Version 4 Release 2

IBM i2 Enterprise Insight Analysis Security White Paper

Note

Before using this information and the product it supports, read the information in “Notices” on page 13.

This edition applies to version 4, release 2, modification 1 of IBM® i2® Analyze and to all subsequent releases and modifications until otherwise indicated in new editions. Ensure that you are reading the appropriate document for the version of the product that you are using. To find a specific version of this document, access the Understanding section of the IBM Knowledge Center, and ensure that you select the correct version.

IBM i2 Analyze security dimensions

A *security dimension* is a way to categorize an i2 Analyze item, with the aim of using its categorization to determine what rights users receive. The security dimensions for any deployment of the platform are defined in the *security schema* for that deployment.

For a particular deployment of i2 Analyze, there might be several different ways of categorizing items, resulting in multiple dimensions. For example:

- Items might be categorized by their security classifications
- Items might be categorized by the type of intelligence that produced them
- Items might be categorized by the roles of the users who are allowed to access them

Each security dimension contains a set of values that items can have in order to classify them within that dimension. To continue the example, the dimensions might have values as follows:

Security classification

Top Secret, Secret, Confidential, Restricted

Intelligence type

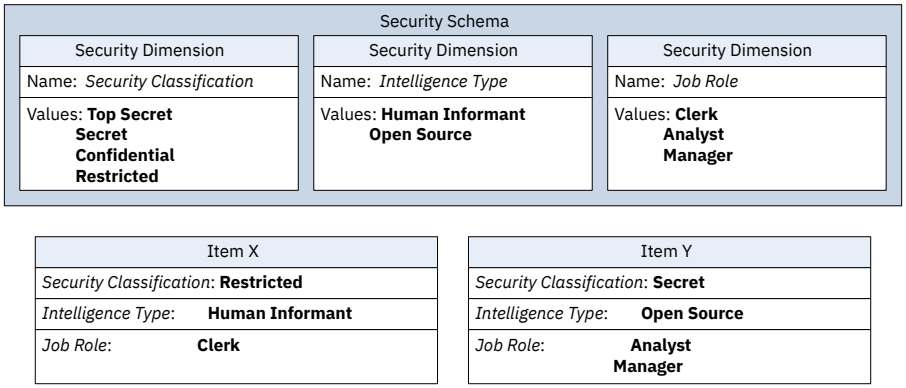
Human Informant, Open Source

Job role

Clerk, Analyst, Manager

In some dimensions (such as security classification), the values form a sequence from which each item takes a single value. In such cases, the values are considered to be levels, where each value supersedes all the values below it. In dimensions where the values do not form a sequence, items can take one or more values.

Every item in an i2 Analyze deployment must be assigned at least one value for each of the dimensions in that deployment. There is no such thing as an "optional" security dimension. For example:



An i2 Analyze deployment provides access to its security schema through the standard info service. The security schema contains the security dimensions and their values. Dimensions and values vary between deployments, and there are no restrictions on the numbers of dimensions or values that a security schema can define.

IBM i2 Analyze security levels

A *security level* is a description of what a user is allowed to do to an item in i2 Analyze. User group membership determines what security level a user receives for any particular item.

i2 Analyze security levels break down into two distinct categories: access levels and grant levels.

Access levels

The security access level of a user relates to their rights to view or edit an item in i2 Analyze.

i2 Analyze defines four security access levels. At any moment in time, a user has one of these levels for each item.

None

The user has no access to the item. The user cannot examine the item data, or even know that the item exists.

Cloaked

The user has access to the fact that the item exists, but cannot examine the item data. An i2 Analyze service can read cloaked item data on behalf of a user, but must not return that data to the user.

Read only

The user has read-only access to the item and its data.

Update

The user can read, modify, and delete the item and its data.

If a user needs a different access level from the cloaked or read-only level that they have, they can interrogate an item for its *signpost*. The signpost contains an indication of the person or team in their organization that is able to give them such access.

Grant levels

The security grant level of a user relates to their rights to change the dimension values of an item. The dimension values that they set affect what security access levels and grant levels they and other users receive for an item.

i2 Analyze defines two security grant levels. At any moment in time, a user has one of these levels for each item.

None

The user is not able to evaluate or change the security dimension values of the item.

Update

The user can evaluate and change the security dimension values of the item.

The interaction between access levels and grant levels means that on a particular item, having the "update" grant level effectively overrides the "none" access level. A user with the "update" grant level on an item is allowed to know that the item exists so that they can change its dimension values.

IBM i2 Analyze security permissions

In i2 Analyze, security permissions provide the link between the security dimension values that an item has, and the security levels that users receive. The platform calculates the access and grant rights of users according to the permissions of the user groups to which they belong.

In an i2 Analyze security schema, the set of security permissions for a user group defines mappings from dimension values to access or grant levels. For any particular item, a user receives the security levels that their user group indicates for the dimension values of that item.

When a user is a member of several user groups, or an item has multiple dimension values, it is possible for a user to receive several security levels from different security permissions. In these circumstances, i2 Analyze computes a single security level from all the contributors.

Security Schema

Permissions for Clerks

Security Dimension	Value	Security Access Level
Security Classification	Secret	Cloaked
Security Classification	Confidential	Read only
Intelligence Type	OS	Read only
Job Role	Clerk	Update

Permissions for Managers

Security Dimension	Value	Security Access Level
Security Classification	Top Secret	Cloaked
Security Classification	Secret	Read only
Intelligence Type	OS	Read only
Intelligence Type	HUMINT	Read only
Job Role	Clerk	Read only
Job Role	Manager	Update

It is not compulsory for a set of permissions for a user group to provide a security level for every value of every dimension. Any dimension value that does not appear in a set of permissions receives a default security level, according to a set of rules:

- For an unordered dimension, a dimension value that does not appear in the permissions receives the "none" security level.
- For an ordered dimension:
  - If the unspecified value is below a dimension value that does appear, then the unspecified value receives the same security level as the specified value.
  - If the unspecified value is above a dimension value that does appear, then the unspecified value receives the "none" security level.

For example, if a particular set of permissions associates the "read only" access level with "restricted" items (and makes no other setting), then the default access level for "confidential" items is "none". However, if the permissions associate the "read only" access level with "confidential" items instead, then "restricted" items also receive that access level for users in the same group.

An i2 Analyze system administrator must arrange the security schema so that all users can receive a security access level that is not "none" for at least one value in every dimension. The same requirement does not apply to security grant levels.

Note: IBM recommends that you do not specify access and grant permissions for the same user group. Instead, you can assign the "update" security grant level to users through membership of a group that is reserved for that purpose.

IBM i2 Analyze security scope

i2 Analyze does not enforce its security model on a deployment-wide basis. Instead, because each service in a deployment can maintain its own data store, the services are responsible for enforcing security on the items that they control.

There are a number of advantages to enforcing the security model at the scope of the services, rather than the scope of the deployment:

- The services can use item caching. Security is applied after retrieving objects from the cache, so cached objects can be reused on behalf of all users. This arrangement makes the cache more effective.
- Security is independent of the underlying storage system. It is not necessary to reimplement security for new storage technologies, and there is no need for new storage technologies to provide security support.
- The code that implements the security model is modular, and used by all the standard services. The code is also available for use by custom services so that they can use the same security model.

Note: None of these details has any bearing on the use of encryption as a security measure. You can enable the encryption of all stored data by configuring the underlying storage system. You might use full disk encryption, for example.

Security model example

At any moment, a user has one security access level and one security grant level for each item in i2 Analyze. The platform calculates these levels according to a consistent set of rules.

The process for determining a security level involves examining security permissions within and across dimensions. The platform does the job in three steps:

1. Bring together the permissions for all the user groups of which the user is a member.
2. Use the permissions to determine all the security levels that the user receives for each dimension value that the item has. Take the least restrictive level in each case.
3. Examine all of these "least restrictive" dimension-specific security levels, and take the most restrictive.

For example, consider the following item, which has one value for each of two security dimensions, and two values for a third.

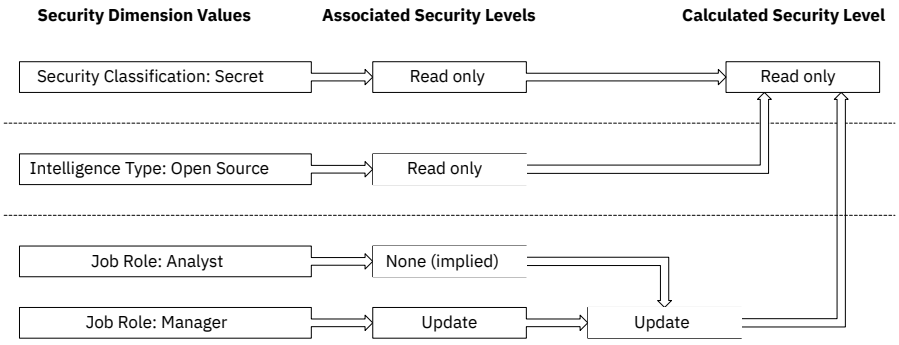
Item Y	
Security Classification: **Secret**	
Intelligence Type:	**Open Source**
Job Role:	**Analyst** **Manager**

Then, consider a user in a group that has the following security permissions. (It does not matter whether the permissions are due to one user group or several.)

Security Access Permissions

Security Dimension	Value	Security Access Level
Security Classification	Top Secret	Cloaked
Security Classification	Secret	Read only
Intelligence Type	OS	Read only
Intelligence Type	HUMINT	Read only
Job Role	Clerk	Read only
Job Role	Manager	Update

The following diagram then represents the process for determining the security access level of the user for this item.



This item has two values in the "Job Role" dimension that map to different access levels for this user. At this stage in the calculation, the less restrictive access level ("update") is taken. However, the values from the "Security Classification" and "Intelligence Type" dimensions both map to the "read only" access level. The final part of the calculation takes the most restrictive level, and the user therefore has the "read only" access level on this item.

In general, a similar calculation is necessary to determine the grant security level for the same user on the same item. What often happens in practice is that either the user is a member of a group that confers grant access on all items, or they are not.

Supplied security implementation

One of the requirements for a deployment of i2 Analyze is a principal provider, which is the mechanism through which the users in an organization are mapped to the user groups in the security schema. When a deployment environment uses WebSphere for user authentication, the i2 Analyze Deployment Toolkit contains a production-quality class that might be an appropriate solution.

The `WebSphereDynamicAccessRoleBasedPrincipalProvider` class from the deployment toolkit performs a direct mapping from the names of user groups in WebSphere to the names of user groups in the security schema. When the user is a member of a WebSphere group, they receive access and grant rights in accordance with the contents of corresponding `<GroupPermissions>` elements in the i2 Analyze security schema.

The i2 Analyze deployment toolkit also includes an example security schema and WebSphere users file that contain correlating group names and dimension values. These files are suitable for use in test deployments, but not for live systems.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM United Kingdom Limited
Hursley House
Hursley Park
Winchester, Hants, SO21 2JN
UK

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, i2, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.