



**Intelligent Plant™**

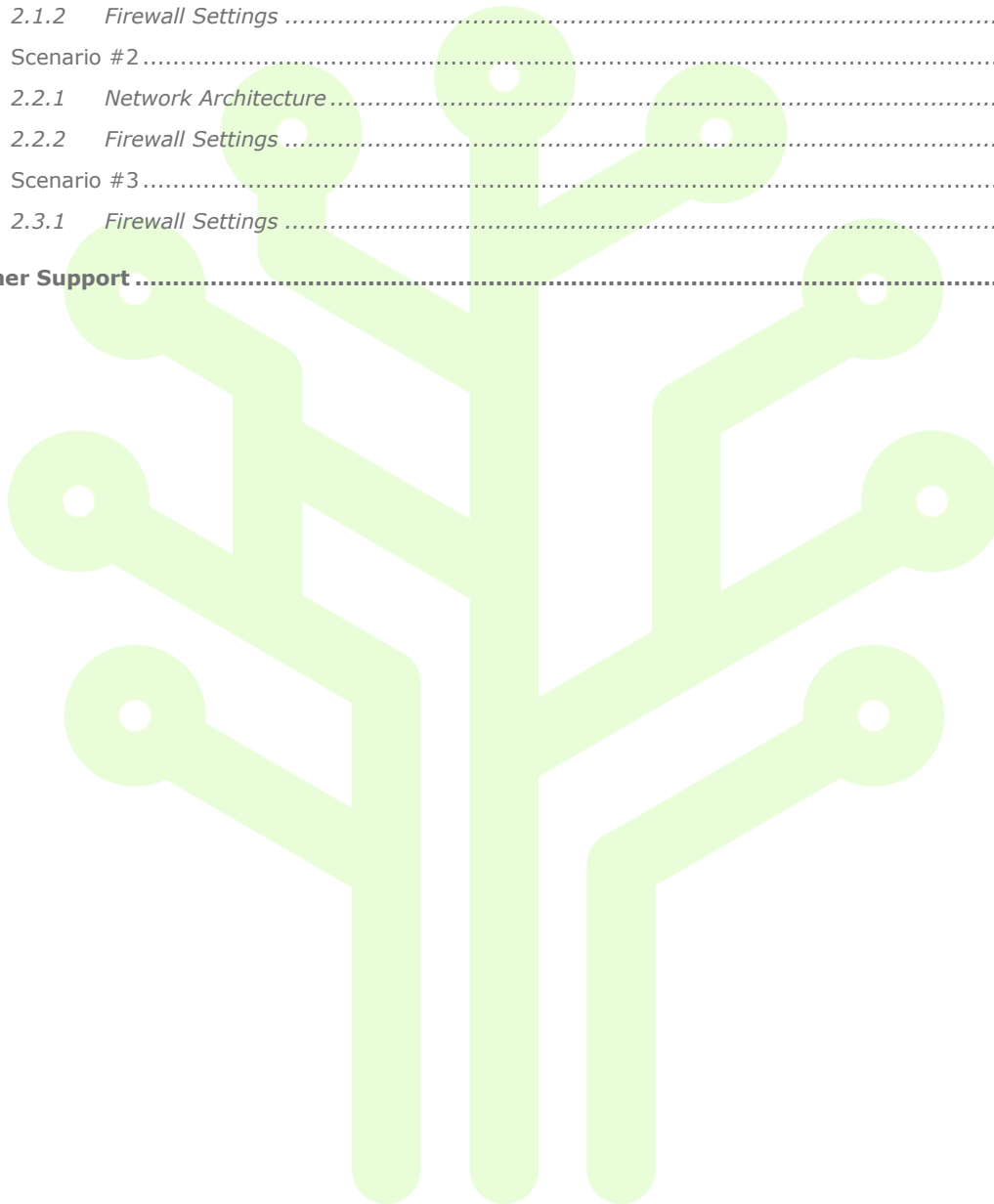
*Inform, Enhance, Grow. Intelligently.*



# **Alarm Analysis Network Architecture**

# Table of Contents

<b>1</b>	<b>Overview</b> .....	<b>3</b>
1.1	Terminology .....	3
<b>2</b>	<b>Installation Scenarios</b> .....	<b>4</b>
2.1	Scenario #1 .....	4
2.1.1	Network Architecture .....	4
2.1.2	Firewall Settings .....	4
2.2	Scenario #2 .....	5
2.2.1	Network Architecture .....	5
2.2.2	Firewall Settings .....	6
2.3	Scenario #3 .....	7
2.3.1	Firewall Settings .....	8
<b>3</b>	<b>Customer Support</b> .....	<b>9</b>



# 1 Overview

Alarm Analysis and Data Core (Intelligent Plant's data-routing and data-access software) provide a highly configurable toolkit for importing and analysing Alarm & Event data.

This document describes best practice for installation of Alarm Analysis software within secure networks, obtaining data from high-security militarized zones, and managing data access from the Industrial App Store.

We cover 3 scenarios:

- A stand-alone installation of Alarm Analysis gathering local data;
- Alarm Analysis on the cloud gathering data from OPC;
- Alarm Analysis on the cloud and installed on the PIN (for users on different domains) gathering data on printer ports.

These illustrate the flexibility of Alarm Analysis and robust, firewall friendly, data transfer of Data Core. It is by no means exhaustive, however. Get in touch to discuss your particular requirements.

## 1.1 Terminology

Alarm Analysis	Intelligent Plant application that processes Alarm & Event data to produce interactive EEMUA (Engineering Equipment and Materials Users Association) grade reports and analysis.
Data Core Node	Intelligent Plant's data-routing and data-access software. Operates as a Windows service.
Industrial App Store	Cloud portal for industrial apps (including online editions of Intelligent Plant applications).
App Store Connect	An instance of Data Core Node pre-configured for secure connections with the Industrial App Store.
PCN	Process Control Network.
PIN	Process Information Network.
BN	Business Network. Also referred to as the Enterprise Network.
HTTPS	Hyper-Text Transfer Protocol Secure. The communication protocol of the Web with encryption.
TCP	Transmission Control Protocol. A network communication protocol.
IIS	Internet Information Server: Microsoft's Web Server for hosting web applications.

## 2 Installation Scenarios

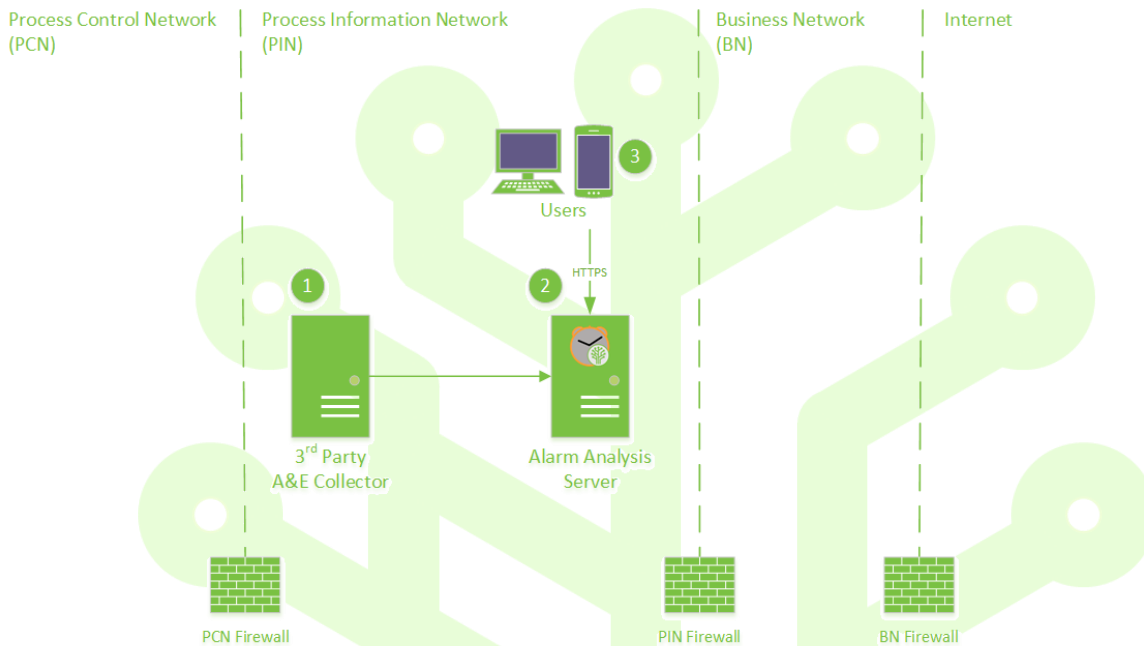
### 2.1 Scenario #1

Stand-alone installation of Alarm Analysis for Process Information Network users only.

Data is polled from a 3<sup>rd</sup> party Alarm & Event collector such as ProcessVue, CiTect or Dynamo.

Users access Alarm Analysis on local intranet.

#### 2.1.1 Network Architecture



1	Alarm & Event data is already collected by a 3 <sup>rd</sup> Party Server (for example, ProcessVue, CiTect, Dynamo).
2	<p>Stand-alone installation of Alarm Analysis on PIN.</p> <p>Alarm Analysis includes a local Data Core node for collecting and processing Alarm &amp; Event data; a local data repository, and uses IIS to present a web-based user interface.</p> <p>Data Core configuration includes:</p> <ul style="list-style-type: none"> <li>- SQL Event Source (polls 3<sup>rd</sup> Party Collector's database for Alarm &amp; Events)</li> <li>- Alarm &amp; Event Collector (recommended, but may not be essential as "raw" data is already in a 3<sup>rd</sup> Party Collector.)</li> <li>- Alarm Analysis Processing (converting A&amp;E data to Alarm Analysis records)</li> </ul>
3	<p>Users inside the PIN access Alarm Analysis on local intranet.</p> <p>HTTPS recommended, which will require SSL Security Certificate installed on IIS.</p>

#### 2.1.2 Firewall Settings

Firewall	Requirements
Computer hosting Alarm Analysis Server <i>Windows Firewall</i>	TCP Port 443 open to inbound traffic

## 2.2 Scenario #2

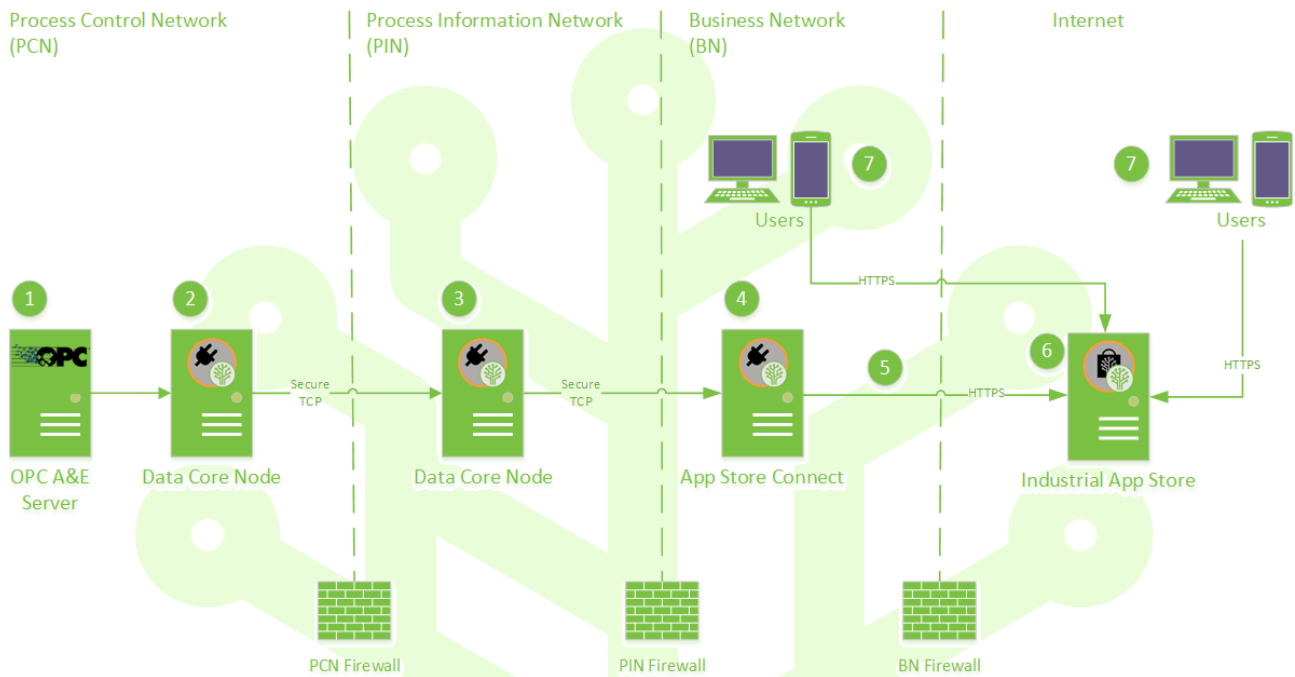
Data source is an OPC Alarm & Event Server hosted on the Process Control Network.

Alarm and Event data is relayed across militarized zones to an App Store Connection on the Business Network.

App Store Connect supports data access from apps hosted on the cloud-based Industrial App Store.

Business Network and Home users access Alarm Analysis on the Industrial App Store via the internet.

### 2.2.1 Network Architecture



1	Alarm & Event is streamed from the Control System via an OPC A&E Server.
2	<p>A Data Core Node relays data from the PCN to the PIN via a resilient stream that guarantees delivery. Data transmitted on the TCP channel is signed and encrypted.</p> <p>Data Core Node configuration includes:</p> <ul style="list-style-type: none"> <li>- OPC listener</li> <li>- Alarm &amp; Event Collector collecting A&amp;E data from the OPC Server (required for resilient transfer)</li> <li>- TCP Out Channel transmitting data to the PIN</li> </ul>
3	<p>A Data Core Node relays data from the PIN to the BN via a resilient stream that guarantees delivery. Data transmitted on the TCP channel is signed and encrypted.</p> <p>Data Core Node configuration includes:</p> <ul style="list-style-type: none"> <li>- TCP In Channel (receiving data from PCN)</li> <li>- TCP Out Channel (transmitting data to the BN)</li> </ul>
4	<p>App Store Connect acts as a local data processor and supports connections to the Industrial App Store</p> <p>App Store Connect configuration includes:</p> <ul style="list-style-type: none"> <li>- TCP Listener (receiving data from PIN)</li> <li>- Alarm &amp; Event Collector (collecting data from the Secure TCP stream)</li> <li>- Alarm Analysis Processing (converting A&amp;E data to Alarm Analysis records)</li> </ul> <p>App Store Connect returns acknowledgements to the upstream Data Core Nodes. Failure to do so initiates data resubmission.</p> <p>For more information, refer to the App Store Wiki: <a href="#">TCP Event Sink and Source</a></p>

	Alarm Analysis data remains on the Business Network.
5	<p>App Store Connect initiates a connection to the Industrial App Store using Microsoft's SignalR technology. This supports secure 2-way communication allowing App Store apps to connect and query data on the Business Network.</p> <p>Access to data via App Store Connect is only available if explicitly shared with another App Store User (see step 7).</p> <p>For more information, refer to the App Store Wiki: <a href="#">Connection Security</a>.</p>
6	The Industrial App Store: a cloud portal of industrial applications that can connect to business data sources through App Store Connect, including Alarm Analysis.
7	<p>Users inside and outside the Business Network (e.g. office and home workers) access Alarm Analysis via the Internet. They log-in to the <a href="#">Industrial App Store</a> and select the Alarm Analysis app.</p> <p>NB. App Store users must be granted access to the Alarm Analysis data source (configured on the Business Network App Store Connection).</p> <p>For instructions on sharing data, refer to the App Store Wiki: <a href="#">Share Data with other App Store Users</a>.</p>

### 2.2.2 Firewall Settings

Firewall	Requirements
BN:Internet <i>Network Firewall</i>	<p>TCP Port 443 open to outbound traffic from computer hosting App Store Connect and user machines to:  <a href="https://appstore.intelligentplant.com">https://appstore.intelligentplant.com</a>  <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> *</p> <p>* Required for Azure Active Directory log-in.            For instructions on enabling log-in to the App Store with business accounts, refer to: <a href="#">App Store Registration for Organisations</a>.</p>
BN Computer hosting App Store Connect <i>Windows Firewall</i>	<p>TCP Port 443 open to outbound traffic            TCP Port 11000 open to inbound traffic</p>
PIN:BN <i>Network Firewall</i>	TCP Port 11000 open to outbound traffic
PIN Computer hosting Data Core Node <i>Windows Firewall</i>	TCP Port 11000 open to inbound and outbound traffic
PCN:PIN <i>Network Firewall</i>	<p>TCP Port 11000 open to outbound traffic            No inbound access required.</p>
PCN Computer hosting Data Core Node <i>Windows Firewall</i>	<p>TCP Port 11000 open to outbound traffic            TCP Port for OPC channel open to inbound traffic</p>

## 2.3 Scenario #3

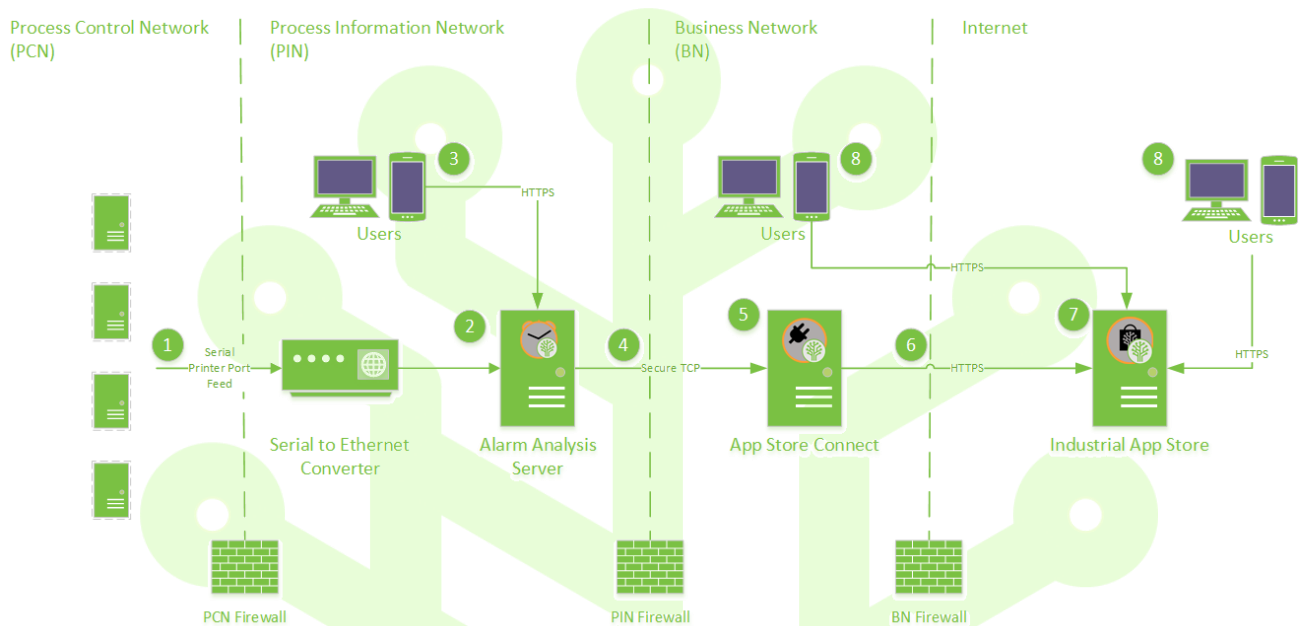
Alarm & Event information arrives from Process Controllers via serial printer-port feeds.

Band-width and reliability from PIN to BN is limited (as is common for offshore assets), thus a stand-alone instance of Alarm Analysis is installed for local PIN users.

Alarm and Event data is relayed across militarized zones to an App Store Connection on the Business Network.

App Store Connect supports data access for apps hosted on the cloud-based Industrial App Store.

Business Network and Home Users access Alarm Analysis on the Industrial App Store via the internet.



1	Alarm & Event data enters the PIN via serial printer-port cables connected to a Serial to Ethernet Converter. This physical architecture guarantees one-way data-flow from the PCN.
2	A stand-alone installation of Alarm Analysis includes a local data-core node for collecting and processing Alarm & Event data; a local data repository, and uses IIS to present a web-based user interface.  Data Core configuration includes: <ul style="list-style-type: none"> <li>- TCP Printer Port listener (receiving input from the Serial to Ethernet Converter)</li> <li>- Alarm &amp; Event Collector (required for resilient transfer)</li> <li>- Alarm Analysis Processing (converting A&amp;E data to Alarm Analysis records)</li> <li>- TCP Out Channel (transmitting data to the BN)</li> </ul>
3	Users on the PIN access a local (stand-alone) instance of Alarm Analysis. HTTPS recommended, which will require SSL Security Certificate installed on IIS.
4	Data Core TCP Out Channel (on the PIN) initiates an authenticated TCP connection with App Store Connect (on the BN). Data transmitted on the TCP channel is signed and encrypted.  Alarm & Event data is sent to App Store Connect. App Store Connect responds with an acknowledgement. If the Alarm Analysis server fails to receive a positive acknowledgement, data is resubmitted.  For more information, refer to the App Store Wiki: <a href="#">TCP Event Sink and Source</a>
5	App Store Connect acts a local data processor and supports connections to the Industrial App Store  App Store Connect configuration includes: <ul style="list-style-type: none"> <li>- TCP Listener (listening for input from the Alarm Analysis server)</li> <li>- Alarm &amp; Event Collector (collecting A&amp;E data from the Alarm Analysis server)</li> <li>- Alarm Analysis Processing (converting A&amp;E data to Alarm Analysis records)</li> </ul>

	Alarm Analysis data remains on the Business Network.
6	<p>App Store Connect initiates a connection to the Industrial App Store using Microsoft's SignalR technology. This supports secure 2-way communication which allows App Store apps to connect and query data on the Business Network.</p> <p>Access to data via App Store Connect is only available if explicitly shared with another App Store User (see step 8).</p> <p>For more information, refer to the App Store Wiki: <a href="#">Connection Security</a>.</p>
7	The Industrial App Store: a cloud portal of industrial applications that can connect to business data sources through App Store Connect.
8	<p>Users inside and outside the Business Network (e.g. office and home workers) access Alarm Analysis via the Internet. They log-in to the <a href="#">Industrial App Store</a> and select the Alarm Analysis app.</p> <p>NB. App Store users must be granted access to the Alarm Analysis data source (configured on the Business Network App Store Connection).</p> <p>For instructions on sharing data, refer to the App Store Wiki: <a href="#">Share Data with other App Store Users</a>.</p>

### 2.3.1 Firewall Settings

Firewall	Requirements
BN:Internet <i>Network Firewall</i>	<p>TCP Port 443 open to outbound traffic from computer hosting App Store Connect and user machines to:  <a href="https://appstore.intelligentplant.com">https://appstore.intelligentplant.com</a>  <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> *</p> <p>* Required for Azure Active Directory log-in.            For instructions on enabling log-in to the App Store with business accounts, refer to: <a href="#">App Store Registration for Organisations</a>.</p>
BN Computer hosting App Store Connect <i>Windows Firewall</i>	<p>TCP Port 443 open to outbound traffic            TCP Port 11000 open to inbound traffic</p>
PIN:BN <i>Network Firewall</i>	TCP Port 11000 open to outbound traffic
PIN Computer hosting Alarm Analysis <i>Windows Firewall</i>	<p>TCP Port 443 open to inbound traffic            TCP Port 11000 open to outbound traffic            TCP Port for Serial to Ethernet Converter channel open to inbound traffic</p>
PCN:PIN <i>Network Firewall</i>	No inbound access required.



### 3 Customer Support

We welcome customer feedback and can provide assistance with any problems you may encounter.

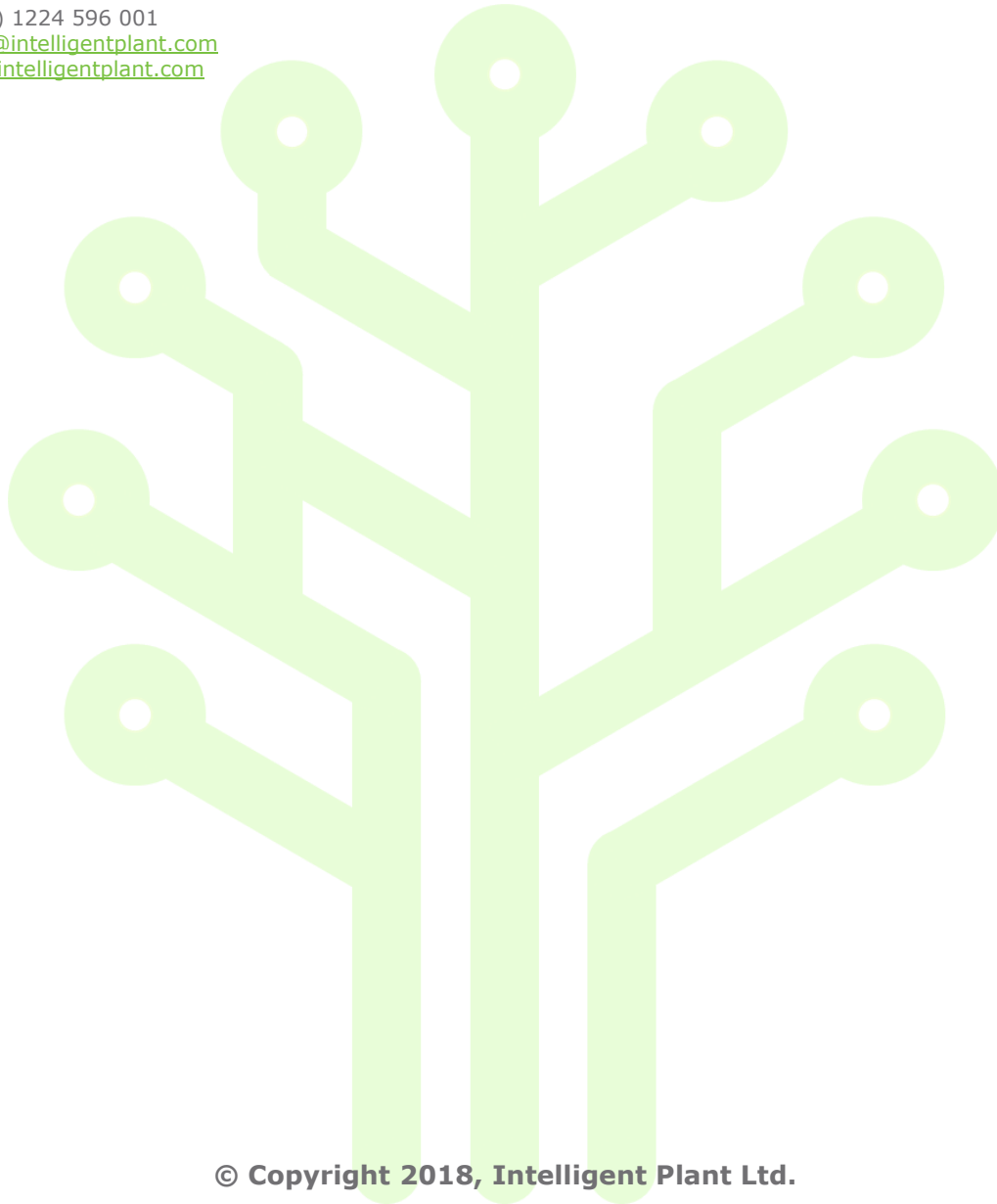
To get in touch, contact us at:

**Intelligent Plant Ltd**  
First Floor  
489 Union Street  
Aberdeen  
AB11 6AZ

**Tel:** +44 (0) 1224 596 001

**Email:** [info@intelligentplant.com](mailto:info@intelligentplant.com)

**Web:** [www.intelligentplant.com](http://www.intelligentplant.com)



© Copyright 2018, Intelligent Plant Ltd.

