KEY2ACT

Connect Security

FAQ

January 10, 2019

Contents

Overview

This document provides answers to common network and security questions about the Connect product from KEY2ACT™.

If there are additional questions that are not covered in this document, please contact a sales representative from KEY2ACT™.

General Security

How do you get data from a sensor/endpoint and into AWS? What level of encryption are you using? If VPN, please reference a standard.

All data is sent from the MiniAgent to the AWS Database via SSL. The SSL Cipher used is ECDHE-RSA-AES256-GCM-SHA384. The data collected from the BAS uses BACnet or oBIX and the level of security is dependent on the level of security setup by the controls installer.

How do you authenticate the connections to the endpoints from AWS to prevent rogue systems from feeding data?

The Connect MiniAgent uses a specific set of credentials set up by K2A and AWS to authenticate to the Database and store the data. All communications are secured via the SSL connection discussed above.

What security controls are in place to manage communications between the endpoints and the gateway device?

We use security groups within an AWS VPC to limit what connections can be made to the database. This is secured not only through firewall protections, but SSL and login credentials as well.

What security controls are in place to lock the gateway down to again protect customers and our systems & interests?

Our MiniAgent only uses outbound ports to AWS, uses SSL to communicate to AWS resources, and each agent has a client certificate for the server to verify the agent is legitimate.

How is patching handled?

We push automatic updates down to all MiniAgents and server patching is handled via a maintenance schedule.

Is there any communication / workflows that is bidirectional to customer equipment from the gateway?

Yes, the MiniAgent can receive requests to activate/adjust points in the BAS, but this must be configured by the installer of Connect. The communication from the configuration software to AWS is all SSL encrypted and locked down through

login credentials. All communication between AWS and the MiniAgent is SSL encrypted and secured as described above.

How are ports filtered and managed?

AWS ports are filtered and managed by AWS security groups, OS Firewall rules, and Network ACL's. Ports on the customer's site where the MiniAgent reside are filtered and managed by their IT provider.

Do the gateways accept ANY information from external networks through the customer connections? IE – is the endpoint EVER routable to the Internet? How do you ensure this independent of customer network configurations?

It is recommended that the MiniAgent be placed behind a firewall with no inbound ports opened and routed to the MiniAgent. With that said, if the MiniAgent is exposed to the web via an inbound firewall port and public IP the device could accept requests, but the requests would need to conform to the Connect proprietary protocol and would require the SSL encryption to be deciphered.

What is the name and address of the location where the data will physically reside?

Amazon Web Services Northern Virginia Region, there are 6 data centers and the data will be spread across them all. Amazon does not provide us with addresses for the data centers.

Does the application encrypt data before sending it over the internet or an open network?

Data is not encrypted at rest, but is encrypted in transit.

If the application includes a web interface, please identify the type(s) of secure connection supported in a comment.

There is currently no Web UI

Can the vendor supply the CPU chassis serial number and hard drive serial number for the hardware that will be utilized?

No, data is hosted in AWS and we have no access to the physical hardware, nor do we know what physical machines at AWS our applications are running on.

Is the application HIPAA compliant?

No

Are you compatible with 3rd party encryption? (McAfee or MS Bitlocker)?

Unknown/Untested

Will you utilize any subcontractors to develop, deliver, support, or process the product or service?

Yes

Has the vendor, product, or service (including subcontractors relevant to this project) been involved in, included with, part of, affiliated with, or in any way connected to or a target or victim of a data breach or security incident?

No

Hosted Environment: Physical Security

Does a third party host the platform?

Yes, Amazon Web Services. SOC1, SOC,2, and SOC3 reports are available. For us to send the SOC reports an NDA between the customer and Amazon must be in place.

Are documented security policies and procedures in place to guide personnel in granting, controlling, and monitoring physical access to the data center facility?

Yes

Is written documentation and supervisor approval needed to add, modify, and/or terminate access privileges?

Yes

Does corporate security management perform a review of badge access privileges and physical keys on a periodic basis to help ensure that access privileges are current?

Yes

Are digital surveillance cameras in place throughout the data center facility to monitor activity?

Yes

Is the data center facility monitored 24 hours per day?

Yes

Is physical hardware maintained behind locked server racks and cages?

Yes

Hosted Environment: System Administrative Security

Are system access privileges of terminated employees revoked as a component of the employee termination process?

Yes

Are strong password controls for access to systems in place?

Yes

Is a Privileged Access Management system in place for administrative access (e.g. password vaulting and activity recording)?

Yes

Are vendor recommended security patches applied in a timely fashion?

Yes, all databases security patches are applied by Amazon. For application servers they are applied as required.

Is intrusion detection/prevention monitoring in place?

Yes

Web Hosted Application Security

Please describe how authentication to the web application is secured (e.g. two factor authentication, password) in a comment.

Username/Password Combination

Please describe how user accounts are provisioned (e.g. separate database, integrated with on premise application, integrated with customer enterprise directory).

Application database in AWS

Network Data Requirements

What are the network bandwidth requirements?

The bandwidth requirements and frequency depend on trend interval and object counts configured by the user in the KEY2ACT Connect software. Connect requires ~25 bytes per object that is trended. If you trend 2,000 objects 4x per hour it's roughly 200kB per hour.

Software updates range in size, but are typically applied once per month and are roughly 8MB.

Are there any load balancing requirements?

No

Are there any layer 2 or layer 3 adjacency requirements?

No

Are there any DNS requirements?

Yes, the MiniAgent installed on-site and the Desktop software will require DNS to access the cloud services for Connect.

Are there any POE requirements? If yes, please list the power draw per types of devices to be deployed.

No

What are the per device overall network throughput projections?

The bandwidth requirements and frequency depend on trend interval and object counts configured by the user in the KEY2ACT Connect software. Connect requires ~25 bytes per object that is trended. If you trend 2,000 objects 4x per hour it's roughly 200kB per hour.

Software updates range in size, but are typically applied once per month and are roughly 8MB.

If we do network maintenance during our standard Sunday 2am to 4am maintenance window, will your application be ok?

Yes

Does this solution need to be able to access public internet?

Yes

Are there any wireless requirements?

No

What are the make, model, and relevant network specifications for each model of hardware that will be deployed?

Embedded Linux device, Model Number MA-001. Network Specs: 100 Mbps Ethernet.

What are the security and/or firewall requirements for this request?

The Connect MiniAgent (physical data pump) will need to be installed on the local network with access to the Building Automation System (BAS). The MiniAgent will require 4-outbound ports (5432, 57000, 57001, and a Custom Port assigned when contract is signed) for connectivity to the KEY2ACT Cloud.

How many connections to the internet are required?

One (1) internet connection is required per MiniAgent. A MiniAgent is required per Building Automation System connection.

What are the IP requirements?

Private Static IP per MiniAgent