Cybersecurity Summary

# Trane® Connect™ | Remote Access

## What is Trane Connect?

Trane Connect is a software-as-a-service that allows authorized users of Tracer® building automation systems (BAS) to access the Trane Cloud environment.

Remote access is achieved with Trane Connect through an initial outbound, secure connection to the Tracer controller behind a building's firewall.

Remote access to a building automation system (BAS) gives authorized users—both a company's and Trane's service personnel—greater flexibility to remotely configure, manage and service a facility faster, cost effectively, and securely.

## HOW IT WORKS

### Endpoint security

Tracer BAS, including Tracer® SC+, SC, and legacy controllers can be configured to connect to the Trane Cloud. This connection utilizes the WebSocket protocol for current product lines and OpenVPN for legacy Trane controllers as a simple and secure solution. This approach provides simple and secure connectivity in a standardized way.

**Security features of Trane Connect**

- Securely connects a Tracer BAS controller with the Trane Cloud to provide remote access to a facility with the latest TLS / SSL encryptions.
- Is a firewall friendly solution to ensure secure connectivity to the Trane Cloud.
- Uses outbound ports Websockets/OpenVPN (TCP 443) for current BAS controllers.
- Uses outbound ports OpenVPN (UDP 1194) for legacy Tracer BAS controllers.
- Uses an encryption level of 256-bit AES.
- The Tracer BAS controller initiates all communication to establish the outbound connection to Trane Cloud. This facilitates the secure remote access connection.
- Remote access connection requires proper user authentication and authorization on the cloud level as well as on the Tracer BAS controller. This is performed in a 3-step approach.

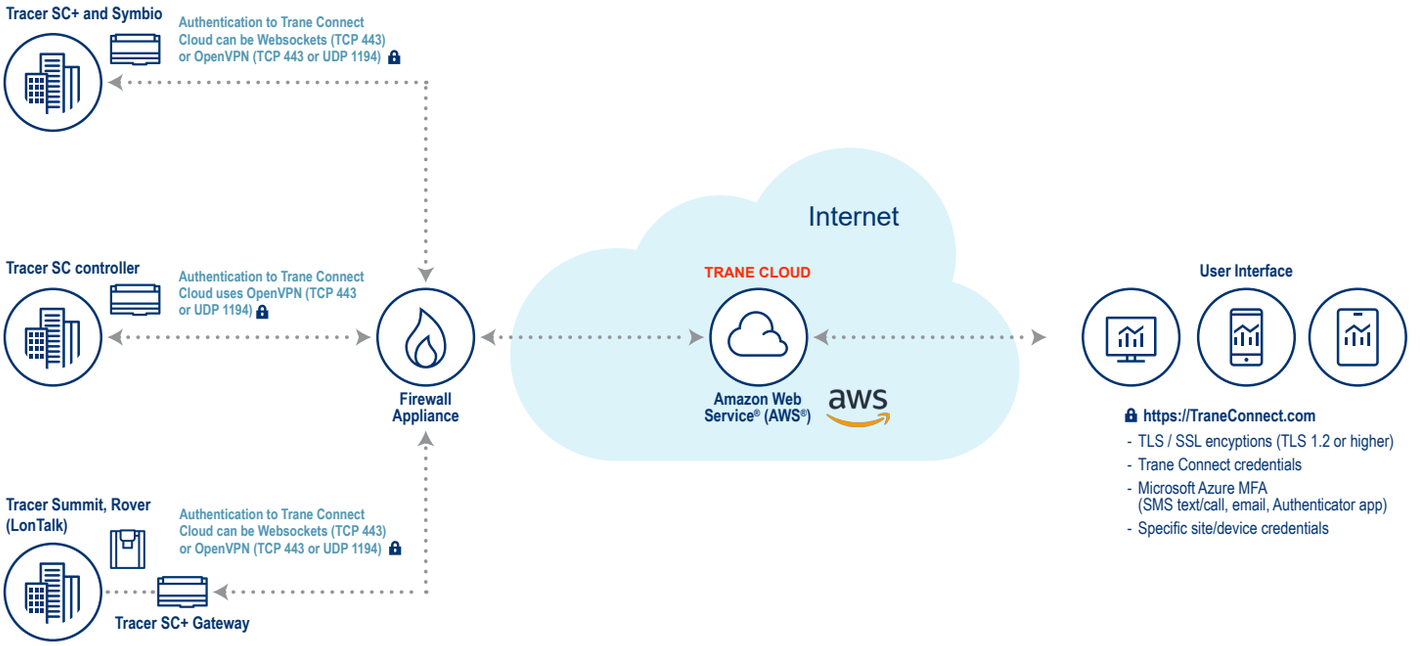
1. Tracer BAS controller initiates the handshake for connectivity.
2. Validate user authorization and authentication in the Trane Cloud*.
3. Direct authentication to the Tracer BAS controller*.

***Note:** Valid credentials are needed

**Firewall requirements for remote access with Trane Connect:**

- Port 443 (TCP) - outbound
- Port 1194 (UDP) - outbound

## Network Security




1. User registers the Tracer BAS controllers on the Trane Cloud. This is performed in a 3-step approach as stated before.
2. User authenticates themself through the Trane Connect portal to access the Tracer BAS controllers. This is the only way to access the established secure tunnel to the Trane BAS controller.
3. Trane Connect uses Microsoft® Azure® multi-factor authentication which is a built-in service. All connections are secured with the latest TLS / SSL encryptions (TLS 1.2 or higher).
4. Once the Trane Connect remote access session has been established, the user must provide login credentials to gain access to every Tracer BAS controller.
5. Every Trane Connect remote access session is deactivated as users log out from each Tracer BAS controller.
6. The Trane Cloud server tracks the remote access activity through the Trane Connect interface.

## Data Privacy

Trane Technologies™ Company, LLC ("Trane Technologies") respects individual privacy and values the confidence of its customers, employees, vendors, consumers, business partners and others. To learn more about Trane Technologies Privacy Policies, please visit https://www.tranetechnologies.com/en/index/privacy-policy.html.

## Data Security

Trane Tracer BAS controllers and Trane Cloud utilization of data is limited to HVAC Machine Data only. HVAC Machine Data is data generated and collected from the product or furnished service without manual entry. HVAC Machine Data is data relating to the physical measurements and operating conditions of a HVAC system, such as but not limited to, temperatures, humidity, pressure, HVAC equipment status. HVAC Machine Data does not include Personal Data and, for the purposes of this document, the names of users of Trane's controls products or hosted applications shall not be Personal Data, if any such user chooses to use his/her name(s) in the created accounts within the controls product (e.g., firstname.lastname@address.com).

HVAC Machine Data may be used by Trane: (a) to provide better support services and/or products to users of its products and services; (b) to assess compliance with Trane terms and conditions; (c) for statistical or other analysis of the collective characteristics and behaviors of product and services users; (d) to backup user and other data or information and/or provide remote support and/or restoration; (e) to provide or undertake: engineering analysis; failure analysis; warranty analysis; energy analysis; predictive analysis; service analysis; product usage analysis; and/or other desirable analysis, including, but not limited to, histories or trends of any of the foregoing; and (f) to otherwise understand and respond to the needs of users of the product or furnished service.

## Technologies used by Trane Connect

The WebSocket protocol facilitates real-time data transfer by providing a standardized way for the server to send content to the client without being first requested by the client. Trane uses WebSocket Secure (wss://) which uses a TLSv1.2 or higher encrypted connection using TCP port number 443 to establish a secure connection to the Trane Cloud. The WebSocket protocol was standardized by the IETF as RFC 6455.

OpenVPN is a software application that implements virtual private network (VPN) techniques for creating secure point-on- point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.




BAS-SLB072
09/19/2023