Cisco Mobility Unified Reporting System Installation and Administration Guide

Version 12.2

Last Updated February 10, 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-25590-02

Cisco Mobility Unified Reporting System 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 5000 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/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 ASR 5000 chassis:

- *ASR 5000 Command Line Interface Reference*
- *Statistics and Counters Reference*
- *Thresholding Configuration Guide*
- *Cisco ASR 5000 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
Mobility Unified Reporting System Overview

This chapter provides an overview of the Mobility Unified Reporting (MUR) application.

This chapter describes the following topics:

Introduction

The Cisco Mobility Unified Reporting (MUR) system is a Web-based application providing a unified reporting interface for diverse data from Cisco Systems In-line service and storage applications.

The MUR application enables:

- Generating customized reports and comparison charts.

  This release of MUR only supports generating HTML-based historical canned reports displaying data in graphical—graphs/charts—and tabular formats. Reports for ad-hoc periods are not supported. For information on the various reports supported, see the Report Types section.

- Analyzing the reporting data and enabling the operator to get a full understanding of the performance of the network, enabling operators to optimally configure and plan their network.
- Supporting distributed installation which allows to view reports from multiple sites.
- Rich visualization (Graphs/tabular form).
- Exporting reports in Microsoft Excel, Adobe PDF, and CSV formats.
- Capacity monitoring and planning of system supporting a suite of products such as PDSN, GGSN, SGSN, and inline service applications like Content Filtering.

The MUR application is available for report generation only when you install the software application on to your local server. For information on the server recommendations, refer to MUR System Requirements section in this guide. For information on how to install the MUR application, refer to *Managing MUR Installation* chapter in this guide.

The MUR application provides comprehensive and consistent set of statistics and customized reports, report scheduling and distribution from ASR chassis / in-line service product. For example, a subscriber's Quality of Experience, top 10 sites visited, top 10 users, and so on.

The MUR application provides reporting capability for Content Filtering (CF) data, bulk statistics, Key Performance Indicators (KPIs), EDRs data from in-line service and storage applications. The MUR application facilitates and enhances the operators' ability to simply and easily determine the health and usage of the network.

Important: In RHEL-based deployment of MUR, L-ESS is NOT required as the ASR chassis Enhanced Charging Services (ECS) module can be configured to push the xDRs directly to the MUR reporting server. Push from ASR chassis is the Cisco recommended deployment model. Currently L-ESS is supported only on Solaris platforms. For information on the L-ESS installation instructions, refer to the *ESS Installation and Administration Guide*. Existing deployments where L-ESS is installed, to pull EDRs from the chassis, may continue with their deployment model in the 12.0 version of MUR Software Release and later.

For information on obtaining and installing the license, see *System Administration Guide* and *Enhanced Charging Services Administration Guide*. For information on configuring the ECS module, see *Configuring Chassis for Mobility Unified Reporting System* chapter in this guide.

MUR receives the following types of EDRs for report processing:

- CF-EDRs
- Flow EDRs
- HTTP EDRs

To reduce disk space and improve performance, MUR limits the bucket distribution for EDR data to ONLY last 2 days in case a EDR is spanning across more than 2 days or so.

For example, if the following EDR is received:

```
#sn-start-time,sn-end-time,radius-calling-station-id,ip-subscriber-ip-address,sn-
subscriber-port,ip-server-ip-address,sn-server-port,sn-app-protocol,p2p-protocol,traffic-
type,voip-duration,sn-volume-amt-ip-bytes-uplink,sn-volume-amt-ip-bytes-downlink,sn-
volume-amt-ip-pkts-uplink,sn-volume-amt-ip-pkts-downlink,bearer-3gpp rat-type,radius-
called-station-id,bearer-3gpp imei,ip-protocol,bearer-3gpp sgsn-address,sn-flow-start-
time,sn-flow-end-time
1275330600,1275334200,9689944191,19.19.1.1,35111,1.1.1.1,21,8,,,0,52428800,1048576,100,20
0,1,apn.org1,35302703-090362-52,6,1.1.1.3,1275330600,1275334200
```

MUR determines the difference between the starttime and endtime attributes and limits the bucket distribution as shown here.

```
#starttime,endtime,protocol,rxbytes,txbytes 2011/02/26 10:00:00,2011/02/28
10:00:00,HTTP,100MB,100MB
```

Important: The bucket distribution calculation will remain intact i.e. the volume will be distributed equally among all the half-hour's buckets that fall in the starttime and endtime.

Important: The MUR receives the data in terms of EDRs which are generated based on the flow. As the EDRs are flow-based and the bulkstats is a real-time data, the volumes reported in the EDR are different from the volumes reported by bulkstats.

For more information on using the MUR application to generate reports, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

Report Types

The MUR application supports generation of canned statistical reports that can be used to analyze network performance, and decide the policies for users, and identify the customer trends, network usage patterns, network categorization, etc. The reports can be per gateway, or multiple gateways (region), or for the overall network. The reports can be generated for the usage of different entities such as gateway, content type, etc on an hourly, daily, weekly, or monthly basis.

The typical canned reports that are supported for the MUR application include:

- Historical summary reports (Daily/Weekly/Monthly)
    - Half-hourly Reports: Usage reporting for the specified time period
    - Daily Reports: Usage reporting for the past 24-hour period (midnight through midnight)
    - Weekly Reports: Usage reporting for the past seven day period (Monday through Sunday)
    - Monthly Reports: Usage reporting for the past 30-day period (1 day of the month through the last day of the month)
- Top "N" Reports
- Statistical and analytical reports
- Bulkstats and KPI reports

The static report layout comprises the following sections:

- The report name
- The report ownership: the user account that requested the report
- The date and time of generation
- The list of report parameters
- The chart legend (displayed under the chart)

On the interactive layout the user can set a series of preferences in a specific manner. The user has the flexibility to change the type of chart from Bar to Pie (supported output types depend on the selected report). Changing the preferences like the chart type or report parameters will cause the report to refresh in the same window.

The interactive chart layout provides the following list of features:

- Tool tip: When the mouse pointer stops over a chart series, after a short time a tool tip is displayed showing the information of the targeted sample.
- Dynamic legend: The legend is located beneath the chart and is used to recognize the series plotted on the screen. In case of series representing either network services or subscriber packages, the colors are bound to the service/package names. This means that, for example, the HTTP Service will be rendered with a specific color for the reports. The legend is usually displayed with check-boxes associated to each color.

The MUR application provides the following reports:

- Traffic Analysis Report: The Traffic Analysis report provides the total usage traffic (including uplink and downlink traffic) details for the following application categories:
  - Video
  - Filesharing
  - Web
  - IM
  - VOIP
  - Standard
  - Streaming
  - Tunnel
  - Gaming
  - Unclassified

  MUR supports traffic type detection for P2P protocols such as Skype, Gtalk, MSN, Yahoo, and Oscar with the use of “traffic-type” attribute present in the EDR fields. Based on the value of this EDR attribute, the data will be classified to respective protocols.

  The usage traffic is expressed in terms of megabytes (MB) or Megabits per second (Mbps) and percentage (%). The traffic can also be in gigabytes (GB) / kilobytes (KB) / bytes depending on the magnitude.
- Traffic Distribution Report: The Traffic Distribution report provides the summary of total traffic distribution for all the protocols application categories over a specified time period. The usage traffic is represented in GB/MB/KB/Bytes and percentage.
- Active Flow Count Report: The Active Flow Count report provides the details of traffic distribution flow count against the different application categories. This report also provides the summary of maximum number of flows in the EDR records.

Important: Active Flow Count report for current date will not be available because daily tables used to fetch this report are generated only at the end of the day. Also when the user selects a date range, for example, 10/1/2011 to 10/5/2011 where 10/5/2011 is the current date, then the report will be shown for the period 10/1/2011 to 10/4/2011 i.e. up till 10/4/2011.

Release 12.2 onwards, the Active Flow Count report will show flow counts for a sample/bucket (as per the configured granularity) that has maximum number of flows for selected filters in flow count summary. This new behavior is applicable to data ONLY after upgrading MUR to 12.2 version. Previous data will be shown as per the old reporting behavior.

- Unique Subscriber Hits Report: The Unique Subscriber Hits report provides an overview of the usage patterns of the entire subscriber population per protocol, for example, how many people are actually using VoIP.

  Important: Unique Subscriber Hits report can be generated ONLY for a single date/week/month and not for any date-range. Also, note that the time selection is also disabled for this report.

  Typically, this report provides the total number of times a subscriber is using a specific protocol. These reports are displayed for all configured gateways.

  Important: Unique Subscriber Hits report for current date will always be available on the subsequent date because unique subscribers hits calculation will be performed at the end of the day.

- TopN versus Total Traffic Report: This report provides the summary of total usage traffic and Top N subscriber traffic for all the protocols over a specified time period. The usage traffic is represented in GB/MB/KB/Bytes and packets.
- Session Duration Report: A session is defined as the combination of GGSN address and charging identifier. Two GGSNs can have the same charging ID. Charging identifier is used together with GGSN address to identify all records produced in SGSN(s) and GGSN involved in a single PDP context.

  Session duration is the time difference between start time and end time for that session. This reports the statistical analysis of user sessions over the session duration.
- TopN Subscribers Report: The TopN Subscribers report simply counts the number of bytes per subscriber for different time intervals. It displays the top 10/100/1000 subscribers for each day/week/month. This report is displayed across all configured gateways, per region or per NOC.

  Important: This report is not available for a multiple date range selection.

  After identifying the total amount of transferred data per subscriber, and identifying the top users, to understand the protocol and services breakdown for each subscriber, this report allows listing the different applications used by the top 10/100/1000 subscribers based on the selection of top subscriber per day/week/month.
- TopN VCD Subscribers Report: The TopN Voice Call Duration (VCD) Subscribers report displays the top N subscribers based on their voice usage (voice duration) for Yahoo, MSN and Skype voice protocols. The summary report displays the voice summary (voice duration) for VoIP category.

  Important: This report is also available per week or month.

- Weekly Report: The weekly report provides details of the following:
  - Total traffic
  - Total traffic by category
  - VOIP Call Duration
  - Total unclassified traffic (TCP and UDP)
  - Top N subscribers
- Monthly Report: The monthly report provides the details of total traffic across the top N protocols / application categories in a month.
- Custom Reporting: MUR supports on-demand offline reporting of subscriber specific information to operators. This ad-hoc request could be a subscriber search request or top N search request.

  Offline Subscriber Report: The MUR aids in searching individual subscribers' data based on certain parameters like IMSI, MSISDN, NAI, IMEI and Public and Private (NAT) subscriber IP address with ports, individually or in combination, and generates a subscriber-specific report showing the list of URLs visited by the subscriber, and other details like QoS, usage traffic, aggregate application/protocol breakdown, etc for the specified time period. MUR mainly supports this search functionality to track a subscriber or a set of subscribers for lawful intercept.

  To use this Offline Reporting feature seamlessly, you must configure the EDR Filename Format appropriately through the Gateway configuration from **ADMIN** tab, and organize the archive directory date-wise. For information on how to manage the archive directory, see the *Managing Archive Directory* section in the *MUR Administration and Management* chapter of this guide.

  Offline Top N Subscribers Report: MUR also facilitates to generate an offline report that covers the % of volume/duration used by top n% subscribers. This report provides information on the absolute number of subscribers and the list of MSISDNs to facilitate correlation with the provisioning data. In this release, this ad-hoc report is available per APN group, Device Group, Location Group, and Service Profile.

  Through this custom TopN reporting feature, it is possible to monitor and report the video traffic usage as and when needed. This report is mainly required to identify TopN hosts for video traffic and also to determine the biggest sources of video traffic, which drives the network load at a greater extent.

  HTTP content type will be used to identify the video traffic. Ideally video traffic should be derived from flow-EDRs. Since the video usage monitoring report is generated based on HTTP content type, only HTTP traffic will be counted.

  For more information on these features, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

  Reports based on Tethering Configuration: Tethering refers to the use of a mobile smartphone as a USB dongle/modem to provide Internet connectivity to PC devices (laptops, PDAs, tablets, and so on) running on the smartphone's data plan. Typically, for smartphone users, most operators have in place an unlimited data plan, the usage of which is intended to be from the smartphone as a mobile device. However, some subscribers use the low cost / unlimited usage data plan to provide Internet connectivity to their laptops in places where normal Internet connection via broadband/WiFi may be costly, unavailable, or insecure.

  The ASR chassis works in conjunction with the MUR application to facilitate tethering detection on the chassis. The EDRs generated by the chassis will be enhanced to include OS signatures.

  MUR processes flow-EDR files containing OS signature and IMEI field, HTTP files containing User Agent and IMEI field, and populates the tethering data in database files.

  For more information on this feature, see the *Cisco Mobility Unified Reporting System Online Help* documentation and *12.2 Enhanced Charging Services Administration Guide Addendum*.

- DPI Report: The Deep Packet Inspection (DPI) reports are the canned statistical reports at the gateway level and region level. You can configure the MUR application to generate the reports for any of the available gateways.

  In this release, MUR supports generating daily, weekly and monthly summary details and busy hour traffic usage details for the following report categories:

  - Traffic Analysis Report
  - Traffic Distribution Report
  - Active Flow Count Report
  - Unique Subscribers Hits Report
  - TopN Reports — Report on Top N vs Total Traffic, TopN subscribers, TopN VCD subscribers
  - Session Duration Report

  > ***Important:*** Release 12.2 onwards, users with only administrative privileges can decrypt the subscriber's MSISDN to make it appear in the clear text format in the weekly reports.

  MUR has the capability to report the following details per protocol:

  - Total volume for the day/week/month
  - Volume distribution in the busy hour
  - Peak performance for the day/week/month
  - Maximum number of unique subscribers
  - Number of sessions hosted by GGSN service and the corresponding duration

  MUR supports additional information breakdown by network characteristics. These include Application Category, Protocol Groups, IP Protocol, Device Group, RAT (Radio Access Type i.e 2G vs 3G), APN (Access Point Name), SGSN group, Service Profile, Roaming Partner, and Location Group. During its development, a device may have several TAC codes and there may be a need to report devices by broader device type such as "Blackberry" or "Smartphone". Device groups allow the operator to combine a range of TACs into a single named group for reporting purposes.

  Busy Hour Reporting: Busy Hour (BH) reporting is mainly useful for the users to monitor different traffic flows in their network during the busy hour. BH indicates the sliding 60-minute period during which occurs the maximum total traffic load in a given 24-hour period.

  Please note the following key points:

  - BH reporting is available ONLY on the GUI and not in xls format.
  - BH reporting is available only under the **DPI** tab.
  - BH radio button is available on the date panel.
  - BH reporting is available for a date, date range, week and month.
  - Busy hour reports are currently available ONLY at the NOC level.

  DSL Reports: The current release of MUR provides the following details for Digital Subscriber Line (DSL) traffic reports:

  - Traffic analysis — uplink DSL, downlink DSL and total DSL traffic including daily weekly, and monthly aggregation/distribution.
  - DSL traffic categorization — total P2P traffic over DSL, IP traffic, web traffic, etc.
  - Top N% DSL subscribers

- Comparison of total DSL traffic versus total UMTS traffic

For information on additional reports supported through DPI, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

- CF-RE Report: Content Filtering (CF) solution enables operators to filter HTTP and WAP requests from mobile subscribers based on the URLs in the requests, so that subscribers are inadvertently not exposed to universally unacceptable content and/or content inappropriate as per the subscribers' preferences.

  The CF-RE report provides the summary of traffic over CF categories, CF actions, and CF ratings. The CF actions that can be taken on the URL are as follows:

  - allow
  - discard
  - redirect-url
  - content-insert
  - terminate-flow
  - reply-code-terminate-flow

  The CF ratings can be one of the following:

  - dynamic
  - static
  - blacklisted

  The CF-RE report also provides the list of top N subscribers and URLs based on their unique subscriber's hit count and total usage.

- HTTP Reports: The MUR application parses HTTP EDRs and then provides the following details for any specific day, week, month and date range:

  - Total traffic per HTTP group / host name and HTTP content type
  - URL hits per HTTP group / host name and HTTP content type
  - Unique subscriber count per HTTP group / host name

  Typically, MUR supports the following categories of HTTP reports:

  - Summary reports — Content type/subtype volume report available for daily, weekly, monthly, and date range
  - Top N reports (Daily/Weekly/Monthly)
    - HTTP Group Aggregation — TopN HTTP group by Volume; TopN HTTP group by Hit count; TopN HTTP group by Unique subscriber hits
    - Top N Referrer Group Aggregation by Hit count
    - TopN User Agent (UA) reports available for APN-TAC combination in addition to individual per APN, per TAC reports.
    - HTTP Services Aggregation — TopN HTTP Services by Volume; TopN HTTP Services by Hit count

  The top N referrers' report provides details of the total hit count for top N referrers and their sub-domain wise traffic distribution.

Important: In the distributed model of MUR, the data received from RDP is populated and TopN referrer report is available only at NOC level.

Important: It is mandatory to configure *http-url* and *http-referer* fields in the EDR records for top N HTTP referrers report generation.

- Top N Unknown Ports: This report highlights the top N ports for which traffic is classified as either unidentified or unknown. This report also lists the underlying IP protocol, downlink volume (in Megabytes), uplink volume (in Megabytes) and total volume (in Megabytes).

  The report on top N unknown ports can be viewed through the link **Edr unknown port infos** under the **System** menu.

- Bulkstat Report: The Bulkstat report provides details of the processed bulk statistics from any application (PDSN, GGSN, SGSN, and so only) on the managed nodes in a timely manner.

  Important: Make sure that you configure the bulkstats schemas through the GUI to generate bulkstats reports for any of the available gateways. For more information on schema configuration, refer to the *Configuring Bulkstats Schemas Using GUI* section in this guide and also *Cisco Mobility Unified Reporting System Online Help* documentation.

  The bulkstat data is sent from the gateway to the MUR server with GMT (UTC Time stamps). The bulkstat file processing is triggered by the MUR scheduler engine. The scheduler processes the bulkstat files line by line for each gateway, and gets the schema, timestamp, and key index. If the index does not exist, the parser creates index and inserts data into bulkstats data table. Once the processing is complete, this data file is moved to the archive directory. Summarization must happen as the user moves from gateway to higher levels.

  Important: For Bulkstat, there is no support for distributed model and all the bulkstat input files will be parsed by master MUR system only.

  MUR supports generation of busy hour reports, top N Min/Max reports, performance aggregation reports i.e. daily, weekly and monthly summary reports.

  Please keep the following key points in mind for bulkstats reporting:

  - The gateway(s) and MUR server need to be NTP synced for accurate BS aggregation reports.
  - Hourly aggregation reports are triggered at 50th minute of every hour.
  - Daily reports are scheduled at 3:45 PM the next day.
  - Weekly reports are scheduled at 5:00 PM every Monday.
  - Monthly reports are scheduled at 06:15 PM on 1st of every month.

- KPI Report: The KPI report provides details of the KPIs for each selected schema. KPIs are the formula-based calculations of selected bulk statistics counters. You can configure the MUR application to generate the reports for any of the available gateways. For a complete listing of supported KPIs and its associated formulas/descriptions, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

Important: Please note that the Bulkstats and KPI reports are displayed based on the gateway's time zone.

Important: Please note that the subscriber's private data like Mobile Station Integrated Services Digital Network (MSISDN) will appear encrypted in all the subscribers reporting. Users with administrative privilege can only decrypt the MSISDNs using a shell script utility. For information on how to use this script, refer to the *MUR Administration and Management* chapter in this guide. The MSISDN decryption can also be accomplished through **Admin > Users** menu in the GUI. For decryption through the GUI, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

Important: Please note that the availability of any report is typically based on the date/date range configurations and purging interval. If you are trying to view a report beyond the configured purging interval, MUR system will display an error message indicating that the report is unavailable.

For more information on each of these reports, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

Exporting Reports to Other File Formats

The MUR application supports exporting reports to the following file formats:

- Microsoft Excel format: To export a report to Microsoft Excel format, use the *get_excel_report* script in the CLI. For more information about this script, refer to the *Generating Reports in Excel Format* section in the *MUR Administration and Management* chapter of this guide.

  Exporting of reports to Excel format is also possible through the GUI by clicking the excel icon present in the tabular view of each of the reports under **HOME** and **DPI** tabs.
- Comma Separated Value (CSV) file format: To view reports in CSV format, in the HOME and DPI tabs, click the csv icon present in the tabular view of each of the reports.
- PDF format: To export a report to PDF format, in the **HOME** and **DPI** tabs of the MUR GUI, click the **PDF** button. The PDF file is displayed in a new window and can be saved for future reference.

  If there is no data available for a report, the **PDF** button is disabled.
- Text File format: This format is applicable only to HTTP User Agent (UA) reports. To export this report in a text file, click **Export to Text** button available in the HTTP UA reporting page.

  For more information, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

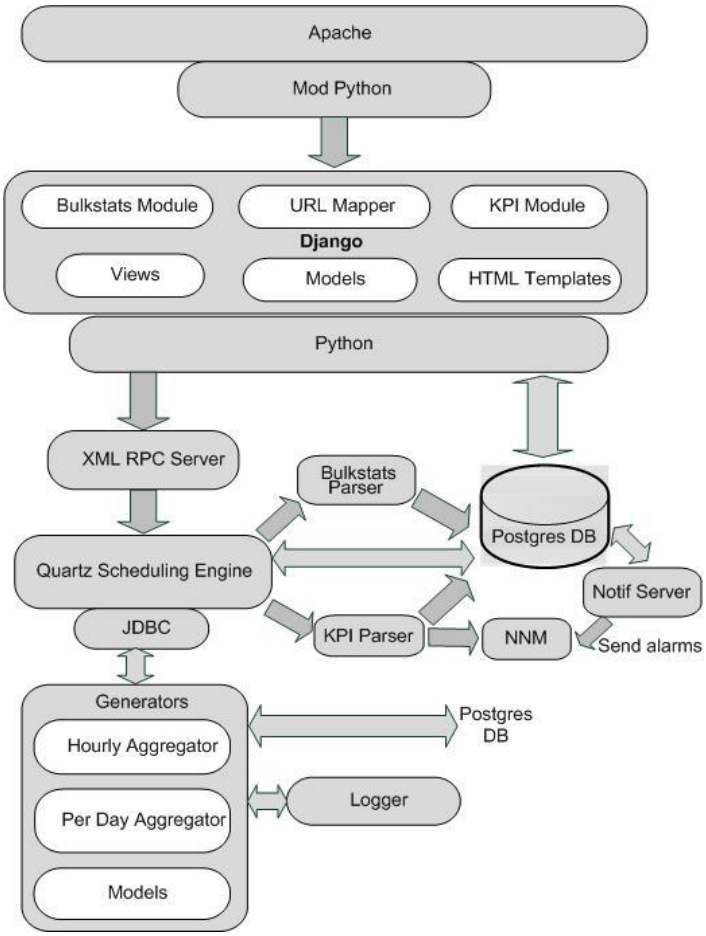
License Requirements

The MUR system is a licensed Cisco product. Contact your Cisco account representative for detailed information on specific licensing requirements.

MUR Architecture

The MUR solution consists of two components — a server and a GUI client. The following figure shows a typical organization of the MUR solution.

Figure 1. Internal Architecture of MUR



The server components include:

- DB Server: This is the standard PostGreSQL 8.3 database server. This is started at the time of application startup.

  MUR uses pgbouncer utility for postgres connection pooling. This utility gets started/stopped with Postgres Server.

- Quartz Scheduling Engine: This is the core of the MUR reporting solution. It is used to schedule different tasks such as parsing of incoming data files (bulkstat, EDR, etc.), trigger various canned reports on a periodic basis, cleaning up of stored outdated data and files, and so on.

- Generators: These are python based scripts that are used for parsing various CSV files. The files are parsed to an extent where generated files (or data in database) themselves represent meaningful data. This is a very powerful concept introduced for faster processing of information.

The generators archive the files once they are parsed. In archival, the files are zipped and placed in the configured location.

- KPI Parser: The KPI Alarm Generator uses the information stored by bulkstat parser in the database for KPI calculations and then, based on the calculations, generates the alarms that are subsequently sent to Network Node Manager (NNM).
- Notif Server: This stands as a separate entity that collects information from the MUR system and generates alarms which are then sent to the NNM for further analysis.
- Loggers: The MUR application uses various loggers so that application logs with various severities are made available for debugging purpose.
- MUR Parser Server: This will be running as daemons, and it will be spawned at the time of **`serv start`** command. Parser server will keep running in background and will perform the parsing activity for all gateways.

  The following is a sample output of the **`serv status`** command:

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

--------------- MUR Process Status ------------

 PID            Process                  Status

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

 4245          Process Monitor           Running

 4256          Scheduling server        Running

 4267          Postgres Server         Running

 4289          Apache Server           Running

 3249          Notif Server           Running

 3243          Parser Server           Running

 2430          Cache Server           Running

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

The following describes the sequential steps associated with the functioning of RPC parser daemons.

1. For each configured gateway, RPC Parser daemon will check if the appropriate reporting (Flow/HTTP/CF) is enabled or not.

   If say, Flow-EDR reporting is enabled for GW1, RPC Parser daemon will check the Process Count configured for Flow-EDR under **System** menu.

2. Depending on the number of processes configured, RPC Parser daemon will spawn those many RPC server instances for GW1. Also, it will update each RPC server URL in DB as shown below:

ID	Gateway ID	Reporting Type	RPC Server URL	Process ID
1	1	Flow-EDR	http://localhost:8000	7643
2	1	Flow-EDR	http://localhost:8001	8756

ID	Gateway ID	Reporting Type	RPC Server URL	Process ID
3	1	Flow-EDR	http://localhost:8002	9054
4	1	Http-EDR	http://localhost:8003	5645
5	1	Http-EDR	http://localhost:8004	6576
6	1	Http-EDR	http://localhost:8005	8678

3. Steps 1 through 3 are repeated for each configured gateway and reporting type.
4. Normalization daemon will pick up the set of files to be parsed. Depending on the number of files to be parsed, it will get the corresponding RPC server information from DB from the above table.
5. Depending on the number of files to be parsed, normalization daemon will spawn those many threads. Each thread will allocate its bunch of files to corresponding RPC server instance. The RPC server instance will parse and store the normalized data in DB and the corresponding thread will exit.
6. If the Process count is increased/reduced, additional RPC server instances will be fired/closed as and when required.
7. Both the normalization daemon and RPC Parser daemon will be continuously running in background.
8. Normalization daemon will be spawned by the scheduler initially. RPC Parser daemon will be spawned through **`serv start`** command.

Some of the components at the client side include Django and Mod_python.

Distributed Architecture of MUR

MUR supports the distributed model to allow the deployment which enables network wide view or work load balancing. Newly introduced component, Remote Data Processor (RDP), plays the role of pre-processing the input files from gateways. One or more RDPs, installed separately on remote machines can be registered to a master MUR and one RDP can process files from one or more gateways.

RDP periodically sends the intermediate data to registered master MUR. The role of MUR in such deployments is mostly for report generation, report viewing, RDP management and optionally data processing.

Important: RDP installation and registration is required only for network wide deployments. For standalone installation no RDP is required. For information on how to install the RDP, refer to the *Managing MUR Installation* chapter of this guide.

Important: Make sure that you first install the master MUR system and then proceed with the RDP installation. Also, note that the RDP and MUR must be installed, upgraded, and uninstalled separately.

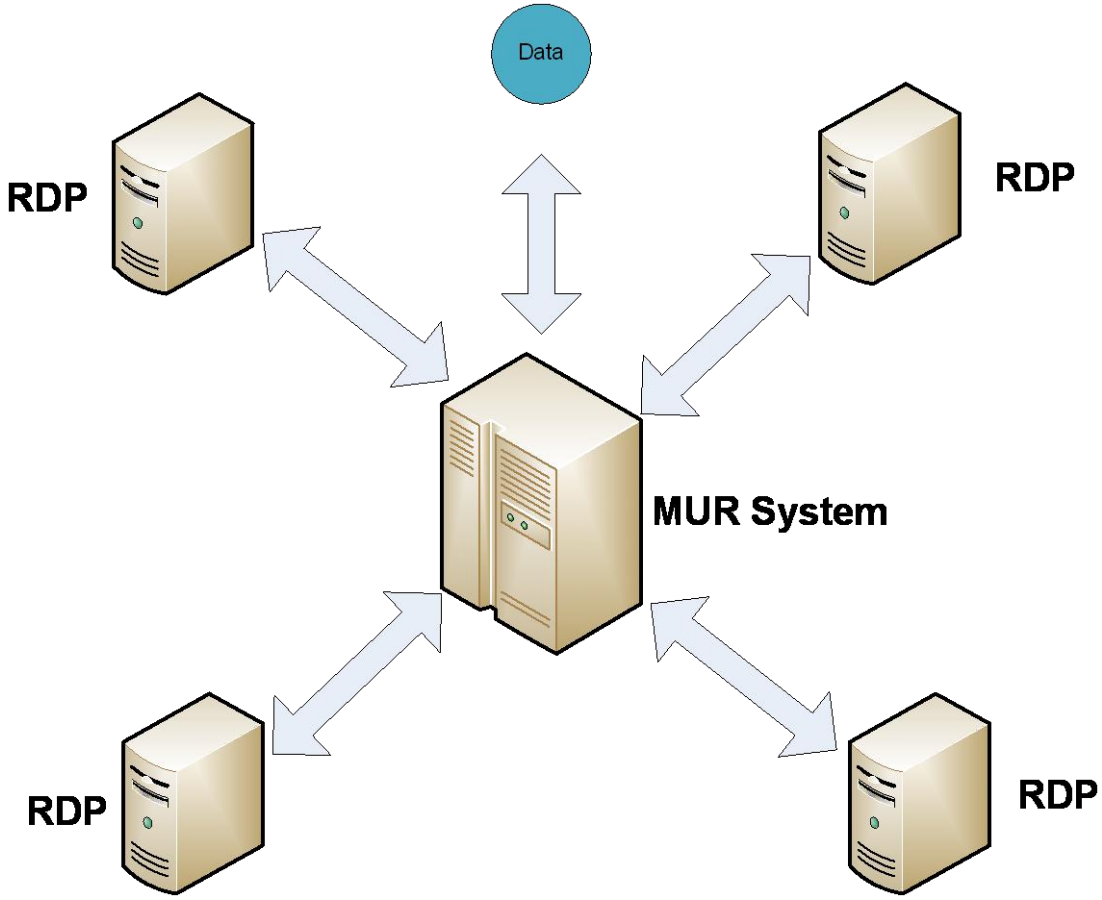
Important: Before registering RDP with the master MUR, ensure that the RDP is installed and running.

Important: The RDP management like configuration and removal is possible from MUR GUI only. For information on managing the RDPs, refer to the *Cisco Mobility Unified Reporting System Online Help* documentation.

Important: For Bulkstat, there is no support for distributed model and all the bulkstat input files will be parsed by master MUR only.

The following figure illustrates the distributed architecture of MUR.

Figure 2. Distributed Architecture of MUR



How RDP works with MUR

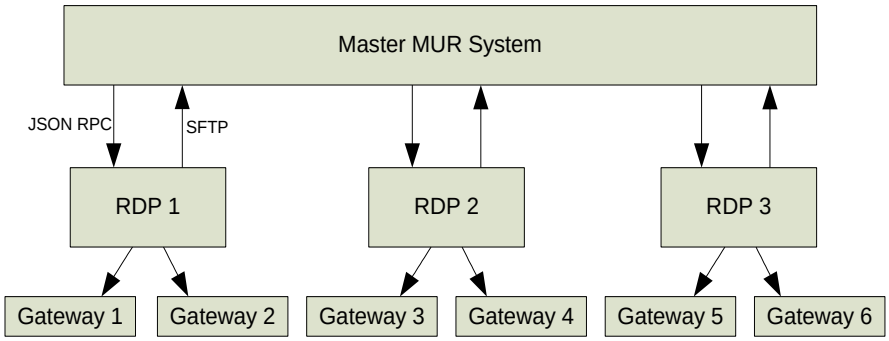
This section describes how the RDP works with the MUR application.

The RDP parses the raw data or EDR files from one or more GGSNs and populates the database for required reports. The RDP pre-processes the data and then periodically forwards them to the master MUR through SFTP for report generation.

Important: If the distributed model of MUR is used, then the SFTP user name and password should be the same as the MUR Administrator user's login name and password provided during installation. For information on configuring SFTP details, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

Each of the RDP and MUR will be assigned a unique ID during installation and will be used for identification of each RDP along with its gateway and data.

Figure 3. MUR with RDPs in Distributed Model



In 12.0 and earlier releases, each of the registered RDPs will form a new region. RDP region can be a child of the root of the MUR (NOC) or can be the child of another region. The gateways associated with a RDP will always be the children of RDP region.

Release 12.2 onwards, users can create individual regions and add RDPs to the regions. All the gateways must be associated with RDP(s) or NOC and not to a region directly.

Important: Only single MUR can communicate with an RDP simultaneously.

Region-based Reporting

In 12.0 and earlier releases, RDP was considered as a region. So, all reports were based on RDP. Whenever an RDP is configured, internally MUR used to create corresponding region for the same. However, with the introduction and need of scalable MUR, one gateway's files will be processed by two or multiple RDPs. In that case, RDP does not stand as a region. So, reports will be required across all the RDPs under one specific region. Particularly, when there are multiple such regions where each region has more than one RDPs, this feature becomes more important. A different case for the requirement of this feature is a region where there are multiple gateways and they are processed by different RDPs. In that case, per RDP based reports will not make sense, rather, region based reports will be required.

Important: In the gateway tree in **DPI**, **HTTP**, **CF** and **Bulkstats** tab, the pseudo gateway is NOT shown. This is because, there are no specific reports to the gateway, it is just a pseudo to original gateway and all the data is coming from the original gateway only.

Tethering Detection Feature

Important: In the current 12.2 release, the Tethering Detection feature is supported only on the GGSN.

Tethering refers to the use of a mobile smartphone as a USB dongle/modem to provide Internet connectivity to PC devices (laptops, PDAs, tablets, and so on) running on the smaprtphone's data plan. Typically, for smartphone users, most operators have in place an unlimited data plan, the usage of which is intended to be from the smartphone as a mobile device. However, some subscribers use the low cost / unlimited usage data plan to provide Internet connectivity to their laptops in places where normal Internet connection via broadband/WiFi may be costly, unavailable, or insecure.

The Tethering Detection feature enables detection of subscriber data traffic originating from PC devices tethered to mobile smartphones, and also provides effective reporting to enable service providers take business decisions on how to manage such usage and to bill subscribers accordingly.

Important: Use of Smartphone tethering detection feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

For detailed information on this feature, refer to *12.2 Enhanced Charging Services Administration Guide Addendum*.

MUR Support for Tethering Detection

The ASR chassis works in conjunction with the MUR application to facilitate tethering detection on the chassis.

MUR is used to collect samples of HTTP and TCP signatures from live traffic to create a database of OS and UA signatures for assorted devices accessing the network through the gateways. For this, offline TAC-device mappings are fed to MUR, and MUR generates the signature databases based on EDRs generated by the chassis for various TAC groups.

Upon enabling tethering detection feature through the GUI, MUR collects samples of HTTP and TCP signatures from live traffic and creates a database of OS and UA signatures for assorted devices accessing the network through the gateways. For this, offline TAC-device mappings are fed to MUR, and MUR generates the signature databases based on EDRs generated by the chassis for various TAC groups.

MUR processes flow-EDR files containing OS signature and IMEI field, HTTP files containing User Agent and IMEI field, and populates the following set of data in the respective database files.

- Laptop (USB Dongles device group) - User Agent data
- Laptop (USB Dongles device group) - OS Signature data
- Smartphone - TAC data

MUR is configured in such a way that the database files are pushed to the ASR chassis under the `/mnt/hd-raid/data/databases/` directory.

For information on how to confiugre tethering detection feature, refer to *Configuring Chassis for Mobility Unified Reporting System* chapter in this guide.

Tethering Detection Databases

The Tethering Detection feature uses the OS signature, UA signature, and TAC databases.

These database files must be populated and loaded on to the chassis by the administrator. The procedure to load the databases is the same for all the three types of databases.

Before the database(s) can be loaded for the first time, tethering detection must be enabled using the **tethering-database** CLI command in the Active Charging Service Configuration Mode.

For all three databases, only a full upgrade of a database file is supported. Incremental upgrade is not supported. If, for any particular database, the upgrade procedure fails, the system will revert back to the previous working version of that database.

OS Signature Database

The OS signature database file is named "os-db". The file contains OS fingerprint signatures that have been identified as non-smartphone signatures.

The OS fingerprint signature string is a null-terminated ASCII string of maximum 32 bytes in the following format:

<tlen>|*<ttl>*|*<d>*|*<wlen>*|*<mss>*|*<wss>*|STEN

Where:

- *tlen*: Total IP Packet Length
- *ttl*: Initial TTL
- *d*: IP DF bit
- *wlen*: TCP Window Length
- *mss*: TCP Maximum Segment Size
- *wss*: TCP option Window Size Scale
- *S*: TCP option Selective ACK OK
- *T*: TCP option Timestamp
- *E*: TCP option EOL
- *N*: TCP option NOP (count)

The maximum number of entries permitted in the os-db file is 16384.

The maximum size of the os-db file can be 524KB + 50 bytes for header and trailer.

In the 12.2 release, the file is in plain text format and contains one TCP signature in ASCII format, one entry per line.

The following is the content of a sample os-db file:

```
VERSION 1.1

BEGIN OS-DB

48|128|1|5840|1460|1|1112

44|128|0|5840|1460|1|1011

END OS-DB
```

UA Signature Database

The UA signature database file is named "ua-db". The file contains UA signatures that have been identified as non-smartphone signatures.

The UA signatures are stored in plain text format in the database file so that manual modification of the database is possible.

The maximum number of entries permitted in the ua-db file is 16384.

The maximum size of the ua-db file can be 67MB + 50 bytes for header and trailer.

The following is the content of a sample ua-db file:

```
VERSION 1.1

BEGIN UA-DB

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2)

END UA-DB
```

TAC Database

The TAC database file is named “tac-db”. The file contains smartphone TACs that are uploaded in MUR by the operator.

The maximum number of entries permitted in the tac-db file is 16384.

The maximum size of the tac-db file can be 147KB + 50 bytes for header and trailer.

The following is the content of a sample tac-db file:

```
VERSION 1.1

BEGIN TAC-DB

01194800

01194801

END TAC-DB
```

Loading and Upgrading Tethering Detection Databases

This section provides an overview of loading and upgrading the OS, UA, and TAC databases used in tethering detection.

The database files from MUR must be copied onto the chassis to the following directory path designated for storing the database files:

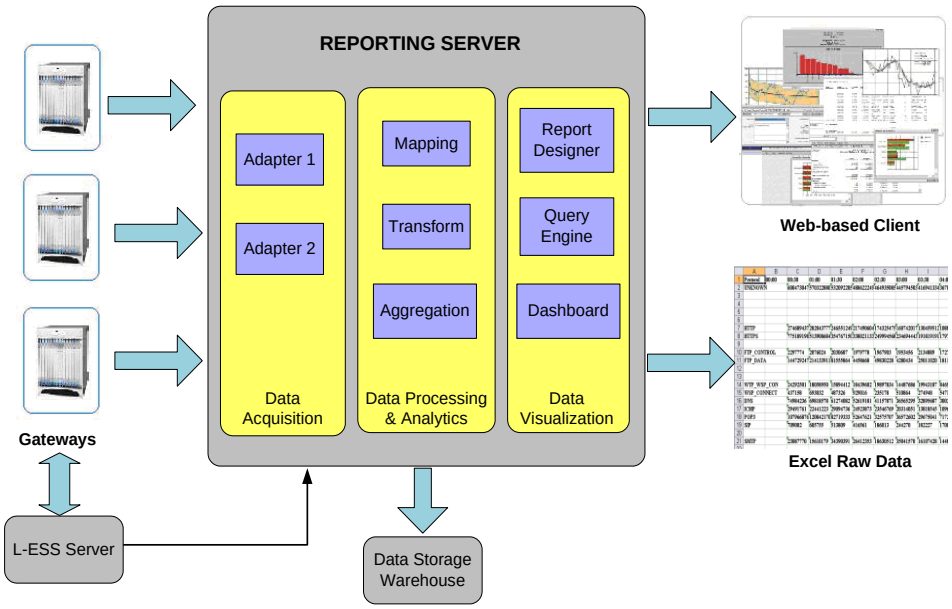
`/mnt/hd-raid/data/databases/`

Any further upgrades to the database files can be done by placing the file named `new-filename` in the designated directory path. ACS auto-detects the presence of files available for upgrade daily. When a new version of a file is found, the upgrade process is triggered. The upgrade can also be forced by running the upgrade command in the CLI. On a successful upgrade this file is renamed to `filename`.

MUR Deployment

The following figure illustrates how the MUR reporting server interacts with the gateways and generates the reports.

Figure 4. End-to-end Component Mapping



The chassis / gateway supports on board Hard Disk Drive (HDD) for extended storage of the xDR files such as EDR, UDR, CDR, and NBR. If the HDD is configured, then the gateway pushes the files to an external entity like External Storage Server (ESS) for short-term storage. In case of no HDD support on the gateway, the Local, short-term External Storage Server (L-ESS) has the capability of pulling the files from gateways via SFTP, and send it for report processing. For more information on L-ESS, refer to the *ESS Installation and Administration Guide*.

The MUR server collects the EDRs, and bulkstats from gateways or L-ESS server, and processes the incoming data files and presents reports on Web-based GUI. The MUR application can generate reports in Excel, CSV, and PDF formats, and present them to users on a request basis.

Important: L-ESS is NOT required as the ASR5K EDR module can be configured to push the xDRs directly to the MUR reporting server. Push from ASR chassis is the Cisco recommended deployment model. Currently, L-ESS is supported only on Solaris platforms. For information on the L-ESS installation instructions, refer to the *ESS Installation and Administration Guide*. Existing deployments where L-ESS is installed, to pull EDRs from chassis, may continue with their deployment model in the 12.0 version of MUR Software Release and later.

For information on how to configure the chassis to push the xDRs, refer to the *Configuring Chassis for Mobility Unified Reporting System* chapter in this guide.

MUR System Requirements

This section identifies the minimum system requirements that are required for the deployment of MUR at the operator's premises.

Important: The hardware required for MUR may vary depending on incoming EDR generation, subscriber count, and number of gateways.

Server Recommendations for Use in Solaris Environment

This section identifies the minimum system requirements recommended when installing the MUR application in Solaris environment.

NEBS Requirements:

The following are the server specifications for MUR when an additional external storage is required:

- Sun Microsystems Netra™ X4270 server
    - Quad-Core two socket Intel Xeon L5518 processor
    - 32GB RAM
    - 2 * 300GB 10K RPM SAS disks
    - SATA DVD drive
    - 8 internal port SAS HBA
    - Choice of AC or DC power supplies
- Sun StorageTek 2540 SAS Array, Rack-Ready Controller Tray
    - 12 * 300GB 15K RPM SAS drives
    - Two redundant AC power supplies
- Operating system:
    - Sun Solaris 10 with latest patches installed

Non-NEBS Requirements:

The following are the server specifications with only the internal storage used:

- Sun Fire X4270 server
    - Intel Xeon processor 5500 series
    - 32GB RAM
    - 16 * 300GB 10K RPM SAS disks
    - SATA DVD drive
- Operating system:
    - Sun Solaris 10 with latest patches installed

Important: It is strongly recommended to update the Operating System with the latest security patches.

Important: The number of disks recommended is purely based on the throughput of the network and data retention configuration. Please contact Cisco Advanced Service Team for data sizing.

ZFS Pooling Recommendations:

This section provides information on the recommendations for ZFS pooling.

- OS pool: This mirrored ZFS pool shall be created for Solaris OS installation.
- MUR pool: This standard ZFS pool shall be created for MUR i.e. MUR installation, incoming data files.
- Postgres pool: This standard ZFS pool shall be created for MUR postgres database.
- Archive pool: This standard ZFS pool shall be created for retaining archived and data backed up files.

Important: ZFS pool shall NOT be created with RAID-Z since ZFS does not allow attaching an additional disk to an existing RAID-Z pool. Hence, this freezes the chances of data scaling.

Server Recommendations for Use in RHEL Environment

This section identifies the requirements of server recommended when installing the MUR application in RHEL environment.

- UCS C460 M2 server
  - 4 x Intel® Xeon® E7-4860 @ 2.26 GHz, 130W 10 Core CPU / 24 MB Cache
  - 128GB RAM
  - 12 * 600 GB SAS 6G, 10K RPM
  - RAID Controller
  - 4Gb Dual port FC Host Bus Adapter

    Important: The number of disks recommended is purely based on the throughput of the network and data retention configuration. Please contact Cisco Advanced Service Team for data sizing.

- Operating System
  - Cisco UCS running OS version ‘Cisco MITG RHEL 5.5’

    For information related to OS installation, refer to the *Cisco MITG RHEL OS v5.5 Application Note*.

    Important: 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*.

    Important: ZFS Pooling recommendations are applicable ONLY for Solaris hardware.

- XFS/EXT-3 File System Volumes & RAID Recommendations

Storage RAID recommendation for MUR Application

CISCO UCS machine supports MegaRAID controller. This allows configuring the UCS hard disks into hardware RAID arrays (disk groups). The MegaRAID controller provides the BIOS utility for configuring the RAID.

The RAID recommendations for MUR are as follows:

- Separate disk arrays for OS, MUR and postgres (data directory).
- RAID Level - Combination of 5 and 0 depending upon the fault tolerance.
- Stripe size should be 256KB
- RAID Controller parameters —
    - Read Policy - Select Adaptive read ahead
    - Write Policy - Select Write Back
    - I/O Policy - Select Direct I/O

For information on configuring the RAID arrays using MegaRAID BIOS, refer to the *Configuring Cisco UCS Servers for MUR System Application Note*.

Storage Recommendation for MUR Application

This section provides the storage recommendations needed for the MUR application.

- Separate storage (single disk or RAID array) for OS. (root and swap space partitions)
- **Two RAID arrays**: RAID-0 for MUR application and RAID-5 for database (Postgres data directory).
- **LVM**: Separate physical volume and volume groups for the three RAID array disk groups.
- **XFS file-system**: block size 4KB, s-unit in terms of RAID stripe size (256KB) and s-width in terms of span of disks in the RAID array.

For information on how to partition storage disk and configure XFS file system, refer to the *Configuring Cisco UCS Servers for MUR System Application Note*.

MUR Ports

This section provides information on various ports and their corresponding port numbers used by the MUR application.

Various ports are used by the MUR for both client-server communication and communication with ASR chassis. If firewalls are used on these interfaces, these ports need to be opened.

The following table lists the ports that are used by MUR.

Table 1. Default Port Utilization

Port Name	Port Number	Usage
TCP Port	22	This port is used by MUR administrator to connect via SSH to UNIX command line on MUR servers for system administration. This port is also used by gateway to upload files via SFTP to MUR servers (stand-alone master and RDPs), and also by RDPs to upload files to the master. In the case of pull model, the L-ESS process on the RDPs or stand-alone master will use SFTP to connect to this port on the gateway. This port is also used between master MUR server and gateway to configure and upload bulkstat files.
TCP Port	25	This port is used to send e-mails to a mail server in case these are configured to deliver reports and alarms.
UDP Port	162	This port is used to send traps to the northbound network management system.
Postgres Port	5432	This port is used by the local processes to access the PostgreSQL server and can be restricted to prevent external access.
Apache Port	8080	For a standalone model: This port is used for communication between client workstation and Apache Webserver on MUR via HTTP. For distributed model: This port is used for both Master to RDP and RDP to Master RPC communication. ***Important:*** When firewall is used, Apache is the only port that should be kept opened.

Typically, MUR starts all its related services with non-root (i.e. muradmin) privileges.

Firewall Settings

When MUR is running on RHEL platform, Firewall is ON by default. In that case, user will NOT be able to get access to MUR GUI. The Firewall MUST be disabled with the following commands:

```
service iptables save

service iptables stop

chkconfig iptables off
```

Using Apache Port

This section provides information on how to configure the Apache port to use in conjunction with the MUR reporting server.

Using Apache in Solaris

In case the user wants to configure Apache port as 80 (i.e. < 1024), it is necessary to run the following command as **root** user so that *muradmin* can start the services on ports < 1024.

usermod -K defaultpriv=basic,net_privaddr *<mur admin user>*

Using Apache in RHEL

Important: Make sure that you disable Firewall before using the Apache port in the RHEL environment.

RHEL does not allow port 80 to be used by non-root users. However, Apache Web server requests made on port 80 can be redirected to a port >1024 defined by the operator, with the following two commands:

iptables -t *nat* **-A** *PREROUTING* **-p** *tcp* **--dport** *80* **-i** *eth0* **-j** *REDIRECT* **--to-port** *<user defined port>* **1024>**

iptables -t *nat* **-A***OUTPUT* **-p** *tcp* **-d** *127.0.0.1* **--dport** *80* **-j** *REDIRECT* **--to-port** *<user defined port>* **1024>**

For example, to redirect requests made on port 80 to port 8080:

iptables -t *nat* **-A** *PREROUTING* **-p** *tcp* **--dport** *80* **-i** *eth0* **-j** *REDIRECT* **--to-port** *8080*

iptables -t *nat* **-A***OUTPUT* **-p** *tcp* **-d** *127.0.0.1* **--dport** *80* **-j** *REDIRECT* **--to-port** *8080*

Once this is done, user will be able to access the MUR GUI directly, without specifying the port in the Web browser URL *http://<serveripaddress>*.

Chapter 2
Configuring Chassis for Mobility Unified Reporting System

This chapter describes the configurations required to source data for the MUR application.

Important: These configurations are on the chassis.

For more information on ECS configurations, see the *Enhanced Charging Services Administration Guide*.

This chapter describes the following topics:

Initial Configuration

If the configurations described in this section are not already available on the system, these must be configured.

Initial configuration steps:

Step 1 Ensure that ECS license is installed on the system.

Step 2 Create the ECS administrative user account as described in the Creating the ECS Administrative User Account section.

Step 3 Enable Active Charging as described in the Enabling Active Charging section.

Step 4 Create Active Charging Service as described in the Creating the Active Charging Service section.

Step 5 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **`save configuration`**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

> ***Important:*** Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Installing the ECS License

To enable and configure ECS functionality on the system you must obtain and install one of the following licenses:

- Starent P/N: 600-00-7526 *Enhanced Charging Bundle 1 1k Sessions license* / Cisco PID: ASR5K-00-CS01ECG1 *Enhanced Charging Bundle 1 1k Sessions license*
- Starent P/N: 600-00-7574 *Enhanced Charging Bundle 2 1k Sessions license* / Cisco PID: ASR5K-00-CS01ECG2 *Enhanced Charging Bundle 2 1k Sessions license* — to enable and configure Diameter and DCCA functionality with ECS

For information on how to install the licenses, see the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Creating the ECS Administrative User Account

At least one administrative user account that has ECS functionality privileges must be configured on the system. This is the account that is used to log on and execute ECS-related commands. For security purposes, it is recommended that these user accounts be created along with general system functionality administration.

Use the following configuration example to create the ECS Administrative user account:

```
configure
   context local
      administrator <user_name> password <password> ecs
```

```
end
```

Notes:

- Aside from having ECS capabilities, an ECS Administrator account also has the same capabilities and privileges as any other system-level administrator account.
- You can also create system ECS user account for a config-administrator, operator, or inspector. ECS accounts have all the same system-level privileges of normal system accounts except that they have full ECS command execution capability. For example, an ECS has rights to execute every command that a regular administrator can in addition to all of the ECS commands.
- Note that only Administrator and Config-administrator-level users can provision ECS functionality. Refer to the *Configuring System Settings* chapter of the *System Administration Guide* for additional information on administrative user privileges.

Enabling Active Charging

Active Charging must be enabled before configuring charging services.

Use the following configuration example to enable Active Charging:

```
configure
   require active-charging
     context local
     interface <interface_name>
        ip address <ipv4/ipv6_address> <ipv4/ipv6_address/mask>
        exit
     server ftpd
     end
```

For more information, refer to the *Enhanced Charging Services Administration Guide*.

Creating the Active Charging Service

Use the following configuration example to create an Active Charging Service:

```
configure
  active-charging service <service_name> [ -noconfirm ]
  end
```

Configuration

The following is the sequence of configurations necessary to source data to the MUR application:

Step 1 Activate P2P analyzer as described in the Activating P2P Analyzer section.

Step 2 Configure EDR flow format as described in the Configuring the EDR Flow Format section.

Step 3 Configure routing ruledefs and rulebase for deep-packet inspection as described in the Configuring Deep Packet Inspection section.

Step 4 Optional. Configure Smartphone tethering detection feature as described in the Configuring Tethering Detection Feature section.

Step 5 Configure EDR module as described in the EDR Module Configuration section.

Step 6 Configure user as described in the Configuring EDR Download Permission section.

Step 7 Configure the bulkstat schemas and then load it onto the gateway.

Step 8 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Activating P2P Analyzer

Use the following configuration example to activate P2P protocol detection:

```
configure
  active-charging service <service_name>
    p2p-detection protocol all
    rulebase <rulebase_name>
      p2p dynamic-flow-detection
      end
```

Notes:

- P2P protocol detection must be activated only within rulebases used by the APNs for which P2P detection is applicable. P2P detection must not be applied to the rulebases used for APNs where such reporting is either not useful or is not possible.

Configuring the EDR Flow Format

Use the following configuration example to configure the EDR format generated for flows:

```
configure
```

```
active-charging service <service_name>
  edr-format <edr_format_name> [ -noconfirm ]
    attribute <attribute> { [ format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS
| YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds } ] [ localtime ] | [ { ip |
tcp } { bytes | pkts } { downlink | uplink } ] priority <priority> }
    rule-variable <protocol> <rule> priority <priority>
    rule-variable traffic-type priority  <priority>
    rule-variable voip-duration priority  <priority>
    event-label <event-label> priority <priority>
    end
```

Notes:

- The **rule-variable traffic-type** and **rule-variable voip-duration** keywords must be configured to enable voice-call-duration (VCD) based reporting.
- *p2p-protocol* is a mandatory field in a flow-edr configurations. However, this field cannot be added to the edr-format configuration unless P2P is licensed. Contact your local Sales or Support representative for information on how to obtain a license.
- For information on EDR format configuration and rule variables, refer to the *EDR Format Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

The following is a sample flow end EDR configuration.

```
configure
  active-charging service ecs_svc1
    edr-format edr_flow_format
      attribute sn-start-time format seconds priority 10
      attribute sn-end-time format seconds priority 20
      attribute radius-calling-station-id priority 30
      rule-variable ip server-ip-address priority 60
      attribute sn-server-port priority 70
      attribute sn-app-protocol priority 80
      attribute sn-parent-protocol priority 81
      rule-variable ip protocol priority 82
      rule-variable p2p protocol priority 90
      attribute sn-volume-amt ip bytes uplink priority 100
```

```
      attribute sn-volume-amt ip bytes downlink priority 110
      attribute sn-volume-amt ip pkts uplink priority 120
      attribute sn-volume-amt ip pkts downlink priority 130
      rule-variable bearer 3gpp charging-id priority 140
      rule-variable bearer 3gpp imei priority 141
      rule-variable bearer 3gpp rat-type priority 142
      rule-variable bearer 3gpp user-location-information priority 143
      rule-variable traffic-type priority 160
      rule-variable voip-duration priority 170
      end
```

The following is a sample HTTP EDR configuration.

```
configure
  active-charging service ecs_svc1
    edr-format edr_http_format
      attribute sn-start-time format seconds priority 10
      attribute sn-end-time format seconds priority 20
      attribute radius-calling-station-id priority 30
      rule-variable ip server-ip-address priority 50
      rule-variable http host priority 70
      rule-variable http content type priority 80
      attribute transaction-downlink-bytes priority 90
      attribute transaction-uplink-bytes priority 100
      attribute transaction-downlink-packets priority 110
      attribute transaction-uplink-packets priority 120
      rule-variable bearer 3gpp charging-id priority 130
      end
```

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

```
show active-charging edr-format name <edr_format_name>
```

Configuring Deep Packet Inspection

This section provides the example configurations that are required for deep packet inspection.

Configuring Routing Rule Definition

Use the following configuration example to create and configure a routing ruledef:

```
configure
  active-charging service <service_name>
    ruledef <ruledef_name>
      <protocol> <expression> <operator> <condition>
         rule-application routing
         end
```

Notes:

- The **rule-application routing** command specifies the ruledef type. If not specified, by default, the system configures the ruledef as a charging ruledef.
- For information on all the protocol types, expressions, operators, and conditions supported, refer to the *Ruledef Configuration Mode Commands* chapter of the *Command Line Interface Reference*.
- Up to 10 rule matches can be configured in one ruledef.
- MMS rules must be set appropriately and MMS should be activated at ECS to support MMS reporting in MUR.

The following is a sample ruledef configuration.

```
configure
   active-charging service srv1
      ruledef http_anymatch
      http any-match = TRUE
      exit
      ruledef icmp_anymatch
      icmp any-match = TRUE
      exit
      ruledef ip_anymatch
      ip any-match = TRUE
```

```
exit
ruledef mms_anymatch
mms any-match = TRUE
exit
ruledef rr_http_80
tcp either-port = 80
rule-application routing
exit
ruledef rr_http_8080
tcp either-port = 8080
rule-application routing
exit
ruledef rr_mms_http_ct
http content type = application/vnd.wap.mms-message
rule-application routing
exit
ruledef rr_mms_http_url
http url ends-with .mms
rule-application routing
exit
ruledef rr_mms_wsp_ct
wsp content type = application/vnd.wap.mms-message
rule-application routing
exit
ruledef rr_mms_wsp_ct_uri
rule-application routing
exit
ruledef rr_mms_wsp_url
wsp url ends-with .mms
```

```
rule-application routing
exit
ruledef rr_wsp_cl_dst_port
udp dst-port = 9200
rule-application routing
exit
ruledef rr_wsp_cl_src_port
udp src-port = 9200
rule-application routing
exit
ruledef rr_wsp_co_dst_port
udp dst-port = 9201
rule-application routing
exit
ruledef rr_wsp_co_src_port
udp src-port = 9201
rule-application routing
exit
end
```

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

show active-charging ruledef routing

Configuring Rulebase

Use the following configuration example to route traffic to the appropriate analyzer within each rulebase where the reporting is applicable.

configure

active-charging service *<service_name>*

rulebase *<rulebase_name>* **[-noconfirm]**

route priority *<priority>* **ruledef** *<ruledef_name>* **analyzer** *<analyzer>* **[description]**

rtp dynamic-flow-detection

flow end-condition handoff timeout normal-end-signaling session-end [charging-edr | edr | reporting-edr *edr_format_name* **]**

edr transaction-complete http [charging-edr | edr-format | reporting-edr *edr_format_name* **]**

end

Notes:

- **charging-edr** will be used as the default option in the **flow end-condition** and **edr transaction-complete** command configurations.
- The **edr** and **edr-format** options are available only in 12.1 and earlier releases. In 12.2 and later releases, these options are deprecated and are replaced by the **charging-edr** option.
- For MUR reporting needs, use the **reporting-edr** keyword in the rulebase configuration.

The following is a sample rulebase configuration for reporting EDRs.

```
configure
  active-charging service ecs_svc1
    rulebase p2p-rb
      flow end-condition handoff timeout normal-end-signaling session-end reporting-edr
edr_flow_format
      action priority 4 ruledef rtsp_setup charging-action standard
      action priority 5 ruledef rtsp_play charging-action standard
      action priority 6 ruledef rtsp_teardown charging-action standard
      action priority 7 ruledef rtsp_anymatch charging-action standard
      action priority 10 ruledef sip_anymatch charging-action handshake
      action priority 11 ruledef rtp_anymatch charging-action handshake
      action priority 12 ruledef udp_anymatch charging-action handshake
      action priority 13 ruledef tcp_anymatch charging-action handshake
      action priority 16 ruledef mms_anymatch charging-action policy1
      action priority 60 ruledef http_anymatch charging-action standard
      action priority 95 ruledef udp_anymatch charging-action standard
      action priority 99 ruledef icmp_anymatch charging-action standard
```

```
action priority 100 ruledef ip_anymatch charging-action handshake
action priority 990 ruledef tcp_anymatch charging-action standard
action priority 1000 ruledef ip_anymatch charging-action standard
route priority 1 ruledef rr_wsp_co_src_port analyzer wsp-connection-oriented
route priority 2 ruledef rr_wsp_co_dst_port analyzer wsp-connection-oriented
route priority 3 ruledef rr_wsp_cl_src_port analyzer wsp-connection-less
route priority 4 ruledef rr_wsp_cl_dst_port analyzer wsp-connection-less
route priority 5 ruledef rr_http_80 analyzer http
route priority 6 ruledef rr_http_8080 analyzer http
route priority 7 ruledef rr_mms_http_ct analyzer mms
route priority 8 ruledef rr_mms_http_url analyzer mms
route priority 9 ruledef rr_mms_wsp_ct analyzer mms
route priority 10 ruledef rr_mms_wsp_url analyzer mms
route priority 11 ruledef rr_mms_wsp_ct_uri analyzer mms
route priority 60 ruledef sip_src analyzer sip
route priority 65 ruledef sip_dst analyzer sip
route priority 70 ruledef rtsp_src analyzer rtsp
route priority 75 ruledef rtsp_dst analyzer rtsp
route priority 250 ruledef sdp_route analyzer sdp
rtp dynamic-flow-detection
edr transaction-complete http reporting-edr edr_http_format
edr voip-call-end reporting-edr edr_flow_format
udr threshold interval 60
udr threshold volume total 100000
p2p dynamic-flow-detection
end
```

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

show active-charging rulebase name <*rulebase_name*>

Configuring Charging Action

Use the following configuration example to configure a charging action:

```
configure
  active-charging service <service_name>
    charging-action <charging_action_name> [ -noconfirm ]
      content-id <content_id>
      retransmissions-counted
      billing-action [ edr <edr_format> [ wait-until-flow-ends ] | egcdr |
exclude-from-udrs | radius ] +
      flow idle-timeout <idle_timeout>
      end
```

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

```
show active-charging charging-action name <charging_action_name>
```

Configuring Tethering Detection Feature

This section describes how to configure the Tethering Detection feature to detect subscriber flows from PC devices tethered to mobile smartphones. For details on how this feature is implemented, see the *Enhanced Charging Services Administration Guide*.

To enable and configure the Tethering Detection feature, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      tethering-database [ os-signature <os_signature_db_file_name> | tac
<tac_db_file_name> | ua-signature <ua_signature_db_file_name> ] +
      ruledef <tethering_detection_ruledef_name>
         tethering-detection { flow-not-tethered | flow-tethered }
         exit
      rulebase <rulebase_name>
         tethering-detection [ os-db-only | ua-db-only ]
         action priority <priority> ruledef <tethering_detection_ruledef_name>
charging-action <charging_action_name>
```

```
...
end
```

Upgrading Tethering Detection Databases

To upgrade the Tethering Detection feature databases, in the Exec mode, use the following CLI command:

```
upgrade tethering-detection database { all | os-signature | tac | ua-signature }
[ -noconfirm ]
```

Sample Configurations

The following examples illustrate two different implementations of the Tethering Detection feature's configuration.

- The following type of configuration is suitable where ECS performance is critical and the operator wants to put in a flat charging plan in place for all the tethered traffic. In such a scenario, addition of a single new ruledef to the configuration suffices. Placing this ruledef at the highest priority in the rulebase will ensure all the tethered flows are charged as per the tariff plan for tethered traffic.

```
configure
   active-charging service ecs_service
      tethering-database
      ruledef tethered-traffic
         tethering-detection flow-tethered
         tcp any-match = TRUE
         exit
      ruledef ftp-pkts
         ftp any-match = TRUE
         exit
      ruledef http-pkts
         http any-match = TRUE
         exit
      ruledef tcp-pkts
         tcp any-match = TRUE
         exit
      ruledef ip-pkts
         ip any-match = TRUE
```

```
      exit
    ruledef http-port
      tcp either-port = 80
      rule-application routing
      exit
    ruledef ftp-port
      tcp either-port = 21
      rule-application routing
      exit
    charging-action premium
      content-id 1
      retransmissions-counted
      billing-action egcdr
      exit
    charging-action standard
      content-id 2
      retransmissions-counted
      billing-action egcdr
      exit
    rulebase consumer
      tethering-detection
      action priority 10 ruledef tethered-traffic charging-action
premium
      action priority 20 ruledef ftp-pkts charging-action standard
      action priority 30 ruledef http-pkts charging-action standard
      action priority 40 ruledef tcp-pkts charging-action standard
      action priority 50 ruledef ip-pkts charging-action standard
      route priority 80 ruledef http-port analyzer http
      exit
```

```
rulebase default

end
```

- The following type of configuration is suitable when operators want to apply differentiated charging to various flows that are found to be tethered. In this case, traffic that requires different charging action or content ID when it is tethered will be identified using two ruledefs, one with “flow-is-tethered = TRUE” option and another without this option. This configuration provides finer granularity of control but results in higher performance degradation because the rule matching tree size increases.

```
configure

   active-charging service ecs_service

      tethering-database

      ruledef ftp-pkts

         ftp any-match = TRUE

         exit

      ruledef ftp-pkts-tethered

         ftp any-match = TRUE

         tethering-detection flow-tethered

         exit

      ruledef http-pkts

         http any-match = TRUE

         exit

      ruledef http-pkts-tethered

         http any-match = TRUE

         tethering-detection flow-tethered

         exit

      ruledef tcp-pkts

         tcp any-match = TRUE

         exit

      ruledef tcp-pkts-tethered

         tcp any-match = TRUE

         tethering-detection flow-tethered
```

```
   exit
ruledef ip-pkts
   ip any-match = TRUE
   exit
ruledef ip-pkts-tethered
   ip any-match = TRUE
   tethering-detection flow-tethered
   exit
ruledef http-port
   tcp either-port = 80
   rule-application routing
   exit
ruledef ftp-port
   tcp either-port = 21
   rule-application routing
   exit
charging-action premium-http
   content-id 10
   retransmissions-counted
   billing-action egcdr
   exit
charging-action premium-ftp
   content-id 20
   retransmissions-counted
   billing-action egcdr
   exit
charging-action premium
   content-id 1
   retransmissions-counted
```

```
            billing-action egcdr
            exit
         charging-action standard
            content-id 2
            retransmissions-counted
            billing-action egcdr
            exit
         rulebase consumer
            tethering-detection
            action priority 10 ruledef ftp-pkts-tethered charging-action
premium-ftp
            action priority 20 ruledef ftp-pkts charging-action standard
            action priority 30 ruledef http-pkts-tethered charging-action
premium-http
            action priority 40 ruledef http-pkts charging-action standard
            action priority 50 ruledef tcp-pkts-tethered charging-action
premium
            action priority 60 ruledef tcp-pkts charging-action standard
            action priority 70 ruledef ip-pkts-tethered charging-action
premium
            action priority 80 ruledef ip-pkts charging-action standard
            route priority 80 ruledef http-port analyzer http
            exit
         rulebase default
            end
```

EDR Module Configuration

Use the following configuration example to configure the EDR module:

```
configure
  context <context_name>
    edr-module active-charging-service [ charging | reporting ]
```

file name *<file_name>* **rotation volume** *<file_size_bytes>* **rotation time** *<file_complete_seconds>* **rotation num-records** *<records_number>* **storage-limit** *<storage_limit_bytes>* **headers reset-indicator edr-format-name trap-on-file-delete compression gzip file-sequence-number rulebase-seq-num**

cdr [push-interval *<interval>* **| remove-file-after-transfer | transfer-mode { pull | push primary { encrypted-url** *<enc_url>* **| url** *<url>* **} [secondary { encrypted-secondary-url** *<enc_sec_url>* **| url** *<sec_url>* **}] } + | use-harddisk]**

end

Notes:

- The *<context_name>* must be the context specified for accounting.
- EDR type configuration is optional. The EDR types can be either **charging** or **reporting**. The **charging** keyword is the default setting.

  For MUR reporting needs, use the **reporting** keyword for the EDR type.
- The **cdr use-harddisk** command is only available on the ASR 5000 platform.
- The **cdr use-harddisk** command specifies storing files on the hard disk. The reporting server will download these files through the SPIO interface on the SMC and will delete the files after successful retrieval.
- The **edr-format-name** keyword must be configured to distinguish between different EDRs. The EDR file name must be configured in an accepted format so that the Offline Subscriber Reporting functionality can be used effectively. For information on this functionality and the EDR file name configuration recommendations, see the *Cisco Mobility Unified Reporting System Online Help* documentation.
- The files will be compressed to save storage and transmission bandwidth.
- For the PULL model, an external device like L-ESS is used to pull the EDR files from the chassis via SFTP. Whereas, for the PUSH model, the chassis is configured to push the files to the required destination.

  Important: The chassis automatically creates */edr* and */udr* directories on the destined path on MUR server when you configure it to push the files.
- The values recommended for **rotation volume** and **rotation time** keywords are 40 MB and 300 seconds respectively.

Important: In RHEL-based deployments, L-ESS is NOT required as the Enhanced Charging Services (ECS) module can be configured to push the xDRs directly to the MUR reporting server. Push from ASR chassis is the Cisco recommended deployment model. Currently L-ESS is supported only on Solaris platforms. For information on the L-ESS installation instructions, refer to the *ESS Installation and Administration Guide*. Existing deployments where L-ESS is installed, to pull EDRs from chassis, may continue with their deployment model in the 12.0 version of MUR Software Release and later.

The following is a sample EDR PUSH configuration.

```
configure
 context test
  edr-module active-charging-service reporting
```

```
    file name EDRFILE rotation num-records 10000 storage-limit 268435456 headers
reset-indicator trap-on-file-delete compression gzip file-sequence-number rulebase-seq-
num

    cdr transfer-mode push primary url sftp://root:nulink@10.4.72.54/inpilot-
local/Ash_Test/starbi/server/data via local-context

    cdr push-interval 60

    cdr remove-file-after-transfer

    cdr use-harddisk

    end
```

The following is a sample EDR PULL configuration.

```
configure

 context local

  edr-module active-charging-service

    file name EDRFILE1 rotation time 300 rotation num-records 10000 storage-limit
268435456 headers reset-indicator trap-on-file-delete compression gzip file-sequence-
number rulebase-seq-num

    cdr remove-file-after-transfer

    cdr use-harddisk

    end
```

Verifying your Configuration

To verify your configuration, in the Exec Mode, enter the following command:

show configuration context <*context_name*>

Pushing EDR/UDR Files Manually

To manually push EDR/UDR files to the configured L-ESS, in the Exec mode, enter the following command:

cdr-push { all | local-filename <*file_name*> **}**

Notes:

- Before you can use this command, in the EDR/UDR Configuration Mode, the CDR transfer mode and file locations must be set to push.
- <*file_name*> must be absolute path of the local file to push.

For more information on the **cdr** command, please refer to the *Command Line Interface Reference*.

Configuring EDR Download Permission

Use the following configuration example to configure EDR download permission:

```
configure
  context local
    administrator <administrator_id> password <password> ftp nocli
    end
```

Notes:

- The user must be configured in the local context with administrative privileges to download and delete EDRs from the hard disk. The **ftp nocli** options restrict access to FTP only.

Configuring Bulkstats Schemas Using GUI

MUR provides a user interface to configure bulk statistics schemas on chassis / gateway via SSH and SFTP. The Client sends HTTP request to MUR to configure schemas on a particular gateway after providing inputs to the parameters needed for schema configuration. MUR server receives the HTTP request, generates a configuration file on the fly, sends the configuration file to the gateway via SFTP and loads it on to the gateway through SSH.

Important: In StarOS 10.0 and earlier releases, WEM is used to configure the bulkstats schemas on the chassis if user has deployed WEM. In case if WEM has not been deployed, then please contact local sales or service representative for obtaining the embedded bulkstats configuration file.

Important: In StarOS 11.0 and later releases, you can configure Bulkstat schemas only through the MUR GUI by selecting **ADMIN** > **BULKSTATS** menu.

Prior to configuring the bulkstats schemas, ensure that the following checks are performed:

- The gateway must be running and active.
- Enable SFTP and FTP services

  For Solaris setup:

  - FTP must be enabled on the MUR server.

    To enable the FTP daemon, use the following command:

    /usr/sbin/svcadm/ enable ftp

    To disable the FTP daemon, use the following command:

    /usr/sbin/svcadm/ disable ftp

  For RHEL setup:

  - FTP must be enabled on the MUR server.

    To enable the FTP daemon, use the following command:

    service vsftpd start

    To disable the FTP daemon, use the following command:

```
service vsftpd stop
```

- SSH version 2.0 key must be generated on the gateway. To generate the SSH version 2.0 key through the CLI, enter the following command:

```
configure
  context local
    ssh generate key type v2-rsa
    ssh generate key type v2-dsa
    end
```

- Secure Shell (SSH) configuration mode must be enabled on the gateway. To enable the SSH configuration mode, enter the following command:

```
configure
  context local
    server sshd
    end
```

- FTP/SFTP must be allowed on the gateway for the "SSH Username" that will be entered in the Bulkstat Schema Configuration screen. For example, if the username is *staradmin* and password is *test* then the following commands should be used to enable FTP/SFTP for *staradmin* user.

```
configure
  context local
    administrator staradmin password test ftp
    end
```

Important: The bulkstats report will be visible to users only when the schemas are configured successfully.

For information on how to configure the bulkstats schemas, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

Supported Bulkstat Schemas

This section provides the list of bulk statistics schemas that are supported in MUR for reporting.

- SS7RD
- MME
- SGW
- MIPV6HA
- PGW
- IMSA
- NAT_REALM
- ASNGW
- PORT
- SGSN
- MISC
- CARD
- MIPFA
- GTPP
- PHSGW
- CSCFINTF
- RADIUS
- APN
- CLOSEDRP
- LAC
- SGTP
- IPPOOL
- SCCP
- GPRS
- SS7LINK
- CSCF
- MAG
- CONTEXT
- SYSTEM
- ECS
- PHSPC
- EGTPC
- RP

- PPP
- MIPHA
- PDG
- GTPC
- PDIF
- IPSG
- LMA
- AAL2
- ALCAP
- ASNPC
- BCMCS
- CS_NW_RANAP
- CS_NW_RTP
- DCCA
- DPCA
- GTPU
- HNBGW_HNBAP
- HNBGW_RANAP
- HNBGW_RTP
- HNBGW_RUA
- HNBGW_SCTP
- LNS
- PCC_POLICY
- PCC_QUOTA
- PCC_SERVICE
- PCC_SP_ENDPT
- PS_NW_RANAP
- MVS

For more information on these bulkstats, refer to the *Statistics and Counters Reference*.

Supported SNMP Traps

The alarm generation feature aids in proactively monitoring the nodes and important resources of MUR. This feature also provides configuration interface for setting up thresholds and other key information related to critical resources. Alarms are generated when these thresholds are exceeded and various actions can be performed such as sending e-mail, syslog messages, Simple Network Management Protocol (SNMP) traps.

It is necessary to configure the SNMP manager or Network Node Manager (NNM) to receive these notifications. The SNMP server and SNMP event configurations can be made through the **System** menu in the Web-based MUR GUI.

Threshold values should be configured for the following event identifiers (event IDs):

- CPU Usage - *CPU* — This alarm is generated when the CPU resource usage exceeds the preset threshold value.
- Disk Usage - *Disk* — This alarm is generated when the disk usage exceeds the threshold.
- Memory (Swap) Usage - *Mem* — This alarm is generated when the memory swap usage exceeds the threshold.
- Unprocessed Files - *UnprocFiles* — This alarm is generated when the count of (HTTP-EDR/EDR/CF-EDR) files pending for getting parsed (in their respective directories), exceeds the threshold value.
- Erroneous Files - *ErrFiles* — This alarm is generated whenever the count of invalid files exceeds the threshold value. The file is considered as invalid either due to missing headers or the file being corrupted.
- Erroneous Records - *ErrRecords* — This alarm is generated when the number of erroneous records breaches the threshold. The EDR records are considered as erroneous when any of the fields are missing in the EDR or when an invalid data is present in a particular field.

In addition to this, MUR also supports *AppStatus* and *TaskLag* event identifiers; however, these are NOT configurable.

- Application Status - *AppStatus* — This alarm is generated when the MUR application is started or stopped.

  Important: Please note that the alarms are sent when Scheduling server/Apache server is started or stopped. However, in the case of Postgres server, alarms are sent only when it is started.

- Task Lag - *TaskLag* — This alarm is generated when a particular script like normalization/aggregation takes more time than expected to complete the job.

  The following scripts have been added for the Task Lag alarms, which play an important role in parsing EDR/HTTP-EDR/CF-EDR. Each of these scripts handle a specific task which is either part of aggregation or normalization.

Script	Default Value of Tasklag Time (in sec/min)
Edr Normalization	300 (5 min)
Http Edr Normalization	300 (5 min)
CF Edr Normalization	300 (5 min)
Protocol Summary	1800 (30 min)
Port Aggregation	1800 (30 min)
Subscriber Aggregation (minutely)	1800 (30 min)
Subscriber Aggregation (hourly)	3600 (60 min)
Flow Count	1800 (30 min)

Script	Default Value of Tasklag Time (in sec/min)
Http Host Aggregation (minutely)	7200 (120 min)
Http Content Summary	7200 (120 min)
Http Host Aggregation (hourly)	7200 (120 min)

Important: Please note that the user does not have the privilege to change these timings.

Note that these alarms (Unprocessed, Error Files, Error Records and TaskLag) can be triggered only for EDR, HTTP-EDR and CF-EDR files, and not for the bulkstats files.

Important: During a fresh installation of MUR, please note that there will no SNMP configurations available.

Important: Users with administrative privilege can only manage this configuration.

Important: The change in the configuration for enabling / disabling the alarm generation feature does not require a restart of the MUR application.

MUR also supports generation of KPI alarms through the GUI. KPI parser calculates the values of KPIs for which the alarms are configured through the GUI. The KPI parser uses the information stored by bulkstat parser in the database for KPI calculations and for sending alarms. This avoids reparsing of the same file and redundant connections to the DB.

KPI parser generates alarms only when the alarm functionality is enabled for MUR. The details of KPI alarms which are successfully sent can be seen through **KPI Alarms Log** under the **System** menu. For details on the log, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

Important: Prior to configuring KPI alarms, you must ensure that the gateways and bulkstat schemas are configured and the bulkstats data are available.

For information on configuring the SNMP parameters, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

For information on the SNMP traps and thresholds supported for MUR, see the *Mobility Unified Reporting System MIB* chapter of the *SNMP MIB Reference*.

Chapter 3
Managing Mobility Unified Reporting System Installation

This chapter describes how to install, upgrade, and uninstall the MUR application.

The following topics are explained in this chapter:

- Installing MUR
- Upgrading MUR
- Uninstalling MUR

Important: The procedures for installation, upgrade, and uninstallation of MUR and RDP remain the same.

Important: Please note that the terminologies “starbi”, “inPilot” and “mur” used throughout this guide mean the same.

Installing MUR

This section provides instructions on how to install the MUR application.

Important: Make sure that your system meets the minimum requirements as indicated in the *MUR System Requirements* section in the *MUR Overview* chapter of this guide.

The following MUR components are installed by MUR installer.

- For Solaris platform
    - Apache v2.2.11 with mod_python v3.3.1
    - Python v2.6.4
    - Postgres v 8.2.0
    - Django v1.0.2
    - JRE v1.6.0_12
    - Quartz Scheduler v1.6.4
- For RHEL platform
    - Apache v2.2.11 with mod_python v3.3.1
    - Python v2.6.1
    - Postgres v 8.3.4
    - Django v1.0.2
    - JRE v1.5.0_11
    - Quartz Scheduler v1.6.4

Important: In RHEL-based deployment of MUR, L-ESS is NOT required as the ECS module can be configured to push the xDRs directly to the MUR reporting server. Push from ASR chassis is the Cisco recommended deployment model. Currently L-ESS is supported only on Solaris platforms. For information on the L-ESS installation instructions, refer to the *ESS Installation and Administration Guide*. Existing deployments where L-ESS is installed, to pull EDRs from the chassis, may continue with their deployment model in the 12.0 version of MUR Software Release and later.

Important: It is recommended that you first install the master MUR before proceeding with the RDP installation.

Setting the Database Environment Strings

Prior to installing the MUR components onto the server hardware, there are numerous system environment configuration settings that should be configured. While PostgreSQL will be installed during the installation procedure, these settings must be configured manually.

WARNING: Failure to configure these settings may cause data loss and will minimally cause errors in the operation.

Settings for Solaris

Add the following values to system file in the */etc/system* directory if they are not present and restart the system before continuing with the installation of MUR components.

```
set msgsys:msginfo_msgmnb=65536

set msgsys:msginfo_msgtql=1024

set shmsys:shminfo_shmmax=10737418240

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=270
```

Settings for RHEL

Add the following values to system file in the */etc/sysctl.conf* if they are not present and restart the system before continuing with the installation of MUR components.

```
kernel.shmmax=10737418240

kernel.shmall=4294967296
```

Pre-installation Checks

Ensure the following checks are made before installing the MUR application.

Important: Please note that L-ESS is required ONLY for a Solaris-based deployment of MUR. In the case of RHEL-based deployment of MUR, the ECS module is configured to push the xDRs directly from the chassis to the MUR reporting server via SFTP.

Step 1 The recommended filesystem for installation is ZFS. If Solaris-based installation is performed on any other filesystem, a warning message appears indicating the recommended filesystem.

Important: Please note that the ZFS related recommendations mentioned throughout this guide are specific to SOLARIS ONLY and NOT for RHEL.

Step 2 MUR must be installed as a **root** user on the system. Installation with other user privileges is not recommended.

Step 3 Make sure no other Apache web server is running on the port being used for installation (default port is 8080). If it is, stop it before proceeding with the installation or provide a different port for Apache server. Check if an application is running on a given port by entering the following command:

netstat -an | grep <*port number*>

Step 4 Make sure no other Postgres server is running on the port being used for installation (default port is 5432). If it is, stop it before proceeding with the installation or provide a different port for Postgres server. Check if an application is running on a given port by entering the following command:

netstat -an | grep <*port number*>

Step 5 Make sure no other application/process is running on the port being used for pgBouncer (default 'Postgres port + 1'). If it is, stop it before proceeding with the installation or provide a different port for Postgres server so that the installer finds two consecutive ports free (one for Postgres and the other one for pgBouncer). Check if an application is running on a given port by entering the following command:

netstat -an | grep <*port number*>

Step 6 Make sure no other server is running on the port being used for installation for XML-RPC (default port is 9999). If it is, stop it before proceeding with the installation or provide a different port for XML-RPC server. Check if an application is running on a given port by entering the following command:

netstat -an | grep <*port number*>

Step 7 MUR installation will ask for the Administrator login and Administrator Primary Group. Administrator login is the OS level administrator of MUR who will own the MUR installation. Administrator Primary Group is the user group of MUR to allow the interaction with external entities like L-ESS.

Step 8 If the Administrator login provided during MUR installation/upgrade already exists, ensure that it is not an already logged in user.

Step 9 L-ESS must be stopped before starting MUR installation / upgrade.

Step 10 If the L-ESS is installed as a **root** user, the ownership of L-ESS installation should be changed from **root** to **non-root** user. This new user must be added to MUR Group. For example, if L-ESS is initially running as **root** and new user created is *essadmin*, then perform the following sequence of operations.

Step a.....Stop L-ESS.

Step b.....Add the user *essadmin* to MUR group by entering the following command as **root** user - **usermod -G <MUR Group> essadmin**

Step c.....Verify whether the user is added correctly to MUR group using the command **groups essadmin**

Step d.....Change the ownership of L-ESS installation to this new user using the following command - **chown -R essadmin <LESS installation directory>**

Step e.....Login as *essadmin* with the command **su essadmin**

Step f .....Start L-ESS again.

Step 11 If the L-ESS is installed as a **non-root** user say *essadmin*, this user should be added to MUR Group.

Step a.....Stop L-ESS

Step b ..... Add the user *essadmin* to MUR group by running the following command as **root**-
```
usermod -G <MUR Group> essadmin
```

Step c..... Log off and relogin again as *essadmin* for the group addition to come into effect.

Step d ..... Start the L-ESS application to continue pulling the EDR files from chassis and forwarding it to MUR.

Step 12 Perform the following steps only if the user wants to push EDR/UDR files from gateway to MUR server using SFTP mechanism. Otherwise, skip this step.

Step a..... Change to the */etc/ssh* directory.

Step b ..... Open *sshd_config file* from the directory using *vi* editor (or any other editor) and observe the default values for the following variables:

PasswordAuthentication

PAMAuthenticationViaKBDInt (Applicable ONLY for SOLARIS)

UsePAM (Applicable ONLY for RHEL)

Step c..... Change the default values for the following variables as indicated here.

PasswordAuthentication = *yes*

PAMAuthenticationViaKBDInt = *no* (Applicable ONLY for SOLARIS)

UsePAM = *no* (Applicable ONLY for RHEL)

Step d ..... After updating restart SSH daemon using the following command:

In the case of SOLARIS:

```
svcadm restart ssh
```

Important: Please note that the above command can be executed only in Solaris 10 environment.

In the case of RHEL:

```
service sshd restart
```

Step 13 The recommended user/group settings for MUR are:

- NIS-USER<->NIS-GROUP
- NON-NIS-USER<->NON-NIS-GROUP

The NIS users should always be associated with NIS Groups. The non NIS users should be associated with Non NIS groups. Also, it is recommended to have separate non NIS users for MUR installation.

MUR Installation

The MUR installation files are distributed as a single compressed file.

Important: In the MUR Software Releases prior to 11.0.100 build, this installation file is distributed with a **.tar.gz** extension. In the MUR Software Release 11.0.100 and later, this file is distributed in zip format.

Important: The MUR application currently supports UCS Linux platform and Solaris-Sparc/Solaris-x86 platform. The installable tar file names help in identifying the platform. For example, mur.x.x.xx_rhel_x86.zip indicates that this file is for RHEL platform. Similarly, mur.x.x.xx_solaris_sparc.zip indicates that this file is for Solaris-Sparc platform.

For information on downloading the appropriate MUR package for your requirements, contact your sales representative.

The MUR application and its components can be installed using one of the following two methods.

- Installing MUR Using Scriptbased Installer
- Installing MUR Using GUIConsole based Installer

Important: Please note that the terminologies “starbi”, “inPilot” and “mur” used throughout this guide mean the same.

Installing MUR Using Script-based Installer

Important: Please note that the legacy script-based installer is not supported in the MUR Software Release 11.0.100 and later.

Important: To perform the installation procedure explained in this section, you must be logged into the server as a **root** user.

Important: Fresh installation for backup recovery purpose should be installed on the same path where last backup is stored and also should have the same IP address and port configuration if the MUR is deployed in distributed mode. Make sure that the existing older installation is either removed or moved to a different directory because the metadata recovered from previously installed MUR will have all references as per older installation e.g. archive path, SFTP details, etc.

After copying the installation file to the server, use the following procedure to install the MUR application.

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

Step 2 Unzip the file by entering the following command:

```
tar -xvf mur_x.x.xx.tar.gz
```

x.x.xx is the version of the MUR installation file.

> ***Important:*** After un-zipping the installation file, set the permission of .tar file to 700 using the following command and then continue with the installation process. **`- chmod 700 starbi_<release no>_<platform>.tar`**

Decompressing the installation file results in the following files:

- *README*: A text file containing information pertaining to the release.
- *install_starbi*: A script to install the MUR application.
- *starbi.tar*: A compressed file containing all the application files required for MUR installation.

- *inst*: A GUI/Console based installer to install the MUR application.
- *In_Pilot_Installer.bin*: The executable used by *inst* to install MUR application.

Step 3 Execute the script by entering the following command:

```
./inst
```

> ***Important:*** The installation script checks the disk space in the system. If the available disk space is lesser, then the script will give an error and abort the installation process.

Step 4 Respond to the on-screen prompts with the help of inputs given in the following table and configure various parameters as required. The following table describes the installation parameters for master MUR.

Parameter	Description	Default Value
System Environment Variable Prompt		
	This dialog or script asks the user to check the variable values in system file. If one or more entries are missing, update the system file and restart the system to re-run installer. For more information, refer to the Setting the Database Environment Strings section.	N/A
MUR Installation		
Want to proceed	Type **(y)es** to proceed with the installation of MUR application.	yes
MUR Installation Directory	Type the directory on the server in which the MUR application is to be installed.	<current_directory>
The following warning appears if the user performs installation on non-ZFS (UFS) partition path. ZFS is the recommended filesystem for installation. `Warning! Path provided lies in ufs filesystem.` `Recommended filesystem for mur is zfs.` `Do you still want to continue? [no] ?` Type **(y)es** or **(n)o** to proceed with the MUR installation. ***Important:*** Please note that the ZFS/UFS related warning messages are specific to SOLARIS ONLY and NOT for RHEL.		no

Parameter	Description	Default Value
Do you want to install MASTER or RDP	Type **i** or press **Enter** to install the MUR application. To install RDP type **r**. Refer to the following table for the parameters associated with the RDP installation. ***Important:*** Make sure that you first install the master MUR and then proceed with the RDP installation.	MASTER
Administrator login	Type an administrator name for the Operating System (OS) level administrator of MUR. ***Important:*** Please note that you should not login as a **root** user. ***Important:*** The Administrator user created should be manually activated with a password once the MUR installation is complete. This can be done by entering the following command as **root** user: **`passwd`** *`<adminusername>`* Upon executing this command, the user will be asked to enter a suitable administrator password.	muradmin
Administrator uid	Type the Administrator User ID for the MUR Administrator login. ***Important:*** This input will be asked only if the Administrator login name provided does not exist.	100014
Administrator Primary Group	Type the Primary Group name for the Administrator. ***Important:*** If the Administrator login name provided already exists, the Primary Group of this login will be considered as the **MUR User Group**. Otherwise, the user will be asked to enter the Primary Group information.	murgroup
Postgres Login	This is a read-only parameter. The Postgres login name will be the same as the Administrator login name provided earlier.	muradmin
Postgres Password	Type the password for accessing the PostgreSQL database.	N/A

Parameter	Description	Default Value
Postgres Port	Type the port number over which PostgreSQL communication will occur with MUR. ***Important:*** Ensure that no other application/process is running on configured port as well as on next consecutive port (as this port will be used for pgBouncer).	5432
Postgres Data Directory	Type the directory path where the postgres data resides.	*<MUR_Installation_Directory>*/starbi/postgres/data
Apache Port	Type the port number over which Apache web server communication will occur with MUR. ***Important:*** Be sure no other Apache web server is running on port which you are using while installation. If the port is being used, abort the installation. **For RHEL:** Apache port provided should be > 1024. RHEL does not allow port 80 to be used by non-root users. However, Apache web server requests made on Port 80 can be redirected to a port >1024 defined by the operator, with the following two commands. For example, to redirect requests made on port 80 to port 8080: **iptables -t** *nat* **-A** *PREROUTING* **-p** *tcp* **--dport** *80* **-i** *eth0* **-j** *REDIRECT* **--to-port** *8080* **iptables -t** *nat* **-A** *OUTPUT* **-p** *tcp* **--d** *127.0.0.1***--dport** *80* **-j** *REDIRECT* **--to-port** *8080* **For Solaris:** For using the Apache port < 1024, run the following command as **root** user once the installation is complete, and restart the Apache server. **usermod -K defaultpriv=basic,net_privaddr** *<MUR admin user>* For example: **usermod -K defaultpriv=basic,net_privaddr muradmin** ***Important:*** This poses a major security concern as it will allow *muradmin* to use all standard ports < 1024.	8080

Parameter	Description	Default Value
Available Port Range for MUR Components (200 Ports)	Type the port number in the start port text area. Note that the end port text area is a READ-ONLY field. End port number will be populated automatically based on the start port number. If any of the port/ports in the specified range is/are not available, then the installer throws error and prompts the user to enter a new start port number.	9001 - 9200
Archive Directory Path	Type the directory path for archiving parsed files.	<*mur_install_dir*>/archive
The following warning appears if the user performs installation on non-ZFS (UFS) partition path. ZFS is the recommended filesystem for installation. `Warning! Path provided lies in ufs filesystem.` `Recommended filesystem for mur is zfs.` `Do you still want to continue? [no] ?` Type **(y)es** or **(n)o** to proceed with the MUR installation. ***Important:*** Please note that the ZFS/UFS related warning messages are specific to SOLARIS ONLY and NOT for RHEL.		no
MUR Configuration Confirmation		
Proceed with installation	Type **(y)es** to proceed with MUR installation.	yes
Do you want to start the MUR components	Type **(y)es** to start the MUR components immediately after installation.	yes

The following table describes the installation parameters for RDP.

Parameter	Description	Default Value

Parameter	Description	Default Value
Administrator login	Type an administrator name for the Operating System (OS) level administrator of RDP. ***Important:*** Please note that you should not login as a **root** user. ***Important:*** The Administrator user created should be manually activated with a password once the MUR installation is complete. This can be done by entering the following command as **root** user: **`passwd`** *<adminusername>* Upon executing this command, the user will be asked to enter a suitable administrator password.	muradmin
Administrator uid	Type the Administrator User ID for the MUR Administrator login. ***Important:*** This input will be asked only if the Administrator login name provided does not exist.	100014
Administrator Primary Group	Type the Primary Group name for the Administrator. ***Important:*** If the Administrator login name provided already exists, the Primary Group of this login will be considered as the MUR User Group. Otherwise, the user will be asked to enter the Primary Group information.	murgroup
Postgres Login	This is a read-only parameter. The Postgres login name will be the same as the Administrator login name provided earlier.	muradmin
Postgres Password	Type the password for the Postgres database administration.	N/A
Postgres Port	Type the port number over which PostgreSQL communication will occur with RDP. ***Important:*** Ensure that no other application/process is running on configured port as well as on next consecutive port (as this port will be used for pgBouncer).	5432

Parameter	Description	Default Value
Apache Port	Type the port number over which Apache web server communication will occur with RDP. **Important:** Be sure no other Apache web server is running on port which you are using while installation. If the port is being used, abort the installation. **For RHEL:** For RHEL, Apache port provided should be > 1024. RHEL does not allow port 80 to be used by non-root users. However, Apache Web server requests made on port 80 can be redirected to a port >1024 defined by the operator, with the following two commands. For example, to redirect requests made on port 80 to port 8080: **iptables -t** *nat* **-A** *PREROUTING* **-p** *tcp* **--dport** *80* **-i** *eth0* **-j** *REDIRECT* **--to-port** *8080* **iptables -t** *nat* **-A***OUTPUT* **-p** *tcp* **-d** *127.0.0.1* **--dport** *80* **-j** *REDIRECT* **--to-port** *8080* **For Solaris:** For using the Apache port < 1024, run the following command as **root** user once the installation is complete, and restart the Apache server. **usermod -K defaultpriv=basic,net_privaddr** *<MUR admin user>* For example: **usermod -K defaultpriv=basic,net_privaddr muradmin** **Important:** This poses a major security concern as it will allow *muradmin* to use all standard ports < 1024.	8080
Available Port Range for MUR Components (200 Ports)	Type the port number in the start port text area. Note that the end port text area is a READ-ONLY field. End port number will be populated automatically based on the start port number. If any of the port/ports in the specified range is/are not available, then the installer throws error and prompts the user to enter a new start port number.	9001 - 9200
Archive Directory	Type the directory path for archiving parsed files.	*<rdp_install_dir>*/archive
The following warning appears if the user performs installation on non-ZFS (UFS) partition path. ZFS is the recommended filesystem for installation. `Warning! Path provided lies in ufs filesystem.` `Recommended filesystem for mur is zfs.` `Do you still want to continue? [no] ?` Type **(y)es** or **(n)o** to proceed with the RDP installation. **Important:** Please note that the ZFS/UFS related warning messages are specific to SOLARIS ONLY and NOT for RHEL.		no

Parameter	Description	Default Value
RDP Configuration Confirmation		
Proceed with installation	Type **(y)es** to proceed with RDP installation.	yes
Do you want to start the RDP components	Type **(y)es** to start the RDP components immediately after installation.	yes

After you have provided the inputs, the installation script starts the MUR components and you receive a message indicating that MUR installation is completed.

When the MUR installation is complete, see the *Cisco Mobility Unified Reporting System Online Help* documentation for information on how to access and use the GUI.

Installing MUR Using GUI/Console based Installer

Important: To perform the installation procedure explained in this section, you must be logged into the server as a **root** user.

Important: Fresh installation for backup recovery purpose should be installed on the same path where last backup is stored and also should have the same IP address and port configuration if the MUR is deployed in distributed mode. Make sure that the existing older installation is either removed or moved to a different directory because the metadata recovered from previously installed MUR will have all references as per older installation e.g. archive path, SFTP details, etc.

Important: In the MUR Software Releases prior to 11.0.100 build, this installation file is distributed with a **.tar.gz** extension. In the MUR Software Release 11.0.100 and later, this file is distributed in zip format.

Follow the instructions below to install MUR using the GUI/Console based installation wizard.

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

Step 2 Unzip the file by entering the following command:

`unzip mur.`*`x.x.xx_os_arch`***`.zip`**

x.x.xx is the version of the MUR installation file.

`os` indicates the Operating System on which the MUR application is running. It can be either RHEL or Solaris.

`arch` indicates the architecture either Sparc or x86.

Important: To unzip the **.gz** package file, use **`tar -xvf <file_name>`** command.

Decompressing the installation file results in the following files:

- *inst*: A GUI/Console based installer to install the MUR application.
- *setup.bin*: The executable used by *inst* to install MUR application.

Step 3 Execute the script by entering the following command:

`./inst [MODE]`

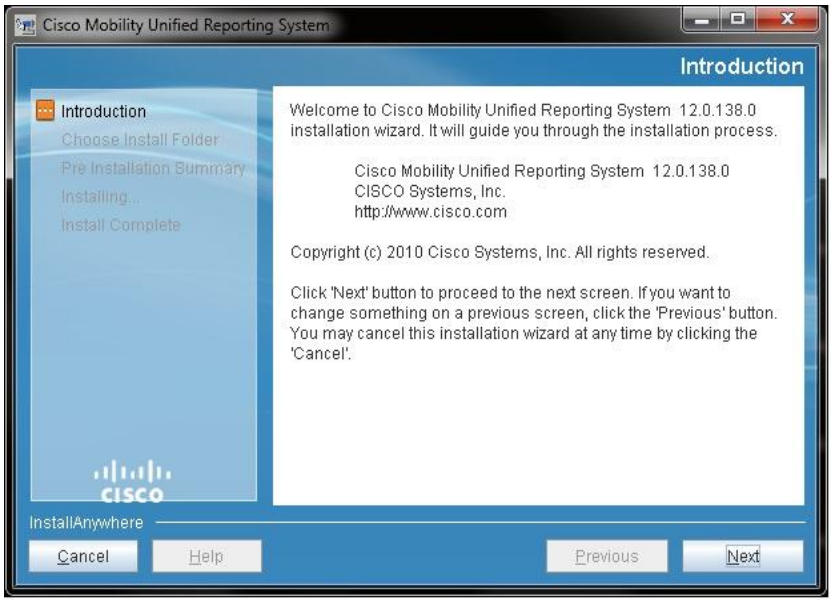
where [MODE] is optional.

Two installation modes are supported namely:

- gui
- console

The command ‘inst/uninst -help' provides usage of the scripts. This script installs the Apache, Postgres and Scheduling servers functionality. The display must be set for running in GUI mode, else the installation will run in Console mode.

The following MUR Installer dialog appears displaying the MUR version getting installed.



Step 4 Click **Next** to proceed.

Step 5 Respond to the on-screen prompts with the help of inputs given in the following table and configure various parameters as required.

Parameter	Description	Default Value
PostgreSQL System Settings screen		
	This dialog asks the user to check the variable values in system file. If one or more entries are missing, click **Cancel** to update the system file and restart the system to re-run installer. For more information, refer to the Setting the Database Environment Strings section.	N/A
MUR Installation Directory screen		
Enter MUR Directory Path	Enter the base directory path where MUR is to be installed. Click **Browse** to change the installation path.	*<current_directory>*

Parameter	Description	Default Value
A Component Type screen appears showing the components for installation. This screen allows you to select either Master MUR or RDP for installation. ***Important:*** Make sure that you first install the master MUR and then proceed with the RDP installation.		
MUR Administrator and Group Configuration screen		
Administrator Login	Enter an administrator name for the Operating System (OS) level administrator of MUR. ***Important:*** Please note that you should not login as a **root** user. ***Important:*** The Administrator user created should be manually activated with a password once the MUR installation is complete. This can be done by entering the following command as **root** user: **`passwd`** *`<adminusername>`* Upon executing this command, the user will be asked to enter a suitable administrator password.	muradmin
Administrator User ID	Type the Administrator User ID for the MUR Administrator login. ***Important:*** This input will be asked only if the Administrator login name provided does not exist.	100014
Administrator Primary Group	Type the Primary Group name for the Administrator. ***Important:*** If the Administrator login name provided already exists, the Primary Group of this login will be considered as the **MUR User Group**. Otherwise, the user will be asked to enter the Primary Group information.	murgroup
PostgreSQL Server Configuration screen		
Postgres Login	This is a read-only parameter. The Postgres login name will be the same as the Administrator login name provided earlier.	muradmin
Postgres password	Enter the password for the Postgres database administration.	N/A

Parameter	Description	Default Value
Postgres Port	Enter the port number on which PostgreSQL communication will be running. ***Important:*** Ensure that no other application/process is running on configured port as well as on next consecutive port (as this port will be used for pgBouncer).	5432
Enter data directory path	Enter the data directory path of postgres being used. Click **Browse** to change the installation path.	<*mur_install_dir*>/starbi/postgres/data
MUR Port Configuration screen		
Apache Port	Type the port number over which Apache web server communication will occur with MUR. ***Important:*** Ensure that no other Apache web server is running on the port being used for installation. If the port is being used, abort the installation. **For RHEL:** For RHEL, Apache port provided should be > 1024. RHEL does not allow port 80 to be used by non-root users. However, Apache Web server requests made on port 80 can be redirected to a port >1024 defined by the operator, with the following two commands. For example, to redirect requests made on port 80 to port 8080: **iptables -t** *nat* **-A** *PREROUTING* **-p** *tcp* **--dport** *80* **-i** *eth0* **-j** *REDIRECT* **--to-port** *8080* **iptables -t** *nat* **-A***OUTPUT* **-p** *tcp* **-d** *127.0.0.1* **--dport** *80* **-j** *REDIRECT* **--to-port** *8080* **For Solaris:** For using the Apache port < 1024, run the following command as **root** user once the installation is complete, and restart the Apache server. **usermod -K defaultpriv=basic,net_privaddr** *<MUR admin user>* For example: **usermod -K defaultpriv=basic,net_privaddr muradmin** ***Important:*** This poses a major security concern as it will allow *muradmin* to use all standard ports < 1024.	8080
Available Port Range for MUR Components (200 Ports)	Type the port number in the start port text area. Note that the end port text area is a READ-ONLY field. End port number will be populated automatically based on the start port number. If any of the port/ports in the specified range is/are not available, then the installer throws error and prompts the user to enter a new start port number.	9001 - 9200

Parameter	Description	Default Value
MUR Archive Directory Configuration screen		
Enter archive directory path	Enter the directory path for archiving parsed files. Click **Browse** to change the installation path.	<*MUR_install_dir*>/archive
Pre-installation Summary screen		
The pre-installation screen displays the product name, install location, other product configurations, and disk space information before installing the product. Click **Cancel** to stop installation or **Install** to continue installation.		
Installing MUR screen		
The screen shows all the contents being loaded on the machine during installation. Click **Cancel** to stop installation.		
MUR Server Startup screen		
Start All Servers After Installation	Select the option to start all servers after installation. Click **Next** to proceed.	Yes
Install Complete screen		
	The screen shows whether installation is successful or failed. Click **Done** to quit the installer.	N/A

When the MUR installation is complete, see the *Cisco Mobility Unified Reporting System Online Help* documentation for information on how to access and use the GUI.

Confirming Successful Installation

Verify that the MUR application is running and accessible by entering the following URL in your Web browser:

`http://<MUR_installation server name or IP address>:<apache port>`

For information on logon details, refer to the *Launching the MUR GUI* section in the *Mobility Unified Reporting System Administration and Management* chapter of this guide.

For information on using the MUR GUI, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

Upgrading MUR

This section provides instructions on how to upgrade the installed MUR application.

Important: In RHEL-based deployments, L-ESS is NOT required as the Enhanced Charging Services (ECS) module can be configured to push the xDRs directly to the MUR reporting server. Push from ASR chassis is the Cisco recommended deployment model. Currently L-ESS is supported only on Solaris platforms. For information on the L-ESS installation instructions, refer to the *ESS Installation and Administration Guide*. Existing deployments where L-ESS is installed, to pull EDRs from the chassis, may continue with their deployment model in the 12.0 version of MUR Software Release and later.

Important: To perform the upgrade procedure explained in this section, you must be logged into the server as a **root** user.

The upgrade procedure ensures that the database content is retained in the new installation. It also ensures that if there are any pending files to be processed in the old installation, then those file are also made available in the new installation.

Important: If MUR is being upgraded from a version in which backup and purging features are not available, to a version in which backup and purging features are supported, then it is recommended that you enable backup feature and take one complete successful snapshot of backup before enabling purging feature. If the backup feature is disabled then enabling purging will cause removal of data without waiting for it to be backed up. If the backup is being taken for the first time after upgrade, then it may take considerable time for first backup.

Important: Before performing the upgrade process, ensure that the browser cache is cleared.

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

Important: If the previous installation is MUR then the installation script will cause upgrading the software to MUR and if the previously installed component is RDP then the script will cause upgrading to RDP.

When upgrading to MUR software version 12.2, file parsing configurations are NOT synced automatically at all RDPs. As a result, EDR file parsing does not happen at RDPs.

To overcome this, peform the following steps in the MUR GUI:

1. After the upgrade, manually attach appropriate RDPs to all relevant gateways.
    - Create appropriate RDP regions through the **System** menu.
    - Attach all RDPs to their respective regions through **Edit RDP** page viewed by clicking **RDP** from **Admin** tab.
    - Attach appropriate gateways to their corresponding RDPs and regions through **Edit Gateway** page viewed by clicking **GATEWAYS** from **Admin** tab.
2. Navigate to **System** > **File-Parsing Configs** menu and then manually save the file parsing configurations for all the gateways which are attached to RDPs.

The MUR upgrade process is carried out in two steps:

1. Online Upgrade
2. Offline Upgrade

The online upgrade is the conventional upgrade process. It will upgrade only last 7 days of available data i.e. it will get the latest date for which data is available and upgrade the last 7 days data only from that date.

Once the online upgrade is complete, offline upgrade starts in the background and it will upgrade all the remaining data older than last 7 days.

During the offline upgrade, there is a possibility of data outage. So, the reports older than last 7 days might be inaccessible from GUI during this period. Once the offline upgrade is over, these reports will be visible again.

Please note the following key points:

- Once MUR is upgraded and if any schemas support additional counter then you should reconfigure schema for that gateway.
- After upgrade is over, the previous data and the schemas displayed earlier for the gateway will be shown on the GUI.
- If you want to perform schema configuration for the gateways which were added prior to upgradation, then you should configure the schemas through the GUI by accessing Bulkstat Schema Configuration screen and disable the earlier file format used on the gateway.

The following steps describe how to upgrade the MUR application:

Step 1 Stop the L-ESS by running the following command from the *<LESS_install_dir>/ess* directory:

```
./serv stop
```

Step 2 Stop the MUR application using the following command from the *<MUR_install_dir>/starbi/bin* directory:

```
./serv stop
```

Important: For all MUR software versions 9.0.16 and later, use the **`serv stop`** command.

or

```
./shutdown.sh
```

Important: For all MUR software versions 9.0.15 and lower, use the **`shutdown`** command.

Then, check the status of processes using the following command:

```
./serv status
```

Important: For all MUR software versions 9.0.16 and later, use the **`serv status`** command.

or

```
./status.sh
```

Important: For all MUR software versions 9.0.15 and lower, use the **`status`** command.

Important: Make sure that none of the processes is running.

Step 3 Install the new release of MUR.

MUR is upgradable from:

- Earlier script installer based version to newer script installer based version
- Earlier script installer based version to GUI/Console installer based version
- Earlier GUI/Console installer based version to subsequent GUI/Console installer based version

For instructions on different MUR installers, refer to the MUR Installation section.

In case of the first two upgrade options mentioned above, make sure that you enter the old installation path (<install_dir>) for upgrade when prompted for the 'MUR Installation directory'. In case of the third upgrade option, it automatically detects the old installation path through registry information. The installation automatically detects earlier setup and reads required configuration for Apache, Postgres and RPC port, etc. You will be prompted with a confirmation message before proceeding with the upgrade process.

After upgrade, the log files are generated at */starbi/logs/* directory.

Important: The installation script will check if the Administrator user and Primary Group information is already present in database. If it does not exist, it will ask the user to enter this information and then continue with the upgrade.

Step 4 After the installation is done, start all the MUR related processes using the following command from the *<MUR_install_dir>/star/bin* directory:

```
./serv start
```

Then, start the L-ESS using the following command from the *<LESS_install_dir>/ess* directory:

```
./serv start
```

Step 5 Modify the L-ESS configuration or HDD configuration to reflect the changes in the MUR installation path.

Step 6 Restart the EDR file generation or HDD file push as needed.

Important: The RDP should be upgraded manually. If the version of the RDP is not compatible with the MUR, then MUR may ignore the data sent by RDP. Thus, RDP should always be upgraded if it is not in sync with the MUR. For change in mode from RDP to MUR or vice-versa, re-installation is required.

Uninstalling MUR

This section provides instructions on how to uninstall the MUR application.

The MUR application and its components can be uninstalled using one of the following two methods:

- Uninstallation Using Script-based Uninstaller
- Uninstallation Using GUIConsolebased Uninstaller

Important: The Administrator user and Primary Group configured during installation / upgrade will not be deleted during uninstallation. These have to be deleted manually by entering the following commands as **root** user: **`userdel`** *<ADMINUSER>* and **`groupdel`** *<ADMINGROUP>*

Uninstallation Using Script-based Uninstaller

Important: Please note that the legacy script-based uninstaller is not supported in the MUR Software Release 11.0.100 and later.

Important: To perform the uninstallation procedure explained in this section, you must be logged into the server as a **root** user.

This method must be used if installation has been done using **install_starbi** script.

Execute the script by entering the following command:

`./uninstall_starbi`

Uninstallation Using GUI/Console-based Uninstaller

This method must be used if installation has been done using GUI/Console based installer (using **inst**).

Important: To perform the uninstallation procedure explained in this section, you must be logged into the server as a **root** user.

Step 1 Change to the *<mur_install_dir>/starbi* directory and enter the following command:

`./uninst` *`[MODE]`*

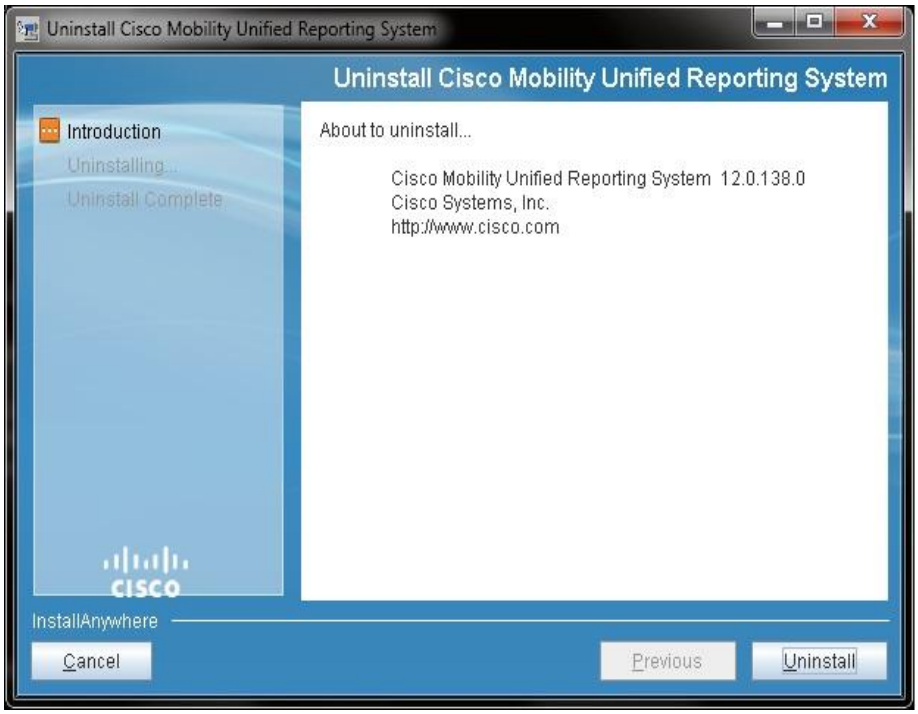
where [MODE] is optional.

Two modes are supported namely:

- gui
- console

The display must be set for running in GUI mode, else the uninstallation will run in Console mode.

The following MUR Uninstaller dialog appears.



Step 2 Click **Uninstall** to proceed.

This uninstall script stops all the servers if it is running and all the data is wiped off.

Important: The uninstall script does not cleanup the archive directory.

Chapter 4
Mobility Unified Reporting System Administration and Management

This chapter provides information on administering and managing the MUR application.

This chapter describes the following topics:

- Launching the MUR GUI
- Administration
- Operations and Management
- Troubleshooting MUR

Important: Please note that the terminologies “starbi”, “inPilot” and “mur” used throughout this guide mean the same.

Launching the MUR GUI

It is recommended to use either Internet Explorer (v 7.0+) or Mozilla Firefox (v 3.0.10+) browser for launching the MUR interface.

Note that:

- No additional plug-in is required.
- The javascript is enabled by default on the intended browser.
- Suggested screen resolution is 1024 x 768 and above.

To launch the MUR interface:

1. In a Web browser, enter the following URL:

   `http://<MUR-server-hostname or IP address>:<apache port>`

   For example, http://10.4.5.2:8080

2. Enter your user name and password, and then click **Log In**. The user name must be an alpha and/or numeric string of 3 through 16 characters in length. The only special character that a user name can include is underscore (_).

   Important: At first log on, the users are expected to enter *admin* as the input for the **Username** and **Password** fields.

   The password must meet the following criteria:

   - Must be a minimum of 8 characters long and a maximum of 32 characters long
   - Must not be a repeat or reverse of the associated user name
   - Must not be more than 3 of the same characters used consecutively
   - Must contain at least 3 of the following combinations:
     - English upper case characters (A through Z)
     - English lower case characters (a through z)
     - Numerical (0 through 9)
     - Special characters (such as _, ., !, @, $, *, =, -, ?, etc)

The only account created after the initial set-up is *admin* / *admin* and it has Administrator privileges.

Once logged-in, the user's Dashboard will be displayed with reports if already configured (the displayed reports are specific to each user account).

Important: At first log on, the users will see an empty Dashboard. The necessary data should be populated and required parameters should be configured for report generation.

The user name is always displayed on the right-up corner of the page until the user logs out of the application.

Administration

This section provides information on how to administer and manage the MUR application.

Managing User Accounts

The MUR application provides two levels of access privileges:

- Administrator: Users in this group have the following privileges:
    - Create, edit, and delete other user accounts
    - Edit configuration settings
    - Activate, deactivate, and reset password for operator users
    - Generate and view reports
- Operator: Users in this group can:
    - Generate reports
    - View module-level reports available to them

Important: Only administrator with *admin* name can create user accounts.

Please note the following limitations with respect to user permissions and privileges:

- All MUR administrators have access to **USERS** and **GROUPS** menu in the **Admin** tab available on the MUR GUI.
- Administrator with *admin* user name will have the rights to modify and delete all the MUR users' accounts. Only users with *admin* user name can modify its own password. Only admin user will be able to delete any administrator or operator user accounts.
- Administrator other than users with *admin* user name will have rights to delete the MUR users except *admin* user and modify user accounts except their passwords.
- After modifying user role from Administrator to Operator and vice-versa, the user should alter the configuration on the GUI to lock/unlock the user account accordingly.

For more details, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

Managing Gateways

The MUR application supports configuring multiple gateways for which reports can be customized and generated. Gateways are the chassis from which EDR and bulkstat files are fetched to the reporting server.

Important: Users with administrative privilege can only add and manage gateways.

When a gateway is added through the GUI, a directory by the name of the gateway is created in the *<mur_install_dir>/starbi/server/data* directory.

The gateway directory structure looks like the following:

<data directory>

|

|--> <Gateway name>

|

|--> edr

The MUR application expects the EDR files in the directories that are created when adding the gateway.

The MUR application supports the distributed model to allow the deployment which enables network wide view or work load balancing. Newly introduced component, Remote Data Processor (RDP), plays the role of pre-processing the input files from gateways. One or more RDPs, installed separately on remote machines can be registered to a master MUR system and one RDP can process files from one or more gateways. The role of MUR system in such deployments is mostly for report generation, report viewing, RDP management and optionally data processing.

The RDP parses the raw data or EDR files from GGSNs and periodically forwards it to the registered master MUR application through SFTP for report generation. For information on how to configure the RDPs, see the *Mobility Unified Reporting System Online Help* documentation.

Important: The gateways can be added on Remote Data Processor (RDP). For adding gateway on particular RDP corresponding RDP's region should be selected. RDP region is available when RDP is added. For information on configuring the RDPs, see *Mobility Unified Reporting System Online Help* documentation.

In 12.0 and earlier releases, each of the registered RDPs were considered to be a new region. RDP region can be a child of the root of the MUR system (NOC) or can be the child of another region. However, all the gateways associated with a RDP will always be the children of RDP region.

Whenever an RDP is configured, internally MUR used to create corresponding region for the same. However, with the introduction of scalable MUR in 12.2 release, one gateway's files will be processed by two or multiple RDPs. In that case, RDP does not stand as a region. Hence, the reports would be required across all the RDPs under one particular region.

Important: Whenever an MUR is upgraded from an older version to 12.2, the logical regions for the MUR gets void and the user will not be able to see any gateways under the **DPI/Bulkstats/CF/KPI** tab. In this scenario, the user should add that gateway under NOC.

Managing Archive Directory

To use the Offline Subscriber Search feature seamlessly, you must organize the archive directory date-wise. For information on this feature, see the *Mobility Unified Reporting Online Help* documentation.

MUR organizes the archive directory such that the directory structure looks like the following:

<Archive Directory>

<Gateway Name>

<Reporting Name>

<Date YYYYMMDD>

<Archived Files>

<Other>

<Archived Files>

For the files that are not satisfying the required EDR file name format, MUR stores the files in the *Other* directory.

Configuring Logging

The MUR application facilitates logging to trace and debug problems identified within the reporting system.

Important: Users with administrative privilege can only manage logging.

Configuring Purging Feature

The MUR application supports purging any kind of aggregated data like half-hourly, daily, weekly, monthly, etc. This also supports purging of weekly summary table, monthly top N table, audit logs, etc. While configuring the purging feature, the MUR provides the flexibility to end-user to configure half-hourly, daily, weekly and monthly report viewing duration so that the historical reports can be viewed even at a lowest granularity level.

Important: It is recommended that you enable backup feature and take one complete successful snapshot of backup before enabling purging feature. If the backup feature is disabled then enabling purging will cause removal of data without waiting for it to be backed up.

Important: The backup snapshot can be identified as complete only if the snapshot directory of format *snapshot_<date>_<time stamp>_<version>*, created under configured backup path does not have the prefix *backup.prog*. The *backup.prog* prefix indicates that the backup is in progress.

MUR uses a python script, *purge_db.py*, to accomplish this task. For more information on the script, refer to the Using the Purging Script section.

Important: Users with administrative privileges can only manage the purging configuration.

Important: The purging configurations are recommended to be a one-time process and should not be changed frequently.

To configure data / file purging through the GUI, see the *Mobility Unified Reporting System Online Help* documentation.

Important: In case of distributed model of MUR, data purging can be done only at the master MUR and file purging can be performed at per RDP level.

Important: For the MUR software with version 10.0.72 and lesser, you must manually purge the archived files. For the MUR software version 10.0.72 and later, you can use the purging script to automate the process.

Configuring Backup Functionality

To avoid data loss due to hardware failure and/or software crash, MUR supports periodical backup and recovery of its database. The backup is actually the snapshot of data tables or meta data on the day when the backup is taken.

In case of hierarchical deployment, when backup feature is enabled, backup of RDP is also taken as per user configured period.

Backup of RDP contains only the metadata i.e. the configuration information and does not consume high disk space. Also this backup snapshot which is taken on RDP node is immediately transferred to Master MUR using SFTP.

The Master MUR moves the snapshot of RDP backup to the backup path configured on RDP. In short, RDP backup snapshot is also stored on user configured backup path.


Important: Please note that the backup and recovery processes are applicable only for MUR database and not for files that are archived.

Please consider the following points while taking backup of the master MUR database.

- Backup related configuration is available under **ADMIN** tab in Web-based MUR GUI.
- Configure the backup path on a separate disk than using the path where MUR is installed. This can be NFS or any other storage path. The File system on storage disk should support creating hard links to the files for performance benefits. For example: UFS, ZFS and NFS.
- MUR takes the snapshot as per the configured period. If the previous snapshot is available on backup path, data which was not modified between last backup and the current backup is copied directly from the previous snapshot. Thus it is recommended that the backup disk path should hold at least the recent snapshot. The disk size for backup path should be selected accordingly. Older snapshots can be archived or deleted regularly.
- If the backup flag is disabled, the purging of data will continue even if some data tables are pending for backup.
- The backup snapshot can be identified as complete only if the snapshot directory of format *snapshot_<date>_<time stamp>_<version>*, created under configured backup path does not have the prefix *backup.prog*. The *backup.prog* prefix indicates that the backup is in progress.
- If MUR is being upgraded from a version in which backup and purging features are not available, to a version in which backup and purging features are supported, then it is recommended that you enable backup feature and take one complete successful snapshot of backup before enabling purging feature. If the backup feature is disabled then enabling purging will cause removal of data without waiting for it to be backed up. If the backup is being taken for the first time after upgrade, then it may take considerable time for first backup.

Configuring Recovery Functionality

To recover the backed up data, use the snapshot recovery script that finds the latest available snapshot amongst all the snapshots under configured path. If you want to recover specific snapshot then move only that snapshot to some other path and provide this new path as a parameter to this script.


Important: In case of hierarchical deployment, recovery of master MUR and RDP should be done separately. After recovering and starting RDP, it will start serving the master to which it is attached.

Please note the following key points while recovering the database.

- The recovery of backed up tables is possible only during a fresh installation of MUR software. The fresh installation version should be same as the version for which snapshot is backed up.
- Fresh installation for recovery purpose should be installed on the same path where last backup is stored and also should have the same IP address and port configuration if the MUR is deployed in distributed mode. Make sure that the existing older installation is either removed or moved to a different directory because the metadata recovered from previously installed MUR will have all references as per older installation e.g. archive path, SFTP details, etc.
- The recovered data contains all the configurations as per older setup. Thus, any changes in the configuration of recovered setup, such as backup interval, etc requires reconfiguration explicitly.

The recovery script provides an option to specify if recovery of data is required for RDP.

For recovery of RDP, backed up snapshot should be copied on a local path or it should be available on path that is accessible to RDP.

For the master MUR, use the following command to recover the data:

`./recover.sh -path` *`<directory path containing data snapshots>`*

For RDP, use the following command to recover the data:

`./recover.sh -path` *`<directory path containing data snapshots>`* **`-r`** *`<RDP_Name>`*

The option **`-r`** *`<RDP_Name>`* denotes the name of RDP for which data should be recovered.

The snapshot of RDP is a tar file and not a directory as in the case of master MUR. The following is a sample of RDP backup tar file naming convention.

RDP_<RDP_Name>_snapshot_<Date>_<timestamp>_<version>.tar

Configuring Offline Mode

MUR can be used in "Offline Subscriber Search Only" mode. In this mode, MUR will not parse incoming EDR files, so no online reports will be generated. It will move the incoming EDR files to archive directory, so that you can avail "Offline Subscriber Search Reports" only. By default, this mode is turned OFF. To run MUR in Offline Mode, please see the configuration parameters OFFLINE_MODE and OFFLINE_SEARCH_PROCESS_COUNT in **Managing System Configurations** > **Config Parameters** in the *Mobility Unified Reporting System Online Help* documentation.

Operations and Management

This section provides information on the scripts that can be used to manage the MUR components and the reports.

Using the Maintenance Utility

A shell script utility called *serv* is included with MUR in the <*MUR_install_dir*>/*starbi/bin* directory.

This serv script can be used to manage the following MUR processes:

- Process Monitor (PSMON) Application
- Scheduling Server
- Postgres Server
- Apache Server
- Notif Server
- Parser Server
- Cache Server

This utility can report the status of the MUR processes on the system or it can be used to stop the MUR process.

Following are the options available with the serv script:

```
./serv { psmonitor | scheduler | postgres | apache | notif_server | parser |
cache_server } [ start | stop | status ]
```

Keyword	Description
psmonitor	This is an optional keyword used with the serv script. This represents the PSMON application. It starts/stops/checks the following MUR processes. • Postgres server • Apache server • Scheduling server • Notif server • Parser server • Cache server
scheduler	This is an optional keyword representing the scheduling server.
postgres	This is an optional keyword representing the postgres server.
apache	This is an optional keyword representing the apache server.
notif_server	This is an optional keyword representing the notif server.
parser	This is an optional keyword representing the parser server.
cache	This is an optional keyword representing the cache server.

Keyword	Description
start	Starts each MUR process.
stop	Kills or stops the running MUR process.
status	Displays the status of each MUR process. By default, it will show the status of all the MUR processes.

For example, if you want to start only the PSMON, then enter the following command:

```
./serv start psmonitor
```

or

```
./serv psmonitor start
```

Important: If you stop the MUR process, make sure that PSMON is not running. Otherwise PSMON will restart the MUR application.

The following is a sample output of the **`serv status`** command:

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

--------------- MUR Process Status ------------

 PID            Process                  Status

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

 4245          Process Monitor           Running

 4256          Scheduling server        Running

 4267          Postgres Server         Running

 4289          Apache Server           Running

 3249          Notif Server           Running

 3243          Parser Server           Running

 2430          Cache Server           Running

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

Using the PSMON Script

PSMON is a perl script that is used to monitor the Scheduling Server, Postgres Server, and Apache Server processes. This script can start or stop the processes based on certain thresholds specified in the MUR configuration file. The PSMON respawns any dead processes using the set of rules defined in the configuration file.

This script can also optionally send notifications to users via e-mail.

Generating Reports in Excel Format

To generate the reports in excel format, execute the following script from the *<MUR_install_dir>/starbi/bin* directory.

./get_excel_report.sh *-day <date for report generation> -f <path where report should be stored> -filter <filter for the report>*

The script takes three parameters, the date for which report is to be generated, the path where generated report is to be stored, and the filter for the reports. The date must be in mm-dd-yyyy format only, and the filter can be based on Type Allocation Code (TAC) or Access Point Name (APN).

Using the unanonymize_msisdn.sh Script

MUR reports the subscribers data like Mobile Station Integrated Network (MSISDN) in the encrypted format both in the GUI and Excel file. Decryption functionality is ONLY supported on CLI through the use of **unanonymize_msisdn.sh** script.

This shell script utility will check for user's privilege before decrypting the MSISDNs. It will prompt for the GUI administrator password.

Usage of unanonymize_msisdn.sh Script:

Important: Please note that this script must be run ONLY in bash shell.

./unanonymize_msisdn.sh *-u <username> -f <input file> -d <output path>*

Option	Meaning
-u	Used to specify GUI Administrator user name.
-f	Used to specify the absolute input file path of a file containing list of anonymized MSISDNs. Each anonymized MSISDN will be separated by a new line.
-d	Used to specify the output directory path where the decrypted MSISDNs file will be stored.
-h, --help	Prints this help.

To decrypt the MSISDN(s), perform the following steps:

1. Get an excel report for the day for which you want to see the clear text top subscribers or MSISDN(s). For information on how to get the excel report, refer to the Generating Reports in Excel Format section in this chapter.
2. Copy all lines from "Anonymized MSISDN" column of work sheet "Top 1000 Subscribers Traffic" and paste them in to a separate text file.
3. Provide this text file as an input to the **unanonymize_msisdn.sh** script.

Important: Please note that the users require GUI administrator credentials to access this utility.

Resetting GUI Administrator User Password

In case the Administrator user forgets the password, a *set_admin_password.py* script is used to reset the password. This script is located at the *<MUR_install_dir>/starbi/server/scripts* directory.

To reset the Administrator user's password, perform the following steps.

Step 1 Execute the following commands to set the environment variables.

```
#source server/env.properties
#export PYTHONPATH
#export LD_LIBRARY_PATH
```

Step 2 Execute the following script.

```
#python2.6.1/bin/python server/scripts/set_admin_password.py
```

The script will update MUR database with Administrator user password as *admin*.

Using the generate_dns_mapp_sql.sh Script

To generate the DNS mapping for the specified list of IP addresses, execute the following script from the *<MUR_install_dir>/starbi/bin* directory:

./generate_dns_mapp_sql.sh *<input file for IP> <output file where mapping should be stored>*

Keyword/Variable	Description
input file for IP	A file containing IP addresses. Each IP address must be present in a new line.
output file where mapping should be stored	An output file for storing the DNS mappings in SQL format.

This script is used to perform Internet DNS lookup of the specified IP addresses. It uses the 'nslookup' system administration command to find the DNS name of the specified IP. Please note that the machine must be connected to Internet for successful execution.

Generating Unknown URL Files

For CF reporting, MUR should parse CF-EDRs and generate the unknown/unrated URL database. This database will be pulled periodically by WEM and subsequently deliver to Rulespace. The unknown URL files can either be time based or count based.

To generate the unknown URL files, execute the following script from the *<MUR_install_dir>/server/scripts/cfedr* directory:

```
./gen_unknown_url.py
```

Important: Please note that up to a maximum of 85,000 Unknown URLs can be present in each file.

Using the getSupportDetails 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 MUR in the *<MUR_install_dir>/starbi/tools/supportdetails/* directory.

This script refers to an XML file to get the list of logs. This XML file 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 (MURsupportDetails.tar.gz), by default it is placed in */tmp/log* directory.

Requirements

Perl 5.8.5 and above is required for running the script.

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
- XML::Parser version 2.34
- XML-Parser-EasyTree
- Devel-CoreStack version 1.3

These modules are installed by default by the product. Please ensure that the above mentioned modules are installed when using a different installation of Perl.

To run the script, change to the directory path where the script is present and type:

`./getSupportDetails.pl` *`[--level=...] [--xmlfile=...] [--help]`*

Keyword/Variable	Description
--level	Specifies the level of debug to run. It can have a maximum of 4 levels. The level 4 provides the most detailed information. Default: 1
--xmlfile	Specifies the xml file name to be used for collecting the log. Default: getSupportDetails.xml
--onlyrecentlogs	Collects only recent logs and skips detailed logs. Default: Collects detailed logs
--collectFor	Collects problem specific logs and information which is not collected under normal levels. This can be combined with --level option. Default: Collects logs covered under '--level' option.
--help	Displays the supported keywords/variables.

For example, **`./getSupportDetails.pl --level=`***`4`* **`--xmlfile=`***`/tmp/getSupportDetails.xml`*

Supported Levels

The logs that can be collected for different levels are as follows:

- Level 1:

- Recent Log files
- Current status (running / not running) of the product
- Current Config files of the product

- Level 2:
  - Logs from Level 1
  - Installation Logs
  - Database Logs (if available)
  - Web Server logs (if available)
  - Information of Solaris version and current patch installed
  - Output of the following commands:

    ```
    netstat -an
    ifconfig -a
    df -k
    etc..
    ```

- Level 3:
  - Logs from level 2
  - Syslog Configuration and log files
- Level 4:
  - Logs from level 3
  - All Log files (including old logs)
  - Crontab entries
  - Information of packages installed
  - Stack trace of any crash files (if debugger is installed on local machine)
  - System Libraries only if any core file present in crash directory
  - Level of Solaris installed
  - Output of the following commands:

    ```
    ipcs
    ps -eaf
    etc..
    ```

Using the Purging Script

The python script, *purge_db.py*, handles both data purging and archived file purging. This script is packaged with MUR in the *<MUR_install_dir>/starbi/server/scripts/utils/* directory.

This script runs daily at the end of the day, picks up the relevant tables, and then purges either data or archived files based on the configurations.

In case of data purging, the script picks up the relevant tables and purges them.

In case of file purging, the script purges the files only if the archived files are organized date-wise for each of the reportings like FLOW-EDR, HTTP-EDR, CF-EDR, and BS. For example, EDR file for 24th September, 2010 is stored in the *archive/<gw>/flowedr/20100924* directory.

Server Script Parameters

The number of files being processed during each parsing interval for HTTP and non-HTTP EDRs can be controlled using the following parameters:

- EDR_TOTAL_NO_OF_FILES = 25
- EDR_MAX_NO_OF_PROCESSES = 5
- HTTP_TOTAL_NO_OF_FILES = 25
- HTTP_MAX_NO_OF_PROCESSES = 5

These parameters are defined in **System** menu under **File parsing configs** option available on the GUI.

With the above default configuration, if the number of files being accumulated are less than 25 and not in multiples of 5, then MUR spawns one more process to parse the remaining files.

Troubleshooting MUR

This section provides information on how to resolve situations you might encounter with using MUR software. This section provides problem definitions, their likely cause(s), and solutions.

Problem:	The EDR files are generated and moved out from the input directory. However, there are no reports getting generated.
Possible Cause(s):	The files may not be available in the archive directory i.e. *<MUR_install_dir>/starbi/archive*.
Action(s):	• Check if the files are available in the archive directory. • Check if they are marked invalid. If yes, check if there are any headers present in the files. If not, you need to configure ECS appropriately. • If the headers are present, check if all the required headers are present in the files.

Problem:	MUR reporting client cannot be started.
Possible Cause(s):	The web browser cache might be full.
Action(s):	The browser cache must be cleared. In the case of Firefox, follow these steps: • On the **Tools** menu, click **Clear Private Data**. • Select **Cache** check box. • Click **Clear Private Data Now**. In the case of Internet Explorer, follow these steps: • On the **Tools** menu, click **Internet Options**. • Click **Delete**. • Select **Temporary Internet files** check box. • Click **Delete**. ***Important:*** The Firefox version supported for MUR is 3.0.10 and later. For Internet Explorer, it is 7.0 and later.

Problem:	The bulkstats or KPI reports are not generated.
Possible Cause(s):	The bulkstats file might not be parsed.

Action(s):	• Check if the bulkstats schemas are properly configured on the gateway through the **BULKSTATS** menu in the **ADMIN** tab. • Check if the prerequisites described in the *Configuring Bulkstats Schemas* section of the *Configuring Chassis for MUR* chapter are met. • On the **ADMIN** menu, check the bulkstats audit under **AUDIT**. The audit should indicate whether the bulkstats files are being parsed or not. For more information, refer to the *Cisco Mobility Unified Reporting System Online Help* documentation. • Check if FTP is enabled on the MUR server. • Check if the bulkstats are FTPed to correct location on the MUR server from the gateway. The path should be as follows: **`$STARBI_HOME/server/data/$gwname/bs`** Where $STARBI_HOME = MUR installation directory, $gwname = Gateway name • Check if the Bulkstats/KPIs UI show only one day data • Check if the counters of same schemas are added in the formula while configuring KPIs. For example, if you are adding KPI in SGSN schema, then you should add counters of SGSN only in the formula. • Check if the bulkstat files are always pushed from gateway to master MUR and not to RDP.

Problem:	Parser is not handling data files properly.
Possible Cause(s):	The file might be corrupted.
Action(s):	• File are marked as 'UNPROCESSED.<file>' and moved to archive directory if one of the following conditions are met: • file is '.gz' and corrupted with CRC error. • file is empty. • file does not have a header. • File are marked as 'CORRUPTED.<file>' and moved to archive directory if the file is '.gz' and corrupted (other than CRC error) like 'invalid compressed data--format violated'

Problem:	Unable to add / edit / delete gateways.
Possible Cause(s):	The gateway configuration may be incorrect.
Action(s):	• Check if correct IP is provided while adding the gateway. • Check if gateway host is reachable from MUR. For more information, refer to the *Cisco Mobility Unified Reporting System Online Help* documentation.

Problem:	Unable to add / edit / delete RDPs.
Possible Cause(s):	The RDP configuration may be incorrect.

Action(s):	• Check if correct IP and port are provided while adding RDP. • Check if RDP is actually running on remote machine. • Check if RDP host is reachable from MUR. For more information, refer to the *Cisco Mobility Unified Reporting System Online Help* documentation.

Problem:	Duplicate reports are generated and/or the reports are incorrect.
Possible Cause(s):	MUR might have parsed half-cooked files.
Action(s):	The chassis tags the EDR files with a prefix 'prog.' while transferring to MUR. After the transfer is complete, the chassis removes the 'prog.' tag. The 'prog.' prefix indicates that the file is half cooked. • Check if the EDR files with the prefix 'prog.' are ignored. • Check if EDR file formats are configured properly.

Problem:	The archived files are not getting purged even after configured purging interval.
Possible Cause(s):	MUR might have parsed half-cooked files.
Action(s):	• Check the ownership of files in the archive directory. They must be owned by MUR group user. • The entity pushing the files to MUR, for example, L-ESS should be added to MUR user group. For details, refer to the *Managing Mobility Unified Reporting System Installation* chapter of this guide.

Problem:	If user is not able to configure bulkstats schema through **Add Schema configuration** screen that appears by selecting **ADMIN** > **Bulkstats** menu.
Possible Cause(s):	The initial prerequisites might not be met.
Action(s):	• Check if the prerequisites described in the *Configuring Bulkstats Schemas Using GUI* section of the *Configuring Chassis for MUR* chapter are met. • Check if the **SSH Username** in the **Add Bulkstats schema configuration** screen is specified correctly. This user name is used to connect to gateway via SSH for schema configuration. For information on how to configure the schemas, refer to the *Configuring Bulkstats Schemas Using GUI* section. Also, see the *Cisco Mobility Unified Reporting System Online Help* documentation.

Problem:	The bulkstats files are not pushed from the chassis to the MUR server even after successfully configuring schemas.
Possible Cause(s):	The related configurations might be incorrect.

Action(s):	• Check if **Username** specified in the **Add Bulkstats schema configuration** screen is present in MUR group on the MUR server. To create the username if it does not exist on MUR server, use the following command: **useradd** *<new user name>* If the user is already present then use the following command to add the user in the MUR group. **usermod -G** *<MUR Group> <user name>* • Check if **Destination** specified in the **Add Bulkstats schema configuration** screen is correct or not.

Problem:	While configuring bulkstat schema if configuration screen hangs for a long time.
Possible Cause(s):	The session might be timed out.
Action(s):	• Close the browser and try to configure the schema again. • Restart apache server by executing the following command from the *<mur_install_dir>/starbi/bin* directory and try again to configure the schema. **./serv start apache**

Problem:	If user is not able to edit the schema configuration through the **Add Bulkstat schema configuration** screen.
Possible Cause(s):	The schemas may not be configured properly.
Action(s):	• Follow the steps mentioned for above 3 cases. • If you are still not able to configure then delete the schema configuration for that particular schema from the GUI and try to configure again.

Problem:	**./serv** status shows Postgres processes as NOT RUNNING
Possible Cause(s):	The shared memory configuration in the */etc/system* directory might not be correct.
Action(s):	• Check if "shmmax" has been appropriately configured in the */etc/system* directory (for Solaris users) or */etc/sysctl.conf* directory (for Linux users). It should be set to 2684354560 (2.5GB). Reboot the system after making the changes to this file. • Check the available disk space (especially swap or /tmp) using **df -hk** command. • Try stopping other MUR instances on the machine. Each MUR instance will consume 2.5 GB of system's shared memory. Use the **prstat --a** command to check the used and free memory.

Problem:	If sftpying of EDR/UDR files failed
Possible Cause(s):	• SSH keys and SFTP server might not be configured appropriately. • SFTP might not be running on MUR server.

Action(s):	SSH keys and SFTP server need to be configured on the chassis and also SFTP should be running on MUR server. • Check if the following variables in the *sshd_config file* present in the */etc/ssh* directory are set appropriately. • PermitRootLogin = yes • PasswordAuthentication = yes • PAMAuthenticationViaKBDInt = no (Applicable ONLY for SOLARIS) • UsePAM = no (Applicable ONLY for RHEL) • Comment the line "PAMAuthenticationViaKBDInt yes" as "#PAMAuthenticationViaKBDInt yes" • Update the SFTP parameters as necessary if the variables are not set properly. • After updating restart SSH daemon using the following commands: **For Solaris 9:** `/etc/init.d/ssh restart` **For Solaris 10:** `svcadm restart svc:/network/ssh:default` **For RHEL:** `service sshd restart` If the problem still persists, remove the EDR generation configuration from the gateway and reconfigure them.

Problem:	If the EDR files are not getting parsed on the RDP and the files still remain in the input directory
Possible Cause(s):	The EDR configuration might be incorrect.
Action(s):	• Click **ADMIN** tab from the MUR GUI. • Click **Edit** for the gateway for which the EDR files are not getting parsed. • Check the values for the "Flow-Edr Filename Path" and "Http-Edr Filename Path" parameters and compare them with the actual path of files on RDP.

Problem:	While adding RDP, if the MUR GUI throws the following error message "Could not communicate with RDP"

Action(s):	• Check if the Apache server of RDP is running. • If it is not running, start the server using **`serv start`** command. • If it is running, check if the Firewall is running on RDP. To check the Firewall status, use the following command: **`service iptables status`** • If the output indicates "No firewalls running", check the Firewall settings for the associated ports and also check if the ports configured for RDP are in use. • From the command output, if you find the Firewall to be running, stop it with the **`service iptables stop`** command and then retry. • If you receive this message "RDP is already configured", please contact Cisco Advanced Service Team for additional support and guidance.

Problem:	Though the EDR files are parsed at the RDP, the reports are not available for a gateway attached to the RDP
Action(s):	• Check if RDP is actually running on remote machine. • Check if there are any pending files in the RDP's */starbi/server/sql_export_data/* directory. • If there are any pending files, check if the following log is shown in the *starbi_server_devel* file located in the */starbi/logs/server/* directory. *Unable to open host keys file" [rdptomaster_file_mover.py ...]"* • If the logs are found, perform the following procedure: • Log on to the RDP machine. Switch the user as RDP admin. If you have set RDP admin as **myrdp** during RDP installation, then execute the following command **`su - myrdp`**. • Create an SFTP session to master (sftp masteradmin@masterhost) The output will look something similar to the following: `Connecting to <masterhost>...` `The authenticity of host <masterhost> (<master ip address)' can't be established.` `RSA key fingerprint is <some key>.` `Are you sure you want to continue connecting (yes/no)?` • Enter **yes** and quit the SFTP session. • Check the files again in the *starbi/server/sql_export_data* directory to identify if they are present now. Then, check the reports after a while. • If the reports are still not seen, check the master configuration in **System** menu. Check if the master login and password are specified. Ensure that master admin password has been set using password command on the master. If the solution provided above does not help to resolve your problem, please contact Cisco Advanced Service Team for additional support and guidance.

Problem:	**./serv** status shows cache server is not running.
Possible Cause(s):	The port used by cache server implicitly is postgres port + 2. This is not a configurable port. Make sure that this port is not occupied by any other process.
Action(s):	• Free the required port for cache server. • Reinstall MUR with postgres port such that postgres port + 2 will be free and can be used by cache server.