Cisco Web Element Manager Installation and Administration Guide

Version 12.2

Last Updated April 30, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25638-04

Cisco Web Element Manager Installation and Administration Guide

CONTENTS

About this Guide

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5x00 Chassis.

This preface includes the following sections:

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electrostatic Discharge (ESD)	Warns you to take proper grounding precautions before handling ESD sensitive components or devices.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents text that appears on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter at the CLI, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* *`slot_number`* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**.

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by braces. They must be entered as part of the command syntax.
[**`keyword`** or *`variable`*]	Optional keywords or variables that may or may not be used are surrounded by brackets.

Command Syntax Conventions	Description
|	Some commands support alternative variables. These "options" are documented within braces or brackets by separating each variable with a vertical bar. These variables can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Go to http://www.cisco.com/cisco/web/support/ to submit a service request. A valid Cisco account (username and password) is required to access this site. Please contact your Cisco account representative for additional information.

Additional Information

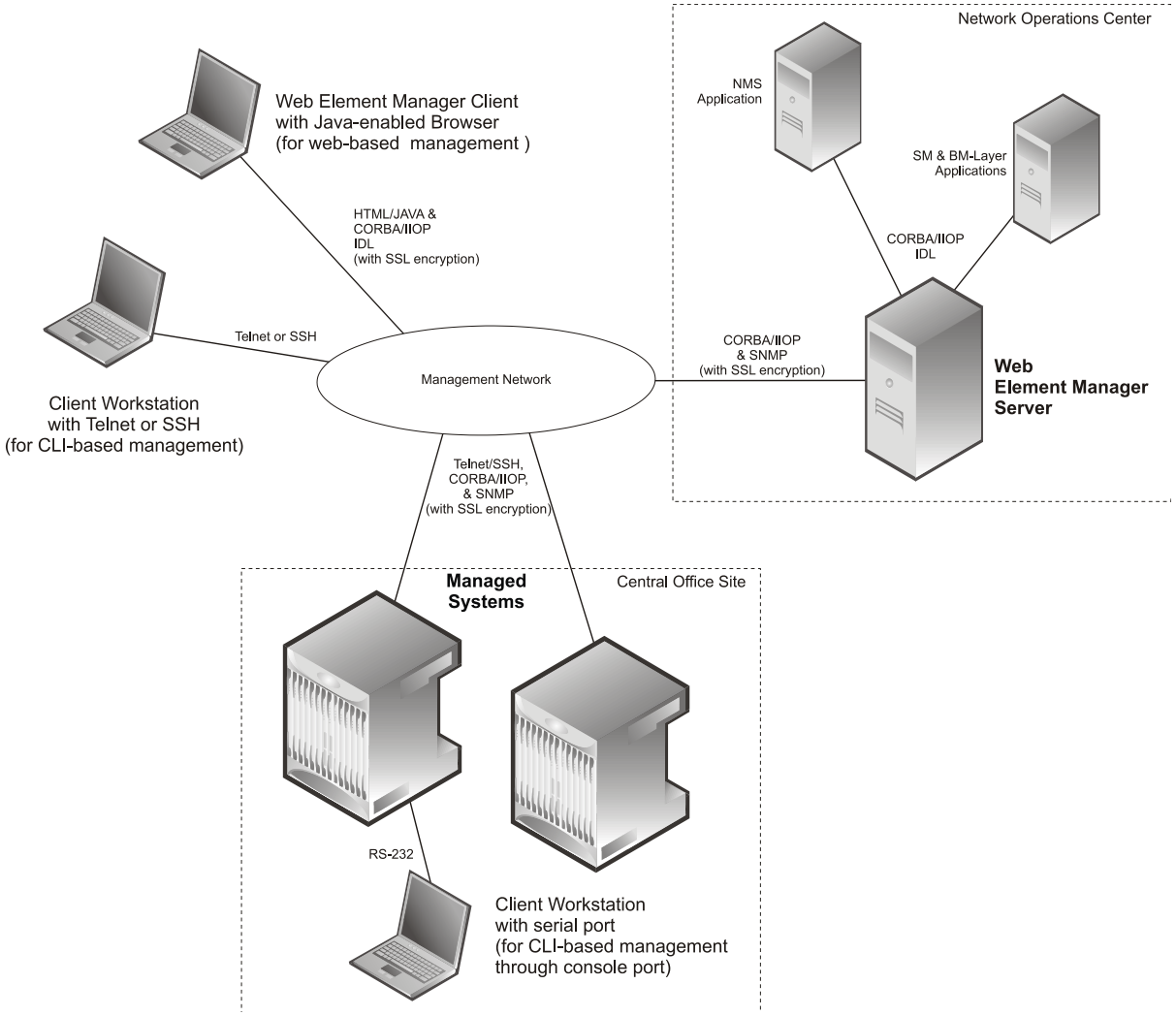
Refer to the following guides for supplemental information about the system:

- *Command Line Interface Reference*
- *Statistics and Counters Reference*
- *Thresholding Configuration Guide*
- *SNMP MIB Reference*
- *Cisco Web Element Manager Installation and Administration Guide*
- Product-specific and feature-specific administration guides
- *Release Notes* that accompany updates and upgrades to StarOS

Chapter 1
Web Element Manager Overview

The Web Element Manager (WEM) is a Common Object Request Broker Architecture (CORBA)-based application that provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) capability for the system under management.

For maximum flexibility and scalability, the WEM application implements a client-server architecture. This architecture allows remote clients with Java-enabled web browsers to manage one or more systems via the server component which implements the CORBA interfaces. The server component is fully compatible with the fault-tolerant Sun® Solaris® and Cisco MITG Red Hat Enterprise Linux operating systems. For added security, management traffic can be encrypted using the Secure Sockets Layer (SSL) protocol, as shown in the following diagram:



Supported Features

FCAPS Support

The Web Element Manager application provides Fault, Configuration, Accounting, Performance and Security (FCAPS) management functionality for the ASR 5000.

Fault Management

Fault management consists of an event logging function wherein all alarms, warnings, and other faults can be configured, reported, and acknowledged by network operations personnel.

The Simple Network Management Protocol (SNMP) is used by both the Web Element Manager and the chassis to report event notifications. The application's fault management system offers the following support for generated alarms:

- Provide mechanisms for viewing both current and pending alarms for both the chassis and the Web Element Manager server.
- Generate audio and visual alerts for alarms based on their severity (the Web Element Manager also supports the configuration of a severity level for each alarm).
- Maintain statistics for generated alarms.
- Store alarm information in the PostgreSQL® database.
- Execute scripts through the Script Server component of the application.
- Send E-mail notifications and/or forward notifications to Network Management Servers (NMSs) using a CORBA/IIOP-based Northbound Interface.
- Compliancy with the following standards:
    - TS 32.111-3, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Fault Management; Part 3: Alarm Integration Reference Point (IRP): Common Object Request Broker Architecture (CORBA) Solution Set (SS)
    - TS 32.303, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Configuration Management (CM); Notification Integration Reference Point (IRP): Common Object Request Broker Architecture (CORBA) Solution Set (SS)

Configuration Management

The Web Element Manager implements an easy to use, point-and-click GUI for providing configuration management for one or more systems. This GUI provides all the flexibility offered by the system's command Line Interface (CLI), while providing the scalability of performing certain functions across multiple chassis. All configuration information is stored in the PostgreSQL Database.

At the system-level, the Web Element Manager application provides support for the following:

- Adding, modifying, or deleting systems to/from the management system
- Performing configuration of card and port-level parameters
- Adding, modifying, or deleting contexts

- Configuring specific protocols and services within defined contexts such as AAA servers, PDSN services, GGSN services, IP access lists, IP interfaces, IP routes, IP address pools, RADIUS accounting and authentication, PPP, subscribers, and others

At the network level, the application is capable of transferring configuration and/or software images to multiple systems simultaneously in advance to performing software upgrades.

The Web Element Manager supports the configuration of all parameters required to perform software upgrades including:

- Adding, deleting, and sorting system boot stack entries; these entries allow multiple fall-backs in the event the system experiences an error in the loading of a particular image or configuration file
- Configuring network options for bootup
- Transferring configuration and image files to/from a chassis
- Initiating and monitoring upgrade status

The Web Element Manager further simplifies the software upgrade process by providing tools for managing system configuration files:

- **Back-up Tool:** Enables the Web Element Manager to transfer a copy of the configuration file currently being used by a managed system at user-defined intervals. Files are transferred to the host server in a specific directory. The number of files to retain in the directory is also configurable. This tool provides a useful mechanism for testing configurations and/or quickly restoring a last-known-good configuration in the event of an error.
- **Compare Tool:** Provides a powerful tool for comparing the configuration files of two managed systems. Once the two files are specified, a dialog appears displaying the two documents side-by-side. Line numbers are added for convenience. Text additions, modifications, and deletions are displayed in different colors for easy recognition. This tool can be useful on its own to determine variations between multiple iterations of the same configuration file, or, when used in conjunction with the Back-up tool, it can provide an audit trail of configuration changes that occurred during system operation.

Configuration Audit Tool

WEM Configuration Audit Tool allows users to monitor specified configuration attributes on a selected system or systems. This can be useful in monitoring configuration changes and problems while performing operation and maintenance tasks.

To effectively use this feature, the user must be familiar how to build queries and interpret query output from the Command Line Interface (CLI). With the Configuration Audit Tool users can:

- Schedule custom periodic configuration audits or execute an on demand configuration audit.
- Configure report distribution parameters that allow the user to notify various groups of individuals that a report is available.
- Have the results of a configuration audit automatically distributed via email to specified individuals or view report results directly via WEM.
- Create custom configuration attribute groups to be used for auditing a specified system.

Online Help is available from the following pages:

- Configuration Audit Query Information
- Configuration Audit Schedule
- On Demand Configuration Audit

- Configuration Audit Results

Accounting Management

Accounting management operations allow users to examine and perform post-process statistical analysis on systems managed by the Web Element Manager application.

The type of statistics used for element management-based accounting are called bulk statistics. Bulk statistics are grouped into categories called schemas and are polled by the system at fixed polling intervals and then transferred to the Web Element Manager at a different transfer intervals (defined in minutes).

Once the Web Element Manager server application, called the receiver, has received bulk statistics files from the managed system, these files are parsed and added to the PostgreSQL database. This database is updated as new files are received.

The Web Element Manager's accounting management functionality is compliant with *TS 32.401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Performance Management (PM); Concept and requirements* and allows you to:

- Collect statistics pertaining to the transfer and collection of bulk statistics
- Views statistics stored on the chassis prior to transfer to the receiver
- Graph multiple received bulk statistics over time as either a line or bar graph; these graphs can be printed to network printers accessible by the server
- Generate eXtensible Markup Language (XML) files for transfer to a Northbound NMS or bulk statistics processor.
- Archive collected bulk statistic information to conserve disk space on the server

Performance Management

Performance management operations supported by the Web Element Manager allow users to examine and perform real-time statistical analysis on systems managed by the application as well as on the server on which the application is running.

Information pertaining to various aspects of the Web Element Manager (CPU and memory utilization, disk space, and process status) and its managed systems (hardware, protocols, software subsystems, and subscribers) is collected in real time and is displayed in tabular format. Alternatively, most of the information can be graphed as a function of time in either line or bar-chart format. Multiple statistics can be graphed simultaneously for quick comparison of data.

In addition to collecting and providing mechanisms for the real-time viewing of statistical information, the Web Element Manager provides useful monitoring tools similar to those found in the CLI. These tools can be used to monitor active subscriber sessions, protocol flows, and port information. Data collected during this monitor operation can be saved to the client machine for further analysis.

Security Management

Security management pertains to the operations related to management users. This includes both Web Element Manager application users and local management users who are configured on the chassis. In many cases, management users can be allowed access to both the system (via its CLI) and the application. It is possible for both management user accounts to share the same username and password.

The security management features of the Web Element Manager allow you to:

- Add, modify, or delete administrative users for both the application and the managed system.

Regardless of the administrative user type, there are four levels of management user privileges:

- **Inspector**: Inspectors are limited to a small number of read-only Exec Mode commands.The bulk of these are "show" commands giving the inspector the ability to view a variety of statistics and conditions. The Inspector cannot execute **`show configuration`** commands and do not have the privilege to enter the Config Mode.
- **Operator**: Operators have read-only privileges to a larger subset of the Exec Mode commands. They can execute all commands that are part of the inspector mode, plus some system monitoring, statistic, and fault management functions. Operators do not have the ability to enter the Config Mode.
- **Administrator**: Administrators have read-write privileges and can execute any command throughout the CLI except for a few security-related commands that can only be configured by Security Administrators. Administrators can configure or modify the system and are able to execute all system commands, including those available to the Operators and Inspectors.
- **Security Administrator**: Security Administrators have read-write privileges and can execute all CLI commands including those available to Administrators, Operators, and Inspectors.

- Provide authentication and privilege restoration based on the login information entered by administrative users.
- Monitor current system or application-level administrative users in real-time and optionally terminate their management session.
- Perform an audit of all managed system configurations performed through both the application and the CLI as well as other operations performed within the application.

  The audit trail functionality supports the configuration of filters defining the type of operations to audit and also provides a dialog for performing the audit in real-time.

  Audit trail results are stored in the PostgreSQL database for later retrieval and analysis.

  The new Network Audit Tool functionality in WEM supports the on-demand or periodic auditing of chassis configuration attributes such as PPP MRU, Auth Sequence, Bulkstats Schema Needs Update, etc.

Additional Features

Additional features provided by the Web Element Manager application include:

High Availability Redundant Server Clustering

Beginning with Release 12.0 redundant servers can be configured using Oracle Cluster software. Much of the information in the following chapters applies equally to a cluster installation although at this time we recommend using the GUI installation method described in *Installing the WEM Software*. A separate appendix addresses the differences between a Standalone installation and a Failover installation and it also defines the steps required to create and configure a cluster.

Management Integration Capabilities

Utilizing the Object Management Group's (OMG) standard CORBA Northbound interface, the Web Element Manager application can be integrated with higher-level TMN-modeled applications such as network, business, and service layer applications. The OMG's Interface Definition Language (IDL) can be used to develop custom interfaces to various other third-party components such as Application Servers, etc.

Database Management and Redundancy Support

All databases used for audit trail, performance and statistical information, event management, and device inventory information will be stored on the Web Element Manager server using the UNIX file system.

Multiple Language Support

The Web Element Manager provides the ability for users to select a specific language the information is provided in. The currently supported languages include U.S. English and Korean.

Context-Sensitive Help System

The Web Element Manager has a complete web-based Help system that provides user assistance for every screen and function available within the application. This Help system resides on the Web Element Manager server and is accessible from any supported client workstation.

Stand-alone Offline Help System

A stand-alone version of the WEM's online help file is provided with the WEM. This stand-alone help contains content identical to the context-sensitive help. Users can save the standalone (.chm) help file to a local drive to conduct off-line WEM-related research. The standalone help file can be downloaded from the main WEM browser page by clicking the *Web Element Manager Offline Help* link under **Help Resources**.

Multiple OS Support

Web Element Manager can be installed on servers running the Sun Solaris or the custom Cisco MITG Red Hat Linux Enterprise v5.5 operating systems. For detailed operating system and hardware platform requirements, refer to the *Web Element Manager System Requirements* section of this chapter.

Caution: The Cisco MITG RHEL v5.5 OS is a custom image that contains only those software packages required to support compatible Cisco MITG external software applications. Users must not install any other applications on servers running the Cisco MITG v5.5 OS. For detailed software compatibility information, refer to the *Cisco MITG RHEL v5.5 OS Application Note*.

Web Element Manager System Requirements

Important: The hardware required for the Web Element Manager server may vary, depending on the operating system being used, the number of chassis being managed, the number of clients that require access, and other variables. The requirements listed in this section support up to 30 Web Element Manager clients, managing up to 25 chassis.

Server Hardware Requirements

This section describes the WEM server hardware requirements for both the Sun Solaris and Cisco MITG Red Hat Enterprise Linux Operating Systems.

Sun Solaris Server Hardware Requirements

WEM servers running the Sun Solaris operating system must be deployed on the following hardware platform:

- Sun Microsystems Netra™ T5220 server
- 1 x 1.2GHz 8 core UltraSPARC T2 processor with 32GB RAM
- 2 x 146GB SAS hard disk drives
- Quad Gigabit Ethernet interfaces
- Internal DVD-ROM drive
- AC or DC power supplies depending on the application

Red Hat Enterprise Linux Server Hardware Requirements

WEM servers running the Cisco MITG RHEL v5.5 operating system must be deployed on the following hardware platform:

- Cisco UCS C210 M2 Rack Server
- Intel Xeon X5675 processor with 16 GB DDR3 RAM
- 300GB 6Gb SAS 10K RPM SFF Hard Disk Drive
- Quad Gigabit Ethernet interfaces
- Internal DVD-ROM drive
- AC or DC power supplies depending on the application

Operating System Requirements

This section describes the Sun Solaris and Cisco MITG Red Hat Enterprise Linux (RHEL) v5.5 operating system requirements for WEM servers.

Sun Solaris Operating System Requirements

This section describes the required Sun Solaris OS requirements for WEM servers, including the required OS patches.

Important: Ensure that all recommended patches are installed before performing a new installation or software upgrade.

- Solaris 8 with Recommended Patch Cluster dated on or after April 2006.

Important: Users based in the United States should ensure that the timezone patch 109809-05 (or later) and libc patch 108993-52 (or later) be installed in support of extended daylight savings time (DST).

- Solaris 9 with Recommended Patch Cluster dated on or after April 2006

Important: Users based in the United States should ensure that the timezone patch 113225-07 (or later) and libc patch 112874-33 (or later) be installed in support of extended daylight savings time (DST) support. In addition, if Solaris 9 is used, it must be installed using the "End User System support 64-bit" software group must be specified during the installation of the operating system. This option installs the libraries required for proper operation of the Web Element Manager.

- Solaris 10 with Recommended Patch Cluster dated on or after April 2011.

  Important: Users based in the United States using Solaris 10 should ensure that the timezone patch 138856-02 or later is installed in support of extended Daylight Savings Time (DST).

Important: The following are important requirements for Solaris 10 users:

Solaris 10 with Recommended Patch Cluster dated on or after July 16, 2007 and not later than Nov 2010. Solaris 10 Kernel patch released between 137137-09 and 142900-04 may result in kernel panic while executing/invoking system calls. We recommend kernel patch 142900-07

Important: Do not install the kernel patch beyond 142900-07.

Solaris 10 Kernel patch released after 142900-07 has an issue, which will result in failure while invoking WEM Monitor subscriber and Monitor protocol screens.

Important: If you plan to install software and maintain the Web Element Manager application and server remotely, it is recommended that you use an X-Windows client.

Red Hat Enterprise Linux Operating System Requirements

This section describes the required Cisco MITG Red Hat Linux (RHEL) operating system (OS) requirements for WEM servers.

- Cisco MITG RHEL v5.5 OS

For hardware platform requirements for the Cisco MITG RHEL v5.5 OS, refer to the *Server Hardware Requirements* section in this chapter. For information related to installation, refer to the *Cisco MITG RHEL OS v5.5 Application Note*.

Caution: The Cisco MITG RHEL v5.5 OS is a custom image that contains only those software packages required to support compatible Cisco MITG external software applications. Users must not install any other applications on servers running the Cisco MITG v5.5 OS. For detailed software compatibility information, refer to the *Cisco MITG RHEL v5.5 OS Application Note*.

Client Access Requirements

- Workstation supporting Solaris/Sun, Linux, UNIX, Microsoft Windows XP, Windows 2000, Windows 7 or Windows NT operating system
- Java Runtime Environment (JRE) version 1.5 or 1.6

Important: It is recommended that users should use JRE 1.4.2_11 (or later) or 1.5 update 6 (or later).

- Java policy file (obtained during initial access to the Web Element Manager server)
- Microsoft Internet Explorer version 5.0 (or higher), Netscape Navigator version 4.72 (or higher), or other Internet browser
- Access to the Web Element Manager server's host network

Important: Web Element Manager clients cannot access the Web Element Manager server if the server is separated by an NAT'd firewall or other device that restricts access between the client workstation and server.

- Configured application user account on Web Element Manager server

WEM Architecture

The WEM architecture consists of the following components:

- Host Filesystem
- Apache Web Server
- WEM Server FCAPS Support
- WEM Process Monitor
- Bulk Statistics Server
- Script Server
- PostgreSQL Database Server
- Northbound Server
- WEM Logger

Host Filesystem

Running on the fault-tolerant Sun Solaris or Red Hat Enterprise Linux operating system, the WEM uses the native filesystem for such things as creating and writing to log files, storing alarm and bulk statistic-related information, and configuration file management.

Apache Web Server

Remote clients interface with the WEM by establishing session with the server using the Hyper Text Transport Protocol (HTTP). The session is hosted by the Apache Web Server which launches a Java applet providing a graphical user interface for managing the system. When HTTPS is mentioned in the URL instead of HTTP, secure connection is established between the WEM client and WEM server. The Apache Web Server is also used to execute Common Gateway Interfaces (CGIs) invoked by the applet using CORBA/Internet Inter-ORB Protocol (IIOP).

WEM Server FCAPS Support

This component provides Fault, Configuration, Accounting, Performance, and Security (FCAPS) functionality.

Important: The Admin can make any menu or submenu item visible or not visible to users as he sees fit. To show or hide a particular menu option, set the flag in the *menu.xml* file as described in the *Configuration File Parameters* chapter of this guide. Please note that it is not possible to actually delete or add a menu or submenu.

Fault Management

Fault management consists of an event logging function wherein all alarms, warnings, and other faults can be configured, reported, and acknowledged by network operations personnel.

The Simple Network Management Protocol (SNMP) is used by both the Web Element Manager and the ASR 5000 to report event notifications. The application's fault management system offers the following support for generated alarms:

- Provide mechanisms for viewing both current and pending alarms for both the chassis and the Web Element Manager server.
- Generate audio and visual alerts for alarms based on their severity (the Web Element Manager also supports the configuration of a severity level for each alarm).
- Maintain statistics for generated alarms.
- Store alarm information in the PostgreSQL® database.
- Execute scripts through the Script Server component of the application.
- Send E-mail notifications and/or forward notifications to Network Management Servers (NMSs) using a CORBA/IIOP-based Northbound Interface.
- Compliance with the following standards:
    - TS 32.111-3, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Fault Management; Part 3: Alarm Integration Reference Point (IRP): Common Object Request Broker Architecture (CORBA) Solution Set (SS)
    - TS 32.303, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Configuration Management (CM); Notification Integration Reference Point (IRP): Common Object Request Broker Architecture (CORBA) Solution Set (SS).

Configuration Management

The Web Element Manager implements an easy to use, point-and-click GUI for providing configuration management for one or more systems. This GUI provides all the flexibility offered by the system's command Line Interface (CLI), while providing the scalability of performing certain functions across multiple systems. All configuration information is stored in the PostgreSQL Database.

At the system-level, the Web Element Manager application provides support for the following:

- Adding, modifying, or deleting systems to/from the management system
- Performing configuration of card and port-level parameters
- Adding, modifying, or deleting contexts
- Configuring specific protocols and services within defined contexts such as AAA servers, PDSN services, GGSN services, IP access lists, IP interfaces, IP routes, IP address pools, RADIUS accounting and authentication, PPP, subscribers, and others

At the network level, the application is capable of transferring configuration and/or software images to multiple systems simultaneously in advance to performing software upgrades.

The Web Element Manager supports the configuration of all parameters required to perform software upgrades including:

- Adding, deleting, and sorting system boot stack entries; these entries allow multiple fall-backs in the event the system experiences an error in the loading of a particular image or configuration file.
- Configuring network options for bootup.
- Transferring configuration and image files to/from systems.
- Initiating and monitoring upgrade status.

The Web Element Manager further simplifies the software upgrade process by providing tools for managing system configuration files:

- **Back-up Tool:** Enables the Web Element Manager to transfer a copy of the configuration file currently being used by a managed system at user-defined intervals. Files are transferred to the host server in a specific directory. The number of files to retain in the directory is also configurable. This tool provides a useful mechanism for testing configurations and/or quickly restoring a last-known-good configuration in the event of an error.
- **Compare Tool:** Provides a powerful tool for comparing the configuration files of two managed systems. Once the two files are specified, a dialog appears displaying the two documents side-by-side. Line numbers are added for convenience. Text additions, modifications, and deletions are displayed in different colors for easy recognition. This tool can be useful on its own to determine variations between multiple iterations of the same configuration file, or, when used in conjunction with the Back-up tool, it can provide an audit trail of configuration changes that occurred during system operation.

Accounting Management

Accounting management operations allow users to examine and perform post-process statistical analysis on systems managed by the Web Element Manager application.

The type of statistics used for element management-based accounting are called bulk statistics. Bulk statistics are grouped into categories called schemas and are polled by the system at fixed polling intervals and then transferred to the Web Element Manager at a different transfer intervals (defined in minutes).

Once the Web Element Manager server application, called the receiver, has received bulk statistics files from the managed system, these files are parsed and added to the PostgreSQL database. This database is updated as new files are received.

The Web Element Manager's accounting management functionality is compliant with *TS 32.401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Performance Management (PM); Concept and requirements* and allows you to:

- Collect statistics pertaining to the transfer and collection of bulk statistics.
- Views statistics stored on the ASR 5000 prior to transfer to the receiver.
- Graph multiple received bulk statistics over time as either a line or bar graph; these graphs can be printed to network printers accessible by the server.
- Generate eXtensible Markup Language (XML) files for transfer to a Northbound NMS or bulk statistics processor.
- Archive collected bulk statistic information to conserve disk space on the server.

Performance Management

Performance management operations supported by the Web Element Manager allow users to examine and perform real-time statistical analysis on systems managed by the application as well as on the server on which the application is running.

Information pertaining to various aspects of the Web Element Manager (CPU and memory utilization, disk space, and process status) and its managed systems (hardware, protocols, software subsystems, and subscribers) is collected in real time and is displayed in tabular format. Alternatively, most of the information can be graphed as a function of time in either line or bar-chart format. Multiple statistics can be graphed simultaneously for quick comparison of data.

In addition to collecting and providing mechanisms for the real-time viewing of statistical information, the Web Element Manager provides useful monitoring tools similar to those found in the CLI. These tools can be used to monitor

active subscriber sessions, protocol flows, and port information. Data collected during this monitor operation can be saved to the client machine for further analysis.

Security Management

Security management pertains to the operations related to management users. This includes both Web Element Manager application users and local management users who are configured on the chassis. In many cases, management users can be allowed access to both the system (via its CLI) and the application. It is possible for both management user accounts to share the same username and password.

While it is possible to authenticate users via RADIUS server configuration, each RADIUS server has its own configuration that is outside the scope of this document. However, you can find the mapping information you would need to configure each of the four levels of administrative user in the "CLI Administrative Users" section of the *CLI Overview* chapter in the *Command Line Interface Reference*.

The security management features of the Web Element Manager allow you to:

- Add, modify, or delete administrative users for both the application and the managed system.
- Regardless of the administrative user type, there are four levels of management user privileges:
    - **Inspector**: Inspectors are limited to a small number of read-only Exec Mode commands.The bulk of these are "show" commands giving the inspector the ability to view a variety of statistics and conditions. The Inspector cannot execute **`show configuration`** commands and do not have the privilege to enter the Config Mode.
    - **Operator**: Operators have read-only privileges to a larger subset of the Exec Mode commands. They can execute all commands that are part of the inspector mode, plus some system monitoring, statistic, and fault management functions. Operators do not have the ability to enter the Config Mode.
    - **Administrator**: Administrators have read-write privileges and can execute any command throughout the CLI except for a few security-related commands that can only be configured by Security Administrators. Administrators can configure or modify the system and are able to execute all system commands, including those available to the Operators and Inspectors.
    - **Security Administrator**: Security Administrators have read-write privileges and can execute all CLI commands including those available to Administrators, Operators, and Inspectors.
- Provide authentication and privilege restoration based on the login information entered by administrative users.
- Monitor current system or application-level administrative users in real-time and optionally terminate their management session.
- Perform an audit of all managed system configurations performed through both the application and the CLI as well as other operations performed within the application.

  The audit trail functionality supports the configuration of filters defining the type of operations to audit and also provides a dialog for performing the audit in real-time.

  Audit trail results are stored in the PostgreSQL database for later retrieval and analysis.

  The new Network Audit Tool functionality in WEM supports the on-demand or periodic auditing of chassis configuration attributes such as PPP MRU, Auth Sequence, Bulkstats Schema Needs Update, etc.

ANSI T1.276 Compliance

The WEM supports ANSI standard T1.276, providing a set of baseline security features to help mitigate security risks in the management of telecommunication networks. New users will be sent a randomly generated password automatically, and will be prompted to provide a new password upon first login. New passwords must meet strict requirements to comply with the ANSI standard:

- Passwords must be a minimum of eight characters long.
- Passwords must not be a repeat or the reverse of the associated user ID.
- Passwords must not be more than three of the same characters used consecutively.
- Passwords must contain at least three of the following character types:
    - At least one lower case alpha character
    - At least one upper case alpha character
    - At least one numeric character
    - At least one special character

Users will also be required to change passwords after a configurable number of days, and will be barred from reusing the same password for a configurable number of password change cycles. Too many failed login attempts will result in an account lockout, which may be removed either by an administrator or by waiting for a defined period of time to elapse.

WEM Process Monitor

The Process Monitor (PSMon) is a Perl script that monitors the status of processes pertaining to the WEM application.

The script is a plain text Apache-style configuration file that allows the user to define a set of rules. These rules describe what processes should always be running on the system, any limitations on concurrent instances, Time-To-Live (TTL), and maximum CPU/memory usage of processes. It can be run as a stand alone program or a fully functional background daemon.

PSMon scans the UNIX process table and, using the set of defined rules, will re-spawn any dead processes, and/or slay or “deal with” any aggressive or illegal processes. The number of retries and time interval the PSMon scans the table is configurable meaning that it will never try to start the process if 'number of retries' exceeds in given time interval.

PSMon logs events to syslog and to a log file and is equipped with customizable e-mail notification facilities.

Bulk Statistics Server

The Bulk Statistics Server process is responsible for collecting and processing all bulk statistic-related information from the system as part of the WEM’s accounting management functionality.

The Bulk Statistics Server parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local filesystem or on an NFS-mounted filesystem on the WEM server.

Script Server

The WEM supports the ability to configure the properties for alarms. One of the properties that can be configured is specifying a script that can be executed upon receipt of that alarm. The Script Server process is responsible for executing the specified script.

Upon receipt of the alarm, the WEM Server FCAPS Support function passes the name of the script to execute and the trap logged time to the Script Server. An acknowledgement is sent and the script is executed by the Script Server. In the event, an error is experienced while executing the script, the Script Server generates an SNMP trap.

PostgreSQL Database Server

The PostgreSQL Database consists of multiple databases maintaining information pertaining to the following WEM functions:

- **Configuration:** This database contains tables which maintain configuration information for user details, topology for maps and manageable systems.
- **Trap:** This database contains tables which maintain SNMP trap configuration information and all the received SNMP traps.
- **MIB:** This database contains all the information required to translate SNMP Object identifiers to proper MIB names and their types as given in the MIB file.
- **Audit Trail:** This database contains table that maintains the configuration trail including the following:
    - Configuration performed on each system through the WEM
    - Configuration done through the system's CLI (this is known via the CORBA notification service)
    - Login/out from the WEM and system CLI
    - The addition/deletion of a new system in the managed system list
- **Bulk Statistics:** This database contains various tables containing counter values periodically received from the system via the File Transfer Protocol (FTP).

Northbound Server

The Northbound Server process is responsible for collecting and transmitting information about WEM system management to an NMS.

WEM supports the Northbound Interface as defined in the 3GPP standards for Telecom Management. 3GPP defines a standard interface (Interface-N) between the EMS and the NMS. It also defines Integration Reference Points (IRPs) through which various aspects of system management (FCAPS) are performed by the NMS.

When the Northbound Server process is enabled, WEM will respond to NMS requests by fetching the required information and transmitting it over the CORBA interface.

Northbound Server is a separately licensed feature.

Currently, WEM supports five IRPs defined by the 3GPP standards. The supported IRPs and corresponding 3GPP standards are:

- **Alarm**: 3GPP TS 32.111-3 (V6.6.0)
- **Basic CM**: 3GPP TS 32.603 (V6.4.0)
- **Notification**: 3GPP TS 32.303 (V6.6.0)
- **Communication Surveillance**: 3GPP TS 32.353 (V6.4.0)
- **Entry Point**: 3GPP 32.363 (V6.4.0)

The supported Network Resource Model is:

- **Generic Network Resource (NRM) IRP**: 3GPP TS 32.623 (v6.50)

  The following table lists the Northbound Interface operations and notifications that are supported for each of the IRPs:

IRP Category	Notification/Operation Description	
Alarm	*Notifications*	notifyNewAlarm
		notifyAckStateChanged
		notifyClearedAlarm
		notifyAlarmListRebuilt
	Operations	get_alarm_irp_versions
		clear_alarms
		get_alarm_list
		next_alarmInformations
		get_alarm_count
		acknowledge_alarms
		unacknowledge_alarms
Basic CM	*Notifications*	Not Applicable
	Operations	get_basic_cm_irp_version
		find_managed_objects
		next_basicCmInformations
Notification	*Notifications*	not applicable
	Operations	get_notification_irp_versions
		attach_push
		change_subscription_filter
		get_subscription_status
		get_subscription_ids
		detach
Communication Surveillance	*Notifications*	notifyHeartbeat
	Operations	get_CS_IRP_versions
		get_heartbeat_period
		set_heartbeat_period
		trigger_heartbeat
Entry Point	*Notifications*	Not Applicable
	Operations	get_EP_IRP_versions
		get_IRP_outline

IRP Category	Notification/Operation Description	
		get_IRP_reference
		release_IRP_reference

WEM Logger

The WEM application generates and stores logs pertaining to server installation and operation. The logs can be stored locally or to another server. In addition, the WEM provides enhanced logging functionality for customizing log output and log files.

Chapter 2
WEM Port and Hardware Information

This chapter provides information on various ports and their corresponding port numbers used by the WEM, and hardware sizing requirements of the WEM application.

This section includes the following:

Important: Unless otherwise specified, the information in this chapter applies to both Sun Solaris and Red Hat Enterprise Linux-based (RHEL) WEM systems.

Web Element Manager Network Considerations

To ensure proper installation and operation of the WEM, the following network considerations must be implemented:

- The WEM server and the ASR 5000 chassis must be located on the same network.
- The Network Address Translation (NAT) protocol should not be used between the system and WEM server.
- If there is a firewall installed between the WEM server and the system, then the port used by the WEM to access the system must be opened. Refer to the Default TCP/UDP Port Utilization section for additional information.
- The WEM server must be able to send and receive Ping and ICMP packets from the system.
- Configured application user account on WEM server.

Default TCP/UDP Port Utilization

Various TCP/UDP ports are used by the WEM for both client-server communication and communication with managed systems. If firewalls are used on these interfaces, these ports need to be opened. The following table lists the ports for which firewall must allow access for a port on that communication path.

Table 1. Default TCP/UDP/ICMP Port Utilization with Firewall

Port Number	Communication Type	Usage
TCP Port:		
20 to 21	• WEM Server to ASR 5000 • ASR 5000 to WEM Server • WEM Server to NMS	Used by FTP server to transfer Bulkstats and in case of software upgrade, Config-backup, Config-update scheduler.
22	• WEM Server to ASR 5000 • ASR 5000 to WEM Server • WEM Server to NMS	Used by SSH or SFTP server for Config-backup, expect scripts.
80	WEM Client to WEM Server (Unsecured)	Used by Apache server for downloading the WEM applet and property files. This port is configurable.
443	WEM Client to WEM Server (Secured)	Used by Apache server for downloading the WEM applet and property files under secured connection. This port is configurable.
14131 to 14132	WEM Server to ASR 5000	Used for CORBA communication. These ports are configurable.
15000 to 15002	• WEM Client to WEM Server • ASR 5000 to WEM Server	Used for WEM client - server communication. WEM server receives requests on these ports from client. The ASR 5000 also sends notifications to the WEM server. The base port is configurable.
15015	NMS to WEM Server	Used by NorthBound server to receive requests on this port from NMS (3GPP standard CORBA NorthBound Interface).
15017	WEM Server to NMS	Used by CORBA Notification service for sending notifications to NMS (3GPP standard CORBA NorthBound Interface).

Port Number	Communication Type	Usage
40000 to 40010	WEM Server to WEM Client	Used for WEM server - client communication. The notifications such as alarms, config changes, monitor protocol, real-time graphs are done by WEM server to WEM client.
UDP Port:		
69	ASR 5000 to WEM Server	Used by TFTP server. If the WEM server machine has the ASR 5000 image/config and if they are to be loaded using TFTP, then this port will be used.
162	ASR 5000 to WEM Server	Default port on which WEM receives SNMP traps from ASR 5000. This port is configurable.
514	ASR 5000 to WEM Server	Used by Syslog server. WEM server machine may be configured to act as a syslog server for the ASR 5000 logs.
ICMP Port:		
-	WEM Server to ASR 5000	WEM server to ASR 5000 keep-alive

The following table lists the ports used by WEM for which there is no need for any firewall to open that port.

Table 2. Default TCP/UDP/ICMP Port Utilization

Port Number	Usage
TCP Port:	
5432	Used by PostgreSQL server for accepting SQL queries from various WEM processes.
22222	Used by WEM Server as "identity" port and is configurable.
22223	Used by Bulkstat Server (XML generator) as "identity" port and is configurable.
22224	Used by Bulkstat Parser as "identity" port and is configurable.
22225	Used by Script Server as "identity" port and is configurable.

WEM Server Hardware Sizing and Provisioning Guidelines

In addition to the minimum system requirements provided in the previous section, the following guidelines offer information that can help you plan hardware sizing needs, based on the exact deployment scenario that you will be using.

The information provided in this section is based on a typical installation that has the following characteristics:

- The WEM server application can manage up to 25 systems.
- No more than 30 clients will be accessing the WEM server simultaneously.
- The WEM application and the server it resides on are used to:
    - Receive, process, correlate, and store SNMPv1 traps sent from the managed system. This operation involves the use of the event database, controlled by the PostgreSQL database engine, and any e-mail notifications configured for each alarm.
    - Receive, process, and store Bulk Statistics information received from the managed system. This operation involves the use of the bulkstats database, controlled by the PostgreSQL database engine.
    - Receive, display, and graph real-time Performance information for any number of statistical counters and polling periods.
    - Administer WEM and CLI management users. This includes the addition, modification, and deletion of WEM-based management users, stored in the users database, controlled by the PostgreSQL database engine.
    - Store, retrieve, and perform various configuration management operations on the managed system. This includes the storage and transfer (via SFTP/FTP) of binary software images, configuration text files, and session license and feature use keys.
- **Hard Drive Partition Recommendations:**
    - The WEM should not be installed in the root (/) partition.
    - The root partition (/) should be at least 1 gigabyte (GB).
    - The /usr partition should be at least 1 GB.
    - The /var partition should be at least 8 GB.
    - The swap partitions should be at least 10 GB.
    - The size of the partition on which the WEM is installed will depend on a variety of site-specific factors, including the number of ASR 5000s to be managed, the average bulkstat file size, the bulkstat file transfer interval, the number of configuration changes per day per ASR 5000 and other considerations. Cisco provides a WEM Sizing Calculator utility to assist with these estimates. Please contact your local Cisco representative during the sizing phase of the planning process to obtain assistance on hard drive partition and disk space estimates for the WEM application.

Important: It is strongly recommended that the WEM application, the Apache web server application, and the PostgreSQL database engine be configured in the same logical hard disk partition.

Chapter 3
Installing the WEM Software

This chapter provides the step-by-step procedure of installing WEM application using the GUI-based installation wizard and the console-based installation. Additionally it provides instructions that need to be followed before starting the WEM installation so that it completes successfully.

This chapter includes the following topics:

Important: Unless otherwise specified, the information in this chapter applies to both Sun Solaris and Red Hat Enterprise Linux-based (RHEL) WEM systems.

Before You Begin

Prior to performing the installation procedure, this section previews each step to ensure that your ready to successfully complete the installation. Detailed installation instructions follow.

Important: Special rules apply when you are installing redundant High Availability servers using Oracle or Veritas clustering software. Refer to the appendices for more information.

Step 1 - Verifying Hardware Status

The first thing that you need to do is to ensure that the WEM server hardware has been provisioned properly for your application. This includes:

- Verifying the correct operating system. This can be accomplished by entering the **uname -a** command.
- Verifying that the hard disk has been partitioned properly using the recommendations outlined in the *WEM Server Hardware Sizing and Provisioning Guidelines* section of the *WEM Port and Hardware Information* chapter.
- Verifying network connectivity through the management LAN.

Step 2 - Setting the WEM Server's Database Environment Strings

This step is required to configure how the PostgreSQL database engine processes, stores, and retrieves information contained in the various databases stored using the UNIX file subsystem. Failure to configure these settings may cause data loss and will minimally cause errors in the WEM's operation. Special instructions apply for updating the Postgres database if you are installing redundant High Availability servers using clustering software. Refer to the appendices for more information before you start installation.

Step 3 - Unpacking the WEM Application Files

WEM installation files are distributed as a single compressed file. Once the file is obtained, it must be copied to the server and unpacked. It is recommended that you copy the file to a temporary directory on the server.

Step 4 - Installing the WEM Software

This step consists of choosing the desired installation method (console-based or the Graphical User Interface (GUI-based) and performing the physical installation onto the WEM server. There are three software components that are installed as part of this procedure. They are:

- WEM software
- Apache Web Server software
- PostgreSQL database engine software

Important: If you are installing the WEM to upgrade an existing version that is currently installed and running, proceed to *Upgrading the WEM Software* chapter of this guide. If you are installing redundant High Availability servers using Clustering software, you should also refer to the appendices for special instructions.

Step 5 - Configuring WEM Client Session Management Parameters

There are numerous client session management parameters that control how many client sessions may be simultaneously accessed, idle timeout periods, and various other client-related items. This configuration file, which resides on the WEM server, should be modified (if needed) prior to starting the WEM server processes.

Caution: Failure to perform the WEM server startup procedure in the exact order shown in this document may prevent the application from initializing and working properly.

Step 6 - Configuring IP Multipathing (IPMP) on WEM Server (Optional)

IPMP, or IP multipathing, is a facility provided by Solaris® to provide physical interface failure detection and transparent network access failover for a system with multiple interfaces on the same IP link. IPMP also provides load spreading of packets for systems with multiple interfaces.

For IPMP configuration, refer to the Configuring IPMP on WEM Server section.

Important: IPMP is a feature supported on Solaris® platforms provided by Oracle. The configuration is documented in the various User Guides from Oracle.

Setting the PostgreSQL Database System Environment Configurations

Prior to installing the WEM application onto the WEM server hardware, there are numerous system environment configuration settings that should be configured. While PostgreSQL is installed during the GUI-based installation procedure, these settings must be configured manually.

Red Hat Enterprise Linux (RHEL) Servers

In the System Settings Check Panel, ensure that following entries are present in '/etc/sysctl.conf'

- kernel.shmmax=536870912
- kernel.shmall=2097152

If one or more entries are missing then abort installation, update '/etc/sysctl.conf', restart the system and re-run installer.

Solaris Servers

In Solaris, the user has to edit the /etc/system file.

Add the following values to the system file in the /etc directory and restart the system before continuing with the installation of the WEM application:

set msgsys:msginfo_msgmnb=65536

set msgsys:msginfo_msgtql=1024

set shmsys:shminfo_shmmax=0x20000000

set shmsys:shminfo_shmmin=1

set shmsys:shminfo_shmmni=256

set shmsys:shminfo_shmseg=256

set semsys:seminfo_semmap=256

set semsys:seminfo_semmni=512

set semsys:seminfo_semmns=512

set semsys:seminfo_semmsl=32

Configuring PostgreSQL Database System Environment

Configuring PostgreSQL Database System Environment		
Step	**Action**	**Observation**
The start point for this procedure is the UNIX shell prompt.		

Configuring PostgreSQL Database System Environment		
Step	**Action**	**Observation**
	Type the vi command:**vi /etc/system <Enter>**	Opens the vi editor and the file where the database strings are located.
	Type the **end of file** command.**<Shift> G <Enter>**	This places the cursor at the bottom of the file in the append mode.
	Type the following environment settings:	Allows the user to enter the new system settings for the database environment.
	set msgsys:msginfo_msgmnb=65536set msgsys:msginfo_msgtql=1024set shmsys:shminfo_shmmax=0x20000000set shmsys:shminfo_shmmin=1set shmsys:shminfo_shmmni=256set shmsys:shminfo_shmseg=256set semsys:seminfo_semmap=256set semsys:seminfo_semmni=512set semsys:seminfo_semmns=512set semsys:seminfo_semmsl=32	
	Verify a lower case letter “L” was used in the msgtql and semmsl entries.	
	Press **<Esc>**.	Returns the user to the command mode.
	Type the **write to file and save** command:**:wq! <Enter>**	Writes the changes to the current open file and exits the vi editor.
	Type the **reboot** command.**reboot <Enter>**A warm reboot may be performed by pressing <Ctrl-Alt-Delete>.	Reboots the system and applies the changes in the /etc/system file.
	- END OF PROCEDURE -	

Unpacking the Installation Files

WEM installation files are distributed as a single compressed file with a ".tar.gz" extension.

Once the installation file has been copied to the server, use the following procedure to unpack the file.

Step 1 Go to the directory in which the file is stored.

Step 2 Unzip the file by entering the following command:

```
gunzip file_name.tar.gz
```

file_name is the name of the WEM application installation file.

Step 3 Un-tar the file by entering the following command:

tar -xvf *file_name* **.tar**

Decompressing the installation file results in the following files:

- **setup.bin**: The installation binary file.
- **inst**: The executable file used to initiate the installation. This file is used for both the console- and the GUI-based methods.
- **uninst**: Once the WEM application has been installed, this file must be copied to the */<ems_dir>/_uninst/* directory. It is the executable file for uninstalling the application for both the console- and GUI-based methods.
- *file_name***.tar**: A compressed file containing all of the application files required for both the script- and GUI-based installation methods.
- **README**: A text file containing information pertaining to the release.
- **sqlfiles.tar**: Script Query Language files related to WEM database functionality.
- **ems_migrate**: A script that performs a backup or restore of the WEM databases.
- **ems_migrate.cfg**: A file that contains configuration information related to the ems_migrate script.
- **README.ems_migrate**: A text file containing information related to the EMS migrate functionality.

Determining the Best Installation Method

The WEM and its ancillary components such as the Apache web server and PostgreSQL database engine, may be installed in one of the following two methods.

- **GUI-based method:** This method is the most commonly used installation procedure. Requirements for using this method include:
    - Logon account to the WEM server with display terminal (monitor) attached and some X-Windows client installed on the server.
    - Network connectivity to WEM server via Telnet or SSH, using some X-Windows client on a remote workstation.
- **Console-based method:** This method is available to users who do not have an X-Windows client available for remote network connectivity to the WEM server via Telnet or SSH.

Installing the WEM Software using the GUI-Based Installation Wizard

Follow the instructions below to install the WEM using the GUI-based installation wizard.

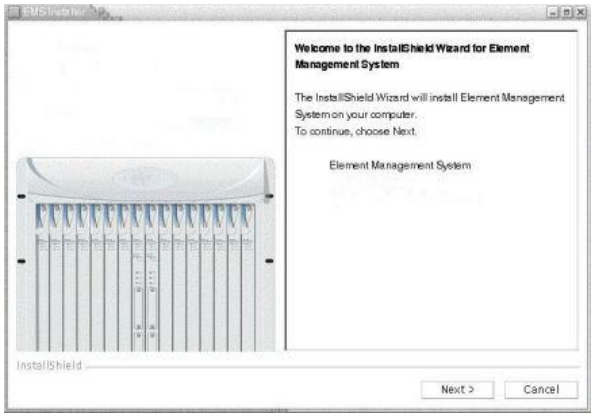
> ***Important:*** If you are installing the WEM to upgrade an existing version that is currently installed and running, proceed to the *Upgrading the WEM Software* chapter of this guide. If you are upgrading software on redundant High Availability servers using clustering software, you should refer to the appendices.

Step 1 Go to the directory in which the WEM installation files are located.

Step 2 Execute the setup file by entering the following command:

```
./inst
```

The WEM Installer dialog appears:



Step 3 Click **Next** to proceed.

Step 4 Follow the on-screen prompts to progress through the various installation dialogs and configure the parameters as required. Refer to the following table for descriptions of the configurable parameters on each of the installation dialogs.

Parameter	Description	Default Value
System Setting for Postgres		
N/A	This dialog or script section is informational and contains no configurable parameters. Information pertaining to these variables is located in the Setting the PostgreSQL Database System Environment Configurations section in this chapter.	N/A
EMS Installation Mode		

Parameter	Description	Default Value
Standalone EMS Failover Mode	This dialog or script section determines how the installation will proceed depending on the type of environment the EMS will be running in. Select Failover Mode if you are configuring a redundant High Availability Cluster. ***Important:*** Future releases will support a Scalable installation mode.	Enabled
Destination directory for Element Management System		
Directory Name	The directory on the server in which the WEM is to be installed. The directory can be manually entered in the field provided or selected using the Browse function. ***Important:*** If you are configuring a High Availability installation using redundant servers in an Oracle Cluster environment there are certain requirements regarding identical setups on both servers. Refer to the appendices for more information **before** proceeding.	/<ems_dir>/ which is */users/ems* by default
Global Configuration		
Select the IP Address	Choose this option to select one of the server IP addresses automatically detected by the WEM installation process. For the GUI-based installation, the IP address is selected from the drop-down menu.	Null
Enter the IP Address	Choose this option to manually specify an IP address. This option can be used to specify an address that has not yet been configured on the server The IP address must be entered in the field provided. ***Important:*** The IP address specified must be ICMP reachable.	Null
SSL Configuration		
Enforce SSL	If this option is selected, then the Secure Sockets Layer (SSL) connection is established for client-to-server and server-to-boxer communication. By default, the SSL encryption feature is enabled. ***Important:*** If the Enforce SSL option is enabled, the configuration settings for the chassis should be changed as needed.	Enabled
Content Filtering / Blacklisting Configuration		

Parameter	Description	Default Value
Enable Content Filtering	Select this option to enable the content filtering service on WEM. This option when enabled allows the user to configure the Master Content Rating Database Server (MCRDBS) and Central Decision Point (CDP). By default, this option is enabled.	Enabled
Enable Blacklisting	Select this option to enable the blacklisting feature on WEM. If this option is enabled, the WEM pulls the files containing the blacklisted URLS from external agency, converts them into binary format and then pushes it to the CDP.	Enabled
EMS Client Configuration		
WEM Identifier Information	If applied at installation time, this identification information will allow users to know which particular WEM they are logged into: useful for working with more than one WEM keeping track of multiple screens. This text would be saved to the *img.html* and *imgdebug.html* files so each time the user logged in the data would be retrieved and provide the WEM identifier detail on each screen automatically.	
Fixed Port Range		
Fixed Port	There are a number of applications on the WEM that require event notifications such as graphing, protocol monitoring, Front and Rear view (FRV) screens, alarms, and software upgrades. Each one requires a dedicated port for itself. Select this option if the WEM Server is to send requests (notifications) to WEM Clients on fixed ports. This is useful if a firewall exists between the Server and the Client. The assigned ports can be opened in the firewall to allow notifications. By default, if enabled, the Server uses a block of 11 ports beginning with the port number specified in by Start Port. If this option is not enabled, the operating system randomly selects open ports for use.	Disabled
Start Port	If the Fixed Port option is enabled, this parameter specifies the initial port number to use for the block of consecutive fixed ports. The port can be configured to any integer value from 1 through 65535. ***Important:*** Ports 1 to 1024 are reserved and should not be used.	40000
End Port	If the Fixed Port option is enabled, this parameter specifies the last port number to use for the block of consecutive fixed ports. The port can be configured to any integer value from 1 through 65535. ***Important:*** Ports 1 to 1024 are reserved and should not be used.	40010
Content Filtering Configuration		
Master Content Rating Database (MCRDBS):		

Parameter	Description	Default Value
MCRDBS User Name	Enter a username for the MCRDBS in the field provided.	Null
MCRDBS Password	Enter a password for the MCRDBS user in the field provided. The password is case sensitive.	Null
MCRDBS Host IP Address	Enter the host IP address of the MCRDBS to which Content Filtering server statistics files are to be sent.	Null
MCRDBS Host Name	Enter the host name for an MCRDBS server in the field provided.	Null
Full Database Import Interval(Hrs)	Enter the time interval in hours for Content Filtering Server to import various databases from MCRDBS (Databases: SFMDB). The range is from 2 to 4320 hours.	24
Incremental Database Import Interval(Hrs)	Enter the time interval in hours for Content Filtering Server to import various databases from MCRDBS (Databases: SFMDB-INC). The range is from 2 to 720 hours.	24
Full Database Backup Limit (number)	Enter the backup limit for full databases.	4
Incremental Database Backup Limit(Days)	Enter the backup limit in days for incremental databases.	30
Full Database Import Path	Enter the path to locate the SFMDB files in MCRDBS. For example: <Mcrdbs server path>/cfems/<cfems ip address>/sfmdb	Null
Incremental Database Import Path	Enter the path to locate the SFMDB-INC files in MCRDBS. For example: <MCRDBS server path>/cfems/<cfems ip address>/sfmincdb	Null
Archive Database Files	Select 1 if you want to archive the database files.	1
Central Decision Point (CDP):		
CDP User Name	Enter a username for the CDP in the field provided.	Null
CDP Password	Enter a password for the CDP user in the field provided. The password is case sensitive.	Null
CDP Host Name	Enter the CDP host name in the field provided.	Null
CDP Host IP Address	Enter the host IP address of the CDP to which CDP statistics files are to be sent.	Null
Optimized Database Export Interval(Hrs)	Enter the time interval in hours for Content Filtering Server to export the OPTCMDB files to CDP. The range is from 2 to 4320 hours.	72
Optimized Incr Database Export Interval(Hrs)	Enter the time interval in hours for Content Filtering Server to export the OPTCMDB incremental files to CDP. The range is from 2 to 720 hours.	24

Parameter	Description	Default Value
Optimized Database File Export Path	Enter the path for Content Filtering Server to export the OPTCMDB files to CDP.	Null
Trap Configuration	Select 1 to enable trap notifications.	1
Blacklisting Configuration		
NCMEC Configuration:		
URL	Enter the cumulative.csv file path at NCMEC.	Null
User Name	Enter the username required for authentication at the NCMEC site.	Null
Password	Enter the password required for authentication at the NCMEC site.	Null
Import interval(Hrs)	Enter the cumulative.csv file import interval in hours.	24
Export to CDP interval(Hrs)	Enter the time interval in hours for Content Filtering Server to export OPTCMDB-BL to CDP. The range is from1 to 5 hours.	2
Apache Server Configuration		
Apache Port (HTTP)	Enter the TCP port that the Apache web server communicates on in the field provided. Enter the port number as an integer, ranging from 0 through 65535.	80
Apache Port (HTTPS)	Enter the TCP port that the Apache web server communicates securely on in the field provided. Enter the port number as an integer, ranging from 0 through 65535. ***Important:*** Apache port HTTP and HTTPS both should be different to establish the successful connection between WEM client and WEM server.	443
Administrator Email-ID	Enter an e-mail address for the web server administrator in the field provided. Use the *username@domain* format.	root@localhost
EMS Server Configuration		
IMG Session Management (ISM):		

Parameter	Description	Default Value
Corba Communication Port	Enter the TCP port over which CORBA communication occurs with the system in the field provided. ***Important:*** This field will not be displayed if the Enforce SSL parameter in the SSL Configuration panel is enabled. ***Important:*** This setting must be identical to the iiop-port setting on the system. The parameter entered here is used as a default value by the application. Once the server installation is complete, a chassis to be managed can be configured each with their own IMG Port value through the client interface. Enter this value as an integer, ranging from 0 to 65535.	14132
Corba Communication Port (SSL)	Enter the port over which CORBA communication occurs with the system in the field provided. The corba communication port is configured same as the SSL port on the boxer. ***Important:*** This field will not be displayed if the Enforce SSL parameter in the SSL Configuration panel is disabled. ***Important:*** This setting **must** be identical to the siop-port setting on the chassis. The parameter entered here is used as a default value by the application. Once the server installation is complete, additional ASR 5000s to be managed can be configured with unique ASR 5000 Port values through via the WEM client interface. Enter this value as an integer, ranging from 0 to 65535.	14131
Application Server ID	Enter the name by which the WEM CORBA application server is identified to the chassis. ***Important:*** This name **must** match the Application Server ID name configured on the chassis for WEM to be able to manage the system. The Application Server ID name entered here is used as a default value by the application. Once the server installation is complete, additional ASR 5000s to be managed can be configured with unique Application Server ID names via the WEM client interface.	CISCO

Parameter	Description	Default Value
Application Server Password	Enter the password used by the WEM CORBA application server when communicating with the chassis. ***Important:*** This password **must** match the Application Server Password configured on the chassis for WEM to be able to manage the system. The password entered here is used as a default value by the application. Once the server installation is complete, additional ASR 5000s to be managed can be configured with unique passwords via the WEM client interface.	Null
Network Management System (NMS):		
FTP User Name	Enter a name for the WEM user with FTP privileges on the chassis in the field provided. For FTP to work properly between the WEM server and any chassis, an administrator user with FTP privileges must be configured through the system's CLI. It is highly recommended that this CLI administrator be configured using the "nocli" option, allowing only FTP privileges into the system. If the WEM server is to manage multiple chassis, then this same CLI user must be configured on each of the chassis.	staradmin
FTP Password	Enter a password for the FTP user in the field provided. The password is case sensitive.	Null
User Limit	Enter the maximum number of WEM users that can simultaneously access the server. The number can be configured to any integer value from 1 through 100.	10
Security Admin Limit	Enter the maximum number of WEM users with *Security Administrator* privileges that can simultaneously access the server. The number can be configured to any integer value from 1 to the number specified as the *User Limit*.	5
User Session Limit	Enter the maximum number of sessions allowed for a single WEM user. The number can be configured to any integer value from 0 to the number specified as the *User Limit*. A value of 0 disables the implementation of user limits on a per-context basis.	5
Context User Limit	Enter the maximum number of Web Element Management user sessions allowed on a per-system context basis. The number can be configured to any integer value from 0 to the number specified as the *User Limit*. A value of 0 disables the implementation of user limits on a per-context basis.	5
FTP Session Limit	Enter the maximum number of simultaneous FTP sessions allowed to the chassis through the WEM. The number can be configured to any integer value from 1 through 20.	5
Storage Server Directory	Enter the name of the directory in which the WEM database backup files would be stored.	./flash

Parameter	Description	Default Value
Syslog Config File	Enter the directory path for the syslog configuration file. This is needed for the WEM's syslog event viewing functionality. ***Important:*** If the file is not found in the specified directory, an error message is displayed.	/etc/syslog.conf
EMS Server Configuration (contd.)		
Fault Management (FM):		
SNMP Trap Port	Enter the TCP port over which SNMP traps are received from the system in the field provided. Enter this value as an integer, ranging from 0 to 65535.	162
SMTP Server Name	Enter a host name or IP address for a Simple Mail Transfer Protocol (SMTP) server, if needed, in the field provided. This is the mail server to which notifications are sent. ***Important:*** This parameter must be configured in order to send e-mails to new users when a trap is generated. E-mail can be configured for a trap in Alarm Configuration screen. 'SMTP Server name' is used as the E-mail Server for those mails.	Null
Sender Email-ID	Configure the e-mail address to which the system is to send notifications in the field provided. The e-mail address should be in the form *username@domain*. ***Important:*** This parameter must be configured in order to send e-mails to new users when a trap is generated. E-mail can be configured for a trap in Alarm Configuration screen. 'Sender E-mail ID' is used as the 'From' (Originator) for those mails.	Null
Bulk Statistics:		
Bulkstat FTP User Name	Enter the name of the user with FTP privileges on the external network management server. This parameter is used in conjunction with the *Bulkstat FTP Perform Operation* parameter.	anonymous
Bulkstat FTP Password	Enter the password of the user with FTP privileges on the external network management server. This parameter is used in conjunction with the *Bulkstat FTP User Name* parameter.	Null
Host IP Address	Enter the IP address of the external network management server to which XML-parsed bulkstatistic files are to be sent. This parameter is used in conjunction with the *Bulkstat FTP Perform Operation* parameter.	127.0.0.1

Parameter	Description	Default Value
Host Base Directory	Enter the directory on the external network management server to which the bulkstatistic files are to be written. The default directory is */tmp*. This parameter is used in conjunction with the *Bulkstat FTP Perform Operation* parameter.	/tmp
Archive Bulkstat Files	Select this option if the WEM is to archive bulkstatistic information from the chassis. Archived data is stored to the */<ems_dir>/server/bulkstat_archive* directory by default.	Disabled
Generate XML Files	Select this option if the server is to create XML files containing processed bulkstatistic information for forwarding to a remote server. XML-parsed data is stored in the */<ems_dir>/server/xmldata* directory by default. ***Important:*** Since the Bulkstat Server process is responsible for XML file generation, if this option is not enabled, the Bulkstat Server process is not started.	Disabled
Bulkstat FTP Perform Operation	Select this option if the server is to transfer XML-parsed bulkstatistic data files to an external network management server. Bulkstatistic information retrieved from the chassis via FTP is stored in the */<ems_dir>/server/data* directory by default prior to processing.	Disabled
User Administration		
EMS Administrator E-Mail Address	Enter an e-mail ID to be used as the originator for e-mails generated during new user account creation or password resets.	Null
Hardware Inventory		
Hardware Notifier Email-ID	Enter an e-mail ID to be used as the originator for e-mails generated as a result of a hardware change.	Null
EMS Process Monitor Configuration		
Poll Interval (sec)	Enter the frequency at which process table queries are performed. The interval is measured in seconds.	30
Number Of Retries	Configure the number of times the system attempts to communicate with a process prior to taking action. If the process has not responded to the final attempt within the configured timeout interval, the system considers it unreachable and takes action.	10
Timeout Interval (sec)	Configure the amount of time the system should wait prior to re-attempting to communicate with an un-responsive process in the field provided. The interval is measured in seconds. Once the time interval has been reached, the system re-attempts communication for the configured number of retries prior to considering the process unreachable and taking action.	330

Parameter	Description	Default Value
SMTP Server Name	Enter a host name or IP address for a Simple Mail Transfer Protocol (SMTP) server, if needed, in the field provided. This is the mail server to which notifications are sent when processes fail/start.	Null
To Email-ID	Configure the e-mail address of the individual to be notified in the field provided. E-mail notifications are sent to this individual when the system cannot communicate with a process. The e-mail address should be in the form *username@domain*.	Takes setting from previous SMTP parameter.
Monitor Process	EMS Process Monitor functionality is capable of monitoring WEM server processes at pre-configured intervals. In the event of a process becoming unresponsive, the system sends notifications and can re-spawn the process. Refer to the *WEM Process Monitor* chapter for additional information. **Important:** Special rules apply to starting processes that will update dateabases whenever you are installing redundant WEM servers using Oracle Cluster Software. Refer to the appendices for more information before starting database processes. The following processes can be monitored: • EMS Server • Bulkstat Server • Bulkstat Parser • Script Server • Northbound Server	• EMS Server: Enabled • Bulkstat Server: Disabled • Bulkstat Parser: Enabled • Script Server: Disabled • Northbound Server: Disabled
Postgres Configuration		
User Name	Enter a username for the Postgres database administrator in the field provided. **Caution:** To ensure proper operation and data integrity, the PostgreSQL database instances installed with the WEM should only be used by the application.	postgres
Password	Enter a password for the user in the field provided. The password is case sensitive.	Null
Use Local Installation	Select this option to install Postgres on the local server If enabled, the system's local IP address of 127.0.0.1 is used. **Important:** This option is not present in the console-based installation script.	Enabled

Parameter	Description	Default Value
Use Remote Installation	Select this option to install Postgres on a remote system. If enabled, configure the IP address of the server in the field provided. ***Important:*** This option is not present in the console-based installation script.	Disabled
Element Management System Installation Confirmation		
	This dialog or script section is informational and contains no configurable parameters.	N/A
Component Starting Panel (Select the components to be started)		
Select the components to be started	Select the WEM software components to start as part of the installation. ***Important:*** Special rules apply to starting services and databases when you install redundant WEM servers using Oracle Cluster Software. Refer to the appendices for more information **before** continuing. The following components are available: • Apache Server • EMS Processes • Restore old Postgres 7.2.4 database into new postgres 8.2.0 Upon selecting the component "Restore old postgres 7.2.4 database into new postgres 8.2.0", the postgres database migration is started from older version to the new version as WEM releases 7.0 and later support only Postgres version 8.2.0. For more details on the database migration process, refer to the log file *.dbmigration.log* in the */<ems_dir>/server/log* directory. ***Important:*** Successful installation of the WEM application requires that the Apache Server and EMS processes be started. The default setting is to enable them. Though prompts are provided to disable them, it is highly recommended that you do not modify the default behavior.	All components selected
Startup Script Panel		
Start EMS at machine startup	Select this option to enable the WEM to start automatically each time the server on which it is installed is rebooted. ***Important:*** This **must** be disabled if you have a redundant High Availability server cluster. See the appendices for more information.	Enabled

Once all components have started, a dialog box appears confirming that the installation was successful.

Step 5 Click the Finish button to exit the GUI-based installation wizard.

Step 6 Verify that all WEM processes were successfully started by looking at the on-screen messages in the console window. The following provides a sample of the messages:

```
Starting WEM Server...

WEM Server started.

PID: 1370

Logfile generated as:

./log/SERVER_LOG_20051220_142931/SERVER_LOG

Starting Script Server...

Script Server started.

PID: 1389

Logfile generated as:

./log/SCRIPT_LOG_20051220_142937/SCRIPT_LOG
```

The following table lists the processes that are started at installation.

Process	Log File
EMS Server	.server.log
Script Server	.scriptserver.log
BulkStat Server	.bulkstatserver.log
BulkStat Parser Server	.bulkstatparser.log
Monitor Server (if enabled)	.watchdog.log
NorthBound Server	.northboundserver.log
Notification Service	.notifyservicescript.log

All log files are stored in the */<ems_dir>/server/log* directory by default. Refer to log files for additional information in the event that one or more of the processes did not start properly.

Step 7 Copy the un-installation script to the *_uninst* directory created during the installation process (*/<ems_dir>/_uninst* by default) by entering the following command:

```
cp uninst /<ems_dir>/_uninst/
```

Step 8 Copy the files related to the WEM migrate script to the scripts directory (*/<ems_dir>/server/scripts* by default) created during the installation process by entering the following commands:

```
cp ems_migrate /<ems_dir>/server/scripts

cp README.ems_migrate /<ems_dir>/server/scripts
```

Step 9 Proceed to the *WEM Server Files and Operation* chapter of this guide for additional information on WEM Server files and functionality.

Important: Please contact Cisco support for default Username and Password.

Installing the WEM Software using the Console-Based Installation Method

Follow the instructions below to install the WEM using the console-based installation script.

> ***Important:*** If you are installing the WEM to upgrade an existing version that is currently installed and running, proceed to the *Upgrading the WEM Software* chapter of this guide.

Step 1 Go to the directory in which the WEM installation files are located.

Step 2 Execute the setup file by entering the following command:

```
./inst -console
```

A message appears welcoming you to the WEM installation.

Step 3 Enter "1" to proceed.

Step 4 Follow the on-screen prompts to proceed through the installation script and configure the various parameters as required. Refer to the *WEM Installation Parameter Descriptions* table for descriptions of the configurable parameters within each of the sections of the script.

Once you have completed the installation configuration and all processes have started, you receive a message indicating that the WEM was successfully installed.

Step 5 Enter "3" to finish the installation.

Step 6 Verify that all WEM processes were successfully started by looking at the on-screen messages in the console window. The following provides a sample of the messages:

```
Starting WEM Server...

WEM Server started.

PID: 1370

Logfile generated as:

./log/SERVER_LOG_20051220_142931/SERVER_LOG

Starting Script Server...

Script Server started.

PID: 1389

Logfile generated as:

./log/SCRIPT_LOG_20051220_142937/SCRIPT_LOG
```

The following table lists the processes that are started at installation:

Process	Log File
EMS Server	.server.log
Script Server	.scriptserver.log
BulkStat Server	.bulkstatserver.log
BulkStat Parser Server	.bulkstatparser.log
Monitor Server (if enabled)	.watchdog.log
NorthBound Server	.northboundserver.log
Notification Service	.notifyservicescript.log

All log files are stored in the */<ems_dir>/server/log* directory by default. Refer to log files for additional information in the event that one or more of the processes did not start properly.

Step 7 Copy the un-installation script to the *_uninst* directory created during the installation process (*/<ems_dir>/_uninst* by default) by entering the following command:

```
cp uninst /<ems_dir>/_uninst/
```

Step 8 Copy the files related to the WEM migrate script to the scripts directory (*/<ems_dir>/server/scripts* by default) created during the installation process by entering the following command:

```
cp ems_migrate /<ems_dir>/server/scripts

cp README.ems_migrate /<ems_dir>/server/scripts
```

Step 9 Refer to the *WEM Server Files and Operation* chapter of this guide for additional information on WEM Server files and functionality.

Important: Please contact Cisco support for default Username and Password.

Configuring IPMP on WEM Server

With IPMP, two or more network interface cards (bge0, bge1 etc.) are dedicated for each network to which the host connects. Each interface is assigned a static “test” IP address, which is used to access the operational state of the interface. Each virtual IP address is assigned to an interface, though there may be more interfaces than virtual IP addresses, some of the interfaces being purely for standby purposes. When the failure of an interface is detected its virtual IP addresses are swapped to an operational interface in the group.

The IPMP load spreading feature increases the machine's bandwidth by spreading the outbound load between all the cards in the same IPMP group.

> ***Important:*** IPMP is a feature supported on Sun® Solaris® provided by Sun Microsystems. The configuration is included in *Section VI* of the *System Administration Guide: IP Services* from Sun Microsystems. For more information, refer to the Sun documentation

This section describes following procedures to configured IP Multipathing on WEM server:

- Configuring Probe-based IP Multipathing
- Configuring Link-based IP Multipathing

Before proceeding for IPMP configuration here are some terms related to IPMP configuration:

- **Multipath Interface Group**: This the name given to the group of network devices in a multipath configuration.
- **Test Addresses**: These are IP addresses assigned to each board/interface of the multipath group, they do not move but should not be used for connections in or out of the host.
- **Multipath/float Address** - This is the IP address allocated to a Multipath Interface Group that is shared between all devices in the group (either by load sharing or active standby).

Configuring Probe-based IP Multipathing

Configuration procedure given here assumes that:

- WEM Server Host name is *hostname*
- *NIC_1* and *NIC_2* are the network interface devices; i.e. bge0, bge1 etc.
- Using network device *NIC_2* as active and *NIC_1* as the Standby
- Multipath Interface Group name is *multipath_grp*
- Multipath IP address is <*multipath_IP_address*>
- Test IP address for <*NIC_1*> interface in <*test_IP_address_NIC_1*>
- Test IP address for <*NIC_2*> interface in <*test_IP_address_NIC_2*>

Step 1 Ensure that the MAC addresses on the host are unique by setting the local-mac-address parameter to true by running following command as *root* user:

```
eeprom local-mac-address?=true
```

Step 2 Create an *NIC_1* for the Standby network device with the following entry:

```
<hostname>-<NIC_1> netmask <netmask> broadcast+group <multipath_grp> deprecated
-failover standby up
```

<*hostname*> is name of the Host and <*NIC_1*> is the network device to be set as *Standby*.

<*multipath_grp*> is Multipath Interface Group name given to the group of network devices in a multipath configuration.

<*netmask*> is the sub-netmask used by network.

Step 3 Create an *NIC_2* for the active network device with the following entry:

```
<hostname>-<NIC_2> netmask 255.255.255.0 broadcast+group <multipath_grp>
deprecated -failover up addif <hostname>-active netmask 255.255.255.0
broadcast+failover up
```

<*hostname*> is name of the Host and <*NIC_2*> is the network device to be set as *Active*.

<*multipath_grp*> is Multipath Interface Group name given to the group of network devices in a multipath configuration.

Step 4 Edit the */etc/hosts* file using "vi editor" and add the following three entries:

```
<multipath_IP_address> <hostname>-active

<test_IP_address_NIC_1> <hostname>-NIC_1

<test_IP_address_NIC_2> <hostname>-NIC_2
```

multipath_IP_address is the IP address allocated to a Multipath Interface Group that is shared between all devices in the group (either by load sharing or *Active-Standby*).

test_IP_address_NIC_1 is the IP addresses assigned to <*NIC_1*> interface of the multipath group, they do not move but should not be used for connections in or out of the host.

test_IP_address_NIC_2 is the IP addresses assigned to <*NIC_2*> interface of the multipath group, they do not move but should not be used for connections in or out of the host.

Step 5 Restart the host by supplying following command:

```
shutdown -i 6 -g 0 -y
```

Configuring Link-based IP Multipathing

Configuration procedure provided here assumes that:

- WEM Server Host name is <*hostname*>
- <*NIC_1*> and <*NIC_2*> are the network interface devices; i.e. bge0, bge1 etc.
- Using network device <*NIC_1*> as *active* and <*NIC_2*> as the *standby*
- Multipath Interface Group name is <*multipath_grp*>
- Multipath IP address is <*multipath_IP_address*>
- Test IP address for <*NIC_1*> interface in <*test_IP_address_NIC_1*>
- Test IP address for <*NIC_2*> interface in <*test_IP_address_NIC_2*>

- <*my_address*> is associated with Multipath IP address <*multipath_IP_address*> in the */etc/hosts* file

Step 1 Ensure that the MAC addresses on the host are unique by setting the local-mac-address parameter to true by running following command as root user:

```
eeprom local-mac-address?=true
```

Step 2 Create an *NIC_1* for the Active network device with the following entry:

```
<my_address> netmask + broadcast + group <multipath_grp> up
```

<*my_address*> is associated with Multipath IP address <*multipath_IP_address*> in the */etc/host* file.

<*multipath_grp*> is Multipath Interface Group name given to the group of network devices in a multipath configuration.

Step 3 Create an *NIC_2* for the Standby network device with the following entry:

```
group <multipath_grp> up
```

Step 4 Restart the host by supplying following command:

```
shutdown -i 6 -g 0 -y
```

Chapter 4
WEM Server Files and Operation

Once the WEM software has been installed correctly, the information in this chapter can be used as a reference for performing further configuration of the Web Element Management Server to customize it to your needs.

This chapter provides information on the WEM Server directory structure and important files, description for the various configuration files supported by the application, and instructions for verifying and stopping/starting component processes.

Important: If no further configuration is needed, proceed to *Preparing and Using the Client Workstation* chapter of this guide for information and instructions for preparing and using WEM Clients.

This chapter includes the following topics:

Important: Unless otherwise specified, all information in this chapter applies to both Sun Solaris- and Red Hat Enterprise Linux-based WEM systems.

Server Directory Structure and Important Files

The following table provides information on the application's directory structure after installation and identifies important files.

Table 3. WEM Server Directory Structure and Important Files

Directory/Filename	Description
/_jvm	Contains files pertaining to Java and Java Runtime Environment (JRE).
/_uninst	Contains files for uninstalling the WEM application.
uninst	Executable file for uninstalling the WEM application.
/apache	Contains files pertaining to the Apache Web Server used to provide access to the WEM.
/bin	Contains files required for starting/stopping the Apache process and HTTP daemon.
apachectl	Executable file for starting/stopping the Apache Web Server. Refer to the Controlling Server Component Processes section later in this chapter for more information.
/client	Contains files pertaining to the WEM Client.
.java.policy	Java Policy file required by client to access the WEM Server. Refer to *Preparing and Using the Client Workstation* chapter of this guide for more information.
/xxxx	A directory containing client files for the current build, xxxx is the last four digits of the current build number.
/audio	.WAV audio files used for WEM's audio alarming functions
/mapimages	.GIF map image files that can be configured for the client(s)
/webhelp	HTML-based online help files for the application; they are accessible through the client Graphical User Interface (GUI).
img.html	Webpage used for accessing WEM. Refer to *Preparing and Using the Client Workstation* chapter of this guide for more information.
imgdebug.html	The same as the img.html file except that it enables application level logs in the Java Console.
policy.html	Provides instructions on how and where to save and where to save the policy file for the varios operating systems that support WEM.
solaris-linux.html	Provides settings required for running WEM using Netscape 6.0 and earlier, and Netscape 6.0 and later, on Solaris/Linux operating systems.
versions.html	Provides the recommended versions for the various Operating Systems that support WEM.
console.log	Log file containing console messages generated during installation.
inst.log	Log file created to track installation progress.
/perlx.x.x	Contains files pertaining to the specified version of the PERL scripting language, x.x.x is the version of PERL.
/postgresx.x.x	Contains files pertaining to the PostgreSQL database used by the WEM, x.x.x is the version of Postgres.

Directory/Filename	Description
/bin	Contains files required for starting/stopping PostgreSQL and the Postmaster daemon.
pg_ctl	Executable for starting/stopping the PostgreSQL server.
pg_start	Executable for starting Postmaster daemon. Refer to the Controlling Server Component Processes section later in this chapter for more information.
pg_stop	Executable for stopping Postmaster daemon. Refer to the Controlling Server Component Processes section later in this chapter for more information.
psql	Enters the PostgreSQL interactive terminal.
vacuumdb	Removes old and/or unused records from the various WEM databases. Refer to *WEM Database Maintenance* chapter of this guide for more information.
logfile	Log file containing information pertaining to PostgreSQL operation.
/server	Contains files pertaining to the WEM Server.
/alarmscripts	A directory for storing user-defined scripts.
/bin	Contains WEM server and component executable files.
/bsschema	Contains WEM Bulk Statistics Schema configuration files.
/bulkstat_archive	Contains Bulk statistics archive files (if collected).
/crondir	A directory for storing cron-specific files.
/dbscripts	Contains scripts for use with the PostgreSQL database.
/data	Contains un-parsed bulk statistic data received from managed systems.
/etc	Contains WEM configuration files. ***Important:*** Many of these files contain user-configurable parameters for tailoring the operation of the WEM. Information on the various parameters in these files is provided within the files. Refer to the Server Configuration Files section of this chapter for more information.
alarmid.cfg	SNMP alarm identification configuration file
audio.cfg	Audio alarms configuration file
blacklist.cfg	Configuration file containing information used to enable the blacklisting feature on WEM.
bs.cfg	Bulk statistic configuration file
bsparser.cfg	Bulk statistic parser configuration file
bsparserlogger.xml	Bulk statistic parser logger file. Refer to *Enhanced WEM Logging* chapter of this guide for more information.
bsserver.cfg	Bulk statistic server module configuration file
bsserverlogger.xml	Bulk statistic server logger file Refer to *Enhanced WEM Logging* chapter of this guide for more information.
bstca.cfg	Bulk statistic threshold configuration file

Directory/Filename	Description
cf.cfg	Configuration file for Content Filtering settings.
configupdate.cfg	System software update functionality configuration file
db.cfg	Postgres database configuration file **Caution:** Improper configuration of this file can adversely affect WEM operation.
emscert.txt	WEM RSA key and certificate **Caution:** Do not alter this file.
emslic.cfg	WEM license configuration file.
emslogger.xml	WEM Server logger file Refer to *Enhanced WEM Logging* chapter of this guide for more information.
fm.cfg	Fault management configuration file containing default severity levels for product SNMP traps.
hwinv.cfg	Contains the e-mail ID used when sending notifications of hardware changes.
ism.cfg	WEM/managed system communication configuration file.
mcrdbs.cfg	MCRDBS configuration file
MeasurementStat.dtd	Document Type Definition (DTD) configuration file for validating bulk statistic data.
nb.cfg	NorthBound Notification Service configuration file
nbserver.cfg	File containing configuration parameters for NorthBound Server and Notification Service processes and other configuration parameters for the NorthBound interface.
nbserverlogger.xml	NorthBound Server logger file
nms.cfg	WEM parameter configuration file
pcrfrepgen.cfg	Configuration file for the generation of 3GPP XML reports for PCRF.
processmonitor.cfg	Process Monitor server configuration file
ps.cfg	Polling support configuration file
psmon.cfg	Process Monitor rule configuration file
pw_dict.*	All pw_dict files pertain to the password-complexity checking algorithm in support of ANSI security.
res.cfg	Screen-specific resource-bundle path configuration file **Caution:** Do not alter this file.
scriptlogger.xml	Script Server logger file Refer to *Enhanced WEM Logging* chapter of this guide for more information.

Directory/Filename	Description
ssl-key-cert.txt	Secure Sockets Layer (SSL) RSA key and certificate configuration file **Caution:** Do not alter this file.
STARENT-EMS-MIB.txt	WEM Server SNMP MIB file. Refer to the *Cisco ASR 5000 Series SNMP MIB Reference* for more information on the objects and alarms defined in the MIB.
thr.cfg	Thread pool configuration file
ua.cfg	User administration configuration file
vacuum.cfg	Database vacuuming configuration file
wblist.cfg	Configuration file storing the white black list database file paths
./flash	Storage Server Directory where the periodic backup of database is stored.
/installdata	Contains copies of the configuration files used at the time of installation.
/log	Contains log files for the various components of the WEM.
psmon	Process Monitor executable file Refer to *WEM Process Monitor* chapter of this guide for more information.
/scripts	Contains script files that can be used in conjunction with the WEM.
serv	Executable file for starting/stopping the WEM Server. Refer to the Controlling Server Component Processes section later in this chapter for more information.
/xmldata	Contains XML-parsed bulk statistic records if the “Generate XML Files” option is enabled.
ems_migrate	Script used for backup and restore of EMS directories. **Important:** This script should be used with the same EMS releases. It will be required in case of EMS setup migration from one machine to another machine, OS change (Solaris 8 to Solaris 10), etc. There is a config file with this script (*ems_migrate.cfg*), in which the list of directories for backup and restore can be specified. For example: dir_list=postgres/data server/etc server/bsschema
/tools	Contains files pertaining to tools that can be used to obtain debugging information.
getSupportDetails.pl	Script used for collecting server logs and other information that is useful for troubleshooting. Refer to the *Capturing WEM Server Logs using Script* section of the *Troubleshooting the WEM* appendix of this guide for more information on using this script.

Server Configuration Files

As identified in the *WEM Server Directory and Important Files* table, the WEM provides a number of configuration files which can be modified to fine-tune the operation of the application. These files are located in the */<ems_dir>/server/etc* directory by default.

This section provides descriptions for each of the configuration files. Details of the parameters in each file is located within the files. The default values for these parameters are suitable for most installations. However, the values can be modified using a text editor (such as *Vi Editor*) if required.

Caution: For most of these files, the WEM application process must be stopped and restarted in order for modifications to take effect. To ensure proper operation, be sure to read and understand all the information provided in the files prior to making changes.

Important: Refer to the *WEM Configuration File Parameters* appendix for detailed information on the server configuration file parameters.

The alarmid.cfg File

This file provides parameters pertaining to the configuration of SNMP alarms received from managed devices.

The audio.cfg File

This file provides alarm severity associations to specific audio files. The audio files are in.WAV format and are played by the WEM when an alarm of that severity is received.

Additionally, this file can be used to associate an audio file to a specific alarm for further customization.

The blacklist.cfg File

This file contains a flag that is set to enable/disable the blacklisting feature on WEM. The file provides parameters for specifying information such as blacklist backup limit, time interval to poll the blacklist directory, etc.

The bs.cfg File

This file provides bulk statistic configuration information pertaining to schemas, formatting, and parameters for specifying time tolerances for searching bulk statistic records.

Caution: To ensure proper operation of the WEM, bulk statistic schema and formatting configuration in this file should not be altered.

The bsparser.cfg File

This file provides parameters for specifying such information as the directories in which bulk statistics records received from the chassis are stored and archived after they are processed, in addition to time intervals for polling and record transfer.


Important: Several parameters contained in this file are configurable through the installation process.

The bsserver.cfg File

This file provides parameters pertaining to the XML-parsing of bulk statistic records received from the chassis. These parameters provide the ability to enable/disable XML parsing and specify such things as the directory in which parsed records are to be stored, time intervals for checking new records, and whether a single XML file should be generated for all subsystems or one XML file per subsystem in accordance with 3GPP TS 32.401 V4.1.0 and 3GPP TS 32.435 V6.2.0. Secure protocols should be used between WEM and the external system while exporting the performance data in the XML format.

The bulk statistics data from a managed system is received by the WEM Server in Comma Separated Value (CSV) format. The data is stored in the */server/data/<system-name>* directory by default. The XML files should get generated under *<server-dir>/xmldata* as long as the files are getting parsed and the data is getting logged in database. This generation of XML files is done by a separate process namely, bulkstatserver.


Important: Several parameters contained in this file are configurable through the installation process.

The bstca.cfg File

This file contains parameters pertaining to the threshold configuration for bulk statistic counters. This file includes the threshold values, i.e. clear threshold and set threshold to notify and clear SNMP traps accordingly. These threshold values are specified based on the threshold limit.

The cdp.cfg File

This file contains CDP specific parameters that are configured for generation of ad-hoc reports. The parameters are also configured to export Optimized Customer Master Database (OPTCMDB) files to CDP.

The cf.cfg File

This file contains Content Filtering configuration settings, including enable/disable, statistics, database archiving, and SNMP settings.

The configupdate.cfg File

This file contains parameters pertaining to performing chassis software configuration updates using the WEM. The directory in which configuration files are stored, and the directory in which configuration update log files have to be stored can be configured.

The db.cfg File

This file contains parameters pertaining to the WEM's use of the Postgres database. It identifies the various databases and their locations.

Caution: Improper configuration of this file can adversely affect WEM operation.

The emslic.cfg File

This file contains license information for the WEM Server installation.

The fm.cfg File

This file contains parameters pertaining to the handling of received alarms. It provides parameters for configuring things such as color indicators for the various severities, E-mail server information for alert notifications, and SNMP operation.

Important: Several parameters contained in this file are configurable through the installation process.

The hwinv.cfg File

This file provides the e-mail ID used when sending hardware change notifications.

Important: The parameter in this file is configurable through the installation process.

The ism.cfg File

This file contains parameters pertaining to communication between the WEM and managed chassis. These parameters include the security information used to access the chassis as well as the ports over which communication takes place.

This file also contains a parameter that provides the ability to enable/disable the SSL encryption for client-to-server and server-to-boxer communication. This parameter is configured so that the SSL encryption feature is enabled by default.

The mcrdbs.cfg File

This file contains parameters that are configured to support conversion of Vendor Format Master Database (VFMDB) to Starent Networks Format Master Database (SFMDB). This file also contains information on how MCRDBS will handle the database files.

The mdproxy.cfg File

This file defines various properties used for MD EMS proxy functionality, including the directory path to log the audit trail to a file.

The nb.cfg File

This file contains parameters for NorthBound interface notifications from the WEM. The information in this file is used by the application for forwarding fault management information to other management devices on the NorthBound interface. Configuration parameters include the device IP address and port number to which WEM will forward notifications.

The nbserver.cfg File

This file contains parameters for the configuration of NorthBound Server and Notification Service processes, and NorthBound interface.

The nms.cfg File

This file contains parameters which control WEM access to the PostgreSQL database, client access to the server, and other properties used by the application for proper operation.


Important: Several parameters contained in this file are configurable through the installation process.

The pcrfrepgen.cfg File

This file contains parameters for 3GPP XML report generation for the PCRF. It includes MPE Manager, report generation, and FTP configuration settings.

The processmonitor.cfg File

This file contains parameters used by the Process Monitor (refer to the *WEM Process Monitor* chapter for more information) function. These include parameters such as the directories from which WEM-related processes are started, polling intervals, and maximum percentage thresholds.

The ps.cfg File

This file contains parameters which control WEM polling intervals for things such as managed chassis and database queries.

The psmon.cfg File

This file contains parameters for the operation of the PSMon (Process Monitor) function supported by the WEM. Additional details on this function and the parameters in this file are located in the *WEM Process Monitor* chapter of this guide.

The res.cfg File

This file contains parameters for associating resource-bundles to specific WEM dialogs.


Caution: To ensure proper operation of the WEM, do not edit the parameters in these files.

The temip.cfg File

This file contains Inventory and Active Alarm file configuration parameters for configuring a flat-file based interface between the WEM and a Telecom Management Information Platform (TeMIP).

The thr.cfg File

This file contains parameters pertaining to the WEM thread pool.


Caution: To ensure proper operation of the WEM, do not edit the parameters in these files.

The ua.cfg File

This file contains parameters pertaining to the WEM's support for the ANSI T1.276 security specification. These include parameters granting and restricting access, login failures, password aging, and password complexity.

The vacuum.cfg File

This file contains parameters pertaining to PostgreSQL database vacuuming. Additional details on this function and the parameters in this file are located in *WEM Database Maintenance* chapter of this guide.

The wblist.cfg File

This file provides information on the white black list database file paths that are mainly used for content filtering.

Server Log Files

By default, log files generated by the WEM application are stored in the */<ems_dir>/server/log* directory. The location is specified in the *xxxxlogger.xml* files stored in the */<ems_dir>/server/etc* directory (refer to the *Enhanced WEM Logging* chapter for information on these files).

Within the *log* directory, subdirectories are created as needed to contain log files for each of the various components that comprise the WEM Server:

- EMS Server = SERVER_LOG
- Script Server = SCRIPT_LOG
- BulkStat Server = BS_SERVER_LOG
- BulkStat Parser = BS_PARSER_LOG

The above directory names are appended with a datestamp (YYYYMMDD) and timestamp (HHMMSS). For example, a subdirectory containing EMS Server logs might be named *SERVER_LOG_20051230_164433*.

Note that logs for the Process Monitor are written to the *watchdog.log* file in the log base directory.

The WEM provides enhanced logging functionality that allows for the customization of the log file output. More detailed information on configuring and using this functionality can be found in the *Enhanced WEM Logging* chapter of this guide.

Log File Severities

There are seven severity levels possible for log messages, as shown below:

- Disabled (value 8)
- Severe (value 7)
- Warning (value 6)
- Info (value 5)
- Config (value 4)
- Fine (value 3)
- Finer (value 2)
- Finest (value 1)

Each message being generated by the server, has one of the above severity levels.

What ever debugging level is configured, the messages with that level and above will be logged in the log file. For example, if level 3 is specified then, all messages of severity *Severe, Warning, Info, Config*, and *Fine* appear in the log, however, those messages with a severity of *Finer* and *Finest* do not.

The logging level is configurable using the WEM Server executable, *serv* (located in the */<ems_dir>/server* directory by default). The default level is *Finest*.

Alternatively, the *xxxxlogger.xml* files stored in the */<ems_dir>/server/etc* directory provide a mechanism for specifying the log level for the specific WEM server modules. These levels only take effect if the configured level is more granular than that configured at the server level.

Server Scripts

As identified in the *WEM Server Directory and Important Files* table, a number of user-executable scripts are provided with the WEM. These scripts are located in the */<ems_dir>/server/scripts* directory by default.

The scripts provide extended, often CPU and memory intensive functionality which is not available through the WEM Client. Because the scripts provide a more efficient mechanism for these processing-intensive functions, WEM Server performance is optimized.

The following scripts are available upon installation:

- **backup.sh:** Used to perform the backup/restore of the WEM databases.
- **batchJob.sh:** Uses user-provided information to telnet into a managed device, execute a command, and write its output to a log file. Refer to the *README.batchJob.txt* file in the same directory for more information.
- **deleteFilesTables.sh:** Deletes unnecessary information from database tables and unused files. The tableFile.cfg file is used to specify the criteria for determining which information or files are "unnecessary". Refer to the *README.deleteFilesTables.txt* file in the same directory for more information.
- **kill_ems_clnt.sh:** Provides a mechanism for terminating specific WEM client sessions. Refer to the *README.kill_ems_clnt.txt* file in the same directory for more information.
- **loadConfig.sh:** Used by the Script Server to load configuration files on the managed systems. This is not a user-executable script.
- **loadRootCron.sh:** Used by the Script Server to load the root user's cron entry for scheduling system configurations as part of the update feature. This is not a user-executable script.
- **set_superuser_password.sh:** This script is used to reset the superuser password as the default.

  Important: If the password is "superuser" then on the next login the user will be prompted to change the password as "Superuser" is a temporary password that does not meet security standards.

- **showCommand.sh:** Used by the Script Server to access and execute commands on managed devices. This is not a user-executable script.
- **showsupportdetails.sh:** Writes the show support details command output from the specified ASR 5000 to a text file for later processing. Refer to the *README.ShowSupportDetails.txt* file in the same directory for more information.
- **sortIPPools.sh**: Used to fetch the information of IP addresses for a given group in a sorted mail and to sort it out. Refer to the *README_sortIPPools.txt* file in the same directory for more information.

The above scripts can be executed by entering the following command as the *root* user:

```
./script_name
```

Where `script_name` is the name of the script as identified above.

Controlling Server Component Processes

This section provides information on verifying and manually stopping and starting WEM component processes.

Manually Verifying that WEM Components are Running

To verify that the various applications are running, follow the procedures in this section.

Verifying that the WEM is Running

Step 1 Log into the server as the user *root*.

Step 2 Go to the *server* directory within the WEM installation directory by entering the following command:

```
cd /<ems_dir>/server
```

Step 3 Verify that the application is running by entering the following command:

```
./serv status
```

The output of this command is a table listing the process, its ID (PID) and its status as shown in the following example:

```
PID     Process                Status

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

2093   Monitor Server         Running

1972   EMS Server             Running

2004   Script Server          Running

1929   BulkStat Server        Running

2022   BulkStat Parser        Running

2076   NorthBound Server      Running

2057   Notification Service   Running

------------------------------------------------------------
```

Verifying that the Apache Web Server is Running

Step 1 Log into the WEM server as the user *root*.

Step 2 Verify that the application is running by entering the following command:

```
ps -aef | grep httpd
```

Verifying that the Posters Database is Running

Step 1 Log into the WEM server as the user *root*.

Step 2 Verify that the application is running by entering the following command:

```
ps -aef | grep postmaster
```

Manually Stopping WEM Component Processes

At times, it may be necessary to manually stop WEM processes. For example, if the server on which the application is installed is to be serviced, the application processes could be stopped prior to beginning.

The WEM application and its ancillary components must be stopped in the exact order as listed below.

Important: These instructions assume that the WEM was installed in the default directory, */users/ems*.

Step 1 Log into the WEM server as the user *root*.

Step 2 Go to the *server* directory within the WEM installation directory by entering the following command:

```
cd /<ems_dir>/server
```

Step 3 Stop the WEM Server processes by entering the following command:

```
./serv stop
```

Step 4 Verify that the WEM server and WEM Script server processes are no longer running by entering the following command:

```
ps -ef | grep server
```

Step 5 Go to the PostgreSQL installation directory by entering the following command:

```
cd /<ems_dir>/postgresx.x.x/bin/
```

Step 6 Stop the Postgres processes that are currently running on the server by entering the following command:

```
./pg_stop
```

Step 7 Verify that the Postgres processes are no longer running by entering the following command:

```
ps -ef | grep postgres
```

Step 8 Go to Apache Web Server installation directory by entering the following command:

```
cd /<ems_dir>/apache/bin/
```

Step 9 Stop the Apache web server process by entering the following command:

```
./apachectl stop
```

Step 10 Verify that the Apache web server processes are no longer running by entering the following command:

```
ps -ef | grep apache
```

Manually Starting the WEM Server Components

At times it may be necessary to manually start WEM processes. For example, if the server on which the application is installed is rebooted, the application processes must be restarted according to the instructions in this section.

The WEM application and its ancillary components must be started in the exact order as listed in this section.

Step 1: Start Apache Web Server

Step 1 Log into the WEM server as the user *root*.

Step 2 Move to the Apache directory by entering the following command:

```
cd /<ems_dir>/apache/bin
```

Step 3 Start the Apache web server by entering the following command:

```
./apachectl start
```

Step 4 Verify that the process is running using the instructions provided in the Manually Verifying that WEM Components are Running section of this chapter.

Step 2: Start Postgres Database

Step 1 Log into the WEM server as the user *root*.

Step 2 Move to the Postgres directory by entering the following command:

```
cd /<ems_dir>/postgresx.x.x/bin
```

Step 3 Start the Postgres database by entering the following command:

```
./pg_start
```

Step 4 Verify that the process is running using the instructions provided in the Manually Verifying that WEM Components are Running section of this chapter.

Step 3: Start WEM Server Application

Step 1 Log into the WEM server as the user *root*.

Step 2 Move to the WEM Server directory by entering the following command:

```
cd /<ems_dir>/server
```

Step 3 Start the WEM server application by entering the following command:

```
./serv start
```

Step 4 Verify that the process is running using the instructions provided in the Manually Verifying that WEM Components are Running section of this chapter.

Chapter 5
WEM Process Monitor

The Process Monitor is a script used for monitoring and maintaining WEM application software processes. It provides the flexibility of being run as a stand-alone program or a fully functional background daemon and is capable of logging to syslog and log file with customizable e-mail notification facilities. The ability to monitor and maintain these processes coupled with the ease and flexibility of this feature's configuration ensure maximum availability and optimum server performance.

The processes are monitored based on rules defined within a configuration file stored on the server. These rules identify criteria for determining the action to be taken if the conditions are met. (For example, if a process becomes unresponsive, the rule could cause the process to be re-spawned.)

Basic parameters pertaining to the Process Monitor were configured as part of the WEM installation or upgrade process. However, additional parameters are available for fine-tuning its configuration to meet the needs of your network.

Important: When installing redundant servers, any WEM services started by the **`<ems/home>/server/servstart`** command and monitored by the Process Monitor are **not** started automatically. Refer to *Appendix A* for information on installing redundant servers using Oracle Cluster software.

This chapter provides information and procedures for modifying the Process Monitor's operation using the configuration file.

This chapter includes the following topics:

Important: Unless otherwise specified, all information in this chapter applies to both Sun Solaris- and Red Hat Enterprise Linux-based WEM systems.

Process Monitor Configuration File

Processes are monitored based on rules defined within a plain-text configuration file called psmon.cfg located in the /users/ems/server/etc directory (by default).

Rules are defined within the file using the following syntax:

```
<Process process_id>
   processing-directives directive_variables
</Process>
```

The following table provides the syntax descriptions.

Table 4. psmon.cfg Rule Syntax Descriptions

Syntax	Description
<Process *process_id*>	Identifies the process to be monitored. The process can be identified by name (i.e. ssh) or by URL (i.e. /users/ems/server/bin/server). Additionally, a wildcard (*) can be specified for monitoring all the processes.
processing-directives *directive_variables*	Identifies the criteria that must be met before action is taken as well as the action to be taken. The criteria are referred to as "Directives", while the actions are referred to as "Process Scope Directives". It is important to note that processing directives can be specified within a specific rule or outside of all rules. When outside, the directive is applied globally to all rules. The psmon.cfg Processing Directives table provides information on the supported processing directives.
</Process>	Indicates the end of a process rule.

Table 5. psmon.cfg Processing Directives

Directive	Description

Directive	Description
Facility	Identifies the syslog facility used for logging. The following facilities are supported: • LOG_KERN • LOG_USER • LOG_MAIL • LOG_DAEMON • LOG_AUTH • LOG_SYSLOG • LOG_LPR • LOG_NEW • SLOG_UUCP • LOG_CRON • LOG_LOCAL0 • LOG_LOCAL1 • LOG_LOCAL2 • LOG_LOCAL3 • LOG_LOCAL4 • LOG_LOCAL5 • LOG_LOCAL6 • LOG_LOCAL7 Default: LOG_DAEMON
LogLevel	Identifies the log level priority used to mark notifications to syslog. The following levels are supported: • LOG_EMERG • LOG_ALERT • LOG_CRIT • LOG_ERR • LOG_WARNING • LOG_NOTICE • LOG_INFO • LOG_DEBUG This directive may also be used in a Process Scope Directive which has precedence over a global declaration. Default: LOG_NOTICE
KillLogLevel (previously KillPIDLogLevel)	Identical to the LogLevel directive, however it only applies to process kill actions. This directive has precedence over the LogLevel Directive and may also be used in a Process Scope Directive which has precedence over a global declaration.

Directive	Description
SpawnLogLevel	Identical to the LogLevel directive, however it only applies to process spawn actions. This directive has precedence over the LogLevel Directive and may also be used in a Process Scope Directive which has precedence over a global declaration.
AdminEmail	Specifies the e-mail address to which notification e-mails should be sent. This directive corresponds to the **To Email-ID** parameter configured during the WEM installation. During the installation, it is stored as a global declaration, however it may also be used in a Process Scope Directive which has precedence over a global declaration. Default: root@localhost
NotifyEmailFrom	Specifies the e-mail address used in the "From" field of sent notification e-mails. Default: <username>@hostname
Frequency	The frequency (measured in seconds) at which the Process Monitor attempts communication with a process. This directive corresponds to the **Poll Interval** parameter configured during the WEM installation. During the installation, it is stored as a global declaration, however it may also be used in a Process Scope Directive which has precedence over a global declaration. Default: 30 seconds
LastSafePID	Specifies the highest process identification number which the Process Monitor cannot "kill". When specified, the Process Monitor never attempts to kill a process ID which is numerically less than or equal to the value defined by this directive. This directive is treated as a global directive by default. Default: 800
ProtectSafePIDsQuietly	Enables or disables the suppression of all notifications for preserved process IDs when used in conjunction with the lastsafepid directive. "On" enables this functionality. "Off" disables it. This directive is treated as a global directive by default. Default: Off
SMTPHost	Specifies the IP address or hostname of the Simple Mail Transport Protocol (SMTP) server used for sending e-mail notifications. This directive corresponds to the **SMTP Server Name** parameter configured during the WEM installation. During the installation, it is stored as a global declaration, however it may also be used in a Process Scope Directive which has precedence over a global declaration. Default: localhost
SMTPTimeout	Specifies the timeout (measured in seconds) used during SMTP connections. Default: 20 seconds
SendmailCmd	Enables the configuration of the **sendmail** command used for sending e-mail notifications if a failure occurs with the SMTP connection to the host specified by the SMTPHost Directive. Default: /usr/sbin/sendmail -t
Dryrun	Forces this Process Monitor to function as if the --dryrun command line switch had been specified. This can be used for forcing a specific configuration file to only report information but never take any automated action. This directive is treated as a global directive by default. Default: False (disabled)

Directive	Description
NotifyDetail	Specifies the verbosity of the notification e-mails. The following levels are supported: • Simple • Verbose • Debug Default: Verbose
PROCESS SCOPE DIRECTIVES	
SpawnCmd	Identifies the full command line to be executed in order to re-spawn a dead process.
KillCmd	Identifies the full command line to be executed in order to gracefully shutdown or kill a rogue process. If the command returns a boolean true exit status then, it is assumed that the command failed to execute successfully. If no KillCmd is specified or the command fails, the process is killed by sending a SIGKILL signal with the standard kill() function.
PIDFile	Identifies the full path and filename of a file created by the process containing the identification number of its main parent process.
NUMRETRY	The number of times the Process Monitor attempts to communicate with an un-responsive process before taking action. If the process has not responded to the final attempt within the configured timeout interval, the system considers it unreachable and takes action. This directive corresponds to the **Number of Retries** parameter configured during the WEM installation. During the installation, it is stored as a Process Scope Directive for each rule defined for WEM process. Default: 10
TMINTVAL	The amount of time (measured in seconds) the system should wait prior to re-attempting to communicate with an un-responsive process. Once the time interval has been reached, the system re-attempts communication for the configured number of retries. This directive corresponds to the **Timeout Interval** parameter configured during the WEM installation. During the installation, it is stored as a Process Scope Directive for each rule defined for WEM process. Default: 330
TTL	Specifies a maximum time-to-live (in seconds) for a process. The process is killed once it has been running longer than this value, and its process identification number is removed from the defined pidfile.
PctCpu	Specifies the maximum allowable percentage of CPU time a process may use. The process is killed once its CPU usage exceeds this threshold and its process identification number is removed from the defined pidfile.
PctMem	Specifies the maximum allowable percentage of total system memory a process may use. The process will be killed once its memory usage exceeds this threshold and its process identification number is removed from the defined pidfile.
Instances	Specifies the maximum number of instances of a process that are allowed to run simultaneously. The process will be killed once its memory usage exceeds this threshold and its process identification number is removed from the defined pidfile.

Directive	Description
NoEmailOnKill	Enables or disables the suppression of e-mail notifications for killed processes. Default: False (disabled)
NoEmailOnSpawn:	Enables or disables the suppression of e-mail notifications for spawned processes. Default: False (disabled)
NoEmail	Enables or disables the suppression of all e-mail notifications. Default: False (disabled)
NeverKillPID	Specifies a list or process identification numbers (separated by spaces) that are never to be killed. Default: 1
NeverKillProcessName	Specifies a list or process names (separated by spaces) that are never to be killed. Default: kswapd kupdated mdrecoveryd

Default Rules

During installation, WEM provided the user with the opportunity to automatically define rules for the following process monitors:

- **EMS Server:** Enabled by default
- **Bulkstat Server:** Disabled by default
- **Bulkstat Parser:** Enabled by default
- **Script Server:** Disabled by default
- **Northbound (NB) Server:** Disabled by default
- **Notification Service:** Disabled by default

> ***Important:*** Two additional WEM processes are pre-configured to be monitored by the Process Monitor: the *Postgres database* process and the *Apache Webserver* process. Configurables for these two processes appear in the *psmon.cfg* file, but they cannot be altered during the WEM installation process.

The following table identifies the default rules configured for each of the above processes.

Table 6. Default Rules for WEM Process Monitors Processes

Process	Default Rule
EMS Server	**<Process** */<ems_dir>/server/bin/server***>** **spawncmd** *(cd /<ems_dir>/server; /<ems_dir>/server/bin/server)* **pidfile** */<ems_dir>/server/server.pid* **numretry** *10* **tmintval** *330* **</Process>**
Bulkstat Server	**<Process** */<ems_dir>/server/bin/bulkstatserver***>** **spawncmd** *(cd /<ems_dir>/server; /<ems_dir>/server/bin/bulkstatserver)* **pidfile** */<ems_dir>/server/bsserver.pid* **numretry** *10* **tmintval** *330* **</Process>**
Bulkstat Parser	**<Process** */<ems_dir>/server/bin/bulkstatparser***>** **spawncmd** *(cd /<ems_dir>/server; /<ems_dir>/server/bin/bulkstatparser)* **pidfile** */<ems_dir>/server/bulkstatparser.pid* **numretry** *10* **tmintval** *330* **</Process>**
Script Server	**<Process** */<ems_dir>/server/bin/scriptsrv***>** **spawncmd** *(cd /<ems_dir>/server; /<ems_dir>/server/bin/scriptsrv)* **pidfile** */<ems_dir>/server/script.pid* **numretry** *10* **tmintval** *330* **</Process>**

Process	Default Rule
Northbound Server	**<Process** */<ems_dir>/server/bin/nbserver***>** **spawncmd** *(cd /<ems_dir>/server; /<ems_dir>/server/bin/nbserver)* **pidfile** */users/ems/server/nbserver.pid* **numretry** *10* **tmintval** *330* **</Process>**
Notify Service	**<Process** */<ems_dir>/server/bin/Notify_Service***>** **spawncmd***(cd /<ems_dir>/server; /<ems_dir>/server/bin/nbSrvr* **pidfile** */<ems_dir>/server/notify_service.pid* **numretry** *10* **tmintval** *330* **</Process>**
Postgres Database	**<Process** */<ems_dir>/postgresx.x.x/bin/postmaster -i***>** **spawncmd** */<ems_dir>/server/scripts/postgresctl start* **pidfile** */<ems_dir>/postgresx.x.x/data/postmaster.pid* **numretry** *10* **tmintval** *330* **</Process>**
Apache Webserver	**<Process** */<ems_dir>/apache/bin/httpd -f /<ems_dir>/apache/conf/httpd.conf***>** **spawncmd** */<ems_dir>/apache/bin/apachectl start* **pidfile** */<ems_dir>/apache/logs/httpd.pid* **numretry** *10* **tmintval** *330* **</Process>**

Verifying the Process Monitor Status

The status of the Process Monitor can be checked at any time by executing either of the following commands:

```
ps -ef | grep psmon
```

or

```
./serv monitor
```

The first command indicates whether or not an active psmon process is running. The second command performs one of the following:

- If the Process Monitor is stopped, executing this command is equivalent to executing the **`./serv monitor start`** command (refer to the Manually Starting the Process Monitor section in this chapter).
- If the Process Monitor is currently running, a message is displayed indicating that it is running. A prompt is also provided that allows you to restart the process. To restart the process, enter **yes**.

Manually Stopping the Process Monitor

Upon installation of the WEM, the Process Monitor is started automatically. This section provides instructions for manually disabling it. This can be useful if changes are made to the configuration file.

Follow the instructions below to manually stop the Process Monitor.

Step 1 Login as the root user.

Step 2 Go to the directory in which the WEM Server application file is located. By default, this is the */<ems_dir>/server* directory. Enter the following command:

```
cd /<ems_dir>/server
```

Step 3 Stop the Process Monitor by entering the following command:

```
./serv monitor stop
```

Step 4 Verify that the Process Monitor has stopped by executing the following command:

```
ps -ef | grep psmon
```

If the Process Monitor was successfully stopped, this command finds no active process and returns no result.

Manually Starting the Process Monitor

Upon installation of the WEM, the Process Monitor is started automatically. However, if the process was stopped, it can be started using the information and instructions in this section.

Step 1 Login as the root user.

Step 2 Go to the directory in which the WEM Server application file is located. By default, this is the */<ems_dir>/server* directory. Enter the following command:

```
cd /<ems_dir>/server
```

Step 3 Start the Process Monitor by entering the following command:

```
./serv monitor start
```

Once the Process Monitor is started, a status message is displayed. The process identification number assigned to the psmon process, and the directory in which the created log file is located is also displayed.

Running the Process Monitor as a Stand-alone Application

As mentioned previously, the Process Monitor can be run as a background deamon (the default operation when enabled during the installation of the WEM) or a stand-alone application.

This section provides information and instructions for running the Process Monitor as a stand-alone application from the command line interface.

To run the Process Monitor from the command line, use the following instructions:

Step 1 Login as the root user.

Step 2 Go to the directory in which the Process Monitor application file is located. By default, this is the */<ems_dir>/server* directory. Enter the following command:

```
cd /<ems_dir>/server
```

Step 3 Launch the Process Monitor application by entering the following command:

```
./psmon [--conf=filename] [--daemon] [--cron] [--user=user] [--
adminemail=emailaddress] [--dryrun] [--help] [--version]
```

Keyword/Variable	Description
--conf=*filename*	Specify an alternate configuration file name (other than the *psmon.cfg* file).
--daemon	Start as background deamon.
--cron	Disables already running errors when trying to launch (i.e. with the --daemon option).
--user=*user*	Specifies that only processes running under the specified username should be scanned.
--adminemail=*emailaddress*	Specifies the e-mail address to send notifications to.
--dryrun	Provides notifications but does not kill or spawn new processes.
--help	Displays the supported keywords.
--version	Displays the version information.

Depending on the command used, the rules dictated by the configuration file are executed.

Chapter 6
Enhanced WEM Logging

The WEM application is equipped with enhanced logging functionality that provides the user with the ability to:

- Dynamically change logger parameter settings in real-time through the use of text-based Extensible Markup Language (XML) configuration files.
- Tailor both the log message and log file format to meet your needs.
- Provide log messages for different severity levels.
- Filter log messages.

This chapter includes the following topics:

Important: Unless otherwise specified, all information in this chpater applies to both Sun Solaris- and Red Hat Enterprise Linux-based WEM systems.

Supported Components

Enhanced logging functionality is supported for the following WEM components:

- **WEM Server:** Logging for the server component of the WEM is facilitated by the *emslogger.xml* file located in the */<ems_dir>/server/etc* directory by default. This component consists of a number of categories (called loggers) as described in the following table.

Table 7. EMS Server Component Logger Categories

Category	Description
AAARADIUS	Pertains to authentication, authorization, and accounting (AAA) functionality using the RADIUS protocol functionality.
ADHOCRPT	Pertains to ad-hoc report generation functionality
AlarmMgmtMain	Pertains to SNMP alarm management functionality.
APN	Pertains to Access Point Name (APN) functionality
CA	Pertains to Context Administration (CA) functionality.
CAT	Pertains to Config Audit Trail (CAT) functionality.
CDR	Pertains to Charging Detail Record (CDR) functionality.
CHARGINGSVC	Pertains to integrated Enhanced Charging Service (ECS) functionality.
CPU	Pertains to system Central Processing Unit (CPU) state information.
CSM	Pertains to Client Session Management (CSM) functionality.
CSP	Pertains to the system's Card, Slot, Port (CSP) software task.
CSS	Pertains to Content Service Steering (CSS) functionality.
DB	Pertains to Data Base (DB) functionality.
DHCP	Pertains to DHCP functionality.
FM	Pertains to Fault Management (FM) functionality.
GBLCMDS	Pertains to system Global Commands (GBLCMDS) functionality.
starent-tableGGSN	Pertains to GGSN functionality.
starent-tableGTPC	Pertains to GTP Control (GTPC) functionality.
GTPP	Pertains to GTP Prime (GTPP) functionality.
IMGCACHE	Pertains to system Information Cache (IMGCACHE) functionality.
IMGKA	Pertains to system Keep-Alive (IMGKA) functionality.
IMGLicense	Pertains to system session and feature-use licensing.
Interceptor	Pertains to Client interceptor methods functionality.

Category	Description
IPSec	Pertains to IP Security functionality.
L2TP	Pertains to L2TP functionality.
Logs	Pertains to system log functionality.
MIP	Pertains to Mobile IP functionality.
Monitor	Pertains to Monitor functionality.
NR	Pertains to Network Reachability Server Configuration functionality.
ORBEM	Pertains to Common Object Broker Request Architecture (CORBA) functionality.
OSPF	Pertains to OSPF routing functionality.
Pdsn	Pertains to PDSN functionality.
PM	Pertains to Process Monitor (PM) functionality.
PortMon	Pertains to system port monitoring functionality.
PPP	Pertains to PPP functionality.
PS	Pertains to polling support functionality.
RP	Pertains to RP interface functionality.
ScbrSessMgt	Pertains to subscriber session management functionality.
SessionSubsystem	Pertains to the system session subsystem software.
SNMP	Pertains to SNMP functionality.
SVPN	Pertains to the system Virtual Private Network (VPN) software tasks.
System	Pertains to system functionality.
TCA	Pertains to threshold crossing alert functionality.
Topology	Pertains to Topology interface functionality.
UA	Pertains to User Administration functionality.
UCM	Pertains to Access Service Configuration (UCM) functionality.
UPref	Pertains to User Preferences functionality.
SWU	Pertains to Software Upgrade functionality.
ConfigBackup	Pertains to the Web Element Manager's configuration backup functionality.

- **Bulk Statistics Parser:** Logging for the Bulk Statistic Parser component of the WEM is facilitated by the *bsparserlogger.xml* file located in the */<ems_dir>/server/etc* directory by default. This component is responsible for analyzing information collected by the Bulk Statistic Server.
- **Bulk Statistics Server:** Logging for the Bulk Statistic Server component of the WEM is facilitated by the *bsserverlogger.xml* file located in the */<ems_dir>/server/etc* directory by default. This component is responsible for collecting bulk statistic information from the system.

- **Script Server:** Logging for the Script Server component of the WEM is facilitated by the *scriptlogger.xml* file located in the */<ems_dir>/server/etc* directory by default. This component supports the ability to execute specific scripts upon the receipt of SNMP alarms.
- **NorthBound Server**: Logging for the NorthBound Server component of the WEM is facilitated by the *nbserverlogger.xml* file located in the */<ems_dir>/server/etc* directory by default. This component is responsible for collecting NB server information from the system.

The XML configuration file for each of the above components consists of the following configurable elements:

- **Appender settings:** Control log file parameters such as naming, output location, format, and sizing specifications.
- **Logger settings:** Control logging parameters for the specified category such as whether or not to use appender settings and the log level. As described previously, the WEM Server component consists of multiple loggers. There is a single logger for the other components.
- **Root element:** Contains references to other appenders that should be added to loggers contained in the XML configuration file. In addition, this element contains a parameter that dictates how often the system is to scan and incorporate changes made to the logger configuration. (Additional information on configuring the scan frequency is provided in the Configuring Support for Dynamic Logging Updates section of this chapter.)

Configuring Appender Settings

Appender settings control log file parameters such as naming, output location, format, and sizing specifications.

Appenders are defined by their class. Each class has related parameters that are configurable. The following appender classes are supported:

- Asynchronous Appender
- Console Appender
- File Appender
- Rolling File Appender
- Daily Rolling File Appender
- Socket Appender
- Telnet Appender
- SMTP Appender
- Syslog Appender

Detailed information for each of the above classes is provided in the sections that follow.

By default, each logging configuration file has a single Rolling File Appender configured called *Main*. Each logger within the file is configured to use this appender by default. (It is referenced in the *root* element in the configuration file.) Additional appenders can be added to the configuration file using a text editor (such as Vi Editor) if desired.

Asynchronous Appender Settings

Asynchronous appenders are used to log events asynchronously. It uses a bounded buffer to store logging events. A separate thread is used to serve the events in its bounded buffer.

Multiple appenders can be attached to an Asynchronous appender. In this scenario, this appender collects the events sent to it and then, dispatches them to all the appenders that are attached to it.

Asynchronous appenders have the following format:

```
<appender name="appender_name" class="AsyncAppender">

   <param name="BufferSize" value="size"/>

   <appender-ref ref="attached_appender"/>

</appender>
```

The variables identified in the format above are described in the following table.

Table 8. Asynchronous Appender Variable Descriptions

Variable	Description
appender_name	The name of the appender.

Variable	Description
size	Specifies the number of events to be stored in buffer. This is configured as a non-negative integer value. The default is 128 events.
attached_appender	The name of an appender to be attached to this appender.

Console Appender Settings

Console appenders display log events to the console display.

Console appenders have the following format:

```
<appender name="appender_name" class="ConsoleAppender">
   <param name="Target" value="output"/>
   <layout class="layout_class">
  <param name="ConversionPattern" value="conv_pattern"/>
   </layout>
</appender>
```

The variables identified in the format above are described in the following table.

Table 9. Console Appender Variable Descriptions

Variable	Description
appender_name	The name of the appender.
output	Specifies the file output as either stdout or stderr. The default target is stdout.
layout_class	Specifies the format of the log file output. Refer to the Log File Output Formats section of this chapter for information on supported output formats.
conv_pattern	Specifies the conversion pattern used to format event related information. Refer to the *Pattern Layout Supported Conversion Characters* table for a list of supported conversion characters.

File Appender Settings

This appender adds log events to a file.

File appenders have the following format:

```
<appender name="appender_name" class="FileAppender">
   <param name="File" value="file_name"/>
```

```
   <param name="Append" value="append_option"/>

   <layout class="layout_class"> <param name="ConversionPattern"
value="conv_pattern"/>

   </layout>

</appender>
```

The variables identified in the format above are described in the following table.

Table 10. File Appender Variable Descriptions

Variable	Description
appender_name	The name of the appender.
file_name	Specifies the name of the output file.
append_option	Dictates whether log information will be appended to the file or not. This can be set to either of the following options: • **true :** Append the information; this is the default setting. • **false :** Do not append the information.
layout_class	Specifies the format of the log file output. Refer to Log File Output Formats section of this chapter for information on supported output formats.
conv_pattern	Specifies the conversion pattern used to format event related information. Refer to the *Pattern Layout Supported Conversion Characters* table for a list of supported conversion characters.

Rolling File Appender Settings

This appender type extends the File Appender capability to backup the log files when they reach a certain size. This is the default appender type.

Rolling File appenders have the following format:

```
<appender name="appender_name" class="RollingFileAppender">

   <param name="File" value="file_name"/>

   <param name="Append" value="append_option"/>

   <param name="MaxFileSize" value="size"/>

   <param name="MaxBackupIndex" value="max_backups"/>

   <layout class="layout_class">

   <param name="ConversionPattern" value="conv_pattern"/>

   </layout>
```

```
</appender>
```

The variables identified in the format above are described in the following table.

Table 11. Rolling File Appender Variable Descriptions

Variable	Description
appender_name	The name of the appender. By default, each configuration file has a single appender configured called Main-- each logger within the file are configured to use this appender by default. Additional appenders can be added to the configuration file using the defined format. This allows you to specify an appender for each logger if desired.
file_name	Specifies the name of the output file.
append_option	Dictates whether log information will be appended to the file or not. This can be set to either of the following options: • **true :** Append the information; this is the default setting. • **false :** Do not append the information.
size	Specifies the maximum size (in mega bytes) a log file can reach before creating a backup file and starting a new log file. This can be configured to any integer value from 0 to (263-1). The suffixes “KB”, “MB” or “GB” so that the integer is interpreted being expressed respectively in kilobytes, megabytes or gigabytes. (For example, the value “10KB” is interpreted as 10240 Bytes.) The default value is 5MB.
max_backups	Specifies How many backup files are kept before the oldest is erased. It can be configured as a non-negative integer value. A value of 0 generates no backup files no backup files and truncates the log file when it reaches MaxFileSize. The default value is 10.
layout_class	Specifies the format of the log file output. Refer to the Log File Output Formats section of this chapter for information on supported output formats.
conv_pattern	Specifies the conversion pattern used to format event related information. Refer to the *Pattern Layout Supported Conversion Characters* table for a list of supported conversion characters.

Daily Rolling File Appender Settings

This appender extends the File Appender capability so that the underlying file is rolled over at a user chosen frequency. The rolling schedule is specified by the DatePattern option. A formatted version of the date pattern is used as the suffix for the rolled file name.

Daily Rolling File appenders have the following format:

```
<appender name="appender_name" class="DailyRollingFileAppender">
   <param name="File" value="file_name"/>
   <param name="Append" value="append_option"/>
   <param name="DatePattern" value="date_format"/>
```

```
   <layout class="layout_class">      <param name="ConversionPattern"
value="conv_pattern"/>

   </layout>

</appender>
```

The variables identified in the format above are described in the following table.

Table 12. Daily Rolling File Appender Variable Descriptions

Variable	Description
appender_name	The name of the appender. By default, each configuration file has a single appender configured called *Main*-- each logger within the file are configured to use this appender by default. Additional appenders can be added to the configuration file using the defined format. This allows you to specify an appender for each logger if desired.
file_name	Specifies the name of the output file.
append_option	Dictates whether log information will be appended to the file or not. This can be set to either of the following options: • **true :** Append the information; this is the default setting. • **false :** Do not append the information.

Variable	Description
date_format	Specifies the date format. The following time and date options are supported: • %a -- Abbreviated weekday name • %A -- Full weekday name • %b -- Abbreviated month name • %B -- Full month name • %c -- Standard date and time string • %d -- Day of month as a decimal(1-31) • %H -- Hour(0-23) • %I -- Hour(1-12) • %j -- Day of year as a decimal(1-366) • %m -- Month as decimal(1-12) • %M -- Minute as decimal(00-59) • %p -- Locale's equivalent of AM or PM • %Q -- Millisecond as decimal (000-999) • %S -- Second as decimal(00-59) • %U -- Week of year, Sunday being first day(0-53) • %w -- Weekday as a decimal(0-6, Sunday being 0) • %W -- Week of year, Monday being first day(0-53) • %x -- Standard date string • %X -- Standard time string • %y -- Year in decimal without century(0-99) • %Y -- Year including century as decimal • %Z -- Time zone name • %% -- The percent sign
layout_class	Specifies the format of the log file output. Refer to the Log File Output Formats section of this chapter for information on supported output formats.
conv_pattern	Specifies the conversion pattern used to format event related information. Refer to the *Pattern Layout Supported Conversion Characters* table for a list of supported conversion characters.

For example, if the File parameter is set to abc.log and the DatePattern parameter is set to *.%Y-%m-%d*, on 2001-02-16 at midnight, the logging file *abc.log* is copied to *abc.log.2001-02-16* and logging for 2001-02-17 will continue in *abc.log* until it rolls over the next day.

Socket Appender Settings

This appender has the following properties:

- If sent to a *Socknode*, remote logging is non-intrusive as far as the log event is concerned. In other words, the event will be logged with the same time stamp, nested diagnostic Context, and location information as if it were logged locally by the client.
- Socket appenders do not use a layout. They ship a serialized *LoggingEvent* object to the server side.
- Remote logging uses the TCP protocol. Consequently, if the server is reachable, then log events eventually arrive at the server.
- If the remote server is down, the logging requests are simply dropped. However, if and when the server comes back up, event transmission is resumed transparently. This transparent re-connection is performed by a connector thread which periodically attempts to connect to the server.

Socket appenders have the following format:

```
<appender name="appender_name" class="SocketAppender">
   <param name="RemoteHost" value="host"/>
   <param name="Port" value="port_no"/>
</appender>
```

The variables identified in the format above are described in the following table.

Table 13. Socket Appender Variable Descriptions

Variable	Description
appender_name	The name of the appender.
host	Specifies the host to log messages to.
port_no	Specifies the port number over which to log events.

Telnet Appender Settings

This appender specializes in writing to a read-only socket. The output is provided in a telnet-friendly way so that a log can be monitored over TCP/IP. Clients using telnet connect to the socket and receive log data. This is handy for remote monitoring, especially when monitoring a servlet.

Telnet appenders have the following format:

```
<appender name="appender_name" class="TelnetAppender">
   <param name="RemoteHost" value="host"/>
   <param name="Port" value="port_no"/>
</appender>
```

The variables identified in the format above are described in the following table.

Table 14. Telnet Appender Variable Descriptions

Variable	Description
appender_name	The name of the appender.
host	Specifies the host to log messages to.
port_no	Specifies the port number over which to log events.

SMTP Appender Settings

This appender supports the sending of an e-mail when a specific logging event occurs, typically on errors or fatal errors.

The number of logging events delivered in this e-mail depend on the value of *BufferSize* option. The SMTP Appender keeps only the last *BufferSize* logging events in its cyclic buffer. This keeps memory requirements at a reasonable level while still delivering useful application context.

SMTP appenders have the following format:

```
<appender name="appender_name" class="SMTPAppender">
   <param name="BufferSize" value="size" />
   <param name="SMTPHost" value="smtp_host"/>
   <param name="From" value="sender"/>
   <param name="To" value="recipient"/>
   <param name="Subject" value="subject"/>
   <layout class="layout_class">
      <param name="ConversionPattern" value="conv_pattern"/>
   </layout>
</appender>
```

The variables identified in the format above are described in the following table.

Table 15. SMTP Appender Variable Descriptions

Variable	Description
appender_name	The name of the appender.

Variable	Description
size	Specifies the maximum number of logging events to collect in a cyclic buffer. When the *BufferSize* is reached, the oldest events are deleted as new events are added to the buffer. The size can be configured to a non-negative integer value. The default size of the cyclic buffer is 512 events.
smtp_host	Specifies the SMTP mail server.
sender	Specifies the e-mail address of the sender.
recipient	Specifies the e-mail address of the recipient.
subject	Specifies a subject for the e-mail.
layout_class	Specifies the format of the log file output. Refer to the Log File Output Formats section of this chapter for information on supported output formats.
conv_pattern	Specifies the conversion pattern used to format event related information. Refer to the *Pattern Layout Supported Conversion Characters* table for a list of supported conversion characters.

Log File Output Formats

The WEM enhanced logging function provides the ability to specify the log file output format. Layout configuration is performed using the *layout class* parameter.

The following formats are supported:

- HTML Layout
- TTCC Layout
- Simple Layout
- Pattern Layout

Detailed information for each of the above classes is provided in the sections that follow.

HTML Layout

This layout displays events in HTML tables. For each event, the following fields are provided:

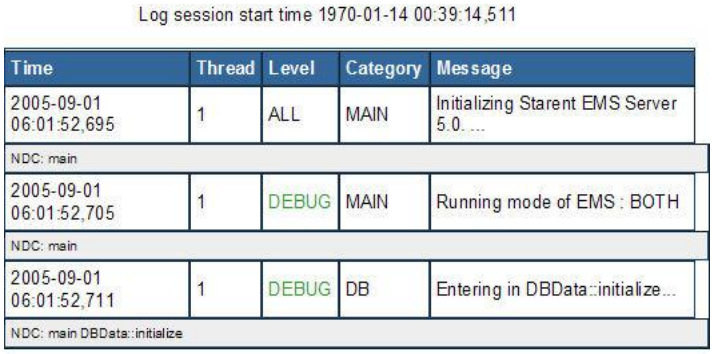
- **Time:** Event time
- **Thread:** Event thread
- **Level:** Event severity Level
- **Category (Module):** The enhanced logging function category that generated the event
- **Message:** Event description

Use the following parameter configuration to use the HTML Layout:

```
<layout class="HTMLLayout"/>
```

An example of this layout's output is shown below.

Figure 1. Sample HTML Layout



Log session start time 1970-01-14 00:39:14,511

Time	Thread	Level	Category	Message
2005-09-01 06:01:52,695	1	ALL	MAIN	Initializing Starent EMS Server 5.0. ...
NDC: main				
2005-09-01 06:01:52,705	1	DEBUG	MAIN	Running mode of EMS : BOTH
NDC: main				
2005-09-01 06:01:52,711	1	DEBUG	DB	Entering in DBData::initialize...
NDC: main DBData::initialize				

TTCC Layout

This layout consists of Time, Thread, Category, and nested diagnostic Context information. Each of these items can be individually enabled or disabled. The time format depends on the *DatePattern* used.

Caution: Do not use the same TTCC Layout instance from within different appenders. The TTCC Layout may not handle event threads properly when used in this way.

Use the following parameter configuration to use the TTCC Layout:

```
<layout class="TTCCLayout"/>

   <param name="DatePattern" value="date_format"/>

</layout>
```

The variables identified in the format above are described in the following table.

Table 16. TTCC Layout Variable Descriptions

Variable	Description

Variable	Description
date_format	Specifies the date format. The following time and date options are supported: • %a -- Abbreviated weekday name • %A -- Full weekday name • %b -- Abbreviated month name • %B -- Full month name • %c -- Standard date and time string • %d -- Day of month as a decimal(1-31) • %H -- Hour(0-23) • %I -- Hour(1-12) • %j -- Day of year as a decimal(1-366) • %m -- Month as decimal(1-12) • %M -- Minute as decimal(00-59) • %p -- Locale's equivalent of AM or PM • %Q -- Millisecond as decimal (000-999) • %S -- Second as decimal(00-59) • %U -- Week of year, Sunday being first day(0-53) • %w -- Weekday as a decimal(0-6, Sunday being 0) • %W -- Week of year, Monday being first day(0-53) • %x -- Standard date string • %X -- Standard time string • %y -- Year in decimal without century(0-99) • %Y -- Year including century as decimal • %Z -- Time zone name • %% -- The percent sign

An example of this layout's output is shown below.

```
176 [main] INFO examples.Sort - Populating an array of 2 elements in reverse
order.

225 [main] INFO examples.SortAlgo - Entered the sort method.
```

Simple Layout

This layout displays the event severity level and the event description.

Use the following parameter configuration to use the Simple Layout:

```
<layout class="SimpleLayout"/>
```

An example of this layout's output is shown below.

```
INFO - Populating an array of 2 elements in reverse order.

INFO - Entered the sort method.
```

Pattern Layout

This layout allows the specification of an output format through the configuration of a pattern string. It formats the log event and returns it as a string.

Use the following parameter configurations to use the Pattern Layout:

```
<layout class="org.apache.log4j.PatternLayout"/>

   <param name="ConversionPattern" value="pattern"/>

</layout>
```

pattern specifies the conversion characters used to format the output. The following table provides information on supported conversion characters.

Table 17. Pattern Layout Supported Conversion Characters

Character	Description
c	Used to output the logger of the logging event. The logger conversion specifier can be optionally followed by precision specifier, that is a decimal constant in brackets. If a precision specifier is given, then only the corresponding number of right most components of the logger name will be printed. By default the logger name is printed in full. For example, for the logger name "a.b.c" the pattern %c{2} will output "b.c".

Character	Description
d	Used to output the date of the logging event. The date conversion specifier may be followed by a date format specifier enclosed between braces. For example, %d{%H:%M:%S} or %d{%d %b %Y %H:%M:%S}. If no date format specifier is given then ISO8601 format is assumed.The following format options are possible: • %a -- Abbreviated weekday name • %A -- Full weekday name • %b -- Abbreviated month name • %B -- Full month name • %c -- Standard date and time string • %d -- Day of month as a decimal(1-31) • %H -- Hour(0-23)%I -- Hour(1-12) • %j -- Day of year as a decimal(1-366) • %m -- Month as decimal(1-12) • %M -- Minute as decimal(00-59) • %p -- Locale's equivalent of AM or PM • %Q -- Millisecond as decimal (000-999) • %S -- Second as decimal(00-59) • %U -- Week of year, Sunday being first day(0-53) • %w -- Weekday as a decimal(0-6, Sunday being 0) • %W -- Week of year, Monday being first day(0-53) • %x -- Standard date string • %X -- Standard time string • %y -- Year in decimal without century(0-99) • %Y -- Year including century as decimal • %Z -- Time zone name • %% -- The percent sign You can also use the enhanced logging function's predefined date formatters. These can be specified using one of the following strings: • **ABSOLUTE :** AbsoluteTimeDateFormat • **DATE :** DateTimeDateFormat • **ISO8601 :** ISO8601DateFormat For example, %d{ISO8601} or %d{ABSOLUTE}.

Character	Description
F	Used to output the file name where the logging request was issued. ***Important:*** Generating caller location information is extremely slow. It's use should be avoided unless execution speed is not an issue.
l	Used to output location information of the caller which generated the logging event. ***Important:*** Though location information can be very useful, it's generation is extremely slow. It's use should be avoided unless execution speed is not an issue.
L	Used to output the line number from where the logging request was issued. ***Important:*** Generating line number information is extremely slow. It's use should be avoided unless execution speed is not an issue.
m	Used to output the application supplied message associated with the logging event.
n	Outputs the platform dependent line separator character or characters. This conversion character offers practically the same performance as using non-portable line separator strings such as "\n", or "\r\n". Thus, it is the preferred way of specifying a line separator.
p	Used to output the level (priority) of the logging event.
r	Used to output the number of milliseconds elapsed since the start of the application until the creation of the logging event.
t	Used to output the name of the thread that generated the logging event.
x	Used to output the NDC (nested diagnostic context) associated with the thread that generated the logging event.
%	The sequence %% outputs a single percent sign.

An example of this layout's output when the following conversion pattern was specified is shown below:

```
%d{%d:%b:%Y %H:%M:%S:%Q}%6p %3t [%-16x] %8m%n

25:Aug:2005 13:14:27:494 INFO 1 [main DBData::initialize] DB info initialized
```

Configuring Logger Settings

Loggers are configured for each of the WEM components described previously in this document. Additionally, for the WEM Server component which consists of multiple categories, loggers are configured for each of the categories.

Loggers are configured using the following format:

```
<logger name="name" additivity="add_option">
   <level value="severity"/>
   <appender-ref ref="appender_name"/>
</logger>
```

Table 18. Logger Variable Descriptions

Variable	Description
name	The name of the WEM component of category for which logging parameters are being configured.
add_option	Specifies whether or not the logger is to inherit the appenders defined within the root element of the configuration file. The following options are supported: • **true :** Use appender defined within root (default) • **false :** Do not use appender defined within root
severity	Specifies the severity level of events to log. The following severity levels are supported: • OFF, 0 • DEBUG, 1I • NFO, 2 • WARN, 3 • SEVERE, 4 • FATAL, 5 • All, 6
appender_name	The name of the appender to use for this logger. ***Important:*** This parameter is used if the *additivity* parameter is set to *false*.

Configuring Log Message Filters

Log messages can be filtered based on the following criteria:

- Level match
- Level range
- String match
- Deny filter

Detailed information for each of the above classes is provided in the sections that follow.

Level Match Filters

This filter displays or rejects logs for events that match the specified severity level.

Level Match filters are configured using the following format:

```
<filter class="LevelMatchFilter">
   <param name="LevelToMatch" value="severity" />
   <param name="AcceptOnMatch" value="accept_option"/>
</filter>
```

Table 19. Level Match Filter Variable Descriptions

Variable	Description
severity	Specifies the severity level of events to filter. The following severity levels are supported: • OFF, 0 • DEBUG, 1 • INFO, 2 • WARN, 3 • SEVERE, 4 • FATAL, 5 • All, 6
accept_option	Specifies whether or not the logger is to accept logs that match the specified severity. The following options are supported: • **true :** Logs matching the severity are accepted • **false :** Logs matching the severity are not accepted

Level Range Filters

This filter displays or rejects logs for events that fall within the specified minimum and maximum severity levels.

Level Range filters are configured using the following format:

```
<filter class="LevelRangeFilter">
   <param name="LevelMax" value="max_sev"/>
   <param name="LevelMin" value="min_sev"/>
   <param name="AcceptOnMatch" value="accept_option"/>
</filter>
```

Table 20. Level Range Filter Variable Descriptions

Variable	Description
max_sev	Specifies the maximum severity level for the range of events to filter. The following severity levels are supported: • OFF, 0 • DEBUG, 1 • INFO, 2 • WARN, 3 • SEVERE, 4 • FATAL, 5 • All, 6
min_sev	Specifies the minimum severity level for the range of events to filter. The following severity levels are supported: • OFF, 0 • DEBUG, 1 • INFO, 2 • WARN, 3 • SEVERE, 4 • FATAL, 5 • All, 6
accept_option	Specifies whether or not the logger is to accept logs that fall within the specified severity range. The following options are supported: • **true :** Logs matching the criteria are accepted • **false :** Logs not matching the criteria are not accepted

String Match Filters

This filter displays or rejects logs for events based on whether or not any part of the event message matches the specified string.

String Match filters are configured using the following format:

```
<filter class="StringMatchFilter">
   <param name="StringToMatch" value="string" />
   <param name="AcceptOnMatch" value="accept_option"/>
</filter>
```

Table 21. String Match Filter Variable Descriptions

Variable	Description
string	Specifies the text string upon which to filter the log.
accept_option	Specifies whether or not the logger is to accept logs that match the specified severity. The following options are supported: • **true :** Logs matching the criteria are accepted • **false :** Logs not matching the criteria are not accepted

Deny Filters

This filter denies all log messages regardless of severity.

Deny filters are configured using the following format:

```
<filter class="DenyAllFilter">
```

This can be used in conjunction with other log message filters that display logs based on the specified criteria. For example, the following configuration displays Warning-level logs and denies all others:

```
<filter class="LevelMatchFilter">
   <param name="LevelToMatch" value="WARN" />
   <param name="AcceptOnMatch" value="true"/>
</filter>
<filter class="DenyAllFilter">
```

Configuring Support for Dynamic Logging Updates

A key benefit of the WEM's logging functionality is the ability to dynamically incorporate changes made to the logging configuration without restarting server processes.

The WEM periodically checks the XML configuration files for changes. If the changes are found, they are automatically applied.

Each XML configuration file contains a parameter called delay value that is used to specify the frequency with which the server looks for changes. This parameter is defined under the root element as shown below:

```
<root>
 <priority value="WARN"/>
 <!-- A delay used by the Watchdog thread to continuously read/check
 the modified configuration applies to EMS Logger-->
<delay value="3000"/>
 <appender-ref ref="Main"/>
</root>
```

The delay is measured in milliseconds (ms). The default value is 3000 ms.

Chapter 7
WEM Database Maintenance

The following table lists the PostgreSQL databases that can be created during the installation of the WEM application. Certain databases are only created if their respective functionality is enabled in the application. Refer to the Determining Available Databases section of this chapter for information on determining which databases have been created.

Table 22. Databases Created by the WEM

Database Name	Description
trapdb	Contains tables pertaining to traps and alarms generated by managed systems.
configdb	Contains tables pertaining to the system and WEM configuration.
mibdb	Contains tables pertaining to SNMP management information base (MIB) objects from managed systems.
templateX	Default PostgreSQL database template(s). X represents the numeric instance of the template.
auditdb	Contains tables pertaining to WEM audit trail information.
bsdb	Contains tables pertaining to bulk statistics generated by managed systems.
p2pdb	Contains tables pertaining to P2P statistics generated by managed systems.

This chapter provides information and instructions for performing the following routine maintenance on these databases to ensure proper data processing and integrity:

- Vacuuming the Databases
- Backing-up WEM Databases

> ***Caution:*** To ensure proper operation and data integrity, the PostgreSQL database instances installed with the WEM should only be used by the application.

This chapter includes the following topics:

> ***Important:*** Unless otherwise specified, all information in this chapter applies to both Sun Solaris- and Red Hat Enterprise Linux-based WEM systems.

Determining Available Databases

Follow the instructions in this section to determine which databases were created during the installation of the WEM application. These instructions assume that you are logged in to the server on which the application is installed as the user root and have access to the server's command line.

Step 1 Go to the "bin" sub-directory of the PostgreSQL installation directory (*/<ems_dir>/postgresx.x.x/* by default) by entering the following command:

```
cd /<ems_dir>/postgres/bin
```

Step 2 Enter the PostgreSQL interactive terminal for template1 database by entering the following command:

```
./psql -U postgres_name template1
```

postgres_name is the name of the PostgreSQL database administrator (postgres by default).

The following prompt appears:

```
template1#
```

Step 3 Display available databases by entering the following command:

```
select datid,datname from pg_stat_database;
```

A table appears listing the database name and its corresponding identification number.

Step 4 Exit the PostgreSQL interactive terminal by entering the following command:

```
\q
```

"Vacuuming" the Databases

Standard PostgreSQL operation periodically leaves older versions of records in the database even after the record has been updated or deleted. This method allows the record to remain available to other processes or transactions. As a result of frequent database deletes and/or updates, the number of these "old" records can grow and hinder database operation and performance. Excessive numbers of these "old" and unused records increase the time required for queries and consume disk space that could be better allocated for current records and processes. For these reasons, it is recommended that these "old" records be removed regularly.

The removal of these "old" records is done by "vacuuming" the database using the PostgreSQL **vacuumdb** command.

It is recommended that all WEM databases be "vacuumed" at least once a week. However, databases that undergo frequent record updates/deletions be vacuumed on a daily basis. Two such databases are the trap database (trapdb) and the bulk statistics database (bsdb).

Caution: Database vacuuming should only be performed at a time when there are minimal database transactions. Typically, this would correspond to a time frame in which no configurations are being performed, infrequent alarm updates, and/or infrequent bulk statistics transfers. Before vacuuming the database, the server must check for already running vacuuming. If this is already running, then the next scheduled vacuum process must be skipped. Hence, WEM must execute only one vacuum query at a time for every database.

Periodic, automatic database vacuuming can be performed through the configuration of a text file as described in the Configuring Automated Periodic Database Vacuuming section that follows. This is the preferred method. One-time automatic vacuuming can be performed through the use of the UNIX cron application as described in the Using Cron to Automate Database Vacuuming section. Vacuuming can also be performed manually as described in the Manually Vacuuming WEM Databases section.

Configuring Automated Periodic Database Vacuuming

The WEM application contains a configuration file called vacuum.cfg that contains parameters related to database vacuuming operation and frequency. The file is located in the */<ems_dir>/server/etc* directory by default.

The parameters provide the flexibility to vacuum either the database as whole or just various tables within the database. The values for these parameters can be modified using a text editor (such as Vi Editor) if required.

Each database and table is configured with a start time, and a frequency that specifies the number of hours that must pass prior to performing the vacuuming function again. For example, if vacuuming of the Configuration database is to start at 12:00 PM, and repeat after 24 hours, the parameter in the vacuum.cfg file would appear as follows:

```
ConfigDB = 12,24
```

Important: A value of 00,00 disables vacuuming for both databases and tables.

Note that the vacuuming of the MIB database is not supported because the content changes infrequently.

The following table provides a list of the parameters within the vacuum.cfg file.

Table 23. Database and Table Parameters in the vacuum.cfg File

Parameter	Description	Default Setting

Parameter	Description	Default Setting
Type		
Vacuum_Type	Specifies the type of vacuum to perform as one of the following: • **VACUUM ANALYZE:** Performs the vacuum function as described previously in this chapter but also collects statistics about the proportions of duplicate values within a column and the min/max value. • **VACUUM:** Performs only the vacuum function. • **VACUUM FULL:** Physically reorders the tables. This requires an exclusive lock on each table while it is being processed.	VACUUM ANALYZE
Database Name*		
ConfigDB	Sets vacuuming parameters for the Configuration database which contains tables pertaining to the system and WEM configuration.	00,00
TrapDB	Sets vacuuming parameters for the Trap database which contains tables pertaining to traps and alarms generated by managed systems.	00,00
AuditDB	Sets vacuuming parameters for the Audit Trail database which contains tables pertaining to WEM audit trail information.	00,00
BulkDB	Sets vacuuming parameters for the Bulk Statistics database which contains tables pertaining to bulk statistics generated by managed systems.	00,00
P2PDB	Sets vacuuming parameters for the P2P database which contains tables pertaining to protocol and threshold statistics generated by managed systems.	00,00
Table Name		
ConfigDB		
CompleteDB	This parameter dictates whether or not vacuuming will be performed on only the database or each table in the database individually. A value of 0 indicates that vacuuming is to be performed on each table. A value of 1 indicates that vacuuming is to be performed only on the database.	1
boxer	Sets vacuuming parameters for the table that contains configuration information pertaining to the system.	00,00
portmontable	Sets vacuuming parameters for the table that contains configuration information pertaining to port monitoring.	00,00
boxeruserinfo	Sets vacuuming parameters for the table that contains configuration information pertaining to administrative users configured on the system.	00,00
userpreference	Sets vacuuming parameters for the table that contains configuration information pertaining to preferences configured for WEM administrative users.	00,00
processthreshold	Sets vacuuming parameters for the table that contains configuration information pertaining to WEM process thresholds.	00,00
ippooldefaults	Sets vacuuming parameters for the table that contains configuration information pertaining to IP address pool default values.	00,00
scbrdefaults	Sets vacuuming parameters for the table that contains information about subscriber default parameters.	00,00

Parameter	Description	Default Setting
csmsessioninfo	Sets vacuuming parameters for the table that contains information on the session id between client and server, client IOR, login time, and address.	00,00
bkinfo	Sets vacuuming parameters for the table that contains information required for configbackup.	00,00
graphscreeninfo	Sets vacuuming parameters for the table that contains configuration information pertaining to graph displays.	00,00
batchjobcleanup	Sets vacuuming parameters for the table that contains information required for cleanup of batch jobs.	00,00
batchjobinfo	Sets vacuuming parameters for the table that contains information required for batch jobs.	00,00
boxeronmap	Sets vacuuming parameters for the table that contains configuration information pertaining to administrative user maps configured on the system.	00,00
dbbackupinfo	Sets vacuuming parameters for the table that contains configuration information pertaining to database backup.	00,00
maptable	Sets vacuuming parameters for the table that contains configuration information pertaining to the map table.	00,00
p2pinfo	Sets vacuuming parameters for the table that contains configuration information pertaining to P2P database.	00,00
updateinfo	Sets vacuuming parameters for the table that contains configuration information pertaining to updates.	00,00
userinfo	Sets vacuuming parameters for the table that contains configuration information pertaining to WEM administrative users.	00,00
dbcurrent	Sets vacuuming parameters for the table that contains configuration information pertaining to the current database.	00,00
hostname	Sets vacuuming parameters for the table that contains configuration information pertaining to host names.	00,00
syslog keyword list	Sets vacuuming parameters for the table that contains configuration information pertaining to the keyword log list configured on the system.	00,00
syslogmsgfileinfo	Sets vacuuming parameters for the table that contains configuration information pertaining to the message log list configured on the system.	00,00
cdpreportinfo	Sets vacuuming parameters for the table that contains configuration information pertaining to CDP reports.	00,00
filefetchinfo	Sets vacuuming parameters for the table that contains configuration information pertaining to fetching of files from the database.	00,00
ongoingsftpinfo	Sets vacuuming parameters for the table that contains configuration information pertaining to the ongoing SFTP.	00,00
TrapDB		
CompleteDB	This parameter dictates whether or not vacuuming will be performed on only the database or each table in the database individually. A value of 0 indicates that vacuuming is to be performed on each table. A value of 1 indicates that vacuuming is to be performed only on the database.	1

Parameter	Description	Default Setting
trap	Sets vacuuming parameters for the table that contains information pertaining to SNMP traps received.	00,00
deletedtrap	Sets vacuuming parameters for the table that contains information pertaining to deleted SNMP traps.	00,00
forwardinginfo	Sets vacuuming parameters for the table that stores the information for forwarding the received SNMP traps in real time.	00,00
forwardpurgeinfo	Sets vacuuming parameters for the table that is used to get information about whether or not to purge the forwarded trap.	00,00
mailinfo	Sets vacuuming parameters for the table that stores trap e-mail address, e-mail type (TO, CC, or BCC), trap type and trap specific number.	00,00
mailmessage	Sets vacuuming parameters for the table that stores trap e-mail subject, trap message, trap type and trap specific number.	00,00
configure	Sets vacuuming parameters for the table that contains information pertaining to SNMP trap configuration.	00,00
schedule	Sets vacuuming parameters for the table that stores the trap severity, Audio start time, audio stop time.	00,00
forwardaddress	Sets vacuuming parameters for the table that contains information pertaining to the forward address.	00,00
pendingtrap	Sets vacuuming parameters for the table that contains information pertaining to the pending SNMP traps.	00,00
trap_current	Sets vacuuming parameters for the table that contains information pertaining to the current SNMP trap.	00,00
trapoperdetails	Sets vacuuming parameters for the table that contains information pertaining to trap operation.	00,00
AuditDB		
CompleteDB	This parameter dictates whether or not vacuuming will be performed on only the database or each table in the database individually. A value of 0 indicates that vacuuming is to be performed on each table. A value of 1 indicates that vacuuming is to be performed only on the database.	1
auditlog	Sets vacuuming parameters for the table that contains information pertaining to the WEM's Audit Trail function.	00,00
chassisinfo	Sets vacuuming parameters for the table that contains information pertaining to the chassis.	00,00
cpuinfo	Sets vacuuming parameters for the table that contains information pertaining to the CPU.	00,00
daughtercardinfo	Sets vacuuming parameters for the table that contains information pertaining to the daughter card.	00,00
hardwareactivity	Sets vacuuming parameters for the table that contains information pertaining to the hardware activity.	00,00
hardwareinfo	Sets vacuuming parameters for the table that contains information pertaining to the hardware.	00,00

Parameter	Description	Default Setting
lcrccspioinfo	Sets vacuuming parameters for the table that contains information pertaining to Line Cards (LC), Redundant Crossbar Cards (RCC), and Switch Processor Input/Output (SPIO) cards.	00,00
pactacinfo	Sets vacuuming parameters for the table that contains information pertaining to the Packet Accelerator Card (PAC) and Telephony Accelerator Card (TAC).	00,00
smcinfo	Sets vacuuming parameters for the table that contains information pertaining to the System Management Card (SMC).	00,00
spccardinfo	Sets vacuuming parameters for the table that contains information pertaining to the Switch Processor Card (SPC).	00,00
imglastevtgentime	Sets vacuuming parameters for the table that contains information pertaining to the last event generation time of the system.	00,00
BulkDB		
CompleteDB	This parameter dictates whether or not vacuuming will be performed on only the database or each table in the database individually. A value of 0 indicates that vacuuming is to be performed on each table. A value of 1 indicates that vacuuming is to be performed only on the database.	1
card	Sets vacuuming parameters for the table that contains information pertaining to the card-level schema.	00,00
port	Sets vacuuming parameters for the table that contains information pertaining to the port-level schema.	00,00
system	Sets vacuuming parameters for the table that contains information pertaining to the system-level schema.	00,00
ggsnsystem	Sets vacuuming parameters for the table that contains information pertaining to the system-level schema for GGSN-based systems.	00,00
ppp	Sets vacuuming parameters for the table that contains information pertaining to the PPP-level schema.	00,00
mipfa	Sets vacuuming parameters for the table that contains information pertaining to the Mobile IP FA-level schema.	00,00
mipha	Sets vacuuming parameters for the table that contains information pertaining to the Mobile IP HA-level schema.	00,00
rp	Sets vacuuming parameters for the table that contains information pertaining to the PDSN-level schema.	00,00
gtpc	Sets vacuuming parameters for the table that contains information pertaining to the GGSN-level schema.	00,00
gtpp	Sets vacuuming parameters for the table that contains information pertaining to the GTPP-level schema.	00,00
ippool	Sets vacuuming parameters for the table that contains information pertaining to the IP Address Pool-level schema.	00,00
apn	Sets vacuuming parameters for the table that contains information pertaining to the APN-level schema.	00,00

Parameter	Description	Default Setting
lac	Sets vacuuming parameters for the table that contains information pertaining to the LAC-level schema.	00,00
radius	Sets vacuuming parameters for the table that contains information pertaining to the RADIUS-level schema.	00,00
imgaccess	Sets vacuuming parameters for the table that contains information on the XML files generated by the Bulk Statistics Server.	00,00
ecs	Sets vacuuming parameters for the table that contains information pertaining to the ECS-level schema.	00,00
misc	Sets vacuuming parameters for the table that contains information pertaining to the miscellaneous schema.	00,00
ipsg	Sets vacuuming parameters for the table that contains information pertaining to the IPSG-level schema.	00,00
asngw	Sets vacuuming parameters for the table that contains information pertaining to the ASNGW-level schema.	00,00
sgsn	Sets vacuuming parameters for the table that contains information pertaining to the SGSN-level schema.	00,00
sgtp	Sets vacuuming parameters for the table that contains information pertaining to the SGTP-level schema.	00,00
sccp	Sets vacuuming parameters for the table that contains information pertaining to the SCCP-level schema.	00,00
ss7rd	Sets vacuuming parameters for the table that contains information pertaining to the SS7RD-level schema.	00,00
mipv6ha	Sets vacuuming parameters for the table that contains information pertaining to the MIPv6 HA-level schema.	00,00
context	Sets vacuuming parameters for the table that contains information pertaining to the context-level schema.	00,00
cscf	Sets vacuuming parameters for the table that contains information pertaining to the CSCF-level schema.	00,00
ss7link	Sets vacuuming parameters for the table that contains information pertaining to the SS7 Link-level schema.	00,00
gprs	Sets vacuuming parameters for the table that contains information pertaining to the GPRS-level schema.	00,00
pdif	Sets vacuuming parameters for the table that contains information pertaining to the PDIF-level schema.	00,00
schemastatus	Sets vacuuming parameters for the table that contains information pertaining to the schema status.	00,00
P2PDB		

Parameter	Description	Default Setting
CompleteDB	This parameter dictates whether or not vacuuming will be performed on only the database or each table in the database individually. A value of 0 indicates that vacuuming is to be performed on each table. A value of 1 indicates that vacuuming is to be performed only on the database.	1
bwstat	Sets vacuuming parameters for the table that contains information pertaining to data traffic bandwidth statistics.	00,00
dailystat	Sets vacuuming parameters for the table that contains information pertaining to daily statistics.	00,00
hourlystat	Sets vacuuming parameters for the table that contains information pertaining to hourly statistics.	00,00
protocolstat	Sets vacuuming parameters for the table that contains information pertaining to protocol statistics.	00,00
scbrdailystats	Sets vacuuming parameters for the table that contains information pertaining to subscriber daily statistics.	00,00
scbrhourlystats	Sets vacuuming parameters for the table that contains information pertaining to subscriber hourly statistics.	00,00
scbrstats	Sets vacuuming parameters for the table that contains information pertaining to subscriber statistics.	00,00
tempp2p	Sets vacuuming parameters for the table that contains information pertaining to P2P statistics.	00,00
thresholdstats	Sets vacuuming parameters for the table that contains information pertaining to threshold statistics.	00,00
* Any non-zero number specified for a database in the Database Name section supersedes the CompleteDB parameter setting for the database. For example, if the start value for the Configuration database is 13 and the databases corresponding CompleteDB parameter is set to 0, then vacuuming is to be done for the entire database and all of the tables. However, if there is a conflict between the start times specified for any of the tables within the database and that specified for the database itself, vacuuming will not be started for that table.		

Using Cron to Automate Database Vacuuming

As mentioned previously, the UNIX cron application can be used to automate database vacuuming. It is a daemon that is capable of executing commands or scripts at regular time intervals. Additional information on cron is available through its manual pages or on the Internet.

To use cron to automate the vacuum process, add an entry to a crontab on the server on which the WEM is installed. The entry specifies the time and database to be vacuumed. For example, if you wanted to vacuum the bulk statistics database (bsdb) every day at 3:00 AM, you might add the following entry in the crontab:

```
00 03 * * * /<ems_dir>/postgresx.x.x/bin/vacuumdb -U postgres -d bsdb > /dev/null
2>&1
```

From the above example, you can see that the **vacuumdb** command is located in the bin sub-directory of the PostgreSQL installation directory (*/<ems_dir>/postgresx.x.x* by default). The -U parameter indicates the PostgreSQL database administrator name (postgres by default).

Manually Vacuuming WEM Databases

Follow the instructions in this section to manually vacuum databases used by the WEM application. These instructions assume that you are logged in to the server on which the application is installed as the user root and have access to the server's command line.

Step 1 Ensure that the database(s) are backed-up prior to vacuuming. Refer to the Backing-up WEM Databases section of this chapter for information on performing a database backup.

Step 2 Go to the "bin" sub-directory of the Postgres installation directory (*/<ems_dir>/postgresx.x.x/* by default) by entering the following command:

```
cd /<ems_dir>/postgres/bin
```

Step 3 Vacuum the desired database by entering the following command:

```
/vacuumdb -U postgres_name -d db_name &
```

Command/Keyword	Description
postgres_name	The name of the PostgreSQL database administrator (postgres by default).
db_name	The name of the database to be vacuumed. Refer to the Determining Available Databases section of this chapter for information on determining which databases are available.

Step 4 Repeat Step 3 to vacuum additional databases.

```
select datid,datname from pg_stat_database;
```

Backing-up WEM Databases

To minimize the risk of data loss, WEM databases should be backed up on a regular basis. It is recommended that databases be backed up at least once a week. However, depending on the environment and frequency of record updates and/or deletions, you may choose to backup the data more often.

Caution: Database backups should only be performed at a time when there are minimal database transactions. Typically, this would correspond to a time frame in which no configurations are being performed, alarm updates are infrequent, and/or infrequent bulk statistics transfers are occurring.

The database backup creates compressed (.gz) files that are saved to the <*emsdir*>/server/flash/backup_<*periodicity*>_<*date+time*>/ems_backup directory. For example: /ems/server/flash/backup_DAILY_20110419153530/ems_backup.These files contains records from the various tables available in the databases. In the event of data corruption or loss, these files can be used to restore the information by using the restoreDb.sh script in the <*ems dir*>/server/scripts directory.

To backup WEM application databases:

Step 1 Log in to the WEM application.

Step 2 On the WEM menu bar, click **Configuration**.

Step 3 Click **System**.

Step 4 Click **WEM Database Periodic Backup**.

The *WEM Database Periodic Backup Configuration Dialog Box* appears.

Step 5 Make the desired *Backup Date*, *Recurrence Pattern* and *Range of Recurrence* entries for WEM database backups. For details on the required entries, click **Help**.

Step 6 Once you have made the required backup configuration entries, click **Apply** to activate your settings.

WEM saves the database backup to the <*emsdir*>/server/flash/backup_<*periodicity*>_<*date+time*>/ems_backup directory.

Backup Script Error Codes

This script returns error codes for any problems encountered during the backup operation, if any. These codes can assist the WEM client user to take appropriate correction.

Following are the supported error codes along with their description:

Table 24. Error Codes Returned During WEM Database Backup Operation

Error Code	Error Name	Description
0	SUCCESS	Successful
1	INVALID_ARGUMENT	Invalid argument
2	REQUIRES_SUPERUSER	This script requires superuser privileges

Error Code	Error Name	Description
3	INVALID_POSTGRES_DIRECTORY	Invalid postgres directory
4	BACKUP_FILE_NOT_EXIST	Specified backup file does not exist
5	BACKUP_FAILED_WITH_ERROR	Backup failed
6	BACKUP_FILE_CREATION_FAILED	Backup file creation failed
7	DATABASE_RESTORE_FAILED	Database restore operation failed
8	POSTGRES_NOT_RUNNING	Postgres process is not running
9	SERV_SCRIPT_NOT_EXIST	<ems_server>/serv script is not present

Restoring the WEM Database

This option is also used with the backup script **backup.sh**. It restores the WEM databases. No extra parameters are required for restoring the database other than the 'restore' keyword. The script itself will prompt for more parameters such as postgres directory path, backup file location, etc.

To restore the WEM database, enter the following command:

```
./backup.sh restore
```

Caution: Use the functionality of the *WEM Database Periodic Backup Dialog Box* in the WEM client application to perform a WEM database backup. The**back.sh** script is used by the WEM periodic backup functionality to backup the WEM database. Refer to the *Backing Up WEM Databases* section in this chapter.

Chapter 8
Preparing and Using the Client Workstation

This chapter provides information on the required files and environment for the WEM client and server machines. It also provides information on the WEM user interface.

This chapter includes the following topics:

Important: Unless otherwise specified, all information in this chapter applies to both Sun Solaris and Red Hat Enterprise Linux-based WEM systems.

Unsecured and Secured Java Policy Files

Instructions on how to download the Java Policy file from the WEM server are displayed when you click the Java Policy File link, located towards the right of the client application's WEM browser display. There are two options: Secured and Unsecured.

- Unsecure Policy Files. These allow the Java applet infinite permissions to access the desktop's file system which includes permission to modify or delete files.
- Secure Policy Files. These allow only a WEM server specified by a secure IP address to have complete access to the desktop's file system.

  The **.java.policy** file is created on the WEM server and downloaded along with the applet.

In each case the entire grant statement has to be replaced before the file is inserted into the correct directory (see Placement of Required Client Files for more information).

- For unsecured connections replace the following grant clause with an IP address using unsecured http:

```
grant codebase "http://X.X.X.X/-"{ permission java.awt.AWTPermission
"accessClipboard"; permission java.lang.RuntimePermission "exitVM";
permission java.lang.RuntimePermission
"accessClassInPackage.sun.security.action"; permission
java.lang.RuntimePermission "shutdownHooks"; permission
java.awt.AWTPermission "showWindowWithoutWarningBanner"; permission
java.lang.RuntimePermission "modifyThread"; permission
java.util.PropertyPermission "*", "read, write"; permission
java.io.FilePermission "<<ALL FILES>>", "read, write, execute"; permission
java.net.SocketPermission "*", "accept, connect, listen, resolve";
permission java.lang.RuntimePermission "queuePrintJob"; permission
java.lang.reflect.ReflectPermission "suppressAccessChecks";};
```

- For secured connections replace the following grant clause with an IP address using secured http:

```
grant codebase "https://X.X.X.X/-"{ permission java.awt.AWTPermission
"accessClipboard"; permission java.lang.RuntimePermission "exitVM";
permission java.lang.RuntimePermission
"accessClassInPackage.sun.security.action"; permission
java.lang.RuntimePermission "shutdownHooks"; permission
java.awt.AWTPermission "showWindowWithoutWarningBanner"; permission
java.lang.RuntimePermission "modifyThread"; permission
java.util.PropertyPermission "*", "read, write"; permission
java.io.FilePermission "<<ALL FILES>>", "read, write, execute"; permission
java.net.SocketPermission "*", "accept, connect, listen, resolve";
permission java.lang.RuntimePermission "queuePrintJob"; permission
java.lang.reflect.ReflectPermission "suppressAccessChecks";};
```

Important: If a single desktop is used to manage multiple WEM servers, there can only be one **.java.policy** file on the desktop. This means the user needs to add a **complete** grant clause with the server's IP address for each server under management.

Placement of Required Client Files

There are two files that are required to enable client access to the WEM from the client workstation. These files are:

- **Java® Runtime Environment (JRE)** - This program must be installed on the client workstation. Versions 1.5, and 1.6 are supported.
- **Java Policy File** - This file may be obtained from the WEM server when you first access the system using the client workstation. For proper authentication, this policy file must be located in an exact location, dependent upon the operating system being used on the client workstation.
    - For the Microsoft® Windows™ NT 4.0 operating system, the **.java.policy** file must be placed in the *<drive_letter>\Profiles\<user_name>* directory.
    - For the Microsoft® Windows™ 2000 and Windows™ XP operating systems, the **.java.policy** file must be placed in the *<drive_letter>\Documents and Settings\<user_name>* directory.
    - For the Microsoft® Windows™ 7 operating system, the **.java.policy** file must be placed in the *<drive_letter>\users\<user_name>* directory.
    - For the Sun® Solaris® (UNIX) and Linux® operating systems, the **.java.policy** file must be placed in the user's home directory.
- Instructions on how to download the Java Policy file from the WEM server are displayed when you click the **Java Policy File** link, located towards the right of the client application's WEM browser display.

Accessing the WEM as a Client on the Web Element Manager Server

In some cases, users may want to access the WEM application using the WEM server as the client. For versions of Netscape earlier than 6.0 (i.e. 4.5), system environment variables must be configured to support this functionality. This section provides instructions for configuring these variables using either the C, Bourne, Korn, and Bourne-again shells.

Environment Settings for CSH

Step 1 Set the following environment variables in your .cshrc file:

```
setenv NPX_PLUGIN_PATH /<java_installation_directory>/jre/plugin/sparc/ns4

setenv NPX_JRE_PATH /<java_installation_directory>

setenv THREADS_FLAG native
```

<java_installation_directory> is the directory in which java is installed (i.e. */usr/java*).

Step 2 Source the *.cshrc* file (or open a new shell) and start the Netscape browser.

Environment Settings for SH, KSH, and BASH

Step 1 Set the following environment variables in your *.profile* file:

```
NPX_PLUGIN_PATH=/<java_installation_directory>/jre/plugin/sparc/ns4

export NPX_PLUGIN_PATH

NPX_JRE_PATH=/<java_installation_directory>

export NPX_JRE_PATH

export THREADS_FLAG native
```

<java_installation_directory> is the directory in which java is installed (i.e. */usr/java*).

Step 2 If these variables are set in a shell, then invoke Netscape from the same shell (e.g. */usr/dt/appconfig/netscape/netscape*).

Accessing the WEM using a Client Workstation

Using an Internet web browser, enter the following command in the address field.

```
http://<Web_Element_Manager_server_IP_address>/ems/img.html
```

The <*Web_Element_Manager_server_IP_address*> variable is the IP address of the WEM server entered in dotted-decimal notation.

Assuming that the Java Policy file and Java Runtime Environment (JRE) files have been loaded in their proper locations, the WEM server will push various .jar files to the client machine and then display the WEM Logon window.

Important: After an upgrade or installing a new version of WEM, it is recommended that the browser cache of the client workstation should be cleared, if it is enabled. To clear the cache in Internet Explorer, click **Tools** menu -> **Internet Options**. Under the **General** tab, click **Delete Files**, click the **Delete all offline content** check box, and then click **OK**.

Logging in to the WEM

To log on to the server for the first time, use the default username of superuser and a password of superuser, which are case sensitive. Once you are successfully logged in, additional user accounts can be configured through the **Security** pull-down menu.

Use of the Superuser Account

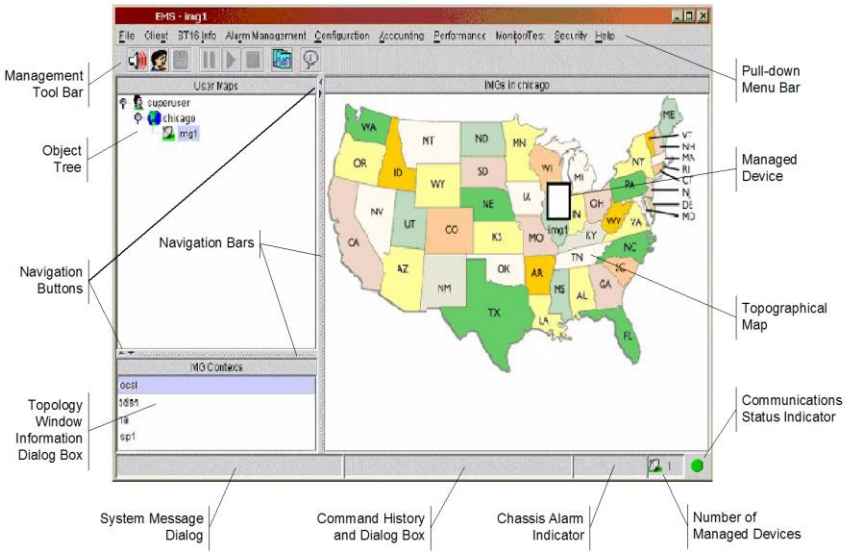
The *superuser* account is the default administrative account on the WEM. This account works similar to the root account on a UNIX machine. A *superuser* administrator would have to create accounts for the individual users in the WEM - like a UNIX machine root user does. The user accounts would then be given to the non-superuser users. The *superuser* password should be kept private to limit access.

Important: The first time you log into the superuser account, you will be prompted to change your password. See *ANSI T1.276 Compliance* in the *Web Element Manager Overview* for more information about password usage.

User Interface

Upon first logging in to the WEM, a dialog appears that functions as the starting point for all FCAPS operations. This dialog is referred to as the Topology Window and is shown in the following figure. It is important to note that during login, the administrative user has the ability to select the desired language used in the Topology Window. U.S. English and Korean are currently supported.

Figure 2. The Web Element Manager Topology Window



From the Topology Window, the systems to be managed can be specified and added to Topographical Maps. Once specified, managed devices can be selected from either the Object Tree or the Topographical Map to provide real-time status information for the system.

System hardware descriptions and state information can be displayed by double-clicking on a managed device. This provides front and rear views of the chassis. Simply hovering the mouse pointer over an interface or an LED displays its status.

Management Toolbar

The Management Toolbar, which can be enabled or disabled from the **View** menu, provides shortcuts to access various functions available via the Pull-down Menu. Shortcuts include:

Table 25. WEM Toolbar Icon Descriptions

Icon	Icon Function	Description

Icon	Icon Function	Description
	Fault Management	Clicking this icon opens the Current Event Log for the selected managed device.
	Web Element Manager User Administration	Clicking this icon enables the User Administration function, located under the Security pull-down menu. This function is used to configure and manage users of the WEM application.
	Save Web Element Manager Configuration	Clicking this icons saves all WEM configuration information, such as Topology Map changes, Object Tree edits, etc. ***Important:*** This operation only saves WEM application configuration items. It does not save any configuration text file operations that are made on a selected system.
	Pause Audio Alarm	Clicking this icon temporarily pauses any audible indications that are generated through the system's internal speaker when a pre-configured fault/trap is received by the WEM server. ***Important:*** This icon is only available when audio alarms are enabled through the **Alarm Management** pull-down menu.
	Resume Audio Alarm	Clicking this icon, available only when audio alarm processing has been paused (see above), will cause the system to once again begin generating audible alarm indications. ***Important:*** This icon is only available when audio alarms are enabled through the **Alarm Management** pull-down menu.
	Stop Audio Alarm	Clicking this icon disables the audible alarm function. ***Important:*** The audible alarm function described here has no effect on audible alarms generated by the chassis itself, through its SMC and SPIO cards. This function is only applicable to the WEM client; and is configurable on a per chassis basis.
	Performance Statistics	Clicking this icon moves user to Performance Statistics graphing tool window for bulk statistics. From this window, users can select various cards or protocols to monitor, configure the statistics to graph, and type of graph to display collected information in, based on historical information collected through Bulk Statistics collection.

Icon	Icon Function	Description
	About Information	Clicking this icon displays uses information related to the WEM application. This includes version number, software build dates, and other important information that may be required when requesting support on this application.

Pull-Down Menu Bar

The pull-down menu bar provides menu-driven user access to all available management operations. These include both WEM application management and configuration operations.

Menu options available to users can be hidden and unhidden at will by setting a flag in the *menu.xml* file. Setting the flag appropriately is described in the *WEM Configuration File Parameters* appendix.

This section provides a brief description for each menu.

File Pull-Down Menu

The **File** pull-down menu option allows users to either log out of a current session, save any configuration changes, or exit the WEM application completely.

Client Pull-Down Menu

The **Client** pull-down allows users to control and customize how the management application and selected devices are viewed on their browser-based client. These settings are configured on a per-user basis. Additionally, this menu provides options for launching other tools that can be used for management purposes such as Telnet and/or Secure Shell (SSH) clients and Management Information Base (MIB) browsers.

System Info Pull-Down Menu

The **System Info** pull-down menu allows you to view system-level information for devices selected in the topology window. From this menu, you also can perform some configuration and system administration operations.

Alarm Management Pull-Down Menu

The **Alarm Management** pull-down menu allows users to manage current, pending, and outstanding events as well as view statistics for alarms. This menu also provides controls for configuring the system Central Office (CO) alarm indicators and audio indicators.

Configuration Pull-Down Menu

The **Configuration** pull-down menu allows administrators to perform various configuration options upon a selected system. This includes system-level parameters such as those for hardware as well as all context-level parameters such as services, interfaces, and protocols. Also included in this menu are the options for specifying the systems to be managed by the WEM.

Performance Pull-Down Menu

The **Performance** pull-down menu allows users to view, configure, modify, collect, and view real-time statistical information for a selected device.

Monitor/Test Pull-Down Menu

The **Monitor/Test** menu offers selections that enable the user to view and configure parameters to monitor and test selected functions such as:

- **EMS Process Monitoring**: This option allows you to view system and disk usage, and interface information about the WEM server application. You can also configure various threshold settings that will create an alarm when the system exceeds your configured thresholds.
- **Monitor Protocol**: This option enables a powerful monitoring tool that can be configured to collect and display specific protocol information for calls coming into or out of the selected system. This powerful tool can be used to help troubleshoot session or connectivity problems.
- **Monitor Subscriber**: This option provides the same powerful monitoring options as explained above, but can be used for a specific subscriber.
- **Port Monitoring** This option allows the users to view, enable/disable the process, and configure the parameter thresholds and intervals for line cards and ports.

The **Test** option allows users to perform tests such as RADIUS server connectivity, PPP echo tests, or AAA packet transmit and receive.

Security Pull-Down Menu

The **Security** pull-down menu provides administrative users with user management functions such as adding and deleting administrative users, monitoring user sessions, and viewing audit trail information.

Help Pull-Down Menu

General help is accessed through the **Help** pull-down menu, located at the top of the menu bar. Click **Contents** to access the main Help screen. It is important to note that context-sensitive help is available for each dialog that possesses a **Help** button. More information on using the online help is available in the *Obtaining Help within the WEM* section later in this chapter.

Object Tree

The object tree presents a hierarchical view of all managed devices, and groups of devices, available to a particular user. This view is based on specifically configured user access rights and may only show a subset of the overall managed network. Management domains identify a group of managed network elements with devices being added to or removed from the object tree by using the **Map** function.

The Object Tree is navigated much like folders and sub-folders are when using the familiar Microsoft® Windows Explorer™ application. WEM users can view either users or management domains from the Object Tree.

Navigation Buttons and Navigation Bars

Navigation buttons and bars are used to change the way that the Topology window is displayed.

Topology Window Information Dialog Box

This portion of the Topology Window provides information about what is being displayed on the Topology Window. The information displayed here will depend on what the administrative user has selected from either the Object Tree or the Topographical Map.

If an administrative user has selected (highlighted) the user information section of the Object Tree, they will view all users logged into the WEM application. If a user has selected a management domain from the Object Tree, they will view information about all devices contained under that domain.

If a user has selected a specific device underneath a management domain, they will view information about the configured contexts within that device. When viewing a domain, users can highlight specific contexts and select them to be the default view for other element management operations.

Topographical Map

The Topology Map provides visual view of all managed devices, and groups of devices, available to a particular user. This view is based on specifically configured user access rights and may only show a subset of the overall managed network.

New topology maps can be added by using the Add function, available from the **Map** pull-down menu. Network devices can be added to an existing topographical map by using the Modify function, available from the **Map** pull-down menu.

Managed network devices are visually represented by device icons that display its manageable state. Device icons with a blue-colored “X” through them denote that the device is reachable, meaning that an administrative user can view the device, but cannot perform any management operations. Device icons with a red-colored “X” through them denote that the device is unreachable, meaning that an administrative user cannot view the device or perform any management operations. Other options can be viewed by right-clicking on the device icon.

System Message Dialog

This area provides system messages from the WEM application to the user. These messages notify the user as to what the application is currently doing. For example, when a user selects a new device from the Topographical Map or Object Tree, the system sends a message to the user that it is attempting to *“Attempting to Fetch Contexts”* for the selected device.

Command History and Dialog Box

This dialog screen area provides a history of command dialog messages for the current session. These messages are received from the managed device upon completion of command execution. This area displays the result of the last command executed.

In addition to command history, this area also provides other key messages reports by the management application.

Chassis Alarm Indicator

This area, when populated, indicates that audible CO alarms are enabled for the managed chassis.

Number of Managed Devices

This area lists the number of managed devices within the currently selected view. The System Message Dialog Area, located on the lower left corner of the topology window, provides more detailed information about each of the devices.

Communication Status Indicator

This indicator shows the status of the communication link between the WEM server and the managed device. The indicator will be one of two colors:

- **Green:** Indicates that a communications link between the WEM server and the client is established and functioning in an idle state
- **Red:** Indicating that the WEM server is busy or a communications problem may be present. During normal operations, the indicator may flash red momentarily, as this indicates that the server is obtaining information from its managed devices (e.g. obtaining a list of contexts from a device or group of devices when a user selects it from the map), but it should return to green in less than 30 seconds.

If the indicator remains red for more than 60 seconds (when using a LAN connection from the client), this indicates that a communications problem is present. Such conditions should be reported and investigated.

Obtaining WEM Help

The WEM's Help system provides users with both context-sensitive Help, used to learn about a specific function, and general Help in which users learn about using the application itself and its associated functions.

Important: This help file is a general purpose file. Accordingly, not all Product features/functionality described in this file are necessarily included in the particular Product version you may be using, or there may be features/functionality contained in a Product version that may not be included in this help file.

Obtaining Help within WEM

General Help is accessed through the **Help** pull-down menu, located at the top of the menu bar. Click the **Contents** option from this menu to access the help system's welcome screen.

Standard Internet browser users should have a frame on the left side of their browser, displaying Contents, Index, and Search tabs. Following are explanations of each tab's purpose.

- **Contents:** The Contents tab provides a "table of contents" for the Help system. Like a printed book, subjects are organized into various sections. To open a particular section, click on the "+" sign to the left of the book icon for that section. When opened, each section will display the various Help topics associated with that section. When a user selects an option, such as a hyperlink or other option from a Help screen, the Contents section will automatically highlight the individual section and topic.
- **Index:** The Index tab is exactly like the index in any document, in that it allows the user to view various entries in alphabetical order. The advantage of a web-based index is that the user may also use the Index function to search for all instances of indexed keywords. When a user enters a search word, the user is moved to the matching area of the index. If there is more than one link available for that indexed keyword, the system will display a pop-up window wherein the user can select the option they want to display.
- **Search:** The Search tab allows the user to perform searches for a specific word or phrase across the entire Help system.

To remove the left-most frame from the display, click the **Hide** button, located at the upper right corner of the main window. To enable the frame, click the **Show** button. These buttons work as a toggle, wherein one or the other appears, as dictated by the status of the help system tab views.

Other browser-based navigation features, such as back and forward, print, and others work as usual.

Accessing Context-Sensitive Help

Context-sensitive help is displayed when a user clicks the **Help** button displayed on an operations screen.

This type of help is displayed in a secondary window that does not show the various tabs available in general help. Each context-sensitive help topic provides basic navigation (scroll up/down/left/right) and print functions as needed, but has no other options.

After a user has reviewed the context-sensitive help topic, they can close the secondary window by clicking anywhere within the help system.

Accessing Offline Help

Offline help can be accessed or downloaded without logging in to the WEM GUI. Navigate to the WEM page using your browser and click the "**Web Element Manager Offline Help**" link under the **Help Resources** section to download the WEM help in .CHM file format.

Chapter 9
Upgrading the WEM Software

The information and instructions in this chapter should be used to upgrade a WEM installation. These instructions assume that you have already obtained the upgrade file(s) and have stored them on the server running the WEM application.

Two upgrade types are currently supported:

- **Automated:** Once executed, the WEM installation file detects previously installed versions of the application. If an older version is present, you are prompted as to whether or not you would like to perform an upgrade.

  Because this process preserves all application database information from the currently installed version, it is only supported for n-2 releases, where n is the new version being installed. For example, the automated process can be used to upgrade either the 4.5.x or 5.0.x releases to version 5.1.x.

- **Manual:** This type involves uninstalling any existing instances of the application and installing the new version.

  This type **must** be used if the current instance is more than two releases older than the new version being installed. For example, the manual upgrade type must be used if 3.5.x is currently installed and you would like to upgrade to 5.1.x.

> ***Caution:*** Please contact your local support representative to ensure compatibility prior to upgrading.

> ***Important:*** The WEM application does not provide an automated mechanism for performing software "downgrades" (reverting to an older software version from a newer one). However, the instructions provided in the Performing a Manual Upgrade section of this chapter can be used since that procedure requires you to uninstall the existing version and install the alternate. Information is also provided for migrating database information.

This chapter includes the following topics:

> ***Important:*** Unless otherwise specified, all information in this chapter applies to both Sun Solaris and Red Hat Enterprise Linux-based WEM systems.

Pre-Upgrade Procedures

Important: Make sure that you check the status of your system with your system administrator before proceeding to the section Performing an Automated Upgrade or Performing a Manual Upgrade .

XML Report Generation

You can enable/disable XML report generation of the bulk statistics by using “Generate XML Files”. Alternatively, it can be enabled/disabled by configuring the XMLDataEnable parameter to 1 in the bsserver.cfg file (in the */<ems_dir>/server/etc* directory by default). If enabled, the files are stored on the EMS server (the */<ems_dir>/server/xmldata* directory by default).

Unpacking the Installation Files

WEM installation files are distributed as a single compressed file with a ".tar.gz" extension.

Once the installation file has been copied to the server, use the following procedure to unpack the file:

Step 1 Go to the directory in which the file is stored.

Step 2 Unzip the file by entering the following command:

`gunzip` *`file_name`***`.tar.gz`**

file_name is the name of the WEM application installation file.

Step 3 Un-tar the file by entering the following command:

`tar -xvf` *`file_name`* **`.tar`**

Decompressing the installation file results in the following files:

- **setup.bin**: The installation binary file.
- **inst**: The executable file used to initiate the installation. This file is used for both the console- and the GUI-based methods.
- **uninst**: Once the WEM application has been installed, this file must be copied to the */<ems_dir>/_uninst/* directory. It is the executable file for uninstalling the application for both the console- and GUI-based methods.
- *`file_name`***.tar**: A compressed file containing all of the application files required for both the script- and GUI-based installation methods.
- **README**: A text file containing information pertaining to the release.
- **sqlfiles.tar**: Script Query Language files related to WEM database functionality.
- **ems_migrate**: A script that performs a backup or restore of the WEM databases.
- **ems_migrate.cfg**: A file that contains configuration information related to the ems_migrate script.
- **README.ems_migrate**: A text file containing information related to the EMS migrate functionality.

Step 4 Proceed to either the Performing an Automated Upgrade or Performing a Manual Upgrade section of this chapter.

Performing an Automated Upgrade

This section provides information and instructions for performing an automated upgrade as described previously in this chapter.

Determining the Best Upgrade Method

The WEM, and its ancillary components such as the Apache web server and PostgreSQL database engine, may be installed using one of following methods.

- **GUI-based method:** This method is the most often used installation procedure. Requirements for using this method include:
  - Logon account to the WEM server with display terminal (monitor) attached and some X-Windows client installed on server.
  - Network connectivity to WEM server via Telnet or SSH, using some X-Windows client on remote workstation.
- **Console-based method:** This method is available to users who do not have an X-Windows client available for remote network connectivity to the WEM server via Telnet or SSH.

It is important to note that the upgrade method is independent of the method used for installation. For example, if the console-based method was used for installation, either the GUI- or console-based method can be used to perform the upgrade.

Depending on the desired installation method, proceed to either the Upgrading the WEM Software using the Console-Based Installation Method or Upgrading the WEM Software using the GUI-Based Installation Wizard section of this chapter.

Upgrading the WEM Software using the GUI-Based Installation Wizard

Follow the instructions below to upgrade the WEM using the GUI-based wizard.

Step 1 Go to the directory in which the WEM upgrade files are located.

Step 2 Execute the setup file by entering the following command:

```
./inst
```

The WEM Installer dialog box appears.

Step 3 Click the **Next** button. The system automatically checks for an installed version of the application. If a version is installed, a warning dialog appears.

Step 4 Click **Yes** to proceed.

Step 5 Follow the on-screen prompts to progress through the various installation dialogs and configure the parameters as required. Refer to the *WEM Installation Parameter Descriptions* table for descriptions of the configurable parameters on each of the installation dialogs.

Once you have completed the upgrade and all processes have started, a confirmation dialog box appears reporting that the installation was successful.

Step 6 Click the **Finish** button to exit the GUI-based installation wizard.

Step 7 Verify that all WEM processes were successfully started by looking at the on-screen messages in the console window. The following provides a sample of the messages:

```
Starting EMS Server...

EMS Server started.

PID: 1370

Logfile generated as:

./log/SERVER_LOG_20051220_142931/SERVER_LOG

Please check file /<ems_dir>/server/log/.server.log for additional debug messages

Starting Script Server...

Script Server started.

PID: 1389

Logfile generated as:

./log/SCRIPT_LOG_20051220_142937/SCRIPT_LOG
```

The following table lists the processes that are started at installation:

Process	Log File
EMS Server	.server.log
Script Server	.scriptserver.log
BulkStat Server	.bulkstatserver.log
BulkStat Parser Server	.bulkstatparser.log
Monitor Server (if enabled)	.watchdog.log
NorthBound Server	.northboundserver.log
Notification Service	.notifyservicescript.log

All log files are stored in the */<ems_dir>/server/log* directory by default. Refer to the log files for additional information in the event that one or more of the processes did not start properly.

Step 8 Copy the uninstallation script to the *_uninst* directory created during the installation process (*/<ems_dir>/_uninst* by default) by entering the following command:

```
cp uninst /<ems_dir>/_uninst/
```

Step 9 Copy the files pertaining to the migrate script to the scripts directory created during the installation process (*/<ems_dir>/server/scripts* by default) by entering the following command:

```
cp ems_migrate /<ems_dir>/server/scripts

cp README.ems_migrate /<ems_dir>/server/scripts
```

Upgrading the WEM Software using the Console-Based Installation Method

Follow the instructions below to upgrade the WEM using the console-based installation script.

Step 1 Go to the directory in which the WEM upgrade files are located.

Step 2 Execute the setup file by entering the following command:

```
./inst -console
```

A message appears welcoming you to the WEM installation.

Step 3 Enter "1" to proceed to the *EMS Upgrade Check* configuration prompts. The system automatically checks for installed version of the application. If a version is installed, a message appears asking if you would like to upgrade the current installation.

Step 4 Enter "1" to proceed.

Step 5 Follow the on-screen prompts to proceed through the upgrade and configure the various parameters as required. Refer to the *WEM Installation Parameter Descriptions* table for descriptions of the configurable parameters within each of the sections of the script.

Once you have completed the upgrade and all processes have started, you receive a message indicating that the WEM was successfully installed.

Step 6 Enter "3" to complete the installation.

Step 7 Verify that all WEM processes were successfully started by looking at the on-screen messages in the console window. The following provides a sample of the messages:

```
Starting EMS Server...

EMS Server started.

PID: 1370

Logfile generated as:

./log/SERVER_LOG_20051220_142931/SERVER_LOG

Please check file /<ems_dir>/server/log/.server.log for additional debug messages

Starting Script Server...

Script Server started.

PID: 1389

Logfile generated as:

./log/SCRIPT_LOG_20051220_142937/SCRIPT_LOG
```

The following table lists the processes that are started at installation:

Process	Log File
EMS Server	.server.log
Script Server	.scriptserver.log
BulkStat Server	.bulkstatserver.log
BulkStat Parser Server	.bulkstatparser.log
Monitor Server (if enabled)	.watchdog.log
NorthBound Server	.northboundserver.log
Notification Service	.notifyservicescript.log

All log files are stored in the */<ems_dir>/server/log* directory by default. Refer to log files for additional information in the event that one or more of the processes did not start properly.

Step 8 Copy the un-installation script to the *_uninst* directory created during the installation process (*/<ems_dir>/_uninst* by default) by entering the following command:

```
cp uninst /<ems_dir>/_uninst/
```

Step 9 Copy the files pertaining to the migrate script to the scripts directory created during the installation process (*/<ems_dir>/server/scripts* by default) by entering the following command:

```
cp ems_migrate /<ems_dir>/server/scripts

cp README.ems_migrate /<ems_dir>/server/scripts
```

Performing a Manual Upgrade

Follow the instructions in this section to perform a manual upgrade as described previously in this chapter. These instructions assume that a version of the application is currently installed and that it was installed in the default directory, /users/ems.

Important: The instructions in this section can also be used to perform a software downgrade of the WEM if required.

Step 1 Log into the WEM server as the user *root*.

Step 2 *Optional*. If you wish to preserve database information for the currently installed version, follow the instructions in the Performing a Database Back-Up using the backup Script section of this chapter and then proceed to *Step 3* of this procedure.

Step 3 Uninstall the WEM using the instructions provided in the *Uninstalling The WEM* chapter of this guide and proceed to *Step 4* of this procedure.

Step 4 Install the desired version of the WEM using the instructions provided in the *Installing the WEM Software* chapter of this guide and proceed to *Step 5* of this procedure.

Step 5 *Optional*. If database information was backed-up per *Step 2* of this procedure, restore the data using the instructions in the Performing a Database Restoration using the backup Script section of this chapter and proceed to *Step 6* of this procedure.

Step 6 Start WEM Server processes using the instructions in the *Step 3: Start WEM Server Application* section of *WEM Server Files and Operation* chapter of this guide.

Reconfiguring Bulkstat Schemas

Once the WEM software upgrade is completed successfully, you are required to configure the schemas.

Important: Bulkstats **must** be reconfigured after an upgrade otherwise any new counters/schemas will not be fetched.

Deleting an Already Configured Schema

For deleting the already configured schemas, follow the instructions below:

Step 1 Login to the WEM application.

Step 2 In the main menu, go to **Accounting > Bulk Statistics Configuration**. The Bulk Statistics dialog box opens.

Step 3 Click the **Configure** button to launch the Bulk Statistics Configuration dialog box.

Step 4 In the Schema tab, select all the configured schemas by clicking any row and then pressing **Ctrl**+**A**.

Step 5 After selecting all the configured schemas, click the **Delete** icon. Warning message displays.

Step 6 Click **Yes** to delete the selected schemas and click the **Apply** button. Another warning message displays.

Step 7 Click **No** to ignore the warning. The successful configuration message displays.

Step 8 Click **OK** to finish.

Reconfiguring Schemas

For reconfiguration of schemas, follow the instructions below:

Step 1 Login to the WEM application.

Step 2 In the main menu, go to **Accounting > Bulk Statistics Configuration**. The Bulk Statistics dialog box opens.

Step 3 Click the **Configure** button to launch the Bulk Statistics Configuration dialog box.

Step 4 Select the schemas to be configured under the **Schema** tab and click the **Add** icon.

Step 5 Click the **Apply** button to configure the selected schemas. You may get a warning message “You have selected some obsolete and/or WEM unsupported counters. Unsupported counters will not be parsed by WEM. Do you want to continue?”

Step 6 Click **Yes** to close the warning. The successful configuration message displays.

Step 7 Click **OK** to finish configuring schemas.

Preserving Database Information

Database preservation is done using the *backup.sh* script located in the */<ems_dir>/server/scripts* directory by default. This script is used to perform both database back-ups and restorations.

Information and instructions for using this script are provided in this section.

Performing a Database Back-Up using the Backup Script

Follow the instructions in this section to back-up database information prior to upgrading or downgrading WEM software.

Important: The instructions provided in this section are intended for use with those located in the Performing a Manual Upgrade section of this chapter.

Step 1 Move to the directory in which the backup script is located by entering the following command:

```
cd /<ems_dir>/server/scripts
```

Step 2 Perform the database back-up by entering the following command:

```
./backup.sh
```

This script automatically stops all WEM processes and takes the backup of the WEM database using `pg_dumpall` command. You are notified once the back-up is complete.

Step 3 Return to *Step 3* of the procedure in the Performing a Manual Upgrade section of this chapter.

Restoring a Database Using the Backup Script

Follow the instructions in this section to restore database information after performing a WEM software upgrade or downgrade.

Important: The instructions provided in this section are intended for use with those located in the Performing a Manual Upgrade section of this chapter.

Step 1 Move to the directory in which the backup script is located by entering the following command:

```
cd /<ems_dir>/server/scripts
```

Step 2 Perform the database restoration by entering the following command:

```
./backup.sh restore
```

This script automatically stops all WEM processes and performs the database restoration. You are notified once the database restoration is complete.

Step 3 Return to *Step 6* of the procedure in the Performing a Manual Upgrade section of this chapter.

Chapter 10
Uninstalling the WEM

This chapter provides the step-by-step procedure of uninstalling WEM application using the GUI-based installation wizard and the console-based installation. Additionally it provides instructions for backing up all the critical files before starting the WEM uninstallation.

This chapter includes the following topics:

Important: Unless otherwise specified, all information in this chapter applies to both Sun Solaris- and Red Hat Enterprise Linux-based WEM systems.

Understanding the Uninstall Process

Upgrading the Web Element software on the server requires that the currently installed version be uninstalled from the server before the newer version can be installed. Failure to do so will prevent your ability to install the new WEM version.

Important: If you are uninstalling WEM in any clustered setup prior to an upgrade, the node has to be put into maintenance mode first (i.e. removed from the resource group). This ensures that all the processes running on this node are stopped and prevents the active node from failing over to become the standby node. For more information on this procedure, please refer to *WEM High Availability Redundancy with Cluster Application* in the appendices.

Following is an overview of the uninstall process.

Step 1 - Make Backup Copies of All Critical Files

This step requires that you archive, at a minimum, the following files.

- All data files, typically located in the */<ems_dir>/server/data* directory and all subdirectories residing there (i.e. */bulkstats*, etc.).
- PostgreSQL data files, located in the *~postgres/data* or *users/postgresx.x.x/data* directory. Refer to the *Backing-up WEM Databases* section of the *WEM Database Maintenance* chapter in this guide for more information.

Important: Downgrading the WEM application to an earlier version is not supported at this time. You must uninstall the current version and install the older version using the instructions located in *Installing the WEM Software* chapter of this guide. Please contact your local sales representative for information on preserving data stored by the current WEM instance prior to uninstalling.

Step 2 - Uninstall WEM Application

The process used to perform this uninstall is dependent upon the method used to install the version currently running. See the section below for information on how to determine which installation method was used previously.

Whichever uninstall method is used, it is generally preferable to install the new version of the application using the GUI-based installation method.

Determining the Best Uninstallation Method

The WEM, and its ancillary components such as the Apache web server and PostgreSQL database engine, may be uninstalled using one of two methods.

- **GUI-based method:** This method is the most often used uninstallation procedure. Requirements for using this method include:
  - Logon account to the WEM server with display terminal (monitor) attached and some X-Windows client installed on server.
  - Network connectivity to WEM server via Telnet or SSH, using some X-Windows client on remote workstation.

  Important: If the uninstall GUI does not open, add X-windows port (TCP/6000) in the exception list of Windows firewall.

- **Console-based method:** This method is available to users who do not have an X-Windows client available for remote network connectivity to the WEM server via Telnet or SSH.

It is important to note that the uninstallation method is independent of the method used for installation. For example, if the console-based method was used for installation, either the GUI- or console-based method can be used to uninstall the program.

Using the GUI-based Uninstall Method

This section provides instructions for uninstalling the WEM application using the GUI-method.

Important: The GUI-based uninstall script is designed to protect all the historical data files that are currently in use. However, it is still recommended that you manually perform a backup of these files before continuing.

Step 1 Log into the server on which the WEM application is installed. Use the root username and password.

Step 2 Go to the directory in which WEM is installed (the */users/ems* directory by default) by entering the following command:

```
cd /<ems_dir>
```

Step 3 Go to the */_uninst* sub-directory by entering the following command:

```
cd _uninst
```

Step 4 Execute the uninstall script by entering the following command:

```
./uninst
```

A dialog box appears welcoming you to the WEM uninstallation wizard.

Step 5 Click the **Next** button. A dialog appears identifying the processes to be stopped.

Step 6 Click **Next** and follow the on-screen instructions.

Step 7 Click **Finish** to complete the uninstallation process.

The uninstall script leaves the */ems* directory in place with several sub-directories.

Step 8 *Optional*: If all critical and historical data files have been properly backed up, delete the */ems* directory using the following commands:

```
cd ..

cd ..

rm -R ems
```

Important: If you decided to keep the /ems directory, it is highly recommended that at the very least you delete the _uninst directory. Failure to remove this directory before installing a new version of the WEM application using the GUI-based installation method will result in a different *_uninst* directory being created each time you perform a software upgrade. This results in the creation of multiple uninstall directories (i.e. named */_uninst2, /_uninst3*, etc.). The uninst file needed for the next uninstall would have to be located there.

Using the Console-based Uninstall Method

This section provides instructions for uninstalling the WEM application using the console-based method.

Important: The console-based uninstall script is designed to protect all the historical data files that are currently in use. However, it is still recommended that you manually perform a backup of these files before proceeding with this procedure.

Step 1 Log into the server on which the WEM application is installed. Use the root username and password.

Step 2 Go to the directory in which WEM is installed (the */users/ems* directory by default) by entering the following command:

```
cd /<ems_dir>
```

Step 3 Go to the */_uninst* sub-directory by entering the following command:

```
cd _uninst
```

Step 4 Execute the uninstall script by entering the following command:

```
./uninst
-console
```

A message appears welcoming you to the WEM uninstallation wizard.

Step 5 Enter "1" to proceed. A message appears listing the application processes to be uninstalled.

Step 6 Enter "1" to proceed with the uninstallation. A number of messages are displayed indicating the progress.

Step 7 Enter "3" to complete the uninstallation process.

Upon completion, the uninstall script indicates that certain sub-directories were not deleted within the */ems* directory.

Step 8 *Optional*: If all critical and historical data files have been properly backed up, delete the */ems* directory using the following commands:

```
cd ..

cd ..

rm -R ems
```

Important: If you decide to keep the /ems directory, it is highly recommended that at the very least you delete the *_uninst* directory. Failure to remove this directory before installing a new version of the WEM application using the GUI-based installation method will result in a different *_uninst* directory being created each time you perform a software upgrade. This results in the creation of multiple uninstall directories (i.e. named */_uninst2, /_uninst3*, etc.). The uninst file needed for the next uninstall would have to be located there.

Appendix A
Troubleshooting the WEM

This appendix provides information on troubleshooting the following:

- Issues Pertaining to Installation
- Issues Related to Starting WEM
- Issues Related to Login
- Issues Related to the Web Browser
- Issues Pertaining to CORBA Communication
- Issues Related to Bulkstatistics
- Issues Pertaining to Configuration Backup
- Issues Pertaining to Alarms
- Issues Pertaining to the Process Monitor (PSMON)
- Issues Pertaining to Starting and Stopping EMS Processes
- Issues Pertaining to Java
- Issues Pertaining to WEM Upgrade

In addition to the above, instructions are also provided for capturing client and server logs. These are provided in the Capturing WEM Client Logs and Capturing WEM Server Logs using Script sections of this appendix.

Important: Unless otherwise specified, all information provided in this chapter applies to both Solaris and Red Hat Enterprise Linux-based WEM systems.

Issues Pertaining to Installation

Problem:	Installer window doesn't appear.
Possible Cause(s):	• If you received the *"ERROR: could not initialize interface awt - exception: java.lang.InternalError: Cannot connect to X11 window server using ':0.0' as the value of the DISPLAY variable."* message, the display settings of your terminal program may be incorrect, or Exceed is not running on the client machine. • The */tmp* directory may be full.
Action(s):	• Verify the display settings of the terminal application on the client machine are correct. • Verify that Exceed is installed properly on the client machine. • Determine the status of the /var/tmp directory by entering the **df -k** command. If it is at or near capacity, choose another directory for the *Host Base Directory* parameter setting. This parameter can be set via the installation process.

Problem:	Received *"Unable to install Element Management System <version> over Element Management System: Installed product has newer version."* message when attempting installation.
Possible Cause(s):	• A later version of the WEM is already installed. • A previously installed version of the WEM was not completely uninstalled, or was uninstalled incorrectly.
Action(s):	• Completely uninstall the newer version and install the desired version. • Determine if WEM packages exist in the */var/sadm/pkg* directory. These packages begin with "EMS". If packages exist, remove them by entering the **pkgrm -n EMS*** command. Once they've been removed, reinstall the application.

Problem:	WEM components did not start successfully upon installation.
Possible Cause(s):	A previously installed version of the WEM was not completely uninstalled, or was uninstalled incorrectly.
Action(s):	• Check the installation log files (located in the directory) and EMS process log files (located in the *<ems_dir>/server/log* directory). • Enter the **ps -ef | grep server** command to determine if any process instances from previous installations are running. If so, stop them using the instructions in the *WEM Server Files and Operation* chapter of this guide. Once stopped, start the processes for the current installation using the instructions in the same appendix.

Issues Related to Starting WEM

Problem:	WEM server doesn't start.
Possible Cause(s):	• The PostgreSQL database is not running. • The *log* directory may have been accidentally deleted. • Processes from a previous WEM are still running. • The *"ServerPort"* and/or *"ServerIIOPPort"* port values configured for the WEM are in use by other processes. • The physical IP address of the WEM server might have been changed without modifying other related WEM configuration appropriately.
Action(s):	• Verify that the Postgres database is running by entering the **ps -ef | grep post** command. If is not, follow the instructions in *WEM Server Files and Operation* chapter of this guide to start it. • Determine if the log directory exists in *<ems_dir>/server* (default directory) using the **ls** command to display the contents of the directory. If it is missing, create it using the **mkdir** command and stop and restart all WEM processes using the instructions in *WEM Server Files and Operation* chapter of this guide. • Enter the **ps -ef | egrep "server|bulkstatparser|bulkstatserver|scriptsrv"** command to determine if WEM server processes are running and, if they are, what directory did they originate from. If they're different, stop the processes and restart the server from within the desired installation directory using the instructions in *WEM Server Files and Operation* chapter of this guide. • Determine if the *"ServerPort"* and/or *"ServerIIOPPort"* port numbers specified in the *nms.cfg* file (located in the *<ems_dir>/server/etc* directory by default) are already in use. The default *"ServerPort"* is 22222, and the default *"ServerIIOPPort"* is 15000. This can be determined by entering the **netstat -a** command which displays a list of all the process addresses and ports in use in *"ipaddress.port"* format. If they are in use, either stop the other processes or configure new values for these parameters. • If the WEM server IP address has been changed, the appropriate modifications need to be made in the *nms.cfg* and */etc/hosts* files, as per the WEM IP Address Change Procedure .

Problem:	Postgres doesn't start.
Possible Cause(s):	• A *.s.PGSQL.5432.lock* lock file is present in the */tmp* directory prior to starting postgres. • Shared resources are not released after another Postgres instance was terminated. • The PostgreSQL system environment variables were not configured properly prior to installation.
Action(s):	• If the lock file is present, delete it using the **rm .s.PGSQL.5432.lock** command. • Determine if a previous Postgres instance is still using system resources by entering the **ipcs** command. If it is, clear the resources by entering the **ipcrm** command. • Ensure that the PostgreSQL system environment variables were configured properly using the information in *Installing the WEM Software* chapter of this guide.

Problem:	Received the following error message in postgres log: “2008-09-13 15:57:31 IST bsdb ERROR: column "data_touseravg_bps" does not exist at character 4332008-09-13 15:57:31 IST bsdb STATEMENT: SELECT "sampledate", "sampletime", "vpnname", "vpnid", "apn", "acc_req_sent", ... FROM apn_current WHERE ("boxername"='bngnc22') AND ((("sampledate"='2008-09-13') AND ("sampletime">='33900')) ... ORDER BY "sampledate", "sampletime", "vpnname", ...; ” **NOTE:** The table name in the above message is after the 'FROM' keyword.
Possible Cause(s):	The mentioned table in error logs may not be in sync with the old table. There are two tables for each bulkstat subsystem in database: old and current (for example, card and card_current, port and port_current, etc.).
Action(s):	There is one workaround for this but there will be data loss for that mentioned counter. Manually drop the column from table to make the tables in sync. There is data loss only for that particular column. After this, restart all the bulkstat processes (*bulkstatparser* and *bulkstatserver*). After restarting, *bulkstatparser* will re-add that column in both the tables and data will be populated for that column.

Problem:	Received the following error message in postgres log: “ERROR: trigger "xxxxxxxxxxxxxxxxxxxx" for table "yyyyyyyyyyyyy" does not exist ERROR: function fffffffffffffffffff() does not exist ERROR: view "vvvvvvvvvvvvvvvvvvvvv" does not exist”
Possible Cause(s):	Error messages regarding function, trigger and view are logged in logfile when the DROP statement is executed while initializing the EMS databases. SQL file used for initializing the database contains a sequence of DROP and CREATE statements for every function, trigger and view. These messages do not have any impact on postgres as well as WEM functionality.
Action(s):	No action required. This is a normal behavior.

Issues Related to Login

Problem:	Could not login to WEM.
Possible Cause(s):	Invalid user name or password.
Action(s):	Verify that the username and password you are entering is correct.

Problem:	Received *"Could not connect to server, destroying applet"* message.
Possible Cause(s):	• WEM Server is not running. • Missing Interoperable Object Reference (IOR) files. • A firewall is prohibiting communication between the client and the server. • The user could have been locked out due to multiple failed login attempts.
Action(s):	• Verify that server processes are running using the information in *WEM Server Files and Operation* chapter of this guide. • Verify that IOR files are present; they are stored in the *<ems_dir>/client/<ems-version-number>/ior* directory by default. A number of files ending in *.ior* should be present. These files pertain to various functions supported by the WEM. • Edit the *img.html* file (located in the *<ems_dir>/client* directory (by default) to use fixed ports and open the required ports in the firewall. This requires the configuration of the "FIXED_PORT", "FIXED_PORT_RANGE_START" and "FIXED_PORT_RANGE_END". • Verify that all the ports between FIXED_PORT_RANGE_START and FIXED_PORT_RANGE_END (both inclusive) are open on the firewall. If they are not, they should be opened. • If the user is *"superuser"*, the *set_superuser_password* script can be used to reset the *"superuser"* password to the default. If the user is not *"superuser"* then the administrator needs to be contacted to reset the user's password.

Problem:	Received *"Java policy file is outdated or missing"* message.
Possible Cause(s):	The *.java.policy file* is either missing from the user's home directory on the client machine or it has expired.
Action(s):	• Verify that the **.java.policy** file is present in your home directory. Refer to *Preparing and Using the Client Workstation* chapter of this guide for more information. • Copy the *.java.policy* file from the *"Java Policy File"* link provided in img.html file to your home directory. Ensure that no extension (i.e., .txt) is appended to the file. ***Important:*** All instances of the browser must be closed and restarted after the policy file has been updated.

Problem:	Received *"Server could not establish connection with client, therefore notifications will not work."* message.
Possible Cause(s):	• A firewall is prohibiting communication between the client and the server. • The Hosts file does not have an entry for the client PC's hostname and corresponding physical IP address.
Action(s):	• Edit the *img.html* file (located in the *<ems_dir>/client* directory (by default) to use fix ports and open the required ports in the firewall. This requires the configuration of the "FIXED_PORT", "FIXED_PORT_RANGE_START" and "FIXED_PORT_RANGE_END". • Verify that all the ports between FIXED_PORT_RANGE_START and FIXED_PORT_RANGE_END (both inclusive) are open on the firewall. If they are not, they should be opened.Edit the Hosts file (located in */etc* directory) with the client PC's hostname and corresponding physical IP address.

Problem:	Superuser (any user) account locked.
Possible Cause(s):	The configured number of consecutive failed logins has been reached.
Action(s):	Check the configuration of the no limit ConsecutiveFailLogin parameter in the ua.cfg file (located in the *<ems_dir>/server/etc* directory by default). If users are frequently locked out due to reaching the maximum limit, you may consider increasing the limit, or disabling the functionality. You may also consider reducing the amount of time the account is locked out by modifying the configuration of the no locked out *LockOutInterval* parameter also contained in the ua.cfg file.

Issues Related to the Web Browser

Problem:	WEM Client cannot be started.
Possible Cause(s):	JRE 1.4.x is installed on the client machine.
Action(s):	JRE 1.4.x is not supported. If it is currently installed on the client machine, uninstall it and install either JRE 1.5 or 1.6.

Problem:	Not able to invoke help
Possible Cause(s):	The browser is configured to block pop-ups.
Action(s):	Configure your browser to allow pop-ups from the WEM server.

Problem:	WEM Client-Server version mismatch message is received.
Possible Cause(s):	Attempting to login into an older version of the WEM after having logged into a newer version of the application.
Action(s):	This is caused by the browser storing the*.jar* files for the newer version of the WEM client in its cache. • **For JRE versions greater that 1.5:** The **Temporary Internet Files** group in the **General** tab of the Java Control Panel should be used to disable caching. • **For JRE versions greater that 1.6:** The **Temporary Internet Files** group in the **General** tab of the Java Control Panel should be used to disable caching.

Problem:	After WEM upgrade or installation of a new version, various screens, for example Graph/ Current Alarm View, do not open.
Possible Cause(s):	Check the java console and if you get exceptions like *"Exception in thread "AWT-EventQueue-2" java.lang.NoClassDefFoundError"*, it could be the case that the browser cache is enabled on your workstation and needs cleanup.
Action(s):	Cleanup the temporary internet cache from your browser and re-invoke the WEM Client.

Issues Pertaining to CORBA Communication

Problem:	IMG is unmanageable.
Possible Cause(s):	• The WEM Server cannot communicate with the system due to network issues. • There is an ORBEM client identification mismatch between the chassis and WEM. • The ORBEM client on the chassis is disabled. • There is an IIOP port configuration mismatch between the chassis and WEM. • The IIOP transport parameter on the chassis is not enabled.The chassis is unmanageable.
Action(s):	• Ensure ICMP connectivity between the system and the WEM Server using the **ping** <*wem_server_ip_address*> command from the chassis' command prompt. Refer to the *Command Line Interface Reference* for more information on using this command. • Verify that the ORBEM client identification on the chassis matches that configured on the WEM. The configuration of this parameter on the chassis can be determined by entering the **show configuration | grep client** CLI command. In WEM, check the ASID (Application Server ID), Port, and SSL-enabled flag (IIOP/SIOP) on the Modify IMG screen. Change these settings as needed. • Check the status of the ORBEM client on the chassis by executing the **show orbem client id** <*client_id*> command on the chassis. The "State" should be *"Enabled"*. If the "State" is *"Disabled"*, execute the **activate client id** <*client_id*> command in the ORBEM Configuration Mode and check the status again--it should now be *"Enabled"*. • Verify that the configuration of the IIOP port on the chassis matches that configured for the WEM. The configuration of this parameter on the chassis can be determined by entering the **show configuration | grep iiop-port**. In WEM, check for the ASID (Application Server ID), Port, and SSL-enabled flag (IIOP/SIOP) on the Modify IMG screen. Change these settings as needed. • Verify that the IIOP transport parameter is enabled on the chassis by entering the **show configuration | grep iiop-transport** command. If it is not, enable using the instructions found in the System Administration and Configuration Guide. • Check if the SSL is enabled and/or enforced on the WEM. If the SSL is enabled, disable the IIOP transport on the chassis and set the value of **IMG Port** for the chassis such that it is identical to the SIOP port parameter configured on the chassis.

Problem:	Received *"Callbacks between server and client are not working. Screen cannot be invoked."* message.
Possible Cause(s):	• A firewall is prohibiting communication between the client and the server. • The network connection between the server and client machine might be slow.

Action(s):	• Edit the *img.html* file (located in the <*ems_dir*>*/client* directory (by default) to use fix ports and open the required ports in the firewall. This requires the configuration of the "FIXED_PORT", "FIXED_PORT_RANGE_START" and "FIXED_PORT_RANGE_END". • Verify that all the ports between FIXED_PORT_RANGE_START and FIXED_PORT_RANGE_END (both inclusive) are open on the firewall. If they are not, they should be opened. • The user can try performing a "ping" or “traceroute” from the server machine for the client's IP address and check for any packet-loss or network delay and contact the network administrator if required.

Issues Related to Bulk Statistics

Problem:	WEM server not receiving bulkstats files.
Possible Cause(s):	• No FTP server is running on the server. • User specified in bulkstats configuration screen to FTP files from chassis to WEM does not exist. • Invalid FTP user password is being used to access the chassis. • No "destination" path for bulkstats files is configured. • Inadequate user privileges for bulkstatistics storage directory. • **Sun Solaris WEM Servers only**: Solaris operating system patches may need to be updated. • Poor quality connection between chassis and WEM.
Action(s):	• Verify that the FTP server process is running on the server by issuing the **ps -ef | grep in.ftpd** command. If it is not, start it. • FTP user needs to be created by Administrator. • Check the username and password used to ftp the bulkstats data from the chassis to Web Element Management server. Compare the *"FTPUserName"* and *"FTPPassword"* parameters in the nms.cfg file located in the *<ems_dir>/server/etc* directory by default to the names of administrative users with FTP privileges on the chassis. • Verify that the *"destination"* directory is configured in the *bsparser.cfg* file located in the *<ems_dir>/server/etc* directory by default. • Verify that the FTP user has permissions to write to the configured storage directory. • **Sun Solaris WEM Servers only**: Verify that the latest Solaris operating system patches are installed. Refer to *WEM Port and Hardware Information* chapter of this guide for more information. • Ensure that the configuration the bulk statistics receiver on the managed system Executing the **show bulkstats** command on the chassis displays this information. The *"Remote File Format"* field should contain a valid directory on the WEM Server. (Also verify that this directory exists on the server.) The *"Bulkstats Receivers"* field should contain the IP address of the WEM Server. • Slow connections could affect the data transfer between the chassis and the WEM server. In this case, contact your system administrator.

Problem:	XML files are not getting generated.
Possible Cause(s):	• The Bulkstats Server component is not running. • Invalid *"sample-interval"* parameter configuration on the system. • Bulkstatistics functionality was configured through the system's command line interface rather than through the WEM. • XML file generation is disabled.

Action(s):	• Verify that the Bulkstats Server process is running by entering the **ps -ef | grep bulkstatserver** command. If it is not, execute the **./serv bulkstatserver start** command from within the server directory (*<ems_dir>/server* by default). • Verify that the *"sample-interval"* parameter on the system is set to either "1" or "5". The value can be determined by entering the **show bulkstats** command on the command line. • Make sure that the bulkstats schema configuration is done through WEM. • Make sure that *"XMLDataEnable"* parameter in the *etc/bsserver.cfg* file is set to "1" (enabled). If it is not, change the setting, save the file, and execute the **./serv bulkstatserver start** command from within the server directory (*<ems_dir>/server* by default).

Problem:	Received *"No matching data found"* error when fetching bulkstatistics reports.
Possible Cause(s):	• The bulk statistics may not be getting parsed properly. • Invalid filter criteria used for the fetch operation.
Action(s):	• Verify that the filter criteria entered is valid. • If you are querying server in another time zone, enter the timing filters according to your time zone only. • Check if the corresponding data is present in the bsdb. • Verify that the *"sample-interval"* parameter on the system is set to either "1" or "5". The value can be determined by entering the **show bulkstats** command on the command line.

Problem:	Bulkstats files are not getting parsed.
Possible Cause(s):	• The Bulkstatistics Parser component is not running. • Bulkstat configuration may have been done through the CLI.
Action(s):	• Verify that the Bulkstatistic Parser process is running by entering the **ps -ef | grep bulkstatparser** command. If it is not, execute the **./serv parserserver** command from within the server directory (*<ems_dir>/server* by default). • Verify that the bulkstatistics format is compatible with the WEM. Refer to the *bs.cfg* file (located in the *<ems_dir>/server/etc* directory by default) for WEM bulkstatistic formatting.

Problem:	Bulkstatserver process is not started.
Possible Cause(s):	The function of 'bulkstatserver' is only to generate the XML files. It is possible that the "Generate XML Files" option was not enabled during installation.

Action(s):	• For an existing installation, edit the *"XMLDataEnable"* parameter in the *etc/bsserver.cfg* file to be set to "1" (enabled). Once the setting is changed and the files is saved, execute the **./serv bulkstatserver start** command from within the server directory (*<ems_dir>/server* by default). • For new installations, ensure that "Generate XML Files" option is selected during the installation process.

Problem:	ASCII files are not getting generated.
Possible Cause(s):	Configuration may not be proper.
Action(s):	Check for the following combination of configurables in bsserver.cfg: 1) XMLFileType = 0 2) ASCIIFileGeneration = 1 3) Configure proper licenses in emslic.cfg To reflect changes in any of the configurable values, restart the bulkstatserver. ***Important:*** If XMLFileType is set to 1, it will generate XML files irrespective of the other two mentioned configurables.

Problem:	File header in bulkstats file is not proper.
Possible Cause(s):	The header might have been configured through CLI.
Action(s):	Always configure the header format through WEM only; else it will affect the bulkstatparser functionality.

Problem:	XML files are getting re-generated.
Possible Cause(s):	OverrideLastAccessFlag may be set to 1.
Action(s):	Check if *OverrideLastAccessFlag* in *bsserver.cfg* is enabled. If it is enabled, disable it and restart the bulkstatserver.

Problem:	XML/ASCII files ftp operation failing frequently.
Possible Cause(s):	• Network problem • PoolSize in bsserver.cfg is not adequate
Action(s):	• Check the network health to see if there is too much delay or packets getting dropped. Contact the network administrator in case of issues. • If FTP is used, it is recommended that PoolSize should be 10. If SFTP is being used, Poolsize must be set to 3.

Problem:	Schema counters are not fetched/plotted properly.

Possible Cause(s):	• Reconfiguration of schema is not done after upgrade. Refer to the *Reconfiguration of Bulkstat Schemas* section of this guide for more information. • Bulkstat parser is not running. • There is no data matching the filter criteria.
Action(s):	• After upgrade, reconfigure the bulkstat schema for reflecting the new schema changes, if any. • Start the bulkstatparser. • Check if the filter criteria is correct and ensure that the data is available for that period.

Problem:	Counter names are visible in data files.
Possible Cause(s):	The counters are not supported on the system. There are two possibilities: • Counters removed from the boxer build. In this case, WEM cannot remove the counters from schemas as WEM maintains backward compatibility. This does not have any impact on the WEM functionality. • System build is older than WEM build (for example, StarOS build 7.0 and WEM build 8.0). This does not have any impact on the WEM functionality. Bulkstat parser will ignore the counter strings while parsing data files.
Action(s):	No action required. This is a normal behavior.

Problem:	Issues with file 2-4 format.
Possible Cause(s):	WEM only supports 'file 1' format for configuring schemas - and only if it is configured through WEM. Problems related to other file formats are out of WEM scope.
Action(s):	No action required.

Issues Pertaining to Configuration Backup

Problem:	Configuration files are not getting backed up.
Possible Cause(s):	• No FTP server is running on the server. • Invalid FTP username password being used to transfer files from chassis to WEM server. • Inadequate user privileges for configbackup storage directory. • **Solaris WEM Servers only**: Solaris operating system patches may need to be updated. • Poor quality connection between chassis and WEM.
Action(s):	• Verify that the FTP server process is running on the server by issuing the **ps -ef | grep in.ftpd** command. If it is not, start it. • Use the Configuration Backup screen to change the *FTPUsername* and *FTPPassword*. • Verify that the FTP user has permissions to write to the configured storage directory. • **Solaris WEM servers only**: Verify that the latest Solaris operating system patches are installed. Refer to *WEM Port and Hardware Information* chapter of this guide for more information. • Slow connections could affect the data transfer between the chassis and the WEM server. In this case, contact your system administrator.

Issues Pertaining to Alarms

Problem:	The WEM is not receiving alarms.
Possible Cause(s):	• Invalid configuration of SNMP target parameters on the chassis. • An alternate application is receiving the alarms using the same port.
Action(s):	• Verify that the SNMP target IP address and port number configured on the chassis match that of the WEM server. The SNMP target configuration on the chassis can be determined by entering the **show snmp transports** command. Check this information against the WEM server IP address (*"ServerIpAddress"*, specified in the *nms.cfg* file) and the SNMP port number (*"SnmpTrapPort"*, specified in the *fm.cfg* file) parameters. (Both of these files are located in the *<ems_dir>/server/etc* directory by default.) • Ensure no other application is running that receives the alarms on the port. Port status on the WEM server can be checked by executing the **netstat -a** command.

Problem:	Not able to receive Mail Notifications
Possible Cause(s):	• The E-mail server is not running. • Invalid Mail identification information configured within the WEM for notifications.
Action(s):	• Verify that the E-mail parameters are properly configured in the *fm.cfg* file (located in the *<ems_dir>/server/etc* directory by default). • Verify that the E-mail server is running. • Verify that the E-mail information configured in the **Alarm Configuration** dialog of the WEM is correct.

Problem:	Script execution on receiving ALARM fails
Possible Cause(s):	• The WEM Script Server is not running. • The script file is missing. • The script file does not have proper executable permissions.
Action(s):	• Verify that the Script Server is running by entering the **ps -ef | grep scriptsrv** command. If it is not, execute the **./serv scriptserver** command from within the server directory (*<ems_dir>/server* by default). • Verify that the script file is located in the *<ems_dir>/server/scripts* directory (this is the default directory). If it is not, copy the script to that location. • Verify that the script can be executed by entering the **ls -al** command from within the directory in which the script is located.

Issues Pertaining to the Process Monitor (PSMON)

Problem:	WEM processes are not restarted after a crash.
Possible Cause(s):	• PSMON is not running • Invalid PSMON configuration • The PSMON may have given up after performing multiple retries in a specific duration
Action(s):	• Verify that PSMON is running by entering the **ps -ef | grep psmon** command. If it is not, start it using the instructions located in *WEM Process Monitor* chapter of this guide. • Verify that PSMON is configured with the proper entries to start WEM processes. These entries may not be available if they were not selected for monitoring during the installation process. Refer to the instructions located in *WEM Process Monitor* chapter of this guide for information on PSMON configuration. • The PSMON tries to restart the processes for "numretry" time within a duration of "tmintval" (refer to *etc/psmon.cfg*) per process. If the process still doesn't start, PSMON no longer monitors this process. Please check the *<ems_dir>/log/watchdog.log* for details. Try restarting the process using the *serv* script.

Issues Pertaining to Starting and Stopping EMS Processes

Problem:	When starting or stopping a WEM process, the user receives the error message *ld.so.1: httpd: fatal: libgcc_s.so.1: open failed: No such file or directory*.
Possible Cause(s):	**Solaris WEM Servers**: The configure runtime linking environment (crle) Default Library Path (ELF) on the Solaris server does not contain the EMS library path. **Red Hat Enterprise Linux WEM Servers**: The configure dynamic linker run time bindings (ldconfig) Default Library Path on the RHEL server does not contain the EMS library path.
Action(s):	**Solaris WEM Server**: • Log into the WEM Server as **root** and enter the **crle** command to view the current Default Library Path path. Here is an example where the crle path does not contain the EMS library path: `# crleConfiguration file [version 4]: /var/ld/ld.config Default Library Path (ELF):/lib:/usr/lib:/opt/gss/lib:/opt/postgres/lib:/users/gss/lib:/users/postgres/lib:/users/usr/lib Trusted Directories (ELF):/lib/secure:/usr/lib/secure(system default) Command line: crle -c /var/ld/ld.config -l /lib:/usr/lib:/opt/gss/lib:/opt/postgres/lib:/users/gss/lib:/users/postgres/lib:/users/usr/lib` • If the crle Default Library Path does not contain the EMS library path, use the following crle command to update it: `# crle –u –l $EMS_INSTALL_PATH/server/lib`
	Red Hat Enterprise Linux WEM Server: • Log into the WEM Server as *root* and verify that the *ems.conf* file is present in the */<ems_dir> /etc/ld.so.conf.d/* directory. To view the exsiting *ems.conf* file, enter the following commands: # cd /etc/ld.so.conf.d # cat ems.conf #This file is used to setup the EMS runtime linking environment • If the *ems.conf* file is not present, enter the following commands to create it: # cd /<*ems_dir*>/ems/server/lib # cd /etc/ld.so.conf.d # echo "$EMS_INSTALL_PATH/server/lib" > ems.conf • Verify that the */etc/ld.so.conf* file contains the *ld.so.conf.d/*.conf* entry. If the entry is not present, add it to the */etc/ld.so.conf* file. • Enter the following command to apply any changes made: ldconfig

Issues Pertaining to Java

Problem:	The following message is displayed when attempting to access WEM dialogs containing tables after changing the look and feel option to Windows: *"java.lang.NullPointerException"*.
Possible Cause(s):	This may be an issue related to JRE 1.4.x.
Action(s):	If JRE 1.4.x is currently installed, uninstall it and then install JRE 1.5.

Problem	The WEM client hangs when the user tries to load the configuration from the client file system. This is typical with older WEM builds
Possible Cause(s)	There is a bug in JRE 1.6.0_24 and above where JFileChooser class checks for the "modifyThreadGroup" permission which may not exist in the current *.java.policy* file.
Action(s)	Update the*.java.policy* file on any client machine that uses JRE 1.6.0_24 and above with the following line: *permission java.lang.RuntimePermission "modifyThreadGroup."*

Problem	An error message displays to update the*.java.policy* file when the user invokes the WEM url. This is typical with newer WEM builds.
Possible Cause(s)	There is a bug in JRE 1.6.0_24 and above, where JFileChooser class checks for the "modifyThreadGroup" permission, which may not exist in the current *.java.policy* file.
Action(s)	Download the *.java.policy* file again from the options located on the WEM splash screen.

Problem:	The WEM Process Monitoring dialog shows *"Could not connect to server. Screen will not be invoked"*.
Possible Cause(s):	This may be an issue related to JRE 1.4.x.
Action(s):	If JRE 1.4.x is currently installed, uninstall it and then install JRE 1.5.

Problem:	After enabling audio support from the Alarm Management menu, the browser window crashes with the following error message: An unexpected exception has been detected in native code outside the VM. Unexpected Signal: EXCEPTION_ACCESS_VIOLATION (0xc0000005) occurred at PC=0x7131B60 Function=[Unknown.] Library=*C:\Program Files\Java\j2re1.4.2_04\bin\jsound.dll* In addition, the stack trace output shows: Current Java thread: at com.sun.media.sound.MixerThread.runNative(Native Method) at com.sun.media.sound.MixerThread.run(Unknown Source)
Possible Cause(s):	This may be an issue related to 1.4.x.
Action(s):	If 1.4.x is currently installed, uninstall it and then, install JRE 1.5.

Issues Pertaining to WEM Upgrade

Problem:	The migrate script is not working if the postgres server is running on a port other than the default port.
Possible Cause(s):	The postgres communication port parameter is not passed to the postgres application call through the migrate script.
Action(s):	A script will prompt you to provide inputs for the postgres communication port at the time of data restoration (not at backup time) along with other input parameters (backup dir, WEM application path, postgres admin, password).

Problem:	Map could not be fetched after manual upgrade from version 'A' to version 'B'.
Possible Cause(s):	While manually upgrading from version 'A' to version 'B', you may have used the original migrate script, i.e., the migrate script from version 'A' (since it is already available on the system) to restore the database.
Action(s):	While manually upgrading from version 'A' to version 'B', if you use the migrate script from version 'A', the database will be backed up. However, to restore the database, you have to use the migrate script from version 'B', i.e., the script that is packaged with the version that you are upgrading to. You will get the latest migrate scripts for restoring the database after unpacking the lastest WEM *install.xxx.tar.gz* bundle. The reason for doing this is that the recent scripts are likely to be upgraded from previous versions.

Capturing WEM Client Logs

In the event that an issue exists that could not be solved using the information provided previously in this chapter, you may need to capture client logs for debugging purposes. This section provides information on how to utilize logging for WEM clients.

Step 1 Launch the web browser on the client machine.

Step 2 Open the Java Console. Assuming that the client is a Microsoft Windows-based machine, this can be done using the following instructions:

Step a..... Right-mouse click on the *Java(TM) 2 Platform* icon in the status area (Windows System Tray).

Step b..... Select **Open Console** from the menu.

Step 3 Open the URL of the Web Element Management Server in the web browser, replacing `img.html` with `imgdebug.html`.

Step 4 Login to the WEM and perform the operations causing the issues.

The Java Console contains log messages that could be used for debugging the issue.

Capturing WEM Server Logs using Script

In the event additional troubleshooting assistance is required, debugging information can be collected using a script called *getSupportDetails.pl*. This script collects different log files and captures the output of certain system commands that aid in troubleshooting issues. This script is packaged with the WEM Server in the *<EMS_INSTALL_DIR>/tools/supportdetails/* directory.

This script refers to an XML file to get the list of logs. This XML resides in the same directory as the script. Once executed, the script retrieves the contents of logs, files, folders, and output of certain commands and prepares a zipped file (*/tmp/log/emssupportDetails.tar.gz*), by default it is placed in */tmp/log* directory.

Requirements:

Perl 5.8.5 and above is required for running the script. This is packaged with the WEM Server.

Apart from standard Perl modules (which are included in default installation of Perl), some additional modules are required for running the script. The list is as follows:

- expat version 1.95.8
- expat version 1.95.8
- XML:Parser version 2.34
- XML-Parser-EasyTree
- Devel-CoreStack version 1.3

These modules are installed by default by the WEM application. Please ensure that the above mentioned modules are installed when using a different installation of Perl.

To run the script, go to the path where the script is present and enter:

```
./getSupportDetails.pl [--level=...] [--xmlfile=...] [--outputDir=] [--help]
```

--level	Specifies the level of debug to run. It can have a maximum of 4 levels. The level 4 provides the most detailed information. Refer to *README.txt* file for more information. Default: 1
--xmlfile	Specifies the xml file name to be used for collecting the log. Default: *getSupportDetails.xml*
--outputDir	Specifies the output directory for the *emssupportDetails.tar.gz* file if different from the default output directory (*/tmp/*).
--help	Display this information.

For example:

```
./getSupportDetails --level=4 --xmlfile=/tmp/something.xml --
outputDir=/mywemlogscripts
```

WEM IP Address Change Procedure

In the event the customer's network evolves, the IP address of the WEM server might be required to change from the existing one. In order to change the WEM server IP address, use the following defined IP planning process:

Step 1 Stop the EMS server using the following command:

```
./serv stop
```

Step 2 Change the interface IP address using the ifconfig command. For example:

```
ifconfig bge0 192.168.1.1 netmask 255.255.255.0 up
```

Step 3 Change the new IP address in the nms.cfg file of the WEM configuration. For this, use the vi editor as follows:

```
vi nms.cfg
```

Replace the IP address with the new IP address in the modify serverIpAddress field. For example:

```
ServerIpAddress = 192.168.1.1
```

Save the file after making the appropriate changes.

Step 4 Modify the host file of the WEM server using following commands:

```
# cat /etc/hosts

<IP address> localhost

<new_IP_address> solaris_hostname

#
```

Step 5 Start the WEM server after these settings changes using the following command:

```
./serv start
```

Important: */etc/netmasks* needs to be modified if the user is subnetting existing address and subsequently using a different network mask than the default one. If the netmask being used for a given IP address is a default one, then there is no need to modify this file.

Appendix B
WEM High Availability Redundancy Installations

Systems that rely on running Web Element Manager on a single server to manage their networks face the possibility of service disruption should the server fail. By using Oracle Clusterware or Symantec Veritas software, it is now possible to create redundant Web Element Manager servers with a primary host server running an active instance of Web Element Manager, and a redundant server in standby mode. This appendix provides information to help you successfully configure redundant instances of Web Element Manager over multiple servers. This appendix works closely with the *Installing the WEM Software* and the *WEM Port and Hardware* chapters in this guide.

Important: Oracle Clusterware is supported on the Solaris operating system; however, Veritas is supported on Solaris and RHEL. During the installation process a radio button is provided to choose the required software.

Configuring High Availability Redundancy Using Solaris Cluster Software

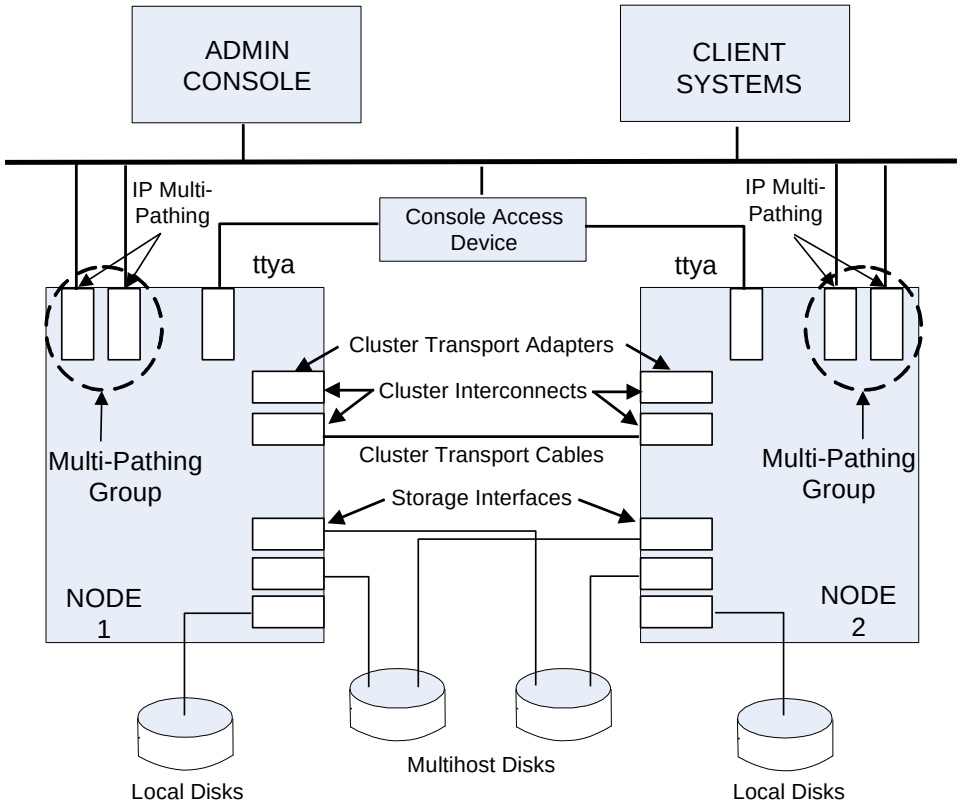
This section describes the installation, configuration and upgrade procedures for High Availabilty on servers using the Solaris OS. You should also refer to the Solaris documentation. In any situation where this guide appears in conflict with the oficial Solaris documentation, the Solaris documentation shall take precedence.

System Requirements

Requirements for implementing High Availability are as follows:

Web Element Manager must be installed on a minimum of two Sun Netra™ T5220 servers equipped with the hardware described in the *Server Hardware Requirements* section of this guide.

We recommend a cluster installation restricted to two servers configured similar to that shown in the diagram below. The sample configurations for Oracle Cluster assume such an installation.



Important: Ensure you have installed the latest version of Oracle Solaris software and all appropriate software patches as described in the Operating System Requirements section.

IPMP is a feature supported on Oracle Solaris. For more complete configuration information, refer to *Configuring IPMP for WEM Server* and also to the Oracle product documentation.

Oracle Solaris Cluster is a feature provided and supported by Oracle. For more complete information on configuring Resource Groups, refer to the Oracle Solaris Cluster product documentation.

Installing Web Element Manager for Failover Mode

This section specifies the configuration changes required when installing WEM in Failover Mode rather than Standalone Mode when following the installation instructions in the *Installing the WEM Software* chapter. For this release, please use the GUI to perform the installation rather than the command line.

Important: Install and configure Web Element Manager in Failover Mode on **both** servers before configuring a cluster resource group.

The following items are either different from, or prerequisites for, the installation steps defined in the *Installing the WEM Software* chapter:

- Create a file directory path <*ems_dir*> or use the default path: */users/ems.*
- The logical hostname and a floating IP address shared between the two nodes must be configured in */etc/hosts*. Ems-Service is used as the logical hostname in the examples in the rest of this appendix.
- Create the global disk path for a shared data directory, for example: */shareddir/ems-share.*

Important: The following options are **not** set when installing in Failover Mode:

- WEM Service started by default and monitored by Process Monitor. (See the *WEM Process Monitor* chapter for more information on processes.)
- Start EMS on machine start-up.

Creating and Configuring a Cluster Resource Group

This section explains how to create a Resource Group specifically for WEM servers in this cluster and configure it appropriately.

Important: This process is configured on only one server in the cluster. It is reflected on both.

Creating a Resource Group

The following describe how to create a Resource Group.

We recommend the cluster binary path is set in the shell environment as this means you can execute the cluster commands from any directory path.

Before **`clsetup`** can create a network resource for any logical hostname, that hostname and a common floating IP address associated with it must be specified in the */etc/hosts* directory on both servers. This example uses *ems-service* as the logical hostname.

Step 1 Login as *root* and run **`clsetup`** to open the Main Menu.

Step 2 From the Main Menu select Option 2: **`Resource Groups`**.

Step 3 From the Resource Groups Menu, select Option 1: **`Create a Resource Group.`**

A resource group is a container into which you can place resources of various types, such as network and data service resources and then manage them. Only failover resource groups can contain network resources. A network resource would include logical hostname.

Step 4 When prompted to create a failover group, enter **`yes`** and select Option 1: **`Create a Failover Group`**. For this example, call the group *ems-rg*.

Step 5 When you are prompted to select a preferred server enter **`yes`** and enter the name of the Preferred server; for this example use *Node1*. Enter **`yes`** to continue the update.

The screen will display the following message:

```
clresourcegroup create -n <Node-1 Node Name> <Node-2 Node Name> ems-rg

Command completed successfully.
```

With the Resource Group created successfully, you can move on to the next step and add the logical hostname.

Adding a Logical Hostname to a Failover Resource Group

Follow steps 1 - 5 to add a logical hostname.

Step 1 After the confirmation screen from the last task displays, press **`Enter`** to continue. Enter **`yes`** when prompted to add network resources.

Step 2 From the Network Resources Menu, select Option 1: **`Add a Logical Hostname`**.

If a failover resource group contains logical hostname resources, the most common configuration is to have one logical hostname resource for each subnet. Enter **1** to create a single resource.

Step 3 When prompted for a logical hostname, enter the logical hostname configured in /etc/hosts for the floating IP address, For this example use *ems-service*.

Step 4 Press **Enter** to continue. The screen displays:

```
clreslogicalhostname create -g ems-rg -p R_description="LogicalHostname
resource for ems-service" ems-service
```

Step 5 Enter **no** when prompted to add any additional network resources.

Adding a Data Service Resource

Follow steps 1 - 4 to add a data service.

Step 1 After the logical hostname confirmation screen, enter **yes** when prompted to begin adding data services.

Step 2 From the Data Services Menu select Option 1: **EMSSCFO Server for Sun Cluster,** and use the name *ems-dsr* for this example.

The screen displays the following message:

```
This data service uses the "Port_list" property. The default "Port_list" for this
data service is as follows: <NULL>
```

Step 3 Enter **no** when prompted to override the default.

Step 4 Enter **no** when prompted to add more properties, then enter **yes** to continue.

The screen displays the following message:

```
Commands completed successfully
```

Bringing the Resource Group Online

Follow steps 1 - 2 to bring the Resource Group online.

Step 1 After the completion confirmation screen, press **Enter** to continue. Enter **no** when prompted to add any additional data service resources. Enter **yes** when prompted to manage and bring this resource group online.

The screen displays the following message:

```
clresourcegroup online -M ems-rg

Commands completed successfully
```

Step 2 Press **Enter** to continue, then select Option **q** to **Quit** and return to the Main Menu.

The process is now complete. At this point you can enter the **scstat** command to display the current online/offline status if required.

Upgrading Web Element Manager in a Clustered Environment

This section describes the process for upgrading Web Element Manager in a two-server cluster.

Important: Network administrators are advised that they should have any connected clients log out at this time. If clients cannot reconnect after the upgrade, please refer to the *Troubleshooting* appendix for information on any Java-related errors.

Prerequisite Steps for the Upgrade Process

For the example configuration that follows you should confirm the following:

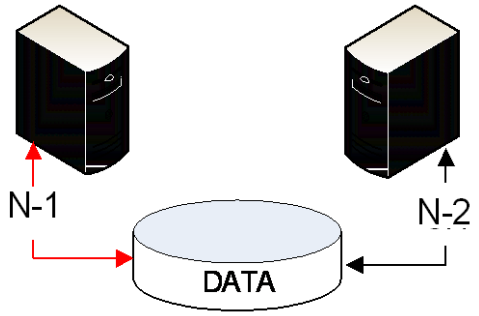
- The same version of Web Element Manager software (12.0 or newer) has been installed on both servers and configured in Failover Mode.
- Config files and scripts are identical.
- Devices can be failed over with no loss in connectivity.

  This can be confirmed either by a software switchover, or by running the **`scstat`** command to confirm the current node status.
- Resources have been configured in the Oracle Solaris Cluster software using the following *example names*:
  - Two Cluster Nodes: *N-1* (initially this is the active node) and *N-2* (initially this is the redundant node).
  - A Resource Group managed by Web Element Manager exists. *ems-rg* is used for this example.
  - A logical hostname and floating (shared) IP address has been configured on both servers. This example uses the default */etc/hosts* folder. Use *ems-service* as the hostname for this example.

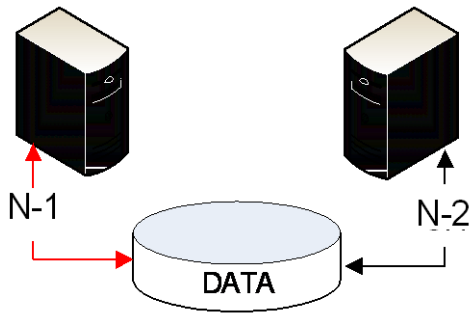
Upgrade Process Overview

This section provides a broad overview of the procedures to follow.

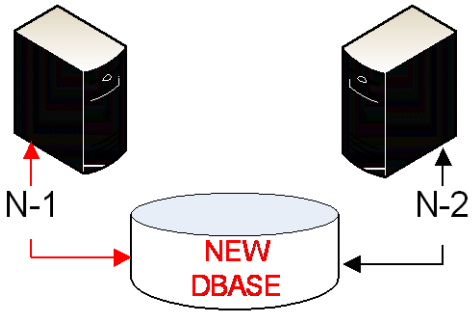
Step 1 Start with two server nodes: *N-1* and *N-2*. They share both data files and database information. *N-1* is currently active and *N-2* is currently in standby mode, as shown below:



Step 2 With Web Element Manager running on *N-1*, put *N-2* into maintenance mode (this is described in Removing an Inactive Node from the Resource Group below). Then upgrade WEM to version 12.0 or later.



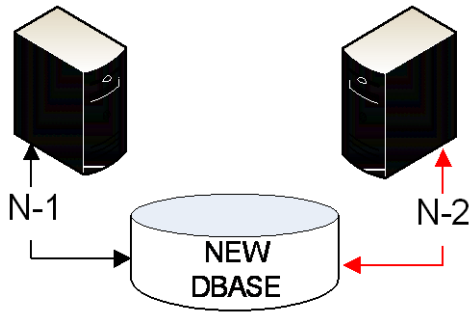
At this point, the database is not yet updated. In cluster mode, when WEM is upgraded on *N-2* the postgres database is **not** started. so a new DB schema is not created. This is because the schema will be updated through the currently active server *N-1* with SQL scripts that are provided as part of the installation package; this is explained in the section *Updating the Databases*. At this point *N-2* is still in maintenance mode but now with updated WEM software, and the database schema has now been updated as shown below:



Step 3 To prepare for the switchover, take *N-2* out of maintenance mode.

Step 4 To upgrade WEM on *N-1*, bring *N-2* back into the cluster and do a switchover from *N-1* to *N-2* so now *N-2* is the active host and WEM starts running processes.

Step 5 Now place the formerly active node *N-1* into maintenance mode and upgrade WEM software while *N-2* is the active node as shown below:



Step 6 Once the upgrade is complete, *N-1* can be switched back to its role of active node if necessary by using the Cluster commands, or *N-2* can continue as the active node.

Important: Refer to the *Installing the WEM Software* chapter for more complete information about scripts and files. All configuration files placed in the *<EMS_HOME>/server/etc* folder and the script files in the *<EMS_HOME>/server/scripts* folder must be identical. This ensures that after the switch between servers, the behavior of EMS does not change in any way.

Removing an Inactive Node from the Resource Group

Complete the following steps to remove *N-2* from the Resource Group. Since the cluster resource group configuration will be same for both nodes, the cluster-related commands can be run on either node.

Step 1 Run the **`scstat`** command. **`scstat`** is used to verify the current status of the cluster resource group and ensures that on switchover/failover the servers will switch correctly. The following screen display reflects a properly configured cluster:

```
Two cluster nodes: Online

Two cluster transport paths: Online

Quorum votes by node: Online

Quorum votes by device: Online

Resource Groups and Resources: ems-rg, ems-service, ems-dsr

Ems-rg group N-1: Online N-2: Offline

IPMP groups: Online
```

Important: *N-2* must **not** be allowed to run any WEM processes. This prevents the secondary node from taking ownership of resources. Removing it from the Resource Group prevents a failover from happening and *N-1* continues to behave like a standalone WEM thus ensuring a successful upgrade. To do this:

Step 2 Enter **`clsetup`** to open the Main Menu and select Option 2: **`Resource Groups Menu`**.

Step 3 From the Resource Groups menu, select Option 8: **`Change the Properties of a Resource Group`**.

Step 4 Enter **`yes`** when prompted to continue.

Step 5 Select the group to be changed by selecting Option 1: *ems-rg*.

Step 6 Select Option 1: **`Change the Nodelist Resource Group Properties`**

Step 7 Enter **`yes`** when prompted to continue. Both *N-1* and *N-2* should now appear in the nodelist.

Step 8 Select Option 2: **`Remove a Node from the Nodelist`**, then select Option 1 to remove *N-2*.

The nodelist now contains only *N-1*. When prompted to update the nodelist property, enter **`yes`**. If your update was successful you will see the following screen confirmation:

```
command completed successfully
```

Press **Enter** to continue. You will receive confirmation that only *N-1* remains in the nodelist. Select Option **q** to **Quit** and exit back to the Resource Group Menu.

Step 9 From the Resource Group Menu select Option **s**: **Show Current Status** to confirm the current network resources if required.

Upgrading WEM on the Inactive Server

Complete the following steps to upgrade WEM on the inactive server, *N-2*.

Step 1 Web Element Manager begins installing along with Apache Server, PostgreSQL Server, and EMS Server. Installation continues until the following warning message appears:

```
Updating PostgreSQL config file...This is an upgrade in Cluster mode; not
updating postgres config.
```

This message is normal because the database is to be updated from the active server, *N-1*.

Step 2 With the installation complete, select Option 3 to finish.

Updating the Databases

Complete the following steps to update the databases from node *N-1*.

Step 1 Copy the sqlfiles.tar file from the N-2 installation to a folder on *N-1* and untar the file. This process is described fully in the *Installing the WEM Software* chapter.

This will create a folder called *sqlfiles*.

Step 2 Go to the *sqlfiles* folder and run *dbClusterUpgrade.sh.*

Step 3 At the prompt, enter the EMS directory name and press **Enter**.

Step 4 Enter a complete directory path for saving the new SQL files and press **Enter**.

Step 5 Enter the postgres administrator name assigned during the installation process. This is *postgres* by default.

Step 6 Press **Enter**.

Step 7 Enter the database port number and press **Enter**.

Important: Currently, this is port 5432, but this may change in a later release.

Step 8 The databases update and the screen displays the following message:

```
Database schema upgraded successfully...
```

Returning the Inactive Node to the Resource Group

Complete the following steps to return *N-2* to the Resource Group and take over resource ownership in order to upgrade the software on *N-1*.

Step 1 Run **`clsetup`** and then log in to access the Main Menu and select Option 2: **`Resource Groups`**.

Step 2 From the Resource Groups Menu select Option 8: **`Change the Properties of a Resource Group`**.

Step 3 Enter **`yes`** when prompted to continue.

Step 4 From the next screen select the Resource Group name.

Step 5 When prompted for the property to change, select Option 1: **`Nodelist`**.

Step 6 Enter yes to continue and open the next screen.

Step 7 Select Option 1: **`Add a Node/Zone to the Top of the Nodelist`**.

Step 8 Select Option 1: **`N-2`**.

Step 9 Enter **`yes`** when prompted to update the nodelist property.

The screen will display the following message:

```
Command completed successfully.
```

Step 10 Press **`Enter`** to continue and select Option **`q`** to **`Quit`** and return to the Resource Groups Menu.

Switching Active Servers

Complete the following steps to make *N-2* the active node so *N-1* can be updated.

Step 1 From the Resource Group Menu Select Option 5: **`Switch over a Resource`**.

Step 2 Scroll through the on-screen description and enter **`yes`** to continue.

Step 3 Select the name of the resource group. In this example it would be *ems-rg.*

Step 4 Select Option 1: **`Switch Group Ownership`**.

Step 5 Select the node to take ownership of *ems-rg,* which would be *N-2*. Enter **`yes`** to confirm. The screen will display the following message:

```
Command completed successfully.
```

Step 6 Press **`Enter`** to continue and select Option **`q`** to **`Quit`** and return to the Resource Group Menu.

Step 7 From the Resource Group Menu select Option **`s Show Current Status`**. This shows that *N-2* is now online and *N-1* is offline.

At this point return to Removing an Inactive Node from the Resource Group and begin the update process for *N-1*.

Important: Since the database schema were previously updated and both *N-1* and *N-2* share the same database, it is **not** necessary to run the SQL scripts again for *N-1*.

High Availability Mode Using Veritas Cluster Software (VCS)

This section provides instructions specific to a Symantec VCS installation to provide redundancy to multiple WEM servers. This software is documented by Symantec, and you will also need to refer to the Install, the Uninstall, and the Upgrade chapters in this guide. Server hardware requirements are in the*WEM Port and Hardware Information* chapter.

Important: Veritas Cluster is supported on both Sun servers using the Solaris Operating System and Cisco UCS servers using the RHEL OS. The VCS installation in this section is directed to installments on the RHEL platform. The VCS itself has a lot in common with the Solaris installation in the previous chapter; however, IPMP is proprietary software and supported only on the Solaris OS. A radio button on the installation screen allows the choice between a Solaris or a RHEL installation; for this reason, please use the GUI to perform the installation rather than the command line.

Important: There are configuration changes required when installing WEM in Failover Mode rather than Standalone Mode. These re described in the *Installing the WEM Software* chapter. For this release, please use the GUI to perform the installation rather than the command line.

Installation

Refer to the relevant documentation to install the appropriate operating system on the servers.

Refer to the VCS documentation for the following steps:

1. Install the the Storage Foundation and Cluster Server software.
2. Configure the Diskgroup, Volume and Mount Resource Groups for creating and mounting the shared-disk.

   There is an example of a valid *Main.cf* configuration below

   These resources need to be online when installing the WEM application on each node. WEM will be part of the 'Application resource' and its status is monitored with the PID file of psmon (Monitor server). In case of WEM application resource failure, VCS will first try to restart WEM on the same node before switchover to the standby node.
3. Mount the shared disk on the first cluster node.
4. Start installing the WEM application on the first cluster node using the instructions in the *Installing the WEM Software* section in this guide.

   Important: Make certain that the WEM application does not start after the installation is complete.
5. Unmount the shared disk from the first cluster node and install it on the second node.
6. Start the WEM installation on the second cluster node. Make sure that you provide the same parameters during installation that were used for the first installation.
7. Refer to the VCS documentation and start configuring resource groups and resources. A sample of the *Main.cf* file follows:

Main.cf File Configuration Example

The following is an example of the main.cf file for resource-groups and resources.

```
group wemFailover (
       SystemList = { pnstextappsucs1 = 0,
pnstextappsucs3 = 1 }        AutoStartList = { pnstextappsucs3 }
      )

Application wemService
(                StartProgram = "/users/ems/postgres//bin/emsctl
start"               StopProgram = "/users/ems/postgres//bin/emsctl
forcestop"               PidFiles = { "/users/ems/server/psmon.pid" }
              RestartLimit = 1               )

   DiskGroup wemDG (
              DiskGroup = wemdg               )

   IP wemIP (
         Device = eth0               Address = "10.4.83.151"
              NetMask = "255.255.255.0"
 )

 Mount wemMount (
             MountPoint = "/apps/wem/"
               BlockDevice = "/dev/vx/dsk/wemdg/wemvol"
               FSType = vxfs               FsckOpt = "-y"
            )

NIC wemNIC (
        Device = eth0               )

 Volume wemVolume (
               DiskGroup = wemdg               Volume = wemvol
            )
```

wemIP requires wemNIC wemMount requires wemVolume wemService requires wemIP wemService requires wemMount wemVolume requires wemDG

// resource dependency tree // // group wemFailover // { // Application wemService // { // IP wemIP // { // NIC wemNIC // } // Mount wemMount // { // Volume wemVolume // { // DiskGroup wemDG // } // } // } // }

Upgrading WEM with VCS

The process for upgrading WEM installed in HA mode with VCS is similar to the Sun Cluster upgrade process described earlier.

With VCS, in order to disable the resource on the standby node, you have to set the resource-group's Disable attribute for the standby node (system). This ensures that the resource group does not failover in between the upgrade and result in any sort of data corruption.

1. Use the following command to disable a cluster resource group:

   $ hagrp -disable <resource-group name> -sys <node2>

2. Use the following command to switch the resource group from one node to another:

   $ hagrp -switch <resource-group name> to <system>

Uninstalling WEM with VCS

Use the following steps to uninstall WEM in redundant mode.

1. Disable the resource on the standby node.

   This will make sure that the resource group does not failover during the uninstall process and result in any sort of data corruption.

   ```
   $ hagrp -disable <resource group name> -sys <node2>
   ```

2. Set the 'Critical' attribute of wem-service resource to '0'

   ```
   $ hares -modify <resource-name> Enabled 0
   ```

3. Enable the resource on the standby node and disable it on current active node.

   This will make sure that the resource group does not failover during the uninstall and result in any sort of data corruption.

   ```
   $ hagrp -enable <resource group name> -sys <node2>
   $ hagrp -disable <resource group name> -sys <node1>
   ```

4. Switchover the resource group to Standby Node.
5. Uninstall WEM from the Standby Node.

Appendix C
WEM Configuration File Parameters

This appendix provides information about the configuration file parameters pertaining to the Web Element Manager. WEM provides a number of configuration files (.cfg and .xml files) which can be modified to fine-tune the operation of the application. These files are located in the */<ems_dir>/server/etc* directory by default.

The following configuration files have been deprecated from WEM:

- fmcorelation.cfg
- description.cfg
- dbphy.cfg
- dblog.cfg

This chapter provides information on the following configuration files:

- The temip.cfg File
- The thr.cfg File
- The ua.cfg File
- The vacuum.cfg File
- The wblist.cfg File
- The menu.xml File

Important: Unless otherwise specified, all information in this chpater applies to both Sun Solaris- and RHEL-based WEM systems.

The alarmid.cfg File

This file provides parameters pertaining to the configuration of SNMP alarms received from managed devices.

Important: This configuration file is customer-specific and is not operational without the appropriate license. Please contact your local sales representative for additional information.

The audio.cfg File

This file provides alarm severity associations to specific audio files. The audio files are in .WAV format and are played by the Web Element Manager when an alarm/trap of that severity is received. Additionally, this file can be used to associate an audio file to a specific alarm for further customizing.

The following table describes the **AUDIO** file parameters.

Table 26. audio.cfg File Parameters

Parameters		
AUDIO: This file contains the mapping of the alarm severity level and the corresponding audio file to be played when an alarm is received. The first field contains the severity level (number): The nth row in the SEVERITY section is n-1 in the *fm.cfg* file. Please use the *fm.cfg* file for the severity configuration information in detail. The second field contains the audio file name. The audio files are present in the **audio** sub-directory in the client installation directory. The format is as follows: Severity Number = WAV File Path For example: 1 = Blank Line - This means that no audio file is to be played when a first level (Indeterminate) severity alarm is received. 3 = audio/chord.wav - This means that the audio/chord.wav file is to be played when a third level (Major) severity alarm is received.		
audioPlayedFor: This option will decide the priority of alarm to play an audio. The default value is 0. Valid configurables are: 0 - Only chassis audio will be played as per severity and no audio will be played for WEM alarm. 1 - Audio for chassis and WEM will be played but severity will be given to chassis alarms. 2 - Audio for chassis and WEM will be played but first priority will be based on device and severity. 3 - Audio will be played strictly based on the severity.		
Severity No.	**Severity Name**	**Audio Filename**
1	Critical	1 = audio/notify.wav
2	Major	2 = audio/ding.wav
3	Minor	3 = audio/chord.wav
4	Warning	4 = audio/Alarmrng.wav

The following table describes the **TRAPAUDIO** file parameters.

Table 27. TRAPAUDIO File Parameters

Parameters

Parameters	
TRAPAUDIO: This section defines the mapping for Trap Number and the corresponding AUDIO file. This file is the default file to be played when the trap is received. If the filename field is kept empty then, the file associated with the severity of the trap will be played. Severity-AudioFilename relationship is defined in the AUDIO section. The format is as follows: Trap Number = File Path For example: 1 = This suggests that no audio file is associated with trap #1. So, the file associated with its severity will be played. 3 = audio/test01.wav - This file will be played whenever trap #3 comes.	
Trap Number	**Trap Name**
Generic Alarms	
1-1	coldStart
1-2	warmStart
1-3	linkDown
1-4	linkUp
1-5	authenticationFailure
1-6	egpNeighborLoss
Enterprise Alarms	
2-1(etc)	***Important:*** A complete and updated list of all traps, including name, number and severity is documented in the "Default Traps and Severities" chapter in the appropriate Cisco SNMP MIB Guide.

The blacklist.cfg File

This file contains the flag that is set to enable or disable the blacklisting feature in WEM. The file provides parameters for specifying information such as blacklist backup limit, time interval to poll the blacklist directory, and so on.

Table 28. blacklist.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
BLACKLIST: This section describes parameters that store information related to blacklisting.				
EnableBlackListFeature	Flag to enable/disable the blacklisting feature in WEM. Setting this flag to 1 will enable the blacklisting feature in WEM. Needs a WEM Server restart. Values: 1: Enable 0: Disable	--	--	0
BlacklistBackupLimit	Number of Blacklist backups to be maintained.	5	15	10
ExportBLtoCDPInterval	BlackList files Export interval. This specifies the time interval in hours for Content Filtering Server to export OPTCMDB-BL to CDP.	1 hr	5 hrs	2 hrs
BlPollInterval	BlackList directory poll interval. This specifies the time interval in minutes to poll the Blacklist directory.	5	60	15
EnableDNSLookup	Flag to enable/disable the DNS lookup functionality. Setting this flag to 1 will enable the DNS lookup functionality. Values: 1: Enable 0: Disable	--	--	0
ThreadPoolSize	Thread pool size.	1	10	5
NCMEC:				
EnableNCMEC	Flag to enable/disable the import of cumulative.csv from NCMEC. Setting this flag to 1 will enable the import of cumulative.csv from NCMEC. Values: 1: Enable - import cumulative.csv from NCMEC 0: Disable - assume cumulative.csv will be available in *<EMS ServerPath>/flash/blacklist/blacklist/* ***Important:*** Do not change the value of configurable as functionality when this flag 0 is disabled	--	--	1
NCMECUrl	This specifies the cumulative.csv file path at NCMEC.	--	--	--

Key	Description	Minimum Value	Maximum Value	Default Value
NCMECAuthUserName	This specifies the username required for authentication at NCMEC site.	--	--	--
NCMECAuthPassword	This specifies the password required for authentication at NCMEC site.	--	--	--
BlacklistImportInterval	This specifies the cumulative.csv file import interval (in hours).	1	168 (one week)	24 (one day)
BlacklistReImportInterval	This specifies the cumulative.csv file re-import interval (in minutes).	1	30	5
BLThreadPoolSize	Specifies the blacklist thread pool size.	5	20	10

The bs.cfg File

This file provides bulk statistic configuration information pertaining to schemas, formatting, and parameters for specifying time tolerances for searching bulk statistic records. This is a multi-section server configuration file for bulkstat module.

Important: Any change in the configuration files will restart the server resulting in client restart.

Caution: To ensure proper operation of the Web Element Manager, bulk statistic schema and formatting configuration in this file should not be altered.

Table 29. bs.cfg File Parameters (Schemas)

Key	Description	Default Value in Config File
Schema: This section provides the schema format string for each subsystem. The parameter values in this section are internally used by the bulkstat server module and should not be changed.		
Card Sch	Card Schema	EMS,Card,%date%,%time%,%card%,%cpubusy%,%cpuidle%,%numproc%,%memused%,%memtotal%,%numcpu%,%cpu0-cpubusy%,%cpu0-cpuidle%,%cpu0-numproc%,%cpu0-memused%,%cpu0-memtotal%,%cpu0-cpuused-user%,%cpu0-cpuused-sys%,%cpu0-cpuused-io%,%cpu0-cpuused-irq%,%cpu0-cpuused-idle%,%cpu1-cpubusy%,%cpu1-cpuidle%,%cpu1-numproc%,%cpu1-memused%,%cpu1-memtotal%,%cpu1-cpuused-user%,%cpu1-cpuused-sys%,%cpu1-cpuused-io%,%cpu1-cpuused-irq%,%cpu1-cpuused-idle%,%cpu2-cpubusy%,%cpu2-cpuidle%,%cpu2-numproc%,%cpu2-memused%,%cpu2-memtotal%,%cpu2-cpuused-user%,%cpu2-cpuused-sys%,%cpu2-cpuused-io%,%cpu2-cpuused-irq%,%cpu2-cpuused-idle%,%cpu3-cpubusy%,%cpu3-cpuidle%,%cpu3-numproc%,%cpu3-memused%,%cpu3-memtotal%,%cpu3-cpuused-user%,%cpu3-cpuused-sys%,%cpu3-cpuused-io%,%cpu3-cpuused-irq%,%cpu3-cpuused-idle%,%15avg-cpubusy%,%15peak-cpubusy%,%5avg-cpubusy%,%5peak-cpubusy%,%1avg-cpubusy%,%15avg-memused%,%15peak-memused%,%5avg-memused%,%5peak-memused%,%1avg-memused%,%cpu0-15avg-cpubusy%,%cpu0-15peak-cpubusy%,%cpu0-5avg-cpubusy%,%cpu0-5peak-cpubusy%,%cpu0-1avg-cpubusy%,%cpu0-15avg-memused%,%cpu0-15peak-memused%,%cpu0-5avg-memused%,%cpu0-5peak-memused%,%cpu0-1avg-memused%,%cpu1-15avg-cpubusy%,%cpu1-15peak-cpubusy%,%cpu1-5avg-cpubusy%,%cpu1-5peak-cpubusy%,%cpu1-1avg-cpubusy%,%cpu1-15avg-memused%,%cpu1-15peak-memused%,%cpu1-5avg-memused%,%cpu1-5peak-memused%,%cpu1-1avg-memused%,%cpu2-15avg-cpubusy%,%cpu2-15peak-cpubusy%,%cpu2-5avg-cpubusy%,%cpu2-5peak-cpubusy%,%cpu2-1avg-cpubusy%,%cpu2-15avg-memused%,%cpu2-15peak-memused%,%cpu2-5avg-memused%,%cpu2-5peak-memused%,%cpu2-1avg-memused%,%cpu3-15avg-cpubusy%,%cpu3-15peak-cpubusy%,%cpu3-5avg-cpubusy%,%cpu3-5peak-cpubusy%,%cpu3-1avg-cpubusy%,%cpu3-15avg-memused%,%cpu3-15peak-memused%,%cpu3-5avg-memused%,%cpu3-5peak-memused%,%cpu3-1avg-memused%,%task-sessmgr-num%
Card Sch2	Card 2 Schema	EMS,Card2,%date%,%time%,%card%,%task-sessmgr-avgcpu%,%task-sessmgr-avgmem%,%task-sessmgr-maxcpu%,%task-sessmgr-maxmem%,%task-a11mgr-num%,%task-a11mgr-maxcpu%,%task-a11mgr-maxmem%,%task-l2tpmgr-num%,%task-l2tpmgr-maxcpu%,%task-l2tpmgr-maxmem%,%task-famgr-num%,%task-famgr-maxcpu%,%task-famgr-maxmem%,%task-hamgr-num%,%task-hamgr-maxcpu%,%task-hamgr-maxmem%,%task-acsmgr-num%,%task-acsmgr-avgcpu%,%task-acsmgr-avgmem%,%task-acsmgr-maxcpu%,%task-acsmgr-maxmem%,%task-vpnmgr-num%,%task-vpnmgr-maxcpu%,%task-vpnmgr-maxmem%

Key	Description	Default Value in Config File
PortSch	PortSchema	EMS,Port,%date%,%time%,%card%,%port%,%rxbytes%,%txbytes%,%ucast_inpackets%,%ucast_outpackets%,%mcast_inpackets%,%mcast_outpackets%,%bcast_inpackets%,%bcast_outpackets%,%rxpackets%,%txpackets%,%rxdiscbytes%,%rxdiscpackets%,%txdiscbytes%,%txdiscpackets%,%maxrate%,%frag-rcvd%,%pkt-reassembled%,%frag-tokernel%,%util-rx-curr%,%util-tx-curr%,%util-rx-5min%,%util-tx-5min%,%util-rx-15min%,%util-tx-15min%
PDSNSystemSch	PDSNSystemSchema	EMS,PDSNSystem,%date%,%time%,%sess-ttlarrived%,%sess-ttlrejected%,%sess-ttlconnected%,%sess-ttlauthsucc%,%sess-ttlauthfail%,%sess-ttllcpup%,%sess-ttlipcpup%,%sess-ttlsrcviol%,%sess-ttlkeepfail%,%sess-curttlcalls%,%sess-cursipconn%,%sess-curmipconn%,%sess-curactcall%,%sess-curdormcall%,%sess-curarrived%,%sess-curlcpnegot%,%sess-curlcpup%,%sess-curauth%,%sess-curauthed%,%sess-curipcpup%,%sess-curdisc%,%a11-ttlarrived%,%a11-ttlrejected%,%a11-ttldemult%,%a11-ttldereg%,%a11-curactive%,%fa-ttlarrived%,%fa-ttlrejected%,%fa-ttldemult%,%fa-ttldereg%,%fa-curactive%,%ha-ttlarrived%,%ha-ttlrejected%,%ha-ttldemult%,%ha-ttldereg%,%ha-curactive%,%sess-calldur-1min%,%sess-calldur-2min%,%sess-calldur-5min%,%sess-calldur-15min%,%sess-calldur-1hour%,%sess-calldur-4hour%,%sess-calldur-12hour%,%sess-calldur-24hour%,%sess-calldur-over24hour%,%sess-setuptime-100ms%,%sess-setuptime-200ms%,%sess-setuptime-300ms%,%sess-setuptime-400ms%,%sess-setuptime-500ms%,%sess-setuptime-600ms%,%sess-setuptime-700ms%,%sess-setuptime-800ms%,%sess-setuptime-900ms%,%sess-setuptime-1sec%,%sess-setuptime-2sec%,%sess-setuptime-3sec%,%sess-setuptime-4sec%,%sess-setuptime-6sec%,%sess-setuptime-8sec%,%sess-setuptime-10sec%,%sess-setuptime-12sec%,%sess-setuptime-14sec%,%sess-setuptime-16sec%,%sess-setuptime-over16sec%,%incremental%,%enddate%,%endtime%,%localenddate%,%localendtime%,%sess-ttlfailed%,%uptime%,%uptimestr%,%lic-pdsn%,%lic-ha%,%lic-ggsn%,%lic-l2tplns%,%sess-txbytes%,%sess-rxbytes%,%sess-txpackets%,%sess-rxpackets%,%sess-siptxbytes%,%sess-siprxbytes%,%sess-miptxbytes%,%sess-miprxbytes%,%aaa-ttlreq%,%aaa-curreq%,%aaa-ttlauthreq%,%aaa-curauthreq%,%aaa-ttlauthprobe%,%aaa-curauthprobe%,%aaa-ttlacctreq%,%aaa-curacctreq%,%aaa-ttlauthsucc%,%aaa-ttlauthfail%,%aaa-ttlauthpurged%,%aaa-ttlauthcancelled%,%aaa-ttlauthdmuchal%,%aaa-ttlradauthreq%,%aaa-curradauthreq%,%aaa-ttlradauthreqretried%,%aaa-ttllclauthreq%,%aaa-curlclauthreq%,%aaa-ttlpseudoauthreq%,%aaa-curpseudoauthreq%,%aaa-ttlauthnulluser%,%aaa-ttlacctsucc%,%aaa-ttlacctpurged%,%aaa-ttlacctcancelled%,%aaa-ttlradacctreq%,%aaa-ttlradacctreqretried%,%disc-reason-summary%,%sess-curaaaactive%,%sess-curaaadeleting%,%sess-curaaaacctpending%,%sess-ttlemptyfwd%,%sess-ttlemptyrev%,%sess-ttlonlineprepaiderr%,%sess-ttlprepaidinitautherr%,%sess-ttlcrprpattempt%,%sess-ttlcrprpsuccess%,%sess-ttlrpcrpattempt%,%sess-ttlrpcrpsuccess%,%sess-curpmipconn%,%sess-curl2tplacconn%,%sess-curalwayson%,%sess-curbcmcsauth%,%sess-curbcmcsconn%,%sess-curhaipsecconn%,%sess-curl2tplacconnecting%,%sess-curpdptypeipconn%,%sess-curpdptypepppconn%,%sess-curprepaid%,%sess-rxpkt-1023%,%sess-rxpkt-127%,%sess-rxpkt-16%,%sess-rxpkt-2047%,%sess-rxpkt-255%,%sess-rxpkt-4095%,%sess-rxpkt-4500%,%sess-rxpkt-511%,%sess-rxpkt-64%,%sess-rxpkt-over4500%,%sess-ttldisconn%,%sess-ttlhandoff%,%sess-ttlonlineauthfail%,%sess-ttlonlineauthreq%,%sess-ttlonlineauthsucc%,%sess-ttlprepaid%,%sess-ttlproxydns-drop%,%sess-ttlproxydns-passthru%,%sess-ttlproxydns-redirect%,%sess-ttlrenewal%,%sess-txpkt-1023%,%sess-txpkt-127%,%sess-txpkt-16%,%sess-txpkt-2047%,%sess-txpkt-255%,%sess-txpkt-4095%,%sess-txpkt-4500%,%sess-txpkt-511%,%sess-txpkt-64%,%sess-txpkt-over4500%,%aaa-ttlauthkeepalive%,%aaa-curauthkeepalive%,%aaa-ttlacctkeepalive%,%aaa-curacctkeepalive%,%aaa-ttlauthkeepalivesuccess%,%aaa-ttlauthkeepalivefailure%,%aaa-ttlauthkeepalivepurged%,%aaa-ttlacctkeepalivesuccess%,%aaa-ttlacctkeepalivetimeout%,%aaa-ttlacctkeepalivepurged%,%ipsg-total-call-arrived%,%ipsg-total-call-rejected%,%ipsg-total-call-demult%,%ipsg-total-dereg-rep-sent%,%ipsg-cur-active-call%,%ipsg-total-active-serv%

Key	Description	Default Value in Config File
PDSNSystemSch2	PDSN 2 System Schema	EMS,PDSNSystem2,%date%,%time%,%asngw-cur-active-call%,%asngw-total-sess-setup%,%asngw-retriesexhaust%,%asngw.sfs%,%asngw.tidfail%,%asngw-handoffattempt%,%asngw-handoffdenied%,%asngw-handoffcomp%,%asngw.authsucc%,%asngw-authfailures%,%sess-ttlcallop%,%sess-curnonanchorconn%,%sess-curdhcppending%,%sess-ttlinterasngwattempt%,%sess-ttlinterasngwsuccess%,%sess-ttlintraasngwattempt%,%sess-ttlintraasngwsuccess%,%sess-ttlconnected-1xrtt%,%sess-txbytes-1xrtt%,%sess-rxbytes-1xrtt%,%sess-txpackets-1xrtt%,%sess-rxpackets-1xrtt%,%sess-ttlconnected-evdorev0%,%sess-txbytes-evdorev0%,%sess-rxbytes-evdorev0%,%sess-txpackets-evdorev0%,%sess-rxpackets-evdorev0%,%sess-ttlconnected-evdoreva%,%sess-txbytes-evdoreva%,%sess-rxbytes-evdoreva%,%sess-txpackets-evdoreva%,%sess-rxpackets-evdoreva%,%flow-ttlestab%,%flow-ttldisconn%,%flow-curdynamic%,%pdif-cursess%,%pdif-curactive%,%pdif-curdormant%,%pdif-ttlsetup%,%sess-15peak-curactcall%,%sess-15peak-curttlcall%,%sess-cursipactive%,%sess-15peak-cursipactive%,%sess-curmipactive%,%sess-15peak-curmipactive%,%a11-15peak-curactive%,%crp-curactive%,%crp-15peak-curactive%,%fa-15peak-curactive%,%ha-15peak-curactive%,%flow-15peak-curdynamic%,%sess-15min-usageactive%,%sess-15min-usageall%,%cc-cursess%,%cc-ttlecsadd%,%cc-ttlstart%,%cc-ttlsessupd%,%cc-ttlterm%,%cc-sessfailover%,%cc-msg-recv%,%cc-msg-sent%,%cc-msg-request%,%cc-msg-answer%,%cc-msg-ccrinit%,%cc-msg-ccainit%,%cc-msg-ccainitaccept%,%cc-msg-ccainitreject%,%cc-msg-ccainittimeout%,%cc-msg-ccrupdate%,%cc-msg-ccaupdate%,%cc-msg-ccaupdatetimeout%,%cc-msg-ccrfinal%,%cc-msg-ccafinal%,%cc-msg-ccafinaltimeout%,%cc-msg-asr%,%cc-msg-asa%,%cc-msg-rar%,%cc-msg-raa%,%cc-msg-ccadropped%,%cc-msgerr-proto%,%cc-msgerr-badanswer%,%cc-msgerr-unknownsess%,%cc-msgerr-unknowncomm%,%cc-msgerr-reqtimeout%
PDSNSystemSch3	PDSN 3 System Schema	EMS,PDSNSystem3,%date%,%time%,%cc-msgerr-parse%,%cc-msgerr-unkratinggrp%,%cc-msgerr-unkrulebase%,%cc-msgerr-unkfailure%,%cc-upd-threshold%,%cc-upd-qht%,%cc-upd-final%,%cc-upd-quotaexhaust%,%cc-upd-validitytime%,%cc-upd-otherquota%,%cc-upd-ratingchange%,%cc-upd-forcedreauth%,%cc-term-diamlogout%,%cc-term-servnotprov%,%cc-term-badanswer%,%cc-term-admin%,%cc-term-linkbroken%,%cc-term-authexpired%,%cc-term-usermoved%,%cc-term-sesstimeout%,%cc-traf-catcreate%,%cc-traf-catdelete%,%cc-traf-catlookup%,%cc-traf-hits%,%cc-traf-misses%,%cc-traf-triggerevent%,%cc-traf-finalunit%,%cc-traf-catsuccess%,%cc-traf-ratingfail%,%cc-traf-servdenied%,%cc-traf-limitreached%,%cc-traf-authreject%,%cc-traf-othererror%,%cf-static-ratereq%,%cf-static-ratesucc%,%cf-static-rateblock%,%cf-static-ratefail%,%cf-static-ratefail-nr%,%cf-static-ratefail-notindb%,%cf-dyn-ratereq%,%cf-dyn-ratesucc%,%cf-dyn-rateblock%,%cf-dyn-ratefail%,%cf-ratereq%,%cf-ratesucc%,%cf-rateblock%,%cf-ratefail%,%ikev2-cursa%,%ikev2-cursainit%,%ikev2-cursaresp%,%ikev2-ttlsa%,%ikev2-ttlsainit%,%ikev2-ttlsaresp%,%ikev2-attempt%,%ikev2-attemptinit%,%ikev2-attemptresp%,%ikev2-rxpacket%,%ikev2-txpacket%,%ikev2-rxoctet%,%ikev2-txoctet%,%ikev2-initfail%,%ikev2-initfail-noresp%,%ikev2-initfail-resp%,%ikev2-invcookie%,%ikev2-nattkeepalive-recv%,%ikev2-nattkeepalive-send%,%ikev2-dpd-recv%,%ikev2-dpd-send%,%ikev2-dpd-recv-reply%,%ikev2-dpd-send-reply%,%ikev2-dpd-timeout%,%ikev2-dpd-disconnect%,%ikev2-dpd-p1rekey%,%lic-combo-phone%,%lic-ecsv2%,%lic-ipservices-gateway%,%lic-evdoreva-pdsn%,%lic-scm-proxyregistrar-ietfrfc3261%,%lic-scm-proxypcscf%,%lic-scm-servingscscf%,%lic-scm-interrogatingicscf%,%lic-asngw%,%lic-asnlr%,%cf-cache-hits%,%cf-cache-misses%,%cf-cache-has-path-hits%,%cf-cache-flushes%,%sess-curimsauthorized%
PDSNSystemSch4	PDSN 4 System Schema	EMS,PDSNSystem4,%date%,%time%,%sess-curimsauthorizing%,%pdif-curchildsa%,%ikev2-ikesadel%,%ikev2-ikesadelrep-recv%,%ikev2-ikesadelrep-sent%,%ikev2-ikesadelreq-recv%,%ikev2-ikesadelreq-sent%,%ipsec-dpd-p1rekey%

Key	Description	Default Value in Config File
GGSNSystemSch	GGSN System Schema	EMS,GGSNSystem,%date%,%time%,%sess-ttlarrived%,%sess-ttlrejected%,%sess-ttlconnected%,%sess-ttlauthsucc%,%sess-ttlauthfail%,%sess-ttllcpup%,%sess-ttlipcpup%,%sess-ttlsrcviol%,%sess-ttlkeepfail%,%sess-curttlcalls%,%sess-cursipconn%,%sess-curmipconn%,%sess-curactcall%,%sess-curdormcall%,%sess-curarrived%,%sess-curlcpnegot%,%sess-curlcpup%,%sess-curauth%,%sess-curauthed%,%sess-curipcpup%,%sess-curdisc%,%sess-calldur-1min%,%sess-calldur-2min%,%sess-calldur-5min%,%sess-calldur-15min%,%sess-calldur-1hour%,%sess-calldur-4hour%,%sess-calldur-12hour%,%sess-calldur-24hour%,%sess-calldur-over24hour%,%sess-setuptime-100ms%,%sess-setuptime-200ms%,%sess-setuptime-300ms%,%sess-setuptime-400ms%,%sess-setuptime-500ms%,%sess-setuptime-600ms%,%sess-setuptime-700ms%,%sess-setuptime-800ms%,%sess-setuptime-900ms%,%sess-setuptime-1sec%,%sess-setuptime-2sec%,%sess-setuptime-3sec%,%sess-setuptime-4sec%,%sess-setuptime-6sec%,%sess-setuptime-8sec%,%sess-setuptime-10sec%,%sess-setuptime-12sec%,%sess-setuptime-14sec%,%sess-setuptime-16sec%,%sess-setuptime-over16sec%,%incremental%,%enddate%,%endtime%,%localenddate%,%localendtime%,%sess-ttlfailed%,%uptime%,%uptimestr%,%lic-ggsn%,%lic-l2tplns%,%sess-txbytes%,%sess-rxbytes%,%sess-txpackets%,%sess-rxpackets%,%sess-siptxbytes%,%sess-siprxbytes%,%sess-miptxbytes%,%sess-miprxbytes%,%aaa-ttlreq%,%aaa-curreq%,%aaa-ttlauthreq%,%aaa-curauthreq%,%aaa-ttlauthprobe%,%aaa-curauthprobe%,%aaa-ttlacctreq%,%aaa-curacctreq%,%aaa-ttlauthsucc%,%aaa-ttlauthfail%,%aaa-ttlauthpurged%,%aaa-ttlauthcancelled%,%aaa-ttlauthdmuchal%,%aaa-ttlradauthreq%,%aaa-curradauthreq%,%aaa-ttlradauthreqretried%,%aaa-ttllclauthreq%,%aaa-curlclauthreq%,%aaa-ttlpseudoauthreq%,%aaa-curpseudoauthreq%,%aaa-ttlauthnulluser%,%aaa-ttlacctsucc%,%aaa-ttlacctpurged%,%aaa-ttlacctcancelled%,%aaa-ttlradacctreq%,%aaa-ttlradacctreqretried%,%disc-reason-summary%,%sess-curaaaactive%,%sess-curaaadeleting%,%sess-curaaaacctpending%,%sess-ttlemptyfwd%,%sess-ttlemptyrev%,%sess-ttlonlineprepaiderr%,%sess-ttlprepaidinitautherr%,%sess-ttlcrprpattempt%,%sess-ttlcrprpsuccess%,%sess-ttlrpcrpattempt%,%sess-ttlrpcrpsuccess%,%sess-curpmipconn%,%sess-curl2tplacconn%,%sess-curalwayson%,%sess-curbcmcsauth%,%sess-curbcmcsconn%,%sess-curhaipsecconn%,%sess-curl2tplacconnecting%,%sess-curpdptypeipconn%,%sess-curpdptypepppconn%,%sess-curprepaid%,%sess-rxpkt-1023%,%sess-rxpkt-127%,%sess-rxpkt-16%,%sess-rxpkt-2047%,%sess-rxpkt-255%,%sess-rxpkt-4095%,%sess-rxpkt-4500%,%sess-rxpkt-511%,%sess-rxpkt-64%,%sess-rxpkt-over4500%,%sess-ttldisconn%,%sess-ttlhandoff%,%sess-ttlonlineauthfail%,%sess-ttlonlineauthreq%,%sess-ttlonlineauthsucc%,%sess-ttlprepaid%,%sess-ttlproxydns-drop%,%sess-ttlproxydns-passthru%,%sess-ttlproxydns-redirect%,%sess-ttlrenewal%,%sess-txpkt-1023%,%sess-txpkt-127%,%sess-txpkt-16%,%sess-txpkt-2047%,%sess-txpkt-255%,%sess-txpkt-4095%,%sess-txpkt-4500%,%sess-txpkt-511%,%sess-txpkt-64%,%sess-txpkt-over4500%,%aaa-ttlauthkeepalive%,%aaa-curauthkeepalive%,%aaa-ttlacctkeepalive%,%aaa-curacctkeepalive%,%aaa-ttlauthkeepalivesuccess%,%aaa-ttlauthkeepalivefailure%,%aaa-ttlauthkeepalivepurged%,%aaa-ttlacctkeepalivesuccess%,%aaa-ttlacctkeepalivetimeout%,%aaa-ttlacctkeepalivepurged%,%ipsg-total-call-arrived%,%ipsg-total-call-rejected%,%ipsg-total-call-demult%,%ipsg-total-dereg-rep-sent%,%ipsg-cur-active-call%,%ipsg-total-active-serv%,%asngw-cur-active-call%,%asngw-total-sess-setup%,%asngw-retriesexhaust%,%asngw.sfs%,%asngw.tidfail%,%asngw-handoffattempt%,%asngw-handoffdenied%,%asngw-handoffcomp%,%asngw.authsucc%,%asngw-authfailures%
PPP1Sch	PPP1 Schema	EMS,PPP1,%date%,%time%,%vpnname%,%vpnid%,%servname%,%init%,%reneg%,%success%,%failed%,%released%,%released-local%,%released-remote%,%lcp-fail-maxretry%,%lcp-fail-option%,%ipcp-fail-maxretry%,%ipcp-fail-option%,%fail-ccp%,%fail-auth%,%entered-lcp%,%entered-auth%,%entered-ipcp%,%reneg-pdsn%,%reneg-mobile%,%reneg-addrmis%,%reneg-other%,%auth-attempt-chap%,%auth-attempt-ppp%,%auth-attemp-mschap%,%auth-success-chap%,%auth-success-pap%,%auth-success-mschap%,%auth-fail-chap%,%auth-fail-pap%,%auth-fail-mschap%,%comp-stac%,%comp-mppc%,%comp-defl%,%rcverr-basfcs%,%rcverr-unknproto%,%rcverr-badaddr%,%rcverr-badctrl%,%comp-vjhdr%,%disc-lcp-remote%,%disc-rp-remote%,%disc-admin%,%disc-idle-timeout%,%disc-abs-timeout%,%disc-ppp-keepalive%,%disc-no-resource%,%disc-misc%,%remote-term%,%misc-fail%

Key	Description	Default Value in Config File
PPP2Sch	PPP2SchEma	EMS,PPP2,%date%,%time%,%vpnname%,%vpnid%,%servname%,%fail-reneg%,%lcp-fail-unknown%,%ipcp-fail-unknown%,%abort-auth%,%rp-disc%,%success-lcp%,%success-auth%,%reneg-rp_handoff%,%reneg-update%,%auth-abort-chap%,%auth-abort-pap%,%auth-abort-mschap%,%sess-skip-auth%,%comp-sess-neg%,%comp-sess-neg-fail%,%disc-rp-local%,%disc-add-flow-fail%,%disc-maxretry-lcp%,%disc-maxretry-ipcp%,%disc-max-setup-time%,%disc-bad-dest-vpn%,%disc-opt-neg-lcp%,%disc-opt-neg-ipcp%,%disc-no-remoteaddr%,%disc-typedetect-fail%,%disc-bad-src-addr%,%disc-remote%,%disc-long-timeout%,%disc-auth-fail%,%lcpecho-req-total%,%lcpecho-req-resent%,%lcpecho-rep-recved%,%lcpecho-timeout%,%recverr-ctrl-field%,%recverr-bad-length%,%in-oct%,%in-ucast%,%in-nucast%,%in-pkt%,%in-discard%,%in-discard-oct%,%out-oct%,%out-ucast%,%out-nucast%,%out-pkt%,%out-discard%,%out-discard-oct%,%num-sessions%,%lcpvse-req-total%,%lcpvse-req-resent%,%lcpvse-rep-recved%,%lcpvse-proto-reject%,%lcpvse-req-maxreach%,%svctype%,%conn-sess-reneg%,%comp-rohchdr%,%altppp-connected%,%reneg-rp-handoff%,%auth-attempt-pap%,%auth-attempt-mschap%
MIPFA1Sch	MIPFA1SchEma	EMS,MIPFA1,%date%,%time%,%vpnname%,%vpnid%,%servname%,%advert-send%,%disc-expiry%,%disc-dereg%,%disc-admin%,%auth-attempt%,%auth-success%,%auth-failure%,%recv-total%,%recv-initial%,%recv-renewal%,%recv-dereg%,%accept-total%,%accept-initial%,%accept-renewal%,%accept-dereg%,%denied-total%,%denied-initial%,%denied-renewal%,%denied-dereg%,%discard-total%,%discard-initial%,%discard-renewal%,%discard-dereg%,%relayed-total%,%relayed-initial%,%relayed-renewal%,%relayed-dereg%,%authfail-total%,%authfail-initial%,%authfail-renewal%,%authfail-dereg%,%denied-pdsn-total%,%denied-pdsn-initial%,%denied-pdsn-renewal%,%denied-pdsn-dereg%,%denied-ha-total%,%denied-ha-initial%,%denied-ha-renewal%,%denied-ha-dereg%,%denied-pdsn-unspec%,%denied-pdsn-timeout%,%denied-pdsn-admin%,%denied-pdsn-resource%,%denied-pdsn-mnauth%,%denied-pdsn-haauth%,%denied-pdsn-lifetoolong%,%denied-pdsn-badreq%,%denied-pdsn-badreply%,%denied-pdsn-missnai%,%denied-pdsn-misshomeagent%,%denied-pdsn-misshomeaddr%,%denied-pdsn-unkchallange%,%denied-pdsn-misschallenge%,%denied-pdsn-stalechallenge%,%denied-pdsn-mntoodistant%,%denied-pdsn-styleunavail%,%denied-pdsn-hanetunreach%,%denied-pdsn-hahostunreach%
MIPFA2Sch	MIPFA2SchEma	EMS,MIPFA2,%date%,%time%,%vpnname%,%vpnid%,%servname%,%denied-pdsn-haportunreach%,%denied-pdsn-haunreach%,%denied-pdsn-invcoa%,%denied-pdsn-encapunavail%,%denied-pdsn-revtununavail%,%denied-pdsn-revtunmand%,%denied-ha-faauth%,%denied-ha-badreq%,%denied-ha-mismatchid%,%denied-ha-simulbind%,%denied-ha-unknownha%,%denied-ha-revtununavail%,%replyrcv-total%,%replyrcv-totalrelayed%,%replyrcv-errors%,%replyrcv-initial%,%replyrcv-initialrelayed%,%replyrcv-renewal%,%replyrcv-renewalrelayed%,%replyrcv-dereg%,%replyrcv-deregrelayed%,%replysent-total%,%replysent-acceptreg%,%replysent-acceptdereg%,%replysent-badreq%,%replysent-lifetoolong%,%replysent-mnauthfail%,%replysent-haauthfail%,%replysent-adminprohib%,%replysent-noresources%,%replysent-revtununavail%,%replysent-revtunmand%,%replysent-senderrors%,%replysent-mntoodistant%,%replysent-invcoa%,%replysent-hanetunreach%,%replysent-hahostunreach%,%replysent-haportunreach%,%replysent-haunreach%,%replysent-regtimeout%,%replysent-missnai%,%replysent-misshomeagent%,%replysent-misshomeaddr%,%replysent-unkchallenge%,%replysent-misschallenge%,%replysent-stalechallenge%,%replysent-badreply%,%reqsent-initial%,%reqsent-initial-resend%,%reqsent-initial-noresend%,%reqsent-renew%,%reqsent-renew-resend%,%reqsent-renew-noresend%,%reqsent-dereg%,%reqsent-dereg-resend%,%reqsent-dereg-noresend%,%denied-pdsn-unkchallenge%,%denied-pdsn-unknowncvse%,%replysent-unspecified%,%replysent-delstyleunavail%,%ttlprepaid%,%curprepaid%,%ttlonlineauthsucc%,%ttlonlineauthfail%,%revoc-sent%,%revoc-retry-sent%,%revoc-ack-recv%,%revoc-timeout%,%revoc-recv%,%revoc-ack-sent%

Key	Description	Default Value in Config File
MIPHASch	MIPHA Schema	EMS,MIPHA,%date%,%time%,%vpnname%,%vpnid%,%servname%,%disconnects%,%expiry%,%dereg%,%admindrop%,%recv-total%,%recv-initial%,%recv-renew%,%recv-dereg%,%accept-total%,%accept-reg%,%accept-renew%,%accept-dereg%,%denied-total%,%denied-initial%,%denied-renew%,%denied-dereg%,%discard-total%,%reply-total%,%reply-acceptreg%,%reply-acceptdereg%,%reply-denied%,%reply-badreq%,%reply-mismatchid%,%reply-adminprohib%,%reply-unspecerr%,%reply-noresource%,%reply-mnauthfail%,%reply-faauthfail%,%reply-simulbind%,%reply-unknownha%,%reply-revtununavail%,%reply-revtunmand%,%reply-encapunavail%,%reply-senderror%,%farevocation%,%accept-ho%,%denied-ho%,%reply-error%,%num-sessions%,%recv-ho%,%revoc-sent%,%revoc-retry-sent%,%revoc-ack-recv%,%revoc-timeout%,%revoc-recv%,%revoc-ack-sent%,%miscerror%,%auth-attempt%,%auth-failure%,%auth-success%,%auth-real-failure%,%auth-misc-failure%,%reply-unknowncvse%,%reply-cong-drop%,%reply-cong-adminprohib%,%reply-cong-unknownha%,%reply-udp-encapunavail%,%ttlprepaid%,%curprepaid%,%ttlonlineauthsucc%,%ttlonlineauthfail%,%paaa-query-total%,%paaa-query-accept%,%paaa-query-denied%,%paaa-resp-sent%,%paaa-resp-found%,%paaa-resp-notfound%,%paaa-resp-poolover%,%paaa-resp-misc%,%ipsec-esp-txpackets%,%ipsec-esp-txbytes%,%ipsec-ah-txpackets%,%ipsec-ah-txbytes%,%ipsec-error-txpackets%,%ipsec-error-txbytes%,%ipsec-esp-rxpackets%,%ipsec-esp-rxbytes%,%ipsec-ah-rxpackets%,%ipsec-ah-rxbytes%,%ipsec-error-packets%,%ipsec-error-bytes%,%ipsec-replay-packets%,%ipsec-replay-bytes%,%ipsec-decode-packets%,%ipsec-decode-bytes%,%ipsec-auth-packets%,%ipsec-auth-bytes%,%ipsec-tooshort-packets%,%ipsec-tooshort-bytes%,%ipsec-dpdreq-sent%,%ipsec-dpdreq-recv%,%ipsec-dpdreply-sent%,%ipsec-dpdreply-recv%,%ipsec-dpdtimeout%,%ipsec-dpddisconn%,%ipsec-dpdrekey%
MIPHA2Sch	MIPHA2 Schema	EMS,MIPHA2,%date%,%time%,%vpnname%,%vpnid%,%servname%,%ipsec-nattkeepalive-sent%,%ipsec-nattkeepalive-recv%,%ipsec-ike-udpflows%,%ipsec-ike-cookieflows%,%ipsec-ike-txpackets%,%ipsec-ike-rxpackets%,%ipsec-ike-reqrecv%,%ipsec-ike-udpflowpackets%,%ipsec-ike-cookieflowpackets%,%ipsec-cur-tun%,%ipsec-cur-tunestablished%,%ipsec-ike-fails%,%ipsec-ttl-tun%,%ipsec-ttl-tunestablished%,%ipsec-call-req-rej%

Key	Description	Default Value in Config File
RP Schema	RP Sch	EMS,RP,%date%,%time%,%vpnname%,%vpnid%,%servname%,%recv-total%,%accept-total%,%denied-total%,%discard-total%,%accept-initial%,%accept-intrapdsn%,%accept-interpdsn%,%denied-initial%,%accept-renew%,%denied-renew%,%accept-dereg%,%denied-dereg%,%send-error%,%hash-error%,%decode-error%,%unhandled%,%seqerror%,%deny-unspec%,%deny-adminprohib%,%deny-noresource%,%deny-auth%,%deny-idmismatch%,%deny-badrequest%,%deny-unknownpdsn%,%deny-revtununavail%,%deny-revtunreq%,%deny-unrecogvend%,%upd-total%,%upd-accept%,%upd-denied%,%upd-unack%,%upd-trans%,%upd-retrans%,%upd-received%,%upd-discard%,%upd-senderror%,%upd-upltrinit%,%upd-other%,%upd-handoff%,%upddeny-unspec%,%upddeny-adminprohib%,%upddeny-auth%,%upddeny-idmismatch%,%upddeny-badrequest%,%sec-violations%,%sec-badauth%,%sec-badid%,%sec-badspi%,%sec-mnhaauth%,%sec-regupdate%,%disc-absent%,%disc-nomem%,%disc-malform%,%disc-authfail%,%disc-bounce%,%disc-inputq%,%disc-mismatchid%,%disc-invpktlen%,%disc-misc%,%reply-total%,%recv-initial%,%accept-active-intrapdsn%,%accept-dormant-intrapdsn%,%recv-renew%,%active-start-renew%,%active-stop-renew%,%recv-dereg%,%active-stop-dereg%,%upd-ttlnoretrans%,%upd-ack-received%,%num-sessions%,%deny-sessclosed%,%deny-cong-drop%,%deny-cong-adminprohib%,%deny-cong-unknownpdsn%,%sess-num-transmitted%,%sess-accepted%,%sess-denied%,%sess-not-acknowledged%,%sess-initial-update%,%sess-update-retransmitted%,%sess-update-ack-received%,%sess-update-ack-discarded%,%sess-update-send-error%,%sess-always-on-indication%,%sess-reason-unspecified%,%sess-PDSN-auth-fail%,%sess-ID-mismatch%,%sess-poorly-formed-update%,%sess-para-not-update%,%sess-absent%,%sess-no-memory%,%sess-malformed%,%sess-auth-fail%,%sess-ID-bounce-error%,%sess-input-Q-exceeded%,%sess-mismatched-ID%,%sess-invalid-packet-length%,%sess-misc-reasons%,%sess-gre-packet-sent-sdb%,%sess-gre-byte-sent-sdb%,%ttlprepaid%,%curprepaid%,%ttlonlineauthsucc%,%ttlonlineauthfail%,%discard-initial%,%recv-initial-setupstart%,%accept-initial-setupstart%,%denied-initial-setupstart%,%discard-initial-setupstart%,%discard-renew%,%recv-renew-noairlink%,%accept-renew-noairlink%,%denied-renew-noairlink%,%discard-renew-noairlink%,%recv-renew-activestart%,%accept-renew-activestart%,%denied-renew-activestart%,%discard-renew-activestart%,%recv-renew-activestop%,%accept-renew-activestop%,%denied-renew-activestop%,%discard-renew-activestop%,%discard-dereg%,%recv-dereg-noactivestop%,%accept-dereg-noactivestop%,%denied-dereg-noactivestop%,%discard-dereg-noactivestop%,%recv-dereg-activestop%,%accept-dereg-activestop%,%denied-dereg-activestop%,%discard-dereg-activestop%,%recv-intrapdsn-activeanidhandoff%,%accept-intrapdsn-activeanidhandoff%,%denied-intrapdsn-activeanidhandoff%,%discard-intrapdsn-activeanidhandoff%,%recv-intrapdsn-dormantanidhandoff%,%accept-intrapdsn-dormantanidhandoff%,%denied-intrapdsn-dormantanidhandoff%,%discard-intrapdsn-dormantanidhandoff%,%recv-interpdsn-activemeianidhandoff%,%accept-interpdsn-activemeianidhandoff%,%denied-interpdsn-activemeianidhandoff%,%discard-interpdsn-activemeianidhandoff%,%rx-pkt-xoff%,%rx-pkt-xon%,%xontoxoff%,%pkt-dropped-xoff%,%bytes-dropped-xoff%

Key	Description	Default Value in Config File
RPSch2	RP2 Schema	EMS,RP2,%date%,%time%,%vpnname%,%vpnid%,%servname%,%a10-cursetup%,%a10-ttlreleased%,%a10-ttlsetup%,%a10aux-cursetup%,%a10aux-ttlreleased%,%a10aux-ttlsetup%,%a10main-cursetup%,%a10main-ttlreleased%,%a10main-ttlsetup%,%deny-badrequest-alractive%,%deny-badrequest-alrdorm%,%deny-badrequest-authextn%,%deny-badrequest-fieldlen%,%deny-badrequest-flags%,%deny-badrequest-hoanonzero%,%deny-badrequest-miscoaaddr%,%deny-badrequest-other%,%deny-badrequest-pkttoolong%,%deny-badrequest-pkttooshort%,%deny-badrequest-setupabsent%,%deny-badrequest-sse%,%deny-badrequest-unkextn%,%deny-badrequest-vse%,%deny-noresource-a11mgrrej%,%deny-noresource-inputq%,%deny-noresource-nomem%,%deny-noresource-nosessmgr%,%deny-noresource-policy%,%deny-noresource-sessmgrrej%,%deny-noresource-sessmgrretried%,%deny-unspec-crphandoff%,%deny-unspec-intrahandoff%,%deny-unspec-lifezero%,%deny-unspec-noairlink%,%deny-unspec-notready%,%deny-unspec-nullpkt%,%reva-rrq-accept%,%reva-rrq-denied%,%reva-rrq-recv%,%reva-rrq-reply%,%rrqdiscard-adminprohib%,%rrqdiscard-authfail%,%rrqdiscard-bounce%,%rrqdiscard-grekey%,%rrqdiscard-inputq%,%rrqdiscard-invlen%,%rrqdiscard-maxsess%,%rrqdiscard-misc%,%rrqdiscard-nomem%,%rrqdiscard-nosessmgr%,%rrqdiscard-overload%,%rrqdiscard-smgrdead%,%rrqdiscard-smgrnotready%,%rrqdiscard-unkpdsn%,%sess-currevasetup%,%sess-cursetup%,%sess-release-dereg%,%sess-release-expiry%,%sess-release-grekey%,%sess-release-other%,%sess-release-pcfmonfail%,%sess-release-ppplayer%,%sess-ttlreleased%,%sess-ttlrevasetup%,%sess-ttlsetup%,%sess-updackdisc-pktnothand%,%sess-updackdisc-sessdisc%,%sess-upddenied-adminprohib%,%sess-upddenied-handoff%,%sess-upddenied-idnotsupp%,%sess-upddenied-noresource%,%sess-updreason-alwayson%,%sess-updreason-qosinfo%,%sess-updreason-qosoptrig%,%sess-updreason-qostftviol%,%sess-updreason-qostrafpol%,%sess-updreason-qostrafviol%,%upd-discard-unhpkt%,%upd-discard-unkpcf%,%upd-lifetime%,%upd-smgrexit%
RPSch3	RP3 Schema	EMS,RP3,%date%,%time%,%vpnname%,%vpnid%,%servname%,%sess-ttlrevareleased%,%sess-ttlrevadowngrade%,%deny-bsninfo%,%upd-uplyrinit%,%upd-discard-absent%,%upd-discard-nomem%,%upd-discard-malform%,%upd-discard-authfail%,%upd-discard-bounce%,%upd-discard-inputq%,%upd-discard-mismatchid%,%upd-discard-invpktlen%,%upd-discard-misc%,%sess-pdsn-auth-fail%,%sess-id-mismatch%,%sess-release-purged%
GTPC1Sch	GTPC1 Schema	EMS,GTPC1,%date%,%time%,%vpnname%,%vpnid%,%servname%,%setup-total%,%setup-ip%,%setup-ppp%,%released-total%,%cpc-total%,%cpc-v0%,%cpc-v1%,%cpc-sec%,%cpc-retrans%,%cpc-accept%,%cpc-deny%,%cpc-discard%,%upc-rx%,%upc-rx-accept%,%upc-rx-deny%,%upc-rx-discard%,%upc-tx%,%upc-tx-accept%,%upc-tx-deny%,%dpc-rx%,%dpc-rx-accept%,%dpc-rx-deny%,%dpc-rx-discard%,%dpc-tx%,%dpc-tx-accept%,%dpc-tx-deny%,%cpc-aa%,%cpc-aa-accept%,%cpc-aa-deny%,%cpc-aa-discard%,%dpc-aa-rx%,%dpc-aa-rx-accept%,%dpc-aa-rx-deny%,%dpc-aa-rx-discard%,%dpc-aa-tx%,%dpc-aa-tx-accept%,%dpc-aa-tx-deny%,%err-ind-rx%,%err-ind-tx%,%cpc-noresource%,%cpc-addr-occupied%,%cpc-nomem%,%cpc-missing-apn%,%cpc-unknown-pdp%,%cpc-auth-fail%,%cpc-sys-fail%,%cpc-sem-tft%

Key	Description	Default Value in Config File
GTPC2Sch	GTPC2 Schema	EMS,GTPC2,%date%,%time%,%vpnname%,%vpnid%,%servname%,%cpc-syn-tft%,%cpc-sem-pktfilter%,%cpc-syn-pktfilter%,%cpc-ie-err%,%cpc-ie-missing%,%cpc-opt-ie-err%,%cpc-malformed%,%cpc-version%,%disc-sgsn%,%disc-path-fail%,%disc-smgr-dead%,%disc-admin%,%disc-other%,%disc-teardown%,%disc-idle%,%disc-absolute%,%disc-src-addr%,%disc-flow-add%,%disc-dhcp-renew-fail%,%disc-long-durn%,%disc-aborted%,%disc-apn-rmvd%,%pdu-notif%,%pdu-notif-accpet%,%pdu-notif-deny%,%pdu-notif-rej%,%pdu-notif-rej-accept%,%pdu-notif-rej-deny%,%pdu-notif-rej-discard%,%sri-req%,%sri-accept%,%sri-deny%,%fail-rep%,%fail-rep-accept%,%fail-rep-deny%,%note-ms-gprs%,%note-ms-gprs-accept%,%note-ms-gprs-deny%,%note-ms-gprs-discard%,%num-bytes-in%,%num-pkts-in%,%num-bytes-out%,%num-pkts-out%,%cpc-srv-not-supp%,%gtpu-echo-req-rx%,%gtpu-echo-req-tx%,%gtpu-echo-rsp-tx%,%gtpu-echo-rsp-rx%,%ctrl-num-bytes-in%,%ctrl-num-pkts-in%,%ctrl-num-bytes-out%,%ctrl-num-pkts-out%,%echo-req-rx%,%echo-req-tx%,%echo-rsp-tx%,%echo-rsp-rx%,%setup-current%,%current-ip%,%current-ppp%,%current-ipv6%,%current-ntwkinitd%,%setup-ipv6%,%setup-sgsn%,%setup-ggsn%,%qosconv-bytes-in%,%qosconv-pkts-in%,%qosconv-bytes-out%,%qosconv-pkts-out%,%qosstrm-bytes-in%,%qosstrm-pkts-in%,%qosstrm-bytes-out%,%qosstrm-pkts-out%,%qosint1-bytes-in%,%qosint1-pkts-in%,%qosint1-bytes-out%,%qosint1-pkts-out%,%qosint2-bytes-in%,%qosint2-pkts-in%,%qosint2-bytes-out%,%qosint2-pkts-out%,%qosint3-bytes-in%,%qosint3-pkts-in%,%qosint3-bytes-out%,%qosint3-pkts-out%,%qosint-bytes-in%,%qosint-pkts-in%,%qosint-bytes-out%,%qosint-pkts-out%,%qosback-bytes-in%,%qosback-pkts-in%,%qosback-bytes-out%,%qosback-pkts-out%,%dyn-ipv4-attempt%,%dyn-ipv6-attempt%,%dyn-ppp-attempt%,%dyn-ipv4-success%,%dyn-ipv6-success%,%dyn-ppp-success%,%cpc-no-apn-subscription%
GTPPSch	GTPP Schema	EMS,GTPP,%date%,%time%,%vpnname%,%vpnid%,%echo-req-rx%,%echo-req-tx%,%echo-rsp-rx%,%echo-rsp-tx%,%redir-rcvd%,%redir-rsp%,%node-alive%,%node-alive-rsp%,%data-rec-trans%,%dup-data-rec-trans%,%send-data-rec%,%rel-data-rec%,%cancel-data-rec%,%data-rec-trans-rsp%,%delete-node%,%node-addr%,%req-accept%,%req-not-fulfil%,%req-malform%,%version-not-supp%,%serv-not-supp%,%mand-ie-err%,%mand-ie-miss%,%opt-ie-err%,%dup-already-fulfil%,%already-fulfil%,%no-resource%,%sys-fail%,%normal-close%,%abnormal-close%,%vol-limit-close%,%time-limit-close%,%open-req%,%aaa-acct-arch%,%rdir-sys-fail%,%rdir-txbuf-full%,%rdir-rxbuf-full%,%other-node-dn%,%self-node-dn%,%rdir-no-res%,%rdir-serv-no%,%rdir-version-not-supp%,%rdir-mand-ie-miss%,%rdir-mand-ie-err%,%rdir-opt-ie-err%,%rdir-malformed%,%rdir-rsp-sys-fail%,%gss-echo-req%,%gss-echo-rsp%,%gss-gtpp-req%,%gss-gtpp-req-ret%,%gss-gtpp-rsp%,%gss-gtpp-rsp-failed%,%gss-gcdr-req%,%gss-gcdr-req-ret%,%gss-gcdr-rsp%,%gss-gcdr-rsp-failed%,%gss-aaaproxy-rec-req%,%gss-aaaproxy-rec-ret%,%gss-aaaproxy-rec-rsp%,%gss-aaaproxy-rec-rsp-failed%,%gss-aaamgr-rec-req%,%gss-aaamgr-rec-ret%,%gss-aaamgr-rec-rsp%,%gss-aaamgr-rec-rsp-failed%,%gss-update-cgf-req%,%gss-update-cgf-req-ret%,%gss-update-cgf-rsp%,%gss-update-cfg-rsp-failed%,%gss-clear-db-req%,%gss-clear-db-req-ret%,%gss-clear-db-rsp%,%gss-clear-db-rsp-failed%,%gss-update-req%,%gss-invalid-req-rcvd%
IPPoolSch	IPPool Schema	EMS,IPPOOL,%date%,%time%,%vpnname%,%vpnid%,%name%,%used%,%hold%,%release%,%free%,%type%,%priority%,%state%,%startaddr%,%groupname%

Key	Description	Default Value in Config File
APN Sch	APN Schema	EMS,APN,%date%,%time%,%vpnname%,%vpnid%,%apn%,%uplnk-bytes%,%dnlnk-bytes%,%uplnk-pkts%,%dnlnk-pkts%,%uplnk-drop%,%dnlnk-drop%,%bad-hdr%,%ttl-excd%,%frag-sent%,%frag-fail%,%inacl-drop%,%outacl-drop%,%bad-src-addr%,%addr-stat%,%addr-lpool%,%addr-rad%,%addr-dhcp%,%addr-dhcp-rly%,%addr-no-alloc%,%sess-curr%,%sess-curr-all%,%sess-tot%,%sess-tot-all%,%uplnk-bytes-drop%,%dnlnk-bytes-drop%,%data-fromuseravg-bps%,%data-touseravg-bps%,%data-fromusersust-bps%,%data-tousersust-bps%,%data-fromuseravg-pps%,%data-touseravg-pps%,%data-fromusersust-pps%,%data-tousersust-pps%,%qosconv-pkts-uplnk%,%qosconv-pkts-dnlnk%,%qosstrm-pkts-uplnk%,%qosstrm-pkts-dnlnk%,%qosint1-pkts-uplnk%,%qosint1-pkts-dnlnk%,%qosint2-pkts-uplnk%,%qosint2-pkts-dnlnk%,%qosint3-pkts-uplnk%,%qosint3-pkts-dnlnk%,%qosint-pkts-uplnk%,%qosint-pkts-dnlnk%,%qosback-pkts-uplnk%,%qosback-pkts-dnlnk%,%att-pdp-ctxt%,%att-deact-pdp-ggsn%,%succ-deact-pdp-ggsn%,%att-deact-pdp-ms%,%succ-deact-pdp-ms%,%dyn-ipv4-attempt%,%dyn-ipv6-attempt%,%dyn-ipv4-success%,%dyn-ipv6-success%,%auth-req-sent%,%auth-acc-rcvd%,%auth-timeout%,%acc-req-sent%,%acc-rsp-rcvd%,%acc-req-timeout%
LAC 1Sch	LAC Schema 1	EMS,LAC1,%date%,%time%,%vpnname%,%vpnid%,%servname%,%tun-conn-attempt%,%tun-conn-success%,%tun-conn-fail%,%tun-conn-curactive%,%sess-attempts%,%sess-successful%,%sess-failed%,%sess-curactive%,%sess-intrapdsnho-attempt%,%sess-intrapdsnho-success%,%sess-intrapdsnho-failed%,%sess-interpdsnho-attempt%,%recv-err-malformed%,%recv-err-ctrlfield%,%recv-err-pktlen%,%recv-err-avplen%,%recv-err-protover%,%recv-err-md5%,%recv-err-invattr%,%recv-err-unkattr%,%recv-err-invsessid%,%recv-err-invstate%,%recv-err-unkmsg%,%recv-err-unmatchpktlen%,%recv-err-invtunid%,%tun-genclear%,%tun-ctrlconnexists%,%tun-unauth%,%tun-badproto%,%tun-reqshutdown%,%tun-statemacherr%,%tun-badlen%,%tun-oor%,%tun-noresource%,%tun-vendspec%,%tun-tryanotherlns%,%tun-unkavp%,%tun-ipsecdisc%,%tun-ipsecfail%,%tun-license%,%tun-newcallpoldisc%,%tun-maxretry%,%tun-syslimit%,%tun-miscerr%,%sess-nogeneral%,%sess-admin%,%sess-lossofcarr%
LAC 2Sch	LAC Schema 2	EMS,LAC2,%date%,%time%,%vpnname%,%vpnid%,%servname%,%sess-remoteadmin%,%sess-nofactemp%,%sess-nofacperm%,%sess-invdest%,%sess-nocarrier%,%sess-busysig%,%sess-nodialtime%,%sess-lactimeout%,%sess-noframing%,%sess-noctrlconn%,%sess-badlen%,%sess-oor%,%sess-noresource%,%sess-invsessid%,%sess-vendspec%,%sess-tryanotherlns%,%sess-unkavp%,%sess-maxtunnel%,%sess-ipsecfail%,%sess-ipsecdisc%,%sess-newcallpoldisc%,%sess-license%,%sess-servmismatch%,%sess-miscerr%
CLOSED RP1 Sch	Closed RP Schema 1	EMS,CLOSEDRP1,%date%,%time%,%vpnname%,%vpnid%,%servname%,%tun-conn-attempt%,%tun-conn-success%,%tun-conn-fail%,%tun-conn-curactive%,%sess-attempts%,%sess-successful%,%sess-failed%,%sess-curactive%,%sess-intrapdsnho-attempt%,%sess-intrapdsnho-success%,%sess-intrapdsnho-failed%,%sess-interpdsnho-attempt%,%recv-err-malformed%,%recv-err-ctrlfield%,%recv-err-pktlen%,%recv-err-avplen%,%recv-err-protover%,%recv-err-md5%,%recv-err-invattr%,%recv-err-unkattr%,%recv-err-invsessid%,%recv-err-invstate%,%recv-err-unkmsg%,%recv-err-unmatchpktlen%,%recv-err-invtunid%,%tun-genclear%,%tun-ctrlconnexists%,%tun-unauth%,%tun-badproto%,%tun-reqshutdown%,%tun-statemacherr%,%tun-badlen%,%tun-oor%,%tun-noresource%,%tun-vendspec%,%tun-tryanotherlns%,%tun-unkavp%,%tun-ipsecdisc%,%tun-ipsecfail%,%tun-license%,%tun-newcallpoldisc%,%tun-maxretry%,%tun-syslimit%,%tun-miscerr%,%sess-nogeneral%,%sess-admin%,%sess-lossofcarr%
CLOSED RP2 Sch	Closed RP Schema 2	EMS,CLOSEDRP2,%date%,%time%,%vpnname%,%vpnid%,%servname%,%sess-remoteadmin%,%sess-nofactemp%,%sess-nofacperm%,%sess-invdest%,%sess-nocarrier%,%sess-busysig%,%sess-nodialtime%,%sess-lactimeout%,%sess-noframing%,%sess-noctrlconn%,%sess-badlen%,%sess-oor%,%sess-noresource%,%sess-invsessid%,%sess-vendspec%,%sess-tryanotherlns%,%sess-unkavp%,%sess-maxtunnel%,%sess-ipsecfail%,%sess-ipsecdisc%,%sess-newcallpoldisc%,%sess-license%,%sess-servmismatch%,%sess-miscerr%,%sess-hocomplete%,%sess-invho%,%sess-duplsess%,%ttlprepaid%,%curprepaid%,%ttlonlineauthsucc%,%ttlonlineauthfail%

Key	Description	Default Value in Config File
RADIUSSch	RADIUS Schema	EMS,RADIUS,%date%,%time%,%vpnname%,%vpnid%,%servertype%,%ipaddr%,%auth-req-sent%,%auth-req-sentwdmu%,%auth-req-pending%,%auth-req-retried%,%auth-req-retriedwdmu%,%auth-chal-rcvd%,%auth-acc-rcvd%,%auth-rej-rcvd%,%auth-rej-rcvdwdmu%,%auth-timeout%,%auth-cons-fail%,%auth-rsp-badauth%,%auth-rsp-malformed%,%auth-rsp-malformedattr%,%auth-rsp-unktype%,%auth-rsp-dropped%,%auth-rsp-roundtripusec%,%probe-issued%,%probe-success%,%probe-failed%,%probe-roundtriptimeusec%,%acc-req-sent%,%acc-req-pending%,%acc-req-retried%,%acc-rsp-rcvd%,%acc-req-timeout%,%acc-req-cons-fail%,%acc-rsp-badresp%,%acc-rsp-malformed%,%acc-rsp-unktype%,%acc-rsp-dropped%,%acc-rsp-roundtripusec%,%port%,%acc-start-sent%,%acc-stop-sent%,%acc-interim-sent%,%acc-start-retries%,%acc-stop-retries%,%acc-interim-retries%,%group%,%acc-ttl-g1%,%acc-ttl-g2%,%online-acc-req-sent%,%online-acc-req-pending%,%online-acc-req-retried%,%online-acc-rsp-rcvd%,%online-acc-rej-rcvd%,%online-acc-req-timeout%,%online-acc-rsp-badauth%,%online-acc-rsp-malformed%,%online-acc-rsp-malformedattr%,%online-acc-rsp-unktype%,%online-acc-badmsgauth%,%online-acc-nomsgauth%,%nasipaddr%,%keepalive-auth-req-sent%,%keepalive-auth-retried%,%keepalive-auth-acc-rcvd%,%keepalive-auth-timeout%,%keepalive-auth-rej-rcvd%,%keepalive-acct-req-sent%,%keepalive-acct-retried%,%keepalive-acct-success%,%keepalive-acct-timeout%,%keepalive-acct-rsp-badauth%,%cons-fail%,%keepalive-auth-rsp-badauth%,%keepalive-auth-rsp-malformed%,%keepalive-auth-rsp-malformedattr%,%keepalive-auth-rsp-unktype%,%keepalive-auth-rsp-dropped%,%acc-on-sent%,%acc-off-sent%,%acc-on-retries%,%acc-off-retries%,%keepalive-acct-rsp-malformed%,%keepalive-acct-rsp-unktype%,%keepalive-acct-rsp-dropped%
MISCSch	Miscellaneous Schema	%ipaddr%,%host%,%uptime%,%time%,%localdate%,%localtime%,%localtz%,%time2%,%localtime2%
MISCSchForEMS	New Miscellaneous Schema	EMS,MISC,%date%,%time%,%ipaddr%,%host%,%uptime%,%localdate%,%localtime%,%localtz%,%time2%,%localtime2%,%swversion%,%swbuild%,%localtzoffset%

Key	Description	Default Value in Config File
ECS1Sch	ECS1 Schema	EMS,ECS1,%date%,%time%,%ecs-subscribers%,%ecs-subscribers-cur%,%gcdrs-generated%,%edrs-generated%,%udrs-generated%,%ip-flows%,%ip-flows-cur%,%ip-uplk-bytes%,%ip-dwnlk-bytes%,%ip-uplk-pkts%,%ip-dwnlk-pkts%,%ip-uplk-pkts-frag%,%ip-dwnlk-pkts-frag%,%ip-uplk-bytes-frag%,%ip-dwnlk-bytes-frag%,%udp-flows%,%udp-flows-cur%,%udp-uplk-bytes%,%udp-dwnlk-bytes%,%udp-uplk-pkts%,%udp-dwnlk-pkts%,%udp-inv-pkts%,%tcp-flows%,%tcp-flows-cur%,%tcp-uplk-bytes%,%tcp-dwnlk-bytes%,%tcp-uplk-pkts%,%tcp-dwnlk-pkts%,%tcp-uplk-bytes-retr%,%tcp-dwnlk-bytes-retr%,%tcp-uplk-pkts-retr%,%tcp-dwnlk-pkts-retr%,%tcp-uplk-pkts-ooo-analyzd%,%tcp-dwnlk-pkts-ooo-analyzd%,%tcp-uplk-pkts-ooo-fail%,%tcp-dwnlk-pkts-ooo-fail%,%tcp-uplk-pkts-ooo-retr%,%tcp-dwnlk-pkts-ooo-retr%,%icmp-flows%,%icmp-flows-cur%,%icmp-uplk-bytes%,%icmp-dwnlk-bytes%,%icmp-uplk-pkts%,%icmp-dwnlk-pkts%,%icmp-ech-req%,%icmp-ech-rep%,%icmp-dst-unrch%,%icmp-redir%,%icmp-tm-excd%,%icmp-trace-route%,%icmp-oth%,%http-flows%,%http-flows-cur%,%http-uplk-bytes%,%http-dwnlk-bytes%,%http-uplk-pkts%,%http-dwnlk-pkts%,%http-uplk-bytes-retr%,%http-dwnlk-bytes-retr%,%http-uplk-pkts-retr%,%http-dwnlk-pkts-retr%,%http-req-succ%,%http-req-fail%,%http-get-req%,%http-post-req%,%http-connect-req%,%http-inv-pkts%,%https-flows%,%https-flows-cur%,%https-uplk-bytes%,%https-dwnlk-bytes%,%https-uplk-pkts%,%https-dwnlk-pkts%,%https-uplk-bytes-retr%,%https-dwnlk-bytes-retr%,%https-uplk-pkts-retr%,%https-dwnlk-pkts-retr%,%wtp-trans%,%wtp-cls-zero%,%wtp-cls-one%,%wtp-cls-two%,%wtp-uplk-bytes%,%wtp-dwnlk-bytes%,%wtp-uplk-pkts%,%wtp-dwnlk-pkts%,%wtp-uplk-bytes-retr%,%wtp-dwnlk-bytes-retr%,%wtp-uplk-pkts-retr%,%wtp-dwnlk-pkts-retr%,%wtp-invk-pkts%,%wtp-invk-tcl-zero%,%wtp-invk-tcl-one%,%wtp-invk-tcl-two%,%wtp-invk-tid-new%,%wtp-rslt-pkts%,%wtp-ack-to-resp%,%wtp-ack-to-init%,%wtp-abrt-to-resp%,%wtp-abrt-to-init%,%wtp-seg-invk%,%wtp-seg-rslt%,%wtp-neg-ack%,%wtp-tid-vrf%,%wtp-noninit-invk%,%wtp-unk-pdu%,%wsp-flows%,%wsp-flows-cur%,%wsp-co-conn%,%wsp-cl-conn%,%wsp-uplk-bytes%,%wsp-dwnlk-bytes%,%wsp-uplk-pkts%,%wsp-dwnlk-pkts%,%wsp-uplk-bytes-retr%,%wsp-dwnlk-bytes-retr%,%wsp-uplk-pkts-retr%,%wsp-dwnlk-pkts-retr%,%wsp-co-req-succ%,%wsp-co-req-fail%,%wsp-cl-req-succ%,%wsp-cl-req-fail%,%wsp-conn-pdu%,%wsp-conn-rep%,%wsp-redir%,%wsp-disc%,%wsp-susp%,%wsp-resm%,%wsp-opt%,%wsp-head%,%wsp-del%,%wsp-trace%,%wsp-reply%,%wsp-put%,%wsp-get%,%wsp-push%,%wsp-conf-push%,%wsp-post%,%wsp-data-frag%,%wsp-rsrvd%,%wsp-inv-pkts%,%mms-send%,%mms-send-succ%,%mms-send-fail%,%mms-retrv%,%mms-retrv-succ%,%mms-retrv-fail%,%mms-uplk-bytes%,%mms-dwnlk-bytes%,%mms-uplk-pkts%,%mms-dwnlk-pkts%,%mms-uplk-bytes-retr%,%mms-dwnlk-bytes-retr%,%mms-uplk-pkts-retr%,%mms-dwnlk-pkts-retr%,%mms-snd-req%,%mms-snd-conf%,%mms-ntf-ind%,%mms-ntf-ind-imm%,%mms-ntf-ind-del%,%mms-ntf-rsp%,%mms-retrv-conf%,%mms-ack-ind%,%mms-delvry-ind%,%mms-unk-pdu%,%mms-inv-pkts%,%sip-flows%,%sip-flows-cur%,%sip-calls%,%sip-uplk-bytes%,%sip-dwnlk-bytes%,%sip-uplk-pkts%,%sip-dwnlk-pkts%,%sip-uplk-bytes-retr%,%sip-dwnlk-bytes-retr%,%sip-uplk-pkts-retr%,%sip-dwnlk-pkts-retr%,%sip-invite%,%sip-bye%,%sip-ack%,%sip-cancel%,%sip-register%,%sip-inv-pkts%,%rtsp-flows%,%rtsp-flows-cur%,%rtsp-sess%,%rtsp-uplk-bytes%,%rtsp-dwnlk-bytes%,%rtsp-uplk-pkts%,%rtsp-dwnlk-pkts%,%rtsp-uplk-bytes-retr%,%rtsp-dwnlk-bytes-retr%,%rtsp-uplk-pkts-retr%,%rtsp-dwnlk-pkts-retr%,%rtsp-play%,%rtsp-setup%,%rtsp-pause%,%rtsp-record%,%rtsp-option%,%rtsp-redir%,%rtsp-desc%,%rtsp-announ%,%rtsp-trdwn%,%rtsp-get-param%,%rtsp-set-param%,%rtsp-inv-pkts%

Key	Description	Default Value in Config File
ECS2Sch	ECS2 Schema	EMS,ECS2,%date%,%time%,%rtp-flows%,%rtp-flows-cur%,%rtp-uplk-bytes%,%rtp-dwnlk-bytes%,%rtp-uplk-pkts%,%rtp-dwnlk-pkts%,%ftp-flows%,%ftp-flows-cur%,%ftp-uplk-bytes%,%ftp-dwnlk-bytes%,%ftp-uplk-pkts%,%ftp-dwnlk-pkts%,%ftp-retr%,%ftp-stor%,%ftp-inv-pkts%,%smtp-flows%,%smtp-flows-cur%,%smtp-uplk-bytes%,%smtp-dwnlk-bytes%,%smtp-uplk-pkts%,%smtp-dwnlk-pkts%,%smtp-uplk-bytes-retr%,%smtp-dwnlk-bytes-retr%,%smtp-uplk-pkts-retr%,%smtp-dwnlk-pkts-retr%,%smtp-unk-cmd%,%smtp-unk-resp%,%smtp-req-succ%,%smtp-req-fail%,%smtp-helo%,%smtp-ehlo%,%smtp-mail-frm%,%smtp-rcpt-to%,%smtp-data%,%smtp-bdat%,%smtp-vrfy%,%smtp-expn%,%smtp-noop%,%smtp-rset%,%smtp-quit%,%smtp-inv-pkts%,%pop3-flows%,%pop3-flows-cur%,%pop3-uplk-bytes%,%pop3-dwnlk-bytes%,%pop3-uplk-pkts%,%pop3-dwnlk-pkts%,%pop3-uplk-bytes-retr%,%pop3-dwnlk-bytes-retr%,%pop3-uplk-pkts-retr%,%pop3-dwnlk-pkts-retr%,%pop3-retr%,%pop3-retr-succ%,%pop3-list%,%pop3-list-succ%,%pop3-inv-pkts%,%imap-uplk-bytes%,%imap-dwnlk-bytes%,%imap-uplk-pkts%,%imap-dwnlk-pkts%,%imap-uplk-bytes-retr%,%imap-dwnlk-bytes-retr%,%imap-uplk-pkts-retr%,%imap-dwnlk-pkts-retr%,%imap-req-succ%,%imap-req-fail%,%imap-reply-untag%,%imap-reply-commcont%,%imap-unk-command%,%imap-unk-reply%,%p2p-flows%,%p2p-flows-cur%,%p2p-skype-uplnk-bytes%,%p2p-skype-dwlnk-bytes%,%p2p-skype-uplnk-pkts%,%p2p-skype-dwlnk-pkts%,%p2p-bittorrent-uplnk-bytes%,%p2p-bittorrent-dwlnk-bytes%,%p2p-bittorrent-uplnk-pkts%,%p2p-bittorrent-dwlnk-pkts%,%p2p-edonkey-uplnk-bytes%,%p2p-edonkey-dwlnk-bytes%,%p2p-edonkey-uplnk-pkts%,%p2p-edonkey-dwlnk-pkts%,%p2p-msn-uplnk-bytes%,%p2p-msn-dwlnk-bytes%,%p2p-msn-uplnk-pkts%,%p2p-msn-dwlnk-pkts%,%p2p-yahoo-uplnk-bytes%,%p2p-yahoo-dwlnk-bytes%,%p2p-yahoo-uplnk-pkts%,%p2p-yahoo-dwlnk-pkts%
ECS3Sch	ECS3 Schema	EMS,ECS3,%date%,%time%,%p2p-orb-uplnk-bytes%,%p2p-orb-dwlnk-bytes%,%p2p-orb-uplnk-pkts%,%p2p-orb-dwlnk-pkts%,%p2p-winny-uplnk-bytes%,%p2p-winny-dwlnk-bytes%,%p2p-winny-uplnk-pkts%,%p2p-winny-dwlnk-pkts%,%p2p-slingbox-uplnk-bytes%,%p2p-slingbox-dwlnk-bytes%,%p2p-slingbox-uplnk-pkts%,%p2p-slingbox-dwlnk-pkts%,%p2p-fasttrack-uplnk-bytes%,%p2p-fasttrack-dwlnk-bytes%,%p2p-fasttrack-uplnk-pkts%,%p2p-fasttrack-dwlnk-pkts%,%p2p-gnutella-uplnk-bytes%,%p2p-gnutella-dwlnk-bytes%,%p2p-gnutella-uplnk-pkts%,%p2p-gnutella-dwlnk-pkts%,%p2p-jabber-uplnk-bytes%,%p2p-jabber-dwlnk-bytes%,%p2p-jabber-uplnk-pkts%,%p2p-jabber-dwlnk-pkts%,%ecs-ttlsuccess%,%ecs-ttlfail%,%ecs-curactive%,%ecs-15peak-curactive%,%ecs-ruleshit%,%ecs-ttldlinkbytes%,%ecs-ttlulinkbytes%,%ecs-ttldlinkpackets%,%ecs-ttlulinkpackets%,%ecs-ttlflowconn%,%ecs-ttlflowdisc%,%ecs-curflow%,%ecs-15peak-curflow%,%ecs-15min-usage-flowall%,%dns-dwnlk-bytes%,%dns-dwnlk-pkts%,%dns-flows%,%dns-flows-cur%,%dns-inv-pkts%,%dns-over-tcp-dwnlk-bytes%,%dns-over-tcp-dwnlk-pkts%,%dns-over-tcp-uplk-bytes%,%dns-over-tcp-uplk-pkts%,%dns-req-a-query%,%dns-req-cname-query%,%dns-req-ns-query%,%dns-req-ptr-query%,%dns-req-unknown-query%,%dns-rsp-a-query%,%dns-rsp-cname-query%,%dns-rsp-ns-query%,%dns-rsp-ptr-query%,%dns-rsp-unknown-query%,%dns-unk-opcode%,%dns-uplk-bytes%,%dns-uplk-pkts%,%icmp-inv-pkts%,%p2p-applejuice-dwlnk-bytes%,%p2p-applejuice-dwlnk-pkts%,%p2p-applejuice-uplnk-bytes%,%p2p-applejuice-uplnk-pkts%,%p2p-ares-dwlnk-bytes%,%p2p-ares-dwlnk-pkts%,%p2p-ares-uplnk-bytes%,%p2p-ares-uplnk-pkts%,%p2p-directconnect-dwlnk-bytes%,%p2p-directconnect-dwlnk-pkts%,%p2p-directconnect-uplnk-bytes%,%p2p-directconnect-uplnk-pkts%,%p2p-feidian-dwlnk-bytes%,%p2p-feidian-dwlnk-pkts%,%p2p-feidian-uplnk-bytes%,%p2p-feidian-uplnk-pkts%

Key	Description	Default Value in Config File
ECS4Sch	ECS4 Schema	EMS,ECS4,%date%,%time%,%p2p-filetopia-dwlnk-bytes%,%p2p-filetopia-dwlnk-pkts%,%p2p-filetopia-uplnk-bytes%,%p2p-filetopia-uplnk-pkts%,%p2p-gadugadu-dwlnk-bytes%,%p2p-gadugadu-dwlnk-pkts%,%p2p-gadugadu-uplnk-bytes%,%p2p-gadugadu-uplnk-pkts%,%p2p-imesh-dwlnk-bytes%,%p2p-imesh-dwlnk-pkts%,%p2p-imesh-uplnk-bytes%,%p2p-imesh-uplnk-pkts%,%p2p-manolito-dwlnk-bytes%,%p2p-manolito-dwlnk-pkts%,%p2p-manolito-uplnk-bytes%,%p2p-manolito-uplnk-pkts%,%p2p-msn-non-voice-dwlnk-bytes%,%p2p-msn-non-voice-dwlnk-pkts%,%p2p-msn-non-voice-uplnk-bytes%,%p2p-msn-non-voice-uplnk-pkts%,%p2p-msn-voice-dwlnk-bytes%,%p2p-msn-voice-dwlnk-pkts%,%p2p-msn-voice-uplnk-bytes%,%p2p-msn-voice-uplnk-pkts%,%p2p-mute-dwlnk-bytes%,%p2p-mute-dwlnk-pkts%,%p2p-mute-uplnk-bytes%,%p2p-mute-uplnk-pkts%,%p2p-pando-dwlnk-bytes%,%p2p-pando-dwlnk-pkts%,%p2p-pando-uplnk-bytes%,%p2p-pando-uplnk-pkts%,%p2p-pplive-dwlnk-bytes%,%p2p-pplive-dwlnk-pkts%,%p2p-pplive-uplnk-bytes%,%p2p-pplive-uplnk-pkts%,%p2p-ppstream-dwlnk-bytes%,%p2p-ppstream-dwlnk-pkts%,%p2p-ppstream-uplnk-bytes%,%p2p-ppstream-uplnk-pkts%,%p2p-qq-dwlnk-bytes%,%p2p-qq-dwlnk-pkts%,%p2p-qqlive-dwlnk-bytes%,%p2p-qqlive-dwlnk-pkts%,%p2p-qqlive-uplnk-bytes%,%p2p-qqlive-uplnk-pkts%,%p2p-qq-uplnk-bytes%,%p2p-qq-uplnk-pkts%,%p2p-skinny-dwlnk-bytes%,%p2p-skinny-dwlnk-pkts%,%p2p-skinny-uplnk-bytes%,%p2p-skinny-uplnk-pkts%,%p2p-skype-non-voice-dwlnk-bytes%,%p2p-skype-non-voice-dwlnk-pkts%,%p2p-skype-non-voice-uplnk-bytes%,%p2p-skype-non-voice-uplnk-pkts%,%p2p-skype-voice-dwlnk-bytes%,%p2p-skype-voice-dwlnk-pkts%,%p2p-skype-voice-uplnk-bytes%,%p2p-skype-voice-uplnk-pkts%,%p2p-sopcast-dwlnk-bytes%,%p2p-sopcast-dwlnk-pkts%,%p2p-sopcast-uplnk-bytes%,%p2p-sopcast-uplnk-pkts%,%p2p-soulseek-dwlnk-bytes%,%p2p-soulseek-dwlnk-pkts%,%p2p-soulseek-uplnk-bytes%
ECS5Sch	ECS5 Schema	EMS,ECS5,%date%,%time%,%p2p-soulseek-uplnk-pkts%,%p2p-yahoo-non-voice-dwlnk-bytes%,%p2p-yahoo-non-voice-dwlnk-pkts%,%p2p-yahoo-non-voice-uplnk-bytes%,%p2p-yahoo-non-voice-uplnk-pkts%,%p2p-yahoo-voice-dwlnk-bytes%,%p2p-yahoo-voice-dwlnk-pkts%,%p2p-yahoo-voice-uplnk-bytes%,%p2p-yahoo-voice-uplnk-pkts%,%p2p-zattoo-dwlnk-bytes%,%p2p-zattoo-dwlnk-pkts%,%p2p-zattoo-uplnk-bytes%,%p2p-zattoo-uplnk-pkts%
IPSGSch	IPSG Schema	EMS,IPSG,%date%,%time%,%vpnname%,%vpnid%,%servname%,%servid%,%rad-servaddr%,%rad-servport%,%total-start-req-rcv%,%total-interim-update-req-rcv%,%total-stop-req-rcv%,%total-unknown-req-rcv%,%total-rsp-sent%,%total-start-req-retrans-rcv%,%total-start-rsp-sent%,%total-discard-msgs-unknown-clnt%,%total-discard-msgs-ignore-interim%,%total-discard-msgs-ignore-stop%,%total-discard-msgs-incorrect-secret%,%total-discard-msgs-attr-missing%

Key	Description	Default Value in Config File
ASNGW1Sch	ASNGW1Schema	EMS,ASNGW1,%date%,%time%,%vpnname%,%vpnid%,%servname%,%servid%,%peeripaddr%,%r6mspreattreq-totsent%,%r6mspreattreq-retranssent%,%r6mspreattreq-totrec%,%r6mspreattreq-totacc%,%r6mspreattreq-totdenied%,%r6mspreattreq-totdiscard%,%r6mspreattreq-badform%,%r6mspreattreq-decodeerr%,%r6mspreattreq-unspecerr%,%r6mspreattreq-missmandtlv%,%r6mspreattreq-tlvvalinval%,%r6mspreattreq-unknowntlv%,%r6mspreattreq-duptlvfound%,%r6mspreattreq-nosessfound%,%r6mspreattreq-transiderr%,%r6mspreattrsp-totsent%,%r6mspreattrsp-retranssent%,%r6mspreattrsp-totrec%,%r6mspreattrsp-totacc%,%r6mspreattrsp-totdenied%,%r6mspreattrsp-totdiscard%,%r6mspreattrsp-badform%,%r6mspreattrsp-decodeerr%,%r6mspreattrsp-unspecerr%,%r6mspreattrsp-missmandtlv%,%r6mspreattrsp-tlvvalinval%,%r6mspreattrsp-unknowntlv%,%r6mspreattrsp-duptlvfound%,%r6mspreattrsp-nosessfound%,%r6mspreattrsp-transiderr%,%r6mspreattack-totsent%,%r6mspreattack-retranssent%,%r6mspreattack-totrec%,%r6mspreattack-totacc%,%r6mspreattack-totdenied%,%r6mspreattack-totdiscard%,%r6mspreattack-badform%,%r6mspreattack-decodeerr%,%r6mspreattack-unspecerr%,%r6mspreattack-missmandtlv%,%r6mspreattack-tlvvalinval%,%r6mspreattack-unknowntlv%,%r6mspreattack-duptlvfound%,%r6mspreattack-nosessfound%,%r6mspreattack-transiderr%,%r6contextreq-totsent%,%r6contextreq-retranssent%,%r6contextreq-totrec%,%r6contextreq-totacc%,%r6contextreq-totdenied%,%r6contextreq-totdiscard%,%r6contextreq-badform%,%r6contextreq-decodeerr%,%r6contextreq-unspecerr%,%r6contextreq-missmandtlv%,%r6contextreq-tlvvalinval%,%r6contextreq-unknowntlv%,%r6contextreq-duptlvfound%,%r6contextreq-nosessfound%,%r6contextreq-transiderr%,%r6contextrepo-totsent%,%r6contextrepo-retranssent%,%r6contextrepo-totrec%,%r6contextrepo-totacc%,%r6contextrepo-totdenied%,%r6contextrepo-totdiscard%
ASNGW2Sch	ASNGW2Schema	EMS,ASNGW2,%date%,%time%,%vpnname%,%vpnid%,%servname%,%servid%,%peeripaddr%,%r6contextrepo-badform%,%r6contextrepo-decodeerr%,%r6contextrepo-unspecerr%,%r6contextrepo-missmandtlv%,%r6contextrepo-tlvvalinval%,%r6contextrepo-unknowntlv%,%r6contextrepo-duptlvfound%,%r6contextrepo-nosessfound%,%r6contextrepo-transiderr%,%r6contextack-totsent%,%r6contextack-retranssent%,%r6contextack-totrec%,%r6contextack-totacc%,%r6contextack-totdenied%,%r6contextack-totdiscard%,%r6contextack-badform%,%r6contextack-decodeerr%,%r6contextack-unspecerr%,%r6contextack-missmandtlv%,%r6contextack-tlvvalinval%,%r6contextack-unknowntlv%,%r6contextack-duptlvfound%,%r6contextack-nosessfound%,%r6contextack-transiderr%,%r6autheaptra-totsent%,%r6autheaptra-retranssent%,%r6autheaptra-totrec%,%r6autheaptra-totacc%,%r6autheaptra-totdenied%,%r6autheaptra-totdiscard%,%r6autheaptra-badform%,%r6autheaptra-decodeerr%,%r6autheaptra-unspecerr%,%r6autheaptra-missmandtlv%,%r6autheaptra-tlvvalinval%,%r6autheaptra-unknowntlv%,%r6autheaptra-duptlvfound%,%r6autheaptra-nosessfound%,%r6autheaptra-transiderr%,%r6autheaptra-outofordrcd%,%r6autheapsta-totrec%,%r6autheapsta-totacc%,%r6autheapsta-totdenied%,%r6autheapsta-totdiscard%,%r6autheapsta-badform%,%r6autheapsta-decodeerr%,%r6autheapsta-unspecerr%,%r6autheapsta-missmandtlv%,%r6autheapsta-tlvvalinval%,%r6autheapsta-unknowntlv%,%r6autheapsta-duptlvfound%,%r6autheapsta-nosessfound%,%r6autheapsta-transiderr%,%r6autheapsta-outofordrcd%,%r6autheapsta-noresourcedrop%,%r6autheapsta-bsinireauth%,%r6msattreq-totsent%,%r6msattreq-retranssent%,%r6msattreq-totrec%,%r6msattreq-totacc%,%r6msattreq-totdenied%,%r6msattreq-totdiscard%,%r6msattreq-badform%,%r6msattreq-decodeerr%,%r6msattreq-unspecerr%,%r6msattreq-missmandtlv%,%r6msattreq-tlvvalinval%,%r6msattreq-unknowntlv%

Key	Description	Default Value in Config File
ASNGW3Sch	ASNGW3Schema	EMS,ASNGW3,%date%,%time%,%vpnname%,%vpnid%,%servname%,%servid%,%peeripaddr%,%r6msattreq-duptlvfound%,%r6msattreq-nosessfound%,%r6msattreq-transiderr%,%r6msattrsp-totsent%,%r6msattrsp-retranssent%,%r6msattrsp-totrec%,%r6msattrsp-totacc%,%r6msattrsp-totdenied%,%r6msattrsp-totdiscard%,%r6msattrsp-badform%,%r6msattrsp-decodeerr%,%r6msattrsp-unspecerr%,%r6msattrsp-missmandtlv%,%r6msattrsp-tlvvalinval%,%r6msattrsp-unknowntlv%,%r6msattrsp-duptlvfound%,%r6msattrsp-nosessfound%,%r6msattrsp-transiderr%,%r6msattack-totsent%,%r6msattack-retranssent%,%r6msattack-totrec%,%r6msattack-totacc%,%r6msattack-totdenied%,%r6msattack-totdiscard%,%r6msattack-badform%,%r6msattack-decodeerr%,%r6msattack-unspecerr%,%r6msattack-missmandtlv%,%r6msattack-tlvvalinval%,%r6msattack-unknowntlv%,%r6msattack-duptlvfound%,%r6msattack-nosessfound%,%r6msattack-transiderr%,%r6datapathregreq-totsent%,%r6datapathregreq-retranssent%,%r6datapathregreq-totrec%,%r6datapathregreq-totacc%,%r6datapathregreq-totdenied%,%r6datapathregreq-totdiscard%,%r6datapathregreq-badform%,%r6datapathregreq-decodeerr%,%r6datapathregreq-unspecerr%,%r6datapathregreq-missmandtlv%,%r6datapathregreq-tlvvalinval%,%r6datapathregreq-unknowntlv%,%r6datapathregreq-duptlvfound%,%r6datapathregreq-nosessfound%,%r6datapathregreq-transiderr%,%r6datapathregrsp-totsent%,%r6datapathregrsp-retranssent%,%r6datapathregrsp-totrec%,%r6datapathregrsp-totacc%,%r6datapathregrsp-totdenied%,%r6datapathregrsp-totdiscard%,%r6datapathregrsp-badform%,%r6datapathregrsp-decodeerr%,%r6datapathregrsp-unspecerr%,%r6datapathregrsp-missmandtlv%,%r6datapathregrsp-tlvvalinval%,%r6datapathregrsp-unknowntlv%,%r6datapathregrsp-duptlvfound%,%r6datapathregrsp-nosessfound%,%r6datapathregrsp-transiderr%,%r6datapathregack-totsent%
ASNGW4Sch	ASNGW4Schema	EMS,ASNGW4,%date%,%time%,%vpnname%,%vpnid%,%servname%,%servid%,%peeripaddr%,%r6datapathregack-retranssent%,%r6datapathregack-totrec%,%r6datapathregack-totacc%,%r6datapathregack-totdenied%,%r6datapathregack-totdiscard%,%r6datapathregack-badform%,%r6datapathregack-decodeerr%,%r6datapathregack-unspecerr%,%r6datapathregack-missmandtlv%,%r6datapathregack-tlvvalinval%,%r6datapathregack-unknowntlv%,%r6datapathregack-duptlvfound%,%r6datapathregack-nosessfound%,%r6datapathregack-transiderr%,%r6datapathderegreq-totsent%,%r6datapathderegreq-retranssent%,%r6datapathderegreq-totrec%,%r6datapathderegreq-totacc%,%r6datapathderegreq-totdenied%,%r6datapathderegreq-totdiscard%,%r6datapathderegreq-badform%,%r6datapathderegreq-decodeerr%,%r6datapathderegreq-unspecerr%,%r6datapathderegreq-missmandtlv%,%r6datapathderegreq-tlvvalinval%,%r6datapathderegreq-unknowntlv%,%r6datapathderegreq-duptlvfound%,%r6datapathderegreq-nosessfound%,%r6datapathderegreq-transiderr%,%r6datapathderegrsp-totsent%,%r6datapathderegrsp-retranssent%,%r6datapathderegrsp-totrec%,%r6datapathderegrsp-totacc%,%r6datapathderegrsp-totdenied%,%r6datapathderegrsp-totdiscard%,%r6datapathderegrsp-badform%,%r6datapathderegrsp-decodeerr%,%r6datapathderegrsp-unspecerr%,%r6datapathderegrsp-missmandtlv%,%r6datapathderegrsp-tlvvalinval%,%r6datapathderegrsp-unknowntlv%,%r6datapathderegrsp-duptlvfound%,%r6datapathderegrsp-nosessfound%,%r6datapathderegrsp-transiderr%,%r6keychadir-totsent%,%r6keychadir-retranssent%,%r6keychadir-totrec%,%r6keychadir-totacc%,%r6keychadir-totdenied%,%r6keychadir-totdiscard%,%r6keychadir-badform%,%r6keychadir-decodeerr%,%r6keychadir-unspecerr%,%r6keychadir-missmandtlv%,%r6keychadir-tlvvalinval%,%r6keychadir-unknowntlv%,%r6keychadir-duptlvfound%,%r6keychadir-nosessfound%,%r6keychadir-transiderr%

Key	Description	Default Value in Config File
ASNGW5Sch	ASNGW5Schema	EMS,ASNGW5,%date%,%time%,%vpnname%,%vpnid%,%servname%,%servid%,%peeripaddr%,%r6keychaack-totsent%,%r6keychaack-retranssent%,%r6keychaack-totrec%,%r6keychaack-totacc%,%r6keychaack-totdenied%,%r6keychaack-totdiscard%,%r6keychaack-badform%,%r6keychaack-decodeerr%,%r6keychaack-unspecerr%,%r6keychaack-missmandtlv%,%r6keychaack-tlvvalinval%,%r6keychaack-unknowntlv%,%r6keychaack-duptlvfound%,%r6keychaack-nosessfound%,%r6keychaack-transiderr%,%r6unknown-totrec%,%r6unknown-totacc%,%r6unknown-totdenied%,%r6unknown-totdiscard%,%r6unknown-badform%,%r6unknown-decodeerr%,%r6unknown-unspecerr%,%r6unknown-missmandtlv%,%r6unknown-tlvvalinval%,%r6unknown-unknowntlv%,%r6unknown-duptlvfound%,%r6unknown-nosessfound%,%r6unknown-transiderr%,%r6datagrerec-totpackrec%,%r6datagrerec-prottyperrror%,%r6datagrerec-totbytrec%,%r6datagrerec-grekeyabs%,%r6datagrerec-grechkerr%,%r6datagrerec-invpacklen%,%r6datagrerec-nosessfou%,%r6datagrerec-unspecerr%,%r6datagresend-totpacksent%,%r6datagresend-senderr%,%r6datagresend-totbytsent%,%r6datagresend-unspeerr%
SGSN1Sch	SGSN1Schema	EMS,SGSN1,%date%,%time%,%vpnname%,%vpnid%,%servname%,%3G-attached%,%2G-attached%,%3G-home-subscribers%,%2G-home-subscribers%,%3G-visiting-national%,%2G-visiting-national%,%3G-visiting-foreign%,%2G-visiting-foreign%,%pmm-connected%,%pmm-idle%,%3G-IMSI-Attch%,%2G-IMSI-Attch%,%3G-ptmsi-Attch%,%2G-ptmsi-Attch%,%3G-attach-accept%,%2G-attch-accept%,%3G-attach-complete%,%2G-attach-complete%,%3G-attach-reject%,%2G-attach-reject%,%3G-intra-rau%,%2G-intra-rau%,%3G-periodic-rau%,%2G-periodic-rau%,%3G-inter-sgsn-rau%,%2G-inter-sgsn-rau%,%3G-rau-complete%,%2G-rau-complete%,%3G-rau-reject%,%2G-rau-reject%,%3G-ms-init-detach%,%2G-ms-init-detach%,%3G-nw-init-detach%,%2G-nw-init-detach%,%3G-ms-init-detach-accept%,%2G-ms-init-detach-accept%,%3G-nw-init-detach-accept%,%2G-nw-init-detach-accept%,%3G-signalling-service-request%,%2G-signalling-service-request%,%3G-data-service-request%,%2G-data-service-request%,%3G-service-response%,%2G-service-response%,%3G-service-reject%,%2G-service-reject%,%3G-paging-request%,%2G-paging-request%,%3G-gmm-status-sent%,%2G-gmm-status-sent%,%3G-gmm-status-rcvd%,%2G-gmm-status-rcvd%,%3G-auth-cipher-request%,%2G-auth-cipher-request%,%3G-auth-cipher-response%,%2G-auth-cipher-response%,%3G-auth-cipher-reject%,%2G-auth-cipher-reject%,%3G-auth-cipher-mac-fail%,%2G-auth-cipher-mac-fail%,%3G-auth-cipher-syn-fail%,%2G-auth-cipher-syn-fail%,%3G-ptmsi-realloc%,%2G-ptmsi-realloc%,%3G-ptmsi-realloc-complete%,%2G-ptmsi-realloc-complete%,%3G-imsi-identity-request%,%2G-imsi-identity-request%,%3G-imeisv-identity-request%,%2G-imeisv-identity-request%,%3G-imsi-identity-response%,%2G-imsi-identity-response%,%3G-imeisv-identity-response%,%2G-imeisv-identity-response%,%3G-unknown-identity-response%,%2G-unknown-identity-response%
SGSN2Sch	SGSN2Schema	EMS,SGSN2,%date%,%time%,%vpnname%,%vpnid%,%servname%,%common-id-sent%,%sec-mode-command%,%sec-mode-complete%,%sec-mode-reject%,%Iu-release-request%,%Iu-release-command%,%Iu-release-complete%,%Reset-received%,%Retransmitted-reset-received%,%Reset-Ack-sent%,%Reset-sent%,%Retransmitted-reset-sent%,%Reset-Ack-received%,%Resource-reset-received%,%Resource-reset-ack-sent%,%Resource-reset-sent%,%Resource-reset-ack-received%,%Error-indication-rcvd%,%Relocation-required%,%Relocation-command%,%Relocation-request%,%Relocation-request-ack%,%Relocation-failure%,%Relocation-prep-failure%,%Relocation-cancel%,%Relocation-cancel-ack%,%Relocation-detect%,%Relocation-complete%,%Forward-srns-context%,%GMM-received-nas-pdu%,%GMM-sent-nas-pdu%,%SM-received-nas-pdu%,%SM-sent-nas-pdu%,%Unidentified-nas-pdu%,%3G-total-actv-req%,%3G-total-actv-accept%,%3G-ms-modify-req%,%3G-ms-modify-accept%,%3G-nw-modify-req%,%3G-nw-modify-accept%,%3G-ms-deactv-req%,%3G-ms-deactv-accept%,%3G-sgsn-init-deact-req%,%3G-sgsn-init-deact-acc%,%RNC-rab-modify-req%,%RNC-rab-rel-req%,%rab-assign-req%,%rab-assign-rsp%,%rab-set/mod-req%,%rab-set/mod-acc%,%rab-rel-req%,%rab-rel-accept%,%map-open-req-tx%,%map-open-req-rx%,%map-open-rsp-tx%,%map-open-rsp-rx%,%map-close-tx%,%map-close-rx%,%map-abort-tx%,%map-abort-rx%,%map-gprs-update-loc-req-tx%,%map-gprs-update-loc-rsp-tx%,%map-gprs-update-loc-err-tx%,%map-gprs-update-loc-timeouts-rx%,%map-cancel-loc-req-rx%,%map-cancel-loc-rsp-tx%,%map-cancel-loc-err-tx%,%map-del-subs-req-rx%,%map-del-subs-rsp-tx%,%map-del-subs-ret-tx%,%map-auth-timeouts-rcvd%,%map-purge-timeouts-rcvd%,%map-insert-subs-rcvd%,%map-standalone-isd-rcvd%,%map-isd-rsp-tx%,%map-isd-err-tx%,%map-auth-fail-rept-req-tx%,%map-auth-fail-rept-rsp-rx%,%map-auth-fail-rept-err-rx%

Key	Description	Default Value in Config File
SGSN3Sch	SGSN3 Schema	EMS,SGSN3,%date%,%time%,%vpnname%,%vpnid%,%servname%,%map-auth-fail-rept-timeouts-rcvd%,%map-hlr-reset-rcvd%,%tcap-total-active-trans%,%tcap-total-active-invoks%,%tcap-total-msg-drops%,%tcap-total-msg-rcvd%,%tcap-total-msg-sent%,%tcap-total-abort-rcvd%,%tcap-total-abort-sent%,%tcap-total-comp-rx%,%tcap-total-comp-tx%,%tcap-comp-reterr-rx%,%tcap-comp-reterr-tx%,%tcap-comp-retrej-rx%,%tcap-comp-retrej-tx%,%tcap-tran-incorrect-rx%,%tcap-tran-incorrect-tx%,%tcap-tran-badformed-rx%,%tcap-tran-badformed-tx%,%tcap-tran-unrecognised-rx%,%tcap-tran-unrecognised-tx%,%tcap-comp-incorrect-rx%,%tcap-comp-incorrect-tx%,%tcap-comp-badformed-rx%,%tcap-comp-badformed-tx%,%tcap-comp-unrec-invid-res-rx%,%tcap-comp-unrec-invid-res-tx%,%tcap-comp-unexp-res-rx%,%tcap-comp-unexp-res-tx%,%tcap-user-unrec-opcode-rx%,%tcap-user-unrec-opcode-tx%,%tcap-user-incorr-params-rx%,%tcap-user-incorr-params-tx%,%tcap-user-resourcelimit-rx%,%tcap-user-resourcelimit-tx%,%rab-set/mod-tmr-expired%,%rab-rel-tmr-expired%,%3G-rau-accept-intra%,%3G-rau-accept-inter%,%2G-rau-accept-intra%,%2G-rau-accept-inter%,%3G-attached-with-pdp%,%3G-attached-no-pdp%,%3G-gmm-info-sent%,%2G-gmm-info-sent%,%3G-auth-cipher-rsp-sres-mismatch%,%2G-auth-cipher-rsp-sres-mismatch%,%3G-auth-unacceptable%,%2G-auth-unacceptable%,%3G-imei-identity-request%,%2G-imei-identity-request%,%3G-imei-identity-response%,%2G-imei-identity-response%,%Initial-UE-Rcvd%,%Direct-Trans-Rcvd%,%Error-indication-sent%,%3G-total-num-actv-pdp%,%3G-primary-actv-req%,%3G-primary-actv-accept%,%3G-primary-actv-reject%,%3G-secondary-actv-req%,%3G-secondary-actv-acc%,%3G-secondary-actv-rej%,%3G-dupl-ti-pdpactive%,%3G-dupl-nsapi-pdpactv%,%3G-dupl-pdpaddr-apn-pdpactv%,%3G-dupl-ti-n-pdpactive%,%3G-dupl-pdpaddr-apn-n-pdpactv%,%3G-ms-modify-rej%,%3G-nw-modify-rej%,%3G-ms-deactv-reject%
SGSN4Sch	SGSN4 Schema	EMS,SGSN4,%date%,%time%,%vpnname%,%vpnid%,%servname%,%3G-sgsn-init-deact-rej%,%3G-total-sm-status-req-rx%,%3G-total-sm-status-req-tx%,%RNC-rab-modify-num%,%RNC-rab-rel-num%,%rab-set/mod-fail%,%rab-rel-fail%,%rab-queued%,%total-rab-rej%,%SRNS-ctxt-req-sent%,%SRNS-ctxt-rsp-rcvd%,%SRNS-ctxt-req-tmr-expired%,%SRNS-ctxt-total-pdp-acc%,%SRNS-ctxt-total-pdp-rej%,%SRNS-data-fwd-cmd-sent%,%map-auth-req-tx%,%map-auth-succes%,%map-auth-fail%,%map-imei-req-tx%,%map-imei-succes%,%map-imei-fail%,%map-imei-timeout%,%map-purge-req-tx%,%map-purge-success%,%map-purge-fail%,%tcap-uni-dir-msg-rcvd%,%tcap-uni-dir-msg-sent%,%tcap-begin-msg-rcvd%,%tcap-begin-msg-sent%,%tcap-continue-msg-rcvd%,%tcap-continue-msg-sent%,%tcap-end-msg-rcvd%,%tcap-end-msg-sent%,%tcap-total-comp-invoke-rx%,%tcap-total-comp-invoke-tx%,%tcap-comp-retresult-rx%,%tcap-comp-retresult-tx%,%tcap-tran-unrec-msgtype-rx%,%tcap-tran-unrec-msgtype-tx%,%tcap-tran-resource-limit-rx%,%tcap-tran-resource-limit-tx%,%tcap-comp-unrecognised-rx%,%tcap-comp-unrecognised-tx%,%tcap-comp-unrec-linkid-rx%,%tcap-comp-unrec-linkid-tx%,%tcap-comp-unrec-invid-err-rx%,%tcap-comp-unrec-invid-err-tx%,%tcap-comp-unexp-err-rx%,%tcap-comp-unexp-err-tx%,%tcap-user-duplicate-invid-rx%,%tcap-user-duplicate-invid-tx%,%tcap-user-unexp-linked-resp-rx%,%tcap-user-unexp-linked-resp-tx%,%tcap-user-unexp-linked-oper-rx%,%tcap-user-unexp-linked-oper-tx%,%tcap-user-res-incorr-params-rx%,%tcap-user-res-incorr-params-tx%,%tcap-user-res-unrec-errcode-rx%,%tcap-user-res-unrec-errcode-tx%,%tcap-user-res-unexp-errcode-rx%,%tcap-user-res-unexp-errcode-tx%,%tcap-user-err-incorr-params-rx%,%tcap-user-err-incorr-params-tx%,%tcap-user-initiate-release-rx%,%tcap-user-initiate-release-tx%,%3G-dupl-nsapi-n-pdpactv%,%Direct-Trans-Sent%,%3G-T3350-expiry%

Key	Description	Default Value in Config File
SGSN5Sch	SGSN5 Schema	EMS,SGSN5,%date%,%time%,%vpnname%,%vpnid%,%servname%,%2G-T3350-expiry%,%3G-T3360-expiry%,%2G-T3360-expiry%,%3G-T3370-expiry%,%2G-T3370-expiry%,%3G-T3322-expiry%,%2G-T3322-expiry%,%3G-T3313-expiry%,%2G-T3313-expiry%,%mcc%,%mnc%,%lac%,%rac%,%2G-local-ptmsi-Attch%,%2G-paging-success%,%2G-remote-ptmsi-Attch%,%3G-actv-rej-apn-restriction-incompatible%,%3G-actv-rej-by-ggsn%,%3G-actv-rej-conditional-ie-err%,%3G-actv-rej-ie-non-existent%,%3G-actv-rej-insufficient-resources%,%3G-actv-rej-invalid-mandatory-info%,%3G-actv-rej-missing-or-unknown-apn%,%3G-actv-rej-msg-not-compatible-with-prot-state%,%3G-actv-rej-msg-type-non-existent%,%3G-actv-rej-network-failure%,%3G-actv-rej-odb%,%3G-actv-rej-pdp-notft-actv%,%3G-actv-rej-prot-err-unspecified%,%3G-actv-rej-recovery-on-timer-expiry%,%3G-actv-rej-semantically-incorrect%,%3G-actv-rej-semantic-err-in-pkt-filter%,%3G-actv-rej-semantic-error-tft-operation%,%3G-actv-rej-service-not-subscribed%,%3G-actv-rej-service-not-supported%,%3G-actv-rej-svc-opt-tmp-out-of-order%,%3G-actv-rej-syntax-err-in-pkt-filter%,%3G-actv-rej-syntax-err-in-tft-operation%,%3G-actv-rej-unknown-pdp-addr-type%,%3G-actv-rej-unknown-pdp-context%,%3G-actv-rej-unspecified-error%,%3G-actv-rej-usr-auth-failed%,%3G-attach-rej-congestion%,%3G-attach-rej-illegal-me%,%3G-attach-rej-illegal-ms%,%3G-attach-rej-implicitly-detach%,%3G-attach-rej-imsi-unknown-at-hlr%,%3G-attach-rej-network-failure%,%3G-attach-rej-plmn-not-allowed%,%3G-attach-rej-unknown-cause%,%3G-detached%,%3G-ggsn-init-deact-acc%,%3G-ggsn-init-deact-rej%,%3G-ggsn-init-deact-req%,%3G-gprs-and-non-gprs-service-not-allowed%,%3G-gprs-service-not-allowed%,%3G-gprs-service-not-allowed-in-this-plmn%,%3G-hlr-init-deact-acc%,%3G-hlr-init-deact-rej%,%3G-hlr-init-deact-req%,%3G-local-ptmsi-Attch%
SGSN6Sch	SGSN6 Schema	EMS,SGSN6,%date%,%time%,%vpnname%,%vpnid%,%servname%,%3G-no-suitable-cells-in-location-area%,%3G-paging-success%,%3G-total-attach-req%,%exist-conn-proc-rej-overload%,%new-connection-rejected-overload%,%3G-total-actv-pdp-with-dir-tunnel%,%3G-remote-ptmsi-Attch%,%3G-roaming-not-allowed-in-this-location-area%,%3G-inter-rau-reject%,%3G-total-inter-rau-failure%,%3G-rau-accept-periodic%,%3G-periodic-rau-reject%,%3G-total-periodic-rau-failure%,%3G-intra-rau-reject%,%3G-total-intra-rau-failure%,%3G-total-attach-fail%,%3G-total-actv-reject%,%3G-total-actv-fail%,%3G-intra-rau-rej-imsi-unknown-hlr%,%2G-intra-rau-rej-imsi-unknown-hlr%,%3G-intra-rau-rej-illegal-ms%,%2G-intra-rau-rej-illegal-ms%,%3G-intra-rau-rej-illegal-me%,%2G-intra-rau-rej-illegal-me%,%3G-intra-rau-rej-gprs-svc-not-allw%,%2G-intra-rau-rej-gprs-svc-not-allw%,%3G-intra-rau-rej-nongprs-svc-not-allow%,%2G-intra-rau-rej-nongprs-svc-not-allow%,%3G-intra-rau-rej-msid-not-derived-by-nw%,%2G-intra-rau-rej-msid-not-derived-by-nw%,%3G-intra-rau-rej-implicitly-detach%,%2G-intra-rau-rej-implicitly-detach%,%3G-intra-rau-rej-plmn-not-allowed%,%2G-intra-rau-rej-plmn-not-allowed%,%3G-intra-rau-rej-loc-area-not-allow%,%2G-intra-rau-rej-loc-area-not-allow%,%3G-intra-rau-rej-roam-not-allow-larea%,%2G-intra-rau-rej-roam-not-allow-larea%,%3G-intra-rau-rej-gprs-svc-not-allow-plmn%,%2G-intra-rau-rej-gprs-svc-not-allow-plmn%,%3G-intra-rau-rej-no-cells-in-loc-area%,%2G-intra-rau-rej-no-cells-in-loc-area%,%3G-intra-rau-rej-msc-not-reachable%,%2G-intra-rau-rej-msc-not-reachable%,%3G-intra-rau-rej-network-failure%,%2G-intra-rau-rej-network-failure%,%3G-intra-rau-rej-mac-failure%,%2G-intra-rau-rej-mac-failure%,%3G-intra-rau-rej-syn-failure%,%2G-intra-rau-rej-syn-failure%,%3G-intra-rau-rej-congestion%,%2G-intra-rau-rej-congestion%

Key	Description	Default Value in Config File
SGSN7Sch	SGSN7 Schema	EMS,SGSN7,%date%,%time%,%vpnname%,%vpnid%,%servname%,%3G-intra-rau-rej-gsm-auth-unacceptable%,%2G-intra-rau-rej-gsm-auth-unacceptable%,%3G-intra-rau-rej-no-pdp-ctx-actv%,%2G-intra-rau-rej-no-pdp-ctx-actv%,%3G-intra-rau-rej-retry-from-new-cell%,%2G-intra-rau-rej-retry-from-new-cell%,%3G-intra-rau-rej-inval-mand-info%,%2G-intra-rau-rej-inval-mand-info%,%3G-intra-rau-rej-msg-type-non-exist%,%2G-intra-rau-rej-msg-type-non-exist%,%3G-intra-rau-rej-mtype-incompat-pstate%,%2G-intra-rau-rej-mtype-incompat-pstate%,%3G-intra-rau-rej-ie-non-existent%,%2G-intra-rau-rej-ie-non-existent%,%3G-intra-rau-rej-cond-ie-error%,%2G-intra-rau-rej-cond-ie-error%,%3G-intra-rau-rej-msg-incompat-prot-state%,%2G-intra-rau-rej-msg-incompat-prot-state%,%3G-intra-rau-rej-prot-error%,%2G-intra-rau-rej-prot-error%,%3G-intra-rau-rej-unknown-error%,%2G-intra-rau-rej-unknown-error%,%3G-intra-prau-rej-imsi-unknown-hlr%,%2G-intra-prau-rej-imsi-unknown-hlr%,%3G-intra-prau-rej-illegal-ms%,%2G-intra-prau-rej-illegal-ms%,%3G-intra-prau-rej-illegal-me%,%2G-intra-prau-rej-illegal-me%,%3G-intra-prau-rej-gprs-svc-not-allow%,%2G-intra-prau-rej-gprs-svc-not-allow%,%3G-intra-prau-rej-nongprs-svc-not-allow%,%2G-intra-prau-rej-nongprs-svc-not-allow%,%3G-intra-prau-rej-msid-not-derived-by-nw%,%2G-intra-prau-rej-msid-not-derived-by-nw%,%3G-intra-prau-rej-implicitly-detach%,%2G-intra-prau-rej-implicitly-detach%,%3G-intra-prau-rej-plmn-not-allowed%,%2G-intra-prau-rej-plmn-not-allowed%,%3G-intra-prau-rej-loc-area-not-allowed%,%2G-intra-prau-rej-loc-area-not-allowed%,%3G-intra-prau-rej-roam-not-allowed-larea%,%2G-intra-prau-rej-roam-not-allowed-larea%,%3G-intra-prau-rej-gprs-svc-not-allowed-plmn%,%2G-intra-prau-rej-gprs-svc-not-allowed-plmn%,%3G-intra-prau-rej-congestion%,%2G-intra-prau-rej-congestion%
SGSN8Sch	SGSN8 Schema	EMS,SGSN8,%date%,%time%,%vpnname%,%vpnid%,%servname%,%3G-intra-prau-rej-gsm-auth-unacceptable%,%2G-intra-prau-rej-gsm-auth-unacceptable%,%3G-intra-prau-rej-no-pdp-ctx-actv%,%2G-intra-prau-rej-no-pdp-ctx-actv%,%3G-intra-prau-rej-retry-from-new-cell%,%2G-intra-prau-rej-retry-from-new-cell%,%3G-intra-prau-rej-sem-wrong-msg%,%2G-intra-prau-rej-sem-wrong-msg%,%3G-intra-prau-rej-inval-mand-info%,%2G-intra-prau-rej-inval-mand-info%,%3G-intra-prau-rej-msg-type-non-exist%,%2G-intra-prau-rej-msg-type-non-exist%,%3G-intra-prau-rej-mtype-incompat-pstate%,%2G-intra-prau-rej-mtype-incompat-pstate%,%3G-intra-prau-rej-ie-non-existent%,%2G-intra-prau-rej-ie-non-existent%,%3G-intra-prau-rej-cond-ie-error%,%2G-intra-prau-rej-cond-ie-error%,%3G-intra-prau-rej-msg-incompat-pstate%,%2G-intra-prau-rej-msg-incompat-pstate%,%3G-intra-prau-rej-prot-error%,%2G-intra-prau-rej-prot-error%,%3G-intra-prau-rej-unknown-error%,%2G-intra-prau-rej-unknown-error%,%3G-inter-rau-rej-imsi-unknown-hlr%,%2G-inter-rau-rej-imsi-unknown-hlr%,%3G-inter-rau-rej-illegal-ms%,%2G-inter-rau-rej-illegal-ms%,%3G-inter-rau-rej-illegal-me%,%2G-inter-rau-rej-illegal-me%,%3G-inter-rau-rej-gprs-svc-not-allow%,%2G-inter-rau-rej-gprs-svc-not-allow%,%3G-inter-rau-rej-nongprs-svc-not-allow%,%2G-inter-rau-rej-nongprs-svc-not-allow%,%3G-inter-rau-rej-msid-not-derived-by-nw%,%2G-inter-rau-rej-msid-not-derived-by-nw%,%3G-inter-rau-rej-implicitly-detach%,%2G-inter-rau-rej-implicitly-detach%,%3G-inter-rau-rej-plmn-not-allowed%,%2G-inter-rau-rej-plmn-not-allowed%,%3G-inter-rau-rej-loc-area-not-allowed%,%2G-inter-rau-rej-loc-area-not-allowed%,%3G-inter-rau-rej-roam-not-allowed-larea%,%2G-inter-rau-rej-roam-not-allowed-larea%,%3G-inter-rau-rej-gprs-svc-not-allowed-plmn%,%2G-inter-rau-rej-gprs-svc-not-allowed-plmn%

Key	Description	Default Value in Config File
SGSN9Sch	SGSN9 Schema	EMS,SGSN9,%date%,%time%,%vpnname%,%vpnid%,%servname%,%3G-inter-rau-rej-no-cells-in-location-area%,%2G-inter-rau-rej-no-cells-in-location-area%,%3G-inter-rau-rej-msc-not-reachable%,%2G-inter-rau-rej-msc-not-reachable%,%3G-inter-rau-rej-network-failure%,%2G-inter-rau-rej-network-failure%,%3G-inter-rau-rej-mac-failure%,%2G-inter-rau-rej-mac-failure%,%3G-inter-rau-rej-syn-failure%,%2G-inter-rau-rej-syn-failure%,%3G-inter-rau-rej-congestion%,%2G-inter-rau-rej-congestion%,%3G-inter-rau-rej-gsm-auth-unacceptable%,%2G-inter-rau-rej-gsm-auth-unacceptable%,%3G-inter-rau-rej-no-pdp-ctx-actv%,%2G-inter-rau-rej-no-pdp-ctx-actv%,%3G-inter-rau-rej-retry-from-new-cell%,%2G-inter-rau-rej-retry-from-new-cell%,%3G-inter-rau-rej-sem-wrong-msg%,%2G-inter-rau-rej-sem-wrong-msg%,%3G-inter-rau-rej-inval-mand-info%,%2G-inter-rau-rej-inval-mand-info%,%3G-inter-rau-rej-msg-type-non-exist%,%2G-inter-rau-rej-msg-type-non-exist%,%3G-inter-rau-rej-mtype-incompat-pstate%,%2G-inter-rau-rej-mtype-incompat-pstate%,%3G-inter-rau-rej-ie-non-existent%,%2G-inter-rau-rej-ie-non-existent%,%3G-inter-rau-rej-cond-ie-error%,%2G-inter-rau-rej-cond-ie-error%,%3G-inter-rau-rej-msg-not-compat-pstate%,%2G-inter-rau-rej-msg-not-compat-pstate%,%3G-inter-rau-rej-prot-error%,%2G-inter-rau-rej-prot-error%,%3G-inter-rau-rej-unknown-error%,%2G-inter-rau-rej-unknown-error%,%3G-intra-ra-upd-rau-fail-iu_release%,%3G-intra-ra-upd-rau-fail-ongoing-proc%,%2G-intra-ra-upd-rau-fail-ongoing-proc%,%3G-intra-perio-rau-fail-iu_release%,%3G-intra-perio-rau-fail-ongoing-proc%,%2G-intra-perio-rau-fail-ongoing-proc%,%3G-inter-rau-fail-iu_release%,%3G-inter-rau-fail-ongoing-proc%,%2G-inter-rau-fail-ongoing-proc%,%3G-attach-fail-iu_release%,%3G-attach-fail-ongoing-proc%,%2G-attach-fail-ongoing-proc%
SGSNASch	SGSNA Schema	EMS,SGSNA,%date%,%time%,%vpnname%,%vpnid%,%servname%,%2G-total-attach-fail%,%3G-total-rau-failure%,%2G-total-rau-failure%,%2G-rau-accept-periodic%,%3G-ret-rau-accept-periodic%,%2G-ret-rau-accept-periodic%,%2G-intra-rau-reject%,%2G-periodic-rau-reject%,%2G-inter-rau-reject%,%2G-total-intra-rau-failure%,%2G-total-periodic-rau-failure%,%2G-total-inter-rau-failure%,%2G-total-actv-req%,%2G-total-actv-accept%,%2G-total-num-actv-pdp%,%2G-primary-actv-req%,%2G-primary-actv-accept%,%2G-total-actv-reject%,%2G-primary-actv-reject%,%2G-secondary-actv-req%,%2G-secondary-actv-acc%,%2G-secondary-actv-rej%,%2G-actv-rej-odb%,%2G-actv-rej-insufficient-resources%,%2G-actv-rej-network-failure%,%2G-actv-rej-missing-or-unknown-apn%,%2G-actv-rej-unknown-pdp-addr-type%,%2G-actv-rej-usr-auth-failed%,%2G-actv-rej-by-ggsn%,%2G-actv-rej-unspecified-error%,%2G-actv-rej-service-not-supported%,%2G-actv-rej-service-not-subscribed%,%2G-actv-rej-svc-opt-tmp-out-of-order%,%2G-actv-rej-apn-restriction-incompatible%,%2G-actv-rej-semantically-incorrect%,%2G-actv-rej-invalid-mandatory-info%,%2G-actv-rej-msg-type-non-existent%,%2G-actv-rej-ie-non-existent%,%2G-actv-rej-conditional-ie-err%,%2G-actv-rej-msg-not-compatible-with-prot-state%,%2G-actv-rej-recovery-on-timer-expiry%,%2G-actv-rej-prot-err-unspecified%,%2G-actv-rej-llc-sndcp-fail%,%2G-actv-rej-qos-not-acc%,%2G-actv-rej-semantic-error-tft-operation%,%2G-actv-rej-syntax-err-in-tft-operation%,%2G-actv-rej-unknown-pdp-context%,%2G-actv-rej-semantic-err-in-pkt-filter%,%2G-actv-rej-syntax-err-in-pkt-filter%,%2G-actv-rej-pdp-notft-actv%,%2G-dupl-ti-pdpactive%,%2G-dupl-nsapi-pdpactv%,%2G-dupl-pdpaddr-apn-pdpactv%,%2G-dupl-ti-n-pdpactive%,%2G-dupl-nsapi-n-pdpactv%,%2G-dupl-pdpaddr-apn-n-pdpactv%

Key	Description	Default Value in Config File
SGSNBSch	SGSNB Schema	EMS,SGSNB,%date%,%time%,%vpnname%,%vpnid%,%servname%,%2G-ms-modify-req%,%2G-ms-modify-accept%,%2G-ms-modify-rej%,%2G-nw-modify-req%,%2G-nw-ret-modify-req%,%2G-nw-modify-accept%,%2G-nw-modify-rej%,%2G-modify-rej-insufficient-resources%,%2G-modify-rej-service-opt-not-supported%,%2G-modify-rej-semantic-err-tft-operation%,%2G-modify-rej-syntax-err-tft-operation%,%2G-modify-rej-semnatic-err-pkt-filter%,%2G-modify-rej-syntax-err-pkt-filter%,%2G-modify-rej-semnatic-incorrect-message%,%2G-modify-rej-invalid-mand-info%,%2G-modify-rej-msg-non-existent%,%2G-modify-rej-ie-non-existent%,%2G-modify-rej-conditional-ie-err%,%2G-modify-rej-msg-not-compatible-prot-state%,%2G-modify-rej-rcvry-on-tmr-expiry%,%2G-modify-rej-prot-err-unspec%,%2G-ms-deactv-req%,%2G-ms-deactv-accept%,%2G-ms-deactv-reject%,%2G-ms-deactv-rej-rx-odb%,%2G-ms-deactv-rej-rx-mbms-cap-insuff-res%,%2G-ms-deactv-rej-rx-llc-sndcp-fail-gb%,%2G-ms-deactv-rej-rx-insuff-res%,%2G-ms-deactv-rej-rx-miss-unkwn-apn%,%2G-ms-deactv-rej-rx-unkwn-pdp-addr%,%2G-ms-deactv-rej-rx-usr-auth-fail%,%2G-ms-deactv-rej-rx-actv-rej-ggsn%,%2G-ms-deactv-rej-rx-actv-rej-unspec%,%2G-ms-deactv-rej-rx-service-opt-no-support%,%2G-ms-deactv-rej-rx-service-opt-no-subs%,%2G-ms-deactv-rej-rx-svc-opt-temp-out-order%,%2G-ms-deactv-rej-rx-nsapi-already-used%,%2G-ms-deactv-rej-rx-reg-deactv%,%2G-ms-deactv-rej-rx-qos-not-acc%,%2G-ms-deactv-rej-rx-nwt-fail%,%2G-ms-deactv-rej-rx-reactivation-req%,%2G-ms-deactv-rej-rx-no-feature-support%,%2G-ms-deactv-rej-rx-sem-err-tft-op%,%2G-ms-deactv-rej-rx-syn-err-tft-op%,%2G-ms-deactv-rej-rx-unknown-ctx%,%2G-ms-deactv-rej-rx-ctx-no-tft-already-actv%,%2G-ms-deactv-rej-rx-mcast-grp-mem-tout%,%2G-ms-deactv-rej-rx-sem-err-pkt-filter%,%2G-ms-deactv-rej-rx-syn-err-pkt-filter%,%2G-ms-deactv-rej-rx-invalid-trans-id%
SGSNCSch	SGSNC Schema	EMS,SGSNC,%date%,%time%,%vpnname%,%vpnid%,%servname%,%2G-ms-deactv-rej-rx-sem-incorrect-msg%,%2G-ms-deactv-rej-rx-inval-mand-info%,%2G-ms-deactv-rej-rx-msg-non-existent%,%2G-ms-deactv-rej-rx-ie-non-existent%,%2G-ms-deactv-rej-rx-cond-ie-err%,%2G-ms-deactv-rej-rx-prot-err-unspec%,%2G-ms-deactv-rej-rx-apn-rest-incomap-actv-pdp%,%2G-ms-deactv-rej-rx-msg-not-compat-prot-state%,%2G-ms-deactv-rej-rx-rcvry-on-tmr-expiry%,%2G-sgsn-init-deact-req%,%2G-sgsn-init-deact-acc%,%2G-sgsn-init-deact-rej%,%2G-ggsn-init-deact-req%,%2G-ggsn-init-deact-acc%,%2G-ggsn-init-deact-rej%,%2G-hlr-init-deact-req%,%2G-hlr-init-deact-acc%,%2G-hlr-init-deact-rej%,%2G-nw-deactv-rej-tx-odb%,%2G-nw-deactv-rej-tx-mbms-cap-insuff-res%,%2G-nw-deactv-rej-tx-llc-sndcp-fail-gb%,%2G-nw-deactv-rej-tx-insuff-res%,%2G-nw-deactv-rej-tx-miss-unkwn-apn%,%2G-nw-deactv-rej-tx-unkwn-pdp-addr%,%2G-nw-deactv-rej-tx-usr-auth-fail%,%2G-nw-deactv-rej-tx-actv-rej-ggsn%,%2G-nw-deactv-rej-tx-actv-rej-unspec%,%2G-nw-deactv-rej-tx-service-opt-no-support%,%2G-nw-deactv-rej-tx-service-opt-no-subs%,%2G-nw-deactv-rej-tx-svc-opt-temp-out-order%,%2G-nw-deactv-rej-tx-nsapi-already-used%,%2G-nw-deactv-rej-tx-reg-deactv%,%2G-nw-deactv-rej-tx-qos-not-acc%,%2G-nw-deactv-rej-tx-nwt-fail%,%2G-nw-deactv-rej-tx-reactivation-req%,%2G-nw-deactv-rej-tx-no-feature-support%,%2G-nw-deactv-rej-tx-sem-err-tft-op%,%2G-nw-deactv-rej-tx-syn-err-tft-op%,%2G-nw-deactv-rej-tx-unknown-ctx%,%2G-nw-deactv-rej-tx-ctx-no-tft-already-actv%,%2G-nw-deactv-rej-tx-mcast-grp-mem-tout%,%2G-nw-deactv-rej-tx-sem-err-pkt-filter%,%2G-nw-deactv-rej-tx-syn-err-pkt-filter%,%2G-nw-deactv-rej-tx-invalid-trans-id%,%2G-nw-deactv-rej-tx-sem-incorrect-msg%,%2G-nw-deactv-rej-tx-inval-mand-info%,%2G-nw-deactv-rej-tx-msg-non-existent%,%2G-nw-deactv-rej-tx-ie-non-existent%
SGSNDSch	SGSND Schema	EMS,SGSND,%date%,%time%,%vpnname%,%vpnid%,%servname%,%2G-nw-deactv-rej-tx-cond-ie-err%,%2G-nw-deactv-rej-tx-prot-err-unspec%,%2G-nw-deactv-rej-tx-apn-rest-incomap-actv-pdp%,%2G-nw-deactv-rej-tx-msg-not-compat-prot-state%,%2G-nw-deactv-rej-tx-rcvry-on-tmr-expiry%,%2G-total-sm-status-req-rx%,%2G-total-sm-status-req-tx%

Key	Description	Default Value in Config File
SGTPSch	SGTP Schema	EMS,SGTP,%date%,%time%,%vpn-name%,%vpn-id%,%service-name%,%sgtpc-cpc-req-v1-pri%,%sgtpc-cpc-req-v0-pri%,%sgtpc-cpc-req-sec%,%sgtpc-cpc-req-accept%,%sgtpc-cpc-rsp-v1-pri%,%sgtpc-cpc-rsp-v0-pri%,%sgtpc-cpc-rsp-sec%,%sgtpc-upc-req-v1-tx%,%sgtpc-upc-req-v0-tx%,%sgtpc-upc-req-v1-rx%,%sgtpc-upc-req-v0-rx%,%sgtpc-upc-req-accept-tx%,%sgtpc-upc-req-accept-rx%,%sgtpc-dpc-req-v1-tx%,%sgtpc-dpc-req-v0-tx%,%sgtpc-dpc-req-v1-rx%,%sgtpc-dpc-req-v0-rx%,%sgtpc-dpc-req-accept-tx%,%sgtpc-dpc-req-accept-rx%,%sgtpc-ident-req-v1-tx%,%sgtpc-ident-req-v0-tx%,%sgtpc-ident-req-v1-rx%,%sgtpc-ident-req-v0-rx%,%sgtpc-ident-req-accept-tx%,%sgtpc-ident-req-accept-rx%,%sgtpc-sgsn-ctxt-req-v1-tx%,%sgtpc-sgsn-ctxt-req-v0-tx%,%sgtpc-sgsn-ctxt-req-v1-rx%,%sgtpc-sgsn-ctxt-req-v0-rx%,%sgtpc-sgsn-ctxt-req-accept-tx%,%sgtpc-sgsn-ctxt-req-accept-rx%,%sgtpc-sgsn-ctxt-ack-accept-tx%,%sgtpc-sgsn-ctxt-ack-accept-rx%,%sgtpc-fwd-reloc-req-tx%,%sgtpc-fwd-reloc-req-rx%,%sgtpc-fwd-reloc-discard-tx%,%sgtpc-fwd-reloc-req-accept-tx%,%sgtpc-fwd-reloc-req-accept-rx%,%sgtpc-fwd-srnsctxt-req-tx%,%sgtpc-fwd-srnsctxt-req-rx%,%sgtpc-fwd-srnsctxt-discard-rx%,%sgtpc-fwd-srnsctxt-ack-tx%,%sgtpc-fwd-srnsctxt-ack-rx%,%sgtpc-fwd-reloc-compl-tx%,%sgtpc-fwd-reloc-compl-rx%,%sgtpc-reloc-cncl-req-tx%,%sgtpc-reloc-cncl-req-rx%,%sgtpc-reloc-cncl-req-accept-tx%,%sgtpc-reloc-cncl-req-accept-rx%,%sgtpc-v1-echo-req-tx%,%sgtpc-v1-echo-req-rx%,%sgtpc-v1-echo-rsp-tx%,%sgtpc-v1-echo-rsp-rx%,%sgtpu-ggsn-pkt-sent%,%sgtpu-rnc-pkt-sent%,%sgtpu-sgsn-pkt-sent%,%sgtpu-ggsn-pkt-rcvd%,%sgtpu-rnc-pkt-rcvd%,%sgtpu-sgsn-pkt-rcvd%,%sgtpu-echo-req-tx%,%sgtpu-echo-req-rx%,%sgtpu-echo-rsp-tx%,%sgtpu-echo-rsp-rx%,%sgtpu-ggsn-errind-sent%,%sgtpu-ggsn-errind-rcvd%,%sgtpu-rnc-errind-sent%,%sgtpu-rnc-errind-rcvd%,%sgtpu-total-active-ggsn%,%sgtpu-total-active-rnc%
SGTP2Sch	SGTP2 Schema	EMS,SGTP2,%date%,%time%,%vpn-name%,%vpn-id%,%service-name%,%sgtpc-total-cpc-req%,%sgtpc-cpc-req-denied%,%sgtpc-total-upc-req%,%sgtpc-upc-req-denied-tx%,%sgtpc-upc-req-denied-rx%,%sgtpc-total-dpc-req%,%sgtpc-dpc-req-denied-tx%,%sgtpc-dpc-req-denied-rx%,%sgtpc-ident-req-denied-tx%,%sgtpc-ident-req-denied-rx%,%sgtpc-sgsn-ctxt-req-denied-tx%,%sgtpc-sgsn-ctxt-req-denied-rx%,%sgtpc-sgsn-ctxt-ack-denied-tx%,%sgtpc-sgsn-ctxt-ack-denied-rx%,%sgtpc-fwd-reloc-denied-tx%,%sgtpc-fwd-reloc-denied-rx%,%sgtpc-fwd-srnsctxt-ack-denied-tx%,%sgtpc-fwd-srnsctxt-ack-denied-rx%,%sgtpc-fwd-rel-compl-ack-accept-tx%,%sgtpc-fwd-rel-compl-ack-accept-rx%,%sgtpc-fwd-rel-compl-ack-denied-tx%,%sgtpc-fwd-rel-compl-ack-denied-rx%,%sgtpc-reloc-cncl-denied-tx%,%sgtpc-reloc-cncl-denied-rx%,%sgtpc-ver-not-supported-rx%,%sgtpc-ver-not-supported-tx%,%sgtpc-supp-extn-hdr-notif-rx%,%sgtpc-supp-extn-hdr-notif-tx%,%sgtpu-ggsn-byts-sent%,%sgtpu-rnc-byts-sent%,%sgtpu-sgsn-byts-sent%,%sgtpu-ggsn-byts-rcvd%,%sgtpu-ggsn-pkt-queued%,%sgtpu-ggsn-byts-queued%,%sgtpu-ggsn-pkt-queue-full%,%sgtpu-ggsn-byts-queue-full%,%sgtpu-ggsn-pkt-unkwn-sess%,%sgtpu-ggsn-byts-unkwn-sess%,%sgtpu-ggsn-pkt-suspended-st%,%sgtpu-ggsn-byts-suspended-st%,%sgtpu-ggsn-pkt-invalid-msg-length%,%sgtpu-ggsn-byts-invalid-msg-length%,%sgtpu-rnc-byts-rcvd%,%sgtpu-rnc-pkt-queued%,%sgtpu-rnc-byts-queued%,%sgtpu-rnc-pkt-queue-full%,%sgtpu-rnc-byts-queue-full%,%sgtpu-rnc-pkt-unkwn-sess%,%sgtpu-rnc-byts-unkwn-sess%,%sgtpu-rnc-pkt-sess-dealloc%,%sgtpu-rnc-byts-sess-dealloc%,%sgtpu-rnc-pkt-invalid-msg-length%,%sgtpu-rnc-byts-invalid-msg-length%,%sgtpu-rnc-pkt-source-ip-viol%,%sgtpu-rnc-byts-source-ip-viol%,%sgtpu-sgsn-byts-rcvd%,%sgtpu-sgsn-pkt-queued%,%sgtpu-sgsn-byts-queued%,%sgtpu-sgsn-pkt-queue-full%,%sgtpu-sgsn-byts-queue-full%

Key	Description	Default Value in Config File
SGTP3Sch	SGTP3Schema	EMS,SGTP3,%date%,%time%,%vpn-name%,%vpn-id%,%service-name%,%sgtpu-sgsn-pkt-unkwn-sess%,%sgtpu-sgsn-byts-unkwn-sess%,%sgtpu-sgsn-pkt-iu-release%,%sgtpu-sgsn-byts-iu-release%,%sgtpu-sgsn-pkt-invalid-msg-length%,%sgtpu-sgsn-byts-invalid-msg-length%,%sgtpc-v0-echo-req-tx%,%sgtpc-v0-echo-req-rx%,%sgtpc-v0-echo-rsp-tx%,%sgtpc-v0-echo-rsp-rx%,%sgtpu-ggsn-pkt-sess-dealloc%,%sgtpu-ggsn-byts-sess-dealloc%,%sgtpu-ggsn-pkt-page-fail%,%sgtpu-ggsn-byts-page-fail%,%sgtpu-ggsn-pkt-v0-seq-num-nt-pres%,%sgtpu-ggsn-byts-v0-seq-num-nt-pres%,%sgtpu-rnc-pkt-rau-in-active-st%,%sgtpu-rnc-byts-rau_in_active-st%,%sgtpu-rnc-pkt-reg_in_rau%,%sgtpu-rnc-byts-reg_in_rau%,%sgtpu-rnc-pkt-suspended-st%,%sgtpu-rnc-byts-suspended-st%,%sgtpu-sgsn-pkt-inconsistent-tunnel-state%,%sgtpu-sgsn-byts-inconsistent-tunnel-state%,%sgtpu-sgsn-pkt-sess-dealloc%,%sgtpu-sgsn-byts-sess-dealloc%,%sgtpu-total-ggsn-pkt-drop%,%sgtpu-total-ggsn-byts-drop%,%sgtpu-total-sgsn-pkt-drop%,%sgtpu-total-sgsn-byts-drop%,%sgtpu-total-rnc-pkt-drop%,%sgtpu-total-rnc-byts-drop%,%sgtpu-ggsn-pkt-drop-suspend-dealloc-st%,%sgtpu-ggsn-byts-drop-suspend-dealloc-st%,%sgtpu-rnc-pkt-rau-in-active-reg-st%,%sgtpu-rnc-byts-rau_in_active-reg-st%,%sgtpu-rnc-pkt-drop-suspended-dealloc-st%,%sgtpu-rnc-byts-drop-suspended-dealloc-st%,%sgtpu-total-pkt-ctxt-preserved%,%sgtpu-total-byts-ctxt-preserved%,%sgtpc-paket-discarded%,%sgtpc-v1-retrnas-echo-req-tx%,%sgtpc-v0-retrnas-echo-req-tx%,%sgtpu-errors-payload-length-mismatch%,%sgtpu-rnc-byts-unknown-version%,%sgtpu-rnc-pkt-unknown-version%,%sgtpu-ggsn-byts-unknown-version%,%sgtpu-sgsn-byts-unknown-version%,%sgtpu-ggsn-pkt-unknown-version%,%sgtpu-sgsn-pkt-unknown-version%,%iups-service%,%rnc-address%,%ggsn-address%
SCCPSch	SCCPSchema	EMS,SCCP,%date%,%time%,%sccp-nw-id%,%ssa-txed%,%ss-oos-grant-txed%,%ss-oos-req-txed%,%ssp-txed%,%ss-status-test-txed%,%ssa-rcvd%,%ss-oos-grant-rcvd%,%ss-oos-req-rcvd%,%ss-prohibit-rcvd%,%ss-status-test-rcvd%,%ss-congested-txed%,%ss-congested-rcvd%,%sccp-rtf-notrans-addr-nature%,%sccp-rtf-notrans-addr-specific%,%sccp-rtf-netwfail-pc-unavail%,%sccp-rtf-netw-conges%,%sccp-rtf-ssn-fail%,%sccp-rtf-ssn-conges%,%sccp-syntax-error%,%sccp-reassem-err-timer%,%sccp-reassem-err-sequence%,%sccp-reassem-err-space%,%sccp-hop-counter-violation%,%sccp-provider-ini-reset%,%sccp-provider-ini-rel%,%sccp-msg-toolarge-segment%,%sccp-segmentation-fail%,%sccp-total-msgs-handled%,%sccp-total-msgs-handl-local-ss%,%sccp-total-msgs-req-gtt%,%sccp-udt-sent%,%sccp-udt-rcvd%,%sccp-udts-sent%,%sccp-udts-rcvd%,%sccp-xudt-sent%,%sccp-xudt-rcvd%,%sccp-xudts-sent%,%sccp-xudts-rcvd%,%sccp-ludt-sent%,%sccp-ludt-rcvd%,%sccp-ludts-sent%,%sccp-ludts-rcvd%,%sccp-cr-sent%,%sccp-cr-rcvd%,%sccp-cc-sent%,%sccp-cc-rcvd%,%sccp-cref-sent%,%sccp-cref-rcvd%,%sccp-rsr-msg-sent%,%sccp-rsr-msg-rcvd%,%sccp-err-msg-sent%,%sccp-err-msg-rcvd%,%sccp-unequipped-user%,%sccp-reason-unknown%,%sccp-class-0-sent%,%sccp-class-0-rcvd%,%sccp-class-1-sent%,%sccp-class-1-rcvd%,%sccp-DT1-sent%,%sccp-DT1-rcvd%,%sccp-rel-compl-supv-fail%,%sccp-rel-disconn-req-rx%,%sccp-routing-fail-invalid-ins-routing-req%,%sccp-routing-fail-invalid-isni-routing-req%,%sccp-routing-fail-isni-constrained-routing%,%sccp-routing-fail-redundant-isni-routing-req%,%sccp-routing-fail-isni-identify-network%,%sccp-inactivity-rcv-tmr-expired%,%sccp-inactivity-test-sent%,%sccp-inactivity-test-received%

Key	Description	Default Value in Config File
SS7RD1Sch	SS7RD1Schema	EMS,SS7RD1,%date%,%time%,%ss7rd-number%,%ss7rd-asp_instance%,%ss7rd-sctp-init-tx%,%ss7rd-sctp-init-rtx%,%ss7rd-sctp-init-rx%,%ss7rd-sctp-init-ack-tx%,%ss7rd-sctp-init-ack-rx%,%ss7rd-sctp-shutdown-tx%,%ss7rd-sctp-shutdown-rtx%,%ss7rd-sctp-shutdown-rx%,%ss7rd-sctp-shutdown-ack-tx%,%ss7rd-sctp-shutdown-ack-rtx%,%ss7rd-sctp-shutdown-ack-rx%,%ss7rd-sctp-cookie-tx%,%ss7rd-sctp-cookie-rtx%,%ss7rd-sctp-cookie-rx%,%ss7rd-sctp-cookie-ack-tx%,%ss7rd-sctp-cookie-ack-rx%,%ss7rd-sctp-data-tx%,%ss7rd-sctp-data-rtx%,%ss7rd-sctp-data-rx%,%ss7rd-sctp-sack-tx%,%ss7rd-sctp-sack-rx%,%ss7rd-sctp-shutdown-compl-tx%,%ss7rd-sctp-shutdown-compl-rx%,%ss7rd-sctp-heartbeat-tx%,%ss7rd-sctp-heartbeat-rx%,%ss7rd-sctp-heartbeat-ack-tx%,%ss7rd-sctp-heartbeat-ack-rx%,%ss7rd-sctp-abort-tx%,%ss7rd-sctp-abort-rx%,%ss7rd-sctp-bytes-tx%,%ss7rd-sctp-bytes-rx%,%ss7rd-mtp3-data-tx%,%ss7rd-mtp3-paused-tx%,%ss7rd-mtp3-resumed-tx%,%ss7rd-mtp3-congest-tx%,%ss7rd-mtp3-restrict-tx%,%ss7rd-mtp3-reset-begin-tx%,%ss7rd-mtp3-reset-end-tx%,%ss7rd-mtp3-reset-upu-tx%,%ss7rd-mtp3-data-rx%,%ss7rd-mtp3-paused-rx%,%ss7rd-mtp3-resumed-rx%,%ss7rd-mtp3-congest-rx%,%ss7rd-mtp3-restrict-rx%,%ss7rd-mtp3-reset-begin-rx%,%ss7rd-mtp3-reset-end-rx%,%ss7rd-mtp3-reset-upu-rx%,%ss7rd-m3ua-data-tx%,%ss7rd-m3ua-duna-tx%,%ss7rd-m3ua-dava-tx%,%ss7rd-m3ua-daud-tx%,%ss7rd-m3ua-scon-tx%,%ss7rd-m3ua-dupu-tx%,%ss7rd-m3ua-drst-tx%,%ss7rd-m3ua-regreq-tx%,%ss7rd-m3ua-regrsp-tx%,%ss7rd-m3ua-deregreq-tx%,%ss7rd-m3ua-deregrsp-tx%,%ss7rd-m3ua-aspup-tx%,%ss7rd-m3ua-aspup-ack-tx%,%ss7rd-m3ua-aspdn-tx%,%ss7rd-m3ua-aspdn-ack-tx%,%ss7rd-m3ua-aspac-tx%,%ss7rd-m3ua-aspac-ack-tx%,%ss7rd-m3ua-aspia-tx%,%ss7rd-m3ua-aspia-ack-tx%,%ss7rd-m3ua-hearbeat-tx%,%ss7rd-m3ua-hearbeat-ack-tx%,%ss7rd-m3ua-error-tx%,%ss7rd-m3ua-notify-tx%,%ss7rd-m3ua-data-rx%
SS7RD2Sch	SS7RD2Schema	EMS,SS7RD2,%date%,%time%,%ss7rd-number%,%ss7rd-asp_instance%,%ss7rd-m3ua-duna-rx%,%ss7rd-m3ua-dava-rx%,%ss7rd-m3ua-daud-rx%,%ss7rd-m3ua-scon-rx%,%ss7rd-m3ua-dupu-rx%,%ss7rd-m3ua-drst-rx%,%ss7rd-m3ua-regreq-rx%,%ss7rd-m3ua-regrsp-rx%,%ss7rd-m3ua-deregreq-rx%,%ss7rd-m3ua-deregrsp-rx%,%ss7rd-m3ua-aspup-rx%,%ss7rd-m3ua-aspup-ack-rx%,%ss7rd-m3ua-aspdn-rx%,%ss7rd-m3ua-aspdn-ack-rx%,%ss7rd-m3ua-aspac-rx%,%ss7rd-m3ua-aspac-ack-rx%,%ss7rd-m3ua-aspia-rx%,%ss7rd-m3ua-aspia-ack-rx%,%ss7rd-m3ua-hearbeat-rx%,%ss7rd-m3ua-hearbeat-ack-rx%,%ss7rd-m3ua-error-rx%,%ss7rd-m3ua-notify-rx%,%ss7rd-m3ua-lower-intf-pdu-tx%,%ss7rd-m3ua-lower-intf-pdu-rx%,%ss7rd-m3ua-upper-intf-pdu-tx%,%ss7rd-m3ua-upper-intf-pdu-rx%,%ss7rd-m3ua-down-no-route-found%,%ss7rd-m3ua-down-pc-unvailable%,%ss7rd-m3ua-down-msg-failed%,%ss7rd-m3ua-down-loadshare-failed%,%ss7rd-m3ua-up-no-route-found%,%ss7rd-m3ua-up-pc-unvailable%,%ss7rd-m3ua-up-msg-failed%,%ss7rd-m3ua-up-loadshare-failed%,%ss7rd-sctp-error-tx%,%ss7rd-sctp-error-rx%,%ss7rd-m3ua-lower-intf-pdusize-tx%,%ss7rd-m3ua-lower-intf-pdusize-rx%,%ss7rd-m3ua-upper-intf-pdusize-tx%,%ss7rd-m3ua-upper-intf-pdusize-rx%,%ss7rd-m3ua-down-pc-congested%,%ss7rd-m3ua-down-no-psp-avail%,%ss7rd-m3ua-down-no-nsap-avail%,%ss7rd-m3ua-down-data-conges-q%,%ss7rd-m3ua-down-data-as-pend-q%,%ss7rd-m3ua-up-pc-congested%,%ss7rd-m3ua-up-no-psp-avail%,%ss7rd-m3ua-up-no-nsap-avail%,%ss7rd-m3ua-up-data-conges-q%,%ss7rd-m3ua-up-data-as-pend-q%,%ss7rd-mtp3-user-part-unavail-tx%,%ss7rd-mtp3-traffic-restart-allowed-tx%,%ss7rd-mtp3-traffic-restart-waiting-tx%,%ss7rd-mtp3-user-part-unavail-rx%,%ss7rd-mtp3-traffic-restart-allowed-rx%,%ss7rd-mtp3-traffic-restart-waiting-rx%,%ss7rd-mtp3-msu-dropped-routing-err%

Key	Description	Default Value in Config File
SS7RD3Sch	SS7RD3Schema	EMS,SS7RD3,%date%,%time%,%ss7rd-number%,%ss7rd-asp_instance%,%ss7rd-m3ua-psp-ps-id%,%ss7rd-m3ua-psp-instance%,%ss7-adjacent-point-code%,%ss7-adjacent-spc-not-accessible%,%ss7rd-m3ua-psp-aspac-ack-rx%,%ss7rd-m3ua-psp-aspac-ack-tx%,%ss7rd-m3ua-psp-aspac-rx%,%ss7rd-m3ua-psp-aspac-tx%,%ss7rd-m3ua-psp-aspdn-ack-rx%,%ss7rd-m3ua-psp-aspdn-ack-tx%,%ss7rd-m3ua-psp-aspdn-rx%,%ss7rd-m3ua-psp-aspdn-tx%,%ss7rd-m3ua-psp-aspia-ack-rx%,%ss7rd-m3ua-psp-aspia-ack-tx%,%ss7rd-m3ua-psp-aspia-rx%,%ss7rd-m3ua-psp-aspia-tx%,%ss7rd-m3ua-psp-aspup-ack-rx%,%ss7rd-m3ua-psp-aspup-ack-tx%,%ss7rd-m3ua-psp-aspup-rx%,%ss7rd-m3ua-psp-aspup-tx%,%ss7rd-m3ua-psp-congestion-count%,%ss7rd-m3ua-psp-congestion-duration%,%ss7rd-m3ua-psp-congestion-level1%,%ss7rd-m3ua-psp-congestion-level2%,%ss7rd-m3ua-psp-congestion-level3%,%ss7rd-m3ua-psp-congestion-queue-hw%,%ss7rd-m3ua-psp-congestion-queue-size%,%ss7rd-m3ua-psp-data-pdu-rx%,%ss7rd-m3ua-psp-data-pdusize-rx%,%ss7rd-m3ua-psp-data-pdusize-tx%,%ss7rd-m3ua-psp-data-pdu-tx%,%ss7rd-m3ua-psp-data-rx%,%ss7rd-m3ua-psp-data-tx%,%ss7rd-m3ua-psp-daud-rx%,%ss7rd-m3ua-psp-daud-tx%,%ss7rd-m3ua-psp-dava-rx%,%ss7rd-m3ua-psp-dava-tx%,%ss7rd-m3ua-psp-deregreq-rx%,%ss7rd-m3ua-psp-deregreq-tx%,%ss7rd-m3ua-psp-deregrsp-rx%,%ss7rd-m3ua-psp-deregrsp-tx%,%ss7rd-m3ua-psp-drst-rx%,%ss7rd-m3ua-psp-drst-tx%,%ss7rd-m3ua-psp-duna-rx%,%ss7rd-m3ua-psp-duna-tx%,%ss7rd-m3ua-psp-dupu-rx%,%ss7rd-m3ua-psp-dupu-tx%,%ss7rd-m3ua-psp-error-rx%,%ss7rd-m3ua-psp-error-tx%,%ss7rd-m3ua-psp-hearbeat-ack-rx%,%ss7rd-m3ua-psp-hearbeat-ack-tx%,%ss7rd-m3ua-psp-hearbeat-rx%,%ss7rd-m3ua-psp-hearbeat-tx%,%ss7rd-m3ua-psp-notify-rx%,%ss7rd-m3ua-psp-notify-tx%,%ss7rd-m3ua-psp-regreq-rx%,%ss7rd-m3ua-psp-regreq-tx%,%ss7rd-m3ua-psp-regrsp-rx%,%ss7rd-m3ua-psp-regrsp-tx%,%ss7rd-m3ua-psp-scon-rx%
SS7RD4Sch	SS7RD4Schema	EMS,SS7RD4,%date%,%time%,%ss7rd-number%,%ss7rd-asp_instance%,%ss7rd-m3ua-psp-scon-tx%,%ss7rd-m3ua-psp-unvailable-count%,%ss7rd-m3ua-psp-unvailable-duration%,%ss7rd-m3ua-psp-up-data-as-pend-q%,%ss7rd-m3ua-psp-up-data-conges-q%,%ss7rd-m3ua-psp-up-loadshare-failed%,%ss7rd-m3ua-psp-up-msg-failed%,%ss7rd-m3ua-psp-up-no-nsap-avail%,%ss7rd-m3ua-psp-up-no-psp-avail%,%ss7rd-m3ua-psp-up-no-route-found%,%ss7rd-m3ua-psp-up-pc-congested%,%ss7rd-m3ua-psp-up-pc-unvailable%
MIPV6HASch	MIPV6HASchema	EMS,MIPV6HA,%date%,%time%,%vpnname%,%vpnid%,%servname%,%servid%,%num-subscriber%,%aaa-attempt%,%aaa-success%,%aaa-totfail%,%aaa-actauthfail%,%aaa-misauthfail%,%bindupdrec-totrec%,%bindupdrec-totacc%,%bindupdrec-totdeny%,%bindupdrec-totdisc%,%bindupdrec-totcongdisc%,%ibindupdreq-receive%,%ibindupdreq-accept%,%ibindupdreq-deny%,%rbindupdreq-receive%,%rbindupdreq-accept%,%rbindupdreq-deny%,%deregreq-receive%,%deregreq-accept%,%deregreq-deny%,%horeq-receive%,%horeq-accept%,%horeq-deny%,%bindacksent-total%,%bindacksent-acceptreg%,%bindacksent-acceptdereg%,%bindacksent-deny%,%denyreason-badreq%,%denyreason-mismatchid%,%denyreason-mnauthfail%,%denyreason-admprohibit%,%denyreason-noresource%,%denyreason-simbindexceed%,%denyreason-senderror%,%denyreason-unspereason%,%denyreason-msgidrequire%,%denyreason-dadfail%,%denyreason-nothomesubnet%,%denyreason-seqoutwindow%,%denyreason-regchadisallow%,%rrqdeny-admprohibit%,%rrqdeny-unknownha%,%datareceive-totpkt%,%datareceive-totpkt6in6%,%datareceive-totbyte%,%datareceive-totbyte6in6%,%datareceive-errorprotocol%,%datareceive-errorinvpkt%,%datareceive-errornosess%,%datasent-totpkt%,%datasent-totpkt6in6%,%datasent-totbyte%,%datasent-totbyte6in6%,%disconnect-lifetimeexp%,%disconnect-deregistration%,%disconnect-admdrop%,%disconnect-othreason%,%icmpv6-toobigreceive%,%icmpv6-toobigforward%,%icmpv6-toobiggenerate%
CONTEXTSch	CONTEXTSchema	EMS,CONTEXT,%date%,%time%,%vpnname%,%vpnid%,%sfw-total-rxpackets%,%sfw-total-rxbytes%,%sfw-total-txpackets%,%sfw-total-txbytes%,%sfw-total-injectedpkts%,%sfw-total-injectedbytes%,%sfw-dnlnk-droppkts%,%sfw-dnlnk-dropbytes%,%sfw-uplnk-droppkts%,%sfw-uplnk-dropbytes%,%sfw-total-malpackets%,%sfw-ip-discardpackets%,%sfw-ip-malpackets%,%sfw-icmp-discardpackets%,%sfw-icmp-malpackets%,%sfw-tcp-discardpackets%,%sfw-tcp-malpackets%,%sfw-udp-discardpackets%,%sfw-udp-malpackets%,%sfw-total-dosattacks%,%sfw-total-flows%

Key	Description	Default Value in Config File
CSCF1Sch	CSCF1 Schema	EMS,CSCF1,%date%,%time%,%vpnname%,%vpnid%,%svcname%,%svcid%,%curregusers%,%failedauth%,%regexp%,%callattrx%,%callatttx%,%callsuccrx%,%callsucctx%,%callfailrx%,%callfailtx%,%curcscfsess%,%callrejpdf%,%callrejloc%,%sesstimeexp%,%hssacc%,%emergcalls%,%tollfreecalls%,%premservcalls%,%internationalcalls%,%longDistancecalls%,%opassistcalls%,%dirassistcalls%,%regreqrx%,%regreqtx%,%invreqrx%,%invreqtx%,%ackreqrx%,%ackreqtx%,%byereqrx%,%byereqtx%,%cancreqrx%,%cancreqtx%,%optreqrx%,%optreqtx%,%prackreqrx%,%prackreqtx%,%subreqrx%,%subreqtx%,%notreqrx%,%notreqtx%,%refreqrx%,%refreqtx%,%inforeqrx%,%inforeqtx%,%updreqrx%,%updreqtx%,%msgreqrx%,%msgreqtx%,%pubreqrx%,%pubreqtx%,%tryrsprx%,%tryrsptx%,%rngrsprx%,%rngrsptx%,%fwdrsprx%,%fwdrsptx%,%quersprx%,%quersptx%,%prgrsprx%,%prgrsptx%,%200-regrsprx%,%200-regrsptx%,%200-invrsprx%,%200-invrsptx%,%200-byersprx%,%200-byersptx%,%200-cnlrsprx%,%200-cnlrsptx%,%200-optrsprx%,%200-optrsptx%,%200-prackrsprx%,%200-prackrsptx%,%200-subrsprx%,%200-subrsptx%,%200-notrsprx%,%200-notrsptx%,%200-infrsprx%,%200-infrsptx%,%200-updrsprx%,%200-updrsptx%,%200-pubrsprx%,%200-pubrsptx%,%200-refrsprx%,%200-refrsptx%,%200-msgrsprx%,%200-msgrsptx%,%202-refrsprx%,%202-refrsptx%,%202-subrsprx%,%202-subrsptx%,%mchrsprx%,%mchrsptx%,%mpersprx%,%mpersptx%,%mtersprx%,%mtersptx%,%upxrsprx%,%upxrsptx%,%altrsprx%,%altrsptx%,%brqerrrx%,%brqerrtx%,%uauerrrx%,%uauerrtx%,%forerrrx%,%forerrtx%,%nfderrrx%,%nfderrtx%,%mnaerrrx%,%mnaerrtx%,%nac406errrx%,%nac406errtx%,%parerrrx%,%parerrtx%,%rtoerrrx%,%rtoerrtx%,%gonerrrx%,%gonerrtx%,%crferrrx%,%crferrtx%,%relerrrx%,%relerrtx%,%rulerrrx%,%rulerrtx%,%umterrrx%,%umterrtx%,%uuserrrx%,%uuserrtx%,%bexerrrx%,%bexerrtx%,%exrerrrx%,%exrerrtx%,%itberrrx%,%itberrtx%,%tnaerrrx%,%tnaerrtx%,%tdnerrrx%,%tdnerrtx%,%ldterrrx%,%ldterrtx%
CSCF2Sch	CSCF2 Schema	EMS,CSCF2,%date%,%time%,%vpnname%,%vpnid%,%svcname%,%svcid%,%tmherrrx%,%tmherrtx%,%adierrrx%,%adierrtx%,%amberrrx%,%amberrtx%,%bhrerrrx%,%bhrerrtx%,%rqcerrrx%,%rqcerrtx%,%namerrrx%,%namerrtx%,%trperrrx%,%trperrtx%,%udperrrx%,%udperrtx%,%ineerrrx%,%ineerrtx%,%nimerrrx%,%nimerrtx%,%bgterrrx%,%bgterrtx%,%suaerrrx%,%suaerrtx%,%gtterrrx%,%gtterrtx%,%bsverrrx%,%bsverrtx%,%mtlerrrx%,%mtlerrtx%,%pcferrrx%,%pcferrtx%,%bewerrrx%,%bewerrtx%,%decerrrx%,%decerrtx%,%neaerrrx%,%neaerrtx%,%nac606errrx%,%nac606errtx%,%callsetuptime%,%callscounted%
SS7LINK1Sch	SS7LINK1 Schema	EMS,SS7LINK1,%date%,%time%,%ss7rd-number%,%ss7-linkset-id%,%ss7-link-id%,%ss7-dpc-point-code%,%ss7-link-mtp3-changeover-order-tx%,%ss7-link-mtp3-changeover-order-rx%,%ss7-link-mtp3-changeover-order-ack-tx%,%ss7-link-mtp3-changeover-order-ack-rx%,%ss7-link-mtp3-changeback-declaration-tx%,%ss7-link-mtp3-changeback-declaration-rx%,%ss7-link-mtp3-changeback-ack-tx%,%ss7-link-mtp3-changeback-ack-rx%,%ss7-link-mtp3-emergency-changeover-tx%,%ss7-link-mtp3-emergency-changeover-rx%,%ss7-link-mtp3-emergency-changeover-ack-tx%,%ss7-link-mtp3-emergency-changeover-ack-rx%,%ss7-link-mtp3-inhibit-tx%,%ss7-link-mtp3-inhibit-rx%,%ss7-link-mtp3-inhibit-ack-tx%,%ss7-link-mtp3-inhibit-ack-rx%,%ss7-link-mtp3-uninhibit-tx%,%ss7-link-mtp3-uninhibit-rx%,%ss7-link-mtp3-uninhibit-ack-tx%,%ss7-link-mtp3-uninhibit-ack-rx%,%ss7-link-mtp3-inhibit-deny-tx%,%ss7-link-mtp3-inhibit-deny-rx%,%ss7-link-mtp3-force-uninhibit-tx%,%ss7-link-mtp3-force-uninhibit-rx%,%ss7-link-mtp3-local-inhibit-test-tx%,%ss7-link-mtp3-local-inhibit-test-rx%,%ss7-link-mtp3-remote-inhibit-test-tx%,%ss7-link-mtp3-remote-inhibit-test-rx%,%ss7-link-mtp3-connection-order-tx%,%ss7-link-mtp3-connection-order-rx%,%ss7-link-mtp3-connection-order-ack-tx%,%ss7-link-mtp3-connection-order-ack-rx%,%ss7-link-mtp3-test-tx%,%ss7-link-mtp3-test-rx%,%ss7-link-mtp3-test-ack-tx%,%ss7-link-mtp3-test-ack-rx%,%ss7-link-mtp3-sif-octet-tx%,%ss7-link-mtp3-sif-octet-rx%,%ss7-link-mtp3-sio-octet-tx%,%ss7-link-mtp3-sio-octet-rx%,%ss7-link-mtp3-sio-msu-tx%,%ss7-link-mtp3-tx-msu-dropped%,%ss7-link-mtp3-tx-msu-congestion-dropped%,%ss7-link-mtp3-invalid-pdu-rx%,%ss7-link-mtp3-congestion-threshold1%,%ss7-link-mtp3-congestion-threshold2%,%ss7-link-mtp3-congestion-threshold3%,%ss7-link-mtp3-unavail-duration%,%ss7-link-mtp3-congested-duration%

Key	Description	Default Value in Config File
SS7LINK2Sch	SS7LINK2 Schema	EMS,SS7LINK2,%date%,%time%,%ss7rd-number%,%ss7-linkset-id%,%ss7-link-id%,%ss7-dpc-point-code%,%ss7-signalling-link-failure%,%ss7-dpc-route-set-test-msg-tx%,%ss7-dpc-route-set-congestion-test-msg-tx%,%ss7-dpc-transfer-prohibited-tx%,%ss7-dpc-transfer-restricted-tx%,%ss7-dpc-transfer-allowed-tx%,%ss7-dpc-transfer-controlled-tx%,%ss7-dpc-sif-octets-tx%,%ss7-dpc-sio-octets-tx%,%ss7-dpc-route-set-test-msg-rx%,%ss7-dpc-route-set-congestion-test-msg-rx%,%ss7-dpc-transfer-prohibited-rx%,%ss7-dpc-transfer-restricted-rx%,%ss7-dpc-transfer-allowed-rx%,%ss7-dpc-transfer-controlled-rx%,%ss7-dpc-usn-msg-rx%,%ss7-dpc-unavailable-duration%,%ss7-dpc-unavailable-count%,%ss7-link-sscf-mtp3-frames-tx%,%ss7-link-sscf-out-of-service-pdu-tx%,%ss7-link-sscf-processor-outage-tx%,%ss7-link-sscf-in-service-pdu-tx%,%ss7-link-sscf-normal-pdu-tx%,%ss7-link-sscf-emergency-pdu-tx%,%ss7-link-sscf-alignment-not-successfull-pdu-tx%,%ss7-link-sscf-management-initiated-pdu-tx%,%ss7-link-sscf-protocol-error-pdu-tx%,%ss7-link-sscf-proving-not-successfull-pdu-tx%,%ss7-link-sscf-mtp3-frames-rx%,%ss7-link-sscf-out-of-service-pdu-rx%,%ss7-link-sscf-processor-outage-rx%,%ss7-link-sscf-in-service-pdu-rx%,%ss7-link-sscf-normal-pdu-rx%,%ss7-link-sscf-emergency-pdu-rx%,%ss7-link-sscf-alignment-not-successfull-pdu-rx%,%ss7-link-sscf-management-initiated-pdu-rx%,%ss7-link-sscf-protocol-error-pdu-rx%,%ss7-link-sscf-proving-not-successfull-pdu-rx%,%ss7-link-qsaal-vpi%,%ss7-link-qsaal-vci%,%ss7-link-qsaal-req-initialization-tx%,%ss7-link-qsaal-req-ack-tx%,%ss7-link-qsaal-connection-reject-tx%,%ss7-link-qsaal-disconnect-command-tx%,%ss7-link-qsaal-disconnect-ack-tx%,%ss7-link-qsaal-resynchronization-command-tx%
SS7LINK3Sch	SS7LINK3 Schema	EMS,SS7LINK3,%date%,%time%,%ss7rd-number%,%ss7-linkset-id%,%ss7-link-id%,%ss7-dpc-point-code%,%ss7-link-qsaal-resynchronization-ack-tx%,%ss7-link-qsaal-recovery-command-tx%,%ss7-link-qsaal-seq-connection-mode-data-tx%,%ss7-link-qsaal-poll-tx%,%ss7-link-qsaal-stat-tx%,%ss7-link-qsaal-ustat-tx%,%ss7-link-qsaal-unnumbered-user-data-tx%,%ss7-link-qsaal-unnumbered-management-data-tx%,%ss7-link-qsaal-unknown-pdu-type-tx%,%ss7-link-qsaal-tx-discarded-sdus%,%ss7-link-qsaal-tx-pdus-error-pdus%,%ss7-link-qsaal-tx-discarded-pdus%,%ss7-link-qsaal-tx-buffer-in-use-counter%,%ss7-link-qsaal-tx-buffer-in-use-gauge%,%ss7-link-qsaal-req-initialization-rx%,%ss7-link-qsaal-req-ack-rx%,%ss7-link-qsaal-connection-reject-rx%,%ss7-link-qsaal-disconnect-command-rx%,%ss7-link-qsaal-disconnect-ack-rx%,%ss7-link-qsaal-resynchronization-command-rx%,%ss7-link-qsaal-resynchronization-ack-rx%,%ss7-link-qsaal-recovery-command-rx%,%ss7-link-qsaal-recovery-ack-rx%,%ss7-link-qsaal-seq-connection-mode-data-rx%,%ss7-link-qsaal-poll-rx%,%ss7-link-qsaal-stat-rx%,%ss7-link-qsaal-ustat-rx%,%ss7-link-qsaal-unnumbered-user-data-rx%,%ss7-link-qsaal-unnumbered-management-data-rx%,%ss7-link-qsaal-unknown-pdu-type-rx%,%ss7-link-qsaal-rx-pdus-error-pdus%,%ss7-link-qsaal-rx-discarded-pdus%,%ss7-link-qsaal-rx-buffer-in-use-counter%,%ss7-link-qsaal-rx-buffer-in-use-gauge%
GPRS1Sch	GPRS1 Schema	EMS,GPRS1,%date%,%time%,%vpnname%,%vpnid%,%servname%,%nse-id%,%ns-num-bytes-rvcd%,%ns-num-bytes-sent%,%ns-num-nsvc-failed%,%ns-num-nsvc-congest%,%ns-num-unit-data-msg-rcvd%,%ns-num-unit-data-msg-sent%,%ns-num-alive-pdu-rcvd%,%ns-num-alive-pdu-sent%,%ns-num-alive-ack-pdu-rcvd%,%ns-num-alive-ack-pdu-sent%,%ns-num-block-pdu-rcvd%,%ns-num-block-pdu-sent%,%ns-num-block-ack-pdu-rcvd%,%ns-num-block-ack-pdu-sent%,%ns-num-unblock-pdu-rcvd%,%ns-num-unblock-pdu-sent%,%ns-num-unblock-ack-pdu-rcvd%,%ns-num-unblock-ack-pdu-sent%,%ns-num-reset-pdu-rcvd%,%ns-num-reset-pdu-sent%,%ns-num-reset-ack-pdu-rcvd%,%ns-num-reset-ack-pdu-sent%,%ns-num-status-pdu-rcvd%,%ns-num-status-pdu-sent%,%num-sns-size-rcvd%,%num-sns-size-ack-sent%,%num-sns-size-fail-rcvd-unknown-nse%,%num-sns-config-rcvd%,%num-sns-config-sent%,%num-sns-config-ack-sent%,%num-sns-config-ack-rcvd%,%sns-config-fail-rcv-pdu-not-compat-state%,%sns-config-fail-sent-pdu-not-compat-state%,%sns-config-fail-rcv-inval-ipv4-endpt%,%sns-config-fail-sent-inval-ipv4-endpt%,%sns-config-fail-rcv-inval-ipv6-endpt%,%sns-config-fail-sent-inval-ipv6-endpt%,%sns-config-fail-rcv-prot-err-unspec%,%sns-config-fail-sent-prot-err-unspec%,%sns-config-fail-rcv-inval-essential-param%,%sns-config-fail-sent-inval-essential-param%,%sns-config-fail-rcv-internal-err%,%sns-config-fail-sent-internal-err%,%sns-config-fail-rcv-inval-weight%,%sns-config-fail-sent-inval-weight%,%sns-config-fail-sent-no-rsp-from-peer%,%num-sns-add-rcvd%,%num-sns-add-sent%,%sns-add-fail-rcv-pdu-not-compat-state%,%sns-add-fail-sent-pdu-not-compat-state%,%sns-add-fail-rcv-inval-ipv4-endpt%,%sns-add-fail-sent-inval-ipv4-endpt%,%sns-add-fail-rcv-inval-ipv6-endpt%,%sns-add-fail-sent-inval-ipv6-endpt%,%sns-add-fail-rcv-prot-err-unspec%

Key	Description	Default Value in Config File
GPRS2Sch	GPRS2 Schema	EMS,GPRS2,%date%,%time%,%vpnname%,%vpnid%,%servname%,%nse-id%,%sns-add-fail-sent-prot-err-unspec%,%sns-add-fail-rcv-inval-essential-param%,%sns-add-fail-sent-inval-essential-param%,%sns-add-fail-rcv-internal-err%,%sns-add-fail-sent-internal-err%,%sns-add-fail-rcv-inval-weight%,%sns-add-fail-sent-inval-weight%,%sns-add-fail-sent-no-rsp-from-peer%,%num-sns-delete-rcvd%,%num-sns-delete-sent%,%sns-delete-fail-rcv-pdu-not-compat-state%,%sns-delete-fail-sent-pdu-not-compat-state%,%sns-delete-fail-rcv-unknown-ip-endpt%,%sns-delete-fail-sent-unknown-ip-endpt%,%sns-delete-fail-rcv-unknown-ip-address%,%sns-delete-fail-sent-unknown-ip-address%,%sns-delete-fail-rcv-prot-err-unspec%,%sns-delete-fail-sent-prot-err-unspec%,%sns-delete-fail-rcv-inval-essential-param%,%sns-delete-fail-sent-inval-essential-param%,%sns-delete-fail-rcv-internal-err%,%sns-delete-fail-sent-internal-err%,%sns-delete-fail-sent-no-rsp-from-peer%,%num-sns-cw-rcvd%,%num-sns-cw-sent%,%sns-cw-fail-rcv-pdu-not-compat-state%,%sns-cw-fail-sent-pdu-not-compat-state%,%sns-cw-fail-rcv-inval-weight%,%sns-cw-fail-sent-inval-weight%,%sns-cw-fail-rcv-unknown-ip-endpt%,%sns-cw-fail-sent-unknown-ip-endpt%,%sns-cw-fail-rcv-unknown-ip-addr%,%sns-cw-fail-sent-unknown-ip-addr%,%sns-cw-fail-rcv-prot-err-unspec%,%sns-cw-fail-sent-prot-err-unspec%,%sns-cw-fail-rcv-inval-essential-param%,%sns-cw-fail-sent-inval-essential-param%,%sns-cw-fail-rcv-internal-err%,%sns-cw-fail-sent-internal-err%,%sns-cw-fail-sent-no-rsp-from-peer%,%sns-num-ack-rcvd%,%sns-num-ack-sent%,%sns-num-unknown-msg%,%sns-num-status-pdu-sent%,%bssgp-total-usr-req-drop%,%bssgp-usr-req-drop-unknown-bvci%,%bssgp-usr-req-drop-blocked-bvc%,%bssgp-usr-req-drop-encoding-fail%,%bssgp-usr-req-drop-bvc-flow-ctrl-rvcd%
	GPRS3 Schema	EMS,GPRS3,%date%,%time%,%vpnname%,%vpnid%,%servname%,%nse-id%,%bssgp-usr-req-drop-bvc-flow-ctrl-ack-sent%,%bssgp-usr-req-drop-block-rvcd%,%bssgp-usr-req-drop-block-ack-sent%,%bssgp-usr-req-drop-unblock-rcvd%,%bssgp-usr-req-drop-unblock-ack-sent%,%bssgp-usr-req-drop-bvc-reset-sent%,%bssgp-usr-req-drop-bvc-reset-rcvd%,%bssgp-usr-req-drop-bvc-reset-ack-sent%,%bssgp-usr-req-drop-bvc-reset-ack-rcvd%,%bssgp-flush-llc-msg-sent%,%bssgp-flush-llc-ack-msg-rcvd%,%bssgp-cs-paging-msg-sent%,%bssgp-ps-paging-msg-sent%,%bssgp-ra-cap-update-msg-rcvd%,%bssgp-ra-cap-update-ack-msg-sent%,%bssgp-radio-status-msg-sent%,%bssgp-radio-status-msg-rcvd%,%bssgp-suspend-msg-rcvd%,%bssgp-suspend-ack-msg-sent%,%bssgp-suspend-nack-msg-sent%,%bssgp-resume-msg-rcvd%,%bssgp-resume-ack-msg-sent%,%bssgp-resume-nack-msg-sent%,%bssgp-downlink-unitdata-sent%,%bssgp-uplink-unitdata-rcvd%,%bssgp-llc-pdu-discard-msg-rcvd%,%bssgp-ms-flow-ctrl-msg-rcvd%,%bssgp-ms-flow-ctrl-ack-msg-sent%,%bssgp-bvc-status-msg-rcvd%,%bssgp-bvc-status-msg-sent%,%sndcp-xid-req-ms-init%,%sndcp-xid-ind-sgsn-init%,%sndcp-npdus-ack-rcvd-ms%,%sndcp-npdus-ack-sent-ms%,%sndcp-npdus-uack-rcvd-ms%,%sndcp-npdus-uack-sent-ms%,%sndcp-bytes-ack-rcvd-ms%,%sndcp-bytes-ack-sent-ms%,%sndcp-bytes-uack-rcvd-ms%,%sndcp-bytes-uack-sent-ms%,%sndcp-pdu-drop-rcvd-from-llc%,%sndcp-inval-ref-num-rcvd-from-llc%,%sndcp-npdu-sent-sgsn-irau%,%sndcp-npdu-rcvd-sgsn-irau%,%llc-data-req-rx%,%llc-data-cfm-tx%,%llc-data-ind-tx%,%llc-data-sent-ind-tx%,%llc-unit-data-req-rx%,%llc-unit-data-ind-tx%,%llc-discarded-frames-rx%,%llc-discarded-frames-tx%,%llc-error-frames-rx%,%llc-unrecog-frames-rx%,%llc-xid-collisions%,%llc-ciphering-errors%,%llc-fcs-errors%,%llc-frame-stats-ui-rx%,%llc-frame-stats-ui-tx%

Table 30. bs.cfg File Parameters (Other)

Directory	Description	Minimum Value	Maximum Value	Default Value
Format: This section deals with the format string other than the subsystem schemas.				
RemoteFile	The parameter values should not be edited manually. Used by the WEM server.			
Tolerance: These values indicate that the server will search records within a range (below and above the expected timestamp) if the exact record is not present. All values are in seconds.				

Directory	Description	Minimum Value	Maximum Value	Default Value
5MinTolerance		0	150 (2.5 mins)	0
15MinTolerance		0	450 (7.5 mins)	0
30MinTolerance		0	900 (15 mins)	0
45MinTolerance		0	1350 (22.5 mins)	0
HourTolerance		0	1800 (30 mins)	0
DayTolerance		0	43200 (12 hrs)	0
MonthTolerance		0	1296000 (15 days)	0
StartDateTime: These values indicate the date and time for fetching the records in case of daily and monthly report type respectively.				
DailyStartTime	From this value, we can configure the time field for daily report type if DailyStartTime is set to 20, then record present at 08:00 PM of every day will be fetched from the database.	23 (11:00 PM)	0 (12:00 AM)	12
MonthlyStartDate	From this value, we can configure the day field for monthly report type if MonthlyStartDate is set to 15, then record present at day 15 of every month will be fetched from the database.	1	31	15

The bsparser.cfg File

This file provides parameters for specifying such information as the directories in which bulk statistics records received from the chassis are stored and archived after they are processed, in addition to time intervals for polling and record transfer.

Important: Any change in the configuration files will restart the server resulting in client restart.

Caution: Several parameters contained in this file are configurable through the installation process.

Table 31. bsparser.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
Directory: This section contains the directory path required for bulk statistics.				
Ftp	Base directory for bulkstat FTP from the ASR 5000. The FTP directory entry can be changed to one of the available directories in the host file system. If the specified directory does not exist, then the bulkstats files will be configured for FTPing in *<serverpath>/data/*. **Important:** The FTP directory path entry should always be an absolute path and not a relative path.	--	--	<serverpath>/data/
SecFtp	Base directory for bulkstat secondary FTP from the ASR 5000. The FTP directory entry can be changed to one of the available directories in the host file system. If the specified directory does not exist, then the bulkstats files will be configured for FTPing in *<serverpath>/data/*. **Important:** The FTP directory path entry should always be an absolute path and not a relative path.	--	--	<serverpath>/data/

Key	Description	Minimum Value	Maximum Value	Default Value
Archive	It is recommended that the WEM server installer/admin changes this entry to one of the available directories in the host file system. This directory contains the archive of the bulkstat files from the ASR 5000. If the directory pointed by this entry is inaccessible or does not exist, then the files FTPed by the ASR 5000 will not be archived. ***Important:*** The Archive directory path entry can be an absolute or relative path.	--	--	./bulkstat_archive/
	FileArchiveEnable: This flag enables/disables the archiving of bulkstat files. • 1 = Enables the archiving of bulkstat files • 0 = Disables this functionality	--	--	0
Polling: This section contains parameters that are used for optimization of the bulkstatistics module in terms of polling.				
PollInterval	Poll interval in seconds.	10 sec	60 sec	30 sec
PoolEnable	• 1 = Enables the thread pool • 0 = Disables the thread pool	--	--	1
Size	Size of the thread pool. ***Important:*** This value should not be greater than the MaxDbConnPool parameter defined in the *etc/db.cfg* file.	5	100	10
FetchConfig	Fetch bulkstat configuration parameters from the ASR 5000. • 1 = Fetch • 0 = Do not fetch	--	--	0
LatencyPeriod	Tolerance period to be considered for Bulkstat FTP operation.	0 min	2 min	2 min
Queue: This section contains parameters that are used for optimization of the bulkstatistics module in terms of queuing.				
QueueInterval	Queue interval in seconds.	10 sec	60 sec	10 sec
DBSession: This section contains parameters that are used for optimization of the bulkstatistics module for database calls in terms of DB sessions.				

Key	Description	Minimum Value	Maximum Value	Default Value
PermanentSession	• PermanentSession 1 = DB actions performed using permanent database sessions • PermanentSession 0 = DB actions performed using temporary database sessions	--	--	0
Parser: This section contains parameters that are used for connection to the Parser Server process.				
ParserPort	The TCP port to which the WEM server binds.	1025	65535	22224

The bsserver.cfg File

This file provides parameters pertaining to the XML-parsing of bulk statistic records received from the chassis. These parameters provide the ability to enable/disable XML parsing and to specify the directory, in which parsed records are to be stored, time intervals for checking for new records, and whether a single XML file should be generated for all subsystems or one XML file per subsystem in accordance with 3GPP TS 32.401 V4.1.0 and 3GPP TS 32.435 V6.2.0.

Important: Any change in the configuration files will restart the server resulting in client restart.

Caution: Several parameters contained in this file are configurable through the installation process.

Table 32. bsserver.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
Port: This section contains the server port to which the BulkStat server binds.				
ServerPort	The TCP port to which the WEM server binds.	1025	65535	22223
Directory: This section contains the directory path required for the BulkStat server.				
XMLDir	Base directory path where the measurement files are to be generated.	--	--	<EMSServerInstallDir>/xmldata/
FTP	Base directory for bulkstat FTP from the ASR 5000. The FTP directory entry can be changed to one of the available directories in the host file system. If the specified directory does not exist, then the bulkstats files will be configured for FTPing in *<serverpath>/data/*.	--	--	<serverpath>/data/
PMFormat	This configurable states the PM table format.	--	--	ST16
XMLDataEnable	• 1 = Enables the XML Data Parsing • 0 = Disables the XML Data Parsing	--	--	0
XMLFileType	• 1 = XML file containing all the subsystem reports • 0 = XML file containing a single subsystem report	--	--	0

Key	Description	Minimum Value	Maximum Value	Default Value
ASCIIFileGeneration	• 1 = Creates ASCII file as per the subsystem report • 0 = Creates XML file as per the subsystem report	--	--	0
XMLFileFormat	• 1 = Creates XML measurement report file using the enhanced 3GPP format (V6.2.0) • 0 = Creates XML measurement report file using the old format	--	--	0
Interval: This section contains the interval parameters for polling operations.				
DataPollInterval	Polling interval in seconds to check the availability of new data samples in the WEM bulkstat database subsystem table.	5 sec	3600 sec	60 sec
SynchInterval	Synchronization interval in seconds to check the availability of new NE (ASR 5000) for polling the data samples in the WEM bulkstat database subsystem table.	5 sec	3600 sec	120 sec
GranularityPeriod	Granularity period to generate XML report files. The following values are only supported: 300 sec (5 min), 900 sec (15 min), 1800 sec (30 min), 3600 sec (60 min) All values other than the above will be ignored and the default value will be used.	300 sec	3600 sec	300 sec
Thread Pool: This section contains the configuration values for the thread pool.				
Size	Size of the thread pool.	5	20	10
Access TIme: This section contains the configuration values for overriding the bulkstat XML measurement generation timestamp.				
OverrideLastAccessFlag	The bulkstat server utility can be made to generate complete data from the Iast record by changing the Override Last Access Flag. • OverideLastAccessFlag = 1 (Set to ON) • OverrideLastAccessFlag = 0 (Set to OFF)	--	--	0
XML Data: The following values are the default data values for the XML Measurement file for the 3GPP recommended XML nodes. For more information, refer to the 3GPP TS 32.401 V4.1.0 (2001-12) document.				
ffv	File format version applied by the EM	--	--	--

Key	Description	Minimum Value	Maximum Value	Default Value
sn	Sender Name	--	--	--
st	Sender Type	--	--	--
vn	Vendor Name	--	--	--
neun	NE User Name	--	--	--
nedn	NE Distinguish Name	--	--	--
nesw	NE Software	--	--	--
rsf	Representative Suspect Flag: Used as an indication to stop collecting data from any NE in abnormal conditions. • 0 (FALSE) in the case of normal condition • 1 (TRUE) if not normal condition	--	--	0
sf	Suspect Flag: Used as an indication of quality for the scanned data. • 0 (FALSE) in the case of reliable data • 1 (TRUE) if not reliable	--	--	0
es	Error State: Used as an indication to state that the statistics data collection is not completed due to the error condition. • 0 (FALSE) in the case of normal condition • 1 (TRUE) if not normal condition	--	--	0
UseIpAddress	Use ASR 5000 IP address as an NE User Name. • 0: Do not use IP address as a neun, that is, use host name as neun. • 1: Use IP address as neun.	--	--	0
Timezone: This section contains the configuration values for overriding the bulkstat XML measurement generation timestamp.				

Key	Description	Minimum Value	Maximum Value	Default Value
TimezoneOffsetToUTC	Configuration for time zone offset for XML file creation. NE generates data in UTC time zone. The timestamp values of the measurement data can be converted to specific time zone by applying the differential value of time in **hhmm** wrt UTC.TimezoneOffsetToUTC=signhhmm • Sign (optional) indicates the sign of the local time differential from UTC (+ or -). '+' is considered if sign is not given. • hh is the two digit number of hours of the local time differential from UTC (-12..+13). • mm is the two digit number of minutes of the local time differential from UTC (00..59). For example: • For IST: Use TimezoneOffsetToUTC=+0530 indicating 05 hours, 30 mins ahead of UTC • For KST: Use TimezoneOffsetToUTC=+0900 indicating 09 hours, 00 mins ahead of UTC • For EST: Use TimezoneOffsetToUTC=-0500 indicating 05 hours, 00 mins behind UTC	--	--	+0000
TimezoneOffsetFromUTC	Use the TimezoneOffsetFromUTC parameter for all ASR 5000s to generate XML report file.UsePerNETimezone=0 • 0 = Use TimezoneOffsetFromUTC parameter as a time zone to generate report file. • 1 = Use time zone from MISC table in database to generate report file.	--	--	+0000

Key	Description	Minimum Value	Maximum Value	Default Value
UsePerNETimezone	This parameter indicates whether to use time zone as per ASR 5000.	--	--	0
BSFTP: The bulkstat server transfers the generated XML file to NM using FTP. This section defines the default values for FTP.				
BSFTPPerformOperation	Flag to indicate whether bulkstat server should perform FTP operation of generated XML files or perform local storage. Values: • 0 = Disable FTP operation • 1 = Enable FTP operation	--	--	0
BSFTPUserName	User name field for FTP operation.	--	--	
BSFTPPassword	Password field for FTP operation.	--	--	
HostIPAddr	IP Address of the host system where the file is to be transferred.	--	--	
HostBaseDir	FTP directory where the file is to be stored on the host system.	--	--	
PoolSize	Pool size for threads.	--	--	• 10 for FTP • 3 for SFTP
PollInterval	Poll interval	--	--	
BSFTPMaxRetries	Maximum retries if FTP failed.	--	--	
BSFTPRetryInterval	Interval between retries of FTP.	--	--	
BSUseSFTP	Flag to indicate whether the bulkstat server should use SFTP/FTP to transfer the XML file to NM. Changing the value of BSUseSFTP requires bulkstat server restart. When BSUseSFTP is set to 0, increase the value of PoolSize to 10. When BSUseSFTP is set to 1, reduce the value of PoolSize to 3. Values: • 0 = Disable SFTP • 1 = Enable SFTP	--	--	0

The bstca.cfg File

This file contains parameters pertaining to the threshold configuration for bulk statistic counters. This file includes the threshold values, that is, clear threshold and set threshold to notify and clear SNMP traps accordingly. These threshold values are specified based on the threshold limit.

Table 33. bstca.cfg File Parameters

Filename	Description
bstca.cfg	This file specifies the threshold configuration for bulkstat counters. • Needs a Bulkstat Parser restart • Can be changed by the use The format is as follows: [schema name] counter name=clear threshold,set threshold *Example of the threshold configuration:* [mipha] expiry=10,20 recv-total=20,40 Threshold Value (Clear) is less than or equal to 10 for delta value of the bulkstat counter “expiry”. Threshold Value (Set) is more than or equal to 20 for delta value of the bulkstat counter “expiry”.

The cdp.cfg File

This file contains CDP specific parameters that are configured for generation of ad-hoc reports. The parameters are also configured to export Optimized Customer Master Database (OPTCMDB) files to CDP.

Table 34. cdp.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
UNKNOWNURL: This section displays unknown URL database files Import interval related information.				
UnknownUrlImportInterval	This specifies time interval in hours for Content Filtering Configuration to import various databases from CDP	1 hr	720 hrs (30 days; 1 Month)	24 hrs
Reports: This section displays the report related information.				
MaxNumberOfReports	This specifies the maximum number of reports that can be present in the *reports/cf/* directory.	50	500	250
ReportDirSizeLimit	This specifies the directory size of the reports in MB.	100	1024	500

The cf.cfg File

This file contains parameters pertaining to content filtering.

Important: Any change in the configuration files will restart the server resulting in client restart.

Table 35. cf.cfg File Parameters

Directory	Description	Minimum Value	Maximum Value	Default Value
ContentFiltering				
EnableCFFeature	Flag to enable/disable the CF features in WEM. Needs a WEM Server restart. Setting this flag to 1 will enable the CF features in WEM.Values: • 1: Enable • 0: Disable	--	--	0
CFStatistics				
CFStatsInterval	Time Interval for generating statistics. This is the time interval in seconds after which the statistics will be generated for CF.	60 sec	1800 sec	300 sec
CFBackupArchiveDatabase: This section contains the config variables related to archive operation of various CF databases.				
FullDbFilesBackupLimit	This specifies the number of backups to be maintained by Content Filtering Server for Full databases.	1	10	4
IncrementalDbFilesBackupLimit	This specifies the number of days incremental backup is to be maintained for incremental databases.	1 day	90 days	30 days
ArchiveDbFiles	This allows user to enable/disable archiving of database files once outdated. Possible values: ENABLE, DISABLE	--	--	DISABLE
ArchivePath	This specifies the path where archive files are maintained. ArchivePath = *./flash/archive/*	--	--	--
CFTRAP				
CFSnmpVersion	SNMP version for generation of WEM traps. The supported version is SNMPv1.	--	--	--

Directory	Description	Minimum Value	Maximum Value	Default Value
CFTrapReceiverHost	Alarm receiver machine IP Address. • Needs a WEM Server restart • Can be changed by the user	--	--	--
CFTrapReceiverPort	The port on which traps will be generated by the WEM server. • Needs a WEM Server restart • Can be changed by the user	1	65535	162
CFThreadPool				
CFThreadPoolSize	This is the thread pool size for export content rating databases to the chassis.	5	20	10
UnkURLImportThreadPool				
UnkURLImportThreadPoolSize	This is the thread pool size for pulling unknown URL databases from the inPilot application.	5	20	10

The configupdate.cfg File

This file contains parameters pertaining to chassis software configuration updates using the Web Element Manager. It includes the directory in which the configuration files are stored and the directory to which configuration update log files can be stored.

Important: Any change in the configuration files will restart the server resulting in client restart.

Table 36. configupdate.cfg File Parameters

Directory	Description	Minimum Value	Maximum Value	Default Value
ConfigUpdate				
LogDirPath	The directory where all generated log files are stored. It can be changed by the user. If the specified directory does not exist, then the config files will be stored in *./flash/ConfigUpdate/log*. **Important:** The config file directory path entry should always be an absolute path and not a relative path.	1	80	./flash/ConfigUpdate/log
ConfigFileDirPath	The directory where all configuration files to be loaded on the ASR 5000 are stored. It can be changed by the user. If the specified directory does not exist, then the config files will be stored in *./flash/ConfigUpdate/config*. **Important:** The config file directory path entry should always be an absolute path and not a relative path.	1	80	./flash/ConfigUpdate/config

The db.cfg File

This file contains parameters pertaining to the WEM's use of the Postgres database. It identifies the various databases and their locations.

Important: Any change in the configuration files will restart the server resulting in client restart.

Caution: Improper configuration of this file can adversely affect WEM operation. To ensure proper operation of the Web Element Manager, do not edit the parameters in these files.

Table 37. db.cfg File Parameters

Directory	Description	Minimum Value	Maximum Value	Default Value
Database	This file contains parameters pertaining to the Database Name, Database type, Host IP Address, Port, User Name and Password of the Web Element Manager application. Here, Database means Postgres, Oracle, etc. and CommitRecTime is in seconds. ***Important:*** Any change in the configuration files will restart the server resulting in client restart. The format is as follows: DbName,Database,HostAddress,Port,UserName,Password • CONFIGDBASE = configdb,postgres,127.0.0.1,5432,postgres,postgres • TRAPDBASE = trapdb,postgres,127.0.0.1,5432,postgres,postgresMI • BDBASE = mibdb,postgres,127.0.0.1,5432,postgres,postgresAU • DITDBASE = auditdb,postgres,127.0.0.1,5432,postgres,postgresB • SDBASE = bsdb,postgres,127.0.0.1,5432,postgres,postgresP2P • DBASE = p2pdb,postgres,127.0.0.1,5432,postgres,postgresNB • DBASE = nbdb,postgres,127.0.0.1,5432,postgres,postgres	--	--	--
MaxDbConnPool	Size of the DB connection pool.	1	50	25
PostgresDIR	This specifies the path of the Postgres directory. PostgresDIR = */<ems_dir>/postgres*	--	--	--

The emslic.cfg File

This file contains license information for the WEM Server installation.

Table 38. emslic.cfg File Parameters

Key	Description	Value	Default Value
License: This is the WEM License file.			
LicenseKey	License key for using WEM. • Needs a WEM Server restart • Can be changed by the user	LicenseKey = Basic|Customer-EU2|Customer-EU4	No default value

The fm.cfg File

This file contains parameters pertaining to the handling of received alarms. It provides parameters for configuring color indicators for the various severities, E-mail server information for alert notifications, and SNMP operation.

Table 39. fm.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
SEVERITY: This section describes the severity configuration for traps that contain various priorities and the color in which the traps of that severity should be displayed. • Needs a WEM Server restart • Can be changed by the user				
Severity Name	The severity name is similar to the severity color. The format is as follows: Severity Name = Severity color Severity color should be specified in a CSV format. (Comma Separated Values: red, green, blue) Valid color values range from 0 to 255. The following are some usual colors with CSV format: 255,0,0 - red 0,255,0 - green 0,0,255 - blue 255,192,203 - pink 190,190,190 - gray 255,255,255 - white 0,0,0 - black 255,255,0 - yellow 0,255,255 - cyan 169,169,169 - darkgray 211,211,211 - lightgray 255,0,255 - magenta 255,165,0 - orange 165,42,42 - brown Color entry can be of a decimal, octal or hexadecimal form. • A decimal constant begins with a non-zero digit, and consists of a sequence of decimal digits. • An octal constant consists of the prefix 0 optionally followed by a sequence of the digits 0 to 7 only. • A hexadecimal constant consists of the prefix 0x or 0X followed by a sequence of the decimal digits and letters a (or A) to f (or F) with values 10 to 15 respectively.	--	--	Default color (red, green, blue) value is 127

Key	Description	Minimum Value	Maximum Value	Default Value
Severity Level	The Severity level (number) for the nth row in the SEVERITY section is n. For example: Clear severity level is 6Minor severity level is 4 The severity levels are as follows: • Severity level 1: This specifies “Indeterminate” alarm with color code “140,140,0”. • Severity level 2: This specifies “Critical” alarm with color code “255,0,0”. • Severity level 3: This specifies “Major” alarm with color code “255,0,255”. • Severity level 4: This specifies “Minor” alarm with color code “204,153,0”. • Severity level 5: This specifies “Warning” alarm with color code “0,145,145”. • Severity level 6: This specifies “Clear” alarm with color code “0,145,0”.	--	--	--
EMAIL: This section describes the E-mail configuration for traps.				
MailFrom	E-mail address of the e-mail notification originator. • Needs a WEM Server restart • Can be changed by the user	--	--	No default value
MailServerAddr	Address in DNS or IP address format on which the SMTP (e-mail) server should be running. • Needs a WEM Server restart • Can be changed by the user	--	--	No default value
MailServerPort	Port number on which the e-mail server should be running. • Needs a WEM Server restart • Can be changed by the user	1	65535	25
DisconnectTime	Time out for mail server TCP connection in seconds. • Needs a WEM Server restart • Can be changed by the user	10 secs	3600 secs	10 secs
URLPath	URL path on which the WEM server should be running. • Needs a WEM Server restart • Can be changed by the user	--	--	No default value

Key	Description	Minimum Value	Maximum Value	Default Value
SCRIPT: This section describes the script configuration for traps.				
ScriptSrvPort	Port number on which the script server should be running. • Needs a WEM Server restart • Can be changed by the user	1	65535	22225
ScriptDirPath	Base directory in which the scripts to be executed are stored. • Needs a WEM Server restart • Must not be changed by the user - There is a separate directory that exists for the user.			<serverpath>/scripts
UserScriptDirPath	Base directory in which the user scripts to be executed are stored. Needs a WEM Server restart			<serverpath>/alarmscripts
TRAP: This section describes the flags for logging traps.				
SnmpTrapPort	The port on which traps will be received by the WEM server. • Needs a WEM Server restart • Can be changed by the user • Server must be run as root in order to receive traps on privileged ports (1 to 1024)	1	65535	162
SelectionFlag	Flag to enable or disable e-mail, notification, forwarding, script execution and syslog. • Needs a WEM Server restart • Can be changed by the user Possible values: ALL, IMG ALL: Processing the traps when it is ASR 5000 or non-ASR 5000 IMG: Only ASR 5000 traps are processed	--	--	ALL
LoggingFlag	Flag for logging traps. • Needs a WEM Server restart • Can be changed by the user Possible values: ALL, IMG ALL: All traps are logged. IMG: Only ASR 5000 traps are logged.	--	--	ALL

Key	Description	Minimum Value	Maximum Value	Default Value
BroadCastFlag	Flag for receiving broadcast-traps (case insensitive). • Needs a WEM Server restart • Can be changed by the user Possible values: ENABLE, DISABLE ENABLE: Receiving broadcast traps DISABLE: Don't receive broadcast traps.	--	--	DISABLE
GlobalOverride	Flag for global override. • Needs a WEM Server restart • Can be changed by the user Possible values: ENABLE, DISABLE ENABLE: Disable sending e-mail and executing script DISABLE: Enable e-mail and script	--	--	DISABLE
SupressEmsTraps	Flag for suppressing WEM-only Traps. • Needs a WEM Server restart • Can be changed by the user Possible values: ENABLE, DISABLE ENABLE: Disable generation of WEM traps DISABLE: Enable generation of WEM traps	--	--	DISABLE
SnmpVersion	SNMP Version for generation of WEM traps. The supported versions are: • SNMPv1 • SNMPv2c	--	--	--
ProxyFwd	Flag for configuring WEM server as proxy to forward the received SNMP traps. In case of forwarding the received SNMP traps as SNMPv2 traps, we need to - # translate the notification parameters to appropriate SNMPv2 parameters.Flag for suppressing WEM-only Traps. • Needs a WEM Server restart • Can be changed by the user Possible values: ENABLE, DISABLE ENABLE: Disable generation of WEM traps DISABLE: Enable generation of WEM traps			ENABLE
SYSLOG: This section describes the Syslog server configuration for traps.				
LogHost	Address of the machine on which syslog should be running. • Needs a WEM Server restart • Can be changed by the user			127.0.0.1

Key	Description	Minimum Value	Maximum Value	Default Value
LogPort	Port number on which syslog should be running. • Needs a WEM Server restart • Can be changed by the user	1	65535	514
Facility	Syslog facility. • Needs a WEM Server restart • Can be changed by the user FACILITY contains the following possible values: LOG_KERN,LOG_USER,LOG_MAIL, LOG_DAEMON, LOG_AUTH,LOG_SYSLOG, LOG_LPR,LOG_NEWS,LOG_UUCP,LOG_CRON,LOG_LOCAL0, LOG_LOCAL1, LOG_LOCAL2,LOG_LOCAL3,LOG_LOCAL4,LOG_LOCAL5,LOG_LOCAL6,LOG_LOCAL7	--	--	LOG_LOCAL3
Priority	Syslog priority. • Needs a WEM Server restart • Can be changed by the user PRIORITY contains the following possible values: LOG_EMERG, LOG_ALERT, LOG_CRIT, LOG_ERR, LOG_WARNING, LOG_NOTICE, LOG_INFO, LOG_DEBUG	--	--	LOG_INFO
EVENTSERVICE				
LogCLIShowCommands	Flag to enable(1)/disable(0) the logging of "show" CLI commands. • Needs a WEM Server restart • Can be changed by the user	0	1	1
AUDIO				
AudioDir	Audio directory which contains audio files. • Needs a WEM Server restart • Can be changed by the user			No default value

Key	Description	Minimum Value	Maximum Value	Default Value
GROUP	Alarm group configuration. • Needs a WEM Server restart • Can be changed by the user The group number for nth row in the GROUP section is n. For example: • "Communications Alarm" group number is 1 • "QOS Alarm" group number is 4 The alarm groups are: • Communications Alarm • Processing Error Alarm • Environmental Alarm • QOS Alarm • Equipment Alarm	--	--	No default value

Key	Description	Minimum Value	Maximum Value	Default Value
PROBABLECAUSE	Alarm probable cause configuration. • Needs a WEM Server restart • Can be changed by the user The probable cause number for nth row in the PROBABLECAUSE section is n. For example: • "Loss of multi frame sync" probable cause number is 1 • "Loss of frame sync" probable cause number is 4 The probable causes are: • Heating or ventilation system failure • Equipment malfunction • Manual configuration, software crash or voltage fluctuation • Module inserted • Module removed • Software failure or crash • Module slot mismatch • Congestion • Communication problem • Configuration or customization error • Manual configuration or threshold crossed • Underlying resource unavailable	--	--	0 (means empty)
CLIInfoPolling: This section provides information needed for the configuration of Thread pool and Polling interval required for the FMCliInfoHandler module.				
CLIInfoPollInterval	Poll interval in seconds. ***Important:*** These value are dependent on the keepalive notification interval.	1 sec	30 sec	15 sec
CLIInfoThreadPoolSize	Size of the Thread Pool.	5	20	10
PENDINGALARM: This section describes the pending alarm related configuration.				

Key	Description	Minimum Value	Maximum Value	Default Value
autoClearInterval	Time-out interval for pending alarms in days. If any alarm is in pending state for this configured interval, then it will be automatically cleared. • Needs a WEM Server restart • Can be changed by the user	1	30	3

The hwinv.cfg File

This file provides the e-mail ID used when sending hardware change notifications.

Important: The parameter in this file is configurable through the installation process.

Table 40. hwinv.cfg File Parameters

Key	Description	Default Value
HWEMAIL: This is the configuration file for Hardware Inventory.		
ChangeInHWMailFrom	• E-mail address of the e-mail notification originator • Needs a WEM Server restart • Can be changed by the user	No default value

The ism.cfg File

This file contains parameters pertaining to communication between the Web Element Manager and managed chassis. These parameters include the security information used to access the chassis as well as the ports over which communication takes place.

This file also contains a parameter that provides the ability to enable/disable the SSL encryption for client-to-server and server-to-boxer communication.

Important: Any change in the configuration files will restart the server resulting in client restart.

Table 41. ism.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
IMGSessMgt: This section describes the parameters that store ASR 5000 login information.				
ASID	Application Server ID that will be used by the WEM server to communicate with ASR 5000. • Needs a WEM Server restart • Can be changed by the user	1	10	STARENT
ASPasswd	Application Server Password for the ASR 5000 that will be used by the WEM server to communicate with the ASR 5000. • Needs a WEM Server restart • Can be changed by the user	1	35	SN123
IMGPort	Port number on which the ASR 5000 should be running. • Needs a WEM Server restart • Can be changed by the user	10000	65535	14132
SSLConnect	Flag to enable or disable the SSL connection. • Needs a WEM Server restart • Can be changed by the user Currently, this feature is disabled and only IIOP connections will be used.	0	1	0

Key	Description	Minimum Value	Maximum Value	Default Value
EnforceSSL	Flag to enforce SSL. • Needs a WEM Server restart. • Can be changed by the user. • Overrides SSLConnect value, if set to 1. Change the value of ENFORCE_SSL parameter in ems/client/img.html and *ems/client/imgdebug.html* if this value is changed. If set to 1, then the sslflag field will be updated to 't' for all existing IMGs in the boxer table in ConfigDB at server restart.	0	1	0
SleepTime	Time for which the cleanup thread sleeps. • Needs a WEM Server restart • Can be changed by the user	5	300	60
MaxIdleTime	Maximum time for which the servant reference can be idle.Needs a WEM Server restartCan be changed by the user	30	1800	300
IMGKeepAlive: This section describes parameters related to the ASR 5000 keep-alive.				
IcmpTimeout	Timeout value for ICMP requests in seconds.	1	60	5
IcmpRetries	Number of retries for ICMP requests.	0	10	2
IcmpKeepAliveInterval	Polling interval for ICMP requests in seconds. ***Important:*** The value must be greater than IcmpTimeout * (IcmpRetries + 1).	5	300	30
CorbaKeepAliveInterval	Polling interval for CORBA requests in seconds. ***Important:*** The value must be greater than or equal to IcmpKeepAliveInterval.	10	600	2 * IcmpKeepAliveInterval

The mcrdbs.cfg File

This file contains parameters that are configured to support the conversion of Vendor Format Master Database (VFMDB) to Starent Networks Format Master Database (SFMDB). This file also contains information on MCRDBS to handle the database files.

Table 42. mcrdbs.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
MCRDBS: This section describes parameters that store MCRDBS related information.				
FullDBFilesImportInterval	Database files Import interval: This specifies the time interval in hours for Content Filtering Server to import various databases from MCRDBS. (Databases: SFMDB)	2 hrs	4320 hrs (90 days; 6 months)	24 hrs
INCDBFilesImportInterval	Database files Import interval: This specifies the time interval in hours for Content Filtering Server to import various databases from MCRDBS. (Databases: SFMDB-INC)	2 hrs	720 hrs (30 days; 1 month)	24 hrs
StarentFormatDbFileImportPath	Starent format database file path: This specifies the path where SFMDB files are located in MCRDBS. Example: *<Mcrdbs server path>/cfems/<cfems ip address>/sfmdb*	--	--	--
StarentFormatIncDbFileImportPath	Starent format incremental database file path: This specifies the path where SFMDB-INC files are located in MCRDBS. Example: *<MCRDBS server path>/cfems/<cfems ip address>/sfmincdb*	--	--	--
MCRDBSInfo	This specifies the MCRDBS information in the following format:MCRDBS Host name, MCRDBS Ip address1, User name1, password1 ***Important:*** If the user does not want to enter any values, leave the fields blank separated by comma. Example: hostName, userName, password (OR), HostIPAddr, userName, Password	--	--	--

The mdproxy.cfg File

This configuration file defines various properties used for the MD EMS Proxy functionality.

Table 43. mdproxy.cfg File Parameters

Key	Description
MDAUDIT	
MDAuditPath	The directory path to log the audit trail into file. The base is the WEM server's directory. MDAuditPath = log/RESP
MDAuditSyncPath	MDAuditSyncPath = log/SYNC_RESP
MDAlarmPath	MDAlarmPath = log/FM

The nb.cfg File

This file contains parameters for NorthBound notifications from the WEM. The information in this file is used by the application for forwarding fault management information to other management devices on the NorthBound interface. This information includes such things as the device IP address and port number on which to forward notifications.

Important: Any change in the configuration files will restart the server resulting in client restart.

Table 44. nb.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
Fault Management: This section describes the parameters that store NorthBound Notification Service related configuration information.				
NSMode	Mode using WEM gets the Notification Service reference.Valid values: URL, IOR, NONE • Needs a WEM Server restart • Can be changed by the user	--	--	NONE
NSMode is URL�	Notification Service URL. The format is as follows: corbaloc:iiop:<NSAddr>:<NSPort>/<ChannelFactoryName>	--	--	corbaloc:iiop:127.0.0.1:5001/NOTIFY_SVC/CHANNEL_FACTORY
NSAddr	Host IP Address on which the Notification Service should be running. • Needs a WEM Server restart • Can be changed by the user	--	--	127.0.0.1
NSPort	Port number on which the Notification Service should be running • Needs a WEM Server restart • Can be changed by the user	1000	65535	5001
ChannelFactoryName	Names to be assigned to the channel factory created by the Notification Service daemon. • Needs a WEM Server restart • Can be changed by the user	--	--	NOTIFY_SVC/CHANNEL_FACTORY

Key	Description	Minimum Value	Maximum Value	Default Value
NSIORFILE	Path name of the Notification Service IOR (String field object reference) file. Here, the NSMode is IOR. • Needs a WEM Server restart • Can be changed by the user	--	--	No default value
NSChannelId	Channel ID through which WEM notifies the events. • Needs a WEM Server restart • Can be changed by the user	0	1000	0

The nbserver.cfg File

This file contains parameters for the configuration of NorthBound Server and Notification Service processes, and NorthBound interface.

Important: Northbound Server is now enabled as part of the basic WEM license. For older versions of WEM where the default value is set to disable Northbound Server, locate the *nbserver.cfg* file and set the *NBIntfEnable* flag to enable Northbound Server.

The nms.cfg File

This file contains parameters which control WEM access to the PostgreSQL database, client access to the server, and other properties used by the application for proper operation.

Important: Many of the parameters contained in this file are configurable through the installation process.

Table 45. nms.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
DATABASE: This section describes parameters that store database configuration information.				
HostAddress	This specifies the host IP address.	--	--	127.0.0.1
UserName	This specifies the username to connect to the database.	--	--	postgres
PassWord	This specifies the password to connect to the database.	--	--	postgres
IOR				
Login		--	--	login.ior
RESPath		--	--	res_path.ior
SVPNIOR		--	--	svpn.ior
ConfigAudit		--	--	audit.ior
ClientSession: This section describes parameters related to client session management.				
UserLimit	Maximum number of user sessions allowed by the server at any time.	1	100	10
SecurityAdminLimit	Maximum number of Security Administrator sessions allowed by the server at any time.	1	UserLimit	5
ActiveToInactiveInterval	Time for activity time out in minutes.	1	-1 (infinite)	15
KeepAliveCallInterval	Keep alive polling time in seconds.	0	8600	15
KeepAliveRetryCnt	Retry count for keep alive: The minimum time for dismissing the client session if it is not reachable = KeepAliveCallInterval * KeepAliveRetryCnt	1	5	2

Key	Description	Minimum Value	Maximum Value	Default Value
SessionInitTime	Time required for a typical session to initialize to ready state. Keep alive will be enabled after a specified time after client login.	KeepAliveCallInterval	86400	120
UserSessionLimit	Maximum number of sessions for a particular user.	1	UserLimit	5
ContextUserLimit	Maximum number of user sessions for a context.	1	UserLimit	5
Notification	Global flag to enable/disable the sending notification. Possible values: ENABLE, DISABLE	--	--	ENABLE
Active timeout interval	This flag allows the user to login to the N+1st WEM Client and also, to cleanup any inactive / dead sessions. Session will get timed out after the given time (minutes) from the login time. Valid User: Security Administrator	--	--	--
DenialService	Global Flag to enable/disable the Denial-Of-Service. Possible Values: ENABLE, DISABLE	--	--	DISABLE

Key	Description	Minimum Value	Maximum Value	Default Value
DefaultUPref	This is the default user preference configuration XML string. DefaultUPref = <xml version="1.0" encoding="UTF-8"> <screen id="SCR_ID_TOPOLOGY"> <dimension> <param name="RESOLUTION" value="1024X768"/> <param name="XPOS" value="137"/> <param name="YPOS" value="89"/> <param name="WIDTH" value="512"/> <param name="HEIGHT" value="384"/> </dimension> <information> <param name="MAP_COLOR" value="-1"/> <param name="MAP_IMAGE" value="none"/> <param name="LOOK_AND_FEEL"value="Metal"/> <param name="LAST_MAP_VISITED" value="true"/> <param name="LAST_MAP_NAME" value="default"/> <param name="LAST_IMG_VISITED" value="true"/> <param name="LAST_IMG_NAME" value="earth"/> <paramname="CLIENT_TIMEOUT" value="60"/> <param name="POLLING_INTERVAL" value="10"/> <param name="AUDIO_ALARMING" value="true"/> <param name="SHOW_TOOLBAR" value="true"/> <param name="TOOLBAR_POSITION" value="North"/> <param name="NOTIFICATION" value="true"/> </information> </screen>	--	--	--

Key	Description	Minimum Value	Maximum Value	Default Value
DefaultAppPath	This is the default Application Path XML string. DefaultAppPath=<xml version="1.0" encoding="UTF-8"> <screen id="SCR_ID_APPLICATION_PATH"> <dimension> <param name="RESOLUTION" value="1024X768"/> <param name="XPOS" value="272"/> <param name="YPOS" value="275"/> <param name="WIDTH" value="608"/> <param name="HEIGHT" value="313"/> </dimension> <os id="Windows 95"> <param name="telnet" value="cmd /c start c:\\telnet.exe"/> <param name="ftp" value="cmd /c start c:\\ftp.exe"/> <param name="ssh" value="cmd /c start c:\\ssh.exe"/> <param name="mibbrowser" value="cmd /c start c:\\mibbrowser.exe"/> </os>	--	--	--
SWUpgrade: This section describes the parameters related to Software Upgrade.				
FTPSessLimit	Maximum number of FTP sessions.	--	--	5
FTPCallBackPeriod	Call back period in seconds with which the status of the FTP will be updated.	--	--	--
NMSIMGBaseDir	Base directory for Software Upgrade Manager - Image files.	--	--	NMSIMGBaseDir = ./flash
NMSIMGBaseDirForFileCompare	Base directory for Config file comparison - Image files.	--	--	NMSIMGBaseDirForFileCompare = ./flash
FRV: This section describes the front/rear-view related parameters.				
PollInterval	Time interval used by the WEM Client for polling. • Does not require WEM Server restart • This value can be changed by the user	10 secs	60 secs	30 secs
Topology				
ClientBaseDir	Client base directory: This value is internally used by the Topology server module and should not be changed.	--	--	--

Key	Description	Minimum Value	Maximum Value	Default Value
MapImageDir	Directory Name which contains image files. This value can be changed and the subdirectory must exist in ClientBaseDir.	--	--	--
POAPolicies: This section describes policies used for the POAs.				
ServerIIOPPort	Using this port, three sequential upward ports will be used to create POAs. Change the value of SERVER_BASE_PORT parameter in ems/client/img.html and ems/client/imgdebug.html if this value is changed.	15000	15002	15000
EMSLicense				
Mode	The mode in which WEM started. Valid values: PDSN, GGSN, BOTH The value must be specified otherwise, the server does not function.	--	--	--
ConfigBackup				
FTPUserName	User name that will be used by the ASR 5000 to upload files on WEM server. This user account should be existing on the WEM server host machine. • Needs server restart • Can be changed by the user	1	64	guest
FTPPassword	Password that will be used by the ASR 5000 while uploading files to WEM server. This user account should be existing on the WEM server host machine. • Needs server restart • Can be changed by the user	1	64	guest12
EMSServer				

Key	Description	Minimum Value	Maximum Value	Default Value
ServerIpAddress	This IP Address will be used by WEM server for generating IOR files. If the field has default loopback interface values then, WEM server will take the first active interface present on the machine. Change this IP value to change IP used for IOR generation. If the specified IP is not active, WEM server will not start.	--	--	127.0.0.1
ServerPort	The TCP port to which the WEM server binds.	1025	65535	22222
EMSORB: This section describes the parameters related to Object Request Broker.				
ORBReadTimeout	The read time out used for sockets in seconds.	5 secs	3600 secs	30 secs
ORBWriteTimeout	The write time out used for sockets in seconds.	5 secs	3600 secs	30 secs
EMSSSLORB				
SSLORBReadTimeout	The read time out used for sockets in seconds.	5 secs	3600 secs	30 secs
SSLORBWriteTimeout	The write time out used for sockets in seconds.	5 secs	3600 secs	30 secs

The pcrefgen.cfg File

Configuration file for 3GPP XML report generation of Camiant PCRF.

Table 46. pcrefgen.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
MPEManagerInfo: This section provides information required to configure the details of MPE Manager making the HTTP Post request.				
MPE Manager IP-address	EMS will make HTTP Post request to the configured address to fetch the MPE OM statistics periodically. Needs a PCRF Report generation restart. Needs a PCRF Report generation restart.	--	--	--
MPE Manager host-name	EMS will use the configured name for generating 3GPP statistics for MPE Manager related counters. This name will be used as userLabel in the 3GPP XML file and also in the file name. This name should not be identical to any MPE name. Can be changed by the user.	--	--	Empty. In this case ip-address will be used.
MPE Manager user-id	EMS will make HTTP Post request to the configured user-id for login to make HTTP Post request to MPE Manager. Can be changed by the user.	--	--	--
MPE Manager password.	EMS will make HTTP Post request to the configured password for login to make HTTP Post request to MPE Manager. Needs a PCRF Report generation restart. Can be changed by the user.	--	--	--
MPE Manager XML interface URL.	This URL, the ip-address and the userId-password will be used to construct the HTTP Post request URL. Needs a PCRF Report generation restart. Can be changed by the user.	--	--	mi/xmlInterfaceRequest.do
XMLInterfaceUrl	--	--	--	mi/xmlInterfaceRequest.do
Report Generation				

Key	Description	Minimum Value	Maximum Value	Default Value
Poll Interval	EMS will poll the MPE Manager as the configured poll-interval.This poll interval should be the same as the sample interval configured at MPEManager. Value in minutes. Can be changed by the user. PollInterval = 15	--	5	15 minutes
Latency Period.	This the latency (delay) in making the request to MPE Manager.So for fetching the statistics for time interval 12:15:00 to 12:30:00, the HTTPPOST request to MPE Manager will be made at 12:32:00 (endTime + LatencyPeriod). Value in seconds. Can be changed by the user. ReqLatencyPeriod = 120	0	900 (15 minutes).	120 seconds.
Initial offset for StartTime.	This is the offset in number of minutes before the utility's startup time to be used for fetching the PCRF statistics from the MPE Manager. e.g. if this value is set as 120 and the utility is started at 08:30:00 then the reports will be generated for statistics from 06:30:00. This value will be overridden by the next StartTime stored in database. Value in minutes. StartTimeOffset = 0	0	1400	0
PCRFUseDoubleQuotes	0 = Disable encapsulating all the values in the generated PCRF files in double quotes. 1 = Enable encapsulating all the values in the generated PCRF files in double quotes. PCRFUseDoubleQuotes=0	--	--	0
PCRFFTP: The pcrfrepgen process transfers the generated 3GPP XML file to NM using ftp. This section defines the default values for ftp. The pcrfrepgen process uses the same host machine used by the bulkstat server for transferring the GGSN files. FTP configuration parameters 'HostIPAddr', BSFTPUserName', 'BSFTPPassword', 'BSFTPMaxRetries', 'BSFTPRetryInterval' and BSUseSFTP' from */etc/bsserver.cfg* will be used to transfer the generated PCRF 3GPP XML files.				
PcrfFTPPort	Port number used to FTP/SFTP the PCRF XML files. This attribute can be changed by the user. When BSUseSFTP is set to 1, set BSFTPPort to 22.	--	--	21 for FTP; 22 for SFTP.
HostIPAddr	IP address of the host system where the file is to be transferred.	--	--	127.0.0.1
BSFTPUserName	User name field for ftp operation.	--	--	Anonymous.
BSFTPPassword	Password field for ftp operation.	--	--	Guest.

The processmonitor.cfg File

This file contains parameters used by the Process Monitor function. These include parameters such as the directories from which WEM-related processes are started, polling intervals, and maximum percentage thresholds.

Table 47. processmonitor.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
ProcessInfo: This section provides all the process information to be monitored by the module.				
ListServer	Lists all the servers to be monitored: 0 = WebServer 1 = DB 2 = EMSServer 3 = EMSScriptServer 4 = BulkstatServer 5 = BulkstatParser 6 = NBServer 7 = NotifyService	--	--	--
WebServer	Web Server Process Information: In this case, it is the Apache Web Server. • Name of the Process executable: ExeName=httpd • Absolute or Relative path for executable file: ExePath=/<*ems_dir*>/*apache/bin* • File name which contains the pid of the process: PidName=httpd.pid • Absolute or Relative path for the pid file: PidPath=/<*ems_dir*>/*apache/logs* • MultiProc: Flag indicating whether the process information should include the information of child processes or not. Valid values: • 0: Disable • 1: Enable	--	--	0

Key	Description	Minimum Value	Maximum Value	Default Value
DB	Database Process Information: In this case, it is Postgres. • Name of the Process executable: ExeName=postmaster • Absolute or Relative path for executable file: ExePath=/<*ems_dir*>/*postgres/bin* • File name which contains the pid of the process: PidName=postmaster.pid • Absolute or Relative path for the pid file: PidPath=/<*ems_dir*>/*postgres/data* • MultiProc: Flag indicating whether the process information should include the information of child processes or not. Valid values: • 0: Disable • 1: Enable	--	--	0
EMSServer	EMS Server Process Information. • Name of the Process executable: ExeName=server • Absolute or Relative path for executable file: ExePath=/<*ems_dir*>/*server/bin* • File name which contains the pid of the process: PidName=server.pid • Absolute or Relative path for the pid file: PidPath=/<*ems_dir*>/*server* • MultiProc: Flag indicating whether the process information should include the information of child processes or not. Valid values: • 0: Disable • 1: Enable	--	--	0

Key	Description	Minimum Value	Maximum Value	Default Value
EMSScriptServer	EMS Script Server Process Information. • Name of the Process executable: ExeName=scriptsrv • Absolute or Relative path for executable file: ExePath=/<*ems_dir*>/*server/bin* • File name which contains the pid of the process: PidName=script.pid • Absolute or Relative path for the pid file: PidPath=/<*ems_dir*>/*server* • MultiProc: Flag indicating whether the process information should include the information of child processes or not. Valid values: • 0: Disable • 1: Enable	--	--	0
BulkstatServer	BulkstatServer Process Information. • Name of the Process executable: ExeName=bulkstatserver • Absolute or Relative path for executable file: ExePath=*./bin* • File name which contains the pid of the process: PidName=bsserver.pid • Absolute or Relative path for the pid file: PidPath=. • MultiProc: Flag indicating whether the process information should include the information of child processes or not. Valid values: • 0: Disable • 1: Enable	--	--	0

Key	Description	Minimum Value	Maximum Value	Default Value
BulkstatParser	BulkstatParser Process Information. • Name of the Process executable: ExeName=bulkstatparser • Absolute or Relative path for executable file: ExePath=./bin • File name which contains the pid of the process: PidName=bulkstatparser.pid • Absolute or Relative path for the pid file: PidPath=. • MultiProc: Flag indicating whether the process information should include the information of child processes or not. Valid values: • 0: Disable • 1: Enable	--	--	0
NBServer	NBServer Process Information. • Name of the Process executable: ExeName=nbserver • Absolute or Relative path for executable file: ExePath=./bin • File name which contains the pid of the process: PidName=nbserver.pid • Absolute or Relative path for the pid file: PidPath=. • MultiProc: Flag indicating whether the process information should include the information of child processes or not. Valid values: • 0: Disable • 1: Enable	--	--	0

Key	Description	Minimum Value	Maximum Value	Default Value
NotifyService	NotifyService Process Information. • Name of the Process executable: ExeName=Notify_Service • Absolute or Relative path for executable file: ExePath=./bin • File name which contains the pid of the process: PidName=notify_service.pid • Absolute or Relative path for the pid file: PidPath=. • MultiProc: Flag indicating whether the process information should include the information of child processes or not. Valid values: • 0: Disable • 1: Enable	--	--	0
DirectoryInfo: This section provides information needed to monitor the directory size.				
DirEMSServer	EMS Server Directory Information. Path of EMS Server directory: DirPath=/<*ems_dir*>/*server*	--	--	--
DirDB	Database Directory Information. Path of Database directory: DirPath=/<*ems_dir*>/*postgres/data*	--	--	--
DirEMSFtp	EMS FTP Directory Information. Path of EMS FTP directory: DirPath=*./data*	--	--	--
DirEMSBlkArch	EMS Bulkstat Archive Directory Information. Path of EMS Bulkstat archive directory: DirPath=*./bulkstat_archive*	--	--	--
DirFTPCFDB	FTP CF DB Directory Information. Path of FTP directory for CF DB: DirPath=*./flash/cf/cfdatabases*	--	--	--
Poll Information: This section provides information needed for the configuration of threshold poll interval in seconds. Each sub-module under monitor has its own poll interval defined to give fine tune support.				
ProcInfoPollInterval	The process which changes frequently can be monitored for threshold limits with a smaller poll interval, say 5 seconds.	1 sec	36000 sec	5 sec
DirInfoPollInterval	The directory size does not change suddenly and can be monitored with 1 Min OR greater than 1 Min poll interval for threshold limit.	60 sec	36000 sec	300 sec
IFInfoPollInterval	If information is constant, it can be monitored once in a Min.	5 sec	36000 sec	60 sec

Key	Description	Minimum Value	Maximum Value	Default Value
Threshold Information: This section provides information needed for the configuration of default threshold values for various parameters monitored by the module. These values (if available to server successfully from this configuration file) are used for default configuration of the threshold values for the parameters.These values indicate the maximum percentage of threshold limits for the individual parameters as the default values. Note: • WEM server will take the current configuration for the latest threshold values from the WEM Database saved in the last session of the server. • The following values can be used as default configuration for the parameter(s) if no value(s) is/are available from the database. For example, first run of the server after a new installation or a database crash, etc.) To use the following values to override the database configurations with configuration values, WEM server administrator can turn on (set value to 1) the *OverrideDBConfig* flag.				
ThreshProcWebServer	This is the threshold value for disk utilization of Web Server process.	0	100	25
ThreshProcDB	This is the threshold value for disk utilization of DB Server process.	0	100	25
ThreshProcEMSServer	This is the threshold value for disk utilization of EMS Server process.	0	100	25
ThreshProcEMSScriptServer	This is the threshold value for disk utilization of EMS Script Server process.	0	100	25
ThreshProcBulkstatServer	This is the threshold value for disk utilization of Bulkstat Server process.	0	100	25
ThreshProcBulkstatParser	This is the threshold value for disk utilization of Bulkstat Parser process.	0	100	25
ThreshProcNBServer	This is the threshold value for disk utilization of NB Server process.	0	100	25
ThreshProcNotifyService	This is the threshold value for disk utilization of Notify Service process.	0	100	25
ThreshProcTotalCPU	This is the threshold value for total disk utilization of CPU.	0	100	60
ThreshProcTotalSwap	This is the threshold value for total disk utilization of swaps.	0	100	75
ThreshDirEMSServer	This is the threshold value for disk utilization of EMS Server Directory.	0	100	25
ThreshDirDB	This is the threshold value for disk utilization of Database Directory.	0	100	25
ThreshDirFTP	This is the threshold value for disk utilization of FTP Directory.	0	100	25
ThreshDirBlkArch	This is the threshold value for disk utilization of Bulkstat Archive Directory.	0	100	25
ThreshDirCFDB	This is the threshold value for disk utilization of CF DB Directory0.	0	100	25

Key	Description	Minimum Value	Maximum Value	Default Value
OverrideDBConfig	Flag to override the current DB Configuration of the threshold values with the configuration values. Values: • 1: True • 0: False	--	--	0
CPU: This section describes the parameters used to calculate the CPU utilization.				
NumberofSample	This calculates the average of 'NumberofSample' given in the config file.	1	360	5

The ps.cfg File

This file contains parameters which control Web Element Manager polling intervals for managed chassis and database queries.

Important: Any change in the configuration files will restart the server resulting in client restart.

Table 48. ps.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
Polling: This section describes the parameters related to polling support.				
MinPollInterval	Minimum time interval used by the WEM server for polling. • Needs a WEM Server restart • Can be changed by the user	10 secs	86400 secs	10 secs
MaxPollInterval	Maximum time interval used by the WEM server for polling. • Needs a WEM Server restart • Can be changed by the user	10 secs	86400 secs	86400 secs
PoolEnable	Flag to enable/disable the thread pool. • Needs a WEM Server restart • Can be changed by the user Values: • PoolEnable 1 = Thread pool enable • PoolEnable 0 = Thread pool disable	0	1	0
Size	Size of the thread pool. • Needs a WEM Server restart • Can be changed by the user	10	100	10
MaxSize	Maximum size of the thread pool. • Needs a WEM Server restart • Can be changed by the user	10	100	10

Key	Description	Minimum Value	Maximum Value	Default Value
ErrorCausingMethodRetries	Number of retries for error causing method. WEM server stops calling the error causing method after configurable successive method calls give the same error. • Needs a WEM Server restart • Can be changed by the user	1	10	3
EnableInterval	Enabling interval for disabled fetch in seconds. The server periodically enables the disabled fetch. • Needs a WEM Server restart • Can be changed by the user	10	600	120
Database: This section describes the parameters related to database information.				
QueryNameLimit	Number of queries to be stored in the database per user per context. • Needs a WEM Server restart • Can be changed by the user	100	200	100

The psmon.cfg File

This file contains parameters for the operation of the PSMon (process monitor) function supported by the WEM.

Table 49. psmon.cfg File Parameters

Key	Description	Default Value
NotifyEmail	Defines the e-mail address where notification e-mails are to be sent.	root@localhost
SmtpHost	Defines the IP address or hostname of the SMTP server to be used to send e-mail notifications.	localhost
Frequency	Defines the frequency of process table queries. This is the polling interval.	60 secs
LastSafePID	When defined, psmon will never attempt to kill a process ID which is numerically less than or equal to the value defined by the last safepid. ***Important:*** Psmon will never attempt to kill a process ID lesser than or equal to 1, or itself.	100
ProtectSafePIDsQuietly	Accepts a boolean value of On or Off. Suppresses all notifications from preserved process IDs when used in conjunction with the last safepid directive.	Off
DryRun	Forces this psmon to as if the --dryrun command line switch had specified. This is useful if you want to force a specific configuration file to only report and never actually take any automated action. This is enabled in this default distribution configuration to prevent people from blindly executing psmon “out of the box” and causing damage in live environments. The <Process *> scope is commented out by default. It should be used with extreme care. If used, run psmon in “DryRun” mode by adding the “DryRun” directive in this configuration file. ***Important:*** Read the config file thoroughly before enabling this feature.	Enabled

Key	Description	Default Value

For example:
Use the following format to configure each process. Copy the following 6 lines for each WEM Process to monitor and modify according to the WEM Path:

```
<Process /<ems_dir>/server/bin/server>
spawncmd (cd /<ems_dir>/server; /<ems_dir>/server/bin/server)
pidfile /<ems_dir>/server/server.pid
numretry 2
tmintval 300
</Process>
```

Note: Do not remove the following statement as it is used to modify the config file while installing through the GUI Installer:

```
<Process /<ems_dir>/postgres/bin/postmaster -i>
spawncmd /<ems_dir>/server/scripts/postgresctl start
pidfile /<ems_dir>/postgres/data/postmaster.pid
numretry 10
tmintval 330
</Process>

<Process /<ems_dir>/apache/bin/httpd -f /<ems_dir>/apache/conf/httpd.conf>
 spawncmd /<ems_dir>/apache/bin/apachectl start
 pidfile /<ems_dir>/apache/logs/httpd.pid
 numretry 10
 tmintval 330
</Process>

<Process /<ems_dir>/server/bin/server>
 spawncmd (cd /<ems_dir>/server; /<ems_dir>/server/bin/server)
 pidfile /<ems_dir>/server/server.pid
 numretry 10
 tmintval 330
</Process>

<Process /<ems_dir>/server/bin/bulkstatserver>
 spawncmd (cd /<ems_dir>/server; /<ems_dir>/server/bin/bulkstatserver)
 pidfile /<ems_dir>/server/bsserver.pid
 numretry 10
 tmintval 330
</Process>
```

Key	Description	Default Value
<Process /<ems_dir>/server/bin/bulkstatparser> spawncmd (cd /<ems_dir>/server; /<ems_dir>/server/bin/bulkstatparser) pidfile /<ems_dir>/server/bulkstatparser.pid numretry 10 tmintval 330 </Process> <Process /<ems_dir>/server/bin/Notify_Service> spawncmd (cd /<ems_dir>/server; /<ems_dir>/server/bin/nbSrvr) pidfile /<ems_dir>/server/notify_service.pid numretry 10 tmintval 330 </Process> <Process /<ems_dir>/server/bin/nbserver> spawncmd (cd /<ems_dir>/server; /<ems_dir>/server/bin/nbserver) pidfile /<ems_dir>/server/nbserver.pid numretry 10 tmintval 330 </Process> <Process /<ems_dir>/server/bin/scriptsrv> spawncmd (cd /<ems_dir>/server; /<ems_dir>/server/bin/scriptsrv) pidfile /<ems_dir>/server/script.pid numretry 10 tmintval 330 </Process> Where: • numretry and tmintval are optional • “tmintval” must be in seconds and greater than ('numretry' * 'Frequency’) • Incase of wrong values, this will not work properly		
New Processes		
Do not edit these lines if you do not have enough information. The instances should not be 0. <Process /<ems_dir>/perl5.8.5/bin/perl -w ./psmon --daemon --cron> pidfile /<ems_dir>/server/psmon.pid instances 1 </Process>		
Sendmail SMTP Mail Daemon		
<Process sendmail> spawncmd /sbin/service sendmail start pidfile /var/run/sendmail.pid </Process>		
Apache Group HTTP Daemon		

Key	Description	Default Value
<Process httpd> spawncmd /sbin/service httpd restart pidfile /var/run/httpd.pid instances 200 pctcpu 80 </Process>		
MySQL Database		
<Process mysqld> spawncmd /sbin/service mysqld restart killcmd /sbin/service mysqld stop pidfile /var/run/mysqld/mysqld.pid pctcpu 90 pctmem 60 </Process>		

The res.cfg File

This file contains parameters for associating resource-bundles to specific Web Element Manager dialogs. This is the configuration file for fetching screen-specific resource-bundle paths. Currently there are only two bundles. The resource-ids must be present in both the sections.

Important: Any change in the configuration files will restart the server resulting in client restart.

Caution: To ensure proper operation of the Web Element Manager, do not edit the parameters in these files.

Table 50. res.cfg File Parameters

Bundle 1	Bundle 2

Bundle 1	Bundle 2
GlobalCommonId = res.globalcommon.GlobalCommonCompFileChooserId = res.components.FileChooserCompColorChooserId = res.components.ColorChooserCompOptionPaneId = res.components.OptionPaneCompTableId=res.components.table.STableScrKeyExport = res.components.table.SExportFileScrKeyBoxerList = res.screens.boxerlist.GlobalListScrKeyUser = res.screens.useradm.UserAdminScrKeySubscriber = res.screens.subscriber.SubscriberScrKeyPPPSession = res.screens.ppp.SPPPScrKeyPPPConfig = res.screens.ppp.SPPPScrKeyPPPCounter = res.screens.ppp.SPPPScrKeyPPPSummary = res.screens.ppp.SPPPScrKeyPPPEchoTest = res.screens.ppp.SPPPScrKeyPPPStat = res.screens.ppp.SPPPScrKeyPPPInfo = res.screens.ppp.SPPPScrKeyAAATest = res.screens.aaa.SRADIUSScrKeyAAARADIUSTest = res.screens.aaa.SRADIUSScrKeyAAARADIUSCounter = res.screens.aaa.SRADIUSScrKeyAAARADIUSCounterDetails = res.screens.aaa.SRADIUSScrKeyAAARADIUSAuth = res.screens.aaa.SRADIUSScrKeyAAARADIUSAuthConfig = res.screens.aaa.SRADIUSScrKeyAAARADIUSAcct = res.screens.aaa.SRADIUSScrKeyAAARADIUSCharging = res.screens.aaa.SRADIUSScrKeyAAARADIUSChargingConfig = res.screens.aaa.SRADIUSScrKeyAAAContextConfig = res.screens.aaa.SRADIUSScrKeyModifyContextAAA = res.screens.aaa.SRADIUSScrKeyAAARADIUSResult = res.screens.aaa.SRADIUSScrKeyAAAGlobalConfig = res.screens.aaa.SRADIUSScrKeyModifyGlobalAAA = res.screens.aaa.SRADIUSScrKeySubsCriteria = res.screens.monitor.SMonitorFilterScrKeyFrontView = res.screens.csp.SCSPScrKeyRearView = res.screens.csp.SCSPScrKeySysInfo = res.screens.csp.SCSPScrKeyCardConfig = res.screens.csp.SCSPScrKeyPortConfig = res.screens.csp.SCSPScrKeyModifyPort = res.screens.csp.SCSPScrKeyPortInformation = res.screens.csp.SCSPScrKeyShowPortCounters = res.screens.csp.SCSPScrKeyIntfPortBind = res.screens.csp.SCSP	ScrKeyBoxerOperation = res.screens.boxerlist.BoxerOperationScrKeyNewMap = res.screens.boxerlist.NewMapScrKeySelectImage = res.screens.boxerlist.SelectImageScrKeyUserAdmin = res.screens.useradm.UserAdminScrKeyUser = res.screens.useradm.UserScrKeySubscriber = res.screens.subscriber.SubscriberScrKeyShowSubscriber = res.screens.subscriber.SShowSubscriberScrKeyShowSubscriberPDSNResult = res.screens.subscriber.SShowSubscriberPDSNResultScrKeyShowSubscriberGGSNResult = res.screens.subscriber.SShowSubscriberGGSNResultScrKeyAbout = res.topology.AboutDialogScrKeyTopology = res.topology.TopologyScrKeyPPPSession = res.screens.ppp.SPPPSessionScrKeyPPPConfig = res.screens.ppp.SPPPConfigScrKeyPPPCounter = res.screens.ppp.SPPPCounterScrKeyPPPSummary = res.screens.ppp.SPPPSummaryScrKeyPPPStat = res.screens.ppp.SPPPStatScrKeyPPPInfo = res.screens.ppp.SPPPInfoScrKeyContextAdministration = res.screens.contextlist.ContextAdministrationScrKeyContextAdd = res.screens.contextlist.ContextAddScrKeyContextModify = res.screens.contextlist.ContextModifyScrKeyAccessListUndefined = res.screens.contextlist.AccessListUndefinedScrKeyContextOperResults = res.screens.contextlist.ContextOperResultsScrKeyConfigPDSN = res.screens.pdsn.PDSNServiceScrKeyShowPDSN = res.screens.pdsn.PDSNServiceScrKeySPIBind = res.screens.pdsn.PDSNServiceScrKeyAddService = res.screens.pdsn.PDSNServiceScrKeyPDSNClosedRP = res.screens.pdsn.SPdsnClosedRPScrKeyPDSNClosedRPConfig = res.screens.pdsn.SPdsnClosedRPConfigScrKeyShowPcfStatus = res.screens.pdsn.SShowPcfStatusScrKeyUserPref = res.screens.userpreferences.UserPreferencesScrKeyAAATest = res.screens.aaa.SAAATestScrKeyAAARADIUSTest = res.screens.aaa.SRADIUSTestScrKeyAAARADIUSCounter = res.screens.aaa.SRADIUSCounter

Bundle 1	Bundle 2
ScrKeyShowCardDiag = res.screens.csp.SCSPScrKeyCardHardware = res.screens.csp.SCSPScrKeyHardwareInventory = res.screens.csp.SCSPScrKeyHardwareVersion = res.screens.csp.SCSPScrKeyMacAddr = res.screens.csp.SCSPScrKeyMIPFA = res.screens.mip.SMIPScrKeyMIPFASess = res.screens.mip.SMIPScrKeyMIPFAStat = res.screens.mip.SMIPScrKeyMIPHA = res.screens.mip.SMIPScrKeyMIPHASess = res.screens.mip.SMIPScrKeyMIPHAStat = res.screens.mip.SMIPScrKeyAuditFilter = res.screens.audit.SAuditScrKeyAuditDetails = res.screens.audit.SAuditScrKeyCardMapping = res.screens.csp.SCSPScrKeySynch = res.screens.csp.SCSPScrKeyVLANDetails = res.screens.csp.SCSPScrKeySShowAlarm = res.screens.csp.SCSPScrKeyPortUtilization = res.screens.csp.SCSPScrKeyPrint = res.print.SPrintScrKey = res.screens.process.SProcessMonitorScrKeyProcessThreshold = res.screens.process.SProcessMonitorScrKeySAPNConfig = res.screens.apn.SAPNScrKeySAPNStat = res.screens.apn.SAPNScrKeyGTPPConf = res.screens.gtpp.SGTPPScrKeyGTPPStat = res.screens.gtpp.SGTPPScrKeyGTPPTest = res.screens.gtpp.SGTPPScrKeyIPSecMap = res.screens.ipsec.SIPSecScrKeyIsakmp = res.screens.ipsec.SIPSecScrKeyIsakmpSA = res.screens.ipsec.SIPSecScrKeyTransform = res.screens.ipsec.SIPSecScrKeyIPSecSA = res.screens.ipsec.SIPSecScrKeyIPSecStat = res.screens.ipsec.SIPSecScrKeyIPSecResult = res.screens.ipsec.SIPSecScrKeyPDSNClosedRPConfig = res.screens.pdsn.SPdsnClosedRPScrKeySPIOTiming=res.screens.csp.SCSP	ScrKeyAAARADIUSCounterDetails = res.screens.aaa.SRADIUSCounterScrKeyAAARADIUSAuth = res.screens.aaa.SRADIUSAuthScrKeyAAARADIUSAuthConfig = res.screens.aaa.SRADIUSAuthScrKeyAAARADIUSAcct = res.screens.aaa.SRADIUSAcctScrKeyAAAContextConfig = res.screens.aaa.SAAAContextConfigScrKeyModifyContextAAA = res.screens.aaa.SAAAContextConfigScrKeyAAARADIUSResult = res.screens.aaa.SRADIUSResultScrKeyAAAGlobalConfig = res.screens.aaa.SAAAGlobalConfigScrKeyModifyGlobalAAA = res.screens.aaa.SAAAGlobalConfigScrKeyRADIUSClientStatus = res.screens.aaa.SRADIUSClientStatusScrKeyAccessList = res.screens.vpn.AccessListScrKeyAccessListOpr = res.screens.vpn.AccessListScrKeyIPRoute = res.screens.vpn.IPRouteScrKeyIPRouteConf = res.screens.vpn.IPRouteScrKeySGetIntf = res.screens.vpn.IPRouteScrKeyIPPool = res.screens.vpn.IPPoolScrKeyIPPoolConf = res.screens.vpn.IPPoolScrKeyIPInterface = res.screens.vpn.IPInterfaceScrKeyIPInterfaceConf = res.screens.vpn.IPInterfaceScrKeyDNSConf = res.screens.vpn.SDNSConfScrKeyShowResult = res.screens.vpn.ResultCodeScrKeyIPInterfaceStats = res.screens.vpn.SIPInterfaceStatsScrKeyBusyoutRangeConf = res.screens.vpn.SBusyoutRangeConfScrKeyShowIPSP = res.screens.vpn.SShowIPSPScrKeyMonitorProtocols = res.screens.monitor.SMonitorScrKeyMonitorSubscribers = res.screens.monitor.SMonitorScrKeyProtoCriteria = res.screens.monitor.SMonitorFilterScrKeySubsCriteria = res.screens.monitor.SMonitorSubsFilterScrKeyFrontView = res.screens.csp.SIMGViewScrKeyRearView = res.screens.csp.SIMGViewScrKeySysInfo = res.screens.csp.SSysInfoScrKeyCardConfig = res.screens.csp.SCardConfig

Bundle 1	Bundle 2
ScrKeyApplicationServerConfig=res.screens.vmg.SApplicationServerScrKeyAsAppDBConfig=res.screens.vmg.SAsAppDBScrKeyAsAppVimConfig=res.screens.vmg.SAsAppVimScrKeyAsAppChatConfConfig=res.screens.vmg.SAsAppChatConfScrKeyVmgMmsConfig=res.screens.vmg.SVmgMmsScrKeyAsDisConfig=res.screens.vmg.SAsDisScrKeyAsAppPttConfig=res.screens.vmg.SAsAppPttScrKeySTiming=res.screens.csp.SCSPScrKeyMultipleColSort = res.components.table.SMultipleColumnSortScrKeyIMGInfo = res.screens.hwinventory.SIMGInfoScrKeyProxyDns = res.screens.vpn.SProxyDnsScrKeyCscfPeerServer = res.screens.ims.SCscfPeerServerScrKeyCscfPolicy = res.screens.ims.SCscfPolicyScrKeyCscfService = res.screens.ims.SCscfServiceScrKeyCscfSessTemp = res.screens.ims.SCscfSessTempScrKeyCscfRoute = res.screens.ims.SCscfRouteScrKeyCscfACL = res.screens.ims.SCscfAclScrKeyCscfTranslation = res.screens.ims.SCscfTranslationScrKeyClassMap = res.screens.vpn.SClassMapScrKeyPolicyMap = res.screens.vpn.SPolicyMapScrKeyPolicyGroup = res.screens.vpn.SPolicyGroupScrKeyCscfURN = res.screens.ims.SCscfUrnScrKeyOnDemandReportConfig=res.screens.cf.SReportCommon	ScrKeyPortConfig = res.screens.csp.SPortConfigScrKeyModifyPort = res.screens.csp.SModifyPortScrKeyPortInformation = res.screens.csp.SPortInformationScrKeyShowPortCounters = res.screens.csp.SShowPortCountersScrKeySystem = res.screens.csp.SSysInfoScrKeyShowCardDiag = res.screens.csp.SShowCardDiagScrKeyCardHardware = res.screens.csp.SCardHardwareScrKeyHardwareInventory = res.screens.csp.SHardwareInventoryScrKeyHardwareVersion = res.screens.csp.SHardwareVersionScrKeyShowPower = res.screens.csp.SShowPowerScrKeySoftUpgrade = res.screens.softupgrade.SSoftUpgradeScrKeyShowVersion = res.screens.softupgrade.SShowVersionScrKeyOnlinePatchUpgrade = res.screens.softupgrade.SOnlinePatchUpgradeScrKeyFCFileSelection = res.screens.softupgrade.SFileSelectionScrKeyFCFileComparisonResult = res.screens.softupgrade.SFileComparisonResultScrKeyFCRemoteFileBrowser = res.screens.softupgrade.SRemoteFileBrowserScrKeyConfigurationFileEditor = res.screens.softupgrade.SConfigurationFileEditorScrKeyBootConfiguration = res.screens.softupgrade.SBootConfigurationScrKeyMIPFA = res.screens.mip.SMIPFAScrKeyMIPFASess = res.screens.mip.SMIPFASessScrKeyMIPFAStat = res.screens.mip.SMIPFAStatScrKeyMIPHA = res.screens.mip.SMIPHAScrKeyMIPHASess = res.screens.mip.SMIPHASessScrKeyMIPHAStat = res.screens.mip.SMIPHAStatScrKeyMIPFAContext = res.screens.mip.SMIPFAContextScrKeyMIPHAContext = res.screens.mip.SMIPHAContextScrKeySubsConfig = res.screens.subscriber.SubsConfigScrKeyChangePassword = res.screens.useradm.SChangePasswordScrKeyChangePasswordDialog = res.screens.useradm.SChangePasswordDialogScrKeyDefaultSubsConfig = res.screens.subscriber.SDefaultSubsConfigScrKeySysLog = res.screens.logging.SSysLogScrKeySysLogConf = res.screens.logging.SSysLog

Bundle 1	Bundle 2
	ScrKeyLoggingConfig = res.screens.logging.SLoggingConfigScrKeyShowResultDialog = res.screens.logging.SResultDialogScrKeySNMPShow = res.screens.snmp.SSNMPScrKeySNMPConfig = res.screens.snmp.SSNMPConfigScrKeySNMPStatistics = res.screens.snmp.SSNMPStatisticsScrKeyUserSessInfo = res.screens.security.SUserSessInfoScrKeyInstall = res.screens.license.SInstallScrKeyLicense = res.screens.license.SLicenseScrKeyClock = res.screens.clock.SClockScrKeyAudit = res.screens.audit.SAuditScrKeyAuditFilter = res.screens.audit.SAuditFilterScrKeyAuditDetails = res.screens.audit.SAuditDetailsScrKeyBulkStat = res.screens.bulkstatistics.BulkStatsScrKeyBulkStatConf = res.screens.bulkstatistics.BulkStatsScrKeyBulkAnalysis = res.screens.bulkstatistics.performancestatScrKeyGraphScreenBulk = res.screens.bulkstatistics.performancestatScrKeyPerformanceStat = res.screens.bulkstatistics.performancestatScrKeyOrbemClientSession = res.screens.orbem.SOrbemClientSessionScrKeyOrbemConfig = res.screens.orbem.SOrbemConfigScrKeyModifyOrbemConfig = res.screens.orbem.SOrbemConfigScrKeyModifyOrbemClient = res.screens.orbem.SModifyOrbemClientScrKeyUCM = res.screens.ucm.SUCMScrKeyCardMapping = res.screens.csp.SCardMappingsScrKeySysInfoAdv = res.screens.csp.SAdvDataScrKeyHalt = res.screens.csp.SHaltScrKeyMigrate = res.screens.csp.SMigrateScrKeyPriority = res.screens.csp.SPriorityScrKeySynch = res.screens.csp.SSynchScrKeyVLANDetails = res.screens.csp.SVLANDetailsScrKeyMacAddr = res.screens.csp.SPortMacAddrScrKeyPortUtilization = res.screens.csp.SPortUtilizationScrKeyAllMgr = res.screens.session.SessionSubsystemScrKeySessRecovery = res.screens.session.SSessRecoveryScrKeyShowSessionProgress = res.screens.session.SShowSessionProgress

Bundle 1	Bundle 2
	ScrKeySessProgressFilterDlg = res.screens.session.SShowSessionProgressScrKeyGenericRP = res.screens.rp.SGenericRPScrKeyGenericBCMCS = res.screens.bcmcs.SGenericBCMCSScrKeyMulticastSessions = res.screens.bcmcs.SMulticastSessionsScrKeyMulticastSessionFilter = res.screens.bcmcs.SMulticastSessionsFilterDialogScrKeyMulticastSessionsResult = res.screens.bcmcs.SShowMulticastSessionsResultScrKeySShowCpu = res.screens.cpu.SShowCpuScrKeySShowCpuDetails = res.screens.cpu.SShowCpuScrKeySShowTask = res.screens.cpu.SShowTaskScrKeyShowResources = res.screens.cpu.SShowResourcesScrKeyTaskConfig = res.screens.cpu.STaskConfigScrKeyProcessThreshold = res.screens.process.SThresholdScrKeyCOAlarms = res.screens.alarm.SCOAlarmsScrKeyAlarmStatFilters = res.screens.alarm.SAlarmStatFiltersScrKeyAlarmStat = res.screens.alarm.SAlarmStatFiltersScrKeyEventSetFilter = res.screens.alarm.SAlarmFilterScrKeyEventConfig = res.screens.alarm.SAlarmConfigScrKeyEvent = res.screens.alarm.SAlarmViewScrKeyEventDesc = res.screens.alarm.SDescScrKeySShowAlarm = res.screens.alarm.SShowAlarmScrKeyShowAlarmStat = res.screens.alarm.SShowAlarmStatScrKeyNTP = res.screens.system.SNTPScrKeyNetReqPDPCtxtConfig = res.screens.system.SNetReqPDPCtxtConfigScrKeyNetReqPDPCtxtConfigDlg = res.screens.system.SNetReqPDPCtxtConfigScrKeySAPN = res.screens.apn.SAPNScrKeySAPNConfig = res.screens.apn.SAPNConfigScrKeySAPNStat = res.screens.apn.SAPNStatScrKeyDhcpShow = res.screens.dhcp.SDHCPShowScrKeyDhcpConfig = res.screens.dhcp.SDHCPConfigScrKeyDhcpStat = res.screens.dhcp.SDHCPStatScrKeySDHCPStatus = res.screens.dhcp.SDHCPStatusScrKeyDhcpCache = res.screens.dhcp.SDHCPCacheScrKeyDhcpTest = res.screens.dhcp.SDHCPTestScrKeyLAC = res.screens.l2tp.L2tpScrKeyLACConfig = res.screens.l2tp.L2tp

Bundle 1	Bundle 2
	ScrKeySShowL2TP = res.screens.l2tp.L2tpScrKeyLTTPTunnelFull = res.screens.l2tp.L2tpScrKeyLTTPTunnelCntrs = res.screens.l2tp.L2tpScrKeyLTTPTunnelSummary = res.screens.l2tp.L2tpScrKeyLTTPSessionFull = res.screens.l2tp.L2tpScrKeyLTTPSessionCntrs = res.screens.l2tp.L2tpScrKeyLTTPSessionSummary = res.screens.l2tp.L2tpScrKeyLTTPStat = res.screens.l2tp.L2tpScrKeyLNSShow = res.screens.l2tp.SLNSShowScrKeyLNSConfig = res.screens.l2tp.SLNSConfigScrKeyGTPPConf = res.screens.gtpp.SGTPPConfScrKeyGTPPStat = res.screens.gtpp.SGTPPStatScrKeyGTPPTest = res.screens.gtpp.SGTPPTestScrKeyGSNConf = res.screens.gtpp.SGSNScrKeyGTPPInterimNow = res.screens.gtpp.SGTPPInterimNowScrKeyShowGTPPCounters = res.screens.gtpp.SShowGTPPCountersScrKeyGTPPStorageSrvStat = res.screens.gtpp.SGTPPStorageServerStatisticsScrKeyGGSNService = res.screens.ggsn.SGGSNServiceScrKeyGGSNServiceInfo = res.screens.ggsn.SGGSNServiceInfoScrKeyGGSNServiceConfig = res.screens.ggsn.SGGSNServiceConfigScrKeyGTPCStat = res.screens.gtpc.SGTPCStatisticsScrKeyGTPCTest = res.screens.gtpc.SGTPCTestScrKeyIPSecMap = res.screens.ipsec.SIPSecMapScrKeyIsakmp = res.screens.ipsec.SIsakmpScrKeyIsakmpSA = res.screens.ipsec.SIsakmpSAScrKeyTransform = res.screens.ipsec.STransformScrKeyIPSecSA = res.screens.ipsec.SIPSecSAScrKeyIPSecStat = res.screens.ipsec.SIPSecStatScrKeyPeriodicSaveBoxerCfg = res.screens.configbackup.SPeriodicSaveBoxerCfgScrKeyIPRIPConfig = res.screens.rip.SIPRIPConfigScrKeyIPRIPConfigDlg = res.screens.rip.SIPRIPConfigScrKeyShowRouterRIPConfig = res.screens.rip.SRouterRIPConfigScrKeyModifyRouterRIPConfig = res.screens.rip.SRouterRIPConfigScrKeyKeyChainConfig = res.screens.rip.SKeyChainConfigurationScrKeyAddKeyChain = res.screens.rip.SKeyChainConfiguration

Bundle 1	Bundle 2
	ScrKeyModifyKeyChainConfig = res.screens.rip.SModifyKeyChainConfigScrKeyExternalInlineServer = res.screens.vpn.SExternalInlineServerScrKeyIPPoolDefConfig = res.screens.vpn.SIPPoolDefaultConfigScrKeyAddBusyoutRangeConf = res.screens.vpn.SAddBusyoutRangeConfScrKeySFetchNonLocalInfo= res.globalcommon.FetchNonLocalInfoScrKeySThreshShow = res.screens.threshold.SThreshShowScrKeyThreshConfig = res.screens.threshold.SThreshConfigScrKeySCongestionControl = res.screens.threshold.SCongestionControlScrKeyCongestionControlStat = res.screens.threshold.SCongestionControlStatScrKeyShowNRPC = res.screens.system.SShowNRPCScrKeyNewCallPolicy = res.screens.system.SNewCallPolicyScrKeySBannerDisplay = res.screens.system.SBannerDisplayScrKeyShowSessionDuration = res.screens.session.SShowSessionDurationScrKeySessDurationFilterDlg = res.screens.session.SShowSessionDurationScrKeySessionDisconnectStatistics = res.screens.session.SessionDisconnectStatisticsScrKeySessionSetuptimeStat = res.screens.session.SSessionSetuptimeStatScrKeyPortMonitor = res.screens.portmonitor.SPortMonitorScrKeyNetworkReachability = res.screens.nr.SNetworkReachabilityScrKeyNrConfig = res.screens.nr.SNrConfigScrKeySShowVMGAll = res.screens.vmg.SShowVMGAllScrKeySShowVMGInterfaces = res.screens.vmg.SShowVMGInterfacesScrKeySShowVMGGCPStat = res.screens.vmg.SShowVMGGCPStatScrKeyVMGgpdsps = res.screens.vmg.SVMGgpdspsScrKeyGTPCInfo = res.screens.gtpc.SGTPCInfoScrKeyGTPCCounters = res.screens.gtpc.SGTPCCountersScrKeyGTPCSummary = res.screens.gtpc.SGTPCSummaryScrKeyGTPCSession = res.screens.gtpc.SGTPCSession

Bundle 1	Bundle 2
	ScrKeyAlarmScheduler = res.screens.alarm.SAlarmSchedulerScrIDGraphConfig = res.graphs.SGraphConfigScrKeyGraphFilter = res.graphs.SGraphFilterScrKeyGraphScreen = res.graphs.SGraphScreenScrKeyIPPoolDetail = res.screens.vpn.IPPoolScrKeyIMGFileBrowser = res.screens.softupgrade.SIMGFileBrowserScrKeyShowGTPPStorageServerCounters = res.screens.gtpp.SSCounterDialogScrKeyOSPFExceptionHandler = res.screens.ospf.SOSPFExceptionHandlerScrKeyShowOSPFInformation = res.screens.ospf.SShowOSPFInformationScrKeyShowOSPFInterface = res.screens.ospf.SShowOSPFInterfaceScrKeyShowOSPFNeighbor = res.screens.ospf.SShowOSPFNeighborScrKeyOSPFConfiguration = res.screens.ospf.SOSPFConfigurationScrKeyModifyOSPFConfiguration = res.screens.ospf.SModifyOSPFConfigurationScrKeySDHCPExcpHandler = res.screens.dhcp.SDHCPExcpHandlerScrKeySDHCPServiceConfig = res.screens.dhcp.SDHCPServiceConfigScrKeySDHCPDetails = res.screens.dhcp.SDHCPDetailsScrKeySDHCPShowConfig = res.screens.dhcp.SDHCPShowConfigScrKeyUDR = res.screens.cdr.SCDRScrKeyUDRConfig = res.screens.cdr.SCDRConfigScrKeyShowOSPFBorderRouters = res.screens.ospf.SShowOSPFBorderRoutersScrKeyShowOSPFRoute = res.screens.ospf.SShowOSPFRouteScrKeyShowOSPFDatabase = res.screens.ospf.SShowOSPFDatabaseScrKeyShowOSPFDebugging = res.screens.ospf.SShowOSPFDebuggingScrKeySPIOTiming=res.screens.csp.SSPIOTimingScrKeyQosNpuStats=res.screens.npu.SQosNpuStatsScrKeyShowQoSNPUTrafficBanwidth = res.screens.npu.SShowQoSNPUTrafficBandwidthScrKeySQosnpuConfig = res.screens.npu.SQosnpuConfigScrKeyIPOSPFInterface = res.screens.ospf.SIPOSPFInterface

Bundle 1	Bundle 2
	ScrKeyModifyIPOSPFInterface = res.screens.ospf.SModifyIPOSPFInterfaceScrKeySDHCPStatistics = res.screens.dhcp.SDHCPStatisticsScrKeyModifyOSPFDebugging = res.screens.ospf.SModifyOSPFDebuggingScrKeyOSPFAreaConfiguration = res.screens.ospf.SOSPFAreaConfigurationScrKeyVirtualLinks = res.screens.ospf.SVirtualLinksScrKeyModifyOSPFAreaConfiguration = res.screens.ospf.SModifyOSPFAreaConfigurationScrKeyBoundPortCounters = res.screens.csp.SBoundPortCountersScrKeyIsakmpKeepAlive = res.screens.ipsec.SIsakmpKeepAliveScrKeyCryptoGroupConfig = res.screens.ipsec.SCryptoGroupConfigScrKeyCryptoGroup = res.screens.ipsec.SShowCryptoGroupScrKeyModifySchema = res.screens.bulkstatistics.SModifySchemaScrKeyShowOSPFNeighborDetail = res.screens.ospf.SShowOSPFNeighborDetailScrKeySDHCPInfo = res.screens.dhcp.SDHCPInfoScrKeyModifyFileSystem = res.screens.softupgrade.SModifyFileSystemScrKeyChargingService = res.screens.chargingservice.SChargingServiceScrKeyModifyChargingServiceConfig = res.screens.chargingservice.SChargingServiceScrKeyCSService = res.screens.css.SCSServiceScrKeyCSServiceConfig =res.screens.css.SAddCSServiceScrKeyCSSServer =res.screens.css.SCSSServerScrKeyCSSServerConfig=res.screens.css.SCSSServerConfigScrKeyCSSDelSeq =res.screens.css.SCSSDeliverySequenceScrKeyCSSDelSeqConfig =res.screens.css.SCSSDeliverySequenceConfigScrKeySGlobalConfiguration =res.screens.chargingservice.SGlobalConfigurationScrKeySCSDetails=res.screens.chargingservice.SCSDetailsScrKeyChargingServiceFlows=res.screens.chargingservice.SChargingServiceFlowsScrKeyChargingServiceSessions = res.screens.chargingservice.SChargingServiceSessions

Bundle 1	Bundle 2
	ScrKeyChargingServiceManagerStats = res.screens.chargingservice.SChargingServiceManagerStatsScrKeyIPAccessGroupStatistics=res.screens.vpn.SIPAccessGroupStatisticsScrKeyCommonClass=res.utils.SCommonClassScrKeySDataHandler=res.utils.SDataHandlerScrKeyAAARADIUSCharging = res.screens.aaa.SRADIUSChargingScrKeyAAARADIUSChargingConfig = res.screens.aaa.SRADIUSChargingScrKeyEDR = res.screens.cdr.SEDRScrKeyEDRConfig = res.screens.cdr.SEDRConfigScrKeyShowASInfo=res.screens.vmg.SShowASInfoScrKeyAsSigRoute=res.screens.vmg.SAsSigRouteScrKeyAsSigRouteConfig=res.screens.vmg.SAsSigRouteConfigScrKeyAsSigSIP=res.screens.vmg.SAsSigSIPScrKeyAsSigSIPConfig=res.screens.vmg.SAsSigSIPConfigScrKeyApplicationServer = res.screens.vmg.SApplicationServerScrKeyApplicationServerConfig = res.screens.vmg.SApplicationServerConfigScrKeyAsAppDB = res.screens.vmg.SAsAppDBScrKeyAsAppDBConfig = res.screens.vmg.SAsAppDBConfigScrKeyAsAppVim = res.screens.vmg.SAsAppVimScrKeyAsAppVimConfig=res.screens.vmg.SAsAppVimConfigScrKeyAsAppChatConf = res.screens.vmg.SAsAppChatConfScrKeyAsAppChatConfConfig=res.screens.vmg.SAsAppChatConfConfigScrKeySShowVMGPacketizers=res.screens.vmg.SShowVMGPacketizersScrKeyAsChatConfTable=res.screens.vmg.SAsChatConfTableScrKeyAsChatConfTableConfig=res.screens.vmg.SAsChatConfTableConfigScrKeyVMGCall=res.screens.vmg.SShowVMGCallScrKeySShowVMGConnections=res.screens.vmg.SShowVMGConnectionsScrKeyVMG=res.screens.vmg.SVMGScrKeyVMGConfig=res.screens.vmg.SVMGConfigScrKeySShowASAnnouncements=res.screens.vmg.SShowASAnnouncementsScrKeyVMGgpdsps= res.screens.vmg.SVMGgpdsps

Bundle 1	Bundle 2
	ScrKeyVMGVop = res.screens.vmg.SVMGVopScrKeyVMGVopConfig = res.screens.vmg.SVMGVopConfigScrKeyVmgMms = res.screens.vmg.SVmgMmsScrKeyVmgMmsConfig=res.screens.vmg.SVmgMmsConfigScrKeyVMGres=res.screens.vmg.SVMGresScrKeyVMGGcp = res.screens.vmg.SVMGGcpScrKeyVMGGcpConfig = res.screens.vmg.SVMGGcpConfigScrKeyPrepaid3GPP2Statistics = res.screens.session.SPrepaid3GPP2StatisticsScrKeyRemoteServerList = res.screens.vpn.SRemoteServerListScrKeyConfigRemoteServerList = res.screens.vpn.SConfigRemoteServerListScrKeyAsDis = res.screens.vmg.SAsDisScrKeyAsDisConfig=res.screens.vmg.SAsDisConfigScrKeyShowAsConf=res.screens.vmg.SShowAsConfScrKeyAsAppPtt = res.screens.vmg.SAsAppPttScrKeyAsAppPttConfig=res.screens.vmg.SAsAppPttConfigScrKeyVMGchannel=res.screens.vmg.SVMGchannelScrKeyAsAppVinfo = res.screens.vmg.SAsAppVinfoScrKeyAsAppVinfoConfig=res.screens.vmg.SAsAppVinfoConfigScrKeyIpv4DnsProxy=res.screens.vpn.SDNSProxyCfgScrKeyORBStats=res.screens.security.SORBStatisticsScrKeyDeleteChargingService = res.screens.chargingservice.SChargingServiceScrKeyChargingServiceOprResult = res.screens.chargingservice.SChargingServiceScrKeySTiming= res.screens.vmg.STimingScrKeyDomainConfig=res.screens.contextlist.SDomainConfigScrKeySessionCounters=res.screens.session.SShowSessionCountersScrKeySROHCStatistics=res.screens.ppp.SROHCStatisticsScrKeyIPPolicyForward=res.screens.vpn.SIPPolicyForwardScrKeyModifyIPPolicyForward=res.screens.vpn.SModifyIPPolicyForwardScrKeyMIPIPAssignment=res.screens.mip.SMIPIPAssignmentScrKeyMIPIPAssignmentConfig=res.screens.mip.SMIPIPAssignmentConfigScrKeyEnforceImsi = res.screens.system.SEnforceImsi

Bundle 1	Bundle 2
	ScrKeyIPv6Pool = res.screens.ipv6.SIPv6PoolScrKeyIPv6PoolConf = res.screens.ipv6.SIPv6PoolConfScrKeyIPv6PoolDetail = res.screens.ipv6.SIPv6PoolDetailScrKeyIPv6ShowResult = res.screens.ipv6.SShowResultScrKeySRPConfiguration = res.screens.srp.SSRPConfigurationScrKeyModifySRPConfiguration = res.screens.srp.SModifySRPConfigurationScrKeySRPStatistics = res.screens.srp.SSRPStatisticsScrKeySRPCheckPointInfo = res.screens.srp.SSRPCheckPointInfoScrKeySRPInfo = res.screens.srp.SSRPInfoScrKeySRPMonitorInformation = res.screens.srp.SSRPMonitorInformationScrKeySupportDetails = res.screens.system.SShowSupportDetailsScrKeyBatchJobs = res.screens.monitor.SBatchJobsScrKeyShowBGP = res.screens.bgp.ShowBGPScrKeyShowBGPDebugging = res.screens.bgp.ShowBGPDebuggingScrKeyShowBGPNeighbor = res.screens.bgp.ShowBGPNeighborScrKeyShowBGPSummary = res.screens.bgp.ShowBGPSummaryScrKeyConfigUpdateScheduler = res.screens.configupdate.SConfigSchedulerScrKeyScheduledConfigUpdate = res.screens.configupdate.SScheduledConfigScrKeyConfigUpdateFilter = res.screens.configupdate.SFilterScreenScrKeyFileTransfer = res.screens.configupdate.SFileTransferScrKeyBGPConfiguration = res.screens.bgp.SBGPConfigurationScrKeyModifyBGPConfiguration = res.screens.bgp.SModifyBGPConfigurationScrKeyClearIPBGPPeer = res.screens.bgp.SClearIPBGPPeerScrKeyAsPathAccessList = res.screens.bgp.AsPathAccessListScrKeyRouteMapConfiguration = res.screens.bgp.SRouteMapConfigurationScrKeyAddModifyRouteMapConfiguration = res.screens.bgp.SAddModifyRouteMapConfigurationScrKeySConfigCriteria = res.screens.showconfig.SConfigCriteriaScrKeySViewConfig = res.screens.showconfig.SViewConfig

Bundle 1	Bundle 2
	ScrKeyShowSystemInfo = res.screens.system.SShowSystemInfoScrKeySearchIPPoolNames = res.screens.vpn.SSearchIPPoolNamesScrKeyAppConfig = res.topology.SApplicationConfigurationScrKeySCrashList = res.screens.crashlist.SCrashListScrKeySCrashInfo = res.screens.crashlist.SCrashInfoScrKeyAddressHoldTimerInformation = res.screens.vpn.SAddressHoldTimerInformationScrKeyPoolAddressInformation = res.screens.vpn.SPoolAddressInformationScrKeySShowSigSipDns = res.screens.vmg.SShowSigSipDnsScrKeyAcsAnalyzerStatistics = res.screens.acs.SAcsAnalyzerStatisticsScrKeyShowAcsSessions = res.screens.acs.ShowAcsSessionsScrKeyShowAcsSessionsFilter = res.screens.acs.ShowAcsSessionsFilterScrKeyShowAcsFlows = res.screens.acs.ShowAcsFlowsScrKeyAcsFlowsFliter = res.screens.acs.ShowAcsFlowsFilterScrKeyShowAcsSubsystem = res.screens.acs.ShowAcsSubsystemScrKeyAsAppVimProfile = res.screens.vmg.SAsAppVimProfileScrKeyAsAppVimProfileConfig = res.screens.vmg.SAsAppVimProfileConfigScrKeyAcsCommonClass=res.screens.acs.SAcsCommonClassScrKeyAcsConf=res.screens.acs.SAcsConfScrKeyAcsOperResults=res.screens.acs.SAcsOperResultsScrKeyAcsCFPolicyConfig=res.screens.acs.SAcsCFPolicyConfigScrKeyAcsRulebaseConfig=res.screens.acs.SAcsRuleBaseConfigScrKeyAcsRuledefConfig=res.screens.acs.SAcsRuleDefConfigScrKeyACS = res.screens.acs.SACSScrKeyACSDetails = res.screens.acs.SACSDetailsScrKeyACSGeneralConfig = res.screens.acs.SACSGeneralConfigScrKeyACSChargingActionConfig = res.screens.acs.SACSChargingActionConfigScrKeyACSEDRConfig = res.screens.acs.SACSEDRConfig

Bundle 1	Bundle 2
	ScrKeyACSUDRConfig = res.screens.acs.SACSUDRConfigScrKeyConfirmAttributeDelete = res.screens.acs.SACSEDRConfigScrKeyShowDiameterRoute = res.screens.acs.SShowDiameterRouteScrKeyDHCPTest = res.screens.dhcp.SDHCPTestScrKeyAcsChargingActionStats = res.screens.acs.SAcsChargingActionStatsScrKeyAcsRulebaseStats = res.screens.acs.SAcsRulebaseStatsScrKeyAcsRuledefStats = res.screens.acs.SAcsRuledefStatsScrKeyGTPPStorageServerStatus = res.screens.gtpp.SShowGTPPStorageServerStatusScrKeyHardwareAudit = res.screens.hwinventory.SHardwareAuditScrKeyAddComment = res.screens.hwinventory.SAddCommentScrKeyHardwareFilter = res.screens.hwinventory.SHardwareFilterScrKeyHardwareDetails = res.screens.hwinventory.SHardwareDetailsScrKeyAcsDccaStats = res.screens.acs.SAcsDccaStatsScrKeyAcsDccaConfig = res.screens.acs.SAcsDccaConfigScrKeyRouteMapEntryDetails = res.screens.bgp.SRouteMapEntryDetailsScrKeyDiameter = res.screens.acs.SDiameterScrKeyDiameterConfig = res.screens.acs.SDiameterConfigScrKeyIMGInfo = res.screens.hwinventory.SIMGInfoScrKeyDiameterPeers = res.screens.acs.SDiameterPeersScrKeyDiameterEndpoint = res.screens.acs.SDiameterEndpointScrKeyDiameterStats = res.screens.acs.SDiameterStatsScrKeyProxyDns = res.screens.vpn.SProxyDnsScrKeySelectCounters = res.screens.bulkstatistics.SSelectCountersScrKeySROHCProfile = res.screens.rohc.SROHCProfileScrKeyPeriodicBackup = res.screens.periodicbackup.SPeriodicBackupScrKeyBackupHistory = res.screens.periodicbackup.SBackupHistoryScrKeyFilterScreen = res.screens.periodicbackup.SFilterScreenScrKeyShowRsvpStatistics = res.screens.rsvp.ShowRsvpStatistics

Bundle 1	Bundle 2
	ScrKeyShowRsvpCounters = res.screens.rsvp.ShowRsvpCountersScrKeyAlarmInformation = res.screens.alarm.AlarmInformationScrKeyRouteAccessList = res.screens.vpn.RouteAccessListxListScrKeyTrapForwarding = res.screens.alarm.TrapForwardingScrKeySMIPFAHAStatus = res.screens.mip.SMIPFAHAStatusScrKeyIPPrefixList = res.screens.vpn.IPPrefixListScrKeyOfflineUpgrade = res.screens.softupgrade.SOfflineUpgradeScrKeyClassMap = res.screens.vpn.SClassMapScrKeyPolicyMap = res.screens.vpn.SPolicyMapScrKeyPolicyGroup = res.screens.vpn.SPolicyGroupScrKeyIpRoutingMaxPath = res.screens.vpn.IPRoutingMaxPathScrKeyAccessFlowStatistics = res.screens.subscriber.AccessFlowStatisticsScrKeySAcsCreditControlSessionStates = res.screens.acs.SAcsCreditControlSessionStatesScrKeyCscfPeerServer = res.screens.ims.SCscfPeerServerScrKeyCscfPolicy = res.screens.ims.SCscfPolicyScrKeyCscfService = res.screens.ims.SCscfServiceScrKeyCscfSessTemp = res.screens.ims.SCscfSessTempScrKeyCscfRoute = res.screens.ims.SCscfRouteScrKeyCscfACL = res.screens.ims.SCscfAclScrKeyCscfTranslation = res.screens.ims.SCscfTranslationScrKeySendBroadcastMessage = res.screens.security.SBroadcastMessageScrKeySendBroadcastMessageAlert = res.screens.security.SBroadcastMessageScrKeySProtocolConfig = res.screens.p2p.SProtocolConfigScrKeySProtocolAnalysis = res.screens.p2p.SProtocolAnalysisScrKeySP2PGraphView = res.screens.p2p.SP2PGraphViewScrKeySP2PTabularView = res.screens.p2p.SP2PGraphViewScrKeyCscfURN = res.screens.ims.SCscfUrnScrKeySyslog = res.screens.syslog.SSyslogScrKeySyslogConfig = res.screens.syslog.SSyslogConfigScrKeyShowMsg = res.screens.syslog.SShowMsg

Bundle 1	Bundle 2
	ScrKeyShowSyslogConf = res.screens.syslog.SShowSyslogConfScrKeyShowSgsnTable = res.screens.ggsn.SGGSNServiceSgsnTableScrKeyShowOspfVirtualLinks=res.screens.ospf.SShowOSPFVirtualLinksScrKeySShowFirewallStatistics = res.screens.firewall.SShowFirewallStatisticsScrKeySRADIUSCounterSummary=res.screens.aaa.SRADIUSCounterSummaryScrKeyOnDemandReportConfig=res.screens.cf.SOnDemandReportConfigScrKeySearchFilter=res.screens.cf.SSearchFilterScrKeyViewStatusReportConfig=res.screens.cf.SViewReportStatusScrKeyReportDetails=res.screens.cf.SReportDetailsScrKeySSGSNMAPStats=res.screens.sgsn.SSGSNMAPStatsScrKeySSGTPUStats=res.screens.sgsn.SSGTPUStatsScrKeySSGTPCStats=res.screens.sgsn.SSGTPCStatsScrKeySSGSNOprPolicy=res.screens.sgsn.SSGSNOprPolicyScrKeySSGSNOprPolicyDetail=res.screens.sgsn.SSGSNOprPolicyScrKeySACSCFCateStatView=res.screens.acs.SACSCFCateStatView.javaScrKeySCFStatistics=res.screens.cf.SCFStatisticsScrKeySCFCategoryDb=res.screens.cf.SCFCategoryDbViewScrKeySSCCPStats=res.screens.sgsn.SSCCPStats

The temip.cfg File

This configuration file is for a flat-file based interface between WEM and TEMIP.

Important: This configuration file is customer-specific and is not operational without the appropriate license. Please contact your local sales representative for additional information.

The thr.cfg File

This file contains parameters pertaining to the WEM thread pool.

Caution: To ensure proper operation of the WEM, do not edit the parameters in these files.

Table 51. thr.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
THREAD: This is the configuration file for Thread pool.				
PoolEnable	Flag for enable or disable the thread pool. • Needs a WEM Server restart • Can be changed by the user Values: • 1 - Thread pool enable • 0 - Thread pool disable	0	1	0
Size	Size of the thread pool. • Needs a WEM Server restart • Can be changed by the user	10	100	10
MaxSize	Maximum size of the thread pool. • Needs a WEM Server restart • Can be changed by the user	10	100	100

The ua.cfg File

This file contains parameters pertaining to the WEM support for the ANSI T1.276 security specification. These include parameters granting and restricting access, login failures, password aging, and password complexity.

Important: Any change in the configuration files will restart the server resulting in client restart.

Table 52. ua.cfg File Parameters

Key	Description	Minimum Value	Maximum Value	Default Value
Security: This file contains the list of security parameters for user access to WEM.				
AllowIpAddress	List of allowed IP addresses and mask. • Needs a WEM Server restart • Can be changed by the user IP address 0.0.0.0: Allows all addresses Format: Allow IP address/subnet-mask number, IP address/subnet-mask number...Nothing: Allow nothing	--	--	--
DenyIpAddress	List of deny IP addresses and mask. • Needs a WEM Server restart • Can be changed by the user IP address 0.0.0.0: Deny all Addresses Format: Deny IP address/subnet-mask number, IP address/subnet-mask number...Nothing in list: Deny nothing	--	--	--
ConsecutiveFailLogin	The system limit on consecutive failed login for a given user ID shall be configurable. • Needs a WEM Server restart • Can be changed by the user Value 0: No limit	0	10	5

Key	Description	Minimum Value	Maximum Value	Default Value
LockOutInterval	Locked out login ID, automatically, following the crossing of a configurable timeframe. Value is in minutes. • Needs a WEM Server restart • Can be changed by the user Value 0: No lock out	0	1440	60
AlertExpiryThreshold	The account alert expiry threshold after WEM generates an alert. Value is in days. • Needs a WEM Server restart • Can be changed by the user Value 0: No alert	0	30	10
MinPasswordChangeInterval	Passwords will be user changeable at the user's discretion following a configurable minimum interval since the last change. Value is in seconds. • Needs a WEM Server restart • Can be changed by the user Value 0: No interval	0	86400	86400
NumOfPasswordInHistory	System will support a password history to prevent password reuse. The parameters will be configurable with a default of at least the past five password iterations. • Needs a WEM Server restart • Can be changed by the user Value 0: No password history	0	10	5
PasswordInHistoryAtLeast	System will support a password history to prevent password reuse. The parameters will be configurable with a default of at least the past 180 days. • Needs a WEM Server restart • Can be changed by the user Value 0: No expiry	0	365	180

Key	Description	Minimum Value	Maximum Value	Default Value
EMSAdminMailId	E-mail address of the WEM account created/reset password notification originator. • Needs a WEM Server restart • Can be changed by the user	--	--	No default value
PasswordComplexityRules	This flag indicates which rules should be used to verify password complexity. • Needs a WEM Server restart • Can be changed by the user Possible values: • 0: None • 1: ANSI	--	--	1
PasswordMinLength	This flag sets the minimum length of a user-defined password. • Needs a WEM Server restart • Can be changed by the user	PasswordComplexityRules = None		
		1	63	8
		PasswordComplexityRules = ANSI		
		3	63	8
PasswordMinCharChange	This flag defines the minimum number of characters that must be changed when a user changes the password. • Needs a WEM Server restart • Can be changed by the user	If PasswordComplexityRules is None, then do not check this. (Value is 0)		
		PasswordComplexityRules = ANSI		
		0	8	2

Key	Description	Minimum Value	Maximum Value	Default Value
ChangePasswordOnNextLogin	If this flag enabled then, on next login, the user will be required to change the password. Else, the user will not be required to change the password. • Needs a WEM Server restart • Can be changed by the user Possible values: • 0: Password change will not be required • 1: Password change will be required	--	--	1

The vacuum.cfg File

This file contains parameters pertaining to PostgreSQL database vacuuming.

Configuring values for CompleteDB:

- If this value is 0, it means that vacuuming needs to be done on all the tables individually.
- If this value is 1, it means that vacuuming is done only to the database and not the tables individually.

Table 53. vacuum.cfg File Parameters

<table>
<tr><th>Key</th><th>Description and Values</th></tr>
<tr><td colspan="2">Type: This section describes the type of vacuum to be done on database.</td></tr>
<tr><td>VACUUM</td><td>This parameter reclaims space and makes it available for re-use. This command can operate in parallel with normal reading and writing of the table, as an exclusive lock is not obtained. This is the default value.</td></tr>
<tr><td>VACUUM ANALYZE</td><td>This parameter performs a VACUUM and then an ANALYZE for each selected table.</td></tr>
<tr><td>VACUUM FULL</td><td>This parameter physically reorders the tables. This requires an exclusive lock on each table while it is being processed.
Important: VACUUM FULL is not recommended for routine use.</td></tr>
<tr><td colspan="2">Database</td></tr>
<tr><td>Database Name = hh,hh</td><td>First "hh" specifies the starting time to vacuum the database or table
Second "hh" specifies the time interval for performing periodic vacuum after the starting time.
Default value for database: 12,12Default value for table: 00, 00. This means that do not vacuum the database or table. It means midnight 12 as we have a separate value for the same, that is, 24.
Any non-zero value for this will override the CompleteDB flag for this database. For example, if the ConfigDB value is 13 and CompleteDB value for ConfigDB is 0, means that the entire DB will be vacuumed along with all the tables. However, if the timestamp of start of vacuum for the DB and any of the tables conflicts, then, vacuum will not be started for that table, and the DB will get precedence in this case.
Max value: 24,24 (24 is same as 12:00 AM)
Important: It is not recommended to start table level vacuuming for all tables at the same time as it will increase number of transactions to the database. Database level vacuuming takes care of table level vacuuming, that means it vacuums whole database including all the tables present in that database so at critical point if we want to start vacuuming on all tables at the same time, at that point, we can start only database level vacuum. If we want to vacuum one or more (but not all) tables from the database, in that case we can use table level vacuuming by enabling vacuum for that tables.
<table>
<tr><th>ConfigDB</th><th>TrapDB</th><th>AuditDB</th><th>BulkDB</th><th>P2PDB</th></tr>
<tr><td>12, 12</td><td>12, 12</td><td>12, 12</td><td>12, 12</td><td>12, 12</td></tr>
</table>
</td></tr>
</table>

Key	Description and Values				
Table Name = hh,hh	**ConfigDB**	**TrapDB**	**AuditDB**	**BulkDB**	**P2PDB**
	CompleteDB= 1boxer = 00,00portmontable = 00,00boxeruserinfo = 00,00userpreference = 00,00processthreshold = 00,00ippooldefaults = 00,00scbrdefaults = 00,00csmsessioninfo = 00,00bkinfo = 00, 00graphscreeninfo = 00,00batchjobcleanup = 00,00batchjobinfo = 00,00boxeronmap = 00,00dbbackupinfo = 00,00maptable = 00,00p2pinfo = 00,00updateinfo = 00,00userinfo = 00,00dbcurrent = 00,00hostname = 00,00syslogkeywordlist = 00,00syslogmsgfileinfo = 00,00	CompleteDB= 1trap = 00,00deletedtrap = 00,00forwardinginfo = 00,00forwardpurgeinfo = 00,00mailinfo = 00,00mailmessage = 00,00configure = 00,00schedule = 00,00forwardaddress = 00,00pendingtrap = 00,00trap_current = 00,00trapoperdetails = 00,00	CompleteDB= 1auditlog = 00,00auditlog_current = 00,00chassisinfo = 00,00cpuinfo = 00,00daughtercardinfo = 00,00hardwareactivity = 00,00hardwareinfo = 00,00lcrccspioinfo = 00,00pactacinfo = 00,00rowcount = 00,00smcinfo = 00,00spccardinfo = 00,00imglastevtgentime = 00,00	CompleteDB= 1card = 00,00card_current = 00,00port = 00,00port_current = 00,00system = 00,00system_current = 00,00ppp = 00,00ppp_current = 00,00mipfa = 00,00mipfa_current = 00,00mipha = 00,00mipha_current = 00,00rp = 00,00rp_current = 00,00gtpc = 00,00gtpc_current = 00,00gtpp = 00,00gtpp_current = 00,00ippool = 00,00ippool_current = 00,00apn = 00,00apn_current = 00,00lac = 00,00lac_current = 00,00closedrp = 00,00closedrp_current = 00,00	CompleteDB= 1bwstat = 00,00bwstat_current = 00,00dailystat = 00,00dailystat_current = 00,00hourlystat = 00,00hourlystat_current = 00,00protocolstat = 00,00protocolstat_current = 00,00scbrdailystats = 00,00scbrdailystats_current = 00,00scbrhourlystats = 00,00scbrhourlystats_current = 00,00scbrstats = 00,00scbrstats_current = 00,00tempp2p = 00,00thresholdstats = 00,00

Key	Description and Values				
				radius = 00,00radius_current = 00,00imgaccess = 00,00ecs = 00,00ecs_current = 00,00misc = 00,00misc_current = 00,00ipsg = 00,00ipsg_current = 00,00asngw = 00,00asngw_current = 00,00sgsn = 00,00sgsn_current = 00,00sgtp = 00,00sgtp_current = 00,00sccp = 00,00sccp_current = 00,00ss7rd = 00,00ss7rd_current = 00,00mipv6ha = 00,00mipv6ha_current = 00,00context = 00,00context_current = 00,00cscf = 00,00cscf_current = 00,00ss7link = 00,00ss7link_current = 00,00gprs = 00,00gprs_current = 00,00	

The wblist.cfg File

This file provides information on the white black list database file paths that are mainly used for content filtering.

Table 54. wblist.cfg File Parameters

Key	Description
WBLIST: This section describes the parameters that store Content Filtering Server information.	
WblistPath	White Black list file path: This specifies the path where white black list database files are located. WblistPath = *./flash/cf/cfdatabases/wblistdb/*

The menu.xml File

This xml file allows the Admin to set a flag to hide and unhide menu options in the WEM GUI

Table 55. menu.cfg File Parameters

File Path	**<***WEM installed dir***>/client/<***version dir***>/menu.xml**
The following instructions describe how to set the flag to hide and unhide menu options in the WEM GUI. After making the change, close the browser and reopen it to see the change in the GUI.	
Set Visible Y/N	The following example shows how to change the setting from Not Visible to Visible for GGSN. GGSN is a Parent and in the following change the flag from "N" to "Y": *<menu menuID="MID_CFG_GGSN" parentMenu="Configuration" menuName="GGSN" visible="N" />* Any Parent sub-menus that need to be hidden/unhidden also need to have the flag set appropriately. For example, to show the APN sub-menu in the topology: *<menu menuID="MID_CFG_APN" parentMenu="GGSN" menuName="APN" visible="Y">*

Appendix D
XML Output Formats

This appendix provides information about the various eXtensible Markup Language (XML) file format definitions in the Bulkstat server. The XML file format definition is based on XML schema. The 3GPP standards are followed to generate XML report files in the XML report generator. These defined file format definitions correspond to each other (except for some minor XML specific optimizations).

This chapter includes the following topics:

Important: Unless otherwise specified, all information in this chapter applies to both Sun Solaris- and Red Hat Enterprise Linux-based WEM systems.

Supported XML Output Formats

The following XML output formats are supported:

- **DTD Based Format:** This format is DTD based and it can be enabled/disabled using the configurable parameter, 'XMLFileFormat' provided in the configuration file *bsserver.cfg* in the */<ems_dir>/etc* directory.
- **3GPP Format:** This is the new and default 3GPP recommended format to generate the XML report file. This format reduces the XML file size.

WEM generates two types of files for the above two formats. These are individual XML files for all subsystems and single XML file for all subsystems which can be configured using the parameter 'XMLFileType' in the *bsserver.cfg* file.

Refer *Appendix B* for information on the configurable parameters in the *bsserver.cfg* file.

Examples of XML Output Formats

This section provides the sample outputs for the DTD based and 3GPP XML formats.

DTD Based Format

This following output is an example of individual files for all subsystems in DTD based XML format.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!DOCTYPE mdc SYSTEM "MeasurementStat.dtd">
<?xml-stylesheet type="text/xsl" href="simple_table.xsl" ?>
<mdc>
 <mfh>
 <ffv>2</ffv>
 <sn>Starent Network Inc.</sn>
 <st>MSC</st>
 <vn>Samsung corp.</vn>
 <cbt>2006-01-03 13:10:00</cbt>
 </mfh>
<md>
 <neid>
 <neun></neun>
 <nedn></nedn>
 <nesw></nesw>
 </neid>
 <mi>
 <mts>2006-01-03 13:15:00</mts>
 <gp>300</gp>
 <rsf>false</rsf>
 <ms>
```

```
<msn>CardStat</msn>
<sf>false</sf>
<es>false</es>
<mt p="0">card</mt>
<mt p="1">cpubusy</mt>
<mt p="2">cpuidle</mt>
<mt p="3">numproc</mt>
<mt p="4">memused</mt>
<mt p="5">memtotal</mt>
<mv>
<moid> card=17 </moid>
<r p="0">6</r>
<r p="1">0.76</r>
<r p="2">99.24</r>
<r p="3">158</r>
<r p="4">1057704</r>
<r p="5">4194304</r>
</mv>
<mv>
<moid> card=8 </moid>
<r p="0">8</r>
<r p="1">0.45</r>
<r p="2">99.55</r>
<r p="3">65</r>
<r p="4">306512</r>
<r p="5">1048576</r>
</mv>
</ms>
</mi>
```

```
 </md>
 <mff>
 <ts>2006-01-03 13:15:00</ts>
 </mff>
</mdc>
```

This following output is an example of all subsystems in a single file in DTD based XML format.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!DOCTYPE mdc SYSTEM "MeasurementStat.dtd">
<?xml-stylesheet type="text/xsl" href="simple_table_all.xsl" ?>
<mdc>
 <mfh>
 <ffv>2</ffv>
 <sn>Starent Network Inc.</sn>
 <st>MSC</st>
 <vn>Samsung corp.</vn>
 <cbt>2006-01-03 13:10:00</cbt>
 </mfh>
 <md>
 <neid>
 <neun></neun>
 <nedn></nedn>
 <nesw></nesw>
 </neid>
 <mi>
 <mts>2006-01-03 13:15:00</mts>
 <gp>300</gp>
 <rsf>false</rsf>
 <ms>
 <msn>CardStat</msn>
```

```
<sf>false</sf>
<es>false</es>
<mt p="0">card</mt>
<mt p="1">cpubusy</mt>
<mt p="2">cpuidle</mt>
<mt p="3">numproc</mt>
<mt p="4">memused</mt>
<mt p="5">memtotal</mt>
<mv>
<moid> card=17 </moid>
<r p="0">17</r>
<r p="1">0</r>
<r p="2">100</r>
<r p="3">0</r>
<r p="4">0</r>
<r p="5">0</r>
</mv>
<mv>
<moid> card=8 </moid>
<r p="0">8</r>
<r p="1">0.45</r>
<r p="2">99.55</r>
<r p="3">65</r>
<r p="4">306512</r>
<r p="5">1048576</r>
</mv>
</ms>
<ms>
<msn>PortStat</msn>
```

```
<sf>false</sf>
<es>false</es>
<mt p="0">card</mt>
<mt p="1">port</mt>
<mt p="2">rxbytes</mt>
<mt p="3">txbytes</mt>
<mt p="4">ucast_inpackets</mt>
<mt p="5">ucast_outpackets</mt>
<mt p="6">mcast_inpackets</mt>
<mt p="7">mcast_outpackets</mt>
<mt p="8">bcast_inpackets</mt>
<mt p="9">bcast_outpackets</mt>
<mt p="10">rxpackets</mt>
<mt p="11">txpackets</mt>
<mt p="12">rxdiscbytes</mt>
<mt p="13">rxdiscpackets</mt>
<mt p="14">txdiscbytes</mt>
<mt p="15">txdiscpackets</mt>
<mt p="16">maxrate</mt>
<mt p="17">frag-rcvd</mt>
<mt p="18">pkt-reassembled</mt>
<mt p="19">frag-tokernel</mt>
<mv>
<moid> card=17,port=1 </moid>
<r p="0">17</r>
<r p="1">1</r>
<r p="2">43346</r>
<r p="3">1792</r>
<r p="4">328</r>
```

```
<r p="5">28</r>
<r p="6">0</r>
<r p="7">0</r>
<r p="8">1</r>
<r p="9">0</r>
<r p="10">329</r>
<r p="11">28</r>
<r p="12">0</r>
<r p="13">0</r>
<r p="14">0</r>
<r p="15">0</r>
<r p="16">0</r>
<r p="17">0</r>
<r p="18">0</r>
<r p="19">0</r>
</mv>
</ms>
<ms>
<msn>IPPoolStat</msn>
<sf>false</sf>
<es>false</es>
<mt p="0">vpnname</mt>
<mt p="1">vpnid</mt>
<mt p="2">name</mt>
<mt p="3">used</mt>
<mt p="4">hold</mt>
<mt p="5">release</mt>
<mt p="6">free</mt>
<mt p="7">type</mt>
```

```
<mt p="8">priority</mt>
<mt p="9">state</mt>
<mv>
<moid> vpnname=network,vpnid=2,name=Pool </moid>
<r p="0">network</r>
<r p="1">2</r>
<r p="2">Pool</r>
<r p="3">0</r>
<r p="4">0</r>
<r p="5">0</r>
<r p="6">254</r>
<r p="7">S</r>
<r p="8">0</r>
<r p="9">G</r>
</mv>
</ms>
</mi>
</md>
<mff>
<ts>2006-01-03 13:15:00</ts>
</mff>
</mdc>
```

3GPP Format

This following output is an example of individual files for all subsystems in 3GPP XML format.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<!--?xml-stylesheet type="text/xsl" href="MeasDataCollection.xsl?"-->
<measCollecFile xmlns="http://www.3gpp.org/ftp/specs/archive/32_series/32.435#measCollec"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
xsi:schemaLocation="http://www.3gpp.org/ftp/specs/archive/32_series/32.435#measCollec
http://www.3gpp.org/ftp/specs/archive/32_series/32.435#measCollec">

 <fileHeader dnPrefix="Unknown" fileFormatVersion="2" vendorName="Sagar">

 <fileSender elementType="Nikhil" localDn="Same"/>

 <measCollec beginTime="2008-04-25 04:40:00"/>

 </fileHeader>

 <measData>

 <managedElement localDn="Same" swVersion="7.1.19504" userLabel="st16"/>

 <measInfo>

 <job jobId="7381"/>

 <granPeriod duration="PT300S" endTime="2008-04-25 04:45:00"/>

 <msn>CardStat</msn>

 <suspect>false</suspect>

 <measTypes>card cpubusy cpuidle numproc memused memtotal</measTypes>

 <measValue measObjLdn="card=22">

 <measResults>22 0 100 0 0 0</measResults>

 </measValue>

 <measValue measObjLdn="card=24">

 <measResults>24 0 100 0 0 0</measResults>

 </measValue>

 </measInfo>

 </measData>

 <fileFooter>

 <measCollec endTime="2008-04-25 04:45:00"/>

 </fileFooter>

</measCollecFile>
```

This following output is an example of all subsystems in a single file in 3GPP XML format.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>

<!--?xml-stylesheet type="text/xsl" href="MeasDataCollection.xsl?"-->
```

```
<measCollecFile
xmlns="http://www.3gpp.org/ftp/specs/archive/32_series/32.435#measCollec"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.3gpp.org/ftp/specs/archive/32_series/32.435#measCo
llec http://www.3gpp.org/ftp/specs/archive/32_series/32.435#measCollec">

 <fileHeader dnPrefix="Unknown" fileFormatVersion="2" vendorName="Sagar">

 <fileSender elementType="Nikhil" localDn="Same"/>

 <measCollec beginTime="2008-04-25 04:40:00"/>

 </fileHeader>

 <measData>

 <managedElement localDn="Same" swVersion="7.1.19504" userLabel="st16"/>

 <measInfo>

 <job jobId="7381"/>

 <granPeriod duration="PT300S" endTime="2008-04-25 04:45:00"/>

 <msn>CardStat</msn>

 <suspect>false</suspect>

 <measTypes>card cpubusy cpuidle numproc memused memtotal</measTypes>

 <measValue measObjLdn="card=22">

 <measResults>22 0 100 0 0 0</measResults>

 </measValue>

 <measValue measObjLdn="card=24">

 <measResults>24 0 100 0 0 0</measResults>

 </measValue>

 <msn>PortStat</msn>

 <suspect>false</suspect>

 <measTypes>card port rxbytes txbytes ucast_inpackets ucast_outpackets
mcast_inpackets mcast_outpackets bcast_inpackets bcast_outpackets rxpackets
txpackets rxdiscbytes rxdiscpackets txdiscbytes txdiscpackets maxrate frag-rcvd
pkt-reassembled frag-tokernel</measTypes>

 <measValue measObjLdn="card=22,port=1">

 <measResults>22 1 1236 1024 16 16 0 0 2 0 18 16 0 0 0 0 100000000 0 0
0</measResults>
```

```
 </measValue>

 <measValue measObjLdn="card=22,port=2">

 <measResults>22 2 212 0 0 0 0 0 2 0 2 0 0 0 0 0 100000000 0 0 0</measResults>

 </measValue>

 <msn>IPPoolStat</msn>

 <suspect>false</suspect>

 <measTypes>vpnname vpnid name startaddr groupname used hold release free type
priority state</measTypes>

 <measValue
measObjLdn="vpnname=egress,vpnid=6,name=dynamic,startaddr=17.0.0.1,groupname=">

 <measResults>egress 6 dynamic 17.0.0.1 0 0 0 65534 P 0 G</measResults>

 </measValue>

 <measValue
measObjLdn="vpnname=egress,vpnid=6,name=static,startaddr=18.0.0.1,groupname=">

 <measResults>egress 6 static 18.0.0.1 0 0 0 65534 S 0 G</measResults>

 </measValue>

 </measInfo>

 </measData>

 <fileFooter>

 <measCollec endTime="2008-04-25 04:45:00"/>

 </fileFooter>

</measCollecFile>
```

File Naming Conventions

The naming conventions for the files are as per 3GPP standard. The naming convention is different only for individual subsystem files where we include subsystem names in the file name (for example, “CardStat”, “PortStat”, etc.).

The following convention will be applied for measurement result file naming:

```
<Type><Startdate>.<Starttime>-[<Enddate>.]<Endtime>_[<UniqueId>][:<RC>]
```

Field Name	Description
Type	Indicates if the file contains measurement results for single or multiple NEs and/or granularity periods, where: • “A” indicates single NE, single granularity period; • “B” indicates multiple NEs, single granularity period; • “C” indicates single NE, multiple granularity periods; • “D” indicates multiple NEs, multiple granularity periods.
Startdate	Indicates the date when the granularity period began if the Type field is set to “A” or “B”. If the Type field is either “C” or “D” then, Startdate contains the date when the first granularity period of the measurement results contained in the file started. The Startdate field is of the form YYYYMMDD, where: • YYYY is the year in four digit notation; • MM is the month in two digit notation (01-12); • DD is the day in two digit notation (01-31).
Starttime	Indicates the time when the granularity period began if the Type field is set to A or B. If the Type field is either “C” or “D” then, Starttime contains the time when the first granularity period of the measurement results contained in the file began. The Starttime field is of the form HHMMshhmm, where: • HH is the two digit hour of the day (local time), based on 24 hour clock (00-23); • MM is the two digit minute of the hour (local time), possible values are 00, 05, 10, 15, 20, 25, 30, 35, 40, 45, 50, and 55; • s is the sign of the local time differential from UTC (+ or -), in case the time differential to UTC is 0 then the sign may be arbitrarily set to “+” or “-”; • hh is the two digit number of hours of the local time differential from UTC (00-23); • mm is the two digit number of minutes of the local time differential from UTC (00-59).
Enddate	This field will only be included if the Type field is set to “C” or “D”, that is, measurement results for multiple granularity periods are contained in the file. It identifies the date when the last granularity period of these measurements ended, and its structure corresponds to the Startdate field.
Endtime	Indicates the time when the granularity period ended if the Type field is set to A or B. If the Type field is either “C” or “D” then, Endtime contains the time when the last granularity period of the measurement results contained in the file ended. Its structure corresponds to the Starttime field, however, the allowed values for the minute of the hour are 05, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, and 00.

Field Name	Description
UniqueId	This is the name of the NE, EM or domain (for example, a distinguishedName). The field may be omitted only if the distinguishedName is not available from the CM applications.
RC	This parameter is a running count, starting with the value of "1", and will be appended only if the filename is not unanimous, that is, more than one file is generated and all other parameters of the file name are identical. Therefore, it may only be used by the Network Element Manager (EM), since the described situation can not occur with Network Element (NE) generated files.

A few examples describing the file naming convention are as follows:

- File name: A20000626.2315+0200-2330+0200_NodeBId;

  Meaning: File produced by NodeB <NodeBId> on June 26, 2000, granularity period 15 minutes from 23:15 local to 23:30 local, with a time differential of +2 hours against UTC.

- File name: B20021224.1700-1130-1705-1130_EMId,

  Meaning: File containing results for multiple NEs, produced by EM <EMId> on December 24, 2002, granularity period 5 minutes from 17:00 local to 17:05 local, with a time differential of –11:30 hours against UTC.

- File name: D20050907.1030+0000-20050909.1500+0000_DomainId:2,

  Meaning: File containing results for NEs belonging to domain <DomainId>, start of first granularity period 07 September 2005, 10:30 local, end of last granularity period 09 September 2005, 15:00 local, with a time differential of 0 against UTC. This file is produced by the EM managing the domain, and it is the second file for this domain/granularity periods combination.

Supported Standards

WEM complies with the following 3rd Generation Partnership Project (3GPP) standards for generation of XML report files in DTD based format and 3GPP format respectively.

- **3GPP TS 32.401 V4.1.0 (2001-12):** "Concept and Requirements"
- **3GPP TS 32.435 V6.2.0 (2006-03):** "Performance measurement: eXtensible Markup Language (XML) file format definition"

Understanding WEM Bulk Statistics Output in XML Reports

WEM can be configured to generate bulk statistics reports in XML format at user-defined intervals. The reports generate statistical output based on the bulk statistic type (Counter or Gauge) and its availability (e.g., per context, per service, per APN or across all services on the system). For bulk statistics of type “Incremental,” WEM will calculate and generate a delta value. For bulk statistics of type “Gauge,” WEM always provides the absolute value.

Important: A bulk statistic type of 'Counter' is referred to as an 'Incremental Counter' in WEM files.

How WEM Parses Bulk Statistic Data

The ASR 5000 chassis keeps a running aggregate total of bulk statistics configured for collection. The total continues to increase until the counters are cleared or the chassis is reset. However, the XML reports generated by WEM do not provide a running aggregate total for each statistical value of a counter of type “Incremental.” Instead, WEM performs a calculation on each bulk statistic counter configured for the XML report so that only the incremental value for a configured time interval appears in the generated report.

Once bulk statistic generation is enabled, WEM uses the first configured report interval to obtain the raw statistical value for each configured bulk statistic. This first group of statistical values will be used by the system as a reference value for each of the bulk statistics configured to appear in the report. WEM does not generate a report based on this first group of reference values.

When the second configured report interval is reached, WEM obtains the raw statistical value from the ASR 5000 chassis, compares those values to the reference values obtained from the first interval, and outputs the delta to the XML report. This process continues for each scheduled time interval, with the latest interval’s statistical output being compared against the previous one, and the delta being generated in succeeding XML reports.

Important: WEM must be able to reference two consecutive bulk statistics collection records before it can generate an XML report. If two consecutive records are not found, WEM does not generate a report.

Example

In this example, a WEM user has enabled bulk statistic collection to occur at 15-minute intervals beginning at 11:00. WEM will then use the information gathered from the ASR 5000 to calculate the incremental totals for each 15-minute interval and output them to reports in XML format.

1. At 11:00, WEM stores the raw statistical reference value for the bulk statistics obtained from the ASR 5000. An XML report is not generated.
2. At 11:15, WEM obtains the raw statistical bulk statistics values for counters of type Incremental and Gauge from the ASR 5000 and compares these to the values obtained at 11:00.
3. For bulk statistics of counter type Incremental, WEM subtracts the stored statistical values of the 11:00 collection from the values obtained at the 11:15 collection. The deltas between the two sets of values are then generated in the XML report. For bulk statistics of type Gauge WEM performs no delta calculation and outputs the absolute value to the XML report.
4. During each of the succeeding report intervals, WEM obtains the raw statistical values of counter type “Incremental” from the chassis and subtracts the previous report’s value from them to calculate and generate the XML output. Bulk statistics of type “Gauge” are always generated as absolute values.

Table 56. Example: Incremental Bulk Statistic Calculations for a WEM XML Report

Report Number	Time	Raw Bulk Statistic Value	Value Generated in XML Report
n/a	11:00	100	Raw reference value obtained. No XML report is generated.
1	11:15	200	**100** (200-100=100)
2	11:30	400	**200** (400-200=200)
3	11:45	1000	**600** (1000-400=600)
4	12:00	1500	**500** (1500-1000=500)

Sample XML Bulk Statistics Report

The generated XML report includes the following information:

- Start and end time of the bulk statistic collection interval.
- The granularity period for bulk statistics collection (in seconds).
- The bulk statistic variable names that have been configured to appear in the report.
- The context, session, service name or APN name associated with the collected bulk statistics. The identifiers available will vary depending on the bulk statistic schema for which statistics are being collected.
- The values for bulks statistics of counter types Incremental and Gauge.

Figure 3. Example WEM XML Report (3GPP 6.2.0 Format)