

IM&P Federation With Microsoft-based Organizations Skype for Business

12/28/2017

I had set this up in a lab when it was first added as a preview feature and did not document as I should have. When I went to implement for a customer, I of course had to repeat troubleshooting. I have configured this again and wanted to document, so I would not have to face this issue again. Hopefully, it will help someone else who is trying to set this up.

Software versions used in lab:

CUCM – 11.5.1.12900-21

IMP – 11.5.1.12900-25

EXP – X8.10.3


Jabber for Windows – 11.8.5


Skype for Business trial account – test domain bmarley@s4bfed.onmicrosoft.com

Steps to configure on IMP:

1. Presence > Inter-Domain Federation > SIP Federation


Add domain that you want to federate with integration type Inter-Domain to OCS/LYNC/S4B.

 Status: Ready

 **SIP Federated Domain Configuration**

IM and Presence Service can be configured to integrate with a foreign domain (inter-domain federation), allowing the IM and Presence Servi

Domain Name*	<input type="text" value="s4bfed.onmicrosoft.com"/>
Description*	<input type="text" value="s4bfed.onmicrosoft.com"/>
Integration Type*	<input type="text" value="Inter-Domain to OCS/Lync/S4B"/>
Direct Federation	<input type="checkbox"/>

 *- indicates required item.

2. Presence > Routing > Static Routes

Add domain to be routed to next hop Expressway C FQDN. Port 5061

Route type – Domain

Protocol Type – TLS

Status
Status: Ready

Static Route Information

Destination Pattern *	.com.onmicrosoft.s4bfed.*
Description	.com.onmicrosoft.s4bfed.*
Next Hop*	expc.nolalab.lids
Next Hop Port*	5061
Route Type*	Domain
Protocol Type	TLS
Priority*	1
Weight*	1
Allow Less-Specific Route*	On
In Service*	On

Block Route

3. System > Security > Incoming ACL

Add Expressway C FQDN and IP address – 2 entries.

I added the sipfed.online.lync.com as well. This is what the SIP federation SRV record for s4bfed.onmicrosoft.com resolves to.

Incoming ACL Entry (1 - 6 of 6)		
Find Incoming ACL Entry where <u>Address Pattern</u> begins with <input type="text"/> Find Clear Filter <input type="button" value="↕"/> <input type="button" value="←"/>		
<input type="checkbox"/>	Address Pattern ▲	
<input type="checkbox"/>	192.100.64.200	expc.nolalab.lids1
<input type="checkbox"/>	cimphq01.nolalab.lids	System Generated Allow Rule
<input type="checkbox"/>	cucmhq01	System Generated Allow Rule
<input type="checkbox"/>	expc.nolalab.lids	expc.nolalab.lids
<input type="checkbox"/>	s4bfed.onmicrosoft.com	System Generated Allow Rule
<input type="checkbox"/>	sipfed.online.lync.com	sipfed.online.lync.com

4. System > Security > TLS Peer Subjects

Add IP and FQDN of Expressway C and Expressway E

TLS Peer Subject (1 - 5 of 5)		
Find TLS Peer Subject where Peer Subject Name begins with		
<input type="checkbox"/>	Peer Subject Name	
<input type="checkbox"/>	192.100.64.200	192.100.64.200
<input type="checkbox"/>	192.100.64.201	
<input type="checkbox"/>	expc.nolalab.lds	expc.nolalab.lds
<input type="checkbox"/>	expe.504voip.com	
<input type="checkbox"/>	sipfed.online.lync.com	sipfed.online.lync.com

5. System > Security > TLS Context Configuration

Under Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context add the IP and FQDN of Expressway C and E. Also add the sipfed.online.lync.com.

TLS Peer Subject Mapping

Available TLS Peer Subjects

> <

Selected TLS Peer Subjects

192.100.64.201
expc.nolalab.lds
expe.504voip.com
192.100.64.200
sipfed.online.lync.com

6. **System > Service Parameters** Select the IMP node and Cisco SIP Proxy Service. Under Federation Routing Parameters (Clusterwide) Make note of the Federation Routing IM/P FQDN. You will need to create a CNAME internal DNS record which points to the IMP PUB FQDN.

Federation Routing Parameters (Clusterwide)

Federation Routing IM/P FQDN *	cimphq01-public.nolalab.lds
--------------------------------	-----------------------------

```
C:\Users\Administrator>nslookup
```

```
Default Server: UnKnown
```

```
Address: ::1
```

```
> cimphq01-public.nolalab.lds
```

```
Server: UnKnown
```

```
Address: ::1
```

```
Name: cimphq01.nolalab.lds
```

```
Address: 192.100.64.15
```

```
Aliases: cimphq01-public.nolalab.lds
```

7. Certificates!!!!!!!

On IMP, you will need to install the Expressway C server certificate, Root CA of S4B (Baltimore Cybertrust Root), and Root CA that issued the Expressway C server certificate.

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
cup-trust	expc.nolalab.lids	CA-signed	RSA	expc.nolalab.lids	NOLALAB-NOLADC-CA	11/18/2019	Signed Certificate
cup-trust	Baltimore_CyberTrust_Root	Self-signed	RSA	Baltimore_CyberTrust_Root	Baltimore_CyberTrust_Root	05/12/2025	Signed Certificate
cup-trust	cmphq01.nolalab.lids	Self-signed	RSA	cmphq01.nolalab.lids	cmphq01.nolalab.lids	12/21/2022	Trusted local cluster own-certificat
cup-trust	cmphq01-EC.nolalab.lids	Self-signed	EC	cmphq01.nolalab.lids	cmphq01-EC.nolalab.lids	12/21/2022	Trusted local cluster own-certificat
cup-trust	NOLALAB-NOLADC-CA	Self-signed	RSA	NOLALAB-NOLADC-CA	NOLALAB-NOLADC-CA	07/31/2020	Signed Certificate

8. Restart services that were requested. Cisco SIP Proxy, Cisco Presence Engine, and XCP router.

Steps to configure on Expressway C:

1. Add a new Zone

- Type – Traversal Client to the Expressway E.
- SIP Mode – ON
- Port – 7003
- Transport – TLS
- TLS Verify Mode – Off (If your certificates are setup correctly, you can set to on. I left it off to test)
- Peer 1 Address – FQDN of Expressway E
- The other settings I left at default.

2. Add another Zone

- Type – Neighbor Zone to IMP PUB
- SIP Mode – ON
- Port – 5062 Zone will not become active if you use 5061.
- Transport – TLS
- TLS Verify Mode – Off (If your certificates are setup correctly, you can set to on. I left it off to test)
- Peer 1 Address – IMP FQDN
- The other settings I left at default.

3. Add 3 Search Rules

A. IMP Neighbor to Traversal Client

- Protocol – SIP
- SIP Variant – Microsoft SIP IM&P
- Source name – IMP Neighbor Zone
- Mode – Alias Pattern Match
- Pattern Type – Regex
- Pattern String - .*@s4bfed.onmicrosoft\.com
- Pattern Behavior – Leave
- On successful Match – Continue
- Target – Traversal to Expressway E

B. Traversal to Neighbor

- Protocol – SIP
- SIP Variant – Microsoft SIP IM&P
- Source name – Traversal Client
- Mode – Alias Pattern Match
- Pattern Type – Regex
- Pattern String - .*@504voip\.com
- Pattern Behavior – Leave
- On successful Match – Continue
- Target – IMP Neighbor

C. Traversal to Neighbor IMP Public FQDN

- Protocol – SIP
- SIP Variant – Microsoft SIP IM&P
- Source name – Traversal Client
- Mode – Alias Pattern Match
- Pattern Type – Regex
- Pattern String - .*cimphq01-public\.nolalab\.lds.*
- Pattern Behavior – Leave
- On successful Match – Continue
- Target – IMP Neighbor

4. Certificates!!!!

You will need to upload the following to the Expressway C Trusted CA:
Root and/or Intermediate that issued Certificate of Expressway E.
Root that issued Certificate for IMP Tomcat certificate.
Tomcat Certificate of IMP PUB.

Steps to configure on Expressway E:

1. Add Zones

- Type – Traversal Server to the Expressway C.
 - SIP Mode – ON
 - Port – 7003
 - Transport – TLS
 - TLS Verify Mode – Off (If your certificates are setup correctly, you can set to on. I left it off to test)
 - The other settings I left at default.
- Add DNS ZONE if one does not already exist.

2. Add 3 Search Rules

A. Traversal Server to DNS 1

- Protocol – SIP
- SIP Variant – Microsoft SIP IM&P
- Source name – Traversal Server
- Mode – Alias Pattern Match
- Pattern Type – Regex
- Pattern String - .*@s4bfed.onmicrosoft\.com
- Pattern Behavior – Leave
- On successful Match – Continue
- Target – DNS

B. Traversal Server to DNS 2

- Protocol – SIP
- SIP Variant – All SIP Variants
- Source name – Traversal Server
- Mode – Any Alias
- On successful Match – Continue
- Target – DNS

C. Default to Traversal Server

- Protocol – SIP
- SIP Variant – Microsoft SIP IM&P
- Source name – Default Zone
- Mode – Alias Pattern Match
- Pattern Type – Regex
- Pattern String - .*@504voip\.com
- Pattern Behavior – Leave
- On successful Match – Continue
- Target – Traversal Server

3. Certificates!!!!

You will need to upload the following to the Expressway E Trusted CA:

Root and/or Intermediate that issued Certificate of Expressway C and E.

Root for S4B – Baltimore Cybertrust Root