



# **Signaling Delivery Controller**

## **Feature List**

4.4

Catalog Number: GD-015-44-31 Ver. 2

Publication Date: June 2015



## Legal Information

### Copyright

© 2005-2015 F5 Networks, Inc. All rights reserved.

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

### Trademarks

AskF5, F5, F5 [DESIGN], F5 Networks, OpenBloX, OpenBloX (design), Rosetta Diameter Gateway, Signaling Delivery Controller, SDC, Traffix, and Traffix [DESIGN] are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

### Patents

This product may be protected by one or more patents indicated at: <http://www.f5.com/about/guidelines-policies/patents>

### Confidential and Proprietary

The information contained in this document is confidential and proprietary to F5 Networks. The information in this document may be changed at any time without notice.

### About F5 Networks

F5 Networks (NASDAQ: FFIV) makes the connected world run better. F5 helps organizations meet the demands and embrace the opportunities that come with the relentless growth of voice, data, and video traffic, mobile workers, and applications—in the data center, the network, and the cloud. The world's largest businesses, service providers, government entities, and consumer brands rely on F5's intelligent services framework to deliver and protect their applications and services while ensuring people stay connected. For more information, visit [www.F5.com](http://www.F5.com) or contact us at [Tfx\\_info@f5.com](mailto:Tfx_info@f5.com).



## About this Document

Document Name: F5 Signaling Delivery Controller Feature List

Catalog Number: GD-015-44-31 Ver. 2

Publication Date: June 2015

## Document Objectives

This document lists the F5 Signaling Delivery Controller's features.



## Document History

Revision Number	Change Description	Change Location
June 2015 – 2	Updated trademark information	Legal Information

## Conventions

The style conventions used in this document are detailed in Table 1.

**Table 1: Conventions**

Convention	Use
<b>Normal Text Bold</b>	Names of menus, commands, buttons, user-initiated CLI commands and other elements of the user interface
<i>Normal Text Italic</i>	Links to figures, tables, and sections in the document, as well as references to other documents
Script	Language scripts
Courier	File names
 Note:	Notes which offer an additional explanation or a hint on how to overcome a common problem
 Warning:	Warnings which indicate potentially damaging user operations and explain how to avoid them



## Table of Contents

1. About F5 Signaling Delivery Controller .....	1
2. Product Features.....	4

## List of Figures

Figure 1: F5 Signaling Delivery Controller.....	1
---	---

## List of Tables

Table 1: Conventions .....	II
Table 2: SDC Feature Description .....	4
Table 3: Terms and Abbreviations .....	19



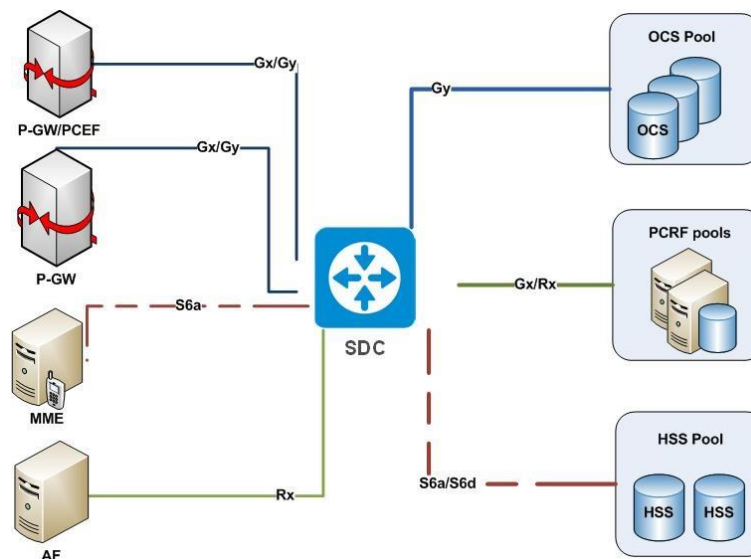
## 1. About F5 Signaling Delivery Controller

The F5® Traffix® Signaling Delivery Controller™ (SDC) is a single modular signaling platform that provides a flexible and robust solution for the emerging control plane connectivity challenges. SDC is shown in *Figure 1*.

SDC was designed to meet the demanding requirements posed by the growing volume of signaling traffic and the complexity of connectivity and signaling in LTE and IMS networks with advanced Diameter Gateway, Diameter Load Balancer, and Diameter Router solutions, consolidated on a single unified platform.

SDC enables service providers to scale and manage services and applications in LTE and IMS networks, supporting millions of concurrent sessions and hundreds of millions of subscribers. The SDC solution centralizes signaling and Diameter routing, traffic management, and load balancing tasks to scale and grow IMS and LTE networks incrementally and cost effectively, while increasing resiliency and reliability to support subscribers' ever increasing service and broadband demands.

**Figure 1: F5 Signaling Delivery Controller**





The core functionality of SDC is based on a powerful contextual routing engine which allows definition and execution of different routing policies that simplify the control plane network management. The routing engine, together with the advanced load balancing algorithms, fast failback detection, failover mechanisms, and congestion control, provide unprecedented scalability and high-availability of Diameter and other nodes.

When deploying SDC between LTE, IMS, and legacy network elements, service providers gain multiple added-value benefits such as:

- **Simple and transparent** Diameter network configuration, administration, and maintenance. Easy installation procedures with a user friendly GUI makes SDC fast to deploy and easy to maintain. Its capabilities are extremely powerful, yet simple to configure and modify. Automatic cluster detection and a secure configuration replication among parallel cluster nodes reduce the administrator's efforts to minimum.
- **Comprehensive network management** using Diameter contextual routing engine that reduces and centralizes the routing logic and relieves Diameter nodes from handling this logic.
- Congestion control for Diameter servers using advanced in-band health monitoring, overload detection and throttling mechanisms. Using the health monitoring mechanisms, SDC manages back-end failures and reduces the risk of unintentionally sending traffic to overloaded or unavailable servers.
- **Scalability and scalability** of Diameter server nodes (such as PCRF, HSS, OCS) using Layer 4-7 load balancing algorithms, and fast failover detection and failback mechanisms. Combined with congestion control mechanisms, SDC assures that signaling traffic is sent to healthy servers and that after unhealthy server recovery, it is automatically and gradually reintroduced to the network.
- SDC provides **flexibility, scripting and customization**. SDC provides full user control for definition for routing and transformation script rules using the Java-based



Groovy scripting language. Using this flexible scripting, the SDC can detect errors in messages or perform interaction with external systems while executing routing decision. When interaction with external systems is required, the SDC can be integrated with 3rd party, Java-based libraries.

- **LTE to legacy interoperability** interconnectivity between new Diameter-based functionalities and legacy infrastructure using legacy signaling protocols.
- Service level **security** and **authorization** for Diameter. To avoid Denial of Service and Distributed Denial of Service attacks, SDC runs different heuristics to protect the system from overrun attempts and invalid requests. It also controls and fine-tunes Denial of Service protection through ACLs.
- **Visibility** into Diameter level performance. The management console allows real time performance visualization and monitoring of SDC internals and back-end servers. The performance counters are also available through multiple methods that allow import to external monitoring systems.
- **Carrier grade** product using off the shelf hardware. SDC supports front-end failover using multiple Virtual IPs. Using multi-threading and internal load balancing, the SDC performance scales linearly with the number of cores/processors and the number of SDC blades. The scale out ability protects SDC and the signaling network from multiple compound failures.

SDC provides Diameter protocol routing, mediation and interworking functions, allowing service providers to manage legacy to LTE and LTE to LTE roaming seamlessly. By avoiding the need of complex integration and customization projects, SDC provides a simple, reliable, and easy to deploy solution to the most challenging control plane connectivity issues.

SDC is the market's only fully native Diameter solution and can be deployed as an IETF Diameter Agent (relay, proxy, redirect and translation), 3GPP Diameter Routing Agent (DRA), GSMA Diameter Edge Agent (DEA) and 3GPP Interworking function (IWF).



## 2. Product Features

The following table details and describes SDC's application features for release 4.4:

**Table 2: SDC Feature Description**

Feature	Description	License Type
Partial Out-of-Service Peer State	<p>The system supports a new defined peer state when a peer is partially out of service. Peers in this state will process existing sessions while not accepting new sessions. Entering to and from this state can be done manually.</p> <p>The new state can be configured programmatically (using groovy script).</p>	Basic
Diameter Identity	<p>When defining the peer profiles for Diameter peers, there is an option to configure specific values to replace the message's origin-host and origin-realm AVPs that the message receives from the FEP. The available Diameter Identity policies include:</p> <ul style="list-style-type: none"><li>• Relay – All the requests or answers will be forwarded without any modification.</li><li>• Client Side proxy – used to abstract the server from clients.</li><li>• Full proxy – used to abstract the servers from the clients and clients from the servers.</li><li>• Roaming proxy – used to abstract the servers from the clients and clients from the servers in roaming use cases.</li></ul> <p>The new AVP values can be configured to be kept for existing sessions in session failover scenarios between mated SDC sites.</p>	Basic
Forwarding to Pool	<p>Requests can be forwarded to pools, as well as to peers, based on one of the request parameters</p>	Basic





Feature	Description	License Type
Logging and Statistics for Session Management	The SDC can be configured to create logs for session life cycle events and session errors. These logs can be used to help troubleshoot when stateful sessions fail to route. The user can configure additional log messages for specific AVPs.	Basic
Session Replication Enhancement	<p><b>Session Expiration:</b></p> <p>To avoid session expiration of a replicated copy of a session on a mated SDC, an enhancement was added to session management mechanism. Following a session expiration, the system checks if a replicated session exists on a mated SDC, and if so, the session is not deleted, and the timer of that session is restarted.</p> <p><b>Session Event Auto-Proxy:</b></p> <ul style="list-style-type: none"><li>▪ If an ongoing session event cannot find a relevant session in a local session repository, it can be seamlessly transferred to the replicated copy of session repository on the mated SDC. The session lookup is then performed on the mated SDC.</li></ul>	Basic
Routing	<p>Routing rules apply different criteria using combinations of Diameter AVP's, request source, and other properties to make decisions. The routing engine natively works with the load balancing and the transformation engines to provide a harmonized solution for the most demanding and highly complex deployments.</p> <p>Basic routing decisions result in the selection of a destination pool for the established Diameter session. Pool selection is done using a combination of different AVPs such as Subscription-Id, APN from Called-Station-ID, Application-ID, Source-Peer, etc. The</p>	Basic



Feature	Description	License Type
	<p>values of the AVPs of the incoming requests are matched with condition sets defined for SDC routing rules or by resolution against external service location functions.</p> <p>In some deployments, routing decisions should be retrieved from an external system. F5 SDC supports several methods of retrieving the routing decisions.</p>	
Bi-Directional In-Session Routing	The Diameter server peer sends the request (e.g. RAR) to the Diameter client peer using the same Diameter Session-ID that was previously established by the Diameter client side. SDC routes the request to the client that established the session.	Basic
Bi-Directional Out of Session Routing	In some cases the communication between the Diameter client and server peers is stateless, meaning that SDC does not maintain a reverse path for the Session-ID. To allow proper handling of out of session server initiated Diameter request, SDC implements advanced routing rules that can be used by the user to define the required behavior. In case no rule is set, SDC sends the request to a client based on the request's "Destination-Host" AVP.	<i>Basic</i>
Redirected Routing	The SDC routing engine supports working in redirect mode. In this mode SDC acts as a Diameter DNS and leases routing decisions to the clients for a predefined and configurable amount of time.	Basic
Session Binding	For some Diameter reference points, there is a need to bind sessions originating from different network elements and share common attributes.	Basic



Feature	Description	License Type
	<p>Bound sessions are related to as Slave Sessions subject to their Master Sessions. The Master Session is the session for which the routing selection is performed based on the routing rules. Slave Sessions are applied with routing rules inherited from the Master Session.</p> <p>The session binding is done using one of several session binding methods and based on binding keys, sets of values extracted from different attributes - AVPs or XML attributes - of the Master Session.</p>	
Multi-Protocol Session Binding	<p>Multiple-protocol session binding is applied by linking Destination Server Peers, in addition to the routine client session binding. When two destination servers share a Binding Name they act as a cluster of servers in which each server handles its corresponding sessions, when handling sessions originating from multiple-protocol Clients.</p>	<p>Basic</p> <p><i>Note: Each additional protocol support is an add-on functionality, however the session binding is not.</i></p>
Load Balancing	<p>SDC offers several load balancing policies. Load balancing policies define the pattern according to which the system decides how to distribute control plane traffic across the peer nodes in the pool:</p> <ol style="list-style-type: none"><li>1. By Precedence: Diameter messages are sent to the first peer in the pool. The messages are sent until health monitoring and overload detection mechanisms decide that the peer is out-of-service. Then Diameter messages are sent to the next Remote Node in the pool, etc.</li><li>2. Contextual: Using this method, messages are sent to a specific Diameter peer according to their Context ID and a predefined proportion.</li><li>3. Round Robin: traffic is evenly distributed across the pool's available Diameter peers and</li></ol>	<p>Basic</p>



Feature	Description	License Type
	<p>the Diameter peer to which the new request is delivered is the next available in row.</p> <p>4. Weighted Round Robin: traffic is distributed across the pool's available Diameter peers according to a predefined proportion defined by a peer's weight.</p> <p>5. Fastest Response Time: messages of new Diameter sessions are distributed to the Remote Node which has the fastest average response time measured during last measurement period.</p> <p>User Defined Policy: the request's destination Diameter peer is selected according to a user defined policy implemented by an external script. The external script can be combined with one of the methods listed and described above.</p>	
Message Transformation	<p>The message transformation mechanism implemented by SDC overcomes interoperability issues between different Diameter vendors and allows the translation from one Diameter protocol to another signaling protocol and vice versa. SDC provides full support for adding, modifying and/or removing AVPs based on user configurable rules. The rules are implemented using smart grids and Groovy scripting language, which provides configuration flexibility and simple management.</p> <p>The solution enables bi-directional Diameter message modification and provides the ability to create different rules of message modification according to the direction of the message flow and/or message type</p>	<p>Each protocol requires an add-on license. The following protocols are supported:</p> <ul style="list-style-type: none"><li>• Diameter</li><li>• HTTP</li><li>• JMS</li><li>• RADIUS</li></ul>



Feature	Description	License Type
Front-End Proxy	FEP is a network distribution point in an F5 appliance. It is built on top of the CPF framework to take advantage of the CPF management, pipeline and other infrastructures. FEP maintains a steady single connection of TCP with the multiple CPF nodes. For each Remote Node, it manages the connection and state machine, providing statistics and management capabilities for the connections and the traffic.	<i>Basic</i>
Overload and Congestion Control	SDC provides multiple mechanisms for resource management and congestion control that protect SDC and the connected Peer nodes from overload conditions, by controlling and limiting the resources usage and allocation, e.g. controlling the incoming/outgoing message/traffic rate. The implemented methods are based on message oriented flow control, traffic shaping algorithms and load shedding algorithms.	Basic
Throttling and Rate Limiting	The throttling and flow control mechanisms implemented in SDC are based on token bucket algorithm. The token bucket algorithm is used to check that data transmissions conform to defined limits on bandwidth and burstiness. SDC implements two types of throttling: message rate limiter and byte rate limiter.	Basic
Overload Control	When overload conditions are detected, incoming messages are either gracefully rejected or discarded. If message rejection is applied, SDC replies with user configurable busy Result-Code (e.g. DIAMETER_TOO_BUSY), while in case of discard the message is dropped immediately, and no processing is applied.	Basic



Feature	Description	License Type
Health Monitoring	SDC provides built in health monitoring mechanisms that are used to identify overload condition or other abnormal behavior of the remote Diameter peers and act accordingly. Two health-monitoring mechanisms are available: In Session Monitoring and External Health Monitoring. When overload or abnormal behavior is detected, proper alarms are sent to the OSS and traffic is routed to an alternative Diameter peer or is gracefully rejected according to the defined policy. The alarms triggered by the system contain sufficient information to describe the type of overload.	Basic
OA&M Support	<p>SDC provides support for Operation, Administration, and Maintenance (OAM) using its Management function. The Management function of the platform is comprised of the following modules:</p> <ul style="list-style-type: none"><li>• Configuration Manager: the configuration repository and configuration distribution service responsible for the distribution of the configuration to all SDC nodes within the cluster. It also provides auditing, backup and restore functions, as well as server for performance statistics collection.</li><li>• Management Console: a Web based client GUI that enables, configures and manages SDC.</li></ul> <p>Provisioning Interface (SOAP API): provides programmatic interface that enables automatic configuration and management of SDC.</p>	Basic
Alarms	The OAM constitutes a collection and aggregation point for all alarms and events issued by the platform components and the deployed applications. Fault	Basic



Feature	Description	License Type
	<p>management capabilities such as alarm clearing, alarm filtering, alarm flood suppression and alarm forwarding are provided. All fault situations are notified with an appropriate alarm. Recovery from a fault situation is also notified with the associated clearance alarm.</p> <p>The OAM uses SNMP to deliver traps to Network Managements Centers. This is done via an SNMP Agent that delivers traps to SNMP managers connected to it. The OAM supports SNMP v2c.</p>	
Tracing and Logging	The OAM ensures management of component-based tracing, logging and statistics reports. The platform provides OAM with configured traces on per-component basis (Node, Peer and Pool). It also updates the configured statistic counters in real-time so that SNMP can generate the required statistic reports.	Basic
Monitoring	The OAM ensures monitoring of manageable components providing real-time information about the status of cluster, nodes, application, service enablers, and protocol stacks. Monitoring of resource usage such as memory and CPU is also provided.	Basic
Performance Management	The OAM supports a predefined set of performance counters and allows for definition of custom performance counters. Monitoring, and scheduling of performance counter as well as statistic collection related to performance counters are supported. The OAM supports the compression of performance reports since those may have a very large size.	Basic



Feature	Description	License Type
Licensing Management	The OAM supports the functions related to licensing and licensing issues notification. License keys, as well as counter reports related to licensing (i.e. reports of number of Sessions Per Second during a predefined period) are monitored by OAM, which acts according to the observed state and counter values. Hence, the OAM can notify the operator about the need of a new license key or of the extension of the licensed traffic volume.	Basic
Lifecycle Management	The OAM supports lifecycle management of the platform's components and services. It also supports dynamic configuration of parameters related to the platform's components and services. Graceful Software and Hardware upgrade (i.e. without service interruption) are part of the OAM configuration management functions.	Basic
SOAP API	<ul style="list-style-type: none"><li>▪ SOAP API is a programmatic interface that allows users to automate commands as well as integrate OAM with umbrella management systems or Network Management Centers for functionalities such as automatic provisioning, queries, lookups and more.</li></ul>	Basic
Cluster Management	The Cluster management process is constantly monitoring platform instances and can take appropriate actions in case of fatal fault situation (for example, restart the Diameter Router instance in case the latter is not responding for a certain period of time).	Basic
Auditing	The OAM documents each of the actions taken in the auditing list. If needed, the audited actions can be used to restore the documented configuration of the	Basic





Feature	Description	License Type
	exact point in time in which the action was performed.	
Backup and Restore	The OAM provides support for backup and restore of the configuration backup. Using this feature, it is possible to restore the configuration back to a working configuration set.	Basic
High Availability and Scalability	<p>The SDC solution provides a vertical and horizontal scalability. Both options are standard, and provided out-of-the-box.</p> <ul style="list-style-type: none"><li>For vertical scalability it implements a message driven component, optimized for low latency processing and multi-core architecture, e.g. SPARC. It relies heavily on multithreading and asynchronous network I/O processing.</li></ul> <p>For horizontal scalability it allows use of multiple servers in two modes; “hot standby deployment” and “scalable deployment”.</p>	Basic
Local Redundancy and Scalability	The SDC solution supports Hot/Standby and N+1 redundancy models. In both models, any failure on the SDC side is transparent to both client and server peers and does not require any manual intervention or reconfiguration of the nodes.	Basic
Geographical Redundancy	SDC supports geographical redundancy by deploying locally redundant SDC clusters in each geographical location site. Each of the locally redundant SDC clusters exposes one or more VIP address/es,	Basic
Network Redundancy	SDC applies the networking redundancy scheme for both TCP and SCTP transport protocols. The network redundancy is achieved using redundant pairs of Switch modules (one pair for Signaling traffic and	Basic <i>Note: The feature is included in the SDC license, however</i>



Feature	Description	License Type
	another pair for O&AM) and NIC bonding for TCP or multi-homing SCTP.	<i>there may be additional HW requirements necessary to support the feature. These additions are not included.</i>
Security Enforcement	<p>SDC enables service providers to apply policy control and different security methods on the peer nodes.</p> <p>The security enforcement is done by setting and applying security rules on both the IP and the application levels.</p> <p>The Security rules at the IP level are defined in ACL format. At the application level, the rules are defined according to fields that are contained in the first request of a specific protocol, e.g. capabilities exchange in Diameter.</p> <p>Fine-grained policy control can be applied for routing by performing deep inspection of the messages for specific values.</p> <p>SDC provides a multi-level security features:</p> <ul style="list-style-type: none"><li>• Diameter topology hiding</li><li>• Diameter connection security</li><li>• Diameter message security</li><li>• OS/System security</li><li>• Network Level Security</li></ul> <p>Security Management includes access rights management, communication links protection and management operation logging.</p>	Basic
Roaming Interworking Function (IWF)	Support for interoperability and routing functions to manage Diameter and SS7/MAP signaling between	Add-on



Feature	Description	License Type
support between Diameter and SS7	visited, home and roaming hub/IPX providers based on 3GPP TS29.305 specifications.	
Enhanced EMS system	Enhancement to the EMS system that will include Centralized Configuration and Administration that allows managing multiple SDC clusters in geo-redundant deployments and Centralized Performance/Fault management.	Add-on
Extract information for Control Plane Analytic system	The feature enables extracting information from the control plane and provides analysis based on specific AVPs in protocol. The analysis will be performed by a tool that will collect the information and will provide the capability to analyze it in different views (e.g. per subscriber, per network entity, per location, etc.)	Basic
Diameter Identity	By default, SDC works as a Relay Agent in the Diameter network. As such, it does not manipulate AVPs. With the Diameter Identity feature, each routing rule can define the SDC as either a Relay or a Proxy Agent. Origin-Host and Origin-Realm AVPs can be manipulated and each Peer Profile can have a specific Origin-Host and Origin-Realm value.	Basic
TDR Reports	<p>TDR (Transaction Data Record) information, defined per routing rule, is sent to EMS, and can be viewed in the EMS Dashboard and Report views.</p> <p>The EMS Dashboard tab displays TDR information of five types: the number of messages, response time, ok responses, timeout events and error responses. The Reports tab details the transaction information, which can be filtered.</p>	Basic



Feature	Description	License Type
	<p>The reports are automatically generated every 30 minutes.</p>	
LDAP Authentication	<p>Lightweight Directory Access Protocol (LDAP) provides centralized authentication of users to a variety of services. SDC supports internal authentication and external authentication using LDAPv3.</p> <p>When a user logs in to SDC, SDC establishes a connection with the LDAP server and searches for the user in its database.</p> <p>Data transferred in LDAP may be encrypted using TLS or SSL encryption method (TLS is the recommended method).</p> <p>Based on a global timeout, SDC caches the user name and its privileges until the session expires. When LDAP authentication is enabled internal authentication is disabled, therefore it is recommended to use a secondary LDAP server for backup.</p>	Basic
Global Properties	<p>AVPs (Attribute Value Properties) can be centrally defined and used, in the global level (EMS) or per site, in various SDC objects such as Peer Profile, Peers and Pools. The properties can be set using the WebUI, API, or via scripting.</p>	Basic
Health Check	<p>Peer health monitoring indicates the health status of each remote peer. The health status is calculated based on different indications of the peer availability based on user-defined parameters defined per peer</p>	Basic



Feature	Description	License Type
	profile. The peer health is presented to the user in the Remote Peers screen with one of three possible icons – green, yellow, or red – representing the different peer health states. Each Pool health status reflects the total health status of its Peers.	
LBO (Local Break Out)	To facilitate EU regulation III that will be in effect from July 2014, the SDC's Diameter peer profiles can be configured with a list of recognized APNs and PLMNs. When enabled, the SDC's Local Break Out feature runs the APN of a received ULR message against the list of supported APNs, and if it appears, continues to check if the message origin-realm is in the list of supported PLMNs. Once it is confirmed that the ULR message's APN and PLMN are supported, a flag is raised on the message and a connection (Local Break Out) can be established with the VPLMN.  This feature is available both for Diameter and SS7.	Basic
Web Service API Authentication	In order to perform any change in the Web Service API one is required to authenticate as an "Expert" user (or any level higher than "Expert").	Basic
Accessibility	The Web UI's color palette was aligned with the accessibility standard. In addition, an option to navigate through the Web UI using the keyboard was added.	Basic
CLI Application	The CLI tool allows monitoring of all peers and pools in the EMS deployment. Adding a peer to a pool, as well as enabling and disabling peers, is possible using the CLI tool.	Basic
Dual IPv4 and IPv6 support	The SDC monitors the "extPdpType" parameter which was introduced in 2G/3G for parallel "dual	Add-on



Feature	Description	License Type
	<p>stack” - allowing both IPv4 and IPv6 usage. The SDC tracks this parameter per message and modifies based on the message destination.</p> <p>This feature is available both for Diameter and sSS7.</p>	



## Glossary

The following table lists the terms and abbreviations used in this document.

**Table 3: Terms and Abbreviations**

Term	Definition
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AF	Application Function
Answer	A message sent from one Client/Server Peer to the other following a request message
API	Application Programming Interface
AVP	Attribute Value Pair
CLI	Command Line Interface
Client Peer	A physical or virtual addressable entity which consumes AAA services
CPF	Control Plane Function
Data Dictionary	Defines the format of a protocol's message and its validation parameters: structure, number of fields, data format, etc.
DEA	Diameter Edge Agent
Destination Peer	The Client/Server peer to which the message is sent
DRA	Diameter Routing Agent
EMS Site	Element Management System Site
FEP-In	In-Front End Proxy
FEP-Out	Out-Front End Proxy
Geo Redundancy	A mode of operation in which more than one geographical location is used in case one site fails



Term	Definition
HA	High Availability
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IMS	IP Multimedia Subsystem
JMS	Java Message Service
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
Master Session	The session for which the routing selection is performed based on the routing rules (Slave Sessions are applied with routing rules inherited from the Master Session)
MME	Mobility Management Entity
NGN	Next Generation Networking
Node	Physical or virtual addressable entity
OAM	Operation, Administration and Maintenance
OCS	Online Charging System
Origin Peer	The peer from which the message is received
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PLMN	Public Land Mobile Network
Pool	A group of Server Peers
RADIUS	Remote Authentication Dial In User Service
Request	A message sent from one Client/Server peer to the other, followed by an answer message





Term	Definition
SCCP	Signaling Connection Control Part
SCTP	Stream Control Transmission Protocol
SDC	Signaling Delivery Controller
SDC Site	The entire list of entities working in a single site
Server Peer	A physical or virtual addressable entity which provides AAA services
Session	An interactive information interchange between entities
Slave (Bound) Session	<a href="#">A session which inherits properties from a master session</a>
SNMP	Simple Network Management Protocol
SS7	Signaling System No. 7
TCP	Transmission Control Protocol
TLS	Transport Layer Security
Transaction	A request message followed by an answer message
Tripo	Session data repository
UDP	User Datagram Protocol
UE	User Equipment
URI	Universal Resource Identification.
Virtual Server	<a href="#">A binding point</a> used by SDC to communicate with the Remote Peers (Clients and Servers)
VPLMN	Visited Public Land Mobile Network
Web UI	Web User Interface
WS	Web Service