Bulk Provisioning Guide

Dialogic® BorderNet™ Session Border Controller (SBC)

Release 3.8.1

June 2019

Table of Contents

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Document History

Version #	Date	Description
1.0	July 2013	Release 3.1.0
2.0	December 2013	Release 3.1.4
3.0	December 2013	Release 3.2.0
4.0	May 2017	Release 3.6.0 - Added static routing & formatting
4.1	August 2017	Release 3.7.0 - Added the Bulk Provisioning limitations
4.2	May 2019	Release 3.8.1

1. Introduction

1.1 Purpose of this Document

This document is intended to familiarize the reader with the **Dialogic BorderNet SBC bulk loading capability** description, and provisioning.

1.2 Glossary

For the purposes of this document the following abbreviations apply:

Abbreviation	Meaning
SBC	Session Border Controller

Table 1: Glossary

1.3 Contact Us

For a list of Dialogic locations and offices, please visit: **https://www.dialogic.com/contact.aspx**.

2. Overview

The BorderNet SBC provides Bulk Provisioning for SIP objects. Bulk Provisioning enables the user to add, update, delete, and export a large number of objects in one operation. Bulk Provisioning works on the following configuration objects:

- SIP Peer
- SIP Interface
- SIP Interface-Peer Associations
- Local DNS
- Advanced Policy
- Static Routing

> **Note:**
>
> Bulk Provisioning is limited to maximum 1000 transaction per action (create, update and delete).

2.1 Accessing Bulk Provisioning

→ To access bulk provisioning:

1. Select Application ➜ Common ➜ Bulk Provisioning. The Bulk Provisioning Configuration window opens:
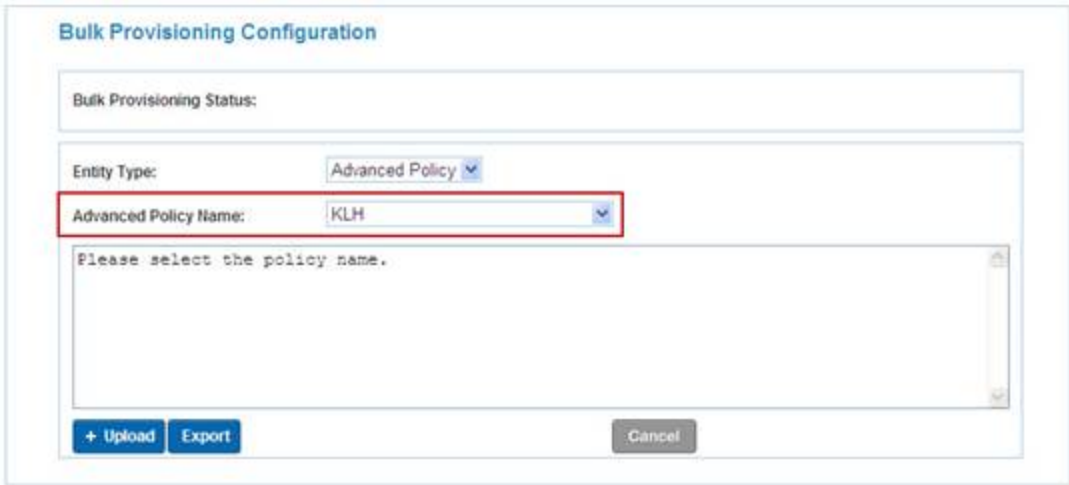
2. Select an **Entity Type** from the drop-down menu.
   - When **Peer**, **Interface**, **Interface-Peer**, or **LocalDNS** is selected, the appropriate template is displayed in the **Template** window. The screen above shows the template that appears when the **Peer** Entity Type is selected. This template can be copied to a .csv or .txt file. Add data below the header to create a complete data file to be added via bulk provisioning.
   - When **Advanced Policy** is selected, the BorderNet SBC displays the **Advanced Policy** drop-down menu, which is automatically populated with available policies (shown below).

- ○ When **Static Routing** is selected

2.2 Uploading a File

Select the **Upload** button to submit .csv or .txt file to the BorderNet SBC. The following window opens:

Click **Browse** and select the desired .cvs or .txt. Click **Save** to upload the file. If the data in the uploaded file is successfully validated, a new pop-up screen appears indicating that the upload was successful. If not, an error message screen will indicate the problem(s) encountered in processing the Bulk Add request.

3. Export Data

Export is an operation that downloads data to a file on a user's computer. In bulk provisioning, all objects of a particular object type can be downloaded.

3.1 Export Data File Description

The first line in the exported data file is the name of the entity type or object type. The second line contains the version of the data.

Note:

When performing a bulk update, be sure to include a version number in the updated data file. If data was modified between the bulk export/update procedures, the version number would cause the bulk update to fail, preventing loss of data.

The third line in the exported data file contains the names of fields in the **Entity Type**. Data of all object instances start at the fourth line of the file.

To perform a bulk add, delete, or update, insert **Add**, **Delete**, or **Update** in the first line of the exported data file. When a user clicks **Upload** button, a new screen asking the user to specify the directory and the name of the data file to upload.

3.2 How to Export Data

1. Select **Application** ➜ **Common** ➜ **Bulk Provisioning**.
2. In the **Bulk Provisioning Configuration** window, select the desired **Entity Type** from the drop-down menu (for example, **Local DNS**).

3. Click the **Export** button. A pop-up window asks the user to open the file or save the file in a local directory:
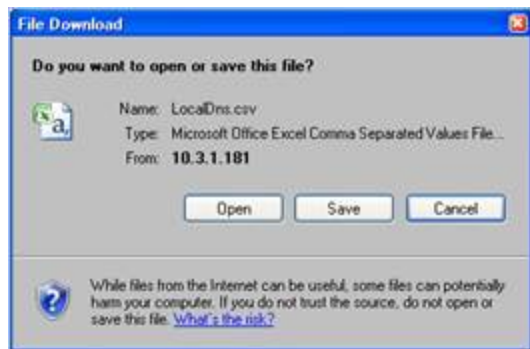
4. Select a file download option.

Once an option is selected, the BorderNet SBC gathers data for all Local DNS objects, downloads the data, and saves the data in a file in either in a temporary directory or at the directory specified by the user.

4. Add Data

Add is an operation that allows a user to submit one data file containing multiple data objects of a particular type to the BorderNet SBC.

4.1 Add Data File Description

The first line in the bulk add data file should be **Add**, followed by a space and the entity type or object type. The second line in the file should contain names of fields in the Entity Type. Data of all object instances start at the third line of the file. If the object contains an "Id" field, the content of the Id field can be populated or left empty. If the content of the Id field is empty, the BorderNet SBC will automatically create an Id for the objects.

4.2 How to Add Data

1. Select **Application ➜ Common ➜ Bulk Provisioning**.
2. In the **Bulk Provisioning Configuration** screen, select the desired **Entity Type** from the drop-down menu (for example, **Peer**). Verify the header in the .csv file matches the header in the bulk provisioning template.

3. Click the Upload button to open the Upload a Bulk Provisioning File screen.

4. Use the **Browse** button to select the desired file and click **Save**.

5. Delete Data

Delete is an operation that allows a user to submit a data file containing data of objects of a particular object type to the BorderNet SBC to delete all objects in the file at one time.

Note:

The BorderNet SBC does not provide the bulk delete function for Advanced Policy.

5.1 Delete Data File Description

The first line in the bulk delete data file should be the manipulating type **Delete**, followed by a space and the entity type or object type. The second line in the bulk delete file should contain names of fields for the data below the line. The supporting names of fields for deletion are **Name** and **Id**.

Note:

Since Local DNS and Interface-Peer Association do not have the **Name** field, the **Id** must be provided to bulk delete those types of objects.

Data of all object instances start at the third line of the data file. A user can put either **Name** or **Id** content in the data file. If both **Name** and **Id** are provided, the BorderNet SBC will delete objects only when contents of both **Name** and **Id** match. If there is no match, the BorderNet SBC will report the error and abort bulk deletion.

5.2 How to Delete Data

1. Select Application ➜ Common ➜ Bulk Provisioning.
2. Select the desired Entity Type from the drop-down menu (for example, Interface). Verify the header in the .csv file matches the header in the bulk provisioning template.

3. Click the Upload button to open the Upload a Bulk Provisioning File screen.

4. Use the **Browse** button to select the desired file and click **Save**.

6. Update Data

Update is an operation that allows the user to submit a data file containing data of objects of a particular object type to the BorderNet SBC to update all objects in the file at one time.

6.1 Update Data File Description

The first line in the bulk update data file should be the manipulating type **Update**, followed by a space and the entity type or object type. The second line should contain the version of the data, for example:

Version="e3a1cad702b074b7ffc4ae32b688639a0c58c832"

The third line in the bulk update data file should contain names of fields in the entity type. Data of all object instances start at the fourth line of the file. The content of Id field is mandatory in the bulk update data file.

If there are no object changes between exporting and bulk updating, the BorderNet SBC wil update the objects in the file at one time. If an object was modified, the version would have changed, causing the version in the bulk update file to be outdated. In this case, the BorderNet SBC will provide a warning:
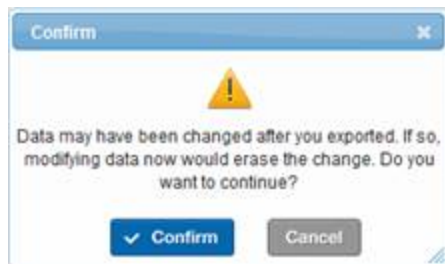
To ignore the warning and update the objects, click **Confirm**. Otherwise, click **Cancel**.

6.2 How to Update Data

1. Select Application ➔ Common ➔ Bulk Provisioning.
2. Select the desired Entity Type from the drop-down menu (for example, Interface-Peer). Verify the header in the .csv file matches the header in the bulk provisioning template.

3. Click the Upload button to open the Upload a Bulk Provisioning File window.

4. Use the **Browse** button to select the desired file and click **Save**.

7. Template Instructions

This section provides additional template instructions for each configuration object.

Note:

Template value fields use **Yes** and **No** to indicate an object's status. In the BorderNet SBC WebUI, the **Yes** value corresponds to **On**, and the **No** value corresponds to **Off**.

7.1 SIP Peer

The Add/Edit SIP Peer windows are used to configure SIP Peers (shown below).

The following table describes the possible values for each SIP Peer field:

Field	Values
Status	On or Off

Field	Values
Name	String value
Class ID	String value
Network Type	Interconnect, Local, Access-Public, Access-Local, or Access-Interconnect
Network Property	Indicates whether Subscriber Traffic is enabled: Yes (checked), No (unchecked)
Source List	This field accepts the value in the following format: Network Type, IP Address, Port Note: The Network Type could be IPv4 or IPv6. For multiple source lists could use ";" or space split the value.
Trust Level	High, Medium, or Low
Destination FQDN/IP	This field accepts the value in the following format: Network Type, IP Address/FQDN, Port Note: The Network Type could be IPv4, IPv6, or FQDN. The Destination FQDN/IP field can only accept only one value.
Destination Port	Indicates the Port.
Protocol	Indicates whether UDP, TCP, or TLS are enabled: Yes (checked), No (unchecked)
Time Zone	Indicates the time zone of the Peer.
TGRP ID	Indicates the Trunk Group ID (if any).
Enforce IPsec	Indicates whether IPsec is enforced (Yes or No).
Parameter Profile, Media Profile, Service Profile, Security Profile	These fields provide drop-down lists that contain the names of the existing profiles on the BorderNet SBC.

7.2 SIP Interface

The Add/Edit SIP Interface windows are used to configure SIP Interfaces (shown below).

The following table describes the possible values for each SIP Peer field:

Field	Values
Status	On or Off
Name	String value
Domain	String value
Network Type	Interconnect, Local, Access-Public, Access-Local, or Access-Interconnect
SIPconnect	Indicates whether SIPconnect is enabled (Yes or No). **Note**: Applicable to Interconnect and Access-Public Network Types only.
SIPconnect Type	Indicates the SIPconnect Type: SIPconnect1.1-BulkOnly, SIPconnect1.1-Mixed **Note**: Applicable to Interconnect and Access-Public Network Types only.
Network Property	Indicates whether Subscriber Traffic is enabled: Yes (checked) , No (unchecked)
Access Type	This fields provides a drop-down list that contains available Access Type options. **Note**: Applicable to Interconnect and Access-Public Network Types only.
Trust Level	High, Medium, or Low
Associated Peers	Indicates whether Peers are associated to this Interface: Yes (checked), No (unchecked)

Field	Values
Transport IP Address Type	IPv4 or IPv6
Signaling IP	This field provides a drop-down list of available VLANs.
Signaling Port	Indicates the Port.
Transport Protocol	This field provides a drop-down list of available Transport Protocols: UDP, UDP-TCP, or TLS. **Note**: The possible Transport Protocols depend upon the Network Type selected.
Time Zone	Indicates the time zone of the Interface.
Signaling TOS	Indicates the Signaling TOS.
Port Allocation	Provides a drop-down list of available Port Allocations.
RegPortReuse	Indicates whether Port Allocation is reused (Yes or No).
TGRP Context	Indicates the Trunk Group Context.
Enforce IPsec	Indicates whether IPsec is enforced (Yes or No).
Parameter Profile, Media Profile, Service Profile, Security Profile	These fields provide drop-down lists that contain the names of the existing profiles on the BorderNet SBC.

7.3 SIP Interface-Peer Association

The Add/Edit SIP Interface-Peer screens are used to associate SIP Interfaces and Peers (shown below).

The following table describes the possible values for each SIP Peer field:

Field	Values
Status	On or Off
Peer	This field provides a drop-down list of configured Peers.
Interface	This field provides a drop-down list of configured Interfaces.
Connectivity Timer	This field contains a positive integer value for the connectivity timer. A 0 value turns off the timer.

7.4 Local DNS

The Add/Edit Local DNS windowss create the Local DNS entries (shown below).

The following table describes the possible values for each Local DNS field:

Field	Values
Status	On or Off
FQDN List	Allows the user to enter multiple FQDN addresses
Resolved FQDN/IP	Provides IPv4 or IPv6 options from the drop-down list. Enter the IP address in the selected format in the next field.
Port	Accepts an integer in the range 0-65535
Transport Protocol	Provides a drop-down list with the possible values: None, TCP, UDP, TLS
Priority	Accepts an integer in the range 0-10
Weight	Accepts an integer in the range 0-100

7.5 Advanced Policy

The Advanced Policy template is more complex than the previous four object types. There are two parts of the Advanced Policy template:

- Advanced Policy header
- Advanced Policy content

An Advanced Policy template for updating could be written as below:

	A	B	C	D	E	F
1	Update Policy					
2	Version="f9681216421d275da2a105855633734f7038fe21"					
3	Policy	No	PolicySample		3 ;	
4	Rule	Yes	CallingPartyUserId	AssignsFrom	String:Test	{
5	Rule	Yes	CallingPartyDomainName	BeginsWith	StringList:409,408		
6	Rule	Yes	MessageRouting	IsPresent	Boolean:Yes	}
7	Rule	Yes	GenericParameter	Contains	StringList:406	{
8	Treatment		Reject 410_GONE	}		

This is the Advanced Policy in the WebUI:

Note:

It is recommended to have each line include only one instance for the content of the Advanced Policy. However, each line can also include multiple instances.

For example, if the Advanced Policy header is:

Policy, No, PolicySample, 3;

- Policy is the **Entity Type**; it must be the first type in the Advanced Policy.
- The second variable is the **Status** of the Advanced Policy; possible values are Yes or No.
- The third variable is the **Name** for the Advanced Policy.
- The fourth variable is the **Id** for the Advanced Policy. This field is optional for the Add Template, but it is mandatory for the Update Template.
- After all fields filled, the Advanced Policy Header should end with the "**;**".

Below the Advanced Policy header is the content of the Advanced Policy. Each line is an instance for the content of the Advanced Policy. For example, in the first instance show above:

Rule, Yes, CallingPartyUserId, AssignsFrom, String:Test

- The first variable is the **Type** of the instance. The supporting instance types are Rule, GoTo, True, or Treatment.
- The second variable is the **Status** of the current instance. Possible values are Yes or No.
- The third variable is the **Operand Parameter** of the instance. Possible values are found in the Rule Parameter list on the WebUI.
- The fourth variable is the **Operator Type**. Possible values are found in the Rule Parameter list Rule Action list on the WebUI.
- The fifth variable is the **Value** of the operator. There are 2 parts in this value:
  - The first part is the value type; in the example above it is "String".
  - The second part is the value content. In the example above, the value content is "Test". The template used ":" to split the value type and the value content.

When an instance is ended, if there is another instance after this instance, specify the relation between the instances. There are two kinds of relations between two instances: Parent-Child relation and Sibling relation. Use "{}" to present the Parent-Child

relation. In the example, Rule in line 5 and Rule in line 6 are the children of Rule in line 4. Use "|" to present the Sibling relation. In the example, Rule in line 5 and Rule in line 6 are Sibling relations, and the "Treatment" is always treated as the Parent-Child relation of a Rule.

For the "Treatment" instance, the template is similar to that of the Rule entity. There are five element types in the treatment entity: Route, Reject, Apply Rule, Media, and Flow Class. Use ";" to separate different elements.

Note:

Instead of writing a template for the specific instance, the use can instead add similar fields from the WebUI, export the template from the bulk provisioning API, and then adopt the format in the exported data file.

7.6 Static Routing

8. Sample Files

8.1 Policy Sample Files

8.1.1 Add Policy Sample File

Add Policy								
Policy	Yes	DialogicAdvancedPolicy		10001 ;				
Rule	Yes	CallingPartyDomainName	BeginsWith	StringList:407,408	(			
Rule	Yes	MessageRouting	IsPresent	Boolean:No	(			
Rule	Yes	PrivateIdentityDomain	BeginsWith	StringList:911,917	(			
Treatment	Reject	403_FORBIDDEN	}	}	}			
Rule	Yes	OriginationTGRPId	AssignsFrom	Parameter:CPC	(			
Rule	Yes	DestinationDomain	IsNotEqualTo	ParameterList:CallingPartyUserId, CalledPartyDomainName	(			
Treatment	Route	Peer,SIP:(DialogicPeer3,[Dialogic])	Interface,SIP:(DialogicIntf1,[Dialogic,Dialogic]),(DialogicIntf4,[Dialogic,Dialogic])	;		Flow Class	White	}	}
Rule	Yes	IncomingInterface	IsEqualTo	InterfaceList:(SIP:DialogicIntf2,DialogicIntf3,DialogicIntf4)				
TRUE	Yes[							
Rule	Yes	RegisteringIdentityDomain	IsEqualTo	StringList:Dialogic	(			
}	}							

8.1.2 Update Policy Sample File

Update Policy								
Version="a402d9662d6dd6659467ee09a2fbfb822d2c172b"								
Policy	No	DialogicAdvancedPolicy		10001 ;				
Rule	Yes	CallingPartyDomainName	BeginsWith	StringList:407,408	(			
Rule	Yes	MessageRouting	IsPresent	Boolean:No	(			
Rule	Yes	PrivateIdentityDomain	BeginsWith	StringList:911,917	(			
Treatment	Reject	403_FORBIDDEN	}	}	}			
Rule	Yes	OriginationTGRPId	AssignsFrom	Parameter:CPC	(			
Rule	Yes	DestinationDomain	IsNotEqualTo	ParameterList:CallingPartyUserId, CalledPartyDomainName	(			
Treatment	Route	Peer,SIP:(DialogicPeer3,[Dialogic])	Interface,SIP:(DialogicIntf1,[Dialogic,Dialogic]),(DialogicIntf4,[Dialogic,Dialogic])	;		Flow Class	White	}	}
Rule	Yes	IncomingInterface	IsEqualTo	InterfaceList:(SIP:DialogicIntf2,DialogicIntf3,DialogicIntf4)				
TRUE	Yes[							
Rule	Yes	RegisteringIdentityDomain	IsEqualTo	StringList:Dialogic	(			
}	}							

8.2 Local DNS Sample Files

8.2.1 Add Local DNS Sample File

Add LocalDns								
Id	Status	FQDN	Resolved	Resolved FQDN/IP	Port	Transport	Priority	Weight
10001	Yes	Dialogic-FQDN1	IPv4	192.5.60.7	0	None	0	11
10002	Yes	Dialogic-FQDN2	IPv4	192.168.77.2	2001	TCP	1	12
10003	Yes	Dialogic-FQDN3	IPv4	10.6.55.4	4023	UDP	2	13
10004	Yes	Dialogic-FQDN4	IPv4	28.45.22.101	5571	TLS	3	14
10005	Yes	Dialogic-FQDN5	IPv4	54.56.154.33	8081	UDP	4	15
10006	Yes	Dialogic-FQDN6 Dialogic-FQDN61	IPv6	2607:f0d0:1002:51::4	2300	None	5	16
10007	Yes	Dialogic-FQDN7	IPv6	2608:f0d0:1002:61::4	6060	TLS	6	17
10008	Yes	Dialogic-FQDN8	IPv6	2607:f1d0:2012:81::8	5651	UDP	7	18
10009	Yes	Dialogic-FQDN9	IPv6	1607:e3f0:2013:71::1	1001	TCP	8	19
10010	Yes	Dialogic-FQDN10 Dialogic-FQDN101 Dialogic-FQDN102	IPv6	1817:23e0:e0f3:c1::e	2762	None	9	20

8.2.2 Update Local DNS Sample File

Update LocalDns								
Version="98874715a995279f85e9e946a312391edd83c379"								
Id	Status	FQDN	Resolved	Resolved FQDN/IP	Port	Transport	Priority	Weight
10001	No	Dialogic-FQDN1	IPv4	192.5.60.7	0	None	9	21
10002	No	Dialogic-FQDN2	IPv4	192.168.77.2	2001	TCP	8	22
10003	No	Dialogic-FQDN3	IPv4	10.6.55.4	4023	UDP	7	23
10004	No	Dialogic-FQDN4	IPv4	28.45.22.101	5571	TLS	6	24
10005	No	Dialogic-FQDN5	IPv4	54.56.154.33	8081	UDP	5	25
10006	No	Dialogic-FQDN6 Dialogic-FQDN61	IPv6	2607:f0d0:1002:51::4	2300	None	4	26
10007	No	Dialogic-FQDN7	IPv6	2608:f0d0:1002:61::4	6060	TLS	3	27
10008	No	Dialogic-FQDN8	IPv6	2607:f1d0:2012:81::8	5651	UDP	2	28
10009	No	Dialogic-FQDN9	IPv6	1607:e3f0:2013:71::1	1001	TCP	1	29
10010	No	Dialogic-FQDN10 Dialogic-FQDN101 Dialogic-FQDN102	IPv6	1817:23e0:e0f3:c1::e	2762	None	0	30

8.2.3 Delete Local DNS Sample File

Delete LocalDns							
Id							
10001							
10002							
10003							
10004							
10005							
10006							
10007							
10008							
10009							
10010							

8.3 Peer Sample Files

8.3.1 Add Peer Sample File

Note:

This file is split in half to show complete data.

Add Peer

Id	Status	Name	Class ID	Network Type	IMS	Subscriber Traffic	Source Type	Source List
	Yes	DialogicPeer1	dialogic.com	Local	No	No	Single	IPv4,192.45.22.56/,5061
	Yes	DialogicPeer2	dialogic.com	Interconnect	No	No	Single	IPv4,192.50.65.22/,2071
	Yes	DialogicPeer3	dialogic.com	Interconnect	Yes	No	Single	IPv6,2607:f0d0:1002:51::4/,2071
	Yes	DialogicPeer4	dialogic.com	Access-Public	Yes	Yes	Group	IPv6,2607:f0d0:1012:51::4/,2871 IPv6,2807:f0d0:e002:51::4/,2271
	Yes	DialogicPeer5	dialogic.com	Access-Local	Yes	Yes	Group	IPv6,2607:f0d1:1015:51::4/, IPv6,2807:e0d4:1035:51::4/,
	Yes	DialogicPeer6	dialogic.com	Access-Interconnect	Yes	Yes	Group	IPv4,192.51.75.32/,3071 IPv4,192.55.75.62/,
	Yes	DialogicPeer7	dialogic.com	Local	No	Yes	Single	IPv4,56.22.47.101/,5427
	Yes	DialogicPeer8	dialogic.com	Interconnect	No	Yes	Single	IPv6,2407:e0d0:1702:81::2/,4088
	Yes	DialogicPeer9	dialogic.com	Interconnect	No	No	Single	IPv4,58.122.32.119/,5066
	Yes	DialogicPeer10	dialogic.com	Local	No	No	Single	IPv4,62.134.77.83/,2792

Trust Level	Destination FQDN/IP	Protocol	Local Operator Id	Time Zone	TGRP ID	Enforce ipsec	Parameter Profile	Media Profile	Service Profile	Security Profile
High	IPv4,10.5.210.100,5063	TLS		US/Pacific		No	Default	Default	Default	Default
Medium	FQDN,dialogic.com,5062	UDP TLS		US/Pacific		No	Default	Default	Default	Default
Low	IPv4,10.5.210.120,5766	TCP	Dialogic	US/Pacific		No	Default	Default	Default	Default
High	FQDN,dialogic.com,5162	UDP	Dialogic	US/Pacific		No				
High	IPv6,2807:e0d4:1035:51::4,5921	UDP	Dialogic	US/Pacific		No				
High	FQDN,dialogic.com,5088	UDP	Dialogic	US/Pacific		No				
Medium	IPv4,192.168.1.22,5266	TLS		US/Pacific		No	Default	thien	Default	Default
Low	IPv6,2827:e1d4:1045:2e::8,5537	TCP UDP		US/Pacific		No	Default	Default	Default	Default
Low	IPv4,192.168.2.57,5401	TCP		US/Pacific		No	Default	Default	Default	Default
Medium	IPv4,162.178.20.157,5401	TCP		US/Pacific		No	Default	Default	Default	Default

8.3.2 Update Peer Sample File

Note:

This file is split in half to show complete data.

Update Peer
Version="d05dcf32b2817b1993f22e5089445de9566469e4"

Id	Status	Name	Class ID	Network Type	IMS	Subscriber Traffic	Source Type	Source List
21	Yes	DialogicPeer1	dialogic.com	Local	No	No	Single	IPv4,192.45.22.56/,5061
31	Yes	DialogicPeer2	dialogic.com	Interconnect	No	No	Single	IPv4,192.50.65.22/,2071
41	Yes	DialogicPeer3	dialogic.com	Interconnect	Yes	No	Single	IPv6,2607:f0d0:1002:51::4/,2071
51	Yes	DialogicPeer4	dialogic.com	Access-Public	Yes	Yes	Group	IPv6,2607:f0d0:1012:51::4/,2871 IPv6,2807:f0d0:e002:51::4/,2271
61	Yes	DialogicPeer5	dialogic.com	Access-Local	Yes	Yes	Group	IPv6,2607:f0d1:1015:51::4/, IPv6,2807:e0d4:1035:51::4/,
71	Yes	DialogicPeer6	dialogic.com	Access-Interconnect	Yes	Yes	Group	IPv4,192.51.75.32/,3071 IPv4,192.55.75.62/,
81	Yes	DialogicPeer7	dialogic.com	Local	No	Yes	Single	IPv4,56.22.47.101/,5427
91	Yes	DialogicPeer8	dialogic.com	Interconnect	No	Yes	Single	IPv6,2407:e0d0:1702:81::2/,4088
101	Yes	DialogicPeer9	dialogic.com	Interconnect	No	No	Single	IPv4,58.122.32.119/,5066
111	Yes	DialogicPeer10	dialogic.com	Local	No	No	Single	IPv4,62.134.77.83/,2792

Trust Level	Destination FQDN/IP	Protocol	Local Operator Id	Time Zone	TGRP ID	Enforce ipsec	Parameter Profile	Media Profile	Service Profile	Security Profile
High	IPv4,10.5.210.100,5063	TLS		US/Pacific		No	Default	Default	Default	Default
Medium	FQDN,dialogic.com,5062	UDP TLS		US/Pacific		No	Default	Default	Default	Default
Low	IPv4,10.5.210.120,5766	TCP	Dialogic	US/Pacific		No	Default	Default	Default	Default
High	FQDN,dialogic.com,5162	UDP	Dialogic	US/Pacific		No				
High	IPv6,2807:e0d4:1035:51::4,5921	UDP	Dialogic	US/Pacific		No				
High	FQDN,dialogic.com,5088	UDP	Dialogic	US/Pacific		No				
Medium	IPv4,192.168.1.22,5266	TLS		US/Pacific		No	Default	thien	Default	Default
Low	IPv6,2827:e1d4:1045:2e::8,5537	TCP UDP		US/Pacific		No	Default	Default	Default	Default
Low	IPv4,192.168.2.57,5401	TCP		US/Pacific		No	Default	Default	Default	Default
Medium	IPv4,162.178.20.157,5401	TCP		US/Pacific		No	Default	Default	Default	Default

8.3.3 Delete Peer Sample File

Delete Peer	
Id	Name
21	DialogicPeer1
31	DialogicPeer2
41	DialogicPeer3
51	DialogicPeer4
61	DialogicPeer5
71	DialogicPeer6
81	DialogicPeer7
91	DialogicPeer8
101	DialogicPeer9
111	DialogicPeer10

8.4 Interface Sample Files

8.4.1 Add Interface Sample

Note:

This file is split in half to show complete data.

Add Interface													
Id	Status	Name	Domain	Network Type	SIPconnect	SIPconnect Type	IMS	Subscriber Traffic	Access Type	Transport IP Address Type	Signaling IP	VLAN Name
	No	DialogicIntf1	dialogic.com	Interconnect	No	None	No	No	IEEE-802.3	IPv4	192.66.7.22	Test_Vlan
	Yes	DialogicIntf2	dialogic.com	Local	No	None	No	Yes	IEEE-802.3	IPv4	192.66.7.22	Test_Vlan
	Yes	DialogicIntf3	dialogic.com	Interconnect	No	None	No	No	IEEE-802.3	IPv4	192.66.7.22	Test_Vlan
	Yes	DialogicIntf4	dialogic.com	Interconnect	No	None	No	Yes	IEEE-802.3	IPv4	192.66.7.22	Test_Vlan
	Yes	DialogicIntf5	dialogic.com	Interconnect	No	None	No	No	IEEE-802.3	IPv4	192.66.7.22	Test_Vlan
	Yes	DialogicIntf6	dialogic.com	Interconnect	No	None	No	No	IEEE-802.3	IPv6	b307:fed0:1032:51::c	Test_Vlan2
	Yes	DialogicIntf7	dialogic.com	Local	No	None	Yes	No	IEEE-802.3	IPv6	b307:fed0:1032:51::c	Test_Vlan2
	Yes	DialogicIntf8	dialogic.com	Local	No	None	Yes	Yes	IEEE-802.3	IPv6	b307:fed0:1032:51::c	Test_Vlan2
	Yes	DialogicIntf9	dialogic.com	Interconnect	No	None	Yes	No	IEEE-802.3	IPv6	b307:fed0:1032:51::c	Test_Vlan2
	Yes	DialogicIntf10	dialogic.com	Interconnect	No	None	No	No	IEEE-802.3	IPv6	b307:fed0:1032:51::c	Test_Vlan2

| Signaling Port	Signaling Pro	Signaling TOS	TGRP Cont	Enforce ipsec	Parameter Pr	Media Pro	Service Pr	Security Pr	Associated Pe	Trust Level	Local Oper	TLS Prof	Time Zone
5081	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	High			
5422	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Medium			America/Anguilla
5701	UDP	0	dialogic	No	Default	Default	Default	Default	Yes	High			America/Anguilla
5882	UDP	0	dialogic	No	Default	Default	Default	Default	Yes	High			America/Anguilla
5329	UDP	0	dialogic	No	Default	Default	Default	Default	Yes	High			America/Anguilla
5901	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Low			America/Anguilla
3120	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Low	dialogic		America/Anguilla
5472	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Medium	dialogic		America/Anguilla
5582	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Medium	dialogic		America/Anguilla
5327	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Medium			America/Anguilla

8.4.2 Update Interface Sample

Note:

This file is split in half to show complete data.

Update Interface
Version="a1ed094fd79cb5b440d8c8b8107326e53556535a"

Id	Status	Name	Domain	Network Type	SIPconnect	SIPconnect Type	IMS	Subscriber Traffic	Access Type	Transport IP Address Type	Signaling IP	VLAN Name
11	No	DialogicIntf1	dialogic.com	Interconnect	No	None	No	No	IEEE-802.3	IPv4	192.66.7.22	Test_Vlan
21	Yes	DialogicIntf2	dialogic.com	Local	No	None	No	Yes	IEEE-802.3	IPv4	192.66.7.22	Test_Vlan
31	Yes	DialogicIntf3	dialogic.com	Interconnect	No	None	No	No	IEEE-802.3	IPv4	192.66.7.22	Test_Vlan
41	Yes	DialogicIntf4	dialogic.com	Interconnect	No	None	No	Yes	IEEE-802.3	IPv4	192.66.7.22	Test_Vlan
51	Yes	DialogicIntf5	dialogic.com	Interconnect	No	None	No	No	IEEE-802.3	IPv4	192.66.7.22	Test_Vlan
61	Yes	DialogicIntf6	dialogic.com	Interconnect	No	None	No	No	IEEE-802.3	IPv6	b307:fed0:1032:51::c	Test_Vlan2
71	Yes	DialogicIntf7	dialogic.com	Local	No	None	Yes	No	IEEE-802.3	IPv6	b307:fed0:1032:51::c	Test_Vlan2
81	Yes	DialogicIntf8	dialogic.com	Local	No	None	Yes	Yes	IEEE-802.3	IPv6	b307:fed0:1032:51::c	Test_Vlan2
91	Yes	DialogicIntf9	dialogic.com	Interconnect	No	None	Yes	No	IEEE-802.3	IPv6	b307:fed0:1032:51::c	Test_Vlan2
101	Yes	DialogicIntf10	dialogic.com	Interconnect	No	None	No	No	IEEE-802.3	IPv6	b307:fed0:1032:51::c	Test_Vlan2

Signaling Port	Signaling Pro	Signaling TOS	TGRP Cont	Enforce ipsec	Parameter Pr	Media Pr	Service Pr	Security Pr	Associated Pee	Trust Level	Local Opera	TLS Pro	Time Zone
5081	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	High			
5422	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Medium			America/Anguilla
5701	UDP	0	dialogic	No	Default	Default	Default	Default	Yes	High			America/Anguilla
5882	UDP	0	dialogic	No	Default	Default	Default	Default	Yes	High			America/Anguilla
5329	UDP	0	dialogic	No	Default	Default	Default	Default	Yes	High			America/Anguilla
5901	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Low			America/Anguilla
3120	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Low	dialogic		America/Anguilla
5472	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Medium	dialogic		America/Anguilla
5582	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Medium	dialogic		America/Anguilla
5327	UDP-TCP	0	dialogic	No	Default	Default	Default	Default	No	Medium			America/Anguilla

8.4.3 Delete Interface Sample

Delete Interface

Id	Name
11	DialogicIntf1
21	DialogicIntf2
31	DialogicIntf3
41	DialogicIntf4
51	DialogicIntf5
61	DialogicIntf6
71	DialogicIntf7
81	DialogicIntf8
91	DialogicIntf9
101	DialogicIntf10

8.5 Interface-Peer Sample Files

8.5.1 Add Interface-Peer Sample

Add Interface-Peer

Id	Status	Peer	Interface	Connectivity Feature
10010	Yes	DialogicPeer1	DialogicIntf2	Yes
10011	Yes	DialogicPeer2	DialogicIntf1	Yes
10012	Yes	DialogicPeer3	DialogicIntf3	No
10013	Yes	DialogicPeer3	DialogicIntf5	No
10014	Yes	DialogicPeer8	DialogicIntf10	No
10015	Yes	DialogicPeer8	DialogicIntf6	Yes
10016	Yes	DialogicPeer9	DialogicIntf3	Yes
10017	Yes	DialogicPeer9	DialogicIntf4	Yes
10018	Yes	DialogicPeer2	DialogicIntf9	Yes

8.5.2 Update Interface-Peer Sample

Update Interface-Peer				
Version="98874715a995279f85e9e946a312391edd83c379"				
Id	Status	Peer	Interface	Connectivity Feature
10010	No	DialogicPeer1	DialogicIntf2	Yes
10011	No	DialogicPeer2	DialogicIntf1	Yes
10012	No	DialogicPeer3	DialogicIntf3	No
10013	No	DialogicPeer3	DialogicIntf5	No
10014	No	DialogicPeer8	DialogicIntf10	No
10015	No	DialogicPeer8	DialogicIntf6	Yes
10016	No	DialogicPeer9	DialogicIntf3	Yes
10017	No	DialogicPeer9	DialogicIntf4	Yes
10018	No	DialogicPeer2	DialogicIntf9	Yes

8.5.3 Delete Interface-Peer Sample

Delete Interface-Peer
Id
10010
10011
10012
10013
10014
10015
10016
10017
10018

8.6 Rule Treatment Sample Files

8.6.1 Add Policy Sample

Add Policy									
Policy	No	RuleTreatmentSamples		20001 ;					
Rule	Yes	CallingPartyURIScheme	IsEqualTo	URIList:SIPS,TEL	{	Treatment	Flow Class	White	}
Rule	Yes	CallingPartyDomainName	BeginsWith	StringList:408,409	{	Treatment	Flow Class	Grey	}
Rule	Yes	CalledPartyDomainName	EndsWith	StringList:917,273	{	Treatment	Flow Class	White	}
Rule	Yes	CalledPartyURIScheme	IsEqualTo	URIList:TEL	{	Treatment	Flow Class	White	}
Rule	Yes	CPC	IsEqualTo	CPCList:Hospital	{	Treatment	Flow Class	Grey	}
Rule	Yes	DestinationDomain	BeginsWith	StringList:411	{	Treatment	Flow Class	Grey	}
Rule	Yes	DestinationTGRPId	Contains	StringList:207	{	Treatment	Flow Class	White	}
Rule	Yes	DestinationTGRPContext	AssignsFrom	Parameter:CallingPartyURIScheme	{	Treatment	Flow Class	Grey	}
Rule	Yes	RegisteringIdentityDomain	IsNotEqualTo	ParameterList:CPC	{	Treatment	Flow Class	White	}
Rule	Yes	MessageRouting	IsPresent	Boolean:Yes	{	Treatment	Flow Class	White	}

8.6.2 Update Policy Sample

Update Policy									
Version="1ad2995cb42ca925fe36060dc5e885fd0c6eb70b"									
Policy	No	RuleTreatmentSamples		20001 ;					
Rule	Yes	CallingPartyURIScheme	IsEqualTo	URIList:SIPS,TEL	{	Treatment	Flow Class	White	}
Rule	Yes	CallingPartyDomainName	BeginsWith	StringList:408,409	{	Treatment	Flow Class	Grey	}
Rule	Yes	CalledPartyDomainName	EndsWith	StringList:917,273	{	Treatment	Flow Class	White	}
Rule	Yes	CalledPartyURIScheme	IsEqualTo	URIList:TEL	{	Treatment	Flow Class	White	}
Rule	Yes	CPC	IsEqualTo	CPCList:Hospital	{	Treatment	Flow Class	Grey	}
Rule	Yes	DestinationDomain	BeginsWith	StringList:411	{	Treatment	Flow Class	Grey	}
Rule	Yes	DestinationTGRPId	Contains	StringList:207	{	Treatment	Flow Class	White	}
Rule	Yes	DestinationTGRPContext	AssignsFrom	Parameter:CallingPartyURIScheme	{	Treatment	Flow Class	Grey	}
Rule	Yes	RegisteringIdentityDomain	IsNotEqualTo	ParameterList:CPC	{	Treatment	Flow Class	White	}
Rule	Yes	MessageRouting	IsPresent	Boolean:Yes	{	Treatment	Flow Class	White	}

END OF DOCUMENT