beam®

suitabletech.com

Network Administrator’s Guide

Overview

Beam® is a comprehensive Smart Presence™ system that couples high-end video, high-end audio, and the freedom of mobility for a crisp and immersive, video experience that enhances collaboration and understanding between communicators.

Suitable Technologies® leveraged years of research and user studies to design the Beam® system to include low-latency, highly-reliable, and business-class video conferencing software within a drivable hardware platform. Sleek, sturdy, and more reliable than any other telepresence product on the market; the Beam system offers an unparalleled user experience with hardware and software specifically designed for an individual’s Smart Presence™ at any remote location.

Purpose of this document?

This guide will help you understand:

- What requirements and considerations you’ll need to ensure proper setup and operation of the Beam® system.
- Beam’s network architecture
- Beam’s security and privacy policies and best practices

This guide should replace any previous network administrator’s guide you may have, vist www.suitabletech.com/documentation to verify you have the most recent version. Publish date of this document is: 03/24/15

Who should read this?

This guide is written for system administrators responsible for managing their business’s networks and hardware. It assumes that you are familiar with:

- Enterprise deployment issues
- Group policy administrations
- Other topics related to network configuration and security (OS requirements are located in our Beam Requirements document)

Table of Contents

1.0 Network Architecture

Sessions between the Beam Smart Presence system (SPS) and the Beam App occur via a direct peer-to-peer UDP connection. When it is not possible to establish a direct connection, a relay server will be used to forward the session traffic. Please refer to "Beam Network Setup" for all information regarding how relays can be used.

The Beam cloud infrastructure is used to get the pilot station in touch with the Beam SPS. When the SPS is connected to the network, it connects to the cloud infrastructure to signal its state. When the Beam App is started, it also connects to the cloud infrastructure to determine which devices are available.
At the start of a session, the cloud infrastructure gives the system and Beam App a channel to assist in setting up a peer to peer connection. The cloud infrastructure is also used to get software updates, upload diagnostic information, and to manage Beams and user permissions.

2.0 Beam Network Setup

The Beam network consists of three different components. The Beam SPS provides remote presence capability, the Beam App provides access to the Beam SPS from a supported computing platform, and relay servers are used to connect sessions across diverse network types.

2.1 Relays

A relay server provides two important services to the Beam.

First, it provides a configuration relay which is used to provide a consistent IP and port to services (such as HTTPS) which do not work with a floating IP. This allows the Beam to maintain a TCP connection when roaming between different access points, networks, and even 4G LTE. The services which make use of the configuration relay, are primarily those needed for the Beam to query the infrastructure regarding its configuration or new software updates. The configuration relay is known as "beam_relay". It is usually set up at port 6868, though this can be configured on a site-to-site basis.

Second, it provides a media relay which is used to help two parties determine each other's IP and port, and to relay media traffic in the event that two parties cannot directly connect. The media relay uses jingle for connection establishment. The media relay is also known as "jingle_relay", and is generally set up to listen on ports 6869-6870.

The Beam SPS will, by default, make use of one or more of Suitable's public relays. These relays are located at various locations across the globe to minimize latency. The Beam SPS will automatically select the best public relay based on ping data, or it can be configured to use private relays hosted by an organization.

In environments with heightened confidentiality requirements, it may be desirable to set up an internal relay so that call traffic will never get routed outside of an organization's firewall or certain private networks. It may also increase call quality if direct connections cannot be made and call traffic is being routed through Suitable's public relays during peak operating hours. Though each organization is free to tailor the specifics of its relay configuration for itself. There are two general internal relay styles that are typically used which are described in the sections below.

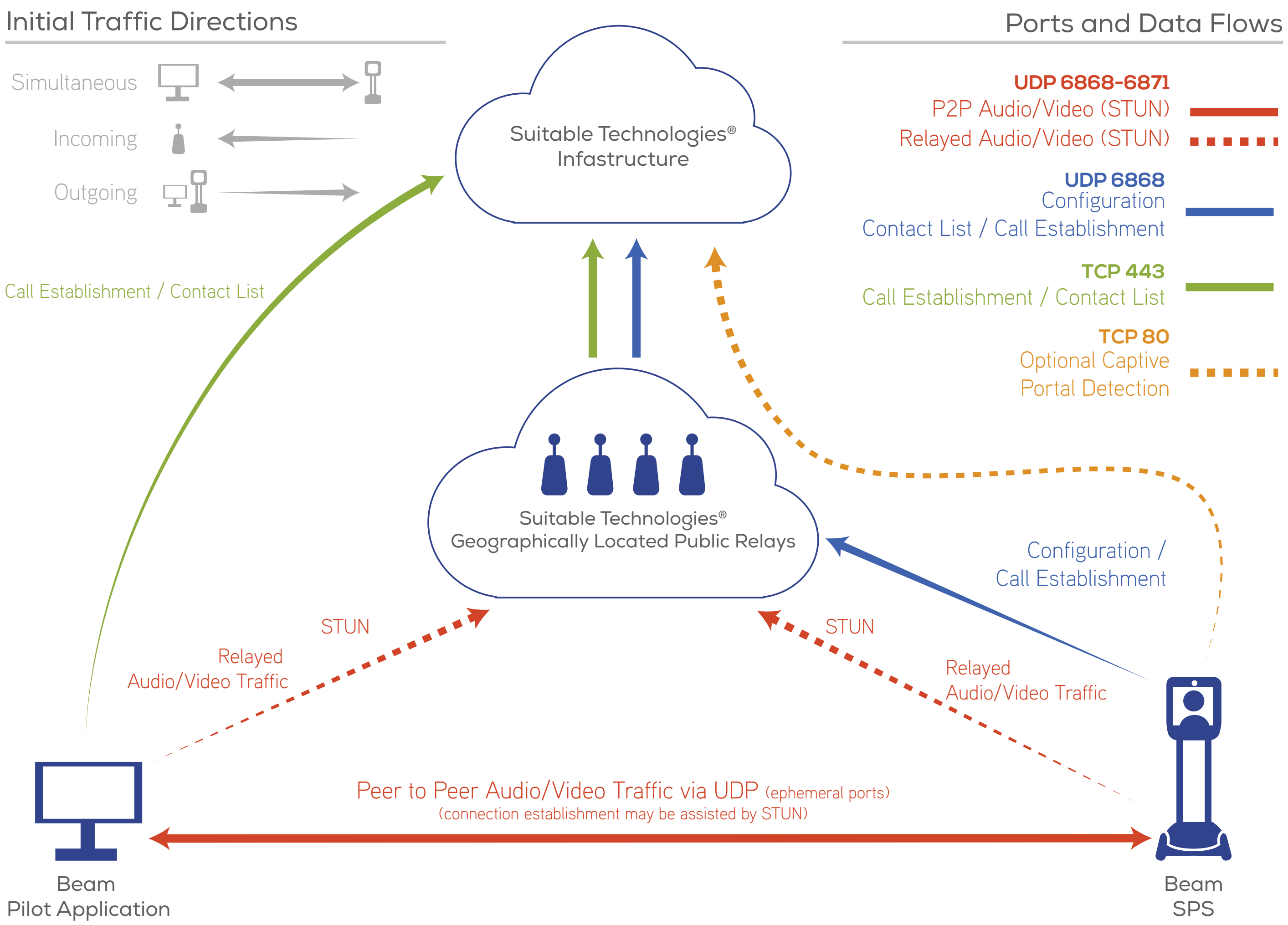
2.1.1 Beam Public Relays

This is our default configuration. It allows for sessions to be created from any location connected to our infrastructure services.

For a list of all public relays, please visit: https://www.suitabletech.com/documentation/relays/

Note: The relay list will change periodically as we add/move relays.

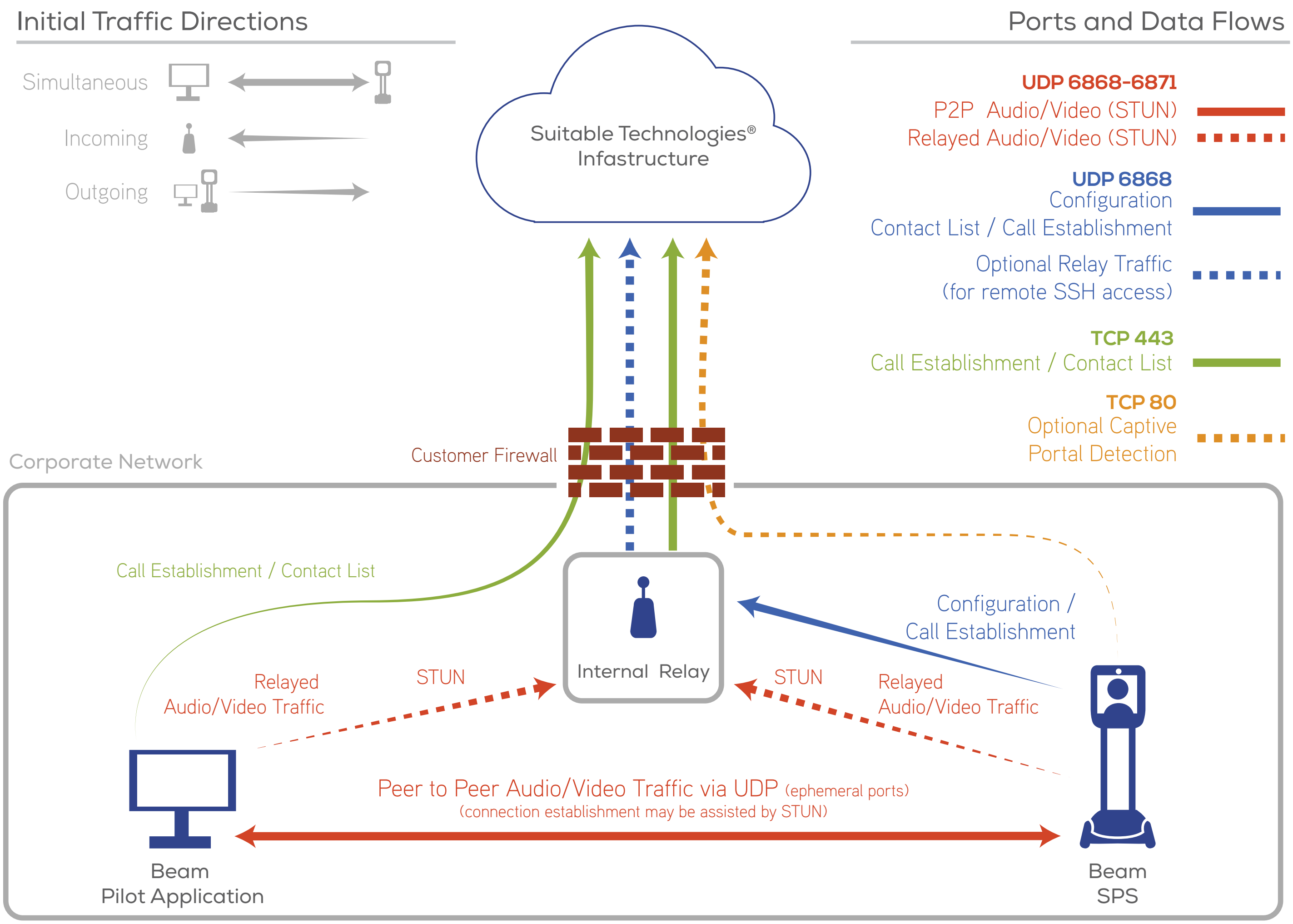
Public Relay Data Traffic



2.1.2 Using Internal (Private Relays)

The relay is configured to demultiplex the configuration and support protocols needed by each Beam SPS and forward them to Suitable's infrastructure. Optionally it maintains a direct connection with Suitable's infrastructure to permit real-time support. The organization can elect to configure its firewall rules to not allow ephemeral UDP connections. This setup prevents egress of call data from the network and provides the most flexibility.

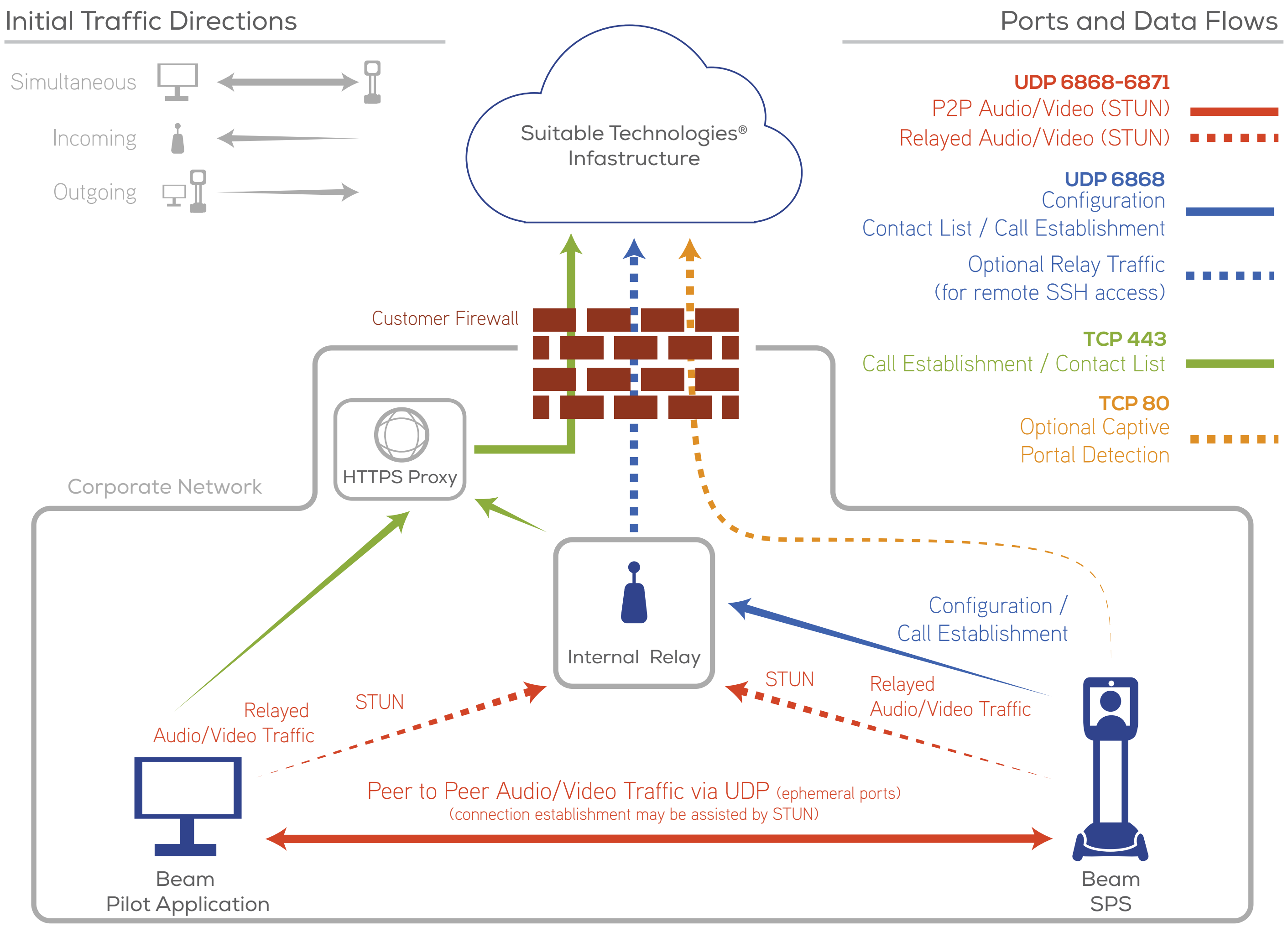
Internal Relay Data Traffic



2.1.3 Using Internal Relays with a Proxy

The relay is configured to route the minimum required services through an HTTPS proxy, which makes the requests to Suitable's infrastructure on the relay's behalf. This setup can be used where HTTPS queries cannot be made directly from the private network. A private network which requires a tunneled setup will generally be unable to make or receive calls outside itself. This setup provides the essential functionality in heavily restricted environments.

Internal Relay (with Proxy) Data Traffic



2.2 The Beam App

The following list covers the network requirements that must be met for Beam service to be possible on all platforms:

1. The Beam App requires broadband internet access with a minimum of 1Mbps upload and 1Mbps download speed (Recommended 3Mbps upload and 3 Mbps download).

2. A connection to Beam relay servers and Suitable Technologies Infrastructure. If you have not set up an internal relay, please refer to the diagram in section 2.1.1. If you are setting up an internal relay, please refer to the diagrams in section 2.1.2 and 2.1.3.

3. **Highly recommended -**To all Beam SPSs: STUN compatible firewall with outgoing and return traffic on all UDP ports.

2.2.1 Beam App Update

When Suitable Technologies releases an update for the App, an update notification is displayed in the App's UI. Once the update is accepted, the installation process is nearly identical to the original installation. User preferences and settings will be preserved across updates.

2.3 The Beam SPS

The Beam SPS requires the following network elements for successful operation:

2.3.1 General Network Requirements

1. The Beam SPS requires broadband internet access with a minimum of 1Mbps upload and 1Mbps download speed (Recommended 3Mbps upload and 3 Mbps download).

2. A DHCP server to obtain IPv4 address(es) for the Beam SPS's wireless interface(s)

3. A connection to Beam relay servers. If you have not set up an internal relay, please refer to the diagram in section 2.1.1. If you are setting up an internal relay, please refer to the diagrams in section 2.1.2 and 2.1.3.

4. **Highly recommended -** To all Beam App: STUN compatible firewall with outgoing and return traffic on all UDP ports.

2.3.2 WiFi Requirements

- Good WiFi coverage across the Beam's operating environment

- 802.11 g (at 2.4 Ghz) or 802.11 a/n (at 5.0 Ghz*) WiFi network coverage over the area where the Beam SPS will be used ***5Ghz is highly recommended, and using (n) is preferred.**

- WiFi Security can be Open, WEP*, WPA/WPA2 Personal, WPA/WPA2 Enterprise. The Beam SPS uses WiFi security only to allow it to connect to your wireless network. All communication to and from the Beam software is independently encrypted. See "Security and Privacy" for more details." ***WEP use is not recommended, as it can result in loss of network throughput.**
- Supported WPA/WPA2 Enterprise EAP methods:
  - » EAP-TLS
  - » EAP-PEAP/MSCHAPv2
  - » EAP-PEAP/GTC
  - » EAP-PEAP/MD5-Challenge
  - » EAP-TTLS/MSCHAPv2
  - » EAP-TTLS/MSCHAP
  - » EAP-TTLS/PAP
  - » EAP-TTLS/CHAP
- Hidden networks are supported only on non-DFS frequencies.
- Load balancing across access points should be turned **OFF**
- Recommend that Access Point features **Dynamic Transmit Power Control** and **Dynamic Channel Assignment** should be turned **OFF** where any Beam SPS will be used.

2.3.3 Firewall and NAT Traversal Requirements

The exact requirements vary from site-to-site. The below requirements assume you are using a public relay configuration. If you are configuring an internal relay, refer to sections 2.1.2 or 2.1.3 . Please contact us if these requirements are incompatible with your network.

1. To Suitable relay servers (https://www.suitabletech.com/documentation/relays/)
   - Outgoing and return traffic on UDP port 6868 to 6871
2. **Highly recommended -** To all Beam App computers: STUN compatible firewall with outgoing and return traffic on all UDP ports

2.3.4 Quality of Service Recommendations

- Quality of Service (QoS) should be set to prioritize any Beam service media traffic on the WiFi network, and on the up-link to the ISP.
- The Beam marks all its outgoing media traffic with a TOS of 0xE0.
- Traffic to the Beam is not marked by the Beam Pilot App
- The Beam SPS communicates from ports 6800-6809 to the Beam relay at port 6868. All other UDP traffic to and from the Beam is media traffic. To set up QoS for traffic going to the Beam, give a high priority to UDP traffic to the Beam on all ports except 6800-6809.

2.3.5 4G LTE Support

The Beam SPS supports several 4G LTE USB modems. Bandwidth requirements are approximately the same as WiFi. Installing a 4G LTE modem on a Beam is not recommended for environments using an internal relay for confidentiality purposes, as 4G LTE traffic is generally routed over the internet.

For more information see, https://www.suitabletech.com/documentation/4G, or contact us at support@suitabletech.com.

2.3.6 DHCP

Each Beam network interface uses DHCP to obtain its configuration. The DHCP host name may vary in future software releases. Since the Beam's name can also be changed by organization administrators, it is strongly recommended that Beams are identified by their MAC addresses rather than their DHCP host name.

The DHCP host name is generally the Beam's name, followed by a dash, followed by the name of the network interface that DHCP is being performed from. Special characters and spaces may be replaced with an underscore and the name may be truncated due to size constraints. For instance, a Beam named "My Beam" could appear with the host name "My_Beam-wlan0".

2.3.7 Captive Portal Detection

Many captive portals will allow a whitelist of MAC addresses to be specified. It is recommended that Beam WiFi interfaces are whitelisted when they are deployed at a facility. If all WiFi interfaces on a Beam are whitelisted, captive portal detection is not needed. The MAC address for all Beam SPS network interfaces can be found in the Beam's "System Info" screen.

Captive portal detection makes an HTTP request to a known web page from the Suitable Technologies servers in order to ascertain whether the network requires sign-in via a web browser to gain access. When the Beam cannot ping its assigned relays, it will employ captive portal detection as part of its diagnostic process. If the detector receives a different web page than it expected or receives an HTTP status code from 300-399 - which are redirects or "use proxy" errors - then the detector will flag that interface as blocked by a captive portal.

When an interface is blocked by a captive portal, the Beam will display a warning on its status screen and WiFi configuration screen. Sign-in is accomplished through the Beam's built-in web browser or by sharing its connection over WiFi, Bluetooth, or Ethernet. If the Beam is temporarily relocated or its battery runs down, the captive portal may require the sign-in process to be repeated when it connects again to the network. If the Beam is whitelisted, no sign-in is necessary.

2.3.8 Beam (SPS) Update

When Suitable Technologies releases a Beam SPS software update, the Beam will automatically update itself, when idle (not in a session). When updating begins, the Beam SPS will display an updating status message.

The update process should only take a few minutes, and the Beam will restart itself when the update has completed. Beam settings such as WiFi configuration will be preserved across software updates, and should not need user interaction. If your company needs more control over the timing of Beam updates or the particular software version your Beams are running, please contact support@suitabletech.com

3.0 Security and Privacy

The following section covers topics related to security and privacy as it relates to your organization's use of Beam and its services.

3.1 Auditing

Suitable has had security reviews by Accuvant (07/2013) and Gotham Digital Science (10/2014) to evaluate the Beam's security. Some customers have with permission attempted to attack the Beam's security. As of the last security audit, no critical security flaws were identified.

3.2 Confidentiality

Beam call data is encrypted using AES-256 in CTR mode, and authenticated using HMAC-SHA1. Encryption and decryption happen at the call endpoints, so if relays are used they only process encrypted data. The AES-256 and HMAC-SHA1 keys are derived using HMAC-SHA1 from random numbers generated by each of the participating parties. The random numbers are exchanged via XMPP meaning that a compromised XMPP server could reconstruct the session keys.

Traffic between the Beam and the infrastructure uses SSL over an unencrypted proprietary relay protocol. SSL ensures the confidentiality and integrity of the communication. A pseudo-randomly generated 64-bit connection identifier identifies each relay connection, allowing the Beam's IP address and port to float around during a connection. An attacker who can guess the connection identifier can temporarily hijack the connection, but the worst he can achieve is to cause the connection to be lost. This compares favorably with TCP where an attacker who guesses a 32-bit sequence number can cause a connection to be lost. The sequence number for a connection is generated pseudo-randomly using Triple-DES applied to a counter with a key taken from /dev/urandom.

On Linux and OSX, cryptographic operations are carried out using OpenSSL implementations. On Windows the Wincrypt API is used, except for AES which uses axTLS and Triple DES which uses libtomcrypt.

Note:

Currently, there is no known way for attackers to eavesdrop on conversations.

3.3 Infrastructure

Suitable technologies has the following levels of access privileges to our infrastructure systems:

Super Users	Have full access and are limited to a core set of support staff within Suitable.
Support Users	Have access to a limited set of tools to help support customer Organizations
Org Admins	Have user level access as well as the ability to add and remove users from their Org.
Org Users	Have access to only the devices the Org Admin designates.

3.3.1 Update Protocol

The Beam automatically checks with the infrastructure using HTTPS to determine whether an update is available. Updates are downloaded by the Beam via SSL and checked with MD5Sum after being downloaded. Although the updates themselves are not signed, the download is done with an encrypted connection over HTTPS/SSL and the certificate used is signed by GoDaddy. The Beam initiates the download. It will not download from any server other than that provided by the relay, which is suitabletech.com on all public servers. It will not download if the certificate is not signed by a valid CA. Only a trusted subset of Suitable Technologies employees can upload new releases via an established deployment process.

3.3.2 Certificates

Suitable's web servers use SSL to prevent man in the middle attacks. We use GoDaddy to sign our web server's certificates.

Suitable's XMPP server also uses SSL. We use our own CA to produce the XMPP certificates. The Beam SPS and Beam App will only accept certificates from the Suitable CA.

The Beam SPS authenticates to the web server and XMPP server using a self-signed certificate that it produces and which is associated with the Beam's device configuration during the manufacturing process. This certificate is used by the Beam to perform authenticated calls to the infrastructure, such as fetching its device configuration and software updates.

3.3.3 Password Storage

Passwords are stored using a password-based key derivation function (PBKDF2). The source password material is hashed 10,000 times with SHA256 using a unique salt per-user.

3.3.4 Data Backup

Databases are backed up nightly and all configuration data is stored in SCM and deployed with a mixture of Fabric and SaltStack.

3.4 Network Service Requirements

The Beam uses DHCP to connect to the user's network and determine its primary relay. Once connected, the Beam will route all connections with our infrastructure through its relay, except for call traffic, which is routed directly to the caller whenever possible. Customers with an internal relay can see and tailor exactly which services the Beam is using via the relay configuration. If your site uses a captive portal to restrict access, the Beam will use DNS and HTTP/S to allow the user to enter credentials to clear it.

3.5 Remote Network Access

If authorized, a support mode can be enabled, per device, that will allow Suitable Technologies SSH access into the Beam SPS for diagnostics purposes. Network access to the SSH server is restricted, only accessible by a small subset of Suitable Technologies employees. This is only enabled with express permission from the customer..

3.6 Beam's Use of Public Internet

At minimum, the Beam software uses Suitable Technologies' infrastructure for configuration purposes. Session setup is entirely handled through Suitable Technologies' Web and XMPP servers. All configuration traffic is secured using TLS.

All media traffic will use a direct connection whenever possible. When using public relays, traffic may travel through the internet during a call. When using an internal relay, traffic may or may not traverse the internet depending on the relevant organization's network configuration. All Beam call traffic is encrypted using AES and authenticated using HMAC-SHA1.

3.7 Local Privacy

The Beam software does not offer any way to listen-in to conversations or retransmit images when the Beam is not in an active session.

3.8 Communication with the Cloud Infrastructure

Communication with the cloud infrastructure is protected using industry standard TLS, with the exception of DNS and Network Time Protocol (NTP) data.

3.9 Privacy Policy

Our privacy policy can be found online at: https://www.suitabletech.com/privacy/

4.0 Support

Our customer success team is available to help with any additional questions or concerns you may have. They can be reached by emailing support@suitabletech.com