Signaling Delivery Controller

Installation Guide

4.4

Catalog Number: RG-015-44-21 Ver. 3

Publication Date: June 2015

Proprietary and Confidential Information of F5 Networks

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* or contact us at *Tfx_info@f5.com*.

About this Document

Document Name: F5 Signaling Delivery Controller Installation Guide

Catalog Number: RG-015-44-21 Ver. 3

Publication Date: June 2015

Document Objectives

This document describes the installation process using the FS SDC Installation Utility. This document describes the installation process for both SDC and EMS sites.

Document History

Revision Number	Change Description	Change Location
May 2015 – 2	Updated Splunk license procedure	*Installing the Splunk License*
June 2015 – 3	Updated note in configure cluster table, updated Legal Information	*Configure Cluster*

Conventions

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

Table 1: Conventions

Convention	Use
Normal Text Bold	Names of menus, commands, buttons, user-initiated CLI commands and other elements of the user interface
Normal Text Italic	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

Proprietary and Confidential Information of F5 Networks

Convention	Use
 Warning:	Warnings which indicate potentially damaging user operations and explain how to avoid them

Proprietary and Confidential Information of F5 Networks

Table of Contents

1. Introduction 1
1.1 What are the Installation Steps? 1
1.1.1 Completing a site survey 1
1.1.2 Installing the Hardware 2
1.1.3 Installing the Installer Server 2
1.1.4 Setting up the Site Servers 2
1.1.5 Creating and Editing the Site Configuration File 2
1.1.6 Installing the SDC or EMS site 3
1.1.7 Performing Post-Installation Tasks 3
1.2 General Prerequisites 3
2. Installing the Installation Utility 4
2.1 Prerequisites 4
2.2 Installing the Installation Utility 4
3. Setting Up the Site Servers 7
4. Creating and Editing the Site Configuration File 9
4.1 Prerequisites 9
4.2 Creating an SDC Site Configuration File 9
4.2.1 Accessing the Installation Utility to Create an SDC Site Configuration File 9
4.2.2 Defining Servers and Ports 10
4.2.3 Define Bonds 12
4.2.4 Configure Networks 14
4.2.5 Configure Cluster 16
4.2.6 Configure Routes 19
4.2.7 Defining the Site Default Gateway 21
4.2.8 Configure Servers 21
4.2.9 Configure Properties 22
4.3 Creating an EMS Site Configuration File 26
4.3.1 Accessing the Installation Utility to Create an EMS Site Configuration File 26
4.3.2 Defining Servers and Ports 26
4.3.3 Define Bonds 29
4.3.4 Configure Networks 30
4.3.5 Configure Cluster 32
4.3.6 Configure Routes 34
4.3.7 Defining the Site Default Gateway 35
4.3.8 Configure Servers 36
4.3.9 Configure Properties 36
4.4 Editing an SDC or EMS Site Configuration File 38
4.4.1 Accessing the Installation Utility to Edit an SDC or EMS Site Configuration File 38
4.4.2 Selecting a Site Configuration File 39
4.4.2.1 Load site configuration file from the installation server 39
4.4.2.2 Upload site configuration file 39
4.4.3 Modifying the Site Configuration File 39
5. Performing the Installation 41
5.1 Accessing the Installation Utility to Perform an Upgrade 41
5.2 Selecting a Site Configuration File 41
5.2.1 Load site configuration file from the installation server 41

 Proprietary and Confidential Information of F5 Networks

5.2.2 Upload site configuration file 41
5.3 Selecting the Installation Type 42
5.4 Viewing the Installation Steps 42
5.5 Defining the Operating System 44
5.6 Confirming the Installation Setup 44
5.7 Monitoring the Installation Progression 44
5.8 Performing Post-Installation Procedures 45
5.9 Switching on the Site Servers 45
6. Post Installation Procedures 46
6.1 Changing the Root Password 46
6.2 Changing the SNMP Community String 46
6.3 Installing the Splunk License 46
6.4 Activating and Installing the SS7 License 50
6.5 Enabling SS7 Driver Redundancy 51
6.6 Enabling Tripo Site Replication 55
6.7 Enabling Keyboard Navigation in the Web UI (Accessibility) 57
A. Appendix A: Working with the Installation Utility 60
Performing common procedures in the Installation Utility 60
Navigating between screens 60
Adding elements 61
Modifying configured elements 62
Deleting elements 62
Saving changes 62
Switching between procedures 62
B. Appendix B: Common Cluster Configurations 63
Cluster Configuration for an SDC site 63
Cluster Configuration for an EMS site 64
C. Glossary 66

List of Figures

Figure 1: Edit Existing Configurations>Configure Network Screen 60
Figure 2: SDC Site Cluster Configuration 64
Figure 3: EMS Site Cluster Configuration 65

List of Tables

Table 1: Conventions II
Table 2: Servers Table Parameters 10
Table 3: Physical Ports Table Parameters 12
Table 4: Bonds Table Parameters 13
Table 5: Configure Network Parameters 14
Table 6: SDC Components 17
Table 7: Cluster Table Parameters 18

 Proprietary and Confidential Information of F5 Networks

Table 8: Configure Routes Table Parameters 20
Table 9: Configure Servers Table Parameters..... 21
Table 10: Configure Site Properties Table Parameters..... 22
Table 11: Servers Table Parameters 27
Table 12: Physical Ports Table Parameters..... 28
Table 13: Bonds Table Parameters 29
Table 14: Configure Network Parameters 31
Table 15: EMS site components..... 33
Table 16: Cluster Table Parameters..... 33
Table 17: Configure Routes Table Parameter..... 35
Table 18: Configure Servers Table Parameters..... 36
Table 19: Configure Site Properties Table Parameters..... 37
Table 20: Installation Steps..... 42
Table 21: Terms and Abbreviations 66

Proprietary and Confidential Information of F5 Networks

1. Introduction

The installation process installs, configures, and enables the necessary hardware, network infrastructure, and site components needed to process the expected variants of message types and traffic load.

The installation process is performed using the F5® Traffix® SDC® Installation Utility. This utility is used both to create and edit the site configuration file and perform the site installation.

1.1 What are the Installation Steps?

Installing an SDC or EMS site includes the following steps, elaborated in the following chapters of this guide:

- Completing a site survey
- Installing the Hardware
- Installing the Installer Server
- Setting up the Site Servers
- Creating and Editing the Site Configuration File
- Installing the SDC or EMS site
- Performing Post-Installation Tasks

1.1.1 Completing a site survey

To correctly assess your specific needs and ensure that the installed solution will meet them, a site survey, reviewing your anticipated traffic type and scope, is completed. Based on the site survey, a solution is built and the hardware requirements and site configuration recommendations are decided upon.

 Note: This document assumes that this stage has been successfully completed.

Proprietary and Confidential Information of F5 Networks

1.1.2 Installing the Hardware

Before accessing the installation utility, setting the site configuration, and performing the software installation, install (and verify the successful installation) of the required hardware, per the recommendations decided upon based on the site survey.

Note: This document assumes that this stage has been successfully completed.

1.1.3 Installing the Installer Server

Using the ISO file, the site server that will be used as the Installer Server is installed with an Operating System and the Installation Utility.

Note: The site configuration file must configure a second server in the site with the "installer" role. Once the site is installed, this second server will act as a backup server, and will take on the role of installation server if the primary installation server malfunctions.

1.1.4 Setting up the Site Servers

Once the installer server is successfully installed, the remaining site servers must be set up with the Operating System running on the installer server. Once the OS is successfully installed, the installation IP on each site server must be modified to ensure communication between the site server and the installer server.

1.1.5 Creating and Editing the Site Configuration File

Using the installation utility, the site configuration file is created and/or edited. The site configuration file defines the site's infrastructure – the hardware that the site uses, which networks are used and their communication paths (both within the SDC site and with external networks), and the SDC components needed to process the expected traffic.

Note: Each time after a site configuration file is edited, you must perform an installation so that the edited changes take effect.

Proprietary and Confidential Information of F5 Networks

1.1.6 Installing the SDC or EMS site

Using the Installation Utility, the SDC or EMS site is installed after both the hardware requirements have been met and the site configuration file has been successfully created and edited (if needed).

For more information about performing the installation, see *Performing the Installation.*

1.1.7 Performing Post-Installation Tasks

After successfully performing the installation using the Installation Utility, there are various post-installation tasks that may need to be performed. For more information about these tasks and their corresponding procedures, see *Post Installation Procedures*.

1.2 General Prerequisites

This document assumes that you have comprehensive understanding of:

- Positioning of the SDC in and/or between networks including the relevant IP and network (i.e. port) information needed for your site
- SDC and EMS deployments
- SDC architecture
- SDC pipeline

Proprietary and Confidential Information of F5 Networks

2. Installing the Installation Utility

The Installation Utility must be installed on at least one server per site. This server is the site's primary installation server, and by default, the installation utility will run on this server. In addition, at least one site server must be configured with the "installer" role. The installation utility will automatically be installed on this server during the site installation, but in standby mode. This server will act as a backup installer server. In the event that the primary installation server is down, this server will take over as the site's active installation server.

This section describes how to install the Installation Utility on the primary installation server, and includes the following topics:

- Prerequisites
- Installing the Installation Utility

2.1 Prerequisites

Before installing the Installation Utility, verify that you have:

- The bootable media with the installation files
- The IP addresses of the machine that will run the Installation Utility.

2.2 Installing the Installation Utility

Note: Installing the Installation Utility takes approximately 35 minutes.

Note: The installation process of the Installation Utility includes the installation of an Operating System. When attempting to install the Installation Utility on a machine with an existing Operating System, the Operating System will be deleted and the Operating System on the bootable media will be installed instead. In addition, all previous data on the machine will be deleted. It is therefore recommended to back up all existing data before beginning the installation process.

Proprietary and Confidential Information of F5 Networks

To install the Installation Utility:

1. Insert the bootable media (either a USB or CD).
2. Reboot the machine.
3. Enter the machine BIOS and configure the machine to boot from the USB/CD.
4. Reboot the machine.
5. From the OS installation UI, select the Install Traffix F5 EL from cdrom option for the relevant server type (bare metal or vmware instance).

Note: This step usually takes about 25 minutes to complete.

---

6. Once the installation is finished, select any key to start rebooting the system.
   The Welcome to Red Hat Enterprise Linux screens is displayed.
7. Click **Reboot**.
8. After rebooting is completed, log in to the server console using your login and password.

Note: The default values for login and password are “root” and “traffix”, respectively.

---

9. Type **menu** in the console to bring up the service menu.
   The F5 Traffix service menu is displayed.
10. Select **2) Network Management**, and then select **2) Management interface configuration (DHCP & Cobbler)**.
    The Traffix SDC System Setup Wizard appears.
11. Configure the following parameters according to your network topology:
    a. Interface
    b. **Hostname** of the installer machine
    c. **IP address** of the installation utility machine

d. Netmask IP address

e. **Default gateway** of the machine.

f. **DHCP first and last address** of the network configuration.

12. After confirming that the information is correct, type **y**.

Note: If the information is not correct, type **n**, and then reenter the corrected information.

The system reconfigures the services to match the parameter settings.

13. Select any key to reboot the system.

The machine is installed with the Operating System and the installation utility.

The processes below are configured on the installer server, and run on the network that was defined to be used for communication between the installer server and the remaining site servers:

- The Installation Utility component runs on port 9090.
- The Cobbler (SDC Repository) runs on port 9090.
- The DHCP runs on port 67/68.

3. Setting Up the Site Servers

This section describes how to set up the servers in your site that are not used as the primary Installation Server (configured in the previous section). Server setup includes installing the Operating System and modifying the installation IP to ensure communication between the site servers and the Installation Server.

To install the Operating System on the site servers:

1. On the installer server, start the DHCP and HTTPD daemon services by running the following commands:

Note: It is important to verify that additional DHCPs do not exist in the Management Network so to avoid DHCP collisions.

---

service dhcpd start

service httpd start

2. Perform the following steps for each remaining site server:

   a. Start up the server and boot it using PXE.

   b. From the setup UI, select the OS option for the relevant server type (blade or VM).

3. After the OS is successfully installed, perform the following steps on each remaining site server to modify the installation IP:

Note: The login credentials on all site servers are the same as the credentials used on the installation server.

---

   a. Type **menu** in the console to bring up the service menu.

   The F5 Traffix service menu is displayed.

   b. Select 2) Network Management, and then select 3) Configure additional interfaces.

Proprietary and Confidential Information of F5 Networks

c. Configure the following parameters according to your network topology:

i. Interface

ii. IP address – the installer IP address defined for the server, based on your site survey.

iii. Netmask IP address

iv. Default gateway of the server

d. Confirm that the information is correct, and type **y**.

 Note: If the information is not correct, type **n**, and then reenter the corrected information.

The system reconfigures the services to match the parameter settings.

Proprietary and Confidential Information of F5 Networks

4. Creating and Editing the Site Configuration File

This section describes how to use the Installation Utility to create and edit site configuration files for an SDC or EMS site, and includes the following topics:

- Prerequisites
- Creating an SDC Site Configuration File
- Creating an EMS Site Configuration File
- Editing an SDC or EMS Site Configuration File

4.1 Prerequisites

Before creating or editing a site configuration file, verify that:

- The hardware requirements for the site are understood and fulfilled.
- The Installation Utility has successfully been installed on one of the site servers. For more information, see *Installing the Installation Utility*
- All additional site servers have successfully been set up. For more information, see *Setting Up the Site Servers*

4.2 Creating an SDC Site Configuration File

Use the Installation Utility to create the configuration file for your SDC site. This section describes the different steps included in the Installation Utility's "Create New Configuration" wizard and what aspect of the site configuration file is created in each step. After each step overview, the parameters in the step screen are detailed.

4.2.1 Accessing the Installation Utility to Create an SDC Site Configuration File

To access the installation utility:

1. In the Installation Utility home page, click **Create New Configuration**.

   The **Define Servers** screen appears.

Proprietary and Confidential Information of F5 Networks

4.2.2 Defining Servers and Ports

In the Define Servers screen you create the base for your configuration file, by defining the hardware that the site will be installed on, and the ports available on the hardware. You also configure the communication path between the installer server and the site servers, and provide authentication details (username and password) to verify that the installer server will be able to access the site servers and install the site configuration as we are about to define it. The screen is also used to define the SDC components that are enabled for each server.

This screen contains two tables – the Servers table and the Physical Ports table. Using the Servers table, define the SDC site server names and provide details about the server's hardware. Once a server is selected in the Servers table, the Physical Ports table displays the physical ports associated with the selected server.

For information about the Servers table parameters for SDC sites, see *Table 2*.

For more information about the Physical Ports table parameters, see *Table 3*.

Table 2: Servers Table Parameters

Parameter	Description	Guidelines
Hostname	The name of the server.	This value is user-defined.  Note: This value cannot contain a period (".") character.
Installation IP	The server's IP address, used by the installation utility to connect to the server.	This IP address should be part of the management network.
Location	The physical location of the server.	
Serial Number	The blade's serial number.	
Admin Status	Indicates if the server is going to be installed as part of the installation.	Select or clear the "Enabled" checkbox. After the checkbox is cleared, the text will change to "Disabled".

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
		Note: If defined as "Disabled", the server will not be installed.
HW	The type of hardware that the server is on.	Select the correct value from the drop-down list. The possible values are: HP-Blade
OS	The Operating System running on the hardware that the server is on.	Select the correct value from the drop-down list, according to the installation type.
Roles	The SDC components that may be run on the server. The available components include: ▪ CPF ▪ Config_Mgr ▪ WebUI ▪ Fep ▪ SplunkForwarder ▪ Nmsagent ▪ SS7 ▪ Tripo ▪ Installer ▪ Peer_Server ▪ Peer_Client ▪ Fileserver	Select all applicable options from the drop-down list. *Note: Verify that one of the site servers (aside for the server that was already installed with the Installation Utility) is defined with the Installer role. This site server will act as a secondary installer, and will take on the role of the installer only when the server with the Installation Utility is not functioning.* *Note: This enables the server to take on the defined roles, but does not enable any role.*
User Name	The user name that the installer will use to connect to the server.	Default: root
Password	The password that the installer will use to connect to the server.	Default: traffix

Proprietary and Confidential Information of F5 Networks

Table 3: Physical Ports Table Parameters

Parameter	Description	Guidelines
Slot	The NIC card ID.	Valid only when the server is located on a bladecenter.
Port	The port ID on the NIC.	Valid only when the server is located on a bladecenter.
MAC Address	The port's physical MAC address. This is unique for each port.	
Port Alias	The port alias. Each Operating System can independently define the port alias. Manually defining the port alias on the BIOS (using the UI) level overrides the OS definition, helping maintain a constant alias for each port, no matter the hardware and OS it is located on. This ensures consistent routing for the port.	Select the desired value (Eth0 to Eth<*number_of_ports*>) from the drop-down list.
Port Name	The name of the port.	

4.2.3 Define Bonds

In this screen, you configure bonds between network interfaces, and define the bond mode.

In the coming screens, you will define the networks that the SDC site will use to both run the SDC components on and also provide communication paths within the SDC site and between the SDC site and external networks. Each network will be configured to use a network interface. Creating a bond between two interfaces (defined in the previous screen), defining them as one new interface, can achieve one of two possible performance enhancements:

- Increased capacity – when two interfaces are defined in an active/active bond, the individual port's capacity is doubled, creating a new interface with double the capacity.

Proprietary and Confidential Information of F5 Networks

- Redundancy – when two interfaces are defined in an active/standby bond – the standby bond is available to take over in case the active bond experiences failure, ensuring continuous performance.

For more information about the Bonds table parameters, see *Table 4*.

Table 4: Bonds Table Parameters

Parameter	Description	Guidelines
Description	The reason for the bond. This is used for maintenance purposes only.	
Bond	The name of the bond.	
Interfaces	The interfaces defined as part of the bond. A bond typically uses two interfaces.	 *Note: Each interface can be assigned to one bond only.*
Mode	The bond mode, used to define the state of the bonded interfaces – Active/Active, to increase capacity, or Active/Standby, to provide redundancy.	Select the desired mode from the drop-down list: For HP servers: Active/Standby. For IBM servers: Active/Active for the IC. For VMware servers: Active/Standby.
Monitoring Cycle Recurrence (Millis)	The interval between health monitoring cycle start times. (In milliseconds)	Recommended value: 100.
Primary Interface	The primary interface used by the bond. In active/standby mode, this interface will be defined as active.	
Tests per Cycle	The number of tests performed in each health monitoring cycle. If the defined number of tests result in failure, the ports changeover and the standby interface takes over.	Recommended value: 10.
Status	Indicates if the bond is going to be installed as part of the installation.	Select or clear the “Enabled” checkbox. After the checkbox is

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
		cleared, the text will change to "Disabled". *Note: If defined as "Disabled", the bond will not be installed.*

4.2.4 Configure Networks

In the coming screens, we are going to configure the SDC components that will run on each SDC site server, and the communication paths between the SDC components and between the SDC site and external networks. In this screen, we configure the networks that the communication paths are going to run on.

The networks needed to ensure proper SDC site activity are:

- Management networks – this network connects the internal SDC components with customer-facing applications.
- Interconnect networks – this internal network connects between all internal SDC components.
- Signaling networks – the network connects the SDC's FEP components with the external networks.

For more information about the Networks table parameters, see *Table 5*.

Table 5: Configure Network Parameters

Parameter	Description	Guidelines
Roles	The SDC components that the network can communicate with. The available components include: ▪ cpf ▪ config_mgr ▪ webui	Select all applicable options from the drop-down list.

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
	▪ fep ▪ splunk ▪ splunkforwarder ▪ splunkmaster ▪ splunksearch ▪ nmsagent ▪ GRDMaster ▪ GRDClient ▪ ss7 ▪ tripo ▪ installer ▪ peer_server ▪ peer_client ▪ fileserver	
Name	The name of the network.	
IPv4 IP Address	The network address.	
IPv4 Net-Mask	The network subnet – the range of IP addresses that belong to the network.	
IPv4 Offset	The number of IP addresses automatically reserved by the network.	*Note: This will be seen in the IPv4 field in the Configuring Servers. The addresses will be completed automatically based on the inserted value.*
IPv6 IP Address	The network IP address.	
IPv6 Net-Mask	The network subnet – the range of IP addresses that belong to the network.	

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
IPv6 Offset	The number of IP addresses automatically reserved by the network.	*Note: This will be seen in the IPv6 field in the Configuring Servers. The addresses will be completed automatically based on the inserted value.*
Local/Remote	Is it a local network - defined on-site - enabling servers to connect to it locally, or do the servers connect to it remotely.	*Note: IP routing must be defined for remote networks.*
VLAN TAG	Defines the VLAN-aware partitioning of the network. This is used to divide a physical port into logical ports.	*Note: Only for local networks.*

4.2.5 Configure Cluster

In the Configure Cluster screen you define which SDC components will run on the SDC site servers, and how each component will run. The SDC components can either be configured as independent **cluster clones** and **group clones**, or as **cluster groups** that contain one or more **cluster resources**.

An independent **cluster clone** is an SDC component that is configured to actively run concurrently on multiple SDC site servers. Cluster clones are configured as applications, running directly on the specified servers. **Group clones** contain two or more **cluster resources** that actively run concurrently on multiple SDC site servers.

A **cluster group** is a group of two or more **cluster resources** that work together to run SDC components. In each cluster group there is at least one cluster resource defined as a VIP. This cluster resource can be run on any one of the specified servers at a time. The cluster resources defined as applications (APPs) belonging to that cluster group will run on the VIP, on the server selected by the VIP. In the event that the server crashes, the VIP will automatically configure itself on the second server, and the APP will continue running on the VIP on the new server.

Proprietary and Confidential Information of F5 Networks

Table 6 specifies the SDC components, the resource type they should be configured as, the network that should run the component (for cluster groups only), and the networks that need to communicate with the component.

Table 6: SDC Components

SDC Component	Cluster Resource Type	Run on Network	Connect to Network(s)
CPF	Cluster Clone		Interconnect
Config manager	Cluster Clone		Interconnect, Management
WebUI	Cluster Group	Management	Interconnect, Management
FEP-TCP-I	Cluster Group	Signaling	Interconnect, Signaling
FEP-TCP-O	Cluster Group	Signaling	Interconnect, Signaling
FEP-SCTP-I	Cluster Group	Signaling	Interconnect, Signaling  *Note: FEPs can only be defined with SCTP in the SDC or EMS Web UI, when configuring the SDC Components. Define the FEP with TCP, and edit the SDC Component after installation, using the Web UI. For more information see the F5 SDC User Guide.*
FEP-SCTP-O	Cluster Group	Signaling	Interconnect, Signaling
SS7	Cluster Group  *Note: The SS7 cluster group is automatically generated by the Installer when the SS7 role is defined in a site and a CPF SDC*		

Proprietary and Confidential Information of F5 Networks

SDC Component	Cluster Resource Type	Run on Network	Connect to Network(s)
	Component is configured for the site.		
Tripo	Cluster Clone		Interconnect
NMS Agent	Cluster Group	Management	Interconnect, Management
Splunk Forwarder	Cluster Group	Interconnect	Interconnect, Management

For more information about the Cluster table parameters, see *Table 7*.

Table 7: Cluster Table Parameters

Parameter	Description	Guidelines
Name	The name and type of the SDC component.	Values: Cluster Group: A group of at least two cluster resources (one VIP resource and one APP resource). Cluster Resource: A component of a cluster group. Can be either a VIP resource or an APP resource. Cluster Clone: An SDC component running simultaneously and directly on the specified site servers. Must only be defined as an APP type resource.
Resource Type	The type of cluster resource.	Values: App: An SDC component that can run directly on a server or on a VIP. VIP: The base for an SDC APP resource to run on.
Value	This field displays the value based on the selected resource type.	Values: For App: displays the role that the application fulfills.

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
		For VIP: displays the virtual IP address.
Instance	Define a name for the configured SDC component.	*Note: All FEPs must be given an instance name.* *Note: Instance names should be unique for repeated resources.*
Location	The servers that the SDC component can run on. For cluster clones and cluster clone groups, the SDC component will always run on all specified servers. For cluster groups and cluster resources, the SDC component will run on one of the specified servers until a failover is needed.	
Status	Indicates if the cluster item is going to be installed as part of the installation.	Select or clear the "Enabled" checkbox. After the checkbox is cleared, the text will change to "Disabled". *Note: If defined as "Disabled", the group will not be installed.*

4.2.6 Configure Routes

The Configure Routes screen displays the external (non-SDC) networks that the SDC is going to communicate with and the route that the SDC will use to communicate with these networks.

There are two types of routing – static routing and fep-specific routing.

Static routing is the term used to describe routing that is per server, without differentiating between the different FEPs installed on the site. When only static routing is configured, all messages from the server are routed to the same (external) destination network.

Fep-specific routing is routing that is configured individually for each FEP installed on the site. Each FEP is configured to communicate with a specific (external) destination network.

Proprietary and Confidential Information of F5 Networks

Both routing options are configured with a gateway address, to ensure access into the destination network. Fep-specific routing includes the option to also define a customized source address for the messages sent to the destination network. Messages configured using static routing will be sent with the default site address as the source address.

Note: If static and fep-specific routing are both configured, only FEPs without specific routing will be configured according to the static routing.

If static routing is not configured, only FEPs configured with Fep-specific routing will communicate with the destination network (as specified in the routing table).

For more information about the Routes table parameters, see *Table 8*.

Table 8: Configure Routes Table Parameters

Parameter	Description	Guidelines
Routing Definition	Defines the FEP that the routing is configured for: **Static** – messages from all FEPs are routed according to this rule. *Note: Only messages from FEPs that do not have a fep-specific route defined for them are routed.* <***fep_name***> - messages from this FEP only are routed according to this rule.	Value: Generic FEP component or a protocol-based FEP, chosen from a drop-down list. *Note: Static routing will be applied if a generic FEP is selected, while dynamic routing – applied only when the FEP is running – will be applied if a protocol-based FEP is selected.*
Destination Network	The (external) network node that receives the message.	Value: Network node, chosen from a drop-down list.
Gateway	The SDC site's gateway address, used to access the destination node.	Value: An IP address that is part of the appropriate signaling network.
Preferred Source Address	The IP address that the destination network will see as the source IP address.	Value: When you have IPs for both the remote network and the FEP instance, it's recommended to define the preferred source

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
		address as the FEP IP, as it is defined in the Cluster table.

4.2.7 Defining the Site Default Gateway

This gateway is used to connect the host network to the destination network.

To edit/define the default gateway:

1. Click the **Site Default Gateway** field and enter the IP address.

4.2.8 Configure Servers

Earlier, you defined the networks used by the SDC site and the SDC components. In the Configure Servers screen, you configure the communication paths between the servers and the networks, by defining the SDC site server network interfaces and IP addresses that each network must use to connect to each server.

For more information about the Servers table parameters, see *Table 9*.

Table 9: Configure Servers Table Parameters

Parameter	Description	Guidelines
Network	The name of the network that the server uses.	
VLAN TAG	The VLAN-aware partitioning of the network. This is used to divide a physical port into logical ports.	
Interface	The name of the interface that the network uses to communicate with the server.	Select the desired value from the drop-down list.
IPv4	The server's IP address in the network.	
IPv6	The server's IP address in the network	

Proprietary and Confidential Information of F5 Networks

4.2.9 Configure Properties

In this screen you configure the internal communication paths between SDC components and general configuration paths between external network peers sending information toward an SDC site. You can also use this screen to verify system properties.

For more information about the site properties table parameters, see *Table 10*.

Table 10: Configure Site Properties Table Parameters

Parameter	Description	Guidelines
System		
SDCVersion	The name of the package as it appears in the Installer repository	For tar.gz files, enter the .tar file name. For .rpm files, enter the version number (for example 4.4-271)
Corosync_backup_net	The backup network used by Corosync.	
isMultiSiteEnv	Is the site an EMS site, or an SDC site managed by an EMS?	Select true/false from the drop-down list. When “true”, the relevant EMS and SDC sites will be connected as part of the installation.
Site_ID	The name of the site	
timezone	The time zone the system is configured to work in	Select the relevant time zone from the drop-down list.
ntpServers	The servers used to synchronize time zones between servers	
Corosync Port	The port used by Corosync to listen to the SDC. This is used for communication between the site servers.	Value: Enter a unique value.
InstallerIp	The IP address of the installer server that the SDC connects to	

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
EmsNmsServer	The address of the NMS instance on the EMS.	
EmsServer1	The address of the Splunk Master instance on the first EMS site server.	
EmsServer2	The address of the Splunk Master instance on the second EMS site server.	
Configuration Manager		
CM_MGT_VIP	An IP address in the SDC site management network.	
CM_IC_VIP	An IP address in the SDC site interconnect network.	
EMS_MGMT_VIP	The VIP address of the EMS Configuration Manager	
Fileserver		
fileServerProductUser		
FileServerVersion		
Installer		
Network	The network that is used for communication between the installation server and the site servers	
Start DHCP	The lower end of the range of IP addresses that can be installed using PXE.	
End DHCP	The upper end of the range of IP addresses that can be installed using PXE.	

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
SS7		
ISccpMode	Enables the SCCP mode	Enter True if your SS7 implementation is going to be used for LBO or Dual Stack. Enter False, if your SS7 implementation is going to be used for IWF or Wifi-Offload.
STP1IP1	The primary IP address defined for STP1	This parameter is configured for both SCCP modes.
STP1IP2	The secondary IP address defined for STP1	This parameter is configured for both SCCP modes.
STP1Port	The STP1 port used by the SS7 driver	This parameter is configured for both SCCP modes.
STP1PC	The point code defined for STP1	This parameter is configured for both SCCP modes.
STP2IP1	The primary IP address defined for STP2	This parameter is configured for both SCCP modes.
STP2IP2	The secondary IP address defined for STP2	This parameter is configured for both SCCP modes.
STP2Port	The STP2 port used by the SS7 driver	This parameter is configured for both SCCP modes.
STP2PC	The point code defined for STP2	This parameter is configured for both SCCP modes.
CPF1PC	The first point code defined for the SS7 driver that is used by CPF.	This parameter is configured for both SCCP modes.  *Note: This parameter is the Originating Point Code for RSI. When RSI is enabled, this value must match the value defined for CPF2PC. When RSI is disabled, this value must be*

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
		different to the value defined for CPF2PC.
CPF2PC	The second point code defined for the SS7 driver that is used by CPF.	This parameter is configured for both SCCP modes.  *Note: This parameter is the Originating Point Code for RSI. When RSI is enabled, this value must match the value defined for CPF1PC. When RSI is disabled, this value must be different to the value defined for CPF1PC.*
RoutingContext1	The routing context that defines a routing key of defined SS7 parameters	Enter a unique value
RoutingContext2	The routing context that defines a routing key of defined SS7 parameters	Enter a unique value
NA	The Network Appearance filed identifies the SS7 network context (i.e. SS7 Point Code) for a routing key	
NI	The Network Indicator field identifies the type of network, (national or international)	Enter 2 for a national network and 0 for an international network
iwfSgsnVirtualGtBase	the IWF Virtual GT prefix of a pool for the MME node (TCAP mode only)	The parameter is only applicable for when your SS7 implementation is going to be used for IWF.
Tripo		

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
TripoVersion	Tripo product version	The default is “latest.” It is recommended to enter the version saved in the topology file.
SecondSiteIP1	The IP address of the first Tripo instance on the second SDC server.	
SecondSiteIP2	The IP address of the second Tripo instance on the second SDC server.	

4.3 Creating an EMS Site Configuration File

Use the Installation Utility to create the configuration file for your EMS site. This section describes the different steps included in the Installation Utility’s “Create New Configuration” wizard and what aspect of the site configuration file is created in each step. After each step overview, the parameters in the step screen are detailed.

4.3.1 Accessing the Installation Utility to Create an EMS Site Configuration File

To access the installation utility:

1. In the Installation Utility home page, click **Create New Configuration**.

   The **Define Servers** screen appears.

4.3.2 Defining Servers and Ports

In this screen you create the base for your configuration file, by defining the hardware that the site will be installed on, and the ports available on the hardware. You also configure the communication path between the installer server and the site servers, and provide authentication details (username and password) to verify that the installer server will be able to access the site servers and install the site configuration as we are about to define it. The screen is also used to define the EMS site components that are enabled for each server.

Proprietary and Confidential Information of F5 Networks

This screen contains two tables – the Servers table and the Physical Ports table. Using the Servers table, define the EMS site server names and provide details about the server's hardware. Once a server is selected in the Servers table, the Physical Ports table displays the physical ports associated with the selected server.

For information about the Servers table parameters for EMS sites, see *Table 11*.

For more information about the Physical Ports table parameters, see *Table 12*.

Table 11: Servers Table Parameters

Parameter	Description	Guidelines
Hostname	The name of the server.	This value is user-defined.  *Note: This field cannot contain underscores.*
Installation IP	The server's IP address, used by the installation utility to connect to the server.	This IP address should be part of the management network.
Location	The physical location of the server.	
Serial Number	The blade's serial number.	
Admin Status	Indicates if the server is going to be installed as part of the installation.	Select or clear the "Enabled" checkbox. After the checkbox is cleared, the text will change to "Disabled".  *Note: If defined as "Disabled", the server will not be installed.*
HW	The type of hardware that the server is on.	Select the correct value from the drop-down list. The possible values are: HP-Blade
OS	The Operating System running on the hardware that the server is on.	Select the correct value from the drop-down list, according to the installation type.
Roles	The EMS site components that may be run on the server.	Select all applicable options from the drop-down list.

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
	The available components include: ▪ Config_Mgr ▪ WebUI ▪ Splunk ▪ SplunkForwarder ▪ SplunkMaster ▪ SplunkSearch ▪ Nmsagent ▪ Installer	*Note: Verify that one of the site servers (aside for the server that was already installed with the Installation Utility) is defined with the Installer role. This site server will act as a secondary installer, and will take on the role of the installer only when the server with the Installation Utility is not functioning.* *Note: This enables the server to take on the defined roles, but does not enable any role.*
User Name	The user name that the installer will use to connect to the server.	
Password	The password that the installer will use to connect to the server.	

Table 12: Physical Ports Table Parameters

Parameter	Description	Guidelines
Slot	The NIC card ID.	Valid only when the server is located on a bladecenter.
Port	The port ID on the NIC.	Valid only when the server is located on a bladecenter.
MAC Address	The port's physical MAC address. This is unique for each port.	
Port Alias	The port alias. Each Operating System can independently define the port alias. Manually defining the port alias on the BIOS (using the UI) level overrides the OS definition, helping maintain a constant alias for each port, no	Select the desired value (Eth0 to Eth<*number_of_ports*>) from the drop-down list.

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
	matter the hardware and OS it is located on. This ensures consistent routing for the port.	
Port Name	The name of the port.	

4.3.3 Define Bonds

In this screen, you configure bonds between network interfaces, and define the bond mode.

In the coming screens, you will define the networks that the EMS site will use to both run the EMS site components on and also provide communication paths within the EMS site and between the EMS site and external networks. Each network will be configured to use a network interface. Creating a bond between two interfaces (defined in the previous screen), defining them as one new interface, can achieve one of two possible performance enhancements:

- Increased capacity – when two interfaces are defined in an active/active bond, the individual port's capacity is doubled, creating a new interface with double the capacity.
- Redundancy – when two interfaces are defined in an active/standby bond – the standby bond is available to take over in case the active bond experiences failure, ensuring continuous performance.

For more information about the Bonds table parameters, see *Table 13*.

Table 13: Bonds Table Parameters

Parameter	Description	Guidelines
Description	The reason for the bond. This is used for maintenance purposes only.	
Bond	The name of the bond.	
Interfaces	The interfaces defined as part of the bond. A bond typically uses two interfaces.	*Note: Each interface can be assigned to one bond only.*

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
Mode	The bond mode, used to define the state of the bonded interfaces – Active/Active, to increase capacity, or Active/Standby, to provide redundancy.	Select the desired mode from the drop-down list: For HP servers: Active/Standby. For IBM servers: Active/Active for the IC. For VMware servers: Active/Standby.
Monitoring Cycle Recurrence (Millis)	The interval between health monitoring cycle start times. (In milliseconds)	Recommended value: 100.
Primary Interface	The primary interface used by the bond. In active/standby mode, this interface will be defined as active.	
Tests per Cycle	The number of tests performed in each health monitoring cycle. If the defined number of tests result in failure, the ports changeover and the standby interface takes over.	Recommended value: 10.
Status	Indicates if the bond is going to be installed as part of the installation.	Select or clear the "Enabled" checkbox. After the checkbox is cleared, the text will change to "Disabled".  *Note: If defined as "Disabled", the bond will not be installed.*

4.3.4 Configure Networks

In the coming screens, we are going to configure the EMS site components that will run on each EMS site server, and the communication paths between the EMS site components and between the EMS site and its managed EMS sites and external network elements. In this screen, we configure the networks that the communication paths are going to run on.

The networks needed to ensure proper EMS site activity are:

Proprietary and Confidential Information of F5 Networks

- Management networks – this network connects the internal EMS site components with customer-facing applications.
- Interconnect networks – this internal network connects between all internal EMS site components.

For more information about the Networks table parameters, see *Table 14*.

Table 14: Configure Network Parameters

Parameter	Description	Guidelines
Roles	The EMS site components that the network can communicate with.	
Name	The name of the network.	
IPv4 IP Address	The network address.	
IPv4 Net-Mask	The network subnet – the range of IP addresses that belong to the network.	
IPv4 Offset	The number of IP addresses automatically reserved by the network.	*Note: This will be seen in the IPv4 field in the Configuring Servers. The addresses will be completed automatically based on the inserted value.*
IPv6 IP Address	The network IP address.	
IPv6 Net-Mask	The network subnet – the range of IP addresses that belong to the network.	
IPv6 Offset	The number of IP addresses automatically reserved by the network.	*Note: This will be seen in the IPv6 field in the Configuring Servers. The addresses will be completed automatically based on the inserted value.*

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
Local/Remote	Is it a local network - defined on-site - enabling servers to connect to it locally, or do the servers connect to it remotely.	*Note: IP routing must be defined for remote networks.*
VLAN TAG	Defines the VLAN-aware partitioning of the network. This is used to divide a physical port into logical ports.	*Note: Only for local networks.*

4.3.5 Configure Cluster

In the Configure Cluster screen you define which EMS site components will run on the EMS site servers, and how each component will run. The EMS site components can either be configured as independent **cluster clones** and **group clones**, or as **cluster groups** that contain one or more **cluster resources**.

An independent **cluster clone** is an SDC component that is configured to actively run concurrently on multiple EMS site servers. Cluster clones are configured as applications, running directly on the specified servers. **Group clones** contain two or more **cluster resources** that actively run concurrently on multiple EMS site servers.

A **cluster group** is a group of two or more **cluster resources** that work together to run EMS site components. In each cluster group there is at least one cluster resource defined as a VIP. This cluster resource can be run on any one of the specified servers at a time. The cluster resources defined as applications (APPs) belonging to that cluster group will run on the VIP, on the server selected by the VIP. In the event that the server crashes, the VIP will automatically configure itself on the second server, and the APP will continue running on the VIP on the new server.

Table 15 specifies the EMS site components, the resource type they should be configured as, the network that should run the component (for cluster groups only), and the networks that need to communicate with the component.

Proprietary and Confidential Information of F5 Networks

Table 15: EMS site components

SDC Component	Cluster Resource Type	Run on Network	Connect to Network(s)
Config manager	Cluster Clone		Interconnect, Management
WebUI	Cluster Group	Management	Interconnect, Management
NMS Agent	Cluster Group	Management	Interconnect, Management
Splunk Forwarder	Cluster Group	Interconnect	Interconnect, Management
Splunk Indexer	Cluster Clone		Interconnect, Management
Splunk Master Node and Search Head	Cluster Group	Management	Interconnect, Management
NMS Manager	Cluster Group	Management	Interconnect, Management

For more information about the Cluster table parameters, see *Table 16*.

Table 16: Cluster Table Parameters

Parameter	Description	Guidelines
Name	The name and type of the SDC component.	Values: Cluster Group: A group of at least two cluster resources (one VIP resource and one APP resource). Cluster Resource: A component of a cluster group. Can be either a VIP resource or an APP resource. Cluster Clone: An SDC component running simultaneously and directly on the specified site servers. Must only be defined as an APP type resource.
Resource Type	The type of cluster resource.	Values:

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
		App: An SDC component that can run directly on a server or on a VIP. VIP: The base for an SDC APP resource to run on.
Value	This field displays the value based on the selected resource type.	Values: For App: displays the role that the application fulfills. For VIP: displays the virtual IP address. The network is defined based on the *Configure Network Parameters* table.
Instance	Define a name for the configured SDC component.	
Location	The servers that the SDC component can run on. For cluster clones and cluster clone groups, the SDC component will always run on all specified servers. For cluster groups and cluster resources, the SDC component will run on one of the specified servers until a failover is needed.	
Status	Indicates if the cluster item is going to be installed as part of the installation.	Select or clear the "Enabled" checkbox. After the checkbox is cleared, the text will change to "Disabled". *Note: If defined as "Disabled", the group will not be installed.*

4.3.6 Configure Routes

The Configure Routes screen displays the external (non-SDC) networks that the SDC is going to communicate with and the route that the SDC will use to communicate with these networks.

For EMS sites, there is one type of routing – static routing.

Proprietary and Confidential Information of F5 Networks

Static routing is configured with a gateway address, to ensure access into the destination network. Messages configured using static routing will be sent with the default site address as the source address.

For more information about the Routes table parameters, see *Table 17*.

Table 17: Configure Routes Table Parameter

Parameter	Description	Guidelines
Routing Definition	Defines the FEP that the routing is configured for: **Static** – messages from all FEPs are routed according to this rule. *Note: Only messages from FEPs that do not have a fep-specific route defined for them are routed.* <***fep_name***> - messages from this FEP only are routed according to this rule.	Value: Generic FEP component or a protocol-based FEP, chosen from a drop-down list. *Note: Static routing will be applied if a generic FEP is selected, while dynamic routing – applied only when the FEP is running – will be applied if a protocol-based FEP is selected.*
Destination Network	The (external) network node that receives the message.	Value: Network node, chosen from a drop-down list.
Gateway	The EMS site's gateway address, used to access the destination node.	Value: An IP address that is part of the appropriate signaling network.
	The IP address that the destination network will see as the source IP address.	Recommended value: When you have IPs for both the remote network and the FEP instance, it's recommended to define the preferred source address as the FEP IP, as it is defined in the Cluster table.

4.3.7 Defining the Site Default Gateway

This gateway is used to connect the host network to the destination network.

Proprietary and Confidential Information of F5 Networks

To edit/define the default gateway:

1. Click the **Site Default Gateway** field and enter the IP address.

4.3.8 Configure Servers

Earlier, you defined the networks used by the EMS site and the EMS site components. In the Configure Servers screen, you configure the communication paths between the servers and the networks, by defining the EMS site server network interfaces and IP addresses that each network must use to connect to each server.

For more information about the Servers table parameters, see *Table 18*.

Table 18: Configure Servers Table Parameters

Parameter	Description	Guidelines
Network	The name of the network that the server uses.	
VLAN TAG	The VLAN-aware partitioning of the network. This is used to divide a physical port into logical ports.	
Interface	The name of the interface that the network uses to communicate with the server.	Select the desired value from the drop-down list.
IPv4	The server's IP address in the network.	
IPv6	The server's IP address in the network	

4.3.9 Configure Properties

In this screen you configure the internal communication paths between EMS site components and general configuration paths between external network peers sending information toward an EMS site. You can also use this screen to verify system properties.

For more information about the site properties table parameters, see *Table 19*.

Proprietary and Confidential Information of F5 Networks

Table 19: Configure Site Properties Table Parameters

Parameter	Description	Guidelines
System		
SDCVersion	The name of the package as it appears in the Installer repository	For tar.gz files, enter the .tar file name. For .rpm files, enter the version number (for example 4.4-271)
Corosync_backup_net	The backup network used by Corosync.	
isMultiSiteEnv	Is the site part of EMS?	
Site_ID	The name of the site	
timezone	The time zone the system is configured to work in	
ntpServers	The servers used to synchronize time zones between servers	
Corosync Port	The corosync listening port used for communication between the site servers.	
InstallerIp	The IP address of the installer server that the SDC connects to	
EmsNmsServer	The address of the NMS instance on the EMS.	
EmsServer1	The address of the Splunk Master instance on the first EMS site server.	
EmsServer2	The address of the Splunk Master instance on the second EMS site server.	
Configuration Manager		

Proprietary and Confidential Information of F5 Networks

Parameter	Description	Guidelines
CM_MGT_VIP	An IP address in the EMS site management network.	
CM_IC_VIP	An IP address in the EMS site interconnect network.	
EMS_MGMT_VIP	The VIP address of the EMS Configuration Manager	
Installer		
Network	The network that is used for communication between the installation server and the site servers	
Start DHCP	The lower end of the range of IP addresses that can be installed using PXE.	
End DHCP	The upper end of the range of IP addresses that can be installed using PXE.	

4.4 Editing an SDC or EMS Site Configuration File

Use the "Edit Existing Configuration" wizard in the Installation Utility to edit an existing SDC or EMS site configuration file. This section describes how you access the wizard and select the relevant site configuration file. This section then directs you to the "Create New Configuration" wizard section, where you will find explanations of the remaining steps in the "Edit Existing Configuration" wizard.

4.4.1 Accessing the Installation Utility to Edit an SDC or EMS Site Configuration File

To access the installation utility:

1. In the Installation Utility home page, click **Edit Existing Configurations**.

Proprietary and Confidential Information of F5 Networks

The **Select Configuration** screen appears.

4.4.2 Selecting a Site Configuration File

Select the site configuration file by choosing the one of the following options:

4.4.2.1 Load site configuration file from the installation server

Choose this option if the file you want to work with is included in the default files included with the Installation Utility, or if the file has previously been uploaded to the Installer server.

To load a file from the installation server:

1. Select the desired file from the drop-down list.

4.4.2.2 Upload site configuration file

Choose this option if the file you want to work with is located locally (for example, on a USB or on the desktop) and has not yet been uploaded to the installation server.

To upload a file to the installation server:

1. Click **Browse** and navigate to the desired file.
2. Click **Open**.

Note: The selected configuration file is now on the installation server, and will appear in the drop-down list of available configuration files.

The **Define Servers** screen appears.

4.4.3 Modifying the Site Configuration File

Your site configuration file is ready to be edited.

For an explanation of the remaining wizard screens to edit an SDC site configuration file, see *Defining Servers and Ports* in the *Creating an SDC Site Configuration File* section.

Proprietary and Confidential Information of F5 Networks

For an explanation of the remaining wizard screens to edit an EMS site configuration file, see *Defining Servers and Ports* in the *Creating an EMS Site Configuration File* section.

Proprietary and Confidential Information of F5 Networks

5. Performing the Installation

The Installation is done with the Installation Utility and is based on the site configuration file.

5.1 Accessing the Installation Utility to Perform an Upgrade

To access the Perform Installation wizard:

1. In the Installation Utility home page, click **Perform Installation**.

   The Select Site Configuration File screen appears.

5.2 Selecting a Site Configuration File

There are two options to retrieve the site configuration file.

5.2.1 Load site configuration file from the installation server

Choose this option if the file you want to work with is included in the default files included with the Installation Utility, or if the file has previously been uploaded to the Installer server.

To load a file from the installation server:

1. Select the desired file from the drop-down list.

5.2.2 Upload site configuration file

Choose this option if the file you want to work with is located locally (for example, on a USB or on the desktop) and has not yet been uploaded to the installation server.

To upload a file to the installation server:

1. Click **Browse** and navigate to the desired file.
2. Click **Open**.

Note: The selected configuration file is now on the installation server, and will appear in the drop-down list of available configuration files.

Proprietary and Confidential Information of F5 Networks

5.3 Selecting the Installation Type

In the Select Installation screen, you need to select the servers that are going to be installed as part of the installation procedure. There are two types of installations:

- **Site Installation** installs all servers that are defined as part of the installation process in the site configuration file
- **Installation Per Server** installs only those servers that are selected from the list of available servers that appears when this option is selected

To apply the configuration file to all site servers:

1. Select **Site Installation**.

To apply the configuration file to specific site servers only

1. Select **Installation per Server**, and then select the relevant servers.

5.4 Viewing the Installation Steps

In the Installation Steps screen, you can view the list of steps that are performed as part of the installation. These steps are described in *Table 20*.

Table 20: Installation Steps

Installation Step	Description
Pre installation Tasks	
Validate Disk Space	
Validate PHY interfaces	
Validate and Configure Repository	
Validate Memory	
Validate System	
Copy Installation Files	Copies the installer scripts and the SDC.tar.gz file
Prepare Operating System	Updates the snmp, rsyslog, logrotate definitions; turns off the SNMP service; builds the /etc/host file; configures the kernel, the core file, the time zone, and

Proprietary and Confidential Information of F5 Networks

Installation Step	Description
	the NTP; starts the coredumps, snmp, and logrotate services; tells the system to remount the /dev/shm/ on boot; configures nsswitch.
Configure Network	Configures the interfaces, bonds, hostname, and static routing.
Reboot	Reboots the machine.
Install installer	Installs the installation utility on the selected servers.
Open SDC Installation Kit	Opens the tar.gz file, builds the /opt/traffix/sdc, and creates a backup of the old one.
Install Tripo Component	Installs and configures Tripo.
File Server installation	Installs and configures the File Server.
Install SS7 Component	Installs and configures SS7.
Install GRD Component	Installs and configures GRD.
Configure Traffix SDC	Builds the configuration file for each component in the /opt/traffix/sdc/config/sysconfig file.
Install NMS Agent Component	Installs and configures the NMS agent
Install Splunk Components	Installs and configures Splunk
Run SDC	Runs the SDC to check the effect the changes had.
Stop SDC	Stops the check.
Configure SDC Cluster	Configures the activeMQ and the config manager group; the servers begin communicating with each other; the cluster between sites is created – before each site was standalone.
Configure Corosync Cluster	Builds the configuration for Corosync
Hardening system (Security)	Performs system hardening according to the product requirements. This step verifies that only the necessary SDC ports are open and ready to accept inbound connections.

Proprietary and Confidential Information of F5 Networks

5.5 Defining the Operating System

In the Define OS screen, you need to define if the operating system should be installed as part of the installation.

To define if the operation system will be installed during the installation process:

1. Select **No** in response to the question: **Do you want to install the operating system during installation**?

5.6 Confirming the Installation Setup

The Summary screen displays all the definitions from the previous screens for your review and asks if you are ready to perform the installation.

To start the installation process:

1. Click **Next**.

To cancel the installation process:

1. Click **Cancel**.

5.7 Monitoring the Installation Progression

In the Installation Progress screen, you can see the installation progression for each installation step for each server. This way, if the installation fails on specific steps for a specific server, you can effectively troubleshoot the cause of the failure.

Note: If the Web UI screen refreshes or is refreshed during the installation, the installation will not complete successfully. If this occurs, the hardware must be cleaned, the installation server must be installed again, and the site servers must be set up again, before retrying the installation.

Proprietary and Confidential Information of F5 Networks

5.8 Performing Post-Installation Procedures

There are a variety of post-installation procedures, depending on your specific installation. Go over the procedures described in the *Post Installation Procedures* section and perform the necessary procedures.

5.9 Switching on the Site Servers

After all necessary post-installation procedures have been successfully performed, switch on the site servers by running the following command on each server:

crm node online

Proprietary and Confidential Information of F5 Networks

6. Post Installation Procedures

The following procedures are performed after the installation process is successfully completed:

- Changing the Root Password
- Changing the SNMP Community String
- Installing the Splunk License
- Activating and Installing the SS7 License
- Enabling SS7 Driver Redundancy
- Enabling Tripo Site Replication

6.1 Changing the Root Password

During installation the Root password is assigned a default value. For increased security, change this value.

To change the root password:

1. Run the Unix "passwd" command.

6.2 Changing the SNMP Community String

To prevent access to the system's SNMP data, change the community "public" string. The change should be performed in two levels: in every SDC and EMS site's OS and in the XML configuration file. For more information, contact F5 Support.

6.3 Installing the Splunk License

To license Splunk on your system, each Splunk component – the Splunk Master, Splunk Search, and Splunk Indexers – must be individually configured to work with the given license.

Proprietary and Confidential Information of F5 Networks

To configure the Splunk license:

1. Verify that all necessary Splunk processes are running for each of the installed Splunk components by running the following command for each Splunk components:

   a. For the Splunk Indexer:

      /opt/traffix/sdc/bin/traffix_splunk_init status

   b. For the Splunk Search:

      /opt/traffix/sdc/bin/traffix_splunksearch_init status

   c. For the Splunk Master:

      /opt/traffix/sdc/bin/traffix_splunkmaster_init status

2. Each component should run the following three processes:

   - splunkd
   - splunk helpers
   - splunkweb

3. If a Splunk component is not running all the necessary processes, start the Splunk component by running the following command:

   a. For the Splunk Indexer:

      /opt/traffix/sdc/bin/traffix_splunk_init start

   b. For the Splunk Search:

      /opt/traffix/sdc/bin/traffix_splunksearch_init start

   c. For the Splunk Master:

   /opt/traffix/sdc/bin/traffix_splunkmaster_init status start

4. Configure the Splunk license on the Splunk Master by performing the following steps:

Proprietary and Confidential Information of F5 Networks

a. Access the Splunk Web UI using the following URL: *http://<Splunk_Group_Virtual_IP_Address>:8100*

b. Go to **Manager>Licensing**.

c. Click **Add License** and then select **Copy & paste the license XML directly....**

d. Enter the license string provided to you by F5.

e. Click **Install**.

f. Restart as prompted.

Note: Verify that all necessary Splunk processes are up after restart by performing steps 1-3 of this procedure.

---

5. Configure the Splunk license on the Splunk Search by performing the following steps:

a. Run the following command on the servers running the Splunk Search:

vi /opt/splunksearch/splunk/share/splunk/search_mrsparkle/templates/account/login.html

b. Access the Splunk Web UI using the following URL:

http://<Server_Management_IP_Address>:8000

c. Go to **Manager>Licensing**.

d. Click **Change to Slave**.

e. Select **Designate a Different Splunk instance as the master license server**.

f. In the **Master license server URI** edit box, enter the following string: *https://splunkmaster.traffix.com:8189*

g. Restart as prompted.

Proprietary and Confidential Information of F5 Networks

h. Migrate the group containing the Splunk Master and Splunk Search to the second site server by running the following command:

crm resource migrate <splunk group name> <second site server name>

i. Repeat steps 4-5 on the second server now running the group containing the Splunk Master and Splunk Search.

Note: Verify that all necessary Splunk processes are up after restart by performing steps 1-3 of this procedure.

---

6. Configure the Splunk license on the Splunk Indexers by performing the following steps:

a. Run the following command on all servers running the Splunk Indexer:

vi /opt/splunk/share/splunk/search_mrsparkle/templates/account/login.html

b. Access the Splunk Web UI using the following URL:

http://<Splunk_Group_Virtual_IP_Address>:8200

c. Go to **Manager>Licensing**.

d. Click **Change to Slave**.

e. Select **Designate a different Splunk instance as the master license server**.

f. In the **Master license server URI** edit box, add the following string: *https://splunkmaster.traffix.com:8189*

g. Restart as prompted.

Note: Verify that all necessary Splunk processes are up after restart by performing steps 1-3 of this procedure.

Proprietary and Confidential Information of F5 Networks

6.4 Activating and Installing the SS7 License

To successfully process SS7 traffic, each SDC server must be configured with an activated SS7 license.

To activate your SS7 license:

1. In your web browser, go to

   http://membersresource.dialogic.com/ss7/license/license.asp.

2. In the License Activation screen, follow the instructions to complete the form.

   a. Run the following command on the server to retrieve the Host ID # (Licensing Host ID):

   cd /opt/DSI

   ./HSTBIN/m3ua –v

   b. Run the following command on the server to retrieve the Machine Name:

   Echo $HOSTNAME

3. Click **Submit**. The license file will be sent to the email address in the form.

4. Copy the license file to `/opt/DSI`.

5. Repeat steps 1-4 for each server that will run SS7.

To install your SS7 license:

1. Copy the activated SS7 license file to the following directory:

   `/opt/DSI`

2. Restart the SS7 driver by running the following command at `/opt/DSI`:

   gctload –x

3. Repeat steps 1-2 on each server that will run SS7.s

6.5 Enabling SS7 Driver Redundancy

Configuring RSI & RMM between two drivers of two CPF instances (A and B):

- Enables rerouting of SS7 traffic from CPF A to the driver serving CPF B when the links of the driver serving CPF A are down.
- Ensures that SS7 responses are sent to the CPF driver that initiated the corresponding SS7 request.

Before enabling SS7 driver redundancy, verify the following prerequisites:

- The SDC should be installed and configured with the required SS7 drivers.
- The SDC should have two CPF instances. Each CPF instance should be on a separate server and have a dedicated Dialogic driver which serves it.

To enable SS7 Driver Redundancy:

1. Modify the system.txt file in the /opt/DSI directory by adding the following three modules:
   - RMM module – identified by module id 0x32 for both drivers.
   - RSI module – identified by module id 0xb0 for both drivers.
   - rsicmd module – identified by module id 0xfd for both drivers.


Note: These modules should be added to both SS7 drivers.

a. Add the following lines to the system.txt file:

```
LOCAL    0x32   *RMM module
LOCAL    0xb0   *RSI module
LOCAL    0xfd   *rsicmd module
```

b. Each driver requires a different redirection configuration.

i. For driver A's redirection configuration, add the following lines to driver A's system.txt file:

```
*
* Definitions for Unit A:
```


Proprietary and Confidential Information of F5 Networks

```
*
REDIRECT 0x52 0xb0 * RMM to unit B
REDIRECT 0x12 0xb0 * M3UA to unit B
REDIRECT 0x53 0xb0 * SCCP to unit B
REDIRECT 0x34 0xb0 * TCAP to unit B
*
REDIRECT 0x42 0x32 * RMM from unit B
REDIRECT 0x02 0xd2 * M3UA from unit B
REDIRECT 0x43 0x33 * SCCP from unit B
REDIRECT 0x24 0x14 * TCAP from unit B
*
```

The first segment redirects traffic from driver A (“Unit A”) modules to driver B (“Unit B”) via the RSI module. The second segment redirects traffic from driver B (“Unit B”) to driver A (“Unit A”) local modules.

ii. For driver B’s redirection configuration, add the following lines to driver B’s system.txt file:

```
*
* Definitions for Unit B:
*
REDIRECT 0x42 0xb0 * RMM to unit A
REDIRECT 0x02 0xb0 * M3UA to unit A
REDIRECT 0x43 0xb0 * SCCP to unit A
REDIRECT 0x24 0xb0 * TCAP to unit A
*
REDIRECT 0x52 0x32 * RMM from unit A
REDIRECT 0x12 0xd2 * M3UA from unit A
REDIRECT 0x53 0x33 * SCCP from unit A
REDIRECT 0x34 0x14 * TCAP from unit A
*
```

The first segment redirects traffic from driver B (“Unit B”) modules to driver A (“Unit A”) via the RSI module. The second segment redirects traffic from driver B (“Unit B”) to driver A (“Unit A”) local modules.

Proprietary and Confidential Information of F5 Networks

c. Use the FORK_PROCESS command to configure and start the modules:

i. Add the following lines to driver A's system.txt file:

```
FORK_PROCESS ./rmm -m0x32 -d
FORK_PROCESS ./monitorScript.sh*
FORK_PROCESS ./rsi -m0xb0 -r./rsi_lnk -l1
FORK_PROCESS ./rsicmd 0 0x32 0 <rem_addr> <rem_port> 0xb0
```

ii. Add the following lines to driver B's system.txt file:

```
FORK_PROCESS ./rmm -m0x32 -d
FORK_PROCESS ./monitorScript.sh*
FORK_PROCESS ./rsi -m0xb0 -r./rsi_lnk -l1
FORK_PROCESS ./rsicmd 0 0x32 1 <rem_addr> <rem_port> 0xb0
```

Note: The syntax for rsicmd is:

rsicmd <link_id> <conc_id> <link_type> <rem_addr> <rem_port> [<rsi_id>]

<link_id> should be set to '0' – represents one link with id '0'.

<conc_id> should be set to "0x32" - identifies the local module which will receive a message when the RSI link fails.

<link_type> should be set to '0' for driver A (represents Client connection type) and should be set to '1' for driver B (represents Server connection type).

<rem_addr> should be configured to the server driver IP address on the IC network.

<rem_port> should be configured to the server driver TCP/IP socket port. Each RSI link should have a unique port value, starting from 9000.

<rsi_id> should be set to "0xb0" – identifies the RSI module.

2. Modify the config.txt file in the /opt/DSI directory by performing the following steps:

Note: These modules should be added to both SS7 drivers.

Proprietary and Confidential Information of F5 Networks

a. To enable RMM transport over RSI, add the <DUAL> parameter to the CNSYS command:

i. For driver A, set the <DUAL> parameter value to ‘A’:

```
CNSYS:IPADDR=10.2.9.7,IPADDR2=10.2.9.9,DUAL=A;
```

ii. For driver B, set the <DUAL> parameter value to 'B’:

```
CNSYS:IPADDR=10.2.9.8,IPADDR2=10.2.9.10,DUAL=B;
```

b. To configure dual-resiliency, edit the SCCP_CONFIG command:

i. Add the SCCP partner module id (<partner id>) for each driver. The <partner id> value should be set to ‘0x53’ on driver A and ‘0x43’ on driver B.

ii. Set the <sccp_instance> parameter to a unique number (between 0 and 15) for each SCCP instance. The <sccp_instance> value should be set to ‘0’ on driver A and ‘1’ on driver B.

Driver A:

```
SCCP_CONFIG 704 0 0x108c0100 1 0x53 0
```

Driver B:

```
SCCP_CONFIG 704 0 0x108c0100 1 0x43 1
```

c. To configure dual-resiliency, edit the TCAP_CONFIG command:

i. Add the TCAP partner module id (<partner id>) for each driver. The <partner id> value should be set to ‘0x34’ on driver A and ‘0x24’ on driver B.

ii. Set the <tcap_instance> parameter to a unique number (between 0 and 15) for each TCAP instance. The <tcap_instance> value should be set to ‘0’ on driver A and ‘1’ on driver B:

Unit A:

Proprietary and Confidential Information of F5 Networks

```
TCAP_CONFIG 0x8000 32767 0x0 32768 0x0100 0 0 0x34 0
```

Unit B:

```
TCAP_CONFIG 0x8000 32767 0x0 32768 0x0100 0 0 0x24 1
```

d. Verify that the OPC (Originating Point Code) defined in the SNAPI command is the same for both drivers:

Driver A:

```
SNAPI:LAS=1,OPC=704,TRMD=LS;
```

Driver B:

```
SNAPI:LAS=1,OPC=704,TRMD=LS;
```

6.6 Enabling Tripo Site Replication

Tripo Site Replication enables the replication of sessions between Tripo instances on mated SDC sites. Enabling the Tripo Site Replication feature is a post-installation step that is performed only after the Tripo site replication on Tripo instances (resources) on both SDC sites has been enabled.

Note: Sessions are replicated to the mated SDC site only for those sessions that are defined with a **Persist and Replicate Session Persistence Policy** in the Web UI (**Routing>Session Management**).

To enable Tripo site replication on each server that has a Tripo resource:

1. Verify the Tripo inter-site connection between the mated SDC sites:
   a. Run the following commands:

   i. **su - traffix**
   ii. **cd /home/traffix/Tripo/env/linux-x86_64/**
   iii. **. DefEnv Tripo**
   iv. **UI_ViewServers -p**

Proprietary and Confidential Information of F5 Networks

b. Verify that the version of both Tripo resources on the SDC site are the same by comparing the **Local version** to a **Local Mate version**.

c. Verify that the IP addresses of the Tripo instances on the remote SDC site are displayed in the **Site IP** column. These IP addresses are configured during the installation.

2. Verify that the connection between each Tripo instance and the Tripo instances on the mated SDC site are established. The verification is done by:

   a. Checking that each Tripo instance has the required connections to both Tripo instances on the mated SDC site.

   b. Checking that each Tripo instance is listening on the Tripo SRR port.

      The following screenshot is an example for a deployment which has two Tripo instances on the local SDC and on the mated SDC site.

3. Enable Tripo Site Replication by running the following commands on each server running Tripo Resource:

   a. **su - traffix**

   b. **cd /home/traffix/Tripo/env/linux-x86_64/**

   c. **. DefEnv Tripo**

   d. **UI_Config**

   e. **set SiteReplication true**

   f. **CTRL–C** to exit from UI_config

   g. **UI_Config -w ConfigParams.cfg**

4. Verify that the Tripo Site Replication was enabled, by running the following commands:

   a. Run **UI_config**

   b. ==>**dump**

   c. Review the *ConfigParams.cfg* file (located in the /*home/traffix/Tripo/cfg/* folder) and check that **SiteReplication = true**

5. Enable Tripo replication on each server that has a CPF resource on both SDC sites:

   a. Go to the following folder: */opt/traffix/sdc/config/sysconfig/*

   b. Within the folder, open the “traffix” file.

   c. Add the parameter USE_TREPO_REPLICATION=true. If the parameter exists, change the setting from false to true.

   d. Save the file and restart each CPF and FEP resource one by one.

Proprietary and Confidential Information of F5 Networks

Note: After changing the **SiteReplication** parameter to true, verify that a "tripoEnableSRR" trap is generated form each Tripo instance.

6.7 Enabling Keyboard Navigation in the Web UI (Accessibility)

In this SDC release, an option to navigate through the SDC and EMS Web UI using a keyboard was added. This must be enabled after installation.

To enable keyboard navigation:

1. Go to the */opt/traffix/sdc/utils/apache-tomcat/webapps/MgmtConsole/MgmtConsole.html* file and perform the following steps:

   a. Locate the following string in the file:

   <!--<script src="Loader/Head/index.js" async="" type="text/javascript"></script>-->

   b. Remove the "**<!--**" string from the beginning of the row and the "**-->**" string from the end of the row.

2. Go to the */opt/traffix/sdc/utils/apache-tomcat/webapps/MgmtConsole/Loader/Head/index.js* file and perform the following steps:

   a. Locate the following string in the file:

   //User1stAppUrl = "http://WEBUI_VIP_ADDRESS:8080/MgmtConsole";

   Note: When using HTTPS, the port number is the URL is 8443, instead of 8080.

   b. Replace "WEBUI_VIP_ADDRESS" with the Web UI Virtual IP Address.

   c. Uncomment the variable **User1stAppUrl**. (remove "//").

Proprietary and Confidential Information of F5 Networks

3. Go to the */opt/traffix/sdc/utils/apache-tomcat/webapps/MgmtConsole/Loader/index.js* file and perform the following steps:

   a. Locate the following string in the file:

   //User1stAppUrl = "http://WEBUI_VIP_ADDRESS:8080/MgmtConsole";

Note: When using HTTPS, the port number is the URL is 8443, instead of 8080.

---

   b. Replace <WEBUI_VIP_ADDRESS> with the Web UI Virtual IP Address.

   c. Uncomment the variable **User1stAppUrl**. (remove "//").

4. Go to the */opt/traffix/sdc/utils/apache-tomcat/webapps/MgmtConsole/CommFrame/index.html* file and perform the following steps:

   a. Locate the following string in the file:

   //User1stAppUrl = "http://<WEBUI_VIP_ADDRESS>:8080/MgmtConsole";

Note: When using HTTPS, the port number is the URL is 8443, instead of 8080.

---

   b. Replace <WEBUI_VIP_ADDRESS> with the Web UI Virtual IP Address.

   c. Uncomment the variable **User1stAppUrl**. (remove "//").

   d. Locate the following string (line 26) and comment it out by adding "//" beforehand.

   script.src = "../Scripts/CommFrameScripts/index.js?ver=0.0.0.50";

   e. Locate the following string (line 28) and uncomment it by remove the "//" beforehand:

Proprietary and Confidential Information of F5 Networks

//script.src = User1stAppUrl +

"Scripts/CommFrameScripts/index.js?ver=0.0.0.50";

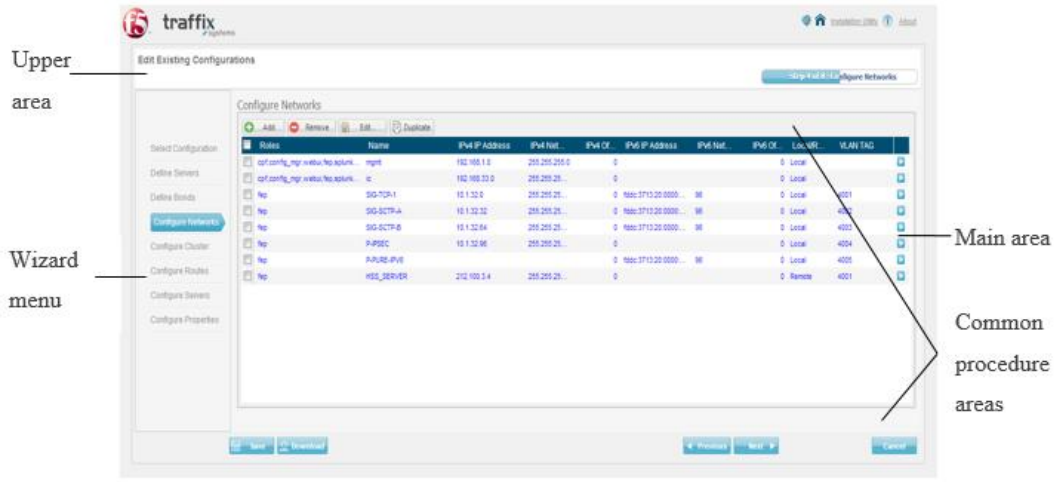
Proprietary and Confidential Information of F5 Networks

A. Appendix A: Working with the Installation Utility

The installation utility is a web-based wizard tool used to create, modify, and install SDC and EMS sites.

Each selected procedure opens a specific wizard of step screens to help you complete the procedure. The Edit Existing Configurations>Configure Network screen (Figure 2) is an example of an installation utility wizard screen.

Figure 1: Edit Existing Configurations>Configure Network Screen



Performing common procedures in the Installation Utility

Navigating between screens

Within each installation utility procedure, you can navigate between the step screens by using either the wizard menu or the quick-click access buttons in the common procedures areas.

Proprietary and Confidential Information of F5 Networks

To navigate between the step screens using the wizard menu:

1. In a step screen, click on the desired step in the wizard menu to move to that screen.

To navigate between the step screens using the navigating buttons:

1. In a step screen, click on one of the following buttons:
    a. **Previous** – Clicking this button opens the previous step's screen.
    b. **Next** – clicking this button opens the next step's screen.
    c. **Cancel** – clicking this button exits the current procedure. The Save Topology dialog box will appear. To save the current configuration, enter a name or select a name from the drop-down list and click OK.

Adding elements

In step screens displaying configured elements, you can add elements using the Add function, or by editing the table values.

To add elements using the Add function:

1. Click **Add**. The first available row in the table will become editable.
2. Click on an editable row and enter the desired values.

Note: For more information about each element's parameters, go to the specific step screen explanation in the Creating and Editing Site Configuration Files section.

To add elements by editing the table values:

1. Click on a table row. The first available row in the table will become editable.
2. Click on an editable row and enter the desired values.

Proprietary and Confidential Information of F5 Networks

Modifying configured elements

In step screens displaying configured elements, you can edit elements by editing the table values.

To edit elements by editing the table values:

1. Click on a table row. The first available row in the table will become editable.
2. Click on an editable row and enter the desired values.

Note: For more information about each element's parameters, go to the specific step screen explanation in the Creating and Editing Site Configuration Files section.

Deleting elements

In step screens displaying configured elements, you can delete elements using the Remove function, or by editing the table values.

To delete elements using the Remove function:

1. Select the checkbox of the row you wish to remove.
2. Click **Remove**. The selected element and its configured parameters will be erased.

Saving changes

The installation utility offers the following options to save your configuration files:

- In the site configuration screens, use the **Save** or **Download** buttons
- In the perform installation screens, use the **Log** or **Stop** buttons.

Switching between procedures

After selecting a procedure, you can return to the installation utility home page by either:

- Clicking **Cancel**.
- Clicking the home icon.

Proprietary and Confidential Information of F5 Networks

B. Appendix B: Common Cluster Configurations

This section provides an overview of the cluster configuration of two common SDC site setups:

- **Signaling Delivery Controller (SDC) sites** – these sites include the network infrastructure and SDC components needed to correctly process messages between the client and server peers.
- **SDC Element Management System (EMS) sites** – these sites include the network infrastructure and EMS site components needed to collect and manage data from SDC sites.

The SDC or EMS site contains one or more servers that are configured in the same configuration file.

Cluster Configuration for an SDC site

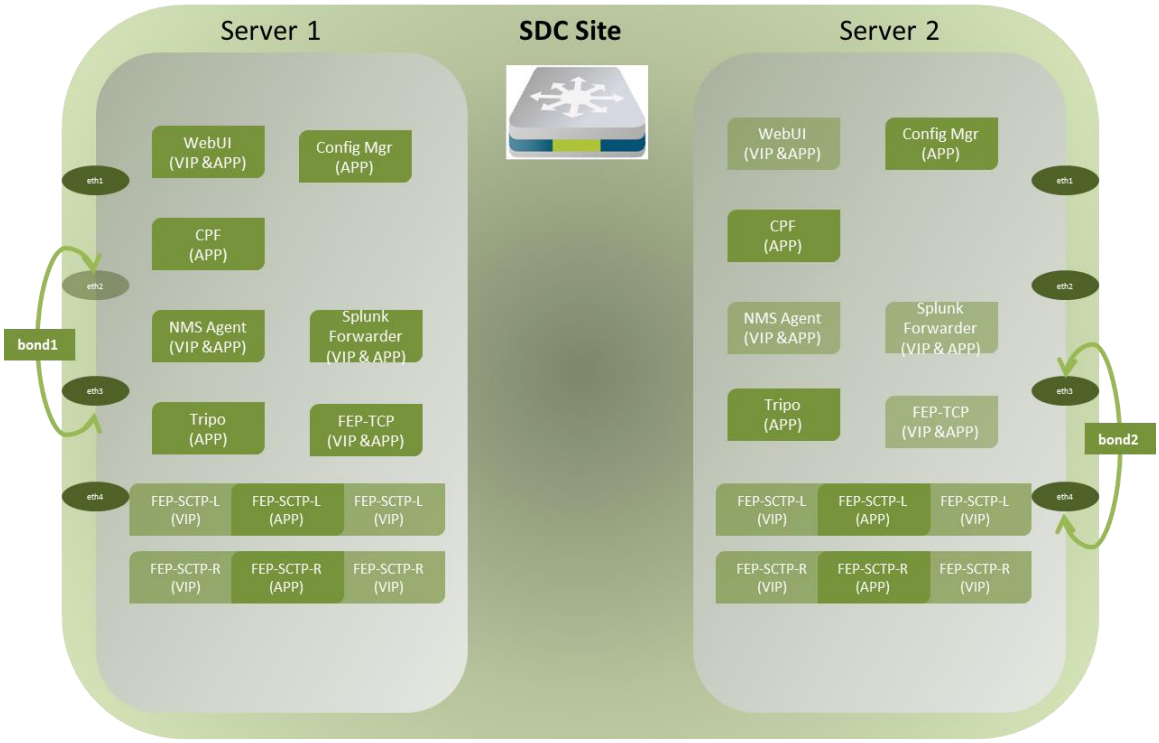
An SDC site includes the network infrastructure and SDC components needed to correctly process messages between the client and server peers. The figure below shows an SDC site cluster configuration. The following components are installed on this site:

- Web UI – running on the management network, the Web UI is run on the active server
- Configuration Manager – running directly on both servers concurrently
- CPF – running directly on both servers concurrently
- Tripo - running directly on both servers concurrently
- NMS Agent - running on the management network, the NMS agent is run on the active server
- Splunk Forwarder - running on the interconnect network, the Splunk Forwarder is run on the active server
- FEP instances – running on a signaling network, the FEP instances are run on the active server
- SS7 – running on the signaling network, running directly on both servers concurrently

Proprietary and Confidential Information of F5 Networks

- File Server – running directly on both servers concurrently

Figure 2: SDC Site Cluster Configuration



Cluster Configuration for an EMS site

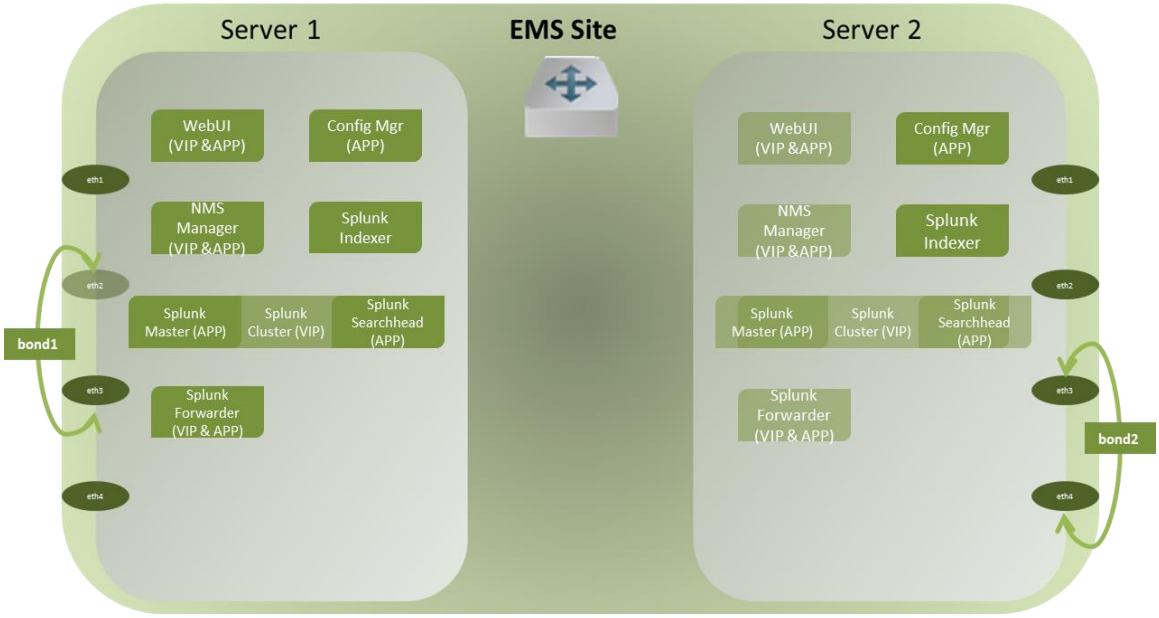
An EMS site includes the network infrastructure and EMS site components needed to collect and manage data from SDC sites. The figure below shows an EMS site cluster configuration. The following components are installed on this site:

- Web UI – running on the management network, the Web UI is run on the active server
- Configuration Manager – running directly on both servers concurrently
- NMS Manager - running on the management network, the Web UI is run on the active server
- Splunk Forwarder - running on the interconnect network, the Web UI is run on the active server
- Splunk Indexer – running directly on both servers concurrently

Proprietary and Confidential Information of F5 Networks

- Splunk Cluster – containing the Splunk Master and Splunk Search Head, running on the management network, the Splunk Cluster is run on the active server

Figure 3: EMS Site Cluster Configuration



Proprietary and Confidential Information of F5 Networks

C. Glossary

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

Table 21: 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

Proprietary and Confidential Information of F5 Networks

Term	Definition
Geo Redundancy	A mode of operation in which more than one geographical location is used in case one site fails
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

Proprietary and Confidential Information of F5 Networks

Term	Definition
Request	A message sent from one Client/Server peer to the other, followed by an answer message
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 session which inherits properties from a master session
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 binding point 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

Proprietary and Confidential Information of F5 Networks