HOW-TO GUIDE

HT0026 rev 6

Security in ABB Ability™ BE Sustainable with Active Energy

ABB Ability™ BE Sustainable with Active Energy has a number of solutions available to allow data that is relevant to the energy consumption in a building to be collected on an automated basis. Examples of this data are:

- Energy Meter Data
- Sensor Data
- Production Data
- Building Occupancy Data
- Data from Building Management Systems/Building Automation Systems

This document describes how to configure a site to allow such data to be collected via SQL databases, CSV files, BACnet networks and **ABB Aspect** series controllers.

1 Introduction

ABB Ability™ BE Sustainable with Active Energy is a Cloud based SaaS (Software as a Service) solution that provides analytical tools to monitor a building's energy consumption in order to identify and target energy efficiency improvements.

Data is collected from the energy meters (electrical, gas, water, etc.) as well as other data that may be relevant to the buildings energy consumption which are known as energy driving factors. Driving factors vary from building to building as they are dependent on factors such as building type, building use and on what mechanical and electrical services are installed in the building. Examples of driving factors are ambient temperature, ambient humidity, ambient light level, building occupancy levels, production levels and building opening hours.

ABB Ability™ BE Sustainable with Active Energy has developed interfaces to collect from the building the data described above from a variety of sources. Examples of data source are

- Building Management Systems (BMS)/ Building Automation Systems (BAS)
- SQL Databases
- CSV Files
- Energy Data Loggers
- Online data sources (such as weather services)

ABB Ability™ BE Sustainable with Active Energy is hosted in Amazon Web Services (AWS). The means of collecting the data and placing it on the ABB Ability™ BE Sustainable with Active Energy servers in AWS depends on the source of the data.

The bureau monitors the data collection to try to prevent loss of data and ensure full data integrity. Restricted access to customer is provided to bureau engineers to trouble shoot any data collection issues.

2 Data Collection Methods

ABB Ability™ BE Sustainable with Active Energy supports a number of connections from the ABB Ability™ BE Sustainable with Active Energy server to the customer site to facilitate data collection. The data is collected from the customer site, then stored and backed-up in ABB Ability™ BE Sustainable with Active Energy databases. The processed data is displayed on the ABB Ability™ BE Sustainable with Active Energy website. Data collection from the customer site can be through one of the following options.

ABB ASPECT SERIES CONTROLLERS (MATRIX/NEXUS/ENTERPRISE)

This solution allows data from ABB Aspect series controllers (Matrix/Nexus/Enterprise) to automatically connect to the ABB Ability™ BE Sustainable with Active Energy servers.

The connection between the Aspect controllers and the ABB Ability™ BE Sustainable with Active Energy is via an API. The data is pushed from the controllers via an outbound internet connection.

DATA COLLECTION AGENT

This solution involves the customer installing a ABB Ability™ BE Sustainable with Active Energy application on a Windows PC which will collect data from the particular data source for that installation. This application is called a Data Collection Agent (DCA) and runs as a schedule task within Windows at configurable intervals. When the DCA runs, it connects to the data source and collects any new data and places it initially in an SQLite database on the Windows PC before sending the data to the ABB Ability™ BE Sustainable with Active Energy servers over a TLS web socket.

There are several variants of the Data Collection Agent (DCA) and the difference between each variant is the way it connects to the data source. The way the DCAs connect to the ABB Ability™ BE Sustainable with Active Energy servers is common across all DCAs

DATA COLLECTION AGENT PC REQUIREMENTS

The DCA should be installed on a PC running Windows 10 (64-bit).

This PC must be constantly powered on and have access to the Internet. TLS connections to the ABB Ability™ BE Sustainable with Active Energy servers are made on TCP port 443 which allow the Data Collection Agent to receive new configuration, return collected data, and return status information.

All communications with the ABB Ability™ BE Sustainable with Active Energy data center are encrypted (using HTTPS). The Installable DCA makes outbound connections only and cannot be accessed remotely.

Once outbound connectivity is in place, the DCA fetches configuration from the ABB Ability™ BE Sustainable with Active Energy servers, collects the data from the data source, and then stores the collected data back to the ABB Ability™ BE Sustainable with Active Energy servers. It is not possible for the ABB Ability™ BE Sustainable with Active Energy servers or anyone else to initiate communications with the DCA from inside or outside the network.

FIREWALL REQUIREMENTS – DATA COLLECTION AGENT

If the network is protected by a firewall that filters outbound traffic, it must be configured to allow the DCA to communicate with ABB Ability™ BE Sustainable with Active Energy. The following network traffic is generated by the DCA:

1. **TLS encrypted connections to activeenergy.ie on TCP port 443**. These are used to fetch configuration information and store collected data.
2. **DNS** requests on UDP port 53.

TLS connections to the ABB Ability™ BE Sustainable with Active Energy servers in Amazon's AWS data centres (EU Ireland) on TCP port 443. These are used to fetch configuration information and store collected data. This endpoint is managed by Amazon's load balancer which distributes uploading across many servers in the EU region. For this reason, no single IP destination can be specified.

The DCA forwards all traffic to these three hostnames on port 443:

- `config.service.activeenergy.ie`
- `storage.service.activeenergy.ie`
- `nagios.service.activeenergy.ie`

Depending on the firewall, you may be able to specify the following rules, in order of preference:

a. Allow all outbound traffic to any destination on port 443
b. Allow all outbound traffic to *.activeenergy.ie on port 443

PROXY REQUIREMENTS

The DCA supports the use of a HTTP CONNECT or SOCKS proxy. The proxy must be configured to allow the DCA to make TLS and HTTPS connections to any server on TCP port 443.

If proxy authentication is required, the DCA can be configured to use HTTP Basic Authentication.

To configure a proxy, update the parameters in the config_agent_task.ini, remote_agent_task.ini and status_agent_task.ini in the \etc\ folder.

[proxy]

type = HTTP

host = 192.168.x.x

port = 8080

username =

password =

The possible proxy types are HTTP, SOCKS4 and SOCKS5.

FIREWALL REQUIREMENTS – ASPECT SERIES CONTROLLERS

If the network is protected by a firewall that filters outbound traffic, it must be configured to allow the Aspect controller to communicate with ABB Ability™ BE Sustainable with Active Energy. The following network traffic is generated by the Aspect series controller:

1. **TLS encrypted connections to cylonaem.com on TCP port 443**. These are used to store collected data.
2. **DNS** requests on UDP port 53.

TLS connections to the ABB Ability™ BE Sustainable with Active Energy servers in Amazon's AWS data centres (EU Ireland) on TCP port 443. These are used to store collected data. This endpoint is managed by Amazon's load balancer which distributes uploading across many servers in the EU region. For this reason, no single IP destination can be specified.

The Aspect series controller forwards all traffic to cylonaem.com on port 443:

Depending on the firewall, you may be able to specify the following rules, in order of preference:

a. Allow all outbound traffic to any destination on port 443
b. Allow all outbound traffic to *.cylonaem.com on port 443
c. DNS requests on UDP port 53.

PROXY REQUIREMENTS

If the Aspect series controller is connected to the customer's network and there is a proxy server in use, the proxy server details can be entered in a `jvm.params.properties` file. The file should be saved into the `userfiles` sub-folder within the Aspect project folder. A sample is detailed here

```
JVMPARAMS="-Dhttp.useProxy=true-Dhttp.proxyHost=10.64.14.152-Dhttp.proxyPort=8080-
Dhttp.nonProxyHosts=\"localhost|127.*|10.82.*|10.65.*\"-Dhttps.useProxy=true-Dhttps.proxyHost=10.64.14.152
-Dhttps.proxyPort=8080"
```

In this example the proxy server is at `10.64.14.152` and local traffic that does not need to go via the proxy is defined in the `Dhttp.nonProxyHosts` Section of the file.

3 Security Overview

ABB Ability™ BE Sustainable with Active Energy utilizes the most advanced technology for internet security available today. When the application is accessed using a ABB Ability™ BE Sustainable with Active Energy-supported browser, Transport Layer Security (TLS) technology protects customers' information using both server authentication and data encryption, ensuring data is safe, secure and available only to customers with current ABB Ability™ BE Sustainable with Active Energy log-in details.

ABB Ability™ BE Sustainable with Active Energy Security:

1. ABB Ability™ BE Sustainable with Active Energy is hosted on Amazon's AWS cloud hosting platform in Europe. Our servers are placed in two completely independent availability zones within AWS and our application is designed to withstand the failure of either availability zone.
2. Our servers are backed up once a day to Amazon's S3 highly redundant storage platform and can be restored from backup very quickly in the event of a complete system failure.
3. The Amazon S3 Service Level Agreement guarantees an uptime of 99.9 percent.
4. Our servers are backed up once a day to Amazon's S3 highly redundant storage platform and can be restored from backup very quickly in the event of a complete system failure.
5. ABB Ability™ BE Sustainable with Active Energy provides each user in an organization with a unique user name and password that must be entered each time a user logs on.
6. ABB Ability™ BE Sustainable with Active Energy is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders.
7. Customer data is located in secure data centers within Europe and have 24-hour security with physical access limited to authorized personnel only.
8. To ensure reliability, data is duplicated across multiple disks, machines and data centers and it is regularly backed up.
9. A load balancer is used to route requests between machines. Machines are constantly monitored using internal and external tools with automated alerts being sent to ABB Ability™ BE Sustainable with Active Energy staff if problems are detected.
10. Data travelling between the customers' site and the ABB Ability™ BE Sustainable with Active Energy Data Storage Server is encrypted using HTTPS protocol (encrypted HTTP) so that it cannot be intercepted.
11. Data travelling between the browser and the web server is protected using industry standard Transport Layer Security (TLS) encryption.
12. ABB Ability™ BE Sustainable with Active Energy uses robust security measures to protect Customer Data from unauthorised access, maintain data accuracy, and help ensure the appropriate use of Customer Data.
13. Customers are responsible for maintaining the security and confidentiality of their ABB Ability™ BE Sustainable with Active Energy usernames and passwords.

4 Amazon WEB Services Security

1. **Amazon Web Services** (**AWS**) is used to host both the data sources and the application(s).
2. **AWS** Security best practices are employed https://aws.amazon.com/architecture/security-identity-compliance/
3. **AWS RDS** is used for housing data. Backup and recovery is managed automatically. https://docs.aws.amazon.com/rds/index.html
4. A clustered apache DS server hosted on AWS EC2 is used to host LDAP. Strict security groups are applied and cloud watch is being used https://aws.amazon.com/ec2/
5. Amazon Web Services can be accessed from ABB offices in Dublin and Atlanta only, using two-factor authentication: a username and password, and a security key obtained from an electronic fob.
6. Amazon security groups (see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html) are applied to **RDS** (see https://aws.amazon.com/rds/) connections, and to virtual machines (https://aws.amazon.com/ec2/). This whitelists access by port, for example; the production database connections are only accessible from the production application servers. Amazon **S3** storage (https://aws.amazon.com/s3/) is used for storage of reports and logos. An access key and secret access key is used to access this API. These keys are maintained in environment specific files, on the production servers.
7. **Amazon Data Centers** are securely designed and controlled. https://aws.amazon.com/compliance/data-center/controls/

5 Security and Privacy

DATA AT REST PROTECTION

Customer data is stored in Amazon Web Services RDS. Energy consumption data has a separate schema per customer in the AWS SQL database.

Data pertaining to our customers is stored in (an) Amazon RDS database(s). AWS security groups are used to restrict access to these databases to the ABB offices in Dublin and Atlanta only. Access to the AWS management console is protected by a username and password pair, electronic fob for two factor authentication, and a machine on the ABB corporate network.

DATA IN TRANSIT PROTECTION

Data sent between the customer site and the ABB Ability™ BE Sustainable with Active Energy servers is secured as detailed in *Data Collection Methods* on page 3. Data is transmitted from Data Collection Agents via a secure web socket to our storage server. TLS is a web standard for encrypting a connection between a client (DCA) and server (storage server).

Data viewed in the active energy management portal is also protected using TLS as all authenticated requests are over HTTP over TLS (or simply https).

IDENTITY MANAGEMENT

All customer user IDs are hashed and salted in a database.

Access is provided to the meter / sensor data via the ABB Ability™ BE Sustainable with Active Energy portal. A unique username and password is provided to each nominated user. Access rights to meter / sensor data is defined by the customer e.g. who can see what data.

Restricted access is provided to ABB employees as required for site set-up and to monitor on-going data accuracy and data integrity.

Multi-tenancy is applied at the application level.

All passwords are hashed and salted in a database.