Feature Overview

DataWalk

DataWalk Access Control

User Permissions and Security Levels

DataWalk is a software platform that enables vast amounts of data from many disparate data sources to be organized in a simple visual model oriented around relevant concepts such as people, transactions, crimes, and so forth. This powers what is effectively an intelligence database, where organizations can store, connect, access, and analyze all their internal and external data. With these capabilities, it is vital to ensure that data access can be tightly controlled, and that implementation of complex data access rights does not significantly degrade performance. Here we highlight how DataWalk meets these critical challenges.

Extreme Flexibility for Data Access Control

A major challenge in analyzing sensitive data is ensuring that the data and the results of system processing are consistent with user privileges. DataWalk explicitly addresses this challenge with an approach that combines two options for control that are designed to work together: multi-dimensional permissions and user security levels. This combined approach enables organizations managing sensitive data to have enormous flexibility in controlling user access to that data. You can easily specify the data that individual users (and/or groups of users) are permitted to see, down to even the level of individual cells (i.e., fields) in a record.

DataWalk's system for multi-dimensional user permissions determines whether and how users and groups of users are able to access data sets, objects, attributes of objects, connections, and analyses, including the ability to read, write, add, and delete (see Figure 1).

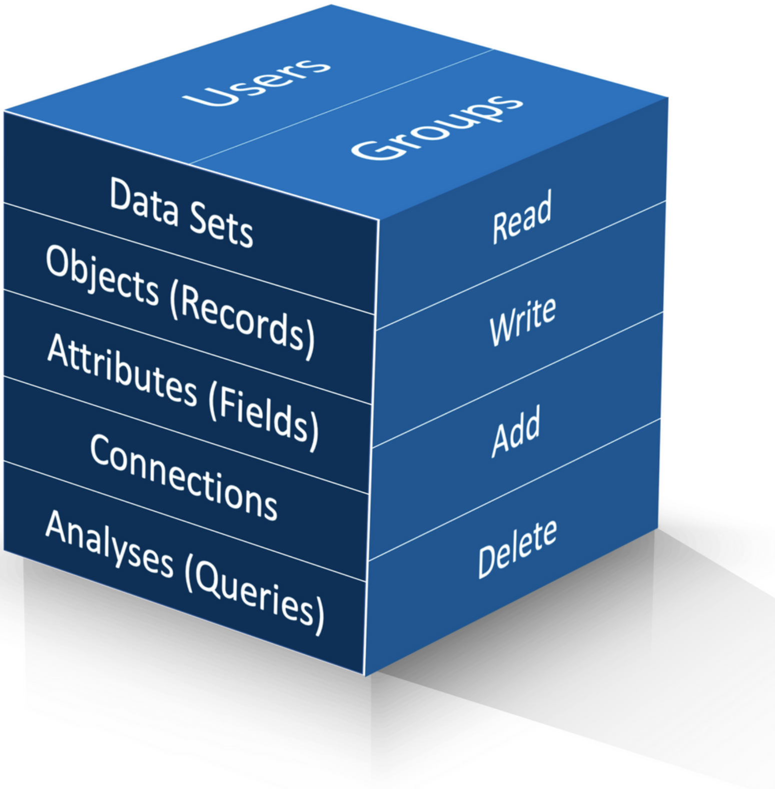


Figure 1. DataWalk's Multi-Dimensional Permissions Structure

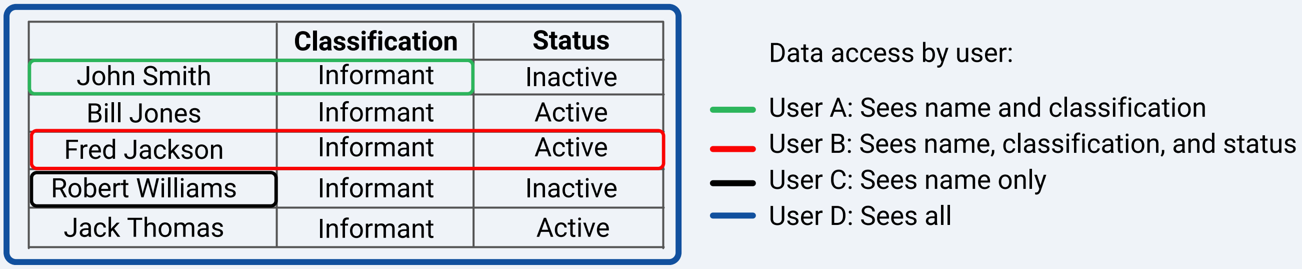
Access to objects (i.e., records) and/or specific cells is managed via predicates, which are simply filters that the system administrator defines for each data set, for a given user or group of users. These filters are applied transparently each time the system is queried by the user, and are highly efficient such that they do not impact system performance. Simple examples include filters that allow a particular user to see data only for a specific state or country, or values under a specified amount.

Permissions are determined by permission schemas. A permission schema can be assigned to one user or a group of users. And a user can be assigned more than one permission schema. Each user is assigned their personal permission schema(s) upon being granted access to the system.

Consider a simple example where highly sensitive data (listing informants) is stored in DataWalk. As shown in Figure 2, different users or groups of users can have read and/or write access to various elements of this data, depending on their permissions. Users who do not have read permissions to any of this data will not be aware that this data even exists in DataWalk.

Access to results of analyses (queries) can also be controlled via permissions. For example, if a query has generated a set of results that contains sensitive information—say individuals in a government organization who may be under suspicion of corruption—then both the existence and results of that analysis are visible only to users with appropriate permissions.

Earlier we mentioned that read/write access to connections can also be specified, and this merits further discussion. For example, if a person in one data set is connected to a sensitive data set, such as the informants list in Figure 2, users without appropriate permissions on connections would be unable to see whether an individual has any connections to this data set of informants.



	Classification	Status
John Smith	Informant	Inactive
Bill Jones	Informant	Active
Fred Jackson	Informant	Active
Robert Williams	Informant	Inactive
Jack Thomas	Informant	Active

Data access by user:

- 🟩 User A: Sees name and classification
- 🟥 User B: Sees name, classification, and status
- ⬛ User C: Sees name only
- 🟦 User D: Sees all

Figure 2. Examples of data access schemes for different users or groups of users.

Permissions Control Data Access and Usage Across the Entire System

DataWalk is a robust system with a variety of features for data analysis and visualization, including visual querying, link analysis, flows analysis, dashboards, and others. Permissions in DataWalk apply across all of these features, and data that a user is not authorized to access will not be included in the results or aggregations that the user sees. For example, if permissions have been set such that a particular user cannot view transactions over $100K, then when that user generates analyses or reports, transactions over $100K will not be included.

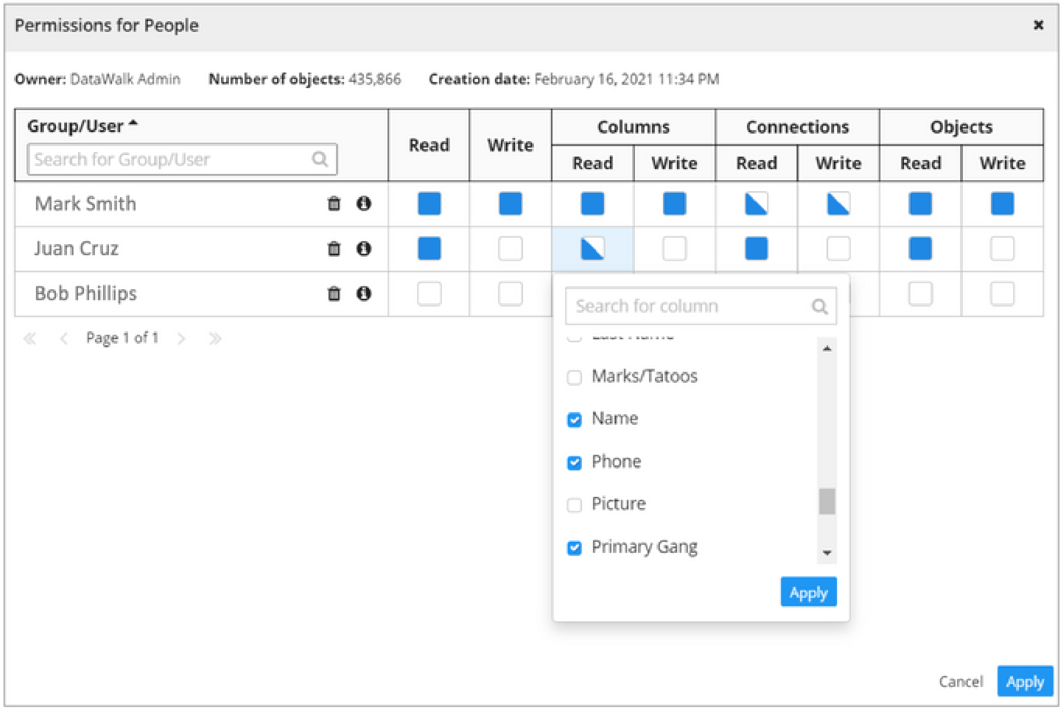
This capability of having a single permissions scheme that applies across all of the features of the system is very powerful, and is a significant differentiator relative to alternative systems that may require permissions to be set for each individual system component.

Better Performance With Complex Permission Structures

Permissions in DataWalk have been architected not only to be exceptionally flexible, but also to support excellent performance even with vast amounts of data and complex permission structures. This is a powerful capability that is uniquely enabled by patent-pending DataWalk technology. While complex permission schemes may be impractical to support on alternative systems due to performance degradation, these can be supported in DataWalk without such significant impacts on system performance.

Configured Via a Graphical Interface

DataWalk permissions are typically set by the system administrator through a graphical interface (see Figure 3). Using the same interface, creators of a specific analysis (query) can specify which other users and groups have access to that analysis.



Permissions for People

Owner: DataWalk Admin **Number of objects:** 435,866 **Creation date:** February 16, 2021 11:34 PM

Group/User	Read	Write	Columns		Connections		Objects	
			Read	Write	Read	Write	Read	Write
Mark Smith	■	■	■	■	◩	◩	■	■
Juan Cruz	■	□	◩	□	■	□	■	□
Bob Phillips	□	□					□	□

Page 1 of 1

☐ Marks/Tatoos

☑ Name

☑ Phone

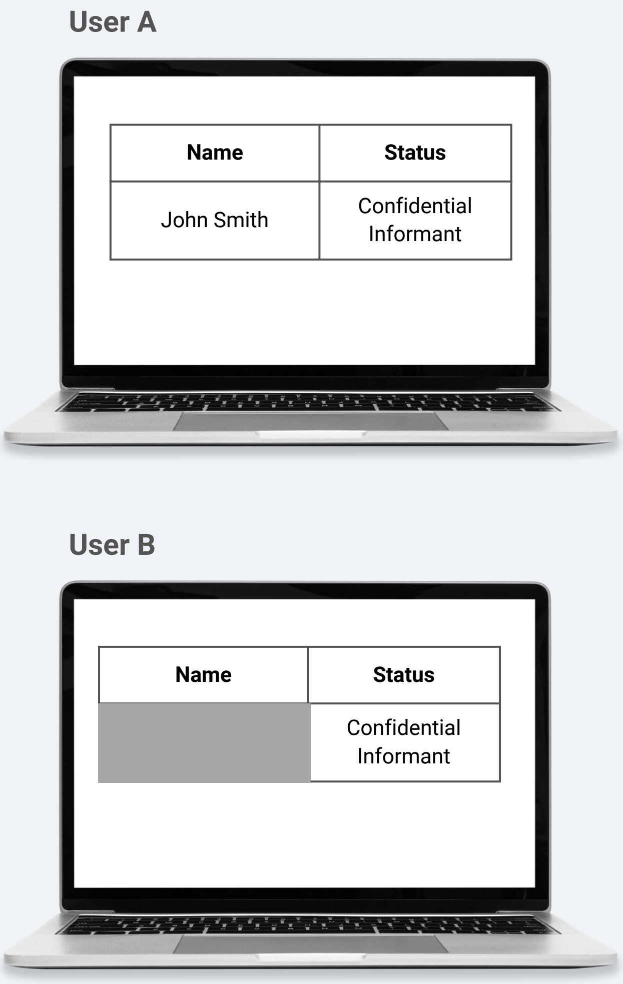
☐ Picture

☑ Primary Gang

Figure 3. Setting DataWalk permissions via a graphical interface.

Complementary Support for User/Data Security Levels

As an option, in addition to multi-dimensional user permissions, DataWalk also supports a security level-based system, which controls visibility and access to specific values based on a user's security level. This means that if a user's security level is lower than the minimum level required to view a particular value, then that value will be obscured, ensuring the highest level of data protection (see Figure 4).



Name	Status
John Smith	Confidential Informant

Name	Status
▨	Confidential Informant

Figure 4. DataWalk's security-level based system controls data visibility and access based on a user's security level.

The control over these specific security settings must be set up within DataWalk. However, the association between user groups and user security levels can be controlled via Single Sign-On (SSO), providing an additional layer of security and control.

Moreover, DataWalk's integration with SAML 2.0 allows for the modification of a user's security level via the SAML Certificate. The security level can be set up within DataWalk as a property of the user, providing even more of a flexible and secure system for managing user access.

The security level-based system is designed to work together with multi-dimensional user permissions to provide the utmost control and flexibility over user access to data. With this combined approach, DataWalk is able to cover the majority of customer security requirements, ranging from access to the set and its properties, through access to the object based on rules, and visibility of the values based on the security level of each value.

Altogether, these features greatly enhance data security and control.

Summary

DataWalk provides multi-dimensional data user access permissions and security levels that are ideal for organizations working with highly sensitive data. The platform enables highly granular permissions, complex permission schemas, and granular security settings, all without significantly impacting performance with large volumes of data. These permissions and security levels can be easily managed by both system administrators and data owners.