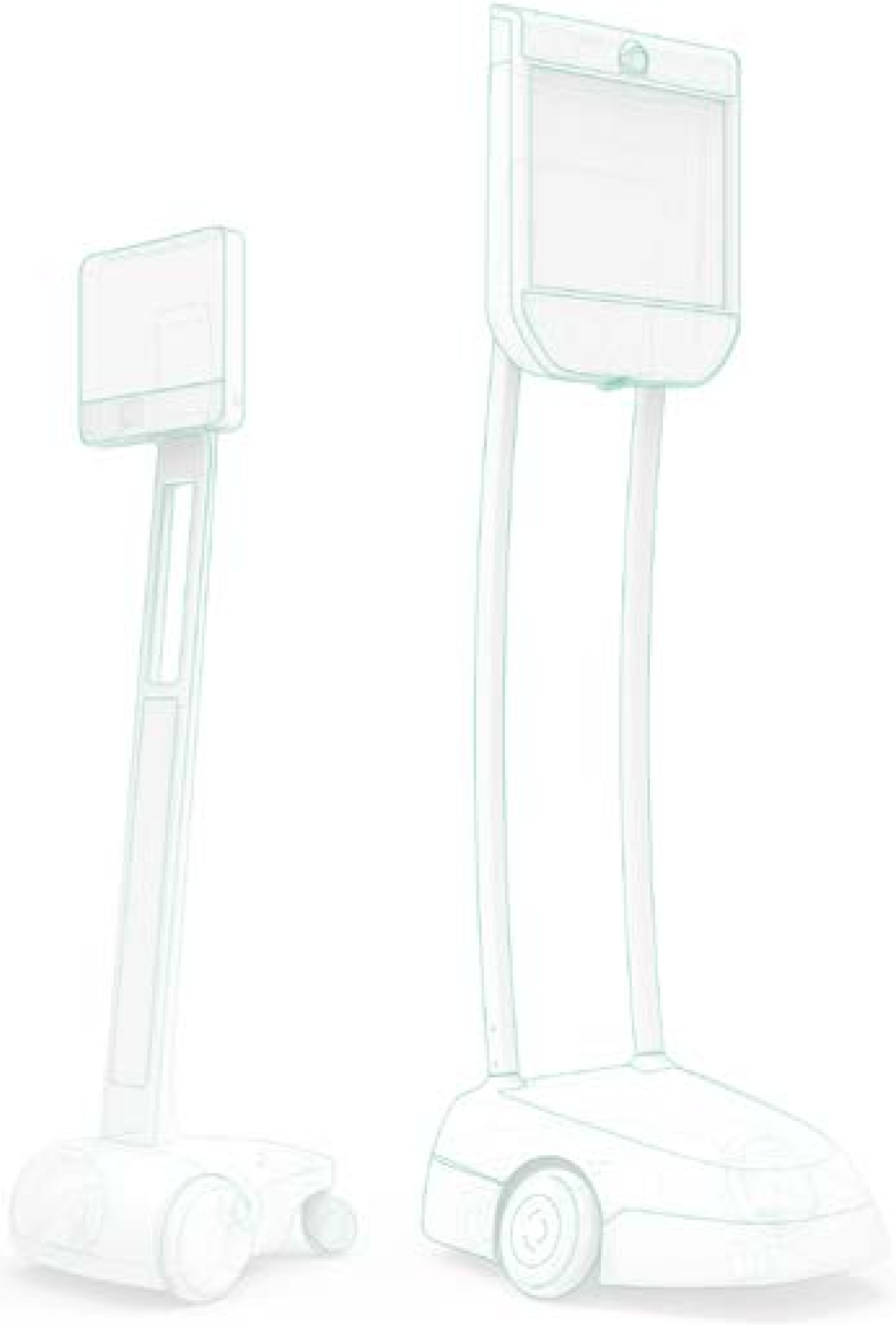
beam®



Network Administrator Guide

Overview

Beam® is a comprehensive Presence System that couples high-end video, high-end audio, and the freedom of mobility to allow for a crisp, immersive experience meant to enhance collaboration and understanding between communicators.

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

Conceptual Purpose

This guide will assist in the understanding of the following concepts:

» Beam best practices
» Beam network architecture
» Beam security and privacy policies
» Requirements and considerations to ensure proper setup and operation of the Beam System

Intended Audience

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

» Enterprise deployment and issues
» Group policy administration
» Network configuration
» Network security

Table of Contents

1.0 Network Architecture

Sessions between the Beam® Presence System (Beam) 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. Refer to section 2.0 Beam Network Setup below for information regarding how relays can be used.

The Beam cloud infrastructure is used to connect the Beam with the Beam App. When the Beam is connected to a LAN, 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 assigns a channel to the Beam and Beam App to assist in the establishment of a peer to peer connection. The cloud infrastructure is also used to send software updates, upload diagnostic information, and manage Beams and user permissions.

2.0 Beam Network Setup

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

2.1 Beam System

2.1.1 General Network Requirements

1. Broadband internet access.
2. Minimum bandwidth of 1 Mbps upload and 1 Mbps download speeds.
3. A DHCP server to obtain IPv4 address(es) for the Beam wireless interface(s).
4. A connection to Beam relay servers. Refer to section 2.3 Public Beam Relays.

» Recommended but not required:

- Bandwidth of 3 Mbps upload and 3 Mbps download speeds.
- STUN compatible firewall with outgoing and return traffic on all UDP ports to all Beam Apps.

2.1.2 WiFi Requirements

1. Satisfactory WiFi coverage across the Beam's operating environment.
   » Ideal Beam RSSI range: -30 dBm to -65 dBm
2. 802.11 g/n (at 2.4 GHz) or 802.11 a/n/ac (at 5.0 GHz) WiFi network coverage over the area where the Beam will be used.
3. WiFi Security can be Open, WPA/WPA2 Personal, WPA/WPA2 Enterprise. Beam 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 section 3.0 Security and Privacy for more details.
4. Supported WPA/WPA2 Enterprise EAP methods:
   » EAP-TLS
   » EAP-PEAP/MSCHAPv2
   » EAP-PEAP/GTC
   » EAP-PEAP/MD5-Challenge
5. Hidden networks are supported on NON-DFS frequencies ONLY.
6. Turn OFF load balancing across access points.

» Recommended but not required:

- 5.0 GHz is highly recommended and using (n) is preferred.
- Access Point features: Dynamic Transmit Power Control and Dynamic Channel Assignment should be turned OFF where any Beam will be used.

2.1.3 Firewall and NAT Traversal Requirements

The below requirements assume you are using a public relay configuration. Exact requirements will vary from site-to-site. Please contact Suitable Technologies if these requirements are incompatible with your network. View a complete list of Beam Relays on our documentation page.

1. Outbound traffic on UDP ports 6868 to 6871. In rare cases, it may be necessary to open outbound and return traffic.

» Recommended but not required:

- STUN compatible firewall with outgoing and return traffic on all UDP ports to all Beam Apps.

2.1.4 Quality of Service (QoS) Recommendations

1. Traffic to the Beam is not marked by the Beam App.
2. The Beam marks all outgoing media traffic with a TOS of 0xB8.
3. QoS should be set to prioritize any Beam service media traffic on the WiFi network and on the up-link to the ISP.
4. The Beam 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.

2.1.5 Beam Updates

When Suitable Technologies releases a Beam software update, the Beam will automatically update itself when idle (not in a session). When updating begins, the Beam 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, contact support@suitabletech.com.

2.1.6 DHCP

Each Beam network interface uses DHCP to obtain its configuration. The DHCP hostname 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 hostname.

The DHCP hostname is generally the Beam's name, followed by a hyphen, followed by the name of the network interface from which the DHCP is being performed. Special characters, including consecutive special characters, and spaces may be replaced with a single hyphen. The name may also be truncated due to size constraints.

For instance, a Beam named "My Beam!" could appear with the hostname "My-Beam-wlan0". Beams equipped with two wireless interfaces will show a second hostname, "My-Beam-wlan1".

2.1.7 4G LTE Support

Beam supports several 4G LTE USB modems. Bandwidth requirements are approximately the same as WiFi. For more information about our supported devices, see our list of Supported 4G Modems and Hotspots.

For confidentiality purposes, installing a 4G LTE modem on a Beam is not recommended for environments using an internal relay as 4G LTE traffic is generally routed over the internet.

2.1.8 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 where a captive portal is in place. If all WiFi interfaces on a Beam are whitelisted, captive portal registration is not needed. The MAC address for all Beam network interfaces can be found in the Beam's UI under "System Info".

Captive portal detection makes an HTTP request to a known web page from 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 relay, it will employ captive portal detection as part of its diagnostic process. If the detector receives a different web page than 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 by sharing the Beam's 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 reconnects to the network. If the Beam is whitelisted, no sign-in is necessary.

2.2 Beam App

2.2.1 General Network Requirements

1. Broadband internet access.
2. Minimum bandwidth of 1 Mbps upload and 1 Mbps download speeds.
3. A connection to Beam relay servers. Refer to section 2.3 Beam Public Relays.

» Recommended but not required:

- Bandwidth of 3 Mbps upload and 3 Mbps download speeds.
- STUN compatible firewall with outgoing and return traffic on all UDP ports to all Beam Systems.

2.2.2 Beam App Updates

When Suitable Technologies releases an update for the Beam 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.

Application updates are not required, but strongly recommended. Failure to update your Beam App software may result in loss of feature. Check our website for a list of Previous Installers.

2.3 Public Beam Relays

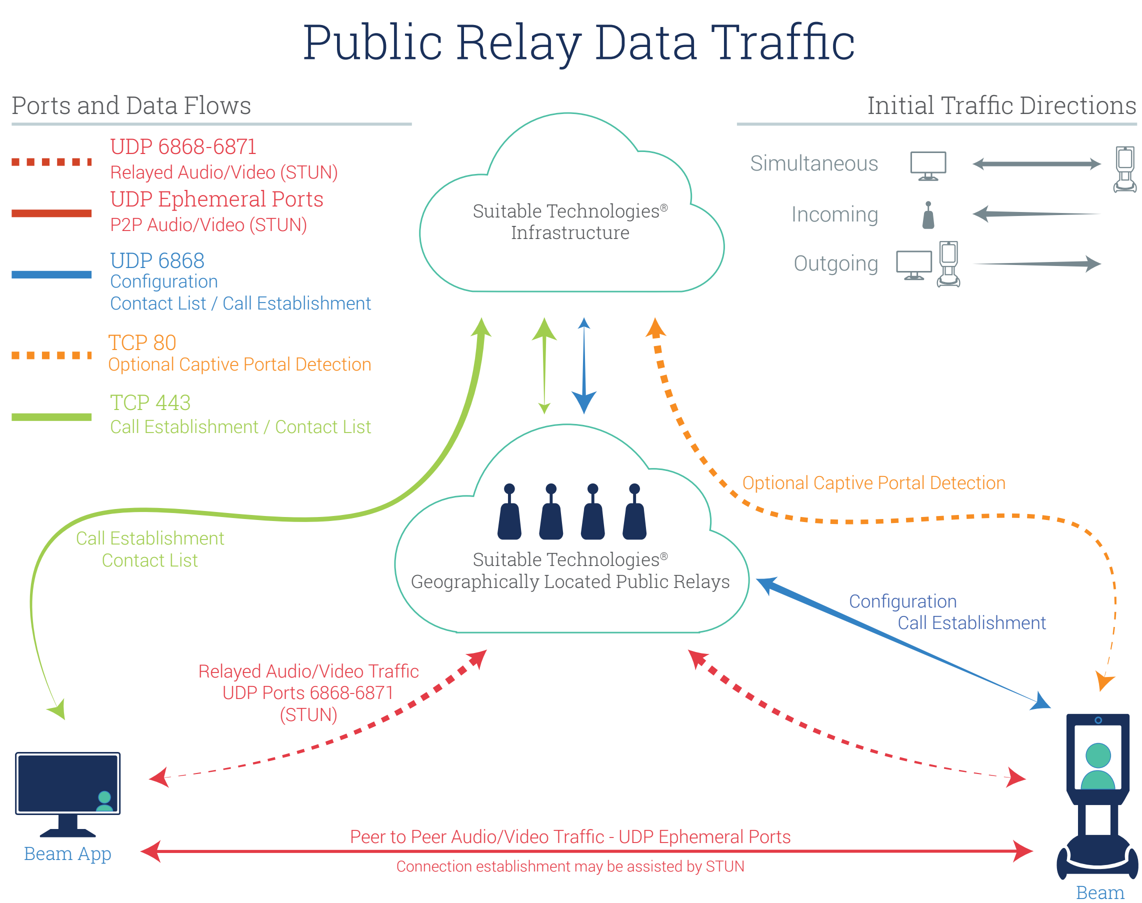
A relay server provides two important services to the Beam:

First, it provides a configuration relay used to offer a consistent IP and port to services (such as HTTPS) which does not support 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 infra-structure regarding its configuration or new software updates. The configuration relay is known as "beam_relay". It is most commonly set up on port 6868, though this can be configured on a site-to-site basis.

Second, it provides a media relay 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 known as "jingle_relay", and is generally set up to listen on ports 6869-6870.

The Beam will, by default, make use of one or more of Suitable's public relays. These relays are geographically positioned across the globe to minimize latency. The Beam will automatically select the most logical public relay based on ping data.

View a complete list of Beam Relays on our documentation page.



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 (07/2017) 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 TLS over an unencrypted proprietary relay protocol. TLS 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; however, the achievable action is limited to session disconnect. 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 OS X, 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.

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

3.3 Privacy Policy

The Beam software offers NO way to listen-in on conversations or retransmit images when the Beam is not in an active session.

For more information, see our [Privacy Policy](#).

3.4 Infrastructure

Suitable Technologies has the following levels of internal system access:

» Super Users	Full access user - Select Suitable personnel only
» Support Users	Limited access user - Organization tools only - Suitable Support
» Organization Admin	User level access - Ability to add and remove devices and users
» Organization Users	User level access - Access to admin designated devices only

3.4.1 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 TLS and checked with MD5Sum after being downloaded. Although the updates themselves are not signed, the download is done with an encrypted connection over HTTPS/TLS and the certificate used is signed by GoDaddy. The Beam initiates the download and will not download from any server that cannot authenticate itself as being suitabletech.com using a certificate is not signed by a valid CA. We are moving towards pinned certificates to protect against the possibility of a CA's private key being compro mised. Only a trusted subset of Beam employees can upload new releases.

3.4.2 Certificates

Suitable's web servers use TLS to prevent man in the middle attacks. Suitable's XMPP server also uses TLS. We use our own CA to produce the XMPP certificates. The Beam and PC client will only accept certificates from the Suitable CA.

The Beam authenticates to the web server and XMPP server using a self-signed certificate that it produces. The certificate is authenticated during the Beam pairing procedure. When the server sees a new certificate, it generates a pairing key, and encrypts it using the Beam's public key. The Beam decrypts the pairing key and displays it on its screen. By entering the pairing key he sees on the Beam's screen, the user ties the certificate currently on the Beam to that Beam's account on the Suitable servers.

3.4.3 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.

3.4.3 Data Backup

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

3.5 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.

3.6 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.

3.7 Beam 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.

3.8 Communication with Cloud Infrastructure

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

4.0 Support

Our Customer Success team is available to assist with any questions or concerns you may have.

» 1-855-200-BEAM (2326) x3
» support@suitabletech.com