Data Insight 5.0

Feature Briefing

User Risk and Insider Threat

This document is about the User Risk and Insider Threat enhancements in Data Insight 5.0

This document applies to the following version(s) of Data Insight 5.0.

If you have any feedback or questions about this document please email them to IIG-TFE@symatec.com stating the document title.

Feature Description

Data Insight (DI 5.0) includes improvements to its ability to monitor user risks and insider threats. These improvements include:

- User Risk Score
- User Watchlist
- Real-Time Alerts

User Risk Score

The User Risk Score allows an organization to gauge a user's risk to the environment, the higher the score, the higher the risk. Items that can affect a user's score include:

- Anomalies
  - Deviation in reads, writes, deletes, and so on
  - Deviation in number of unique files accessed
  - Deviation in number of unique sensitive files accessed
  - Percentage of distinct DLP (Data Loss Prevention) policies touched
- Alerts
  - Number of alerts against the user
- Access
  - Number of file shares the user can access
  - Number of file shares of which the user is a custodian (owner)

User Watchlist

The watchlist contains a list of users or groups who may be under scrutiny by an organization. Once a user or group is added to the watchlist, users can be monitored much more closely for any unusual activities.

Real-time Alerts

Real-time alerts provide reporting on users who are being monitored. Alerts are generated when a user accesses sensitive files as determined by DLP (Data Loss Prevention).

Business Value

User Risk Score, User Watchlist, and Real-time Alerts provide the following benefits to an organization:

- Identify users who have access to numerous files, file shares, or sensitive data
- Identify users who are custodians of a large number of file shares
- Ability to closely monitor the activities of users on a watchlist such as
  - A long-serving employee who is leaving the organization

  - A user or group who has access to a number of content repositories that store sensitive data
  - An individual who may be suggested by the Data Insight Social Network Map
- Provide real time alerting when users access content of a sensitive nature

Underlying Principles

User Risk Assessment

Data Insight assesses the risk of users' access to files and shares. Data Insight uses what is called a user risk score to determine the overall risk associated with a user having access to files and share. This user risk score is a summary of various aspects of recent user activity and is calculated on a daily basis. The user risk score summary consists of:

- Activities and events including read, write, delete, create and security sensitivity
- Number of alerts against a user and the severity of the alert (critical, medium, and low)
- Number of shares the user has read and write access on
- Number of shares the user is a custodian on
- Number of unique sensitive files accessed by the user
- Number of distinct DLP policies the user has touched sensitive data from

Each of these components will include a weighted score for both sensitive and non-sensitive files. The aggregate of these scores will calculate the overall user risk score. Customers have the option of determining their own risk scores and the severity of those scores for user risk detection.

User Watchlist

Once a user or group is added to the watchlist, Data Insight will keep track of the monitored users' activities. Selected users will show up under the "Watchlist" list view under the Data Insight Dashboard.

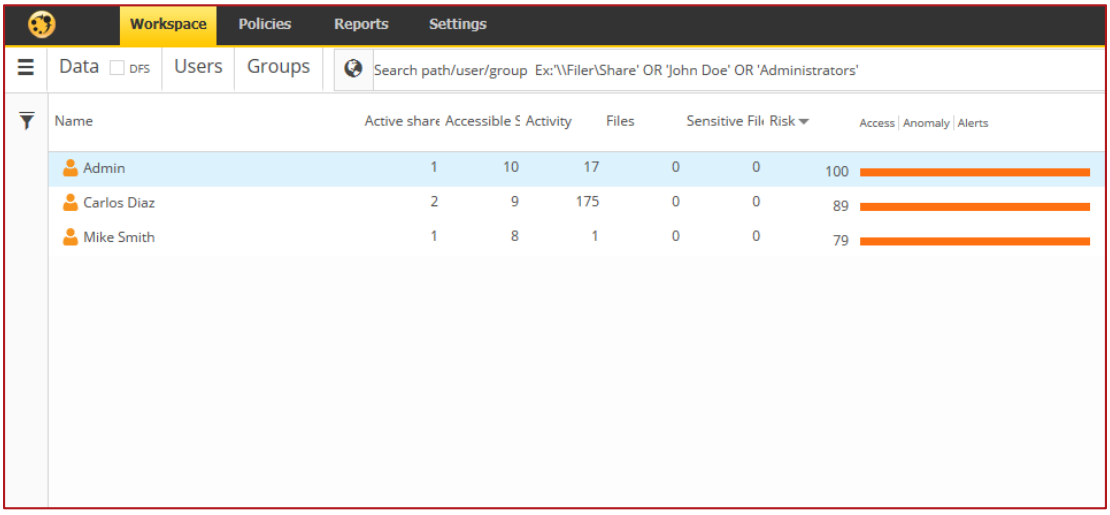

Figure 1 – Watchlist list view on the Data Insight Dashboard

Real-time Alerts

Complementing the user risk assessment in Data Insight are access alerts. Files and shares that are accessed by users with high-risk scores, may initiate an alert to Data Insight administrators. The alerts are based on the users' risk score and the threshold set by Data Insight administrators when sensitive and non-sensitive files are accessed. Additionally, access alerts may:

- Generate near real-time alerts based on data activity triggers and whitelist/blacklist conditions
- Monitor for alerts for sensitive data matching DLP policies
- Add users to a "watchlist" so their activity can be monitored

Guided Tour

User Risk Score

The User Risk Score assessment is easily viewable on the main Data Insight Dashboard. Once on the dashboard, simply click on the Users subtab (as shown in Figure 2). The Risk column will show risk score for each known user. Users who are already on a watchlist will have an orange user icon associated with them.

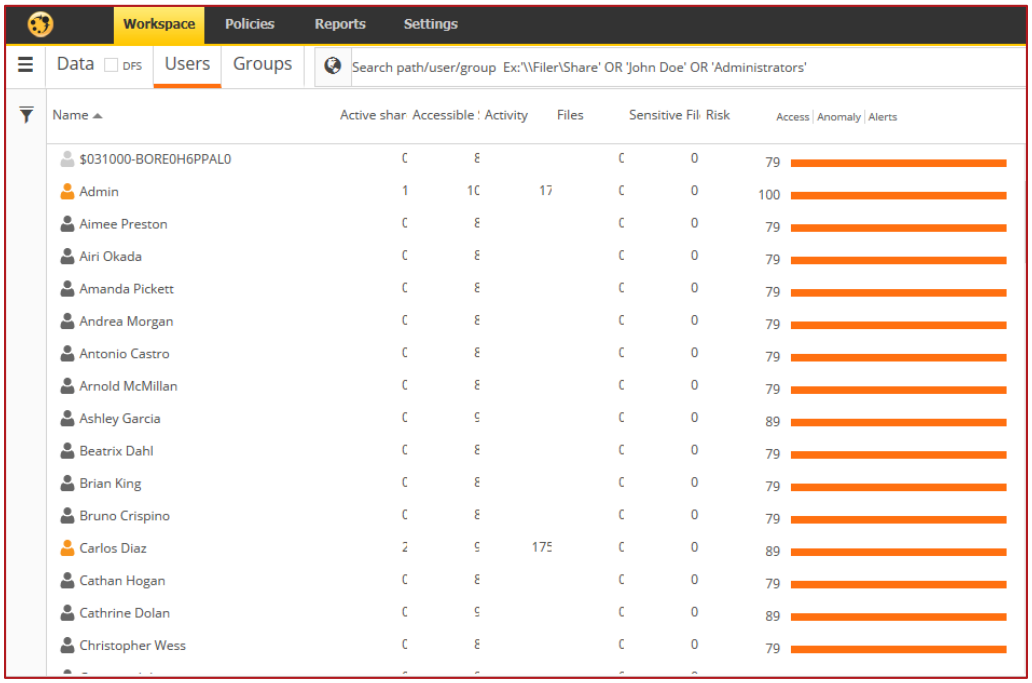

Figure 2 – User Risk Score on the Data Insight Dashboard

User Watchlist

To add a user to a watchlist, an administrator must add the user or group. This can be done by navigating to **Settings -> Global Settings -> Watchlist Settings**. Select either User or Group and then select the desired objects. A list of users or groups can be imported as well from a CSV file. See the Data Insight 5.0 administrator guides for more information.

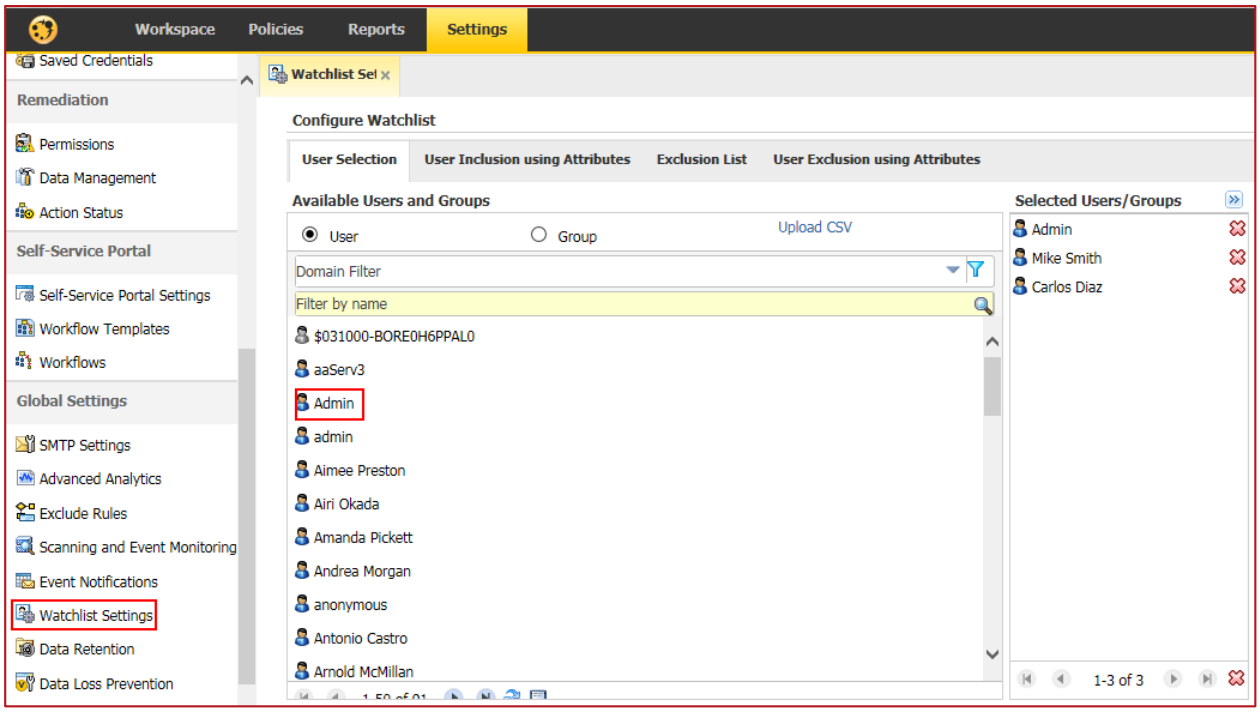

Figure 3 – Adding users or groups to the watchlist

Users and groups can be excluded from the watchlist as well by clicking on the **Exclusion List** tab.

Users can be included and excluded from the watchlist based on attributes such as login name, email address, manager, and so on, as show in Figure 4.

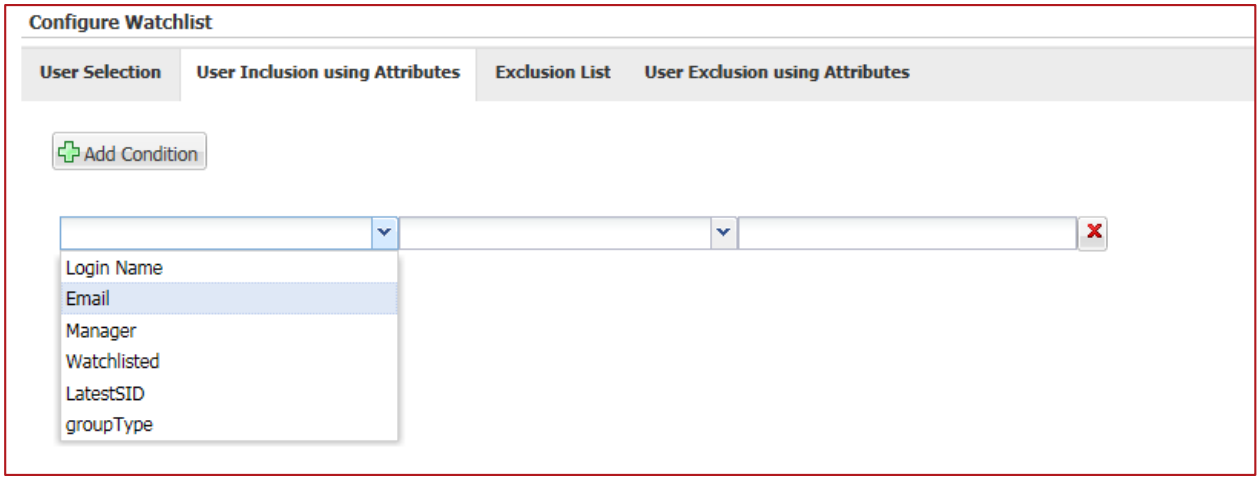

Figure 4 – Adding users to the watchlist based on attributes

Real-Time Alerts

To create a real-time alert, a Data Insight administrator needs to navigate to **Policies -> Real-time Sensitive Data Activity Policy**. From there, the administrator can add a new policy or edit an existing policy.

When creating a new policy, the administrator must define at minimum the following information:

- Policy Information – Name, description, severity, and so on
- Configure Policy – Metadata access, detailed access, DLP policy, and so on
- User/Group selection
- Notification options

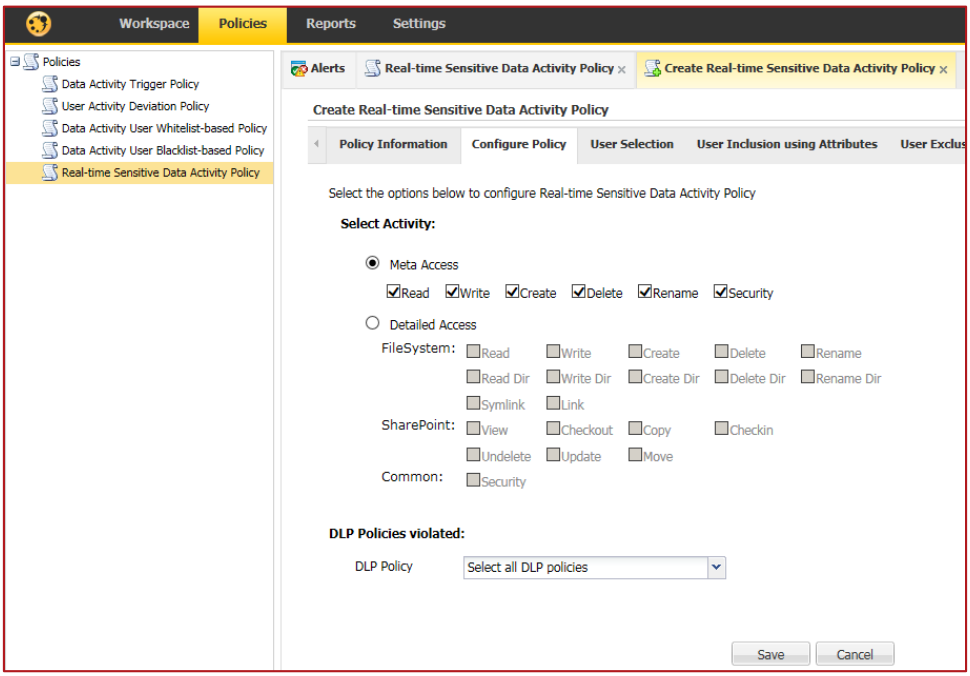

Figure 5 – Configuring real-time alert policies

Support considerations

User Risk Score

Ensure that a connection to Active Directory has been configured in Data Insight.

User Watchlist

Ensure that a connection to Active Directory has been configured in Data Insight.

Real-Time Alerts

For Real-Time Alerts to work properly, DLP must be configured properly. Without DLP configuration, a list of DLP policies will not be visible when creating real time alert policies.

About Symantec:
Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Symantec Corporation

World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA

+1 (650) 527 8000

+1 (800) 721 3934

For specific country offices and contact numbers, please visit our Web site: **www.symantec.com**