



Managing Reports

The reports in Cisco Secure ACS, Release 5.8.1 are enhanced to have a new look and feel that is more simple and easy to use. The reports are grouped in to logical categories to provide information related to authentication, session traffic, device administration, ACS server configuration and administration, and troubleshooting. The enhanced dynamic export option allows you to export the selected reports to an excel spreadsheet as a comma-separated values (.csv) file. The enhanced scheduling service allows you to queue reports and receive notification when the reports are available.

ACS 5.8.1 uses the flex based web interface to display reports. The new reports web interface in ACS 5.8.1 generates the RADIUS and TACACS+ reports three to four times faster (on an average) than ACS 5.5 reports. The report names and their filters are displayed on the left-hand side and the reports are displayed on the right-hand side of the Reports web interface. The enhanced web interface help you to navigate through the reports easily and to have a better control over different types of reports from left-pane, than going to the right-pane and make selection. ACS 5.8.1 does not support the Interactive Viewer feature as a whole; however, the “show or hide columns” and “fixing columns” (constituents of Interactive Viewer feature) are supported. You can export the report to a comma separated values file, open the file using Microsoft Excel Spreadsheet or using any other supported tool, and use the excel options to perform the operation.

The Monitoring and Reports drawer appears in the ACS web interface and contains the Launch Monitoring and Report Viewer option. Click **Launch Monitoring and Report Viewer** to open the Monitoring and Reports Viewer in a new window, which contains the following drawers:

- Monitoring and Reports
- Monitoring Configuration. (See [15, page 15-1.](#))

The Monitoring and Reports drawer on the web interface contains the Reports option. Click **Reports** to open the Reports Viewer in a new window.

You can run reports from Reports Web interface from any of the following pages:

- Favorites—**Reports > Favorites**
- ACS Reports—**Reports > ACS Reports > <report_type>**
- Saved and Scheduled Reports—**Reports > Saved and Scheduled Reports**

The reports that reside in these pages can be:

- System reports—Preconfigured with the ACS software; you can view the list of system reports in the **Reports > ACS Reports** pages.
- Customized reports—System reports that you have configured and saved.

For easy access, you can add reports to your Favorites page, from where you can customize and run reports. You can customize the reports and save them to access them frequently and run the customized reports. The saved reports are displayed under the Saved and Scheduled Reports drawer. The ACS

Reports provide a rich set of reports on log, diagnostic, and troubleshooting data retrieved from the ACS servers in your deployment. You can view these reports as tables, graphs, or charts and drill down further for more granular data.

Further, ACS allows you to:

- Filter the data in your report based on your requirements
- Add the reports periodically or on demand to a comma separated values file and print it
- Add the report to your list of favorites, from where you can access them frequently
- Customize a report and save it.

This chapter covers the following topics:

- [ACS Reports, page 13-2](#)
- [Running Reports, page 13-3](#)
- [Reports Navigation, page 13-3](#)
- [Exporting Reports, page 13-8](#)
- [Saving and Scheduling Reports, page 13-9](#)
- [Favorite Reports, page 13-14](#)
- [Available Reports, page 13-15](#)
- [Available Filters, page 13-20](#)
- [Changing Authorization for RADIUS Active Sessions Dynamically, page 13-22](#)
- [Understanding Charts, page 13-25](#)

ACS Reports

The Monitoring and Reports Viewer offers you a powerful dashboard that you can use to monitor the health of all ACS servers in your deployment. The dashboard also provides information on network access patterns and trends in traffic that you can use to administer your network efficiently. The Monitoring and Report Viewer provides you real-time data and vital statistics that help you proactively manage your network and prevent any attacks.

The Monitoring and Report Viewer component of Cisco Secure ACS collects log and configuration data from various ACS servers in your deployment, aggregates it, and provides interactive reports that help you analyze the data. It also provides you integrated monitoring, reporting, and troubleshooting capabilities to efficiently manage your network and troubleshoot network-related problems.

ACS comes with a set of predefined reports that you can run to obtain meaningful information from the log and configuration data obtained from ACS servers. [Table 13-2](#) lists the reports that are available in ACS under various categories. The report names and its filters and displayed in the left-pane. You can add or remove filters and run a report. The generated report appears on the right-pane.

Related Topics

- [Running Reports, page 13-3](#)
- [Reports Navigation, page 13-3](#)
- [Available Reports, page 13-15](#)
- [Available Filters, page 13-20](#)
- [Saving and Scheduling Reports, page 13-9](#)

Running Reports

This section describes how to run reports using reports view:

-
- Step 1** Choose **Monitoring and Reports > Reports > ACS Reports**.
- Step 2** Click a report from the report categories available.
- Step 3** Select one or more filters to run a report. Each report has different filters available that are case sensitive, of which some are mandatory and some are optional. See [Table 13-3](#) for list of available filters.
- You can add or remove filters from the **Filters** drop-down list:
- To add filters, select the required filters from the **Filters** drop-down list. You can find a green color tick mark appears near the filter name after you select it.
 - To remove filters, deselect the filters from the **Filters** drop-down list. The green color tick mark disappears after you deselect the filter name.
- Step 4** Click **OK**.
- Step 5** Enter an appropriate value for the filters.
- Step 6** Click **Run**.
- ACS displays the generated report on the right pane.
-

**Note**

ACS displays a maximum of 250 pages per report with 100 records per page for RADIUS and TACACS+ AAA reports. For other reports, ACS displays a maximum of 50 pages per report with 100 records per page.

**Note**

When you click a link from the reports on Reports web interface, ACS opens that link in a new window. In ACS, the aggregation happens at 00:05 hrs every day and the cross launches from ACS reports details page display only the reports that are aggregated before the aggregation time. The logs that are generated after aggregation are not displayed until the next aggregation is complete. This limitation is applicable only for the cross launches in the reports details web interface. However, the Reports web interface displays all the reports irrespective of the aggregation time.

Related Topics

- [Exporting Reports, page 13-8](#)
- [Saving Reports, page 13-9](#)
- [Favorite Reports, page 13-14](#)
- [Scheduling Reports, page 13-12](#)

Reports Navigation

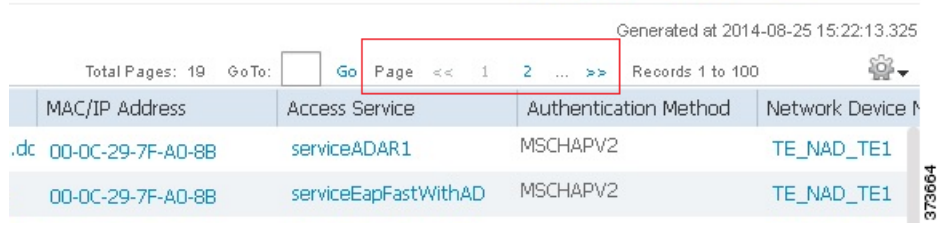
You can get detailed information from the reports output. For example, if you have generated a report for a period of five months, the graph and table will list the aggregate data for the report in a scale of months.

You can click a particular value from the table to see another report related to this particular field. For example, an authentication summary report will display the failed count for the user or user group. When you click the failed count, an authentication summary report is opened for that particular failed count.

When you run a report in the Reports Viewer, you see the first page data. To view or work with data, you use tools that help you navigate the report.

In the Reports Viewer, you can navigate through a report by using the paging tool as displayed in [Figure 13-1](#). Using this tool, you can click an arrow to view the next and previous page in the report.

Figure 13-1 Paging Tool



Generated at 2014-08-25 15:22:13.325

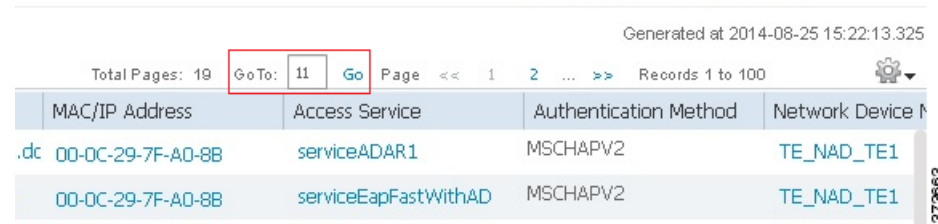
Total Pages: 19 Go To: Go Page << 1 2 ... >> Records 1 to 100

MAC/IP Address	Access Service	Authentication Method	Network Device M
.dc 00-0C-29-7F-A0-8B	serviceADAR1	MSCHAPV2	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithAD	MSCHAPV2	TE_NAD_TE1

373664

The viewer also supports going to a specific page by typing a page number in **Go To** as displayed in [Figure 13-2](#), and click **Go** the field.

Figure 13-2 Going to a Specific Page



Generated at 2014-08-25 15:22:13.325

Total Pages: 19 Go To: Go Page << 1 2 ... >> Records 1 to 100

MAC/IP Address	Access Service	Authentication Method	Network Device M
.dc 00-0C-29-7F-A0-8B	serviceADAR1	MSCHAPV2	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithAD	MSCHAPV2	TE_NAD_TE1

373663

The viewer displays the total number of pages and the current page as displayed in [Figure 13-3](#), and click **Go** the field.

Figure 13-3 Total Pages



Generated at 2014-08-25 15:22:13.325

Total Pages: 19 Go To: Go Page << 1 2 ... >> Records 1 to 100

MAC/IP Address	Access Service	Authentication Method	Network Device M
.dc 00-0C-29-7F-A0-8B	serviceADAR1	MSCHAPV2	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithAD	MSCHAPV2	TE_NAD_TE1

373666

For every reports that are displayed on the reports viewer, you can add, remove, or fix columns from the list using the column settings option available just above the reports header on the right-hand side as displayed in [Figure 13-4](#).

Figure 13-4 Report Settings

Generated at 2014-08-25 15:22:13.325

Total Pages: 19 Go To: Go Page << 1 2 ... >> Records 1 to 100 

MAC/IP Address	Access Service	Authentication Method	Network Device M
.dc 00-0C-29-7F-A0-8B	serviceADAR1	MSCHAPV2	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithAD	MSCHAPV2	TE_NAD_TE1

373665

You change the order in which the reports header appear in the reports table. To change the reports header order, you need to drag the column and drop it in the place required.

Related Topics

- [Show or Hide Columns in Reports Table, page 13-5](#)
- [Fixing Columns in Reports Table, page 13-6](#)

Show or Hide Columns in Reports Table

Reports Viewer provides an option to show a column from the available list or hide an existing column in the reports table using the column settings feature. You can click on the column settings icon to see the available list of column names. If you find a green color tick mark near a column name as displayed in [Figure 13-5](#), that means the column name is selected and the selected column names appear in the reports table. The column names that does not have a tick mark near them are not selected; thus it will not appear in the reports table. You can show or hide multiple columns together.

To show or hide columns in reports table.

-
- Step 1** Choose **Monitoring and Reports > Reports > ACS Reports > report_type**.
- Step 2** Run a report, as described in [Running Reports, page 13-3](#).
- Step 3** Click the arrow the settings icon.
- Step 4** Click **Columns**.
- Step 5** Do one of the following:
- To show a column, select the column name from the drop-down list. A green color tick mark appears near the column name after you select it.
 - To hide a column, deselect the column name from the drop-down list. The green color tick mark disappears after you deselect the column name.
- Step 6** Click **Close**.
-



Note

You can click **Reset** to change the configuration to its default settings.

Figure 13-5 Show or Hide Columns

The screenshot shows a table with the following data:

MAC/IP Address	Access Service
00-0C-29-7F-A0-8B	serviceADAR1
00-0C-29-7F-A0-8B	serviceEapFastWithA
00-0C-29-7F-A0-8B	serviceEapFastWithA
00-0C-29-7F-A0-8B	serviceEapFastWithA
00-0C-29-7F-A0-8B	serviceEapFastWithA
00-0C-29-7F-A0-8B	serviceEapFastWithA
00-0C-29-7F-A0-8B	serviceEapFastWithA
00-0C-29-7F-A0-8B	serviceEapFastWithA
00-0C-29-7F-A0-8B	serviceEapFastWithA
00-0C-29-7F-A0-8B	serviceADAR1

The settings menu is open, showing a list of columns with green checkmarks indicating they are fixed:

- ACSVIEW Timestamp
- ACS Timestamp
- RADIUS Status
- NAS Failure
- Details
- User Name
- MAC/IP Address
- Access Service
- Authentication Met...
- Network Device Name
- NAS IP Address
- NAS Port Id
- CTC Security Group

The menu also includes a 'Fix Columns' section with the following items:

- TE_NAD_TE1
- TE_NAD_TE1
- TE_NAD_TE1
- TE_NAD_TE1
- TE_NAD_TE1
- TE_NAD_TE1
- TE_NAD_TE1
- TE_NAD_TE1
- TE_NAD_TE1
- TE_NAD_TE1
- SimRadius

Buttons for 'Close' and 'Reset' are visible at the bottom of the menu.

Fixing Columns in Reports Table

Reports Viewer provides an option to fix the reports header so that you cannot move that column inside the table as displayed in Figure 13-6. To fix columns in reports table.

- Step 1** Choose **Monitoring and Reports > Reports > ACS Reports > report_type**.
- Step 2** Run a report, as described in [Running Reports, page 13-3](#).
- Step 3** Click the arrow the settings icon.
- Step 4** Click **Fix Columns**.
- Step 5** Do one of the following:
 - To fix a column, select the column name from the drop-down list. A green color tick mark appears near the column name after you select it.
 - To remove a fixed column, deselect the column name from the drop-down list. The green color tick mark disappears after you deselect the column name.
- Step 6** Click **Close**.



Note

You can click **Reset** to change the configuration to its default settings.

Figure 13-6 Fixing Columns

Generated at 2014-08-25 15:22:13.325

Total Pages: 19 GoTo: Go Page << 1 2 ... >> Records 1 to 100

MAC/IP Address	Access Service	Authentication Method	Columns
00-0C-29-7F-A0-8B	serviceADAR1	ACSView Timestamp	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	ACS Timestamp	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	RADIUS Status	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	NAS Failure	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	Details	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	User Name	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	MAC/IP Address	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	Access Service	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	Authentication Met...	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	Network Device Name	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	NAS IP Address	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	NAS Port Id	TE_NAD_TE1
	serviceADAR1	CTC Security Group	SimRadius
	serviceEapFastWithA		SimRadius
	serviceEapFastWithAD	PAP_ASCII	SimRadius

Sorting Data in Reports Table

ACS 5.8.1 allows the user to sort data in the reports table based on the entries in the column either in ascending or descending order. You can click a column title once to sort the complete reports table based on the selected column entries in ascending order. You can find an upward-pointing arrow to the right of the column title indicating that the column entries are sorted in ascending order. You can click on a column title again to sort the table based on the selected column entries in descending order. You can find a downward-pointing arrow to the right of the column title indicating that the column entries are sorted in descending order.

Filtering Data in Reports Table

ACS 5.8.1 allows the user to filter the data entries in reports table column-wise. ACS 5.8.1 uses the “contains” parameter to filter the data. The reports table has either a drop-down list or a text box each column heading except a few columns to which the filtering is not applicable. Click the drop-down list to view the available filtering options. You have to select the entry or multiple entries from the drop down list or enter the text in the text box to filter table entries.

To Filter reports table based on column entries:

-
- Step 1** Choose **Monitoring and Reports > Reports > ACS Reports > report_type**.
 - Step 2** Run a report, as described in [Running Reports, page 13-3](#).
 - Step 3** Perform one of the following actions:
 - Click the drop-down arrow near the column heading to view the list of available filter values which has a check box to the left of each value. Check the check box near the filters. You can select multiple check boxes.

- If a column has a text box, then enter the filter text in the text box.

Step 4 Click **OK**.

The reports table is now filtered based on the selected column entries.

Exporting Reports

In ACS 5.8.1, you can export report data to an excel spreadsheet as a comma-separated values (.csv) file. Previous releases of ACS allowed you to export reports and copy the comma separated value file to the local file system. You need to copy the exported file using the **copy** command to a remote location. But in ACS 5.8.1, you have the option to configure the remote repository to which the exported reports are stored. After you export the data, you will receive an email detailing the location of the report. You can track the status of the records in the scheduler page.



Note

To receive an email notification for the exported reports, you need to configure the email server details on the Email Settings page. See [Specifying E Mail Settings, page 15-16](#) to configure email server details. You will not receive any email if you did not configure the email server details from Email Settings page.

Step 1 Select **Monitoring and Reports > Reports > ACS Reports > report_type >**, where *report_type* is the type of report.

The available reports for the report type you selected are displayed.

Step 2 Run a report, as described in [Running Reports, page 13-3](#).

Step 3 Click **Export**.

Step 4 Choose a repository from the drop-down list.

You cannot export the following reports:

- Authentication Summary
- Health Summary
- All Security Group Access reports except RBACL Drop Summary report
- Endpoint reports
- Network Device Session Status



Note

When you export an ACS Administrator Entitlement Summary Report to a remote repository, ACS 5.6 exports the two columns “Administrator” and “Roles” from the reports table to a comma separated values file (csv). But, ACS 5.8.1 exports the additional column “Resources and Privileges” along with the Administrator and Roles columns.

If you configure a new repository when you are generating reports from the reports web interface, the newly configured repository will not be available for exporting the generated reports. You need to close the reports web interface and open it again to view the newly configured repository to export the generated reports.

**Note**

To view the non-English characters correctly after exporting a report, you must import the file into Microsoft Excel by enabling UTF-8 character encoding. If you choose to open the exported .csv file directly in Microsoft Excel without enabling UTF-8 character encoding, the non-English characters in the report appear in some garbage form.

**Note**

When you use Microsoft Excel to view the exported records, you should be aware of the worksheet size limitations. In Microsoft Excel 2007 and 2010, the maximum limit for a worksheet size is 1,048,576 rows by 16,384 columns. For more information, see: <http://office.microsoft.com/en-us/excel-help/excel-specifications-and-limits-HP010342495.aspx>.

Saving and Scheduling Reports

In ACS 5.8.1, you can save or schedule reports from the new Reports web interface. The Saved and Scheduled Reports section of the Reports web interface has the following options:

- [Saved Reports, page 13-9](#)
- [Scheduled Reports, page 13-11](#)

Saved Reports

This section contains the following topics:

- [Saving Reports, page 13-9](#)
- [Editing Saved Reports, page 13-10](#)
- [Deleting Saved Reports, page 13-10](#)

Saving Reports

You can customize a report and save the changes as a new report. The saved reports are displayed under Saved and Scheduled reports section of Reports web interface.

- Step 1** Run a report as described in [Running Reports, page 13-3](#).
- Step 2** Click **Save As** in the top right-hand corner of the report summary page.
- Step 3** Choose **Report**.
- Step 4** Enter the **Name** and **Description** in the dialog box.
- Step 5** Click **Save**.

The report is now saved along with the selected filter values.

**Note**

You can edit the report name and description of the saved reports. To edit the report name and description of the saved reports, select the report that you want to edit and click **Edit Setting**.

Editing Saved Reports

You can customize a report and save that as a new report in Saved reports page. The saved reports appear with the customized filters. You can add new filters or remove the existing filters, edit them, and save that as a new report. You can customize a saved report and save that report as a new report using the **Save As New** option.

-
- Step 1** Choose **Monitoring and Reports > Reports > Saved and Scheduled Reports > Saved Reports**.
- Step 2** Select the report that you want to edit.
- Step 3** The selected saved reports appear with the existing filters.
- Step 4** You can add or remove filters from the **Filters** drop-down list:
- To add filters, select the required filters from the **Filters** drop-down list. You can find a green color tick mark near the selected filters.
 - To remove filters, deselect the filters from the **Filters** drop-down list. The green color tick mark disappears after you deselect it.
- Step 5** Click **OK**.
Selected filters appears under the saved reports with its default values.
- Step 6** Enter the required details for the selected filters and click **Run**.
- Step 7** Click **Save As** in the top right-hand corner of the report summary page.
- Step 8** Choose **Report**.
- Step 9** Enter the **Name** and **Description** in the dialog box.
- Step 10** Click **Save** to save the report or **Save As New** to save this report as a new report.
- If you click **Save**, ACS overrides the existing customization and save this report.
 - If you click **Save As New**, ACS do not override the existing customization. The edited report is now saved as a new report with the name specified.
-

Deleting Saved Reports

To delete a report from the Saved Reports page:

-
- Step 1** Choose **Monitoring and Reports > Reports > Saved and Scheduled Reports > Saved Reports**.
- Step 2** Select the report that you want to delete, and click **Delete**.
- Step 3** Click **OK** to confirm that you want to delete the selected saved report.
The Saved Report is now deleted.
-

Related Topics

[Saving Reports, page 13-9](#)

Scheduled Reports

In ACS 5.8.1, you can schedule reports for a future date in such a way that ACS automatically generates the report. This can be done using the scheduled reports feature available in the Saved and Scheduled Reports drawer of Reports web interface.

In ACS 5.5, this feature is available only for the RADIUS authentication, RADIUS accounting, TACACS+ authentication, TACACS+ authorization, and TACACS+ accounting reports. But in ACS 5.8.1, this feature is available for all the ACS Reports other than a few reports listed below.

You cannot schedule the following reports in ACS 5.8.1:

- ACS Health Summary
- ACS Instance Authentication Summary
- Top N Authentication by ACS Instance
- AAA Down Summary
- Top N AAA Down By Network Device
- RBACL Drop Summary
- RADIUS Active Sessions
- RADIUS Session History
- RADIUS Terminated Sessions
- TACACS Active Sessions
- TACACS Session History
- TACACS Terminated Sessions

In ACS 5.8.1, you have the option to configure the remote repository to which the generated reports are exported and stored. ACS generates the scheduled reports based on the given time range, exports them to a comma separated values file, and stores them in the specified remote repository.

An email notification is sent whenever a scheduled report is generated successfully. To receive a email notification for the scheduled reports, you need to configure the email server details on the Email Settings page. See [Specifying E Mail Settings, page 15-16](#) to configure email server details. The email notification contains the following information:

- File Name—Name of the generated report file. The format of the filename is RptExp_<admin_name>_<scheduledreport_name>_<generated_on>_<randomnumber>.csv. For instance, if the name of the scheduled report is “report1”, then the filename is displayed as: RptExp_acsadmin_report1_2014-08-05_14-00-00.000000182.csv.
- Repository Name—Name of the remote repository where the generated reports are stored.
- Generated on—The date and time at which the report is generated.

ACS does not generate any alarms or email notifications if a scheduled report generation fails. To know the status of the scheduled reports, go to the **Monitoring Configuration > System Operations > Scheduler** page and check for the status.

This section contains the following topics:

- [Scheduling Reports, page 13-12](#)
- [Deleting Scheduled Reports, page 13-13](#)

**Note**

When you upgrade from ACS 5.5 to 5.8.1, the existing Scheduled Reports in ACS 5.5 will be displayed under **Saved and Scheduled Reports > Scheduled Reports** Page in ACS 5.8.1.

Scheduling Reports

To schedule ACS reports:

- Step 1** Choose **Monitoring and Reports > Reports > Saved and Scheduled Reports > Scheduled Reports**.
- Step 2** Run the report as described in [Running Reports, page 13-3](#).
- Step 3** Click **Save As** in the top right-hand corner of the report summary page.
- Step 4** Choose **Scheduled Report**.

The Scheduled Reports properties page appears. Complete the fields in the Scheduled Reports page as described [Table 13-1](#).

Table 13-1 *Scheduled Reports Properties Page*

Option	Description
Identification	
Name	(Required) Name of the scheduled report.
Description	(Optional) A brief description of the scheduled report.
Repository	(Required) Select a remote repository from the drop-down list to export and store in it. You need to configure the remote repositories using the ACS CLI interface or the ACS web interface.
Send Email Notification	(Required) Enter the email address to which an email notification or alarm should be sent upon successful generation of the scheduled report. You can add multiple email addresses separating them with a comma. You will not receive an email for the scheduled reports if you do not configure the email server details on the Email Settings page. To configure email server details, see Specifying E Mail Settings, page 15-16 .
Schedule	
Frequency	(Required) Select the frequency of the scheduled report from the drop-down list. The available frequencies are One Time, hourly, daily, weekly, and monthly. <ul style="list-style-type: none"> • One Time—ACS generates the report only once based on the schedule. • Hourly—ACS generates the report on an hourly basis for the specified time period. • Daily—ACS generates the report every day at the specified time. • Weekly—ACS generates the report on the specified day or days of every week. You must configure the day or days in the Day option. • Monthly—ACS generates the report on the specified day or days of every month. You must configure the day or days in Day option. • Yearly—ACS generates the report on the specified day of the selected month. You must configure the day, month, and time.

Table 13-1 Scheduled Reports Properties Page (continued)

Option	Description
At Time	(Required) Select the hour and minutes of the day at which the report should be triggered. The time ranges between 12:00 AM and 11:30 PM. For example, if you select 6:30 AM, the report is generated at 6:30 a.m. for the specified time period.
Every	(Optional) Select the hour (<i>n</i>) of the day from the drop-down list to run the report for every <i>n</i> hour on that day between the configured time interval. In addition, select the time range from the drop-down list for which you want ACS to generate the report between <i>x</i> and <i>y</i> hours. For example, if you select 3 hours and run between 8 AM and 5 PM, then the report runs for every three hours between 8 AM and 5 PM. This option appears only when you select the frequency as hourly.
Month	(Optional) Select the month on which you want to run your report. This option appears only when you select the frequency as Monthly.
On Day	(Optional) Check the check boxes the days or select the day from the drop-down list on which to generate the reports. This option over rules the Frequency sometimes. For example, if you select the frequency as daily and select the days Monday, Tuesday, and Thursday; the reports are generated only for the selected days and not daily. When you set the frequency as hourly, daily, or weekly, this option displays the check boxes from Monday to Sunday. You need to check the appropriate check box or boxes the days. When you set the frequency as monthly or yearly, this option displays the a drop-down list that ranging from day 1 through 31 and last day. You need to select day from the drop-down list. For example, if you select 5 from the drop-down list, the reports run on 5th day of every month.
Start Date	(Optional) Click the icon the Start Date field to select a date from when you want ACS to start generating the scheduled reports. The date format is YYYY/MM/DD.
End Date	(Optional) Click the icon the End Date field to select a date on which you want ACS to stop generating the scheduled reports. The date format is YYYY/MM/DD.

Step 5 Click **Save**.

The scheduled report is saved.

Deleting Scheduled Reports

To delete a report from the Scheduled Reports page:

Step 1 Choose **Monitoring and Reports > Reports > Saved and Scheduled Reports > Scheduled Reports**.

Step 2 Select the report that you want to delete, and click **Delete**.

Step 3 Click **OK** to confirm that you want to delete the selected report.

The Scheduled Report is now deleted.

Favorite Reports

You can add reports that you most frequently use to your Favorites page so that you do not have to navigate each time to get to your favorite report. In ACS 5.5, you can customize the catalog reports (ACS reports in ACS 5.8.1) and add them to favorite reports along with the customized parameters so that you can run the customized report from favorite reports section next time. But in ACS 5.8.1, the favorite reports provide the same functionality of ACS reports.

When you upgrade from ACS 5.5, 5.6, or 5.7 to 5.8.1, the existing favorite reports in ACS 5.5, 5.6, or 5.7 will be displayed under Saved reports section in ACS 5.8.1. The favorite reports section in ACS 5.8.1 displays the following default favorite reports:

- ACS Configuration Audit
- ACS System Diagnostics
- RADIUS Authentication
- TACACS Authentication

This section contains the following topics:

- [Adding Favorite Reports, page 13-14](#)
- [Deleting Reports from Favorites, page 13-14](#)

Adding Favorite Reports

You can add preconfigured system reports to your favorites list, as well as reports that you have customized. You can add reports that you use frequently to a list of favorites to make them easier to find, similar to how you bookmark favorite websites in a browser. You can view and edit the parameters of your favorite reports, and then save the customized reports for reuse.

To add a report to your Favorites page:

Step 1 Select **Monitoring and Reports > Reports > ACS Reports > *report_type* >**, where *report_type* is the type of report.

The available reports for the report type you selected are displayed.

Step 2 Run a report, as described in [Running Reports, page 13-3](#).

Step 3 Click **Favorite in the top right-hand corner of the report summary page**.

The report appears in your Favorites list.

Deleting Reports from Favorites

To delete a report from the Favorites page:

Step 1 Select **Monitoring and Reports > Reports > Favorites**.

Step 2 Select the report that you want to delete from favorites, and click **Unfavorite** in the top right-hand corner of the report summary page.

The selected report disappears from the Favorites section.



Note

Favorite Reports in ACS may disappear from the Reports web interface after every database purge activity. This issue occurs when the report is created by an external identity store user. At the time of database purge activity, ACS verifies the internal user database to check if the user who created the favorite reports is available in the internal identity store users list. If the user is not available in the internal identity store user list, ACS deletes that report from the Reports web interface. The workaround for this issue is to create a local ACS administrator with the same name as the external identity store user, so that the favorite reports will not be deleted after every database purge activity.



Note

When you delete a system report from the Favorites page, the system report is not displayed in the favorites page. The system report will not be deleted from the **ACS Reports** section.



Note

The shared reports that were created in ACS 5.5, 5.6, or 5.7 are deleted after you upgrade to ACS 5.8.1.

Available Reports

[Table 13-2](#) lists the preconfigured reports, grouped according to their category. Descriptions of the report functionality and logging category are also provided. These reports are available when you select Monitoring and Reports, launch Monitoring and Report Viewer, and then select **Monitoring and Reports > Reports > ACS Reports**.

Table 13-2 Available Reports

Report Name	Description	Logging Category
AAA Protocol		
AAA diagnostics	Provides AAA diagnostic details based on severity for a selected time period.	Policy diagnostics, identity stores diagnostics, authentication flow diagnostics, RADIUS diagnostics, TACACS+ diagnostics
Authentication Trend	Provides RADIUS and TACACS+ authentication summary information for a selected time period; along with a graphical representation.	Passed authentications, failed attempts
RADIUS Accounting	Provides user accounting information based on RADIUS for a selected time period.	RADIUS accounting
RADIUS Authentication	Provides RADIUS authentication details for a selected time period.	Passed authentications, failed attempts
TACACS Accounting	Provides user or command accounting information for TACACS+ authentications for a selected time period.	TACACS+ accounting
TACACS Authentication	Provides TACACS+ authentication details for a selected time period.	Passed authentications, failed attempts

Table 13-2 Available Reports (continued)

Report Name	Description	Logging Category
TACACS Authorization	Provides TACACS+ authorization details for a selected time period.	Passed authentications, failed attempts
Access Service		
Access Service Authentication Summary	Provides RADIUS and TACACS+ authentication summary information for a particular access service for a selected time period; along with a graphical representation.	Passed authentications, failed attempts
Top N Authentications By Access Service	Provides the top N passed, failed, and total authentication count for RADIUS and TACACS+ authentications with respect to the access service for a selected time period.	Passed authentications, failed attempts
ACS Instance		
ACS Administrator Entitlement	Shows the role of the administrator in ACS and the: <ul style="list-style-type: none"> • Tasks in ACS that the administrator is entitled to access • Privileges that the administrator has for each of those operations 	None
ACS Administrator Logins	Provides access-related events for administrators that includes login, logout, events, and reasons for failed login attempts.	Administrative and operational audit
ACS Configuration Audit	Provides all the configuration changes done in ACS by the administrator for a selected time period.	Administrative and operational audit
ACS Health Summary	Provides the CPU, memory utilization, RADIUS and TACACS+ latency and throughput (in tabular and graphical formats). It also gives process status, process downtime, and disk space utilization for a particular ACS instance in a selected time period.	System statistics
ACS Instance Authentication Summary	Provides RADIUS and TACACS+ authentication summary information for a particular ACS instance for a selected time period; along with a graphical representation. This report could take several minutes to run depending on the number of records in the database. When you reload this report, if rate of incoming syslog messages is around 150 messages per second or more, the total number of passed and failed authentications that appear above the graph and the passed and failed authentication count that is displayed in the table do not match.	Passed authentications, failed attempts
ACS Log Information	Provides ACS log information for a particular log category and ACS server for a selected time period.	All log categories

Table 13-2 Available Reports (continued)

Report Name	Description	Logging Category
ACS Operations Audit	Provides all the operational changes done in ACS by the administrator for a selected time period.	Administrative and operational audit
ACS System Diagnostics	Provides system diagnostic details based on severity for a selected time period.	Internal Operations Diagnostics, distributed management, administrator authentication and authorization
Top N Authentication by ACS Instance	Provides the top N passed, failed, and total authentication count for RADIUS and TACACS+ protocol with respect to a particular ACS instance for a selected time period.	Passed authentications, failed attempts
User Change Password Audit	Provides the username of the internal user, identity store name, name of the ACS instance, and time when the user password was changed. Helps to keep track of all changes made to internal user passwords across all ACS interfaces.	Administrative and operational audit
AD Connector Operations	Provides background operations performed by AD connector, such as ACS server password refresh, Kerberos ticket management, DNS queries, DC discovery, LDAP, and RPC connections management. If you encounter any Active Directory failures, you can review the details in this report to identify the possible causes.	
Endpoint		
Endpoint MAC Authentication Summary	Provides the RADIUS authentication summary information for a particular MAC or MAB for a selected time period; along with a graphical representation.	Passed authentications, failed attempts
Top N Authentications By Endpoint MAC Address	Provides the top N passed, failed, and total authentication count for RADIUS protocol with respect to MAC or MAB address for a selected time period.	Passed authentications, failed attempts
Top N Authentications By Machine	Provides the top N passed, failed, and total authentication count for RADIUS protocol with respect to machine information for a selected time period.	Passed authentications, failed attempts
Failure Reason		
Authentication Failure Code Lookup	Provides the description and the appropriate resolution steps for a particular failure reason.	N/A
Failure Reason Authentication Summary	Provides the RADIUS and TACACS+ authentication summary information for a particular failure reason; along with a graphical representation for a selected time period.	Failed attempts
Top N Authentications By Failure Reason	Provides the top N failed authentication count for RADIUS and TACACS+ protocols with respect to Failure Reason for a selected time period.	Failed attempts

Table 13-2 Available Reports (continued)

Report Name	Description	Logging Category
Network Device		
AAA Down Summary	Provides the number of AAA unreachable events that a NAD logs within a selected time period.	N/A
Network Device Authentication Summary	Provides the RADIUS and TACACS+ authentication summary information for a particular network device for a selected time period, along with the graphical representation.	Passed authentications, failed attempts
Network Device Log Messages	Provides you the log information of a particular network device, for a specified time period.	N/A
Session Status Summary	Provides the port sessions and status of a particular network device obtained by SNMP. This report uses either the community string provided in the report or the community string configured in the web interface Monitoring And Reports -> Launch Monitoring And Report Viewer -> Monitoring Configuration -> SNMP Settings .	N/A
Top N AAA Down By Network Device	Provides the number of AAA down events encountered by each of the network devices.	N/A
Top N Authentications by Network Device	Provides the top N passed, failed, and total authentication count for RADIUS and TACACS+ protocols with respect to network device for a selected time period.	Passed authentications, failed attempts
Security Group Access		
RBACL Drop Summary	Provides a summary of RBACL drop events for a selected time period.	N/A
SGT Assignment Summary	Provides a summary of SGT assignments for a selected time period.	Passed authentications
Top N RBACL Drops By Destination	Provides the top N RBACL drop event count with respect to destination for a selected time period.	N/A
Top N RBACL Drops By User	Provides the top N RBACL drop event count with respect to the user for a selected time period.	N/A
Top N SGT Assignments	Provides the top N SGT assignment count for a selected time period.	Passed authentications
Session Directory		

Table 13-2 Available Reports (continued)

Report Name	Description	Logging Category
RADIUS Active Sessions	Provides information on RADIUS authenticated, authorized, and started sessions. RADIUS Active Sessions report allows you to dynamically control active RADIUS sessions. With this feature, you can send a reauthenticate or disconnect request to a NAD to: <ul style="list-style-type: none"> • Reauthenticate the user • Terminate the session • Terminate the session and restart the port • Terminate the session and shut down the port 	Passed authentications, RADIUS accounting
RADIUS Session History	Provides a summary of RADIUS session history, such as total authenticated, active, and terminated sessions and total and average session duration and throughput for a selected time period.	Passed authentications, RADIUS accounting
RADIUS Terminated Sessions	Provides all the RADIUS terminated session information for a selected time period.	Passed authentications, RADIUS accounting
TACACS Active Sessions	Provides information on TACACS+ active sessions.	TACACS+ accounting
TACACS Session History	Provides TACACS+ session history summary, such as total active and terminated sessions and total and average session duration and throughput for a selected time period.	TACACS+ accounting
TACACS Terminated Sessions	Provides TACACS terminated session details for a selected time period.	TACACS+ accounting
User		
Top N Authentications By User	Provides top N passed, failed, and total authentication count for RADIUS and TACACS+ protocol with respect to users for a selected time period.	Passed authentications, failed attempts
User Authentication Summary	Provides RADIUS and TACACS+ authentication summary information for a particular user for a selected time period; along with the graphical representation.	Passed authentications, failed attempts

**Note**

ACS 5.8.1 displays a detailed audit reports on ACS configuration audit reports page for creating, editing, or re-ordering access service policies from the ACS web interface.

**Note**

ACS displays the current day report for the summary reports having hyperlinks. To generate report for an older date or a time range, you must run a manual report for the user.

Available Filters

ACS 5.8.1 provides you an option to select the filter values from the available values for all the filters. You have to enter the first three letters of the filter values in the filter fields. ACS displays the available values after entering the first three letters.



Note

Not all options listed in [Table 13-3](#) are used in selecting data for all reports.

Table 13-3 Available Filters

Option	Description
User	Enter a valid username on which to configure your threshold.
MAC Address	Enter a valid MAC address on which to run your report.
Identity Group	Enter a valid identity group name on which to run your report.
Device Name	Enter a valid device name on which to run your report.
Device IP	Enter a valid device IP address on which to run your report.
SNMP Community	Configure SNMP preferences to authenticate access to MIB objects. For more information, see Configuring SNMP Preferences, page 15-19 . This community string is used by ACS to query information using SNMP on AAA client, and cannot be used by SNMP manager to query MIB information on ACS.
Device Group	Enter a valid device group name on which to run your report.
Access Service	Enter a valid access service name on which to run your report.
Identity Store	Enter a valid identity store name on which to run your report.
ACS Instance	Enter an valid ACS instance name on which to run your report.
Failure Reason	Enter a valid failure reason name on which to run your report.
Protocol	Use the drop down list box to select which protocol on which you want to run your report. Valid options are: <ul style="list-style-type: none"> • RADIUS • TACACS+
Authentication Status	Use the drop down list box to select which authentication status on which you want to run your report. Valid options are: <ul style="list-style-type: none"> • Pass Or Fail • Pass • Fail
Radius Audit Session ID	Enter the RADIUS audit session identification name on which you want to run a report.
ACS Session ID	Enter the ACS session identification name on which you want to run a report.

Table 13-3 Available Filters (continued)

Option	Description
Severity	Use the drop down list box to select the severity level on which you want to run a report. This setting captures the indicated severity level and those that are higher within the threshold. Valid options are: <ul style="list-style-type: none"> • Fatal • Error • Warning • Info • Debug
End Point IP Address	Enter the end point IP address on which you want to run a report.
Command Accounting Only	Check the check box to enable your report to run for command accounting.
Top	Use the drop down list box to select the number of top (most frequent) authentications by access service on which you want to run your report. Valid options are: <ul style="list-style-type: none"> • 10 • 50 • 100 • 500 • 1000 • 5000
By	Use the drop down list box to select the type of authentications on which you want to run your report. Valid options are: <ul style="list-style-type: none"> • Passed Authentications • Failed Authentications • Total Authentications
Administrator Name	Enter the administrator username for which you want to run your report.
Object Type	Enter a valid object type on which you want to run your report.
Object Name	Enter the name of the object on which you want to run your report.
Authorization Status	Use the drop down list box to select which authentication status on which you want to run your report. Valid options are: <ul style="list-style-type: none"> • Pass Or Fail • Pass • Fail

Table 13-3 Available Filters (continued)

Option	Description
Time Range	<p>Use the drop down list box to select the time range on which you want to run your report. Valid options are:</p> <ul style="list-style-type: none"> • Last 30 Minutes (for AAA Protocol reports and ACS Health Summary report only) • Last Hour (for AAA Protocol reports and ACS Health Summary report only) • Last 12 Hours (for AAA Protocol reports and ACS Health Summary report only) • Today • Yesterday • Last 7 Days • Last 30 Days • Custom—You must configure a Start Date and End Date, or a Day. <p>Note Some options are not valid for some Time Range entries of the various reports.</p>
Start Date	Enter a date, or click the date selector icon to enter the start date for which you want run your report.
End Date	Enter a date, or click the date selector icon to enter the end date for which you want run your report.
Start Time	Enter the start time you want to run the report.
End Time	Enter the end time you want to run the report.
Day	Enter a date, or click the date selector icon to enter the end date for which you want run your report.
Run	Click to run the report for which you have made selections.

Related Topics

- [ACS Reports, page 13-2](#)
- [Favorite Reports, page 13-14](#)
- [Available Reports, page 13-15](#)
- [Running Reports, page 13-3](#)

Changing Authorization for RADIUS Active Sessions Dynamically

ACS provides the Dynamic Change of Authorization (CoA) feature through a new report, the RADIUS Active Sessions report, which allows you to dynamically control active RADIUS sessions. With this feature, you can send a reauthenticate or disconnect request to a NAD to:

- Troubleshoot issues related to authentication—You can use the Disconnect:None option to follow up with an attempt to reauthenticate again.
You must not use the disconnect option to restrict access. To restrict access, use the shutdown option.
- Block a problematic host—You can use the Disconnect:Port Disable option to block an infected host that sends a lot of traffic over the network.

The RADIUS protocol currently does not support a method for re-enabling a port that is shut down.

- Force endpoints to reacquire IP addresses—You can use the Disconnect:Port Bounce option for endpoints that do not have a supplicant or client to generate a DHCP request after VLAN change.
- Push an updated authorization policy to an endpoint—You can use the Re-Auth option to enforce an updated policy configuration, such as a change in the authorization policy on existing sessions based on the administrator’s discretion.

For example, if posture validation is enabled, when an endpoint gains access initially, it is usually quarantined. After the endpoint’s identity and posture are known, it is possible to send the CoA Re-Auth command to the endpoint for the endpoint to acquire the actual authorization policy based on its posture.

Legacy NAS devices do not support the CoA feature. Cisco plans to support CoA in all its devices as part of the NPF program.



Note

For the CoA commands to be understood correctly by the device, it is important that you configure the options appropriately.

For the CoA feature to work properly, you must configure in ACS the shared secret of each and every device for which you want to dynamically change the authorization. ACS uses the shared secret configuration, both for requesting access from the device and for issuing CoA commands to it.

This section contains the following topics:

- [Enabling RADIUS CoA Options on a Device, page 13-23](#)
- [Changing Authorization and Disconnecting Active RADIUS Sessions, page 13-24](#)

Enabling RADIUS CoA Options on a Device

To view all the RADIUS Active Session reports you have to enable RADIUS CoA options on the device.

To configure the RADIUS CoA options:

Step 1 Configure MAB, 802.1X and Web Authentication on the NAD against ACS RADIUS Server.

Step 2 Configure CoA on the NAD as follows, which is connected to the supplicant.

```
aa server radius dynamic-author
client {<ip_addr> - <name>} [vrf <vrfname>] [server-key<string>]
server-key [0 - 7] <string>
port <port-num>
auth-type {any - all - session-key}
ignore session-key
ignore server-key
```

Step 3 Configure the authentication order.

Changing Authorization and Disconnecting Active RADIUS Sessions



Note

Some of the NADs in your deployment do not send an Accounting Stop or Accounting Off packet after a reload. As a result of this, you might find two sessions in the Session Directory reports, one of which has expired. Hence, when you want to dynamically change the authorization of an active RADIUS session or disconnect an active RADIUS session, ensure that you always choose the most recent session.

To change authorization or disconnect an active RADIUS session:

- Step 1** Run the RADIUS Active Sessions report under Session Directory.
See [Running Reports, page 13-3](#) for information on how to run a RADIUS Active Sessions report. A report similar to the one shown in [Table 13-3](#) appears.

Figure 13-7 RADIUS Active Session Report

Initiated	Updated	Dur	Packets In	Packets Out	User Name	Radius User Name	CTS Security Group	Framed IP	Session	CoA	ACS Server	Audit Session	Acct Session Id	Calling Station ID	NA
2014-09-04 1	2014-09-0	88	0	0	testuser	testuser			Started		acs68		123	1.1.1.4	10
2014-09-04 1	2014-09-0	128	0	0	sarathi	sarathi			Started		acs68		123	1.1.1.4	10
2014-09-04 1	2014-09-0	132	0	0	sarathi	sarathi			Authenticated		acs68			1.1.1.4	10
2014-09-04 1	2014-09-0	169	0	0	sarathi	sarathi			Authenticated		acs68			1.1.1.4	10

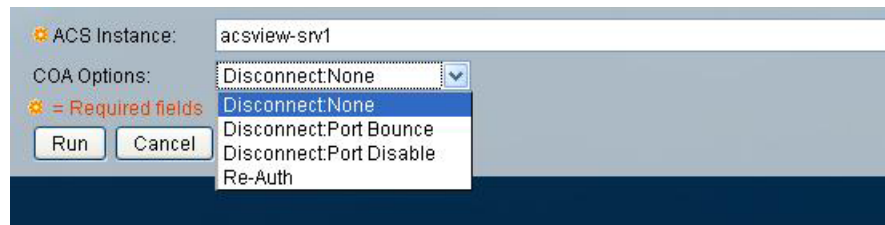
- Step 2** Click the CoA link from the RADIUS session that you want to reauthenticate or terminate.
The Change of Authorization Request page appears.

- Step 3** Select a CoA option from the CoA option drop-down list box shown in [Figure 13-8](#).

Valid options are:

- Disconnect:None—Do not terminate the session.
- Disconnect:Port Bounce—Terminate the session and restart the port.
- Disconnect:Port Disable—Terminate the session and shut down the port.
- Re-Auth—Reauthenticate the user.

Figure 13-8 CoA Options



Step 4 Click **Run** to reauthenticate or disconnect the RADIUS session.

If your change of authorization fails, it might be because of any of the following reasons:

- Device does not support CoA
- Changes to the identity or authorization policy
- Shared secret mismatch

Step 5 See the [Troubleshooting RADIUS Authentications, page 14-6](#) to troubleshoot a failed change of authorization attempt.

A failed dynamic CoA will be listed under failed RADIUS authentications.

Understanding Charts

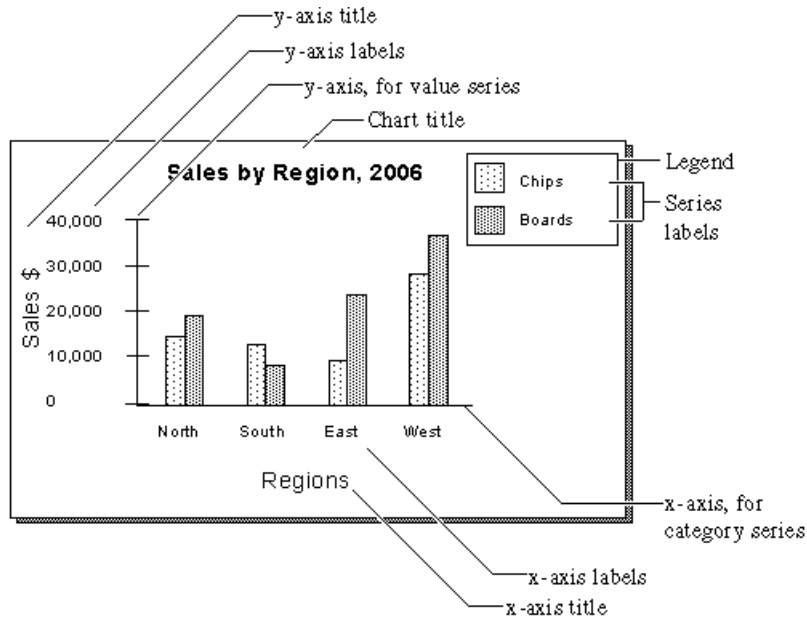
A chart is a graphical representation of data or the relationships among data sets. Charts display complex data in an easy-to-assimilate format. In ACS 5.8.1, you cannot customize the charts from Reports web interface.

[Figure 13-9](#) shows the parts of a basic bar chart. A chart displays data as one or more sets of points. The chart organizes data points into sets of values called series. The two types of series are:

- Category series—The category series typically determines what text, numbers, or dates you see on the x-axis.
- Value series—The value series typically determines the text, numbers, or dates on the y-axis.

In [Figure 13-9](#), the category series contains a set of regions, and the value series contains a set of sales figure values.

Figure 13-9 *Parts of a Basic Bar Chart*



There are a variety of chart types. Some types of data are best depicted with a specific type of chart. Charts can be used as reports in themselves and they can be used together with tabular data report styles.

204474