# HID SAFE™ Analytics

## MINIMIZE RISKS AND MANAGE BUSINESS PROCESSES MORE EFFECTIVELY AND EFFICIENTLY

**BENEFITS**

- Identify high-probability risks while there is time to act on them
- Automate appropriate actions upon risk discovery
- Minimize security and compliance risks
- Prevent security mishaps

### THE BUSINESS CHALLENGE

With the onset of rapid globalization, there has been an increase in the security threats faced by organizations. Yet many lack the capabilities to handle these risks. Organizations have traditionally spent a fortune on reactive security systems, which consume a lot of resources in monitoring physical and cyber systems but have failed to detect or prevent a major crime. This results in inefficient spending that only aids in detecting crimes after they are committed rather than preventing crimes before they occur. The truth remains that it is far more expensive to have to explain what went wrong than to allocate funds toward improving security processes and addressing vulnerabilities.

### HID SAFE™ ANALYTICS

HID SAFE™ Analytics enables organizations to take the power of their physical security data beyond traditional reporting and use it to predict possible security risks. HID SAFE™ Analytics utilizes the logs maintained for your security systems and, through the use of predictive analytics, transforms this data into critical knowledge and actionable insights. This helps your organization be aware of potential risks in advance and take preventive actions on a possible threat – potentially preventing a catastrophe.

### Risk Summary

The risk summary dashboard gives a birds-eye view of all the potential risks associated with an identity in the system. This view takes into account multiple Level 2 factors that affect risk, known as Indicators of Compromise (IOCs), and computes an overall score for the identity based on weights assigned for each IOC parameter. The impact of these IOCs on the overall risk score can also be customized as per an organization's requirements.

This dashboard helps you derive deeper insights on risks associated with identities, ranked in the order of severity. You can also drill down to an individual IOC or an identity to understand the data used to derive these risk scores and patterns that indicate deviant behavior.

The risk summary dashboard enables you to take necessary action to minimize any potential risks and prevent mishaps even before they happen.

### Indicators of Compromise

Indicators of Compromise (IOCs) are standardized parameters that are used to evaluate the risk associated with identities (such as employees, visitors and contractors). Each IOC is measured with a help of a risk score and is attributed to the identity.

**FEATURES**

HID SAFE™ Analytics takes a multi-layered approach to analyzing your physical access logs, thereby uncovering deeper insights from past access trends.

The assessment of risks based on IOCs is divided into two categories as below:

Expert Indicators: This approach relies on the characteristics that identities possess, which give scope for a potential misuse or threat. The system looks for known suspicious patterns and flags risks based on occurrence of such patterns. The risk measures are defined by estimating the assets/access that an identity possesses and evaluating it against the need for such privileges. A few important expert indicator characteristics include:

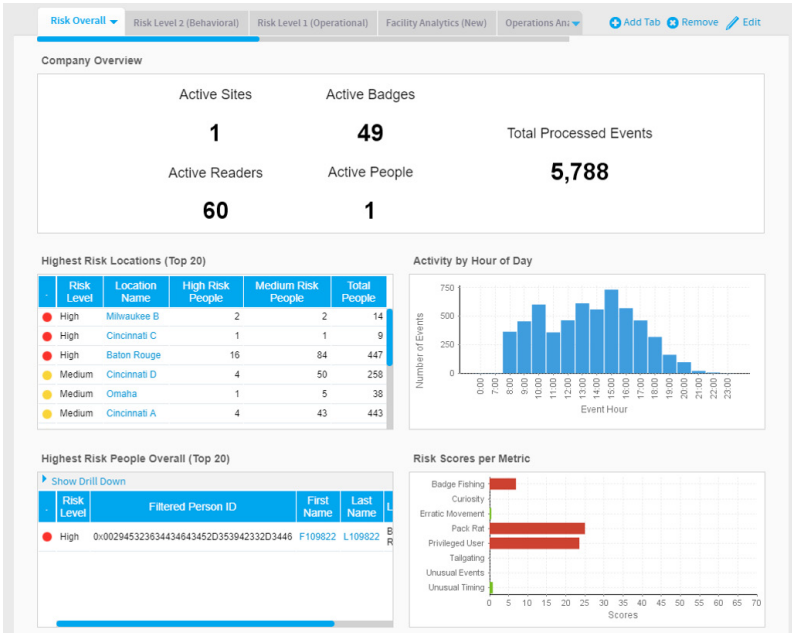
- **Tailgating:** employees who explore areas by following others who have access (piggybacking), or who hold doors open for others
- **Zombie Badge:** people who use a deactivated access card of an ex-employee
- **Badge Fishing:** employees who are exploring places that are not relevant to them or places where they don't normally go
- **Pack-Rat:** employees in possession of unusually large amounts of unused access or unnecessary assets
- **Privileged User:** employees with unusually extensive access or control of assets

Behavioral Indicators: Using behavioral analysis of access data, you can identify, understand and take measures to tackle deviant behavioral changes exhibited by identities. Behavioral analysis establishes base-line patterns for every identity and every device in the system in order to search for anomalies that indicate risk. A few important behavioral indicators include:

- **Erratic Movement:** employees with unusual pace of movement.
- **Unusual Timing:** employees who are arriving or departing at unusual hours.
- **Card Fraud:** employees who have either willingly given their credentials to others or whose cards have been stolen and can be potentially misused.

## The HID SAFE™ Analytics Difference

The key differential of HID SAFE™ Analytics boils down to actionable insights. HID SAFE™ Analytics provides risk-based analytics, allowing your organization to have a clear understanding of current risk levels across your global infrastructure. In addition, HID SAFE™ Analytics also recommends actionable responses that help mitigate risks. Once you understand your organization's operations and have a better understanding for risk levels, you will be able to make smarter decisions, have greater visibility on activities in high risk areas you need to monitor and continually improve processes to streamline operations, making you more efficient.




**hidglobal.com**


North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 55 5081 1650




2018-07-13-iams-hid-safe-analytics-ds-en
PLT-04012