Oracle® Communications Diameter Signaling Router

Subscriber Database Server User's Guide

E63663 Revision 02

October 2015

ORACLE®

Oracle® Communications Diameter Signaling Router Subscriber Database Server User's Guide

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

Introduction provides a content overview of this guide with a brief summary about incidents, notifications, and the ID ranges for alarms and events. It also includes contact information and how to locate product documentation on the Customer Support site.

The SDS Help System

Subscriber Database Server (SDS) provides the central provisioning of the Full-Address Based Resolution (FABR) data. The SDS, which is deployed geo-redundantly at a Primary and Disaster recovery site, connects with the Query server and the Data Processor Site Operation Administration and Maintenance (DP SOAM) servers at each diameter routing site or a standalone DP site to replicate and recover provisioned data to the associated components.

The Getting Started section of the Help provides an overview of the SDS and a description of how to use the Help. In this section you can find information about SDS including a product overview, the system architecture, and functions. Additionally, the Getting Started section familiarizes you with common GUI features including user interface elements, main menu options, supported browsers, and common user interface widgets.

Scope and Audience

This guide is intended for trained and qualified system operators and administrators who are responsible for managing an SDS system.

Manual organization

This document is organized into the following chapters:

- *Introduction* contains general information about the Diameter and Mediation help documentation, the organization of this manual, and how to get technical assistance.
- *About SDS* contains general information about the SDS documentation, the organization of this manual, and how to get technical assistance.
- *Configuration* describes the SDS Configuration menus options and their associated functions.
- *Maintenance* describes the SDS Maintenance menu options and their associated functions.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of *personal injury*.)
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology Network (OTN) site. See *Locate Product Documentation on the Oracle Help Center Site* for more information.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, *http://docs.oracle.com*. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at *http://www.adobe.com*.

1. Access the Oracle Help Center site at *http://docs.oracle.com*.
2. Click **`Industries`**.
3. Under the Oracle Communications subheading, click the **`Oracle Communications documentation`** link.
   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings “Network Session Delivery and Control Infrastructure” or “Platforms.”
4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.

5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

My Oracle Support (MOS)

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select **1**
   - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Chapter 2

About SDS

Topics:

This section of documentation describe the SDS application, its GUI, the system architecture, and centralized configuration.

Subscriber Database Server (SDS) provides the central provisioning of the Full-Address Based Resolution (FABR) data. The SDS, which is deployed geo-redundantly at a Primary and Disaster recovery site, connects with the Query server and the Data Processor Site Operation Administration and Maintenance (DP SOAM) servers at each diameter routing site or a standalone DP site to replicate and recover provisioned data to the associated components.

Introduction to SDS

The SDS/DP system consists of a Primary Provisioning Site, a Disaster Recovery (DR) Provisioning Site, and up to 24 Signaling Site servers with redundant DP SOAM servers and up to 10 DP servers. Each Provisioning Site has an active/standby pair of servers in a high availability (HA) configuration and a third server configured as a Query server.

The SDS/DP system is built upon the AppWorks platform. This platform provides a variety of services such as site-based GUI, HA capabilities (active/standby switchover and DR switchover), and database functionality (replication, backup, restore).

Every server within the SDS/DP system collects measurements, alarms, and events data. This functionality is provided by AppWorks. Every server sends its traps directly to the customer's SNMP Manager. Every server can collect measurement data. This measurement data is merged up in reverse direction of replication. The DP measurements are sent to the Active DP SOAM server, which sends the measurements from all DP servers and itself to the Primary Provisioning Site's Active SDS.

This introduction will familiarize you with the basic operation, features, and components of SDS.

SDS functionality

SDS provides the following functionality:

- SDS Database – Stores subscriber data needed by the FABR application
- GUI-based provisioning
- Support SOAP over HTTP and XML over TCP as provisioning interfaces
- SQL Interface – At query server for query only
- CSV and/or XML format export and import of database contents
- Real Time replication to:
  - Local standby server at Primary site
  - Local query server at Primary site
  - Each server at Disaster Recovery site
  - Each DP SOAM and DP at up to 24 sites
- DP - DB Processor – A server that has a replica of the SDS database and is available for query by FABR applications
- Automatic scheduled NPA Split processing
- Provisioning Measurements and KPIs
- Alarms, Events and Logs for all interfaces
- DB Audit - Replication audit within replicas and Active SDS, and remote audit between SDS and HLR Router
- Query server
- Backup and Restore of SDS database components
- Disaster Recovery SDS – Geo-diverse site
- Automated Performance Data Export (APDE)
- Manage and associate routing destinations for routing entities that represent Subscriber identities
- Monitor exceptions
- Subscriber identity grouping

- Blacklist support
- Address resolution – Full address, as well as prefix address support

System Architecture

SDS consists of an active/standby pair of SDS servers in an HA configuration, a third SDS server configured as a Query server, an optional DR SDS, redundant DP SOAM servers, and up to 10 DPs (Database Processor) servers. An SDS can have up to 24 sites, each capable of supporting up to 512 remote signaling points.

This figure provides an overview of the SDS architecture.

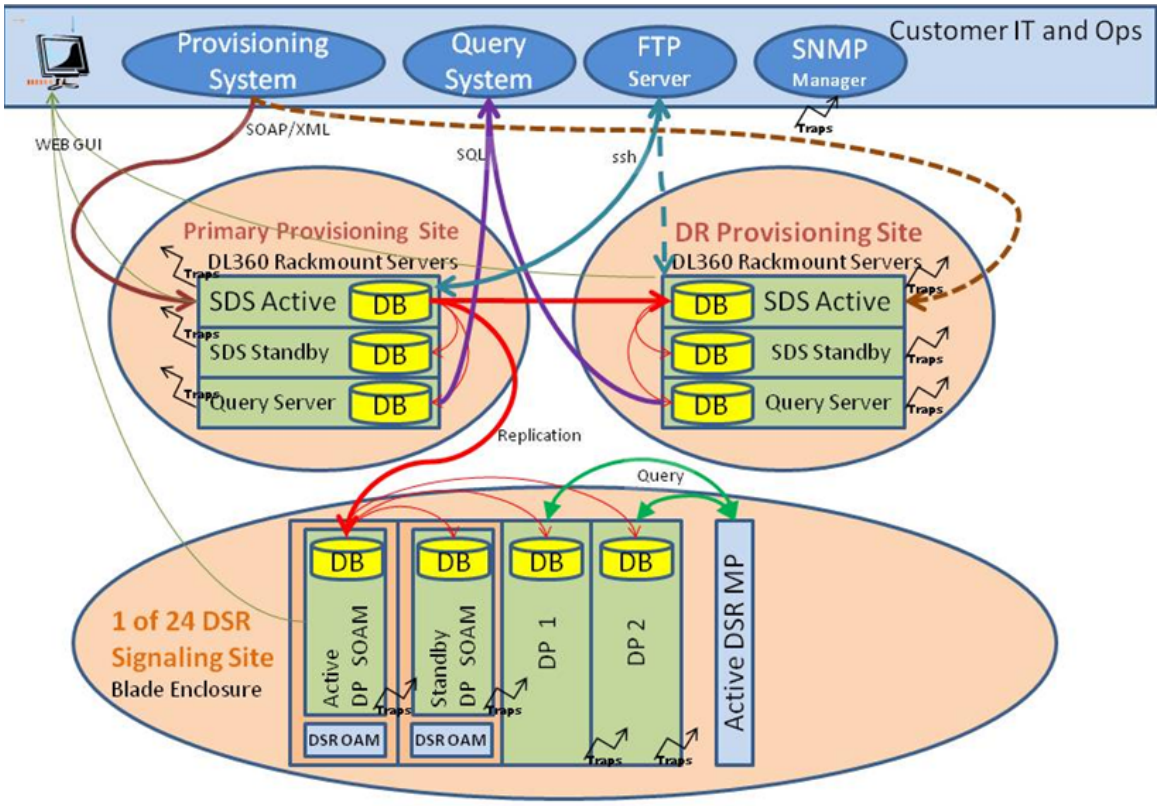

Figure 1: SDS System Diagram

SDS Components

SDS

The SDS is one active and one standby server running the SDS application and operating in a high availability configuration. It accepts subscriber data provisioned by the customer over SOAP or XML and replicates it to the DR SDS, the Query server, and all underlying SDSes. It also provides a GUI which is used for configuration, user administration, and the viewing of alarms and measurements.

SDS distributes all successful incoming subscriber provisioning data, independent of source, to all downstream Network Elements (NEs) and to the DR SDS at a rate of up to 200 provisioning database updates per second. To ensure the database levels of the Network Elements are less than the database levels of the SDS and DR SDS, the active provisioning site SDS provisions the DR SDS prior to updating the Network Elements.

DR SDS

The DR SDS is a geographically independent SDS component. The DR SDS has the same hardware configuration and network accessibility as the SDS.

The DR SDS's databases are kept up to date through real-time replication of subscriber and application data from the Active SDS. Under normal operating conditions, the DR SDS does not provision any downstream systems but if made Active, it will take over all the functions of the Active SDS including the provisioning and database replication to underlying DP SOAMs.

DP SOAM

The DP SOAM is the combination of an active and a standby application server running the DP SOAM application and operating in a high availability configuration. It accepts subscriber data replicated from the Active SDS and in turn replicates it to all underlying DPs located in the same physical frame. DP SOAM also provides a GUI used for local DP configuration and viewing alarms and measurements details specific to components located within the frame (DP SOAM, DP).

The DP SOAM supports up to 10 DPs.

Query Server

The Query server is an independent application server containing a replicated version of the provisioning database. It accepts replicated subscriber data from the SDS and stores it in a customer accessible MySQL database. A Query server is located in the same physical frame as each SDS component (SDS/DR SDS).

Network Element

Network Elements are containers that group and create relationships between servers in the network. There are two types of Network Elements:

- SDS: such as the SDS and the DR SDS
- DP SOAM: contains a pair of DP SOAM servers and one or more DP servers

The system can support two SDS Network Elements and up to 24 DP SOAM Network Elements.

DPs

The Data Processors (DP) are servers with the SDS application installed that are configured for DP functionality. They accept replicated subscriber data from the local DP SOAM and store it in a subscriber database.

The DP are servers that are configured for DP functionality. They accept replicated subscriber data from the local DP SOAM and store it in a subscriber database. The DPs are used for processing queries from the Message Processor (MP) for destination address resolution. DP receives database queries that include user identities such as MSISDN, IMSI or URI and destination types and return the resolved destination’s address FQDN and/or realm values.

Each Signaling Site can support multiple DP servers deployed in a single frame in order to scale query capacity (by increments of 50,000 QPS per DP). Each Signaling Site can support up to 10 DPs; however, only 2 DPs are supported in the initial release.

The DP servers all contain a copy of the same SDS data. They are configured in an active/active mode. The MP is responsible for load-balancing requests across DP servers.

The DP is deployed at each site on Data Processor (DP) servers with n+m redundancy. Initially n=1 and m=1.

Distributed configuration

The SDS supports centralized configurations:

- Centralized configuration:
  - All subscriber data configuration and maintenance occurs at the SDS level
  - Application management, such as configuring servers, occurs at the SDS level

Due to distributed configuration:

- All OAM Administration, Configuration, and Status & Manage tasks can only be performed when you are logged into an active SDS.
- SDS tasks related to the subscriber database are only available when logged into an active SDS, with the exception of querying the database.
- All Alarms, KPIs, Measurements, and Events are accessible from the SDS.

Centralized configuration

Subscriber provisioning data is provisioned at the active server of the Primary SDS cluster and replicated to all servers on the network. System configuration and subscriber data is provisioned at the active server of the Primary SDS cluster, replicated to all other SDS, and then replicated to the active DP SOAM of each Network Element.

SOAP/XML

The main method of subscriber data provisioning is SOAP or XML Interfaces. They allow one or several independent information systems supplied and maintained by the network operator to be used for provisioning databases and for configuring systems. Through the SOAP/XML interfaces, independent information systems may add, delete, change or retrieve information about any Destinations Routing Entities.

GUI Provisioning

Local provisioning can be done using the SDS GUI. The GUI can be used to manage Provisioning setup, to make direct changes to the subscriber database entries, and to perform application operations, management, and provisioning.

This table shows the GUI options available when logged into an SDS.

Table 2: SDS Main Menu Options

Menu Item	Function
Administration	All options available: • Users • Groups • Sessions • Single Sign-On • Authorized IPs • Options • SNMP • ISO • Upgrade • Software Versions • Export server
Configuration	All options available: • Network Elements • Services • Resource Domains • Servers • Server Groups • Network
Alarms & Events	All options available: • View Active • View History • View Trap Log
Security Log	All options available: • View History
Status & Manage	All options available: • Network Elements • Server • HA • Database • KPIs • Processes • Tasks • Files
Measurements	All options available: • Report

Menu Item	Function
Communication Agent	All options available: • Configuration • Maintenance
SDS	Configuration: • Options • Connections • NAI Hosts • Destinations • Destination Map • Routing Entities • Subscribers • Blacklist Maintenance: • Connections • Command Log • Relay Exception Log • Import Status • Routing Entities • Export • Remote Audit • Query • NPA Splits

Chapter 3

Configuration

Topics:

The **SDS Configuration** menu options allow you to configure provisioning options and view, insert, edit, and delete provisioning connections, NAI hosts, destinations, and routing entities.

The available database menu options will vary based on the type of server you are logged into and the permissions assigned to your group. If you do not see a menu option you need, make sure you are logged into the appropriate type of server and ask your administrator to make sure the group your user ID belongs to has the appropriate permissions.

Options configuration

The **Options** page allows you to control how the mechanized interface works and controls features such as Import and Export.

Provisioning options

Connections between the application and the provisioning client are set up using the **Connections** page (for more information, see *Connections configuration*. The **Options** page allows you to manage configuration options for these connections. Use this page to configure:

- Whether to allow connections and the maximum number of connections allowed
- Number of seconds of inactivity allowed before a connection is timed out
- Whether to log provisioning messages
- Number of seconds allowed between a transaction being committed and becoming durable
- TCP listening ports
- Whether to allow to importing from and exporting to a Remote Host

Import options

The status of provisioning imports can be viewed using the **SDS Maintenance Import** page. For more information, see *Import Status maintenance*. Provisioning imports from a remote host are configured through the **SDS Configuration Options** page. Use this page to configure:

- Whether provisioning imports are enabled
- Remote host information, including the IP address, username, password, and import directory name
- Whether the import mode is blocking or non-blocking

Export options

Provisioning exports are scheduled through the **SDS Configuration Export** page and the export status can be viewed through the **SDS Maintenance Export Status** page. For more information about this see *Import Status maintenance*. Use the **SDS Configuration Options** page to configure:

- Whether or not exports are allowed to be copied from this server to the remote host
- Remote host information, including the IP address, username, password, and export directory name
- Whether the export mode is blocking or non-blocking

Options configuration elements

This table describes the fields on the Options page.

Table 3: Options Configuration Elements

Element	Description	Data Input Notes
Display Command Output	If checked, the commands and responses will be displayed on the GUI when provisioning data.	Format: Check box Range: Checked, Unchecked Default: Unchecked
Allow Connections	If checked, incoming provisioning connections are allowed.	Format: Check box Range: Checked, Unchecked Default: Checked
Max Transaction Size	The maximum number of database manipulation commands per transaction.	Format: Digits only Range: 1–100 Default: 50
Log Provisioning Messages	If checked, all incoming and outgoing provisioning messages will be logged in the command log.	Format: Check box Range: Checked, Unchecked Default: Checked
Transaction Durability Timeout	The number of seconds allowed between a transaction being committed and it becoming durable. If Transaction Durability Timeout lapses, DURABILITY_TIMEOUT (1024) response is sent to the originating client. The associated request should be resent to ensure that the request was committed.	Format: Digits only; seconds Range: 2–3600 Default: 5
Remote Import Enabled	If checked, import files are imported from a remote host.	Format: Check box Range: Checked, Unchecked Default: Unchecked
Remote Import Mode	If set to **Non-Blocking**, updates are allowed on all provisioning connections while the remote import operation is in progress. If set to **Blocking**, updates are not allowed.	Format: Pulldown menu Range: Non-Blocking, Blocking Default: Non-Blocking
Remote Import Host IP Address	The IP address of remote import host periodically queried for import files.	Format: Alphanumeric Range: 0–39 characters Range: Either an IPv4 or an IPv6 IP address.

Element	Description	Data Input Notes
		IPv4 addresses are 32 bits, represented in a dot-decimal notation like this: x.x.x.x where each x (called an octet) is a decimal value from 0 to 255. They are separated by periods. For example: 1.2.3.4 and 192.168.1.100 are valid IPv4 addresses. IPv6 addresses are 128 bits, represented in a colon-hexadecimal notation like this: z:z:z:z:z:z:z:z where each z is a group of hexadecimal digits ranging from 0 to ffff. They are separated by colons. Leading zeros may be omitted in each group. "::" can be used (at most once) in an IPv6 address to represent a range of as many zero fields as needed to populate the address to eight fields. So the IPv6 address 2001:db8:c18:1:260:3eff:fe47:1530 can also be represented as 2001:0db8:0c18:0001:0260:3eff:fe47:1530 and the IPv6 address ::1 is the same as 0000:0000:0000:0000:0000:0000:0000:0001
Remote Import User	The Username for remote import host user.	Format: Alphanumeric Range: 0–255 characters
Remote Import Password	The password to exchange ssh keys with the remote import host. The password is cleared from this table after the keys have been exchanged.	Format: Alphanumeric Range: 0–255 characters
Remote Import Directory	The directory where import files exist on the remote import host.	Format: Alphanumeric Range: 0–255 characters
Export Mode	If set to **Non-Blocking**, updates are allowed on all provisioning connections while the export operation is in progress. If set to **Blocking**, updates are not allowed.	Format: Pulldown menu Range: Non-Blocking, Blocking Default: Non-Blocking

Element	Description	Data Input Notes
Remote Export Transfers Enabled	If checked, export files will be copied to the remote export host.	Format: Check box Range: Checked, Unchecked Default: Unchecked
Remote Export Host IP Address	The IP address of the remote export host to where export files may be configured automatically transferred.	Format: Alphanumeric Range: 0–39 characters Range: Either an IPv4 or an IPv6 IP address. IPv4 addresses are 32 bits, represented in a dot-decimal notation like this: x.x.x.x where each x (called an octet) is a decimal value from 0 to 255. They are separated by periods. For example: 1.2.3.4 and 192.168.1.100 are valid IPv4 addresses. IPv6 addresses are 128 bits, represented in a colon-hexadecimal notation like this: z:z:z:z:z:z:z:z where each z is a group of hexadecimal digits ranging from 0 to ffff. They are separated by colons. Leading zeros may be omitted in each group. "::" can be used (at most once) in an IPv6 address to represent a range of as many zero fields as needed to populate the address to eight fields. So the IPv6 address 2001:db8:c18:1:260:3eff:fe47:1530 can also be represented as 2001:0db8:0c18:0001:0260:3eff:fe47:1530 and the IPv6 address ::1 is the same as 0000:0000:0000:0000:0000:0000:0000:0001
Remote Export User	The username for remote export host user.	Format: Alphanumeric Range: 0–255 characters
Remote Export Password	The Password to exchange ssh keys with the remote export host. The password is cleared from this table after the keys have been exchanged.	Format: Alphanumeric Range: 0–255 characters

Element	Description	Data Input Notes
Remote Export Directory	If export is configured, the export files are transferred to the location on the remote export host.	Format: Alphanumeric Range: 0–255 characters
Remote Audit Receive Window Size	The maximum number of retrieval messages that can be received and buffered by the Provisioning Database Application on the remote system. After this amount is reached, no more messages will be sent until acknowledgments are received from the remote system.	Format: Digits only Range: 5–2500 Default: 500
Remote Audit Send Message Rate	The maximum rate of messages/second in which retrieval messages will be sent to the Provisioning Database Application on the remote systems.	Format: Digits only Range: 5–2500 Default: 500
Remote Audit Number Range Limit	The maximum number of records that can be queried per request message.	Format: Digits only Range: 100–100000 Default: 1000
PDB Relay Enabled	Whether or not to relay successful incoming provisioning requests to a Provisioning Database Application on a remote system. **Note:** This feature requires that the Log Provisioning Messages option is enabled.	Format: Check box Range: Checked, Unchecked Default: Unchecked
PDB Relay Primary Remote System VIP Address	The VIP address of the primary remote system of that the Provisioning Database Application is running. **Note:** Changes to the VIP address listening port do not take affect until PDB Relay is restarted.	Format: Alphanumeric Range: 0–39 characters Range: Either an IPv4 or an IPv6 IP address. IPv4 addresses are 32 bits, represented in a dot-decimal notation like this: x.x.x.x where each x (called an octet) is a decimal value from 0 to 255. They are separated by periods. For example: 1.2.3.4 and

Element	Description	Data Input Notes
		192.168.1.100 are valid IPv4 addresses. IPv6 addresses are 128 bits, represented in a colon-hexadecimal notation like this: z:z:z:z:z:z:z:z where each z is a group of hexadecimal digits ranging from 0 to ffff. They are separated by colons. Leading zeros may be omitted in each group. "::" can be used (at most once) in an IPv6 address to represent a range of as many zero fields as needed to populate the address to eight fields. So the IPv6 address 2001:db8:c18:1:260:3eff:fe47:1530 can also be represented as 2001:0db8:0c18:0001:0260:3eff:fe47:1530 and the IPv6 address ::1 is the same as 0000:0000:0000:0000:0000:0000:0000:0001
PDB Relay Disaster Recovery Remote System VIP Address	The VIP address of the Disaster Recovery remote system on which the Provisioning Database Application is running. **Note:** Changes to the VIP address do not take affect until PDB Relay is restarted.	Format: Alphanumeric Range: 0–39 characters IPv4 addresses are 32 bits, represented in a dot-decimal notation like this: x.x.x.x where each x (called an octet) is a decimal value from 0 to 255. They are separated by periods. For example: 1.2.3.4 and 192.168.1.100 are valid IPv4 addresses. IPv6 addresses are 128 bits, represented in a colon-hexadecimal notation like this: z:z:z:z:z:z:z:z where each z is a group of hexadecimal digits ranging from 0 to ffff. They are separated by colons. Leading zeros may be omitted in each group. "::" can be used (at most once) in an IPv6 address to represent a range of as many zero fields as needed to populate the address to eight fields. So the IPv6 address

Element	Description	Data Input Notes
		2001:db8:c18:1:260:3eff:fe47:1530 can also be represented as 2 001:0db8:0c18:0001:0260:3eff:fe47:1530 and the IPv6 address ::1 is the same as 0000:0000:0000:0000:0000:0000:0000:0001
PDB Relay Remote System Port	The TCP listening port of the Provisioning Database Application on the remote system. **Note:** Changes to the TCP listening port do not take affect until PDB Relay is restarted.	Format: Digits only Range: 0–65535 Default: 5873
PDB Relay Receive Window Size	The maximum number of provisioning commands that can be received and buffered by the Provisioning Database Application on the remote system. After this amount is reached, no more commands will be sent until acknowledgments are received from the remote system.	Format: Digits only Range: 5–2500 Default: 500
PDB Relay Send Command Rate	The maximum rate (in commands/second) in which commands will be relayed/sent to the Provisioning Database Application on remote system.	Format: Digits only Range: 5–2500 Default: 500
PDB Relay Timestamp (read-only)	The timestamp of the last provisioning message relayed to the Provisioning Database Application on the remote system.	Format: Read-only timestamp
XML Interface Port	XML interface TCP (unsecured) listening port. To disable this port, set it to **0**. **Note:** Changes to the TCP listening port do not take effect until the xds process is restarted. You must also specify a different port other than the SOAP interface.	Format: Digits only Range: 0–65535 Default: 5875

Element	Description	Data Input Notes
XML Interface Idle Timeout	The maximum number of seconds that an open connection will remain active without a request being sent before the connection is dropped.	Format: Digits only; seconds Range: 1–86400 Default: 1200
Maximum XML Connections	The maximum number of simultaneous XML interface client connections. **Note:** Changes to the Maximum XML Connections option do not take effect until the xds process is restarted.	Format: Digits only Range: 1–120 Default: 120
SOAP Interface Port	The SOAP interface TCP listening port. To disable this port, set it to **0**. **Note:** Changes to the TCP listening port do not take effect until the xds process is restarted. You must also specify a different port other than the XML interface.	Format: Digits only Range: 0–65535 Default: 5876
SOAP Interface Idle Timeout	The maximum time (in seconds) that an open connection will remain active without a request being sent, before the connection is dropped.	Format: Digits only Range = 1-86400 Default = 1200
Maximum SOAP Connections	The maximum number of simultaneous SOAP interface client connections. **Note:** Changes to the Maximum SOAP Connections option do not take effect until the xds process is restarted.	Format: Digits only Range: 1–120 Default: 120
SOAP Secure Mode	If set to **Secure**, the SOAP interface operates in secure mode (using TSL). **Note:** Changes to the SOAP Secure Mode option do not take effect until the xds process is restarted.	Format: Pulldown menu Range: Secure, Unsecure Default: Unsecure

Element	Description	Data Input Notes
Maximum Transaction Lifetime	The maximum number of seconds that a transaction will remain open before automatically being rolled back if a commit or rollback is not performed. To disable this timeout, set it to **0**.	Format: Digits only; seconds Range: 0–3600 Default: 60

Editing options

You can only perform this task when logged into the active SDS server.

1. Select **SDS** > **Configuration** > **Options**.
   The **SDS Configuration Options** page appears.
2. Modify the options you want to change by entering information in the appropriate fields.
   For a detailed explanation about the options and valid input for these fields, see *Options configuration elements*.
3. Click **Apply**.
   If field validations succeed, the changes are saved and you remain on the same page. A successful update message appears.
   If the page contains any values that are not valid or are out of range, an error message appears.

Connections configuration

The **Connections** page allows you to manage the configuration for servers permitted to establish a connection to the active Primary Provisioning Site's Active SDS server. Only the servers specified in the Connections list are allowed to remotely connect to the server and execute commands.

Note: The client host being associated with permissions must exist in the system prior to adding a subscribing client permission record.

SDS allows up to 120 simultaneous provisioning connections and supports secure and unsecure SOAP connections. While the application is capable of supporting 120 connections, the maximum number of connections allowed can be limited using the **Options** page. For more information about this option, see *Options configuration*.

From the **Connections** page, you can:

- Filter the list of server to display only the desired servers.
- View the list of servers allowed to establish a remote connection and each server's permissions.
- Configure the SDS to allow connection requests from remote servers.
- Modify the System ID, IP address, and permissions for listed servers.
- Delete servers from the connections list.

Connections configuration elements

This table describes the fields on the Connections View page.

Table 4: Connections Configuration Elements

Element	Description	Data Input Notes
Action columns	Selectable columns where you can choose to edit or delete selections.	Format: Selectable items.
Filter fields	Pulldown menu of available filters and additional fields to modify the search options.	Format: Selectable list.
System ID	Identification for the system	Format: Alphanumeric Range: 1–8 characters
IP Address	IP address of the client that will connect to SDS	Format: Alphanumeric Range: Either an IPv4 or an IPv6 IP address. IPv4 addresses are 32 bits, represented in a dot-decimal notation like this: x.x.x.x where each x (called an octet) is a decimal value from 0 to 255. They are separated by periods. For example: 1.2.3.4 and 192.168.1.100 are valid IPv4 addresses. IPv6 addresses are 128 bits, represented in a colon-hexadecimal notation like this: z:z:z:z:z:z:z:z where each z is a group of hexadecimal digits ranging from 0 to ffff. They are separated by colons. Leading zeros may be omitted in each group. "::" can be used (at most once) in an IPv6 address to represent a range of as many zero fields as needed to populate the address to eight fields. So the IPv6 address 2001:db8:c18:1:260:3eff:fe47:1530 can also be represented as 2 001:0db8:0c18:0001:0260:3eff:fe47:1530 and the IPv6 address ::1 is the same as 0000:0000:0000:0000:0000:0000:0000:0001
Permission	Database permissions for this client	Format: Pulldown list Range: READ_ONLY, READ_WRITE Default: READ_ONLY

Viewing connections

You can perform this task when logged into an SDS or from the DP SOAM GUI.

Select **SDS** > **Configuration** > **Connections**.

The **Connections** page appears.

The currently allowed connections are listed in the table.

Inserting connections

You can only perform this task when logged into the Active Primary SDS.

1. Select **SDS** > **Configuration** > **Connections**.
   The **Connections** page appears.
2. Click **Insert**.
   The **SDS Configuration Connections [Insert]** page appears.
3. Enter a system ID in the **System ID** field.
4. Enter a unique IP address for the connection in the **IP Address** field.
5. Select the permissions level for the connection from the **Permissions** pulldown menu.
   - Select **READ_ONLY** to grant read-only access for the client with this connection. This is the default.
   - Select **READ_WRITE** to grant read and write access for the client with this connection.
6. Perform one of the following:
   - Click **OK** to save the connection and return to the SDS configuration connections page.
   - Click **Apply** to save the connection and remain on this page.
   - Click **Cancel** to return to the **SDS Configuration Connections** page without saving the changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Any required field is empty; no value was entered or selected
   - The entry in any field is not valid (wrong data type or out of the valid range)
   - The IP Address is not unique; it already exists in the system

Editing connections

You can only perform this task when logged into the Active Primary SDS.

1. Select **SDS** > **Configuration** > **Connections**.
   The **SDS Configuration Connections** page appears.
2. Locate the connection you want to edit and click **Edit**.
   The **SDS Configuration Connections [Edit]** page appears.
3. Edit the System ID, IP Address, and/or Permission for the connection.
   For more information about these fields, see *Connections configuration elements*.
4. Perform one of the following:
   - Click **OK** to save the changes and return to the SDS configuration connections page.
   - Click **Apply** to save the changes and remain on this page.

   If field validations succeed, the connection is saved.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - If the entry in any field is not valid or are out of range

- If a required field is empty (not entered)
- If the IP Address is not unique

Deleting connections

You can only perform this task when logged into the Active Primary SDS.

1. Select **SDS** > **Configuration** > **Connections**.
   The **SDS Configuration Connections** page appears.
2. Locate the connection you want to delete and click **Delete**.
   A popup confirmation window appears.
3. Perform one of the following actions:
   - Click **OK** to delete the connection.
   - Click **Cancel** to cancel the delete function and return to the **SDS Configuration Connections** page.

NAI Hosts configuration

The **NAI Hosts** page allows you to manage the Network Access Identifier (NAI) host systems that are used for provisioning NAI User-associated routing entities.

From the **NAI Hosts** page, you can:

- Filter the list of hosts to display only the desired hosts.
- View the NAI Hosts configured for NAI User.
- Add a NAI Host.
- Delete a NAI Host.

NAI Hosts configuration elements

This table describes the fields on the NAI Hosts View and Insert pages.

Table 5: NAI Hosts Configuration Elements

Element	Description	Data Input Notes
NAI Host	Network Access Identifier hostname	Format: alphanumeric (A-Z, a-z, 0-1) and special characters: period (.), hyphen (-), plus (+), underscore (_), At sign (@), dollar sign ($), pound or number sign (#), forward slash (/), double quote ("), asterisk (*), exclamation point (!), and colon (:) Range: 1–64 characters

Viewing NAI hosts

You can perform this task when logged into an SDS or from the DP SOAM GUI.

Select **SDS** > **Configuration** > **NAI Hosts**.
The **SDS Configuration NAI Hosts** page appears.

The current NAI hosts are listed in the table.

Inserting NAI hosts

You can only perform this task when logged into the Active Primary SDS.

1. Select **SDS** > **Configuration** > **NAI Hosts**.
   The **SDS Configuration NAI Hosts** page appears.
2. Click **Insert**.
   The **SDS Configuration NAI Hosts [Insert]** page appears.
3. Enter a unique hostname in the **NAI Host** field.
4. Perform one of the following:
   - Click **OK** to save the hostname and return to the SDS configuration **NAI Hosts** page.
   - Click **Apply** to save the hostname and remain on this page.
   - Click **Cancel** to return to the **SDS Configuration NAI Hosts** page without saving the changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - The required field is empty; no value was entered.
   - The entry in the **NAI Host** field contains an invalid character.
   - The hostname is not unique; it already exists in the system.

Deleting NAI hosts

You can only perform this task when logged into the Active Primary SDS.

Before performing this task, disable and delete any association that may exist between the NAI host and routing entity (NAI User or Wildcard NAI User).

1. Select **SDS** > **Configuration** > **NAI Hosts**.
   The **SDS Configuration NAI Hosts** page appears.
2. Locate the NAI host you want to delete and click **Delete**.
   A popup confirmation window appears.
3. Perform one of the following actions:
   - Click **OK** to delete the NAI Host.
   - Click **Cancel** to cancel the delete function and return to the **SDS Configuration NAI Hosts** page.

   If **OK** is clicked and the following condition exists, an error message appears:
   - The NAI Host is in use by a routing entity.

Destinations configuration

The **Destinations** page allows you to manage routing destinations used by routing entities.

From the **SDS Configuration Destination** page, you can perform the following actions:

- Retrieve information for a specific Destination.
- Add a Destination.
- Update the information associated with an existing Destination.
- Delete a Destination.

Destinations configuration elements

This table describes the fields on the Destination Retrieve, Add, Update, and Delete tabs.

Table 6: Destinations Configuration Elements

Element	Description	Data Input Notes
Retrieve and Delete tabs		
Name	Name of the destination	Format: Alphanumeric (A-Z, a-z, 0-1) and special characters: period (.), hyphen (-), plus (+), underscore (_), At sign (@), dollar sign ($), pound or number sign (#), forward slash (/), double quote ("), asterisk (*), exclamation point (!), and colon (:) Range: 1–32 characters; cannot start with a digit and must contain at least one alpha character.
Add and Update tabs		
Name	Name of the destination	Format: Alphanumeric (A-Z, a-z, 0-1) and special characters: period (.), hyphen (-), plus (+), underscore (_), At sign (@), dollar sign ($), pound or number sign (#), forward slash (/), double quote ("), asterisk (*), exclamation point (!), and colon (:) Range: 1–32 characters; cannot start with a digit and must contain at least one alpha character.
Type	Type of destination	Format: Pulldown list • IMS HSS • LTE HSS • PCRF • OCF • OFCS • AAA • User defined 1 • User defined 2

Element	Description	Data Input Notes
FQDN	Unique fully qualified domain name	Format: String consisting of a list of labels separated by dots. A label might contain letters, digits, dash (-), and underscore (_). A label must begin with a letter or underscore, and must end with a letter or digit. Underscore can be used only as the first character. Range: 0-255 characters
Realm	Realm	Format: String consisting of a list of labels separated by dots. A label might contain letters, digits, dash (-), and underscore (_). A label must begin with a letter or underscore, and must end with a letter or digit. Underscore can be used only as the first character. Range: 0-255 characters

Retrieving destinations

You can perform this task when logged into an SDS or from the DP SOAM GUI.

1. Select **SDS** > **Configuration** > **Destinations**.
   The **SDS Configuration Destinations** page appears.

   By default, the **Retrieve** tab is the viewable tab. If not, select the **Retrieve** tab.

2. Enter the destination you want to view in the **Name** field.

   Note: For a list of Destinations, select **SDS** > **Maintenance** > **Query**; then, select Destination from the **Data** pulldown list.

3. Click **Retrieve**.
   The destination appears.

Adding destinations

You can only perform this task when logged into the Active Primary SDS.

1. Select **SDS** > **Configuration** > **Destinations**.
   The **SDS Configuration Destinations** page appears.
2. Select the **Add** tab.
   The **Add** tab appears.
3. Enter a unique name in the **Name** field.
4. Select the type of destination from the **Type** pulldown list.
5. Enter a fully-qualified domain name (FQDN) in the **FQDN** field.
6. Enter the realm in the **Realm** field.
7. Click **Add** to save the destination.
   When **Add** is clicked and any of the following conditions exist, an error message appears:
   - The entry in any field is not valid (wrong data type).

- The Destination name is not unique; it already exists in the system.

Updating destinations

You can only perform this task when logged into the Active Primary SDS.

1. Select **SDS** > **Configuration** > **Destinations**.
   The **SDS Configuration Destinations** page appears.
2. Select the **Update** tab.
   The **Update** tab appears.
3. Enter the destination you want to update in the **Name** field. Click **Lookup**.
   The **Update** tab appears. with the destination information.
4. Edit the **FQDN** and/or **Realm** fields.

   Use the keyword **none** to clear the attribute.

   For more information about these fields, see *Destinations configuration elements*.

   Note: When updating a destination, you are permitted to leave both the **FQDN** and **Realm** empty. This action is permitted and the destination is retained despite having no data for these attributes.

5. Click **Update** to save the changes to the destination.

   When **Update** is clicked and any of the following conditions exist, an error message appears:

   - The entry in any field is not valid (wrong data type).
   - The Destination and its associated change exists.

Deleting destinations

You can only perform this task when logged into the Active Primary SDS.

A Destination cannot be deleted while any routing entity, NAI/Wildcard User, or Destination remains associated with them. Before you perform this task, disable and delete any connections that use the Destination

1. Select **SDS** > **Configuration** > **Destinations**.
   The **SDS Configuration Destinations** page appears.
2. Select the **Delete** tab.
3. Enter a valid destination you want to delete in the **Name** field. Click **Delete**.
   A popup confirmation window appears.
4. Perform one of the following actions:

   - Click **OK** to delete the destination.
   - Click **Cancel** to cancel the delete function and return to the **SDS Configuration Destinations** page.

   If **OK** is clicked and the following condition exists, an error message appears:

   - No updates were made to the database.
   - Field Name contains invalid character(s).
   - Object currently in use; destination is used by a route.
   - Object currently in use; destination is used by a destination map.

Destination map configuration

The **Destination map** page allows you to add, modify, or delete additional data on an existing Destination.

From the **Destination Map** page, you can associate a destination to a HLR Router Network entity.

Destination map configuration elements

The **SDS** > **Configuration** > **Destination Map** page displays information in a tabular format. The following table describes elements on this page.

Table 7: Destination Map Elements

Element	Description	Data Input Notes
Action columns	Selectable columns where you can choose to edit or delete selections	Format: Selectable items
Filter fields	Pulldown menu of available filters and additional fields to modify the search options	Format: Selectable list
Destination	Destination field	Format: Alphanumeric Range: 1–32 characters
Network Entity	The E.164 address of a service node used by HLR Router	Format: Numeric Range: 8–15 characters

Viewing Destination Map connections

Use this page to view the list of Destination Map entries.

Select **SDS** > **Configuration** > **Destination Map**.
The **Destination Map** page appears.

The current destination maps are listed in the destination map table.

Inserting Destination Maps

Use this page to manually add a destination map to the database. A Destination and Network Entity must be provided when adding a Destination Map entry. The Destination value must match a name of an existing Destination entry. The **OK** and **Apply** buttons are disabled until a character is entered into either the Destination or Network Entity field.

Note: You can only perform this task when logged into the Active Primary SDS.

1. Select **SDS** > **Configuration** > **Destination Map**.

The **Destination Map** page appears.

2. Click **Insert**.
   The **Destination Map [Insert]** page appears.
3. Enter a Destination name in the **Destination** field. The name must match a Destination name that has already been entered into the database.
4. Enter a E.164 address for the server node for the **Network Entity** in the Network Entity field.
5. Perform one of the following:
   - Click **OK** to save the destination map and return to the **Destinations Map** page.
   - Click **Apply** to save the destination map and remain on this page.
   - Click **Cancel** to return to the **Destinations Map** page without saving the changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Missing required information in the **Destination** field.
   - Missing required information in the **Network Entity** field.
   - Invalid characters in the **Destination** field.
   - Only digits are allowed in the **Network Entity** field.
   - The **Network Entity** field must contain at least eight digits.
   - Destination not found.
   - The Destination's type must be IMS HSS to have a Destination Map entry.

Editing Destination Maps

Use this page to manually change an existing destination map in the database. The **OK** and **Apply** buttons are disabled until a character is entered into either the Destination or Network Entity field.

You can only perform this task when logged into the Active Primary SDS.

Note: A service node must be provided when modifying a destination map.

1. Select **SDS** > **Configuration** > **Destination Map**.
   The **Destination Map** page appears.
2. Locate the map you want to edit and click **Edit**.
   The **Destination Map [Edit]** page appears.
3. Edit the E.164 address for the server node in the **Network Entity** field.
4. Perform one of the following:
   - Click **OK** to save the destination map and return to the **Destination Map** page.
   - Click **Apply** to save the destination map and remain on this page.
   - Click **Cancel** to return to the **Destination Map** page without saving the changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:
   - Missing required information in the **Network Entity** field.
   - Only digits are allowed in the **Network Entity** field.
   - The **Network Entity** field must contain eight digits.

Deleting Destination Maps

This page allows you to manually delete a destination map from the database. A Destination Map cannot be deleted while any IMSI or MSISDN routing entities remain associated with the destination.

Note: You can only perform this task when logged into the Active Primary SDS.

1. Select **SDS** > **Configuration** > **Destination Map**.
   The **Destination Map** page appears.
2. Locate the map you want to delete and click **Delete**.
   A popup confirmation window appears.
3. Perform one of the following actions:
   - Click **OK** to delete the map.
   - Click **Cancel** to cancel the delete function and return to the **Destination Map** page.

If **OK** is clicked and any of the following conditions exist, and error message appears:

- Destination is in use by a route.

Routing entities configuration

The **Routing Entities** page allows you to manage the supported routing entities:

- IMSI
- MSISDN
- NAI User
- Wildcard NAI User Prefix
- IMSI Prefix
- MSISDN Prefix

Note: A routing entity can be a stand-alone routing entity or a routing entity that is part of a subscriber (group of related routing entities and Account ID values).

From the **SDS Configuration Routing Entities** page, you can perform the following actions:

- Retrieve information for a specific Routing Entity.
- Add a supported Routing Entity.
- Update the information associated with an existing Routing Entity.
- Delete a Routing Entity.

Routing entities configuration elements

This table describes the fields on the Routing Entities Retrieve, Add, Update, and Delete tabs.

Table 8: Routing Entities Configuration Elements

Element	Description	Data Input Notes
Retrieve and Delete tabs		

Element	Description	Data Input Notes
Type	Type of supported routing entity	Format: pulldown list Range: One of the following - MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix
Address (Except WC NAI User)	The routing entity address	Format: alphanumeric and underscore Range: Depends on Type • MSISDN: 8–15 digits • IMSI: 10–15 digits • NAI User: 1–64 characters • MSISDN Prefix and IMSI Prefix: 1 - 15 digits
Address Prefix (WC NAI User Only)	The routing entity address	Wildcard NAI User: 1–64 characters
NAI Host	NAI Host; available only when **NAI User** or **Wildcard NAI User** is selected as the **Type** It is not visible when **Type** is MSISDN, IMSI, MSISDN Prefix, or IMSI Prefix.	Format: pulldown list Range: available NAI Hosts
Add and Update tabs		
Type	Type of supported routing entity	Format: pulldown list Range: One of the following - MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix **Note:** If **Type** is MSISDN or IMSI on the Update tab and the Address is part of a Subscriber that has more than 1 MSISDN or IMSI routing entity, the update is automatically applied to all of the subscriber's MSISDN and IMSI routing entities
Address (Except WC NAI User)	The routing entity address	Format: alphanumeric and underscore Range: Depends on Type • MSISDN: 8–15 digits • IMSI: 10–15 digits • NAI User: 1–64 characters • MSISDN Prefix and IMSI Prefix: 1 - 15 digits
Address Prefix (WC NAI User Only)	The routing entity address	Wildcard NAI User: 1–64 characters

Element	Description	Data Input Notes
NAI Host	NAI Host; available only when **NAI User** or **Wildcard NAI User** is selected as the **Type** It is not visible when **Type** is MSISDN, IMSI, MSISDN Prefix, or IMSI Prefix.	Format: pulldown list Range: available NAI Hosts
IMS HSS (available on the Add tab only)	IMS HSS destination	Format: pulldown list Range: available IMS HSS destinations
LTE HSS (available on the Add tab only)	LTE HSS destination	Format: pulldown list Range: available LTE HSS destination
PCRF (available on the Add tab only)	IMS HSS destination	Format: pulldown list Range: available PCRF destinations
OCS (available on the Add tab only)	IMS HSS destination	Format: pulldown list Range: available OCS destinations
OfCS (available on the Add tab only)	IMS HSS destination	Format: pulldown list Range: available OfCS destinations
AAA (available on the Add tab only)	IMS HSS destination	Format: pulldown list Range: available AAA destinations
User defined 1 (available on the Add tab only)	IMS HSS destination	Format: pulldown list Range: available User defined 1 destinations
User defined 2 (available on the Add tab only)	IMS HSS destination	Format: pulldown list Range: available User defined 2 destinations

Retrieving routing entities

You can perform this task when logged into an SDS or from the DP SOAM GUI.

Before performing this task, make sure that Destinations and NAI Hosts have been configured.

1. Select **SDS** > **Configuration** > **Routing Entities**.
   The **SDS Configuration Routing Entities** page appears.

By default, the **Retrieve** tab is the viewable tab. If not, select the **Retrieve** tab.

2. Select the type of routing entity from the **Type** pulldown list.
3. Enter the route identifier for the routing entity in the **Address** or **Address Prefix** field.

   Note: The **Address** field requirements depend on the type of blacklist routing entity. For more information on this field, see *Blacklist configuration elements*.

4. If NAI User or Wildcard NAI User is selected as the **Type**, select a NAI host from the **NAI Host** pulldown list.
5. Click **Retrieve**.

   When **Retrieve** is clicked and the following condition exists, an error message appears:

   - If either MSISDN or IMSI was selected as the **Type**, and a non-digit character was entered.
   - Field Address contains invalid characters.

Adding routing entities

You can only perform this task when logged into the Active Primary SDS.

Before performing this task, make sure that Destinations and NAI Hosts have been configured.

1. Select **SDS** > **Configuration** > **Routing Entities**.
   The **SDS Configuration Routing Entities** page appears.
2. Select the **Add** tab.
3. Select the type of routing entity from the **Type** pulldown list.
4. Enter the route identifier for the routing entity in the **Address** or **Address Prefix** field.

   Note: The **Address** field requirements depend on the type of blacklist routing entity. For more information on this field, see *Blacklist configuration elements*.

5. If NAI User or Wildcard NAI User is selected as the **Type**, select a NAI host from the **NAI Host** pulldown list.
6. Select the associated destination(s) from the applicable destination(s) pulldown list.

   At least one destination must be selected, although a destination can selected for each of the destination types.

7. Click **Add**.

   When **Add** is clicked and any of the following conditions exist, an error message appears:

   - Either MSISDN or IMSI was selected as the **Type** and a non-digit character was entered.
   - At least one destination was not selected.
   - Field Address contains invalid characters.

Updating routing entities

You can only perform this task when logged into the Active Primary SDS.

1. Select **SDS** > **Configuration** > **Routing Entities**.
   The **SDS Configuration Routing Entities** page appears.

2. Select the **Update** tab.
3. Select the type of routing entity from the **Type** pulldown list.
4. Enter the route identifier for the routing entity in the **Address** or **Address Prefix** field.

   Note: The **Address** or **Address Prefix** field requirements vary depending on the type of routing entity. For more information on this field, see *Routing entities configuration elements*.

5. If NAI User or Wildcard NAI User is selected as the **Type**, select a NAI host from the **NAI Host** pulldown list.
6. Click **Lookup**.

   Note: If the route was not located during the **Lookup**, an error message appears.

   The **Update** tab appears with the routing entity information.
7. Edit the appropriate destination(s).

   For more information about these fields, see *Routing entities configuration elements*.

   Note: Although at least one destination is required when adding a routing entity, there is no minimum requirement for destinations when updating the routing entity. For example, all of the destinations could possibly be set to NONE

8. Click **Update**.

Deleting routing entities

You can only perform this task when logged into the Active Primary SDS.

1. Select **SDS** > **Configuration** > **Routing Entities**.
   The **SDS Configuration Routing Entities** page appears.
2. Select the **Delete** tab.
3. Select the type of routing entity from the **Type** pulldown list.
4. Enter the route identifier for the routing entity in the **Address** or **Address Prefix** field.

   Note: The **Value** field requirements depend on the type of identifier. For more information about this field, see *Subscribers elements*.

5. If NAI User or Wildcard NAI User is selected as the **Type**, select a NAI host from the **NAI Host** pulldown list.

   If **Type** is MSISDN or IMSI and the Address is part of a Subscriber that has more than 1 MSISDN and/or IMSI value, only the entered value is deleted (not all routing entities for the subscriber). If you want to delete the whole subscriber, you must do this from the **SDS** > **Configuration** > **Subscriber [Delete]**.

   If **Type** is MSISDN or IMSI and the Address is part of a Subscriber that has only 1 MSISDN or IMSI value, the routing entity will not be deleted; the subscriber must be deleted.

6. Click **Delete**.
   A popup confirmation window appears.
7. Perform one of the following actions:

   - Click **OK** to delete the connection.

- Click **Cancel** to cancel the delete function and return to the **SDS Configuration Routing Entities** page.

If **OK** is clicked and any of the following conditions exist, an error message appears:

- Either MSISDN or IMSI was selected as the **Type** and a non-digit character was entered in the **Route** field
- The route identifier was not found.
- Field Address contains invalid characters.

Subscribers

SDS Subscriber Identity Grouping (**Subscribers** page) allows you to group a customer-specified account ID, multiple MSISDN routing entities and multiple IMSI routing entities together into one Subscriber. After a Subscriber (a group of related routing entities and an optional Account ID value) is created, you can update destinations for all of the related routing entities, read all data from the subscriber and delete the subscriber by using any of the subscriber's addresses (for example, account ID, MSISDN, or IMSI). You can also modify addresses within a subscriber by specifying any of the subscriber's addresses.

Restrictions:

- This is a provisioning-only feature.
- The relationships between routing entities is only available on A-level servers, which are the SDS servers and the Query server.

The following restrictions apply to all Subscribers that contain a group of related MSISDN and IMSI routing entities and an optional Account ID. These rules do not apply to stand-alone routing entities.

- Every subscriber must have at least 1 routing entity (MSISDN or IMSI).
- All of the subscriber's routing entities must have the same destination values.
- Every subscriber can be accessed by specifying any of its routing entity values or its Account ID value.
- When you create a new subscriber, destinations are optional. If you do not specify a destination, destinations are set based upon the existing routing entities.
- All provisioning commands are for a single subscriber. All specified accountid, imsi, and msisdn values must be assigned to one subscriber or they can exist in a stand-alone routing entity.

From the **Subscriber** page, you can do the following:

- Retrieve information for a specific Subscriber.
- Create a Subscriber.
- Modify a previously defined Subscriber.
- Delete a selected Subscriber.

Subscribers elements

Use the **SDS Configuration Subscribers** page to manage SDS Subscribers. This table describes fields on this page.

Table 9: Subscribers Elements

Element	Description	Data Input Notes
Field	Type of data in the Value field used to find desired Subscriber (Account ID, MSISDN, IMSI)	Format: pulldown list One of the following - Account ID, MSISDN, or IMSI Default: Account ID
Value	The value of the Account ID, MSISDN or IMSI values for the subscriber	Format: Integer Range limits depends on Field value: • Account ID: 1-26 digits • MSISDN: 8-15 digits • IMSI: 10-15 digits Default: blank

Retrieving subscribers

Use this process to retrieve information about a single Subscriber and all of the Subscriber's routing entities.

You can perform this task when logged into an SDS or from the DP SOAM GUI.

Before performing this task, make sure that Destinations have been configured.

1. Select **SDS** > **Configuration** > **Subscribers**.
   The **SDS Configuration Subscribers** page appears.

   By default, the **Retrieve** tab is the viewable tab. If not, select the **Retrieve** tab.
2. Select the type of identifier from the **Field** pulldown list.
3. Enter the identifier for the subscriber in the **Value** field.

   Note: The **Value** field requirements depend on the type of identifier. For more information about this field, see *Subscribers elements*.
4. Click **Retrieve**.

   When **Retrieve** is clicked and the following condition exists, an error message appears:

   • A non-digit was entered for the **Value** field.

Creating Subscribers

Use this process to create a new subscriber and group the specified MSISDN, IMSI, and Account ID values into one Subscriber record. The specified MSISDN and IMSI values can be for existing stand-alone or new MSISDN or IMSI routing entities. If the MSISDN or IMSI value does not exist as a stand-alone routing entity, the routing entity is automatically added, and the MSISDN or IMSI value is added to

the Subscriber. All destination values from existing stand-alone routing entities must be the same prior to applying the values that you enter on the **Subscribers Create** page.

Specifying destinations is optional. You can check the Inherit Destinations checkbox to inherit the current destination values from a subscriber's existing routing entity.

Before performing this task, make sure that Destinations have been configured.

If no MSISDN or IMSI values currently exist as a stand-alone entry, then at least one destination must be provided.

At least one MSISDN or IMSI value must exist for the Subscriber.

1. Select **SDS** > **Configuration** > **Subscribers**.
   The **SDS Configuration Subscribers** page appears.
2. Select the **Create** tab.
3. Enter an **Account ID** to associate a unique number to the Subscriber's account.
   Note: This is an optional field and contains a value 1-26 digits in length.
4. Enter MSISDN values to associate MSISDNs with the subscriber. Click **Add**, **Remove**, or **Clear All** to implement your updates. A maximum of 6 MSISDNs are supported. At least one destination must be provided when creating a new MSISDN or IMSI.
5. Enter IMSI values to associate IMSIs with the subscriber. Click **Add**, **Remove**, or **Clear All** to implement your updates. A maximum of 6 IMSIs are supported. At least one destination must be provided when creating a new MSISDN or IMSI.
6. Optionally, select **Inherit Destination** to inherit the current destination values from a subscriber's existing routing entity.
   Note: The base field set info that appears here is for display purposes only. See *Subscribers elements* for more information on each field.
7. Select from any of the following pulldown lists to name one of each type of destination.
   - **IMS HHS**
   - **LTE HSS**
   - **PCRF**
   - **OCS**
   - **OfCS**
   - **AAA**
   - **User defined 1**
   - **User defined 2**

Modifying Subscribers

This page allows you to locate and modify a single Subscriber.

Use this procedure to update the identification (MSISDN, IMSI, and Account ID) values for a Subscriber and/or update the Subscriber's destination values.

1. Select **SDS** > **Configuration** > **Subscribers**.
   The **SDS Configuration Subscribers** page appears.
2. Select the **Modify** tab.

The **SDS Configuration Subscribers** page appears.

3. Select the type of identifier from the **Field** pulldown menu (Account ID, MSISDN, or IMSI).
4. Enter one of the Account ID, MSISDN or IMSI values for the subscriber in the **Value** field. For more information about this field, see *Subscribers elements*.

   Note: The **Value** field requirements depend on the type of identifier data. For more information about this field, see *Subscribers elements*.

5. Click **Lookup**.
   If the Subscriber is located, this page will be populated with information previously defined for the selected Subscriber. At least one MSISDN or IMSI value must exist for the Subscriber. For more information about these fields, see *Creating Subscribers*.

   Note: Destinations must be configured before you can enter a route using them.

6. Modify the fields on this page as needed.
7. Click **Modify** to complete the task.
   A popup confirmation appears to complete the task.

Deleting Subscribers

Follow these steps to delete the Subscriber and all of the Subscriber's routing entities.

Note: Global Data Delete permission is required for this function.

1. Select **SDS** > **Configuration** > **Subscriber**.
   The **SDS Configuration Subscriber** page appears.
2. Select the **Delete** tab.
3. Select the type of identifier data from the **Field** pulldown list.
4. Enter the identifier for the subscriber in the **Value** field.

   Note: The **Value** field requirements depend onthe type of identifier. For more information about this field, see *Subscribers elements*.

5. Click **Delete**.
   A popup confirmation window appears.
6. Perform one of the following actions:

   - Click **OK** to delete the Subscriber.
   - Click **Cancel** to cancel the delete function and return to the **SDS Configuration Subscriber** page.

   After you press **Delete**, a warning dialog box is displayed that indicates that all associated MSISDNs and IMSIs will also be deleted.

Blacklist

The Blacklist function (**Blacklist** page) allows you to provision IMSI and MSISDN Blacklist values that can be searched prior to searching the MSISDN or IMSI Routing Entities to determine if a value is blacklisted.

Both MSISDN and IMSI blacklist data is supported in SDS/DP systems.

From the SDS Configuration **Blacklist** page, you can perform the following actions:

- Retrieve a previously defined blacklist value
- Add a new blacklist value
- Delete an existing blacklist value

Blacklist configuration elements

This table describes the fields on the Blacklist Retrieve, Add, and Delete tabs.

Table 10: Blacklist Configuration Elements

Element	Description	Data Input Notes
Type	Type of routing entity to blacklist	Format: pulldown list Range: One of the following - MSISDN or IMSI
Address	The routing entity address	Format: alphanumeric and underscore Range: Depends on Type • MSISDN: 8–15 digits • IMSI: 10–15 digits

Retrieving blacklist values

Follow these steps to retrieve a single MSISDN or IMSI Blacklist value. These are values that will not be routed to a destination.

1. Select **SDS** > **Configuration** > **Blacklist**.
   The **SDS Configuration Blacklist** page appears.

   By default, the **Retrieve** tab is the viewable tab. If not, select the **Retrieve** tab.

2. Select the type of blacklist routing entity from the **Type** pulldown list.
3. Enter the route identifier for the routing entity in the **Address** field.

   Note: The **Address** field requirements depend on the type of blacklist routing entity. For more information on this field, see *Blacklist configuration elements*.

4. Click **Retrieve**.

   When **Retrieve** is clicked and the following condition exists, an error message appears:

   - If a non-digit character was entered.

Adding blacklist values

Follow these steps to add a single MSISDN or IMSI Blacklist value. These are values that will not be routed to a destination.

1. Select **SDS** > **Configuration** > **Blacklist**.
   The **SDS Configuration Blacklist** page appears.
2. Select the **Add** tab.
3. Select the type of blacklist routing entity from the **Type** pulldown list.
4. Enter the blacklist route identifier for the routing entity in the **Address** field.

   Note: The **Address** field requirements depend on the type of blacklist routing entity. For more information on this field, see *Blacklist configuration elements*.

   Note: .

5. Click **Add**.

   When **Add** is clicked and any of the following conditions exist, an error message appears:

   - If a non-digit character was entered.
   - The value entered for the MSISSDN or IMSI value already exists in the routing entities table.

Deleting blacklist values

Follow these steps to delete a single MSISDN or IMSI Blacklist value.

Note: Global Data Delete permission is required for this function.

1. Select **SDS** > **Configuration** > **Blacklist**.
   The **SDS Configuration Blacklist** page appears.
2. Select the **Delete** tab.
3. Select the type of blacklist routing entity from the **Type** pulldown list.
4. Enter the blacklist route identifier for the routing entity in the **Address**.

   Note: The Value field requirements depend on the type of blacklist routing entity. For more information about this field, see *Blacklist configuration elements*

5. Click **Delete**.
   A popup confirmation window appears.
6. Perform one of the following actions:

   - Click **OK** to delete the blacklist.
   - Click **Cancel** to cancel the delete function and return to the **SDS Configuration Blacklist** page.

   If **OK** is clicked and any of the following conditions exist, an error message appears:

   - If a non-digit character was entered.
   - The route identifier was not found.
   - **Address** contains invalid characters.

Chapter 4

Maintenance

Topics:

The **Maintenance** menu options allow you to query and audit data, view up-to-date status of the database and various features, initiate import and exports.

From the maintenance menu on an SDS you can:

- Query the database for specified:
  - MSISDN
  - MSISDN Prefix
  - MSISDN Blacklist
  - IMSI
  - IMSI Prefix
  - IMSI Blacklist
  - NAI user
  - Wildcard NAI user ranges
- View provisioning connections, command logs, relay exception logs, and the status of imports and exports
- Configure and manage NPA Splits
- Schedule exports
- Perform remote audits

When you are logged into an DP SOAM you cannot request a remote audit, update splits, or schedule an export on the DP SOAM GUI.

The available menu options will vary based on the type of server you are logged into and the permissions assigned to your group. If you do not see a menu option you need, please make sure you are logged into the appropriate type of server and ask your administrator to make sure the group your user ID belongs to has the appropriate permissions.

The **SDS Maintenance** pages provide maintenance information related to provisioning connections and data. With this page you can monitor provisioning

connections; view every provisioning message exchanged between provisioning systems in the command log, view the status of imports and exports; open import and export files and import result logs.

All provisioning maintenance tasks are only available when logged into an SDS.

Connections maintenance

The **SDS -> Maintenance -> Connections** page allows you to view the "currently in-use" external connections. A list of all provisioning connections established to the system can be viewed. A display filter can be applied for a specified search. The information is displayed in tabular format.

Any local connections (including the one from the GUI itself) are not included.

Connections maintenance elements

The **SDS -> Maintenance -> Connections** page displays information in a tabular format. *Table 11: Connections Maintenance Elements* describes elements on the **SDS -> Maintenance -> Connections** page.

Table 11: Connections Maintenance Elements

Field	Definition	Data Notes
Timestamp	Time the connection was established	Format: Year-Month-Day Hour-Minute-Second
CID	Connection ID	N/A
Remote IP	IP address for the remote client	Format: Valid IP address Range: Either an IPv4 or an IPv6 IP address. IPv4 addresses are 32 bits, represented in a dot-decimal notation like this: x.x.x.x where each x (called an octed) is a decimal value from 0 to 255. They are separated by periods. For example: 1.2.3.4 and 192.168.0.100 are valid IPv4 addresses. IPv6 addresses are 128 bits, represented in a colon-hexadecimal notation like this: z:z:z:z:z:z:z:z where each z is a group of hexadecimal digits ranging from 0 to ffff. They are separated by colons. Leading zeros may be omitted in each group. "::" can be used (at most once) in an IPv6 address to represent a range of as many zero fields as needed to populate the address to eight fields. So the IPv6 address

Field	Definition	Data Notes
		2001:db8:c18:1:260:3eff:fe47:1530 can also be represented as 2 001:0db8:0c18:0001:0260:3eff:0fe 47:1530 and the IPv6 address ::1 is the same as 0000:0000:0000:0000:0000:0000:0000:0001
Remote Port	Port used for the remote client connection	Format: Valid port number
Version	Version of API this client application is using	Default: 1.0
Cnx Manager	Connection manager	Options: Pdba, Xds, XmlImport, XmlExport, PdbRelay, PdbAudit
Txn Mode	Database transaction mode	Range: • normal: All updates must be sent inside a transaction explicitly begun and ended by begin_txn and end_txn/abort_txn requests respectively. • single: Transactions are implicitly begun and ended for individual update requests Default: normal
Idle Timeout	Number of minutes the connection can be idle before it is automatically timed out.	Range: • 0 (the connection is never terminated) • 1 - 44640 minutes Default: 0

Viewing connections status

Use this task to view a list of information of all provisioning connections established to the system. The listing of connections may be filtered.

1. Select **SDS** > **Maintenance** > **Connections**.

   The **SDS Maintenance Connections** page appears. All provisioning connections are displayed in tabular form. The fields are described in *Connections maintenance elements*.

2. Select the category by which to perform the filtering.

Table 12: Connection Status filtering categories

Category	Desscription
Timestamp	Time the connection was established.
CID	The Connection ID to filter on.
Remote IP	IP address for the remote client.
Remote Port	Port used for the remote client connection.
Version	Version of API this client application is using.
Txn Mode	Database transaction mode.
Idle Timeout	Number of minutes the connection can be idle before it is automatically timed out.

3. Choose the filtering operator.

Table 13: Connection Status filtering operators

Operator	Description
=	Is equal to
!=	Is not equal to
>	Is greather than
>=	Is equal to or greater than
<	Is less than
<=	Is equal to or less than
Like	Is Like (wildcard is * character)
Is Null	has no entry (is zero)

4. Enter the target character string to filter on in the text box.
5. Use Auto Refresh to select the time interval for the status to be refreshed.

Table 14: Connection status refresh time

Time	Description
15	15 seconds
30	30 seconds
Off	Off (default)

6. Click **Go** to show results.

Command Log maintenance

The **SDS -> Maintenance -> Command Log** page shows a table that contains a history of commands and their responses. This table shows the **Timestamp**, **System ID**, **CID**, and the **Text** of the commands received from both remote and local connections, including the GUI.

Every provisioning message exchanged between provisioning systems is written to the command log and is stored for up to seven days.

Command Log maintenance elements

The **SDS -> Maintenance -> Command Log** page displays information in a tabular format. This table describes elements on the **SDS -> Maintenance -> Command Log** page.

Table 15: Command Log Maintenance Elements

Element	Description
Timestamp	Date and time the command was logged
System ID	System identifier of the originating client
CID	Client connection identifier
Text	Exact command and response message

Viewing maintenance command logs history

Use this task to view a list of information of a history of commands and their responses. The history is displayed as a table that shows the **Timestamp**, **System ID**, **CID**, and the **Text** of the commands received from both remote and local connections, including the GUI. The history may be filtered by category.

Note: You can check mark the **Pause updates** check box to temporarily stop this command log from being updated.

1. Select **SDS** > **Maintenance** > **Command Log**.
   The **SDS Maintenance Command Log** page appears.
2. Select the category by which to perform the filtering.

   Table 16: Command Log filtering categories

Category	Description
None	Show all commands
System ID equal to...	A hidden text box becomes visible for you to enter the System ID to filter on.
CID equal to...	A hidden text box becomes visible for you to enter the Connection ID to filter on.

Category	Description
Log text contains...	A hidden text box becomes visible for you to enter one or more keywords to filter on.
Error responses	Shows all commands with error responses.
Time range...	When selected, hidden select boxes for "**From**" and "**To**" times become visible for you to enter the time range to filter on.

3. Click **Display** to show results.

   When results are filtered, the highlighted text, RESULTS FILTERED, is displayed at the bottom of the results.

Relay Exception Log

The **SDS** > **Maintenance** > **Relay Exception Log** page shows a table containing all types of exceptions (unexpected results) found while processing SDS to HLRR relay or export functionality. Consequently, all fields do not always contain data. All entries in the Relay Exception Log contain enough data so that you can determine what SDS data caused the exception.

Ideally, the Relay Exception Log would be empty, which means that SDS has all of the data required to create an HLRR provisioning command and all of the required Network Entities are provisioned for the HLR Router. Because the most likely cause of an error would be associated with relaying new provisioning commands to HLRR, the Relay Exception Log displays column headings for exceptions created by pdbrelay. Deviations for other creators include:

- If no command is relayed to HLRR, the Derived Relay Request value is `None.`
- If the Creator value is not equal to `pdbrelay`, the Derived Relay Request value from the SDS Command Log section is blank.

Relay Exception Log maintenance elements

The **SDS** > **Maintenance** > **Relay Exception Log** page displays information in a tabular format. This table contains a list of exceptions found while processing data that should be relayed from SDS to HLRR.

Note: Display limit must be a numeric integer greater than zero.

The following table describes elements on the **SDS** > **Maintenance** > **Relay Exception Log** page.

Table 17: Exception Log Maintenance Elements

Element	Description
Timestamp	Date and time when the exception occurred
Seq Num	Exception sequence number
Creator	Name of process that created the exception

Element	Description
Reason	Reason that the exception was created
Derived Relay Request	Command created and relayed to HLR Router
Command	Command text from the SDS Command Log
Seq Num	Sequence number form the SDS Command Log
Timestamp	Timestamp from the SDS Command Log

Viewing exception logs history

Use this task to view a list of information of a history of commands and their responses. The history is displayed as a table that shows the **Timestamp**, **System ID**, **CID**, and the **Text** of the commands received from both remote and local connections, including the GUI. The history may be filtered by category.

Note: You can check mark the **Pause updates** check box to temporarily stop this command log from being updated.

1. Select **SDS** > **Maintenance** > **Relay Exception Log**.
   The **SDS Relay Exception Log** page appears.
2. Select the category by which to perform the filtering.

   Table 18: Relay Exception Log filtering categories

Category	Description
None	Show all commands
Exception Seq Num equal to...	A hidden text box becomes visible for you to enter the Exception Sequence Number to filter on.
Exception Creator equal to...	A hidden text box becomes visible for you to enter the Exception Creator to filter on.
Exception Reason text contains...	A hidden text box becomes visible for you to enter one or more Exception Reasons keywords to filter on.
Exception Time range...	When selected, hidden select boxes for "**From**" and "**To**" times become visible for you to enter the time range to filter on.
Command text contains...	A hidden text box becomes visible for you to enter Command text to filter on.

3. Click **Display** to show results.

   When results are filtered, the highlighted text, RESULTS FILTERED, is displayed at the bottom of the results.

Import Status maintenance

Allows an operator to view the status of all Imports.

Data can be imported from a provisioning import file to add new, or update existing, data in the database. Imports are not scheduled through the user interface but import settings are configured with the provisioning options page.

Import files that are placed in a specific location on a remote serverr (**Remote Import Directory**) are detected within five minutes and automatically downloaded via SSH File Transfer Protocol (SFTP) to the file management storage area. For a file to be imported, it must:

- be properly named following the naming convention. For more information see the SDS Administration Manual.
- have been placed in the remote directory after the time when provisioning import last ran
- must not have been previously imported. A file that has already been imported into the local directory will not be imported again, even if its status is Failed.

  Note: To import a previously Failed file, correct the file as necessary, rename the file, and then place the renamed file in the remote directory.

Once fully downloaded, each file is automatically imported into the Provisioning Database sequentially in the order in which their download completed. The provisioning import file is an ASCII text file that contains a series of database manipulation requests in provisioning format.

The **SDS Maintenance Import Status** page allows you to view the status of provisioning imports. Import records with a status of Completed or Failed can be deleted from this table.

Import Status maintenance elements

The **SDS -> Maintenance -> Import Status** page displays information in a tabular format. *Table 19: Import Status Maintenance Elements* describes elements on the **SDS -> Maintenance -> Import Status** page.

Table 19: Import Status Maintenance Elements

Field	Description
Action	Allows user to delete import file entries.
Import File	Name of import file
Time Queued	Time the import was queued
Time Started	Time the import started
Time Completed	Time the import completed
Progress	Percentage of import progress
Result Log	Name/heading of result log
Pass Count	The number of successful import commands

Field	Description
Fail Count	The number of unsuccessful import commands
Status	Status of the import

Viewing import files

This task allows you to view the status of all Imports. Imports are not scheduled through the GUI. They are initiated by the presence of a file placed in the Remote Import Directory.

- If the filename in the **Import File** or **Result Log** column exceeds 24 characters, it is truncated at 22 characters and the characters "..." are appended to the end of the truncated string to signify that the filename was truncated.
- The filenames in both the **Import File** or **Result Log** columns are hyperlinks. You can click on the links to view the files as text or to save them locally.
- You cannot edit an imported file using this form.
- You may delete an Import Status record if the **Status** is **Completed**, or **Failed**.

1. Select **SDS** > **Maintenance** > **Import Status**.

   The **SDS Maintenance Import Status** page appears. All provisioning connections are displayed in tabular form. The display fields are described in *Import Status maintenance elements*.

2. Select the category by which to perform the filtering.

   Table 20: Import Status filtering categories

Category	Description
Time Queued	Time the import was queued
Time Started	Time the import started
Time Completed	Time the import completed
Progress	Percentage of import progress
Pass Count	The number of successful import commands
Fail Count	The number of unsuccessful import commands
Status	Status of the import

3. Choose the filtering operator.

   Table 21: Connection Status filtering operators

Operator	Description
=	Is equal to
!=	Is not equal to
>	Is greater than

Operator	Description
>=	Is equal to or greater than
<	Is less than
<=	Is equal to or less than
Like	Is Like (wildcard is * character)
Is Null	has no entry (is zero)

4. Enter the target character string to filter on in the text box.
5. Use Auto Refresh to select the time interval for the status to be refreshed.

Table 22: Connection status refresh time

Time	Description
15	15 seconds
30	30 seconds
Off	Off (default)

6. Click **Go** to show results.
7. To delete an import record, click on the associated **Delete** link.

   Note: The import record can only be deleted if the **Status** is **Completed** or **Failed**. A popup confirmation dialog appears. For all other imports, the **Delete** action is inactive (grayed-out).

   A confirmation dialog to complete the delete action appears. For all other imports, the **Delete** action is inactive (grayed-out).

Export maintenance

Provisioning data can be exported to an ASCII file in either XML or CVS format using the application user interface. The **SDS Maintenance Export** pages allow you to view the status, progress, and data count information for scheduled provisioning exports. You may use exported records to do data manipulation of subscriber data.

Note: Export is a time consuming operation recommended to be scheduled during off-peak hours. SDS operators can schedule one-time or recurring exports.

Exported data may also be offloaded to a remote server. The exported text file is also available to be downloaded from the 'file transfer area'. Export is a periodic task. Any changes done to export table shall take effect on next export period. The following is the functionality of Export:

- You can configure and schedule data export on a daily, weekly or monthly basis.
- The exported files will be sFTPed or transferred via SSH to a server configured on SDS.
- Data can be exported to a file in XML commands or CSV format.

- You can export subscriber data (in XML or CSV format) as shown in *Table 23: Interfaces for Subscriber Data Types*:

Table 23: Interfaces for Subscriber Data Types

Subscriber Data Type	GUI (add, change, delete and query)	SOAP and/or XML (add, change, delete and query)	XML Export and Import	CSV Export and Import	SQL Query (from Query Server)	HLRR
MSISDN	yes	yes	yes	yes	yes	yes
IMSI	yes	yes	yes	yes	yes	yes
NAI User	yes	yes	yes	yes	yes	no
Wildcard NAI User	yes	no	no	yes	yes	no
NAI Host	yes	no	no	yes	yes	no
Destination	yes	no	no	yes	yes	no
Destination Map	yes	no	no	no	yes	no
MSISDN Prefix	yes	no	no	yes	yes	no
IMSI Prefix	yes	no	no	yes	yes	no
MSISDN Blacklist	yes	no	no	yes	yes	no
IMSI Prefix	yes	no	no	yes	yes	no
Subscriber	yes	yes	yes	yes	yes	no

Schedule

The **SDS -> Maintenance -> Export -> Schedule** page displays information in a tabular format for all exports scheduled for this system.

Export Schedule maintenance elements

Table 24: Export Schedule Maintenance Elements describes elements on the **SDS -> Maintenance -> Export -> Schedule** page.

Table 24: Export Schedule Maintenance Elements

Field	Description
Action	Edit or Delete scheduled export
Identifier	Name of export file
File format	Format of the export file (CSV, XML, or HLRR)
Export Data	Type of data to export
First Export	The first time this export is scheduled to run
Next Export	The next time this export is scheduled to run
Repeat	How often to repeat export
Comment	Purpose of export

Additionally, you can insert an export schedule by clicking on the **[Insert]** button on the page.

Viewing export schedule

The **SDS -> Maintenance -> Export -> Schedule** page shows the scheduled exports for this system.

1. Select **SDS -> Maintenance -> Export -> Schedule**.

   The **SDS Maintenance Export Schedule** page appears. All exports are displayed in tabular form. The display fields are described in *Export Schedule maintenance elements*.

   - Click on the **[Insert]** button, located on the bottom of the page, to insert a new export schedule.
   - Click **Edit** in the **Action** column on an export record to edit that export.
   - Click **Delete** in the **Action** column on an export record to delete that export.

2. Select the category by which to perform the filtering.

   Table 25: Export Schedule filtering categories

Field	Description
Identifier	Name of export file
File format	Format of the export file (CSV, XML, or HLRR)
Export Data	Type of data to export
First Export	The first time this export is scheduled to run
Next Export	The next time this export is scheduled to run
Repeat	How often to repeat export
Comment	Purpose of export

3. Choose the filtering operator.

Table 26: Export Schedule filtering operators

Operator	Description
=	Is equal to
!=	Is not equal to
>	Is greather than
>=	Is equal to or greater than
<	Is less than
<=	Is equal to or less than
Like	Is Like (wildcard is * character)
Is Null	has no entry (is zero)

4. Enter the target character string to filter on in the text box.
5. Click **Go** to show results.

Inserting an export schedule

The **SDS** > **Maintenance** > **Export** > **Schedule [Insert]** page allows you to create an export for this system.

The field or fields highlighted in yellow are keys and must be unique within this table in order to be successful. Fields marked with a red asterisk (*) require a value.

1. Select **SDS** > **Maintenance** > **Export** > **Schedule**.
   The **SDS Maintenance Export Schedule** page appears.
2. Click on the **[Insert]** button located on the bottom of the page.
   The **SDS Maintenance Insert Export Schedule** page appears.
3. Enter an identifying string for the scheduled export in the **Identifier** text box.
   The identifier must be 4 to 12 characters.
4. Use the radio buttons **csv**, **xml**, or **hlrr** to choose the **File Format** of the export file.
5. From the **Export Data** drop down list, select the type of data to be exported.
   The available type data selections are csv or xml file format.

Table 27: Export Data Types

Type of Data	csv Format	xml Format	hlrr Format
All	all formats listed	all formats listed	all formats listed
MSISDN	X	X	X
MSISDN Blacklist	X		
MSISDN Prefix	X		
IMSI	X	X	X

Type of Data	csv Format	xml Format	hlrr Format
IMSI Blacklist	X		
IMSI Prefix	X		
NAI User	X	X	
Wildcard NAI User	X		
NAI Host	X		
Destinations	X		
Subscribers	X	X	

Note: For HLRR-formatted exports of "All" data, a pop-up appears warning that, because of updates to the PDB Relay Timestamp, the HLRR-formatted exports must only be run as part of the HLR Router Bulk Load Procedure.

Note: For HLRR-formatted exports of "All" data, the PDB Relay feature must be disabled before an export will succeed.

6. Use the appropriate drop down list to select the initial date at which this export should run.
7. Use the appropriate drop down list to select the initial time at which this export should run.
8. Use the appropriate drop down list to select how often this export should be repeated.
9. In the Comment text box, enter text that may be used to describe the purpose of this export.

   Note: You can enter up to 255 characters for a comment.

10. Perform one of these actions:
    - Click **OK**. If field validations succeed, the new export is saved and the previous page appears. If the page contains any values that are not valid, or if a required field is empty, an error message appears.
    - Click **Apply**. If field validations succeed, the new export is saved and you remain on the same page.
    - Click **Cancel** to abort changes on this page and return to the previous page.

Editing an export schedule

The **SDS -> Maintenance -> Export -> Schedule [Edit]** page allows you to manually change an existing export job by editing an entry in the Export Schedule.

The field or fields highlighted in yellow are keys and must be unique within this table in order to be successful. Fields marked with a red asterisk (*) require a value.

1. Select **SDS -> Maintenance -> Export -> Schedule**.

   The **SDS Maintenance Export Schedule** page appears.

2. Click **Edit** in the **Action** column of the export record to be edited.

   The **SDS Maintenance Edit Export Schedule** page appears.

3. Enter an identifying string for the scheduled export in the **Identifier** text box.

The identifier must be 4 to 12 characters.

4. Use the radio buttons **csv**, **xml** or **hlrr** to choose the **File Format** of the export file.
5. From the **Export Data** drop down list, select the type of data to be exported.

   The available type data selections are csv and xml file format.

   Table 28: Export Data Types

Type of Data	csv Format	xml Format	hlrr Format
All	all formats listed	all formats listed	all formats listed
MSISDN	X	X	X
MSISDN Blacklist	X		
MSISDN Prefix	X		
IMSI	X	X	X
IMSI Blacklist	X		
IMSI Prefix	X		
NAI User	X	X	
Wildcard NAI User	X		
NAI Host	X		
Destinations	X		
Subscribers	X	X	

6. Use the appropriate drop down list to select the initial date at which this export should run.
7. Use the appropriate drop down list to select the initial time at which this export should run.
8. Use the appropriate drop down list to select how often this export should be repeated.
9. In the Comment text box, enter text that may be used to describe the purpose of this export.

   Note: You can enter up to 255 characters for a comment.

10. Perform one of these actions:

    - Click **OK**. If field validations succeed, the new export is saved and the previous page appears. If the page contains any values that are not valid, or if a required field is empty, an error message appears.
    - Click **Apply**. If field validations succeed, the new export is saved and you remain on the same page.
    - Click **Cancel** to abort changes on this page and return to the previous page.

Deleting an export schedule

The **SDS -> Maintenance -> Export -> Schedule [Delete]** page allows you to manually delete an export job by deleting an entry from the Export Schedule Table.

1. Select **SDS -> Maintenance -> Export -> Schedule**.

   The **SDS Maintenance Export Schedule** page appears.

2. Click **Delete** in the **Action** column of the export record to be deleted.

   A confirmation dialogue box opens, "Are you sure you want to delete this row?"

   - Click **OK** to confirm the action to delete the export record and return to the **SDS -> Maintenance -> Export -> Schedule** page.
   - Click **Cancel** to abort the delete action and return to the **SDS -> Maintenance -> Export -> Schedule** page.

Status

The **SDS -> Maintenance -> Export -> Status** page displays information in a tabular format and shows all in-progress and completed scheduled exports in this system.

Export Status maintenance elements

Table 29: Export Status Maintenance Elements describes elements on the **SDS -> Maintenance -> Export -> Status** page.

Table 29: Export Status Maintenance Elements

Field	Description
Export File	Name of export file
Time Queued	Time the export was queued
Time Started	Time the export started
Time Completed	Time the export completed
Subscribers	Number of exported Subscribers
MSISDNs	Number of MSISDNS exported
IMSIs	Number of IMSIs exported
MSISDN Prefix	Number of MSISDI Prefixes exported
IMSI Prefix	Number of IMSI Prefixes exported
MSISDN Blacklist	Number of MSISDI Blacklists exported
IMSI Blacklist	Number of IMSI Blacklists exported
NAI Hosts	Number of NAI Hosts exported
NAI Users	Number of NAI Users exported
Wildcard NAIs	Number of Wildcard NAIs exported
Destinations	Number of Destinations exported
Status	Status of export

Field	Description
Comment	Descriptive text about export. This field is optional, so it may be blank.

Viewing export status

The **SDS -> Maintenance -> Export -> Status** page shows the status of all in-progress and completed scheduled exports for this system.

- If the filename in the **Export File** column exceeds 24 characters, it is truncated at 22 characters and the characters "..." are appended to the end of the truncated string to signify that the filename was truncated.
- The filenames in the **Export File** column are hyperlinks. You can click on the links to view the files as text or to save them locally.
- You can not modify or delete an export record using this form.
- Records are automatically removed after 7 days.

1. Select **SDS -> Maintenance -> Export -> Status**.

   The **SDS Maintenance Export Status** page appears. All exports are displayed in tabular form. The display fields are described in *Export Status maintenance elements*.

2. Select the category by which to perform the filtering.

   Table 30: Export Status filtering categories

Category	Description
Time Queued	Time the import was queued
Time Started	Time the import started
Time Completed	Time the import completed
Subscribers	Number of Subscribers exported
MSISDNs	Number of MSISDNS exported
IMSIs	Number of IMSIs exported
MSISDN Prefix	Number of MSISDN Prefixes exported
IMSI Prefix	Number of IMSI Prefixes exported
MSISDN Blacklist	Number of MSISDN Blacklists exported
IMSI Blacklist	Number of IMSI Blacklists exported
NAI Hosts	Number of NAI Hosts exported
NAI Users	Number of NAI Users exported
Wildcard NAIs	Number of Wildcard NAIs exported
Destinations	Number of Destinations exported
Status	Status of export

Category	Description
Comment	Descriptive text about export. This field is optional, so it may be blank.

3. Choose the filtering operator.

Table 31: Export Status filtering operators

Operator	Description
=	Is equal to
!=	Is not equal to
>	Is greater than
>=	Is equal to or greater than
<	Is less than
<=	Is equal to or less than
Like	Is Like (wildcard is * character)
Is Null	has no entry (is zero)

4. Enter the target character string to filter on in the text box.
5. Use Auto Refresh to select the time interval for the status to be refreshed.

Table 32: Export status refresh time

Time	Description
15	15 seconds
30	30 seconds
Off	Off (default)

6. Click **Go** to show results.

Remote Audit

The **SDS Maintenance Remote Audit** menu option allows you to access an on-demand ability to initiate an audit of the remote HLR Router provisioning database and flag any differences found between the SDS and the HLR Router databases. This provisioning database audit includes MSISDNs and, IMSIs and their associated Network Entity address values, which are extracted from the Destination Map table.

When you submit an audit request on the SDS GUI maintenance page, a PDBI client called *pdbaudit* connects to the local PDBA and to the remote PDBA running on the HLR Router system. It sends request commands to both PDBAs, compares the response data, and reports any discrepancies between

the two databases. Then you can check the status and review the results of the audit on the SDS GUI status page.

SDS supports manual audit runs between the SDS master data base instance and the HLR Router data base instance. Configurable automated audit runs are those runs that run at configured times to verify the accuracy of SDS master and HLR Router data base instances. A manual audit allows specification of audit between SDS master and HLR Router data base instances, based on some data range (for example, audit IMSI range) or single MSISDN or IMSI value.

SDS supports an on-demand ability to initiate an audit of the remote HLR Router provisioning database and flag any differences found between the SDS and the HLR Router databases. HLR Router provisioning data to be audited can be specified in one of two ways - by a single range of numbers, or by an input file containing multiple ranges of numbers. Using an input file allows an operator to specify multiple IMSI and MSISDN ranges at one time versus scheduling multiple remote HLR Router audits on a single range.

Use the following tabs to view the status of the database remote audits and to request a site-wide database audit of a specified subset of provisioning data:

- The **Remote Audit Status** tab allows you to view all pending, completed, and failed database remote audits of data performed throughout the system.
- The **Remote Audit Request** tab allows you to request a remote audit between SDS and HLR Router data using a subset of MSISDN or IMSI values.

  Since each node is responsible for managing its own resources, some nodes may decide to delay or cancel the requested audit in order to maintain sufficient resources to process signaling traffic.

Remote Audit elements

The **SDS Maintenance Remote Audit** page consists of two tabs: Status and Request. Each tab contains their own associated elements described in *Table 33: Remote Audit Request Elements* and *Table 34: Remote Audit Status Elements*.

Table 33: Remote Audit Request Elements

Element	Description
Data Type	Type of audit; MSISDN or IMSI
Audit By	Audit type; Range or File
Start of Range	Starting address of data to be included in this audit request
End of Range	Ending address of data to be included in this audit request. This field is optional.
Input File	File that contains ranges of values to be included in this audit. **Note:** You can type 80 or more characters, but only 80 character file names are supported.
Comment	Optional text used to provide information about the audit. For example, an explanation of the purpose or the audit owner's name. This field is optional.

Table 34: Remote Audit Status Elements

Element	Description	Description
Action	Available actions	Format: Selectable word
Type	Type of data being audited	Format: MSISDN or IMSI
Range/File	Range of data being audited or file name that contains ranges of data being audited	Format: Digits only Range: 8 - 15 digits for MSISDN Range: 10 - 15 for IMSI
Remote IP	IP address for Remote HLR Router system used for auditing	Format: Digits only Range: Either an IPv4 or an IPv6 IP address. IPv4 addresses are 32 bits, represented in a dot-decimal notation like this: x.x.x.x where each x (called an octet) is a decimal value from 0 to 255. They are separated by periods. For example: 1.2.3.4 and 192.168.1.100 are valid IPv4 addresses. IPv6 addresses are 128 bits, represented in a colon-hexadecimal notation like this: z:z:z:z:z:z:z:z where each z is a group of hexadecimal digits ranging from 0 to ffff. They are separated by colons. Leading zeros may be omitted in each group. "::" can be used (at most once) in an IPv6 address to represent a range of as many zero fields as needed to populate the address to eight fields. So the IPv6 address 2001:db8:c18:1:260:3eff:fe47:1530 can also be represented as 2001:0db8:0c18:0001:0260:3eff:fe47:1530 and the IPv6 address ::1 is the same as 0000:0000:0000:0000:0000:0000:0000:0001
Remote Port	Port for Remote HLR Router system used for auditing	Format: Digits only
Start Time/Completion Time	Date and time audit started and completed	Format: Time notation
State	Current state of the Remote audit	Format: Alpha • Submitted • Queued • In Progress • Aborting • Aborted • Failed

Element	Description	Description
		• Completed
Audited	Total number of records audited	Format: Digits
Same	Number of matched records on both SDS and the Remote HLR Router system	Format: Digits
Diff	Number of mismatched records between SDS and Remote HLR Router system	Format: Digits
Missing	Number of SDS records that are missing on the Remote HLR Router system	Format: Digits
Extra	Number of HLR Router records that are missing on the local SDS system.	Format: Digits
Unknown	Number of records in SDS and/or HLR Router on which a retrieve data command timed out	Format: Digits
Errors	Number of errors that occurred during the audit. See trace log for more information	Format: Digits
Report	Name of generated remote audit report	Format: Alphanumeric

Viewing the status of a remote audit

The **SDS -> Maintenance -> Remote Audit** page allows you to view all pending, completed, and failed remote database audits of data performed throughout the system.

1. Select **SDS -> Maintenance -> Remote Audit**.
   The **SDS Maintenance Remote Audit** page appears.
2. Select the **Status** tab.

   The **SDS -> Maintenance -> Remote Audit** page appears. All audits are displayed in tabular form. The display fields are described in *Remote Audit elements*.

3. Select the category by which to perform the filtering.
4. Choose the filtering operator.

Table 35: Remote Audit filtering operators

Operator	Description
=	Is equal to

Operator	Description
!=	Is not equal to
>	Is greater than
>=	Is equal to or greater than
<	Is less than
<=	Is equal to or less than
Like	Is Like (wildcard is * character)
Is Null	Has no entry (is zero)

5. Enter the target character string to filter on in the text box.
6. Use Auto Refresh to select the time interval for the status to be refreshed.

Table 36: Remote Audit display refresh time

Time	Description
15	15 seconds
30	30 seconds
Off	Off (default)

7. Click **Go** to show results.

Requesting a remote audit

You can use this task to request a site-wide remote database audit of a specified subset of MSISDN, IMSI, NAI User or Wildcard NAI User data. The request is sent to all nodes and the results are merged back up to SDS. Because each node is responsible for managing its own resources, some nodes might decide to delay or cancel the requested audit in order to maintain sufficient resources to process signaling traffic.

Note: A valid input file name can be up to 80 characters in length.

1. Select **SDS -> Maintenance -> Remote Audit**.
   The **SDS Maintenance Remote Audit** page appears.
2. Select the **Request** tab.
3. Select the type of data you want included in the audit from the **Data Type** pulldown list.

   If you select **NAI User** or **Wildcard NAI User**, go to Step 5.

4. Select a range for **Audit By**, enter data in the following fields:
   - **Start of Range** field: Starting address of data to be included in this audit. This must be between 8 and 15 digits for MSISDN or 10-15 for IMSI.
   - **End of Range** field: Ending address of data to be included in this audit. This is an optional field that, if used, must be between 8 and 15 digits for MSISDN or 10-15 for IMSI.

5. Provide the file name that contains ranges of values to be included in this audit.
6. Enter any text about the audit you want to include in the **Comment** field, if needed.
7. Click **Request**.

The database audit request is made. The status of the request can be viewed on the **SDS -> Maintenance -> Remote Audit** page.

Query

The **SDS Maintenance Query** page allows you to query database information for a single provisioning database entry, or for a range of the same type of provisioning database entries, on an available server. Any server that hosts a copy of the provisioning database can be used. Query options include MSISDN, IMSI, Destination, NAI Host, NAI User, Wildcard NAI User, Counts, Counts by Destination, and DB Level.

Querying a server for provisioning data allows you to see if data is being replicated correctly to each server, and allows you to see if adjustments to data management or to the subscriber database need to be made.

Query elements

The **SDS Maintenance Query** page consists of query entry dialogue boxes and results display. Not all elements of the entry dialogue boxes or query results may be used once the "Data" type is selected. All elements available through Query entry dialogue boxes are presented in *Table 37: Query Entry Elements*. All elements available through Query results display, in alphabetical order, are presented in *Table 38: Query Results Elements*.

Table 37: Query Entry Elements

Element	Description	Data Input Notes
Data	Type of data to include in query	Format: Drop down list Range: MSISDN, IMSI, MSISDN Prefix, IMSI Prefix, MSISDN Blacklist, IMSI Blacklist, NAI Host, NAI User, Wildcard NAI User, Destination, Counts, Counts by Destination, DB Level Default: MSISDN
Start Address	Starting address of data to be included in this query (applies to MSISDN, IMSI, MSISDN Prefix, IMSI Prefix, MSISDN Blacklist and IMSI Blacklist query requests only)	Format: Digits only Range: 8 - 15 digits for MSISDN or MSISDN Blacklist, 10 - 15 for IMSI or IMSI Blacklist, 1 - 15 for MSISDN or IMSI Prefix

Element	Description	Data Input Notes
End Address	Ending address of data to be included in this query (applies to MSISDN, IMSI, MSISDN Prefix, IMSI Prefix, MSISDN Blacklist and IMSI Blacklist query requests only)	Format: Digits only Range: 8 - 15 digits for MSISDN or MSISDN Blacklist, 10 - 15 for IMSI or IMSI Blacklist, 1 - 15 for MSISDN or IMSI Prefix Default: blank
NAI Host	NAI Host to query applies to NAI users only	NAI Host defaults to the first one configured in the table.
Server	Server on which to run the query	Format: Alphanumeric Range: up to 35 characters Default: local server

Table 38: Query Results Elements

Result Element	Description	Data Value Selected
AAA	AAA Destination record (with type= aaa) or blank for none	MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix
Destination(s)	Unique text used to identify a Destination	Counts, Counts by Destination
FQDN	A 1-255 character string for the Diameter FQDN for the Destination. The value can be null	Destination
Host	A unique string of 1 -64 characters for NAI Host Name	NAI User, Wildcard NAI User, NAI Host
IMSI(s)	A unique string of 10-15 decimal digits identifying the IMSI	IMSI, Counts, Counts by Destination
IMSI Blacklist	A unique string of 10-15 decimal digits identifying the IMSI Blacklist value	IMSI Blacklist, Counts
IMSI Prefix	A unique string of 1-15 decimal digits identifying the IMSI Prefix	IMSI Prefix, Counts, Counts by Destination
IMSHSS	IMS HSS Destination record (with type= imsHss) or blank for none	MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix
LTEHSS	LTE HSS Destination record (with type= lteHss) or blank for none	MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix
MSISDN(s)	A unique string of 8-15 decimal digits identifying the MSISDN	MSISDN, Counts, Counts by Destination
MSISDN Blacklist	A unique string of 8-15 decimal digits identifying the MSISDN Blacklist value	MSISDN Blacklist, Counts
MSISDN Prefix	A unique string of 1-15 decimal digits identifying the MSISDN Prefix	MSISDN Prefix, Counts, Counts by Destination

Result Element	Description	Data Value Selected
NAI Host	Number of NAI hosts	Counts
NAI User	A string of 1-64 characters for the NAI User Name	NAI User, Counts, Counts by Destination
Name	A unique string of 1-32 characters to identify the Destination	Destination
OCS	OCS Destination record (with type= ocs) or blank for none	MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix
OfCS	OFCS Destination record (with type= ofcs) or blank for none	MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix
PCRF	PCRF Destination record (with type= pcrf) or blank for none	MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix
Realm	A 1-255 character string for the Diameter Realm for the Destination. The value can be null	Destination
Type	Destination type	Destination
USERDEF1	UserDef1 Destination record (with type= userDef1) or blank for none	MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix
USERDEF2	UserDef2 Destination record (with type= userDef2) or blank for none	MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix
Wildcard NAI User	A string of 1-64 characters for the wild carded NAI User Name.	Wildcard NAI User, Counts, Counts by Destination
DB Level	Numeric value of Database level	DB Level

Running a query (MSISDN, IMSI, MSISDN Prefix, IMSI Prefix, MSISDN Blacklist, IMSI Blacklist)

Use this task to query a single (or range of) MSISDN, IMSI, MSISDN Prefix, IMSI Prefix, MSISDN Blacklist, IMSI Blacklist values on any server within the system.

1. Select **SDS** > **Maintenance** > **Query**.

   The **SDS Maintenance Query** page appears.
2. Select a value from the **Data** pulldown list.
3. Enter the starting address of data to be included in this query in the **Start Address** field.
4. Enter the ending address of data to be included in this query in the **End Address** field.
5. Select the server you want to run the query on in the **Server** pulldown list.
6. Click **Query**.

The query is run and any relevant data is displayed on the page. See *Table 38: Query Results Elements*.

Running a query (NAI User)

You can use this task to query all of the NAI Users on any host and server within the server within the system.

1. Select **SDS** > **Maintenance** > **Query**.
   The **SDS Maintenance Query** page appears.
2. Select **NAI User** from the **Data** pulldown list.
3. Select the NAI Host to be included in this query in the **NAI Host** field.
4. Select the server you want to run the query on in the **Server** pulldown list.
5. Click **Query**.

The query is run and any relevant data is displayed on the page. See *Table 38: Query Results Elements*.

Running a query (Wildcard NAI User, NAI Host, Destination, Counts, Counts by Destination, or DB Level)

You can use this task to query all of the following:

- Wildcard NAI User
- NAI Host
- Destination
- Counts
- Counts by Destination Users on any server within the system

1. Select **SDS** > **Maintenance** > **Query**.
   The **SDS Maintenance Query** page appears.
2. Select one of the following from the **Data** pulldown list:
   - **Wildcard NAI User**
   - **NAI Host**
   - **Destination**
   - **Counts**
   - **Counts by Destination**
   - **DB Level**
3. Select the server you want to run the query on in the **Server** pulldown list.
4. Click **Query**.

The query is run and any relevant data is displayed on the page. See *Table 38: Query Results Elements*.

NPA Splits maintenance

Use this selection when you want to manage an NPA split in advance of a Permissive Dialing Period.

NPA Split refers to the telephone-numbering scheme that subdivides an old area code (old NPA) by the creation of a new area code (new NPA). This is necessary when the number of telephones in an

old area code (old NPA) grows to an excessive number. As new area codes are defined (new NPA), some existing exchanges (NXX) may be assigned to the new area code (new NPA) from the old area code (old NPA).

The split is in the Pending state until it becomes Active on the Start date of the PDP. While in the Active state, Dialed Numbers (DN) in the split's NXX can use either the old NPA or the new NPA. After the split becomes complete on the End date of the PDP, only the new NPA can be used in a DN.

To manage NPA splits through the GUI, you must have group permission access to **NPA Splits** and **NPA Split Maintenance**.

NPA Splits elements

Use the **SDS Maintenance NPA Splits** page to manage NPA splits. This table describes fields on this page.

Table 39: NPA Splits Maintenance Elements

Element	Description	Data Input Notes
Old NPA	The Numbering Plan Area that the DNs will be split from. (Retrieve splits in which this NPA was the old NPA)	Format: Integer Range: 200 - 999, 3-digit number Default: blank
New NPA	The Numbering Plan Area that the DNs will be split to. (Retrieve splits in which this NPA was the new NPA)	Format: Integer Range: 200 - 999, 3-digit number Default: blank
NXX	The exchange code value for this split. (Retrieve splits in which this NXX was the NXX.) On the **Modify** and **Delete** tabs, an **All** selection box is also available. If this box is check marked (the default) when the **Modify** or **Delete** button is clicked, all NXXs are modified or deleted.	Format: Integer Range: 000 - 999, 3-digit number Default: blank
PDP Start	The start of the Permissive Dialing Period for this split. Grayed if NPA split is active. • This date cannot be in the past, and must be before the PDP End date. • Activation occurs within the first 15 minutes of the PDP Start date.	Format: Pulldown menus Range: Valid date Default: Tomorrow's date

Element	Description	Data Input Notes
	• If today's date is entered, activation occurs within 15 minutes of the **Create** or **Modify** button being clicked. • This field only appears on the **Create** and **Modify** tabs.	
PDP End	The end of the Permissive Dialing Period for this split. • This date cannot be in the past, and must be after the PDP Start date. • Termination occurs within the first 15 minutes of the PDP End date. • The date cannot be changed once the NPA split is complete. • This field only appears on the **Create** and **Modify** tabs.	Format: Pulldown menus Range: Valid date Default: Tomorrow's date + 90 days

Viewing NPA Splits

Use this task to display active or non-active NPA Split information.

From the View Tab, all NPA Split information can be displayed. Each field can be used as a filter option when viewing NPA splits.

If you click **View** while all three fields are empty, the GUI displays all NPA splits found in the PDB database. If the **Save Results** checkbox is check marked, the results are also saved to a CSV file named `NpaSplitReport.guiadmin.<timestamp>.csv`. This file can then be viewed and downloaded in the SDS file management area (**Status & Manage > Files>**).

1. Select **SDS** > **Maintenance** > **NPA Splits**.
   The **SDS Maintenance NPA Splits** page appears, with the **View** tab displayed.
2. Add search criteria to the fields in the **Value** column, as desired.
3. To save results of NPA split information to a file for further viewing and/or processing, click to check mark **Save Results**.
4. Click **View**.

The NPA splits in the PDB database that match the criteria entered are shown on the bottom of the page. For information about how to filter this information, see *NPA Splits elements*.

If **Save Results** was checked, the CSV file is generated.

Creating an NPA Split

From within the Create Tab, you can create NPA Splits.

Use this procedure to create an NPA split and define its characteristics, including the old NPA code, the new NPA code, the central office exchange (NXX) code(s) to be transferred to the new NPA, and the beginning and ending dates of the Permissive Dialing Period (PDP).

1. Select **SDS** > **Maintenance** > **NPA Splits**
   The **SDS Maintenance NPA Splits** page appears.
2. Click the **Create** tab.
   The NPA Splits **Create** table appears.
3. Enter data to provision an NPA split. Values must be entered for **Old NPA**, **New NPA**, and **NXX**. If dates are entered in the **PDP Start** and/or **PDP End** dates, these dates must be greater than today's date.

   For more information about these fields, see *NPA Splits elements*.
4. Click **Create**.

The NPA Split record is provisioned. Its state is initialized to Pending.

Modifying an NPA Split

Use this procedure to modify the start and/or end the Permissive Dialing Period (PDP) dates of one or more existing NPA splits.

1. Select **SDS** > **Maintenance** > **NPA Splits**.
   The **SDS Maintenance NPA Splits** page appears.
2. Click the **Modify** tab.
   The **NPA Splits Modify** page appears.
3. Enter the **Old NPA**, **New NPA**, and **NXX** fields to select the NPA to modify. To modify all **NXX**, leave the **All** selection box check marked.
4. Enter the **PDP Start** and/or **PDP End** dates, as needed.

   Both the **PDP Start** and **PDP End** dates can be modified for pending splits. Only the **PDP End** date can be modified for active splits. Neither can be modified for completed splits. The **PDP End** date must be greater than today's date.

   For more information about these fields, see *NPA Splits elements*.
5. Click **Modify.**

The NPA splits are updated.

Deleting an NPA Split

Use this procedure to delete NPA Splits whose Permissive Dialing Period is pending or has expired.

1. Select **SDS** > **Maintenance** > **NPA Splits**.
   The **SDS Maintenance NPA Splits** page appears.
2. Select the **Delete** tab.
   The **NPA Splits Delete** tab appears.
3. Enter values into the fields to select the NPA splits you want to delete. To delete all **NXX**, leave the **All** selection box check marked.
4. Click **Delete**.
   A confirmation pop up window appears, asking if you are sure you want to delete this NPA split.

5. Click **OK** to continue with the deletion.

The selected NP splits are deleted, and a Delete successful message is displayed.

Glossary

A

AAA	Authentication, Authorization, and Accounting (Rx Diameter command)
APDE	Automated Performance Data Export

C

CID	Connection ID

D

DP	Data Processor The repository of subscriber data on the individual node elements. The DP hosts the full address resolution database.
DP SOAM	Data Processor System Operations, Administration, and Maintenance
DR	Disaster Recovery

F

FABR	Full Address Based Resolution Provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server addresses based on individual user identity addresses in the incoming Diameter request messages.
FQDN	Fully Qualified Domain Name

F

	The complete domain name for a specific computer on the Internet (i.e., www.oracle.com). A domain name that specifies its exact location in the tree hierarchy of the DNS.

G

GUI	Graphical User Interface The term given to that set of items and facilities which provides you with a graphic means for manipulating screen data rather than being limited to character based commands.

H

HA	High Availability High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.
HLRR	HLR Router
HSS	Home Subscriber Server A central database for subscriber information.
HTTP	Hypertext Transfer Protocol

I

IMS	IP Multimedia Subsystem These are central integration platforms for controlling mobile communications services, customer management and accounting for mobile communications services

I

	based on IP. The IMS concept is supported by 3GPP and the UMTS Forum and is designed to provide a wide range of application scenarios for individual and group communication.
IP	Internet Protocol - IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.

L

LTE	Long Term Evolution The next-generation network beyond 3G. In addition to enabling fixed to mobile migrations of Internet applications such as Voice over IP (VoIP), video streaming, music downloading, mobile TV, and many others, LTE networks will also provide the capacity to support an explosion in demand for connectivity from a new generation of consumer devices tailored to those new mobile applications.

N

NE	Network Element An independent and identifiable piece of equipment closely associated with at least one processor, and within a single location.

N

	In a 2-Tiered DSR OAM system, this includes the NOAM and all MPs underneath it. In a 3-Tiered DSR OAM system, this includes the NOAM, the SOAM, and all MPs associated with the SOAM.
NPA	Number Plan Area The North American "Area Codes." (3 digits: 2- to-9, 0 or 1, 0-to-9. Middle digit to expand soon).
NXX	Central Office Exchange Code

O

OCS	Online Charging Server

P

PCRF	Policy and Charging Rules Function The ability to dynamically control access, services, network capacity, and charges in a network. Maintains rules regarding a subscriber's use of network resources. Responds to CCR and AAR messages. Periodically sends RAR messages. All policy sessions for a given subscriber, originating anywhere in the network, must be processed by the same PCRF.
PDP	Permissive Dialing Period

S

SDS	Subscriber Database Server Subscriber Database Server (SDS) provides the central provisioning

S

	of the Full-Address Based Resolution (FABR) data. The SDS, which is deployed geo-redundantly at a Primary and Disaster recovery site, connects with the Query Server and the Data Processor System Operations, Administration, and Maintenance (DP SOAM) servers at each Diameter Signaling Router (DSR) site or a standalone DP site to replicate and recover provisioned data to the associated components.
SNMP	Simple Network Management Protocol. An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.
SOAM	System Operations, Administration, and Maintenance
SQL	Structured Query Language A special programming language for querying and managing databases.

T

TCP	Transmission Control Protocol A connection-oriented protocol used by applications on networked hosts to connect to one another and

T

to exchange streams of data in a reliable and in-order manner.

X

XML

eXtensible Markup Language

A version of the Standard Generalized Markup Language (SGML) that allows Web developers to create customized tags for additional functionality.