**Network Information:**

RedSky assumes that the customer has the appropriate level of expertise required to configure their own devices. Customers are responsible for the configuration and operation of their own equipment.

1. **Method of Connectivity to the Anywhere 7 Service**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| a) |  | . |  | . |  | . |  |
| b) |  | . |  | . |  | . |  |
| c) |  | . |  | . |  | . |  |
| d) |  | . |  | . |  | . |  |

IP Address of Termination Point:

(Public IP the SIP Invite is coming from)

Transport Method: UDP

TCP

TLS

1. **RedSky Gateway Information**

|  |  |
| --- | --- |
| **RedSky Voice Gateway** | **IP** |
| gw1.anywhere.e911cloud.com | 3.135.80.158 |
| gw1west.anywhere.e911cloud.com | 50.112.56.223 |
| gw2.anywhere.e911cloud.com | 18.217.182.60 |
| gw2west.anywhere.e911cloud.com | 35.167.102.28 |

|  |  |
| --- | --- |
| **RedSky Protocol** | **RedSky Port** |
| TCP/UDP | 5060 |
| TLS SIP | 5061 |
| RTP / SRTP | 30000 - 60000 |

***\*Note, if using TLS the FQDN must be used instead of the IP address***

**Call Flow Diagram**

The diagram below documents the SIP dialog between a customer’s call sever and the RedSky Gateway.

RedSky

Customer Gateway E911 Service

| | | |

| INVITE F1 | | |

|------------------->| | |

| 100 Trying F2 | | |

|<-------------------| | INVITE F3 |

| | |------------------->|

| | | 100 Trying F4 |

| | |<-------------------|

| | | 180 Ringing F5 |

| 180 Ringing F6 | |<-------------------|

|<-------------------| | |

| | | 200 OK F7 |

| 200 OK F8 | |<-------------------|

|<-------------------| | ACK F9 |

| ACK F10 | |------------------->|

|------------------->| | |

| RTP Media | | RTP Media |

|<==================>| |<==================>|

| BYE F11 | | |

|------------------->| | BYE F12 |

| 200 OK F13 | |------------------->|

|<-------------------| | 200 OK F14 |

| | |<-------------------|

| | | |

Session Initiation Protocol (SIP) is a signaling, presence and instant messaging IP based protocol. SIP signaling occurs on port 5060 utilizing TCP or UDP, or port 5061 if utilizing TLS. SIP also negotiates the setup of sessions by including Session Description Protocol (SDP) within the SIP INVITE message. The SDP describes the parameters of the media session. This includes information such as media encoding, IP address, and port that will be used for RTP/SRTP or the media portion of a SIP based call.

**RedSky SIP INVITE Requirements**

The Request-URI in the INVITE line will be sent to 911. This indicates the resource where the request will be sent.

Example:

INVITE sip:911@3.135.80.158:5060 SIP/2.0  
  
The connection information line (c=), in the SDP, will be set to a public IP. The connection address IP is where media will be delivered.

Example:

c=IN IP4 *<Connection Address>*

**RedSky Gateway Allowed Codecs**

ulaw - G.711/PCMU

**SIP over TLS Best Practices:**

1. Comodo/Sectigo root certificate has been added to Trusted Root CA Certificate store.

**Note**: RedSky gateways present the entire certificate chain during the TLS handshake.

If needed, Comodo/Sectigo root certificate can be downloaded from the following link:

[Comodo/Sectigo Root CA Certificate](https://resources.e911cloud.com/certs/AAACertificateServices.crt)

1. SIP signaling is sent to voice gateway FQDN instead of the IP addresses

(i.e., gw1.anywhere.e911cloud.com, gw2.anywhere.e911cloud.com, etc.)

1. SIP signaling is sent to port 5061, not to port 5060
2. SIP traffic is encrypted using TLS 1.2, and SIP signaling messages are not using unencrypted UDP/TCP protocol
3. TLS 1.2 is used, and not an older version of TLS/SSL

**Supported TLS 1.2 Ciphers:**

* TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (secp384r1)
* TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (secp384r1)
* TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (secp384r1)
* TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (dh 4096)
* TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (dh 4096)
* TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (dh 4096)
* TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (dh 4096)
* TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (rsa 2048)
* TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (rsa 2048)
* TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (rsa 2048)
* TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (rsa 2048)
* TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (secp384r1)
* TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (secp384r1)
* TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (secp384r1)
* TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (dh 4096)
* TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (dh 4096)
* TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (dh 4096)
* TLS\_DHE\_RSA\_WITH\_SEED\_CBC\_SHA (dh 4096)
* TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA (dh 4096)
* TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (rsa 2048)
* TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (rsa 2048)
* TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (rsa 2048)
* TLS\_RSA\_WITH\_SEED\_CBC\_SHA (rsa 2048)
* TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA (rsa 2048)
* TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (secp384r1)
* TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (dh 4096)
* TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (rsa 2048)
* TLS\_RSA\_WITH\_IDEA\_CBC\_SHA (rsa 2048)
* TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA (secp384r1)
* TLS\_RSA\_WITH\_RC4\_128\_SHA (rsa 2048)
* TLS\_RSA\_WITH\_RC4\_128\_MD5 (rsa 2048)

**Supported SRTP Ciphers:**

* AES\_CM\_128\_HMAC\_SHA1\_80
* AES\_CM\_128\_HMAC\_SHA1\_32
* AES\_CM\_256\_HMAC\_SHA1\_80
* AES\_CM\_256\_HMAC\_SHA1\_32
* AES\_GCM\_128
* AES\_GCM\_256
* AES\_GCM\_128\_8
* AES\_GCM\_256\_8
* AES\_CM\_192\_HMAC\_SHA1\_80
* AES\_CM\_192\_HMAC\_SHA1\_32

RedSky gateways will use the strongest cipher offered by the client.

**Testing Phases:**

The Testing Phases are outlined below. You will need to configure on your SBC a test route or alternate route (ex. 811 or 8911) to route your calls to the RedSky IP Address/ Port Number. This will allow you to test without impacting your existing live 911 route. Once the SBC configurations are completed, testing will be coordinated with your RedSky Project Manager.

**Phase 1:**

* You will make calls on your test route which will point to a CID player (Caller ID) with a recording that will read back to you the Address, Dispatchable Location, and callback number of the caller.
* Be sure the address and location information that is read back matches the information provisioned in the Teams LIS. If it does not, you will only hear the callback number and Location is “Unknown”.
* Once you are comfortable with what is read back to you, we can continue to the next phase of testing.

**Phase 2:**

* Next, you will continue to make test calls on your test route but this time, the calls will route to the local PSAP.
  + **Note:** RedSky will need to make a quick change on their end to facilitate this test.
* **Note:** Prior to testing, you will need to contact the local non-emergency number (usually the local police dept.) to schedule testing with them.
* When a test call is made, the live operator will read back to you the address, dispatchable location, and callback number. In some cases, the live operator will only acknowledge what you tell them. All PSAPs respond differently.
  + If any of the information that is reported back is not correct, please have the operator verify they have checked all their screens and not just the main screen.

**Phase 3:**

* When you are comfortable with phase 2 testing, then you can switch back over to your normal 911 production route pointing to RedSky IP Address / Port Number to make 911 calls.
* During testing, you will need to verify that both 911 and 9911 are working.

**Ongoing Testing:** Calls sent to 933 will always route to the test player. This can be a useful tool to test new sites after the main 911 route has been turned to live.

**Important Note:** Any 911 call which is not associated with an address will route to the National PSAP (ECRC) and the customer will be charged **$100 per call.**