Secure Data Collection

Adding value to your BAS with intelligent analytics

Safely tapping the powers of BAS information

A network-based Trane® Building Automation System (BAS) enables you to join the new era of Intelligent Buildings and Building Energy Management Systems (BEMS).

- Now Trane can continuously monitor your BAS, and provide advisories to your local Trane service team so they can keep your HVAC system finely tuned
- During the first year warranty period, Trane uses the BAS data to troubleshoot and triage potential HVAC equipment issues
- Over the long term, Trane can use analytics to recommend additional ways to drive building performance even higher, and positively impact your business outcomes

All this, and much more, is made possible when Trane collects data from your building automation system—under the industry's most rigorous and consistent cyber security practices.

Intelligent analytics are included in your first year Tracer® BAS controller support.

With your approval, we will automatically initiate secure data collection to enhance that support.

As a global leader in commercial air conditioning systems, services and solutions, Trane has developed industry-leading best practices for cyber security. When Trane systems operate on your network, your cyber security is always a top priority.

Trane Security Practices for Intelligent Analytics

At Trane, we're making sure that intelligent buildings don't open the door to cyber threats. Our practices for secure data collection utilize the latest cyber security methods to mitigate the risks.

We Only Collect HVAC System Data

Data collection by Trane is limited to HVAC equipment and system operating data. Depending on your company's goals, we may also look at energy use and demand.

You Own Your Data

You grant Trane permission to use the data to help improve the performance of your building automation system. Trane does not share your information externally. We never share your data or expose the source of that data to anyone outside our company.

Our Cloud is Secure

A multi-level security approach uses both Amazon Web Services and OS level firewalls. Data can only be accessed by authenticated Trane personnel, or by customers who have been authorized to use the Trane portal. The Trane Cloud is redundant—a loss of any instance does not impact our environment. All data communication is encrypted via SSL/TLS and access is authenticated and audited to verify security.

Secure Data Collection: How it works

1. Your Tracer® BAS controller initiates outbound communication to the Trane Intelligent Services server
2. Data collection only requires an outbound port: Port 443 (TCP)
3. The BAS controller sends an HTTPS POST to send data to the Trane Cloud
4. All data traveling from the Tracer BAS controller to Trane is encrypted using Transport Layer Security (TLS)
5. Regular data collection is configurable, and may be sent every 5 to 15 minutes
6. The Tracer BAS ontroller sends notification of alarms immediately when they occur
7. The Trane Cloud receives data and stores it for analytical and service uses—data is stored in a multi-tenant database
8. Only authenticated Trane personnel, and customers who have been authorized to use the Trane portal, can access data
9. Accessibility is limited using precisely defined user role-based access control, as well as data/ domain-level access control

TRANE

Trane – by Trane Technologies (NYSE: TT), a global climate innovator – creates comfortable, energy efficient indoor environments through a broad portfolio of heating, ventilating and air conditioning systems and controls, services, parts and supply. For more information, please visit *trane.com* or *tranetechnologies.com*.

BAS-SLB073-EN
04/27/2020