
Ribbon SBC Core Interop with ATOS LIOS for PC2.0 LI : Interoperability Guide



Table of Contents

- [Interoperable Vendors](#)
- [Copyright](#)
- [Document Overview](#)
- [Scope](#)
- [Non-Goals](#)
- [Introduction](#)
- [Audience](#)
- [Product and Device Details](#)
- [Network Topology Diagram](#)
 - [Deployment Topology](#)
 - [Interoperability Test Lab Topology](#)
- [SBC Configuration](#)
 - [Diameter Node](#)
 - [Enable the Calea user](#)
 - [Call Data Channel](#)
 - [Enabling remote PSX server](#)
- [PSX Configuration](#)
- [EMS Configuration](#)
- [ATOS ADMF/DF2/DF3 Configuration](#)
 - [To generate self-signed certificate](#)
 - [Target creation example](#)
 - [Sample surveillances](#)
 - [Surveillance Creation](#)
 - [Surveillance Deletion](#)
 - [Surveillance Audit](#)
- [Supplementary Services & Features Coverage](#)
- [Caveats](#)
- [Support](#)
- [References](#)
- [Conclusion](#)

Interoperable Vendors



Copyright

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved. The compilation (meaning the collection, arrangement and assembly) of all content on this site is protected by U.S. and international copyright laws and treaty provisions and may not be used, copied, reproduced, modified, published, uploaded, posted, transmitted or distributed in any way, without prior written consent of Ribbon Communications Inc.

The trademarks, logos, service marks, trade names, and trade dress ("look and feel") on this website, including without limitation the RIBBON and RIBBON logo marks, are protected by applicable US and foreign trademark rights and other proprietary rights and are the property of Ribbon Communications Operating Company, Inc. or its affiliates. Any third-party trademarks, logos, service marks, trade names and trade dress may be the property of their respective owners. Any uses of the trademarks, logos, service marks, trade names, and trade dress without the prior written consent of Ribbon Communications Operating Company, Inc., its affiliates, or the third parties that own the proprietary rights, are expressly prohibited.

Document Overview

This document provides a configuration guide for Ribbon Solution (SBC/PSX) with ATOS LIOS PC2.0LI

- For additional information on Ribbon SBC, refer to <https://ribboncommunications.com/>

Scope

This document provides the Ribbon Solution (SBC/PSX/EMS) Core configuration for performing PC2.0 LI with ATOS LIOS. This is a general reference document that requires user input during the configuration. For PSX/SBC configurations, the screen captures in this document are limited to only necessary provisioning areas.

Non-Goals

This document does not provide the test cases details, the success criteria, processes and execution steps of testing that were performed. Also, this document does not focus on general EMA/PSX configurations and provisioning areas.

Introduction

Lawful Intercept (LI) flavor PC2.0 Interop testing is performed between Ribbon's Solution (EMS/SBC/PSX) and ATOS LIOS LIMA platform. This document outlines the SBC, PSX and EMS configurations required to achieve this purpose.

Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring the Ribbon Products(SBC/PSX/EMS).

To perform this interop, you need:

- to use graphical user interface (GUI) or command line interface (CLI) of the Ribbon products.
- to understand the basic concepts of TCP/UDP/TLS and IP/Routing.
- to have SIP/RTP/SRTP to complete the configuration and for troubleshooting.



Note

This configuration guide is offered as a convenience to Ribbon customers. The specifications and information regarding the product in this guide are subject to change without notice. All statements, information, and recommendations in this guide are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided "AS IS". Users must take full responsibility for the application of the specifications and information in this guide.

Product and Device Details

The configuration uses the following equipment and software:

Table 1: Requirements

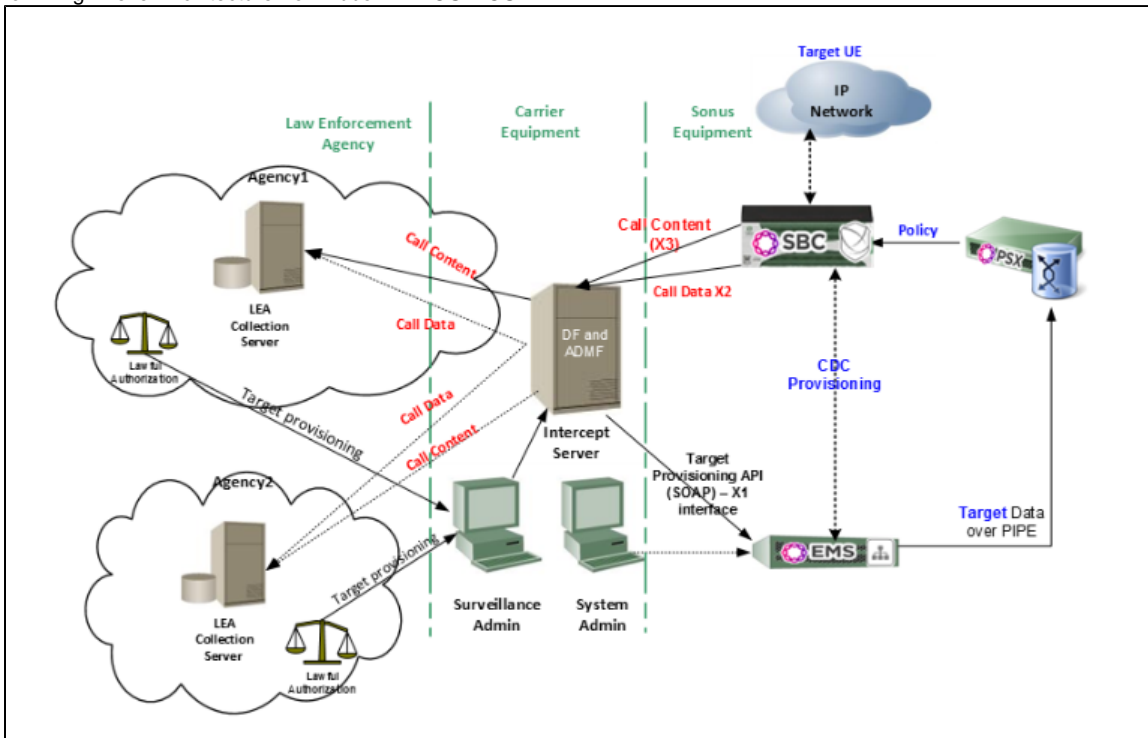
Product	Equipment	Software Version
Ribbon Communications	Ribbon SBC	V10.00.00-R000
	Ribbon PSX	V12.02.02-R000
	Ribbon EMS	V14.00.00-R000
ATOS LIOS	ADMF	N/A
	DF2	N/A
	DF3	N/A

Network Topology Diagram

The following figure illustrates connectivity between the ATOS LIMA platform and Ribbon via VPN tunnel.

Deployment Topology

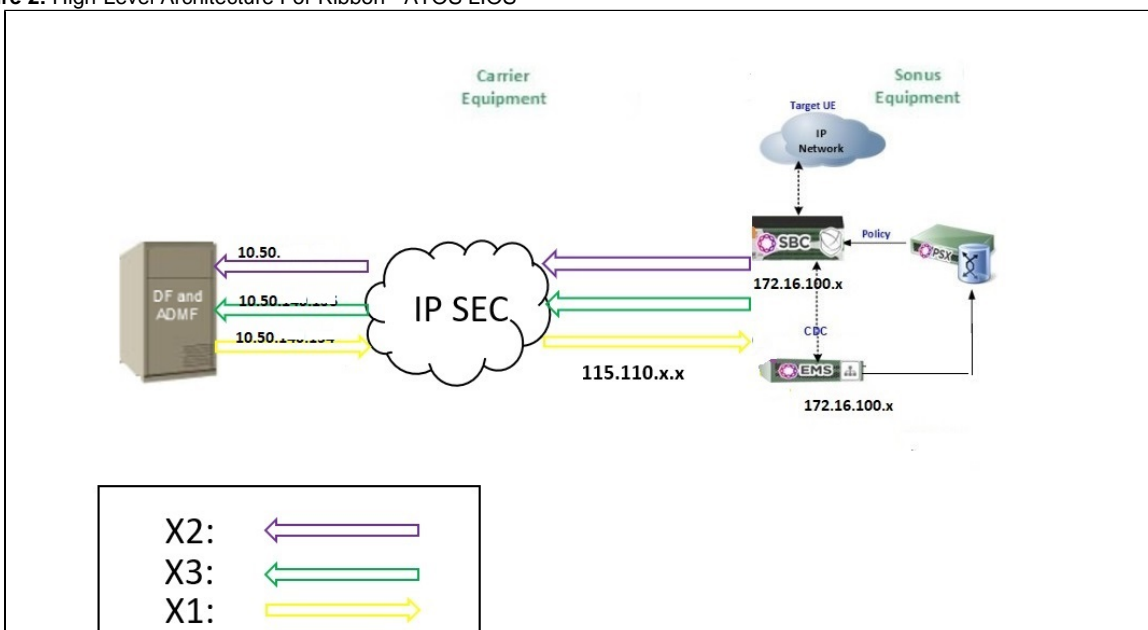
Figure 1: High-Level Architecture For Ribbon - ATOS LIOS



Interoperability Test Lab Topology

The following lab topology diagram shows connectivity between Ribbon and ATOS LIMA via the IP Sec tunnel.

Figure 2: High-Level Architecture For Ribbon - ATOS LIOS



SBC Configuration



This section provides the SBC configurations specific to LI only.

It will not cover any configurations such as ipInterfaceGroup/zone/sipSigPort/sipTrunkGroup/staticRoute.

For all the above configurations, please refer to the standard SBC configuration guide in the [SBC Core Documentation](#).

Diameter Node

Create diameter node and specify the IP Interface Group name and IP address. The SBC uses this IP address to send the x2/x3 data towards ATOS LIOS after interception.

```
set addressContext default diamNode dNode originRealm sonus.com primaryOriginHost pl.sonus.com
ipInterfaceGroupName UNTRUST state enabled dumpPdu enabled ipv4Address x.x.x.x
commit
```

When the SBC is in HA mode, use the following diameter code.

```
set addressContext default diamNode dNode originRealm sonus.com primaryOriginHost pl.sonus.com
ipInterfaceGroupName UNTRUST secondaryOriginHost p2.sonus.com state enabled dumpPdu enabled ipv4Address x.x.x.x
commit
```

Enable the Calea user

Through the admin login, create the calea user. Change your password after the first login.

```
set oam localAuth user calea group Calea
commit
```

Call Data Channel



Note

This step should be performed using a calea user.

```
admin@SBCNAME% ssh calea@0
```

Create a Call Data Channel based on the configurations provided by ATOS LIOS. These are the LIMA platform IP and FQDN's for the x2/x3 reception.

In this example,

- The df group name is df21.
- The realm name is lios1.com.
- The peer fqdn is df21.lios1.com.
- The x2 data is sent to the IP 1.1.1.1
- The x3 data is sent to the IP 1.1.1.2 and port number 61318.

```
set addressContext default intercept callDataChannel CDC ipInterfaceGroupName UNTRUST mediaIpInterfaceGroupName
UNTRUST
set addressContext default intercept callDataChannel CDC interceptStandard packetcableVTwo
set addressContext default intercept callDataChannel CDC vendorId atos
set addressContext default intercept callDataChannel CDC diamNode dNode
set addressContext default intercept callDataChannel CDC mediationServer MS1 signaling
set addressContext default intercept callDataChannel CDC mediationServer MS1 signaling dfGroupName df21
set addressContext default intercept callDataChannel CDC mediationServer MS1 signaling realmName lios1.com
set addressContext default intercept callDataChannel CDC mediationServer MS1 signaling mode inService
set addressContext default intercept callDataChannel CDC mediationServer MS1 signaling state enabled
set addressContext default intercept callDataChannel CDC mediationServer MS1 media udp
set addressContext default intercept callDataChannel CDC mediationServer MS1 media udp ipAddress 1.1.1.2
set addressContext default intercept callDataChannel CDC mediationServer MS1 media udp portNumber 61318
set addressContext default intercept callDataChannel CDC diameterPeer Peer1 fqdn df21.lios1.com ipAddress 1.1.1.1
```

```

set addressContext default intercept callDataChannel CDC diameterPeer Peer1 deviceWatchdogTimer 10000
set addressContext default intercept callDataChannel CDC diameterPeer Peer1 state enabled
set addressContext default intercept callDataChannel CDC diameterRealmRoute Peer1 realm lios1.com diameterPeer
Peer1
set addressContext default intercept callDataChannel CDC diameterRealmRoute Peer1 appId x2
set addressContext default intercept callDataChannel CDC diameterRealmRoute Peer1 state enabled
commit

```

Enabling remote PSX server



Note

For this release, it is mandatory to enable the External PSX for Routing.

Use the following command to disable the local PSX server, and then enable the remote PSX server.

```

% set system policyServer localServer "PSX_LOCAL_SERVER" state "disabled" mode "outOfService"
% commit
% set system policyServer remoteServer "ATOSPSX" ipAddress "<PSX_MGMT_IP>" state "enabled" mode "active"
% commit

```

PSX Configuration

There are no specific PSX configurations required for this feature to run. Please refer the standard Ribbon PSX guide for generic configurations on <https://doc.rbbn.com/>.

EMS Configuration

Please refer the page [Lawful Intercept](#) for the configurations related to EMS for this deployment.

ATOS ADMF/DF2/DF3 Configuration

For configurations related to ATOS LIOS products, please contact ATOS technical support team on <https://atos.net/en/>.

To generate self-signed certificate

In order to generate a self-signed certificate to be used in X1 requests, log in to the EMS and perform the following steps:

```

Go to /opt/sonus/ems/weblogic/sonusEms/data/sys
keytool -export -alias demo -keystore ems.keystore -rfc -file <filename>.cert
(give the password as sonusems)

```

Target creation example

The following example provides the targets created on the EMS.

Figure 3: Created targets

Results									
Number of Surveillances : 6									
Device Name	Tap Id	PNI	txCcDfName	txCcDfPort	rxCcDfName	rxCcDfPort	Target ID	cdDfGroupName	
atosems	000010*8888	true	10. .156	61318	10. .156	61319	*8888	df21	
atosems	0000108888*	true	10. .156	61318	10. .156	61319	8888*	df21	
atosems	000010A*5559995100	true	10. .156	61318	10. .156	61319	*5559995100	df21	
atosems	000010A5*	true	10. .156	61318	10. .156	61319	5*	df21	

Sample surveillances

The following section lists sample surveillances that are performed in this interop.

Surveillance Creation

X1 Request

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="https://clicktime.symantec.com/39LLLiWRL9DgHq1VYdSV9xe6H2?u=http%3A%2F%2Fschemas.xmlsoap.org%2Fsoap%2Fenvelope%2F%26quot;
    xmlns:xsd="https://clicktime.symantec.com/3UFwpPT2WYij6j5hktZLiZv6H2?u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema%26quot;
    xmlns:xsi="https://clicktime.symantec.com/3GYLvhbfc3of1CQNNiBk8nQ6H2?u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema-instance%2522%253E
    <soapenv:Body>
        <editConfig xmlns="https://clicktime.symantec.com/3UZ1FDi5JnuM22F33kTVxmQ6H2?u=http%3A%2F%2Fwww.nextone.com%2Ffivms%2Fschema%2Fconfig%2522%253E
            <config>
                <ns1:credential xmlns:ns1="https://clicktime.symantec.com/3QGARvuvAZc6ZQekbZzmdHK6H2?u=http%3A%2F%2Fwww.nextone.com%2Ffivms%2Fschema%2Fcommon%2522%253E
                    <ns1:user>calea</ns1:user>
                    <ns1:password>calea</ns1:password>
                </ns1:credential>
                <surveillanceConfig command="addSurveillance">
                    <Surveillance>
                        <deviceName>atosems</deviceName>
                        <pni>true</pni>
                        <txCcDfName><name>1.1.1.1</name></txCcDfName>
                        <txCcDfPort>61318</txCcDfPort>
                        <rxCcDfName><name>1.1.1.1</name></rxCcDfName>
                        <rxCcDfPort>61319</rxCcDfPort>
                        <targetId><name>7774446100</name></targetId>
                        <cdDfGroupName><name>df21</name></cdDfGroupName>
                        <tapId><name>000010A7774446100</name></tapId>
                    </Surveillance>
                </surveillanceConfig>
            </config>
            <ns2:errorOption xmlns:ns2="https://clicktime.symantec.com/3KFlzM1MekJH9rPh54egmmQ6H2u=http%3A%2F%2Fwww.nextone.com%2Ffivms%2Fschema%2Fcommon%2522%253Eignore-error%253C%2Fns2%3AerrorOption%253E
        </editConfig>
    </soapenv:Body>
</soapenv:Envelope>
```

X1 Response

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="https://clicktime.symantec.com/39LLLiWRL9DgHq1VYdSV9xe6H2?u=http%3A%2F%2Fschemas.xmlsoap.org%2Fsoap%2Fenvelope%2F%26quot;
    xmlns:xsd="https://clicktime.symantec.com/3UFwpPT2WYij6j5hktZLiZv6H2?u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema%26quot;
    xmlns:xsi="https://clicktime.symantec.com/3GYLvhbfc3of1CQNNiBk8nQ6H2?u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema-instance%2522%253E
    <soapenv:Body>
        <reply xmlns="https://clicktime.symantec.com/3UZ1FDi5JnuM22F33kTVxmQ6H2?u=http%3A%2F%2Fwww.nextone.com%2Ffivms%2Fschema%2Fconfig%2522%253E
            <ok xmlns="">ok</ok>
        </reply>
    </soapenv:Body>
</soapenv:Envelope>
```

Surveillance Deletion

X1 Request

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="https://clicktime.symantec.com/39LLLiWRL9DgHq1VYdSV9xe6H2?u=http%3A%2F%2Fschemas.xmlsoap.org%2Fsoap%2Fenvelope%2F%26quot;
    xmlns:xsd="
https://clicktime.symantec.com/3UFwpPT2WYij6j5hktZLiZv6H2?u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema%26quot;
    xmlns:xsi="
https://clicktime.symantec.com/3GYLvhbfc3of1CQNNiBk8nQ6H2?u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema-instance%2522%253E
```

```

<soapenv:Body>
  <editConfig xmlns="https://clicktime.symantec.com/3UZ1FDi5JnuM22F33kTVxmQ6H2?
u=http%3A%2F%2Fwww.nextone.com%2Fivms%2Fschema%2Fconfig%2522%253E
  <config>
    <ns1:credential xmlns:ns1="https://clicktime.
symantec.com/3QGARvuwAZc6ZQekbZzmdHK6H2?u=http%3A%2F%2Fwww.nextone.com%2Fivms%2Fschema%2Fcommon%2522%253E
      <ns1:user>calea</ns1:user>
      <ns1:password>calea</ns1:password>
    </ns1:credential>
    <surveillanceConfig command="removeSurveillance">
      <Surveillance>
        <deviceName>atosems</deviceName>
        <pni>false</pni>
        <txCcDfName xsi:
nil="true"/>
        <txCcDfPort xsi:
nil="true"/>
        <rxCcDfName xsi:
nil="true"/>
        <rxCcDfPort xsi:
nil="true"/>
        <targetId xsi:nil="
true"/>
        <cdDfGroupName xsi:
nil="true"/>
      </Surveillance>
    </surveillanceConfig>
  </config>
  <ns2:errorOption xmlns:ns2="https://clicktime.symantec.com
/3KF1zM1MekJH9rPh54egmmQ6H2?u=http%3A%2F%2Fwww.nextone.com%2Fivms%2Fschema%2Fcommon%2522%253Eignore-error%253C%
2Fns2%3AerrorOption%253E
  </editConfig>
</soapenv:Body>
</soapenv:Envelope>

```

X1 Response

```

<soapenv:Envelope xmlns:soapenv="https://clicktime.symantec.com/39LLLiWRL9DgHq1VYdSV9xe6H2?u=http%3A%2F%2Fschemas.
xmlsoap.org%2Fsoap%2Fenvelope%2F%26quot;
  xmlns:xsd="
https://clicktime.symantec.com/3UFwpPT2WYij6j5hktZLiZv6H2?u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema%26quot;
  xmlns:xsi="https://clicktime.symantec.com/3GYLvhbfc3of1CQNNiBk8nQ6H2?u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema-
instance%2522%253E
  <soapenv:Body>
    <reply xmlns="https://clicktime.symantec.com/3UZ1FDi5JnuM22F33kTVxmQ6H2?u=http%3A%
2F%2Fwww.nextone.com%2Fivms%2Fschema%2Fconfig%2522%253E
      <ok xmlns="">ok</ok>
    </reply>
  </soapenv:Body>
</soapenv:Envelope>

```

Surveillance Audit

X1 Request

```

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="https://clicktime.symantec.com/3RsdQHCP9fzTnT5edfCTDwL6H2?u=http%3A%2F%2Fschemas.
xmlsoap.org%2Fsoap%2Fenvelope%2F%26quot;
  xmlns:xsd="https://clicktime.symantec.com/3AAGgus4JjWjAGQWhaxM4Mk6H2?u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema%
26quot;
  xmlns:xsi="https://clicktime.symantec.com/35YHYa7PMJzvHdu3QGz85876H2?u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema-
instance%2522%253E
  <soapenv:Body>
    <getConfig xmlns="https://clicktime.symantec.com/3Djh1N12YCxqCopsM5HdeWi6H2?u=http%3A%2F%2Fwww.nextone.com%2Fivms%
2Fschema%2Fconfig%2522%253E
      <ns1:credential xmlns:ns1="https://clicktime.symantec.com/3U9HmdznLxQxwzZUDLdq9276H2?u=http%3A%2F%2Fwww.nextone.
com%2Fivms%2Fschema%2Fcommon%2522%253E

```



```

<ns1:user>calea</ns1:user>
<ns1:password>calea</ns1:password>
</ns1:credential>
<SurveillanceFilter sequenceNumber="0">
<deviceName>atosems</deviceName>
<tapId><name>000010A7774446100</name></tapId>
</SurveillanceFilter>
</getConfig>
</soapenv:Body>
</soapenv:Envelope>

X1 Response

<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="https://clicktime.symantec.com/3RsdQHCP9fzTnT5edfCTDwL6H2?u=http%3A%2F%2Fschemas.xmlsoap.org%2Fsoap%2Fenvelope%2F%26quot;
xmlns:xsd="https://clicktime.symantec.com/3AAGgus4JJwjAGQWhaxM4Mk6H2?
u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema%26quot;
xmlns:xsi="https://clicktime.symantec.com/35YHYa7PMJzvHDU3QGz85876H2?
u=http%3A%2F%2Fwww.w3.org%2F2001%2FXMLSchema-instance%2522%253E
<soapenv:Body>
<reply xmlns="https://clicktime.symantec.com/3DjhlN12YCxqCopsM5HdeWi6H2?u=http%3A%2F%2Fwww.nextone.com%2Fivms%2Fschema%2Fconfig%2522%253E
<ok xmlns="">ok</ok>
<SurveillanceConfig>
<deviceName>atosems</deviceName>
<pni>>true</pni>
<txCcDfName><name>1.1.1</name></txCcDfName>
<txCcDfPort>61318</txCcDfPort>
<rxCcDfName><name>1.1.1</name></rxCcDfName>
<rxCcDfPort>61319</rxCcDfPort>
<targetId><name>7774446100</name></targetId>
<cdDfGroupName><name>df21</name></cdDfGroupName>
<tapId><name>000010A7774446100</name></tapId>
</SurveillanceConfig>
</data>
</reply>
</soapenv:Body>
</soapenv:Envelope>

```

Supplementary Services & Features Coverage

The following checklist depicts the set of services/features covered through the configuration defined in this Interop Guide.

Sr. No.	Supplementary Services/ Features	Coverage
1	Registration over UDP	✓
2	Basic Call Setup & Termination	✓
3	Cancel Call, No Answer, Busy and Call Rejection	✓
4	FAX	✗
5	DTMF	✓
6	Call Forward - Unconditional, Busy and No Answer	✓
7	Out of dialog messages (SUBSCRIBE/NOTIFY/OPTIONS)	✓
8	Call Transfer (Refer-relay)	✓
9	Call Hold and Resume	✓
10	Attended Call Transfer	✓

11	Video Call	✓
----	------------	---

Legend

Supported	✓
Not Supported	✗

Caveats

Note the following items in relation to this Interop:

- In this release Ribbon does not accept creation of duplicate targets with different TapID. This functionality is expected to be available in the upcoming releases.
- When adding a surveillances, Ribbon does not check whether the supplied DF Group Name actually is configured in the SBC database. It only checks for the syntax errors.
- When an SBC switchover is performed without any active calls, new calls are not getting intercepted even though targets are present.

Support

For any support related queries about this guide, please contact your local Ribbon representative, or use the details below:

- Sales and Support: 1-833-742-2661
- Other Queries: 1-877-412-8867
- Website: <https://ribboncommunications.com/services/ribbon-support-portal>

References

For detailed information about Ribbon products & solutions, please visit:

<https://ribboncommunications.com/products>

Conclusion

This document describes the configuration steps required for the Ribbon Solution to successfully test interop with ATOS LIOS. All feature and serviceability test cases were completed and passed.

All features and capabilities tested are detailed within this document - any limitations, notes or observations are also recorded in order to provide the reader with an accurate understanding of what has been covered, and what has not.

Configuration guidance is provided to enable the reader to replicate the same base setup - there maybe additional configuration changes required to suit the exact deployment environment.

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved.