Introduction

When key employees are out of touch, even for a few moments, the business can suffer in many ways. Avaya “IP Office One-X Mobile Preferred” gives employees on the go, the communications capabilities needed to keep them connected and ready to do business on virtually any device. This whitepaper aims at explaining the setup of IP Office One-X Mobile Preferred. It is assumed that the IP Office and One-X Portal for IP Office Server are operational.
System Requirements

- One-X Portal Server/Service 9.0+
- Voicemail Pro (Preferred) 9.0+

Licensing
- IP Office Preferred System License
- One Mobile Worker or Power User License per client
- No need for IP Office End Point License in VoIP Mode

Trunk Support
- Trunks that support clearing supervision
- IP500 Universal PRI (Not Carrier/Legacy)
- IP500BRI
- SIP
- No Loop Start Analog

Supported Devices

One-X Mobile preferred mobility client will support VoIP mode on both iOS and Android devices
- iPhones – 4, 4S & 5 OS 5.0+ (Apple App store)
- Android - OS 4.0+ (Google Play Store)
- Flare Experience for iPad
- Flare Experience for Windows

- Server Edition runs 3 services - IP Office, VMPRO & One-X Portal. It only supports Power User license. The Mobile User license is unavailable

- Ensure users are able to login to one-X Portal http://IPAddress_OneXPortal:8080/onexportal.html from any PC on the network

- On Android the following have been tested for acoustic performance - Samsung Galaxy S3, S4, Note2, LG Optimus E975 and HTC One-S
Avaya one-X Mobile Preferred application must be able to connect through the Internet to Avaya one-X® Portal and to the IP Office, using either a 3G network or an external Wi-Fi. If you deploy Avaya one-X® Portal and IP Office behind a router or firewall, ensure that the correct TCP ports can gain access through the firewall by creating port forwarding rules on the Firewall/Router.
You must assign an FQDN to the public IP address of the router fronting Avaya one-X® Portal that is resolvable over the Internet.

SIP & RTP Ports are “not set in stone”; they can be configured to fit customer’s network requirements.

DNS and Remote SIP Worker are the pillars of seamless roaming inside and outside corporate office.

Why Split DNS?

- A Split-DNS provides alternative DNS resolution of public DNS names on local network
- Only needed if roaming is required (Internal network / public network)
  - If no roaming is required?
    - Use local IP addresses for local non-roaming clients
    - Use public DNS or public IP address for public-side-only clients
- Allows local clients to contact One-X/IP Office directly and avoid hairpinning
- Router Hairpinning can sometimes be an issue with VoIP clients (bad quality speech etc.)
Client Registration to One-X Portal FQDN

**Phone inside the office using Corporate WiFI:**

**Step 1:** Phone queries the DNS server for Fully Qualified Domain Name (FQDN) of OnexPortal Server.
  - DNS returns IP Address of the OnexPortal Server.

**Step 2:** Phone sends encrypted messages to OneXPortal Server on Port 8444 (bootstrap REST API call traffic) to query about Presence & SIP FQDN.

**Step 3:** OneXPortal sends encrypted messages to IP Office on Port 8443 (Windows) or Port 9443 (Linux).

**Step 4:** OneXPortal relays response back to Phone using Port 8444.
Step 5: Phone registers to OneXPortal server using XMPP Ports 5222 over TLS (secure).

Android

Apple

1. Home screen showing call facility as "Work" by default, tap this Call Facility icon to show VoIP & Call-Back radio buttons

2. Upon tapping Call facility icon, Call facility screen is presented

3. User selects VoIP radio button and taps this screen

4. After successful registration Phone icon turns to green
Step6: User selects VoIP - Phone sends SIP Register Request to IP Office. Note first request is unauthorized by IP Office since no Authentication is sent by the phone. The Second SIP register request includes user authentication details and is accepted by IP Office (200 OK).

- At this point VoIP is Green indicating completely connected and the phone operates as a SIP Phone as indicated by system monitor
- You can use IP Office System Monitor to see SIP messages between phone and IPO: Filters > SIP > SIP Reg/Opt Rx & Tx
Why SRV Records?

- No need for separate XMPP/SIP domains for Onex / Office (Use same DNS name for SIP and XMPP)
- Allows services (SIP, XMPP, SMTP, etc.) resolution for single domain
- Allow use of non-standard ports for SIP, XMPP, etc. Example can use port 5080 instead of 5060 for SIP

With A & SRV Record for Domain Name

With only A Record (bench4.mobility.lab is the FQDN for OneXPortal Server)
### Configuration of DNS Server with A & SRV Records

#### Private Side

**A Name Records**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>a</em></td>
<td>Service Location (SRV)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
<tr>
<td><em>sdbfs</em></td>
<td>Service Location (SRV)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
<tr>
<td><em>ip</em></td>
<td>Service Location (GRP)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
<tr>
<td><em>sip</em></td>
<td>Service Location (GRP)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
<tr>
<td><em>sip</em></td>
<td>Service Location (GRP)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
</tbody>
</table>

**TCP SRV Records**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>a</em></td>
<td>Service Location (SRV)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
<tr>
<td><em>sdbfs</em></td>
<td>Service Location (SRV)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
<tr>
<td><em>ip</em></td>
<td>Service Location (GRP)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
<tr>
<td><em>sip</em></td>
<td>Service Location (GRP)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
</tbody>
</table>

**UDP SRV Records**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>a</em></td>
<td>Service Location (SRV)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
<tr>
<td><em>sdbfs</em></td>
<td>Service Location (SRV)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
<tr>
<td><em>ip</em></td>
<td>Service Location (GRP)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
<tr>
<td><em>sip</em></td>
<td>Service Location (GRP)</td>
<td>192.168.9.10</td>
<td>1/8/2015 6:00:00 PM</td>
</tr>
</tbody>
</table>
Below is a sample of Phone (192.168.0.13) doing a XMPP DNS Query to DNS Server (192.168.0.10) using A & SRV records for MOBILITY.LAB.

DNS answers back with a response that XMPP is located on bench4.mobility.lab and its IP is 192.168.0.10 (Note we used same server for DNS and Onex Portal Server running on a Windows Server at 192.168.0.10)

Below is a sample of Phone (192.168.0.13) doing a SIP DNS Query to DNS Server (192.168.0.10) using A & SRV records for MOBILITY.LAB. It first attempts a TLS request and not successful tries TCP request. Note the SRV requests do not have the port numbers, only the DNS response includes port numbers for the service.
Configuration of DNS Server with A & SRV Records

Public Side

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Data</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip_tcp</td>
<td>A</td>
<td>10.131.95.101</td>
<td>static</td>
</tr>
<tr>
<td>sip</td>
<td>A</td>
<td>10.131.95.101</td>
<td>static</td>
</tr>
<tr>
<td>ldap</td>
<td>A</td>
<td>10.131.95.101</td>
<td>static</td>
</tr>
<tr>
<td>_sip_tcp</td>
<td>SRV</td>
<td>10.131.95.101</td>
<td>static</td>
</tr>
<tr>
<td>_sip</td>
<td>SRV</td>
<td>10.131.95.101</td>
<td>static</td>
</tr>
<tr>
<td>_ldap</td>
<td>SRV</td>
<td>10.131.95.101</td>
<td>static</td>
</tr>
</tbody>
</table>

Domain Name System (response)

[Request in 471]
- Flags: 0x0880, Standard query response, No error
- Questions: 1
- Authority RRs: 0
- Additional RRs: 1

Queries:
- _sip_tcp.mobility.lab: type SRV, class IN
  - Name: _sip_tcp.mobility.lab
  - Type: SRV (Service location)
  - Class: IN (0x0001)
- _sip.mobility.lab: type SRV, class IN, priority 2, weight 0, port 5060, target ipo.mobility.lab

Answers:
- _sip_tcp.mobility.lab: type SRV, class IN, addr 192.168.0.11
- ipo.mobility.lab: type A, class IN, addr 192.168.0.11
< System Monitor Snippet begins>

SIP Tx: TLS 192.168.0.11:5081 -> 10.136.85.100:39702
SIP/2.0 200 OK
Via: SIP/2.0/TLS 10.10.10.101:39702;branch=z9hG4bKfaa-4682-7f8a-67eda7fd9e
From: "Nirmal Android" <sip:8007@mobility.lab>;tag=cdf35957-9dd3-4132-9484-5e94fa2bd322
CSeq: 2 REGISTER
User-Agent: IP Office 9.1.0.0 build 437
Server: IP Office 9.1.0.0 build 437
Supported: timer
Contact: <sip:8007@10.136.85.100:39702;transport=tls>
Date: Wed, 14 Jan 2015 01:29:43 GMT
Expires: 180

20:18:04   34683657mS Sip: SIP Ext 8007 change registration state to registered mobile simultaneous, reason:Login
20:18:04   34683657mS Sip: SIP user NirmalAndroid extn 8007 supports summary mwi 0 allows transfer 1 supports conferencing 0
20:18:04   34683657mS Sip: SIPExtNtv- ExtnFault now 0
20:18:04   34683659mS LIC: ObtainRemoteWorkerLicence: obtained remote worker license for extn 8007 user NirmalAndroid
20:18:04   34683659mS Sip: SIP Ext 8007 changed the number of simultaneous users to 1
20:18:04   34683659mS Sip: SIP: REG: SetMethodSupport for 110000 phone 8007
20:18:04   34683660mS Sip: SIPPhoneReceiver 31 attached to extn 8007, phones 1 sip_phone_receivers 1
20:18:04   34683660mS Sip: SIP REG: Phone(8007)(ip=10.136.85.100) is on PRIVATE network (has NO corporate NAT and phone behind its own NAT. URI_type=SIPURI
20:18:04   34683662mS Sip: User NirmalAndroid(8007) remove address 10.136.85.100 reg-id=1 sip.instance="<urn:uuid:f2e21a47195d6254>" from blacklist
20:18:04   34683662mS SipDialog f58174c deleted, dialogs 0
20:18:04   34683664mS PRN: Config Write Wake Up
20:18:04   34683759mS SipDialog f4eb972c created, dialogs 1
20:18:04   34683760mS Sip: f4eb972c OPTIONS SENT TO 10.136.85.100 37615
< System Monitor Snippet ends>
Configuration of IP Office
You can either set to use STUN to resolve automatically or provide a static public IP below in Public IP Field.

To provide NAT Traversal for remote clients, enter here the public IP of Corporate Router.

Each Remote Worker must have a Power User license configured in Manager.

You need “Power User” profile to support VoIP mode.

Mobile Worker license only supports “Callback” method for calls, not VoIP.
Troubleshooting

**ERROR MESSAGES**

An icon in the Status bar of the one-X Mobile Preferred application displays the status of the connection to IP Office. When the application disconnects from the Avaya one-X® Portal server, the icon turns red. A red or yellow icon indicates a connection issue. Users can press the Trouble icon to view a popup that displays more information on the problem.

If you cannot register the one-X Mobile Preferred application using VoIP, the phone icon turns gray.
The following table lists the error messages most commonly reported and the possible causes of the error. For complete list please refer the Administering Avaya one-X® Mobile for IP Office guide on the IP Office Knowledgebase.

<table>
<thead>
<tr>
<th>PROBLEM</th>
<th>REASON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Server</td>
<td>Configured Server cannot be resolved through DNS</td>
</tr>
<tr>
<td>Server Unreachable</td>
<td>Avaya one-X® Mobile cannot contact the server using the configured server name and port.</td>
</tr>
<tr>
<td>Server Request Timed out</td>
<td>The connection to the configured server on a specified port timed out.</td>
</tr>
<tr>
<td>Invalid user credentials</td>
<td>The configured user name or password is incorrect</td>
</tr>
<tr>
<td>User has no XMPP account</td>
<td>The one-X Mobile Preferred client contacted the server to retrieve the XMPP account information and found that the user has no active XMPP account.</td>
</tr>
<tr>
<td>Failed to retrieve XMPP account information</td>
<td>The one-X Mobile Preferred client contacted the server to retrieve the XMPP account information and was unable to complete the operation.</td>
</tr>
<tr>
<td>Network is unavailable</td>
<td>The connection to the server failed because the network is unavailable on the mobile phone.</td>
</tr>
<tr>
<td>XMPP connection is unavailable</td>
<td>The client was unable to establish or maintain an XMPP connection to the server.</td>
</tr>
<tr>
<td>iPhone one-X Mobile Preferred client fails to connect despite providing the correct credentials and the server domain is reachable</td>
<td>Ensure that the XMPP domain is not 127.0.0.1 and you configure the correct domain.</td>
</tr>
</tbody>
</table>

Troubleshooting connection issues

When the one-X Mobile Preferred client is disconnected from IP Office, the one-X Mobile Preferred client attempts to establish a connection in the background. Use the following list to troubleshoot connection problems if the application cannot connect to IP Office.

- Ensure that the user has an appropriate license.
- Verify that the following TCP ports are open: Port 5222 is for XMPP traffic and port 8444 is for bootstrap REST API call traffic.
- Verify that the FQDN resolves to the correct IP address.
- If Avaya one-X® Mobile can connect when the user is on a cellular network, but cannot connect on an internal Wi-Fi network, verify that your router supports packet hair-pinning. If the router does not support packet hair-pinning, deploy a split DNS solution to resolve the problem.
- Ensure that the Server certificates check box is not selected in the client settings.
- You can use following links to test your SIP and XMM server connection from any PC.
  - [https://FQDN:8444/rest/my/sip-info](https://FQDN:8444/rest/my/sip-info)
  - [https://FQDN.lab:8444/rest/my/im-info](https://FQDN.lab:8444/rest/my/im-info)
To check xmpp connection - https://mobility.lab:8444/rest/my/im-info

This XML file does not appear to have any style information associated with it.

```xml
  <im-info>
    <imId>nirmalandroid@mobility.lab</imId>
    <imPassword>8007</imPassword>
    <myBuddyId>mybuddy@mobility.lab</myBuddyId>
  </im-info>
```
To Check SIP Connection
https://mobility.lab:8444/rest/my/sip-info

This XML file does not appear to have any style information associated with it. The

Mobile Application Logs
When escalating an issue to Avaya support, the user can use Problem Reporting facility within the application to provide logs from the application via email.

- IP hone: App Settings (wheel icon) > System messages > Report Problem
- Android: Settings > Advanced > Submit Problem Report

By default, logs are disabled; they can be activated in the phone’s settings menu.

The Email template uses the default email address of Avaya R&D, User should change the address to a recipient who can receive the email and log file and then pass on to Avaya support. Password related information is stripped from the logs.

An Android User experiencing problems can also upload the logs to the One-X Portal server. Go to Android Menu -> About -> Menu -> Log Upload to initiate the transfer Logs will appear on One-X Server.

Linux server under: /opt/Avaya/oneXportal/<version>/apache-tomcat/logs/smack-file-transfer
Windows Server under: \Program Files (x86) \Avaya\oneXportal\Tomcat\Server\logs\smack-file-transfer

Log name is in format logs_217_11_08_17_15_47_55.zip where 217 is the user, then date, and time when the logs were taken.

Troubleshooting VoIP Issues
Perform the following checks to troubleshoot VoIP issues:

- Use Avaya IP Office System Monitor SIP Phone Status to check the SIP registrations.
• Use the Android and iPhone client to check the registration error messages.

Android

On Android You can use the client details dialog box:
  o Check if the RX/TX counters are running.
  o If the Android client is local, the local IP address of IP Office must be Remote.
  o If the Android client is remote, the public IP address of IP Office of the corporate router must be Remote. Also, the remote ports must be from the RTP port range.