Managing Alarms

The Monitoring feature in ACS generates alarms to notify you of critical system conditions. The monitoring component retrieves data from ACS. You can configure thresholds and rules on this data to manage alarms.

Alarm notifications are displayed in the web interface and you can get a notification of events through e-mail and Syslog messages. ACS filters duplicate alarms by default.

This chapter contains the following sections:

Understanding Alarms

There are two types of alarms in ACS:

Threshold Alarms

Threshold alarms are defined on log data collected from ACS servers that notify you of certain events. For example, you can configure threshold alarms to notify you of ACS system health, ACS process status, authentication activity or inactivity, and so on.

You define threshold conditions on these data sets. When a threshold condition is met, an alarm is triggered. While defining the threshold, you also define when the threshold should be applied (the time period), the severity of the alarm, and how the notifications should be sent.

Fifteen categories of available alarm thresholds allow you to monitor many different facets of ACS system behavior. See Creating, Editing, and Duplicating Alarm Thresholds, page 12-11 for more information on threshold alarms.

System Alarms

System alarms notify you of critical conditions encountered during the execution of the ACS Monitoring and Reporting viewer. System alarms also provide informational status of system activities, such as data purge events or failure of the log collector to populate the View database.

You cannot configure system alarms, which are predefined. However, you do have the option to disable system alarms or decide how you want to be notified if you have enabled them.

This section contains the following topics:

Evaluating Alarm Thresholds

ACS evaluates the threshold conditions based on a schedule. You define these schedules and, while creating a threshold, you assign a schedule to it. A schedule consists of one or more continuous or noncontinuous periods of time during the week.

For example, you can create a schedule that is active from 8:00 a.m. to 5:00 p.m., Monday through Friday. See Understanding Alarm Schedules, page 12-9 for more information. When you assign this schedule to a threshold, ACS evaluates the threshold and generates alarms only during the active period.

ACS evaluates the thresholds periodically depending on the number of thresholds that are currently enabled.

Table 12-1 provides the length of the evaluation cycle for a given number of thresholds.

Table 12-1 Evaluation Cycle of Alarm Thresholds

Number of Enabled Thresholds	Evaluation Cycle[1]
1 to 20	Every 2 minutes
21 to 50	Every 3 minutes
51 to 100	Every 5 minutes

1. If the time taken to evaluate the thresholds increase, then the evaluation cycle increases from 2 to 3 minutes, 3 to 5 minutes, and from 5 to 15 minutes. The evaluation cycle time is reset to 2, 3, and 5 minutes every 12 hours.

When an evaluation cycle begins, ACS evaluates each enabled threshold one after another. If the schedule associated with the threshold allows the threshold to be executed, ACS evaluates the threshold conditions. An alarm is triggered if the condition is met. See Creating, Editing, and Duplicating Alarm Thresholds, page 12-11 for more information.

Note System alarms do not have an associated schedule and are sent immediately after they occur. You can only enable or disable system alarms as a whole.

Notifying Users of Events

When a threshold is reached or a system alarm is generated, the alarm appears in the Alarms Inbox of the web interface. From this page, you can view the alarm details, add a comment about the alarm, and change its status to indicate that it is Acknowledged or Closed.

The alarm details in this page, wherever applicable, include one or more links to the relevant reports to help you investigate the event that triggered the alarm.

The Dashboard also displays the five most recent alarms. Alarms that you acknowledge or close are removed from this list in the Dashboard.

ACS provides you the option to receive notifications in the following formats:

- E-mail—Contains all the information that is present in the alarm details page. You can configure a list of recipients to whom this e-mail must be sent. ACS 5.6 provides you the option to receive notification of events through e-mail in HTML format.
- Syslog message—Sent to the Linux or Windows machines that you have configured as alarm syslog targets. You can configure up to two alarm syslog targets.

Viewing and Editing Alarms in Your Inbox

You can view alarms that ACS generates based on a threshold configuration or a rule on a set of data collected from ACS servers. Alarms that have met the configured thresholds are sent to your inbox. After you view an alarm, you can edit the status of the alarm, assign the alarm to an administrator, and add notes to track the event.

To view an alarm in your inbox, select **Monitoring and Reports > Alarms > Inbox**.

The Inbox page appears with a list of alarms that ACS triggered. Table 12-2 describes the fields on the Alarms page. Table 12-3 lists the system alarms in ACS 5.6 and its severity.

Table 12-2 Alarms Page

Option	Description
Severity	*Display only.* Indicates the severity of the associated alarm. Options are: • Critical • Warning • Info
Name	Indicates the name of the alarm. Click to display the Alarms: Properties page and edit the alarm.

Table 12-2 Alarms Page (continued)

Option	Description
Time	*Display only.* Indicates the time of the associated alarm generation in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • *timezone* = The time zone. • yyyy = A four-digit representation of the year.
Cause	*Display only.* Indicates the cause of the alarm.
Assigned To	*Display only.* Indicates who is assigned to investigate the alarm.
Status	*Display only.* Indicates the status of the alarm. Options are: • New—The alarm is new. • Acknowledged—The alarm is known. • Closed—The alarm is closed.
Edit	Check the check box next to the alarm that you want to edit, and click **Edit** to edit the status of the alarm and view the corresponding report.
Close	Check the check box next to the alarm that you want to close, and click **Close** to close the alarm. You can enter closing notes before you close an alarm. Closing an alarm only removes the alarm from the dashboard. It does not delete the alarm.
Delete	Check the check box next to the alarm that you want to delete, and click **Delete** to delete the alarm.

Table 12-3 System Alarms in ACS 5.6

Alarm	Severity
Purge Related Alarms	
Backup failed. Backup failed before Database Purge.	Critical
Backup successful. Backup failed before Database Purge.	Info
Database Purge for Daily Tables failed. Exception Details.	Critical
Database Purge for Monthly Tables failed. Exception Details.	Critical
Database Purge for Yearly Tables failed. Exception Details.	Critical
Incremental backup is not configured. Configuring incremental backup is necessary to make the database purge successful. This will help to avoid disk space issues. View database Size is file size in GB and size it occupies on the hard disk is actual db size in GB.	Warning
Configure Incremental Backup Data Repository as Remote Repository otherwise backup will fail and Incremental backup mode will be changed to off.	Warning

Table 12-3 System Alarms in ACS 5.6 (continued)

Alarm	Severity
Configure Remote Repository under Purge Configuration which is used to take a backup of data before purge.	Warning
View database size exceeds the maximum limit of maxLimit GB. View database Size is file size GB and size it occupies on the hard disk is actualDBSize GB. View database size exceeds the max limit of maxlimit GB.	Critical
View database size exceeds the upper limit of upperLimit GB. View database Size is file size GB and size it occupies on the hard disk is actualDBSize GB. View database size exceeds the upper limit of upperLimit GB.	Critical
ACS View DB Size exceeds the lower limit lowerLimit GB. View database Size is file size GB and size it occupies on the hard disk is actualDBSize GB. View database size exceeds the lower limit of lowerLimit GB.	Warning
DB Purge. Database Start Purging.	Info
Disk Space Limit Exceeded - Window at : Disk Space Limit Exceeded recommended threshold at one month data. Now Purging week data till it reaches lower limit.	Warning
ACS view Application Exceeded its Maximum Allowed Disk size. Disk Space Exceeded recommended threshold, extra monthsinnumber month(s) data purged.	Warning
ACS view Application Exceeded its Maximum Allowed Disk size. Disk Space Exceeded recommended threshold monthsinnumber month(s) data purged.	Info
Purge is successful. The size of records present in view data base is actualsizeinGB GB. The physical size of the view data base on the disk sizeinGB GB. If you want to reduce the physical size of the view data base, run acsview-db-compress command from acs-config mode through command line.	Warning
Purge process removed week week(s) data to reach lower limit	Info
Purge process was tried to remove maximum data to reach lower limit by purging last three weeks data but still acsview database size is having greater than lower limit. Currently we are keeping only last 1 week data.	Warning
The number of incoming log messages is reaching threshold value: GB's. Make sure that you configured ACS to send only the important category of messages to Log collector.	Warning
Incremental Backup	
On-demand Full Backup failed: Exception Details.	Critical
Full Database Backup failed. Exception Details.	Critical
Full Database Purge Backup failed. Exception Details.	Critical
Incremental Backup Failed. Exception Details.	Critical
Incremental Restore Successful.	Info
Incremental Restore failed. Reason: Exception Details	Critical
On-demand Full Backup failed: Exception Details	Critical
Full Database Backup failed: Exception Details.	Critical
Full Database Purge Backup failed: Exception Details	Critical
Incremental Backup Failed: Exception Details	Critical

Table 12-3 System Alarms in ACS 5.6 (continued)

Alarm	Severity
Log Recovery	
Log Message Recovery failed: Exception Details	Critical
View Compress	
Database rebuild operation has started. The Log collector services would be shut down during this operation and they would be made up after rebuild operation is completed. If log recovery option is enabled already, any log messages that may be received during the rebuild operation would be recovered after log collector services are up.	Critical
The database reload operation completed.	Info
System detects a need to compress the database. Run the view database compress operation manually during maintenance window, otherwise, automatic database rebuild would be triggered to avoid disk space issue.	Warning
Automatic database rebuild operation has started. The Log collector services would be shut down during this operation and they would be made up after rebuild operation is completed. If log recovery option is enabled already, any log messages that may be received during the rebuild operation would be recovered after log collector services are up.	Critical
The database reload operation completed.	Info
Automatic database rebuild operation would be triggered as the size of the database exceeds the limit to avoid disk space issue. Enable log recovery feature to recover missed log messages during database rebuild operation. Database re-build operation will not continue till log recovery feature enabled.	Warning
Threshold Executor	
Could not complete executing all thresholds in the allocated thresholdEvaluationInterval minute interval. Thresholds will be evaluated again in the next interval. This error could have happened because: The system is under heavy load (example: During Purging) There might be too many thresholds active at this time.	Info
Session Monitor	
Active sessions are over limit. Session is over 250000.	Warning
Syslog Collector Failure	
Please see Collector log for details.	Critical
Scheduled ACS Backup	
Scheduled backup of ACS configuration db failed to start due to invalid character in backup name.	Critical
Scheduled backup of ACS configuration db failed to start due to invalid repository. Please verify that repository exists.	Critical
Unable to get hostname. Scheduled backup of ACS configuration db failed. Please check ADE.log for more details.	Critical
Failed to load backup library. Scheduled backup of ACS configuration db failed. Please check ADE.log for more details.	Critical

Table 12-3 System Alarms in ACS 5.6 (continued)

Alarm	Severity
Symbol lookup error. Scheduled backup of ACS configuration db failed. Please check ADE.log for more details.	Critical
Failed to perform ACS backup due to internal error. Please check ADE.log for more details.	Critical
System Diagnostics	
Secondary node stopped from processing replications.	Critical
Secondary node cannot establish communication channel against Primary node on Heartbeat/Replication/Replay topic.	Warning
Primary node cannot establish communication channel against secondary node on Heartbeat/Replication/Replay topic.	Warning
Heartbeat from Primary/Secondary indicates that Secondary is not synchronized with Primary for long time.	Warning
No heartbeat status is received from the secondary node for certain amount of time.	Warning
No heartbeat status is received from the primary node for certain amount of time.	Warning
Disk Size Check	
Backup of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit backup process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical
Patch of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit patch installation process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical
Support bundle of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit support bundle collection process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical
Backup of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit restore process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical
Disk Quota	
ACS DB size has exceeded allowed quota.	Critical
ACS View DB size has exceeded allowed quota.	Critical
View Data Upgrade	
Database conversion has successfully completed. The View newVersion database has been upgraded to installedVersion and is ready for activation.	Warning
Database conversion did not complete successfully. The View newVersion upgrade process encountered errors and was not able to complete. The upgrade log contains detailed information.	Critical
Others	

Table 12-3 System Alarms in ACS 5.6 (continued)

Alarm	Severity
Aggregator is busy. Dropping syslog.	Critical
Collector is busy. Dropping syslog.	Critical
Unregistered ACS Server servername.	Warning
Unknown Message code received.	Critical

Note The Alarm for ACS database exceeding the quota is sent only when the total size of the ACS database exceeds the quota. Total size of ACS database = acs*.log + acs.db where acs*.log is the ACS database log file. Both the acs*.log and acs.db files are present under /opt/CSCOacs/db.

Note ACS cannot be used as a remote syslog server. But, you can use an external server as a syslog server. If you use an external server as a syslog server, no alarms can be generated in the ACS view as the syslog messages are sent to the external syslog server. If you want to generate the alarms in ACS view, set the logging option as localhost using CLI.

To edit an alarm:

Step 1 Select **Monitoring and Reports > Alarms > Inbox**.

The Inbox page appears with a list of alarms that ACS triggered.

Step 2 Check the check box next to the alarm that you want to edit and click **Edit**.

The Inbox - Edit page appears with the following tabs:

- Alarm—This tab provides more information on the event that triggered the alarm. Table 12-4 describes the fields in the Alarm tab. You cannot edit any of the fields in the Alarm tab.

Table 12-4 Inbox - Alarm Tab

Option	Description
Occurred At	Date and time when the alarm was triggered.
Cause	The event that triggered the alarm.
Detail	Additional details about the event that triggered the alarm. ACS usually lists the counts of items that exceeded the specified threshold.
Report Links	Wherever applicable, one or more hyperlinks are provided to the relevant reports that allow you to further investigate the event.
Threshold	Information on the threshold configuration.

- Status—This tab allows you to edit the status of the alarm and add a description to track the event.

Step 3 Modify the fields in the Status tab as required. Table 12-5 describes the fields.

Table 12-5 Inbox - Status Tab

Option	Description
Status	Status of the alarm. When an alarm is generated, its status is New. After you view the alarm, change the status of the alarm to Acknowledged or Closed to indicate the current status of the alarm.
Assigned To	(Optional) Specify the name of the user to whom this alarm is assigned.
Notes	(Optional) Enter any additional information about the alarm that you want to record.

Step 4 Click **Submit** to save the changes.

The Alarms page appears with the changes you made.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Deleting Alarm Thresholds, page 12-36

Understanding Alarm Schedules

You can create alarm schedules to specify when a particular alarm threshold is run. You can create, edit, and delete alarm schedules. You can create alarm schedules to be run at different times of the day during the course of a seven-day week.

By default, ACS comes with the non-stop alarm schedule. This schedule monitors events 24 hours a day, seven days a week.

To view a list of alarm schedules, choose **Monitoring and Reports > Alarms > Schedules**. The Alarm Schedules page appears. Table 12-6 lists the fields in the Alarm Schedules page.

Table 12-6 Alarm Schedules Page

Option	Description
Filter	Enter a search criterion to filter the alarm schedules based on your search criterion.
Go	Click **Go** to begin the search.
Clear Filter	Click **Clear Filter** to clear the search results and list all the alarm schedules.
Name	The name of the alarm schedule.
Description	(Optional) A brief description of the alarm schedule.

This section contains the following topics:

- Creating and Editing Alarm Schedules, page 12-10
- Assigning Alarm Schedules to Thresholds, page 12-10
- Deleting Alarm Schedules, page 12-11

Creating and Editing Alarm Schedules

To create or edit an alarm schedule:

Step 1 Choose **Monitoring and Reports > Alarms > Schedules**.

The Alarm Schedules page appears.

Step 2 Do either of the following:

- Click **Create**.
- Check the check box next to the alarm schedule that you want to edit, then click **Edit**.

The Alarm Schedules - Create or Edit page appears. Table 12-7 lists the fields in the Alarms Schedules - Create or Edit page.

Table 12-7 Alarm Schedules - Create or Edit Page

Option	Description
Identification	
Name	Name of the alarm schedule. The name can be up to 64 characters in length.
Description	A brief description of the alarm schedule; can be up to 255 characters in length.
Schedule	
Click a square to select or deselect that hour. Use the Shift key to select or deselect a block starting from the previous selection. For more information on schedule boxes, see Schedule Boxes, page 5-17.	
Select All	Click **Select All** to create a schedule that monitors for events all through the week, 24 hours a day, 7 days a week.
Clear All	Click **Clear All** to deselect all the selection.
Undo All	When you edit a schedule, click **Undo All** to revert back to the previous schedule.

Step 3 Click **Submit** to save the alarm schedule.

The schedule that you create is added to the Schedule list box in the Threshold pages.

Assigning Alarm Schedules to Thresholds

When you create an alarm threshold, you must assign an alarm schedule for the threshold. To assign an alarm schedule:

Step 1 Choose **Monitoring and Reports > Alarms > Thresholds**.

The Thresholds page appears.

Note This procedure only describes how to assign a schedule to a threshold. For detailed information on how to create, edit, or duplicate a threshold, see Creating, Editing, and Duplicating Alarm Thresholds, page 12-11.

Step 2 Do one of the following.

- Click **Create**.
- Check the check box next to the threshold that you want to edit and click **Edit**.
- Check the check box next to the threshold that you want to duplicate and click **Duplicate**.

Step 3 In the General tab, choose the schedule that you want from the Schedule drop-down list box.

Step 4 Click **Submit** to assign the schedule to the threshold.

Deleting Alarm Schedules

Note Before you delete an alarm schedule, ensure that it is not referenced by any thresholds that are defined in ACS. You cannot delete the default schedule (nonstop) or schedules that are referenced by any thresholds.

To delete an alarm schedule:

Step 1 Choose Monitoring and **Reports > Alarms > Schedules**.

The Alarm Schedules page appears.

Step 2 Check the check box next to the alarm schedule that you want to delete, then click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item(s)?
```

Step 3 Click **Yes** to delete the alarm schedule.

The alarm schedule page appears without the schedule that you deleted.

Creating, Editing, and Duplicating Alarm Thresholds

Use this page to configure thresholds for each alarm category. You can configure up to 100 thresholds.

To configure a threshold for an alarm category:

Step 1 Select **Monitoring and Reports > Alarms > Thresholds**.

The Alarms Thresholds page appears as described in Table 12-8:

Table 12-8 Alarm Thresholds Page

Option	Description
Name	The name of the alarm threshold.
Description	The description of the alarm threshold.

Table 12-8 Alarm Thresholds Page (continued)

Option	Description
Category	The alarm threshold category. Options can be: • Passed Authentications • Failed Authentications • Authentication Inactivity • TACACS Command Accounting • TACACS Command Authorization • ACS Configuration Changes • ACS System Diagnostics • ACS Process Status • ACS System Health • ACS AAA Health • RADIUS Sessions • Unknown NAD • External DB Unavailable • RBACL Drops • NAD-reported AAA Down
Last Modified Time	The time at which the alarm threshold was last modified by a user.
Last Alarm	The time at which the last alarm was generated by the associated alarm threshold.
Alarm Count	The number of times that an associated alarm was generated.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the alarm that you want to duplicate, then click **Duplicate**.
- Click the alarm name that you want to modify, or check the check box next to the alarm that you want to modify, then click **Edit**.
- Check the check box next to the alarm that you want to enable, then click **Enable**.
- Check the check box next to the alarm that you want to disable, then click **Disable**.

Step 3 Modify fields in the Thresholds page as required. See the following pages for information about valid field options:

- Configuring General Threshold Information, page 12-16
- Configuring Threshold Criteria, page 12-17
- Configuring Threshold Notifications, page 12-35

Step 4 Click **Submit** to save your configuration.

The alarm threshold configuration is saved. The Threshold page appears with the new configuration.

Related Topics

- Configuring General Threshold Information, page 12-16
- Configuring Threshold Criteria, page 12-17
- Configuring Threshold Notifications, page 12-35

Alarm Threshold Messages

A general alarm threshold message would include the following:

<month> <date> <time> <acs instance name> <alarm category> <syslog id> <number of fragments> <first fragment> <alarm threshold name = “Value”>, <severity = “value”>, <cause = “value”>, <Detail = “Other details”>.

A sample alarm threshold message is given below:

<178> Apr 2 13:23:00 ACS Server1 0000000005 1 0 ACSVIEW_ALARM Threshold alarm name = “System_Diagnostics”, severity = Warn, cause = “Alarm caused by System_Diagnostics threshold”, detail = “(ACS Instance = ACS Server, Category = CSCOacs_Internal_Operations_Diagnostics, Severity = Warn, Message Text = CTL for syslog server certificate is empty)”

Table 12-9 displays the list of all alarm threshold messages.

Table 12-9 List of Alarm Threshold Messages

Alarm Threshold Category	Alarm Header	Alarm Name	Severity	Cause	Details
Passed Authentication	<month><date><time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 00000001 Number of Fragments: 1 First Fragment: 0	Authentication	Critical/ Warning/ Info	This alarm is raised when the authentication threshold is reached.	User: user1 Passed authentication count: 2
Failed Authentication	<month><date><time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 00000002 Number of Fragments: 1 First Fragment: 0	Authentication	Critical/ Warning/ Info	This alarm is raised when the authentication threshold is reached.	User: user1 Failed authentication count: 2

Table 12-9 List of Alarm Threshold Messages (continued)

Alarm Threshold Category	Alarm Header	Alarm Name	Severity	Cause	Details
Authentication Inactivity	<month><date><time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 000000081 Number of Fragments: 1 First Fragment: 0	Authentication inactivity	Critical/ Warning/ Info	This alarm is raised when the authentication inactivity has occurred.	Following ACS instance(s) did not receive any authentication request between <month> <date> <time> <timezone> <year> and <month> <date> <time> <timezone> <year>: acsserver1
TACACS Command Accounting	<month><date><time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000127 Number of Fragments: 1 First Fragment: 0	TACACS Accounting	Critical/ Warning/ Info	This alarm is caused when the TACACS+ accounting threshold is reached.	ACS instance: acsserver1 Time: <month> <date> <time> <timezone> <year> User: user1 Privilege: 0 Command: CmdAV = show run
TACACS Command Authorization	<month><date><time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000128 Number of Fragments: 1 First Fragment: 0	TACACS Authorization	Critical/ Warning/ Info	This alarm is caused when the TACACS+ authorization threshold is reached.	ACS instance: acsserver1 Time: <month> <date> <time> <timezone> <year> Network Device: device1 User: user1 Privilege: 0 Command: CmdAV = show run Authorization Result: Passed Identity Group: All Groups, Device Group & Device Type: All Device Types Location: All Locations
ACS Configuration Changes	<month><date><time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000002 Number of Fragments: 1 First Fragment: 0	Configuration Changes	Critical/ Warning/ Info	This alarm is caused when the configuration changes threshold is reached.	ACS instance: acsserver1 Time: <month> <date> <time> <timezone> <year> Administrator: acsadmin Object Name: ACSAdmin Object Type: Administrator Account Change: UPDATE

Table 12-9 List of Alarm Threshold Messages (continued)

Alarm Threshold Category	Alarm Header	Alarm Name	Severity	Cause	Details
ACS System Diagnostics	<month><date><time> <acs instance name> Syslog ID: 0000000005 Number of Fragments: 1 First Fragment: 0	System Diagnostics	Critical/ Warning/ Info	This alarm is caused when the system diagnostics threshold is reached.	ACS instance: acsserver1 Category: CSCOacs_Internal_Operations_ Diagnostics Severity: warning Message Text: CTL for Syslog server certificate is empty
ACS Process Status	<month><date><time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000001 Number of Fragments: 1 First Fragment: 0	Authentication	Critical/ Warning/ Info	This alarm is caused when the authentication threshold is reached.	No process status updates have been received since the ACS View may be down.
ACS System Health	<month><date><time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000004 Number of Fragments: 1 First Fragment: 0	Authentication	Critical/ Warning/ Info	This alarm is caused when the authentication threshold is reached.	ACS instance: acsserver1 CPU utilization(%): 0.96 Memory utilization(%): 91.73 Disk space used /opt(%): 14.04 Disk space used /localdisk(%): 8.94
ACS AAA Health	<month><date><time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000003 Number of Fragments: 1 First Fragment: 0	AAA Health	Critical/ Warning/ Info	This alarm is caused when the AAA health threshold is reached.	ACS instance: acsserver1 RADIUS throughput (transactions per second): 0.00
RADIUS Sessions	<month><date><time> <acs instance name> Syslog ID: 0000000003 Number of Fragments: 1 First Fragment: 0	RADIUS Session	Critical/ Warning/ Info	This alarm is caused when the RADIUS sessions threshold is reached.	ACS instance: acsserver1 Device IP: 192.168.1.2 Count: 12

Table 12-9 List of Alarm Threshold Messages (continued)

Alarm Threshold Category	Alarm Header	Alarm Name	Severity	Cause	Details
Unknown NAD	<month><date><time> <acs instance name> Syslog ID: 0000000002 Number of Fragments: 1 First Fragment: 0	Unknown NAD	Critical/ Warning/ Info	This alarm is caused when the unknown NAD threshold is reached.	ACS instance: acsserver1 Unknown NAD count: 12
External Database Unavailable	<month><date><time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000001 Number of Fragments: 1 First Fragment: 0	External database	Critical/ Warning/ Info	This alarm is caused when the external database threshold is reached.	ACS instance: acsserver1 External database unavailable: 6
NAD-reported AAA Down	<month><date><time> <acs instance name> Syslog ID: 0000000004 Number of Fragments: 1 First Fragment: 0	NAD_Reported _AAA_Down	Critical/ Warning/ Info	This alarm is caused when the NAD_Reported _AAA_ Down threshold is reached.	ACS instance: acsserver1 AAA down count: 10

Configuring General Threshold Information

To configure general threshold information, fill out the fields in the General Tab of the Thresholds page. Table 12-10 describes the fields.

Table 12-10 General Tab

Option	Description
Name	Name of the threshold.
Description	(Optional) The description of the threshold.
Enabled	Check this check box to allow this threshold to be executed.
Schedule	Use the drop-down list box to select a schedule during which the threshold should be run. A list of available schedules appears in the list.

Related Topics

- Configuring Threshold Criteria, page 12-17
- Configuring Threshold Notifications, page 12-35

Configuring Threshold Criteria

ACS 5.6 provides the following threshold categories to define different threshold criteria:

Passed Authentications

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ passed authentications that occurred during the time interval that you have specified up to the previous 24 hours.

These authentication records are grouped by a common attribute, such as ACS Instance, User, Identity Group, and so on. The number of records within each of these groups is computed. If the count computed for any of these groups exceeds the specified threshold, an alarm is triggered.

For example, if you configure a threshold with the following criteria: Passed authentications greater than 1000 in the past 20 minutes for an ACS instance. When ACS evaluates this threshold and three ACS instances have processed passed authentications as follows:

ACS Instance	Passed Authentication Count
New York ACS	1543
Chicago ACS	879
Los Angeles	2096

An alarm is triggered because at least one ACS instance has greater than 1000 passed authentications in the past 20 minutes.

Note You can specify one or more filters to limit the passed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the authentication records and only those records whose filter value matches the value that you specify are counted. If you specify multiple filters, only the records that match all the filter conditions are counted.

Modify the fields in the Criteria tab as described in Table 12-11 to create a threshold with the passed authentication criteria.

Table 12-11 Passed Authentications

Option	Description
Passed Authentications	Enter data according to the following: greater than *count* > **occurrences |%>** in the past *time* > *Minutes* | *Hours* for a *object*, where: • *count* values can be the absolute number of occurrences or percent. Valid values are: – *count* must be in the range 0 to 99 for greater than. – *count* must be in the range 1 to 100 for lesser than. • **occurrences | %>** value can be occurrences or %. • *time* values can be 5 to 1440 minutes, or 1 to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be: – ACS Instance – User – Identity Group – Device IP – Identity Store – Access Service – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel In a distributed deployment, if there are two ACS instances, the count is calculated as an absolute number or as a percentage for each of the instances. ACS triggers an alarm only when the individual count of any of the ACS instance exceeds the specified threshold.
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
User	Click **Select** to choose or enter a valid username on which to configure your threshold.
Identity Group	Click **Select** to choose a valid identity group name on which to configure your threshold.
Device Name	Click **Select** to choose a valid device name on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.

Table 12-11 Passed Authentications (continued)

Option	Description
Device Group	Click **Select** to choose a valid device group name on which to configure your threshold.
Identity Store	Click **Select** to choose a valid identity store name on which to configure your threshold.
Access Service	Click **Select** to choose a valid access service name on which to configure your threshold.
MAC Address	Click **Select** to choose or enter a valid MAC address on which to configure your threshold. This filter is available only for RADIUS authentications.
NAD Port	Click **Select** to choose a port for the network device on which to configure your threshold. This filter is available only for RADIUS authentications.
AuthZ Profile	Click **Select** to choose an authorization profile on which to configure your threshold. This filter is available only for RADIUS authentications.
AuthN Method	Click **Select** to choose an authentication method on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP AuthN	Click **Select** to choose an EAP authentication value on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP Tunnel	Click **Select** to choose an EAP tunnel value on which to configure your threshold. This filter is available only for RADIUS authentications.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: • RADIUS • TACACS+

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

Failed Authentications

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ failed authentications that occurred during the time interval that you have specified up to the previous 24 hours. These authentication records are grouped by a common attribute, such as ACS Instance, User, Identity Group, and so on.

The number of records within each of these groups is computed. If the count computed for any of these groups exceeds the specified threshold, an alarm is triggered.

For example, if you configure a threshold with the following criteria: Failed authentications greater than 10 in the past 2 hours for Device IP. When ACS evaluates this threshold, if failed authentications have occurred for four IP addresses in the past two hours as follows:

Device IP	Failed Authentication Count
a.b.c.d	13
e.f.g.h	8

Device IP	Failed Authentication Count
i.j.k.l	1
m.n.o.p	1

An alarm is triggered because at least one Device IP has greater than 10 failed authentications in the past 2 hours.

Note You can specify one or more filters to limit the failed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the authentication records and only those records whose filter value matches the value that you specify are counted. If you specify multiple filters, only the records that match all the filter conditions are counted.

Modify the fields in the Criteria tab as described in Table 12-12 to create a threshold with the failed authentication criteria.

Table 12-12 Failed Authentications

Option	Description
Failed Authentications	Enter data according to the following: greater than *count* > **occurrences | %>** in the past *time*> *Minutes|Hours* for a *object*, where: • *count* values can be the absolute number of occurrences or percent. Valid values must be in the range 0 to 99. • **occurrences | %>** value can be occurrences or %. • *time* values can be 5 to 1440 minutes, or 1 to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be: – ACS Instance – User – Identity Group – Device IP – Identity Store – Access Service – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel In a distributed deployment, if there are two ACS instances, the count is calculated as an absolute number or as a percentage for each of the instances. ACS triggers an alarm only when the individual count of any of the ACS instance exceeds the specified threshold.
Filter	
Failure Reason	Click **Select** to enter a valid failure reason name on which to configure your threshold.

Table 12-12 Failed Authentications (continued)

Option	Description
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
User	Click **Select** to choose or enter a valid username on which to configure your threshold.
Identity Group	Click **Select** to choose a valid identity group name on which to configure your threshold.
Device Name	Click **Select** to choose a valid device name on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click **Select** to choose a valid device group name on which to configure your threshold.
Identity Store	Click **Select** to choose a valid identity store name on which to configure your threshold.
Access Service	Click **Select** to choose a valid access service name on which to configure your threshold.
MAC Address	Click **Select** to choose or enter a valid MAC address on which to configure your threshold. This filter is available only for RADIUS authentications.
NAD Port	Click **Select** to choose a port for the network device on which to configure your threshold. This filter is available only for RADIUS authentications.
AuthZ Profile	Click **Select** to choose an authorization profile on which to configure your threshold. This filter is available only for RADIUS authentications.
AuthN Method	Click **Select** to choose an authentication method on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP AuthN	Click **Select** to choose an EAP authentication value on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP Tunnel	Click **Select** to choose an EAP tunnel value on which to configure your threshold. This filter is available only for RADIUS authentications.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: • RADIUS • TACACS+

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

Authentication Inactivity

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ authentications that occurred during the time interval that you have specified up to the previous 31 days. If no authentications have occurred during the specified time interval, an alarm is triggered.

You can specify filters to generate an alarm if no authentications are seen for a particular ACS instance or device IP address during the specified time interval.

If the time interval that you have specified in the authentication inactivity threshold is lesser than that of the time taken to complete an aggregation job, which is concurrently running, then this alarm is suppressed.

The aggregation job begins at 00:05 hours every day. From 23:50 hours, up until the time the aggregation job completes, the authentication inactivity alarms are suppressed.

For example, if your aggregation job completes at 01:00 hours today, then the authentication inactivity alarms will be suppressed from 23:50 hours until 01:00 hours.

Note If you install ACS between 00:05 hours and 05:00 hours, or if you have shut down your appliance for maintenance at 00:05 hours, then the authentication inactivity alarms are suppressed until 05:00 hours.

Choose this category to define threshold criteria based on authentications that are inactive. Modify the fields in the **Criteria** tab as described in Table 12-13.

Table 12-13 Authentication Inactivity

Option	Description
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
Device	Click **Select** to choose a valid device on which to configure your threshold.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: • RADIUS • TACACS+
Inactive for	Use the drop-down list box to select one of these valid options: • Hours—Specify the number of hours in the range from 1 to 744. • Days—Specify the number of days from 1 to 31.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

TACACS Command Accounting

When ACS evaluates this threshold, it examines the TACACS+ accounting records that it received during the interval between the previous and current alarm evaluation cycle.

If one or more TACACS+ accounting records match, it calculates the time that has elapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines the TACACS+ accounting records received during the interval between the previous and current alarm evaluation cycle. I

If one or more TACACS+ accounting records match a specified command and privilege level, an alarm is triggered.

You can specify one or more filters to limit the accounting records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on TACACS commands. Modify the fields in the **Criteria** tab as described in Table 12-14.

Table 12-14 TACACS Command Accounting

Option	Description
Command	Enter a TACACS command on which you want to configure your threshold.
Privilege	Use the drop-down list box to select the privilege level on which you want to configure your threshold. Valid options are: • Any • A number from 0 to 15.
Filter	
User	Click **Select** to choose or enter a valid username on which to configure your threshold.
Device Name	Click **Select** to choose a valid device name on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click **Select** to choose a valid device group name on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

TACACS Command Authorization

When ACS evaluates this threshold, it examines the TACACS+ accounting records that it received during the interval between the previous and current alarm evaluation cycle.

If one or more TACACS+ accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines the TACACS+ authorization records received during the interval between the previous and current alarm evaluation cycle.

If one or more TACACS+ authorization records match a specified command, privilege level, and passed or failed result, an alarm is triggered.

You can specify one or more filters to limit the authorization records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on TACACS command authorization profile. Modify the fields in the **Criteria** tab as described in Table 12-15.

Table 12-15 TACACS Command Authorization

Option	Description
Command	Enter a TACACS command on which you want to configure your threshold.
Privilege	Use the drop-down list box to select the privilege level on which you want to configure your threshold. Valid options are: • Any • A number from 0 to 15.

Table 12-15 TACACS Command Authorization

Option	Description
Authorization Result	Use the drop-down list box to select the authorization result on which you want to configure your threshold. Valid options are: • Passed • Failed
Filter	
User	Click **Select** to choose or enter a valid username on which to configure your threshold.
Identity Group	Click **Select** to choose a valid identity group name on which to configure your threshold.
Device Name	Click **Select** to choose a valid device name on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click **Select** to choose a valid device group name on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

ACS Configuration Changes

When ACS evaluates this threshold, it examines the accounting records that it received during the interval between the previous and current alarm evaluation cycle.

If one or more accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines the ACS configuration changes made during the interval between the previous and current alarm evaluation cycle. If one or more changes were made, an alarm is triggered.

You can specify one or more filters to limit which configuration changes are considered for threshold evaluation. Each filter is associated with a particular attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on configuration changes made in the ACS instance. Modify the fields in the **Criteria** tab as described in Table 12-16.

Table 12-16 ACS Configuration Changes

Option	Description
Administrator	Click **Select** to choose a valid administrator username on which you want to configure your threshold.
Object Name	Enter the name of the object on which you want to configure your threshold.
Object Type	Click **Select** to choose a valid object type on which you want to configure your threshold.

Table 12-16 ACS Configuration Changes

Option	Description
Change	Use the drop-down list box to select the administrative change on which you want to configure your threshold. Valid options are: • Any • Create—Includes "duplicate" and "edit" administrative actions. • Update • Delete
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

ACS System Diagnostics

When ACS evaluates this threshold, it examines the accounting records that it received during the interval between the previous and current alarm evaluation cycle.

If one or more accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines system diagnostic records generated by the monitored ACS during the interval.

If one or more diagnostics were generated at or above the specified security level, an alarm is triggered. You can specify one or more filters to limit which system diagnostic records are considered for threshold evaluation.

Each filter is associated with a particular attribute in the records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on system diagnostics in the ACS instance. Modify the fields in the **Criteria** tab as described in Table 12-17.

Table 12-17 ACS System Diagnostics

Option	Description
Severity at and above	Use the drop-down list box to choose the severity level on which you want to configure your threshold. This setting captures the indicated severity level and those that are higher within the threshold. Valid options are: • Fatal • Error • Warning • Info • Debug
Message Text	Enter the message text on which you want to configure your threshold. Maximum character limit is 1024.
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

ACS Process Status

When ACS evaluates this threshold, it examines the accounting records that it received during the interval between the previous and current alarm evaluation cycle.

If one or more accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS determines whether any ACS process has failed during that time.

If ACS detects one or more failures, an alarm is triggered. You can limit the check to particular processes or a particular ACS instance or both.

Choose this category to define threshold criteria based on ACS process status. Modify the fields in the **Criteria** tab as described in Table 12-18.

Table 12-18 ACS Process Status

Option	Description
Monitor Processes	
ACS Database	Check the check box to add the ACS database to your threshold configuration.
ACS Management	Check the check box to add the ACS management to your threshold configuration.
ACS Runtime	Check the check box to add the ACS runtime to your threshold configuration.
Monitoring and Reporting Database	Check the check box to have this process monitored. If this process goes down, an alarm is generated.

Table 12-18 ACS Process Status

Option	Description
Monitoring and Reporting Collector	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Monitoring and Reporting Alarm Manager	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Monitoring and Reporting Job Manager	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Monitoring and Reporting Log Processor	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

ACS System Health

When ACS evaluates this threshold, it examines whether any system health parameters have exceeded the specified threshold in the specified time interval up to the previous 60 minutes. These health parameters include percentage of CPU utilization, percentage of memory consumption, and so on.

If any of the parameters exceed the specified threshold, an alarm is triggered. By default, the threshold applies to all ACS instances in your deployment. If you want, you can limit the check to just a single ACS instance.

Choose this category to define threshold criteria based on the system health of ACS. Modify the fields in the **Criteria** tab as described in Table 12-19.

Table 12-19 ACS System Health

Option	Description
Average over the past	Use the drop-down list box to select the amount of time you want to configure for your configuration, where <min> is minutes and can be: • 15 • 30 • 45 • 60
CPU	Enter the percentage of CPU usage you want to set for your threshold configuration. The valid range is from 1 to 100.
Memory	Enter the percentage of memory usage (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.

Table 12-19 ACS System Health

Option	Description
Disk I/O	Enter the percentage of disk usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/opt	Enter the percentage of /opt disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/local disk	Enter the percentage of local disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/	Enter the percentage of the / disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/tmp	Enter the percentage of temporary disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

ACS AAA Health

When ACS evaluates this threshold, it examines whether any ACS health parameters have exceeded the specified threshold in the specified time interval up to the previous 60 minutes. ACS monitors the following parameters:

- RADIUS Throughput
- TACACS Throughput
- RADIUS Latency
- TACACS Latency

If any of the parameters exceed the specified threshold, an alarm is triggered. By default, the threshold applies to all monitored ACS instances in your deployment. If you want, you can limit the check to just a single ACS instance.

Modify the fields in the **Criteria** tab as described in Table 12-20.

Table 12-20 ACS AAA Health

Option	Description
Average over the past	Use the drop-down list box to select the amount of time you want to configure for your configuration, where <min> is minutes and can be: • 15 • 30 • 45 • 60
RADIUS Throughput	Enter the number of RADIUS transactions per second you want to set (lesser than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
TACACS Throughput	Enter the number of TACACS+ transactions per second you want to set (lesser than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
RADIUS Latency	Enter the number in milliseconds you want to set for RADIUS latency (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
TACACS Latency	Enter the number in milliseconds you want to set for TACACS+ latency (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

RADIUS Sessions

When ACS evaluates this threshold, it determines whether any authenticated RADIUS sessions have occurred in the past 15 minutes where an accounting start event has not been received for the session. These events are grouped by device IP address, and if the count of occurrences for any device IP exceeds the specified threshold, an alarm is triggered. You can set a filter to limit the evaluation to a single device IP.

Choose this category to define threshold criteria based on RADIUS sessions. Modify the fields in the **Criteria** tab as described in Table 12-21.

Table 12-21 RADIUS Sessions

Option	Description
More than *num* authenticated sessions in the past 15 minutes, where accounting start event has not been received for a Device IP	*num*—A count of authenticated sessions in the past 15 minutes.
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.

Unknown NAD

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ failed authentications that have occurred during the specified time interval up to the previous 24 hours. From these failed authentications, ACS identifies those with the failure reason Unknown NAD.

The unknown network access device (NAD) authentication records are grouped by a common attribute, such as ACS instance, user, and so on, and a count of the records within each of those groups is computed. If the count of records for any group exceeds the specified threshold, an alarm is triggered. This can happen if, for example, you configure a threshold as follows:

Unknown NAD count greater than 5 in the past 1 hour for a Device IP

If in the past hour, failed authentications with an unknown NAD failure reason have occurred for two different device IP addresses as shown in the following table, an alarm is triggered, because at least one device IP address has a count greater than 5.

Device IP	Count of Unknown NAD Authentication Records
a.b.c.d	6
e.f.g.h	1

You can specify one or more filters to limit the failed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on authentications that have failed because of an unknown NAD. Modify the fields in the **Criteria** tab as described in Table 12-22.

Table 12-22 Unknown NAD

Option	Description
Unknown NAD count	greater than *num* in the past *time Minutes|Hours* for a *object*, where: • *num* values can be any five-digit number greater than or equal to zero (0). • *time* values can be 5 to 1440 minutes, or 1 to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be: – ACS Instance – Device IP
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: • RADIUS • TACACS+

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

External DB Unavailable

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ failed authentications that have occurred during the specified interval up to the previous 24 hours.

From these failed authentications, ACS identifies those with the failure reason, External DB unavailable. Authentication records with this failure reason are grouped by a common attribute, such as ACS instance, user, and so on, and a count of the records within each of those groups is computed.

If the count of records for any group exceeds the specified threshold, an alarm is triggered. This can happen if, for example, you configure a threshold as follows:

External DB Unavailable count greater than 5 in the past one hour for a Device IP

If in the past hour, failed authentications with an External DB Unavailable failure reason have occurred for two different device IP addresses as shown in the following table, an alarm is triggered, because at least one device IP address has a count greater than 5.

Device IP	Count of External DB Unavailable Authentication Records
a.b.c.d	6
e.f.g.h	1

You can specify one or more filters to limit the failed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on an external database that ACS is unable to connect to. Modify the fields in the **Criteria** tab as described in Table 12-23.

Table 12-23 External DB Unavailable

Option	Description
External DB Unavailable	*percent|count* greater than *num* in the past *time Minutes|Hours* for a *object*, where: • Percent|Count value can be Percent or Count. • *num* values can be any one of the following: – 0 to 99 for percent – 0 to 99999 for count • *time* values can be 5 to 1440 minutes, or 1 to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be: – ACS Instance – Identity Store
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
Identity Group	Click **Select** to choose a valid identity group name on which to configure your threshold.
Identity Store	Click **Select** to choose a valid identity store name on which to configure your threshold.
Access Service	Click **Select** to choose a valid access service name on which to configure your threshold.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: • RADIUS • TACACS+

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

RBACL Drops

When ACS evaluates this threshold, it examines Cisco Security Group Access RBACL drops that occurred during the specified interval up to the previous 24 hours. The RBACL drop records are grouped by a particular common attribute, such as NAD, SGT, and so on.

A count of such records within each of those groups is computed. If the count for any group exceeds the specified threshold, an alarm is triggered. For example, consider the following threshold configuration:

RBACL Drops greater than 10 in the past 4 hours by a SGT.

If, in the past four hours, RBACL drops have occurred for two different source group tags as shown in the following table, an alarm is triggered, because at least one SGT has a count greater than 10.

SGT	Count of RBACL Drops
1	17
3	14

You can specify one or more filters to limit the RBACL drop records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the RBACL drop records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Modify the fields in the **Criteria** tab as described in Table 12-24.

Table 12-24 RBACL Drops

Option	Description
RBACL drops	greater than *num* in the past *time Minutes|Hours* by a *object*, where: • *num* values can be any five-digit number greater than or equal to zero (0). • *time* values can be 5 to 1440 minutes, or 1 to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be: – NAD – SGT – DGT – DST_IP
Filter	
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
SGT	Click **Select** to choose or enter a valid source group tag on which to configure your threshold.
DGT	Click **Select** to choose or enter a valid destination group tag on which to configure your threshold.
Destination IP	Click **Select** to choose or enter a valid destination IP address on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

NAD-Reported AAA Downtime

When ACS evaluates this threshold, it examines the NAD-reported AAA down events that occurred during the specified interval up to the previous 24 hours. The AAA down records are grouped by a particular common attribute, such as device IP address or device group, and a count of records within each of those groups is computed.

If the count for any group exceeds the specified threshold, an alarm is triggered. For example, consider the following threshold configuration:

AAA Down count greater than 10 in the past 4 hours by a Device IP

If, in the past four hours, NAD-reported AAA down events have occurred for three different device IP addresses as shown in the following table, an alarm is triggered, because at least one device IP address has a count greater than 10.

Device IP	Count of NAD-Reported AAA Down Events
a.b.c.d	15
e.f.g.h	3
i.j.k.l	9

You can specify one or more filters to limit the AAA down records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the AAA down records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on the AAA downtime that a network access device reports. Modify the fields in the **Criteria** tab as described in Table 12-25.

Table 12-25 NAD-Reported AAA Downtime

Option	Description
AAA down	greater than *num* in the past *time Minutes|Hours* by a *object*, where: • *num* values can be any five-digit number greater than or equal to zero (0). • *time* values can be 5 to 1440 minutes, or 1to 24 hours. • Minutes|Hours value can be Minutes or Hours. • *object* values can be: – Device IP – Device Group

Table 12-25 NAD-Reported AAA Downtime

Option	Description
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click **Select** to choose a valid device group name on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Configuring General Threshold Information, page 12-16
- Configuring Threshold Notifications, page 12-35

Configuring Threshold Notifications

Use this page to configure alarm threshold notifications.

Step 1 Select **Monitoring and Reports > Alarms > Thresholds**, then do one of the following:

- Click **Create** to create a new alarm threshold.
- Click the name of an alarm threshold, or check the check box next to an existing alarm threshold and click **Edit** to edit a selected alarm threshold.
- Click the name of an alarm threshold, or check the check box next to an existing alarm threshold and click **Duplicate** to duplicate a selected alarm threshold.

Step 2 Click the **Notifications** tab.

The Thresholds: Notifications page appears as described in Table 12-26:

Table 12-26 Thresholds: Notifications Page

Option	Description
Severity	Use the drop-down list box to select the severity level for your alarm threshold. Valid options are: • Critical • Warning • Info
Send Duplicate Notifications	Check the check box to be notified of duplicate alarms. An alarm is considered a duplicate if a previously generated alarm for the same threshold occurred within the time window specified for the current alarm.

Table 12-26 Thresholds: Notifications Page (continued)

Option	Description
Email Notification	
Email Notification User List	Enter a comma-separated list of e-mail addresses or ACS administrator names or both. Do one of the following: • Enter the e-mail addresses. • Click **Select** to enter valid ACS administrator names. The associated administrator is notified by e-mail only if there is an e-mail identification specified in the administrator configuration. See Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-7 for more information. When a threshold alarm occurs, an e-mail is sent to all the recipients in the Email Notification User List. Click **Clear** to clear this field.
Email in HTML Format	Check this check box to send e-mail notifications in HTML format. Uncheck this check box to send e-mail notifications as plain text.
Custom Text	Enter custom text messages that you want associated with your alarm threshold.
Syslog Notification	
Send Syslog Message	Check this check box to send a syslog message for each system alarm that ACS generates. **Note** For ACS to send syslog messages successfully, you must configure Alarm Syslog Targets, which are syslog message destinations. Understanding Alarm Syslog Targets, page 12-38 for more information.

Related Topics

- Viewing and Editing Alarms in Your Inbox, page 12-3
- Creating, Editing, and Duplicating Alarm Thresholds, page 12-11
- Deleting Alarm Thresholds, page 12-36

Deleting Alarm Thresholds

To delete an alarm threshold:

Step 1 Select **Monitoring and Reports > Alarms > Thresholds**.

The Alarms Thresholds page appears.

Step 2 Check one or more check boxes next to the thresholds you want to delete, and click **Delete**.

Step 3 Click **OK** to confirm that you want to delete the selected alarm(s).

The Alarms Thresholds page appears without the deleted threshold.

Configuring System Alarm Settings

System alarms are used to notify users of:

- Errors that are encountered by the Monitoring and Reporting services
- Information on data purging

Use this page to enable system alarms and to specify where alarm notifications are sent. When you enable system alarms, they are sent to the Alarms Inbox. In addition, you can choose to send alarm notifications through e-mail to select recipients and as syslog messages to the destinations specified as alarm syslog targets.

From the Monitoring and Report Viewer, choose **Monitoring Configuration > System Configuration > System Alarm Settings**.

Table 12-27 System Alarm Settings Page

Option	Description
System Alarm Settings	
Notify System Alarms	Check this check box to enable system alarm notification.
System Alarms Suppress Duplicates	Use the drop-down list box to designate the number of hours that you want to suppress duplicate system alarms from being sent to the Email Notification User List. Valid options are 1, 2, 4, 6, 8, 12, and 24.
Email Notification	
Email Notification User List	Enter a comma-separated list of e-mail addresses or ACS administrator names or both. Do one of the following: • Enter the e-mail addresses. • Click **Select** to enter valid ACS administrator names. The associated administrator is notified by e-mail only if there is an e-mail identification specified in the administrator configuration. See Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-7 for more information. When a system alarm occurs, an e-mail is sent to all the recipients in the Email Notification User List. Click **Clear** to clear this field.
Email in HTML Format	Check this check box to send e-mail notifications in HTML format. Uncheck this check box to send e-mail notifications as plain text.
Syslog Notification	
Send Syslog Message	Check this check box to send a syslog message for each system alarm that ACS generates. For ACS to send syslog messages successfully, you must configure Alarm Syslog Targets, which are syslog message destinations. Understanding Alarm Syslog Targets, page 12-38 for more information.

This section contains the following topics:

Understanding Alarm Syslog Targets

Alarm syslog targets are the destinations where alarm syslog messages are sent. The Monitoring and Report Viewer sends alarm notification in the form of syslog messages. You must configure a machine that runs a syslog server to receive these syslog messages.

To view a list of configured alarm syslog targets, choose **Monitoring Configuration > System Configuration > Alarm Syslog Targets**.

Note You can configure a maximum of two syslog targets in the Monitoring and Report Viewer.

This section contains the following topics:

Creating and Editing Alarm Syslog Targets

To create or edit an alarm syslog target:

Step 1 Choose **Monitoring Configuration > System Configuration > Alarm Syslog Targets**.

The Alarm Syslog Targets page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the alarm syslog target that you want to edit, then click **Edit**.

The Alarm Syslog Targets Create or Edit page appears.

Step 3 Modify the fields described in Table 12-28.

Table 12-28 Alarm Syslog Targets Create or Edit Page

Option	Description
Identification	
Name	Name of the alarm syslog target. The name can be 255 characters in length.
Description	(Optional) A brief description of the alarm that you want to create. The description can be up to 255 characters in length.
Configuration	
IP Address	IP address of the machine that receives the syslog message. This machine must have the syslog server running on it. We recommend that you use a Windows or a Linux machine to receive syslog messages.

Table 12-28 Alarm Syslog Targets Create or Edit Page

Option	Description
Use Advanced Syslog Options	
Port	Port in which the remote syslog server listens. By default, it is set to 514. Valid options are from 1 to 65535.
Facility Code	Syslog facility code to be used for logging. Valid options are Local0 through Local7.

Step 4 Click **Submit**.

Related Topics

- Understanding Alarm Syslog Targets, page 12-38
- Deleting Alarm Syslog Targets, page 12-39

Deleting Alarm Syslog Targets

Note You cannot delete the default *nonstop* schedule.

To delete an alarm syslog target:

Step 1 Choose **Monitoring Configuration > System Configuration > Alarm Syslog Targets**.

The Alarm Syslog Targets page appears.

Step 2 Check the check box next to the alarm syslog target that you want to delete, then click **Delete**.

The following message appears:

```
Do you want to delete the selected item(s)?
```

Step 3 Click **Yes**.

The Alarm Syslog Targets page appears without the deleted alarm syslog targets.