



Cisco Insight Reporter User Guide

Release 4.0.0

Cisco Systems, Inc.

www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

Following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of following measures:

Turn the television or radio antenna until the interference stops.

Move the equipment to one side or the other of the television or radio.

Move the equipment farther away from the television or radio.

Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED AS IS WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco Ironport, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Insight Reporter v4.0.0 User Guide

Copyright © 2013 Cisco Systems, Inc.

All rights reserved.



Introduction	i
Document Revision History	i
Audience	ii
Organization	ii
Related Documentation	iii
Document Conventions	iii
Obtaining Documentation and Submitting a Service Request	iv

CHAPTER 1. General Overview 1-1

1.1 Introduction	1-1
1.2 About Cisco Insight Reporter	1-1
1.3 Features Overview	1-3
1.3.1. Deployment Scenarios	1-3
1.3.2. Authentication and Authorization	1-6
1.3.3. Look and Feel	1-6
1.3.4. SCE Terminology	1-6
1.3.5. Favorite Reports	1-6
1.3.6. Scheduled Reports	1-6
1.3.7. Report Presentation Configuration	1-6
1.3.8. Search Tool	1-7
1.3.9. Context Sensitive Help	1-7
1.4 Features	1-8
1.4.1 Settings Management	1-8
1.4.2 Network Topology	1-9
1.4.3 Account Management	1-9
1.4.4 Report Wizard	1-9
1.4.5 Application Monitoring	1-10

CHAPTER 2. Connecting to Cisco Insight Reporter 2-1

2.1 Login	2-2
2.1.1 Welcome Screen	2-3
2.1.2 Dashboard	2-5
2.1.3 Module Launcher	2-5

2.1.4	Windows Controls and Main Menu	2-7
2.2	Logout	2-8

CHAPTER 3. Settings Management 3-1

3.1	Introduction	3-1
3.2	Global Settings	3-2
3.2.1	Advanced Settings	3-2
3.2.2	Local Database	3-3
3.2.3	SMTP	3-5
3.2.4	Logging	3-6
3.2.5	Localization	3-7
3.3	Traffic Database Configuration	3-8
3.3.1	Configure a new Traffic Database	3-8
3.3.2	Edit a Traffic Database	3-11
3.3.3	Delete an existing Traffic Database	3-13
3.4	Device Configuration	3-14
3.4.1	Configure a new SCE Device	3-16
3.4.2	Edit an existing Device	3-17
3.4.3	Delete an existing Device	3-18
3.5	Configuring AAA Server for Authentication	3-19
3.5.1	Configure a new Server	3-20
3.5.2	Delete an existing Server	3-21
3.5.3	Edit an existing server	3-22

CHAPTER 4. Network Wizard 4-1

4.1	Introduction	4-1
4.2	Defining a Network	4-2
4.2.1	Configure a New Network	4-2
4.2.2	Edit an existing Network	4-3
4.2.3	Delete an existing Network	4-4
4.3	Managing Network Devices	4-5
4.3.1	Setting the Master Device	4-5
4.4	Defining Device Topology	4-7
4.4.1	View by Device Type	4-7
4.4.2	View by Custom Device Group	4-8
4.5	Defining Service Hierarchy	4-11

- 4.5.1 Service Families 4-11
- 4.5.2 Custom Service View 4-12
- 4.6 Managing Report Filters 4-14
- 4.7 Assigning Custom Colors 4-16
- 4.8 Monitoring Traffic Thresholds 4-17

CHAPTER 5. Account Management 5-1

- 5.1 Introduction 5-1
- 5.2 Defining a Role 5-2
- 5.3 Defining Account Groups 5-6
- 5.4 Defining Visibility Rights 5-11
- 5.5 Defining an Account 5-16
- 5.6 Viewing Capabilities 5-21
- 5.7 Editing the Personal Profile 5-22

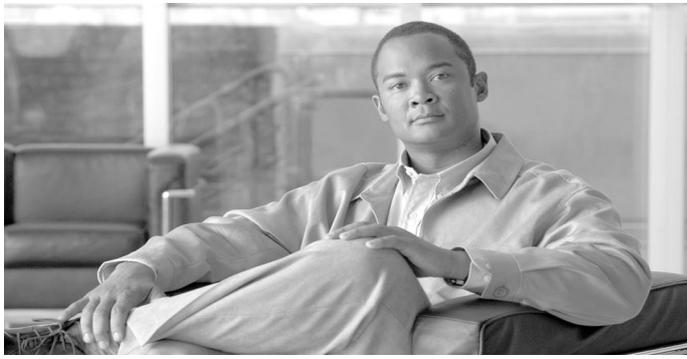
CHAPTER 6. Reporting 6-1

- 6.1 Introduction 6-1
- 6.2 Report Template 6-1
 - 6.2.1 Traffic Monitoring 6-2
 - 6.2.2 Video 6-25
 - 6.2.3 VoIP 6-28
 - 6.2.4 Web 6-33
 - 6.2.5 P2P Group 6-35
 - 6.2.6 Mobile 6-36
 - 6.2.7 Malicious Traffic 6-42
 - 6.2.8 Traffic Discovery Reports 6-45
- 6.3 Running Reports 6-49
 - 6.3.1 Network 6-50
 - 6.3.2 Topic 6-51
 - 6.3.3 Date and Time 6-52
 - 6.3.4 Topology 6-53
 - 6.3.5 Services 6-54
 - 6.3.6 View 6-55
 - 6.3.7 Parameters 6-56
 - 6.3.8 Protocols 6-58
- 6.4 Running an Interactive Report 6-60

6.4.1	Chart	6-61	
6.4.2	Legend for Series displayed in Chart	6-63	
6.4.3	Leading Input	6-63	
6.4.4	Time Controller	6-64	
6.4.5	Report Toolbar	6-65	
6.4.6	Save to Dashboard	6-67	
6.4.7	Scheduling a Report	6-68	
6.4.8	Saving a Report	6-69	
6.4.9	Exporting Report Output	6-69	
6.5	Mapping with Database Tables	6-69	
6.6	My Favorites	6-79	
6.6.1	Reports	6-79	
6.6.2	Thematic Dashboards	6-83	
6.7	Report Gallery	6-85	
6.7.1	Publish a Report Output	6-85	
6.7.2	Remember a Report	6-87	
6.7.3	Merging Reports	6-88	
6.8	Scheduled Reports	6-89	
6.8.1	Delete a Scheduled Report	6-90	
6.8.2	Edit a Scheduled Report	6-91	

CHAPTER 7. Monitoring 7-1

7.1	Introduction	7-1	
7.2	Performance	7-1	
7.3	Logging	7-2	



About this Guide

Introduction

This preface describes who should read the *Cisco Insight Reporter v4.0.0 User Guide*, how it is organized, its document conventions, and how to obtain documentation and technical assistance.

This chapter includes the following sections:

- Document Revision History
- Audience
- Organization
- Related Documentation
- Conventions
- Obtaining Documentation and Submitting a Service Request



Note

This document assumes a basic familiarity with the concept of Service Control Application (SCA), Service Control Engine (SCE) platforms, Collection Manager, Subscriber Manager (SM), and Broadband Console (BB Console).

Document Revision History

Cisco Service Center Release	Part Number	Publication Date
Release 4.0.0	OL-29184-01	Jun 24 2012

Audience

This software is a web reporting solution for Business Intelligence DPI (Deep Packet Inspection) deployments based on the Cisco Service Control Engine (SCE).



Note

Insight Reporter 4.0.0 supports SCE deployments running SCOS up to version 4.0.0 and is backward compatible with earlier releases.

The *Cisco Insight Reporter v4.0.0 User Guide* is addressed to:

- Administrators responsible for the platform installation, provisioning, and daily maintenance.
- End-user operators such as people from marketing or engineering divisions of the service providers, Data Centers, and Enterprise customers.

Organization

The *Cisco Insight Reporter v4.0.0 User Guide* is categorized into following chapters:

Table 1. Document Organization

Chapter	Title	Description
1	General Overview	Provides a brief overview of this application and the application modules with the terms and concepts used in this document.
2	Connecting to Cisco Insight Reporter	Provides instructions to launch this application and describes its various components.
3	Settings Management	Describes the application parameters and system logging.
4	Network Wizard	Provides information about the configuration of the network topology and the modality to configure the network objects and visibility rights.
5	Account Management	Describes how to configure the roles, accounts, account groups, and their visibility rights.
6	Reporting	Describes the reporting parameters and a step by step procedure to run a report.
7	Monitoring	Describes the tracking abilities of the application and provides information to debug all situations in which the report generation fails.

 Note	Means <i>reader take note</i> .
 Tip	Means <i>the following information will help you solve a problem</i> .
 Caution	Means <i>reader be careful</i> . In this situation, you might perform an action that could result in equipment damage or loss of data.
 Timesaver	Means <i>the described action saves time</i> . You can save time by performing the action described in the paragraph.
 Warning	Means <i>reader be warned</i> . In this situation, you might perform an action that could result in bodily injury

Related Documentation

For additional information about how to install and set up the Cisco Insight Reporter application, please refer to *Cisco Insight Reporter v3.3 Installation Guide*.

Document Conventions

The document follows following conventions:

Table 2. Conventions

Convention	Indication
bold font	Commands, keywords, and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{ x y z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A non-quoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to the desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.



CHAPTER 1. General Overview

1.1 Introduction

This chapter provides a general overview of this software. It introduces the product concept, key features, and reporting capabilities.

This chapter contains following sections:

- About Cisco Insight Reporter v4.0.0
- Features Overview

1.2 About Cisco Insight Reporter

Cisco Insight Reporter is a software platform based on web 2.0 user experience standards, designed to collect and present reports, charts, and statistics about the traffic data collected by Cisco SCE devices. It extends the existing features of its former releases v2.x and v3.x as web reporting platform for the Cisco Service Control Application for Broadband.

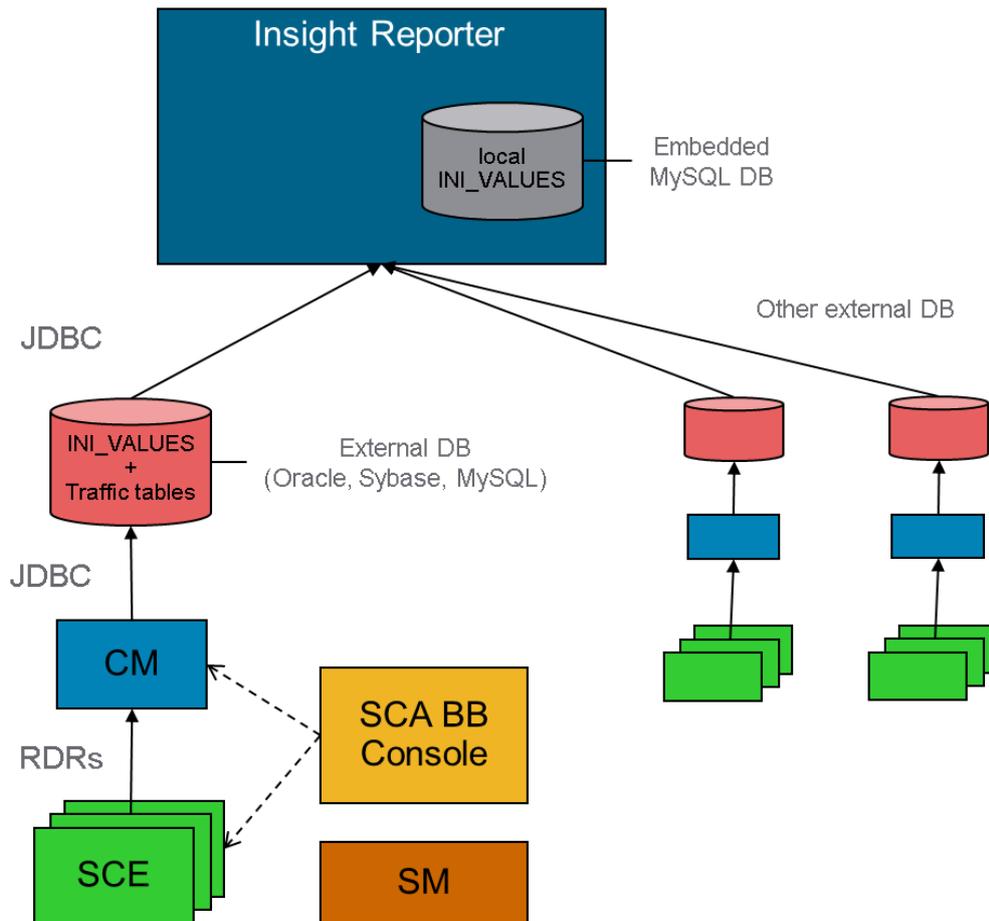
This software is 100% compatible with the existing report templates developed for SCA BB releases 3.5.0 to 4.0.0.

Here is a quick summary of the main features:

- Appealing and easy-to-use user interface, that gives the best experience in terms of usability and computer graphics.
- Supports multi-vendor databases (MySQL, Oracle, and Sybase).
- Scalable back-end software with the ability to address distributed data storage.
- Highly customizable on per-user basis in terms of reports and views. It enables the operator to target the needs of all roles within the different company departments (IT, Operations, Marketing).
- Scalable architecture for targeting both the mid-small and large ISP markets.
- Provides localization at menu voices and page layouts level to target the ISP market on a global basis.
- Flexible role-based model for authentication and authorization.
- Robust and customizable framework for report running, generation, and presentation.
- Enhanced notification mechanism.
- Support of all the previous reports developed for earlier software releases
- Multi-user, profile-based access with customizable network, report, and user visibility policies.
- Enhanced Business Intelligence-oriented capabilities to interact, share, store, and export reports.
- Multi-time zone support
- Device abstraction layer - Support for reporting on traffic based on SCE
- Several deployment scenarios supported, including virtualization and high-availability
- Support for Multi-tenancy and reporting as a service

Cisco Insight Reporter is an independent component of the SCA solution, but has some dependencies on the database schema of the deployed SCA Collection Managers and SCE devices. In some situations, this software can be installed on the same appliance hosting the Cisco Collection Manager and its database, where traffic data is stored.

The figure below shows how the application can connect to the internal and also external databases to run reports based on the RDR data collected from SCE devices.

Figure 1. Connectivity of Cisco Insight Reporter with internal/external data sources

1.3 Features Overview

1.3.1. Deployment Scenarios

This software is designed to support a series of deployment scenarios to match different customer's use cases.

1. *Single Appliance Scenario* — In the single appliance scenario, Cisco Insight Reporter is installed on a single appliance running a supported version of Red Hat Enterprise Linux, CentOS Linux or Solaris (depending on the bus architecture).

Table 3. Single Appliance Scenario

Single Appliance Scenario	Description
Totally dedicated to Cisco Insight Reporter	This is the default and recommended, where the appliance is 100% dedicated to Cisco Insight Reporter. This is the recommended configuration for large SCE deployments.

Shared with a traffic database and a Collection Manager software instance	<p>This scenario is similar to the previous one, but it is used when only one Collection Manager is required and it is embedded in the Cisco Insight Reporter appliance (thus sharing the hardware resources with the application and the database).</p> <p>This configuration should be used only for very small deployments (up to 5 SCE devices). Performance of this appliance scenario gets reduced because it works in shared mode.</p>
Shared with a traffic database	<p>The Cisco Insight Reporter appliance also contains the traffic database (populated by one or more external CMs). The traffic database is MySQL and also hosts the internal schema of the application (but still independent from the Collection Manager schema).</p> <p>This scenario is used for small deployments with one to five SCEs requiring only a single traffic database to store traffic information.</p> <p>The number of supported SCEs is dependent on the RDR frequency (such as transactional or real-time subscriber monitoring).</p>

2. *Multiple Appliance Scenarios* - This scenario satisfies high availability of requirements. It is an extension of the previous scenario providing high-availability and redundancy functions by clustering the software and/or hardware layers.

This software provides high-availability and redundancy using solutions such as:

- Cold Failover - Two identical appliances can be deployed to provide a “cold” fail-over solution. No data is lost in case of failure of one of the appliances, but all pending operations with the clients are dropped and need to be restarted.
- Bundled MySQL engine for internal operations - When configuring an active or standby cluster for this software, MySQL can be configured with table replication to provide data consistency and keep the tables of the clustered system in synchronized state.



Note

The High-Availability configuration that can be setup for the Cisco Insight Reporter only applies to the reporting capability, not to traffic data collection and storage: the redundancy of the database layer should be manually set up (by the Collection Manager databases).

3. *Multi-Insight Deployment*—Cisco Insight Reporter supports the multi-instance scenario because it can use any traffic database as a data source. Traffic databases can be shared by different Insight systems. As these traffic databases are accessed in read-only mode, several application instances can establish connections. Through this deployment scenario, Cisco Insight Reporter supports multi-tenancy and network segmentation.
4. *Multi-tenancy Scenario* - A single instance of this software can serve one or more customer organizations (single ISP or ISP with multiple enterprise customers).

Table 4. Multi-tenancy scenarios

Multi-tenancy Scenarios	Description
ISP with one or more networks	<p>This is the most common scenario, where an ISP has one or more SCE networks sharing the same service configuration. For example, an ISP with a mobile network and a fixed network.</p> <p>In this case, administrators can create a single group of users, defining discrete visibility rights on networks, reports, packages, and subscribers. For example, some users can run reports only for the mobile network, others only for the fixed network, and some others can see both networks.</p> <p>Based on the ISP organization, an alternative can be creating a user group for each network, thus allowing network segmentation based on user groups. In this situation, sharing reports will be allowed only for users belonging to the same group.</p>
ISP with hosted customer networks	<p>In this scenario, the ISP has multiple customer networks and needs to provide a reporting service for each customer.</p> <p>In this case, customers can self-manage their users by adding, changing, or removing accounts and also create new custom roles (based on report capabilities).</p> <p>For example, customers can have their own SCEs, Collection Manager and database; centralized software can be connected to all these Traffic Databases to provide reporting services.</p> <p>The ISP can also create a user group with visibility over multiple customer networks. This can be useful when there is a partner in charge of monitoring the different customer networks using this software.</p>
Internet Data Center with one network shared by multiple customers	<p>In this scenario, the software supports SCEs positioned at the edge of a Data Center to monitor a Server Farm.</p> <p>The monitored subscribers or end-users are on the internal LAN and are typically the hosted or housed servers for end users. End users can access the Cisco Insight Reporter platform to run reports to monitor their own traffic.</p> <p>Usage of the server Multi-tenancy based on the network is not enough as segmentation for visibility, (Subscriber segmentation is required because Cisco Insight Reporter accounts can configured to have visibility only on specific subscribers [their owned servers]) An alternative requirement to provide subscriber visibility segmentation is to define filters for Subscriber Packages.</p>

1.3.2. Authentication and Authorization

This software supports three modes for authenticating the users. Users can be authenticated against RADIUS or TACACS+ based authentication servers or can be authenticated using the local Cisco Insight Reporter authentication module.

It supports role-based and configurable access to various operations. A set of allowed operations are assigned to the user role. For example, a user with role *manager* could be granted universal (read or write or execute) access, whether a user with the *admin* role can do all operations on the software.

1.3.3. Look and Feel

The look and feel of the software is mature, which makes it appealing and easy to use. This software's GUI gives the best experience in terms of usability and computer graphics.

1.3.4. SCE Terminology

This software supports the SCE network terminology and concepts like links, SCE, services, packages, subscribers, zones, etc. Additional levels of topology aggregations can also be defined such as PoPs, cities, regions...). Users can create and run reports over a selected aggregation level.

1.3.5. Favorite Reports

This software has the capability to store a list of chosen reports on the server machine. The stored reports are available as *My Favorites*. Users *can* add, modify, or delete items.

1.3.6. Scheduled Reports

This software has the ability to define an automatic execution of pre-defined reports with a pre-configured time and interval (it might be a single execution).

For example, where an administrator user needs to periodically share a set of reports with his or her managers or peers, he/she can define a list of users that will receive a notification on report batch completion and can have access to the report results.

The users can edit the report definition, remove, or duplicate existing reports.

1.3.7. Report Presentation Configuration

This software provides extensive and intuitive configuration for defining the presentation of report results. It includes:

- Presentation type: Chart, table, PDF, and CSV
- Report Title
- Type of chart: Bar, Pie, Stacked Area, Line, etc.

- Fonts, colors, labels, scales, axis
- Type, size, location of legend, etc.

User can select the context of the report base, for example, whether the report to be generated is based on bandwidth, volume, number of connections etc.

Using this software, user can compare multiple report results. The software can generate several reports together and display them on a single chart.

It is also possible to customize reports by inserting the company logo to the report in each of the presentation views.

1.3.8. Search Tool

Large lists such as services, packages, virtual links are not easy to navigate in, thus this software provides interactive search functionality within such lists.

1.3.9. Context Sensitive Help

This software GUI displays a help area based on context of the view that is currently displayed. This section contains static and dynamic information about the selection made by the user.

1.4 Features

This software's features are explained in following sections:

- Settings Management
- Network Topology
- Account Management
- Report Wizard
- **Application** Monitoring

1.4.1 Settings Management

This module provides tools to adjust the system global settings, configure databases, and manage devices.

- **Global Settings** - Global settings are configured during the installation but can be changed at any time by the administrator. The data structures that support the application global settings are:
 - **Advanced Settings**—It maintains a directory to save the exported reports on the user workstation.
 - **Local Database**—It stores the system hostname and IP address.
 - **SMTP** - Host name and IP address of the SMTP server are entered here. User can set up a user name and password for the outgoing email connectivity.
 - **Logging** - User can easily maintain product logs. It provides the ability to run first-level debugging.
 - **Localization** - Set language and the time zone.
- **Traffic Databases** - It helps in creating, editing, or deleting a connection to a Traffic Database. User can run the device discovery process, check the database connectivity, check the table status and database usage, retrieve the INI_VALUES table, and set the frequency of the polling process.
- **Device Configuration** - It helps in getting the device information such as IP address, external database, hostname, description, device type, number of links, location and time zone, monitored flag, master flag for configuration, etc. By using this feature, user can add a new device manually.
- **AAA Server** - Used to configure the authentication mode used by operators to connect to the application. Supported modes are:
 - local - using the internal MySQL database
 - external – using RADIUS or TACACS+ servers

1.4.2 Network Topology

This software supports multiple SCE configurations (one master SCE configuration per network type created by the administrator). There is a one-to-one mapping between the topology and its associated network. It discovers the active device list automatically. After administrator has configured a network and defined its topology, all users (operators) will be able to work with reports using the user-friendly and logical concepts.

It also supports the definition of a custom view for the network topology. Administrators can arrange SCEs in some specific logic, for example, aggregate devices by geography.

For SCE based networks, Insight Reporter V4.0.0 supports definition of Customer Interface View, which allows user to group and create hierarchy of monitored interfaces.

1.4.3 Account Management

This module provides list of mechanisms that allows the setup of user accounts, account groups, their roles, and capabilities.

After the platform installation, a default role: administrator is provided to the users. This role is defined at the initial level. User account and account groups can be added, updated, or deleted at any time.

Based on the credentials provided, user is assigned an access level which determines which screens and operations are available. The set of allowed operations will be based on the user role. The system allows configuration of the access per screen or object on the screen or operation. For example, a user with manager role is granted universal read, write, or execute access, whereas, a user with the administrator role can do everything but cannot change user or own credentials. The role-based model is very flexible to accommodate potential requirements of different types of customer.

1.4.4 Report Wizard

This module provides a series of reporting tools that enable users to run interactive reports, save and share report definitions, schedule recurring reports, view and customize a Dashboard, and share results.

The available reporting capabilities as presented using the GUI are:

- **Running a Report** —Using this software, user can open multiple report wizards at the same time, so that they can lead parallel analysis on different topics. In this way, it is possible to tile two or more open widgets and compare several reports on the same screen.
- **My Favorites** —User can select all mandatory parameters of a report and save it as a template that can be used during later sessions. The report template allows running reports while skipping all the wizard steps. User has the option to set a report custom name or use the default.
- **Report Gallery** —The Report Gallery is a tool where user can view all:
 - Report results shared by other accounts (only the reports that fulfill the report visibility constraints of the account are displayed).
 - Personal reports that were published on the gallery (these can be private or shared with other users).
 - Results of personal scheduled reports.

- Temporary reports saved with the “Remember” action on the workspace. These will be removed after the current session is over.
- **Scheduled Reports** — This software supports the ability to automatically run the several pre-defined reports each in a pre-configured time and interval. For example, an administrator needs to periodically share a set of reports with his or her managers or peers. The user (administrator) can define a list of users (managers) that will receive a notification on report batch completion and will have access to the report results as well. Scheduled reports run in background and are designed to produce a static output that can be sent via email and stored on the file system of the server.

1.4.5 Application Monitoring

This software components support common standards for server hardware and software monitoring, operations, and maintenance. The same information is viewable via UI as well.

Information that can be monitored includes:

- User statistics such as:
 - Number of logged-in users
 - Number of reports per user session (min, max, or avg.)
 - Favorite reports per user (min, max, or avg.)
 - Scheduled reports per user (min, max, or avg.)
- Report performance statistics such as:
 - Report transactions (from each kind user-generated and automatic)
 - Report response time (min, max, or avg.)
 - Failed report transactions
- General performance and capacity such as:
 - CPU load
 - Database capacity



CHAPTER 2. Connecting to Cisco Insight Reporter

This chapter provides instructions on how to launch this application after it is installed on a server and describes the various components that are available.

This chapter contains following sections:

- Login
- Logout

After the application is installed on server, user will be able to execute it using the browser.

The default URL to run this software is:

http://<server_IP>

Where *<server_IP>* needs to be replaced with the IP address of the server hosting the Cisco Insight Reporter software.

2.1 Login

When user runs the application, the Login page shown in figure 2 will appear:

Figure 2. Login Page

Step 1 Enter the username in **Username** textbox.

Step 2 Enter the password in **Password** textbox.

If user does not have the login credentials, contact the administrator.

A default account with *super user* privileges is pre-configured by the installation script.

In addition to the usage of the reporting tools, the *super user* privileges include the capability of account management, network management, and change of global settings and usage of the monitoring tools.



Note

The credentials of the default *super user* account, pre-configured during the installation process, are:

Login: **cisco**
 Password: **cisco**

For security reasons, it is strongly suggested to change the *cisco* account password after the first login into the application.

**Note**

User session automatically logs off, depending on the time period defined in the settings of the application.

After logging off, a new user authentication is required.

A user with any role can run only two sessions of a given instance with provided login credentials. If more than two sessions are created, the user will get the following error :
“Access denied - No more sessions allowed for this role”

After log in, user will be able to see following four main components of the application:

- Welcome Screen
-

- Dashboard
- Module Launcher
- Windows Controls and Main Menu

2.1.1 Welcome Screen

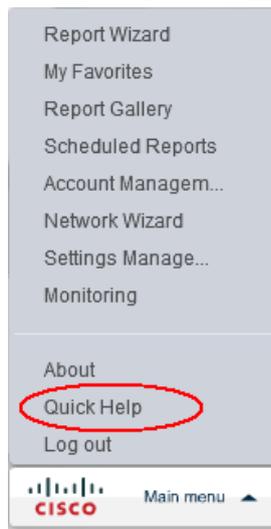
The **Welcome screen** displays the steps to configure the application to generate the first reports. All operators will see the Welcome panel the first time they connect to the application

Figure 3. Welcome screen



It has **Close** button and **Don't show again** checkbox. If the user clicks on **Close** button with enabling **Don't show again** checkbox, user will not be able to see this screen again. Even if the user has closed Welcome screen permanently, he/she still has the option to see this screen again from the main menu, click **Quick Help** link.

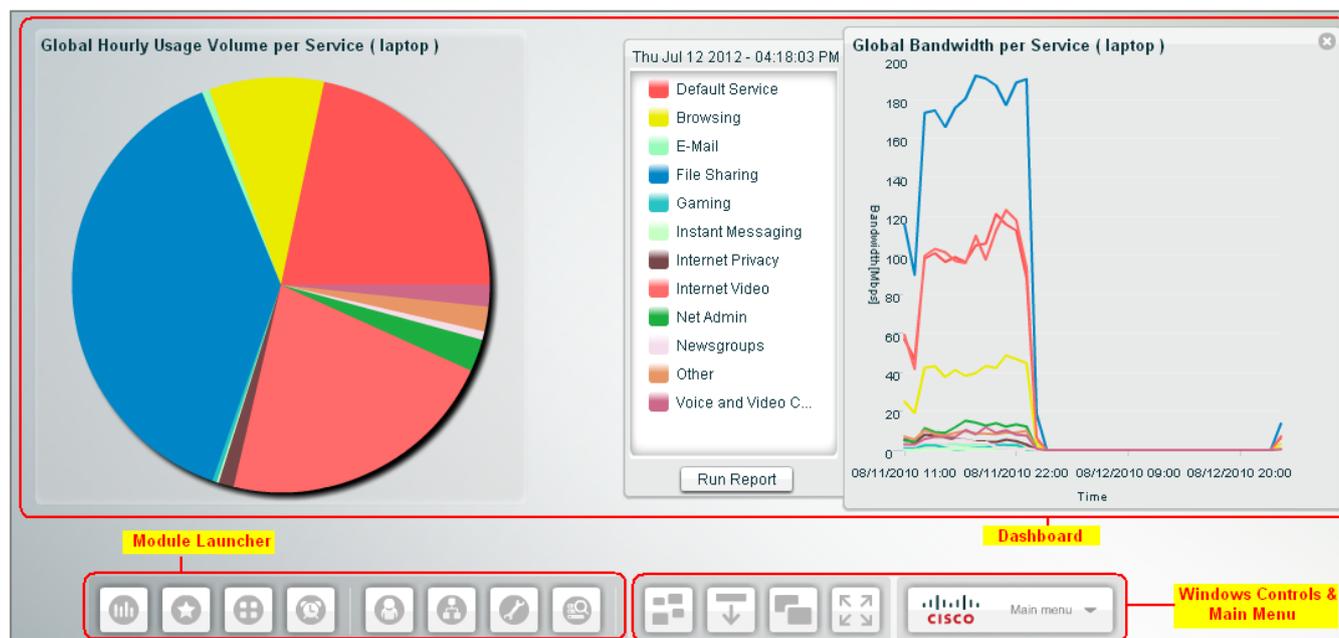
Figure 4. Main Menu



2.1.2 Dashboard

The **Dashboard** displays reports saved by user. It is the base for the report modules. The other components such as widgets and **Module Launcher** appear below the **Dashboard**. The connected user can view all the saved and scheduled reports on the Dashboard. User can load and monitor six reports at a time on the Dashboard.

Figure 5. Dashboard



Note When user logs in for the first time, the Dashboard will be empty. User can add reports on Dashboard through the Report Wizard. A newly added widget is positioned on the top-left corner of the Dashboard and has to be manually positioned if multiple widgets overlap.

2.1.3 Module Launcher

The **Module Launcher** is the most important component of this software. User can check the current status; can generate the reports using the Module Launcher. It also provides the main menu of the application, which helps in performing various operations.

After logging into the application, the following toolbar will appear at the bottom of the screen:

Figure 6. Module Launcher

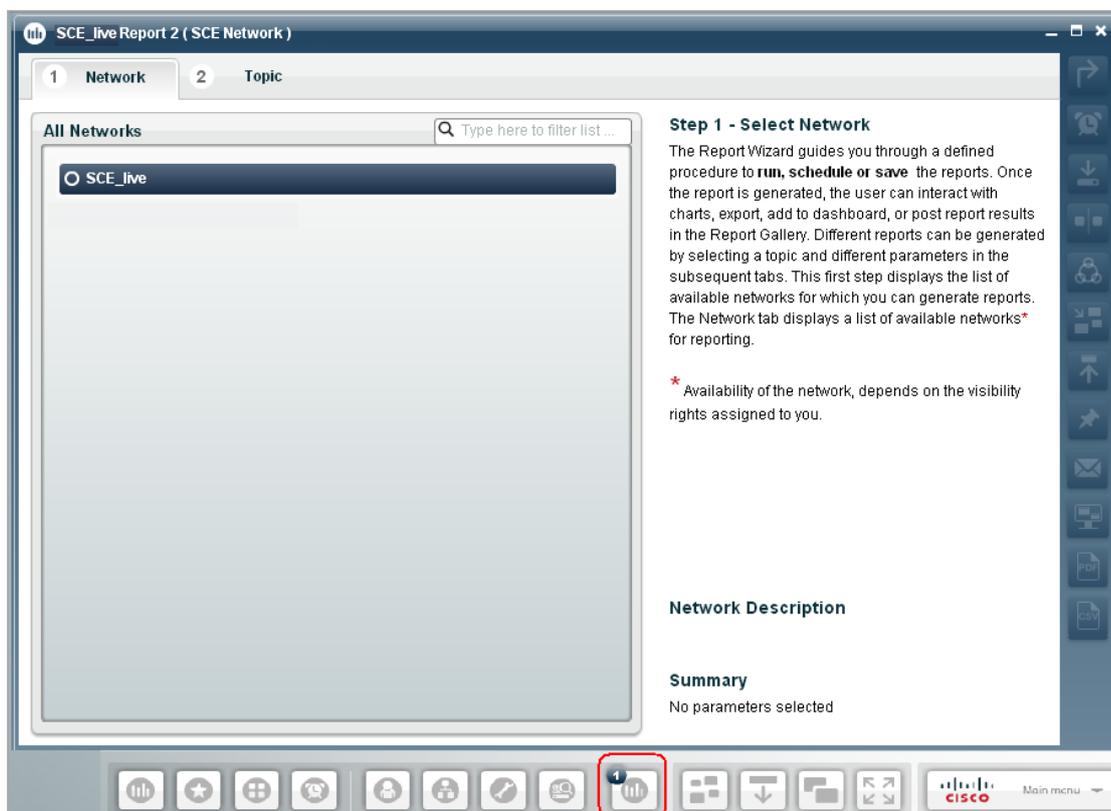


The **Module Launcher** is divided into the modules described in Table 5.

Table 5. Module Description

Module	Description	Icon
Settings Management	To set up application parameters and configure traffic and local databases.	
Network Wizard	To configure network topology on the application.	
Account Management	To manage user accounts, roles, and visibility rights.	
Report Wizard	To set up report parameters, schedule recurring reports, and share results.	
Monitoring	To check status of the active reports, log messages, and debug reports.	
My Favorites	To view and use the most-used reports.	
Report Gallery	Repository of report output published by the user (private) or shared by other users (public).	
Scheduled Reports	Repository of reports which the user has scheduled for execution in future. The possible destination for such reports can be Dashboard, email, or Report Gallery	

When opening the Report Wizard module, a new icon (with dynamic bubble) appears as shown below:

Figure 7. Report Wizard

A bubble (embedded with counter) on the new icon shows the total number of report wizards opened in the current user session.

2.1.4 Windows Controls and Main Menu

Widgets are components in which modules are shown to the user. Essentially all module windows are widgets. Widgets are equipped with the window controls such as maximizing, minimizing, tile, cascade, etc. Widgets can be positioned, aligned, resized, launched, and closed.

Figure 8. Window Controls and Main Menu

All the modules which can be opened using the Module Launcher can be opened using the **Main menu** option.

Within the same user session, multiple instances of the Report Wizard could be open simultaneously; however, all other modules (Network Management, Account Management, Settings Management, My Favorites, Report Gallery, Schedule Reports, and Monitoring) support only a single instance.

Table 6. Window Controls

Control	Description	Icon
Change View Mode	To change view of the screen. On click it will display the Dashboard over the opened window or vice a versa.	
Minimize All Windows	To minimize all open windows.	
Cascade Windows	To display all open window as cascade.	
Go Full Screen	To view in full screen.	

Modules other than **Report Wizard** if minimized can be restored by clicking the respective icon on the launcher. The instances of minimized **Report Wizard** windows can be reopened by clicking the bubble on the **Opened Reports** icon on the launcher. This will show a list of minimized windows that can be selected.

**Note**

When using the Full Screen button in the Launcher bar, all the keyboard printing keys will be disabled. Alternatively user can use the browser Full Screen (F11) option that allows maximizing the browser window with active keyboard input.

2.2 Logout

User can log out from the application, by choosing the **Logout** option in the Main menu on the Module Launcher. On clicking, all sessions will be closed, the current user will be logged off, and the application will automatically show the login page.

**Note**

When using the application, closing the tab or browser itself or refreshing the browser content will end the session and user would be logged out.

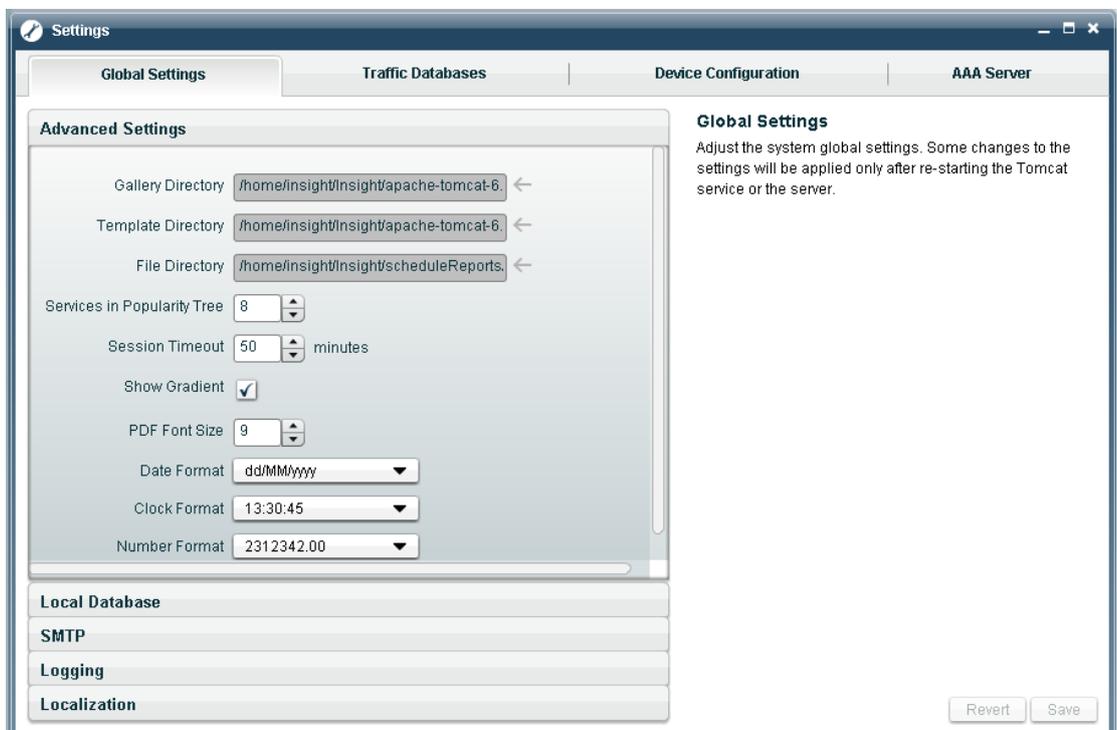


CHAPTER 3. Settings Management

3.1 Introduction

This chapter describes how to setting up of main application parameters and configuring traffic and local databases.

Figure 9. Settings Management



This chapter contains following sections:

- Global Settings
- Traffic Database Configuration
- Device Configuration
- Configuring AAA Server for Authentication

3.2 Global Settings

Global Settings enables the user to apply general settings to the application, configure Global database and SMTP server, log debug messages, and localize the application. Global settings are configured during the installation process but can be changed at any time by the administrator. The entire Global Settings will be applied for the whole application.

To access and display the **Global Settings** tab, click **Setting Management** icon on the Module Launcher.

Settings that support the **Global Settings** tab are:

- Advanced Settings
-
- Local Database
-

- SMTP

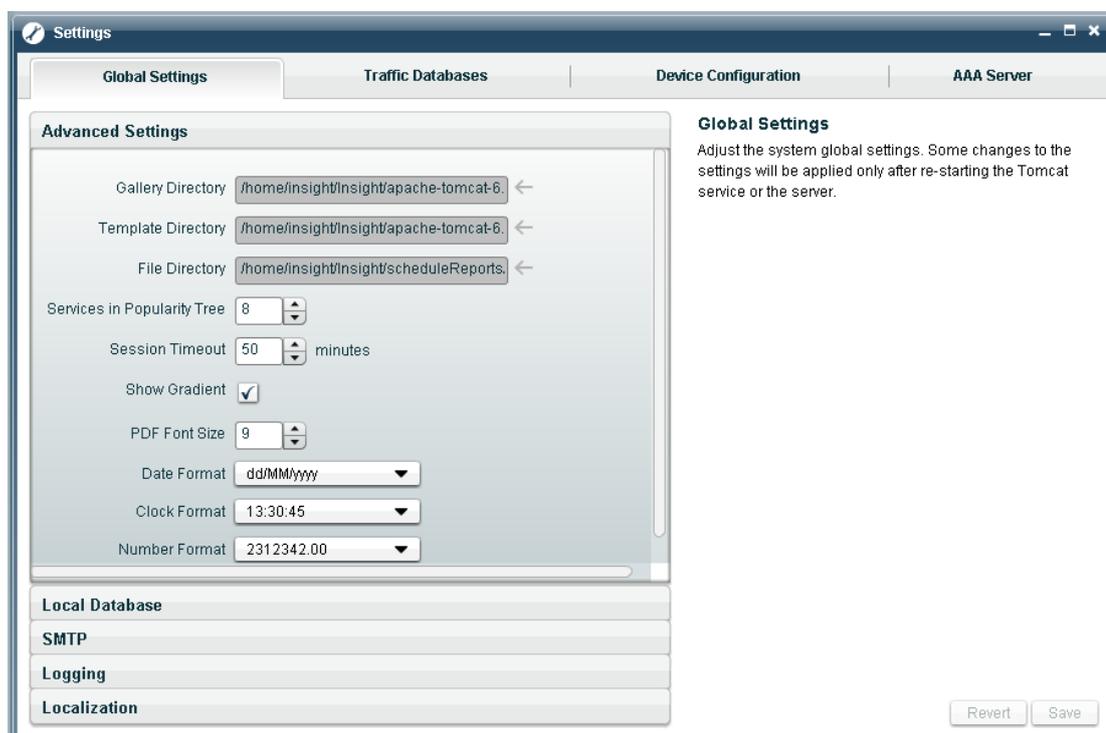
- Logging
- Localization

3.2.1 Advanced Settings

The **Advanced Settings** pane of the **Global Settings** tab identifies the paths (application, templates, reports exported in PDF and CSV) created during the installation process on this software's local file system.

On selecting **Advanced Settings** pane, it will display the following screen:

Figure 10. Advanced Settings



To create or edit the path information, perform the following steps:

- Step 1** This field displays the path to create or edit the base directory for PDF, CSV, and Image reports generated in the **Gallery Directory** field. This field is non-editable as sometimes changing location of base directory, would create problem in the application.
- Step 2** This field displays the path to create or edit the directory for the report template files in the **Template Directory** field. This field is non-editable as sometimes changing location of template directory, would create problem in the application.
- Step 3** This field displays the path to create or edit the directory where the output of scheduled reports will be placed on the local file system. A default value is populated by the installation script, but can be changed in case of specific needs.

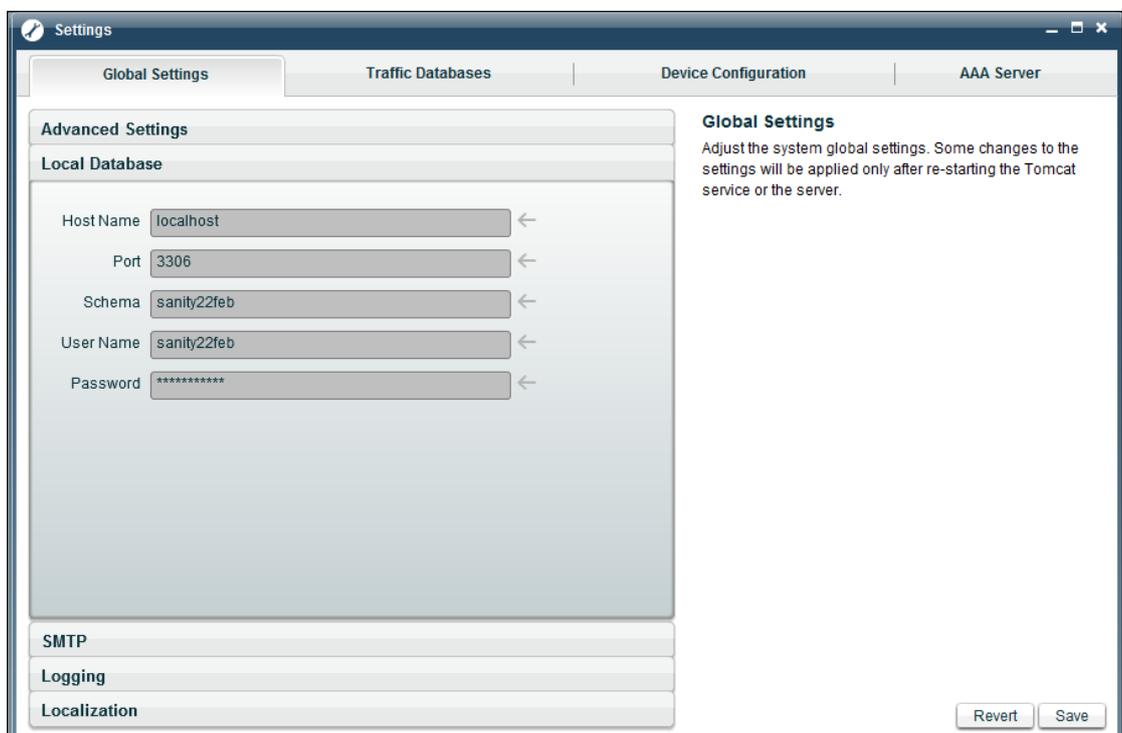
- Step 4** In the **Services in Popularity Tree** text box, enter the number of top popular services to be shown as non-aggregated (all other minor services will be shown as a single, aggregated series).
- Step 5** Enter the number of seconds in **Session Time Out** text box to set the time to wait for a database connection.
- Step 6** Check **Show Gradient** checkbox to view the charts with some dazzling effect. By default this checkbox is checked.
- Step 7** Set the font size for PDF files in **PDF Font Size** text box.
- Step 8** Select the date format in **Date Format** drop down.
- Step 9** Select the clock format in **Clock Format** drop down.
- Step 10** Select the clock format in **Number Format** drop down.
- Step 11** Click the **Revert** button to return to the previous page or click the **Save** button to confirm.

3.2.2 Local Database

The Local Database pane is used to store application-specific configurations, global data, etc. User must establish a connection to the local database. All the fields are non-editable because changes in these fields do not impact database settings.

After user selects the **Local Database** pane, it will display the following screen:

Figure 11. Local Database



- Step 1** This field displays hostname or IP address of the internal database in the **Host Name** field.
- Step 2** This field displays server port number of local database in the **Port** field.
- Step 3** This field displays name of internal database schema in the **Schema** field.
- Step 4** This field displays the username in the **Username** field.
- Step 5** This field displays the password in the **Password** field.
- Step 6** Click the **Revert** button to return to the previous page, or click the **Save** button to confirm.
-

3.2.3 SMTP

To configure the application to schedule the reports and send them via e-mail, user needs to configure an external SMTP server.

After user selects the **SMTP** pane of the **Global Settings** tab, it will display following screen:

Figure 12. SMTP Settings

The screenshot shows a web-based configuration interface for SMTP settings. The window title is "Settings" and it has four tabs: "Global Settings", "Traffic Databases", "Device Configuration", and "AAA Server". The "Global Settings" tab is active. On the left side, there is a sidebar with sections: "Advanced Settings", "Local Database", "SMTP", "Logging", and "Localization". The "SMTP" section is expanded, showing the following fields:

- Host Name:** mail.cisco.com
- Port:** 25
- User Name:** sanity22feb@cisco.com
- Password:** [masked with asterisks]
- Email:** sanity22feb@cisco.com

On the right side, under the "Global Settings" heading, there is a note: "Adjust the system global settings. Some changes to the settings will be applied only after re-starting the Tomcat service or the server." At the bottom right of the window, there are two buttons: "Revert" and "Save".

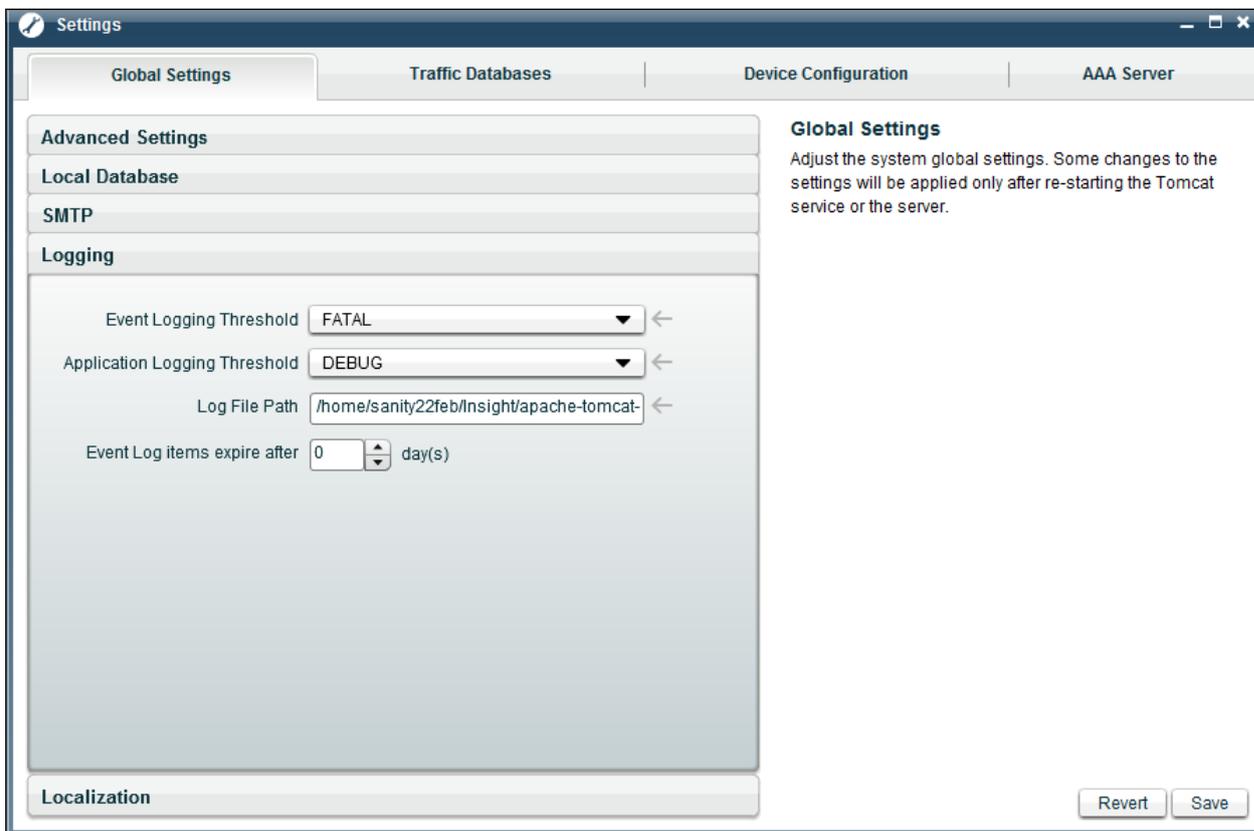
To configure the SMTP server, perform the following steps:

- Step 1** Enter hostname or IP address of the SMTP server, in the **Host Name** text box.
- Step 2** Enter server port number, in the **Port** text box.
- Step 3** Enter the username to connect to the SMTP server in the **Username** text box.
- Step 4** Enter the password to connect to the SMTP server in the **Password** text box.
- Step 5** Enter the email id that will be used to exchange the emails in the **Email** text box.
- Step 6** Click the **Revert** button to return to the previous page, or click the **Save** button to confirm.

3.2.4 Logging

User can easily collect product logs by using this application. To store debug reports in the system or to retrieve logs, user must configure the logs. To configure the log, select the **Logging** pane of the **Global Settings** tab, it will display following screen:

Figure 13. Logging



To configure debug message logging, perform the following steps:

- Step 1** Cisco Insight Reporter generates events for which notifications are delivered to the System Administrator via E-Mail. These events can be accessed and controlled from the application. From the **Event Logging Threshold** drop-down list, choose the level of verbosity range from ERROR (all error conditions will be reported) to FATAL (only critical errors will be reported).
- Step 2** Cisco Insight Reporter generates the application logs in separate log file. These logs can be accessed only through file system, but their verbosity can be controlled from application. From the **Application Logging Threshold** drop-down list, choose the level of verbosity range from DEBUG (maximum amount of details) to ERROR (only errors will be reported).

- Step 3** Enter the path in the **Log File Path** field, to create the logs folder under the application base directory.
- Step 4** Enter the number of days in the **Event Log items expire after** field to set the time for the log existence.
- Step 5** Click the **Revert** button to return to the previous page, or click the **Save** button to confirm.

**Note**

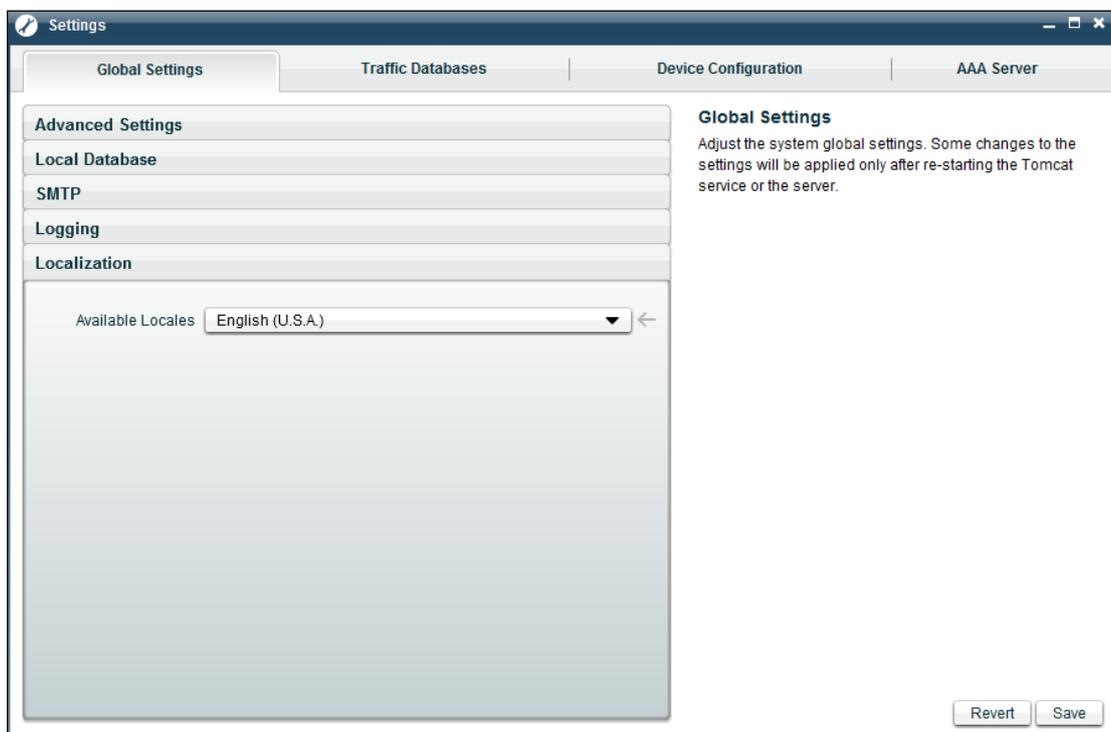
Event notifications are delivered to user (Notification preference can be set for each account through account management module) whereas the application logs are available for platform administrators and are available on the server at the “Log File Path” specified in Step 3 above.

3.2.5 Localization

To localize the system in the preferred language, user must configure the localization settings. User performs localization configuration at the time of the installation but can localize the configuration at any time. Any changes will affect the menu items, navigation elements, and the report output.

After selecting the **Localization** pane of the **Global Settings** tab, it will display following screen:

Figure 14. Localization



To localize the application, perform the following steps:

-
- Step 1** Choose the available language from the **Locale** drop-down list.
 - Step 2** Click the **Revert** button to return to the previous page, or click the **Save** button to confirm.
-

**Note**

The default localization of the application is English (United States). Other localization packages could be available for download. Check Cisco CCO site or contact the local Account Manager.

3.3 Traffic Database Configuration

The **Traffic Database Configuration** tab enables the user to configure a connection to a Traffic Database which contains the traffic information collected by the DPI devices and populated by the Cisco Collection Manager. User can run the SCE discovery process, check the database connectivity, check the table status and database usage, retrieve the content of configuration tables, and set the frequency of the polling process.

User should configure one or more databases that will be used as a source of data for generating reports.

Each database requires a set of connections, thus the user must define connection properties (database name, IP address, port, schema version, credentials, and other connection options).

To access the **Traffic Database Configuration** tab, click the **Setting Management** icon on the Module Launcher.

Using the **Traffic Database Configuration** tab, user can:

- Configure a new Traffic Database
- Edit a Traffic Database
- Delete an existing Traffic Database

**Note**

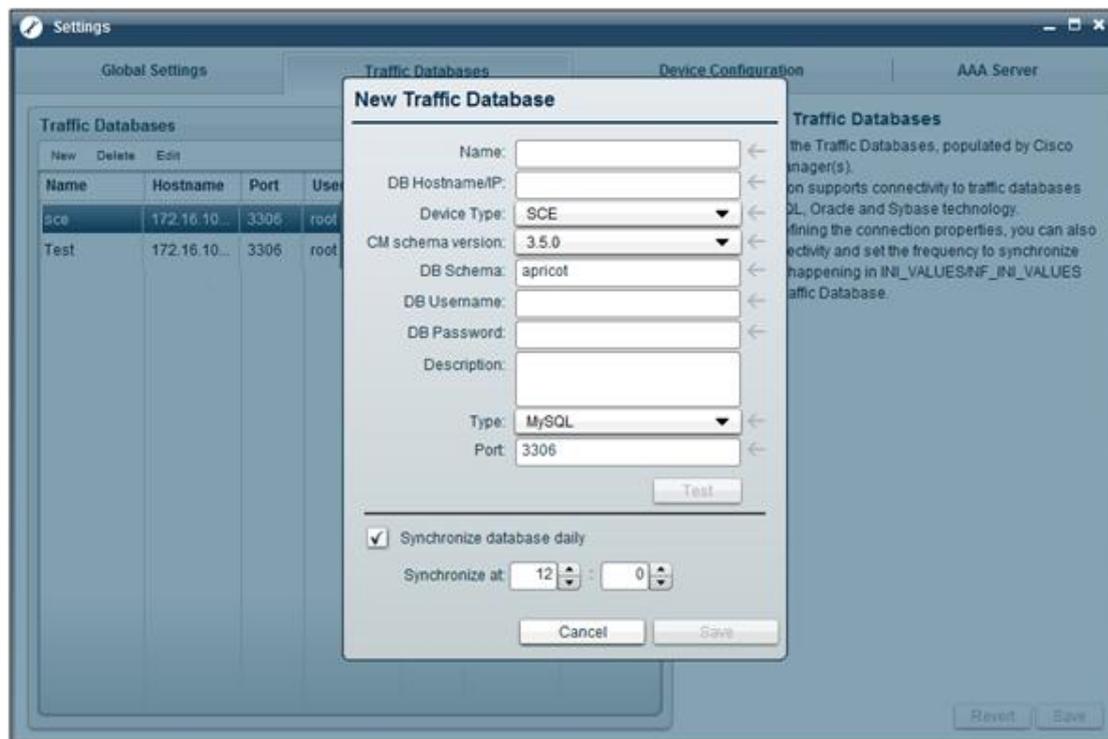
The default installation kit is bundled with JDBC connector for MySQL 5.x. To use Sybase (ASE v 12.x or later) or Oracle (v 9.x or later) as Traffic Database, please copy the compatible JDBC connector jars (not provided with the Cisco Insight Reporter) for the respective database server to following directory:
< [user home directory]/Insight/apache-tomcat-6.0.20/webapps/insight/WEB-INF/lib >

3.3.1 Configure a new Traffic Database

To configure a new **Traffic Database**, perform the following steps:

- Step 1** Select **New** option in the **Traffic Database** tab. It will display the **New Traffic Database** pop-up.

Figure 15. New Traffic Database



- Step 2** Enter name of the database in the **Name** text box.
- Step 3** Enter host name or IP address of database in the **DB Hostname/IP** text box.
- Step 4** Select the type of device in the **Device Type** drop down.
- Step 5** Select the version of CM schema in the **CM schema version** drop down.
- Step 6** Enter name of traffic database schema in the **DB Schema** text box. By default it displays **apricot** for SCE.
- Step 7** Enter traffic database user name in the **DB Username** text box.
- Step 8** Enter traffic database password in the **DB Password** text box.
- Step 9** Enter description in **Description** text box.

Step 10 Select the DB type in the **Type** drop down.

Step 11 Enter DB port in the **Port** text box.

Step 12 Click the **Test** button to test the connection status.

**Note**

On testing the connection with a traffic database, Insight checks for the availability of INI_VALUES (for SCE) tables. Please make sure that the tables are available and are accessible.

Step 13 Check the **Synchronize database daily** check box, if user wants to synchronize the database on a daily basis. During the synchronization process, the application reads the latest configuration for the Master device from the traffic database.

Step 14 Set the time for synchronizing the database automatically, by entering the time in the provided field.

Step 15 Click the **Cancel** button to return to the previous page, or click the **Save** button to confirm.

**Note**

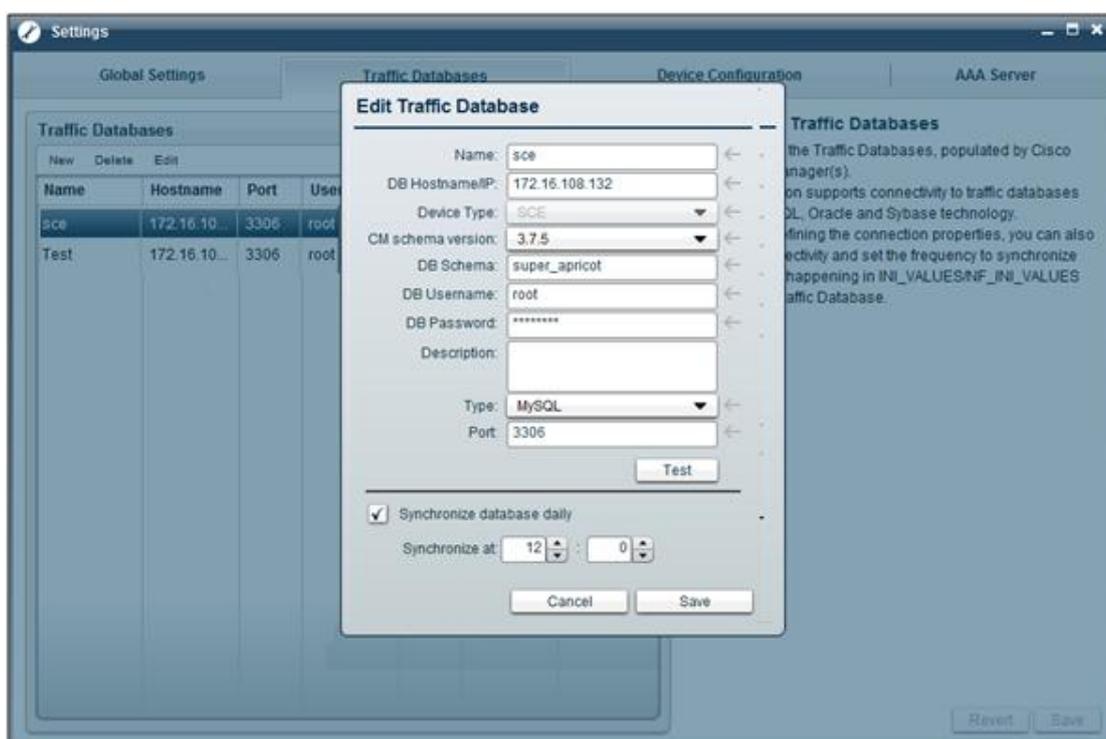
If the connection is not available during the synchronization process, the configurations will be synchronized only when the process runs the next day. In such case, user can force the update by doing "Get Master Values" for the selected network in the Network Wizard.

3.3.2 Edit a Traffic Database

To edit the configuration of a Traffic Database, perform the following steps:

Step 1 Select the **Edit** option in the **Traffic Database** tab. It will display the **Edit Traffic Database** pop-up.

Figure 16. Edit Traffic Database



Step 2 Edit name of the database in the **Name** text box.

Step 3 Edit host name or IP address of database in the **DB Hostname/IP** text box.

Step 4 Edit the version of CM schema in the **CM schema version** drop down.

Step 5 Edit name of traffic database schema in the **DB Schema** text box.

Step 6 Edit traffic database user name in the **DB Username** text box.

Step 7 Edit traffic database password in the **DB Password** text box.

Step 8 Edit description in **Description** text box.

Step 9 Edit the DB type in the **Type** drop down.

Step 10 Edit DB port in the **Port** text box.

Step 11 Click the **Test** button to test the connection status.

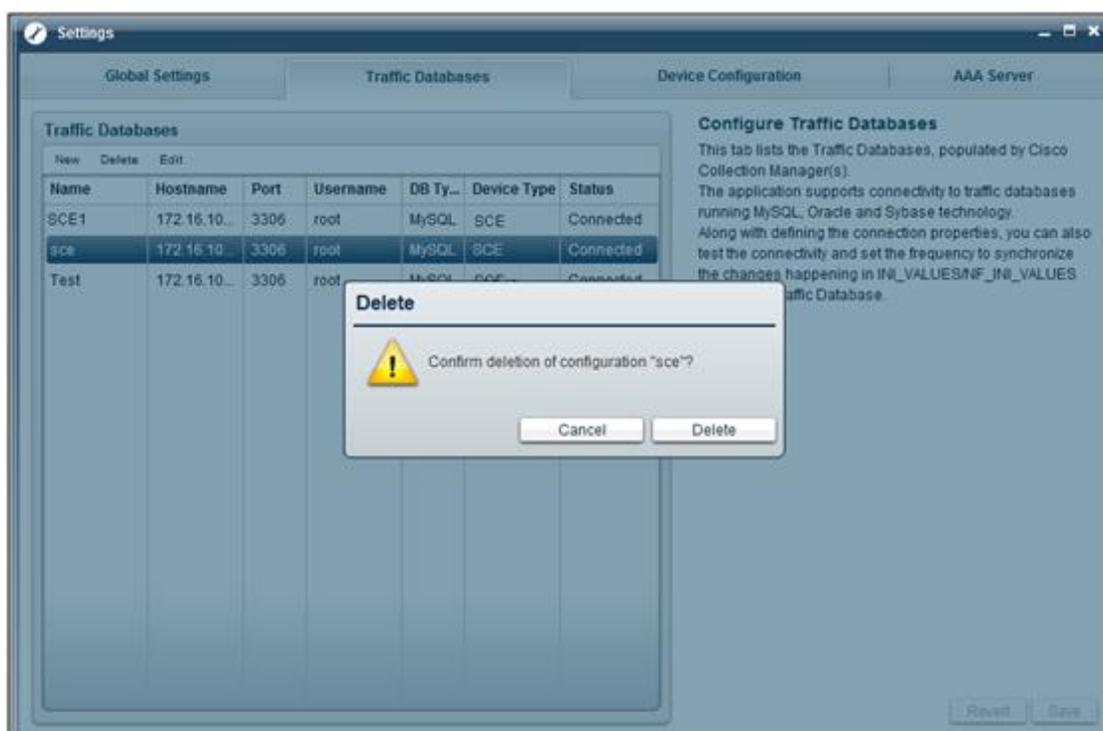
- Step 12** Check the **Synchronize database daily** check box, if user wants to synchronize the database on a daily basis. During the synchronization process, the Cisco Insight Reporter reads the latest configuration for the Master device from the traffic database.
- Step 13** Edit the time for synchronizing the database automatically, by entering the time in the provided field.
- Step 14** Click the **Cancel** button to return to the previous page, or click the **Save** button to confirm.
-

3.3.3 Delete an existing Traffic Database

To delete a Traffic Database, perform the following steps:

- Step 1** Select the database from the list of Traffic Databases.
- Step 2** Select the **Delete** option in the Traffic Database Configuration tab. A dialog box appears asking user to confirm the deletion.

Figure 17. Delete a Traffic Database



- Step 3** Click the **Cancel** button to return to the previous page, or click the **Delete** button to confirm.

3.4 Device Configuration

Using the Device Configuration tab user can configure SCEs of a SCE Traffic Database. User can browse the SCE Traffic Databases (prefixed by “SCE”), to get a list of SCE devices identified by their IP addresses.

The SCE devices can be populated by:

1. **Manual Provisioning:**—User can add SCE devices) for reporting by providing the valid details of device. This process is beneficial, when user is aware about the device configuration and user wants to use specific device.
2. **Auto Discovery**—Using this feature user can discover the SCE devices) defined on Traffic Database. This feature is beneficial, when user is unaware about the devices, and user wants to see all the devices available on Traffic Database.

In this tab, a list of SCEs is displayed detailing the device information:

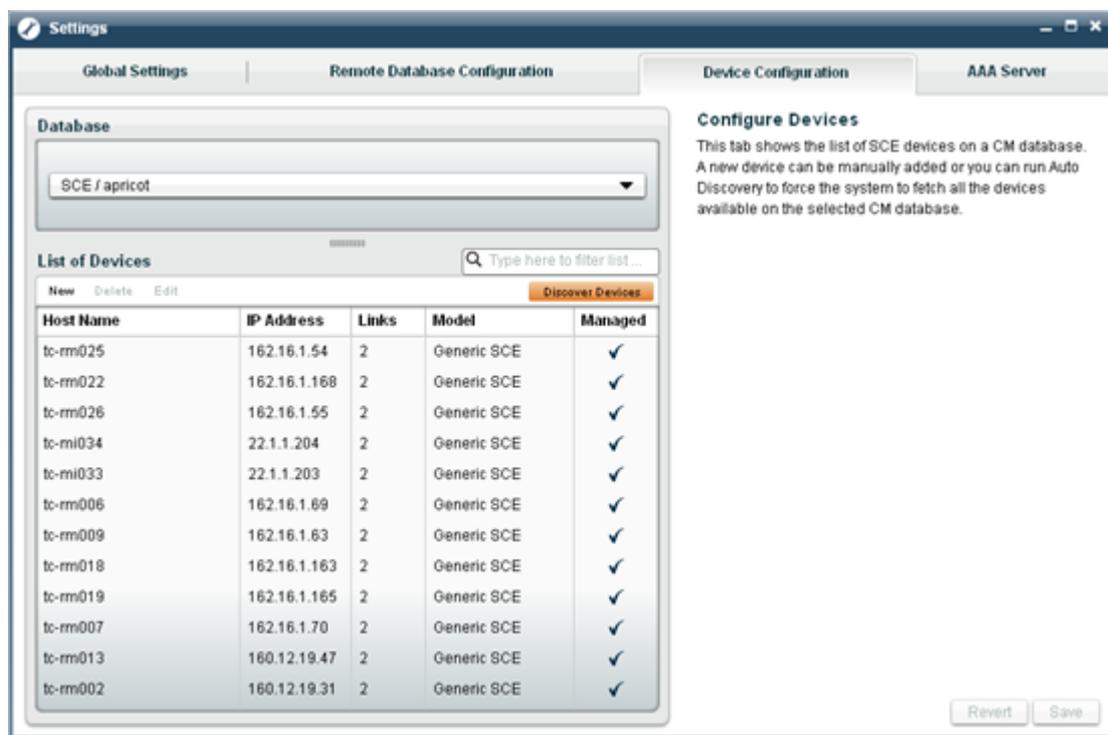
Table 7. SCE Device Information

Device Information	Description
Hostname	Name of the device
IP address	IP address of the device.
Links	Number of links.
Model	SCE Device type. At present, only SCE1010, SCE2020, and SCE8000 are supported.
Managed	Device is managed or not.

To access and display the **Device Configuration** tab, click the **Setting Management** icon on the Module Launcher.

After user selects the **Device Configuration** tab, following screen will appear:

Figure 18. Device Configuration - showing list of SCE devices



Using the **Device Configuration** tab, the user can perform the following actions:

- Configure a new Server
- Delete an Existing Device
- Edit an existing server

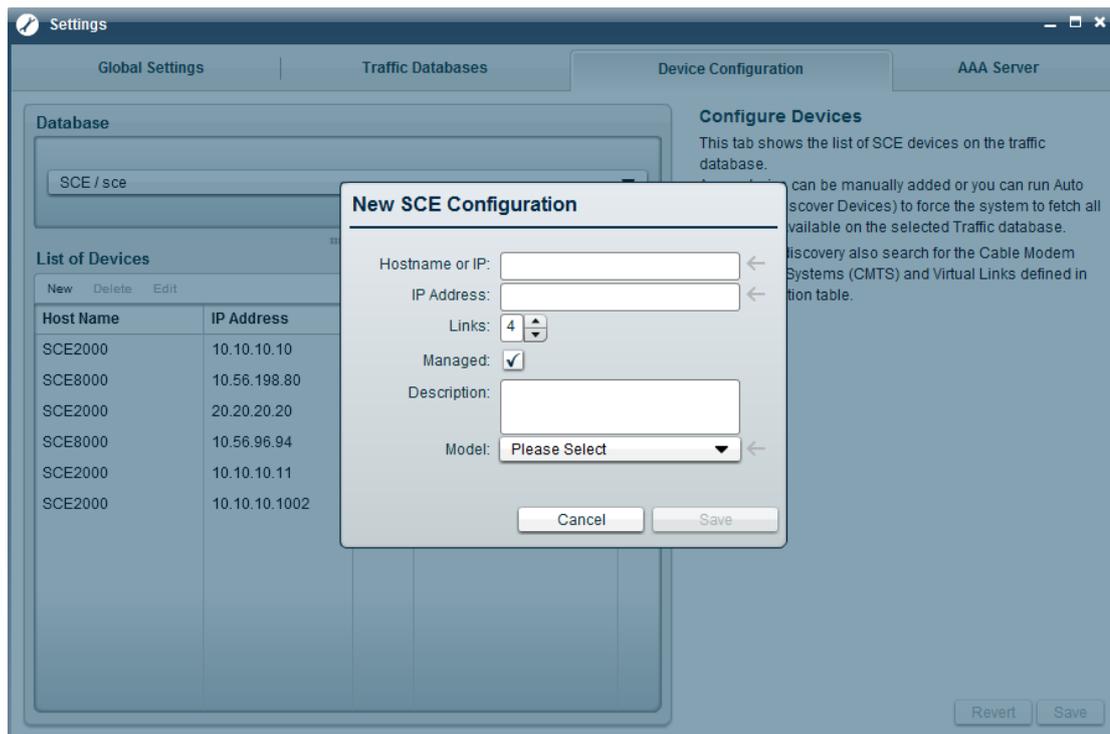
3.4.1 Configure a new SCE Device

To add a new SCE device, perform the following steps:

Step 1 Choose the SCE database in which the new SCE device has to be configured from the **Database** drop-down list.

Step 2 Click the **New** option. On clicking, following pop-up will appear:

Figure 19. Configuring a New SCE Device



Step 3 Enter the required device information such as **Host Name**, **IP Address**, **Links**, **Managed**, **Description**, and **Model**.

Step 4 Click the **Cancel** button to return to the previous page, or click the **Save** button to confirm.

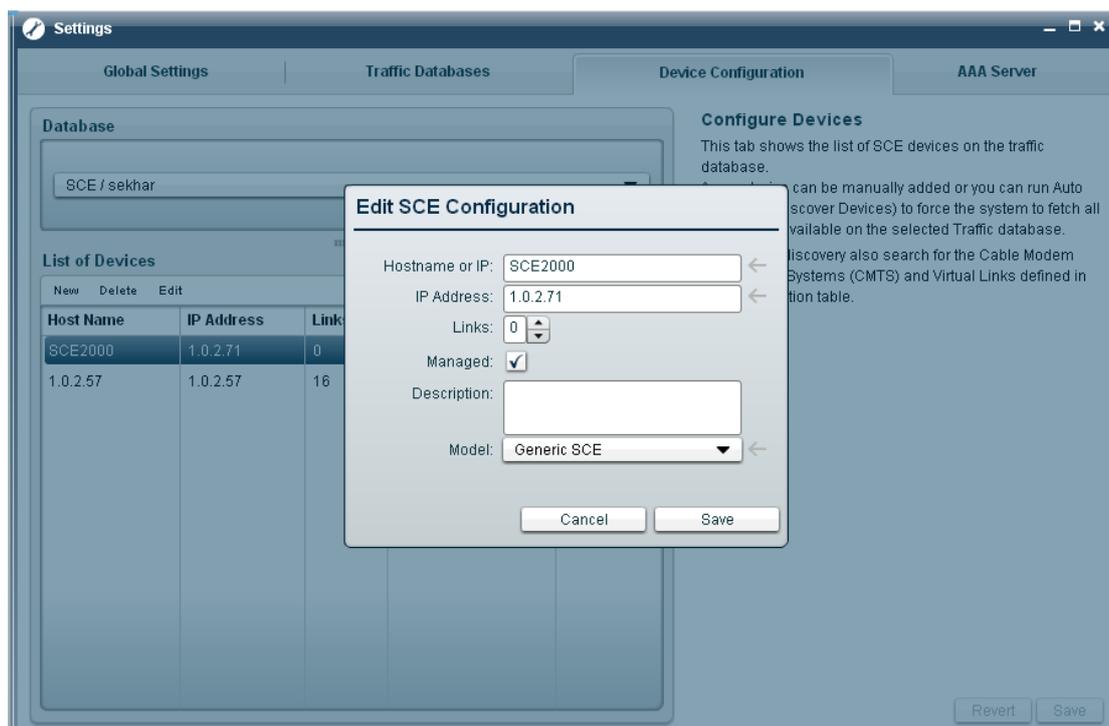
3.4.2 Edit an existing Device

To edit an existing device, perform the following steps:

Step 1 Choose the database for which user wants to edit the device to configure, from the **Database** drop down list.

Step 2 Click the **Edit** option. On clicking, following pop-up will appear:

Figure 20. Edit a Device



Step 3 Edit the device information such as Host Name/IP, IP Address, Managed, Description Model, and Aggregation interval.

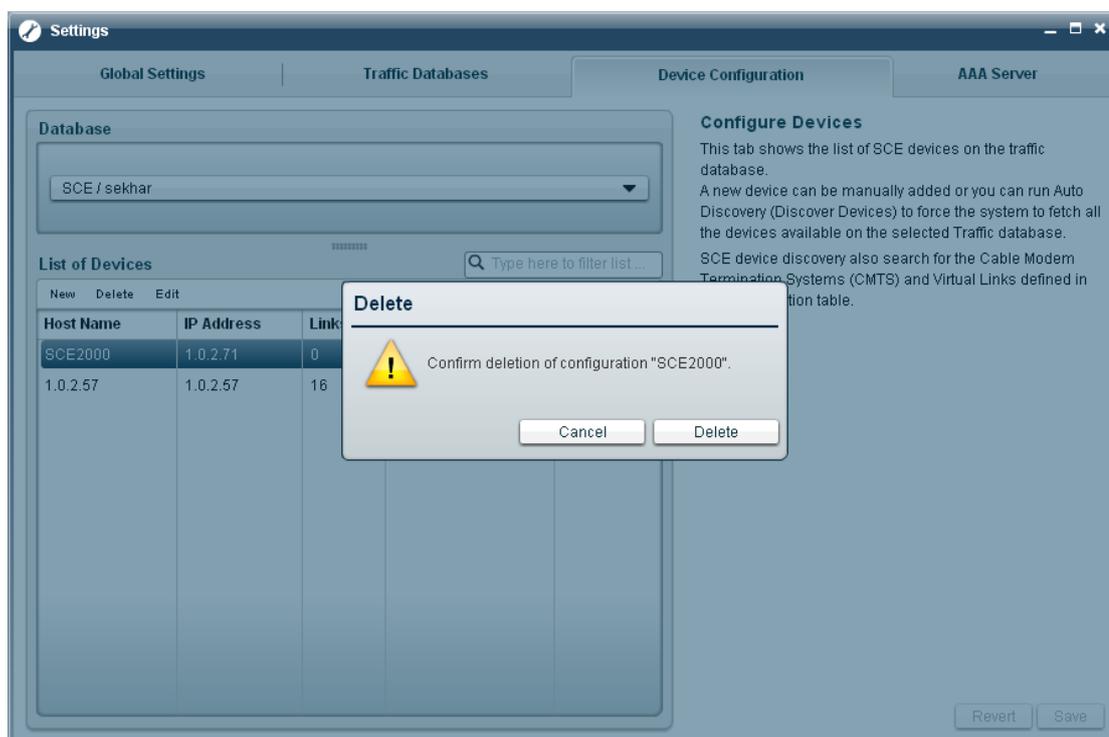
Step 4 Click the **Cancel** button to return to the previous page, or click the **Save** button to confirm.

3.4.3 Delete an existing Device

To delete an existing device, perform the following steps:

- Step 1** Select the device from the list of devices.
- Step 2** Select the **Delete** option. A Confirm deletion dialog box appears asking user to confirm the deletion.

Figure 21. Delete a Device



- Step 3** Click the **Cancel** button to return to the previous page, or click the **Delete** button to delete.

3.5 Configuring AAA Server for Authentication

AAA stands for authentication, authorization, and accounting. Currently, application is leveraging only authentication from AAA servers. Application is taking care of accounting and authorization by its own.

This tab displays list of AAA servers. Administrators can configure as well as test the connectivity with the configured AAA servers.

The first server appearing in the list is the Primary server while the remaining are Secondary servers.

User is first authenticated against the Primary server and in case the primary server is not reachable (network/connection error), the user is authenticated against the secondary server(s) in the order of creation. In order to reset the authentication order, the servers can be dragged and dropped to the appropriate place in the list.

The Local Authentication mode is by default enabled, in which case, user will be authenticated against the local database.

Other than Local AAA mode, both RADIUS and TACACS+ modes can be disabled. If an authentication mode is disabled, new user cannot be assigned that authentication mode and user has to be assigned the Local Authentication. If there are existing users assigned to an authentication mode, that mode cannot be disabled until all the users are moved to some other mode.

Figure 22. AAA Server

The screenshot displays the 'AAA Server' configuration window. It features a 'TACACS+' section with an 'Enable' checkbox and a table of servers. The table has columns for 'Name', 'IP/Hostname', and 'Status'. One server is listed: 'tacacs+ server' with IP '172.16.32.108' and status 'Disconnected'. Below the table are 'RADIUS' and 'Local' sections, each with an 'Enable' checkbox. The 'Local' checkbox is checked. A 'Revert' and 'Save' button are located at the bottom right.

Name	IP/Hostname	Status
tacacs+ server	172.16.32.108	Disconnected

In the **AAA Server** tab, the user can perform the following actions:

- Configure a New Server
- Deleting an existing Server
- Edit an Existing Server

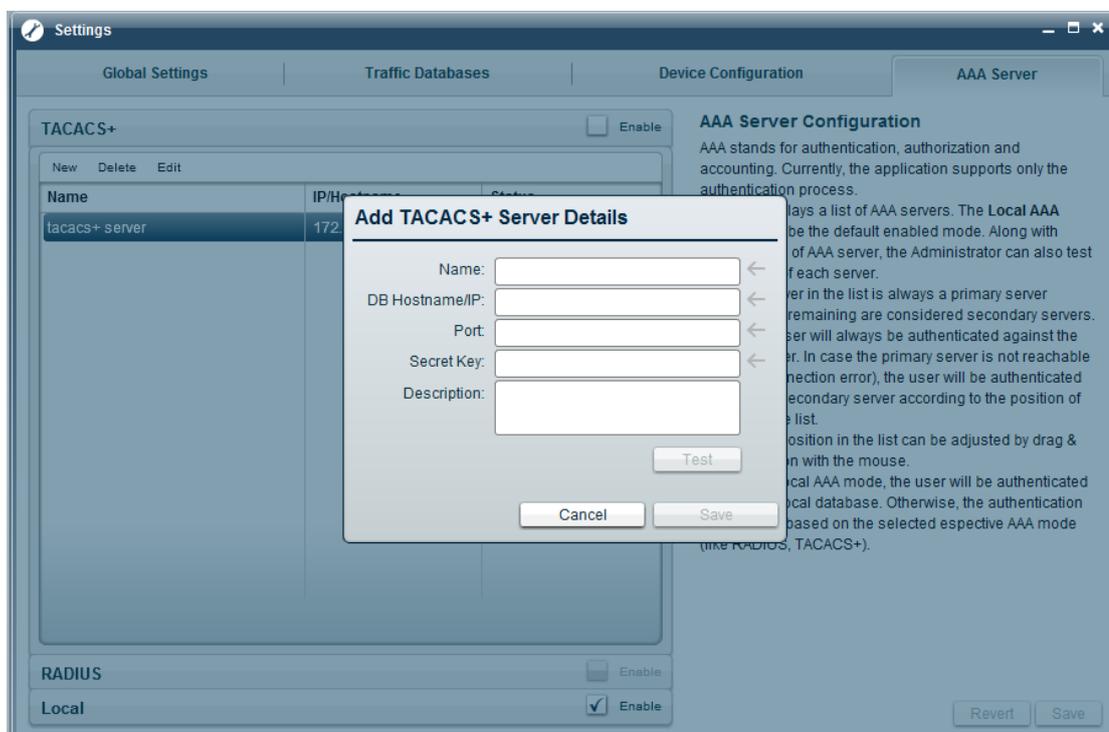
3.5.1 Configure a new Server

To add a new server, perform the following steps:

Step 1 Choose an authentication mode between TACACS+ or RADIUS.

Step 2 Select the **New** option. On clicking, following pop-up will appear:

Figure 23. Configuring a New Server



Step 3 Enter the required server information such as **Name**, **DB Hostname/IP address**, **Port**, **Secret Key**, and **Description**.

Step 4 Click the **Test** button to test the connection status.

Step 5 Click the **Cancel** button to return to the previous page, or click the **Save** button to confirm.



Note

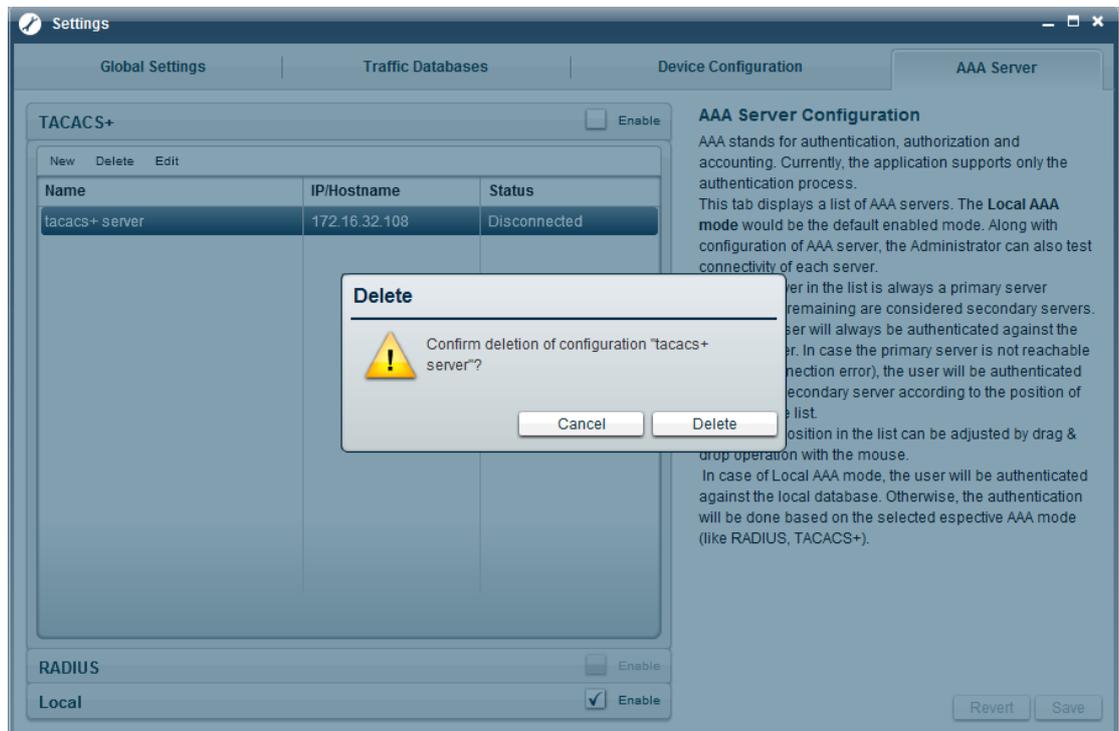
Each mode except Local can have maximum five AAA servers by default.

3.5.2 Delete an existing Server

To delete an existing device, perform the following steps:

- Step 1** Choose an authentication mode between TACACS+ or RADIUS.
- Step 2** Select the server from the list of servers.
- Step 3** Select the **Delete** option. A **Confirm deletion** dialog box appears asking user to confirm the deletion.

Figure 24. Delete a Server



- Step 4** Click the **Cancel** button to return to the previous page, or click the **Delete** button to delete.



Note

Unless there are other configured AAA servers supporting a specific authentication mode, an AAA server cannot be deleted until all accounts utilizing that mode have been removed or migrated to a different authentication mode.

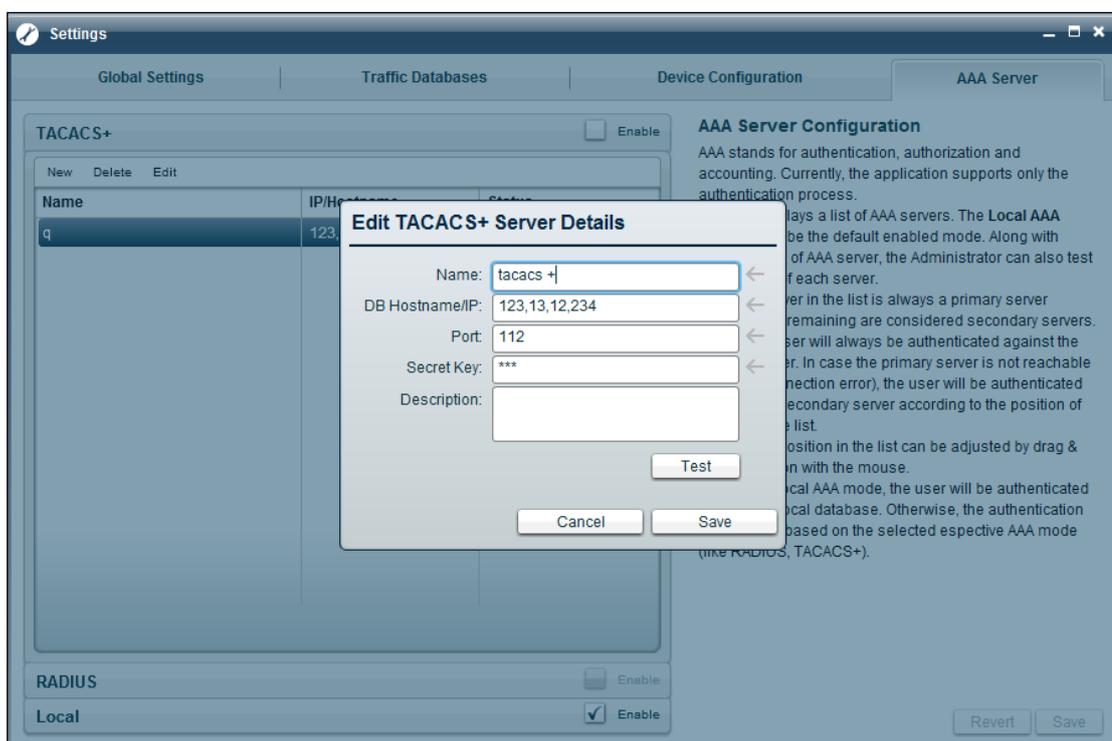
3.5.3 Edit an existing server

To edit an existing server, perform the following steps:

Step 1 Choose an authentication mode between TACACS+ or RADIUS.

Step 2 Select the **Edit** option. On clicking, following pop-up will appear:

Figure 25. Edit an existing Server



Step 3 Edit the required server information such as **Name**, **DB Hostname/IP address**, **Port**, **Secret Key** and **Description**.

Step 4 Click the **Test** button to test the connection status.

Step 5 Click the **Cancel** button to return to the previous page, or click the **Save** button to confirm.

Click the **Save** button to confirm the changes in settings or click **Revert** button to revert the changes.



CHAPTER 4. Network Wizard

4.1 Introduction

The **Network Wizard** is used to create and manage networks of devices by defining the topology structure of the deployment and providing all mandatory settings.

After the configuration of external databases is complete and all devices (SCEs) are provisioned, the administrator can create a list of networks. Networks are used to group devices sharing the same configuration in order to produce reports for aggregated traffic.

Administrators can add networks and group devices for reporting. Each device to be used in reporting must be associated to at least one network. The network definition includes the device topology and service or application hierarchy. A service or application hierarchy of a network is the service or application definition of its Master device on the Traffic Database.



Note

The Cisco Insight Reporter currently works with Networks containing only one type of devices (no mixed-device networks).

Data can only be aggregated for devices belonging to same network.

Network cannot be made of devices whose information is stored on different traffic DBs. Thus traffic can be aggregated only for devices whose data is stored on a specific DB and belonging to the same Network.

It contains the following sections:

- Defining a Network
- Managing Network Devices
- Setting the Master Device
-
- Defining Device Topology
- Defining Service Hierarchy
- Managing Report Filters
-
- Assigning Custom Colors

4.2 Defining a Network

Networks are the source of the data traffic information required for reporting. Users must define a network connection before running a report.

To access and display the **Network** tab, click the **Network Wizard** icon on the Module Launcher.

In this tab, the user can:

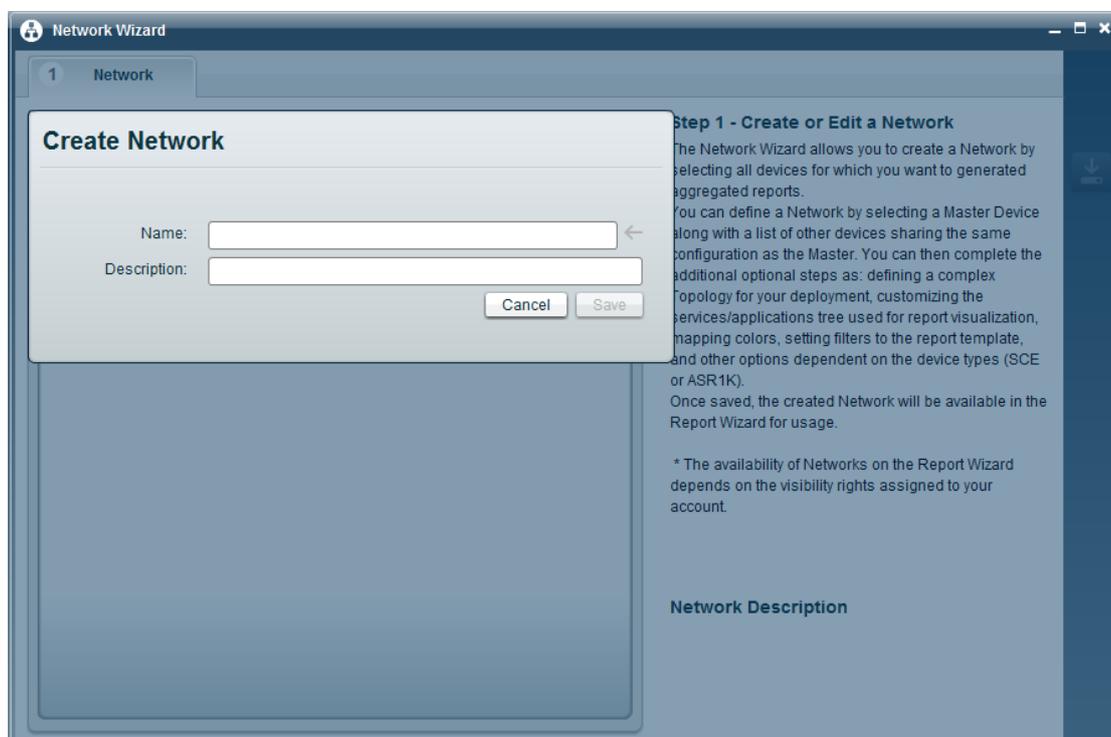
- Configure a New Network

4.2.1 Configure a New Network

To configure a new network, perform the following steps:

Step 1 Choose the **New** option. After user selects the **New** option in the **Network** tab, following screen will appear:

Figure 26. Defining a Network



- Step 2** Enter the **Name** and **Description** of the network to be configured.
- Step 3** Click the **Cancel** button to return to the previous page, or click the **Save** button to confirm.

4.2.2 Edit an existing Network

To edit an existing a network, perform the following steps:

- Step 1** Choose the **Edit** option. On clicking, following screen will appear:

Figure 27. Edit an existing Network



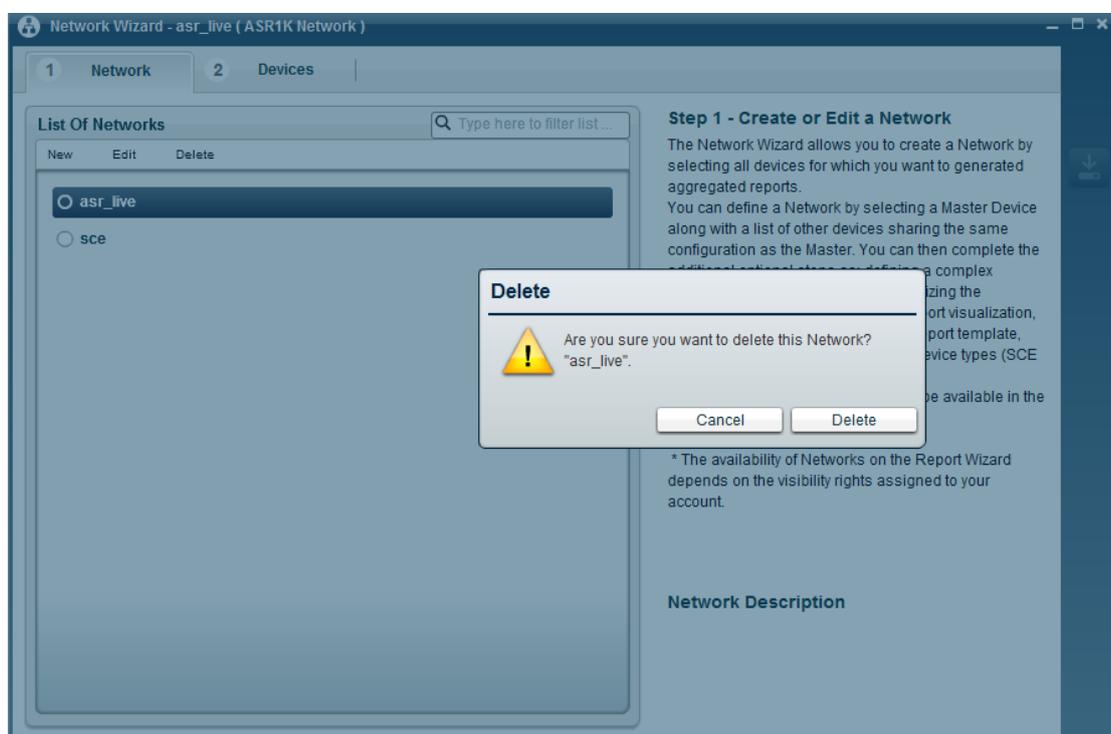
- Step 2** Enter the **Name** and **Description** of the network to be configured.
- Step 3** Click the **Cancel** button to return to the previous page, or click the **Save** button to confirm.

4.2.3 Delete an existing Network

To delete a network, perform the following steps:

- Step 1** Select the network from the list of networks.
- Step 2** Select the **Delete** option. A **Confirm deletion** dialog box appears asking user to confirm the deletion.

Figure 28. Delete a Network



- Step 3** Click the **Cancel** button to return to the previous page, or click the **Delete** button to delete.



Note

Network deletion can lead to following consequences:

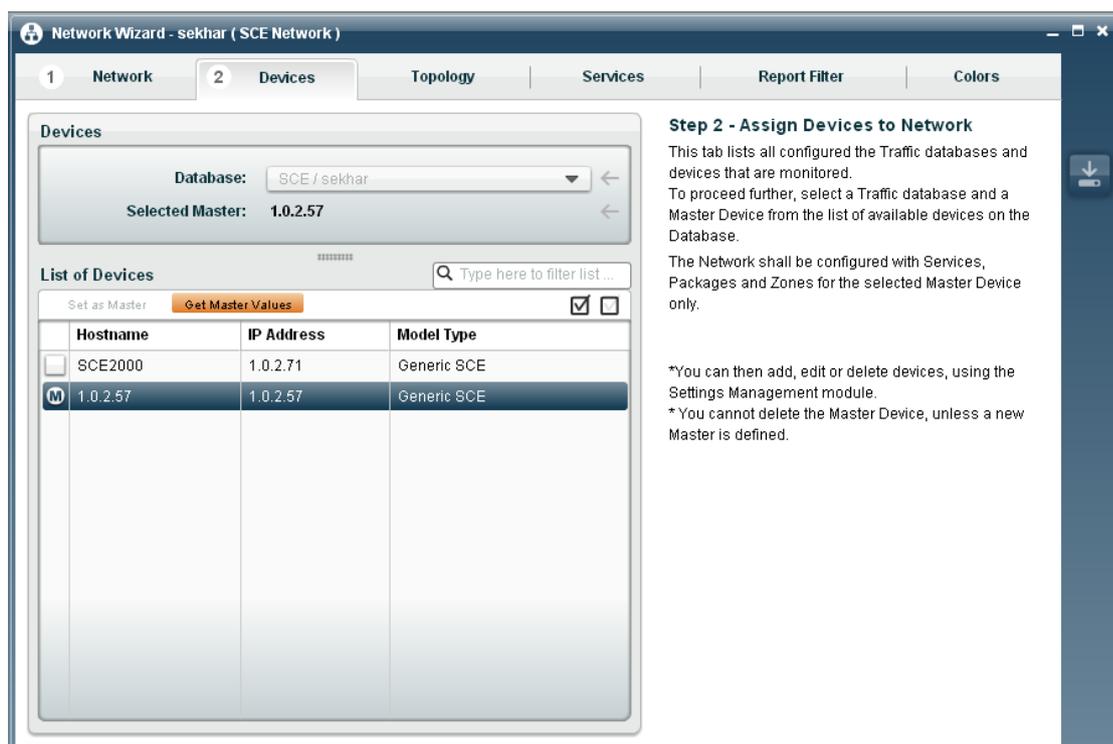
- It deletes scheduled reports on the same network.
- It vanishes all reports related to that network and configured on the Dashboard
- It deletes all entries of My Favorites reports of the specific network.

4.3 Managing Network Devices

The **Devices** tab displays all configured databases and devices, enables to report on data traffic information of the selected devices.

To access and display the **Devices** tab, click the **Network Wizard** icon on the Module Launcher. The **Device** tab displays devices related to selected database in **Network** tab. On clicking the **Device** tab, following screen will appear:

Figure 29. Devices



4.3.1 Setting the Master Device

Master device is the device which configurations & settings will be applicable to all the devices.

After user selects the device, he should select a master SCE, to be used as reference for the service configuration. All devices of a particular network should share the same configuration services or applications, of which, user can select one of the device as a Master device.

The Network uses this device as a reference device and creates service tree, packages, and zones in case of SCE networks.

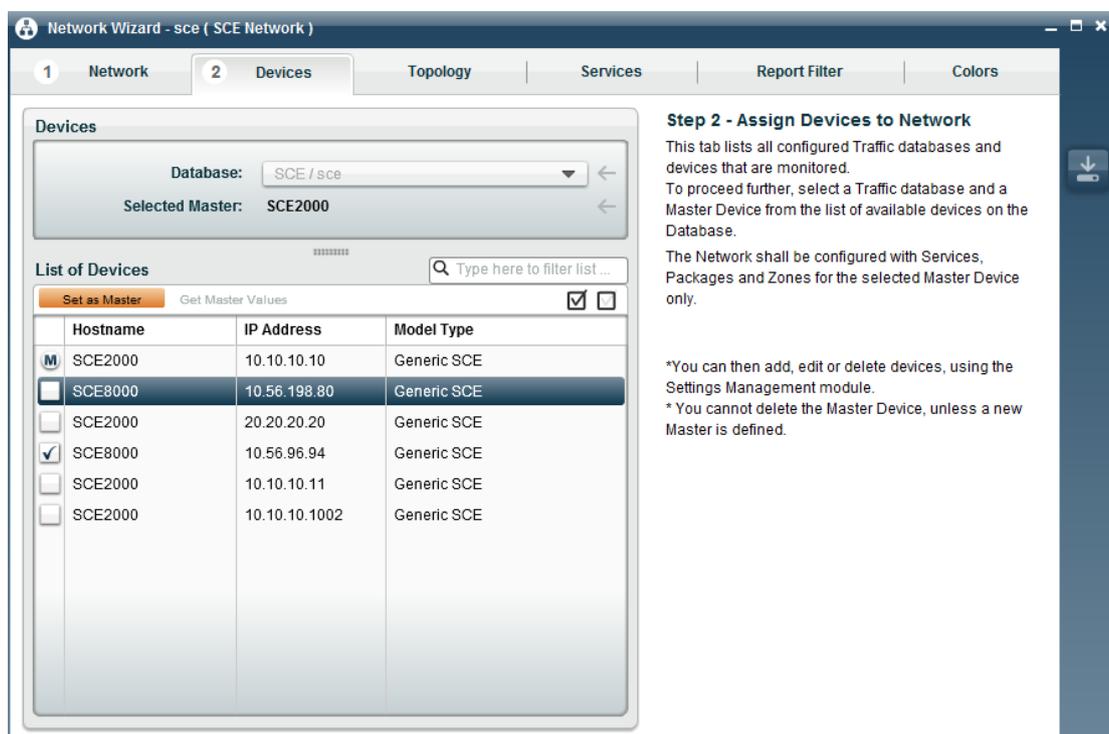
To set a Master device, perform the following steps:

Step 1 Select the device to be set as master.

Step 2 Click **Set as Master**.

When user sets a Master device, following screen will appear:

Figure 30. Setting Master Device (SCE)



The device which is set as **Master Device** will contain  icon.



Note

User **cannot delete** the Master device, unless a new Master is defined.

4.4 Defining Device Topology

The **Topology** tab enables the user to create a topology tree where he can view selected network per device or per custom view. The topology tree (devices or custom) allows the user to expand or hide trees to achieve the right view on the chart.

To access and display the **Topology** tab, click on the **Network Wizard** icon on the Module Launcher.

In this tab, the user can select from following views:

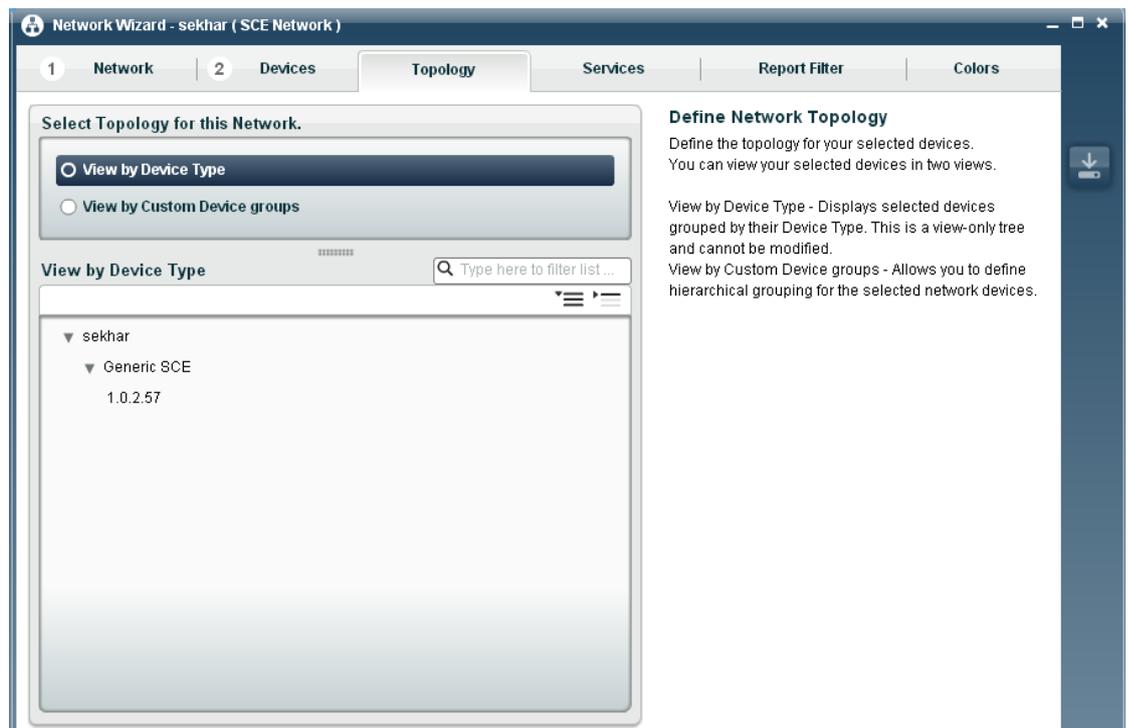
- [View by Device Type](#)
- [View by Custom Device Group](#)

4.4.1 View by Device Type

The **Device View** option displays a pre-defined structure of the networks. User cannot edit or change this view because it is automatically configured.

On selecting **View by Device Type**, following screen will appear:

Figure 31. Device Type View



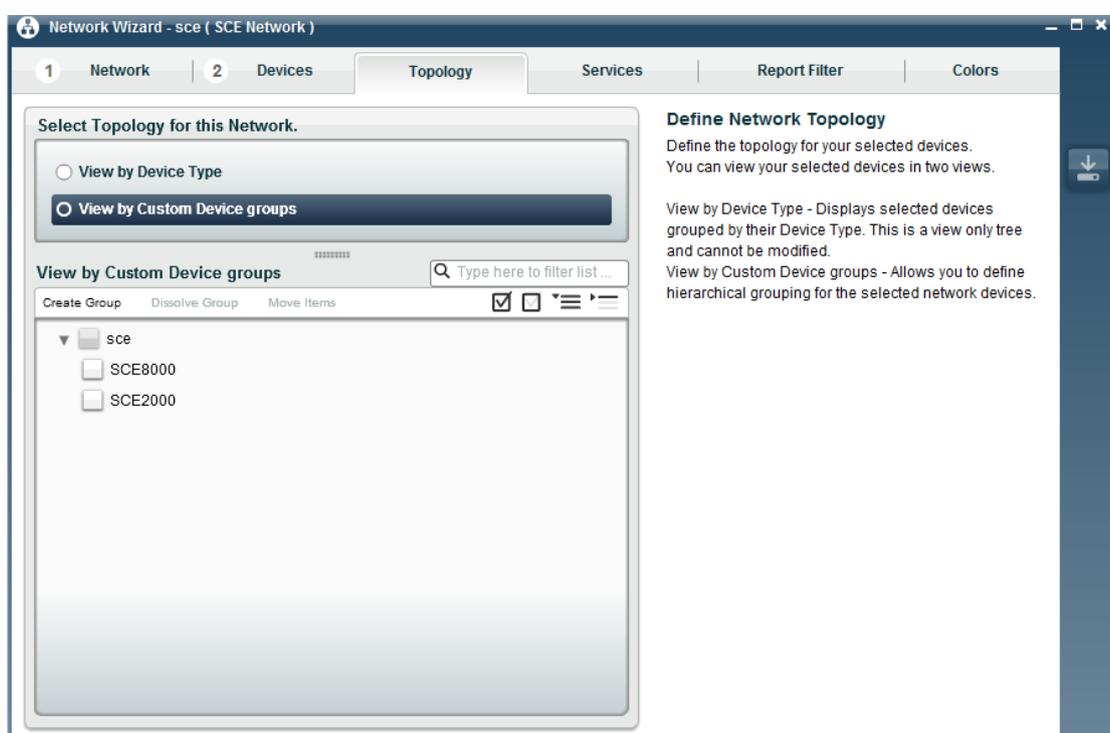
4.4.2 View by Custom Device Group

The **Custom Device View** is used to group network devices according to the customer needs. This view is represented by a hierarchical tree structure. User can define new levels of aggregations and arrange devices (SCEs) in logical groups (that is, POPs, cities, regions etc.). In such tree structures, the root element is the network name, the SCEs are the leaves of the hierarchical tree, and intermediate nodes may represent the geographical aggregations. All nodes can be collapsed or expanded down to the device level.

As soon as a network is defined, the custom view of the topology is just a flat tree containing all the devices as children elements of a unique node (the network name).

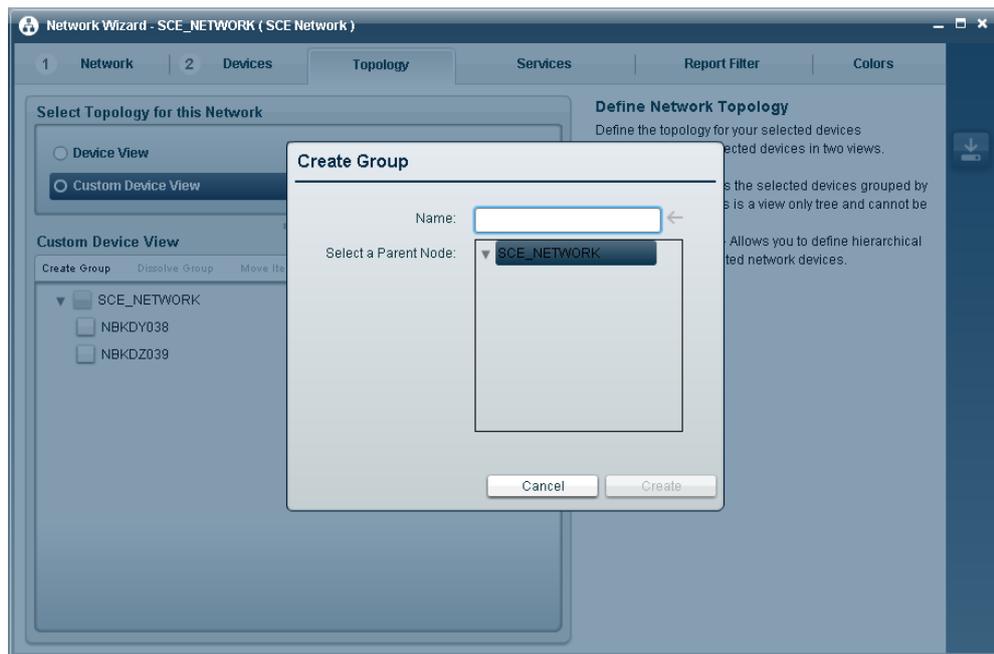
On selecting the **Custom Device View**, following screen will appear:

Figure 32. Custom Device View



To define a **Custom Device**, perform the following steps:

-
- Step 1** Select the **Network** (for example, Mobile) to create the groups by region,
 - Step 2** Select **Create Group**. A new window appears.

Figure 33. Create Group

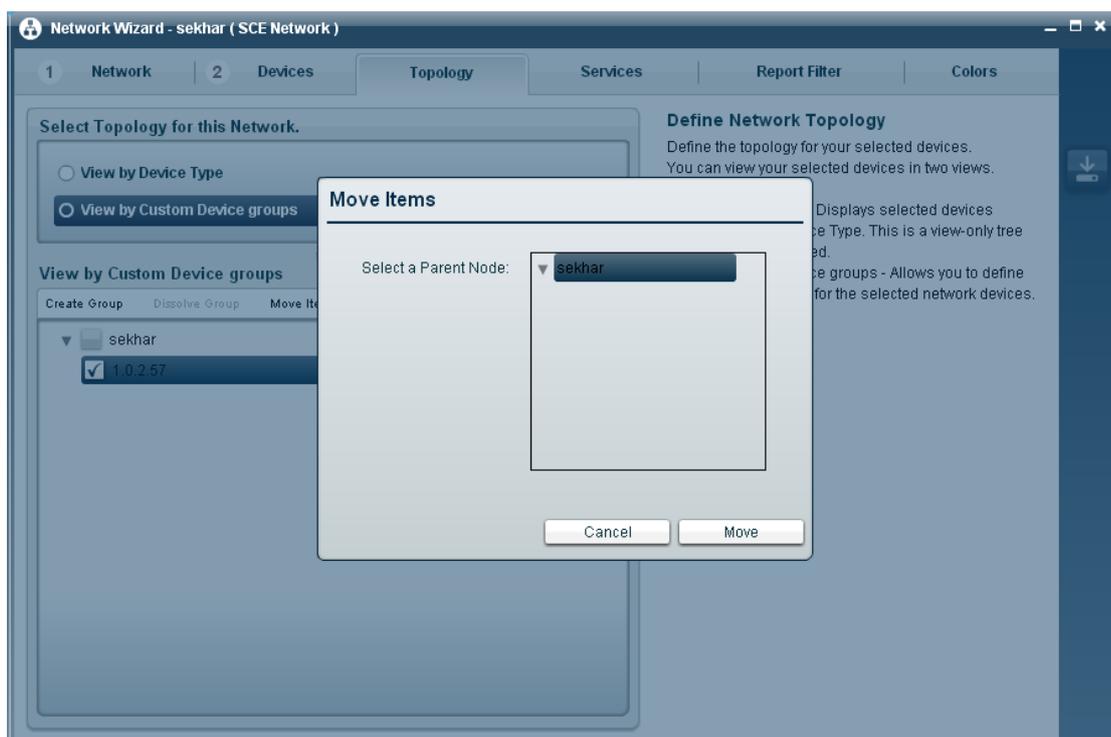
- Step 3** Enter the **Name** of the group (for example, East Coast, West Coast etc).
- Step 4** Select the parent node in **Select a Parent Node** drop down.
- Step 5** Click the **Cancel** button to return to previous page, or click the **Save** button to confirm.

**Note**

Follow the same procedure, if user wants to add more groups at the same level.

To Move Items, following are the steps:

- Step 1** Check the check boxes for the SCEs that user wants to move under the subgroups.
- Step 2** Select **Move Items**. A new window appears.

Figure 34. Move Items

Step 3 Select the **Parent Node** to move the items.

Step 4 Click the **Cancel** button to discard changes, or click the **Move** button to confirm. All the devices get listed under the selected parent node.

To dissolve a group, following are the steps:

Step 1 Select the group that user wants to dissolve.

Step 2 Select **Dissolve Group**. The group will be deleted.



Note

There is no limit to the number of elements contained within a specific level, because there is no limit to the number of intermediate levels.

4.5 Defining Service Hierarchy

Using the service tree, user can view the selected services per service families or per custom services. The service tree (service families or custom) allows user to expand or contract trees to achieve a right view on the chart.

When working on a specific service configuration, the list of services can be represented using two different views:

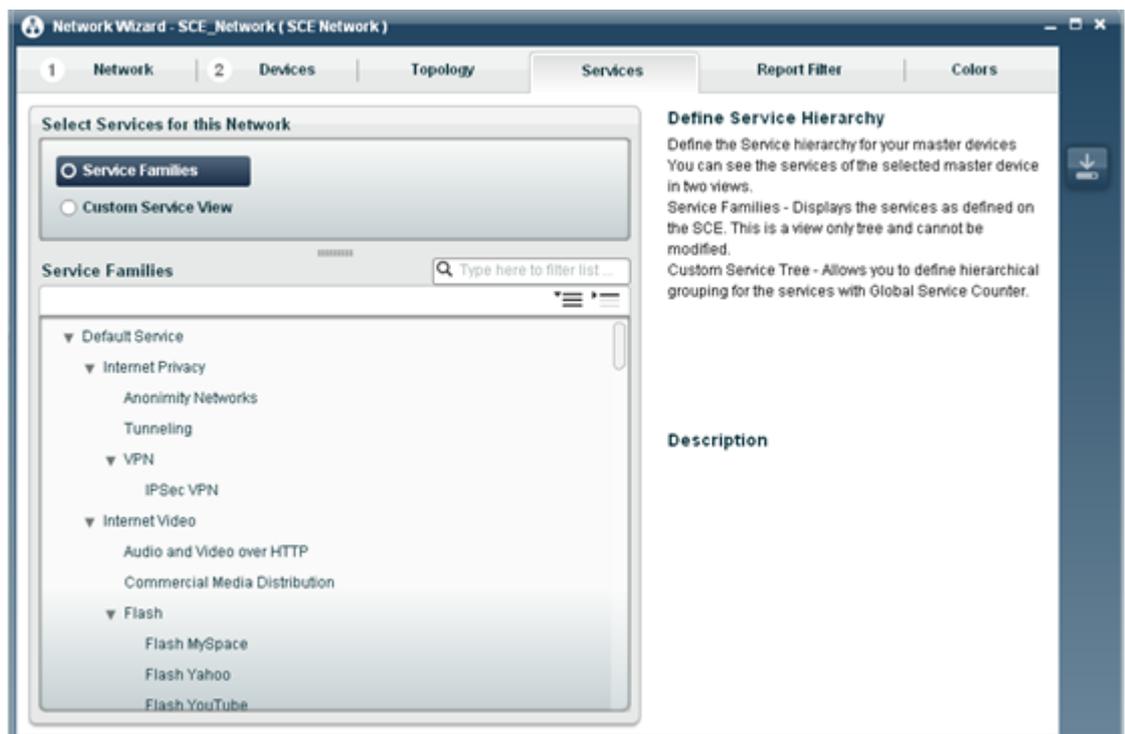
- Service Families
- Custom Service View

4.5.1 Service Families

The **Service Families** view represents a hierarchical description of network services.

When user selects the service family view, following screen will appear:

Figure 35. Service Families



4.5.2 Custom Service View

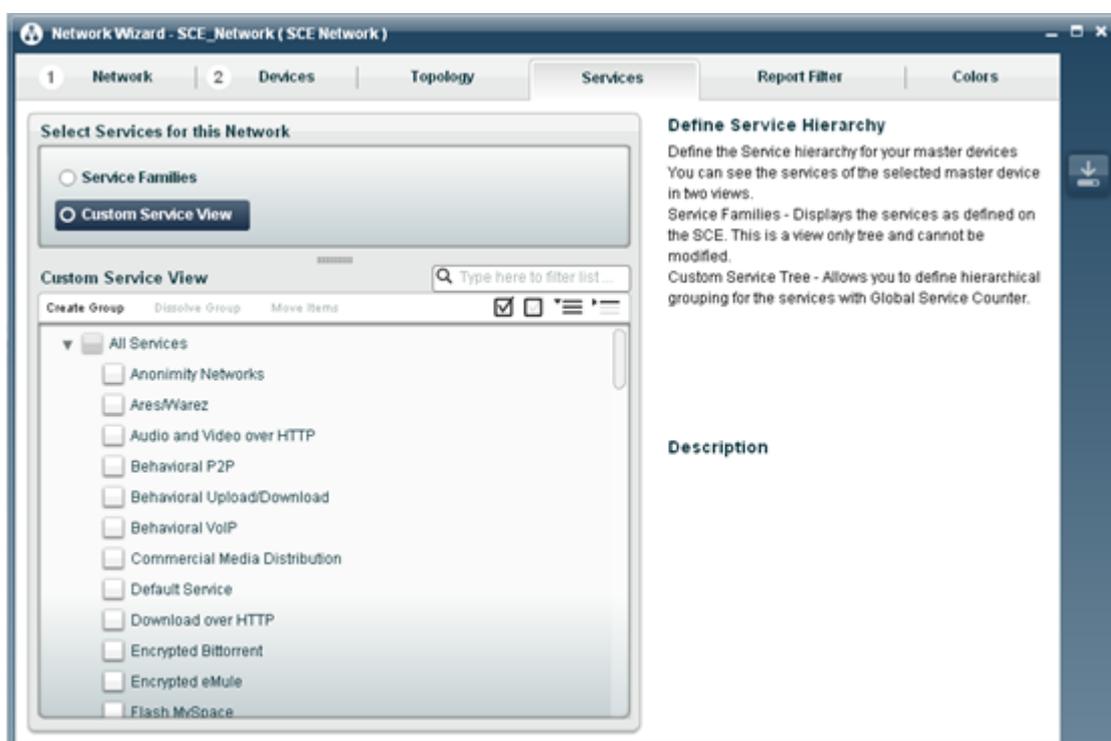
Custom Service View is used to define a new visualization option for grouping services without changing the SCE configuration.

By defining a custom service tree, user can create new service families based on other aggregation criteria than those defined in the SCE service configuration.

When a new custom tree is defined, by default, all services are placed under a default family. Then, each user can start creating customized service families, and services can be arranged following different aggregation logics.

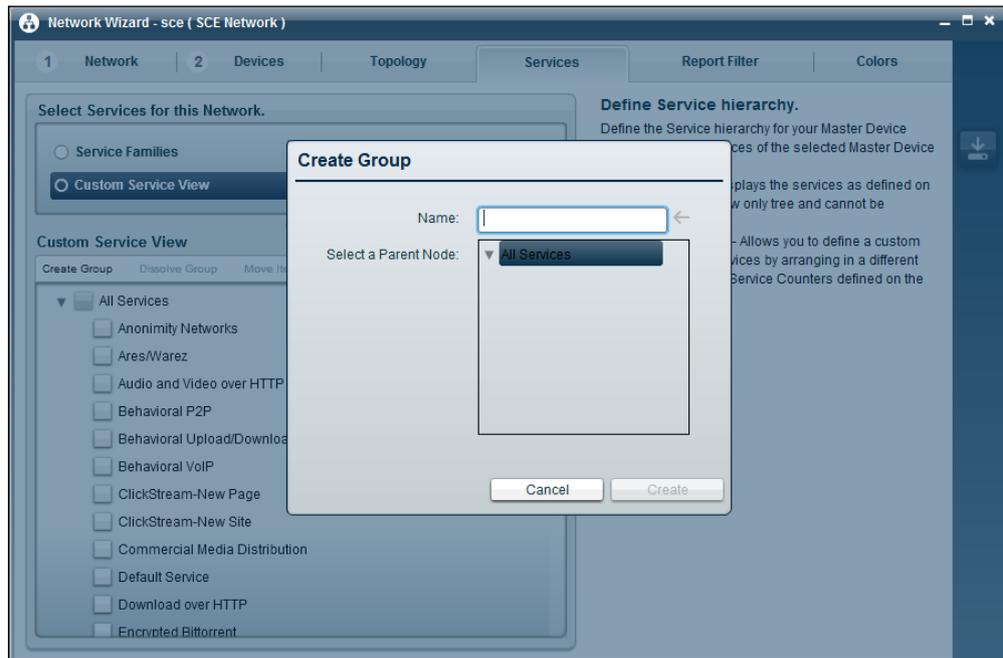
When user selects the **Custom Service View**, the following screen will appear:

Figure 36. Custom Service View



To customize a service tree, perform the following steps:

- Step 1** Select the services to make a group.
- Step 2** Select the **Create Group** option. A new window appears.

Figure 37. Custom Service View

Step 3 Enter the **Name** of the group.

Step 4 Select a parent node in **Parent node** drop down.

Step 5 Click the **Cancel** button to discard changes, or click the **Save** button to confirm.



Note

To add more groups, just repeat the same procedure.

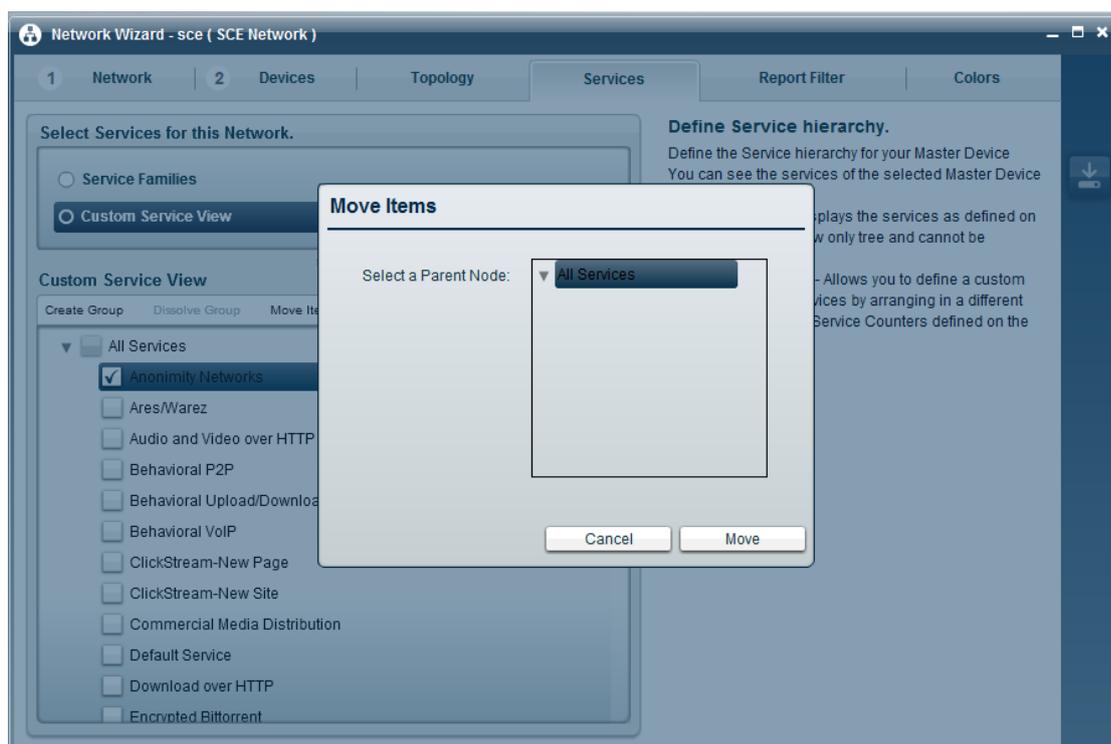
To dissolve a group:

Step 1 Select a group to dissolve.

Step 2 Select the **Dissolve Group** option. The group will be deleted.

Step 3 Select the services that user wants to move under the subgroups.

Step 4 Select **Move Items**. A new window appears.

Figure 38. Custom Service View

Step 5 Select the **Parent Node**.

Step 6 Click the **Cancel** button to return to previous page, or click the **Move** button to confirm. All the services will get listed under the group.



Note

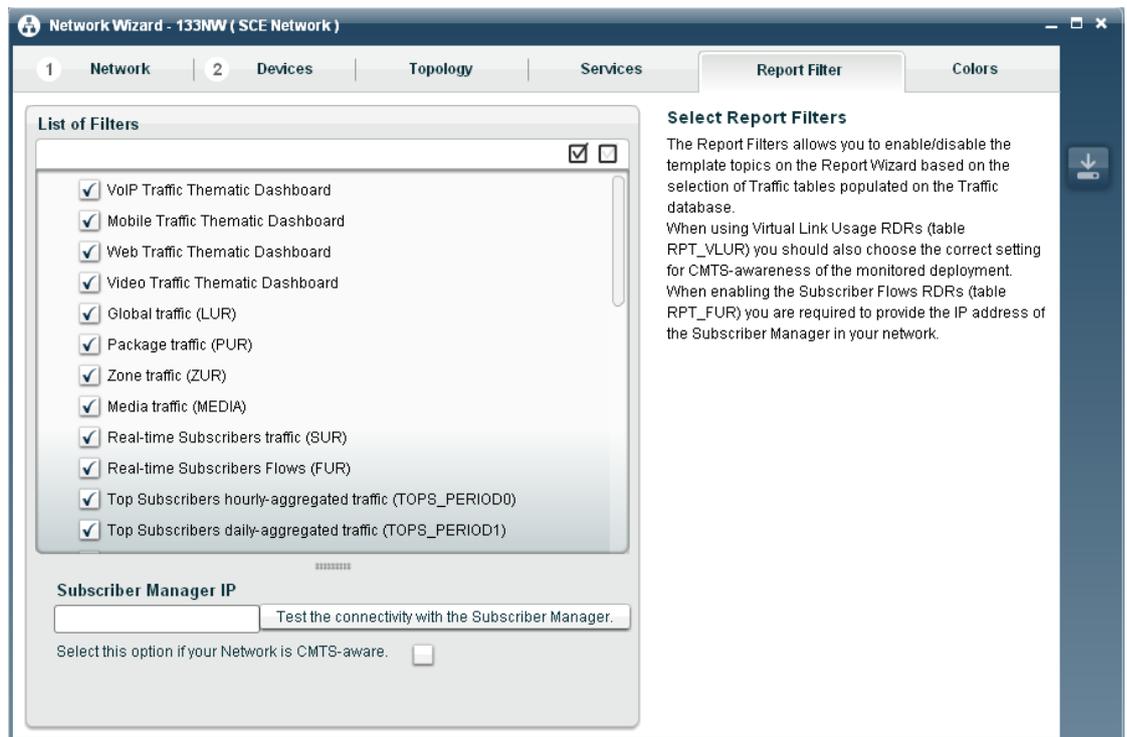
Users will be able to see the Services Tab only when a SCE Network is selected.

In case of changes to the SCE configuration, the application updates the service tree as well as the custom service tree. But in the custom service tree, if any new service has been configured, that service will be added directly to the root node. The application expects from the user, he/she should put new service under the correct custom group otherwise the new service become itself a self-containing group

4.6 Managing Report Filters

The **Report Filter** tab provides the ability to filter out all the report topics and report families.

Administrators can use this tab to manually set the mapping between the available report templates based on the SCE or CM configuration for the selected network.

Figure 39. Report Filters

When working with the latest CM database schema, the available configuration options for the report template filters are:

Options related to the Thematic Dashboards:

- VoIP Traffic Thematic Dashboard
- Mobile Traffic Thematic Dashboard
- Web Traffic Thematic Dashboard
- Video Traffic Thematic Dashboard

Options related to traffic reports:

- Global traffic (LUR)
- Package traffic (PUR)
- Zone traffic (ZUR)
- Media traffic (MEDIA)
- Real-time Subscribers traffic (SUR)
- Real-time Subscribers Flows (FUR)
- Top Subscribers hourly-aggregated traffic (TOPS_PERIOD0)
- Top Subscribers daily-aggregated traffic (TOPS_PERIOD1)
- Top Subscribers hourly-cumulative traffic (TOPS_PERIOD0_CUMULATIVE)

- Top Subscribers daily-cumulative traffic (TOPS_PERIOD1_CUMULATIVE)
- Top Subscribers peak-hours traffic (TOPS_PEAK_PERIOD)
- Top Subscribers peak-hours cumulative traffic (TOPS_PEAK_CUMULATIVE)
- Malicious traffic (MALUR)
- SPAM traffic (SPAM)
- Statistical Transaction traffic (TR)
- Global Virtual Links traffic (VLUR)
- Subscriber Downstream Virtual Links traffic (DVLINK)
- Subscriber Upstream Virtual Links traffic (UVLINK)
- Top Video Hosts traffic (TOP_VIDEO_HOSTS)
- Top Video Domains traffic (TOP_VIDEO_DOMAINS)
- Top HTTP Hosts traffic (TOP_HTTP_HOSTS)
- Top HTTP Domains traffic (TOP_HTTP_DOMAINS)
- IPv6 traffic (GUR)
- Mobile Top Device Types traffic (TOP_DEVICE_TYPE)
- Mobile Top User Locations traffic (TOP_USER_LOCATION)
- Mobile Top APNs traffic (TOP_APN)
- Mobile Top Network Types traffic (TOP_NETWORK_TYPE)
- Mobile Top SGSNs traffic (TOP_SGSN)
- Mobile - CDMA Top Home Agents traffic (TOP_HOME_AGENT Table)
- Mobile - CDMA Top Device Types traffic (TOP_MEID Table)
- Mobile - CDMA Top PCFs traffic (TOP_SGSN Table)
- OS Finger Prints (RPT_OSFP Table)



Note

If SCEs are configured in **Asymmetric Routing Traffic** operational mode, it is possible to disable some reports by un-checking the appropriate filters (for example, transactional traffic information).

4.7 Assigning Custom Colors

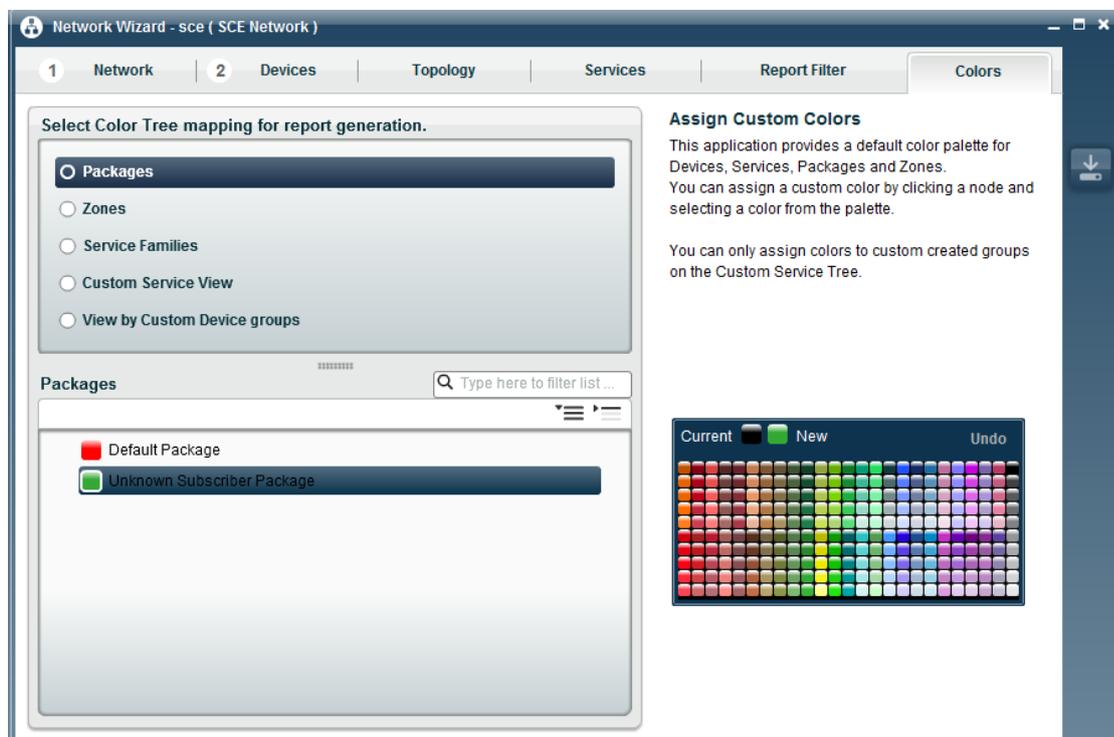
Cisco Insight Reporter provides a default color palette, but user can customize the color of the chart series in following way:

- The associated color to specific element of SCE configuration can be changed permanently in **Colors** tab of Network Wizard.
- The associated color can be changed using the interactive GUI. The change does not impact the global settings, but reflects only on the specific report tab and its export formats.

For SCE based networks user can change the color of the services, zones, packages, and topology elements by clicking the colored boxes for each node.

To change the color of a node, click on the color box of the node, after clicking a color palette will appear. User can select new color from the color palette.

Figure 40. Assigning Custom Colors



Step 1 Click the color icon that user wants to change. It will open the color palette.

Step 2 Select the new color in color palette.

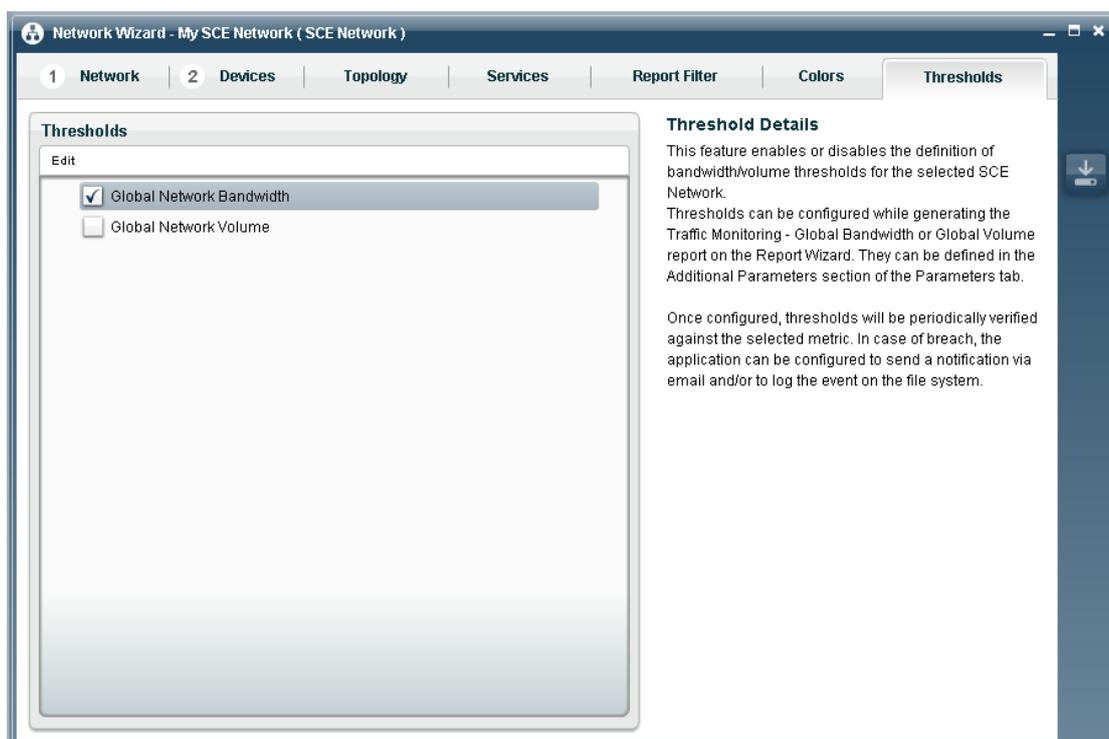
4.8 Monitoring Traffic Thresholds

Cisco Insight Reporter now supports monitoring bandwidth and volume thresholds for global traffic at the Network level.

If this feature is enabled, the volume and/or bandwidth generated for all the SCE Network will be monitored against a specific threshold. If that threshold is breached, all users that have visibility on that Network and have the “Notify me of Errors” flag active on their Personal Profile, will get an email notification.

The breach event can also be logged on the application log, on the local file system.

Global Thresholds for bandwidth and volume can also be plotted on bandwidth/volume charts of the Traffic Monitoring → Global → Bandwidth and Traffic Monitoring → Global → Volume topics, under the Report Wizard.

Figure 41. Enabling Thresholds on Network Wizard

When selecting the global bandwidth or volume threshold and clicking on the **Edit** button, you can define the threshold's parameters, as described below:

- **Limit:** value of the threshold, expressed in the selected units
- **Aggregation:** time granularity of samples. Thresholds will be compared with traffic samples calculated with the selected granularity. (e.g. if setting the aggregation to "1 hour", the average hourly bandwidth/volume will be compared against the threshold value)
- **Monitoring Period:** the time span of data traffic examined to evaluate the threshold breach.
- **Frequency:** the frequency of verification of the query for possible threshold breaches.
- **Send Alarm flag:** if active, threshold breaches will be notified via email (the application shall be configured to send email messages)
- **Logged flag:** if active, threshold breaches will be logged in the application log, on the local file system.

Figure 42. Configure the Bandwidth Global Threshold for the selected Network

Edit Threshold -Global Network Bandwidth

Limit: 100 Mbps

Aggregation: none

Monitoring Period: 1 hours

Frequency: 15 mins

Send Alarm:

Logged:

Cancel Save

Figure 43. Configure the Volume Global Threshold for the selected Network

Edit Threshold -Global Network Volume

Limit: 100 L3Mbytes

Aggregation: 1 hour

Monitoring Period: 1 hours

Frequency: 15 mins

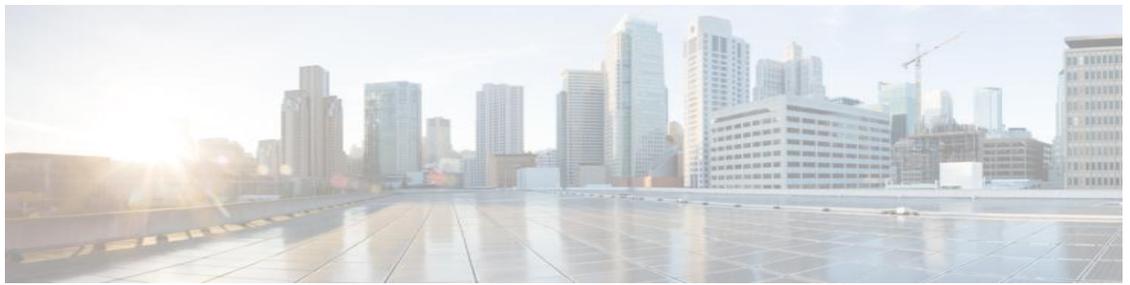
Send Alarm:

Logged:

Cancel Save

To configure and activate the monitoring of the global bandwidth/volume threshold for the selected Network, on the Network Wizard module, follow the steps below:

-
- Step 1** Open the Network Wizard, select a Network and go on the **Thresholds** tab.
 - Step 2** Click on the checkboxes corresponding to the type of thresholds you want to activate on reports.
Available values are:
 - a. Global Network Bandwidth
 - b. Global Network Volume
 - Step 3** Adjust the threshold settings by selecting one element and click on the **Edit** button. A pop-up window will display.
 - Step 4** Configure all required parameters as explained earlier and click on **Save**.
 - Step 5** Save the Network settings
-



CHAPTER 5. Account Management

5.1 Introduction

This chapter describes how to set up user accounts, account groups, roles, and capabilities on the Cisco Insight Reporter application.

Account Management provides a list of functions that allows the setup of user accounts, account groups, their roles, and capabilities.

After platform installation, by default “Super User” role and “Default” account group is provided only to the Super User (cisco).

Roles, Visibility Rights, User Accounts, and Account Groups can be added, updated, or deleted at any time.



Note

Cisco Insight Reporter does not let any user to view the account management objects (Roles/ Visibility Rights/Accounts/ Account Groups) created by any other user. This is for controlling the visibility of these objects across different account Only the default Super User account “cisco” is allowed to see everything.

This chapter contains the following sections:

- Introduction
- Defining a Role
- Defining Account Groups
- Defining Visibility Rights
- Defining an Account
- Viewing Capabilities mapped to Roles
- Editing the Personal Profile

5.2 Defining a Role

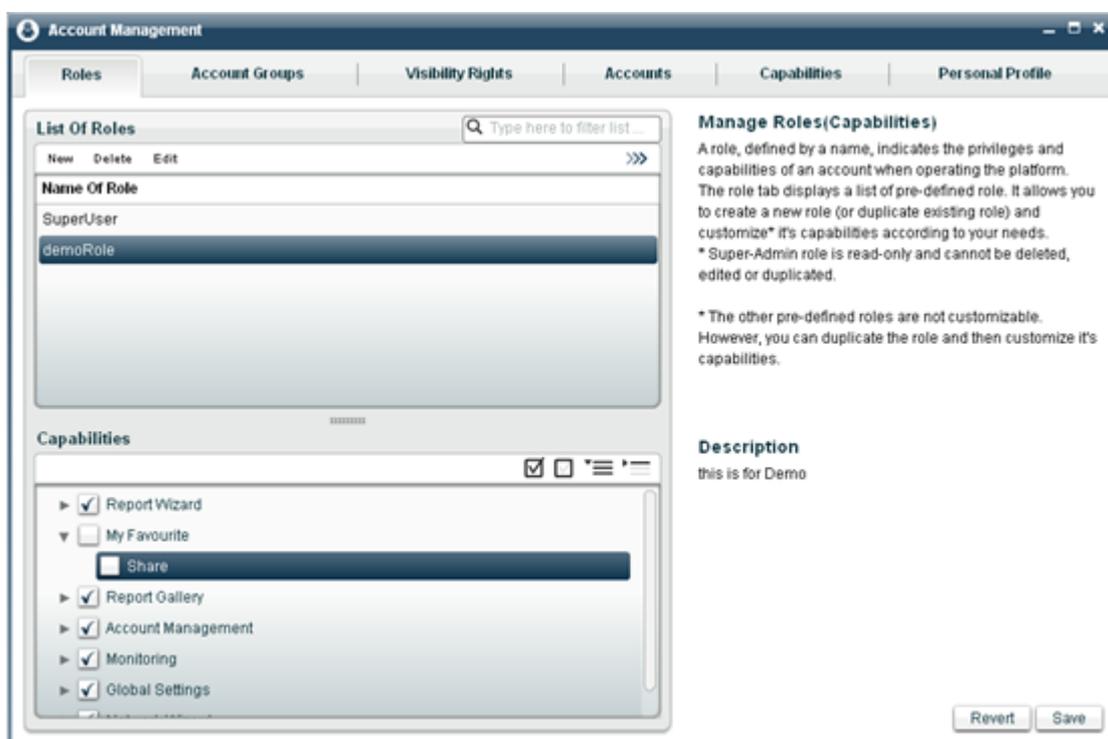
A role, defined by a name, determines the privileges and the capabilities of an account when operating on the platform.

To access and display the **Roles** tab, click the **Account Management** icon on the Module Launcher. This tab has two panes:

- **List of Roles**—Lists all the predefined roles.
- **Capabilities**—Lists all the functions that a role can perform.

On selecting the **Roles** tab, following screen will appear:

Figure 44. Defining Roles

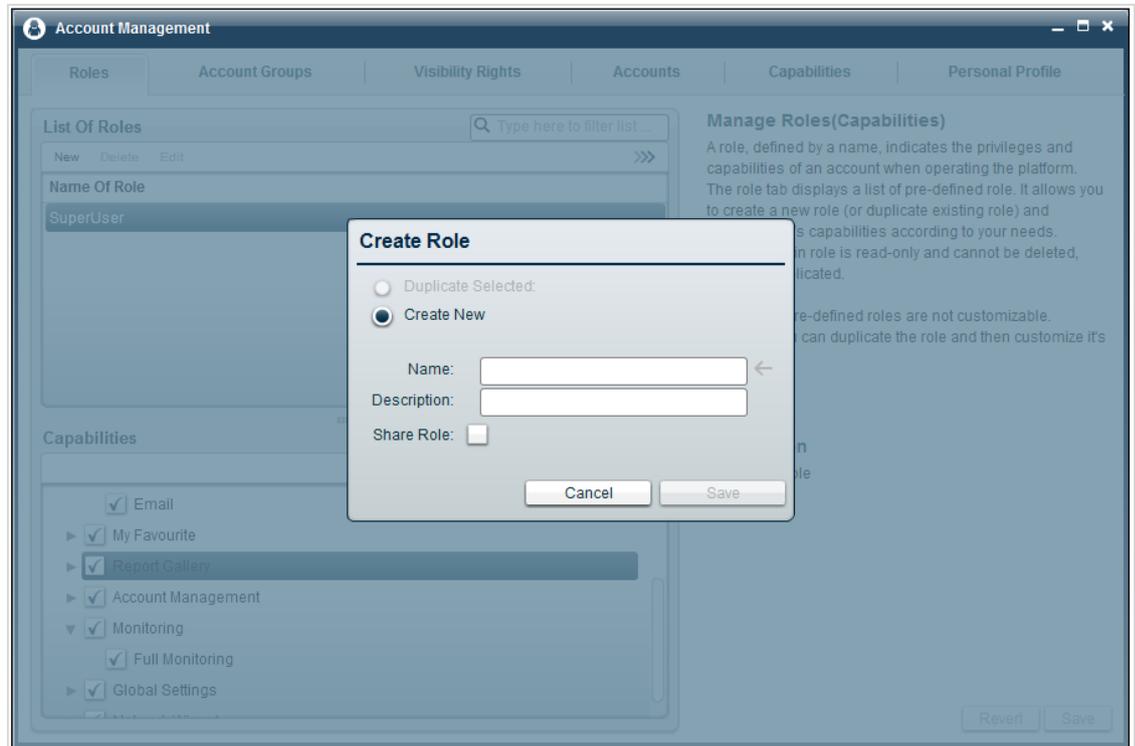


After selecting each role, the **Capabilities** pane displays a list of all functions that a role can perform. A filtering option is also available for easy navigation.

To define a role, perform the following steps:

Step 1 Click the **New** option in the List of Roles pane. A **Create Role** dialog box appears:

Figure 45. Create Roles



Step 2 Select the **Create New** option.



Note

Choose **Duplicate** to create a copy of a pre-defined role and continue with Step 4.

Step 3 Enter the **Name** and **Description** of the role in the respective fields.

Step 4 Click **OK** to confirm, or **Cancel** to return to the previous page.



Note

To edit a role, select the **Edit** option in the List of Roles pane, and perform Step 3 and Step 4 as mentioned above.

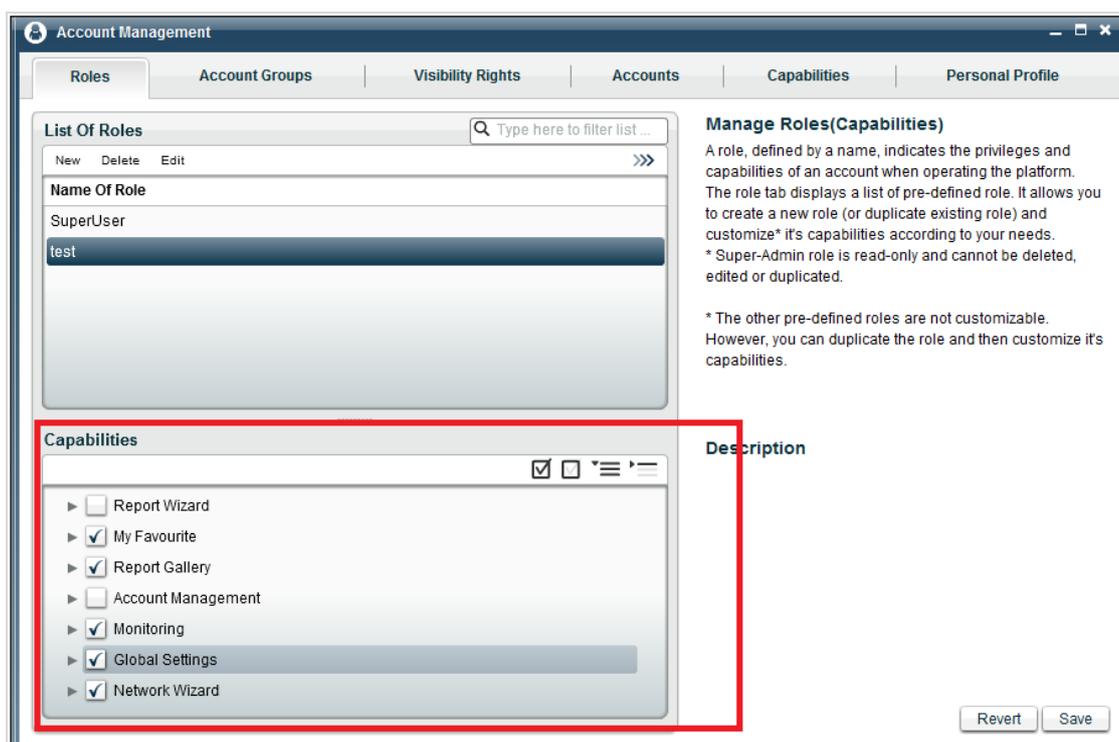
Step 5 On clicking **OK**, the list gets updated. This newly created role cannot perform any task unless it is assigned to do so.

To assign tasks to a role, perform the following steps:

Step 1 Select the role.

Step 2 Check the tasks available in the **Capabilities** pane.

Figure 46. Assign Capabilities



Step 3 Click **Save** to confirm, or click **Revert** to return to the previous page.



Note

User can also delete the role by selecting the **Delete** option in the List of Roles pane.



Note

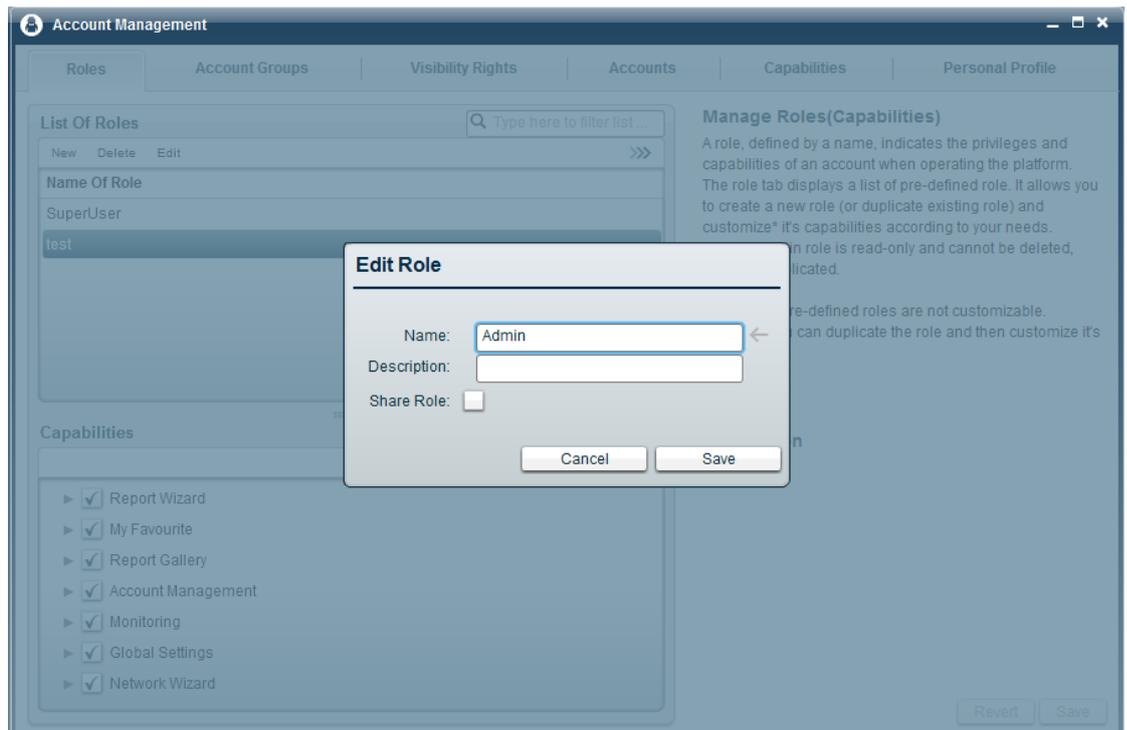
Super user role is read-only and cannot be deleted, changed, or duplicated.

User cannot customize the other predefined roles. However, user can duplicate the role and then customize its capabilities.

To edit a role, perform the following steps:

Step 1 Click the **Edit** option in the List of Roles pane. Following pop-up will appear:

Figure 47. Edit Role



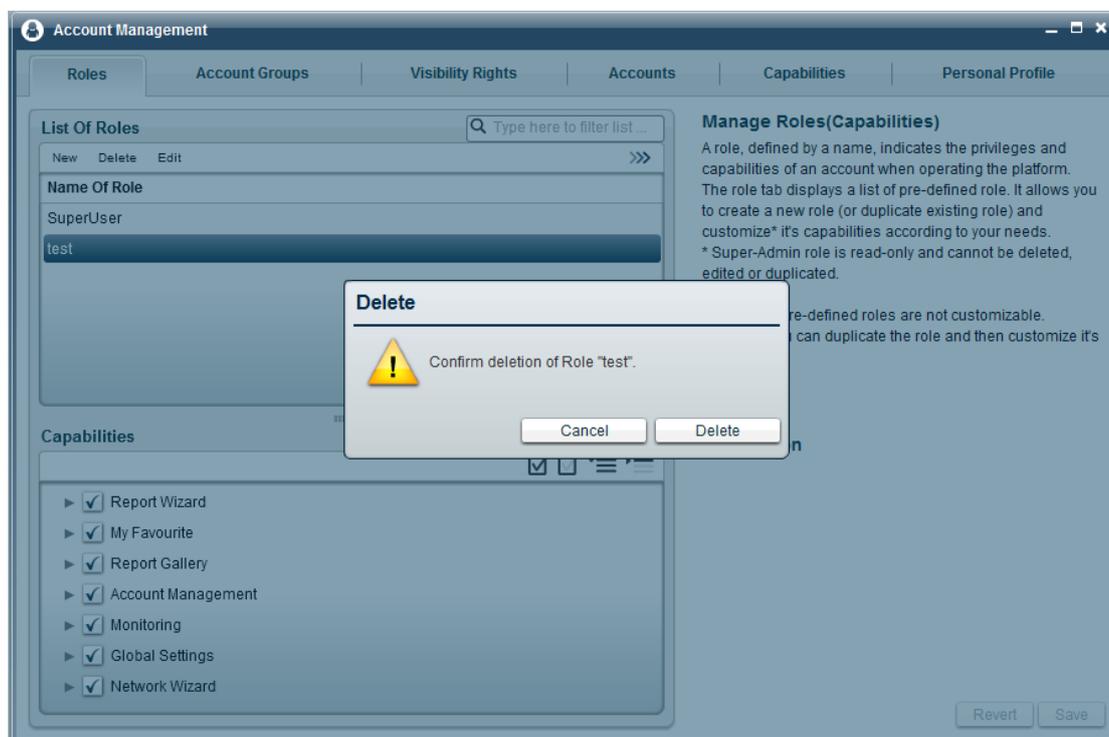
Step 2 Enter the **Name** and **Description** of the role in the respective fields.

Step 3 Click **OK** to confirm, or **Cancel** to return to the previous page.

To delete a role, perform the following steps:

Step 1 Click the **Edit** option in the List of Roles pane. Following pop-up will appear:

Figure 48. Delete Role



Step 2 Select the role to delete.

Step 3 Click **Delete** button.

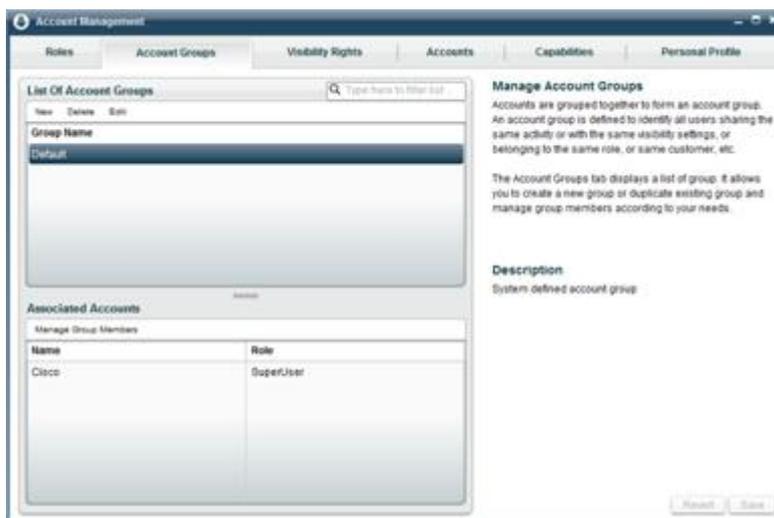
5.3 Defining Account Groups

Accounts are grouped together to form an account group. An account group identifies all users sharing the same activity. Accounts that belong to the same Account Group have the capability to share reports with each other.

To access and display the Account Groups tab, click the **Account Management** icon on the Module Launcher. This tab has two panes:

- **List of Account Groups**—Lists all the predefined account groups.
- **Associated Accounts**—Lists all the accounts that an account group has.

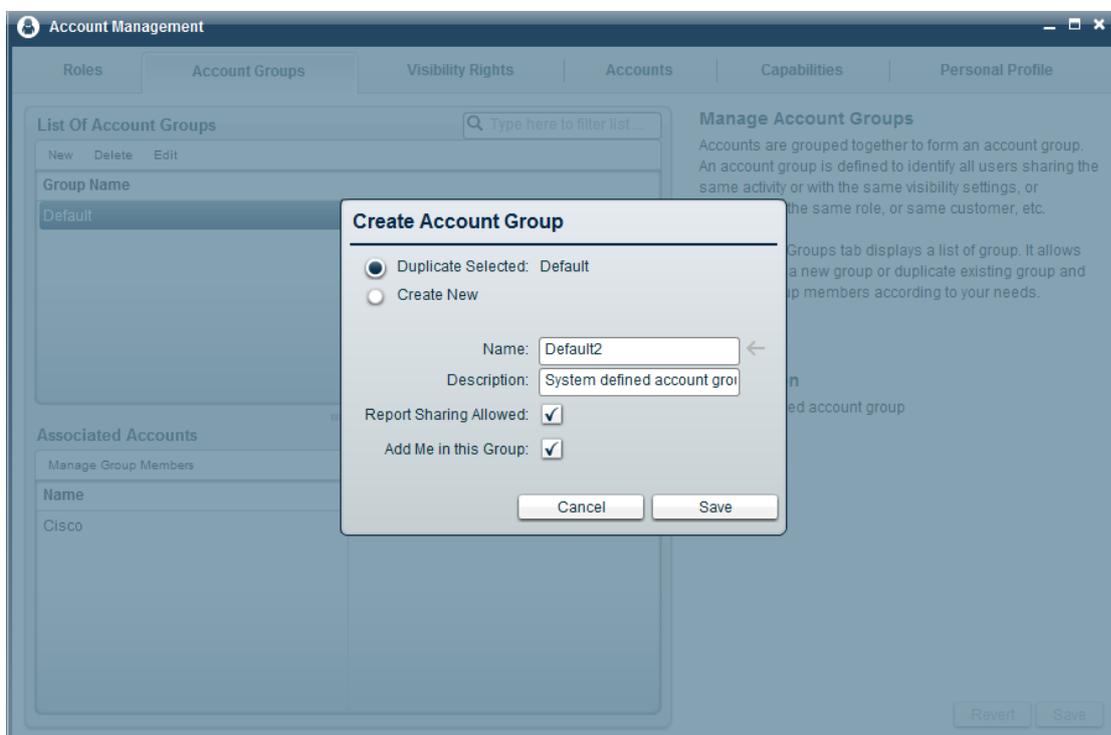
When user selects the **Account Groups** tab, following screen will appear:

Figure 49. Defining Account Groups

To define an account group, perform the following steps:

Step 4 Select the **New** option in the List of Account Groups panel. A **Create Account Group** dialog box appears.

Step 5 Select the **Create New** option. It will display following pop-up:

Figure 50. Defining Account Groups**Note**

Choose **Duplicate** to create a copy of a pre-defined account group and continue with Step 3.

- Step 6** Enter the **Name** and **Description** of the group in the respective fields.
- Step 7** If user wants to share the reports with the members in the group, check the **Report Sharing Allowed** check box.
- Step 8** If user wants to share the reports with the logged in users, checks the **Add me in this Group** check box.
- Step 9** Click **OK** to confirm, or click **Cancel** to return to the previous page.

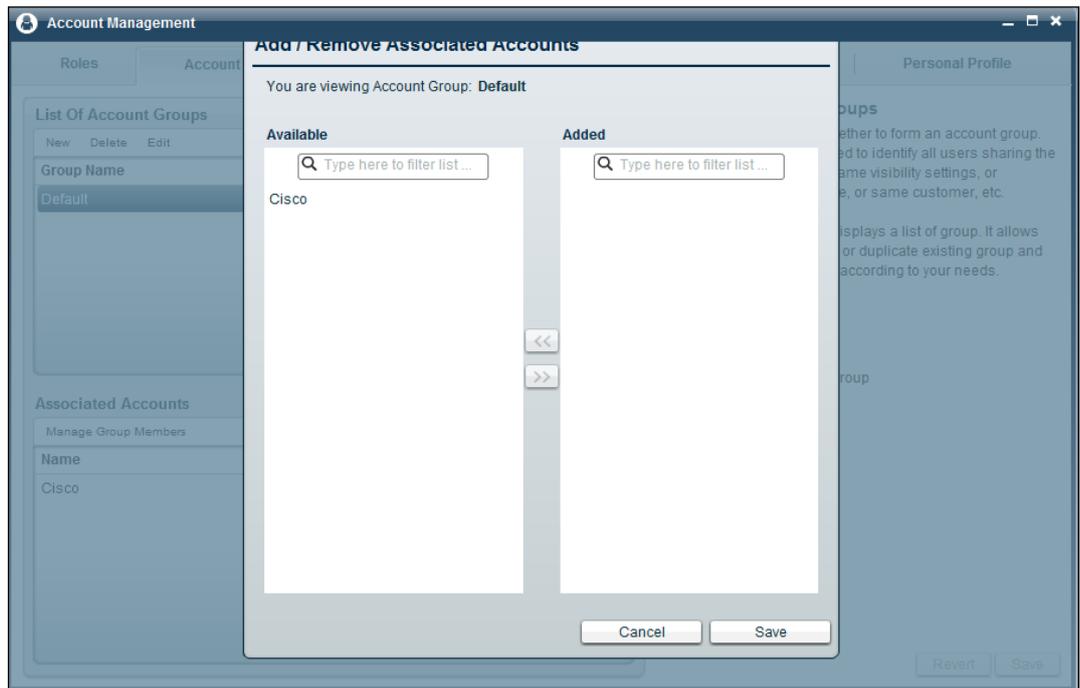
**Note**

To edit the account group, select the **Edit** option in the List of Account Groups pane, and perform Step 3, Step 4, and Step 5 as mentioned above.

When user clicks **OK**, the list gets updated. This newly created account group has no group members.

To add group members to the group, perform the following steps:

- Step 1** Select the group.
- Step 2** Select the **Manage Group Members** option available in the Associated Group pane. A list of available accounts appears in a new dialog box.

Figure 51. Add/Remove Associated Account

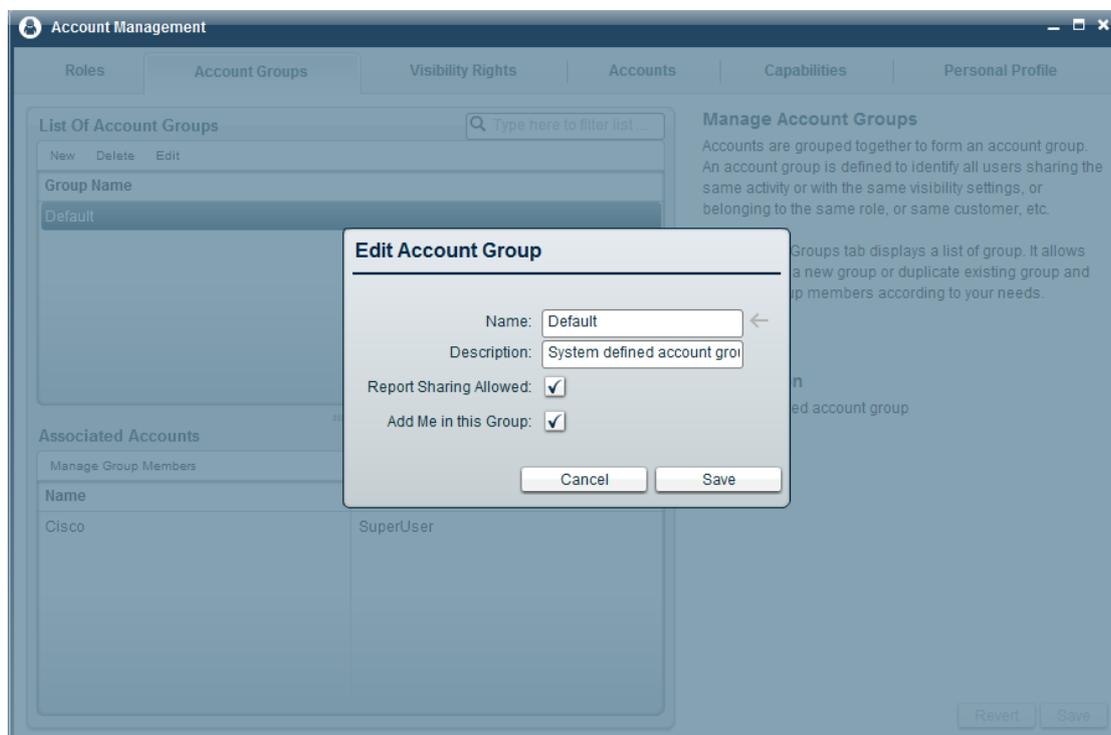
Step 3 Select accounts and move to the right column by using the arrow button.

Step 4 Click **Save** to confirm, or click **Revert** to return to the previous page.

To edit an Account Group, perform the following steps:

Step 1 Select the account group to edit.

Step 2 Click **Edit** button. On clicking following pop-up will appear:

Figure 52. Edit Account Group

Step 3 Edit the details.

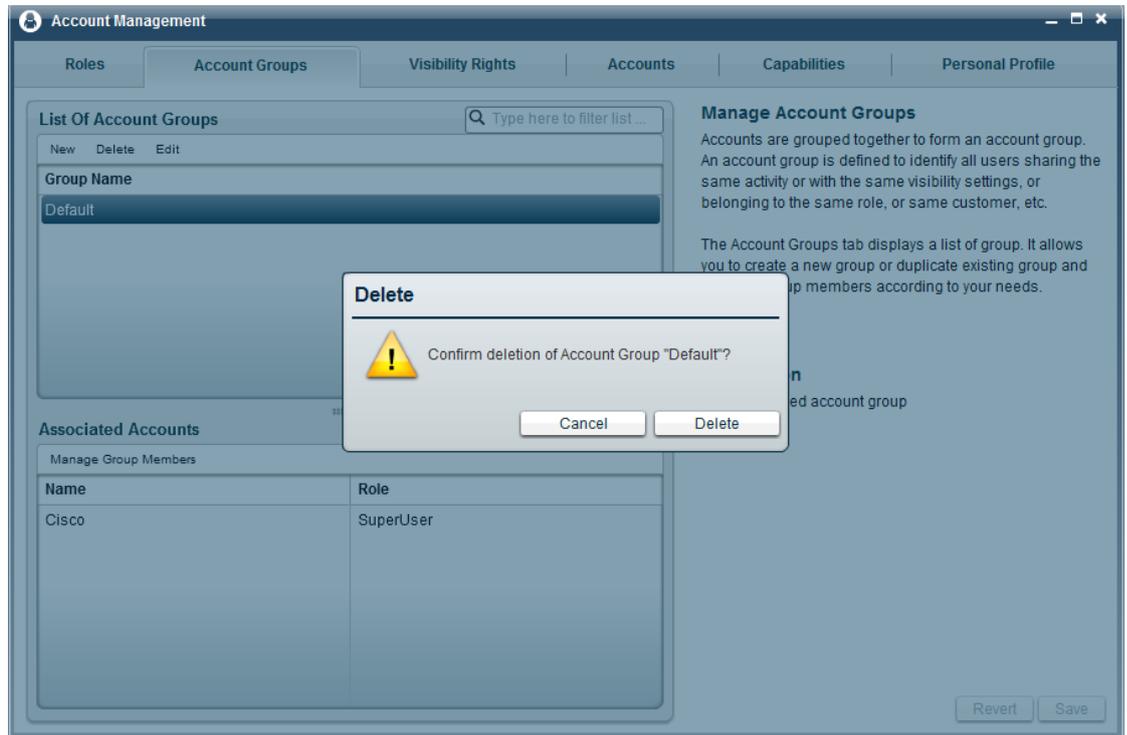
Step 4 Click **Save** to save the changes or **Cancel** to return to the previous page.

To delete an account group:

Step 1 Select the account group to delete.

Step 2 Click **Delete** button.

Step 3 On clicking the **Delete** button, following message will appear:

Figure 53. Delete Account Group

Step 4 Click **Delete** button to delete the account group or **Cancel** to return to the previous page.

5.4 Defining Visibility Rights

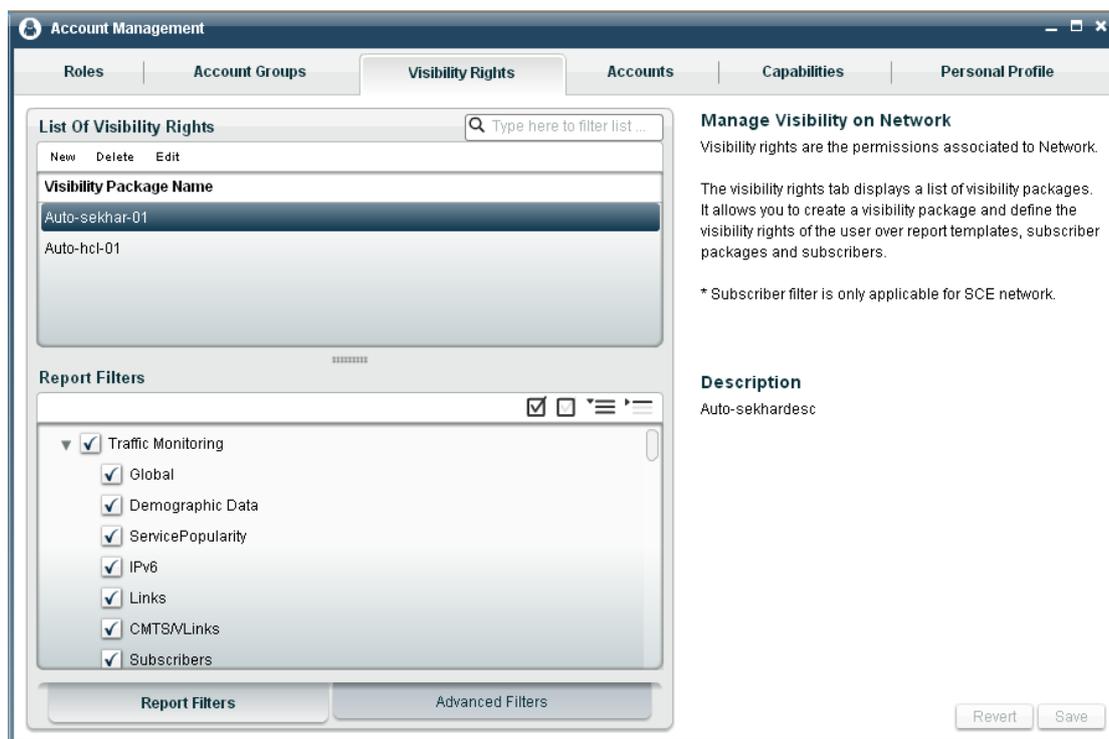
Visibility rights define the permissions to run reports on a particular Network and are associated with an account during creation. The Visibility Rights tab allows user to create a visibility package and define the visibility rights of the user over networks, report templates, subscriber packages, and subscribers.

To access and display the Visibility Rights tab, click the **Account Management** icon on the Module Launcher. This tab has two panes:

- **List of Visibility Rights**—Lists all the predefined visibility packages.
- **Report/Advanced Filters (only Available while defining rights on SCE Networks)**—Lists all the associated filters.

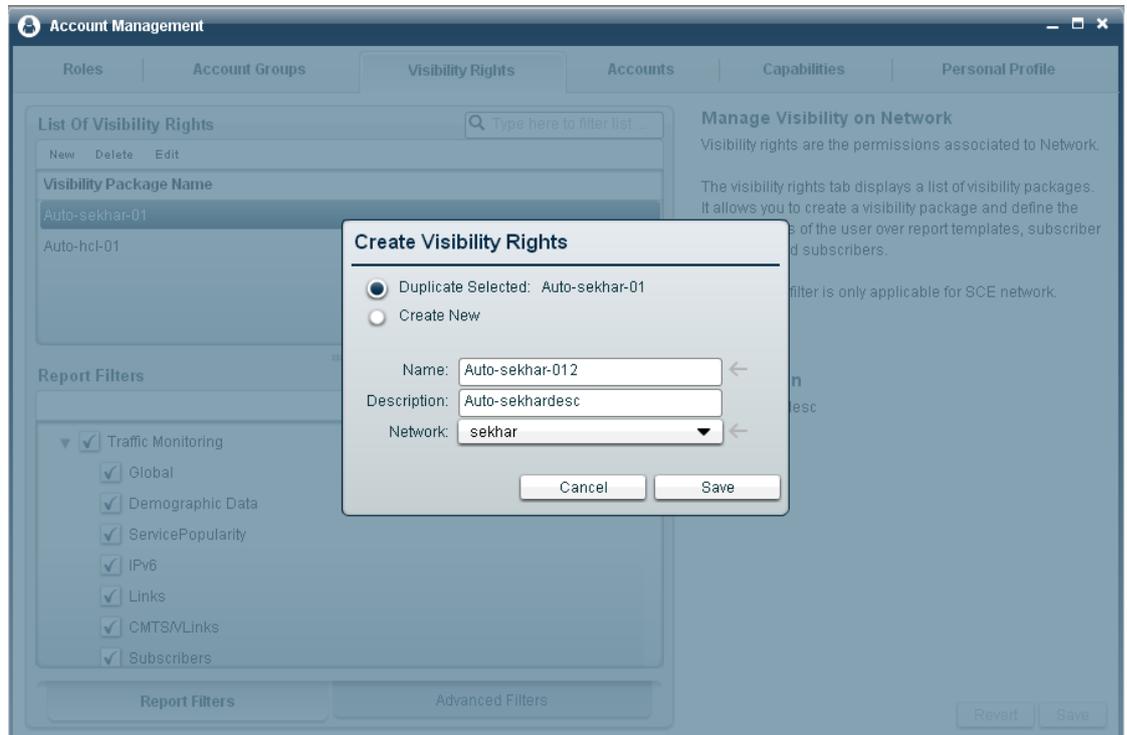
On selecting the **Visibility Rights** tab, following screen will appear:

Figure 54. Defining Visibility Rights for Network



To define a visibility rights package, perform the following steps:

- Step 1** Select the **New** option in the List of Visibility Rights panel. A **Create Visibility Rights** dialog box appears.
- Step 2** Choose the **Create New** option. On clicking, following pop-up will appear:

Figure 55. Create Visibility Rights**Note**

Choose **Duplicate** to create a copy of a predefined visibility right and continue with Step 4.

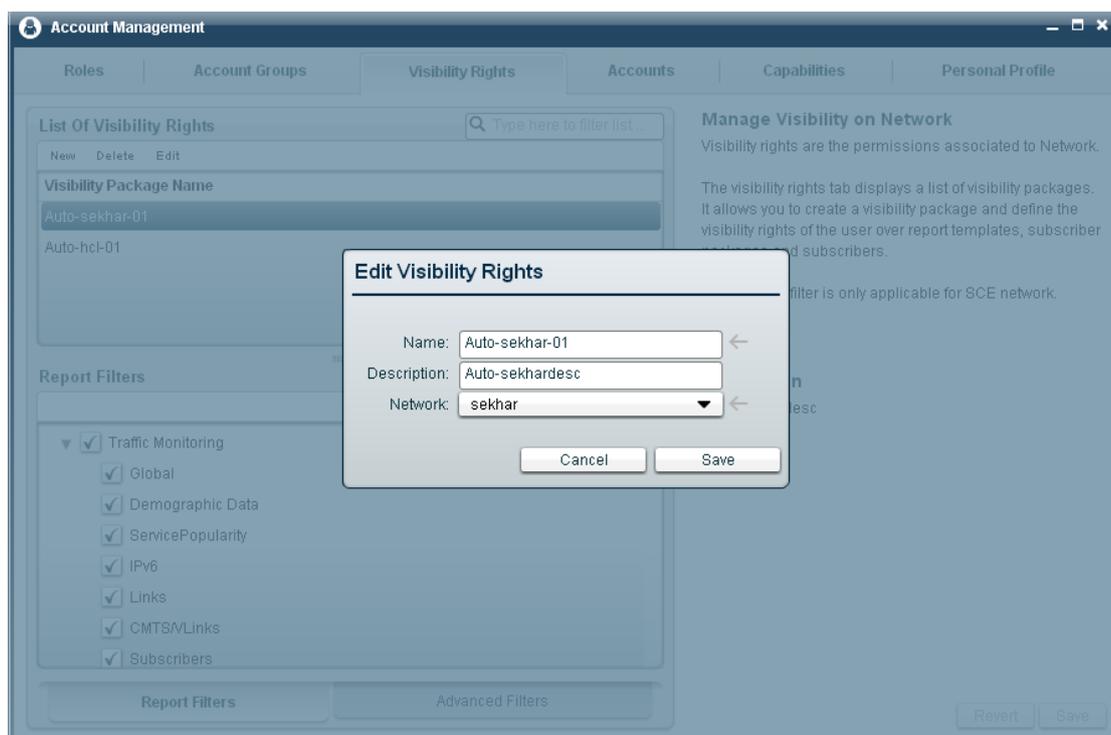
- Step 3** Enter the **Name** and **Description** of the visibility rights package in the respective fields.
- Step 4** Select a network from the **Network** drop-down list.
- Step 5** Click **OK** to confirm, or click **Cancel** to return to the previous page.

To edit Visibility Rights, perform the following steps:

Step 1 Select the visibility right to edit.

Step 2 Click **Edit** option. On clicking following pop-up will appear:

Figure 56. Edit Visibility Rights



Step 3 Edit the details.

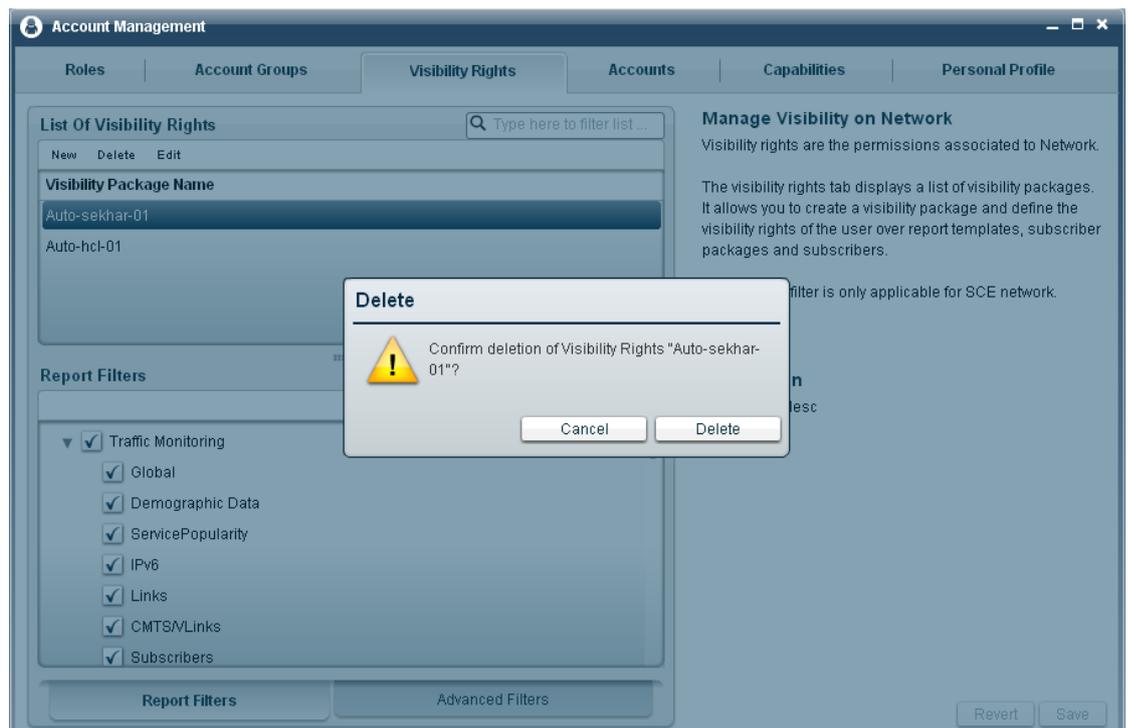
Step 4 Click **Save** to save the changes or **Cancel** to return to the previous page.

To delete visibility rights:

Step 1 Select the visibility rights to delete.

Step 2 Click **Delete** option. On clicking, following message box will appear:

Figure 57. Delete Visibility Rights



Step 3 Click **Delete** button to delete or **Cancel** to return to the previous page.

When user clicks **OK**, the list gets updated. This newly created visibility package does not provide any control over the networks, report template, subscriber packages, and subscribers, unless assigned.

To assign visibility rights to a specific visibility package, perform the following steps:

-
- Step 1** Select the Visibility package.
 - Step 2** Check the report templates in the **Report Filter** pane to set the visibility of topics.
 - Step 3** Check the packages in the **Advanced Filter** pane, to set the visibility of packages and subscriber to set visibility on subscriber. If Admin wants to set account level Subscriber Filter he/she can use Advance Filter options.
 - Step 4** Click **OK** to confirm, or click **Cancel** to return to the previous page.

**Note**

Advanced Filters for Packages and Subscribers are only available for visibility on SCE networks. Enabling Package Filter for SCE networks: User is allowed to enable or disable the package filter when creating a visibility for SCE networks.

If the package filter is enabled, only allowed packages are visible for selection in the report wizard. If new packages are found in the INI_VALUES of the traffic database for the Master devices of such network (On Get Master Values or schedules synchronization), they are not visible in the report wizard unless manually allowed in the visibility package.

If the package filter is disabled, all the packages are shown to the user while running the report. If new packages are found in the INI_VALUES of the traffic database for the Master devices of such network (On Get Master Values or schedules synchronization), they are also shown to the user irrespective of whether they are allowed or not in the visibility package.

5.5 Defining an Account

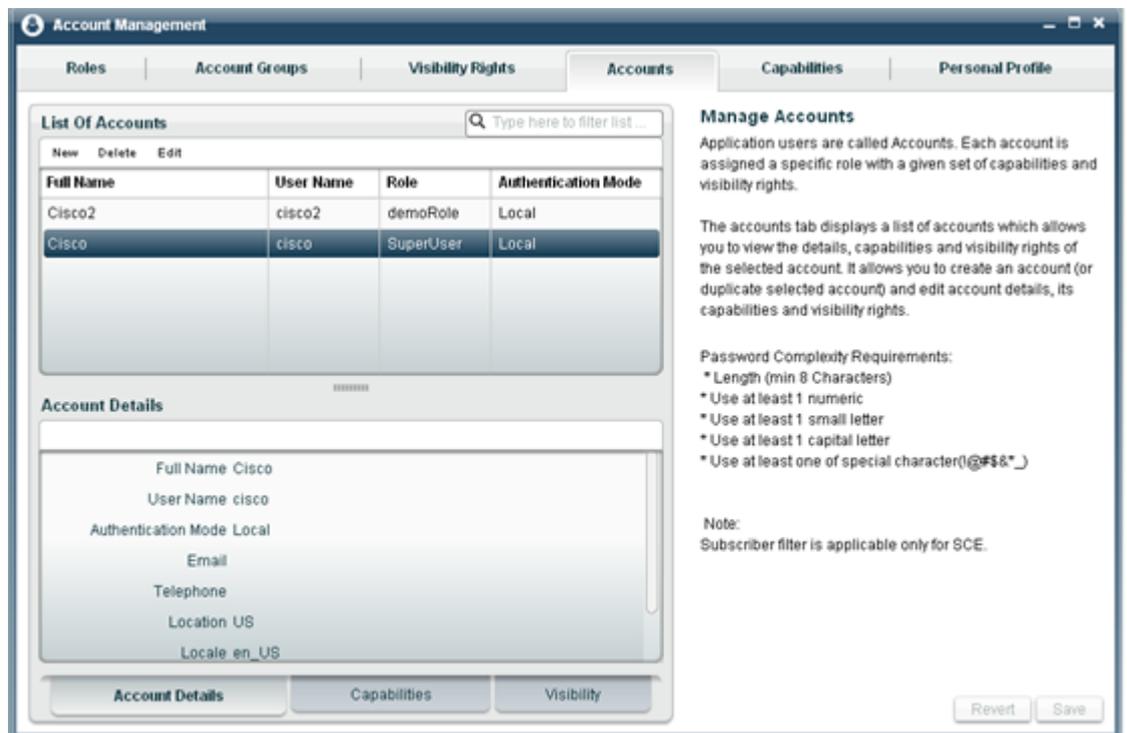
This software's users are called accounts. Each account is assigned a specific role with a given set of capabilities and visibility rights. The Accounts tab displays a list of accounts which allows user to view the details, capabilities, and visibility rights of the selected account.

To access and display the **Accounts** tab, click the **Account Management** icon on the Module Launcher. This tab has following panes:

- **List of Accounts**—Displays all the predefined accounts
- **Account Details**—Displays all the details of the account, selected in the **List of Accounts**
- **Capabilities**—Displays list of modules and sub modules accessible by the account, selected in the **List of Accounts**
- **Visibilities**—Displays visibility of the account, selected in the **List of Accounts**

When user clicks the **Accounts** tab, following screen will appear:

Figure 58. Defining Accounts



To create a new account, perform the following steps:

Step 1 Click the **New** button. On click following screen will appear:

Figure 59. New Account Creation

Create Account

Duplicate Selected: Cisco
 Create New

Name:

Description:

User Name:

Password:

Repeat Password:

Email:

Telephone:

Location:

Timezone:

Automatically adjust Daylight Saving ...

Locale:

Role:

Visibility: Auto-SCE_Network-01

Groups: Default
 Default AG

Subscriber filter:

**Note**

Step 2 Select the **Create New** option.

Choose **Duplicate** to create a copy of a predefined account and continue with Step 4.

Step 3 Enter a name.

Step 4 Enter a short description about the account in the **Description** field.

Step 5 Enter the username which is used for login.

Step 6 Select authentication mode as 'LOCAL'/RADIUS/TACACS+.

Step 7 Enter the password and reenter it.

Step 8 Enter the valid email ID, telephone number, and location for the user.

Step 9 Select the time zone. If day light saving is applicable to that time zone, it will display a checkbox to adjust the same, automatically.

Step 10 Select the locale.

Step 11 Select roles, visibilities, and account groups for the user.

Step 12 Enter the subscriber filter for which the user will have rights to run reports.

Step 13 Click **Save** to confirm, or click **Cancel** to discard any changes.

Step 14 On clicking the **Save** button, the list gets updated.

**Note**

The Local authentication mode is available by default. RADIUS and TACACS+ modes are available only if enabled in the Settings Module.

Each account belongs to one single role and can be associated to one or more account groups and visibility packages.

User can edit an account by clicking the **Edit** button, which displays:

Figure 60. Edit Account

The screenshot shows a web form titled "Edit Cisco2" with various fields for account configuration. The fields are as follows:

- Name: Cisco2
- Description: Insight Super User
- User Name: cisco2
- Authentication Mode: Local
- Password: [Redacted]
- Repeat Password: [Redacted]
- Email: [Empty]
- Telephone: [Empty]
- Location: US
- Timezone: (UTC-09:00) Alaska
- Automatically adjust Daylight Saving ...
- Locale: English (U.S.A.)
- Role: demoRole
- Visibility: Auto-SCE_Network-01
- Groups: Default, Default AG
- Subscriber filter: [Empty]

At the bottom of the form are "Cancel" and "Save" buttons.

**Note**

To edit the account, select the **Edit** option in the List of Accounts pane, and perform Step 3 and Step 4 as mentioned above for new account creation.

To delete the account, select the **Delete** option in the List of Accounts pane.

5.6 Viewing Capabilities

The Capabilities tab is read-only and is updated with the information from the actual mapping between the capability set and the defined roles.

To access and display the **Capabilities** tab, click the **Account Management** icon on the Launcher.

On clicking the **Capabilities** tab, the following screen will appear:

Figure 61. Capability Mapping Across Roles

Capability Mapping Across Roles			
Read Only			
	SuperUser	demoRole	
Report Wizard	✓	✓	
Create/Edit Report Definition	✓	✓	
Run Existing Report Definition	✓	✓	
Export	✓	✓	
Schedule	✓	✓	
Email	✓	✓	
My Favourite	✓		
Share	✓		
Report Gallery	✓	✓	
View Public	✓	✓	
Publish Public	✓	✓	
Account Management	✓	✓	
Create/Edit New Account Group	✓	✓	
Create New Account	✓	✓	
Create New Visibility Rights	✓	✓	

5.7 Editing the Personal Profile

The **Personal Profile** tab enables the user to change user-specific information.

To access and display the Personal Profile tab, click the **Account Management** icon on the Module Launcher.

On clicking the **Personal Profile** tab, following screen will appear:

Figure 62. Personal Profile

Personal Profile

This screen shows your Profile Information

* The changes made would be applicable on your next login

Password Complexity Requirements:

- * Length (min 8 Characters)
- * Use at least 1 numeric
- * Use at least 1 small letter
- * Use at least 1 capital letter
- * Use at least one of special character(!@#&*_)

Note:
Subscriber filter is applicable only for SCE.

Revert Save

In the above screen, user can update personal information such as name, description, password, location, locale, email, telephone number, and time zone. User can also select or unselect the option to receive error emails. By default, it performs daylight saving related adjustments automatically. Depending upon the changes in the information, **Save** and **Revert** buttons get enabled.



Note

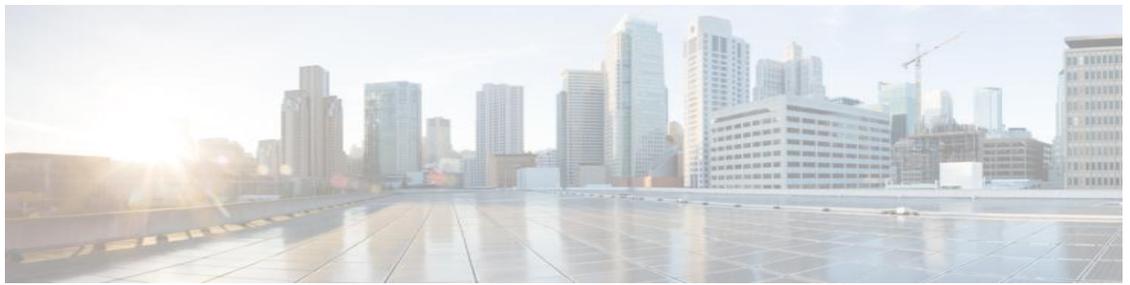
Cisco Insight Reporter generates reports according to the time zone configured in the personal profile settings of the connected Account. Operators should set the time zone according to their geographical location.



Tip

Password Complexity Requirements:

- * Length (min 8 Characters)
- * Use at least 1 numeric
- * Use at least 1 small letter
- * Use at least 1 capital letter (Except the first letter)
- * Use at least one of special character(!@#&*_) (Except the first letter)



CHAPTER 6. Reporting

6.1 IntroductionError! Bookmark not defined.

Cisco Insight Reporter provides a series of actions allowing users to run interactive reports, save and share report definitions, schedule recurring reports, view and customize a Dashboard or share results.

These actions can be executed through the Report Wizard module that significantly enhances the application usability as operators are driven in the process of choosing the desired reports. The wizard has a step-by-step procedure where all mandatory and optional parameters can be populated, then user can run, schedule, or save the report.

This approach has several benefits:

- It hides the complexity of the original template, structured as a list of report groups, each based on specific traffic tables.
- It reduces the redundancy of similar reports spread across the template.
- It creates a friendly interface for operators not having a deep knowledge of the SCE environments.

To access and display the report parameters, click the **Report Wizard** icon on the Module Launcher.

This chapter contains the following sections:

- Report Template
-
- Running Reports
- Running an Interactive Report
- Mapping with Database Tables
- **Error! Reference source not found.**
- My Favorites
- Report Gallery
- Scheduled Reports

6.2 Report Template

The SCE report template can be navigated through the Report Wizard on the Topic tab.

The operator needs to select a previously defined SCE Network and then click on the Topic tab. The list of available report topics will be displayed.



Note

The list of available Topics is dependent on:

- the CM database schema version chosen in the Settings Management module
- the Report Filters settings defined in the Network Wizard for the selected Network

The latest available report template is organized in the following topics:

- Traffic Monitoring
- Video
- VoIP
- Web
- P2P
- Mobile
- Malicious
- Traffic Discovery
- Traffic per Service
- Traffic Comparison
- Traffic per Package

6.2.1 Traffic Monitoring

Global

The Global group provides statistics about the traffic bandwidth or volume that was consumed. The bandwidth or volume consumption can be displayed per service for the entire link.

The Global group includes following reports:

Report Metrics	Report Topic Name	Description
Active Subscribers	Global Active Subscribers per Service	For a given time frame, shows the distribution of Active Subscribers between the different services defined in the system.
Active Subscribers	Global Active Subscribers per Topology	For a given time frame, shows the distribution of Active Subscribers between the different topologies defined in the system.

Report Metrics	Report Topic Name	Description
Active Subscribers	Package Active Subscriber per Service	For a given time frame, shows the distribution of Active Subscribers between the different services defined in the system for all subscribers belonging to a particular package.
Active Subscribers	Package Active Subscriber per Topology	For a given time frame, shows the distribution of Active Subscribers between the different topologies defined in the system for all subscribers belonging to a particular package.
Active Subscribers	Package Active Subscriber Comparison	For a given time frame, shows the active subscriber comparison belonging to a particular package.
Active Subscribers	Zone Active Subscribers per Service	For a given time frame, shows the distribution of Active Subscribers between the different services defined in the system for all subscribers belonging to a particular zone.
Active Subscribers	Zone Active Subscribers per Topology	For a given time frame, shows the distribution of Active Subscribers between the different topologies defined in the system for all subscribers belonging to a particular zone.
Active Subscribers	Zone Active Subscribers Comparison	For a given time frame, shows the active subscriber comparison belonging to a particular zone.
Bandwidth	Daily peak BW for All Packages	For a given time frame, shows the value per day of the maximum one-hour or two-hour bandwidth for all the packages defined in the system.
Bandwidth	Global Bandwidth per Service vs. Total Bandwidth	For a given time frame, shows the distribution of bandwidth of a specific service compared to the total bandwidth.
Bandwidth	Global Bandwidth per Service Comparison	For a given time frame, shows the global bandwidth per service comparison.
Bandwidth	Global Bandwidth per Service	For a given time frame, shows the distribution of bandwidth between the different services defined in the system.
Bandwidth	Global Bandwidth per Topology	For a given time frame, shows the distribution of bandwidth between the different networks defined in the system.

Report Metrics	Report Topic Name	Description
Bandwidth	Global Bandwidth per Traffic Direction	For a given time frame, shows the global bandwidth per traffic direction.
Bandwidth	Link Daily peak BW for All Packages	For a given time frame, shows value per day of maximum one hour or two hour bandwidth for specific package define in the system.
Bandwidth	Link Bandwidth per Service vs. Total Bandwidth	For a given time frame, shows the distribution of bandwidth of a specific service compared to the total bandwidth for all subscribers belonging to a particular link
Bandwidth	Link Bandwidth per Service comparison	For a given time frame, shows the global bandwidth per service comparison for all the subscribers belonging to a particular link
Bandwidth	Daily peak BW per Package	For a given time frame, shows the value per day of the maximum one-hour or two-hour bandwidth for a specific package defined in the system.
Bandwidth	Multi Package Bandwidth per Service	For a given time frame, shows the distribution of bandwidth between the different services defined in the system for all subscribers belonging to the selected packages.
Bandwidth	Package Bandwidth per Service	For a given time frame, shows the distribution of bandwidth between the different services defined in the system for all subscribers belonging to a particular package.
Bandwidth	Package Bandwidth per Topology	For a given time frame, shows the distribution of bandwidth between the different topologies defined in the system for all subscribers belonging to a particular package.
Bandwidth	Package Bandwidth Comparison	For a given time frame, shows the bandwidth comparison for the selected list of packages.
Bandwidth	Package Bandwidth per Service comparison	For a given time frame, shows the global bandwidth per service comparison for all the subscribers belonging to a particular package.
Bandwidth	Package Bandwidth per Traffic Direction	For a given time frame, shows the distribution of bandwidth between the different traffic directions defined in the system for all subscribers belonging to a particular package.

Report Metrics	Report Topic Name	Description
Bandwidth	Package Bandwidth per Service vs. Total Bandwidth	For a given time frame, shows the distribution of bandwidth of a specific service compared to the total bandwidth for all subscribers belonging to a particular package
Bandwidth	Daily peak BW per Zone	For a given time frame, shows the value per day of the maximum one-hour or two-hour bandwidth for a specific zone defined in the system.
Bandwidth	Multi Zone Bandwidth per Service	For a given time frame, shows the distribution of bandwidth between the different services defined in the system for all subscribers belonging to the selected zones.
Bandwidth	Zone Bandwidth per Service	For a given time frame, shows the distribution of bandwidth between the different services defined in the system for all subscribers belonging to a particular zone.
Bandwidth	Zone Bandwidth per Topology	For a given time frame, shows the distribution of bandwidth between the different topologies defined in the system for all subscribers belonging to a particular zone.
Bandwidth	Zone Bandwidth Comparison	For a given time frame, shows the bandwidth comparison for the selected list of zones.
Bandwidth	Zone Bandwidth per Service comparison	For a given time frame, shows the global bandwidth per service comparison for all the subscribers belonging to a particular zone.
Bandwidth	Zone Bandwidth per Traffic Direction	For a given time frame, shows the distribution of bandwidth between the different traffic directions defined in the system for all subscribers belonging to a particular zone.
Bandwidth	Zone Bandwidth per Service vs. Total Bandwidth	For a given time frame, shows the distribution of bandwidth of a specific service compared to the total bandwidth for the subscribers belonging to a particular zone.
Concurrent Sessions	Global Concurrent Sessions per Service	For a given time frame, shows the distribution of concurrent sessions between the different services defined in the system.
Concurrent Sessions	Global Concurrent Sessions per Topology	For a given time frame, shows the distribution of concurrent sessions between the different topologies defined in the system.

Report Metrics	Report Topic Name	Description
Concurrent Sessions	Package Concurrent Sessions per Service	For a given time frame, shows the distribution of concurrent sessions between the different services defined in the system for all subscribers belonging to a particular package.
Concurrent Sessions	Package Concurrent Sessions per Topology	For a given time frame, shows the distribution of concurrent sessions between the different topologies defined in the system for all subscribers belonging to a particular package.
Concurrent Sessions	Package Concurrent Sessions Comparison	For a given time frame, shows the concurrent sessions comparison for the selected list of packages.
Concurrent Sessions	Zone Concurrent Sessions per Service	For a given time frame, shows the distribution of concurrent sessions between the different services defined in the system for all subscribers belonging to a particular zone.
Concurrent Sessions	Zone Concurrent Sessions per Topology	For a given time frame, shows the distribution of concurrent sessions between the different topologies defined in the system for all subscribers belonging to a particular zone.
Concurrent Sessions	Zone Concurrent Sessions Comparison	For a given time frame, shows the concurrent sessions comparison for the selected list of zones.
Duration	Global Hourly Aggregated Minutes per Service	For a given time frame, shows the total number of minutes spent for services defined in the system.
Duration	Global Hourly Aggregated Minutes per Topology	For a given time frame, shows the total number of minutes spent for topologies defined in the system.
Duration	Package Hourly Aggregated Minutes per Service	For a given time frame, shows the total number of minutes spent for services defined in the system for all subscribers belonging to a particular package.
Duration	Package Hourly Aggregated Minutes per Topology	For a given time frame, shows the total number of minutes spent for topologies defined in the system for all subscribers belonging to a particular package.
Duration	Package Hourly Aggregated Minutes Comparison	For a given time frame, shows the hourly aggregated minutes comparison for the selected list of packages.

Report Metrics	Report Topic Name	Description
Duration	Zone Hourly Aggregated Minutes per Service	For a given time frame, shows the total number of minutes spent for services defined in the system for all subscribers belonging to a particular zone.
Duration	Zone Hourly Aggregated Minutes per Topology	For a given time frame, shows the total number of minutes spent for topologies defined in the system for all subscribers belonging to a particular zone.
Duration	Zone Hourly Aggregated Minutes Comparison	For a given time frame, shows the hourly aggregated minutes comparison for the selected list of zones.
Sessions	Global Daily Usage Sessions per Service	For a given time frame, shows the distribution of sessions between the different services defined in the system.
Sessions	Global Daily Usage Sessions per Topology	For a given time frame, shows the distribution of sessions between the different topologies defined in the system.
Sessions	Global Hourly Usage Sessions per Service	For a given time frame, shows the distribution of sessions between the different services defined in the system.
Sessions	Global Hourly Usage Sessions per Topology	For a given time frame, shows the distribution of sessions between the different topologies defined in the system.
Sessions	Package Hourly Usage Sessions per Service	For a given time frame, shows the distribution of sessions between the different services defined in the system for all subscribers belonging to a particular package.
Sessions	Package Hourly Usage Sessions per Topology	For a given time frame, shows the distribution of sessions between the different topologies defined in the system for all subscribers belonging to a particular package.
Sessions	Package Hourly Usage Sessions Comparison	For a given time frame, shows the hourly usage sessions comparison for the selected list of packages.
Sessions	Zone Daily Usage Sessions per Service	For a given time frame, shows the daily session distribution between the different services for the selected zone
Sessions	Zone Daily Usage Sessions per Topology	For a given time frame, shows the daily session distribution between the different topologies for the selected zone.

Report Metrics	Report Topic Name	Description
Sessions	Zone Daily Usage Sessions Comparison	For a given time frame, shows the daily usage sessions comparison for the selected list of zones.
Sessions	Zone Hourly Usage Sessions per Service	For a given time frame, shows the distribution of sessions between the different services defined in the system for all subscribers belonging to a particular zone.
Sessions	Zone Hourly Usage Sessions per Topology	For a given time frame, shows the distribution of sessions between the different topologies defined in the system for all subscribers belonging to a particular zone.
Sessions	Zone Hourly Usage Sessions Comparisons	For a given time frame, shows the hourly usage sessions comparison for the selected list of zones.
Top by Usage Volume	Global Aggregated Usage Volume per Service	For a given time frame, shows the aggregated distribution of volume between the different services defined in the system.
Top by Usage Volume	Global Aggregated Usage Volume per Topology	For a given time frame, shows the aggregated distribution of volume between the different topologies defined in the system.
Top by Usage Volume	Package Aggregated Usage Volume per Service	For a given time frame, shows the most popular services for all subscribers belonging to a particular package.
Top by Usage Volume	Package Aggregated Usage Volume per Topology	For a given time frame, shows the most popular topology for all subscribers belonging to a particular package.
Top by Usage Volume	Package Aggregated Usage Volume Comparison	For a given time frame, shows the aggregated usage volume comparison for the selected list of packages.
Top by Usage Volume	Zone Aggregated Usage Volume per Service	For a given time frame, shows the most popular services for all subscribers belonging to a particular zone.
Top by Usage Volume	Zone Aggregated Usage Volume per Topology	For a given time frame, shows the most popular topology for all subscribers belonging to a particular zone.
Top by Usage Volume	Zone Aggregated Usage Volume Comparison	For a given time frame, shows the aggregated usage volume comparison for the selected list of zones.

Report Metrics	Report Topic Name	Description
Volume	Global Daily Usage Volume per Service	For a given time frame, shows the distribution of volume between the different services defined in the system.
Volume	Global Daily Usage Volume per Topology	For a given time frame, shows the distribution of volume between the different topologies defined in the system.
Volume	Global Hourly Usage Volume per Service	For a given time frame, shows the distribution of volume between the different services defined in the system.
Volume	Global Hourly Usage Volume per Topology	For a given time frame, shows the distribution of volume between the different topologies defined in the system.
Volume	Global Busy Hours Usage Volume per Service	For a given time frame, shows the distribution of volume between the different services during the busy hours.
Volume	Package Daily Usage Volume per Service	For a given time frame, shows the distribution of volume between the different services defined in the system for all subscribers belonging to a particular package.
Volume	Package Daily Usage Volume per Topology	For a given time frame, shows the distribution of volume between the different topologies defined in the system for all subscribers belonging to a particular package.
Volume	Package Daily Usage Volume Comparison	For a given time frame, shows the daily usage volume comparison for the selected list of packages.
Volume	Package Hourly Usage Volume per Service	For a given time frame, shows the distribution of volume between the different services defined in the system for all subscribers belonging to a particular package.
Volume	Package Hourly Usage Volume per Topology	For a given time frame, shows the distribution of volume between the different topologies defined in the system for all subscribers belonging to a particular package.
Volume	Package Hourly Usage Volume Comparison	For a given time frame, shows the hourly usage volume comparison for the selected list of packages.
Volume	Zone Daily Usage Volume per Service	For a given time frame, shows the distribution of volume between the different services defined in the system for all subscribers belonging to a particular zone.

Report Metrics	Report Topic Name	Description
Volume	Zone Daily Usage Volume per Topology	For a given time frame, shows the distribution of volume between the different topologies defined in the system for all subscribers belonging to a particular zone.
Volume	Zone Daily Usage Volume Comparison	For a given time frame, shows the daily usage volume comparison for the selected list of zones.
Volume	Zone Hourly Usage Volume per Service	For a given time frame, shows the distribution of volume between the different services defined in the system for all subscribers belonging to a particular zone.
Volume	Zone Hourly Usage Volume per Topology	For a given time frame, shows the distribution of volume between the different topologies defined in the system for all subscribers belonging to a particular zone.
Volume	Zone Hourly Usage Volume Comparison	For a given time frame, shows the hourly usage volume comparison for the selected list of zones.

Figure 63. Sample Report – Global Bandwidth per Service



Demographic Data

The Demographic Data group includes following reports:

Report Metrics	Report Topic Name	Description
Active Subscribers	Total Active Subscribers	Shows the daily or weekly average trend in total number of active subscribers.
Cumulative Distributions	Cumulative Distribution of Subscriber Usage	For a given time frame, show a list of subscriber consumption.
Cumulative Distributions	Subscribers Average Consumption	For a given time frame, shows a list of subscriber consumption.

Service Popularity

The Service Popularity group is designed to present statistics about demographic usage of the network (distributions, trends, etc).

The service popularity group includes following reports:

Report Metrics	Report Topic Name	Description
Average	Service Popularity among Subscribers (Average)	For a given time frame, shows the distribution of Active Subscribers between the different services defined in the system.
Average	Service Popularity among Subscribers of Specific Package (Average)	For a given time frame, shows the distribution of Active Subscribers between the different services defined in the system for all subscribers belonging to a particular package.
Average	Service Popularity among Subscribers of Specific Zone (Average)	For a given time frame, shows the distribution of Active Subscribers between the different services defined in the system for all subscribers belonging to a particular zone.
Time Analysis	Service Popularity among Subscribers	For a given time frame, shows the popularity of a specific service against all services among subscribers defined in the system.
Time Analysis	Service Popularity among Subscribers of Specific Package	For a given time frame, shows the popularity of a specific service against all services among subscribers defined in the system for all subscribers belonging to a particular package.
Time Analysis	Service Popularity among Subscribers of Specific Zone	For a given time frame, shows the distribution of Active Subscribers between the different services defined in the system for all subscribers belonging to a particular zone.

IPv6

The IPv6 group includes the following reports:

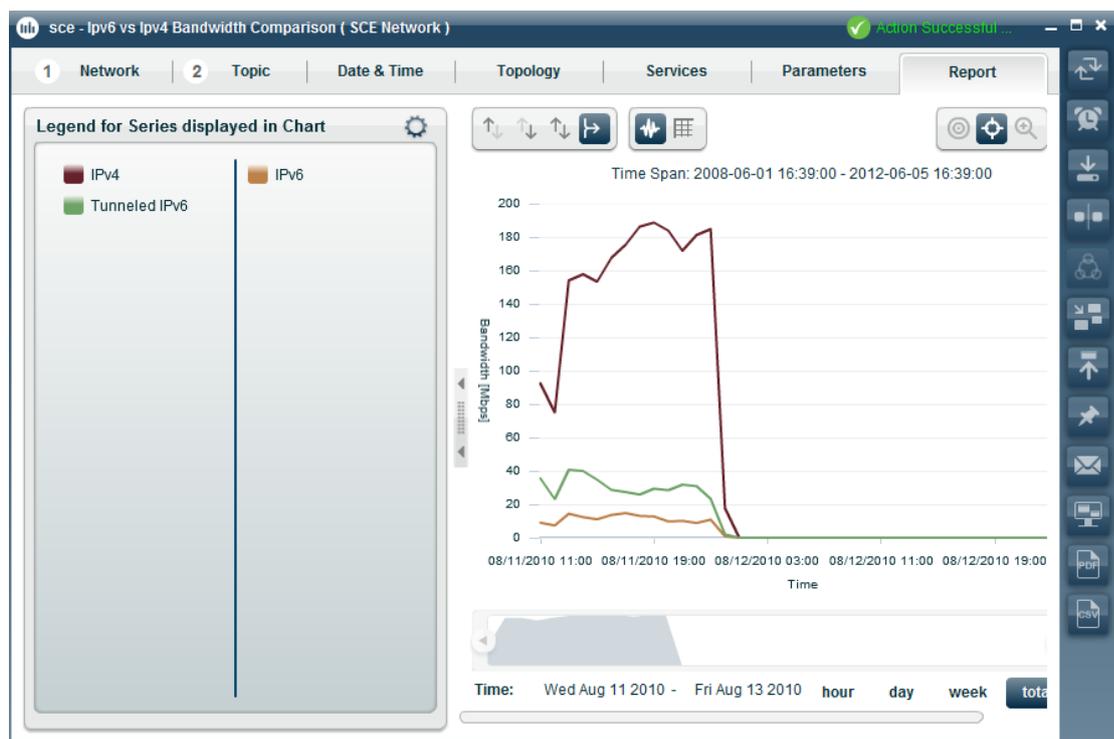
Report Metrics	Report Topic Name	Description
Active Subscribers	IPv6 Active Subscribers	For a given time frame, shows the IPv4/IPv6 active subscribers.
Average Subscriber Bandwidth	IPv6 Average Subscriber Bandwidth	For a given time frame, shows the IPv4/IPv6 average subscriber bandwidth.
Concurrent Sessions	IPv6 Concurrent Sessions	For a given time frame, shows the IPv4/IPv6 concurrent sessions.



Note

In **IP Type** drop-down, please do not select **Tunneled IPv6** option. This option is not supported in latest SCE release.

Figure 64. Sample Report – IP Version Bandwidth Comparison



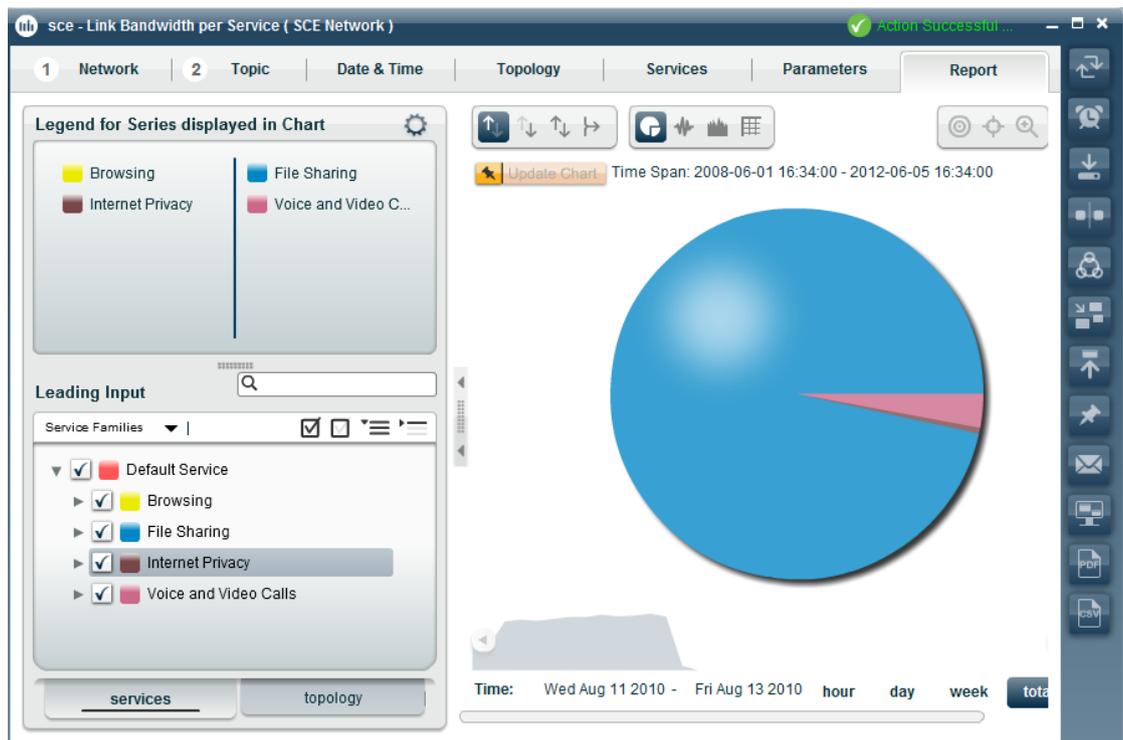
Links

The Link monitoring reports provides the statistics of the links. The Link group includes following reports:

Report Metrics	Report Topic Name	Description
Bandwidth	Link Bandwidth per Service	For a given time frame, shows the distribution of bandwidth between the different services for the selected Link.
Bandwidth	Link Bandwidth per Topology	For a given time frame, shows the distribution of bandwidth between the different topologies for the selected link.
Bandwidth	Link Bandwidth per Traffic Direction	For a given time frame, shows the distribution of bandwidth between the different traffic directions for the selected VLink.
Concurrent Sessions	Link Concurrent Sessions per Service	For a given time frame, shows the concurrent session distribution between the different services for the selected link.
Concurrent Sessions	Link Concurrent Sessions per Topology	For a given time frame, shows the concurrent session distribution between the different topologies for the selected link.
Duration	Link Hourly Aggregated Minutes per Service	For a given time frame, shows the hourly aggregated minutes distribution between the different services for the selected link.
Duration	Link Hourly Aggregated Minutes per Topology	For a given time frame, shows the hourly aggregated minutes distribution between the different topologies for the selected link.
Sessions	Link Daily Usage Sessions per Service	For a given time frame, shows the daily session distribution between the different services for the selected link.
Sessions	Link Daily Usage Sessions per Topology	For a given time frame, shows the daily session distribution between the different topologies for the selected link.
Sessions	Link Hourly Usage Sessions per Service	For a given time frame, shows the hourly sessions distribution between the different services for the selected link.
Sessions	Link Hourly Usage Sessions per Topology	For a given time frame, shows the hourly sessions distribution between the different topologies for the selected link.

Top by Usage Volume	Link Aggregated Usage Volume per Service	For a given time frame, shows the aggregated usage volume per service for the selected link.
Top by Usage Volume	Link Aggregated Usage Volume per Topology	For a given time frame, shows the aggregated usage volume per topology for the selected link.
Top by Usage Volume	Link Aggregated Usage Volume Comparison	For a given time frame, shows the aggregated usage volume comparison for the selected list of links.
Volume	Link Daily Usage Volume per Service	For a given time frame, shows the daily volume distribution between the different services for the selected link.
Volume	Link Daily Usage Volume per Topology	For a given time frame, shows the daily volume distribution between the different topologies for the selected link.
Volume	Link Hourly Usage Volume per Service	For a given time frame, shows the hourly volume distribution between the different services for the selected link.
Volume	Link Hourly Usage Volume per Topology	For a given time frame, shows the hourly volume distribution between the different topologies for the selected link.
Volume	Link Busy Hours Usage Volume per Service	For a given time frame, shows the volume distribution between the different services for the selected link during the busy hours.

Figure 65. Sample Report – Link Bandwidth per Service



CMTS/VLinks

The CMTS/VLinks group provides statistics related to traffic usage for cable operators. The reports expose different metrics to monitor CMTS, virtual links and virtual channels with the granularity of each single SCE service (service usage counter).

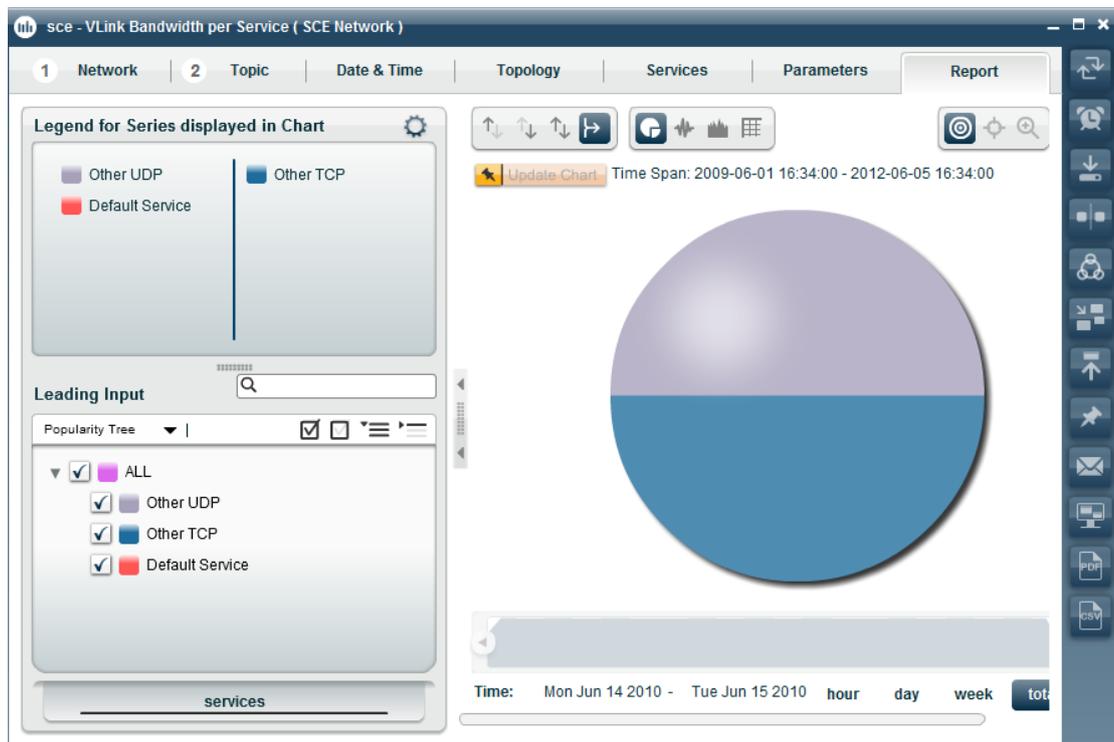


Note

These reports shall not be used if SCE devices are not configured to monitor traffic in symmetric mode. cannot be generated using data collected from an SCE platform running in Asymmetric Routing Classification mode.

The CMTS/VLinks group includes the following reports:

Report Metrics	Report Topic Name	Description
Bandwidth	Daily peak BW for VLinks	For a given time frame, shows the value per day of the maximum one-hour to two-hour bandwidth for specific VLinks.
Top VLinks by Volume	Top VLinks by Usage Volume	For a given time frame, shows the most popular VLinks ordered by volume.
Active Subscribers	Total Active Subscribers per VLink	For a given time frame, shows the daily or weekly average trend for the total number of active subscribers for the selected VLink.
Top Services by Volume	VLink Aggregated Usage Volume per Service	For a given time frame, shows the aggregated usage volume per service for the selected VLink.
Bandwidth	VLink Bandwidth per Package	For a given time frame, shows the distribution of bandwidth between the different packages for the selected VLink.
Bandwidth	VLink Bandwidth per Service	For a given time frame, shows the distribution of bandwidth between the different services for the selected VLink.
Volume	VLink Daily Usage Volume per Service	For a given time frame, shows the daily volume distribution between the different services for the selected VLink.
Volume	VLink Hourly Usage Volume per Service	For a given time frame, shows the hourly volume distribution between the different services for the selected VLink.
Bandwidth	VLink BW per Cable-Modems group	For a given time frame, shows the distribution of bandwidth between the different cable-modems group for the selected VLink.

Figure 66. Sample Report – VLink Bandwidth per Service

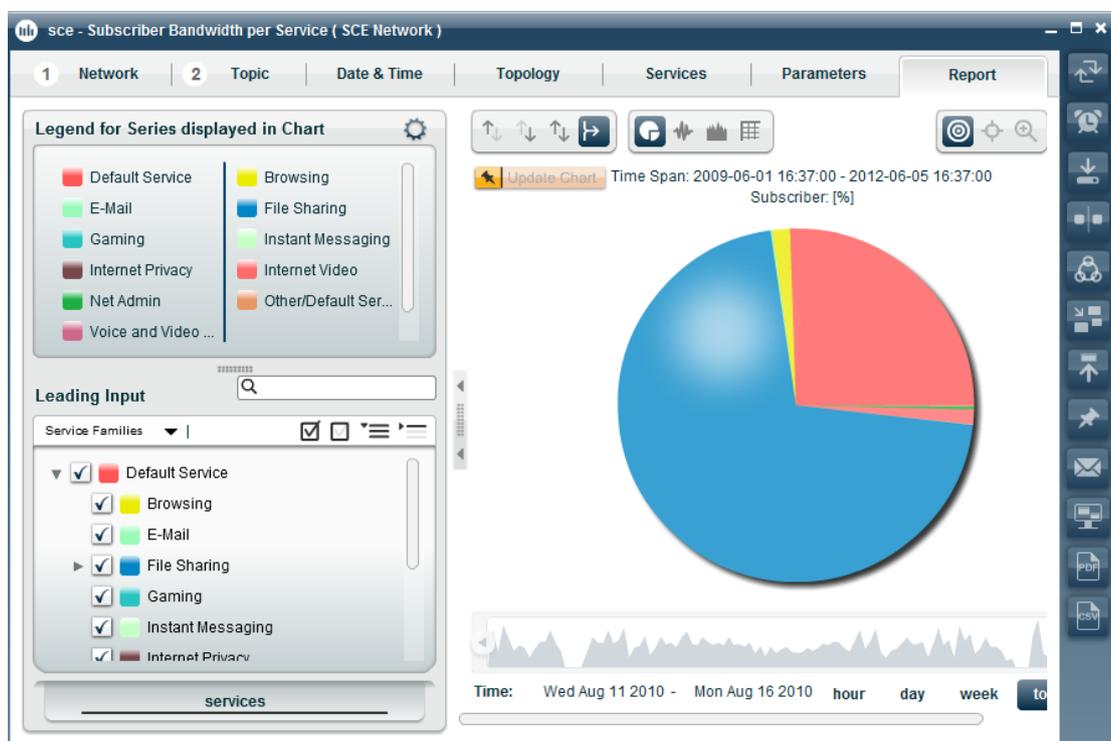
Subscribers

The Subscriber Monitoring group is designed to view statistics about the bandwidth or volume of traffic used by SCE subscribers. The reports are provided per service usage counter for the total volume consumed by the subscriber. The Subscribers group includes following reports:

Report Metrics	Report Topic Name	Description
Average Bandwidth	Average Subscriber BW	For a given time frame, shows the distribution of bandwidth between the different services defined in the system.
Average Bandwidth	Average Subscriber BW per Service	For a given time frame, shows the distribution of bandwidth between the different services defined in the system.
Average Sessions	Average Subscriber Concurrent Sessions	For a given time frame, shows the average subscriber concurrent sessions.
Average Sessions	Average Subscriber Concurrent Sessions per Service	For a given time frame, shows the average subscriber concurrent sessions per service.
Bandwidth	Daily peak BW for Specific Subscriber	For a given time frame, shows value per day of the maximum one-hour or two-hour bandwidth for a specific subscriber.
Bandwidth	Peak Bandwidth per Subscriber	For a given time frame, shows the peak bandwidth per subscriber for specific, all, or by subscriber ID pattern.
Bandwidth	Subscriber Bandwidth per Service	For a given time frame, shows the distribution of bandwidth between the different services defined in the system for a particular subscriber.
Bandwidth Comparison	Subscriber Bandwidth Comparison	For a given time frame, shows the bandwidth comparison for the selected list of subscribers.
Duration	Subscriber Hourly Aggregated Minutes per Service	For a given time frame, shows the hourly total number of minutes spent for services defined in the system for a particular subscriber.
Real-Time Flows	Subscriber Flows Detail	For a given time frame, shows the real-time flow details for a specific subscriber.
Sessions	Subscriber Daily Usage Sessions per Service	For a given time frame, shows the daily session's distribution between the different services defined in the system for a particular subscriber.
Sessions	Subscriber Hourly Usage Sessions per Service	For a given time frame, shows the hourly sessions distribution between the different services defined in the system for a

		particular subscriber.
Top Services by Usage Volume	Subscriber Aggregated Usage Volume per Service	For a given time frame, shows the most popular services for the selected monitored subscribers.
Volume	Subscriber Daily Usage Volume per Service	For a given time frame, shows the daily volume distribution between the different services defined in the system for a particular subscriber.
Volume	Subscriber Hourly Usage Volume per Service	For a given time frame, shows the hourly volume distribution between the different services defined in the system for a particular subscriber.

Figure 67. Sample Report – Subscriber Bandwidth per Service



Top Subscribers

A Top Subscribers report identifies the most consuming subscribers in terms of traffic volume (for all or specific services). Subscriber bandwidth and volume reports can be generated for those subscribers configured for real-time monitoring.

The Top Subscribers group includes following reports:

Report Metrics	Report Topic Name	Description
List	Top Subscribers	For a given time frame, shows a list of consumption by the subscriber. Note the specified time will be rounded to the nearest Day or Hour. The number of available entries depends on the TA adapter configuration.
Relative Consumption	Relative Consumption of Top Subscribers	For a given time frame, shows the relative consumption of a specific number of subscribers.
Service Distribution	Top Subscribers Usage Distribution per Service	For a given time frame, shows the usage distribution per service of specific subscriber or all subscribers if not specified.

IP Version Comparison

The IP Version Comparison group includes the following reports:

Report Metrics	Report Topic Name	Description
Bandwidth	IP Version Bandwidth Comparison	Report to compare the bandwidth of IPv6 and IPv4 traffic for the specified time period.
Volume	IP Version Volume Comparison	Report to compare the volume of IPv6 and IPv4 traffic for the specified time period.
Sessions	IP Version Session Comparison	Report to compare the sessions of IPv6 and IPv4 traffic for the specified time period.
Concurrent Sessions	IP Version Concurrent Session Comparison	Report to compare the Concurrent sessions of IPv6 and IPv4 traffic for the specified time period.
Duration	IP Version Duration Comparison	Report to compare the duration of IPv6 and IPv4 traffic for the specified time period.

OSFP (OS Finger Print)

The OSFP group includes the following reports:

Report Metrics	Report Topic Name	Description
OS Hits	OS Hits	Report to verify the number of hit counts per OS, as identified by OS fingerprint.
Top OS	Top OS	List of Operating Systems, as identified by OS fingerprint
Subscriber List	Subscriber List	List of Subscribers grouped by Operating System, as identified by OS fingerprint

Figure 68. Sample report: Traffic Monitoring - OSFP - OS Hits

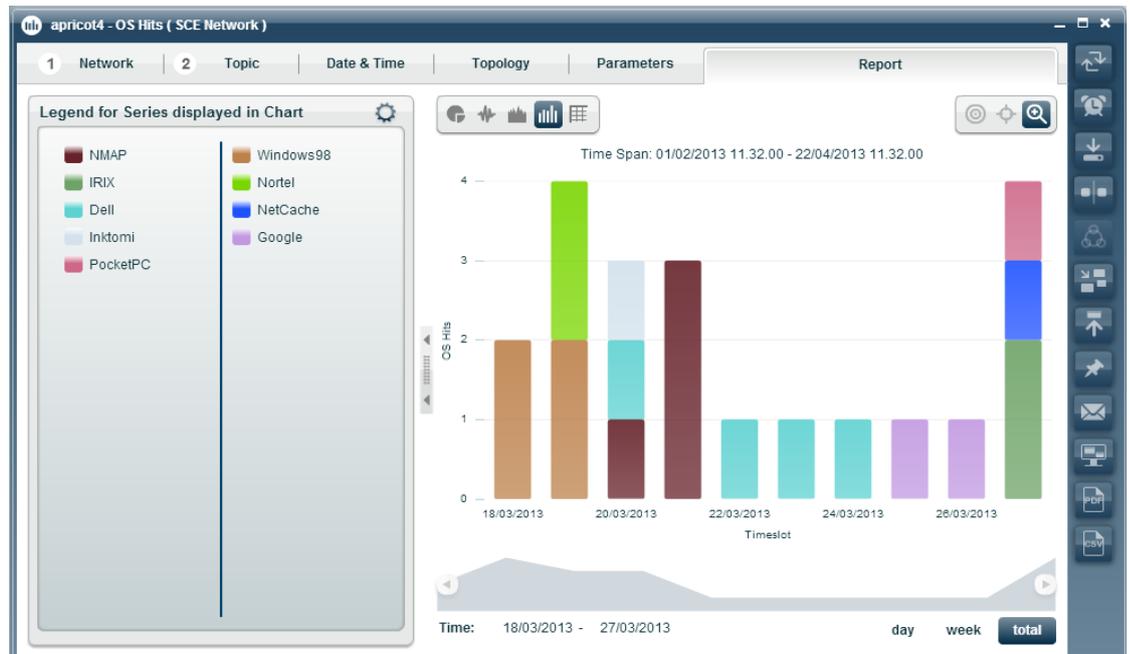
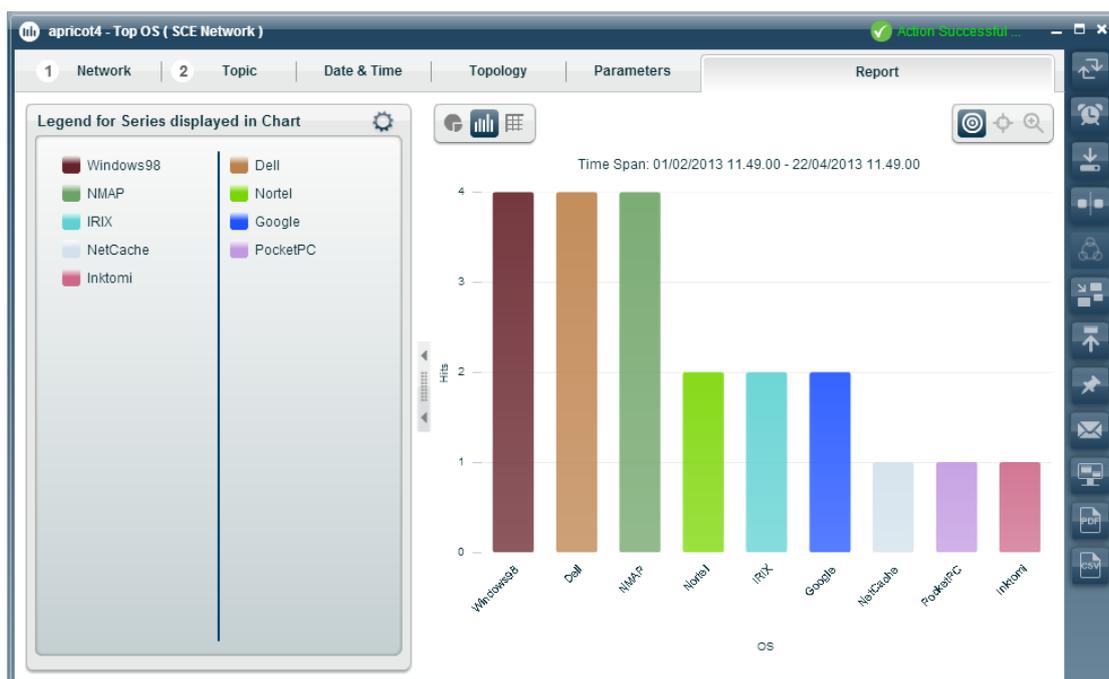


Figure 69. Sample report: Traffic Monitoring - OSFP - Top OS**Figure 70.** Sample report: Traffic Monitoring - OSFP – Subscriber List

Time	Subscriber Name	OS Name
2013-03-20 00:00:00.0	sub7	Dell
2013-03-22 00:00:00.0	sub1	Dell
2013-03-23 00:00:00.0	sub5	Dell
2013-03-24 00:00:00.0	sub1	Dell

6.2.2 Video

The Video group allows user to view statistics of the video traffic.

Bandwidth Monitoring

The Bandwidth Monitoring group includes the following reports:

Report Metrics	Report Topic Name	Description
Bandwidth Monitoring	Global Bandwidth per Video Service	For a given time frame, shows the distribution of bandwidth between the different Video services defined in the system.
Bandwidth Monitoring	Package Bandwidth per Video Service	For a given time frame, shows the distribution of bandwidth between the different Video services defined in the system for all subscribers belonging to a particular package.
Bandwidth Monitoring	Zone Bandwidth per Video Service	For a given time frame, shows the distribution of bandwidth between the different Video services defined in the system for all subscribers belonging to a particular zone.

Consumers

The Consumers group includes following report:

Report Metrics	Report Topic Name	Description
Video Monitoring	Top Video Consumers	For a given time frame, shows the most popular video consumers.

Hosts

The Hosts group includes following reports:

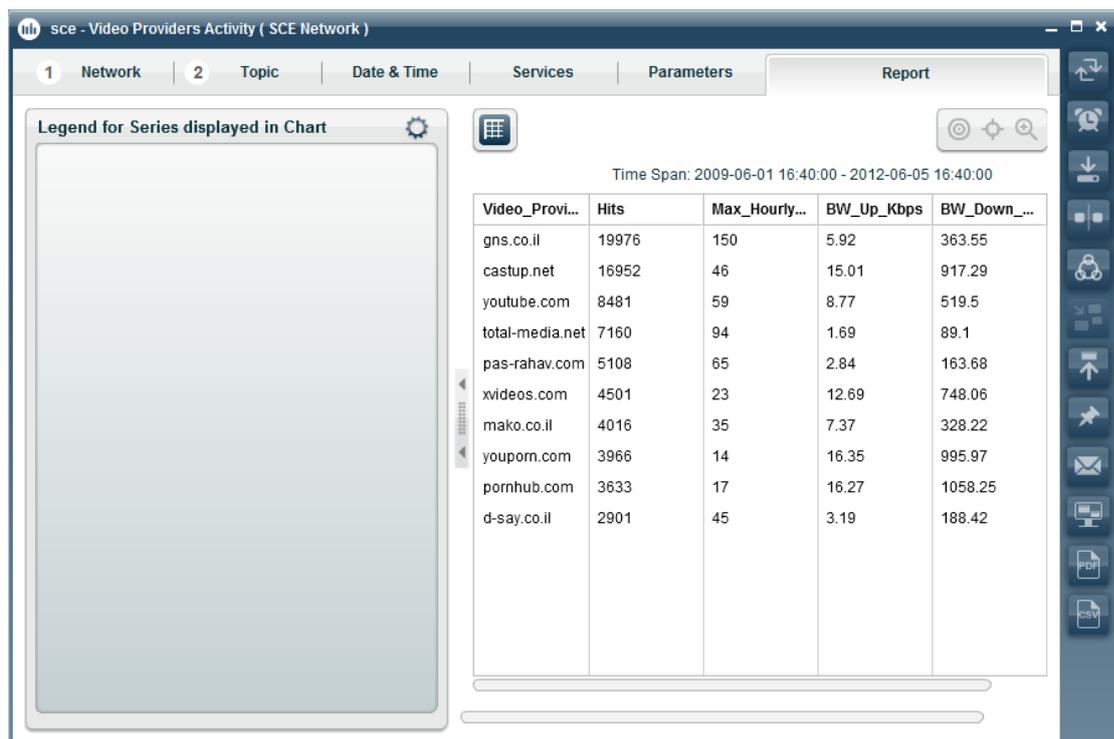
Report Metrics	Report Topic Name	Description
Popularity	Video Hosts Popularity	For a given time frame, shows the most popular video hosts ordered by the selected metric.
Time of Day Access	Time of Day Access pattern per Video Host	For a given time frame, shows the access pattern for a video hosts in a certain time of day.
Top	Top Video Hosts	For a given time frame, shows the most popular video hosts.

Figure 71. Sample Report – Video Hosts Popularity

Providers

The Providers group includes following reports:

Report Metrics	Report Topic Name	Description
Activity	Video Providers Activity	For a given time frame, shows the statistics about the most popular video providers.
Popularity	Video Providers Popularity	For a given time frame, shows the most popular video providers ordered by the selected metric.
Time of Day Access	Time of Day Access pattern per Video Provider	For a given time frame, shows the access pattern for a video provider in a certain time of day.
Top	Top Video Providers	For a given time frame, show the most popular video providers.
Top	Top Video Providers Trend	For a given time frame, shows the trend of the most popular video providers.
Trend	Video Provider Trend	For a given time frame, shows the trend of video providers.

Figure 72. Sample Report – Video Providers Activity

Services

The Services group includes following reports:

Report Metrics	Report Topic Name	Description
Distribution	Global Video Service Distribution	For a given time frame, shows the most popular video services.
Distribution	Package Video Service Distribution	For a given time frame, shows the most popular video services of a particular package.
Distribution	Zone Video Service Distribution	For a given time frame, shows the most popular video services of a particular zone.

6.2.3 VoIP

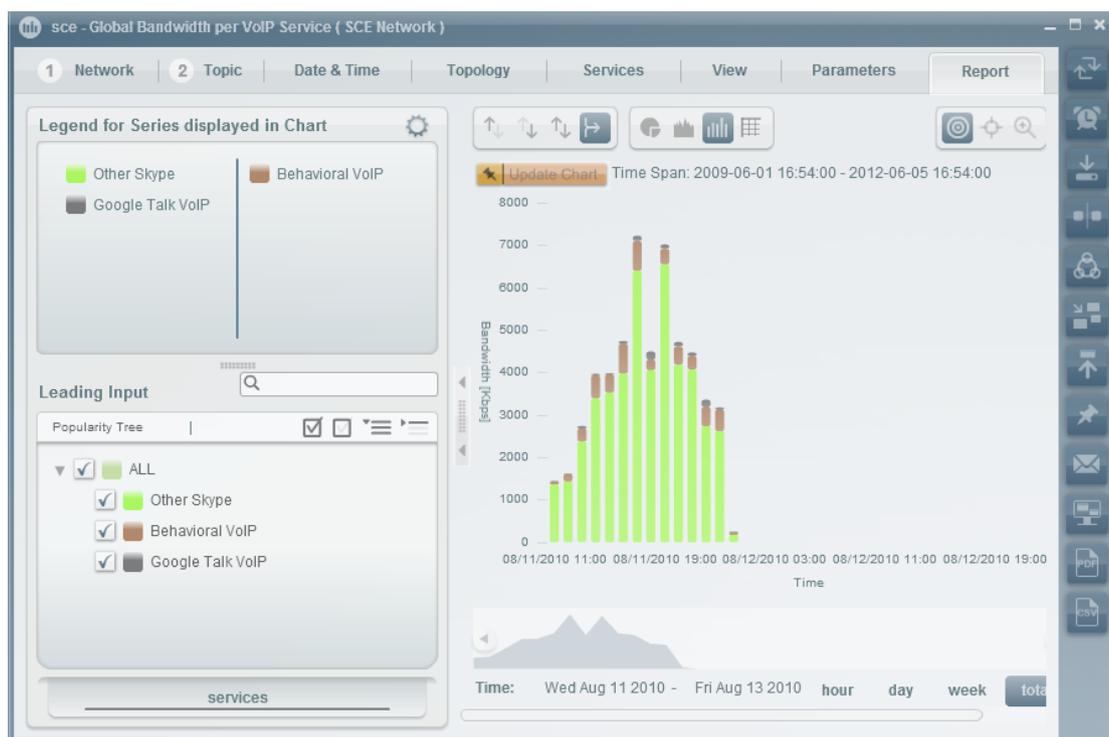
The VoIP group of reports allows user to view statistics of the VoIP traffic.

These reports cannot be generated using data collected from the SCE running in asymmetric routing classification mode.

Global

The Global group includes following reports:

Report Metrics	Report Topic Name	Description
Bandwidth	Global Bandwidth per VoIP Service	For a given time frame, shows the Global Bandwidth per VoIP Service for selected domains.
Bandwidth	Package Bandwidth per VoIP Service	For a given time frame, shows the Package Bandwidth per VoIP Service for selected domains.
Bandwidth	Zone Bandwidth per VoIP Service	For a given time frame, shows the zone Bandwidth per VoIP Service for selected domains.
Concurrent Calls	Global Concurrent Calls per VoIP Service	For a given time frame, shows the Global Concurrent Calls per VoIP Service for selected domains.
Concurrent Calls	Package Concurrent Calls per VoIP Service	For a given time frame, shows the Package Concurrent Calls per VoIP Service for selected domains.
Concurrent Calls	Zone Concurrent Calls per VoIP Service	For a given time frame, shows the zone Concurrent Calls per VoIP Service for selected domains.
Duration	Global Call Minutes per VoIP Service	For a given time frame, shows the distribution of concurrent VoIP calls between the different services defined in the system.
Duration	Global Hourly Call Minutes per VoIP Service	For a given time frame, shows the Global Hourly Call Minutes per Service for selected domains.
Duration	Package Hourly Call Minutes per VoIP Service	For a given time frame, shows the Package Hourly Call Minutes per Service for selected domains.
Duration	Zone Hourly Call Minutes per VoIP Service	For a given time frame, shows the zone Hourly Call Minutes per Service for selected domains.

Figure 73. Sample Report – Global Bandwidth per VOIP Service

QoS

The QoS group includes following reports:

Report Metrics	Report Topic Name	Description
Distribution	Global VoIP Codec Distribution	For a given time frame, shows the Global VoIP Codec Distribution.
Distribution	Global VoIP MOS Distribution	For a given time frame, shows the Global VoIP MOS Distribution for selected domains.
Global	Global VoIP Jitter	For a given time frame, shows the Global VoIP Jitter for selected domains.
Global	Global VoIP MOS	For a given time frame, shows the Global VoIP MOS for selected domains.
Global	Global VoIP Packets Loss	For a given time frame, shows the Global VoIP Packets Loss for selected domains.
Hourly Average	Global Hourly Average VoIP Jitter	For a given time frame, shows the Global Hourly Average VoIP Jitter for selected domains.

Hourly Average	Global Hourly Average VoIP MOS	For a given time frame, shows the Global Hourly Average VoIP MOS for selected domains.
Hourly Average	Global Hourly Average VoIP Packets Loss	For a given time frame, shows the Global Hourly Average VoIP Packets Loss for selected domains.

Figure 74. Sample Report – Global VoIP Codec Distribution



SIP Domains

The SIP Domains group includes following reports:

Report Metrics	Report Topic Name	Description
Average MOS	Average MOS per SIP Domain	For a given time frame, shows the Average MOS per SIP domain.
Calls Duration	Calls Duration per SIP Domains	For a given time frame, shows the call duration per SIP domain.
Number of Calls	Number of Calls per SIP Domain	For a given time frame, shows the most popular SIP or Vonage domains per number of calls.
Top	Top SIP Domains	For a given time frame, shows the most popular SIP or Vonage domains.

Top	Top SIP Domains by Unique Users	For a given time frame, shows the most popular SIP Domains ordered by Unique Users.
Top User Agents	Top SIP User Agents	For a given time frame, shows the most popular SIP User Agents.

Subscribers

The Subscribers group includes following reports:

Report Metrics	Report Topic Name	Description
Top	Top Talkers	For a given time frame, shows the most popular VoIP subscribers ordered by the selected metric.
Bandwidth	Subscriber Bandwidth per VoIP Service	For a given time frame, shows the distribution of bandwidth between the different VoIP services defined in the system for a particular subscriber.
Duration	Subscriber Hourly Call Minutes per VoIP Service	For a given time frame, shows the total number of call minutes spent for services defined in the system for a specific subscriber.

6.2.4 Web

The Web Monitoring reports provide statistics for web (HTTP) traffic.

Domains

The Domains group includes the following reports:

Report Metrics	Report Topic Name	Description
Activity	Domains Activity	For a given time frame, shows the web domain activity.
Popularity	Domains Popularity	For a given time frame, shows the most popular web domains.
Time of Days Access	Time of Day Access pattern per Domain	For a given time frame, shows the access pattern for a web domain in a certain time of day.
Top	Top Domains	For a given time frame, shows the most popular web domains.
Top	Top Domains Trend	For a given time frame, shows the trend of the most popular web domains.
Trend	Domain Trend	For a given time frame, shows the web domain trend.

Hosts

The Web and Streaming group allows user to compile statistics presenting the most popular servers or hosts for the various predefined system classes (such as Browsing, Streaming, and Downloading) and for user-defined classes.

The Hosts group includes the following reports:

Report Metrics	Report Topic Name	Description
Popularity	Hosts Popularity	For a given time frame, shows the most popular web hosts.
Time of Day Access	Time of Day Access pattern per Host	For a given time frame, shows the access pattern for a web host in a certain time of day.
Top	Top Hosts	For a given time frame, shows the most popular web hosts.

Consumers

The Consumers group includes the following reports:

Report Metrics	Report Topic Name	Description
Consumers	Top Browsing Consumers	For a given time frame, shows the list of the most browsing subscribers.

6.2.5 P2P Group

The P2P group presents some statistics about peer-to-peer traffic.

P2P reports cannot be generated using data collected from the SCE platform running in Asymmetric Routing Classification mode.

Consumers

The Consumers group includes following report topics:

Report Metrics	Report Topic Name	Description
Top	Top P2P Consumers	For a given time frame, shows the most popular P2P consumers for selected domains ordered by traffic volume.
Top	Top P2P Downloader	For a given time frame, shows the most popular P2P download consumers.
Top	Top P2P Uploaders	For a given time frame, shows the most popular P2P upload consumers.

Protocols

The Protocols group includes following report topics:

Report Topic Name	Description
Top P2P Protocols	For a given time frame, shows the most popular P2P protocols for selected domains ordered by traffic volume.

6.2.6 Mobile

The Mobile group includes reports to monitor metrics specific to GSM and CDMA mobile networks.

The topic structure is implemented as per below:

Device Type

The Device Type group includes the following reports:

Report Metrics	Report Topic Name	Description
Distribution	Device Type distribution (IMEI)	For a given time frame, shows the distribution by Device Type popularity.
Volume	Application usage for specific device	For a given time frame, shows the application usage for the selected specific device.
Aggregated Usage	Usage per Device type	For a given time frame, shows the aggregated usage per device.

Figure 75. Sample Report – Mobile Device Type Distribution



Network Type

The Network Type group includes the following reports:

Report Metrics	Report Topic Name	Description
Volume	Application usage for specific Network Type	For a given time frame, shows the application usage for the selected specific network type.
Aggregated Usage	Usage per Network Type	For a given time frame, shows the aggregated usage per network.

APN

The APN group includes the following reports:

Report Metrics	Report Topic Name	Description
Volume	Application usage for specific APN	For a given time frame, shows the application usage for the selected specific APN.
Aggregated Usage	Usage per APN	For a given time frame, shows the aggregated usage per APN.

User Location

The User Location group includes the following reports:

Report Metrics	Report Topic Name	Description
Subscribers	Number of subscribers per User Location	For a given time frame, shows the number of active subscribers per location.
Aggregated Usage	Usage per Location	For a given time frame, shows the aggregated usage per location.

SGSN

The SGSN group includes the following reports:

Report Metrics	Report Topic Name	Description
Aggregated Usage	Usage per SGSN	For a given time frame, shows the aggregated usage per SGSN.

Manufacturer

The Manufacturer group includes the following reports:

Report Metrics	Report Topic Name	Description
Distribution	Mobile Device Manufacturer Distribution (MEID)	For a given time frame, shows the mobile device manufacturers.
Volume	Usage per Manufacturer Device	For a given time frame, shows the usage of mobile manufacturer wise.
Aggregated Usage	Application Usage for specific Manufacturer Device	For a given time frame, shows the usage of application for a specific manufacturer.

Home Agent

The Home Agent group includes the following reports:

Report Metrics	Report Topic Name	Description
Volume	Application Usage for specific Home Agent	For a given time frame, shows the application usage for a home agent.
Aggregated Usage	Usage per Home Agent	For a given time frame, shows the usage home agent wise.

PCF

The PCF group includes the following reports:

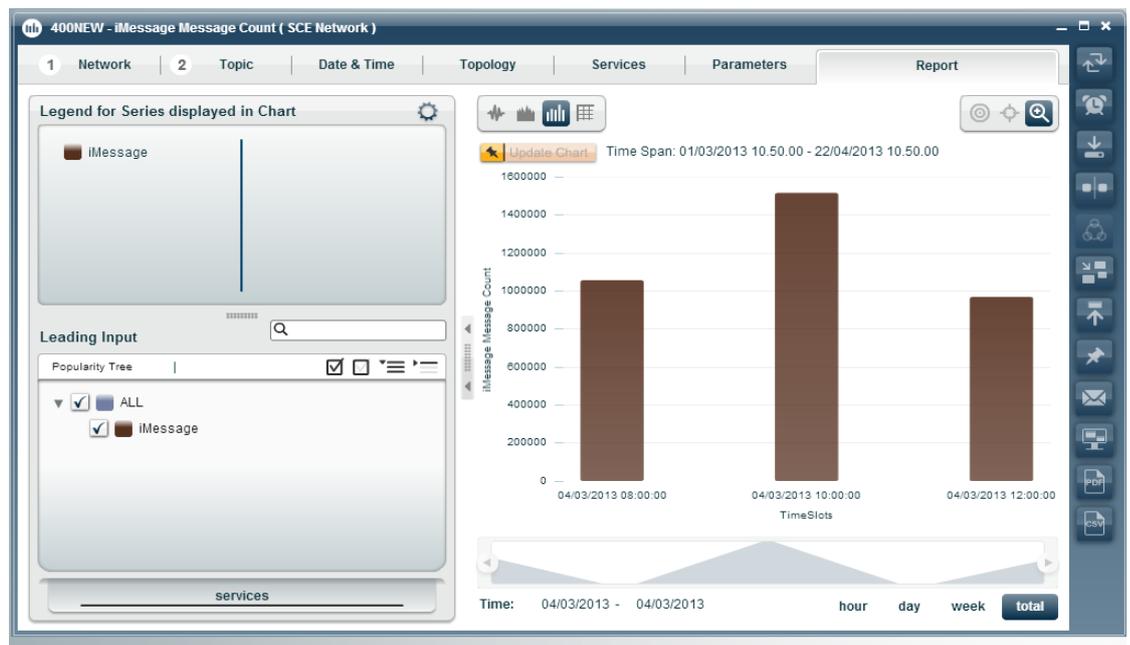
Report Metrics	Report Topic Name	Description
Aggregated Usage	Usage per PCF	For a given time frame, shows the usage PCF wise.

iMessage

The iMessage group provides the following reports to analyze the iMessage mobile app usage:

Report Metrics	Report Topic Name	Description
Message Count	iMessage Message Count	For a given time frame, shows the number of iMessage messages grouped by timeslot.

Figure 76. Sample Report – Mobile – iMessage Message Count

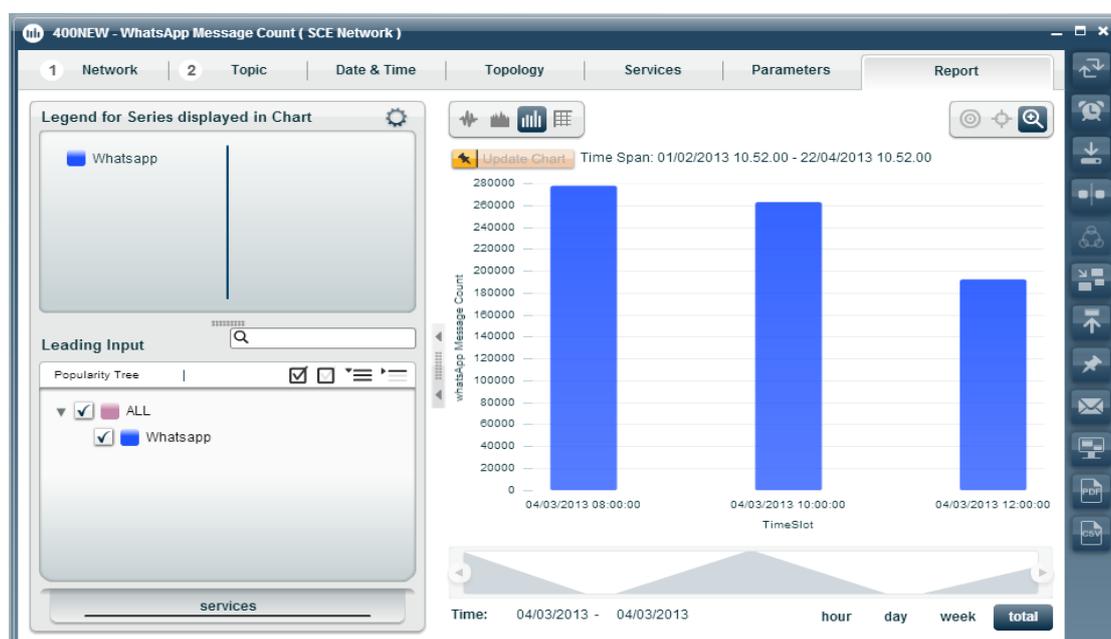


WhatsApp

The WhatsApp group provides the following reports to analyze the WhatsApp mobile app usage:

Report Metrics	Report Topic Name	Description
Message Count	WhatsApp Message Count	For a given time frame, shows the number of WhatsApp messages grouped by timeslot.

Figure 77. Sample Report – Mobile – WhatsApp Message Count

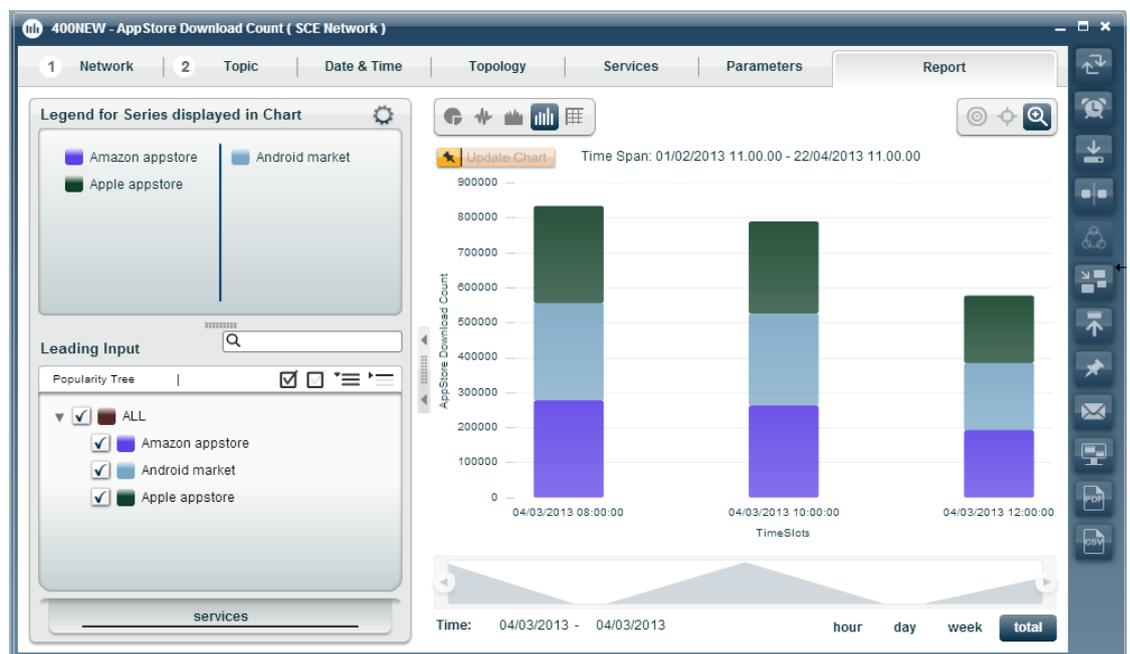


AppStore

The AppStore group provides the following reports to analyze the AppStore mobile app usage:

Report Metrics	Report Topic Name	Description
Download Count	AppStore Download Count	For a given time frame, shows the number of downloads per AppStore type grouped by timeslot..

Figure 78. Sample Report – Mobile – AppStore Download Count



6.2.7 Malicious Traffic

The Malicious Traffic group allows user to view statistics of the malicious events accrued in the system.

DoS

The DoS group includes following reports:

Report Metrics	Report Topic Name	Description
Attacked Subscribers	DoS Attacked Subscribers	For a given time frame, shows the distribution of DoS-attacked subscribers over time for the different IP protocols defined in the system.
Top	Top DoS Attacked Hosts	For a given time frame, shows the most DoS-attacked hosts.
Top	Top DoS Attacked Subscribers	For a given time frame, shows the most DoS-attacked subscribers.

Scans/Attacks

The Scans/Attacks group includes following reports:

Report Metrics	Report Topic Name	Description
Rate	Global Scan or Attack Rate	For a given time frame, shows the global scan or attack rate.
Top	Top Scanned or Attacked ports	For a given time frame, shows the most scanned or attacked ports.
Top	Top Scanning or Attacking Hosts	For a given time frame, shows the most scanning or attacking hosts.
Top	Top Scanning or Attacking Subscribers	For a given time frame, shows the most scanning or attacking subscribers.

SPAM

The Spam group includes following reports:

Report Metrics	Report Topic Name	Description
Distribution	Cumulative Distribution of Subscriber's SMTP Sessions	For a given time frame, shows the cumulative distribution of subscriber's SMTP sessions.
Distribution	Subscriber Average SMTP Sessions	For a given time frame, shows the average SMTP sessions distribution.
Hourly Sessions	Global Hourly Spam Sessions	For a given time frame, shows the hourly spam sessions distribution.
Top	Top Spammers	For a given time frame, shows the top spammers.

Figure 79. Sample Report – Average MOS per SIP Domain



Subscribers

The Subscribers group includes following reports:

Report Metrics	Report Topic Name	Description
Infected	Infected Subscribers	For a given time frame, shows the list of infected subscribers.
Infected	Infected Subscribers vs. Active Subscribers	For a given time frame, shows the distributions of infected and active subscribers.

6.2.8 Traffic Discovery Reports

The Traffic Discovery-Statistics group of report templates allows user to view statistics compiled from the source and destination IP addresses and ports of the system traffic.

The reports cannot be generated using data collected from an SCE platform running in asymmetric routing classification mode.



Note

The reports in this group are not per subscriber; they supply general port and IP address information.

Clients

The Clients group includes following reports:

Report Metrics	Report Topic Name	Description
Top	Top Client IP to Server IP	For a given time frame, shows the most popular Client IP to Server IP for specific domains.
Top	Top Client IP to Server IP and Server Port	For a given time frame, shows the most popular Client IP, Server IP, and Server Port for specific domains.
Top	Top Client IP to Server Port	For a given time frame, shows the most popular Client IP and Server Port for specific domains.
Top	Top Clients	For a given time frame, shows the most popular clients for specific domains.

Protocol

The Protocol group includes following reports:

Report Metrics	Report Topic Name	Description
Generic	Top Protocols	For a given time frame, shows the most popular protocol for specific domains.
IP	Top IP Protocols	For a given time frame, shows the most popular IP protocol for specific domains.
Top	Top P2P Protocols	For a given time frame, show the most popular protocol.

Servers

The Servers group includes following reports:

Report Metrics	Report Topic Name	Description
Distribution by Subscriber Packages	Service Distribution by Subscriber Packages	For a given time frame, shows the most popular Service grouped by the package of the requesting subscriber.
Distribution by Subscriber Packages	FTP Server Distribution by Subscriber Packages	For a given time frame, shows the most popular FTP server grouped by the package of the requesting subscriber.
Distribution by Subscriber Packages	MMS Server Distribution by Subscriber Packages	For a given time frame, shows the most popular MMS server grouped by the package of the requesting subscriber.
Distribution by Subscriber Packages	RTSP Host Distribution by Subscriber Packages	For a given time frame, shows the most popular RTSP host grouped by the package of the requesting subscriber.
Distribution by Subscriber Packages	Web Hosts Distribution by Subscriber Packages	For a given time frame, shows the most popular web host grouped by the package of the requesting subscriber.
Distribution by Subscriber Packages	NNTP Server Distribution by Subscriber Packages	For a given time frame, shows the distribution by Subscriber Packages.
Distribution by Subscriber Packages	POP3 Server Distribution by Subscriber Packages	For a given time frame, shows the distribution by Subscriber Packages.

Distribution by Subscriber Packages	SMTP Server Distribution by Subscriber Packages	For a given time frame, shows the distribution by Subscriber Packages.
Top	Top Server IP to Server Port	For a given time frame, show the most popular Server IP and Server Port for specific domains.
Top	Top Server Ports	For a given time frame, show the most popular server ports for specific domains.
Top	Top Servers	For a given time frame, show the most popular servers for specific domains.
Top	Top FTP Servers	For a given time frame, shows Top FTP servers for selected domains ordered by volume.
Top	Top MMS Servers	For a given time frame, shows Top MMS servers for selected domains ordered by volume.
Top	Top RTSP Hosts	For a given time frame, shows the most popular RTSP servers.
Top	Top Service Servers	For a given time frame, shows the most popular Service servers.
Top	Top Web Hosts	For a given time frame, shows the most popular web servers.
Top	Top Email Account Owners	For a given time frame, shows the most popular Email Account Owners.
Top	Top Email Recipients	For a given time frame, shows the most popular email recipients ordered by selected metric.
Top	Top Email Senders	For a given time frame, shows the most popular email senders ordered by selected metric.
Top	Top Newsgroups	For a given time frame, shows the most popular newsgroups ordered by selected metric.
Top	Top NNTP Consumers	For a given time frame, shows the most popular NNTP consumers ordered by selected metric.
Top	Top NNTP Servers	For a given time frame, shows the most popular NNTP servers for selected domains ordered by traffic volume.
Top	Top POP3 Servers	For a given time frame, shows the most popular POP3 servers for selected domains ordered by traffic volume.

Top	Top SMTP Servers	For a given time frame, shows the most popular SMTP servers for selected domains ordered by traffic volume.
Top	Top Subscriber to Newsgroups	For a given time frame, shows the most popular subscribers to newsgroups.

Services

The Services group includes following report:

Report Metrics	Report Topic Name	Description
Top	Top Service Ports	For a given time frame, shows distribution Server Ports of a certain service for specific domains.

6.3 Running Reports

The Report Wizard module enables a user to run reports for the selected Network.

Through series of steps, user can select a report (through the Topic Tab) and specify the parameters like date range (Date/Time tab) devices (Topology tab), services (Service tab) or applications (Applications tab) to filter the data for generating reports. Report wizard also lets user to choose some other parameters like traffic direction, unit of result and chart type etc. to customize the report result.

Once all selections have been made, user can run the report and see the report result on the final report wizard tab. He can schedule, add the report to Dashboard or gallery, export the report, remember the report, duplicate the report, or simply refresh the report all through report wizard.

- Network
- Topic
- Date and Time
- Topology
- Services
- View
- Parameters
- Protocols

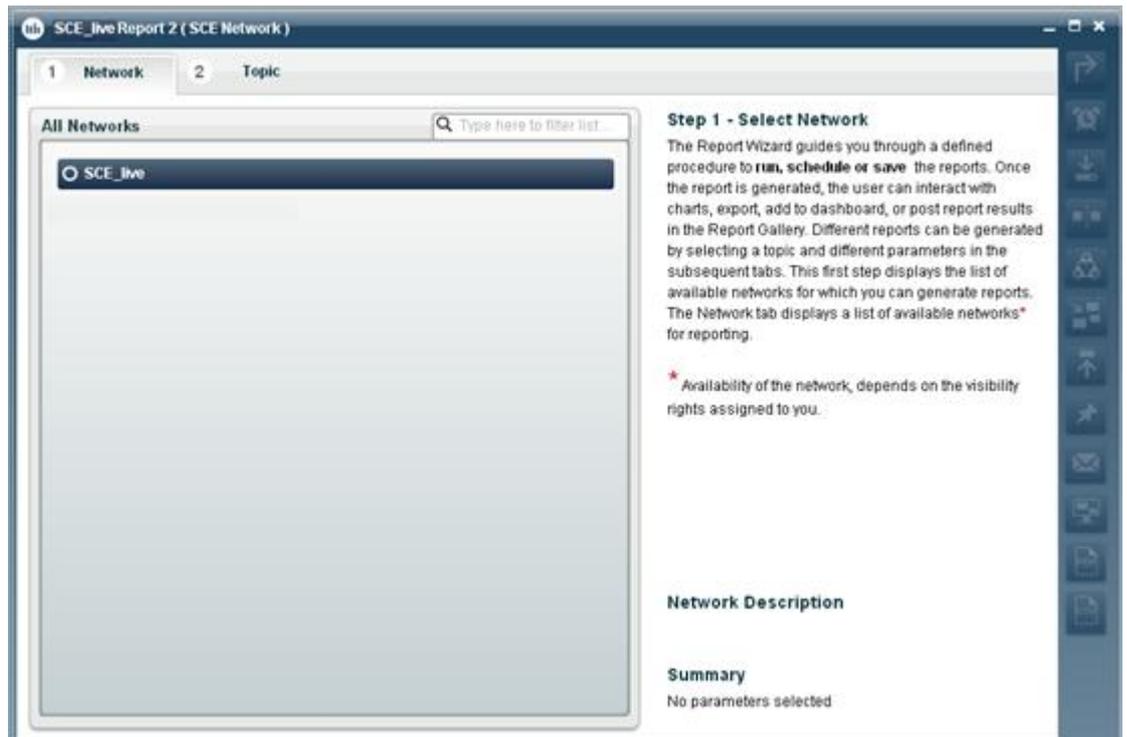
6.3.1 Network

This is the first and the mandatory tab. It shows the list of available that the operator is allowed to see and use for reporting.

If more than one network is available, the last chosen network will become the pre-selected network for the user, at the time of launching a new report wizard.

On clicking the **Network** tab, following screen will appear:

Figure 80. Selecting Network

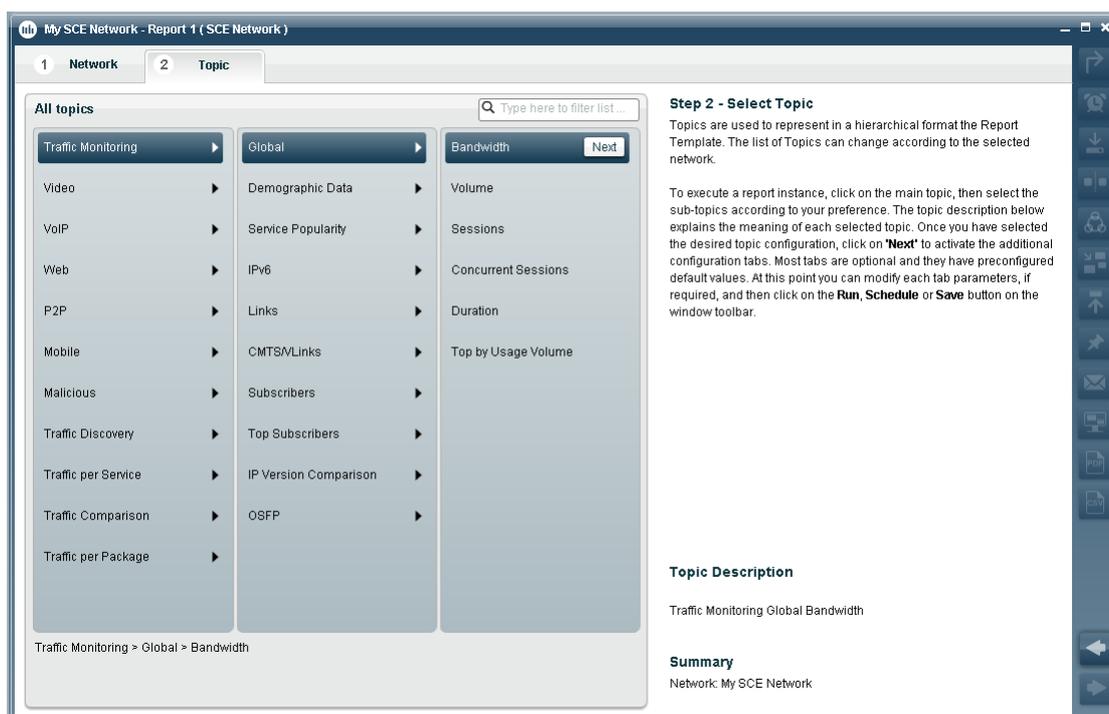


6.3.2 Topic

This is the second tab and it is also mandatory. In the Report wizard, the Topic tab allows the operator to select the desired type of traffic analysis. It shows the available report topics by using multi-step selection (up to three steps) to let the operator select the needed report by specifying the main topic, desired metric, and other report features.

On clicking the **Topic** tab, the following screen will appear:

Figure 81. Selecting Topic



Note

On selecting any report in **Topic** tab by clicking **Next** button, more tabs will appear. Details of those tabs are given below.

6.3.3 Date and Time

This is the third tab and is optional. It has some default settings (usually a time window of the last 24 hours, days or weeks, but this depends on the selected topic). User needs to enter the details in the tab only if user wants to set a different time interval.

To enter the details in the tab with a different time interval, uncheck the **Show Last 24 hours** check box. User can enter date and time by:

- Entering the date and hours manually or using the up and down arrow buttons.
- Clicking on the calendar dates.

For reports supporting a Start date or End date (based on SCE time stamps), can select a time zone option to run the report by:

- Using the time zone of each SCE device.

When the format type is Start date or End date, the operator can also set the time aggregation from the **Aggregation** drop-down list. Not all reports support time aggregation, whereas some reports only allow a limited set of aggregation options. As a consequence, the aggregation drop-down list can be disabled or show only limited values.

The effect of time aggregation on reports will display a time-based X axis with the distribution of samples on specific time intervals, as imposed by the selected aggregation value (For example, 30 minutes, hourly, daily, and so on). For these reports, the metric shown on the Y axis is averaged or summed according to the selected report. For example, if user has selected aggregation value as hourly and the data available is in seconds interval, in that case it will summed the data for each hour and display.

On clicking the **Date & Time** tab, following screen will appear:

Figure 82. Setting the Date and Time



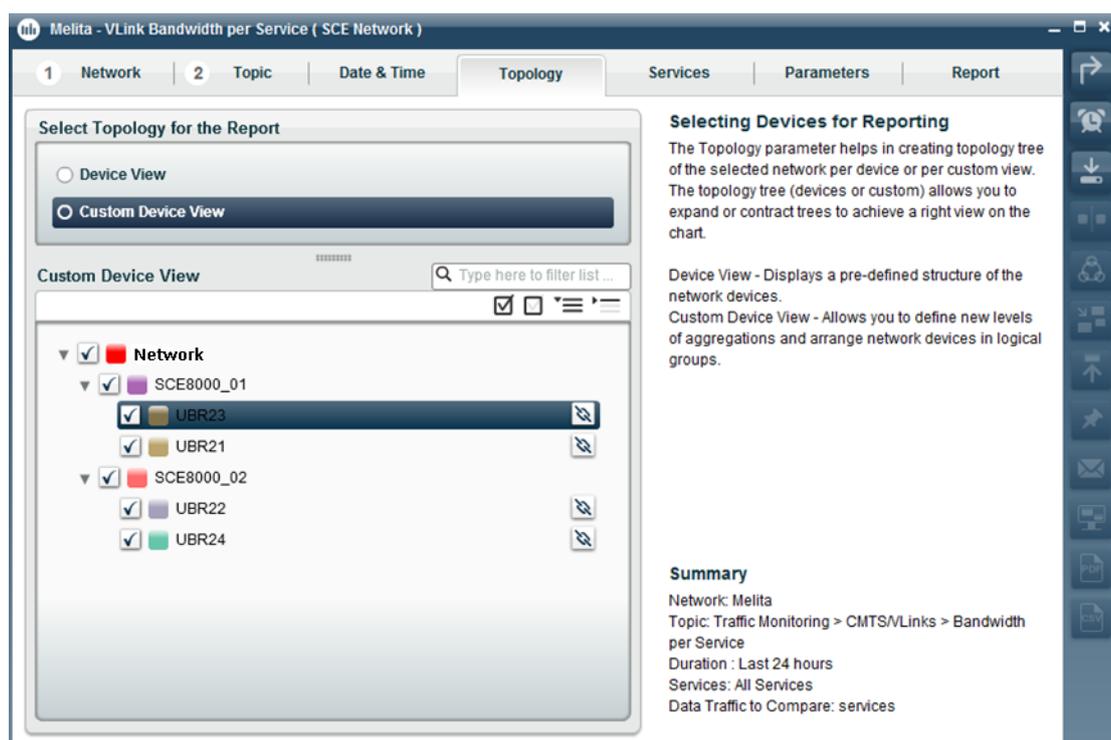
6.3.4 Topology

This tab is optional and dynamic, because it is not always required. It shows the topology view of the selected networks. The trees view (custom or devices) allows either selecting devices easily or grouping of devices to achieve the right view on the chart. User can save the tree configuration in the Report wizard in the form of collapsed or expanded layers.

Topology can be drilled down up to the Links, Virtual Links, or Virtual Channel level for SCE networks to include details in the report generated.

When user clicks the **Topology** tab, following screen will appear:

Figure 83. Selecting Topology



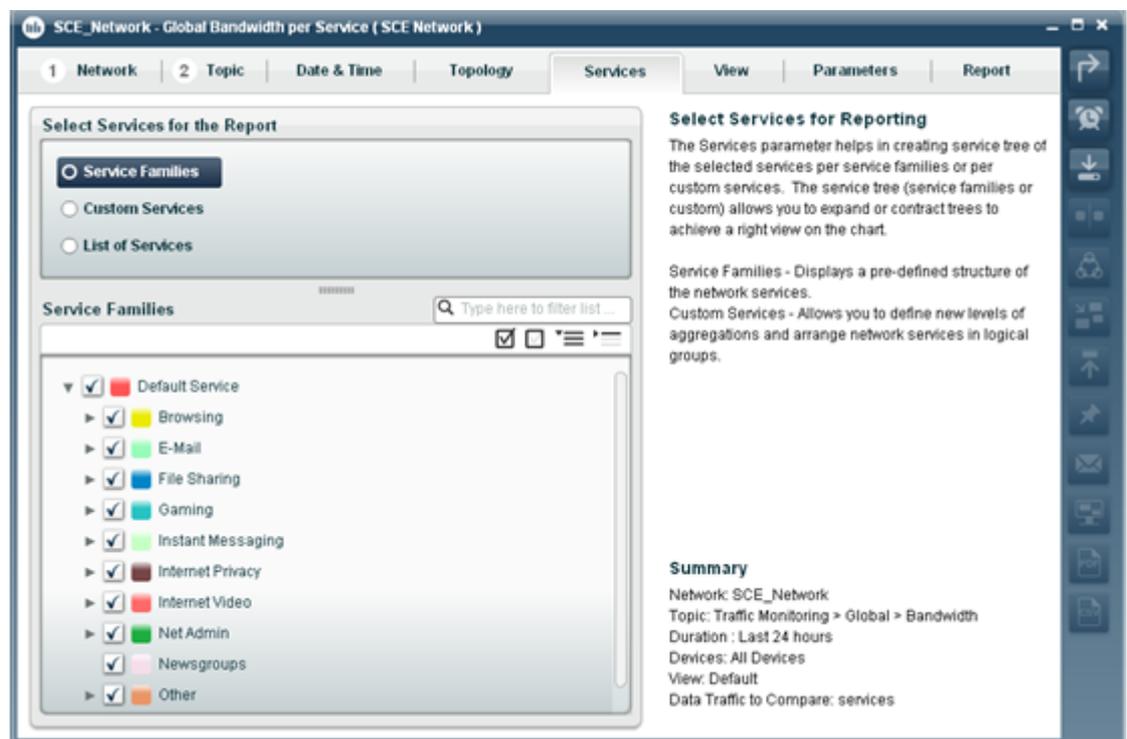
6.3.5 Services

This tab is optional and dynamic, because is not always required. It displays the services enabled in the SCE's of the selected networks.

The operator can switch to the trees view (service families, custom services, or list of services) allowing a better understanding of services and family of services and achieving the right view on the chart. The tree configuration can be saved as personal settings in the form of collapsed or expanded layers.

On clicking the **Services** tab, following screen will appear:

Figure 84. Selecting Services

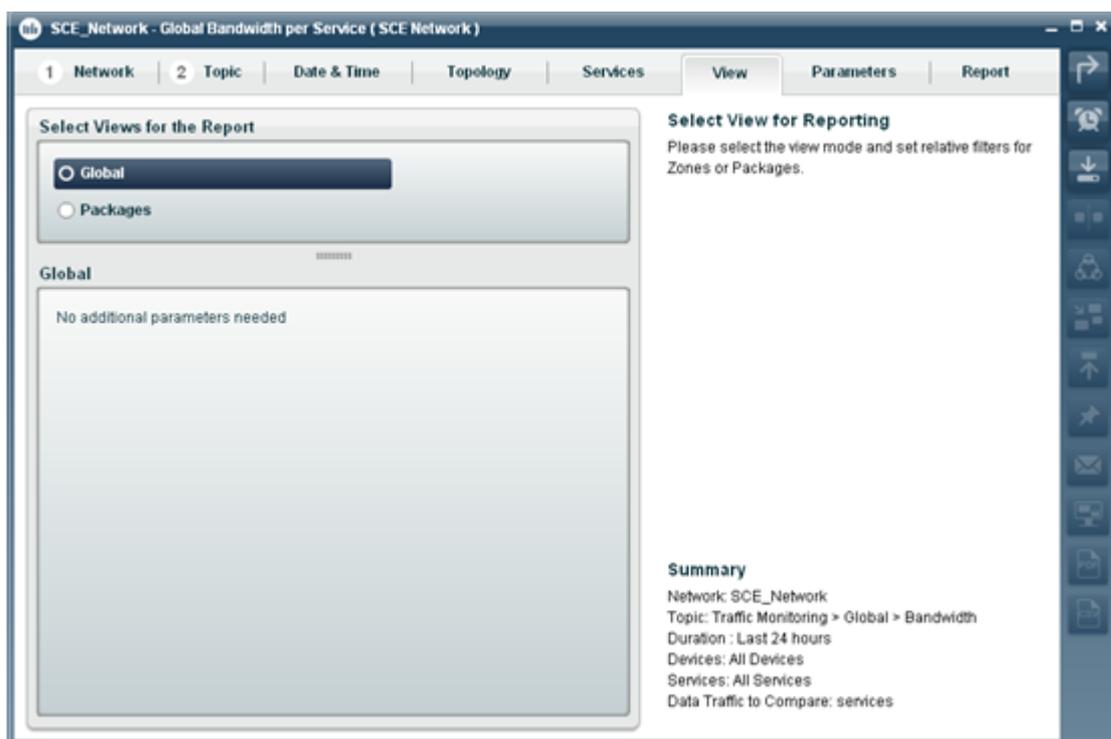


6.3.6 View

This tab is optional and dynamic, because it is required only when user needs to make a choice between package and zone. It shows zone and package lists as alternative selection. User can choose package or zone as the first selection and save this as personal settings for the tab.

On clicking the **View** tab, following screen will appear:

Figure 85. Selecting Views



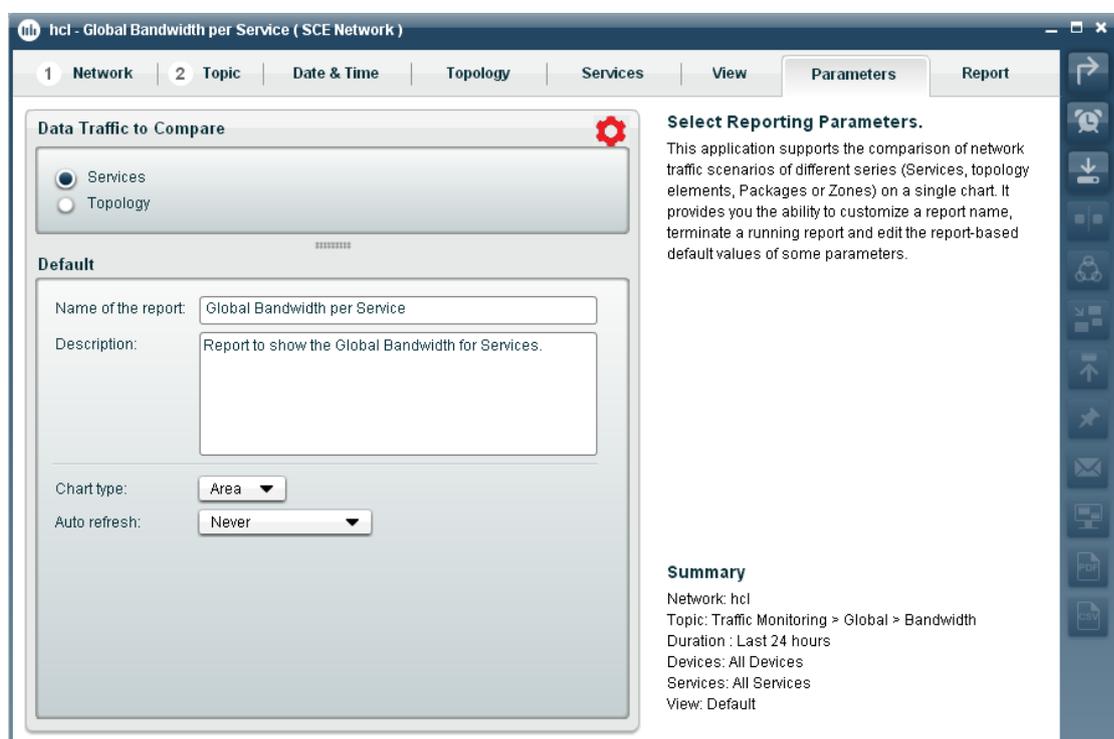
6.3.7 Parameters

As an optional step, the wizard allows setting more optional parameters such as:

- Customization of the report name and description - All reports available in this software have a default name, as taken from the original template. User can provide a customized report name and description in the respective fields.
- Metric unit. User can select any available option (Kbps, Mbps, and Gbps) from the **Metric unit** drop-down list.
- Traffic direction. User can generate the chart in upstream, downstream, or both.
- Chart type. User can get the output chart in the form of a pie, bar, or line diagram.

On clicking the **Parameters** tab, following screen will appear

Figure 86. Setting Parameters



This tab has an advanced section that contains additional parameters. The advanced section can be made visible by clicking on the dedicated wheel button . On clicking the wheel button, some additional parameters will appear on the right panel.

Figure 87. Additional Parameters

The screenshot shows the 'Additional Parameters' configuration window in Cisco Insight Reporter. The window title is 'hcl - Global Bandwidth per Service (SCE Network)'. The 'Parameters' tab is active, showing the following settings:

- Data Traffic to Compare:** Radio buttons for 'Services' (selected) and 'Topology'.
- Default:**
 - Name of the report: Global Bandwidth per Service
 - Description: Report to show the Global Bandwidth for Services.
 - Chart type: Area
 - Auto refresh: Never
- Additional Parameters:**
 - Traffic Direction: aggregated
 - Unit Of Result: Mbps
 - Show Daily Peaks/Total Bandwidth: None
 - Search: Type here to filter list...
 - IP Type list:
 - IPv4
 - IPv6

**Note**

There are different additional parameters for different reports.

Plotting global bandwidth/volume thresholds on charts

Starting from Cisco Insight Reporter release 4.0.0, it is possible to plot traffic thresholds on report charts using the Report Wizard.

**Note**

This feature is currently limited to plotting thresholds for Traffic Monitoring → Global → Bandwidth and/or Volume reports.

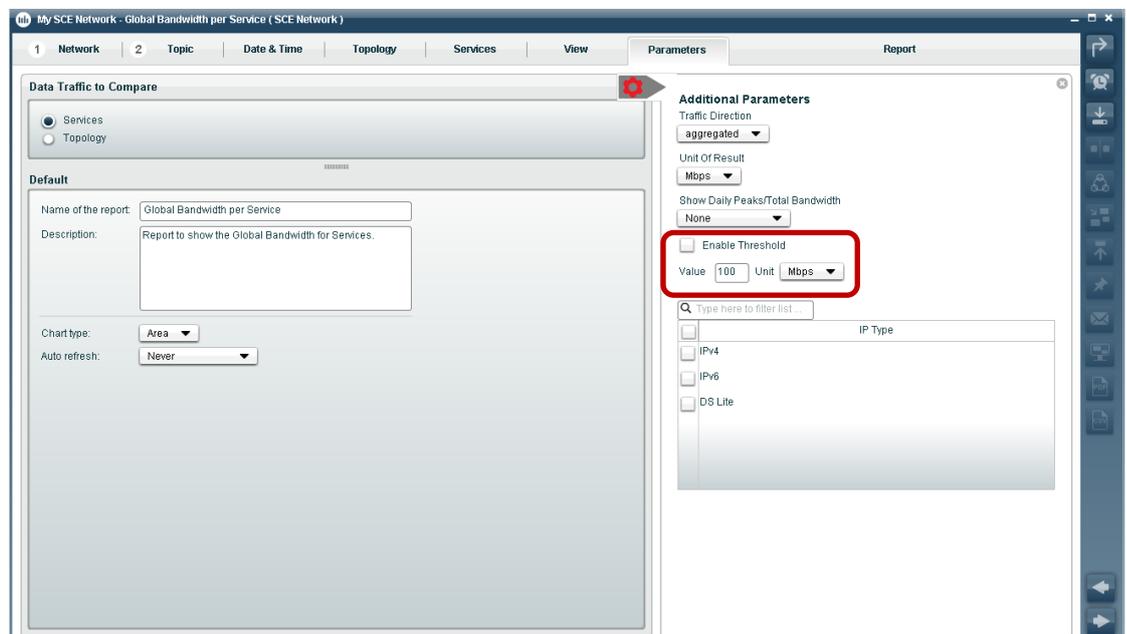
If a global threshold has been scheduled for the selected Network through the Network Wizard, the threshold value available in the Parameters tab of the Report Wizard will be automatically preset with the appropriate value.

If there is no scheduled global threshold defined in the Network Wizard, then it is still possible to plot a graphical threshold on global bandwidth/volume reports.

To enable the threshold line on global bandwidth/volume charts under the Report Wizard, follow the below steps:

- Step 1** Open a Report Wizard window, select the Network and choose the Traffic Monitoring → Global → Bandwidth or Traffic Monitoring → Global → Volume report
- Step 2** In the Parameters tab click on Enable Threshold and set the appropriate value and unit (these will be pre-populated either by default values or by values taken from the scheduled threshold under the Network Wizard, if defined)
- Step 3** The threshold line will be displayed as an independent series on the chart, once the report is generated.

Figure 88. Configure graphical thresholds on Report Wizard



6.3.8 Protocols

This is an optional tab and appears only for selected set of report topics which are configured to show data specific to protocols or applications. On click, following screen will appear:

Figure 89. Protocol Selection

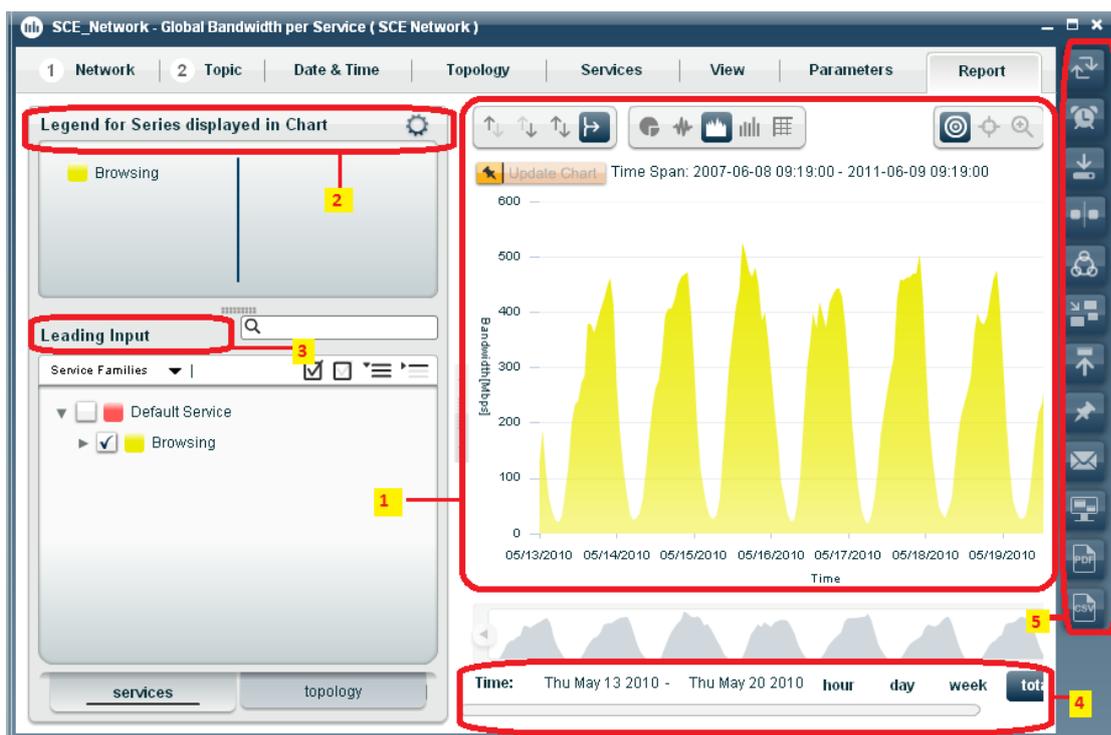
User can go back to some tabs, change some parameters, and then choose to save, run, or schedule a report. This technique can be used to quickly generate, save, or schedule, a series of similar reports without repeating all the steps in the wizard.

6.4 Running an Interactive Report

User executes at least all the mandatory steps in the wizard, the report can be displayed in the **Report** tab by clicking the **Generate Report/Refresh Report** button. The report is interactive and user can perform a series of real-time actions using the different available graphical widgets.

When user executes a report, screen similar to below given screenshot will appear:

Figure 90. Running an Interactive Report



The **Report** tab has five main sections:

Sections	Description
1. Chart	It contains the chart itself, chart name, time span, axis, and labels.
2. Legend for Series displayed in Chart	To the left of the chart, there is a section with two tabs, one with the legend, detailing the series colors and labels, and the second with the list of selected parameters, detailing all the previous selections for the chart.
3. Leading Input	It displays the service tree of the services that appear in the chart and allows user to choose the level of detail based on the Popularity Tree, Service Families, and Custom Tree.

4. Time controller	With time-based reports, under the chart, there is a time controller allowing the change of timeframe to display in the chart.
5. Report Toolbar	It displays different tools related to reports.

**Note**

The current implementation of reports causes all bandwidth samples below 1024 Kbps to be truncated to 0 (zero) when the user selects a higher measurement unit such as Mbps and Gbps.

When the application plots a stacked-area chart containing several "minor" services or applications, these series will disappear when switching from Kbps to Mbps, thus the total amount of traffic could be inaccurate.

6.4.1 Chart

User can generate following type of chart:

1. Pie Chart
 2. Line Chart
 3. Bar Chart
 4. Area Chart
1. **Pie Chart**—A pie chart is a circular chart divided into sectors or slices, illustrating proportion of the total data set.
 2. **Line Chart**—A line chart is a type of chart, which displays data as a series of data points connected by straight line segments.
 3. **Bar Chart**—A bar chart is a chart with rectangular bars with lengths proportional to the values that they represent. If data for different **Leading Inputs** is available for same point of time, in that case it will display stacked bar chart in place of bar chart.
 4. **Area Chart**—An area chart is much like a line chart, but it fills different colors in the areas below the lines. If data for different **Leading Inputs** is available for same point of time, in that case it will display stacked area chart in place of area chart.

**Note**

Sometimes user would be able to generate pie and bar chart for the given data but not the line and area chart. If user doesn't have two data points for the chart, it will not generate the line or area chart.

For example, if the user has different bandwidths corresponding to a date in Global Bandwidth per Application report. In this case, user would be able to generate the pie and bar chart but not the line and area chart as date is same so it would get only one data point (bandwidth) for generating the chart.

Following chart elements are provided:

Figure 91. Chart Elements



Chart Elements	Description
Upstream and downstream details on the same chart 	<p>Reports showing service series and supporting a filter on traffic direction, can display the information about the upstream component only, the downstream only, or both directions.</p> <p>When displaying bidirectional service series (when the traffic direction filter is set to “Both”), a flag allows expanding each service contribution into upstream and downstream components.</p>
Drill-down reports 	<p>The application supports the drill-down feature on interactive charts. When focusing on a specific series, the operator can launch a new report based on the selected series and related to the source report.</p> <p>This feature is used to navigate through different reports when performing some specific analysis.</p> <p>Note Not all reports will support the drill-down option.</p>
Data Marker 	<p>It provides an interactive data indicator that can be positioned on the plot to mark a specific position in terms of coordinates. The data indicator follows the series plot when moved on the chart— so when it is moved in the X-axis direction, the Y-axis positioning will follow the plot automatically and vice versa.</p> <p>The indicator must have a display which provides information about its current location, for example, the relevant X, and Y axis percentage value in the cumulative report.</p> <p>Note When printing or exporting the chart, user can choose to display the indicator or not.</p>
Chart zoom in/out 	<p>In interactive view, user can zoom out interactively and define the level of zoom into the current report chart.</p> <p>Note When printing or exporting a chart after the zoom operation has been used, the layout of the output reproduce what the operator sees on the screen (the information of the applied zoom level is not lost).</p>
Chart Types 	<p>A list of alternative chart types is displayed in the upper-right corner of the Report tab. User can choose any of the chart types before exporting or printing the report.</p>

6.4.2 Legend for Series displayed in Chart

This defines legends used in chart to display the data. If user is displaying data for multiple legends in a chart, sometimes it displays stacked bar chart in place of bar chart, and stacked area chart, in place of area chart because at a single point of time, data could be available for different legends. For example, if the user wants to display file sharing (in mbps) and voice calls (in mbps) data in bar chart, there can be any point of time where data would be available for both (file sharing & voice calls). In that case it will display stacked bar chart in place of bar chart.

6.4.3 Leading Input

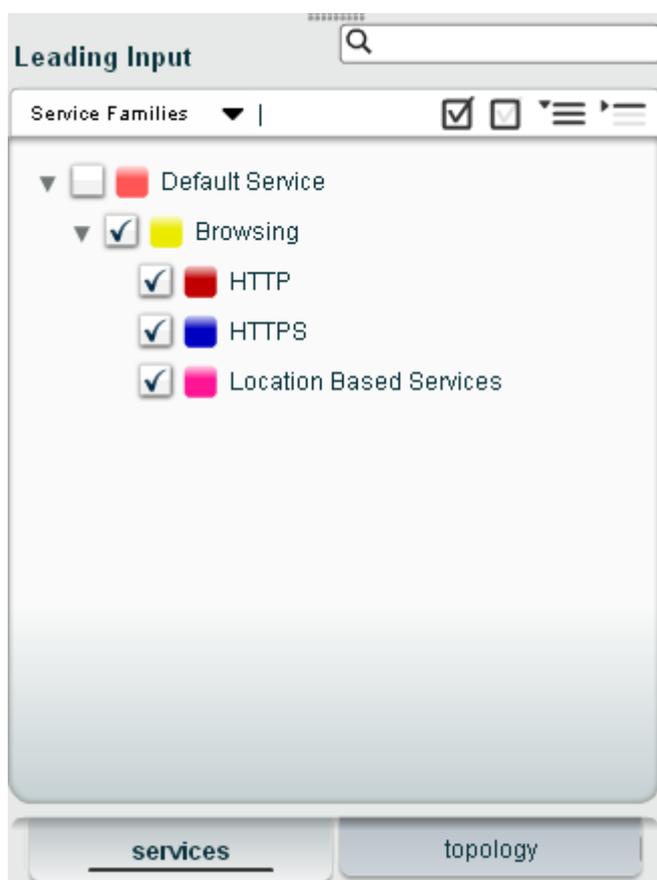
The tree controllers are present on the **Report** tab of the wizard as well. It displays the service tree of the services that appear in the chart and allows user to choose the level of detail based on the tree status.

User can perform operations on the chart such as print or export based on the current hierarchy status of the chart.

User can also define the hierarchy type and the depth of the tree when defining a scheduled report.

The software provides the ability to configure the number of items displayed in the initial group and the number of items displayed on each expansion of 'other'.

Figure 92. Tree Controllers



6.4.4 Time Controller

It describes a multi-graph view feature. It provides the ability to create reports that combine several different series into the same view.

Following time controller, associated with time-based charts and positioned under the time axis, can be an example:

Figure 93. Time Controller



The time controller introduced by this software, supports manual positioning of the sliding time window. User can do that by using the scroll buttons on the extreme corners of the time controller widget.

The software has the following time interval options for trend analysis reports:

- **Hour**—Displays the available data aggregated on hourly interval
- **Day**—Displays the available data aggregated on daily interval
- **Week**—Displays the available data aggregated on weekly interval
- **Month**—Displays the available data aggregated on monthly interval
- **Total**—Displays the available data without any aggregation

The effect of time aggregation on charts will display a time-based X axis with the distribution of samples on specific time intervals, as imposed by the selected time interval. For these reports, the metric shown on the Y axis is averaged or summed according to the selected report. For example, if the user has selected time interval as hourly and the data available is in seconds interval, in that case it will summed the data for each hour and display.

6.4.5 Report Toolbar

This software provides following tools for generating reports:

Figure 94. Report Tools



Chart Elements	Description
	Click to refresh the report.
	Click to schedule the report.
	Click to save the report.
	Click to open a duplicate Report Wizard.
	Click to generate reports which use same tables that current report is using.
	Click to save the report on Dashboard.
	Click to save the report to Report Gallery .

	Click to save the report to Report Gallery but when users logout, report will be deleted from there.
	Click to email the report.
	Click to open the image in Image Viewer.
	Click to open the report in PDF format.
	Click to open the report in CSV format.

When the tab with the report chart is in focus, the toolbar can be used to perform the following operations (according to the capabilities of the connected operator):

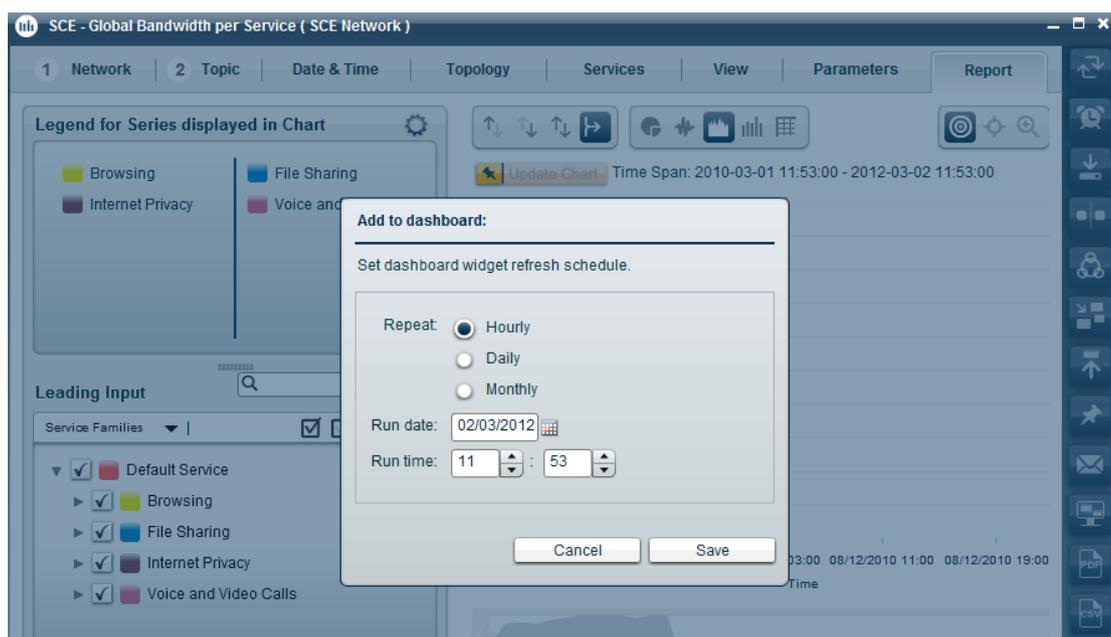
- Chart
- Legend for Series displayed in Chart
- Leading Input
- Time Controller
- Report Toolbar
- Save to Dashboard
- Scheduling a Report
- Saving a Report
- Exporting Report Output

6.4.6 Save to Dashboard

User can save the reports on Dashboard. To save a report to Dashboard, perform the following steps:

- Step 1** Select **Save to Dashboard** option from the toolbar. On selection, following pop-up will appear:

Figure 95. Add to Dashboard



- Step 2** Set all desired parameters (Repeat, Run Date & time) for the report.

- Step 3** Click **Cancel** to return to previous page, or click **Save** to save the report on Dashboard.

6.4.7 Scheduling a Report

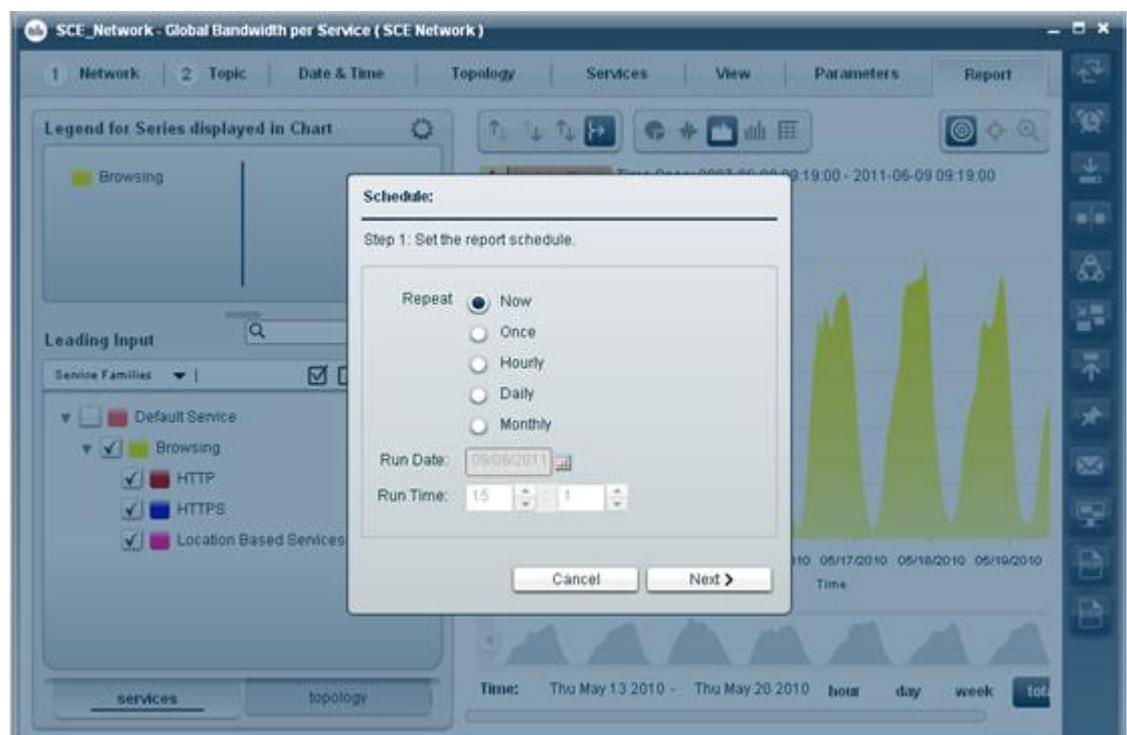
Reports can be run immediately or scheduled to be executed with a programmable delay or with a specific frequency. These reports can further be sent via email to a list of recipients (this software must be configured to communicate with an SMTP server before using this feature).

To schedule a report, perform the following steps:

- Step 1** Select the **Schedule** option from the toolbar. A schedule dialog box will appear allowing the setting of all required parameters.

When user selects the schedule option, following screen will appear:

Figure 96. Schedule Report



- Step 2** Set all desired parameters (time, destination, export format, report name, layout etc.) for the upcoming reports.
- Step 3** Click **Cancel** to return to previous page, or click **Schedule** to schedule the report.

A summary of the scheduled report will be shown under the scheduled reports module. To edit or delete the scheduled reports, click the

Scheduled Reports icon in the Module Launcher.

6.4.8 Saving a Report

When user sets all mandatory parameters of a report or have in focus a generated report, user can save it as a template that can be used during later sessions. A template enables the user to run a report quickly, skipping the wizard steps. User can set a report custom name or use the default.

After a report has been saved, the number on the icon of the launcher gets updated, which shows that a new saved report is available.

6.4.9 Exporting Report Output

When user works with the Report tab in focus, all possible export formats (PDF, image, CSV) are available on the toolbar. When user clicks one of these exports, a dialog box appears, allowing to set what needs to be exported (chart, table, legends, titles, etc), the export format type (PDF, image, CSV), and the template layout.

6.5 Mapping with Database Tables

Following is the list of different database tables associated with different reports:

S.No.	Report Name	Table	Topic
1	IP Version Bandwidth Comparison	RPT_LUR	Traffic Monitoring -> IP Version Comparison ->Bandwidth
2	IP Version Volume Comparison	RPT_LUR	Traffic Monitoring -> IP Version Comparison ->Volume
3	IP Version New IP Flows Comparison	RPT_LUR	Traffic Monitoring -> IP Version Comparison ->New IP Flows
4	IP Version Concurrent IP Flows Comparison	RPT_LUR	Traffic Monitoring -> IP Version Comparison ->Concurrent IP Flows
5	IP Version Duration Comparison	RPT_LUR	Traffic Monitoring -> IP Version Comparison ->Duration
6	Top P2P Downloaders	RPT_TR	P2P Traffic --> Consumers --> Top
7	Top P2P Uploaders	RPT_TR	P2P Traffic --> Consumers --> Top
8	Top P2P Protocols	RPT_TR	Traffic Discovery --> Protocols --> Top P2P
9	Average Subscriber BW per Service	RPT_LUR	Traffic Monitoring --> Subscribers --> Average Bandwidth
10	Average Subscriber BW	RPT_LUR	Traffic Monitoring --> Subscribers --> Average Bandwidth
11	Average Subscriber Concurrent Sessions	RPT_LUR	Traffic Monitoring --> Subscribers --> Average Sessions
12	Average Subscriber Concurrent Sessions per Service	RPT_LUR	Traffic Monitoring --> Subscribers --> Average Sessions
13	Daily peak BW for All Packages	RPT_LUR	Traffic Monitoring --> Global --> Bandwidth
14	Daily peak BW for All Packages	RPT_LUR	Traffic Monitoring --> Global --> Bandwidth

15	Global Bandwidth per Service vs. Total Bandwidth	RPT_LUR	Traffic Monitoring --> Global --> Bandwidth
16	Global Bandwidth per Service comparison	RPT_LUR	Traffic Monitoring --> Global --> Bandwidth
17	Global Aggregated Usage Volume per Service	RPT_LUR	Traffic Monitoring --> Global --> Top by Usage Volume
18	Global Aggregated Usage Volume per Topology	RPT_LUR	Traffic Monitoring --> Global --> Top by Usage Volume
19	Global Bandwidth per Service	RPT_LUR	Traffic Monitoring --> Global --> Bandwidth
20	Global Bandwidth per Topology	RPT_LUR	Traffic Monitoring --> Global --> Bandwidth
21	Global Bandwidth per Traffic Direction	RPT_LUR	Traffic Monitoring --> Global --> Bandwidth
22	Global Concurrent Sessions per Service	RPT_LUR	Traffic Monitoring --> Global --> Concurrent Sessions
23	Global Concurrent Sessions per Topology	RPT_LUR	Traffic Monitoring --> Global --> Concurrent Sessions
24	Global Daily Usage Sessions per Service	RPT_LUR	Traffic Monitoring --> Global --> Sessions
25	Global Daily Usage Sessions per Topology	RPT_LUR	Traffic Monitoring --> Global --> Sessions
26	Global Daily Usage Volume per Service	RPT_LUR	Traffic Monitoring --> Global --> Volume
27	Global Daily Usage Volume per Topology	RPT_LUR	Traffic Monitoring --> Global --> Volume
28	Global Hourly Aggregated Minutes per Service	RPT_LUR	Traffic Monitoring --> Global --> Duration
29	Global Hourly Aggregated Minutes per Topology	RPT_LUR	Traffic Monitoring --> Global --> Duration
30	Global Hourly Usage Sessions per Service	RPT_LUR	Traffic Monitoring --> Global --> Sessions
31	Global Hourly Usage Sessions per Topology	RPT_LUR	Traffic Monitoring --> Global --> Sessions
32	Global Hourly Usage Volume per Service	RPT_LUR	Traffic Monitoring --> Global --> Volume
33	Global Hourly Usage Volume per Topology	RPT_LUR	Traffic Monitoring --> Global --> Volume
34	Global Busy Hours Usage Volume per Service	TOPS_PEAK_PERIOD	Traffic Monitoring --> Global --> Volume
35	Link Daily peak BW for All Packages	RPT_LUR	Traffic Monitoring --> Global --> Bandwidth
36	Link Bandwidth per Service vs. Total Bandwidth	RPT_LUR	Traffic Monitoring --> Global --> Bandwidth
37	Link Bandwidth per Service comparison	RPT_LUR	Traffic Monitoring --> Global --> Bandwidth
38	Link Aggregated Usage Volume per Service	RPT_LUR	Traffic Monitoring --> Link --> Top by Usage Volume
39	Link Aggregated Usage Volume per Topology	RPT_LUR	Traffic Monitoring --> Link --> Top by Usage Volume
40	Link Aggregated Usage Volume Comparison	RPT_LUR	Traffic Monitoring --> Link --> Top by Usage Volume
41	Link Bandwidth per Service	RPT_LUR	Traffic Monitoring --> Link --> Bandwidth
42	Link Bandwidth per Topology	RPT_LUR	Traffic Monitoring --> Link --> Bandwidth
43	Link Bandwidth per Traffic Direction	RPT_LUR	Traffic Monitoring --> Link --> Bandwidth

44	Link Concurrent Sessions per Service	RPT_LUR	Traffic Monitoring --> Link --> Concurrent Sessions
45	Link Concurrent Sessions per Topology	RPT_LUR	Traffic Monitoring --> Link --> Concurrent Sessions
46	Link Daily Usage Sessions per Service	RPT_LUR	Traffic Monitoring --> Link --> Sessions
47	Link Daily Usage Sessions per Topology	RPT_LUR	Traffic Monitoring --> Link --> Sessions
48	Link Daily Usage Volume per Service	RPT_LUR	Traffic Monitoring --> Link --> Volume
49	Link Daily Usage Volume per Topology	RPT_LUR	Traffic Monitoring --> Link --> Volume
50	Link Hourly Aggregated Minutes per Service	RPT_LUR	Traffic Monitoring --> Link --> Duration
51	Link Hourly Aggregated Minutes per Topology	RPT_LUR	Traffic Monitoring --> Link --> Duration
52	Link Hourly Usage Sessions per Service	RPT_LUR	Traffic Monitoring --> Link --> Sessions
53	Link Hourly Usage Sessions per Topology	RPT_LUR	Traffic Monitoring --> Link --> Sessions
54	Link Hourly Usage Volume per Service	RPT_LUR	Traffic Monitoring --> Link --> Volume
55	Link Hourly Usage Volume per Topology	RPT_LUR	Traffic Monitoring --> Link --> Volume
56	Daily peak BW per Package	RPT_PUR	Traffic Monitoring --> Global --> Bandwidth
57	Package Aggregated Usage Volume per Service	RPT_PUR	Traffic Monitoring --> Global --> Top by Usage Volume
58	Package Aggregated Usage Volume per Topology	RPT_PUR	Traffic Monitoring --> Global --> Top by Usage Volume
59	Package Aggregated Usage Volume Comparison	RPT_PUR	Traffic Monitoring --> Global --> Top by Usage Volume
60	Package Bandwidth per Service	RPT_PUR	Traffic Monitoring --> Global --> Bandwidth
61	Package Bandwidth per Topology	RPT_PUR	Traffic Monitoring --> Global --> Bandwidth
62	Package Bandwidth Comparison	RPT_PUR	Traffic Monitoring --> Global --> Bandwidth
63	Package Bandwidth per Service comparison	RPT_PUR	Traffic Monitoring --> Global --> Bandwidth
64	Package Bandwidth per Traffic Direction	RPT_PUR	Traffic Monitoring --> Global --> Bandwidth
65	Package Bandwidth per Service vs. Total Bandwidth	RPT_PUR	Traffic Monitoring --> Global --> Bandwidth
66	Package Concurrent Sessions per Service	RPT_PUR	Traffic Monitoring --> Global --> Concurrent Sessions
67	Package Concurrent Sessions per Topology	RPT_PUR	Traffic Monitoring --> Global --> Concurrent Sessions
68	Package Concurrent Sessions Comparison	RPT_PUR	Traffic Monitoring --> Global --> Concurrent Sessions
69	Package Daily Usage Volume per Service	RPT_PUR	Traffic Monitoring --> Global --> Volume
70	Package Daily Usage Volume per Topology	RPT_PUR	Traffic Monitoring --> Global --> Volume
71	Package Daily Usage Volume Comparison	RPT_PUR	Traffic Monitoring --> Global --> Volume
72	Package Hourly Aggregated Minutes per Service	RPT_PUR	Traffic Monitoring --> Global --> Duration

73	Package Hourly Aggregated Minutes per Topology	RPT_PUR	Traffic Monitoring --> Global --> Duration
74	Package Hourly Aggregated Minutes Comparison	RPT_PUR	Traffic Monitoring --> Global --> Duration
75	Package Hourly Usage Sessions per Service	RPT_PUR	Traffic Monitoring --> Global --> Sessions
76	Package Hourly Usage Sessions per Topology	RPT_PUR	Traffic Monitoring --> Global --> Sessions
77	Package Hourly Usage Sessions Comparison	RPT_PUR	Traffic Monitoring --> Global --> Sessions
78	Package Hourly Usage Volume per Service	RPT_PUR	Traffic Monitoring --> Global --> Volume
79	Package Hourly Usage Volume per Topology	RPT_PUR	Traffic Monitoring --> Global --> Volume
80	Package Hourly Usage Volume Comparison	RPT_PUR	Traffic Monitoring --> Global --> Volume
81	Daily peak BW per Zone	RPT_ZUR	Traffic Monitoring --> Global --> Bandwidth
82	Zone Aggregated Usage Volume per Service	RPT_ZUR	Traffic Monitoring --> Global --> Top by Usage Volume
83	Zone Aggregated Usage Volume per Topology	RPT_ZUR	Traffic Monitoring --> Global --> Top by Usage Volume
84	Zone Aggregated Usage Volume Comparison	RPT_ZUR	Traffic Monitoring --> Global --> Top by Usage Volume
85	Zone Bandwidth per Service	RPT_ZUR	Traffic Monitoring --> Global --> Bandwidth
86	Zone Bandwidth per Topology	RPT_ZUR	Traffic Monitoring --> Global --> Bandwidth
87	Zone Bandwidth Comparison	RPT_ZUR	Traffic Monitoring --> Global --> Bandwidth
88	Zone Bandwidth per Service comparison	RPT_ZUR	Traffic Monitoring --> Global --> Bandwidth
89	Zone Bandwidth per Traffic Direction	RPT_ZUR	Traffic Monitoring --> Global --> Bandwidth
90	Zone Bandwidth per Service vs. Total Bandwidth	RPT_ZUR	Traffic Monitoring --> Global --> Bandwidth
91	Zone Concurrent Sessions per Service	RPT_ZUR	Traffic Monitoring --> Global --> Concurrent Sessions
92	Zone Concurrent Sessions per Topology	RPT_ZUR	Traffic Monitoring --> Global --> Concurrent Sessions
93	Zone Concurrent Sessions Comparison	RPT_ZUR	Traffic Monitoring --> Global --> Concurrent Sessions
94	Zone Daily Usage Sessions per Service	RPT_ZUR	Traffic Monitoring --> Global --> Sessions
95	Zone Daily Usage Sessions per Topology	RPT_ZUR	Traffic Monitoring --> Global --> Sessions
96	Zone Daily Usage Sessions Comparison	RPT_ZUR	Traffic Monitoring --> Global --> Sessions
97	Zone Daily Usage Volume per Service	RPT_ZUR	Traffic Monitoring --> Global --> Volume
98	Zone Daily Usage Volume per Topology	RPT_ZUR	Traffic Monitoring --> Global --> Volume
99	Zone Daily Usage Volume Comparison	RPT_ZUR	Traffic Monitoring --> Global --> Volume
100	Zone Hourly Aggregated Minutes per Service	RPT_ZUR	Traffic Monitoring --> Global --> Duration
101	Zone Hourly Aggregated Minutes per Topology	RPT_ZUR	Traffic Monitoring --> Global --> Duration

102	Zone Hourly Aggregated Minutes Comparison	RPT_ZUR	Traffic Monitoring --> Global --> Duration
103	Zone Hourly Usage Sessions per Service	RPT_ZUR	Traffic Monitoring --> Global --> Sessions
104	Zone Hourly Usage Sessions per Topology	RPT_ZUR	Traffic Monitoring --> Global --> Sessions
105	Zone Hourly Usage Sessions Comparison	RPT_ZUR	Traffic Monitoring --> Global --> Sessions
106	Zone Hourly Usage Volume per Service	RPT_ZUR	Traffic Monitoring --> Global --> Volume
107	Zone Hourly Usage Volume per Topology	RPT_ZUR	Traffic Monitoring --> Global --> Volume
108	Zone Hourly Usage Volume Comparison	RPT_ZUR	Traffic Monitoring --> Global --> Volume
109	Daily peak BW for VLinks	RPT_VLUR	Traffic Monitoring --> CMTS/VLinks --> Bandwidth
110	Top VLinks by Usage Volume	RPT_VLUR	Traffic Monitoring --> CMTS/VLinks --> Top VLinks by Volume
111	Total Active Subscribers per VLink	RPT_VLUR	Traffic Monitoring --> CMTS/VLinks --> Active Subscribers
112	VLink Aggregated Usage Volume per Service	RPT_VLUR	Traffic Monitoring --> CMTS/VLinks --> Top Services by Volume
113	VLink Bandwidth per Package	RPT_DVLINK + RPT_UVLINK	Traffic Monitoring --> CMTS/VLinks --> Bandwidth
114	Vlink Bandwidth per Service	RPT_VLUR	Traffic Monitoring --> CMTS/VLinks --> Bandwidth
115	VLink BW per Cable-Modems group	RPT_VLUR	Traffic Monitoring --> CMTS/VLinks --> Bandwidth
116	VLink Daily Usage Volume per Service	RPT_VLUR	Traffic Monitoring --> CMTS/VLinks --> Volume
117	VLink Hourly Usage Volume per Service	RPT_VLUR	Traffic Monitoring --> CMTS/VLinks --> Volume
118	Daily peak BW for Specific Subscriber	RPT_SUR	Traffic Monitoring --> Subscribers --> Bandwidth
119	Peak Bandwidth per Subscriber for specific Service	RPT_SUR	Traffic Monitoring --> Subscribers --> Bandwidth
120	Subscriber Aggregated Usage Volume per Service	RPT_SUR	Traffic Monitoring --> Subscribers --> Top Services by Usage Volume
121	Subscriber Bandwidth per Service	RPT_SUR	Traffic Monitoring --> Subscribers --> Bandwidth
122	Subscriber Daily Usage Sessions per Service	RPT_SUR	Traffic Monitoring --> Subscribers --> Sessions
123	Subscriber Daily Usage Volume per Service	RPT_SUR	Traffic Monitoring --> Subscribers --> Volume
124	Subscriber Hourly Aggregated Minutes per Service	RPT_SUR	Traffic Monitoring --> Subscribers --> Duration
125	Subscriber Hourly Usage Sessions per Service	RPT_SUR	Traffic Monitoring --> Subscribers --> Sessions
126	Subscriber Hourly Usage Volume per Service	RPT_SUR	Traffic Monitoring --> Subscribers --> Volume
127	Top Subscribers	RPT_TOPS_PERIOD0 RPT_TOPS_PERIOD1 RPT_TOPS_PEAK_PERIOD*	Traffic Monitoring --> Top Subscribers --> List
128	Subscriber Bandwidth Comparison*	RPT_SUR	Traffic Monitoring --> Subscribers --> Aggregated Bandwidth Comparison

129	Subscriber Flows Details*	RPT_FUR	Traffic Monitoring --> Subscribers --> Real-Time Flows
130	Top Client IP to Server IP and Server Port	RPT_TR	Traffic Discovery --> Clients --> Top
131	Top Client IP to Server IP	RPT_TR	Traffic Discovery --> Clients --> Top
132	Top Client IP to Server Port	RPT_TR	Traffic Discovery --> Clients --> Top
133	Top Clients	RPT_TR	Traffic Discovery --> Clients --> Top
134	Top IP Protocols	RPT_TR	Traffic Discovery --> Protocols --> IP
135	Top Protocols	RPT_TR	Traffic Discovery --> Protocols --> Generic
136	Top Server IP to Server Port	RPT_TR	Traffic Discovery --> Servers --> Top
137	Top Servers Ports	RPT_TR	Traffic Discovery --> Servers --> Top
138	Top Servers	RPT_TR	Traffic Discovery --> Servers --> Top
139	Top Service Ports	RPT_TR	Traffic Discovery --> Services --> Top
140	Cumulative Distribution of Subscriber Usage	RPT_TOPS_PERIOD0_CUMULATIVE RPT_TOPS_PEDIOD1_CUMULATIVE RPT_TOPS_PEAK_CUMULATIVE*	Traffic Monitoring --> Demographic Data --> Cumulative Distributions
141	Global Active Subscribers per Service	RPT_LUR	Traffic Monitoring --> Demographic Data --> Active Subscribers
142	Package Active Subscribers per Service	RPT_PUR	Traffic Monitoring --> Demographic Data --> Active Subscribers
143	Zone Active Subscribers per Service	RPT_ZUR	Traffic Monitoring --> Demographic Data --> Active Subscribers
144	Relative Consumption of Top Subscribers	RPT_TOPS_PERIOD0 RPT_TOPS_PERIOD1 RPT_TOPS_PEAK_PERIOD*	Traffic Monitoring --> Top Subscribers --> Relative Consumption
145	Service Popularity among Subscribers (Average)	RPT_LUR	Traffic Monitoring --> Service Popularity --> Average
146	Service Popularity among Subscribers of Specific Package (Average)	RPT_PUR	Traffic Monitoring --> Service Popularity --> Average
147	Service Popularity among Subscribers of Specific Zone (Average)	RPT_ZUR	Traffic Monitoring --> Service Popularity --> Average
148	Service Popularity among Subscribers	RPT_LUR	Traffic Monitoring --> Service Popularity --> Time Analysis
149	Service Popularity among Subscribers of Specific Package	RPT_PUR	Traffic Monitoring --> Service Popularity --> Time Analysis
150	Service Popularity among Subscribers of Specific Zone	RPT_ZUR	Traffic Monitoring --> Service Popularity --> Time Analysis
151	Subscribers Average Consumption	RPT_TOPS_PERIOD0_CUMULATIVE RPT_TOPS_PEDIOD1_CUMULATIVE RPT_TOPS_PEAK_CUMULATIVE*	Traffic Monitoring --> Demographic Data --> Cumulative Distributions
152	Top Subscribers usage distribution per service	RPT_TOPS_PERIOD0 RPT_TOPS_PERIOD1 RPT_TOPS_PEAK_PERIOD*	Traffic Monitoring --> Top Subscribers --> Service Distribution
153	Total Active Subscribers	RPT_LUR	Traffic Monitoring --> Demographic Data --> Total Active Subscribers

154	Service Distribution by Subscriber Packages	RPT_TR	Traffic Discovery --> Servers --> Distribution by Subscriber Packages
155	FTP Server Distribution by Subscriber Packages	RPT_TR	Traffic Discovery --> Servers --> Distribution by Subscriber Packages
156	MMS Server Distribution by Subscriber Packages	RPT_TR	Traffic Discovery --> Servers --> Distribution by Subscriber Packages
157	RTSP Host Distribution by Subscriber Packages	RPT_TR	Traffic Discovery --> Servers --> Distribution by Subscriber Packages
158	Top FTP Servers	RPT_TR	Traffic Discovery --> Servers --> Top
159	Top MMS Servers	RPT_TR	Traffic Discovery --> Servers --> Top
160	Top RTSP Hosts	RPT_TR	Traffic Discovery --> Servers --> Top
161	Top Service servers	RPT_TR	Traffic Discovery --> Servers --> Top
162	Top Web Hosts	RPT_TR	Traffic Discovery --> Servers --> Top
163	Web Host Distribution by Subscriber Packages	RPT_TR	Traffic Discovery --> Servers --> Distribution by Subscriber Packages
164	NNTP Server Distribution by Subscriber Packages	RPT_TR	Traffic Discovery --> Servers --> Distribution by Subscriber Packages
165	POP3 Server Distribution by Subscriber Packages	RPT_TR	Traffic Discovery --> Servers --> Distribution by Subscriber Packages
166	SMTP Server Distribution by Subscriber Packages	RPT_TR	Traffic Discovery --> Servers --> Distribution by Subscriber Packages
167	Top Email Account Owners	RPT_TR	Traffic Discovery --> Servers --> Top
168	Top Email recipients	RPT_TR	Traffic Discovery --> Servers --> Top
169	Top Email senders	RPT_TR	Traffic Discovery --> Servers --> Top
170	Top Newsgroups	RPT_TR	Traffic Discovery --> Servers --> Top
171	Top NNTP Consumers	RPT_TR	Traffic Discovery --> Servers --> Top
172	Top NNTP Servers	RPT_TR	Traffic Discovery --> Servers --> Top
173	Top POP3 Servers	RPT_TR	Traffic Discovery --> Servers --> Top
174	Top SMTP Servers	RPT_TR	Traffic Discovery --> Servers --> Top
175	Top Subscribers To Newsgroup	RPT_TR	Traffic Discovery --> Servers --> Top
176	Top P2P Consumers	RPT_TOPS_PERIOD0 RPT_TOPS_PERIOD1 RPT_TOPS_PEAK_PERIOD*	P2P Traffic --> Consumers --> Top
177	Top P2P Downloaders	RPT_TOPS_PERIOD0 RPT_TOPS_PERIOD1 RPT_TOPS_PEAK_PERIOD*	P2P Traffic --> Consumers --> Top
178	Top P2P Protocols	RPT_TR	Traffic Discovery --> Protocols --> Top
179	Top P2P Uploaders	RPT_TOPS_PERIOD0 RPT_TOPS_PERIOD1 RPT_TOPS_PEAK_PERIOD*	P2P Traffic --> Consumers --> Top
180	Top Talkers	RPT_TOPS_PERIOD0 RPT_TOPS_PERIOD1 RPT_TOPS_PEAK_PERIOD*	VoIP Traffic --> Subscribers --> Top
181	Average MOS per SIP Domains	RPT_MEDIA	VoIP Traffic --> SIP Domains --> Average MOS
182	Calls Duration per SIP Domains	RPT_MEDIA	VoIP Traffic --> SIP Domains --> Calls Duration
183	Global Call Minutes per VoIP Service	RPT_LUR	VoIP Traffic --> Global --> Duration
184	Global Concurrent Calls per VoIP Service	RPT_LUR	VoIP Traffic --> Global --> Concurrent Calls

185	Global Hourly Average VoIP Packets Loss	RPT_MEDIA	VoIP Traffic --> QoS --> Hourly Average
186	Global Hourly Average VoIP MOS	RPT_MEDIA	VoIP Traffic --> QoS --> Hourly Average
187	Global Hourly Average VoIP Jitter	RPT_MEDIA	VoIP Traffic --> QoS --> Hourly Average
188	Global Hourly Call Minutes per VoIP Service	RPT_LUR	VoIP Traffic --> Global --> Duration
189	Global VoIP Codec Distribution	RPT_MEDIA	VoIP Traffic --> QoS --> Distribution
190	Global VoIP Jitter	RPT_MEDIA	VoIP Traffic --> QoS --> Global
191	Global VoIP MOS Distribution	RPT_MEDIA	VoIP Traffic --> QoS --> Distribution
192	Global VoIP MOS	RPT_MEDIA	VoIP Traffic --> QoS --> Global
193	Global VoIP Packets Loss	RPT_MEDIA	VoIP Traffic --> QoS --> Global
194	Number of Calls per SIP Domains	RPT_MEDIA	VoIP Traffic --> SIP Domains --> Number of Calls
195	Package Concurrent Calls per VoIP Service	RPT_PUR	VoIP Traffic --> Global --> Concurrent Calls
196	Package Hourly Call Minutes per VoIP Service	RPT_PUR	VoIP Traffic --> Global --> Duration
197	Zone Concurrent Calls per VoIP Service	RPT_ZUR	VoIP Traffic --> Global --> Concurrent Calls
198	Zone Hourly Call Minutes per VoIP Service	RPT_ZUR	VoIP Traffic --> Global --> Duration
199	Subscriber Hourly Call Minutes per VoIP Service	RPT_SUR	VoIP Traffic --> Subscribers --> Duration
200	Global Bandwidth per VoIP Service	RPT_LUR	VoIP Traffic --> Global --> Bandwidth
201	Package Bandwidth per VoIP Service	RPT_PUR	VoIP Traffic --> Global --> Bandwidth
202	Zone Bandwidth per VoIP Service	RPT_ZUR	VoIP Traffic --> Global --> Bandwidth
203	Subscriber Bandwidth per VoIP Service	RPT_SUR	VoIP Traffic --> Subscribers --> Bandwidth
204	Top SIP Domains by Unique Users	RPT_MEDIA	VoIP Traffic --> SIP Domains --> Top
205	Top SIP Domains	RPT_MEDIA	VoIP Traffic --> SIP Domains --> Top
206	Top SIP User Agents	RPT_MEDIA	VoIP Traffic --> SIP Domains --> Top User Agents
207	Global Bandwidth per Video Service	RPT_LUR	Video Traffic --> Bandwidth monitoring
208	Package Bandwidth per Video Service	RPT_PUR	Video Traffic --> Bandwidth monitoring
209	Zone Bandwidth per Video Service	RPT_ZUR	Video Traffic --> Bandwidth monitoring
210	Time of Day Access pattern per Video Host	RPT_TOP_VIDEO_H OSTs	Video Traffic --> Hosts --> Time of Day Access
211	Time of Day Access pattern per Video Provider	RPT_TOP_VIDEO_D OMAINS	Video Traffic --> Providers --> Time of Day Access
212	Top Video Consumers	RPT_TOPS_PERIOD0 RPT_TOPS_PERIOD1 RPT_TOPS_PEAK_PERIOD*	Video Traffic --> Consumers --> Top
213	Top Video Hosts	RPT_TOP_VIDEO_H OSTs	Video Traffic --> Hosts --> Top

214	Top Video Providers Trend	RPT_TOP_VIDEO_D OMAINS	Video Traffic --> Providers --> Top
215	Top Video Providers	RPT_TOP_VIDEO_D OMAINS	Video Traffic --> Providers --> Top
216	Video Hosts Popularity	RPT_TOP_VIDEO_H OSTS	Video Traffic --> Hosts --> Popularity
217	Video Provider Trend	RPT_TOP_VIDEO_D OMAINS	Video Traffic --> Providers --> Trend
218	Video Providers Activity	RPT_TOP_VIDEO_D OMAINS	Video Traffic --> Providers --> Activity
219	Video Providers Popularity	RPT_TOP_VIDEO_D OMAINS	Video Traffic --> Providers --> Popularity
220	Global Video Service Distribution	RPT_LUR	Video Traffic --> Services --> Distribution
221	Package Video Service Distribution	RPT_PUR	Video Traffic --> Services --> Distribution
222	Zone Video Service Distribution	RPT_ZUR	Video Traffic --> Services --> Distribution
223	Domain Trend	RPT_TOP_HTTP_DO MAINS	Web Traffic --> Domains --> Trend
224	Domains Activity	RPT_TOP_HTTP_DO MAINS	Web Traffic --> Domains --> Activity
225	Domains Popularity	RPT_TOP_HTTP_DO MAINS	Web Traffic --> Domains --> Popularity
226	Hosts Popularity	RPT_TOP_HTTP_HO STS	Web Traffic --> Hosts --> Popularity
227	Time of Day Access pattern per Domain	RPT_TOP_HTTP_DO MAINS	Web Traffic --> Domains --> Time of Day Access
228	Time of Day Access pattern per Host	RPT_TOP_HTTP_HO STS	Web Traffic --> Hosts --> Time of Day Access
229	Top Browsing Consumers	RPT_TOPS_PERIOD0 RPT_TOPS_PERIOD1 RPT_TOPS_PEAK_PE RIOD*	Web Traffic --> Consumers --> Top
230	Top Domains Trend	RPT_TOP_HTTP_DO MAINS	Web Traffic --> Domains --> Top Trend
231	Top Domains	RPT_TOP_HTTP_DO MAINS	Web Traffic --> Domains --> Top
232	Top Hosts	RPT_TOP_HTTP_HO STS	Web Traffic --> Hosts --> Top
233	DoS Attacked Subscribers	RPT_MALUR	Malicious Traffic --> DoS --> Attacked Subscribers
234	Global Scan or Attack Rate	RPT_MALUR	Malicious Traffic --> Scans/Attacks --> Rate
235	Infected Subscribers vs. Active Subscribers	RPT_MALUR	Malicious Traffic --> Subscribers --> Infected
236	Infected Subscribers	RPT_MALUR	Malicious Traffic --> Subscribers --> Infected
237	Top DoS Attacked Hosts	RPT_MALUR	Malicious Traffic --> DoS --> Top
238	Top DoS Attacked Subscribers	RPT_MALUR	Malicious Traffic --> DoS --> Top
239	Top Scanned or Attacked ports	RPT_MALUR	Malicious Traffic --> Scans/Attacks --> Top
240	Top Scanning or Attacking Hosts	RPT_MALUR	Malicious Traffic --> Scans/Attacks --> Top
241	Top Scanning or Attacking Subscribers	RPT_MALUR	Malicious Traffic --> Scans/Attacks --> Top

242	IP Version Bandwidth Comparison	RPT_LUR + RPT_GUR	Traffic Monitoring --> IPv6 --> IPv6/IPv4 Bandwidth Comparison
243	Tunneled IPv6 Active Subscribers	RPT_LUR + RPT_GUR	Traffic Monitoring --> IPv6 --> Tunneled Active Subscribers
244	Tunneled IPv6 Average Subscriber Bandwidth	RPT_GUR	Traffic Monitoring --> IPv6 --> Tunneled Average Subscriber Bandwidth
245	Tunneled IPv6 Concurrent Sessions	RPT_GUR	Traffic Monitoring --> IPv6 --> Tunneled Concurrent Sessions
246	Top Spammers	RPT_SPAM	Malicious Traffic --> Spam --> Top
247	Global Hourly Spam sessions	RPT_SPAM	Malicious Traffic --> Spam --> Hourly Sessions
248	Cumulative distribution of subscriber's SMTP sessions	RPT_TOPS_PERIOD0_CUMULATIVE RPT_TOPS_PEDIOD1_CUMULATIVE RPT_TOPS_PEAK_CUMULATIVE*	Malicious Traffic --> Spam --> Distributions
249	Subscriber average SMTP sessions	RPT_TOPS_PERIOD0_CUMULATIVE RPT_TOPS_PEDIOD1_CUMULATIVE RPT_TOPS_PEAK_CUMULATIVE*	Malicious Traffic --> Spam --> Distributions
250	Device Type distribution (IMEI)	RPT_TOP_DEVICE_TYPE	Mobile --> Device Type --> Distribution
251	Application usage for specific device	RPT_TOP_DEVICE_TYPE	Mobile --> Device Type --> Usage Volume per Service
252	Usage per Device type	RPT_TOP_DEVICE_TYPE	Mobile --> Device Type --> Aggregated Usage
253	Application usage for Specific Network Type	RPT_TOP_NETWORK_TYPE	Mobile --> Network Type --> Usage Volume per Service
254	Usage per Network Type	RPT_TOP_NETWORK_TYPE	Mobile --> Network Type --> Aggregated Usage
255	Application usage for Specific APN	RPT_TOP_APN	Mobile --> APN --> Usage Volume per Service
256	Usage per APN	RPT_TOP_APN	Mobile --> APN --> Aggregated Usage
257	Number of subscribers per location	RPT_TOP_USER_LOCATION	Mobile --> User Location --> Active Subscribers
258	Usage per Location	RPT_TOP_USER_LOCATION	Mobile --> User Location --> Aggregated Usage
259	Usage per SGSN	RPT_TOP_SGSN	Mobile --> SGSN --> Aggregated Usage
260	iMessage Message Count	RPT_LUR	Mobile --> iMessage --> Message Count
261	WhatsApp Message Count	RPT_LUR	Mobile --> WhatsApp --> Message Count
262	AppStore Download Count	RPT_LUR	Mobile --> AppStore --> Download Count
263	OS Hits	RPT_OSF	Traffic Monitoring --> OSFP --> OS Hits
264	Top OS	RPT_OSF	Traffic Monitoring --> OSFP --> Top OS
265	Subscriber List	RPT_OSF	Traffic Monitoring --> OSFP --> Subscriber List

6.6 My Favorites

Using **My Favorite** icon, user can access saved reports without performing any required steps, and can view the Thematic Dashboards.

Features supported by **My Favorites** menu are:

- Reports
-

- Thematic Dashboards

6.6.1 Reports

User can select all mandatory parameters of a report and save it as a template that can be used later. The report template allows running reports while skipping all the wizard steps. User can set a report custom name or use the default.

To access and display the saved reports, click the **Reports** tab of **My Favorites** icon  on the Module Launcher.

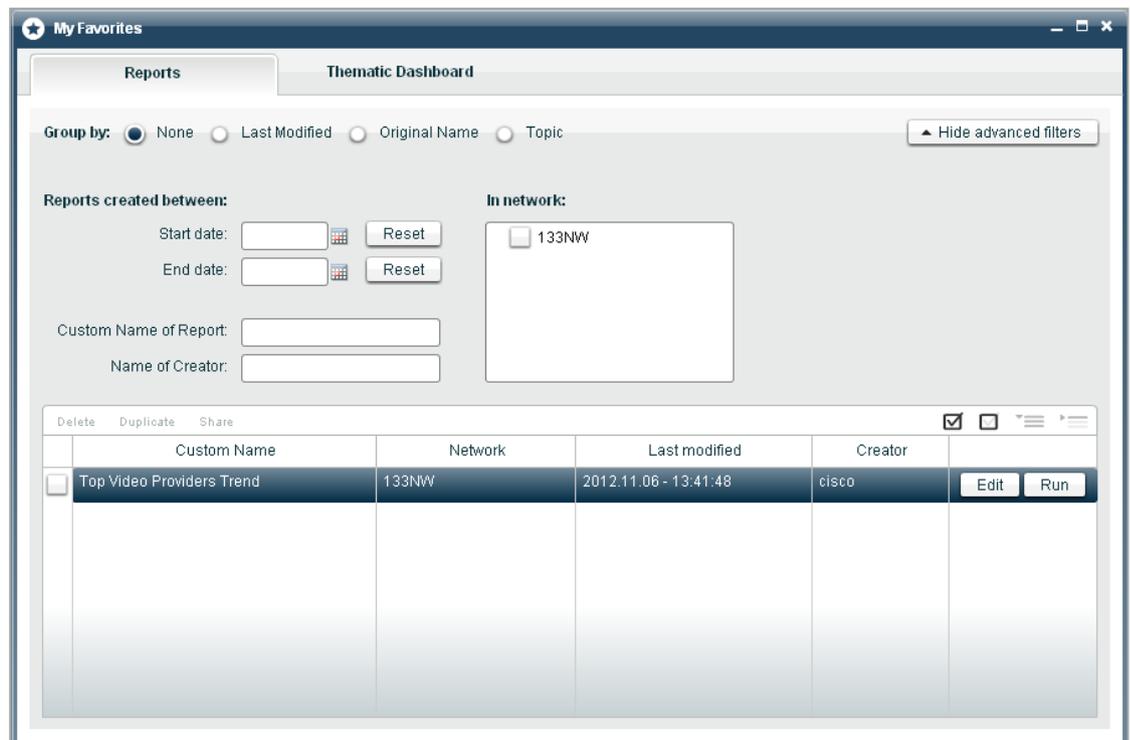
It shows a list of report templates, with report custom name, network, modified date, and creator name. User can search for the report from the list and can use the filters.

To use the filter, perform the following steps:

-
- Step 1** Click the **Additional Filters** option on the top-right corner of the **My Favorites** module. The various filter options are displayed.
 - Step 2** Filter and sort reports using any one of following criteria— **Creation date**, **Network name**, **Custom name** of the report, **Creators name**, etc.
-

On filtering the reports, following filters will appear:

Figure 97. Filtering Reports



On applying the above mentioned filters, the report list gets updated.

With the saved reports, following actions can be performed:

-

- Sharing a Report Definition
- Duplicating a Report Definition

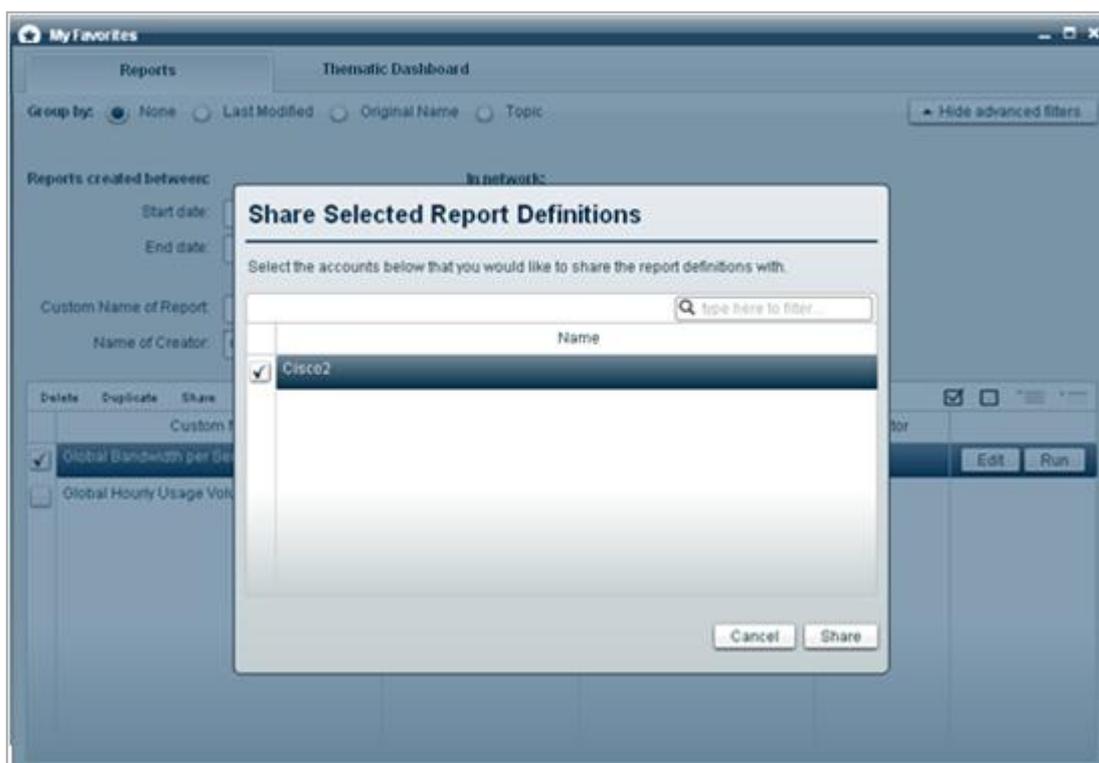
Sharing a Report Definition

User can customize the parameters to generate the reports according to their requirement means they can set report definition as required. By default, a report definition is user specific but the user can share that.

To share a report definition, perform the following steps:

- Step 1** Select the report definitions user wants to share.
- Step 2** Click **Share Selected**. On clicking the **Share Selected Report Definitions** following dialog box will appear.

Figure 98. Sharing Report Definition



- Step 3** Select the network group whose visibility rights are compatible with the selected favorite report.
- Step 4** Click **Share**. Each target account will get a copy of the select report in the respective favorite lists.



Note

Because this operation creates a new element in the favorite report list of the target accounts, a notification gets displayed on the favorite report module on the Module Launcher of those accounts.

Similarly, the user can un-share a shared report definition.

Duplicating a Report Definition

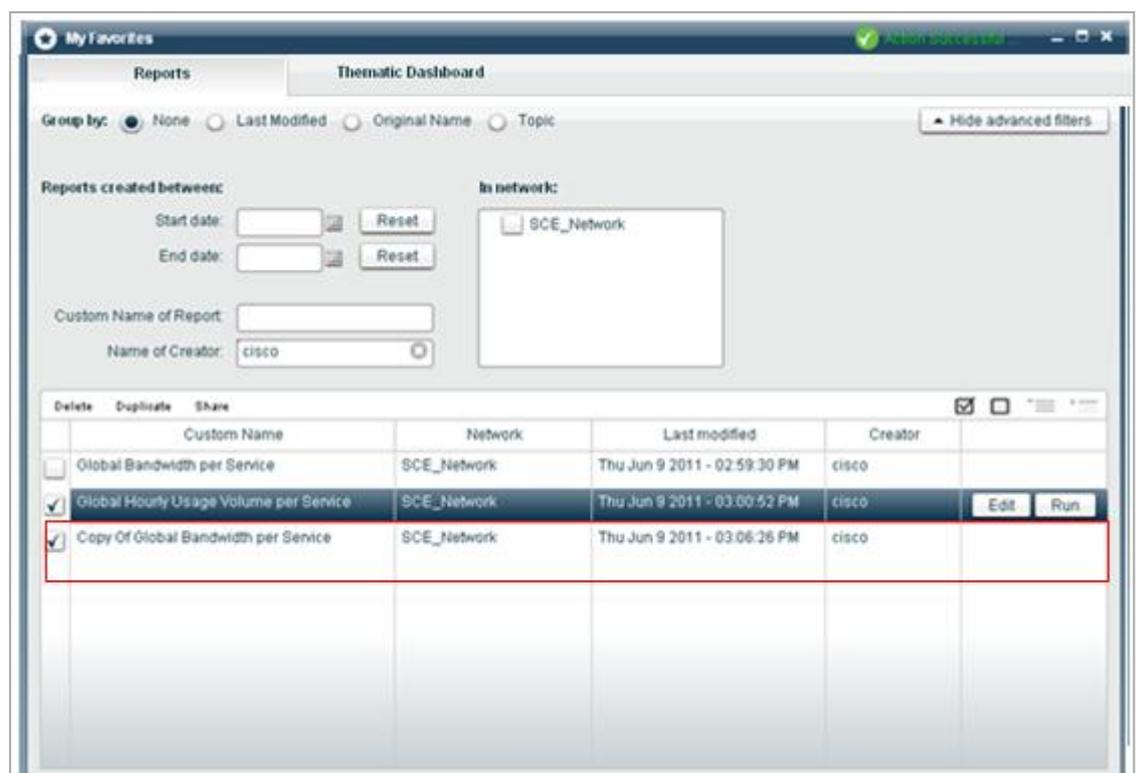
User can quickly create the exact copy of a selected report and can conveniently change only a subset of parameters as needed. This allows the user to open and compare several charts on a single screen.

To duplicate a report definition, perform the following steps:

-
- Step 1** Select the report definitions that user wants to duplicate.
 - Step 2** Select the **Duplicate Selected** option.
-

When user selects **Duplicate Selected**, following screen will appear:

Figure 99. Duplicating a Report Definition



The duplicated report definitions are labeled as Copy of (old report name) and are selected by default after duplication.

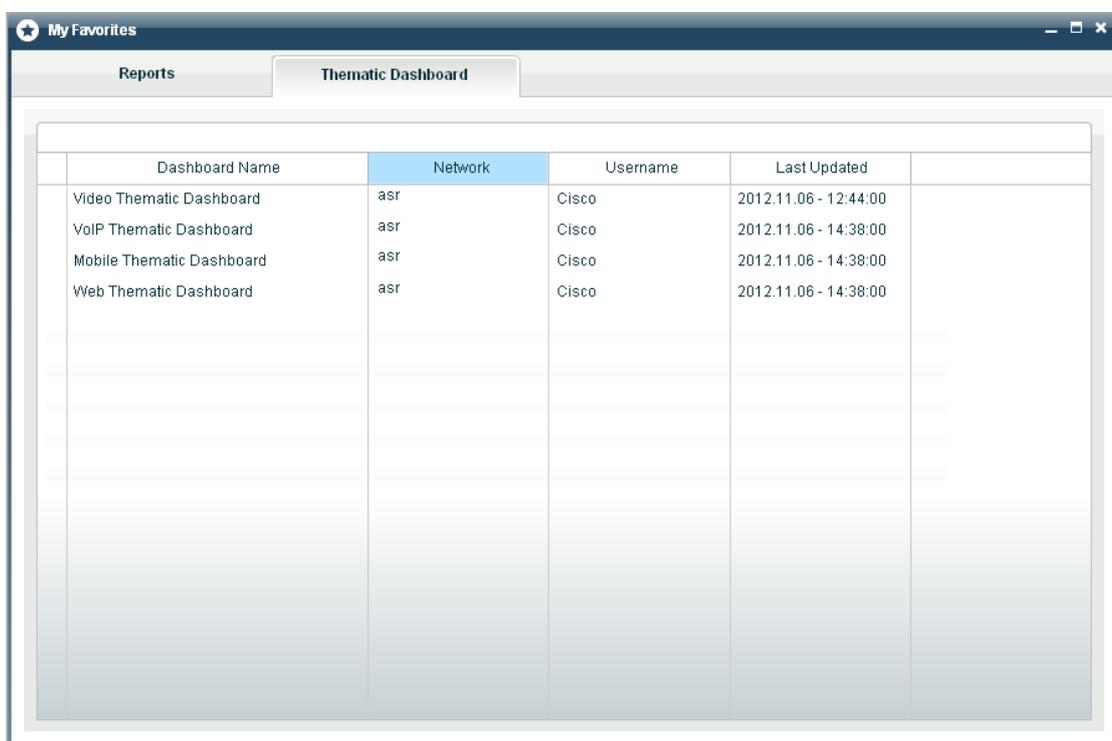
6.6.2 Thematic Dashboards

Thematic Dashboards are preconfigured dashboards for specific report categories.

The following four types of Thematic Dashboards are currently supported:

1. VOIP Thematic Dashboard
2. Mobile Thematic Dashboard
3. Web Thematic Dashboard
4. Video Thematic Dashboard

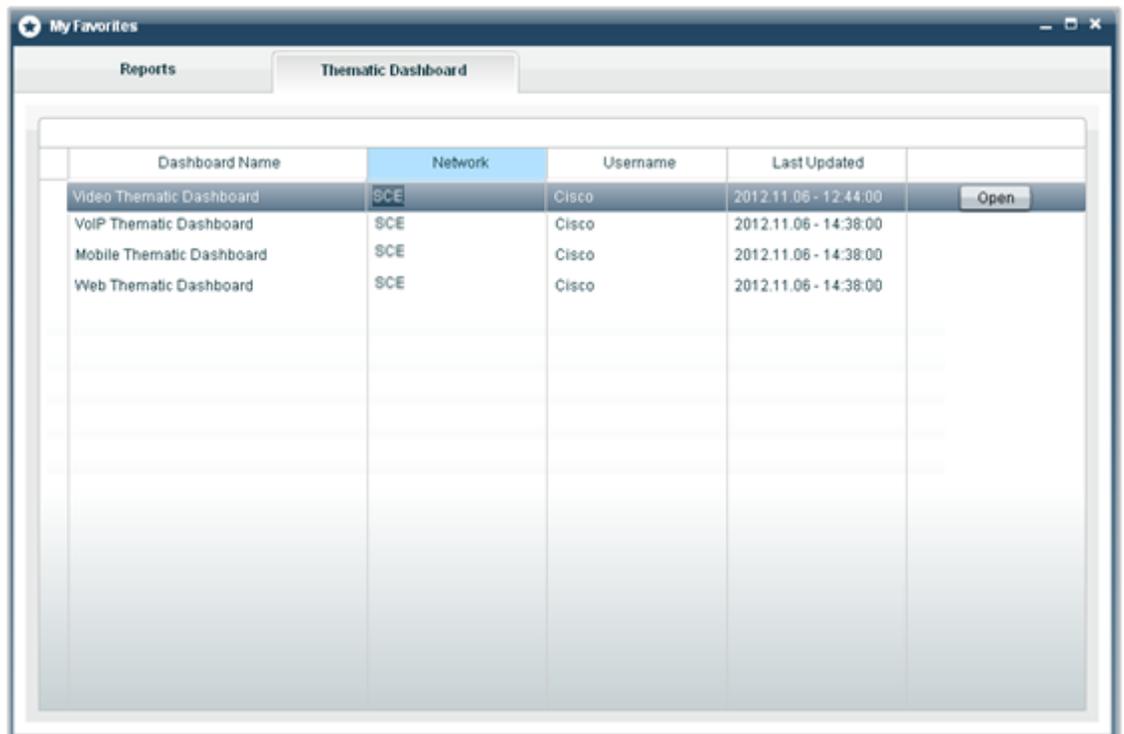
Figure 100. Thematic Dashboard



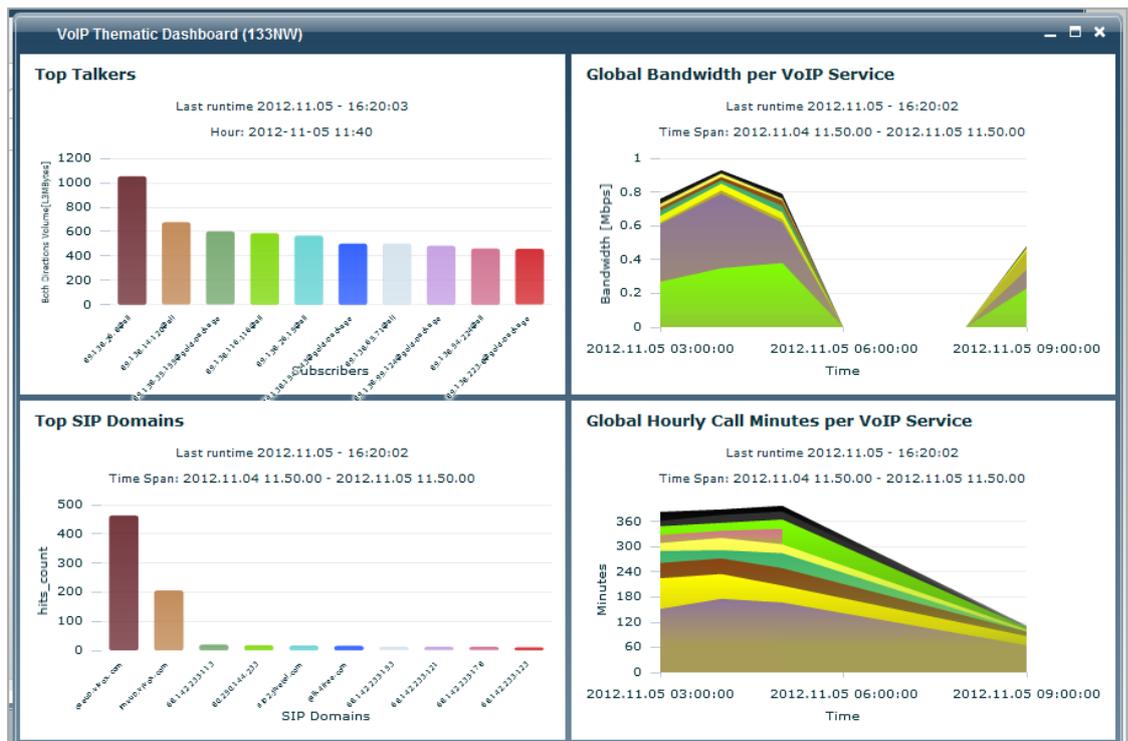
Dashboard Name	Network	Username	Last Updated
Video Thematic Dashboard	asr	Cisco	2012.11.06 - 12:44:00
VoIP Thematic Dashboard	asr	Cisco	2012.11.06 - 14:38:00
Mobile Thematic Dashboard	asr	Cisco	2012.11.06 - 14:38:00
Web Thematic Dashboard	asr	Cisco	2012.11.06 - 14:38:00

These Thematic Dashboards are pre-configured with a list of reports taken from the report template for each category and displays data using default selection given in report template.

To view the Thematic Dashboard for a report category, click **Open** button corresponding to that category.

Figure 101. Opening a Thematic Dashboard

On clicking the **Open** button, a new window will appear.

Figure 102. VOIP Thematic Dashboard

It displays four charts for the respective report category. Each chart contains:

- Chart
- Time Span for which report get executed.
- Last run time of that report.

All reports run on relative time span and lasts 24 hours or last hour. The user cannot change report parameters.

6.7 Report Gallery

Report Gallery is a tool using which user can view following report results:

- Report results shared by other accounts (only reports fulfilling the report visibility constraints of the accounts will be displayed).
- Personal reports that were published on the gallery (these can be private or shared with other users).
- Results of personal scheduled reports.
- Temporary reports saved with the “Remember” action on the workspace. These will be removed after the current session is over.

To access and display the published reports, click the **Report Gallery** icon on the Module Launcher.

Using a report gallery, user can perform the following:

- Publish a Report Output
-

- Remember a Report
- Merging Reports

6.7.1 Publish a Report Output

Using **Report Gallery**, user can save their customize reports there. **Report Gallery** can be user specific or can be shared among members of a group.

To publish a report output, perform the following steps:

-
- Step 1** Click **Publish** from the toolbar. A publish dialog box appears.
 - Step 2** Select the type of output to be published to the report gallery.
 - Step 3** Check the **Share with** checkbox, if user wants to share the published report with a particular account group.
-

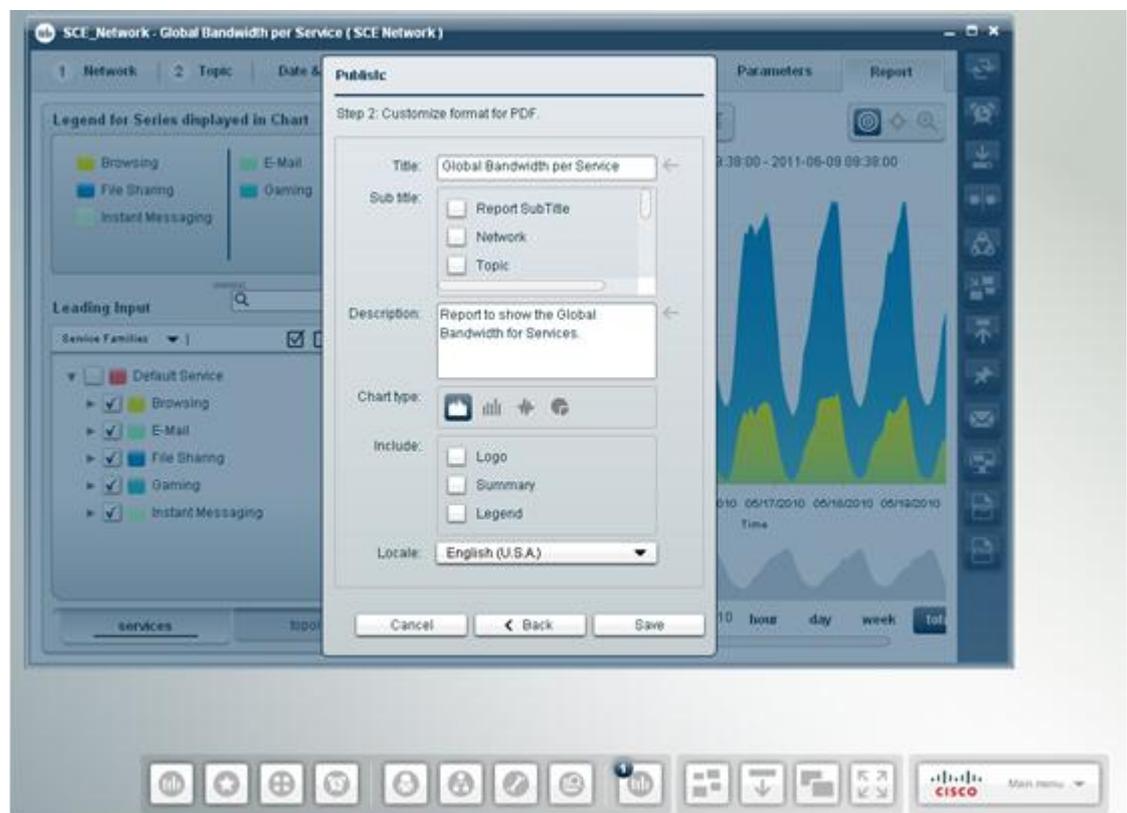


Note

If user wants to publish the report as a CSV file, click **Next**, and the file will get published to the report gallery.

- Step 4** Click **Next**. A dialog box similar to following appears on the screen:

Figure 103. Publishing a Report Output



- Step 5** Set all the desired parameters (report title, subtitle, description, chart type, locale, and elements to include such as logo, legend, summary table).

Step 6 Click **Done**.

6.7.2 Remember a Report

Using **Remember a Report**, user can save the report in **Report Gallery** but this report will be deleted when user logout from the application or his session terminated. Using this option, user can create a combined PDF file for 2 or more PDF reports. To remember a report, perform the following steps:

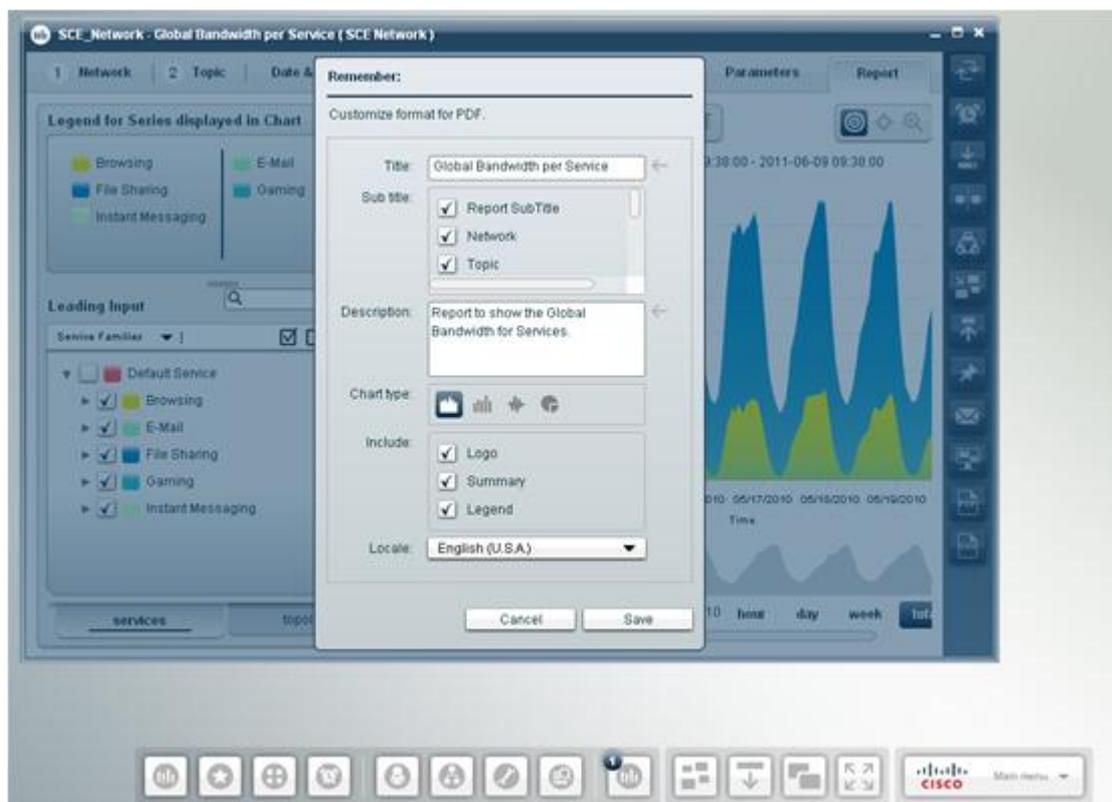


Note

User can merge only those reports which are available in PDF format not in image or CSV format.

Step 1 Click **Remember** from the toolbar. A Remember dialog box as shown below appears.

Figure 104. Remembering a Report



Step 2 Set all the desired parameters (report title, subtitle, description, chart type, locale, and elements to include such as logo, legend, summary table).

Step 3 Click **Done**.

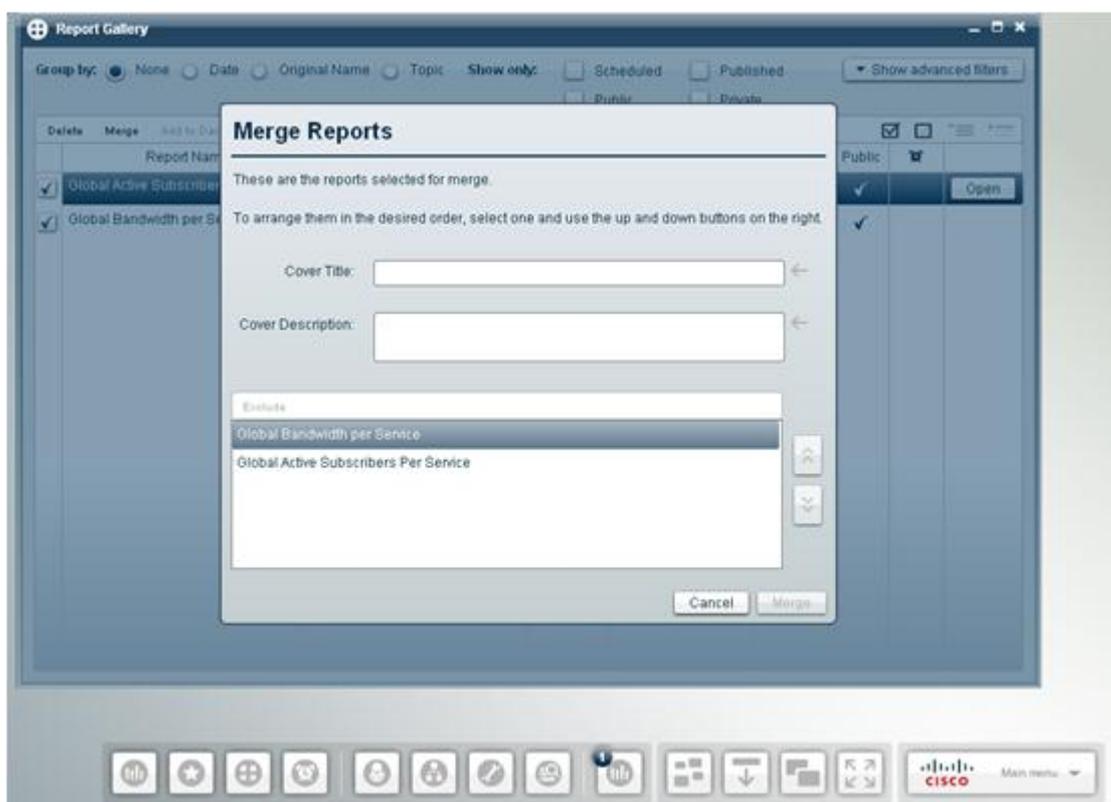
A notification appears on the report gallery icon, which shows that a new report has been published to the report gallery.

6.7.3 Merging Reports

To merge multiple report results (only PDF) from the Gallery into a single layout, perform the following steps:

- Step 1** Select multiple reports (only PDF) from the report gallery to merge.
- Step 2** Click **Merge** on the toolbar. A dialog box similar to following appears on the screen:

Figure 105. Merging Report Output



- Step 3** In the Merger Reports dialog box, provide the cover title and description to be shown on the cover page of the merged output.
- Step 4** Select the order of the reports in which user wants to see the generated output.
- Step 5** Click **Merge**.

A new browser window opens showing the merged PDF output containing contents from all the selected reports.

6.8 Scheduled Reports

This software supports the ability to automatically run the several predefined reports each in a preconfigured time and interval. For example, an administrator needs to periodically share a set of reports with his managers or peers. The user (administrator) can define a list of users (managers) that will receive a notification on report batch completion and will have access to the report results as well.

Scheduled reports run in background and are designed to produce a static output that can be sent via email or stored on the file system of the server.

To access and display the saved reports, click the **Scheduled Reports** icon on the Module Launcher.

Using a scheduled report, the user can perform the following functions:

-

- Delete a Scheduled Report
- Edit a Scheduled Report

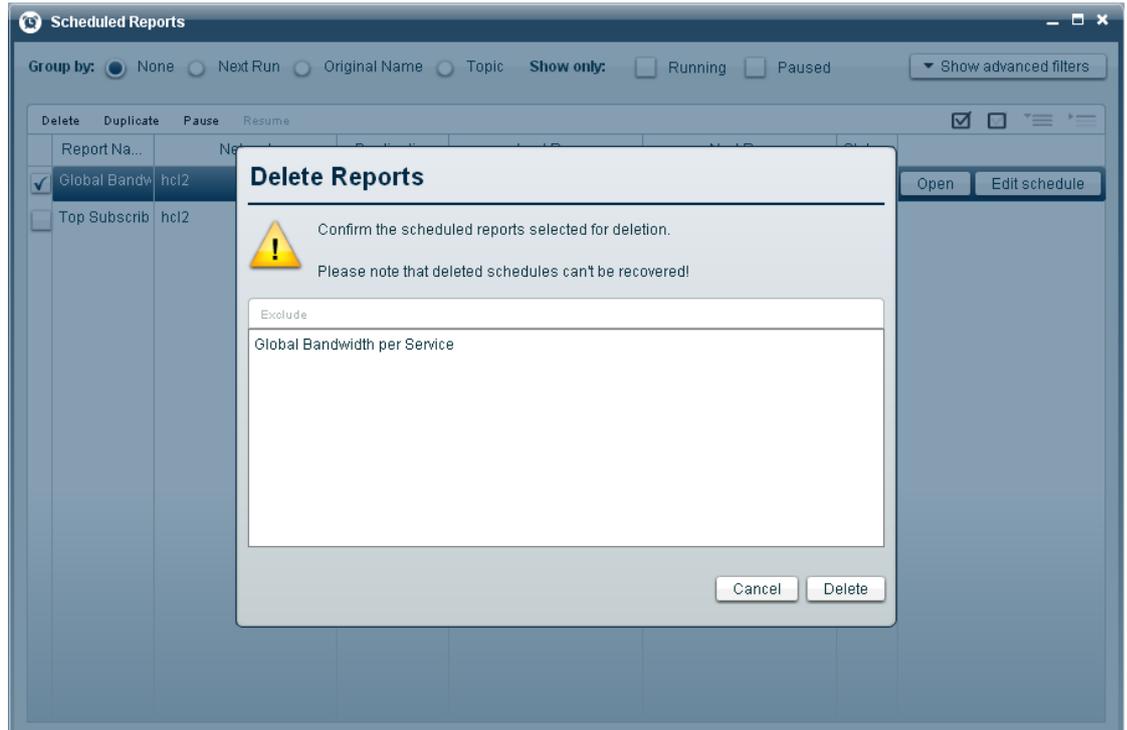
6.8.1 Delete a Scheduled Report

To delete a scheduled report, perform the following steps:

Step 1 Select the target report definitions.

Step 2 Choose **Delete**. A delete dialog box similar to following appears:

Figure 106. Deleting a Scheduled Report



Step 3 Review the name of the reports to be deleted.

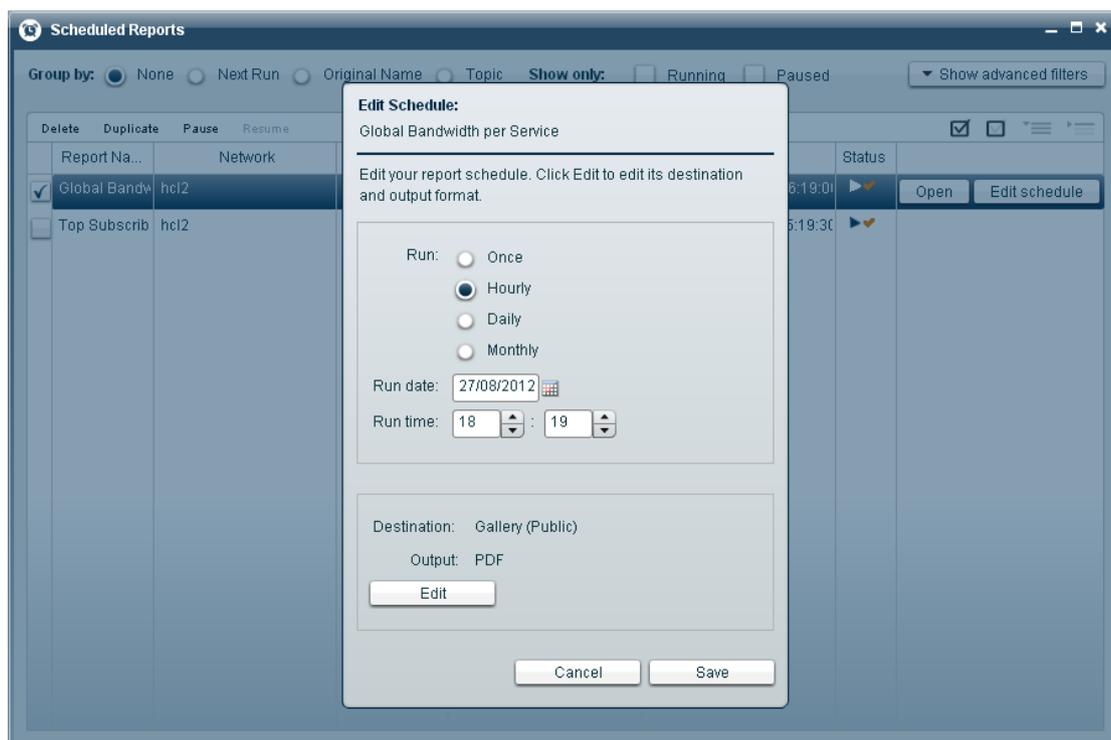
Step 4 Click **Delete** to confirm.

6.8.2 Edit a Scheduled Report

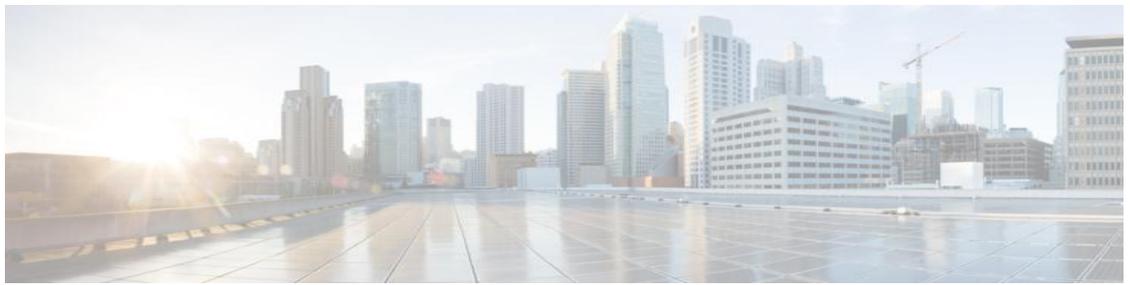
To edit a scheduled report, perform the following steps:

- Step 1** Select the target report from the list of scheduled reports.
- Step 2** Select the **Edit schedule** option located at the extreme right of the report name. An Edit Schedule dialog box as shown below appears:

Figure 107. Editing a Scheduled Report



- Step 3** Set the report schedule as needed. Click **Next** to confirm. A new dialog box appears.
- Step 4** Select the report output. Click **Next** to confirm. A new dialog box appears on the screen.
- Step 5** Set all the desired parameters (report title, subtitle, description, chart type, locale, and elements to include such as logo, legend, summary table). Click **Next** to confirm.
- Step 6** Select report destination and choose to publish the report as private or public.
- Step 7** Click **Save**.



CHAPTER 7. Monitoring

7.1 Introduction

The **Monitoring** module performs the task of overload detection and load monitoring. It maintains the latest statistical counters for reports being run or scheduled and sends email and logs appropriate errors if any statistics exceeds (or falls short of) its configured value.

Cisco Insight Reporter components support common standards for server hardware, software monitoring, operation, and maintenance. The same information is viewable via WEB UI as well.

This chapter contains following sections:

- [Performance](#)
- [Logging](#)

7.2 Performance

User can see various metrics about the current performance of the application and system on which the application is running.

Information that can be monitored is categorized in to following categories and metrics:

- User statistics such as:
 - Number of logged-in users
 - Number of reports per user session (min, max, and avg.)
 - Favorite-reports per user (min, max, and avg.)
 - Scheduled-reports per user (min, max, and avg.)
- Report performance statistics such as:
 - Report transactions (from each kind – user-generated and automatic)
 - Report response time (min, max, and avg.)
 - Failed report transactions.
- General performance and capacity such as:
 - CPU Utilization
 - Memory Utilization

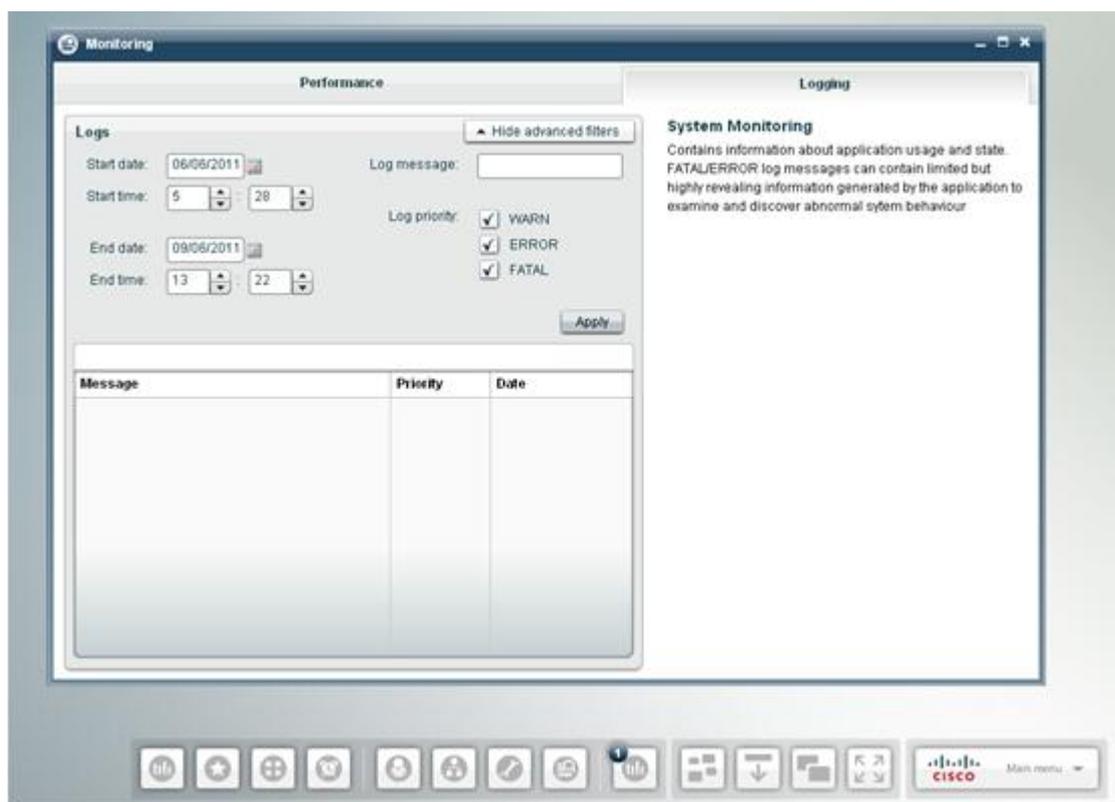
To access and display the Performance tab, click the **Monitoring** icon on the Module Launcher. Following screenshot will appear:

Figure 108. Performance Statistics



7.3 Logging

To access and display the Logging tab, click the **Monitoring** icon on the Module Launcher. Using this tab, user can monitor the problems occurring in the system.

Figure 109. Logging Tab

User can also search logs based on following parameters:

- Start and End date and time
- Log message
- Log priority



Note

If no warning and error logs displays, please check the “Log Level” configuration parameter on the Settings Management Module.

For the complete list of error messages and codes generated by the Cisco Insight Reporter, refer the chapter on “Troubleshooting” in the Cisco Insight Reporter Installation Guide.