ALPHATOUCH™

WHITE PAPER

Alpha Communications and Alpha Media, Inc.

Address Information

42 Central Drive, Farmingdale NY 11735-1202, USA
Phone: 631.777.5500 | **Fax:** 631.777.5599
Web: https://alphatouch.info

AWD281
September 2020, Rev: 01

SYSTEM OVERVIEW

The AlphaTouch system is an IP based smart video-intercom system that allows residents to have a two way video call with their visitors and release the door by using their AlphaTouch app on their smartphone. At its core, the AlphaTouch system features one or more touchscreen door entry stations, for easy installation and years of trouble-free operation. The system provides audio and visual calls without the need for pricey video-intercom monitors and their related wiring, labor and power supply requirements.

AlphaTouch Devices

In this whitepaper the terms "AlphaTouch Devices" or "Devices" are used to describe AlphaTouch brand hardware devices including Entry Panels, Concierge/Doorman/Staff Stations, and Video Monitors. These terms do not include third party device such as smart phones, smart speakers or standard telephones.

INTERNET SECURITY

TLS ENCRYPTION

All web session traffic between AlphaTouch devices, the AlphaTouch Cloud, and the AlphaTouch app is encrypted using a 256-bit Transport Layer Security (TLS) to protect all data. The AlphaTouch service supports up to TLS 1.2. The TLS protocol provides data encryption and authentication between devices, our servers, and the app to prevent third parties from stealing information.

The TLS connection is encrypted using AES-256, with SHA256 for message authentication and a 2048-bit RSA key exchange mechanism.

The certificate information used can be viewed from any web browser by going to AlphaTouch.info and clicking to view the certificate in your browser.

USER AUTHENTICATION

Any resident, building manager or administrator that logs into the AlphaTouch website or the AlphaTouch App is authenticated by entering an email and password. The email/password combination allows AlphaTouch to verify that the person attempting to connect to AlphaTouch is, in fact, using a valid pair of identifiers to gain access to the AlphaTouch Cloud.

The entire email/password exchange takes place within a Transport Layer Security (TLS) session that begins when the user accesses the logon screen of the AlphaTouch website or app via Hypertext Transfer Protocol Secure (HTTPS). The TLS session protects the exchange of authentication data by encrypting it thus establishing secure communication.

User passwords must meet the following criteria:

- Must be between 8 and 20 characters in length
- Must contain at least one lowercase letter
- Must contain at least one uppercase letter
- Must contain at least one numeric digit

If a password is forgotten a reset link can be emailed to the user

DEVICE AUTHENTICATION

All AlphaTouch Devices authenticate themselves when sending and retrieving API data by exchanging credentials and commands with the AlphaTouch Cloud. Devices use the same process that a user would authenticate themselves through a digital certificate at the AlphaTouch data center. A device establishes a TLS session with AlphaTouch before it begins to exchange information.

In doing so, AlphaTouch presents its digital certificate to the device, which it can check in much the same manner as a web browser would. Unlike user authentication, this process is automated by the device software when required.

When a device attempts to establish a TLS session to download data or send commands, the AlphaTouch servers force it to present its client certificate before gaining access to the system. If it has valid credentials that were issued by AlphaTouch a TLS session will be initiated and the device can download data and send commands. If not, it is blocked from any further activity.

NETWORK

The AlphaTouch devices will not accept inbound connections. It will only listen to network traffic within the HTTPS session which was initiated by the AlphaTouch Cloud servers itself. This protects the AlphaTouch devices against unauthorized access because it simply will not accept unsolicited communications.

For example, it is not possible to do any of the following to an AlphaTouch device. Initiate a Telnet, FTP, HTTP/S or any other type of communications session; burden the device through a denial of service (DoS) attack; give the device a virus; or gain access to the file system.

IP CONFIGURATION AND DHCP

AlphaTouch devices must still have some communications with the rest of the IP network on which it resides, particularly with respect to establishing network operating parameters.

A device will need to have an IP address. This can be established in one of two ways:

- Using the "DHCP" protocol, where your device is dynamically assigned an IP address from the router it is connecting to.
- Using a Static IP if required by the local network, which can be configured on the device's Operating System settings.

AlphaTouch devices support the DHCP protocol for ease of configuration. DHCP has become the preferred method of managing network devices on most corporate LANs. Supporting DHCP presents no additional security risks for the control panel or the AlphaTouch Cloud itself and greatly simplifies network administration.

For networks that do not support DHCP, or network administrators who would prefer to assign an IP address manually, a device has a local settings interface that allows an administrator to enter all network configuration parameters directly from the device itself.

ALPHATOUCH CLOUD DATA CENTER AND HOSTING

PHYSICAL SECURITY

AlphaTouch data centers are outfitted with biometric scanners and secure card access to the collocation services areas of the data center. Additionally, all AlphaTouch equipment is kept in secure locations. On-site security personnel monitor hosting facilities 24/7 via indoor and outdoor video surveillance. Data center access requires security desk check-in and is managed 24/7. Local key management is enforced for racks and cabinets.

ALPHATOUCH CLOUD NETWORK

The AlphaTouch Cloud is hosted on servers through Rackspace. They are an **SSAE 18 (SOC1 / SOC2 / SOC3)** audited data center. **SSAE 18** is the authoritative auditing standard and means that they have been through an in-depth audit of their data centers' privacy and security. This standard was developed by the American Institute of Certified Public Accountants (AICPA). It demonstrates that they have adequate controls and safeguards when they host or process data belonging to their customers.

For more information on security at Rackspace please visit the ssae16.com, which describes the SSAE 18 standard in greater depth.

BACKUPS

Regular backups are performed on all AlphaTouch data, including installation and building information, call logs, resident information, and billing information. All backups are stored redundantly and are encrypted using a 256-bit Advanced Encryption Standard (AES-256), one of the strongest encryption standards available for electronic data.

PAYMENT SECURITY

PAYMENT DATA

To ensure that we deploy the highest security measures for all billing information, we do not store any credit card data on our servers. Instead, all credit card information is encrypted with AES-256 and handled by our payment platform vendor. In addition, decryption keys are stored separately, and the infrastructure for storing, decrypting, and processing credit card information runs on an entirely separate infrastructure.

PCI COMPLIANCE

Our payment platform vendor is PCI DSS (Payment Card Industry Data Security Standard) compliant. This means that they are validated and held to the same industry standards as all major credit cards including Visa, MasterCard, American Express and Discover.

CONTACT US

For more details and information or to request a demo of AlphaTouch please contact us.

TOLL-FREE Customer Service: 1-800-666-4800

Email: info@alphatouch.info

For help with AlphaTouch you can visit the AlphaTouch Help page.