Support Note: Using SSL Certificates

SSL Certificates

Warning These instructions are intended for system administrators or persons responsible for maintaining your network infrastructure. They should be familiar with installing certificates.

For highest security, we recommend using web browser certificates for native HTTPS connections with your Auto-Count/Plant Manager installation. Please see the Support Note *Using Web Browser Certificates for Native HTTPS*. But for small organizations with limited resources, you can implement browser traffic to be routed through a proxy service which uses a SSL (Secure Sockets Layer) certificate. However, this does not secure the traffic between Auto-Count 4D and Plant Manager and still uses http.

Auto-Count and Plant Manager can be hosted behind a reverse proxy such that calls to https://ServerName/Application are routed to the correct web interface. The recommended application to use is Nginx. Using this method, the translation between https and http is handled by Nginx and the Auto-Count products are simply installed as normal.

Obtaining an SSL (Secure Sockets Layer) certificate is beyond the scope of this document, but the reader should change the following example to point to the correct location of the certificate and key files. More information can be found at the Nginx website. http://nginx.org/en/docs.

A sample configuration suitable for a small single server installation is below:

```
worker_processes  1;
events {
    worker_connections  1024;
}

http {
    include       mime.types;
    default_type  application/octet-stream;
    sendfile        on;
    keepalive_timeout  65;
    server {
             listen       443 ssl;
             server_name  servername www.servername;
add_header    Access-Control-Allow-Origin *;

ssl_certificate      C:\certs\plantmanager.online-chain.pem;
ssl_certificate_key  C:\certs\plantmanager.online-key.pem;
ssl_protocols       TLSv1 TLSv1.1 TLSv1.2;

location /PlantManagerWeb/ {
proxy_pass http://localhost:5000/PlantManagerWeb/;
}

location /Reporting.Service/ {
proxy_pass http://localhost/Reporting.Service/;
}

location /PlantManager/ {
proxy_pass http://localhost/PlantManager/;
}

location /PlantManagerConnector/ {
proxy_pass http://localhost/PlantManagerConnector/;
}
      }
}
```

Configure Plant Manager Web

The only added changes needing to be made are to the Plant Manager Web UI app-config.json, (change the server's name as needed). See below:

```
{
    "apiHost"             : "servername",
    "apiPort"             : "",
    "replaceConfig"       : "true",
    "useSSL"              : "true",
    "reportServiceBaseURL":
"https://servername/Reporting.Service/ReportServiceWCF/webjson/"
}
```

And to the appsettings.json to configure the back end listen on port 5000

```
{
  "AllowedHosts": "*",
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "Urls": "http://*:5000"
}
```