



# Canary User Conference

August 11- 14 State College, Pennsylvania



# Keeping Canary Secure



Steve Mason



Chris Brooks



# How does Canary manage its security?

At Canary we care deeply about the security of your systems and data. We take a comprehensive approach to prevent bad actors from unauthorized access to your systems and data as well as our own internal management and security of customer data entrusted to us.

## The Identity Services

- Authentication
- Authorization
- API Tokens
- Tag Security
- File Security (new in v25.3.1)



# What can the Identity service do for you?

## Before Identity (v23-)

- Each Canary service managed its own authorization
- Tag Security was managed by Views
- Only supported Windows AD for user authentication and SAML (Axiom only)

## After Identity (v24+)

- Identity manages authorization for ALL Canary services
- More granular control over user authorization (especially in Axiom)
- Tag Security management is migrated to Identity
- Supports Windows AD, Kerberos, OpenID Connect for ALL Canary clients (better SSO integration)

# Authentication

Canary supports Windows AD, Kerberos, and OpenID Connect (i.e. Entra ID, Okta, Google and SSO integration when using Kerberos or OIDC.

## How it works...

1. An internal “Canary” account is generated and mapped to the external account coming from the IDP when the user logs in
2. All external groups the user is a member of are discovered
3. Internal “Canary” groups can be created.
4. Internal “Canary” groups are then mapped to the external group

The screenshot displays the Canary Admin interface. At the top right, there's a 'Sign in to Canary Admin' overlay with the Canary logo and three buttons: 'Sign in with Kerberos', 'Sign in with Active Directory', and 'Sign in Anonymously'. The main interface has a sidebar with 'Configuration' and 'Security' options. The 'OpenID Connect Providers' section shows a table with columns: CLIENT ID, CLIENT SECRET, GROUP ID CLAIM, ISSUER, PROVIDER NAME, USER ID CLAIM, and USER NAME CLAIM. Below this, 'EXTERNAL PROVIDER OPTIONS' includes checkboxes for 'Enable Anonymous' (checked), 'Enable Kerberos', and 'Enable Active Directory'. The 'Canary Groups' section shows a table with 'CANARY GROUP ID' and 'GROUP NAME'. The 'External Groups' section shows a table with columns: PROVIDER ID, EXTERNAL NAME, EXTERNAL ID, CANARY GROUP ID, CANARY GROUP, and USERS. Red boxes and numbers 1 through 4 highlight specific elements: 1 points to the 'Edward Byers' user in the 'USERS' column; 2 points to the 'OT\_ADMINS' external group; 3 points to the 'Canary Admins' group name; 4 points to the 'Canary Admins' group ID.

CLIENT ID	CLIENT SECRET	GROUP ID CLAIM	ISSUER	PROVIDER NAME	USER ID CLAIM	USER NAME CLAIM
<b>EXTERNAL PROVIDER OPTIONS</b>						
<input checked="" type="checkbox"/> Enable Anonymous						
<input type="checkbox"/> Enable Kerberos						
<input type="checkbox"/> Enable Active Directory						

CANARY GROUP ID	GROUP NAME
5852cd44-1f9a-4530-8ff3-e59a8433fa7b	Canary Admins
a21abe5d-5b63-4529-984b-fa33130efd03	Everyone
ab39b217-6fc0-44f9-92a3-c89ee9ea3869	Administrators

PROVIDER ID	EXTERNAL NAME	EXTERNAL ID	CANARY GROUP ID	CANARY GROUP	USERS
windows	Everyone	S-1-1-0	a21abe5d-5b63-4529-984b-fa33130e	Everyone	
windows	OT_ADMINS	S-1-5-21-16014904	5852cd44-1f9a-4530-8ff3-e59a8433f	Canary Admins	Edward Byers
windows	OPERATIONS	S-1-5-21-16014904			Edward Byers
windows	DEVELOPMENT	S-1-5-21-16014904			Edward Byers
windows	AUTOMATION	S-1-5-21-16014904			Edward Byers
windows	Domain Users	S-1-5-21-16014904			Edward Byers
windows	Administrators	S-1-5-32-544	ab39b217-6fc0-44f9-92a3-c89ee9ea3	Administrators	



# Authorization

Once authenticated, users are allowed or denied access to certain features within the Canary system.

## Key Identity Functions

- **Manages** ALL of Canary's access control lists.
- **Controls** what a user is permitted to do within Canary.
- **Authorizes** other remote Canary services
- **Utilizes** “Canary” users/groups
- **Provides granular control** over what a user has permission to do.



▸ Axiom

▸ Data Entry Control

**Axiom Data Entry Control**  
Access Control List to determine which users/groups are allowed to use the Axiom Data Entry Control.

ADD EDIT REMOVE

ENTITY	KIND	ACCESS	↑
Anonymous	User	Deny	
canaryadmin	User	Allow	
Edward Byers	User	Allow	
Administrators	Group	Allow	

▸ Everyone Preferences

▸ Logon

▸ Read Only Folder

▸ Report

▸ Script

▸ Calculations

▸ Admin

▸ Logon

**Admin Logon**  
Access Control List to determine which users/groups are allowed to connect to the Admin service remotely.

ADD EDIT REMOVE

ENTITY	KIND	ACCESS	↑
canaryadmin	User	Allow	
Administrators	Group	Allow	
Canary Admins	Group	Allow	

▸ Historian

▸ Identity

▸ Views



# API Tokens

API tokens are unique security credentials, typically alphanumeric strings, that function as a form of authentication for accessing Application Programming Interfaces (APIs). They require clients to prove their identity and obtain permission to interact with an API.






API tokens are created and managed within the Identity Service and are linked to internal “Canary” user which, in turn, can be linked to an external user or a standalone “Canary” user

## Key Functions

- Read/Write API
- Adding a Remote Historian to Views
- Restricting write access from remote Collectors
- Authenticating with the ODBC and Excel Add-In Clients

## Key Benefits

- Obscure credentials
- Can be configured to expire or deleted
- Simplifies the process of using the API to read/write data

API Tokens						ADD	EDIT	REMOVE	INFO
TOKEN	COPY	DESCRIPTION	EXPIRATION DATE	USER	STATE				
0221f183-7c70-4965-a143-ε		Remote SaF Token	Never	Remote SaF	Allow				
11111111-2222-3333-4444-		API Token created for the Anonymous Canary User account.	Never	Anonymous	Allow				
55310382-5709-4528-a054-		Default token for the Installer's migration process.	Never	Installer Migration Service	Allow				
5c42caf6-b977-42c2-a05c-e		Power Bi	Never	canaryadmin	Allow				
e8e830a0-5ba9-4d69-8339-		Default token for Axiom Reporting.	Never	Axiom Report Service Acc	Allow				



# Tag Level Security

Prior to Version 24 tag level security resided in Views. Now it is managed by the Identify Service .

## Key Features

- When enabled, controls user/group access to tag data.
- Inherited permissions from previous levels.
- Permissions can be assigned at the tag level.
- Explicit permissions override inherited ones.
- Controls both Read and Write access.
- Requires Remote Collectors to be configured with an API token when Tag Security is enabled
- The Identity service can connect to a remote Views service to configure its Tag Security

VIEWS ENDPOINT

Host:  Port:

CONFIGURATION

☒ Enable Tag Security

BROWSE

Views

Canary Oil

DiagnosticHealthSystem

Hays Model

SMASON

Calcs

Canary Oil

Comal

Data Generation

DHS\_Calcs

Guadalupe

Hays

IgnitionData

MQTTData

NewDataSet

Oil and Gas SQL

Oil and Gas SQL2

Oil and Gas SQL3

EXPLICIT PERMISSIONS

ADD

EDIT

REMOVE

COPY

PASTE

USER	PATH	ACCESS
Remote SaF	SMASON	Write

INHERITED PERMISSIONS

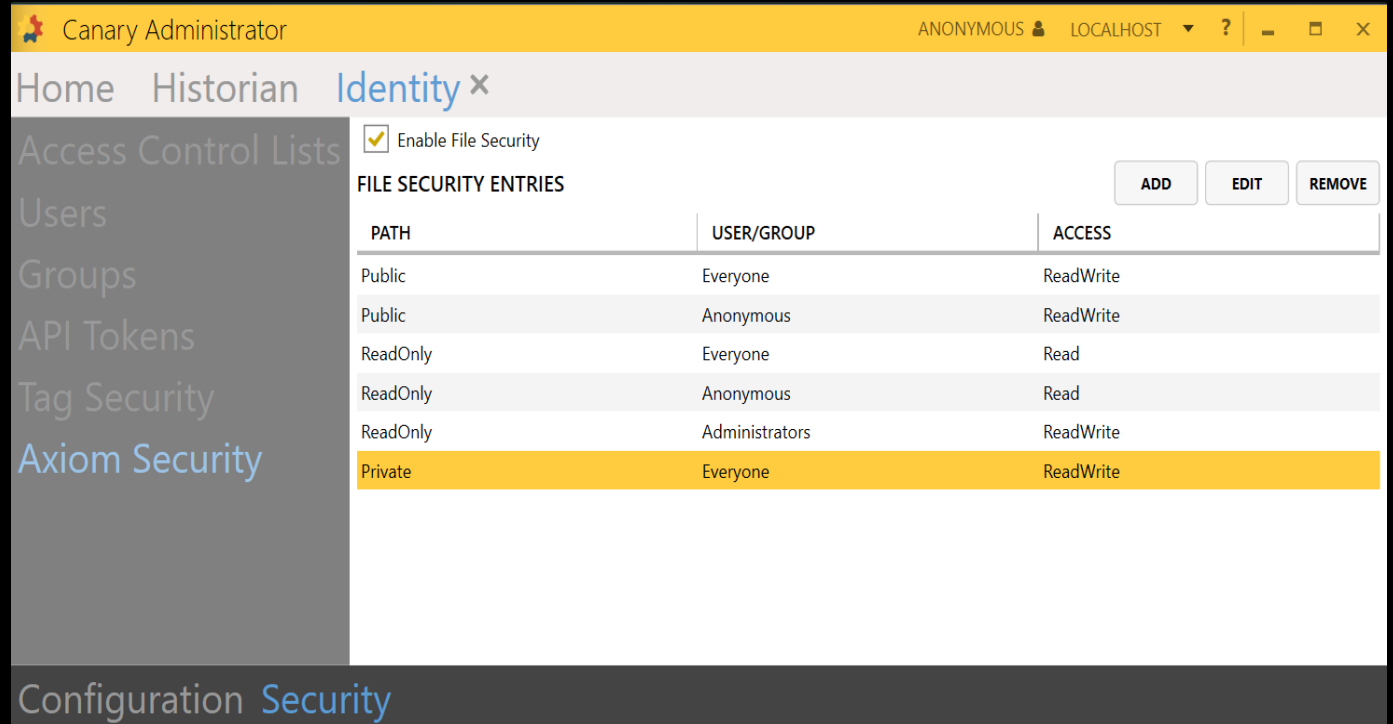
USER	PATH	ACCESS
Canary Admins	ROOT	ReadWrite
canaryadmin	ROOT	ReadWrite
Anonymous	ROOT	None



# File Security

A new File Security feature has been added in v25.3.1. Prior to this release users need to apply file/folder permissions through Windows to restrict access to Axiom applications

- To support our strategy to become OS agnostic, we develop a new way of accomplishing file security from within Canary.
- Like Tag Security, Canary users/groups can be given read/write access to specific folders which are then inherited to subfolders.



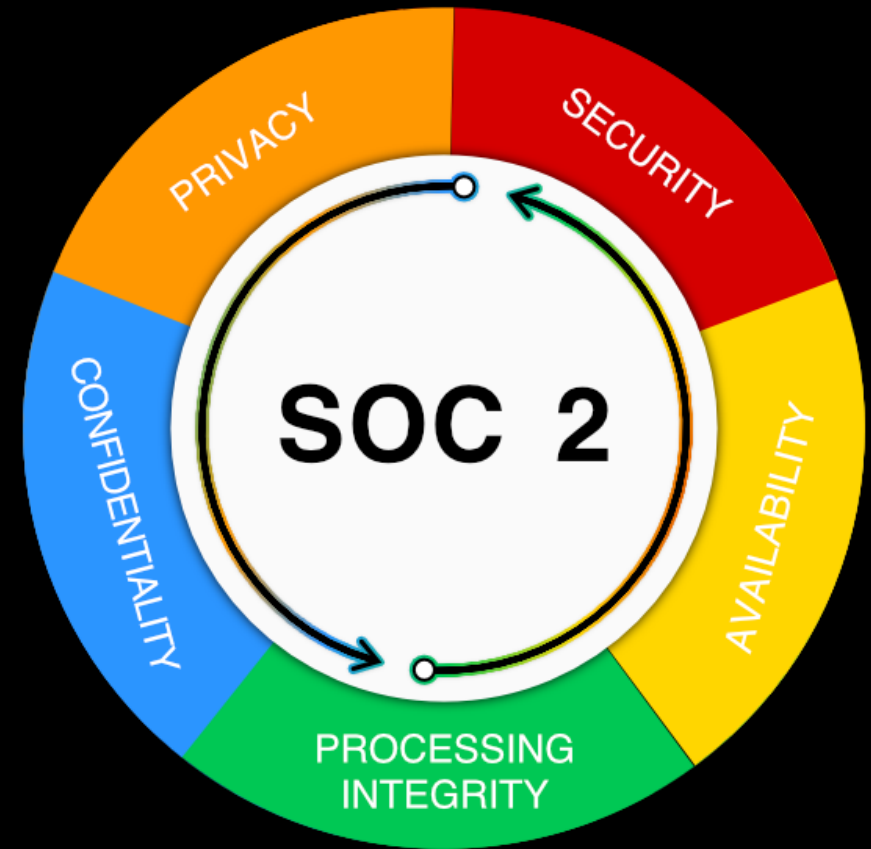
The screenshot shows the Canary Administrator web interface. The top navigation bar includes 'Home', 'Historian', and 'Identity' (selected). The left sidebar lists 'Access Control Lists', 'Users', 'Groups', 'API Tokens', 'Tag Security', and 'Axiom Security' (selected). The main content area is titled 'FILE SECURITY ENTRIES' and features a checkbox for 'Enable File Security' which is checked. Below this is a table with three columns: 'PATH', 'USER/GROUP', and 'ACCESS'. The table contains six entries, with the 'Private' entry highlighted in orange. At the bottom of the interface, there are tabs for 'Configuration' and 'Security' (selected).

PATH	USER/GROUP	ACCESS
Public	Everyone	ReadWrite
Public	Anonymous	ReadWrite
ReadOnly	Everyone	Read
ReadOnly	Anonymous	Read
ReadOnly	Administrators	ReadWrite
Private	Everyone	ReadWrite

# SOC 2- Type 2 Compliance

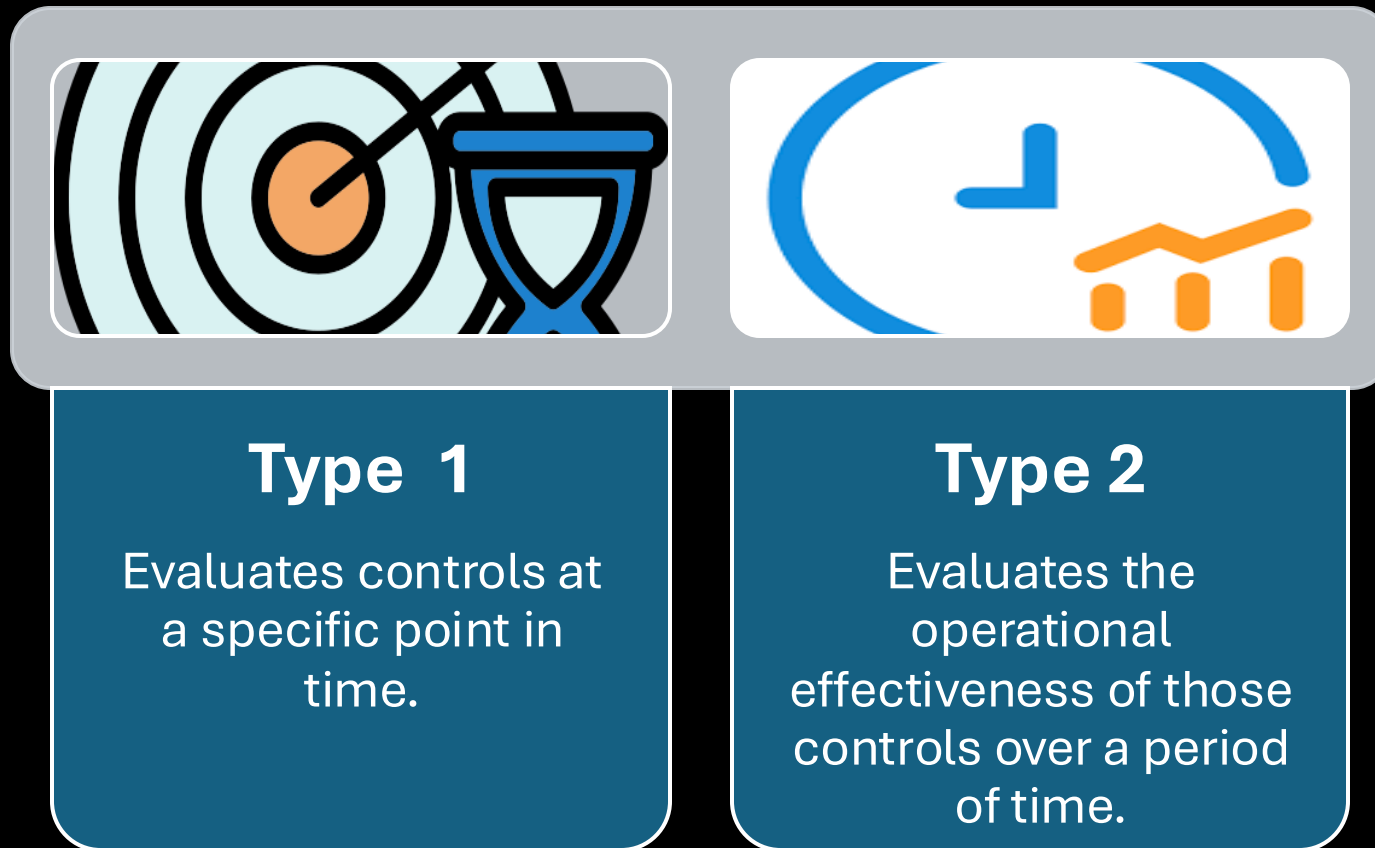
## Building Trust Through Security at Canary Labs

- SOC 2 stands for System and Organization Controls 2.
- Developed by the AICPA, it evaluates how companies manage customer data based on five Trust Services Criteria:
  - Security
  - Privacy
  - Confidentiality
  - Processing Integrity
  - Availability



# SOC 2 - Type 1 vs Type 2

Canary Labs is SOC 2 Type 2 compliant, meaning our controls are well-designed and consistently followed.



# Why Does SOC 2 Type 2 Matter?

# Data breaches affected over 1.35 billion people last year.

- Customers deserve proof that their data is secure.
- SOC 2 Type 2 provides third-party validation that Canary Labs:
  - ✓ Protects sensitive data
  - ✓ Detects and responds to threats
  - ✓ Maintains system availability and integrity



# Benefits to Canary Customers



## **Trust & Transparency**

Customers know their data is handled securely.



## **Risk Reduction**

Minimizes chances of data loss or unauthorized access.



## **Business Continuity**

Ensures systems are reliable and resilient.



## **Competitive Advantage**

Helps customers meet their own compliance needs.

# How Canary Labs Achieved SOC 2 Type 2

- Implemented robust security policies and procedures
- Continuous monitoring and auditing
- Independent third-party assessment
- Commitment to ongoing improvement





# Real-World Impact

Customers in critical industries (e.g., manufacturing, energy, infrastructure) rely on Canary's software for real-time data.

## SOC 2 Compliance Ensures

- Operational reliability
- Secure data transmission
- Confidentiality of sensitive process data



# What This Means for You!

## **Peace of mind knowing Canary Labs:**

- Meets industry standards
- Is committed to security
- Supports your own compliance efforts



# Final Thoughts

- SOC 2 Type 2 isn't just a certification—it's a promise.
- Canary Labs is dedicated to protecting your data, earning your trust, and supporting your success.
- Canary's SOC 2 Type 2 report is available at our trust center, <https://trust.canarylabs.com>



# Thank You



Steve Mason



Chris Brooks

# Questions