Whitepaper

Deploying the Canary Historian in Compliance with 21 CFR Part 11

Catalyx Implementation Blueprint for Life Sciences Data Integrity

catalyx

Foreword

This whitepaper, authored by Catalyx in close collaboration with our partner Canary Labs, outlines how to configure and deploy the Canary System for full 21 CFR Part 11 compliance — enabling secure, auditable, and trustworthy data across pharmaceutical and life sciences environments.

As certified integrators of the Canary platform, Catalyx brings globally trained teams and decades of experience in regulated automation and digital transformation. With over 3,000 successful projects delivered across nine countries, we've helped clients embed historian technologies like Canary into validated systems that meet the highest standards of data integrity, traceability, and operational performance.

This guide reflects real-world deployments — not theory — and draws on our field-proven methodologies for configuring, securing, and managing time-series data in line with FDA expectations.

We hope it empowers your teams to confidently implement scalable and compliant Canary solutions that support next-generation manufacturing.

— The Catalyx Team

Introduction

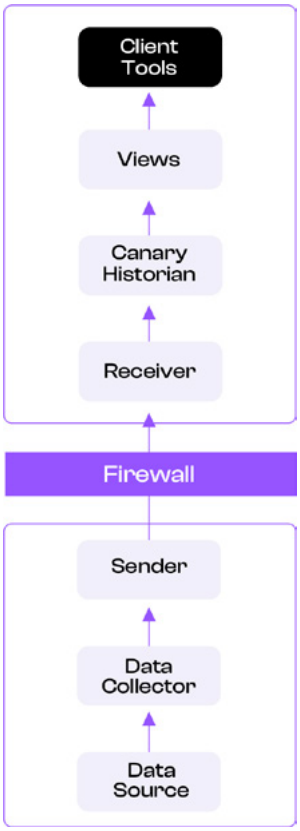
The Canary System provides companies a solution for storing, contextualizing, and acting upon their time series process data. With flexible deployment options, the Canary System covers a variety of complex architectures including cloud-based solutions and traversing DMZs. Whether monitoring data from a single production line, an entire plant, or providing streams of real time data to corporate Canary instances, Canary's solution can scale accordingly.

The pharmaceutical and life science industries have strict requirements around the collection and reporting of reliable and trustworthy data. One of the key requirements for any software is compliance with the Code of Federal Regulations (CFR) that defines all FDA protocols surrounding electronic signatures and records. Title 21 CFR Part 11 (Part 11) primarily defines the measures needed to ensure that electronic records are as trustworthy and tamper-proof as the paper records they have replaced.

For a data historian solution to be Part 11 compliant, access to its database and the records that it contains, must be secure and auditable. Additionally, the integrity of the data stored must meet the ALCOA+ framework: Attributable, Legible, Contemporaneous, Original, and Accurate (ALCOA), as well as Available, Enduring, Consistent, and Complete (+).

Canary Systems can be deployed and configured to comply with Part 11 standards. In addition, using the platform all ALCOA+ concepts can be implemented to provide data integrity. The steps contained within this whitepaper can be configured and implemented to achieve these results.

Understanding Architecture



Canary software is comprised of .NET Windows Services that function as one complete industrial database solution. The key Canary components that are used to collect, store, and recall time series data are Data Collectors, the Sender service, the Receiver service, the Canary Historian, and Views. Specific Canary Data Collectors are available to connect to both OPC UA and MQTT Sparkplug data servers. Additional data collectors are available for other protocols, but OPC and MQTT data protocols will be referenced throughout this paper as they cover the vast majority of pharmaceutical and life science automation systems. Other Data Collectors can use the same approach of configuration.

The appropriate data collector is matched and installed local to the data source, along with the Canary Sender Service and the Canary Admin application. Using the Canary Admin, the Data Collector is then configured to read data from the source.

The Data Collector then passes the data to the Canary Sender which in turn communicates with the remotely installed Receiver using TLS over TCP for secure and encrypted messaging. The Receiver compresses the data using a loss-loss algorithm and writes it to the Canary Historian and provides the Sender with confirmation that the data packets have successfully been written. If the Receiver is not able to successfully write data to the Historian, the Sender automatically caches data to a local disk until the Historian is available.

The Canary Historian is a modified NoSQL database that is organized into DataSets, or groups of tags. Each DataSet consists of daily historical files. At a defined interval, each DataSet's current historical database (HDB) file is automatically closed and validated. All tag data, including timestamps, values, quality scores, and metadata, are permanently and securely stored in these files.

As clients need to access data within the Canary Historian, they query a single endpoint, Canary's Views Service. Views authorize and authenticate the client, read the historical archive, and process the data per the client's specification before encrypting and securely transferring the data packet to the client.

Understanding Architecture

The Canary System provides system administrators tools to manage data access, including data logging, data storage, and data retrieval. Canary system administrators use the Canary Administrator application to manage the Canary Services. By default, access to the Canary Administrator application is restricted to only those Active Directory (AD) users that have been identified as local computer administrators. Additionally, individual AD users/groups can be granted permission to the Canary Administrator application or have their permission revoked. Access to the Canary Administrator endpoint is configurable and can be turned on or off to restrict all remote access. The Administrator client will try to connect using the user's Windows credentials. If the user is not in the Administrator service access list, they will be prompted for a new username/password. By default, any user logged into the Canary Administrator's local machine is granted access to the application. To require separate application login, the Net.Pipe

– Anonymous (Local Only) endpoint must be disabled on the Admin tab of the Canary Administrator.

Data Logging

Any Sender that wishes to write data to a Canary Historian, must securely connect to the Receiver service via TLS over TCP through a single configurable port. Each Sender is assigned a unique GUID identifier and requires a system administrator to initialize the connection by granting access to the Sender session on the receiving computer through the Canary Administrator. Alternatively, a domain account, with write access to DataSet(s), may be configured run the sender service. If a Sender session has not been authorized, the Receiver will ignore all data and the Sender will buffer data to local disk.

Data Storage

Once data has been written to the Canary Historian it is part of the permanent data record, stored in HDB2 files. Raw data values are stored in proprietary format and cannot be accessed without using Canary software. System administrators manage global permissions that can prevent data values from being inserted, edited, or deleted. Access to the Canary Historian's hard drive should be restricted to authorized personnel to prevent deletion of data.

Data Retrieval

Using Active Directory as the Canary user source, access to Canary Views, as well as Canary client tools, Axiom and the Excel Add-in, is granted to users with their domain username and password. This ensures that all users are uniquely identified and that they can only access data based on preconfigured permissions. These permissions are defined as having no access, access to read data only, access to write data only or access to both read and write data.

Axiom

Historical data may be viewed through Canary's HTML Axiom client over a configurable web port. Axiom clients request data from Views and by default are read only. Access to Axiom may be restricted by listing Active Directory users or groups within the Canary Administrator. Access to specific tags and datasets within Axiom may be further restricted through Views security.

Axiom should be configured to connect to the webserver through HTTP over TLS to ensure the data is encrypted in transit and anonymous logon should be denied.

Messages and Audit Trail

Canary stores its system audit trail and diagnostics log in a SQLite database which can be viewed using the Message component of the Canary Admin application.

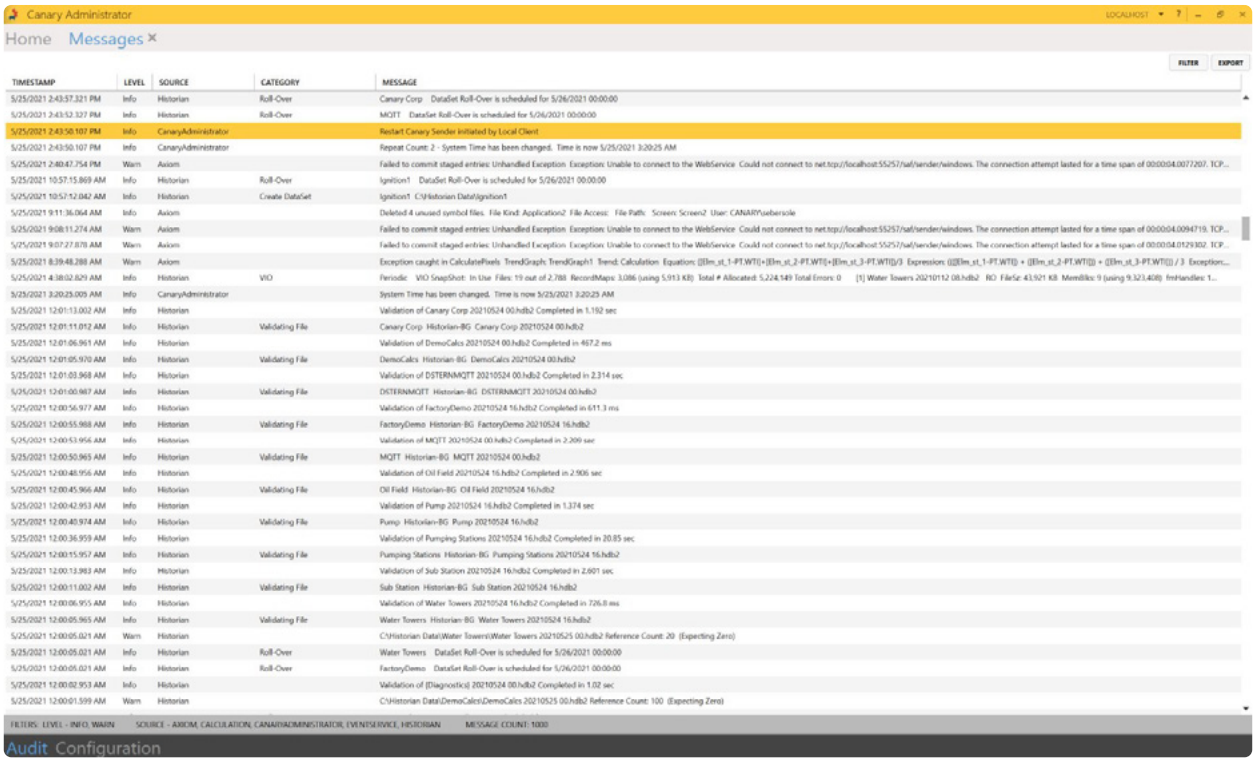


Figure 2: Canary Admin - Messages

The diagnostic log captures informational and error messages for each of the services and is trimmed after 1 year or if the log exceeds 1.5 million messages. The audit trail, introduced in v22.0, captures the AD username, timestamp, and a high-level description of changes to system configuration or state of a service. Beginning in v22.2.1, the audit trail records actions in a JSON structure which additionally captures the before and after state of each configuration that was changed. For versions prior to v22.2.1, it is recommended to implement a procedural method in concert with the audit trail to capture the specific change implemented. The audit trail must be manually enabled after installation but once enabled, it stores the records indefinitely with no option to edit or delete either log. As of v22.2.0, the audit trail may be exported as CSV or PDF.

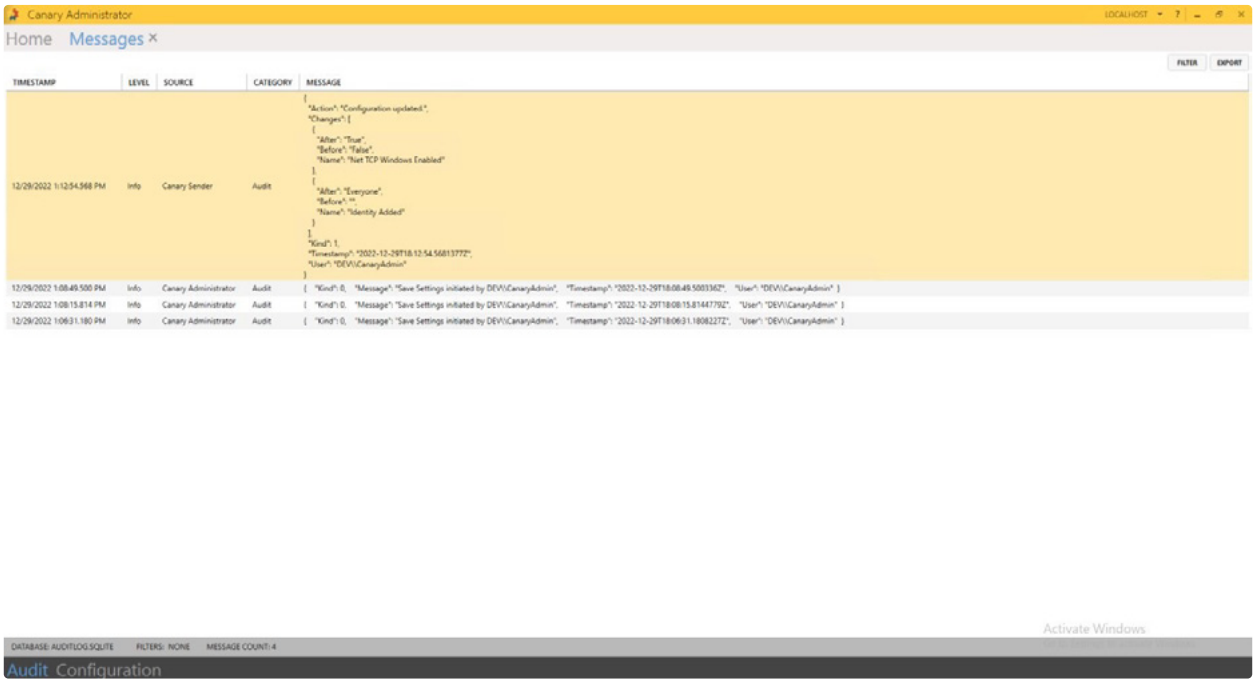


Figure 3: Example Audit Trail Message

Manual data entry and edits to data points are captured in the Historian DataSet. Each input is listed on the corresponding datapoint that was added or changed, and captures the timestamp, previous value, and the username. Subsequent edits are captured as additional lines underneath the data point, retaining all previous entries. As of version 22.2.0, manual data entry is also logged in the central audit trail.

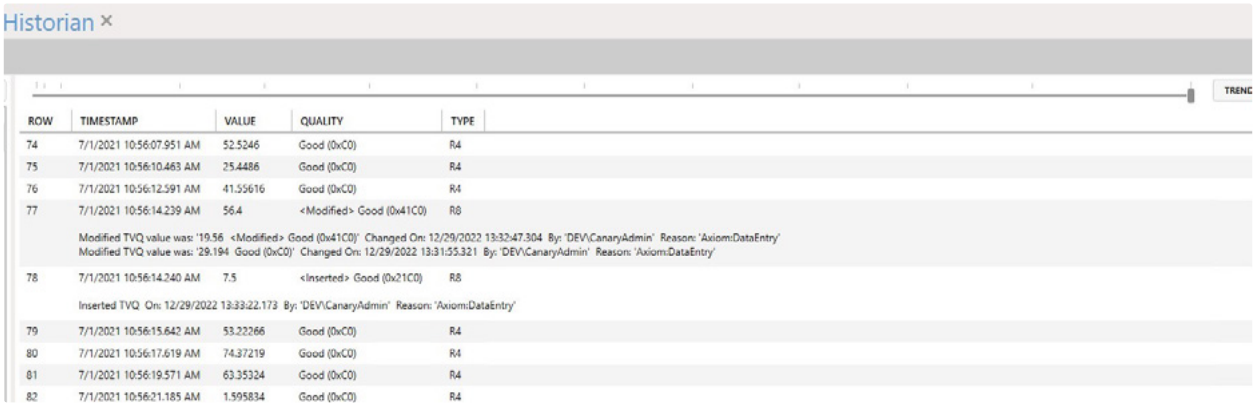


Figure 4: Example Manual Data Entry Audit Trail

Axiom creation/usage is tracked in the Audit tab under the Axiom tile. The Axiom audit trail is limited the user and the time of the session, but does not capture changes to screens. As of version 22.2.0, changes to Axiom projects are logged in the central audit trail.

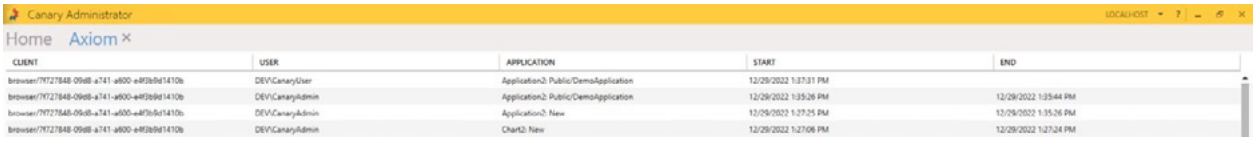


Figure 5: Axiom Creation/Usage Audit Trail

Configuration

These simple steps can be done during installation and configuration to ensure compliance with Part 11. If Canary is being installed on an open system (the system environment is not owned by the same organization as the one managing Canary), the archive files and buffer files should be configured to be encrypted at rest through the operating system or 3rd party service.

Installation and Setup for OPC Collector

The installation of the following software should be configured such that the data sources are unlikely to become disconnected. Typically, this is installed on a process network.

1. Install OPC UA Collector, Sender Service, and Canary Admin Service local to the OPC Server.
2. Messages Tile
   a. Configuration – Verbosity
      i. Enable "Enable EAL (Enhanced Audit Logging)" to enable the audit trail.
3. Admin Tile
   a. Endpoints: Enable only 'Net. TCP – Windows' and 'Net.TCP – Username'.
      i. Disable 'Net.Pipe – Anonymous (Local Only)' (see section Enforce Canary Administrator Security for versions prior to v22.2.1).
   b. Access: Allow only computer ad ministrators or specific administrative users/groups.
4. Sender Tile
   a. Credentials: Set a unique Identity for the sender service. If the Sender Service access needs to be limited to specific DataSet(s), enter a valid Active Directory account in the User field with corresponding DataSet write permissions configured in the View security on the Canary Historian server.
   b. Endpoints: Enable only 'Net. TCP – Windows' and 'Https - User name (Web API)' as required.
   c. Access: Allow 'Administrators' (or specific users/groups).
   d. To set up Backup Buffering, follow the steps in section "Sender Service Buffering".
5. OPC Collector Tile
   a. Enable 'Use Security' on the configured session. Certificates may need to be installed on the OPC server if the connection is not local.

Installation and Setup for MQTT Collector

The installation of the following software should be configured such that the data sources are unlikely to become disconnected, although MQTT sparkplug B supports edge buffering.

1. Install MQTT Collector, Sender, and Canary Admin Service local to the MQTT Broker.
2. Messages Tile
   a. Configuration – Verbosity
      i. Enable "Enable EAL (Enhanced Audit Logging)" to enable the audit trail.
3. Admin Tile
   a. Endpoints: Enable only 'Net.TCP – Windows' and 'Net.TCP – Username'.
      i. Disable 'Net.Pipe – Anonymous (Local Only)' (see section Enforce Canary Administrator Security for versions prior to v22.2.1).
   b. Access: Allow only computer administrators or specific administrative users/groups.
4. Sender Tile
   a. Credentials: Set a unique Identity for the sender service. If the Sender Service access needs to be limited to specific DataSet(s), a valid Active Directory account may be defined in the User field with corresponding DataSet write permissions configured in the View security on the Data Archive server.
   b. Endpoints: Enable only 'Net. TCP – Windows' and 'Https - Username (Web API)' as required.
   c. Access: Allow 'Administrators' (or specific users/groups).
   d. To set up Backup Buffering, follow the steps in section "Sender Service Buffering".
5. MQTT Collector
   a. Define a MQTT Client ID and enable the "SparkplugB Primary Application". It is recommended assign the Canary collector as the Primary Client on edge nodes to allow edge buffering.
   b. Connect to the MQTT Broker(s) through a secure port with username and password.
   c. Enable "Enable SSL/TLS" and "Client Certificate".

Installation and Setup for Data Archive

The installation of the following software should be configured such that access to the data is limited to those who need to see the data.

1. Install Historian, Canary Admin Service, Sender, Receiver, Virtual Views, and Axiom.
   a. Calculation & Events, ODBC, and Publisher may be installed if required.
2. Messages
   a. Configuration – Verbosity
      i. Enable "Enable EAL (Enhanced Audit Logging)" to enable the audit trail.
3. Admin Tile
   a. Endpoints: Enable only 'Net.TCP – Windows' and 'Net.TCP – Username'.
      i. Disable 'Net.Pipe – Anonymous (Local Only)' (see section Enforce Canary Administrator Security for versions prior to v22.2.1).
   b. Access: Allow only computer administrators or specific administrative users/groups.
4. Sender Tile
   a. Credentials: Set a unique Identity for the sender service. If the Sender Service access needs to be limited to specific DataSet(s), a valid Active Directory account may be defined in the User field with corresponding DataSet write permissions configured in the View security on the Data Archive server.
   b. Endpoints: Enable only 'Net.TCP – Windows' and 'Https - Username (Web API)' as required.
   c. Access: Set Deny 'Anonymous Logon' to remove unauthenticated data editing access from Axiom. If data entry/edits are required, add only authorized users/groups to the Allow list.
5. Receiver Service
   a. Endpoints: Enable only 'Net.TCP – Username'.
   b. Senders: If using the Identity property on the Sender Service, approve the Identity on the Senders tab on the Receiver Service.
6. Views (Applies to Axiom, the Excel Add-In, and APIs)
   a. Configuration
      i. Endpoints: Enable only 'Net.TCP – Windows', 'Net.TCP – Username', 'Net.TCP – Secure', 'Https – Username (Web API)' as required.
      ii. Access: Allow 'Everyone' (or specific users/groups) and Deny 'Anonymous Logon'. This field limits security for all views. If granular security is not required, the Views Security section can be skipped.
   b. Security:
      i. Permission: Access can be configured per DataSet or per tag basis.
         1. It is recommended to limit access based on user job functions.

2. No account/group should be granted write access unless using the User credentials on a sender service. If manual entry of data is required, limit write (or read/write) access to specific accounts/groups. Note: Write access does not grant permission to view the DataSet/tag structure, therefore read/ write is the preferred option. The user will also need to be added to the Sender Allow lists as well for write access.

ii. Settings: Enable 'Enable security'.

7. Axiom
   a. Endpoints: Enable 'Https – Username' and 'Http – Anonymous'.
   b. Access: Set Allow to select Axiom users or groups and Deny to 'Anonymous Logon'. This will allow redirection of the client from HTTP to HTTPS.

Sender Service Buffering

As of v22.0, the sender service can be configured to store the buffer files for a configurable duration in the event that they need to be recovered. The buffered files are stored locally on the sender computer in the

"C:\ProgramData\Canary\Sender\Backup" folder. To enable the buffering, the following line must be added to the file "C:\Program Files\Canary\Sender\CanarySender.exe.settings".

CanarySender.exe.settings

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <senderSettings>
    <backupDays>1</backupDays>
    <clientTimeout>60000</clientTimeout>
    <fileSize>32</fileSize>
    <packetSize>1024000</packetSize>
    <packetDelay>0</packetDelay>
    <packetZip>false</packetZip>
    <receiverPort />
    <trackErrors>false</trackErrors>
  </senderSettings>
  <receiverSettings>
    <autoCreateDataSets>false</autoCreateDataSets>
    <autoWriteNoData>true</autoWriteNoData>
    <extendData>true</extendData>
    <insertReplaceData>false</insertReplaceData>
    <suppressTimestampErrors>false</suppressTimestampErrors>
    <externalPropertyStorage>false</externalPropertyStorage>
  </receiverSettings>
</configuration>
```

Figure 6: Line Added to Enable Buffering

Enforce Canary Administrator Security

Prior to v22.2.1, there is no configuration setting within the Canary Administrator GUI authenticate the user when accessing the Canary Administrator application from the local server. To force user authentication, the following line (Line 185 in Figure 7) must be deleted from the file “C:\Program Files\Canary\Canary Admin\CanaryAdministrator.exe.config” on each computer that has the Canary Administrator installed.

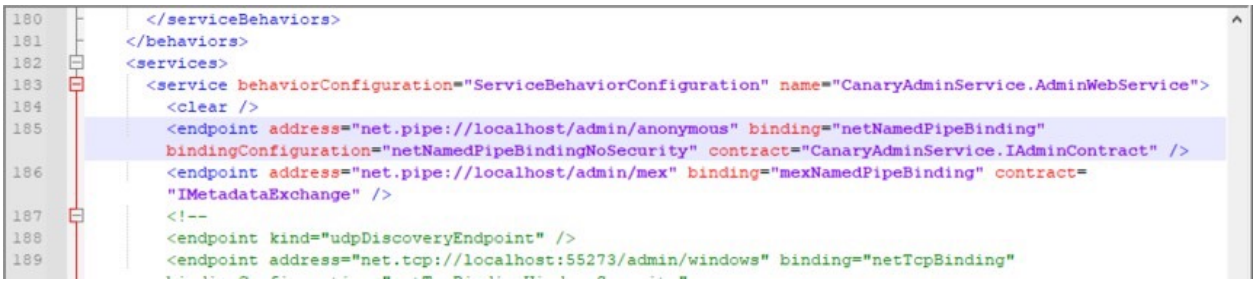


Figure 7: Line deleted to force user authentication

Ensure that proper users/groups are assigned under the Admin Access permissions prior to updating the file. Once the change is made, restart the Canary Admin service. Note that this setting does not persist on version upgrade.

Summary

As the Life Sciences industry continues to move toward data centric models, data integrity principles and Part 11 compliance are more critical than ever to ensure the accuracy and reliability of records. By following the configuration settings listed above, Canary can be deployed as a robust, secure, and compliant historian solution. Leveraging its segregated infrastructure, security for each service can be configured to minimize user access. Additionally, administrators can feel confident that all changes to system configuration are securely tracked through the enhanced audit log, allowing for traceability and accountability throughout the system. For more information, please contact Canary Labs at **https://www.canarylabs.com.**

About Catalyx

Catalyx is a global machine vision and automation company that integrates technology and people to help manufacturers and logistics providers achieve next-generation levels of quality and throughput.

For over thirty years, the minds behind Catalyx have been at work maximizing operational processes across highly regulated industries by inventing new technology applications and supporting companies with deep technical expertise. With nine global offices, more than 550 team members, and over 3,000 successful projects, Catalyx has the scale, skillset, and reach to solve unique process problems at enterprise scale — and the vision to keep doing what's never been done before.

To learn more or speak with our team about 21 CFR Part 11 readiness, historian deployment, or broader automation strategy, get in touch.

info@catalyx.ai
www.catalyx.ai
USA | IRELAND | UK | CONTINENTAL EUROPE