Intelligent Plant™

*Inform, Enhance, Grow. Intelligently.*

# App Store Connect Quick Reference

# Table of Contents

# 1 App Store Connect

App Store Connect is the software that allows users to connect their data to cloud applications on the Industrial App Store. It is free to download from the Industrial App Store and installed to a client site.

Using the App Store Connect, an administrator can:

- Authorize a secure channel to the Industrial App Store
- Create connections to client data sources (e.g. process data historians, alarm and event collectors, etc.)
- Administer data sharing to App Store users

## 1.1 Connection Security

App Store Connect connects to the App Store using Microsoft's SignalR technology, which supports secure 2-way communication.

The exact communication protocol is determined by the capabilities of the computer running App Store Connect; if the computer is capable of using HTML5 websockets (Windows Server 2012 or later, Windows 8 or later), the App Store connection will automatically be upgraded to a secure websocket connection for best performance. Earlier versions of Windows will fall back to other communication protocols, but the connection is always encrypted, regardless of which protocol is used.

The secure connection allows App Store Connect to communicate with the App Store, and vice versa, but prevents any application from accessing your data unless it meets several layers of security requirements.

For more information, refer to the App Store Wiki: Connection Security.

## 1.2 User Access to data available on App Store Connect

The data sources configured on App Store Connect are only available to users via explicit role-based permissions.

For instructions on sharing data, refer to the App Store Wiki: Share Data with other App Store Users.

## 1.3 Application Access

Apps on the Industrial App Store can only access App Store Connections data-sources with user permission.

For more information, refer to the App Store Wiki: Application Permission.

## 1.4 Database Management

App Store Connect operates with the following types of database:

| | |
|---|---|
| Elasticsearch | App Store Connect ships with Elasticsearch 2.4 configured for local data storage.<br>For custom configuration, including using an alternative Elasticsearch instance, or modifying the default store location, refer to the App Store Wiki: Big Data Service Advanced Configuration. |
| Process Historians | App Store Connect connects to all industry standard Process Historians. For a complete list, refer to the App Store Wiki: Advanced Data Core configuration.<br>If you have further requirements, contact Intelligent Plant. |
| Alarm Collectors | App Store Connect connects to all industry standard Alarm Collectors. For a complete list, refer to the App Store Wiki: Advanced Data Core configuration.<br>If you have further requirements, contact Intelligent Plant. |

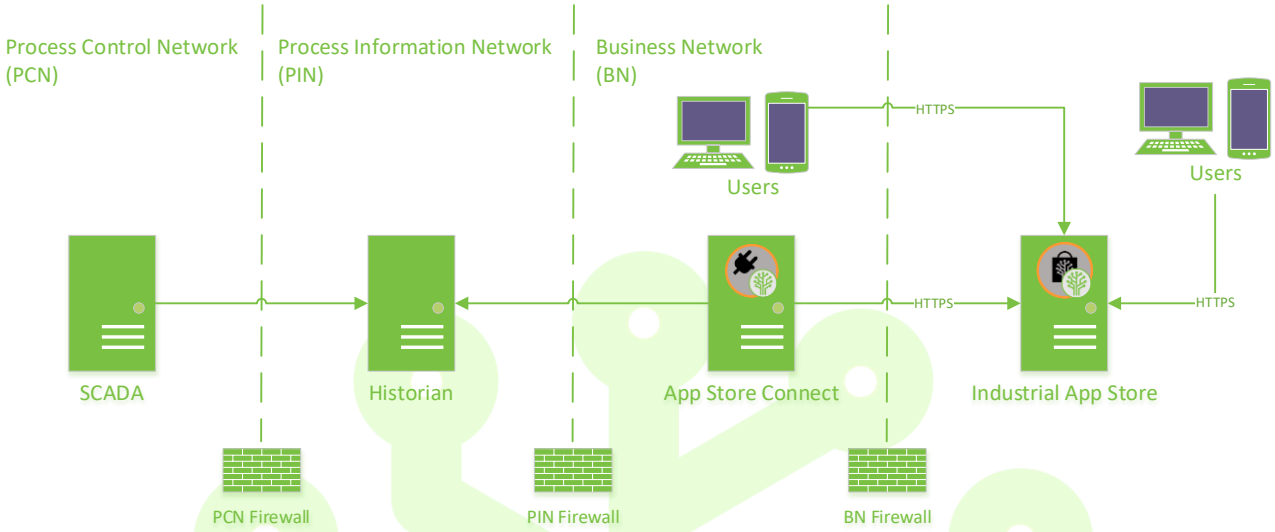
## 1.5 Data Storage and Backup

App Store Connect configuration and data should be backed up regularly.

For guidelines refer to the App Store Wiki: App Store Connect Back-up and Restore.

## 1.6 System Security and Firewalls

App Store Connect is firewall friendly and designed to operate in a multi-firewall protected architecture.




The above diagram illustrates a typical architecture - directions of arrows indicate the direction in which a connection is initiated. App Store Users (internal and external) can only access business data from the Industrial App Store through the secure App Store Connection.

**Firewall Requirements**

| | |
|---|---|
| BN Firewall | TCP Port 443 open to outbound traffic from computer hosting App Store Connect to<br>https://appstore.intelligentplant.com<br>https://packages.intelligentplant.com<br>https://api.intelligentplant.com<br><br>TCP Port 443 open to outbound traffic from user workstation to authentication provider:<br>Microsoft Azure Active Directory: https://login.microsoftonline.com |
| App Store Connect Host Computer | TCP Port 443 open to outbound traffic |
| PIN Firewall | *Site specific.*<br>App Store Connect supports connection to all industry standard Process Historians. Protocols will depend on the Historian vendor. |
| PCN Firewall | *Out-of-scope.*<br>No direct App Store Connect access required. |

## 1.7 System and Software Requirements

App Store Connect is a highly configurable tool that can perform multiple functions such as pass-through query, local historization, intensive on-prem data monitoring and calculation. The following spec is for a general use-case that covers all of these options to a degree. For specialist operation or other use-cases, we advise you to consult the driver specifications and/or request Intelligent Plant assistance. For fluid projects, we recommend using a Virtual Machine with capacity to modify requirements on demand.

**Basic Requirements**

- Windows Server 2019 x64 or later
- 4-Core CPU standard deployment or 8-Core CPU for Foundation Analytics
- 32 GB RAM
- .Net Framework 4.8

**Data Drive Requirements**

By default, data files are stored to the system drive. However, if using Edge Historian and/or Alarm Analysis we strongly recommend using a dedicated data volume appropriate for storing data at scale.

- 1 TB SSD
- RAID 1

*For more information, refer to the Industrial App Store Wiki: Modify Big Data Storage Location.*

**Facit Monitoring Requirements**

Facit will incur extra demand on the App Store Connect server as high numbers of calculations are performed and stored. A multi-core processor is essential for parallel processing of calcs.

- An 8-Core CPU will allow up to 7 calculation threads.

**Edge Historian Requirements**

- Edge Historian requires approximately 60 MB of storage per 1 million samples.
- For high volume processing, you should consider increasing the CPU and/or RAM of the installation machine.
- Increase dedicated Big Data Service RAM.
  *For more information, refer to the Industrial App Store Wiki: Increase Big Data Service RAM.*

**Alarm Analysis Requirements**

- Alarm Analysis requires approximately 3 GB of storage per 1 million alarm & event records.
- For high volume processing, you should consider increasing the CPU and/or RAM of the installation machine.
- Increase RAM dedicated to the Big Data Service.
  *For more information, refer to the Industrial App Store Wiki: Increase Big Data Service RAM.*

**Anti-Virus Exclusion Rules**

Facit Monitoring, Edge Historian and Alarm Analysis all employ local data storage functions. For efficient processing, data folders and files should be excluded from virus scanning.

*For more information, refer to the Industrial App Store Wiki: Anti-Virus Exclusion*

**Service Account**

By default, App Store Connect runs as the machine's Local System account. You may need to modify the service to run as a different account if required by your IT department's security rules.

*For more info, refer to the Industrial App Store Wiki: How to run App Store Connect under a Service Account.*

**Internet Connectivity Requirements / Firewall Rules**

The identity for the App Store Connect service requires outgoing HTTPS (port 443) internet connectivity to the following DNS names:

- appstore.intelligentplant.com
- packages.intelligentplant.com
- api.intelligentplant.com
- login.microsoftonline.com

*continued overleaf…*

**Security Requirements**

The Industrial App Store uses Let's Encrypt HTTPS certificates.

Manual registration of the root certificates may be required if automatic root CA updates have been disabled on the App Store Connect server.

*For more information, refer to Let's Encrypt "Chain of Trust" documentation.*

**OPC Classic (DA/HDA/AE) Requirements**

- Connecting to OPC Classic data or event sources requires OPC Core Components (32-bit) to be installed. These components are supplied by the OPC server vendor.

**AVEVA (OSIsoft) PI and Asset Framework Requirements**

- Connecting to an AVEVA (OSIsoft) PI or Asset Framework data source requires the PI AF Client 2014 (64-bit) or later to be installed. This component is supplied by AVEVA/OSIsoft.

## 1.8 Encrypted Credentials

All sensitive data stored in App Store Connect configuration is encrypted using the Windows Data Protection API (DPAPI). Encrypted data can only be decrypted on the machine that it was encrypted on.

# 2 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
492 Union Street
Aberdeen
AB10 1TS

**Tel:** +44 (0) 1224 596 001
**Email:** info@intelligentplant.com
**Web:** www.intelligentplant.com