Oracle® Communications Subscriber Database Server

User Guide

Release 9.1.0.0.0
G11856-01
November 2024

Oracle Communications Subscriber Database Server User Guide, Release 9.1.0.0.0

G11856-01

Contents

My Oracle Support

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

Call the Customer Access Support 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 My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New in This Release

This section introduces the documentation updates for release 9.1.0.0.0.

Release 9.1.0.0.0 - G11856-01 - November 2024

Updated the default value for the PDB relay receive window size and PDB relay send command rate in the Options configuration elements section as there is an increase in the PDBI rate.

1
Introduction

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.

1.1 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.

1.2 Scope and Audience

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

1.3 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.

2
About SDS

This section of documentation describes 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.

2.1 Introduction to SDS

The SDS/DP system consists of a Primary Provisioning Site, a Disaster Recovery (DR) Provisioning Site, and up to 32 Signaling Site servers with redundant DP SOAM servers and up to 10 DP servers in each site. Each Provisioning Site has an active/standby pair of servers in a high availability (HA) configuration and an optional third server configured as a Query server.

The SDS/DP system is built upon the EAGLE XG 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. Every server has the ability to send traps directly to the customer's SNMP Manager and 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.

2.1.1 SDS Functionality

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 Signaling Router (DSR) site or a standalone DP site to replicate and recover provisioned data to the associated components.

SDS provides the following functionality:

- SDS Database – Stores subscriber data needed by the FABR application
- GUI-based provisioning
- Control the Diameter Internet Engineering Task Force (IETF) specification called Diameter Routing Message Priority (DRMP) to establish relative message priorities
- Enhanced Subscriber Table add functionality
- Support SOAP over HTTP and XML over TCP as provisioning interfaces

- SQL Interface – At query server for query only
- CSV and/or XML-formatted 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 32 sites
- DP - DB Processor – A server that has a replica of the SDS database and is available for query by server 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

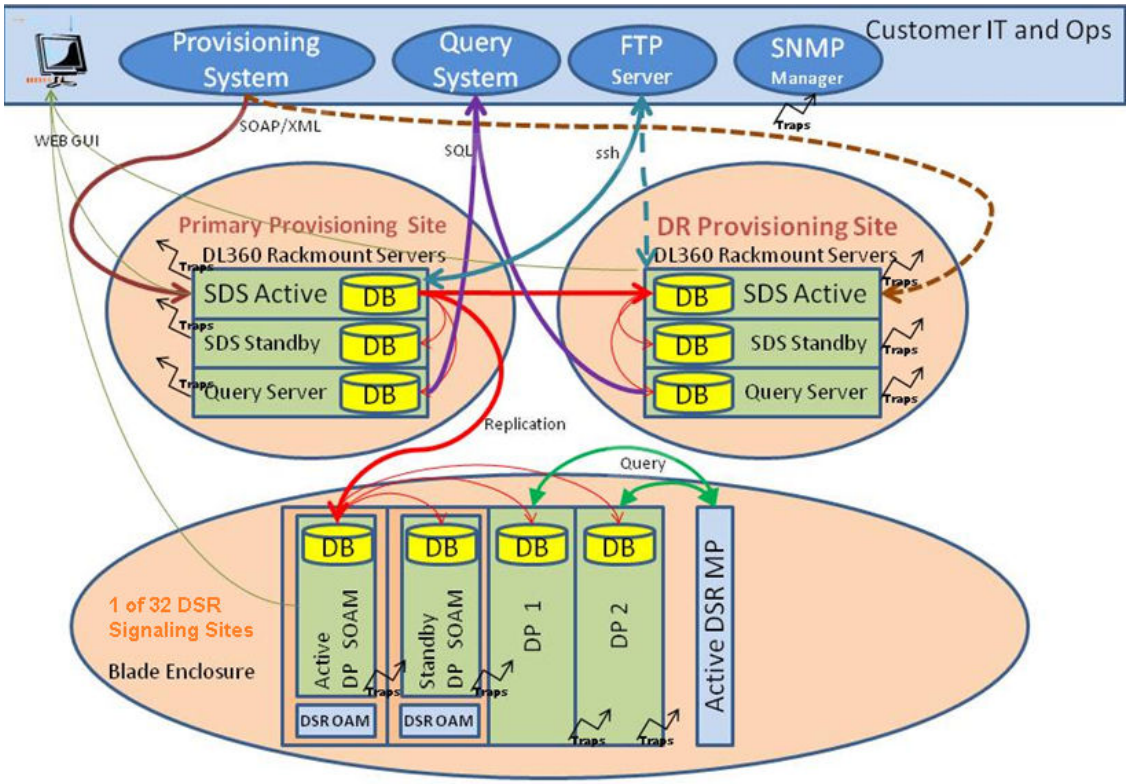
> **Note:**
>
> SDS 9.0.0.0.0 is backward compatible with old SDS Release supported SOAP messages.

2.2 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 32 sites, each capable of supporting up to 512 remote signaling points.

This figure provides an overview of the SDS architecture.

Figure 2-1 SDS System Diagram



2.2.1 SDS Components

SDS

The SDS has 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 servers. It also provides a GUI, which is used for configuration, user administration, and viewing 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 NEs are less than the database levels of the SDS and DR SDS, the active provisioning site SDS provisions the DR SDS before updating the NEs.

DR SDS

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

The DR SDS's databases are kept updated through real-time replication of subscriber and application data from the active primary SDS. Under normal operating conditions, the DR SDS does not provision any downstream systems, but if made active, it takes 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 primary SDS and in turn replicates it to all underlying DPs located in the same physical site. DP SOAM also provides a GUI used for viewing alarms and measurements details specific to components located within the site (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 active primary SDS and stores it in a customer accessible SQL interface. A Query server is located in the same physical site as each SDS component (SDS/DR SDS).

Network Element

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

- 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 NEs and up to 32 DP SOAM NEs.

DPs

The Data Processors (DPs) 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 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, URI, or External Identifiers, and destination types and return the resolved destination's address FQDN and/or realm values.

Each Signaling Site can support multiple DP servers deployed at a single site to scale query capacity (by increments of 140,000 QPS per DP). Each Signaling Site can support up to 10 DPs.

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.

2.3 Distributed configuration

The SDS supports centralized configurations where:

- All subscriber data configuration and maintenance occurs at the SDS level, and
- 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 primary SDS.
- SDS tasks related to the subscriber database are only available when logged into an active primary SDS, with the exception of querying the database.

- All Alarms, KPIs, Measurements, and Events are accessible from the SDS.

2.3.1 Centralized configuration

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 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 2-1 SDS Main Menu Options

Menu Item	Function
Administration	All options available: • General Options • Access Control – Users – Groups – Sessions – Certificate Management – Authorized IPs – SFTP Users • Software Management – Versions – Upgrade • Remote Servers – LDAP Authentication – SNMP Trapping – Data Export – DNS Configuration

Table 2-1 (Cont.) SDS Main Menu Options

Menu Item	Function
Configuration	All options available: • Network Elements • Network – Devices – Routes • Services • Servers • Server Groups • Resource Domains • Places • Place Associations • DSCP – Interface DSCP – Port DSCP
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 – Active Tasks – Scheduled Tasks • Files
Measurements	All options available: • Report
Communication Agent	All options available: • Configuration – Remote Servers – Connection Groups – Routed Services • Maintenance – Connection Status – Routed Services Status – HA Services Status

Table 2-1 (Cont.) SDS Main Menu Options

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

3
Configuration

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 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.

3.1 Options configuration

The Options page controls 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 manages 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 an idle connection is timed out
- Whether to allow 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

> **Note:**
>
> Command logs can be exported to a server other than the single remote server supported by APDE; **Log Provisioning Messages** must be enabled on the NO. Click **SDS**, and then **Maintenance**, and then **Command Log** page to export logs.

3.1.1 Options configuration elements

This table describes the fields on the SDS Configuration Options page.

Table 3-1 Options Configuration Elements

Element	Description	Data Input Notes
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 are logged in the command log. **Note**: Command logs can be exported to a server other than the single remote server supported by APDE.	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 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: list Range: Non-Blocking, Blocking Default: Non-Blocking

Table 3-1 (Cont.) Options Configuration Elements

Element	Description	Data Input Notes
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. 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: list Range: Non-Blocking, Blocking Default: Non-Blocking
Remote Export Transfers Enabled	If checked, export files are copied to the remote export host	Format: Check box Range: Checked, Unchecked Default: Unchecked

Table 3-1 (Cont.) Options Configuration Elements

Element	Description	Data Input Notes
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
Remote Export Directory	The directory in the Remote Export Host to which export files are transferred if configured	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 are sent until acknowledgments are received from the remote system.	Format: Digits only Range: 5–2500 Default: 500

Table 3-1 (Cont.) Options Configuration Elements

Element	Description	Data Input Notes
Remote Audit Send Message Rate	The maximum rate of messages/second in which retrieval messages are 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 the Provisioning Database Application that 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 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

Table 3-1 (Cont.) Options Configuration Elements

Element	Description	Data Input Notes
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 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 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 are sent until acknowledgments are received from the remote system.	Format: Digits only Range: 5–2500 Default: 1000
PDB Relay Send Command Rate	The maximum rate (in commands/second) in which commands are relayed/sent to the Provisioning Database Application on remote system	Format: Digits only Range: 5–2500 Default: 1000

Table 3-1 (Cont.) Options Configuration Elements

Element	Description	Data Input Notes
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
XML Interface Idle Timeout	The maximum number of seconds an open connection remains 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) an open connection remains 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: list Range: Secure, Unsecure Default: Unsecure

Table 3-1 (Cont.) Options Configuration Elements

Element	Description	Data Input Notes
Maximum Transaction Lifetime	The maximum number of seconds a transaction remains 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
Maintain Subscriber Timestamp (read-only)	Whether or not to maintain subscriber creation and last updated timestamp. **Note**: Changes to this option do not take effect until the application processes are restarted.	Format: Check box Range: Checked, Unchecked Default: Unchecked

3.1.2 Editing options

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

1. Click **SDS**, and then **Configuration**, and then **Options**.
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 displays.
   If the page contains any values that are not valid or are out of range, an error message displays.

3.2 DRMP configuration

The DRMP page controls the Diameter Internet Engineering Task Force (IETF) specification called Diameter Routing Message Priority (DRMP). DRMP allows Diameter nodes to embed the relative priority of the message into a Diameter message used for routing decisions, resource allocation, and overload abatement decisions. The priorities are based on a scale of 0 to 15, where priority value 0 is specified as the highest priority and priority value 15 is the lowest priority. DRMP performs congestion control and message throttling decisions based on DRMP-based relative priority of the Diameter message.

> **Note:**
>
> DRMP priority value of 0 is treated as highest priority and 15 as lowest priority, which is in reverse order of DSR priority values.

When making routing and resource allocation decisions, Diameter nodes currently have no generic mechanism to determine the relative priority of Diameter messages. IETF DRMP addresses this by defining a mechanism to allow diameter endpoints to indicate the relative

priority of Diameter transactions. With this information, Diameter nodes can factor that priority into routing, resource allocation, and overload abatement decisions. For example, this includes first responder related signaling, emergency call related signaling, differentiated services, Application specific priorities, and so on. This allows SDS to support a custom policer mode based on tracker/shaper algorithm for managing congestion for all internal congestion points.

The custom policer mode tracks the offered traffic to each congestion point and arranges them by priority and color segments and stacks it according to the Site MO Discard Policy:

- Discard by Priority Only
- Discard by Color within Priority
- Discard by Priority within Color

If any of the congestion point's (Task Queue, Task Thread Pool, and so on) congestion level is above normal, the custom policer discards a fixed percentage of messages depending on Discard Policy (of that site) starting from messages lowest in stacking order. The percentage of messages discarded are configured as:

- CL1 Discard %: 15%
- CL2 Discard %: 30%
- CL3 Discard %: 45%

For information about DRMP APV and IETF, see *Diameter User's Guide*.

3.2.1 DRMP configuration elements

This table describes the fields on the DRMP page. You can perform this task when logged into an SDS or from the DP SOAM GUI. Use this page to view the DRMP Admin State and the priority values set for each SOAM Server group. For more information, see *Diameter User's Guide.*

Table 3-2 DRMP Configuration Elements

Element	Description	Data Input Notes
SOAM Server Group Name	The name of the server group.	Format: alphanumeric Range: NA Default: NA
16 Priority Admin State	The server group administrative state; determines 16 or 4 message priorities support. **Note**: Application restart is required.	Format: textbox Range: Enabled (supports 16 internal message priorities [0-15]), Disabled (supports 4 internal message priorities [(0-3]). Default: Disabled
NGN-PS Admin State	Defines whether the NGN-PS feature is enabled or not. **Note**: This parameter is disabled and non-editable when 16 Priority Admin State is disabled.	Format: textbox Range: Enabled, Disabled Default: Disabled (the system does not provide NGN-PS treatment to any messages)

Table 3-2 (Cont.) DRMP Configuration Elements

Element	Description	Data Input Notes
Minimum Inviolable Priority	Defines the minimum priority the system considers inviolable from a message priority treatment. A Stack Event with a priority greater than or equal to this attribute is not subject to congestion controls.	Format: digits only Range: 3, 15, or 99 • 3 - when 16 Priority Admin State is Disabled (irrespective of NGN-PS Admin State) • 15 - when 16 Priority and NGN-PS Admin State are Enabled • 99 - when 16 Priority Admin State is Enabled, but NGN-PS Admin State is Disabled Default: 3
Minimum Response Priority	Defines the minimum priority the system assigns to ingress Diameter Answer message.	Format: digits only Range: 0 or 2 • 2 - when 16 Priority Admin State is Disabled • 0 - when 16 Priority Admin State is Enabled Default: 2
Discard Policy	The order of priority and/or color-based traffic segments to consider when determining discard candidates for the application of treatment during SDS Congestion processing.	Format: alpha Range: Priority Only, Priority Within Color, Color Within Priority Default: Priority Only

3.2.2 Adding DRMP attributes

You can only perform this task for the given SOAM Server Group.

1. Select **SDS**, and then **Configuration**, and then **DRMP**.
2. Click **Insert**.
3. Select a SOAM server group name in the **Server Group Name** list.
4. Set the **16 Priority Admin State**.
5. Set the **NGN-PS Admin State**.
6. Set the **Minimum Inviolable Priority**.
   - Select 3 when 16 Priority Admin State is Disabled (irrespective of NGN-PS Admin State). This is the default.
   - Select 15 when 16 Priority and NGN-PS Admin State are Enabled.
   - Select 16 when Priority Admin State is Enabled but NGN-PS Admin State is Disabled.
7. Set the **Minimum Response Priority**. Select **0** or **2**.
8. Set the **Discard Priority**. Select **Priority Only**, **Priority Within Color**, **Color Within Priority**.
9. Perform one of the following:

- Click **OK** to save the connection and return to the SDS configuration DRMP page.
- Click **Apply** to save the connection and remain on this page.
- Click **Cancel** to return to the DRMP page without saving the changes.

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:

- 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)

3.2.3 Editing DRMP attributes

You can only perform this task for the given SOAM Server Group.

1. Select **SDS**, and then **Configuration**, and then **DRMP**.
2. Click **Edit**.
3. Modify the attributes 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 DRMP configuration elements.
4. Click **OK**.

   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.

3.2.4 Deleting DRMP connections

You can only perform this task for the given SOAM Server Group.

1. Select **SDS**, and then **Configuration**, and then **DRMP**.
2. Highlight the DRMP connection you want to delete and click **Delete**.
3. Perform one of the following actions on the confirmation screen:
   - Click **OK** to delete the connection.
   - Click **Cancel** to cancel the delete function and return to the DRMP page.

3.3 Connections configuration

The Connections page manages the configuration for servers connected to the active Primary Provisioning Site's Active SDS server. Only the servers specified in the Connections list can remotely connect to the server and execute commands.

> **Note:**
>
> The client host being associated with permissions must exist in the system before 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.

3.3.1 Connections configuration elements

This table describes the fields on the SDS Configuration Connections page.

Table 3-3 Connections Configuration Elements

Element	Description	Data Input Notes
Filter fields	List of available filters and additional fields to modify the search options	Format: selectable list
System ID	Identification for the system	Format: alphanumeric Range: 1– 255 characters

Table 3-3 (Cont.) Connections Configuration Elements

Element	Description	Data Input Notes
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 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
Permission	Database permissions for this client	Format: list Range: READ_ONLY, READ_WRITE Default: READ_ONLY

Table 3-4 Connections 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)

3.3.2 Viewing connections

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

1. Select **SDS**, and then **Configuration**, and then **Connections**.

   The SDS Configuration Connections page appears with the currently allowed connections listed in the table. Click on any column heading to reorder the rows.
2. To look for a specific connection, click **Filter**.
3. Select Connection from the **Display Filter** list.
4. Select the category to perform the filtering.

Table 3-5 Connections Status Filtering Categories

Category	Description
System ID	Identifying text for the system
IP Address	IP address (either an IPv4 or IPv6) of the client that connects to SDS
Permission	Database permission group for the client

5. Select the filtering operator.

Table 3-6 Connections 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)

6. Enter the target character string to filter on in the textbox.
7. Click **Go**.

3.3.3 Adding connections

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

1. Select **SDS**, and then **Configuration**, and then **Connections**.
2. Click **Insert**.
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** list.
   - 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 field validations succeed, the connection is saved. 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

3.3.4 Editing connections

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

1. Select **SDS**, and then **Configuration**, and then **Connections**.
2. Highlight the connection you want to edit by clicking on the row and then click **Edit**.
3. Edit the System ID, IP Address, and/or Permission for the connection.

   For more information about these fields, see Connections configuration elements.
4. Click **OK** to save the changes and return to the SDS Configuration Connections page.

   If field validations succeed, the connection is saved. If any of the following conditions exist, an error message displays:
   - 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

3.3.5 Deleting connections

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

1. Select **SDS**, and then **Configuration**, and then **Connections**.
2. Highlight the connection you want to delete and click **Delete**.
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.

3.4 NAI hosts configuration

The NAI Hosts page manages the Network Access Identifier (NAI) host systems 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

3.4.1 NAI hosts configuration elements

This table describes the fields on the SDS Configuration NAI Hosts page.

Table 3-7 NAI Hosts Configuration Elements

Element	Description	Data Input Notes
Filter fields	List of available filters and additional fields to modify the search options	Format: selectable list
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

3.4.2 Viewing NAI hosts

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

1. Select **SDS**, and then **Configuration**, and then **NAI Hosts**.

   The SDS Configuration NAI Hosts page displays with the current NAI hosts listed in the table. Click on any column heading to reorder the rows.
2. To look for a specific NAI Host, click **Filter**.
3. Select NAI Host from the **Display Filter** list.
4. Select the filtering operator.

   Table 3-8 NAI Hosts 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)
5. Enter the NAI Host to filter on in the textbox.

6. Click **Go**.

3.4.3 Adding NAI hosts

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

1. Select **SDS**, and then **Configuration**, and then **NAI Hosts**.
2. Click **Insert**.
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 field validation succeeds, the host is saved. 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.

3.4.4 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**, and then **Configuration**, and then **NAI Hosts**.
2. Highlight the NAI host you want to delete and click **Delete**.
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.

3.5 Destinations configuration

The Destinations page manages 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

3.5.1 Destinations configuration elements

This table describes the fields on the SDS Configuration Destinations page.

Table 3-9 Destinations Configuration Elements

Element	Description	Data Input Notes
Filter fields	List of available filters and additional fields to modify the search options	Format: selectable list
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: list • IMS HSS • LTE HSS • MTC HSS • PCRF • OCF • OFCS • AAA • User defined 1 • User defined 2
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

3.5.2 Viewing destinations

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

1. Select **SDS**, and then **Configuration**, and then **Destinations**.

   The SDS Configuration Destinations page displays with the current destinations listed in the table.
2. To look for a specific Destination, click **Filter**.
3. Select `Destination Name` from the **Display Filter** list.
4. Select the filtering operator.

Table 3-10 Destinations 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)

5. Enter the Destination Name to filter on in the textbox.
6. Click **Go**.

3.5.3 Adding destinations

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

1. Select **SDS**, and then **Configuration**, and then **Destinations**.
2. Click **Insert**.
3. Enter a unique name in the **Name** field.
4. Select the type of destination from the **Type** list.
5. Enter a fully-qualified domain name (FQDN) in the **FQDN** field.
6. Enter the realm in the **Realm** field.
7. Perform one of the following:
   - Click **OK** to save the Destination and return to the SDS configuration connections page.
   - Click **Apply** to save the Destination and remain on this page.
   - Click **Cancel** to return to the SDS Configuration Destinations 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)

3.5.4 Editing destinations

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

1. Select **SDS**, and then **Configuration**, and then **Destinations**.
2. Highlight the destination you want to edit and click **Edit**.
3. Edit the **FQDN** and/or **Realm** fields.

   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.

4. Perform one of the following:
   - Click **OK** to save the changes to the destination and return to the SDS Configuration Destinations page.
   - Click **Cancel** to return to the SDS Configuration Destinations page without saving the changes.

3.5.5 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 using the Destination.

1. Select **SDS**, and then **Configuration**, and then **Destinations**.
2. Highlight the destination you want to delete and click **Delete**.
3. 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 any of the following conditions exist, and error message appears:
   - No updates were made to the database.
   - Object currently in use; destination is used by a route.
   - Object currently in use; destination is used by a destination map.

3.6 Domain Identifier configuration

The Domain Identifier page adds, modifies, or deletes domain identifiers associated with a destination.

3.6.1 Domain Identifiers configuration elements

This table describes the fields on the SDS Domain Identifiers page.

Table 3-11 Domain Identifiers Configuration Elements

Element	Description	Data Input Notes
Filter fields	List of available filters and additional fields to modify the search options	Format: selectable list
Domain Identifier	Domain Identifier hostname	Format: textbox Range: 1-128 characters
IMS HSS (available on the Insert page only)	IMS HSS destination	Format: list Range: available IMS HSS destinations
LTE HSS (available on the Insert page only)	LTE HSS destination	Format: list Range: available LTE HSS destination
MTC HSS	MTC HSS destination	Format: list Range: available MTC HSS destinations
PCRF (available on the Insert page only)	PCRF destination	Format: list Range: available PCRF destinations
OCS (available on the Insert page only)	OCS destination	Format: list Range: available OCS destinations
OfCS (available on the Insert page only)	OfCS destination	Format: list Range: available OfCS destinations
AAA (available on the Insert page only)	AAA destination	Format: list Range: available AAA destinations
User defined 1 (available on the Insert page only)	User defined destination	Format: list Range: available User defined 1 destinations
User defined 2 (available on the Insert page only)	User defined destination	Format: list Range: available User defined 2 destinations

3.6.2 Viewing domain identifiers

Use this page to view the list of Domain Identifiers.

1. Select **SDS**, and then **Configuration**, and then **Domain Identifiers**.

   The SDS Domain Identifiers page displays with the current domain identifiers listed in the Domain Identifiers table. Click on any column heading to reorder the rows.

2. To look for specific Domain Identifiers, click **Filter**.
3. Select `Domain Identifier` from the **Display Filter** list.

4. Select the filtering operator.

Table 3-12 Domain Identifier 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)

5. Enter the Domain Identifier Name to filter on in the textbox.
6. Click **Go**.

3.6.3 Adding domain identifiers

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

1. Select **SDS**, and then **Configuration**, and then **Domain Identities**.
2. Click **Insert**.
3. Enter a unique name in **Domain Identifier** field.

> **Note:**
>
> The domain identifier is case insensitive and the value is stored in lower case (for example, ORACLE.com is stored as oracle.com).

4. Select the associated destination(s) from the applicable destination(s) list.

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

   - **IMS HSS**
   - **LTE HSS**
   - **MTC HSS**
   - **PCRF**
   - **OCS**
   - **OfCS**
   - **AAA**
   - **User defined 1**
   - **User defined 2**

5. Perform one of the following:
   - Click **OK** to save the domain identifier and return to the SDS Domain Identifiers page.
   - Click **Apply** to save the domain identifier and remain on this page.

- Click **Cancel** to return to the SDS Domain Identifiers page without saving the changes.

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

- Field Domain Identifier contains invalid characters.
- At least one destination was not selected.

3.6.4 Editing domain identifiers

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

1. Select **SDS**, and then **Configuration**, and then **Domain Identifiers**.
2. Select a Domain Identifier and click **Edit**.
3. Edit the Domain Identifier

   For more information about these fields, see Domain Identifiers configuration elements.
4. Click **OK** or **Cancel**.

3.6.5 Deleting domain identifiers

This page allows you to delete a domain identifier. A domain identifier cannot be deleted while any routing entity remains associated with them.

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

1. Select **SDS**, and then **Configuration**, and then **Domain Identifer**.
2. Highlight the domain identifier you want to delete and click **Delete**.
3. Perform one of the following actions:
   - Click **OK** to delete the domain identifier.
   - Click **Cancel** to cancel the delete function and return to the SDS Configuration Domain Identifier page.

   If **OK** is clicked and any of the following conditions exist, and error message displays:
   - Domain identifier is in use by a route.

3.7 Destination Map configuration

The Destination map page adds, modifies, or deletes additional data on an existing Destination.

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

3.7.1 Destination Map configuration elements

This table describes elements on the SDS Configuration Destination Map page.

Table 3-13 Destination Map Elements

Element	Description	Data Input Notes
Filter fields	List of available filters and additional fields to modify the search options	Format: 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

3.7.2 Viewing destination maps

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

1. Select **SDS**, and then **Configuration**, and then **Destination Map**.

   The SDS Configuration Destination Map page displays with the current destination maps listed in the Destination Map table. Click on any column heading to reorder the rows.
2. To look for a specific Destination Map, click **Filter**.
3. Select the category to perform the filtering.

Table 3-14 Destination Map Filtering Categories

Category	Description
Destination	Destination Name
Network Entity	The E.164 address of a service node used by the HLR router

4. Select the filtering operator.

Table 3-15 Destination Map 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)

5. Enter the Destination Name to filter on in the textbox.
6. Click **Go**.

3.7.3 Adding destination maps

Use this page to add a destination map to the database. An IMS HSS 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. Click **SDS**, and then **Configuration**, and then **Destination Map**.
2. Click **Insert**.
3. Enter a Destination name in the **Destination** field. The name must match an IMS HSS Destination name 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 SDS Configuration Destinations Map page without saving the changes.

   If field validations succeed, the destination map is saved. 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

3.7.4 Editing destination maps

Use this page to change an existing destination map in the database. The **OK** button is 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. Click **SDS**, and then **Configuration**, and then **Destination Map**.

2. Highlight the Destination map you want to edit and click **Edit**.
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 **Cancel** to return to the SDS Configuration Destination Map page without saving the changes.

   If 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.

3.7.5 Deleting destination maps

This page allows you to delete a destination map from the database. A destination map cannot be deleted while any IMSI or MSISDN routing entity remains associated with the destination.

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

1. Select **SDS**, and then **Configuration**, and then **Destination Map**.
2. Highlight the destination map you want to delete and click **Delete**.
3. Perform one of the following actions:
   - Click **OK** to delete the map.
   - Click **Cancel** to cancel the delete function and return to the SDS Configuration Destination Map page.

   If **OK** is clicked and any of the following conditions exist, and error message displays:
   - Destination is in use by a route.

3.8 Routing entities configuration

The Routing Entities page manages the supported routing entities:

- MSISDN
- IMSI
- IMSI Prefix
- MSISDN Prefix
- NAI User
- Wildcard NAI User Prefix
- Local Identifier

> **Note:**
>
> A routing entity can be a standalone 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

3.8.1 Routing entities configuration elements

This table describes the fields on the SDS Configuration Routing Entities page.

Table 3-16 Routing Entities Configuration Elements

Element	Description	Data Input Notes
Filter fields	List of available filters and additional fields to modify the search options	Format: selectable list
Type	Type of supported routing entity	Format: list Range: One of the following - MSISDN, IMSI, MSISDN Prefix, IMSI Prefix, NAI User, Wildcard NAI User, External Identifier, Local Identifier **Note**: If **Type** is MSISDN, IMSI, or External Identifier on the Insert or Edit pages and the Address is part of a Subscriber that has more than 1 MSISDN, IMSI, or External Identifier routing entity, the update is automatically applied to all of the subscriber's MSISDN, IMSI, and External Identifier 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 • Local Identifier: 1-128 characters • Domain Identifier: 1-128 characters
Address Prefix (WC NAI User Only)	The routing entity address	Wildcard NAI User: 1–64 characters

Table 3-16 (Cont.) Routing Entities Configuration Elements

Element	Description	Data Input Notes
Local Identifier	The routing entity address. Available only when `External Identifier` is selected as the **Type**.	Format: textbox Range: 1-128 characters
Domain Identifier	Address length. Available only when `External Identifier` is selected as the **Type**. If `External Identifier` is selected, then a **Domain Identifier** must be selected.	Format: list Range: 1-128 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: list Range: available NAI Hosts
IMS HSS (available on the Insert page only)	IMS HSS destination	Format: list Range: available IMS HSS destinations
LTE HSS (available on the Insert page only)	LTE HSS destination	Format: list Range: available LTE HSS destination
MTC HSS	MTC HSS destination	Format: list Range: available MTC HSS destinations
PCRF (available on the Insert page only)	PCRF destination	Format: list Range: available PCRF destinations
OCS (available on the Insert page only)	OCS destination	Format: list Range: available OCS destinations
OfCS (available on the Insert page only)	OfCS destination	Format: list Range: available OfCS destinations
AAA (available on the Insert page only)	AAA destination	Format: list Range: available AAA destinations
User defined 1 (available on the Insert page only)	User defined destination	Format: list Range: available User defined 1 destinations
User defined 2 (available on the Insert page only)	User defined destination	Format: list Range: available User defined 2 destinations

3.8.2 Retrieving routing entities

Use this process to retrieve route information.

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

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

1. Select **SDS**, and then **Configuration**, and then **Routing Entities**.
2. Select the type of routing entity from the **Type** list.
3. If `NAI User` or `Wildcard NAI User` is selected as the **Type**, select an NAI host from the list.
4. If `Local Identifier` is selected as the **Type**, select a Domain Identifier from the list.
5. 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.

6. Click **Go**.

   When **Go** is clicked and the following condition exists, an error message displays:

   - A non-digit was entered for the **Value** field.
   - Field Address or Domain Identifier contains invalid characters.

3.8.3 Adding routing entities

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

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

1. Select **SDS**, and then **Configuration**, and then **Routing Entities**.
2. Click **Insert**.
3. Select the type of routing entity from the **Type** 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** list.
6. If `External Identifier` is selected as the **Type**, enter a **Local Identifier** and select a **Domain Identifier**.
7. Select the associated destination(s) from the applicable destination(s) list.

   At least one destination must be selected, although a destination can be selected for each of the destination types.
8. Perform one of the following:
   - Click **OK** to save the Routing Entity and return to the SDS Routing Entities page.
   - Click **Apply** to save the Routing Entity and remain on this page.

- Click **Cancel** to return to the SDS Configuration Routing Entities page without saving the changes.

If **OK** or **Apply** 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 or Local Identifier contains invalid characters.

3.8.4 Editing routing entities

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

1. Select **SDS**, and then **Configuration**, and then **Routing Entities**.
2. Filter the list of Routing Entities using the Retrieving routing entities procedure.
3. Click **Edit**.
4. Edit the routing entity.

   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**.

5. Click **OK** or **Cancel**.

3.8.5 Deleting routing entities

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

1. Select **SDS**, and then **Configuration**, and then **Routing Entities**.
2. Select the type of Routing Entity from the **Type** list.
3. If `NAI User` or `Wildcard NAI User` is selected as the **Type**, select NAI host from the **NAI Host** list.

   If **Type** is MSISDN, IMSI, or External Identifier 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**, and then **Configuration**, and then **Subscriber [Delete]**.

   If **Type** is MSISDN, IMSI, or External Identifier 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.

4. Type the **Address** of the Routing Entity you want to delete.
5. Click **Go**.

> **Note:**
>
> If the route was not located during the search, a message appears at the bottom of the screen.

6. Highlight the Routing Entity and click **Delete**.
7. Perform one of the following actions:
   - Click **OK** to delete the Routing Entity.
   - 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 displays:
   - 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

3.9 Subscribers

SDS Subscriber Identity Grouping (Subscribers page) groups a customer-specified account ID, multiple MSISDN routing entities, multiple IMSI routing entities, and multiple external identifiers 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, IMSI, or External Identifier). You can also modify addresses within a subscriber by specifying any of the subscriber's addresses.

Restrictions:

- This is a provisioning-only feature. For information, see *Subscriber Database Server Provisioning Interface*.

> **Note:**
>
> You can only add a subscriber to a subscriber table, if the Account ID, MSISDN, IMSI, or External Identifier is not already in the table. If the table already contains any of these values, the add function fails and an error condition report is generated that contains the reason for the failure.

- 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 standalone routing entities.

- Every subscriber must have at least 1 routing entity (MSISDN, IMSI, or External Identifier).
- 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 account ID, MSISDN, IMSI, or External Identifier values must be assigned to one subscriber or they can exist in a standalone 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

3.9.1 Subscribers elements

Use the SDS Configuration Subscribers page to manage SDS Subscribers. This table describes fields on this page. Use the filter function to make initial selections for the elements you want to work with.

To add a Subscriber Table, use **Create** to indicate that a new insert is being performed.

> **Note:**
>
> You can only add a subscriber to a subscriber table, if the Account ID, MSISDN, IMSI, or External Identifier is not already in the table. If the table already contains any of these values, the add function fails and an error condition report is generated that contains the reason for the failure.

Table 3-17 Subscribers Elements

Element	Description	Data Input Notes
Field	Type of data in the Value field used to find desired Subscriber (Account ID, MSISDN, IMSI, External Identifier)	Format: textbox One of the following - Account ID, MSISDN, IMSI, External Identifier Default: Account ID
Value	The value of the Account ID, MSISDN, IMSI, External Identifier 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 • External Identifier: 1-257 characters Default: blank Use **Add**, **Remove**, or **Clear All** to manipulate values within the fields.

Table 3-17 (Cont.) Subscribers Elements

Element	Description	Data Input Notes
External Identifiers	External Identifiers associated with this subscriber	Format: • Domain Identifiers: list • Local Identifiers: textbox Range: External Identifier: 1-257 characters Default: blank Use **Add**, **Remove**, or **Clear All** to manipulate values within the fields.
Inherit Destinations (available on the Insert page only)	If checked, subscriber inherits destinations from specified routing entities.	Format: Checkbox Range: Checked, Unchecked Default: Unchecked
IMS HSS	IMS HSS destination	Format: list Range: available IMS HSS destinations
LTE HSS	LTE HSS destination	Format: list Range: available LTE HSS destination
MTC HSS	MTC HSS destination	Format: list Range: available MTC HSS destinations
PCRF	PCRF destination	Format: list Range: available PCRF destinations
OCS	OCS destination	Format: list Range: available OCS destinations
OfCS	OfCS destination	Format: list Range: available OfCS destinations
AAA	AAA destination	Format: list Range: available AAA destinations
User defined 1	User defined destination	Format: list Range: available User defined 1 destinations
User defined 2	User defined destination	Format: list Range: available User defined 2 destinations

3.9.2 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 Destinations have been configured.

1. Select **SDS**, and then **Configuration**, and then **Subscribers**.
2. Select the type of identifier from the **Type** list.
3. If `External identifier` is selected as the **Type**, select a Domain Identifier from the list.
4. Enter the route identifier for the subscriber in the **Address** or **Address Prefix** field.
5. Enter the subscriber identifier in the **Value** field.

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

6. Click **Go**.

   When **Go** is clicked and the following condition exists, an error message displays:

   - A non-digit was entered for the **Value** field.
   - If `MSISDN`, `IMSI`, or `Local Identifier` was selected as the **Type** and a non-digit character was entered.

3.9.3 Adding subscribers

Use this process to create a new subscriber and group the specified Account ID, MSISDN, IMSI, and External Identifiers into one Subscriber record. The specified MSISDN, IMSI, and External Identifiers can be for existing standalone or new MSISDN, IMSI, or External Identifier routing entities. If the MSISDN, IMSI, or External Identifier does not exist as a standalone routing entity, the routing entity is automatically added, and the MSISDN, IMSI, or External Identifier is added to the Subscriber. All destination values from existing standalone routing entities must be the same before applying the values 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 Destinations have been configured.

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

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

1. Select **SDS**, and then **Configuration**, and then **Subscribers**.
2. Click **Insert**.
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 is 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 is supported. At least one destination must be provided when creating a new MSISDN or IMSI.
6. Select an External Identifier and enter the Local Identifier. Click **Add**, **Remove**, or **Clear All** to implement your updates. A maximum of 10 External Identifiers is supported.
7. Optionally, select **Inherit Destination** to inherit the current destination values from a subscriber's existing routing entity.

> **Note:**
>
> The base field set information that appears here is for display purposes only. See Table 3-17 for more information on each field.

8. Select from any of the following lists to name one of each type of destination.
   - **IMS HSS**
   - **LTE HSS**
   - **MTC HSS**
   - **PCRF**
   - **OCS**
   - **OfCS**
   - **AAA**
   - **User defined 1**
   - **User defined 2**
9. Perform one of the following:
   - Click **OK** to save the Subscriber and return to the SDS Configuration Subscribers page.
   - Click **Apply** to save the Subscriber and remain on this page.
   - Click **Cancel** to return to the SDS Configuration Subscribers page without saving the changes.

   If field validations succeed, the subscriber is saved. If **OK** or **Apply** 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 Account ID or Local Identifier contains invalid characters.

3.9.4 Editing 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**, and then **Configuration**, and then **Subscribers**.
2. Select a **Display Filter** from the list and type the corresponding address or identification number.
3. Click **Go**.

> **Note:**
>
> If a subscriber was not located during the search, a message appears at the bottom of the screen.

4. Highlight the Subscriber you want to edit and click **Edit**.
5. Edit the information you want to change.

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

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

6. Click **OK** or **Cancel**.

3.9.5 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**, and then **Configuration**, and then **Subscriber**.
2. Select a **Display Filter** from the list and type the corresponding address or identification number.
3. Click **Go**.

> **Note:**
>
> If a subscriber was not located during the search, a message appears at the bottom of the screen.

4. Highlight the Subscriber you want to delete and click **Delete**.
5. 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 click **Delete**, a warning dialog box displays indicating all associated MSISDNs and IMSIs are also deleted.

3.10 Blacklist

The Blacklist function (SDS Configuration Blacklist page) provisions IMSI and MSISDN Blacklist values that can be searched before searching the MSISDN or IMSI Routing Entities to determine if a value is blacklisted.

Both MSISDN and IMSI blacklist data are 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

3.10.1 Blacklist configuration elements

This table describes the fields on the SDS Configuration Blacklist page.

Table 3-18 Blacklist Configuration Elements

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

3.10.2 Retrieving blacklist values

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

1. Select **SDS**, and then **Configuration**, and then **Blacklist**.
2. Select the type of blacklist routing entity from the **Type** 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 **Go**.

   When **Go** is clicked and the following condition exists, an error message displays:

   - If a non-digit character was entered for the **Value** field.

3.10.3 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**, and then **Configuration**, and then **Blacklist**.
2. Click **Insert**.
3. Select the type of blacklist routing entity from the **Type** 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. Perform one of the following:
   - Click **OK** to save the Blacklist and return to the SDS Configuration Blacklist page.
   - Click **Apply** to save the Blacklist and remain on this page.
   - Click **Cancel** to return to the SDS Configuration Blacklist page without saving the changes.

   If field validations succeed, the blacklist value is saved. If **OK** or **Apply** 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.

3.10.4 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**, and then **Configuration**, and then **Blacklist**.
2. Select the type of Routing Entity from the **Type** list.
3. Type the **Address** of the Routing Entity you want to delete.
4. Click **Go**.

> **Note:**
>
> If the route was not located during the search, a message appears at the bottom of the screen.

5. Highlight the Routing Entity you no longer want to Blacklist and click **Delete**.
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 displays:
   - If a non-digit character was entered
   - The route identifier was not found
   - **Address** contains invalid characters

4
Maintenance

The Maintenance menu options allow you to query and audit data, view up-to-date status of the database and various features, and 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, including command logs
- 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 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.

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.

4.1 Connections maintenance

The **SDS**, and then **Maintenance**, and then **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 tables.

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

4.1.1 Connections maintenance elements

Table 4-1 describes elements on the **SDS**, and then **Maintenance**, and then **Connections** page.

Table 4-1 Connections Maintenance Elements

Element	Description	Data Input Notes
Timestamp	Time the connection was established	Format: Year-Month-Day Hour-Minute-Second
CID	Connection ID	N/A
Remote IP Address	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 2001:db8:c18:1:260:3eff:fe47:1530 can also be represented as 2001:0db8:0c18:0001:0260:3eff:0fe47:1530 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

Table 4-1 (Cont.) Connections Maintenance Elements

Element	Description	Data Input Notes
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
Cnx Manager	Connection manager	Options: Pdba, Xds, XmlImport, XmlExport, PdbRelay, PdbAudit
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

4.1.2 Viewing connections status

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

1. Select **SDS**, and then **Maintenance**, and then **Connections**.

   All provisioning connections are displayed in the table. Click on any column heading to reorder the rows.

2. To look for a specific connection, click **Filter**.
3. Select the category to perform the filtering.

   The fields are described in Connections maintenance elements.

4. Choose the filtering operator.

Table 4-2 Connections 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)

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

4.2 Command log maintenance

The **SDS**, and then **Maintenance**, and then **Command Log** page shows a table containing 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.

You can view provisioning logs of SDS data being provisioned from various sources. Also, you can export these provisioning logs.

To enable provisioning commands logging (including their responses), you must activate that functionality. Upon feature activation, the command log information is visible on the GUI. Each provisioning command has a response, both of which are stored in the command log information database. The rate of log table export is related to the **System ID** set in the **SDS**, and then **Configuration** , and then **Connections** page.

When calculating the command log export parameters, consider the following:

- When the storage table is full, new entries begin to overwrite newer entries overwrite the oldest entries.
- The table should be exported frequently enough to avoid information loss, but not so frequently that it becomes a resource drain.
- Consider the rate of command/response pairs when setting the log export parameters.
- It is recommended to export the command log data on a daily basis.

To prevent loss of data, you should export the logs before the data is overwritten by the latest entry in table after the table is filled completely. Based on the system usage, you can calculate when the records reach the throttle limit and logs need to be exported. If the log or logs reaches the throttling limit in one day, you must ensure to export the data on daily basis. Typical rates observed in the field tend to be close to 20 commands/second. Based on that rate, the command log would wrap in close to 3 days.

You can calculate your system setup's throttle limits to help determine when logs should be exported. Based on typical in-field throttle rates, a 2 GB table can store 5 million comments. If the system on average takes *x* commands per seconds, then the table will be overwritten by the latest entry in:

5000000/x seconds = 83333/x minutes = 1389/x hours = 58/x days (where *x* is the commands per second)

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

4.2.1 Command log maintenance elements

Table 4-3 describes elements on the **SDS**, and then **Maintenance**, and then **Command Log** page.

Table 4-3 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

Table 4-3 (Cont.) Command Log Maintenance Elements

Element	Description
Text	Exact command and response message

4.2.2 Viewing maintenance command logs history

Use this task to view a history list of commands and their responses. The history is displayed as a table showing the **Timestamp**, **System ID**, **CID**, and **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**, and then **Maintenance**, and then **Command Log**.
2. Click **Show Errors** at the bottom of the table to display only the error responses out of all the records.
3. To look for a specific log, click **Filter**.
4. Select the category to perform the filtering.

   The fields are described in Table 4-3.
5. Choose the filtering operator.

Table 4-4 Command Log Filtering Operators

Operator	Description
=	Is equal to
Like	Is Like (wildcard is * character)

6. Enter the target character string to filter on in the text box.
7. Enter the maximum number of records to display.
8. Mark the **Time Range** checkbox and enter a date range of the records to display.
9. Click **Go** to show results.

4.2.3 Exporting maintenance command logs

Use this task to export provisioning log commands and their responses to a database. The exported files are copied to a remote server. This is a server other than the single remote server supported by **APDE**. The files are then deleted from the local system after the transfer is complete. Files exported to the file management area can be viewed and imported on the local system.

> **Note:**
>
> The export file is in CSV format.

1. Select **SDS**, and then **Maintenance**, and then **Command Log**.
2. Click **Export**.
3. Choose the filtering operators to filter and control command log exportation functionality.

   The fields are described in Table 4-5.

Table 4-5 Exporting Command Log Filtering Operators

Operator	Description
None	No filter
System ID	View exported logs by System ID
CID	View exported logs by CID
Log Text	View exported logs by Log Text

4. Enter the maximum number of records to display.
5. Enter the export logs value for last number of hours.
6. Set the export frequency to determine to select how often the data is written to the export directory. The export frequency gives you a way to limit the size of the export to a configurable number of hours prior to the start of the export. This helps you control system resources that are used for the export function.
7. Enter a periodic export task name.
8. Enter a name for this export file.
9. Enter a periodic export task description.
10. Select the directory in which the export file or files will be placed. Exported files are automatically overwritten in the **Data Export Server Directory** if the remote server is set up. The files are then deleted from the local system after the transfer. Files exported to the **File Management Directory** can be viewed and imported on the local system.

    The Remote Server is configured through Multiple Export Server on the Administration -> Remote Servers -> Data Export page..
    See *Operations, Administration, and Maintenance (OAM) User's Guide* for information about Multiple Export Server and Filename Prefix. Filename Prefix is an optional export filename prefix that pre-pends the generated export filename.
11. Select the minute of each hour when the data is written to the export directory.
12. Select the time of day when the data is written to the export directory.
13. Select the day of week when the data is written to the export directory.
14. Click **OK**.

4.3 Relay exception log

The **SDS**, and then **Maintenance**, and then **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 you can determine what SDS data caused the exception.

Ideally, the Relay Exception Log would be empty, which means 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.

4.3.1 Relay Exception Log maintenance elements

Table 4-6 contains a list of exceptions found while processing data that should be relayed from SDS to HLRR on the **SDS**, and then **Maintenance**, and then **Relay Exception Log** page.

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

Table 4-6 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
Reason	Reason 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

4.3.2 Viewing relay 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 showing 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**, and then **Maintenance**, and then **Relay Exception Log**.
2. To look for a specific log, click **Filter**.

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

   The fields are described in Table 4-6.

4. Choose the filtering operator.

Table 4-7 Relay Exception Log Filtering Operators

Operator	Description
=	Is equal to
Like	Is Like (wildcard is * character)

5. Enter the target character string to filter on in the text box.
6. Enter the maximum number of records to display.
7. Mark the **Time Range** checkbox and enter a date range of the records to display.
8. Click **Go** to show results.

4.4 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 server (**Remote Import Directory**) are detected within five minutes and automatically downloaded using 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 containing 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.

4.4.1 Import status maintenance elements

Table 4-8 describes elements on the **SDS**, and then **Maintenance**, and then **Import Status** page.

Table 4-8 Import Status Maintenance Elements

Element	Description
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
Success Count	Number of successful import commands
Fail Count	Number of unsuccessful import commands
Progress	Percentage of import progress
Result Log	Name/heading of result log
Status	Status of the import

4.4.2 Viewing import status 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 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**, and then **Maintenance**, and then **Import Status**.

   Click on any column heading to reorder the rows.
2. To look for a specific import, click **Filter**.
3. Select the category to perform the filtering.

   The fields are described in Table 4-8.
4. Choose the filtering operator.

Table 4-9 Connection 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)

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

7. To delete an import record, select a record and click **Delete**.

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

4.5 Export schedule and status 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 the export table take effect on next export period. The following is the functionality of Export:

- You can configure and schedule data export on daily, weekly, or monthly.
- The exported files are sFTPed or transferred via SSH to a server configured on SDS.
- Data can be exported to a file in XML, CSV, or HLRR formats to be used as import files for an HLRR.
- You can export subscriber data (in XML or CSV format) as shown in Table 4-10:

Table 4-10 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
Subscriber	yes	yes	no	no	yes	yes
MSISDN	yes	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)
IMSI	yes	yes	yes	yes	yes	yes
MSISDN Prefix	yes	yes	no	no	no	yes
IMSI Prefix	yes	yes	no	no	yes	yes
MSISDN Blacklist	yes	yes	no	no	yes	yes

Table 4-10 (Cont.) 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
IMSI Blacklist	yes	yes	no	no	yes	yes
Domain Identifiers	yes	yes	yes	yes	yes	yes
Local Identifiers	yes	yes	yes	yes	yes	yes
NAI Hosts	yes	yes	yes	yes	yes	yes
NAI Users	yes	yes	yes	yes	yes	yes
Destination	yes	yes	no	no	yes	yes
Destination Map	yes	yes	no	no	yes	yes

4.5.1 Export Schedule

The **SDS**, and then **Maintenance**, and then **Export Schedule** page displays information for all exports scheduled for this system.

4.5.1.1 Export schedule maintenance elements

Table 4-11 describes elements on the **SDS**, and then **Maintenance**, and then **Export Schedule** page.

Table 4-11 Export Schedule Maintenance Elements

Element	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

4.5.1.2 Viewing export schedule

The **SDS**, and then **Maintenance**, and then **Export Schedule** page shows the scheduled exports for this system.

1. Select **SDS**, and then **Maintenance**, and then **Export Schedule**.

   The SDS Maintenance Export Schedule page displays with all exports displayed as a table. Click on any column heading to reorder the rows.

2. To look for a specific export schedule, click **Filter**.
3. Select the category to perform the filtering.

The fields are described in Table 4-11.

4. Choose the filtering operator.

Table 4-12 Export Schedule 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)

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

4.5.1.3 Inserting an export schedule

The **SDS**, and then **Maintenance**, and then **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. Click **SDS**, and then **Maintenance**, and then **Export Schedule**.
2. Click **Insert** located on the bottom of the page.
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 select the **File Format** of the export file.
5. Use the lists to select the initial date at which this export should run.
6. Use the lists to select the initial time at which this export should run.
7. 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 4-13 Export Data Types

Type of Data	CSV Format	XML Format	HLRR Format
All	X	X	X
Subscriber	X	X	
MSISDN	X	X	X
IMSI	X	X	X
MSISDN Prefix	X		
IMSI Prefix	X		
MSISDN Blacklist	X		
IMSI Blacklist	X		

Table 4-13 (Cont.) Export Data Types

Type of Data	CSV Format	XML Format	HLRR Format
NAI Host	X		
NAI User	X	X	
Wildcard NAI User	X		
Destinations	X		
Local Identifier	X	X	
Domain Identifier	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.

8. Use the radio buttons **None**, **Daily**, **Weekly**, or **Monthly** 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 displays.
    - 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.

4.5.1.4 Editing an export schedule

The **SDS**, and then **Maintenance**, and then **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 to be successful. Fields marked with a red asterisk (*) require a value.

1. Select **SDS**, and then **Maintenance**, and then **Export Schedule**.
2. Highlight the export you want to edit and click **Edit**.

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 select the **File Format** of the export file.
5. Use the appropriate drop down list to select the initial date at which this export should run.
6. Use the appropriate drop down list to select the initial time at which this export should run.
7. 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 4-14 Export Data Types

Type of Data	CSV Format	XML Format	HLRR Format
All	X	X	X
Subscriber	X	X	
MSISDN	X	X	X
IMSI	X	X	X
MSISDN Prefix	X		
IMSI Prefix	X		
MSISDN Blacklist	X		
IMSI Blacklist	X		
NAI Host	X		
NAI User	X	X	
Wildcard NAI User	X		
Destinations	X		
Local Identifier	X	X	
Domain Identifier	X	X	

8. Use the radio buttons **None**, **Daily**, **Weekly**, or **Monthly** to select how often this export should be repeated.
9. In the Comment text box, enter text 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 **Cancel** to abort changes on this page and return to the previous page.

4.5.1.5 Deleting an export schedule

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

1. Select **SDS**, and then **Maintenance**, and then **Export Schedule**.
2. Highlight the destination you want to delete and click **Delete**.

3. Perform one of the following actions:
   - Click **OK** to confirm the action to delete the export record and return to the **SDS**, and then **Maintenance**, and then **Export Schedule** page.
   - Click **Cancel** to abort the delete action and return to the **SDS**, and then **Maintenance**, and then **Export Schedule** page.

4.5.2 Export Status

The **SDS**, and then **Maintenance**, and then **Export**, and then **Status** page shows all in-progress and completed scheduled exports in this system.

4.5.2.1 Export status maintenance elements

Table 4-15 describes elements on the **SDS**, and then **Maintenance**, and then **Export Status** page.

Table 4-15 Export Status Maintenance Elements

Element	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
Domain Identifiers	Number of Domain Identifiers exported
Local Identifiers	Number of Local Identifiers 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
Comment	Descriptive text about export. This field is optional, so it may be blank.

4.5.2.2 Viewing export status

The **SDS**, and then **Maintenance**, and then **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 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**, and then **Maintenance**, and then **Export Status**.

   The SDS Maintenance Export Status page appears with all exports displayed as a table. Click on any column heading to reorder the rows.

2. To look for a specific export status, click **Filter**.
3. Select the category by which to perform the filtering.

   The fields are described in Table 4-15.

4. Choose the filtering operator.

Table 4-16 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)

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

4.6 Remote audit

The SDS Maintenance Remote Audit page 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 and configurable automated audit runs between the SDS master database instance and the HLR Router database instance. Configurable automated audit runs are those runs that run at configured times to verify the accuracy of SDS master and HLR Router database instances. A manual audit allows specification of audit between SDS master and HLR Router database 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 SDS Maintenance Remote Audit page to:

- View the status of the database remote audits and to request a site-wide database audit of a specified subset of provisioning data, and/or
- 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 to maintain sufficient resources to process signaling traffic.

4.6.1 Remote audit elements

Table 4-17 describes the elements on the **SDS**, and then **Maintenance**, and then **Remote Audit** page.

Table 4-17 Remote Audit Elements

Element	Description	Data Input Notes
Type	Type of data being audited	Format: MSISDN or IMSI
Range/File	Range of data being audited or file name containing ranges of data being audited	Format: Digits only Range: 8 - 15 digits for MSISDN Range: 10 - 15 for IMSI

Table 4-17 (Cont.) Remote Audit Elements

Element	Description	Data Input Notes
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 0000:0000:0000:0000:00000:0000:0000:0001
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 • 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

Table 4-17 (Cont.) Remote Audit Elements

Element	Description	Data Input Notes
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

4.6.2 Viewing the status of a remote audit

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

1. Select **SDS**, and then **Maintenance**, and then **Remote Audit**.

   The SDS Maintenance Remote Audit page appears with all pending, completed, and failed remote database audits of data performed throughout the system displayed as a table. Click on any column heading to reorder the rows.

2. To look for a specific audit, click **Filter**.
3. Select the category to perform the filtering.

   The fields are described in Remote audit elements.

4. Choose the filtering operator.

Table 4-18 Remote Audit 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)

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

4.6.3 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**, and then **Maintenance**, and then **Remote Audit**.
2. Click **Insert** located on the bottom of the page.
3. Select the type of data you want included in the audit from the **Data Type** list.
4. Select Range for **Audit By** and 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.

   Or, select File for **Audit By** and browse to the file containing ranges of values to be included in this audit.
5. Enter any text about the audit you want to include in the **Comment** field, if needed.
6. Perform one of these actions.
   - Click **OK**. If field validations succeed, the database audit request is made. The status of the request can be viewed on the **SDS**, and then **Maintenance**, and then **Remote Audit** page. If the page contains any values that are not valid, or if a required field is empty, an error message appears.
   - Click **Cancel** to abort changes on this page and return to the previous page.

4.7 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 hosting 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.

4.7.1 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 4-19. All elements available through Query results display, in alphabetical order, are presented in Table 4-20.

Table 4-19 Query Entry Elements

Element	Description	Data Input Notes
Data	Type of data to include in query	Format: 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
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 4-20 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
DB Level	Numeric value of Database level	DB Level
Destination(s)	Unique text used to identify a Destination	Counts, Counts by Destination
External Identifier	Number of subscribers with external identifiers	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

Table 4-20 (Cont.) Query Results Elements

Result Element	Description	Data Value Selected
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
IMS HSS	IMS HSS Destination record (with type= imsHss) or blank for none	MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix
LTE HSS	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
MTC HSS	MTC HSS Destination record (with type-mtcHss) or blank for none	MSISDN, IMSI, NAI User, Wildcard NAI User, MSISDN Prefix, IMSI Prefix
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

4.7.2 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. Click **SDS**, and then **Maintenance**, and then **Query**.
2. Select a value from the **Data** 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** list.
6. Click **Query**.

The query is run and any relevant data displays on the page. See Table 4-20.

4.7.3 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. Click **SDS**, and then **Maintenance**, and then **Query**.
2. Select **NAI User** from the **Data** 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** list.
5. Click **Query**.

The query is run and any relevant data is displayed on the page. See Table 4-20.

4.7.4 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. Click **SDS**, and then **Maintenance**, and then **Query**.
2. Select one of the following from the **Data** 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** list.
4. Click **Query**.

The query is run and any relevant data is displayed on the page. See Table 4-20.

4.8 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.

4.8.1 NPA Splits elements

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

Table 4-21 NPA Splits Maintenance Elements

Element	Description	Data Input Notes
Old NPA	The Numbering Plan Area 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 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 Edit and Delete pages, an **All** selection box is also available. If this check box is marked (the default) when the **OK** button is clicked, all NXXs are modified or deleted.	Format: Integer Range: 000 - 999, 3-digit number Default: blank

Table 4-21 (Cont.) NPA Splits Maintenance Elements

Element	Description	Data Input Notes
Start PDP Date	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. • If today's date is entered, activation occurs within 15 minutes of the **Insert** or **Edit** button being clicked. • This field only appears on the Insert and Edit pages.	Format: list Range: Valid date Default: Tomorrow's date
End PDP Date	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 Insert and Edit pages.	Format: list Range: Valid date Default: Tomorrow's date + 90 days

4.8.2 Viewing NPA Splits

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

If the **Save Results** checkbox is 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**, and then **Files**).

1. Select **SDS**, and then **Maintenance**, and then **NPA Splits**.

   The SDS Maintenance NPA Splits page appears with all NPA Split information found in the PDB database. Click on any column heading to reorder the rows.
2. To look for a specific NPA Split, click **Filter**.
3. Add search criteria to the fields in the Value column, as desired.
4. Mark or unmark any **All** checkboxes.
5. Click **Go** to show results.

   The SDS Maintenance NPA Splits (Filtered) page displays the results.

4.8.3 Creating an NPA Split

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**, and then **Maintenance**, and then **NPA Splits**
2. Click **Insert** located at the bottom of the page.

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. Perform one of these actions:

   - Click **OK**. The NPA Split record is provisioned. Its state is initialized to Pending 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.

4.8.4 Editing 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**, and then **Maintenance**, and then **NPA Splits**.
2. Highlight the NPA Split you want to edit and click **Edit**.
3. To modify all **NXX**, make sure the **All** checkbox is 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. Perform one of these actions:

   - Click **OK**. If field validations succeed, the NPA splits are updated. If the page contains any values that are not valid, an error message appears.
   - Click **Cancel** to abort changes on this page and return to the previous page.

4.8.5 Deleting an NPA Split

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

1. Select **SDS**, and then **Maintenance**, and then **NPA Splits**.
2. Highlight the NPA Split you want to delete and click **Delete**.

   A confirmation pop up window appears, asking if you are sure you want to delete this NPA Split.

3. Perform one of the following actions:

   - Click **OK** to confirm the action to delete NPA Split and return to the **SDS**, and then **Maintenance**, and then **NPA Splits** page.
   - Click **Cancel** to abort the delete action and return to the **SDS**, and then **Maintenance**, and then **NPA Splits** page.