

    config
Security Command Reference

— system
  — security
    — 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
    — profile user-profile-name
    — no profile
    — [no] restricted-to-home

Dot1x Commands

config
  — system
    — security
      — dot1x
        — radius-plcy name
          — retry count
          — no retry
          — server (dot1x) server-index address ip-address secret key [port port]
          — source-address ip-address
          — [no] shutdown
          — timeout seconds
          — no timeout
    — [no] shutdown

Keychain Commands

config
  — system
    — security
      — [no] keychain keychain-name
        — description description-string
        — no description
        — direction {uni | bi}
        — bi
          — entry entry-id key [authentication-key | hash-key | hash2-key] [hash | hash2] algorithm algorithm
            — begin-time [date] [hours-minutes] [UTC] [now] [forever]
            — [no] shutdown
            — tolerance [seconds | forever]
          — uni
            — receive
              — entry entry-id key [authentication-key | hash-key | hash2-key] [hash | hash2] algorithm algorithm
                — begin-time [date] [hours-minutes] [UTC] [now] [forever]
                — end-time [date][hours-minutes] [UTC] [now] [forever]
                — [no] shutdown
                — tolerance [seconds | forever]
         — send
— **entry** entry-id key [authentication-key | hash-key |
hash2-key] [hash | hash2] algorithm algorithm
— **begin-time** [date] [hours-minutes] [UTC] [now]
  [forever]
  [no] shutdown
— [no] shutdown
— **tcp-option-number**
  — receive option-number
  — send option-number
Login Control Commands

```
config
    system
        login-control
            [no] exponential-backoff
            ftp
                inbound-max-sessions value
                no inbound-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
            telnet
                inbound-max-sessions value
                no inbound-max-sessions
                outbound-max-sessions value
                no outbound-max-sessions
```
Show Commands

Security

show
  — system
    — security
      — access-group [group-name]
      — authentication [statistics]
      — communities
      — management-access-filter [entry-id]
      — password-options
      — profile [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
Configuration Commands

General Security Commands

description

Syntax  
(description description-string

no description

Context  
config>system>security>mgmt-access-filter>entry
config>sys>security>keychain>direction>bi>entry
config>system>security>keychain>direction>uni>receive>entry
config>system>security>keychain>direction>uni>send>entry

Description  
This command creates a text description stored in the configuration file for a configuration context.
This command associates a text string with a configuration context to help identify the context in the configuration file.
The no form of the command removes the string.

Default  
No description associated with the configuration context.

Parameters  
string — 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>mgmt-access-filter
config>system>security>keychain>direction>bi>entry
config>system>security>keychain>direction>uni>receive>entry
config>system>security>keychain>direction>uni>send>entry

Description  
The shutdown command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the no shutdown command. 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 may be deleted.
The no form of the command puts an entity into the administratively enabled state.

Default  
no shutdown
security

Syntax        security
Context       config>system
Description   This command creates the context to configure security settings.

Security commands manage user profiles and user membership. Security commands also manage user login registrations.

ftp-server

Syntax        [no] ftp-server
Context       config>system>security
Description   This command enables FTP servers running on the system.

FTP servers are disabled by default. At system startup, only SSH server are enabled. The no form of the command disables FTP servers running on the system.

hash-control

Syntax        hash-control [read-version {1 | 2 | all}] [write-version {1 | 2}]
no hash-control
Context       config>system>security
Description   Whenever the user executes a save or info command, the system will encrypt all passwords, MD5 keys, etc., for security reasons. At present, two algorithms exist.

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, even the casual observer will notice that it is the same key.

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.

Default       all — read-version set to accept both versions 1 and 2
Parameters    

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.

write-version  {1 | 2} — Select 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.
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 app [ip-int-name|ip-address]
no application app

**Context**  
config>system>security>source-address

**Description**  
This command specifies the application to use the source-IP address specified by the source-address command.

**Parameters**
- **app** — Specify the application name.
  - **Values**  
    - telnet, ftp, ssh, radius, tacplus, snmptrap, syslog, ping, traceroute, dns, sntp, ntp, cflowd
  - **ip-int-name | ip-address** — Specifies the name of the IP interface, 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 networks limit a Telnet clients to three retries to login. The Telnet server disconnects the Telnet client session after three retries.

The **no** form of the command disables Telnet servers running on the system.
Login, Telnet, SSH and FTP Commands

exponential-backoff

Syntax  [no] exponential-backoff

Context  config>system>login-control

Description  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.

The no form of the command disables exponential-backoff.

Default  no exponential-backoff

ftp

Syntax  ftp

Context  config>system>login-control

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

idle-timeout

Syntax  idle-timeout {minutes | disable}

no idle-timeout

Context  config>system>login-control

Description  This command configures the idle timeout for FTP, console, or Telnet sessions before the session is terminated by the system.

By default, an idle FTP, console, or Telnet session times out after 30 minutes of inactivity. This timer can be set per session.

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

Default  30 — Idle timeout set for 30 minutes.

Parameters  minutes — The idle timeout in minutes. Allowed values are 1 to 1440. 0 implies the sessions never timeout.

Values  1 — 1440

disable — When the disable option is specified, a session will never timeout. To re-enable idle timeout, enter the command without the disable option.
inbound-max-sessions

Syntax

```
inbound-max-sessions value
```

```
no inbound-max-sessions
```

Context
config>system>login-control>ftp

Description
This command configures the maximum number of concurrent inbound FTP sessions. This value is the combined total of inbound and outbound sessions. The `no` form of the command reverts to the default value.

Default
3

Parameters

```
value — The maximum number of concurrent FTP sessions on the node.
```

Values

```
0 — 5
```

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 and SSH sessions. A maximum of 15 telnet and ssh connections can be established to the router. The local serial 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 — 15
```

login-banner

Syntax

```
[no] login-banner
```

Context
config>system>login-control

Description
This command enables or disables the display of a login banner. The login banner contains the copyright and build date information for a console login attempt. The `no` form of the command causes only the configured pre-login-message and a generic login prompt to display.
**Configuration Commands**

### login-control

**Syntax**

```plaintext
login-control
```

**Context**

`config>system`

**Description**

This command creates the context to configure the session control for console, Telnet and FTP.

### motd

**Syntax**

```plaintext
motd {url url-prefix: source-url | text motd-text-string}
        no motd
```

**Context**

`config>system>login-control`

**Description**

This command creates the message of the day displayed after a successful console login. Only one message can be configured. The `no` form of the command removes the message.

**Default**

No `motd` is defined.

**Parameters**

- `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.

- `text motd-text-string` — The text of the message of the day. The `motd-text-string` must be enclosed in double quotes. Multiple text strings are not appended to one another.

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.

### outbound-max-sessions

**Syntax**

```plaintext
outbound-max-sessions value
        no outbound-max-sessions
```

**Context**

`config>system>login-control>telnet`

**Description**

This parameter limits the number of outbound Telnet and SSH sessions. A maximum of 15 telnet and ssh connections can be established from the router. The local serial port cannot be disabled.

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

**Default**

5

**Parameters**

- `value` — The maximum number of concurrent outbound Telnet sessions, expressed as an integer.

**Values**

0 — 15
pre-login-message

Syntax    pre-login-message login-text-string [name]  no pre-login-message

Context    config>system>login-control

Description This command creates a message displayed prior to console login attempts on the console via Telnet. Only one message can be configured. If multiple pre-login-messages are configured, the last message entered overwrites the previous entry. It is possible to add the name parameter to an existing message without affecting the current pre-login-message. The no form of the command removes the message.

Default No pre-login-message is defined.

Parameters login-text-string — The string can be 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.

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.

ssh

Syntax    ssh

Context    config>system>security

This command enables the context to configure the SSH parameters.

preserve-key

Syntax    [no] preserve-key

Context    config>system>security>ssh

Description After enabling this command, private keys, public keys, and host key file will be saved by the server. It is restored following a system reboot or the ssh server restart. The no form of the command specifies that the keys will be held in memory by the SSH server and is not restored following a system reboot.

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 ssh-version
no version

Context
config>system>security>ssh

Description
Specifies the SSH protocol version that will be supported by the SSH server.

Parameters

Parameters

Values

Values

Values

Values

Values

Values

Values

Values

Values

Values

Values

Values

Values

Values

Default
2

telnet

Syntax
telnet

Context
config>system>login-control

Description
This command creates the context to configure the Telnet login control parameters.
Management Access Filter Commands

management-access-filter

**Syntax**

[no] management-access-filter

**Context**

config>system>security

**Description**

This command creates the context to edit management access filters and to reset match criteria. Management access filters control all traffic in and out of the router. They can be used to restrict management of the router by other nodes outside either specific (sub)networks or through designated ports. Management filters, as opposed to other traffic filters, are enforced by system software. The **no** form of the command removes management access filters from the configuration.

**Default**

No management access filters are defined.

action

**Syntax**

action (permit | deny | deny-host-unreachable)

no action

**Context**

config>system>security>mgmt-access-filter>entry

**Description**

This command creates the action associated with the management access filter match criteria entry. 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. If the packet does not meet any of the match criteria the configured default action is applied.

**Default**

none — The action is specified by default-action command.

**Parameters**

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

default-action

**Syntax**

default-action {permit | deny | deny-host-unreachable}

**Context**

config>system>security>mgmt-access-filter
**Description**

This command creates the default action for management access in the absence of a specific management access filter match.

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.

**Default**

No default-action is defined.

**Parameters**

- **permit** — Specifies that packets not matching the configured selection criteria in any of the filter entries will be permitted.
- **deny** — Specifies that packets not matching the selection criteria be denied and that an ICMP host unreachable message will not be issued.
- **deny-host-unreachable** — Specifies that packets not matching the selection criteria be denied and a host unreachable message will be issued.

**dst-port**

**Syntax**

```
[no] dst-port value [mask]
```

**Context**

```
config>system>security>mgmt-access-filter>entry
```

**Description**

This command configures a source TCP or UDP port number or port range for a management access filter match criterion.

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

**Default**

No src-port match criterion.

**Parameters**

- **value** — The source TCP or UDP port number as match criteria.

  **Values**
  
  1 — 65535 (decimal)

- **mask** — Mask used to specify a range of source port numbers as the match criterion.

  This 16 bit mask can be configured using the following formats:

<table>
<thead>
<tr>
<th>Format Style</th>
<th>Format Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decimal</td>
<td>DDDDD</td>
<td>63488</td>
</tr>
<tr>
<td>Hexadecimal</td>
<td>0xHHHH</td>
<td>0xF800</td>
</tr>
<tr>
<td>Binary</td>
<td>0BBBBBBBBBBBB</td>
<td>0b1111100000000000</td>
</tr>
</tbody>
</table>

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

  **Default**
  
  65535 (exact match)

  **Values**
  
  1 — 65535 (decimal)
entry

[no] entry entry-id

Context config>system>security>mgmt-access-filter

Description This command is used to create or edit a management access filter entry. Multiple entries can be created with unique entry-id numbers. The 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.

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.

The no form of the command removes the specified entry from the management access filter.

Default No entries are defined.

Parameters entry-id — An entry ID uniquely identifies a match criteria and the corresponding action. It is recommended that entries are numbered in staggered increments. This allows users to insert a new entry in an existing policy without having to renumber the existing entries.

Values 1 — 9999

protocol

Syntax [no] protocol protocol-id

Context config>system>security>mgmt-access-filter>entry

Description This command configures an IP protocol type to be used as a management access filter match criterion.

The protocol type, such as TCP, UDP, and OSPF, is identified by its respective protocol number. Well-known protocol numbers include ICMP (1), TCP (6), and UDP (17).

The no form the command removes the protocol from the match criteria.

Default No protocol match criterion is specified.

Parameters protocol — The protocol number for the match criterion.

Values 1 to 255 (decimal)

renum

Syntax renum old-entry-number new-entry-number

Context config>system>security>mgmt-access-filter
**Description**

This command renumbers existing management access filter entries to re-sequence filter entries. The exits on the first match found and executes the actions in accordance with the accompanying action command. This may require some entries to be re-numbered differently from most to least explicit.

**Parameters**

- **old-entry-number** — Enter the entry number of the existing entry.
  
  **Values**  
  1 — 9999

- **new-entry-number** — Enter the new entry number that will replace the old entry number.
  
  **Values**  
  1 — 9999

---

**src-port**

**Syntax**

```
src-port {port-id | cpm | lag port-id}
```

**no src-port**

**Context**

```
config>system>security>mgmt-access-filter>entry
```

**Description**

This command restricts ingress management traffic to either the CPM Ethernet port or any other logical port (LAG or port) on the device.

When the source interface is configured, only management traffic arriving on those ports satisfy the match criteria.

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

**Default**

any interface

**Parameters**

- **port-id** — The port ID in the following format: slot[/mda]/port.
  
  **Syntax:**  
  port-id: slot/mda/port

---

**src-ip**

**Syntax**

```
[no] src-ip ([ip-prefix/mask] | [ip-prefix])
```

**Context**

```
config>system>security>mgmt-access-filter>entry
```

**Description**

This command configures a source IP 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 (e., 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  No source IP match criterion is specified.

Parameters  

\textit{ip-prefix’mask} — The IP prefix for the IP match criterion in dotted decimal notation.

\textit{mask} — Specifies the subnet mask length expressed as a decimal integer.

Values 1 — 32 (mask length), 0.0.0.0 — 255.255.255.255 (dotted decimal)
Password Commands

admin-password

Syntax

admin-password password [hash | hash2]
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. This password is valid only for one session. When enabled, no authorization to TACACS+ or RADIUS is performed and the user is locally regarded as an admin user.

This functionality can be enabled in two contexts:

```
config>system>security>password>admin-password
<global> enable-admin
```

NOTE: See the description for the enable-admin on the next page. If the admin-password is configured in the config>system>security>password context, then any user can enter the special mode by entering the enable-admin command.

enable-admin 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, user is given unrestricted access to all the commands.

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

NOTE: The password argument of this command is not sent to the servers. This is consistent with other commands which configure secrets.

Also note that usernames 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 cf1:\destfile
```

In this example, the username '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

password — Configures the password which enables a user to become a system administrator. The maximum length can be up to 20 characters if unhashed, 32 characters if hashed, 54 characters if the hash2 keyword is specified.

hash — Specifies the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted...
**hash2** — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

### enable-admin

**Syntax**
```
enable-admin
```

**Context**
```
<global>
```

**Description**

**NOTE:** See the description for the **admin-password** on the previous page. 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, user is given unrestricted access to all the commands.

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

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

- **show users** — 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:ALA-1# show users
================================================================================
User Type From Login time Idle time
================================================================================
admin Telnet 10.20.30.93 09AUG2006 08:35:23 0d 00:00:00 A
================================================================================
Number of users : 2
'A' indicates user is in admin mode
================================================================================
A:ALA-1#
A:ALA-1# enable-admin
MINOR: CLI Already in admin mode.
A:ALA-1#
```

### aging

**Syntax**
```
aging days
no aging
```

**Context**
```
config>system>security>password
```

7210 SAS-E OS System Management Guide  Page 97
Description
This command configures the number of days a user password is valid before the user must change their password. This parameter can be used to force the user to change the password at the configured interval.

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

Default
No aging is enforced.

Parameters

- **days** — The maximum number of days the password is valid.
  
  **Values**
  
  1 — 500

---

**attempts**

**Syntax**

```
attempts count [time minutes1 [lockout minutes2]]
no attempts
```

**Context**
config>system>security>password

**Description**
This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame.

If the threshold is exceeded, the user is locked out for a specified time period.

If multiple attempts commands are entered, each command overwrites the previously entered command.

The no attempts command resets all values to default.

**Default**
- **count**: 3
- **time minutes**: 5
- **lockout minutes**: 10

**Parameters**

- **count** — The number of unsuccessful login attempts allowed for the specified time. This is a mandatory value that must be explicitly entered.
  
  **Values**
  
  1 — 64

- **time minutes** — The period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out.
  
  **Values**
  
  0 — 60

- **lockout minutes** — The lockout period in minutes where the user is not allowed to login. Allowed values are decimal integers.
  
  **Values**
  
  0 — 1440

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.

**Default**
- **lockout minutes**: 10

**Values**
- **lockout minutes**: 0 — 1440
authentication-order

**Syntax**

```
authentication-order [method-1] [method-2] [method-3] [exit-on-reject]

no authentication-order
```

**Context**

`config>system>security>password`

**Description**

This command configures the sequence in which password authentication, authorization, and accounting is attempted among RADIUS, TACACS+, and local passwords.

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.

If all (operational) methods are attempted and no authentication for a particular login has been granted, then an entry in the security log register the failed attempt. Both the attempted login identification and originating IP address is logged with the a timestamp.

The `no` form of the command reverts to the default authentication sequence.

**Default**

```
authentication-order radius tacplus local
```

- The preferred order for password authentication is 1. RADIUS, 2. TACACS+ and 3. local passwords.

**Parameters**

`method-1` — The first password authentication method to attempt.

- **Default**  radius
- **Values**  radius, tacplus, local

`method-2` — The second password authentication method to attempt.

- **Default**  tacplus
- **Values**  radius, tacplus, local

`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 if 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 as 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:
Configuration Commands

•

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
Context
Description

[no] complexity [numeric] [special-character] [mixed-case]
config>system>security>password
This command configures the complexity requirements of locally administered passwords, HMACMD5-96, HMAC-SHA-96 and des-keys configured in the authentication section.
If more than one complexity command is entered, each command overwrites the previous command.
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.

Default
Parameters

No complexity requirements are configured.
mixed-case — Specifies that at least one upper and one lower case 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.
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 special-character parameters.
However, if this command is used with the authentication none command, the complexity
command is rejected.
Special characters include: ~!@#$%^&*()_+|{}:”<>?`-=\[];’,./.

health-check
Syntax
Context
Description

Page 100

[no] health-check
config>system>security>password
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, based on the
type of the server, a trap will be sent.

7210 SAS-E OS System Management Guide


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.

**Default**  
`health-check`  

### minimum-length

**Syntax**  
`minimum-length value`  
`no minimum-length`  
**Context**  
`config>system>security>password`  
**Description**  
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 system security section. If multiple minimum-length commands are entered each command overwrites the previous entered command. The `no` form of the command reverts to default value.

**Default**  
`minimum-length 6`  
**Parameters**  
`value` — The minimum number of characters required for a password.  
**Values**  
`1 — 8`

### password

**Syntax**  
`password`  
**Context**  
`config>system>security`  
**Description**  
This command creates the context to configure password management parameters.
Profile Management Commands

action

Syntax  
action \{deny | permit\}

Context  
config>system>security>profile user-profile-name>entry entry-id

Description  
This command configures the action associated with the profile entry.

Parameters  
deny — Specifies that commands matching the entry command match criteria are to be denied.
permit — Specifies that commands matching the entry command match criteria will be permitted.

match

Syntax  
match command-string

no match

Context  
config>system>security>profile user-profile-name>entry entry-id

Description  
This command configures a command or subtree commands in subordinate command levels are specified.

Because the 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.

All commands below the hierarchy level of the matched command are denied.

The no form of this command removes a match condition

Default  
none

Parameters  
command-string — The CLI command or CLI tree level that is the scope of the profile entry.

copy

Syntax  
copy \{user source-user | profile source-profile\} to destination [overwrite]

Context  
config>system>security

Description  
This command copies a profile or user from a source profile to a destination profile.

Parameters  
source-profile — The profile to copy. The profile must exist.
dest-profile — The copied profile is copied to the destination profile.
overwrite — Specifies that the destination profile configuration will be overwritten with the copied source profile configuration. A profile will not be overwritten if the overwrite command is not specified.

**default-action**

**Syntax**

default-action {deny-all | permit-all | none}

**Context**

config>system>security>profile user-profile-name

**Description**

This command specifies the default action to be applied when no match conditions are met.

**Default**

none

**Parameters**

deny-all — Sets the default of the profile to deny access to all commands.

permit-all — Sets the default of the profile to permit access to all commands.

Note: permit-all does not change access to security commands. Security commands are only and always available to members of the super-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 the permit-all is executed first. Set the first profile default action 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 deny-all takes effect.

**description**

**Syntax**

description description-string

no description

**Context**

config>system>security>profile user-profile-name>entry entry-id

**Description**

This command creates a text description stored in the configuration file for a configuration context. The description command associates a text string with a configuration context to help identify the context in the configuration file.

The no form of the command removes the string from the context.

**Default**

No description is configured.

**Parameters**

string — 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.
entry

Syntax | [no] entry entry-id
Context | config>system>security>profile user-profile-name
Description | This command is used to create a user profile entry. More than one entry can be created with unique entry-id numbers. 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.

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.

The no form of the command removes the specified entry from the user profile.

Default | No entry IDs are defined.
Parameters | entry-id — An entry-id uniquely identifies a user profile command match criteria and a corresponding action. If more than one entry is configured, the entry-ids should be numbered in staggered increments to allow users to insert a new entry without requiring renumbering of the existing entries.

Values | 1 — 9999

profile

Syntax | [no] profile user-profile-name
Context | config>system>security
Description | This command creates a context to create user profiles for CLI command tree permissions. Profiles are used to either deny or permit user console access to a hierarchical branch or to specific commands.

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. The user-profile-name can consist of up to 32 alphanumeric characters.

The no form of the command deletes a user profile.

Default | user-profile default
Parameters | user-profile-name — 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.
renum

Syntax  renum old-entry-number new-entry-number

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

Description  This command renumbers profile entries to re-sequence the entries.

Since the exits when the first match is found and executes the actions according to accompanying action command, re-numbering is useful to rearrange the entries from most explicit to least explicit.

Parameters  old-entry-number — Enter the entry number of an existing entry.

  Values  1 — 9999

new-entry-number — Enter the new entry number.

  Values  1 — 9999
User Management Commands

access

Syntax

```
[no] access [ftp] [snmp] [console]
```

Context

```
config>system>security>user
config>system>security>user-template
```

Description

This command grants a user permission for FTP, SNMP, console or lawful intercept (LI) access.

If a user requires access to more than one application, then multiple applications can be specified in a single command. Multiple commands are treated additively.

The no form of command removes access for a specific application.

**no access** 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.

Default

No access is granted to the user by default.

Parameters

- **ftp** — Specifies FTP permission.
- **snmp** — Specifies SNMP permission. This keyword is only configurable in the `config>system>security>user` context.
- **console** — Specifies console access (serial port or Telnet) permission.

authentication

Syntax

```
authentication {[none] | [[hash] {md5 key-1 | sha key-1}] privacy {none | des-key key-2}]
```

Context

```
config>system>security>user>snmp
```

Description

This command configures the authentication and encryption method the user must use in order to be validated by the device. SNMP authentication allows the device to validate the managing node that issued the SNMP message and determine if the message has been tampered.

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 **key** parameter.

Default

**authentication none** - No authentication is configured and privacy cannot be configured.

Parameters

- **none** — Do not use authentication. If **none** is specified, then privacy cannot be configured.
- **hash** — When **hash** is not specified, then non-encrypted characters can be entered. When **hash** is configured, then 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.
- **md5 key** — The authentication protocol can either be HMAC-MD5-96 or HMAC-SHA-96.
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).

The complexity of the key is determined by the `complexity` command.

`sha key` — The authentication protocol can be either HMAC-MD5-96 or HMAC-SHA-96.

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).

The complexity of the key is determined by the `complexity` command.

`privacy none` — Do not perform SNMP packet encryption.

Default `privacy none`

`privacy des-key key` — 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.

To remove a previously configured `des-key`, enter `privacy none`.

The complexity of the key is determined by the `complexity` command.

Default `privacy none`

group

group

group group-name
no group

Context `config>system>security>user>snmp`

Description This command associates (or links) a user to a group name. The group name must be configured with the `config>system>security>user>snmp>group` command. 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 `group-name` — 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.

cannot-change-password

cannot-change-password

Syntax `[no] cannot-change-password`

Context `config>system>security>user>console`

Description This command allows a user the privilege to change their password for both FTP and console login.
To disable a user’s privilege to change their password, use the **cannot-change-password** form of the command.

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.

**Default**

**no cannot-change-password**

### Console

**Syntax**

```console
console
```

**Context**

```conf
config>system>security>user
config>system>security>user-template
```

**Description**

This command creates the context to configure user profile membership for the console (either Telnet or serial port user).

### Copy

**Syntax**

```copy
{user source-user | profile source-profile} to destination [overwrite]
```

**Context**

```conf
config>system>security
```

**Description**

This command copies a specific user’s configuration parameters to another (destination) user. The password is set to a carriage return and a new password at login must be selected.

**Parameters**

- `source-user` — The user to copy. The user must already exist.
- `dest-user` — The copied profile is copied to a destination user.
- `overwrite` — Specifies that the destination user configuration will be overwritten with the copied source user configuration. A configuration will not be overwritten if the **overwrite** command is not specified.

### Home-Directory

**Syntax**

```home-directory
url-prefix [directory] [directory/directory…]
```

```no home-directory```

**Context**

```conf
config>system>security>user
config>system>security>user-template
```

**Description**

This command configures the local home directory for the user for both console and FTP access. If the URL or the specified URL/directory structure is not present, then a warning message is issued and the default is assumed. The **no** form of the command removes the configured home directory.
Default

No home-directory

NOTE: If restrict-to-home has been configured no file access is granted and no home-directory is created, if restrict-to-home is not applied then root becomes the user’s home-directory.

Parameters

local-url-prefix [directory] [directory/directory…] — The user’s local home directory URL prefix and directory structure up to 190 characters in length.

profile

Syntax

profile user-profile-name

no profile

Context

config>system>security>user-template

Description

This command configures the profile for the user based on this template.

Parameters

user-profile-name — 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.

login-exec

Syntax

[no] login-exec url-prefix: source-url

Context

config>system>security>user-console
config>system>security>user-template>console

Description

This command configures a user’s login exec file which executes whenever the user successfully logs in to a console session.

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.

The no form of the command disables the login exec file for the user.

Default

No login exec file is defined.

Parameters

url-prefix: source-url — 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 user-profile-name [user-profile-name…]

no member user-profile-name

Context

config>system>security>user>console

Description

This command is used to allow 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**

*user-profile-name* — The user profile name.

### new-password-at-login

**Syntax**

[no] new-password-at-login

**Context**

config>system>security>user>console

**Description**

This command forces the user to change a password at the next console login. The new password applies to FTP but the change can be enforced only by the console, SSH, or Telnet login. The no form of the command does not force the user to change passwords.

**Default**

no new-password-at-login

### password

**Syntax**

password [password] [hash | hash2]

**Context**

config>system>security>user

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

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 if it is a valid hash 2 key to store in the database.

For example,

```plaintext
cfg>system>security# user testuser1
config>system>security>user$ password "zx/Uhc6ReMOZ3BVrWcvk." hash2
config>system>security>user# exit

config>system>security# info
-------------------------------------
... user "testuser1"
     password "zx/Uhc6ReMOZ3BVrWcvk." hash2
     exit
... -------------------------------------
config>system>security#
```
Parameters  

**password** — This is 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 chars if unhashed, 32 characters if hashed. The complexity requirements for the password is determined by the `complexity` command.

All password special characters (#, $, spaces, etc.) must be enclosed within double quotes.

For example:  
```plaintext
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 a # 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: (carriage return).

**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 if 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 if 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`  
`config>system>security>user-template`

**Description**  

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.

If a home-directory is not configured or the home directory is not available, then the user has no file access.

The **no** form of the command allows the user access to navigate to directories above their home directory.

**Default**  

`no restricted-to-home`

---

**snmp**

**Syntax**  

```
snmp
```

---
Context  config>system>security>user
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 node.
7210 SAS OS always uses the configured SNMPv3 user name as the security user name.

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 TACACS+ user template is actively applied to the TACACS+ user.
radius_default — specifies that the default RADIUS user template is actively applied to the RADIUS user if no VSAs are returned with the auth-accept from the RADIUS server.

user

Syntax  [no] user user-name
Context  config>system>security
Description  This command creates a local user and a context to edit the user configuration.
If a new user-name is entered, the user is created. When an existing user-name is specified, the user parameters can be edited.
When creating a new user and then entering the info command, the system displays a password in the output. This is expected behavior in the hash2 scenario. However, when using that user name, there will be no password required. The user can login to the system and then <ENTER> at the password prompt, the user will be logged in.
Unless an administrator explicitly changes the password, it will be null. The hashed value displayed uses the username and null password field, so when the username is changed, the displayed hashed value will change.
The no form of the command deletes the user and all configuration data. Users cannot delete themselves.
Default  none
Parameters  user-name — The name of the user up to 16 characters.
RADIUS Client Commands

access-algorithm

Syntax

access-algorithm {direct | round-robin}
no access-algorithm

Context
config>system>security>radius

Description
This command indicates the algorithm used to access the set of RADIUS servers.

Default
direct

Parameters
direct — The first server will be used as primary server for all requests, the second as secondary and so on.

round-robin — The first server will be used as primary server for the first request, the second server as primary for the second request, and so on. If the router gets to the end of the list, it starts again with the first server.

accounting

Syntax

[no] accounting

Context
config>system>security>radius

Description
This command enables RADIUS accounting.

The no form of this command disables RADIUS accounting.

Default
no accounting

accounting-port

Syntax

accounting-port port
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
port — Specifies the UDP port number.

Values
1 — 65535

Default
1813
authorization

Syntax  [no] authorization

Context  config>system>security>radius

Description  This command configures RADIUS authorization parameters for the system.

Default  no authorization

port

Syntax  port port
        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, Remote Authentication Dial In User Service (RADIUS))

Parameters  port — The TCP port number to contact the RADIUS server.

Values  1 — 65535

radius

Syntax  [no] radius

Context  config>system>security

Description  This command creates the context to configure RADIUS authentication on the router.
             Implement redundancy by configuring multiple server addresses for each router.
             The no form of the command removes the RADIUS configuration.

retry

Syntax  retry count
        no retry

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

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 — 10

**Syntax**

```
server index address ip-address secret key [hash | hash2]
```

**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**

- **index** — 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 — 5

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

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

Syntax  [no] shutdown
Context  config>system>security>radius
Description  This command administratively disables the RADIUS 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. Many objects must be shut down before they may be deleted.

The no form of the command administratively enables the protocol which is the default state.
Default  no shutdown

timeout

Syntax  timeout seconds
        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 seconds
Parameters  seconds — The number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.

Values  1 — 90

use-default-template

Syntax  [no] use-default-template
Context  config>system>security>radius
Description  This command specifies whether the RADIUS user template is actively applied to the RADIUS user if no VSAs are returned with the auth-accept from the RADIUS server. When enabled, the RADIUS user template is actively applied if no VSAs are returned with the auth-accept from the RADIUS server.

The no form of the command disables the command.
TACACS+ Client Commands

server

Syntax

```
server index address ip-address secret key
no server index
```

Context

```
config>system>security>tacplus
```

Description

This command adds a TACACS+ server and configures the TACACS+ server IP address, index, and key values.

Up to five TACACS+ servers can be configured at any one time. TACACS+ servers are accessed in order from lowest index to the highest index for authentication requests.

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

Default

No TACACS+ servers are configured.

Parameters

- `index` — 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.
  - **Values**
    - `1 — 5`

- `address ip-address` — 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.
  - **Values**
    - `ipv4-address a.b.c.d (host bits must be 0)`

- `secret key` — 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 the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.

- `hash2` — Specifies the key is entered in a more complex encrypted form. If the hash2 parameter is not used, the less encrypted hash form is assumed.
  - **Values**

shutdown
**shutdown**

**Syntax**
[no] shutdown

**Context**
config>system>security>tacplus

**Description**
This command administratively disables the TACACS+ 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. Many objects must be shut down before they may be deleted.

The **no** form of the command administratively enables the protocol which is the default state.

**Default**
no shutdown

**tacplus**

**Syntax**
[no] tacplus

**Context**
config>system>security

**Description**
This command creates the context to configure TACACS+ authentication on the router. Configure multiple server addresses for each router for redundancy.

The **no** form of the command removes the TACACS+ configuration.

**accounting**

**Syntax**
accounting [record-type {start-stop | stop-only}]

no accounting

**Context**
config>system>security>tacplus

**Description**
This command 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 be sent or just stop packets be sent.

**Default**
record-type stop-only

**Parameters**

- **record-type start-stop** — Specifies that a TACACS+ start packet is sent whenever the user executes a command.
- **record-type stop-only** — Specifies that a stop packet is sent whenever the command execution is complete.

**authorization**

**Syntax**
[no] authorization
Context config>system>security>tacplus

Description This command configures TACACS+ authorization parameters for the system.

Default no authorization

timeout

Syntax timeout seconds
    no timeout

Context config>system>security>tacplus

Description This command configures the number of seconds the router waits for a response from a TACACS+ server.
The no form of the command reverts to the default value.

Default 3

Parameters seconds — The number of seconds the router waits for a response from a TACACS+ server, expressed as a decimal integer.

Values 1 — 90

shutdown

Syntax [no] shutdown

Context config>system>security>tacplus

Description This command administratively disables the TACACS+ 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. Many objects must be shut down before they may be deleted.
The no form of the command administratively enables the protocol which is the default state.

Default no shutdown

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. |
Generic 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 router.

The **no** form of the command removes the 802.1x configuration.

**radius-plcy**

**Syntax**

[no] radius-plcy

**Context**

config>system>security>dot1x

**Description**

This command creates the context to configure RADIUS server parameters for 802.1x network access control on the router.

NOTE: The RADIUS server configured under the config>system>security>dot1x>radius-plcy context authenticates clients who get access to the data plane of the router as opposed to the RADIUS server configured under the config>system>radius context which authenticates CLI login users who get access to the management plane of the router.

The **no** form of the command removes the RADIUS server configuration for 802.1x.

**retry**

**Syntax**

retry count

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 — 10
server (dot1x)

Syntax

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

Context

config>system>security> dot1x>radius-plcy

Description

This command adds a Dot1x server and configures the Dot1x server IP address, index, and key values.

Up to five Dot1x servers can be configured at any one time. Dot1x 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 Dot1x 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 Dot1x servers are configured.

Parameters

server-index — The index for the Dot1x 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 — 5

address ip-address — The IP address of the Dot1x server. Two Dot1x servers cannot have the same IP address. An error message is generated if the server address is a duplicate.

secret key — The secret key to access the Dot1x server. This secret key must match the password on the Dot1x server.

Values Up to 20 characters in length.

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

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

acct-port acct-port — The UDP port number on which to contact the RADIUS server for accounting requests.

auth-port auth-port — specifies a UDP port number to be used as a match criteria.

Values 1 — 65535

type server-type — Specifies the server type.

Values authorization, accounting, combined
source-address

Syntax  

source-address ip-address  

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  

By default the System IP address is used in the NAS field.

Parameters  

ip-address — The IP prefix for the IP match criterion in dotted decimal notation.

Values  

0.0.0.0 — 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 which is the default state.

Default  

shutdown

timeout

Syntax  

timeout seconds  

no timeout

Context  

config>system>security> dot1x>radius-plcy

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 seconds

Parameters  

seconds — The number of seconds the router waits for a response from a RADIUS server, expressed as a decimal integer.

Values  

1 — 90
TCP Enhanced Authentication

keychain

Syntax  [no] keychain keychain-name
Context  config>system>security
Description  This command enables the context to configure keychain parameters. A keychain must be configured on the system before it can be applied to a session.

The no form of the command removes the keychain nodal context and everything under it from the configuration. If the keychain to be removed is in use when the no keychain command is entered, the command will not be accepted and an error indicating that the keychain is in use will be printed.

Default  none

Parameters  keychain-name — Specifies a keychain name which identifies this particular keychain entry.

Values  An ASCII string up to 32 characters.

direction

Syntax  direction
Context  config>system>security>keychain
Description  This command specifies the data type that indicates the TCP stream direction to apply the keychain.

Default  none

bi

Syntax  bi
Context  config>system>security>keychain>direction
Description  This command configures keys for both send and receive stream directions.

Default  none

uni

Syntax  uni
Context  config>system>security>keychain>direction
Description: This command configures keys for send or receive stream directions.

Default: none

receive

Syntax: receive

Context: config>system>security>keychain>direction>uni

Description: This command enables the receive nodal context. Entries defined under this context are used to authenticate TCP segments that are being received by the router.

Default: none

send

Syntax: send

Context: config>system>security>keychain>direction>uni

Description: This command specifies the send nodal context to sign TCP segments that are being sent by the router to another device.

Default: none

entry

Syntax: entry entry-id key [authentication-key | hash-key | hash2-key] [hash | hash2] algorithm

Context: config>system>security>keychain>direction>bi
config>system>security>keychain>direction>uni>receive
config>system>security>keychain>direction>uni>send

Description: This command defines a particular key in the keychain. Entries are defined by an entry-id. A keychain must have valid entries for the TCP Enhanced Authentication mechanism to work.

The no form of the command removes the entry from the keychain. If the entry is the active entry for sending, then this will cause a new active key to be selected (if one is available using the youngest key rule). If it is the ONLY possible send key, then the system will reject the command with an error indicating the configured key is the only available send key.

If the key is one of the eligible keys for receiving, it will be removed. If the key is the ONLY possible eligible key, then the command will not be accepted, and an error indicating that this is the only eligible key will be output.

The no form of the command deletes the entry.
**Default**
There are no default entries.

**Parameters**

- **entry-id** — Specifies an entry that represents a key configuration to be applied to a keychain.
  - **Values**
    - 0 — 63

- **key** — Specifies a key ID which is used along with **keychain-name** and **direction** to uniquely identify this particular key entry.

- **authentication-key** — Specifies the **authentication-key** that will be used by the encryption algorithm. The key is used to sign and authenticate a protocol packet.
  - The **authentication-key** can be any combination of letters or numbers.
  - **Values**
    - A key must be 160 bits for algorithm hmac-sha-1-96 and must be 128 bits for algorithm aes-128-cmac-96. If the key given with the entry command amounts to less than this number of bits, then it is padded internally with zero bits up to the correct length.

- **algorithm-algorithm** — Specifies an enumerated integer that indicates the encryption algorithm to be used by the key defined in the keychain.
  - **Values**
    - aes-128-cmac-96 — Specifies an algorithm based on the AES standard
    - hmac-sha-1-96 — Specifies an algorithm based on SHA-1.

- **hash-key | hash2-key** — The hash key. The key can be any combination of ASCII characters up to 33 for the **hash-key** and 96 characters for the **hash2-key** in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").
  - This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

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

- **hash2** — Specifies the key is entered in a more complex encrypted form.

**begin-time**

**Syntax**

```
begin-time [date] [hours-minutes] [UTC] [now] [forever]
```

**Context**

- `config>system>security>keychain>direction>bi>entry`
- `config>system>security>keychain>direction>uni>receive>entry`
- `config>system>security>keychain>direction>uni>send>entry`

**Description**

This command specifies the calendar date and time after which the key specified by the keychain authentication key is used to sign and/or authenticate the protocol stream.

If no date and time is set, the begin-time is represented by a date and time string with all NULLs and the key is not valid by default.

**Parameters**

- **date hours-minutes** — Specifies the date and time for the key to become active.
  - **Values**
    - date: YYYY/MM/DD
    - hours-minutes: hh:mm[ss]
now — Specifies the key should become active immediately.

forever — Specifies that the key should always be active.

effective-time

Syntax

end-time [date] [hours-minutes] [UTC] [now] [forever]

Context

config>system>security>keychain>direction>uni>receive>entry
cfg>system>security>keychain>direction>uni>send>entry

description

This command specifies the calendar date and time after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream.

default

forever

Parameters

date — Specifies the calendar date after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream in the YYYY/MM/DD format. When no year is specified the system assumes the current year.

hours-minutes — Specifies the time after which the key specified by the authentication key is no longer eligible to sign and/or authenticate the protocol stream in the hh:mm[:ss] format. Seconds are optional, and if not included, assumed to be 0.

UTC — Indicates that time is given with reference to Coordinated Universal Time in the input.

now — Specifies a time equal to the current system time.

forever — Specifies a time beyond the current epoch.

tolerance

Syntax

tolerance [seconds | forever]

Context

config>system>security>keychain>direction>bi>entry
cfg>system>security>keychain>direction>uni>receive>entry
cfg>system>security>keychain>direction>uni>send>entry

description

This command configures the amount of time that an eligible receive key should overlap with the active send key or to never expire.

Parameters

seconds — Specifies the duration that an eligible receive key overlaps with the active send key.

Values

0 — 4294967294 seconds

forever — Specifies that an eligible receive key overlap with the active send key forever.
tcp-option-number

Syntax: tcp-option-number
Context: config>system>security>keychain

Description: This command enables the context to configure the TCP option number to be placed in the TCP packet header.

receive

Syntax: receive option-number
Context: config>system>security>keychain>tcp-option-number

Description: This command configures the TCP option number accepted in TCP packets received.
Default: 254

Parameters:
- **option-number** — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header.
  
  Values: 253, 254, 253&254

send

Syntax: send option-number
Context: config>system>security>keychain>tcp-option-number

Description: This command configures the TCP option number accepted in TCP packets sent.
Default: 254

Parameters:
- **option-number** — Specifies an enumerated integer that indicates the TCP option number to be used in the TCP header.
  
  Values: 253, 254

dst-port

Syntax: dst-port [tcp/udp port-number] [mask] no dst-port
Context: config>sys>sec>cpm>entry>match

Description: This command specifies the TCP/UDP port to match the destination-port of the packet.
The **no** form of the command removes the destination port match criterion.
Parameters

\textit{dst-port-number} — Specifies the destination port number to be used as a match criteria expressed as a decimal integer.

\textbf{Values} \quad 0 — 65535 (accepted in decimal hex or binary)

\textit{mask} — Specifies the 16 bit mask to be applied when matching the destination port.

**eth-cfm**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>eth-cfm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>config&gt;sys&gt;security&gt;cpu-protection&gt;policy</td>
</tr>
</tbody>
</table>
Show Commands

Security Commands

access-group

**Syntax**  
`access-group [group-name]`

**Context**  
`show>system>security`

**Description**  
This command displays SNMP access group information.

**Parameters**  
*group-name* — This command displays information for the specified access group.

**Output**  
**Security Access Group Output** — The following table describes security access group output fields.

**Table 6: Show System Security Access Group Output Fields**

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

**Sample Output**

```
A:ALA-4# show system security access-group

--------------------------------------------------------------------------
Access Groups
--------------------------------------------------------------------------

<table>
<thead>
<tr>
<th>group name</th>
<th>security model</th>
<th>security level</th>
<th>read view</th>
<th>write view</th>
<th>notify view</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-ro</td>
<td>snmpv1</td>
<td>none</td>
<td>no-security</td>
<td>no-security</td>
<td>no-security</td>
</tr>
<tr>
<td>snmp-ro</td>
<td>snmpv2c</td>
<td>none</td>
<td>no-security</td>
<td>no-security</td>
<td>no-security</td>
</tr>
<tr>
<td>snmp-rw</td>
<td>snmpv1</td>
<td>none</td>
<td>no-security</td>
<td>no-security</td>
<td>no-security</td>
</tr>
<tr>
<td>snmp-rw</td>
<td>snmpv2c</td>
<td>none</td>
<td>no-security</td>
<td>no-security</td>
<td>no-security</td>
</tr>
<tr>
<td>snmp-rwa</td>
<td>snmpv1</td>
<td>none</td>
<td>iso</td>
<td>iso</td>
<td>iso</td>
</tr>
<tr>
<td>snmp-rwa</td>
<td>snmpv2c</td>
<td>none</td>
<td>iso</td>
<td>iso</td>
<td>iso</td>
</tr>
</tbody>
</table>
```
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**

**Authentication Output** — The following table describes system security authentication output fields.

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

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

A:ALA-7>show>system>security# authentication statistics
===============================================================================
Authentication                  sequence : radius tacplus local
===============================================================================
server address   status  type    timeout(secs)  single connection  retry count
-------------------------------------------------------------------------------
10.10.10.103     up      radius  5              n/a                5
10.10.0.1        up      radius  5              n/a                5
10.10.0.2        up      radius  5              n/a                5
10.10.0.3        up      radius  5              n/a                5
-------------------------------------------------------------------------------
radius admin status  : down
tacplus admin status : up
health check         : enabled
-------------------------------------------------------------------------------
No. of Servers: 4
===============================================================================
Login Statistics
===============================================================================
server address      connection errors   accepted logins     rejected logins
-------------------------------------------------------------------------------
10.10.10.103        0                   0                   0
10.10.0.1           0                   0                   0
10.10.0.2           0                   0                   0
10.10.0.3           0                   0                   0
local               n/a                 1                   0
===============================================================================
Authorization Statistics [TACACS+]
===============================================================================
server address      connection errors   sent packets        rejected packets
-------------------------------------------------------------------------------
10.10.10.103        0                   0                   0
===============================================================================
Accounting Statistics
===============================================================================
server address      connection errors   sent packets        rejected packets
-------------------------------------------------------------------------------
10.10.10.103        0                   0                   0
communities

Syntax

Communities

Context

Show>system>security

Description

This command displays SNMP communities.

Output

Communities Output — The following table describes community output fields.

Table 8: Show Communities Output Fields

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

Sample Output

A:ALA-48# show system security communities

Communities

<table>
<thead>
<tr>
<th>community</th>
<th>access</th>
<th>view</th>
<th>version</th>
<th>group name</th>
</tr>
</thead>
<tbody>
<tr>
<td>c11-readonly</td>
<td>r</td>
<td>iso</td>
<td>v2c</td>
<td>c11-readonly</td>
</tr>
<tr>
<td>c11-readwrite</td>
<td>rw</td>
<td>iso</td>
<td>v2c</td>
<td>c11-readwrite</td>
</tr>
<tr>
<td>public</td>
<td>r</td>
<td>no-security</td>
<td>v1 v2c</td>
<td>snmp-ro</td>
</tr>
</tbody>
</table>

No. of Communities: 3

A:ALA-48#
keychain

Syntax  keychain [key-chain] [detail]

Context  show>system>security

Description  This command displays keychain information.

Parameters  key-chain — Specifies the keychain name to display.
detail — Displays detailed keychain information.

Sample Output

*A:ALA-A# show system security keychain test
===============================================================================
Key chain:test
===============================================================================
TCP-Option number send : 254       Admin state : Up
TCP-Option number receive: 254     Oper state : Up
===============================================================================
*A:ALA-A#

*A:ALA-A# show system security keychain test detail
===============================================================================
Key chain:test
===============================================================================
TCP-Option number send : 254       Admin state : Up
TCP-Option number receive: 254     Oper state : Up
===============================================================================
Key entries for key chain: test
===============================================================================
Id               : 0
Direction        : send-receive         Algorithm        : hmac-sha-1-96
Admin State      : Up                   Valid            : Yes
Active           : Yes                  Tolerance        : 300
End Time         : N/A                  End Time (UTC)   : N/A
===============================================================================
Id               : 1
Direction        : send-receive         Algorithm        : aes-128-cmac-96
Admin State      : Up                   Valid            : Yes
Active           : No                   Tolerance        : 300
===============================================================================
Id               : 2
Direction        : send-receive         Algorithm        : aes-128-cmac-96
Admin State      : Up                   Valid            : Yes
Active           : No                   Tolerance        : 500
===============================================================================
*A:ALA-A#
management-access-filter

Syntax  management-access-filter [entry-id]

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  entry-id — Displays information about the specified management access filter entry.

Default  All filter entries

Values  1 — 9999

Output  Management Access Filter Output — The following table describes management access filter output fields.

Table 9: Show Management Access Filter Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Def. action</td>
<td>Permit — Specifies that packets not matching the configured selection criteria in any of the filter entries are permitted.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Deny-host-unreachable — Specifies that packets not matching the configured selection criteria in the filter entries are denied.</td>
</tr>
<tr>
<td>Entry</td>
<td>The entry ID in a policy or filter table.</td>
</tr>
<tr>
<td>Description</td>
<td>A text string describing the filter.</td>
</tr>
<tr>
<td>Src IP</td>
<td>The source IP address used for management access filter match criteria.</td>
</tr>
<tr>
<td>Src interface</td>
<td>The interface name for the nexthop to which the packet should be forwarded if it hits this filter entry.</td>
</tr>
<tr>
<td>Dest port</td>
<td>The destination port.</td>
</tr>
<tr>
<td>Matches</td>
<td>The number of times a management packet has matched this filter entry.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The IP protocol to match.</td>
</tr>
<tr>
<td>Action</td>
<td>The action to take for packets that match this filter entry.</td>
</tr>
</tbody>
</table>
Sample Output

A:ALA-7# show system security management-access-filter
============================================================================= Management Access Filters
=============================================================================

Def. Action : deny
----------------------------------------------------------------------------
Entry         : 10
Description   :
Src IP        : 10.10.10.104
Src interface : undefined
Dest port     : 10.10.10.103
Protocol      : 6
Action        : permit
Matches       : 3876
----------------------------------------------------------------------------
Entry         : 20
Description   : Allow westcoast
Src IP        : 192.168.0.0/16
Src interface : undefined
Dest port     : undefined
Protocol      : undefined
Action        : permit
Matches       : 3876
=============================================================================

password-options

Syntax      password-options
Context      show>system>security
Description  This command displays configured password options.

Output      Password Options Output — The following table describes password options output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password aging in days</td>
<td>Displays the number of days a user password is valid before the user must change their password.</td>
</tr>
<tr>
<td>Number of invalid attempts permitted per login</td>
<td>Displays the number of unsuccessful login attempts allowed for the specified time.</td>
</tr>
<tr>
<td>Time in minutes per login attempt</td>
<td>Displays the period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out.</td>
</tr>
</tbody>
</table>
Table 10: Show Management Access Filter Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lockout period (when threshold breached)</td>
<td>Displays the lockout period in minutes where the user is not allowed to login.</td>
</tr>
<tr>
<td>Authentication order</td>
<td>Displays the sequence in which password authentication is attempted among RADIUS, TACACS+, and local passwords.</td>
</tr>
<tr>
<td>Configured complexity options</td>
<td>Displays the complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96 and DES-keys configured in the authentication section.</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>Displays 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.</td>
</tr>
</tbody>
</table>

Sample Output

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

profile

Syntax        profile [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 are displayed.
Parameters    profile-name — Displays information for the specified user profile.
Output

User Profile Output — The following table describes user profile output fields.

Table 11: Show User Profile Output Fields

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

Sample Output

A:ALA-7# show system security profile administrative
==================================================================================
User Profile
==================================================================================
User Profile : administrative
Def. Action : permit-all
==================================================================================
Entry : 10
Description :
Match Command: configure system security
Action : permit
==================================================================================
Entry : 20
Description :
Match Command: show system security
Action : permit
==================================================================================
No. of profiles:
==================================================================================
A:ALA-7#
source-address

Syntax  source-address
Context  show>system>security
Description  This command displays source-address configured for applications.
Output  Source Address Output — The following table describes source address output fields.

Table 12: Show Source Address Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Displays the source-address application.</td>
</tr>
<tr>
<td>IP address</td>
<td>Displays the source address IP address or interface name.</td>
</tr>
<tr>
<td>Interface Name</td>
<td></td>
</tr>
<tr>
<td>Oper status</td>
<td></td>
</tr>
<tr>
<td>Up</td>
<td>The source address is operationally up.</td>
</tr>
<tr>
<td>Down</td>
<td>The source address is operationally down.</td>
</tr>
</tbody>
</table>

Sample Output

A:SR-7# 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:SR-7#

ssh

Syntax  ssh
Context  show>system>security
Description  This command displays all the SSH sessions as well as the SSH status and fingerprint.
Output  SSH Options Output — The following table describes SSH output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH status</td>
<td>SSH is enabled — Displays that SSH server is enabled.</td>
</tr>
<tr>
<td></td>
<td>SSH is disabled — Displays that SSH server is disabled.</td>
</tr>
</tbody>
</table>
### Security

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Preserve Key</td>
<td>Enabled — Displays that preserve-key is enabled.</td>
</tr>
<tr>
<td></td>
<td>Disabled — Displays that preserve-key is disabled.</td>
</tr>
<tr>
<td>SSH protocol version 1</td>
<td>Enabled — Displays that SSH1 is enabled.</td>
</tr>
<tr>
<td></td>
<td>Disabled — Displays that SSH1 is disabled.</td>
</tr>
<tr>
<td>SSH protocol version 2</td>
<td>Enabled — Displays that SSH2 is enabled.</td>
</tr>
<tr>
<td></td>
<td>Disabled — Displays that SSH2 is disabled.</td>
</tr>
<tr>
<td>Key fingerprint</td>
<td>The key fingerprint is the server’s identity. Clients trying to connect to</td>
</tr>
<tr>
<td></td>
<td>the server verify the server’s fingerprint. If the server fingerprint is not</td>
</tr>
<tr>
<td></td>
<td>known, the client may not continue with the SSH session since the server</td>
</tr>
<tr>
<td></td>
<td>might be spoofed.</td>
</tr>
<tr>
<td>Connection</td>
<td>The IP address of the connected router(s) (remote client).</td>
</tr>
<tr>
<td>Encryption</td>
<td>des — Data encryption using a private (secret) key.</td>
</tr>
<tr>
<td></td>
<td>3des — An encryption method that allows proprietary information to be</td>
</tr>
<tr>
<td></td>
<td>transmitted over untrusted networks.</td>
</tr>
<tr>
<td>Username</td>
<td>The name of the user.</td>
</tr>
<tr>
<td>Number of SSH sessions</td>
<td>The total number of SSH sessions.</td>
</tr>
</tbody>
</table>

### Sample output

**ALA-7# show system security ssh**

SSH is enabled  
SSH preserve key: Enabled  
SSH protocol version 1: Enabled  

SSH protocol version 2: Enabled  

<table>
<thead>
<tr>
<th>Connection</th>
<th>Encryption</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.5.218</td>
<td>3des</td>
<td>admin</td>
</tr>
</tbody>
</table>

Number of SSH sessions : 1

**ALA-7#**

A:ALA-49>config>system>security# show system security ssh  
SSH is disabled  
A:ALA-49>config>system>security#
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**  
**User Output** — The following table describes user output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The name of a system user.</td>
</tr>
</tbody>
</table>
| Need new pwd        | Y — The user must change his password at the next login.  
                     | N — The user is not forced to change his 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 in which the user must change his login password. |
| Attempted logins    | The number of times the user has attempted to login 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. |
Sample Output

A:ALA-7# show system security user

===============================================================================

Users
===============================================================================

<table>
<thead>
<tr>
<th>user id</th>
<th>need</th>
<th>user permissions</th>
<th>password</th>
<th>attempted</th>
<th>failed</th>
<th>local</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin</td>
<td>n</td>
<td>y</td>
<td>n</td>
<td>n</td>
<td>never</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

===============================================================================

A:ALA-7#

A:

ALA-7# show system security user detail

===============================================================================

Users
===============================================================================

<table>
<thead>
<tr>
<th>user id</th>
<th>need</th>
<th>user permissions</th>
<th>password</th>
<th>attempted</th>
<th>failed</th>
<th>local</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin</td>
<td>n</td>
<td>y</td>
<td>n</td>
<td>n</td>
<td>never</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

===============================================================================

User Configuration Detail

===============================================================================

user id : admin

-------------------------------------------------------------------------------

console parameters

-------------------------------------------------------------------------------

new pw required : no           cannot change pw : no
home directory  : cf1:\nrestricted to home : no
login exec file : profile : administrative

-------------------------------------------------------------------------------

snmp parameters

===============================================================================

A:ALA-7#
view

**Syntax**

```
view [view-name] [detail]
```

**Context**

```
show>system>security
```

**Description**

This command displays the SNMP MIB views.

**Parameters**

- `view-name` — Specify the name of the view to display output. If no view name is specified, the complete list of views displays.
- `detail` — Displays detailed view information.

**Output**

**View Output** — The following table describes show view output fields.

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

**Sample Output**

```
A:ALA-48# show system security view
===============================================================================
Views
===============================================================================
view name         oid tree                        mask              permission
-------------------------------------------------------------------------------
iso               1                                                 included
read1             1.1.1.1                         11111111          included
write1            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
no-security       1                                                 included
no-security       1.3.6.1.6.3                                   excluded
```
<table>
<thead>
<tr>
<th>Security</th>
<th>Value</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-security</td>
<td>1.3.6.1.6.3.10.2.1</td>
<td>included</td>
</tr>
<tr>
<td>no-security</td>
<td>1.3.6.1.6.3.11.2.1</td>
<td>included</td>
</tr>
<tr>
<td>no-security</td>
<td>1.3.6.1.6.3.15.1.1</td>
<td>included</td>
</tr>
<tr>
<td>on-security</td>
<td>2</td>
<td>00000000</td>
</tr>
</tbody>
</table>

No. of Views:

A:ALA-48#
## Login Control

**users**

**Syntax**
```
users
```

**Context**
```
show
```

**Description**
Displays console user login and connection information.

**Output**
**Users Output** — The following table describes show users output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user name.</td>
</tr>
<tr>
<td>Type</td>
<td>The user is authorized this access type.</td>
</tr>
<tr>
<td>From</td>
<td>The originating IP address.</td>
</tr>
<tr>
<td>Login time</td>
<td>The time the user logged in.</td>
</tr>
<tr>
<td>Idle time</td>
<td>The amount of idle time for a specific login.</td>
</tr>
<tr>
<td>Number of users</td>
<td>Displays the total number of users logged in.</td>
</tr>
</tbody>
</table>

**Sample Console Users Output**

```
A:ALA-7# show users
```

```
<table>
<thead>
<tr>
<th>User</th>
<th>Type</th>
<th>From</th>
<th>Login time</th>
<th>Idle time</th>
</tr>
</thead>
<tbody>
<tr>
<td>testuser</td>
<td>Console</td>
<td>--</td>
<td>21FEB2007 04:58:55</td>
<td>0d 00:00:00 A</td>
</tr>
</tbody>
</table>
```

Number of users : 1
'A' indicates user is in admin mode
Clear Commands

Authentication Commands

statistics

**Syntax**

```
statistics [interface ip-int-name | ip-address]
```

**Context**

clear>router>authentication

**Description**

This command clears authentication statistics.

**Parameters**

- `ip-int-name` — 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.

- `ip-address` — 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 hex format.
In This Chapter

This chapter provides information to configure SNMP.

Topics in this chapter include:

- SNMP Overview on page 150
  → SNMP Architecture on page 150
  → Management Information Base on page 150
  → SNMP Protocol Operations on page 151
  → SNMP Versions on page 151
  → Management Information Access Control on page 152
  → User-Based Security Model Community Strings on page 153
  → Views on page 153
  → Access Groups on page 153
  → Users on page 154
- Which SNMP Version to Use? on page 155
- Configuration Notes on page 157
SNMP Overview

SNMP Architecture

The Service Assurance Manager (SAM) is comprised of two elements: managers and agents. The manager is the entity through which network management tasks are facilitated. Agents interface managed objects. 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 which 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 router.

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 Alcatel-Lucent (TiMetra) 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 Alcatel-Lucent’s router.

**SNMP Protocol Operations**

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 notifies the manager of significant events that occur on the router.

**SNMP Versions**

The agent supports multiple versions of the SNMP protocol.

- SNMP Version 1 (SNMPv1) is the original Internet-standard network management framework.
  
  SNMPv1 uses a community string match for authentication.

- The implementation uses SNMPv2c, the community-based administrative framework for SNMPv2. SNMPv2c uses a community string match for authentication.

- In SNMP Version 3 (SNMPv3), USM defines the user authentication and encryption features. 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 username match for authentication.
Management Information Access Control

By default, the 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 provide 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 which 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 router.

Alcatel-Lucent’s 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 associates 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 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 for the view 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.

Pre-defined views are available that are particularly useful when configuring SNMPv1 and SNMPv2c.

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

Access Groups

Access groups associate a user group and a security model to 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, in essence, is a template which defines a combination of access privileges and views. A group can be associated to 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 which a user must use in order to be validated by the device 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 (see Access Groups).
Which SNMP Version to Use?

SNMPv1 and SNMPv2c do not provide security, authentication, or encryption. Without authentication, a non authorized 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 device. SNMP authentication allows the router to validate the managing node that issued the SNMP message and determine if the message was tampered with.

Figure 3 depicts the configuration requirements to implement SNMPv1/SNMPv2c, and SNMPv3.
Figure 3: SNMPv1 and SNMPv2c Configuration and Implementation Flow
Configuration Notes

This section describes SNMP configuration caveats.

General

- To avoid management systems attempting to manage a partially booted system, SNMP will remain in a shut down state if the configuration file fails to complete during system startup. While shutdown, 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` CLI 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 not, the previously configured SNMP communities and logger trap-target notify communities will not be valid for the new engine ID.
Configuring SNMP with CLI

This section provides information about configuring SNMP with CLI.

Topics in this chapter include:

- SNMP Configuration Overview on page 160
- Basic SNMP Security Configuration on page 161
- Configuring SNMP Components on page 162
SNMP Configuration Overview

This section describes how to configure SNMP components which apply to SNMPv1 and SNMPv2c, and SNMPv3 on the router.

- Configuring SNMPv1 and SNMPv2c on page 160
- Configuring SNMPv3 on page 160

Configuring SNMPv1 and SNMPv2c

Alcatel-Lucent routers are based on SNMPv3. To use routers with SNMPv1 and/or SNMPv2c, SNMP community strings must be configured. Three pre-defined 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

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

- Configure views
- Configure access groups
- Configure 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.

```
A:ALA-1(config)# system security snmp# info detail
----------------------------------------------
view iso subtree 1
  mask ff type included
  exit
view no-security subtree 1
  mask ff type included
  exit
view no-security subtree 1.3.6.1.6.3
  mask ff type excluded
  exit
view no-security subtree 1.3.6.1.6.3.10.2.1
  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 on page 163
- Configuring View Options on page 164
- Configuring Access Options on page 165
- Configuring USM Community Options on page 167
- Configuring Other SNMP Parameters on page 168

**CLI Syntax:**
```
config>system>security>snmp
    attempts [count] [time minutes1] [lockout minutes2]
    community community-string access-permissions [version SNMP version]
    usm-community community-string 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
    [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 these 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 pre-configured by the agent for SNMPv1/SNMPv2c.

Use the following CLI syntax to configure community options:

**CLI Syntax:**
```plaintext
config>system>security>snmp
community community-string access-permissions [version SNMP version]
```

The following displays an SNMP community configuration example:

```
*A:cses-A13>config>system>security>snmp# info
----------------------------------------------
community "uTdc9j48PRkxn5DcSjchk" hash2 rwa version both
community "Lla.RtAyRW2" hash2 r version v2c
community "r0a159kIOfg" hash2 r version both
----------------------------------------------
*A:cses-A13>config>system>security>snmp#
```
Configuring View Options

Use the following CLI syntax to configure view options:

**CLI Syntax:**
```
cfg>system>security>snmp
    view view-name subtree oid-value
        mask mask-value [type {included|excluded}]
```

The following displays a view configuration example:

```
*A:cses-A13>cfg>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 "uTd9j48PBRkxn5DcSjchk" hash2 rwa version both
community "Lla.RtAyRW2" hash2 r version v2c
community "r0al59kIOfg" hash2 r version both
----------------------------------------------
*A:cses-A13>cfg>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 SNMPv2. 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 displays an access configuration with the view configurations.

```
*A:cses-A13>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 "test" security-model usm security-level auth-no-pr
    ivacy read "testview" write "testview" notify "testview"
    community "uTdc9j48PBRRkxn5DcSjchk" hash2 rwa version both
    community "Lla.RtAyRW2" hash2 r version v2c
    community "r0a159kIOf" hash2 r version both
-------------------------------
*A:cses-A13>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 displays a user’s SNMP configuration example.

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

```
A:ALA-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 implementation of SNMP uses SNMPv3. However, to implement SNMPv1 and SNMPv2c, USM community strings must be explicitly configured.

Use the following CLI syntax to configure USM community options:

**CLI Syntax:**
```
cfg>system>snmp
    usm-community community-string group group-name
```

The following displays a SNMP community configuration example:

A:ALA-1>config>system>snmp# info
-----------------------------------------------
view "testview" subtree "1"
    mask ff
    exit
    view "testview" subtree "1.3.6.1.2"
    mask ff type excluded
    exit
    access group "test" security-model usm security-level auth-no-prv
    ivaly read "testview" write "testview" notify "testview"
    community "uTdc9j48PRkxn5DcSjchk" hash2 rwa version both
    community "Lla.RtAyRW2" hash2 r version v2c
    community "r0a159kIOfg" hash2 r version both
-----------------------------------------------
A:ALA-1>config>system>snmp#

The group **grouptest** was configured in the **cfg>system>snmp>access** CLI context.
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:

```
A:ALA-104>config>system>snmp# info detail
----------------------------------------------
shutdown
engineID  "0000xxxx00000000xxxxx00"
packet-size 1500
general-port 161
----------------------------------------------
A:ALA-104>config>system>snmp#
```
SNMP Command Reference

Command Hierarchies

Configuration Commands

SNMP System Commands

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

SNMP Security Commands

```plaintext
config
  — system
  — security
    — snmp
      — access group group-name security-model [security-model] security-level [context context-name [prefix-match]] [read view-name-1] [write view-name-2] [notify view-name-3]
      — no access group group-name [security-model] [security-model] 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 access-permissions [version SNMP-version]
      — 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]
        — mask mask-value [type {included | excluded}]
        — no mask
```
The following commands configure user-specific SNMP features. Refer to the Security section for CLI syntax and command descriptions.

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

**Show Commands**

**show**
- snmp
  - counters
- system
  - information
  - security
    - access-group [group-name]
    - authentication [statistics]
    - communities
    - password-options [entry-id]
    - password-options
    - profile [profile-name]
    - ssh
    - user [user-id] [detail]
    - view [view-name] [detail]
### Configuration Commands

## SNMP System Commands

### engineID

**Syntax**

```
[no] engineID engine-id
```

**Context**

```
config>system>snmp
```

**Description**

This command sets the SNMP engineID to uniquely identify the SNMPv3 node. By default, the engineID is generated using information from the system backplane.

If 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 not, the previously configured SNMP communities and logger trap-target notify communities will not be valid for the new engine ID.

**Note:** In conformance with IETF standard RFC 2274, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, hashing algorithms which generate SNMPv3 MD5 or SHA security digest keys use the engineID. Changing the SNMP engineID invalidates all SNMPv3 MD5 and SHA security digest keys and may render the node unmanageable.

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 engineID.

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

**Default**

The engine ID is system generated.

**Parameters**

- `engine-id` — 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 port-number
no general-port
```

**Context**

```
config>system>snmp
```

**Description**

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 `config>log>snmp-trap-group>trap-target` CLI command.
The `no` form of the command reverts to the default value.

**Default**

161

**Parameters**

`port-number` — The port number used to send SNMP traffic other than traps.

**Values**

1 — 65535 (decimal)

---

### packet-size

**Syntax**

```
packet-size bytes
no packet-size
```

**Context**

`config>system>snmp`

**Description**

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.

The `no` form of this command to revert to default.

**Default**

1500 bytes

**Parameters**

`bytes` — The SNMP packet size in bytes.

**Values**

484 — 9216

---

### snmp

**Syntax**

```
snmp
```

**Context**

`config>system`

**Description**

This command creates the context to configure SNMP parameters.

---

### shutdown

**Syntax**

```
[no] shutdown
```

**Context**

`config>system>snmp`

**Description**

This command administratively disables SNMP agent operations. System management can then only be performed using the command line interface (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 `config>log>snmp-trap-group` context.

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.

The `no` form of the command administratively enables SNMP which is the default state.

**Default**

`no shutdown`
SNMP Security Commands

access group

Syntax: [no] 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]

Context: config>system>security>snmp

Description: 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 SNMPv2. An access group is defined by a unique combination of the group name, security model and security level.

Access must be configured unless security is limited to SNMPv1/SNMPv2c with community strings (see the community on page 175).

Default access group configurations cannot be modified or deleted.

To remove the user group with associated, security model(s), and security level(s), use:
no access group group-name

To remove a security model and security level combination from a group, use:
no access group group-name security-model {snmpv1 | snmpv2c | usm} security-level {no-auth-no-privacy | auth-no-privacy | privacy}

Default: none

Parameters:

- group-name — Specify a unique group name up to 32 characters.

- 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.

- 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.

- 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.

- 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).

**read view-name** — 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.

Default none

**write view-name** — 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** — specifies 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 none

### attempts

**Syntax**

```
attempts [count] [time minutes1] [lockout minutes2]
no attempts
```

**Context**

config>system>security>snmp

**Description**

This command configures a threshold value 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.

If the threshold is exceeded, the host is locked out for the lockout time period.

If multiple attempts commands are entered, each command overwrites the previously entered command.

The no form of the command resets the parameters to the default values.

**Default**

```
attempts 20 time 5 lockout 10
```

— 20 failed SNMP attempts allowed in a 5 minute period with a 10 minute lockout for the host if exceeded.

**Parameters**

**count** — The number unsuccessful SNMP attempts allowed for the specified time.

Default 20

Values 1 — 64

**time minutes1** — The period of time, in minutes, that a specified number of unsuccessful attempts can be made before the host is locked out.

Default 5

Values 0 — 60
lockout minutes — The lockout period in minutes where the host is not allowed to login. 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.

Default 10
Values 0 — 1440

community

Syntax community community-string access-permissions [version SNMP-version]
no community community-string]
Context config>system>security>snmp
Description 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.

When configured, community implies a security model for SNMPv1 and SNMPv2c only. For SNMPv3 security, the access group command on page 173 must be configured.

The no form of the command removes a community string.

Default none
Parameters community-string — Configure the SNMPv1 / SNMPv2c community string.
access-permissions — • 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.
• rwa — Grants read and write access to all objects in the MIB, including security.
• vpls-mgmt — Assigns a unique SNMP community string to the management virtual router.
version {v1 | v2c | both} — Configures the scope of the community string to be for SNMPv1, SNMPv2c, or both SNMPv1 and SNMPv2c access.

Default both

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 would be 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 such 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**

none

**Parameters**

mask-value — The mask value associated with the OID value determines whether the sub-identifiers are included or excluded from the view. (Default: all 1s)

The mask can be entered either:

- In hex. For example, 0xfc.

- In binary. 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.

**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. (Default: included).

- excluded - All MIB subtree objects that are identified with a 1 in the mask are denied access in the view. (Default: included).

Default included

---

**snmp**

**Syntax**

`snmp`

**Context**

`config>system>security`

**Description**

This command creates the context to configure SNMPv1, SNMPv2, and SNMPv3 parameters.
usm-community

Syntax

usm-community community-string group group-name
no usm-community community-string

Context

config>system>security>snmp

Description

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.

Alcatel-Lucent’s SR 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 which specify more specific OIDs (MIB objects in the subtree) can be configured.

The no form of this command removes a community string.

Default

none

Parameters

community-string — Configures the SNMPv1/SNMPv2c community string to determine the SNMPv3 access permissions to be used.

group — Specify 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.

(Default: none)

view

Syntax

view view-name subtree oid-value
no view view-name [subtree oid-value]

Context

config>system>security>snmp

Description

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.

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 which are used to assign specific access group permissions to created views and assigned to particular access groups.

Multiple subtrees can be added or removed from a view name to tailor a view to the requirements of the user access group.

The no view view-name command removes a view and all subtrees.

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

Default

No views are defined.

Parameters

view-name — Enter a 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 for customizing visibility and write capabilities to specific user requirements.
Show Commands

counters

**Syntax**
counters

**Context**
show>snmp

**Description**
This command displays SNMP counters information. SNMP counters will continue to increase even when SNMP is shut down. Some internal modules communicate using SNMP packets.

**Output**

**Counters Output** — The following table describes SNMP counters output fields.

**Table 15: Counters Output Fields**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in packets</td>
<td>Displays the total number of messages delivered to SNMP from the transport service.</td>
</tr>
<tr>
<td>in gets</td>
<td>Displays the number of SNMP get request PDUs accepted and processed by SNMP.</td>
</tr>
<tr>
<td>in getnexts</td>
<td>Displays the number of SNMP get next PDUs accepted and processed by SNMP.</td>
</tr>
<tr>
<td>in sets</td>
<td>Displays the number of SNMP set request PDUs accepted and processed by SNMP.</td>
</tr>
<tr>
<td>out packets</td>
<td>Displays the total number of SNMP messages passed from SNMP to the transport service.</td>
</tr>
<tr>
<td>out get responses</td>
<td>Displays the number of SNMP get response PDUs generated by SNMP.</td>
</tr>
<tr>
<td>out traps</td>
<td>Displays the number of SNMP Trap PDUs generated by SNMP.</td>
</tr>
<tr>
<td>variables requested</td>
<td>Displays the number of MIB objects requested by SNMP.</td>
</tr>
<tr>
<td>variables set</td>
<td>Displays the number of MIB objects set by SNMP as the result of receiving valid SNMP set request PDUs.</td>
</tr>
</tbody>
</table>

**Sample Output**

A:ALA-1# show snmp counters

SNMP counters:

  in packets : 463
information

Syntax

information

Context

show>system

Description

This command lists the SNMP configuration and statistics.

Output

System Information Output Fields — The following table describes system information output fields.

Table 16: Show System Information Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>The name configured for the device.</td>
</tr>
<tr>
<td>System Contact</td>
<td>The text string that identifies the contact name for the device.</td>
</tr>
<tr>
<td>System Location</td>
<td>The text string that identifies the location of the device.</td>
</tr>
<tr>
<td>System Coordinates</td>
<td>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.</td>
</tr>
<tr>
<td>System Up Time</td>
<td>The time since the last reboot.</td>
</tr>
<tr>
<td>SNMP Port</td>
<td>The port which SNMP sends responses to management requests.</td>
</tr>
<tr>
<td>SNMP Engine ID</td>
<td>The ID for either the local or remote SNMP engine to uniquely identify the SNMPv3 node.</td>
</tr>
<tr>
<td>SNMP Max Message Size</td>
<td>The maximum size SNMP packet generated by this node.</td>
</tr>
<tr>
<td>SNMP Admin State</td>
<td>Enabled – SNMP is administratively enabled. Disabled – SNMP is administratively disabled.</td>
</tr>
<tr>
<td>SNMP Oper State</td>
<td>Enabled – SNMP is operationally enabled. Disabled – SNMP is operationally disabled.</td>
</tr>
</tbody>
</table>
Table 16: Show System Information Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| SNMP Index Boot Status | Persistent — Persistent indexes at the last system reboot was enabled.  
Disabled — Persistent indexes at the last system reboot was disabled. |
| SNMP Sync State | The state when the synchronization of configuration files between the primary and secondary sessions finish. |
| Telnet/SSH/FTP Admin | Displays the administrative state of the Telnet, SSH, and FTP sessions. |
| Telnet/SSH/FTP Oper | Displays 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 | Displays the URL and filename of the configuration file used for the most recent boot. |
| Last Boot Cfg Version | Displays the version of the configuration file used for the most recent boot. |
| Last Boot Config Header | Displays header information of the configuration file used for the most recent boot. |
| Last Boot Index Version | Displays the index version used in the most recent boot. |
| Last Boot Index Header | Displays the header information of the index used in the most recent boot. |
| Last Saved Config | Displays the filename of the last saved configuration. |
### Table 16: Show System Information Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Last Saved</td>
<td>Displays the time the configuration was most recently saved.</td>
</tr>
<tr>
<td>Changes Since Last Save</td>
<td>Yes — The configuration changed since the last save.</td>
</tr>
<tr>
<td></td>
<td>No — The configuration has not changed since the last save.</td>
</tr>
<tr>
<td>Time Last Modified</td>
<td>Displays the time of the last modification.</td>
</tr>
<tr>
<td>Max Cfg/BOF Backup Rev</td>
<td>The maximum number of backup revisions maintained for a configuration file.</td>
</tr>
<tr>
<td></td>
<td>This value also applies to the number of revisions maintained for the BOF file.</td>
</tr>
<tr>
<td>Cfg-OK Script</td>
<td>URL — The location and name of the CLI script file executed following successful completion of the boot-up configuration file execution.</td>
</tr>
<tr>
<td></td>
<td>N/A — No CLI script file is executed.</td>
</tr>
<tr>
<td>Cfg-OK Script Status</td>
<td>Successful/Failed — The results from the execution of the CLI script file specified in the Cfg-OK Script location.</td>
</tr>
<tr>
<td></td>
<td>Not used — No CLI script file was executed.</td>
</tr>
<tr>
<td>Cfg-Fail Script</td>
<td>URL — The location and name of the CLI script file executed following a failed boot-up configuration file execution.</td>
</tr>
<tr>
<td></td>
<td>Not used — No CLI script file was executed.</td>
</tr>
<tr>
<td>Cfg-Fail Script Status</td>
<td>Successful/Failed — The results from the execution of the CLI script file specified in the Cfg-Fail Script location.</td>
</tr>
<tr>
<td></td>
<td>Not used — No CLI script file was executed.</td>
</tr>
<tr>
<td>Management IP address</td>
<td>The Management IP address of the node.</td>
</tr>
<tr>
<td>DNS Server</td>
<td>The DNS address of the node.</td>
</tr>
<tr>
<td>DNS Domain</td>
<td>The DNS domain name of the node.</td>
</tr>
<tr>
<td>BOF Static Routes</td>
<td>To — The static route destination.</td>
</tr>
<tr>
<td></td>
<td>Next Hop — The next hop IP address used to reach the destination.</td>
</tr>
<tr>
<td></td>
<td>Metric — Displays the priority of this static route versus other static routes.</td>
</tr>
<tr>
<td></td>
<td>None — No static routes are configured.</td>
</tr>
</tbody>
</table>
### Sample Output

```
A:ALA-1# show system information
===============================================================================================
System Information
===============================================================================================
System Name            : ALA-1
System Type            :
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             : cf1:
Image Source           : primary
Config Source          : primary
Last Boot Cfg Version  : THU FEB 15 16:58:20 2007 UTC
Last Boot Config Header: # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SR
                          Copyright (c) 2000-2007 Alcatel-Lucent. # All rights reserved. All use subject to applicable license agreements. # Built on Sun Feb 11 19:26:23 PST 2007 by builder in /rel0.0/I1042/panos/main # Generated THU FEB 11 16:58:20 2007 UTC
Last Boot Index Version: N/A
Last Boot Index Header  : # TiMOS-B-0.0.I1042 both/i386 Alcatel-Lucent SR
                          Copyright (c) 2000-2007 Alcatel-Lucent. # All rights reserved. All use subject to applicable license agreements. # Built on Sun Feb 11 19:26:23 PST 2007 by builder in /rel0.0/I1042/panos/main # Generated THU FEB 15 16:58:20 2007 UTC
Last Saved Config      : N/A
Time Last Saved        : N/A
Changes Since Last Save: No
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
DNS Server             : 192.168.1.246
DNS Domain             : eng.timetra.com
BOF Static Routes      :
```

access-group

Syntax  access-group group-name

Context  show>system>security

Description  This command displays access-group information.

Output  System Information Output — The following table describes the access-group output fields.

Table 17: Show System Information Output Fields

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

Sample Output

A:ALA-1# 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  no-security  
snmp-ro     snmpv2c   none      no-security  no-security  
snmp-rw     snmpv1    none      no-security  no-security  
===============================================================================
A:ALA-1#
authentication

Syntax  authentication [statistics]

Context  show>system>security

Description  This command displays authentication information.

Output  Authentication Output — The following table describes the authentication output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sequence</td>
<td>The authentication order in which password authentication, authorization, and accounting is attempted among RADIUS, TACACS+, and local passwords.</td>
</tr>
<tr>
<td>server address</td>
<td>The address of the RADIUS, TACACS+, or local server.</td>
</tr>
<tr>
<td>status</td>
<td>The status of the server.</td>
</tr>
<tr>
<td>type</td>
<td>The type of server.</td>
</tr>
<tr>
<td>timeout (secs)</td>
<td>Number of seconds the server will wait before timing out.</td>
</tr>
<tr>
<td>single connection</td>
<td>Specifies whether a single connection is established with the server. The connection is kept open and is used by all the TELNET/SSH/FTP sessions for AAA operations.</td>
</tr>
<tr>
<td>retry count</td>
<td>The number of attempts to retry contacting the server.</td>
</tr>
</tbody>
</table>
Sample Output

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

communities

Syntax communities
Context show>system>security
Description This command lists SNMP communities and characteristics.
Output Communities Output — The following table describes the communities output fields.
Table 18: Show Communities Output Fields

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

Sample Output

A:ALA-1# show system security communities
-----------------------------------------------------------------------------------------------
Communities
-----------------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>community</th>
<th>access</th>
<th>view</th>
<th>version</th>
<th>group name</th>
</tr>
</thead>
<tbody>
<tr>
<td>private</td>
<td>rw</td>
<td>iso</td>
<td>v1 v2c</td>
<td>snmp-rwa</td>
</tr>
<tr>
<td>public</td>
<td>r</td>
<td>no-security</td>
<td>v1 v2c</td>
<td>snmp-ro</td>
</tr>
<tr>
<td>rwa</td>
<td>rwa</td>
<td>n/a</td>
<td>v2c</td>
<td>snmp-trap</td>
</tr>
</tbody>
</table>
-----------------------------------------------------------------------------------------------
No. of Communities: 3
-----------------------------------------------------------------------------------------------
A:ALA-1#

password-options

Syntax        | password-options
Context       | show>system>security
Description   | This command displays password options.
**Password-Options Output** — The following table describes password-options output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password aging in days</td>
<td>Number of days a user password is valid before the user must change his password.</td>
</tr>
<tr>
<td>Number of invalid attempts permitted per login</td>
<td>Displays the maximum number of unsuccessful login attempts allowed for a user.</td>
</tr>
<tr>
<td>Time in minutes per login attempt</td>
<td>Displays the time in minutes that user is to be locked out.</td>
</tr>
<tr>
<td>Lockout period (when threshold breached)</td>
<td>Displays the number of minutes the user is locked out if the threshold of unsuccessful login attempts has exceeded.</td>
</tr>
<tr>
<td>Authentication order</td>
<td>Displays the most preferred method to authenticate and authorize a user.</td>
</tr>
<tr>
<td>Configured complexity options</td>
<td>Displays the complexity requirements of locally administered passwords, HMAC-MD5-96, HMAC-SHA-96 and DES-keys configured in the authentication section.</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>Displays the minimum number of characters required in the password.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
A:ALA-48>show>system>security# password-options
===============================================================================
Password Options
===============================================================================
Password aging in days                           : 365
Number of invalid attempts permitted per login   : 5
Time in minutes per login attempt                : 5
Lockout period (when threshold breached)         : 20
Authentication order                             :
Configured complexity options                    :
Minimum password length                          : 8
===============================================================================
A:ALA-48>show>system>security#
```

**profile**

**Syntax**  
`profile [profile-name]`

**Context**  
`show>system>security`

**Description**  
This command displays user profiles for CLI command tree permissions.
**Parameters**  
*profile-name* — Specify the profile name to display information about a single user profile. If no profile name is displayed, the entire list of profile names are listed.

**Output**  
**Profile Output** — The following table describes the profile output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Profile</td>
<td>default — The action to be given to the user profile if none of the entries match the command.</td>
</tr>
<tr>
<td></td>
<td>administrative — specifies the administrative state for this profile.</td>
</tr>
<tr>
<td>Def. Action</td>
<td>none — No action is given to the user profile when none of the entries match the command.</td>
</tr>
<tr>
<td></td>
<td>permit-all — The action to be taken when an entry matches the command.</td>
</tr>
<tr>
<td>Entry</td>
<td>10 - 80 — Each entry represents the configuration for a system user.</td>
</tr>
<tr>
<td>Description</td>
<td>A text string describing the entry.</td>
</tr>
<tr>
<td>Match Command</td>
<td>administrative — Enables the user to execute all commands.</td>
</tr>
<tr>
<td></td>
<td>configure system security — Enables the user to execute the <strong>config system security</strong> command.</td>
</tr>
<tr>
<td></td>
<td>enable-admin — Enables the user to enter a special administrative mode by entering the <strong>enable-admin</strong> command.</td>
</tr>
<tr>
<td></td>
<td>exec — Enables the user to execute (exec) the contents of a text file as if they were CLI commands entered at the console.</td>
</tr>
<tr>
<td></td>
<td>exit — Enables the user to execute the <strong>exit</strong> command.</td>
</tr>
<tr>
<td></td>
<td>help — Enables the user to execute the <strong>help</strong> command.</td>
</tr>
<tr>
<td></td>
<td>logout — Enables the user to execute the <strong>logout</strong> command.</td>
</tr>
<tr>
<td></td>
<td>password — Enables the user to execute the <strong>password</strong> command.</td>
</tr>
<tr>
<td></td>
<td>show config — Enables the user to execute the <strong>show config</strong> command.</td>
</tr>
<tr>
<td></td>
<td>show — Enables the user to execute the <strong>show</strong> command.</td>
</tr>
<tr>
<td></td>
<td>show system security — Enables the user to execute the <strong>show system security</strong> command.</td>
</tr>
<tr>
<td>Action</td>
<td>permit — Enables the user access to all commands.</td>
</tr>
<tr>
<td></td>
<td>deny-all — Denies the user access to all commands.</td>
</tr>
</tbody>
</table>
A:ALA-48>config>system>snmp# show system security profile
===============================================================================
User Profile
===============================================================================
User Profile : test
Def. Action : none
-------------------------------------------------------------------------------
Entry : 1
Description :
Match Command: 
Action : unknown
===============================================================================
User Profile : default
Def. Action : none
-------------------------------------------------------------------------------
Entry : 10
Description :
Match Command: exec
Action : permit
-------------------------------------------------------------------------------
Entry : 20
Description :
Match Command: exit
Action : permit
-------------------------------------------------------------------------------
Entry : 30
Description :
Match Command: help
Action : permit
-------------------------------------------------------------------------------
Entry : ...
-------------------------------------------------------------------------------
Entry : 80
Description :
Match Command: enable-admin
Action : permit
===============================================================================
User Profile : administrative
Def. Action : permit-all
-------------------------------------------------------------------------------
Entry : 10
Description :
Match Command: configure system security
Action : permit
-------------------------------------------------------------------------------
Entry : 20
Description :
Match Command: show system security
Action : permit
-------------------------------------------------------------------------------
No. of profiles: 3
===============================================================================
A:ALA-48>config>system>snmp#
ssh

Syntax  ssh
Context  show>system>security
Description  This command displays all the SSH sessions as well as the SSH status and fingerprint.
Output  **SSH Options Output** — The following table describes SSH output fields.

### Table 19: Show SSH Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH status</td>
<td><strong>SSH is enabled</strong> — Displays that SSH server is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>SSH is disabled</strong> — Displays that SSH server is disabled.</td>
</tr>
<tr>
<td>Key fingerprint</td>
<td>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.</td>
</tr>
<tr>
<td>Connection</td>
<td>The IP address of the connected router(s) (remote client).</td>
</tr>
<tr>
<td>Encryption</td>
<td>des — Data encryption using a private (secret) key.</td>
</tr>
<tr>
<td></td>
<td>3des — An encryption method that allows proprietary information to be transmitted over untrusted networks.</td>
</tr>
<tr>
<td>Username</td>
<td>The name of the user.</td>
</tr>
<tr>
<td>Number of SSH sessions</td>
<td>The total number of SSH sessions.</td>
</tr>
</tbody>
</table>

### Sample output

```
A:ALA-7# show system security ssh
SSH is enabled
===========================================================================
Connection    Encryption    Username
===========================================================================
192.168.5.218  3des          admin
===========================================================================
Number of SSH sessions : 1
===========================================================================
A:ALA-7#

A:ALA-49>config>system>security# show system security ssh
SSH is disabled
A:ALA-49>config>system>security#
```
user

Syntax  
users [user-id] [detail]

Context  
show>system>security

Description  
This command displays user information.

Output  
User Output — The following table describes user information output fields.

Table 20:  Show User Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The name of a system user.</td>
</tr>
<tr>
<td>Need New PWD</td>
<td>Yes — The user must change his password at the next login.</td>
</tr>
<tr>
<td></td>
<td>No — The user is not forced to change his password at the next login.</td>
</tr>
<tr>
<td>User Permission</td>
<td>Console — Specifies whether the user is permitted console/Telnet access.</td>
</tr>
<tr>
<td></td>
<td>FTP — Specifies whether the user is permitted FTP access.</td>
</tr>
<tr>
<td></td>
<td>SNMP — Specifies whether the user is permitted SNMP access.</td>
</tr>
<tr>
<td>Password expires</td>
<td>The date on which the current password expires.</td>
</tr>
<tr>
<td>Attempted logins</td>
<td>The number of times the user has attempted to login irrespective of whether the login succeeded or failed.</td>
</tr>
<tr>
<td>Failed logins</td>
<td>The number of unsuccessful login attempts.</td>
</tr>
<tr>
<td>Local Conf.</td>
<td>Y — Password authentication is based on the local password database.</td>
</tr>
<tr>
<td></td>
<td>N — Password authentication is not based on the local password database.</td>
</tr>
</tbody>
</table>

Sample Output

A:ALA-1# show system security user
===============================================================================
Users
===============================================================================
user id          need new pwd console ftp snmp password expires attempted logins failed logins local
---              ----- ------- ------- ------- ------- --------- ----------- ------------ -----
admin            n y n n n never 2 0 y
#testuser        n n n y never 0 0 y
-----------------------------------------------------------------------------
Number of users : 2
===============================================================================
A:ALA-1#
view

Syntax  view [view-name] [detail]

Context show>system>security

Description This command lists one or all views and permissions in the MIB-OID tree.

Output System Security View Output — The following table describes system security view output fields.

Table 21: Show System Security View Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View name</td>
<td>The name of the view. Views control the accessibility of a MIB object within the configured MIB view and subtree.</td>
</tr>
<tr>
<td>OID tree</td>
<td>The Object Identifier (OID) value. OIDs uniquely identify MIB objects in the subtree.</td>
</tr>
<tr>
<td>Mask</td>
<td>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.</td>
</tr>
<tr>
<td>Permission</td>
<td>Included — Specifies to include MIB subtree objects.</td>
</tr>
<tr>
<td></td>
<td>Excluded — Specifies to exclude MIB subtree objects.</td>
</tr>
<tr>
<td>No. of Views</td>
<td>The total number of configured views.</td>
</tr>
<tr>
<td>Group name</td>
<td>The access group name.</td>
</tr>
</tbody>
</table>

Sample Output

A:ALA-1# show system security view
-----------------------------------------------------------------------------------------------------------------------------------
Views
-----------------------------------------------------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>view name</th>
<th>oid tree</th>
<th>mask</th>
<th>permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>iso</td>
<td>1</td>
<td></td>
<td>included</td>
</tr>
<tr>
<td>no-security</td>
<td>1</td>
<td></td>
<td>included</td>
</tr>
<tr>
<td>no-security</td>
<td>1.3.6.1.6.3</td>
<td></td>
<td>excluded</td>
</tr>
<tr>
<td>no-security</td>
<td>1.3.6.1.6.3.10.2.1</td>
<td></td>
<td>included</td>
</tr>
<tr>
<td>no-security</td>
<td>1.3.6.1.6.3.11.2.1</td>
<td></td>
<td>included</td>
</tr>
<tr>
<td>no-security</td>
<td>1.3.6.1.6.3.15.1.1</td>
<td></td>
<td>included</td>
</tr>
</tbody>
</table>
-----------------------------------------------------------------------------------------------------------------------------------
No. of Views: 6
-----------------------------------------------------------------------------------------------------------------------------------
A:ALA-1#
A:ALA-1# show system security view no-security detail

Views

<table>
<thead>
<tr>
<th>view name</th>
<th>oid tree</th>
<th>mask</th>
<th>permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-security</td>
<td>1</td>
<td>included</td>
<td></td>
</tr>
<tr>
<td>no-security</td>
<td>1.3.6.1.6.3</td>
<td>excluded</td>
<td></td>
</tr>
<tr>
<td>no-security</td>
<td>1.3.6.1.6.3.10.2.1</td>
<td>included</td>
<td></td>
</tr>
<tr>
<td>no-security</td>
<td>1.3.6.1.6.3.11.2.1</td>
<td>included</td>
<td></td>
</tr>
<tr>
<td>no-security</td>
<td>1.3.6.1.6.3.15.1.1</td>
<td>included</td>
<td></td>
</tr>
</tbody>
</table>

No. of Views: 5

no-security used in

<table>
<thead>
<tr>
<th>group name</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-ro</td>
</tr>
<tr>
<td>snmp-rw</td>
</tr>
</tbody>
</table>

A:ALA-1#
Event and Accounting Logs

In This Chapter

This chapter provides information about configuring event and accounting logs in the 7210 SAS.

Topics in this chapter include:

- Logging Overview on page 196
- Log Destinations on page 198
- Event Logs on page 203
  - Event Sources on page 204
  - Event Control on page 206
  - Log Manager and Event Logs on page 208
  - Event Filter Policies on page 209
  - Event Log Entries on page 210
  - Simple Logger Event Throttling on page 212
  - Default System Log on page 213
- Accounting Logs on page 214
  - Accounting Records on page 214
- Configuration Notes on page 218
Logging Overview

The two primary types of logging supported in the 7210 SAS OS 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. The 7210 SAS groups events into three major categories or event sources:

- Security events — Events that pertain to attempts to breach system security.
- Change events — Events that pertain to the configuration and operation of the node.
- Main events — Events that pertain to applications that are not assigned to other event categories/sources.
- Debug events — Events that pertain to trace or other debugging information.

The following are events within the 7210 SAS and have the following characteristics:

- A time stamp 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 whether the event should be generated or suppressed. The severity numbers and severity names supported in the 7210 SAS OS conform to ITU standards M.3100 X.733 & X.21 and are listed in Table 22.

Table 22: Event Severity Levels

<table>
<thead>
<tr>
<th>Severity Number</th>
<th>Severity Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>cleared</td>
</tr>
<tr>
<td>2</td>
<td>indeterminate (info)</td>
</tr>
<tr>
<td>3</td>
<td>critical</td>
</tr>
<tr>
<td>4</td>
<td>major</td>
</tr>
<tr>
<td>5</td>
<td>minor</td>
</tr>
<tr>
<td>6</td>
<td>warning</td>
</tr>
</tbody>
</table>
Events that are suppressed by event control will not generate any event log entries. 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 7210 SAS OS associates the event sources with logging destinations. Examples of logging destinations include, the console session, a specific telnet or SSH 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, VRF ID, and the subject of the event.

The 7210 SAS accounting logs collect comprehensive accounting statistics to support a variety of billing models. The routers collect accounting data on services and network ports 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 on network ports can be used to track link utilization and network traffic pattern trends. This information is valuable for traffic engineering and capacity planning within the network core.

Accounting statistics are collected according to the parameters defined within the context of an accounting policy. Accounting policies are applied to . Accounting statistics are collected by counters for individual service defined on the customer’s SAP or by the counters within forwarding class (FC) queues defined on the network ports.

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

The only supported destination for an accounting log is a compact flash system device (cf1:). 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. 7210 SAS-Series devices support the following log destinations:

- Console on page 198
- Session on page 198
- Memory Logs on page 198
- Log Files on page 199
- SNMP Trap Group on page 201
- Syslog on page 201

Only a single log destination can be associated with an event log or with an accounting log. 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 which 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 devices (specifically cf1:) in the file system.

A log file is identified with a single log file ID, but a log file will generally be composed of a number 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, complying to 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.

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 specified compact flash device. The naming convention for event log files is:

`log eeff-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 \( yyyy-mm-dd-hh-mm-ss \)

where:

\( yyyy \) is the four-digit year (for example, 2007)
\( mm \) 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 a compact flash device (cf1). The naming convention for accounting log files is nearly the same as for log files except the prefix `act` is used instead of the prefix `log`. The naming convention for accounting logs is:

```
act.aaff-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 form of `yyyyymmdd-hhmms`

where:

- `yyyy` is the four-digit year (for example, 2007)
- `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 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 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.
- 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 in-band, the source IP address of the trap is the system IP address of the 7210 SAS.

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.
- The UDP port used to send the syslog message.
- The Syslog Facility Code (0 - 23) (default 23 - local 7).
- The Syslog Severity Threshold (0 - 7) - events exceeding the configured level will be sent.
Because syslog uses eight severity levels whereas the 7210 SAS-Series uses six internal severity levels, the severity levels are mapped to syslog severities. Table 23 displays the severity level mappings to syslog severities.

**Table 23: 7210 SAS-Series to Syslog Severity Level Mappings**

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Numerical Severity (highest to lowest)</th>
<th>Syslog Configured Severity</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>emergency</td>
<td></td>
<td>System is unusable</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>alert</td>
<td>Action must be taken immediately</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>critical</td>
<td>Critical conditions</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>error</td>
<td>Error conditions</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>warning</td>
<td>Warning conditions</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>notice</td>
<td>Normal but significant condition</td>
</tr>
<tr>
<td>1 cleared</td>
<td>6</td>
<td>info</td>
<td>Informational messages</td>
</tr>
<tr>
<td>2 indeterminate</td>
<td>7</td>
<td>debug</td>
<td>Debug-level messages</td>
</tr>
</tbody>
</table>
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 7210 SAS.

Figure 4 depicts a function block diagram of event logging.
Event Logs

Event Sources

In Figure 4, 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 7210 SAS.

Examples of applications within 7210 SAS include IP, MPLS, OSPF, CLI, services, etc. Figure 5 displays an example of the `show log applications` command output which displays all applications.
*A:ALU-7210# show log applications
==================================
Log Event Application Names
==================================
Application Name
----------------------------------
CHASSIS
DEBUG
DOTIAG
DOTIX
EFM_OAM
FILTER
IGMP
IP
LAG
LOGGER
MIRROR
NTP
OAM
PORT
QOS
SECURITY
SNMP
STP
SVCMGR
SYSTEM
TIP
TOD
USER
VRTR
==================================
*A:ALU-7210#
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 it never reaches the log manager.

Simple event throttling is another method of event control and is configured similarly to the generation and suppression options. See Simple Logger Event Throttling on page 212.

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
-----------------------------------------------------------------------
CHASSIS: 2001 cardFailure                      MA  gen          0           0
         2002 cardInserted                     MI  gen          2           0
         2003 cardRemoved                      MI  gen          0           0
         2004 cardWrong                        MI  gen          0           0
         2005 EnvTemperatureTooHigh            MA  gen          0           0
         2006 fanFailure                       CR  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
IGMP: 2001 vRtrIgmpIfRxQueryVerMismatch      WA  gen          0           0
         2002 vRtrIgmpIfCModeRxQueryMismatch   WA  gen          0           0
         2003 vRtrIgmpMaxGrpsLimitExceeded     WA  gen          0           0
         2004 vRtrIgmpMcacPclyDropped          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
...  
SYSTEM:
  2001 stiDateAndTimeChanged            WA  gen          0           0
  2002 ssiSaveConfigSucceeded           MA  gen          1           0
  2003 ssiSaveConfigFailed              CR  gen          1           0
  2004 sbiBootConfig                    MA  gen          1           0
  2005 sbiBootSnmpd                      MA  gen          1           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 ten 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 allow fine control over which events are forwarded or dropped based on various criteria. Like other policies with the 7210 SAS, 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 24:

**Table 24: Valid Filter Policy Operators**

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq</td>
<td>equal to</td>
</tr>
<tr>
<td>neq</td>
<td>not equal to</td>
</tr>
<tr>
<td>lt</td>
<td>less than</td>
</tr>
<tr>
<td>lte</td>
<td>less than or equal to</td>
</tr>
<tr>
<td>gt</td>
<td>greater than</td>
</tr>
<tr>
<td>gte</td>
<td>greater than or equal to</td>
</tr>
</tbody>
</table>

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 appropriate for the specific destination whether it be recorded to a file or sent as an SNMP trap, but log event entries have common elements or properties. All application generated events have the following properties:

- A time stamp 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 2006/11/27 00:19:40.38 WARNING: SNMP #2007 Base 1/1/1
"interface 1/1/1 came up"

The specific elements that compose the general format are described in Table 25.

Table 25: Log Entry Field Descriptions

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nnnn</td>
<td>The log entry sequence number.</td>
</tr>
<tr>
<td>YYYY/MM/DD</td>
<td>The UTC date stamp for the log entry.</td>
</tr>
<tr>
<td></td>
<td>YYYY — Year</td>
</tr>
<tr>
<td></td>
<td>MM — Month</td>
</tr>
<tr>
<td></td>
<td>DD — Date</td>
</tr>
<tr>
<td>HH:MM:SS.SS</td>
<td>The UTC time stamp for the event.</td>
</tr>
<tr>
<td></td>
<td>HH — Hours (24 hour format)</td>
</tr>
<tr>
<td></td>
<td>MM — Minutes</td>
</tr>
<tr>
<td></td>
<td>SS.SS — Seconds</td>
</tr>
</tbody>
</table>
Table 25: Log Entry Field Descriptions  (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;severity&gt;</td>
<td>The severity level name of the event.</td>
</tr>
<tr>
<td></td>
<td>CLEARED — A cleared event (severity number 1).</td>
</tr>
<tr>
<td></td>
<td>INFO — An indeterminate/informational severity event (severity level 2).</td>
</tr>
<tr>
<td></td>
<td>CRITICAL — A critical severity event (severity level 3).</td>
</tr>
<tr>
<td></td>
<td>MAJOR — A major severity event (severity level 4).</td>
</tr>
<tr>
<td></td>
<td>MINOR — A minor severity event (severity level 5).</td>
</tr>
<tr>
<td></td>
<td>WARNING — A warning severity event (severity 6).</td>
</tr>
</tbody>
</table>

| <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 event types can be configured to be throttled. Once the throttling event limit is exceeded in a throttling interval, any further events of that type cause the dropped events counter to be incremented. Dropped events counts are displayed by the `show>log>event-control` context. 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 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. It also does not know which events may eventually 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 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 pre-configured memory-based log which logs events from the main event source (not security, debug, etc.). Log 99 exists by default.

The following example displays the log 99 configuration.

```
ALA-1>config>log# info detail
#------------------------------------------
echo "Log Configuration "
#------------------------------------------
...
    snmp-trap-group 7
    exit
...
    log-id 99
    description "Default system log"
    no filter
    from main
    to memory 500
    no shutdown
    exit
#------------------------------------------
ALA-1>config>log#
```
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 compact flash (cf1:) in a compressed (tar) XML format and can be retrieved using FTP or SCP.

A file ID can only be assigned to either one event log ID or one accounting log.

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.

The record name, sub-record types, and default collection period for service and network accounting policies are shown below.

Table 26: Accounting Record Name and Collection Periods

<table>
<thead>
<tr>
<th>Record Name</th>
<th>Sub-Record Types</th>
<th>Accounting Object</th>
<th>Default Collection Period (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>service-ingress-octets</td>
<td>sio</td>
<td>SAP</td>
<td>5</td>
</tr>
<tr>
<td>service-ingress-packets</td>
<td>sip</td>
<td>SAP</td>
<td>5</td>
</tr>
<tr>
<td>network-ingress-octets</td>
<td>nio</td>
<td>network port</td>
<td>15</td>
</tr>
<tr>
<td>network-ingress-packets</td>
<td>nip</td>
<td>network port</td>
<td>15</td>
</tr>
<tr>
<td>service-egress-pkts</td>
<td>sep</td>
<td>SAP</td>
<td>5</td>
</tr>
<tr>
<td>combined-service-ingress-egress-pkts</td>
<td>cmSip &amp; cmSep</td>
<td>SAP</td>
<td>5</td>
</tr>
</tbody>
</table>

When creating accounting policies, one service accounting policy and one network accounting policy can be defined as default. If statistics collection is enabled on a SAP or network port 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 is in turn composed of multiple fields. Table 27 lists the accounting policy record names and the statistics that are collected with each.
In 7210 SAS-E, the ingress SAP counter operates in either octet or packet mode. The mode of the counter can be configured to collect data in either packets or octets. The counter mode can be specified for ingress SAP counters only. The egress SAP counters collect only the number of packets. The accounting records collect the packet or octet count on a SAP based on the accounting policy associated with the SAP. The default mode of the ingress SAP counter is set to packet. The egress SAP counter is disabled by default.

<table>
<thead>
<tr>
<th>Record Name</th>
<th>Sub-Record</th>
<th>Field</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service-ingress-octets (sio) (***)</td>
<td>sio</td>
<td>svc</td>
<td>SvclId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sap</td>
<td>SapId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mid</td>
<td>MeterId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iof</td>
<td>InProfileOctetsForwarded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>oof</td>
<td>OutOfProfileOctetsForwarded</td>
</tr>
<tr>
<td>Service-ingress-packets (sip) (<em>) (</em>**)</td>
<td>sip</td>
<td>svc</td>
<td>SvclId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sap</td>
<td>SapId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mid</td>
<td>MeterId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ipf</td>
<td>InProfilePktsForwarded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opf</td>
<td>OutOfProfilePktsForwarded</td>
</tr>
<tr>
<td>Network-ingress-octets (nio)</td>
<td>nio</td>
<td>port</td>
<td>PortId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mid</td>
<td>MeterId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iof</td>
<td>InProfileOctetsForwarded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>oof</td>
<td>OutOfProfileOctetsForwarded</td>
</tr>
<tr>
<td>Network-ingress-packets (nip)</td>
<td>nip</td>
<td>port</td>
<td>PortId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mid</td>
<td>MeterId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ipf</td>
<td>InProfilePktsForwarded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opf</td>
<td>OutOfProfilePktsForwarded</td>
</tr>
<tr>
<td>Service-egress-pkts (sep) (<em>) (</em>**)</td>
<td>sep</td>
<td>svc</td>
<td>SvclId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sap</td>
<td>SapId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>epf</td>
<td>PacketsForwarded</td>
</tr>
<tr>
<td>Combined-service-ingress-egress-pkts</td>
<td>cmSip cmSep</td>
<td>svc</td>
<td>SvclId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sap</td>
<td>SapId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>epf</td>
<td>PacketsForwarded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ipo</td>
<td>PacketsReceived</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mid</td>
<td>MeterId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ipf</td>
<td>InProfilePktsForwarded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>opf</td>
<td>OutOfProfilePktsForwarded</td>
</tr>
</tbody>
</table>
Notes:

1. The mode of the counter cannot be changed if an accounting policy is already associated with a SAP.
2. Ensure that egress SAP counters are enabled before associating accounting records of type Service-egress-pkts and Combined-service-ingress-egress-pkts.
3. Before modifying the counter, disable account log generation. Execute the `no collect-stats` command. Changing the mode of the counter results in loss of previously collected counts and resets the counter.
4. Egress SAP statistics are not available on any of the SAPs of a port, on which a dot1q SAP and dot1q default SAP configuration are present at the same time.
Reporting and Time-Based Accounting

Node support for volume and time-based accounting concept provides an extra level of intelligence at the network element level in order to provide service models such as “prepaid access” in a scalable manner. This means that the network element gathers and stores per-subscriber accounting information and compares it with “pre-defined” quotas. Once a quota is exceeded, the pre-defined action (such as re-direction to a web portal or disconnect) is applied.
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, or applied to a network port.
- The snmp-trap-id must be the same as the log-id.
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 220
  → Log Types on page 220
- Basic Event Log Configuration on page 221
- Common Configuration Tasks on page 222
- Log Management Tasks on page 231
Log Configuration Overview

Configure logging parameters to save information in a log file or direct the messages to other devices. Logging does the following:

- Provides you with logging information for monitoring and troubleshooting.
- Allows you to select the types of logging information to be recorded.
- Allows you to assign a severity to the log messages.
- Allows you to select the source and target of logging information.

Log Types

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 which 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 its associated destination.
- Event throttling rate — Defines the rate of throttling events.
Basic Event Log Configuration

The most basic log configuration must have the following:

- Log ID or accounting policy ID
- A log source
- A log destination

The following displays a log configuration example.

```
A:ALA-12>config>log# info
#------------------------------------------
echo "Log Configuration "
#------------------------------------------
event-control " 2001 generate critical
   file-id 1
      description "This is a test file-id."
      location cf1:
      exit
   file-id 2
      description "This is a test log."
      location cf1:
      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
#------------------------------------------
A:ALA-12>config>log#
```
Common Configuration Tasks

The following sections are basic system tasks that must be performed.

- Configuring a File ID on page 224
- Configuring an Event Log on page 222
- Configuring an Accounting Policy on page 225
- Configuring Event Control on page 226
- Configuring a Log Filter on page 228
- Configuring an SNMP Trap Group on page 229
- Configuring a Syslog Target on page 230

Configuring an Event Log

A 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 a log file configuration example:

```
ALA-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
...
----------------------------------------------
ALA-12>config>log>log-id#
```
Configuring a File ID

To create a log file a file ID is defined, specifies the target CF 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 CF before it is deleted.

Use the following CLI syntax to configure a log file:

**CLI Syntax:**
```
config>log
    file-id log-file-id
    description description-string
    location cflash-id
    rollover minutes [retention hours]
```

The following displays a log file configuration example:

```
A:ALA-12>config>log# info
-----------------------------
    file-id 1
        description "This is a log file."
        location cf1:
            rollover 600 retention 24
    exit
-----------------------------
A:ALA-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 of compact flash (cf1:) in a compressed (tar) XML format and can be retrieved using FTP or SCP. See Configuring an Event Log on page 222 and Configuring a File ID on page 224.

Accounting policies must be configured in the `config>log` context before they can be applied to a service SAP or service interface, or applied to a network port.

The default accounting policy statement cannot be applied to LDP nor RSVP statistics collection records.

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 and one network accounting policy can be defined as default. If statistics collection is enabled on a SAP or network port 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 a accounting policy configuration example:

```
A:ALA-12>config>log# info
----------------------------------------------
    accounting-policy 5
      description "This is a test accounting policy."
      record service-ingress-packets
      to file 3
    exit
----------------------------------------------
A:ALA-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 event control configuration:

```
A:ALA-12>config>log# info
#------------------------------------------
echo "Log Configuration"
#------------------------------------------
  throttle-rate 500 interval 10
event-control "oam" 2001 generate throttle
event-control "ospf" 2001 suppress
event-control "ospf" 2003 generate cleared
event-control "ospf" 2014 generate critical
...
#------------------------------------------
A:ALA-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 a throttle rate configuration example:

```
*A:gal171>config>log# info
---------------------------------------------
    throttle-rate 500 interval 10
    event-control "aps" 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 [regexp]
    severity {eq|neq|lt|lte|gt|gte} severity-level
    subject {eq|neq} subject [regexp]
```

The following displays a log filter configuration example:

```
A:ALA-12>config>log# info
#------------------------------------------
echo "Log Configuration "
#------------------------------------------
file-id 1
  description "This is our log file."
  location cf1:
    rollover 600 retention 24
  exit
filter 1
  default-action drop
  description "This is a sample filter."
  entry 1
    action forward
    match
      application eq "mirror"
      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
... 
#------------------------------------------
A:ALA-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 communi-
           tyName | snmpv3SecurityName [security-level {no-
           auth-no-privacy|auth-no-privacy|privacy}]
```

The following displays a basic SNMP trap group configuration example:

```
A:ALA-12>config>log# info
----------------------------------------------
... snmp-trap-group 2
   trap-target 10.10.10.104:5 "snmpv3" notify-community "coummunitystring"
   exit
... log-id 2
   description "This is a test log file."
   filter 1
      from main security
      to file 1
   exit
...----------------------------------------------
A:ALA-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 a syslog configuration example:

```
A:ALA-12>config>log# info
----------------------------------------------
...  
syslog 1
    description "This is a syslog file."
    address 10.10.10.104
    facility user
    level warning
    exit
...  
----------------------------------------------
A:ALA-12>config>log# 
```
Log Management Tasks

This section discusses the following logging tasks:

- Modifying a Log File on page 232
- Deleting a Log File on page 234
- Modifying a File ID on page 235
- Deleting a File ID on page 236
- Modifying a Syslog ID on page 237
- Deleting a Syslog on page 238
- Modifying an SNMP Trap Group on page 239
- Deleting an SNMP Trap Group on page 240
- Modifying a Log Filter on page 241
- Deleting a Log Filter on page 243
- Modifying Event Control Parameters on page 244
- Returning to the Default Event Control Configuration on page 245
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:

```
ALA-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
...----------------------------------------------
ALA-12>config>log>log-id#
```

The following displays an example to modify 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:

A:ALA-12>config>log# info
----------------------------------------------
...
  log-id 2
description "Chassis log file."
  filter 2
  from security
to file 1
  exit
...
----------------------------------------------
A:ALA-12>config>log#
Deleting a Log File

The log ID must be shutdown first before it can be deleted. In a previous example, file 1 is associated with log-id 2.

```
A:ALA-12>config>log# info
----------------------------------------------
file-id 1
   description "LocationTest."
   location cf1:
   rollover 600 retention 24
   exit
...
log-id 2
   description "Chassis log file."
   filter 2
   from security
   to file 1
   exit
...
----------------------------------------------
A:ALA-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 to delete 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 not cleared, the old location remains in effect.

Use the following CLI syntax to modify a log file:

**CLI Syntax:**
```
config>log
  file-id log-file-id
description description-string
location [cflash-id]
rollover minutes [retention hours]
```

The following displays the current log configuration:

```
A:ALA-12>config>log# info
------------------------------------------
  file-id 1
  description "This is a log file."
  location cf1:
  rollover 600 retention 24
  exit
------------------------------------------
A:ALA-12>config>log#
```

The following displays an example to modify log file parameters:

**Example:**
```
config# log
config>log# file-id 1
config>log>file-id# description "LocationTest."
config>log>file-id# rollover 2880 retention 500
config>log>file-id# exit
```

The following displays the file modifications:

```
A:ALA-12>config>log# info
------------------------------------------
...  
  file-id 1
  description "LocationTest."
  location cf1:
  rollover 2880 retention 500
  exit
...  
------------------------------------------
A:ALA-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 log ID:

**CLI Syntax:**

```
config>log
  no file-id log-file-id
```

The following displays an example to delete a file ID:

**Example:**

```
config>log# no file-id 1
```
Modifying 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 modify a 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:

```
A:ALA-12>config>log# info
----------------------------------------------
... 
syslog 1
  description "Test syslog."
  address 10.10.0.91
  facility mail
  level info
  exit
... 
----------------------------------------------
A:ALA-12>config>log#
```
Deleting a Syslog

Use the following CLI syntax to delete a syslog file:

**CLI Syntax:**
```
config>log
   no syslog syslog-id
```

The following displays an example to delete 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:

```
A:ALA-12>config>log# info
----------------------------------------------
... snmp-trap-group 10
   trap-target 10.10.10.104:5 "snmpv3" notify-community "communitystring"
   exit
...----------------------------------------------
A:ALA-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 10.10.104:5
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:

```
A:ALA-12>config>log# info
----------------------------------------------
... snmp-trap-group 10
   trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
   exit
...----------------------------------------------
A:ALA-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:

```
A:ALA-12>config>log# info
----------------------------------------------
... snmp-trap-group 10
    trap-target 10.10.0.91:1 "snmpv2c" notify-community "com1"
    exit
...----------------------------------------------
A:ALA-12>config>log#
```

The following displays an example to delete 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 [regexp]
         severity {eq|neq|lt|lte|gt|gte} severity-level
         subject {eq|neq} subject [regexp]
```

The following output displays the current log filter configuration:

```
ALA-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 "mirror"
         severity eq critical
      exit
      exit
      exit
...
------------------------------------------
ALA-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:

A:ALA-12>config>log>filter# info
----------------------------------------
... filter 1
   description "This allows <n>.
   entry 1
      action drop
      match
         application eq "user"
         number eq 2001
      exit
   exit
   exit
... ----------------------------------------
A:ALA-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:

```
A:ALA-12>config>log>filter# info
----------------------------------------
... filter 1
description "This allows <n>.
entry 1
    action drop
    match
        application eq "user"
        number eq 2001
    exit
    exit
exit
...----------------------------------------
A:ALA-12>config>log>filter#
```

The following displays an example of the command usage 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:

```
A:ALA-12>config>log# info
----------------------------------------------
... event-control "" 2014 generate critical
... ----------------------------------------------
A:ALA-12>config>log#
```

The following displays an example of an event control modifications:

**Example:**
```
config# log
config>log# event-control 2014 suppress
```

The following displays the log filter configuration:

```
A:ALA-12>config>log# info
----------------------------------------------
... event-control "" 2014 suppress
... ----------------------------------------------
A:ALA-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 modify event control parameters:

**CLI Syntax:**
```
config>log
    no event-control application [event-name | event-nunber]
```

The following displays an example of the command usage to return to the default values:

**Example:**
```
config>log
    no event-control "" 2001
    no event-control "" 2002
    no event-control "" 2014
```

```
A:ALA-12>config>log# info detail
-----------------------------------------------
#------------------------------------------
echo "Log Configuration"
#------------------------------------------
  event-control "" 2001 generate minor
  event-control "" 2002 generate warning
  event-control "" 2003 generate warning
  event-control "" 2004 generate critical
  event-control "" 2005 generate warning
  event-control "" 2006 generate warning
  event-control "" 2007 generate warning
  event-control "" 2008 generate warning
  event-control "" 2009 generate warning
  event-control "" 2010 generate warning
  event-control "" 2011 generate warning
  event-control "" 2012 generate warning
  event-control "" 2013 generate warning
  event-control "" 2014 generate warning
  event-control "" 2015 generate critical
  event-control "" 2016 generate warning
...
```

```
A:ALA-12>config>log#
```
Log Command Reference

Command Hierarchies

- Log Command Reference on page 247
  - Accounting Policy Commands on page 247
  - File ID Commands on page 248
  - Event Filter Commands on page 248
  - Log ID Commands on page 249
  - SNMP Trap Group Commands on page 249
  - Syslog Commands on page 250
- Show Commands on page 251
- Clear Command on page 251

Log Configuration 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 [event-name | event-number]
    throttle-rate events [interval seconds]
    no throttle-rate

ACCOUNTING POLICY COMMANDS
config
  log
    accounting-policy acct-policy-id
    no accounting-policy acct-policy-id
    [no] default
    description description-string
    no description
    record record-name
    no record
    [no] shutdown
    to file log-file-id
```
FILE ID COMMANDS

```plaintext
config
  log
    [no] file-id log-file-id
    — description description-string
    — no description
    — location cflash-id
    — rollover minutes [retention hours]
    — no rollover
```

EVENT FILTER COMMANDS

```plaintext
config
  log
    [no] filter filter-id
    — default-action {drop | forward}
    — no default-action
    — description description-string
    — no description
    — entry entry-id
      — action {drop | forward}
      — no action
      — description description-string
      — no description
      — [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
```
LOG ID COMMANDS

```bash
config  log
          [no] log-id log-id
          description description-string
          no description
          filter filter-id
          no filter
          from {main [security] [change] [debug-trace]}
          no from
          [no] shutdown
          [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 GROUP COMMANDS

```bash
config  log
          [no] 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
```
SYSLOG COMMANDS

    config
      log
        [no] syslog syslog-id
        — address ip-address
        — no address
        — description description-string
        — no description
        — ipv4-address a.b.c.d facility syslog-facility
        — no ipv4-address a.b.c.d facility
        — level {emergency | alert | critical | error | warning | notice | info | debug}
        — no level
        — log-prefix log-prefix-string
        — no log-prefix
        — port port
        — no port
Show Commands

`show`
  — `log`
    — `accounting-policy [acct-policy-id] [access | network]`
    — `accounting-records`
    — `applications`
    — `event-control [application [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 Command

`clear`
  — `log log-id`
Configuration Commands

Generic Commands

description

Syntax

```
description string
no description
```

Context

```
config>log>filter
config>log>filter>entry
config>log>log-id
config>log>accounting-policy
config>log>file-id
config>log>syslog
config>log>snmp-trap-group
```

Description

This command creates a text description stored in the configuration file for a configuration context. The `description` command associates a text string with a configuration context to help identify the content in the configuration file.

The `no` form of the command removes the string from the configuration.

Default

No text description is associated with this configuration. The string must be entered.

Parameters

`string` — 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
config>log>accounting-policy
```

Description

This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. 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 may be deleted.

The `no` form of this command administratively enables an entity.

Default

```
no shutdown
```

Special Cases

`log-id log-id` — When a `log-id` is shut down, no events are collected for the entity. This leads to the loss of event data.
accounting-policy accounting Policy — 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.
Event Control

**Syntax**
```
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 [event-name | event-number]
```

**Context**
```
config>log
```

**Description**
This command is used to specify that a particular event or all events associated with an application is either generated or suppressed.

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 which directs it to be generated or suppressed.

Events are generated with a default severity level that can be modified by using the `severity-level` option.

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 squelched. In reverse, indiscriminate application may cause excessive overhead.

The rate of event generation can be throttled by using the `throttle` parameter.

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.

**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:

```
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 `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-name** — An ASCII string representing the severity level to associate with the specified generated events

**Default** The system assigned severity name

**Values** One of: cleared, indeterminate, critical, major, minor, warning.

**throttle** — Specifies whether or not 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** — This keyword 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
Log File Commands

**file-id**

**Syntax**  
`[no] file-id file-id`

**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/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 in 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:

<table>
<thead>
<tr>
<th>File Type</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log File</td>
<td><code>logllff-timestamp</code></td>
</tr>
<tr>
<td>Accounting File</td>
<td><code>actaaff-timestamp</code></td>
</tr>
</tbody>
</table>

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 `yyyyymmdd-hhmmss` where:
  - `yyyy` is the year (for example, 2006)
  - `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.
- If the event log file was closed properly, the sequence number of the last event stored on the log is recorded.

If the process of writing to a log file fails (for example, the compact flash card is full) and if a backup location is not specified or fails, the log file will not become operational even if the compact flash card is replaced. Enter either a `clear log` command or a `shutdown/no shutdown` command to reinitialize the file.

If the primary location fails (for example, the compact flash card fills up during the write process), a trap is sent and logging continues to the specified backup location. This can result in truncated files in different locations.

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**

- `file-id` — The file identification number for the file, expressed as a decimal integer.

  **Values**

  - 1 — 99

**location**

**Syntax**

```
location cflash-id
no location
```

**Context**

`config>log>file file-id`

**Description**

This command specifies the primary location where the log or billing file will be created.

When creating files, the primary 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 a compact flash is either not available or that no space is available on the specified flash and that the backup location is being used.

A high priority alarm condition is raised if none of the configured compact flash devices for this file ID are present or if there is insufficient space available. If space does becomes available, then the alarm condition will be cleared.

Use the `no` form of this command to revert to default settings.

**Default**

Log files are created on cf1: and accounting files are created on cf1:.  

Page 258
Parameters  

$cflash-id$ — Specify the primary location.

Values  
cflash-id: cfl:

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.

When multiple rollover commands for a file-id are entered, the last command overwrites the previous command.

Default  
rollover 1440 retention 12

Parameters  

minutes — The rollover time, in minutes.

Values  
5 — 10080

retention hours. The retention period in hours, expressed as a decimal integer. The retention time is based on the time creation time of the file. The file becomes a candidate for removal once the creation datestamp + rollover time + retention time is less than the current timestamp.

Default  
12

Values  
1 — 500
Log Filter Commands

filter

Syntax  

[no] filter filter-id

Context  

config>log

Description  

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.

Filters are configured in the filter filter-id context and then applied to a log in the log-id log-id context. Only events for the configured log source streams destined to the log ID where the filter is applied are filtered.

Any changes made to an existing filter, using any of the sub-commands, are immediately applied to the destinations where the filter is applied.

The no form of the command removes the filter association from log IDs which causes those logs to forward all events.

Default  

No event filters are defined.

Parameters

filter-id — The filter ID uniquely identifies the filter.

Values  

1 — 1000

default-action

Syntax  

default-action {drop | forward}

no default-action

Context  

config>log>filter filter-id

Description  

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.

When multiple default-action commands are entered, the last command overwrites the previous command.

The no form of the command reverts the default action to the default value (forward).

Default  

default-action forward — The events which are not explicitly dropped by an event filter match are forwarded.

drop — The events which are not explicitly forwarded by an event filter match are dropped.

forward — The events which are not explicitly dropped by an event filter match are forwarded.
Log Filter Entry Commands

**action**

| Syntax       | action {drop | forward} |
|--------------|----------------------|
| no action    |                      |

**Context**

config>log>filter filter-id>entry entry-id

**Description**

This command specifies a drop or forward action associated with the filter entry. 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.

Multiple action statements entered will overwrite previous actions.

The **no** form of the command removes the specified action statement.

**Default**

Action specified by the default-action command will apply.

**Parameters**

- **drop** — Specifies packets matching the entry criteria will be dropped.
- **forward** — Specifies packets matching the entry criteria will be forwarded.

**entry**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>[no] entry entry-id</th>
</tr>
</thead>
</table>

**Context**

config>log>filter filter-id

**Description**

This command is used to create or edit an event filter entry. Multiple entries may be created using unique entry-id numbers. The TiMOS implementation exits the filter on the first match found and executes the action in accordance with the action command.

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.

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. Entries without the action keyword will be considered incomplete and are rendered inactive.

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-id’s where the filter is applied.

**Default**

No event filter entries are defined. An entry must be explicitly configured.
**Parameters**  
*entry-id*. The 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 — 999
Log Filter Entry Match Commands

match

Syntax      [no] match  
Context     config>log>filter filter-id>entry entry-id  
Description This command creates context to enter/edit match criteria for a filter entry. When the match criteria is satisfied, the action associated with the entry is executed. 

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. 

Use the application command to display a list of the valid applications.

Match context can consist of multiple match parameters (application, event-number, severity, subject), but multiple match statements cannot be entered per entry.

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

Default No match context is defined.

application

Syntax      application {eq | neq} application-id  
no application  
Context     config>log>filter filter-id>entry entry-id>match  
Description This command adds an OS application as an event filter match criterion.

An OS application is the software entity that reports the event. Applications include IP, MPLS, OSPF, CLI, SERVICES etc. Only one application can be specified. The latest application command overwrites the previous command.

The no form of the command removes the application as a match criterion.

Default no application — No application match criterion is specified.

Parameters eq | neq — The operator specifying the type of match. Valid operators are listed in the table below.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq</td>
<td>equal to</td>
</tr>
<tr>
<td>neq</td>
<td>not equal to</td>
</tr>
</tbody>
</table>

application-id — The application name string.
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 an SR OS application event number as a match criterion.

SR OS event numbers uniquely identify a specific logging event within an application.

Only one number command can be entered per event filter entry. The latest number command
overwrites the previous command.

The no form of the command removes the event number as a match criterion.

Default    no event-number — No event ID match criterion is specified.

Parameters eq | neq | lt | lte | gt | gte — This operator specifies the type of match. Valid operators are listed in
        the table below. Valid operators are:

        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 — 4294967295

router

Syntax    router {eq | neq} router-instance [regexp]
        no router

Context   config>log>filter>entry>match

Description This command specifies the log event matches for the router.

Parameters eq — Determines if the matching criteria should be equal to the specified value.

        neq — Determines if the matching criteria should not be equal to the specified value.

        router-instance — Specifies a router name up to 32 characters to be used in the match criteria.
**regexp** — Specifies the type of string comparison to use to determine if the log event matches the value of **router** command parameters. When the **regexp** 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.

---

**severity**

**Syntax**  
```severity \{eq | neq | lt | lte | gt | gte\} severity-level```

**Context**  
`config>log>filter>entry>match`

**Description**  
This command adds an event severity level as a match criterion. Only one severity command can be entered per event filter entry. The latest severity command overwrites the previous command. The **no** form of the command removes the severity match criterion.

**Default**  
**no severity** — No severity level match criterion is specified.

**Parameters**  
`eq | neq | lt | lte | gt | gte` — This operator specifies the type of match. Valid operators are listed in the table below.

| Operator | Notes
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>eq</td>
<td>equal to</td>
</tr>
<tr>
<td>neq</td>
<td>not equal to</td>
</tr>
<tr>
<td>lt</td>
<td>less than</td>
</tr>
<tr>
<td>lte</td>
<td>less than or equal to</td>
</tr>
<tr>
<td>gt</td>
<td>greater than</td>
</tr>
<tr>
<td>gte</td>
<td>greater than or equal to</td>
</tr>
</tbody>
</table>

**severity-name** — The ITU severity level name. The following table lists severity names and corresponding numbers per ITU standards M.3100 X.733 & X.21 severity levels.

<table>
<thead>
<tr>
<th>Severity Number</th>
<th>Severity Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>cleared</td>
</tr>
<tr>
<td>2</td>
<td>indeterminate (info)</td>
</tr>
<tr>
<td>3</td>
<td>critical</td>
</tr>
<tr>
<td>4</td>
<td>major</td>
</tr>
<tr>
<td>5</td>
<td>minor</td>
</tr>
<tr>
<td>6</td>
<td>warning</td>
</tr>
</tbody>
</table>

**Values**  
cleared, intermediate, critical, major, minor, 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. The latest
subject command overwrites the previous command.

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

Default  no subject — No subject match criterion specified.

Parameters  eq | neq — This operator specifies the type of match. Valid operators are listed in the following table:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq</td>
<td>equal to</td>
</tr>
<tr>
<td>neq</td>
<td>not equal to</td>
</tr>
</tbody>
</table>

subject — A string used as the subject match criterion.

regexp — Specifies the type of string comparison to use to determine if the log event matches the
value of subject command parameters. When the regexp 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 regexp keyword is not specified, the subject command string is matched exactly by the
event filter.
Syslog Commands

syslog

Syntax     [no] syslog syslog-id
Context    config>log
Description This command creates the context to configure a syslog target host that is capable of receiving selected syslog messages from this network element.

A valid syslog-id must have the target syslog host address configured.

A maximum of 10 syslog-id’s can be configured.

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.

Default No syslog IDs are defined.

Parameters syslog-id — The syslog ID number for the syslog destination, expressed as a decimal integer.

Values 1 — 10

address

Syntax     address ip-address
no address
Context    config>log>syslog syslog syslog-id
Description This command adds the syslog target host IP address to/from a syslog ID.

This parameter is mandatory. If no address is configured, syslog data cannot be forwarded to the syslog target host.

Only one address can be associated with a syslog-id. If multiple addresses are entered, the last address entered overwrites the previous address.

The same syslog target host can be used by multiple log IDs.

The no form of the command removes the syslog target host IP address.

Default no address — There is no syslog target host IP address defined for the syslog ID.

Parameters ip-address — The IP address of the syslog target host in dotted decimal notation.

ipv4-address a.b.c.d
facility

Syntax

```
facility syslog-facility
no facility
```

Context

```
config>log>syslog syslog syslog-id
```

Description

This command configures the facility code for messages sent to the syslog target host. 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. 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. The `no` form of the command reverts to the default value.

Default

`local7` — syslog entries are sent with the local7 facility code.

Parameters

```
syslog-facility — The syslog facility name represents a specific numeric facility code. The code should be entered in accordance with the syslog RFC. However, the software does not validate if the facility code configured is appropriate for the event type being sent to the syslog target host.
```

Values

kernel, user, mail, systemd, auth, syslogd, printer, net-news, uucp, cron, authpriv, ftp, ntp, logaudit, logalert, cron2, local0, local1, local2, local3, local4, local5, local6, local7

Valid responses per RFC3164, *The BSD syslog Protocol*, are listed in the table below.

<table>
<thead>
<tr>
<th>Numerical Code</th>
<th>Facility Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>kernel</td>
</tr>
<tr>
<td>1</td>
<td>user</td>
</tr>
<tr>
<td>2</td>
<td>mail</td>
</tr>
<tr>
<td>3</td>
<td>systemd</td>
</tr>
<tr>
<td>4</td>
<td>auth</td>
</tr>
<tr>
<td>5</td>
<td>syslogd</td>
</tr>
<tr>
<td>6</td>
<td>printer</td>
</tr>
<tr>
<td>7</td>
<td>net-news</td>
</tr>
<tr>
<td>8</td>
<td>uucp</td>
</tr>
<tr>
<td>9</td>
<td>cron</td>
</tr>
<tr>
<td>10</td>
<td>auth-priv</td>
</tr>
<tr>
<td>11</td>
<td>ftp</td>
</tr>
<tr>
<td>12</td>
<td>ntp</td>
</tr>
<tr>
<td>13</td>
<td>log-audit</td>
</tr>
<tr>
<td>14</td>
<td>log-alert</td>
</tr>
<tr>
<td>15</td>
<td>cron2</td>
</tr>
<tr>
<td>16</td>
<td>local0</td>
</tr>
</tbody>
</table>
log-prefix

Syntax  log-prefix log-prefix-string
       no log-prefix

Context  config>log>syslog syslog-id

Description  This command adds the string prepended to every syslog message sent to the syslog host.

RFC3164, *The BSD syslog Protocol*, allows a 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.

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.

The **no** form of the command removes the log prefix string.

Default  no log-prefix — no prepend log prefix string defined.

Parameters  log-prefix-string — An alphanumeric string of up to 32 characters. Spaces and colons (:) cannot be used in the string.

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 levels are entered, the last **level** entered will overwrite the previously entered commands.

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

**Parameters**

*value* — The threshold severity level name.

**Values**

- emergency
- alert
- critical
- error
- warning
- notice
- info
- debug

<table>
<thead>
<tr>
<th>severity level</th>
<th>Numerical Severity (highest to lowest)</th>
<th>Configured Severity</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>emergency</td>
<td>system is unusable</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>alert</td>
<td>action must be taken immediately</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>critical</td>
<td>critical condition</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>error</td>
<td>error condition</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>warning</td>
<td>warning condition</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>notice</td>
<td>normal but significant condition</td>
</tr>
<tr>
<td>1 cleared</td>
<td>6</td>
<td>info</td>
<td>informational messages</td>
</tr>
<tr>
<td>2 indeterminate</td>
<td>7</td>
<td>debug</td>
<td>debug-level messages</td>
</tr>
</tbody>
</table>

**port**

**Syntax**

```
port value
no port
```

**Context**

```
config>log>syslog syslog-id
```

**Description**

This command configures the UDP port that will be used to send syslog messages to the syslog target host.

The port configuration is needed if the syslog target host uses a port other than the standard UDP syslog port 514.

Only one port can be configured. If multiple **port** commands are entered, the last entered port overwrites the previously entered ports.

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

**Default**

```
no port
```

**Parameters**

*value* — The value is the configured UDP port number used when sending syslog messages.

**Values**

- 1 — 65535
throttle-rate

Syntax       throttle-rate  events [interval  seconds]
no throttle-rate

Context      config>log

Description  This command configures an event throttling rate.

Parameters   events — 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, for example, 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.

Values       10 — 20000
Default       500

interval seconds — Specifies the number of seconds that an event throttling interval lasts.

Values       1 — 60
Default       1
SNMP Trap Groups

snmp-trap-group

Syntax  
\[no\] snmp-trap-group \textit{log-id}

Context  
config>log

Description  
This command creates the context to configure a group of SNMP trap receivers and their operational parameters for a given log-id.

A group specifies the types of SNMP traps and specifies the log ID which will receive the group of SNMP traps. A trap group must be configured in order for SNMP traps to be sent.

To suppress the generation of all alarms and traps see the \texttt{event-control} command. To suppress alarms and traps that are sent to this log-id, see the \texttt{filter} 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.

The \texttt{no} form of the command deletes the SNMP trap group.

Default  
There are no default SNMP trap groups.

Parameters  
log-id — The log ID value of a log configured in the \texttt{log-id} context. Alarms and traps cannot be sent to the trap receivers until a valid \texttt{log-id} exists.

Values  
1 — 99

trap-target

Syntax  
\texttt{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 \texttt{trap-target name}}

Context  
config>log>snmp-trap-group

Description  
This command adds/modifies a trap receiver and configures the operational parameters for the trap receiver. A trap reports significant events that occur on a network device such as errors or failures.

Before an SNMP trap can be issued to a trap receiver, the \texttt{log-id}, and at least one \texttt{trap-target} must be configured.
The `trap-target` command is used to add/remove a trap receiver from an . 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 that 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 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 in dotted decimal notation. Only one IP address destination can be specified per trap destination group.
  - **Values** `ipv4-address` `a.b.c.d` (host bits must be 0)
- `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 then multiple ports must be configured.
  - **Default** 162
  - **Values** `1 — 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` 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 `security-name` that is used by `snmpv3`.

The keyword `snmpv2c` selects the SNMP version 2c format. When specifying `snmpv2c`, the `notify-community` 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** 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**.

Pre-existing conditions are checked before the snmpv3SecurityName is accepted. These are:

- The user name must be configured.
- The v3 access group must be configured.
- The v3 notification view must be configured.

**Default**  
```
   snmpv3
```

**Values**  
```
   snmpv1, snmpv2c, snmpv3
```

**notify-community community | security-name** — Specifies the community string for **snmpv1** or **snmpv2c** or the **snmpv3** **security-name**. If no **notify-community** is configured, then no alarms nor 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 31 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 31 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 no authentication and no privacy (encryption) are required.

The keyword **auth-no-privacy** specifies 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 both authentication and privacy (encryption) is required. When this option is configured the **security-name** must be configured for authentication and privacy.

**Default**  
```
   no-auth-no-privacy.
```

**Values**  
```
   no-auth-no-privacy, auth-no-privacy, privacy
```
Logging Destination Commands

filter

**Syntax**
```
filter filter-id
no filter
```

**Context**
```
config>log>log-id log-id
```

**Description**
This command adds an event filter policy with the log destination.

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.

An event filter policy defines (limits) the events that are forwarded to the destination configured in the log-id. The event filter policy can also be used to select the alarms and traps to be forwarded to a destination `snmp-trap-group`.

The application of filters for debug messages is limited to application and subject only.

Accounting records cannot be filtered using the `filter` command.

Only one filter-id can be configured per log destination.

The `no` form of the command removes the specified event filter from the log-id.

**Default**
`no filter` — No event filter policy is specified for a log-id.

**Parameters**
`filter-id`. The event filter policy ID is used to associate the filter with the log-id configuration. The event filter policy ID must already be defined in `config>log>filter filter-id`.

**Values**
1 — 1000

from

**Syntax**
```
from {main} [security] [change] [debug-trace]
no from
```

**Context**
```
config>log>log-id log-id
```

**Description**
This command selects the source stream to be sent to a log destination.

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`).

Only one `from` command may be entered for a single log-id. If multiple `from` commands are configured, then the last command entered overwrites the previous `from` command.

The `no` form of the command removes all previously configured source streams.
Default

No source stream is configured.

Parameters

- **main** — Instructs all events in the main event stream to be sent to the destination defined in the `to` command for this destination `log-id`. 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` command.

- **security** — Instructs all events in the security event stream to be sent to the destination defined in the `to` command for this destination `log-id`. 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` command.

- **change** — Instructs all events in the user activity stream to be sent to the destination configured in the `to` command for this destination `log-id`. 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` command.

- **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 `log-id`. Filters applied to debug messages are limited to application and subject.

log-id

**Syntax**

```
[no] log-id log-id
```

**Context**

`config>log`

**Description**

This command creates a context to configure destinations for event streams.

The `log-id` context is used to direct events, alarms/traps, and debug information to respective destinations.

A maximum of 10 logs can be configured.

Before an event can be associated with this `log-id`, the `from` command identifying the source of the event must be configured.

Only one destination can be specified for a `log-id`. The destination of an event stream can be an in-memory buffer, console, session, snmp-trap-group, syslog, or file.

Use the `event-control` command to suppress the generation of events, alarms, and traps for all log destinations.

An event filter policy can be applied in the log-id context to limit which events, alarms, and traps are sent to the specified log-id.

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.

Note that Log-ID 99 provides valuable information for the admin-tech file. Removing or changing the log configuration may hinder debugging capabilities. It is strongly recommended not to alter the configuration for Log-ID 99.
The `no` form of the command deletes the log destination ID from the configuration.

**Default**
No log destinations are defined.

**Parameters**

- **log-id** — The log ID number, expressed as a decimal integer.
  
  **Values**
  
  1 — 100

### to console

**Syntax**
to console

**Context**
config>log>log-id log-id

**Description**
This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to the console. If the console is not connected, then all the entries are dropped.

The source of the data stream must be specified in the `from` command prior to configuring the destination with the `to` command.

The `to` command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

**Default**
No destination is specified.

### to file

**Syntax**
to file log-file-id

**Context**
config>log>log-id log-id

**Description**
This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the events selected for the log ID to be directed to a specified file.

The source of the data stream must be specified in the `from` command prior to configuring the destination with the `to` command.

The `to` command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

**Default**
No destination is specified.

**Parameters**

- **log-file-id** — Instructs the events selected for the log ID to be directed to the `log-file-id`. The characteristics of the `log-file-id` referenced here must have already been defined in the `config>log>file log-file-id` context.

  **Values**
  
  1 — 99
### to memory

**Syntax**
```
to memory [size]
```

**Context**
```
config>log>log-id log-id
```

**Description**
This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. 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.

The source of the data stream must be specified in the `from` command prior to configuring the destination with the `to` command.

The `to` command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

**Default**
none

**Parameters**
- **size** — The `size` parameter indicates the number of events that can be stored in the memory.
  - **Default**
    - 100
  - **Values**
    - 50 — 1024

### to session

**Syntax**
```
to session
```

**Context**
```
config>log>log-id log-id
```

**Description**
This command specifies a log ID destination. This parameter is mandatory when configuring a log destination. 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 `session` destination is not saved in the configuration file.

The source of the data stream must be specified in the `from` command prior to configuring the destination with the `to` command.

The `to` command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

**Default**
none
Event and Accounting Logs

### to snmp

**Syntax**
```
to snmp [size]
```

**Context**
```
config>log>log-id log-id
```

**Description**
This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination. This command instructs the alarms and traps to be directed to the `snmp-trap-group` associated with `log-id`.

A local circular memory log is always maintained for SNMP notifications sent to the specified snmp-trap-group for the `log-id`.

The source of the data stream must be specified in the `from` command prior to configuring the destination with the `to` command.

The `to` command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

**Default**
none

**Parameters**
- `size` — The `size` parameter defines the number of events stored in this memory log.
  - **Default**
    - 100
  - **Values**
    - 50 — 1024

### to syslog

**Syntax**
```
to syslog syslog-id
```

**Context**
```
config>log>log-id
```

**Description**
This is one of the commands used to specify the log ID destination. This parameter is mandatory when configuring a log destination.

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 1k bytes.

The source of the data stream must be specified in the `from` command prior to configuring the destination with the `to` command.

The `to` command cannot be modified or re-entered. If the destination or maximum size of an SNMP or memory log needs to be modified, the log ID must be removed and then re-created.

**Default**
none

**Parameters**
- `syslog-id` — Instructs the events selected for the log ID to be directed to the `syslog-id`. The characteristics of the `syslog-id` referenced here must have been defined in the `config>log>syslog syslog-id` context.
  - **Values**
    - 1 — 10
time-format

Syntax  
\texttt{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  
\texttt{utc}

Parameters  
\texttt{local} — Specifies that timestamps are written in the system’s local time.

\texttt{utc} — Specifies that timestamps are written using the UTC value. This was formerly called Greenwich Mean Time (GMT) and Zulu time.
Accounting Policy Commands

accounting-policy

Syntax:

- `accounting-policy policy-id [interval minutes]`
- `no accounting-policy policy-id`

Context:

`config>log`

Description:

This command creates an access or network accounting policy. An accounting policy defines the accounting records that are created.

Access accounting policies are policies that can be applied to one or more SAPs. Changes made to an existing policy, using any of the sub-commands, are applied immediately to all SAPs where this policy is applied.

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. If a default access policy is not specified, then no accounting records are collected other than the records for the accounting policies that are explicitly configured.

Only one policy can be regarded as the default access policy. If a policy is configured as the default policy, then a `no default` command must be used to allow the data that is currently being collected to be written before a new access default policy can be configured.

Network accounting policies are policies that can be applied to one or more network ports. Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all network ports where this policy is applied.

If no accounting policy is defined on a network port, accounting records will be produced in accordance with the default network policy as designated with the default command. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured.

Only one policy can be regarded as the default network policy. If a policy is configured as the default policy, then a `no default` command must be used to allow the data that is currently being collected to be written before a new network default policy can be configured.

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, network ports or channels where the policy is applied.

Default:

No default accounting policy is defined.

Parameters:

`policy-id` — The policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.

Values:

- `1 — 99`
default

Syntax  [no] default
Context  config>log>accounting-policy
Description  This command configures the default accounting policy to be used with all SAPs that do not have an 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, then no accounting records will be collected other than the records for the accounting policies that are explicitly configured.

If no network accounting policy is defined on a network port, accounting records will be produced in accordance with the default network policy. If no network default policy is created, then no accounting records will be collected other than the records for the accounting policies explicitly configured.

Only one access accounting policy ID can be designated as the default access policy. Likewise, only one network accounting policy ID can be designated as the default network accounting 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 or network ports 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. A record name can only be used in one accounting policy. To obtain a list of all record types that can be configured, use the show log accounting-records command.

A:ALU-7210# show log accounting-records
==================================================================================================================================================================
Accounting Policy Records
==================================================================================================================================================================
<table>
<thead>
<tr>
<th>Record #</th>
<th>Record Name</th>
<th>Def. Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>service-ingress-octets</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>service-ingress-packets</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>network-ingress-octets</td>
<td>15</td>
</tr>
<tr>
<td>4</td>
<td>network-ingress-packets</td>
<td>15</td>
</tr>
</tbody>
</table>
==================================================================================================================================================================
A:ALU-7210#
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 then the record command with the new record name can be entered and it will replace the old record name.

When configuring an accounting policy for network ports, a network record should be selected. When changing the record name to another network record, the record command with the new record name can be entered and it will replace the old record name.

If the change required modifies the record from one type to another, then the old record name must be removed using the **no** form of this command.

Only one record may be configured in a single accounting policy. For example, if an accounting-policy is configured with a **access-egress-octets** record, in order to change it to **service-ingress-octets**, use the **no record** command under the accounting-policy to remove the old record and then enter the **service-ingress-octets** record.

Note that 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. The following table lists the accounting record names available and the default collection interval.

---

**to**

**Syntax**
```plaintext
to file file-id
```

**Context**
```plaintext
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 selected for this destination. The characteristics of the file-id must have already been defined in the `config>log>file` context. A file-id can only be used once.

The file is generated when the file policy is referenced. This command identifies the type of accounting file to be created. The file definition defines its characteristics.

If the **to** command is executed while the accounting policy is in operation, then it becomes active during the next collection interval.

| Values | 1 — 99 |
Show Commands

accounting-policy

Syntax: accounting-policy [acct-policy-id] [access | network]

Context: show>log

Description: This command displays accounting policy information.

Parameters:
- policy-id — The policy ID that uniquely identifies the accounting policy, expressed as a decimal integer.

Values:
- 1 — 99

access — Only displays access accounting policies.

network — Only displays network accounting policies.

Output: Accounting Policy Output — The following table describes accounting policy output fields.

Table 28: Show Accounting Policy Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy ID</td>
<td>The identifying value assigned to a specific policy.</td>
</tr>
<tr>
<td>Type</td>
<td>Identifies accounting record type forwarded to the configured accounting file.</td>
</tr>
<tr>
<td></td>
<td>access — Indicates that the policy is an access accounting policy.</td>
</tr>
<tr>
<td></td>
<td>network — Indicates that the policy is a network accounting policy.</td>
</tr>
<tr>
<td></td>
<td>none — Indicates no accounting record types assigned.</td>
</tr>
<tr>
<td>Def</td>
<td>Yes — Indicates that the policy is a default access or network policy.</td>
</tr>
<tr>
<td></td>
<td>No — Indicates that the policy is not a default access or network policy.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Displays the administrative state of the policy.</td>
</tr>
<tr>
<td></td>
<td>Up — Indicates that the policy is administratively enabled.</td>
</tr>
<tr>
<td></td>
<td>Down — Indicates that the policy is administratively disabled.</td>
</tr>
<tr>
<td>Oper State</td>
<td>Displays the operational state of the policy.</td>
</tr>
<tr>
<td></td>
<td>Up — Indicates that the policy is operationally up.</td>
</tr>
<tr>
<td></td>
<td>Down — Indicates that the policy is operationally down.</td>
</tr>
</tbody>
</table>
A:ALA-1# show log accounting-policy

A:ALA-1# show log accounting-policy 10

A:ALA-1# show log accounting-policy network
### Accounting Policies

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Def Admin Oper</th>
<th>Intvl</th>
<th>File Record Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>State State</td>
<td>Id</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>----------------</td>
<td>-------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>1</td>
<td>network No Up Up Up 15 1</td>
<td>network-ingress-packets</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>network Yes Up Up Up 15 2</td>
<td>network-ingress-octets</td>
<td></td>
</tr>
</tbody>
</table>

```
A:ALA-1# show log accounting-policy access
```

```
A:ALA-1# show log accounting-policy access
```

### Accounting Records

**Syntax**
```
accounting-records
```

**Context**
```
show>log
```

**Description**
This command displays accounting policy record names.

**Output**

**Accounting Records Output.** The following table describes accounting records output fields.

#### Table 29: Accounting Policy Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record #</td>
<td>The record ID that uniquely identifies the accounting policy, expressed as a decimal integer.</td>
</tr>
<tr>
<td>Record Name</td>
<td>The accounting record name.</td>
</tr>
<tr>
<td>Def. Interval</td>
<td>The default interval, in minutes, in which statistics are collected and written to their destination.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
*A:7210-E>show>log# accounting-records
```

```
Accounting Policy Records

Record # Record Name Def. Interval
---------------------------
1 service-ingress-octets 5
```

7210 SAS E OS System Management Guide Page 287
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:ALA-1# show log applications
==================================
Log Event Application Names
==================================
Application Name
-----------------------------------
CCAG
CHASSIS
CPMHWFILTER
DHCP
DEBUG
DOT1X
FILTER
IGMP
IGMP_SNOOPING
IP
ISIS
LAG
LDP
LOGGER
MIRROR
MPLS
OAM
OSPF
PORT
PPP
QOS
RIP
ROUTE_POLICY
RSVP
SECURITY
SNMP
STP
SVCMGR
SYSTEM
USER
VRRP
VRTR
==================================
event-control

**Syntax**
```
event-control [application [event-name | event-number]]
```

**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**
- **application** — Only displays event control for the specified application.
  - **Default** All applications.
- **event-name** — Only displays event control for the named application event.
  - **Default** All events for the application.
- **event-number** — Only displays event control for the specified application event number.
  - **Default** All events for the application.

**Output**
- **Show Event Control Output** — The following table describes the output fields for the event control.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>The application name.</td>
</tr>
<tr>
<td>ID#</td>
<td>The event ID number within the application.</td>
</tr>
<tr>
<td></td>
<td>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”.</td>
</tr>
<tr>
<td>Event Name</td>
<td>The event name.</td>
</tr>
<tr>
<td>P</td>
<td>CL — The event has a cleared severity/priority.</td>
</tr>
<tr>
<td></td>
<td>CR — The event has critical severity/priority.</td>
</tr>
<tr>
<td></td>
<td>IN — The event has indeterminate severity/priority.</td>
</tr>
<tr>
<td></td>
<td>MA — The event has major severity/priority.</td>
</tr>
<tr>
<td></td>
<td>MI — The event has minor severity/priority.</td>
</tr>
<tr>
<td></td>
<td>WA — The event has warning severity/priority.</td>
</tr>
<tr>
<td>g/s</td>
<td>gen — The event will be generated/logged by event control.</td>
</tr>
<tr>
<td></td>
<td>sup — The event will be suppressed/dropped by event control.</td>
</tr>
<tr>
<td></td>
<td>thr — Specifies that throttling is enabled.</td>
</tr>
</tbody>
</table>
### Sample Output

```bash
A:gal171# show log event-control
```

<table>
<thead>
<tr>
<th>Application</th>
<th>ID#</th>
<th>Event Name</th>
<th>P</th>
<th>g/s</th>
<th>Logged</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHASSIS:</td>
<td>2001</td>
<td>cardFailure</td>
<td>MA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2002</td>
<td>cardInserted</td>
<td>MI</td>
<td>gen</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2003</td>
<td>cardRemoved</td>
<td>MI</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2004</td>
<td>cardWrong</td>
<td>MI</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2005</td>
<td>EnvTemperatureTooHigh</td>
<td>MA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPM/HWFILTER:</td>
<td>2001</td>
<td>sdptIsDHCPSusiciousPcktRcvd</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DHCP:</td>
<td>2002</td>
<td>sapTlsDHCPLseSTEntriesExceeded</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2003</td>
<td>sapTlsDHCPLseStateOverride</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2004</td>
<td>sapTlsDHCPSusiciousPcktRcvd</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2005</td>
<td>svcTlsDHCPLseSTRestoreProblem</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2006</td>
<td>svcTlsDHCPLseStatePopulateErr</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2007</td>
<td>tmnxVRtrDHCPLeaseStsExceeded</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2008</td>
<td>tmnxVRtrDHCPLeaseStateOverride</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2009</td>
<td>tmnxVRtrDHCPSusiciousPcktRcvd</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2010</td>
<td>tmnxVRtrDHCPLeaseSTRestoreProblem</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2011</td>
<td>tmnxVRtrDHCPLeaseStatePopulateErr</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DEBUG:</td>
<td>L 2001</td>
<td>traceEvent</td>
<td>MI</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DOTIX:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FILTER:</td>
<td>2001</td>
<td>filterPBRPacketsDropped</td>
<td>MI</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IP:</td>
<td>L 2001</td>
<td>clearRTMErro</td>
<td>MI</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>L 2002</td>
<td>ipEtherBroadcast</td>
<td>MI</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>L 2003</td>
<td>ipDuplicateAddress</td>
<td>MI</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>L 2004</td>
<td>ipArpInfoOverwritten</td>
<td>MI</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>L 2005</td>
<td>fibAddFailed</td>
<td>MA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>L 2006</td>
<td>qosNetworkPolicyMallocFailed</td>
<td>MA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>L 2007</td>
<td>ipArpBadInterface</td>
<td>MI</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>L 2008</td>
<td>ipArpDuplicateIpAddress</td>
<td>MI</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>L 2009</td>
<td>ipArpDuplicateMacAddress</td>
<td>MI</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ISIS:</td>
<td>2001</td>
<td>vRtrIsisDatabaseOverload</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2002</td>
<td>vRtrIsisManualAddressDrops</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2003</td>
<td>vRtrIsisCorruptedLSPDetected</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2004</td>
<td>vRtrIsisMaxSegExceedAttempt</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2005</td>
<td>vRtrIsisIDLenMismatch</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>2006</td>
<td>vRtrIsisMaxAreaAddrMismatch</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logged</td>
<td>The number of events logged/generated.</td>
</tr>
<tr>
<td>Dropped</td>
<td>The number of events dropped/suppressed.</td>
</tr>
</tbody>
</table>

*Label Description (Continued)*
Event and Accounting Logs

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

VRRP:
2001 vrrpTrapNewMaster MI  gen  0  0
2002 vrrpTrapAuthFailure MI  gen  0  0
2003 tmnxVrrpIPListMismatch MI  gen  0  0
2004 tmnxVrrpIPListMismatchClear MI  gen  0  0
2005 tmnxVrrpMultipleOwners MI  gen  0  0
2006 tmnxVrrpBecomeBackup MI  gen  0  0
L  2007 vrrpPacketDiscarded MI  gen  0  0

VRTR:
2001 tmnxVRtrMidRouteTCA MI  gen  0  0
2002 tmnxVRtrHighRouteTCA MI  gen  0  0
2003 tmnxVRtrHighRouteCleared MI  gen  0  0
2004 tmnxVRtrIllegalLabelTCA MA  gen  0  0
2005 tmnxVRtrMcastMidRouteTCA MI  gen  0  0
2006 tmnxVRtrMcastMaxRoutesTCA MI  gen  0  0
2007 tmnxVRtrMcastMaxRoutesCleared MI  gen  0  0
2008 tmnxVRtrMaxArpEntriesTCA MA  gen  0  0
2009 tmnxVRtrMaxArpEntriesCleared MI  gen  0  0
2011 tmnxVRtrMaxRoutes MI  gen  0  0

A:ALA-1#

A:ALA-1# show log event-control ospf

Log Events

Application

<table>
<thead>
<tr>
<th>ID#</th>
<th>Event Name</th>
<th>P</th>
<th>g/s</th>
<th>Logged</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>ospfVirtIfStateChange</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2002</td>
<td>ospfNbrStateChange</td>
<td>WA</td>
<td>gen</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2003</td>
<td>ospfVirtNbrStateChange</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2004</td>
<td>ospfIfConfigError</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2005</td>
<td>ospfVirtIfConfigError</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2006</td>
<td>ospfIfAuthFailure</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2007</td>
<td>ospfVirtIfAuthFailure</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2008</td>
<td>ospfIfRxBadPacket</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2009</td>
<td>ospfVirtIfTxRetransmit</td>
<td>WA</td>
<td>sup</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2010</td>
<td>ospfIfTxRetransmit</td>
<td>WA</td>
<td>sup</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2011</td>
<td>ospfVirtIfTxRetransmit</td>
<td>WA</td>
<td>sup</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2012</td>
<td>ospfOriginateLsa</td>
<td>WA</td>
<td>sup</td>
<td>0  404</td>
<td>0</td>
</tr>
<tr>
<td>2013</td>
<td>ospfMaxAgeLsa</td>
<td>WA</td>
<td>gen</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2014</td>
<td>ospfLsdbOverflow</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2015</td>
<td>ospfLsdbApproachingOverflow</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2016</td>
<td>ospfIfStateChange</td>
<td>WA</td>
<td>gen</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2017</td>
<td>ospfRnssTranslatorStatusChange</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
2018 vRtrOspfSpfRunsStopped WA gen 0 0
2019 vRtrOspfSpfRunsRestarted WA gen 0 0
2020 vRtrOspfOverloadEntered WA gen 1 0
2021 vRtrOspfOverloadExited WA gen 0 0
2022 ospfRestartStatusChange WA gen 0 0
2023 ospfNbrRestartHelperStatusChange WA gen 0 0
2024 ospfVirtNbrRestartHelperStsChg WA gen 0 0

A:ALA-1#

A:ALA-1# show log event-control ospf ospfVirtIfStateChange

Log Events

Application

<table>
<thead>
<tr>
<th>ID#</th>
<th>Event Name</th>
<th>P</th>
<th>g/s</th>
<th>Logged</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>ospfVirtIfStateChange</td>
<td>WA</td>
<td>gen</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

file-id

**Syntax**  
file-id [log-file-id]

**Context**  
show>log

**Description**  
This command displays event file log information.

If no command line parameters are specified, a summary output of all event log files is displayed.

Specifying a file ID displays detailed information on the event file log.

**Parameters**  
log-file-id — Displays detailed information on the specified event file log.

**Output**  
Log File Output — The following table describes the output fields for a log file summary.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file-id</td>
<td>The log file ID.</td>
</tr>
<tr>
<td>rollover</td>
<td>The rollover time for the log file which is how long in between partitioning of the file into a new file.</td>
</tr>
<tr>
<td>retention</td>
<td>The retention time for the file in the system which is how long the file should be retained in the file system.</td>
</tr>
<tr>
<td>admin location</td>
<td>The primary flash device specified for the file location.</td>
</tr>
<tr>
<td>none</td>
<td>indicates no specific flash device was specified.</td>
</tr>
<tr>
<td>oper location</td>
<td>The actual flash device on which the log file exists.</td>
</tr>
<tr>
<td>file-id</td>
<td>The log file ID.</td>
</tr>
</tbody>
</table>
Event and Accounting Logs

Sample Output

filter-id

**Syntax**  
filter-id [filter-id]

**Context**  
show>log

**Description**  
This command displays event log filter policy information.

**Parameters**  
filter-id — Displays detailed information on the specified event filter policy ID.

**Output**  
**Event Log Filter Summary Output** — The following table describes the output fields for event log filter summary information.

**Table 30: Event Log Filter Summary Output Fields**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rollover</td>
<td>The rollover time for the log file which is how long in between partitioning of the file into a new file.</td>
</tr>
<tr>
<td>retention</td>
<td>The retention time for the file in the system which is how long the file should be retained in the file system.</td>
</tr>
<tr>
<td>file name</td>
<td>The complete pathname of the file associated with the log ID.</td>
</tr>
<tr>
<td>expired</td>
<td>Indicates whether or not the retention period for this file has passed.</td>
</tr>
</tbody>
</table>
| state       | in progress — Indicates the current open log file.  
complete — Indicates the old log file. |

---

7210 SAS E OS System Management Guide   Page 293
Sample Output

*A:ALA-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:ALA-48>config>log#

Event Log Filter Detailed Output — The following table describes the output fields for detailed event log filter information.

Table 31: Event Log Filter Detail Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter-id</td>
<td>The event log filter ID.</td>
</tr>
<tr>
<td>Applied</td>
<td>no — The event log filter is not currently in use by a log ID.</td>
</tr>
<tr>
<td></td>
<td>yes — The event log filter is currently in use by a log ID.</td>
</tr>
<tr>
<td>Default Action</td>
<td>drop — The default action for the event log filter is to drop events</td>
</tr>
<tr>
<td></td>
<td>not matching filter entries.</td>
</tr>
<tr>
<td></td>
<td>forward — The default action for the event log filter is to forward</td>
</tr>
<tr>
<td></td>
<td>events not matching filter entries.</td>
</tr>
<tr>
<td>Description</td>
<td>The description string for the filter ID.</td>
</tr>
<tr>
<td>(Filter-id)</td>
<td></td>
</tr>
</tbody>
</table>

Table 32: Log Filter Match Criteria Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry-id</td>
<td>The event log filter entry ID.</td>
</tr>
<tr>
<td>Action</td>
<td>default — There is no explicit action for the event log filter entry</td>
</tr>
<tr>
<td></td>
<td>and the filter’s default action is used on matching events.</td>
</tr>
<tr>
<td></td>
<td>drop — The action for the event log filter entry is to drop matching</td>
</tr>
<tr>
<td></td>
<td>events.</td>
</tr>
<tr>
<td></td>
<td>forward — The action for the event log filter entry is to forward</td>
</tr>
<tr>
<td></td>
<td>matching events.</td>
</tr>
</tbody>
</table>
Table 32: Log Filter Match Criteria Output Fields  (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description (Entry-id)</td>
<td>The description string for the event log filter entry.</td>
</tr>
<tr>
<td>Application</td>
<td>The event log filter entry application match criterion.</td>
</tr>
<tr>
<td>Event Number</td>
<td>The event log filter entry application event ID match criterion.</td>
</tr>
<tr>
<td>Severity</td>
<td>cleared — The log event filter entry application event severity cleared match criterion.</td>
</tr>
<tr>
<td></td>
<td>indeterminate — The log event filter entry application event severity indeterminate match criterion.</td>
</tr>
<tr>
<td></td>
<td>critical — The log event filter entry application event severity critical match criterion.</td>
</tr>
<tr>
<td></td>
<td>major — The log event filter entry application event severity cleared match criterion.</td>
</tr>
<tr>
<td></td>
<td>minor — The log event filter entry application event severity minor match criterion.</td>
</tr>
<tr>
<td></td>
<td>warning — The log event filter entry application event severity warning match criterion.</td>
</tr>
<tr>
<td>Subject</td>
<td>Displays the event log filter entry application event ID subject string match criterion.</td>
</tr>
<tr>
<td>Router</td>
<td>Displays the event log filter entry application event ID router router-instance string match criterion.</td>
</tr>
<tr>
<td>Operator</td>
<td>There is an operator field for each match criteria: application, event number, severity, and subject.</td>
</tr>
<tr>
<td></td>
<td>equal — Matches when equal to the match criterion.</td>
</tr>
<tr>
<td></td>
<td>greaterThan — Matches when greater than the match criterion.</td>
</tr>
<tr>
<td></td>
<td>greaterThanOrEqual — Matches when greater than or equal to the match criterion.</td>
</tr>
<tr>
<td></td>
<td>lessThan — Matches when less than the match criterion.</td>
</tr>
<tr>
<td></td>
<td>lessThanOrEqual — Matches when less than or equal to the match criterion.</td>
</tr>
<tr>
<td></td>
<td>notEqual — Matches when not equal to the match criterion.</td>
</tr>
<tr>
<td></td>
<td>off — No operator specified for the match criterion.</td>
</tr>
</tbody>
</table>
Sample Output

*A:ALA-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:ALA-48>config>log#

log-collector

Syntax log-collector

Context show>log

Description Show log collector statistics for the main, security, change and debug log collectors.

Output Log-Collector Output — The following table describes log-collector output fields.

Table 33: Show Log-Collector Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Collector Name&gt;</td>
<td>Main — The main event stream contains the events that are not explicitly directed to any other event stream.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Change — The change event stream contains all events that directly affect the configuration or operation of this node.</td>
</tr>
<tr>
<td></td>
<td>Debug — The debug-trace stream contains all messages in the debug stream.</td>
</tr>
<tr>
<td>Dest. Log ID</td>
<td>Specifies the event log stream destination.</td>
</tr>
</tbody>
</table>
Table 33: Show Log-Collector Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter ID</td>
<td>The value is the index to the entry which 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.</td>
</tr>
<tr>
<td>Status</td>
<td>Enabled — Logging is enabled.</td>
</tr>
<tr>
<td></td>
<td>Disabled — Logging is disabled.</td>
</tr>
<tr>
<td>Dest. Type</td>
<td>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 will be directed to a file on one of the system's compact flash disks. Memory — All selected log events will be directed to an in-memory storage area.</td>
</tr>
</tbody>
</table>

Sample Output

A:ALA-1# show log log-collector

Log Collectors

<table>
<thead>
<tr>
<th>Dest Log Id</th>
<th>Filter Id</th>
<th>Status</th>
<th>Dest Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>99</td>
<td>0</td>
<td>enabled</td>
<td>memory</td>
</tr>
<tr>
<td>100</td>
<td>1001</td>
<td>enabled</td>
<td>memory</td>
</tr>
</tbody>
</table>

Security  Logged : 3  Dropped : 0
Change     Logged : 3896 Dropped : 0
Debug      Logged : 0   Dropped : 0

A:ALA-1#
log-id

Syntax

log-id [log-id] [severity severity-level] [application application] [sequence from-seq [to-seq]] [count count] [router router-instance [expression]] [subject subject [regexp]] [ascending | descending]

Context show>log

Description

This command displays an event log summary with settings and statistics or the contents of a specific log file, SNMP log, or memory log.

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.

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.

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.

Parameters

log-id — Displays the contents of the specified file log or memory log ID. The log ID must have a destination of an SNMP or file log or a memory log for this parameter to be used.

Default Displays the event log summary

Values 1 — 99

severity severity-level — Displays only events with the specified and higher severity.

Default All severity levels

Values cleared, indeterminate, critical, major, minor, warning

application application — Displays only events generated by the specified application.

Default All applications

expression — Specifies to use a regular expression as match criteria for the router instance string.

sequence from-seq [to-seq] — Displays the log entry numbers from a particular entry sequence number (from-seq) to another sequence number (to-seq). The to-seq value must be larger than the from-seq value.

If the to-seq number is not provided, the log contents to the end of the log is displayed unless the count parameter is present in which case the number of entries displayed is limited by the count.

Default All sequence numbers

Values 1 — 4294967295

count count — Limits the number of log entries displayed to the number specified.

Default All log entries

Values 1 — 4294967295

router-instance — Specifies a router name up to 32 characters to be used in the display criteria.
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 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

Show Log-ID Output — The following table describes the log ID field output.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Id</td>
<td>An event log destination.</td>
</tr>
<tr>
<td>Source</td>
<td>no — The event log filter is not currently in use by a log ID.</td>
</tr>
<tr>
<td></td>
<td>yes — The event log filter is currently in use by a log ID.</td>
</tr>
<tr>
<td>Filter ID</td>
<td>The value is the index to the entry which defines the filter to be applied</td>
</tr>
<tr>
<td></td>
<td>to this log's source event stream to limit the events output to this log's</td>
</tr>
<tr>
<td></td>
<td>destination. If the value is 0, then all events in the source log are</td>
</tr>
<tr>
<td></td>
<td>forwarded to the destination.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up — Indicates that the administrative state is up.</td>
</tr>
<tr>
<td></td>
<td>Down — Indicates that the administrative state is down.</td>
</tr>
<tr>
<td>Oper State</td>
<td>Up — Indicates that the operational state is up.</td>
</tr>
<tr>
<td></td>
<td>Down — Indicates that the operational state is down.</td>
</tr>
<tr>
<td>Logged</td>
<td>The number of events that have been sent to the log source(s) that were</td>
</tr>
<tr>
<td></td>
<td>forwarded to the log destination.</td>
</tr>
<tr>
<td>Dropped</td>
<td>The number of events that have been sent to the log source(s) that were</td>
</tr>
<tr>
<td></td>
<td>not forwarded to the log destination because they were filtered out by the</td>
</tr>
<tr>
<td></td>
<td>log filter.</td>
</tr>
<tr>
<td>Dest. Type</td>
<td>Console — All selected log events are directed to the system console.</td>
</tr>
<tr>
<td></td>
<td>If the console is not connected, then all entries are dropped.</td>
</tr>
<tr>
<td></td>
<td>Syslog — All selected log events are sent to the syslog address.</td>
</tr>
<tr>
<td></td>
<td>SNMP traps — Events defined as SNMP traps are sent to the configured SNMP</td>
</tr>
<tr>
<td></td>
<td>trap destinations and are logged in NOTIFICATION-LOG-MIB tables.</td>
</tr>
<tr>
<td></td>
<td>File — All selected log events will be directed to a file on one of the</td>
</tr>
<tr>
<td></td>
<td>'s compact flash disks.</td>
</tr>
</tbody>
</table>
Sample Output

A:ALA-1# show log log-id

=====================================================================
Event Logs
=====================================================================

<table>
<thead>
<tr>
<th>Log Source</th>
<th>Filter</th>
<th>Admin</th>
<th>Oper</th>
<th>Logged</th>
<th>Dropped</th>
<th>Dest</th>
<th>Dest Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>none</td>
<td>none</td>
<td>up</td>
<td>down</td>
<td>52</td>
<td>0</td>
<td>file</td>
</tr>
<tr>
<td>2</td>
<td>C</td>
<td>none</td>
<td>up</td>
<td>up</td>
<td>41</td>
<td>0</td>
<td>syslog</td>
</tr>
<tr>
<td>99</td>
<td>M</td>
<td>none</td>
<td>up</td>
<td>up</td>
<td>2135</td>
<td>0</td>
<td>memory</td>
</tr>
</tbody>
</table>

=====================================================================
A:ALA-1#

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=70 (not wrapped)]

69 2007/01/25 18:20:40.00 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode. There is no standby CPM card."

68 2007/01/25 17:48:38.16 UTC WARNING: SYSTEM #2006 Base LOGGER
"New event throttle interval 10, configuration modified"

67 2007/01/25 00:34:53.97 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode. There is no standby CPM card."

66 2007/01/24 22:59:22.00 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode. There is no standby CPM card."

65 2007/01/24 02:08:47.92 UTC CRITICAL: SYSTEM #2029 Base Redundancy
"The active CPM card A is operating in singleton mode. There is no standby CPM card."
...

A:gal171

A:NS061550532>config>log>snmp-trap-group# show log log-id 1

A:NS061550532>config>log>snmp-trap-group# show log log-id 1

A:gal171

A:NS061550532>config>log>snmp-trap-group# show log log-id 1

A:gal171

A:NS061550532>config>log>snmp-trap-group#

snmp-trap-group

Syntax snmp-trap-group [log-id]

Context show>log

Description This command displays SNMP trap group configuration information.

Parameters log-id — Displays only SNMP trap group information for the specified trap group log ID.

Values 1 — 99

Output SNMP Trap Group Output — The following table describes SNMP trap group output fields.

Table 34: SNMP Trap Group Output Fields

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log-ID</td>
<td>The log destination ID for an event stream.</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address of the trap receiver,</td>
</tr>
<tr>
<td>Port</td>
<td>The destination UDP port used for sending traps to the destination, expressed as a decimal integer.</td>
</tr>
<tr>
<td>Version</td>
<td>Specifies the SNMP version format to use for traps sent to the trap receiver. Valid values are snmpv1, snmpv2c, snmpv3.</td>
</tr>
</tbody>
</table>
Table 34: SNMP Trap Group Output Fields (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community</td>
<td>The community string required by snmpv1 or snmpv2c trap receivers.</td>
</tr>
<tr>
<td>Security-Level</td>
<td>The required authentication and privacy levels required to access the views on this node.</td>
</tr>
</tbody>
</table>

Sample SNMP Trap Group Output

```
A:SetupCLI>config>log>snmp-trap-group# show log snmp-trap-group 44

SNMP Trap Group 44
Description : none

Name : ntt-test
Address : 10.10.10.3
Port : 162
Version : v2c
Community : ntttesting
Sec. Level : none

Name : test2
Address : 20.20.20.5
Port : 162
Version : v2c
Community : ntttesting
Sec. Level : none
```

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 — 10
```
**Output**

**Syslog Event Log Destination Summary Output** — The following table describes the syslog output fields.

**Table 35: Show Log Syslog Output Fields**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog ID</td>
<td>The syslog ID number for the syslog destination.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the syslog target host.</td>
</tr>
<tr>
<td>Port</td>
<td>The configured UDP port number used when sending syslog messages.</td>
</tr>
<tr>
<td>Facility</td>
<td>The facility code for messages sent to the syslog target host.</td>
</tr>
<tr>
<td>Severity Level</td>
<td>The syslog message severity level threshold.</td>
</tr>
<tr>
<td>Below Level Dropped</td>
<td>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.</td>
</tr>
<tr>
<td>Prefix Present</td>
<td>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.</td>
</tr>
<tr>
<td>Description</td>
<td>A text description stored in the configuration file for a configuration context.</td>
</tr>
<tr>
<td>LogPrefix</td>
<td>The prefix string prepended to the syslog message.</td>
</tr>
<tr>
<td>Log-id</td>
<td>Events are directed to this destination.</td>
</tr>
</tbody>
</table>

**Sample Syslog Event Log Destination Summary Output**

*A:ALA-48>config>log# show log syslog

===============================================================================
Syslog Target Hosts
===============================================================================
<table>
<thead>
<tr>
<th>Id</th>
<th>Ip Address</th>
<th>Port</th>
<th>Facility</th>
<th>Sev Level</th>
<th>Below Level Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>unknown</td>
<td>514</td>
<td>local7</td>
<td>info</td>
<td>yes</td>
</tr>
<tr>
<td>3</td>
<td>unknown</td>
<td>514</td>
<td>local7</td>
<td>info</td>
<td>yes</td>
</tr>
<tr>
<td>5</td>
<td>unknown</td>
<td>514</td>
<td>local7</td>
<td>info</td>
<td>yes</td>
</tr>
<tr>
<td>10</td>
<td>unknown</td>
<td>514</td>
<td>local7</td>
<td>info</td>
<td>yes</td>
</tr>
</tbody>
</table>

*A:ALA-48>config>log#

*A:MV-SR>config>log# show log syslog 1
Syslog Target 1

IP Address : 192.168.15.22
Port : 514
Log-ids : none
Prefix : Sr12
Facility : local1
Severity Level : info
Prefix Level : yes
Below Level Drop : 0
Description : Linux Station Springsteen

*A:MV-SR>config>log#
Clear Commands

log

Syntax  log log-id
Context  clear

Description  Reinitializes/rolls over the specified memory/file event log ID. Memory logs are reinitialized and cleared of contents. File logs are manually rolled over by this command.

This command is only applicable to event logs that are directed to file destinations and memory destinations.

SNMP, syslog and console/session logs are not affected by this command.

Parameters  log-id. The event log ID to be initialized/rolled over.

Values  1 — 100
Standards and Protocol Support

Standards Compliance
IEEE 802.1d Bridging
IEEE 802.1p/Q VLAN Tagging
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Based Network Access Control
IEEE 802.1ad Provider Bridges
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3ah Ethernet OAM
IEEE 802.3u 100BaseTX
IEEE 802.3z 100BaseSX/LX

Protocol Support

DIFFERENTIATED SERVICES
RFC 2474 Definition of the DS Field in the IPv4 and IPv6 Headers (Rev)
RFC 2597 Assured Forwarding PHB Group (rev 3260)
RFC 2598 An Expedited Forwarding PHB
RFC 3140 Per-Hop Behavior Identification Codes

TCP/IP
RFC 768 UDP
RFC 1350 The TFTP Protocol (Rev.
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 1519 CIDR
RFC 1812 Requirements for IPv4 Routers
RFC 2347 TFTP option Extension
RFC 2328 TFTP Blocksize Option
RFC 2349 TFTP Timeout Interval and Transfer Size option

RADIUS
RFC 2856 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

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

TACACS+
draft-grant-tacacs-02.txt

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 1215 A Convention for Defining Traps for use with the SNMP
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2096 IP-FORWARD-MIB
RFC 2138 RADIUS
RFC 2571 SNMP-FRAMEWORK-MIB
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 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 3014 NOTIFICATION-LOGMIB

RFC 3164 Syslog
RFC 3273 HCRMON-MIB
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
IANA-Iftype-MIB
IEEE8023-LAG-MIB

Proprietary MIBs
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-DOT3-OAM-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-IEEE8021-CFM-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MIRROR-MIB.mib
TIMETRA-NTP-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-SAS-GLOBAL-MIB.mib
TIMETRA-SAS-PORT-MIB.mib
TIMETRA-SAS-QOS-MIB.mib
TIMETRA-SAS-SYSTEM-MIB.mib
TIMETRA-SCHEDULER-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SUBSCRIBER-MGMT-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TCP-MIB.mib
TIMETRA-VRTR-MIB.mib
INDEX

B
BOF
overview
compact flash
storing log files 199
synchronization
VSA home directory 30

L
Log
overview 196
accounting 214
accounting records 214
default system log 213
destinations 198
event control 206
event filter policies 209
event log entries 210
event logs 203
event sources 204
log files 199
log manager 208
SNMP trap groups 201
syslog 201
configuring
accounting policy 225
basic 221
command reference
  file ID commands 248
  filter commands 248
  log ID commands 249
  syslog commands 250
event control 226
event log 222
file ID 224
log filter 228
log types 220
management tasks 231
overview 220
SNMP trap group 229
syslog target 230

S
Security
overview
AAA 16
accounting 24
RADIUS 24
TACACS+ 24
authentication 17
RADIUS 18
TACACS+ 21
authorization 22
controls 26
encryption 39
SSH 35
configuring
accounting 49
RADIUS 65
TACACS+ 69
authentication 46
RADIUS 63
TACACS+ 67
authorization 47
RADIUS 64
TACACS+ 68
basic 50
login controls 71
management access filters 53
password management 55
profiles 56
SSH 70
users 57
encryption 39
keychains 42
SSH 35
VSAs 29
Alcatel-Lucent Dictionary 32

SNMP
overview
Index

access control 152
  access groups 153
  users 154
  USMs 153
  views 153
architecture 150
MIBs 150
versions 151
configuring
  access options 165
  basic 161
command reference
  security commands 169
  show commands 170
  system commands 169
community strings 163
SNMPv1 and SNMPv2 160
SNMPv3 160
USM community options 167
view options 164
command reference
  system commands 169
  user commands 170