DASSAULT SYSTEMES

ENOVIA

IP SECURITY MANAGER

OBJECTIVE

IP Security Manager is used to maintain the security rule and exception classification framework that authorizes and prevents unauthorized disclosure of intellectual property (IP) within the **3D**EXPERIENCE® platform.

OVERVIEW

IP Security Manager enables organizations to classify data properly with defined security rules (based on organization, citizenship, physical location and their combination) and exceptions in an evaluated expression. This classification enables the enforcement filter to protect data from unauthorized disclosure within the **3D**EXPERIENCE® platform. This classification framework complements the general purpose access controls available with the **3D**EXPERIENCE platform and implements the description of category-specific rules that must be met by any user trying to access a data item.

IP Security Manager defines and maintains the classification of information items in **3D**EXPERIENCE platform along with the classification including the associated security rules and exceptions. That classification information is used by the platform option **IP Controlled Access** to determine whether to authorize or refuse access to the requested data item.

This method of classification and enforcement for data items in the **3D**EXPERIENCE platform (internal or by federation) means that a single **3D**EXPERIENCE platform instance can manage all relevant product data in the organization's enterprise and safely share that information according to their organization, nationality or physical location. Without this capability, organizations may be required to protect IP by storing the data in physically separate systems — with all the inconsistency, process delays and extra overhead costs these create.

HIGHLIGHTS

Define IP Security Classifications

This role is delivered with a set of pre-defined security classes, each with a unique set of credentials or conditions that must be met by a user to gain access to the information in the class. The classes can be modified or new ones created. The user credentials that are used to evaluate whether to show an item of information include citizenship, country-of-birth, organization affiliation, and current (country) location.

Granular Denied-Access Control

The customer can configure what behavior is desired when access is denied by IP classes. Items can be completely hidden from users—they appear not to exist at all—or they can be exposed in a limited way. Denial of access behavior is controlled by policy settings made with either **IP Security Manager** or **Enterprise Modeling Administrator**. Access denial results in:

- The user has no access to view any part of the item by default if read and show access are revoked.
- The user sees the Type, Name and Revision of the item if only read access is revoked.
- The user sees the Type, Name and Revision of the item and can navigate to its attributes when "show" and "read" are not revoked.
- In many case, the file content of an item is the information to be denied without authorization. Therefore, only "checkout" is revoked and other access for read, modify, show is left as is for user actions. If checkout is revoked and the user is not authorized, then the user will have no awareness that a file exists on the item.

Access Exceptions

It is common to create exceptions to the rules. In commercial settings, the exceptions are often handled with Non-Disclosure Agreements (NDAs) — in which one company grants another company (or selected people within it) access to some IP. In the context of government controls, a common mechanism is to grant an export license to waive the normal restrictions under certain, specific conditions. Such exceptions are recorded and are automatically respected by the checking mechanism in **IP Controlled Access**, which is the complimentary product for enforcing the export classifications. **IP Security Manager** can list the items covered by the exception and the people or organizations granted the access by the exception. The exceptions can also contain the documents (e.g. an NDA agreement, an export license) on which they are based and which they are designed to implement. The exceptions have their own lifecycles and properties and can participate in any relevant business processes for submission and approval.

Key Benefits:

- Companies can protect electronic IP in a robust and consistent way as a standard across the entire platform.
- Customers, partners, suppliers and employees can work in one environment while protecting each party's IP.
- All types of data in the platform can be protected with the same approach and allow an audit review of users and access in one environment.
- Multiple systems and data stores used previously for IP protection by physical data segregation can be decommissioned.
- End users can define security classifications, rules and exceptions, as well as perform security audits, without requiring the IT team.

Classification Access Audit Administration

Some functions, which can also be performed by IT personnel using other tools, are available to IP and export control professionals using the Web interface. Functions to audit and modify the administrative policy definitions for objects are available to control authorization by security classes. The capability does not expose the whole policy definition. Therefore, the policy settings made by IT are protected from inadvertent modification by the IP control team. Additionally, logs that record file transfers between sites and the location settings of users during login are available to both IT and IP professionals. The display of logged information is consolidated into a summary report with charts and data that can be navigated to more fully investigate what has occurred.

Collaboration and Approvals

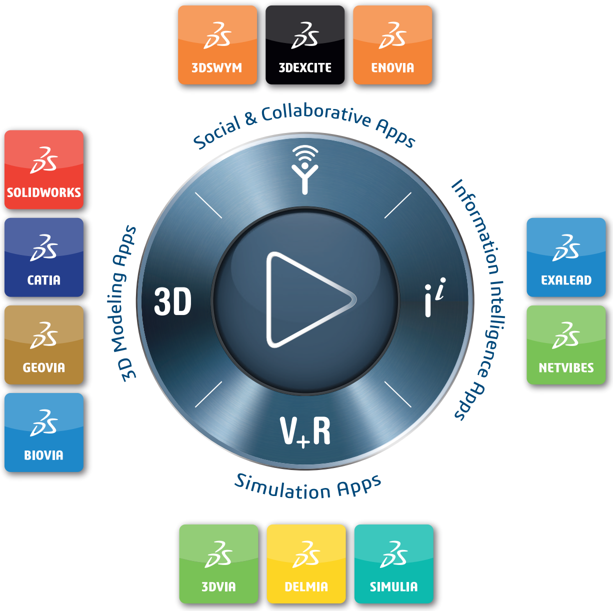
Users can benefit from a wide range of capabilities for global enterprise collaboration. Those capabilities include the ability to manage and organize shared documents and structured product data; they also enable the creation of digital workspaces for virtual teams to work together. Users can easily raise issues, organize meetings, and track decisions, while any object lifecycle modifications can be formally approved using routes defined by end-users, or to simplify and facilitate a repeatable approval process, standard route templates.

Microsoft Integration

Users can create and access **3D**EXPERIENCE data from the most popular Microsoft applications: Word®, Excel®, PowerPoint®, Outlook®, Windows Explorer, and Windows Desktop Search. This capability enables enterprise-level collaboration while not disrupting the established productivity of end-users. With product content being managed in **3D**EXPERIENCE rather than on users' PCs, organizations are able to create, manage and review product content more securely.

Our **3D**EXPERIENCE® platform powers our brand applications, serving 12 industries, and provides a rich portfolio of industry solution experiences.

Dassault Systèmes, the **3D**EXPERIENCE® Company, provides business and people with virtual universes to imagine sustainable innovations. Its world-leading solutions transform the way products are designed, produced, and supported. Dassault Systèmes' collaborative solutions foster social innovation, expanding possibilities for the virtual world to improve the real world. The group brings value to over 190,000 customers of all sizes in all industries in more than 140 countries. For more information, visit **www.3ds.com**.



DASSAULT SYSTEMES | The **3D**EXPERIENCE® Company

Europe/Middle East/Africa
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
France

Asia-Pacific
Dassault Systèmes K.K.
ThinkPark Tower
2-1-1 Osaki, Shinagawa-ku,
Tokyo 141-6020
Japan

Americas
Dassault Systèmes
175 Wyman Street
Waltham, Massachusetts
02451-1223
USA