

# Hitachi ID Bravura Group simplifies group lifecycle management with self-service requests, automated processes, reviews, and cleanup to make the right level of access and security available for everyone.

## DATA SHEET

## Hitachi ID Bravura Group

Access Security Groups underpin security in most systems and applications. If users are assigned to the wrong groups, they can gain inappropriate access to applications or data, which can compromise the safety of your data and organization. It is essential to assign groups based on business needs and in compliance with policy.

Hitachi ID Bravura Group simplifies group lifecycle management with self-service requests, automated processes, reviews, and cleanup to make the right level of access and security available for everyone.

### Simply Manage Group Lifecycles

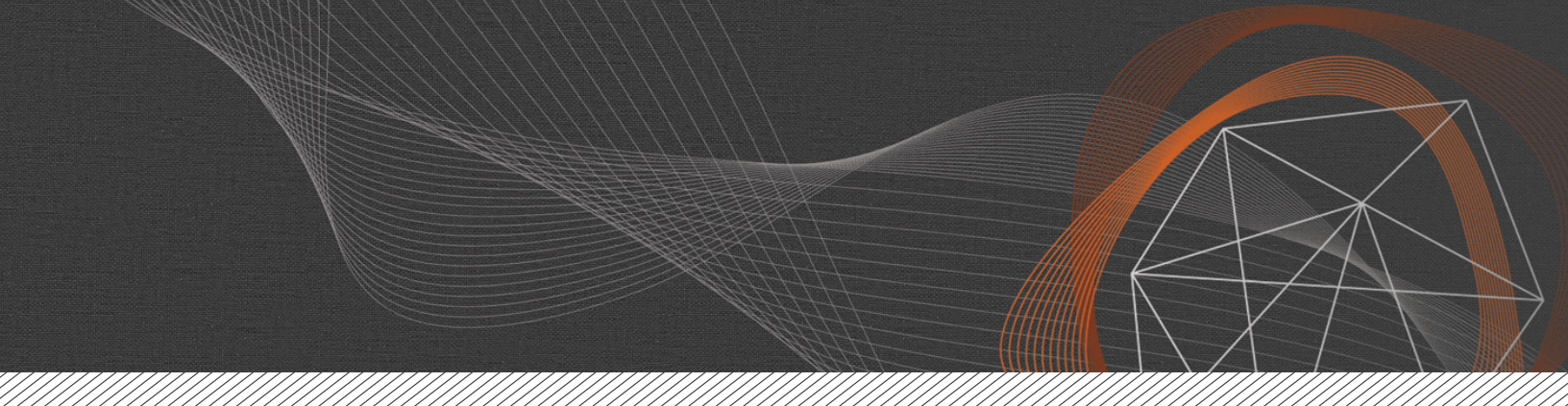
Hitachi ID Bravura Group calculates and automates appropriate access so you can simply manage group life cycles. Easily create new groups, manage group objects and memberships, plus control nested, child, and out-of-band processes. Move groups from one container to another, change names, descriptions or other attributes, assign and update owners, and ultimately delete groups to keep access tight.

More securely manage groups and mail distribution lists in directories, including Active Directory, Google, UCP, and LDAP, and access a rich set of reports to identify problems and quickly deploy remedies with automated request feedback. Moving these functions from IT to the business lowers costs while improving controls.

### Deploy Intelligent Automation and Self-Service

When users shift responsibilities (for example by being assigned to new projects), they need new access rights. Delays in the access request, approval, and fulfillment process block their ability to work. Hitachi ID Bravura Group can automatically detect newly created groups and calculate appropriate membership using authoritative data (e.g., department, location, or manager modifications), owner data, and description metadata (e.g., cost centers or country codes). Bravura Group also allows admins to include white- or black-lists as exceptions to the calculation process.

The Hitachi ID Bravura Security Fabric has the technological and architectural building blocks with decades of proven reliability to manage and protect your entire digital identity and access infrastructure from malicious attackers. It encompasses all of the Hitachi ID Bravura solutions including Identity, Privilege, Pass, and Group with the Hitachi ID Bravura Discover threat detection and response (TDR) layer together in a singular, powerful platform.



For less predictable groups, Hitachi ID Bravura Group offers a request portal combined with approval workflows. Hitachi ID Bravura Group also helps users formulate clear access control requests with appropriate group memberships. Additionally, Bravura Group enables requests for particular roles that include multiple groups and can model understandable business functions, offering requesters items that are popular among the peers of a recipient. Hitachi ID Bravura Group also includes a periodic review process where stakeholders such as managers or group owners can either certify members or revoke access.

### Control and Enforce Policies in Real Time

Group membership is normally subject to policy controls, including approvals for change requests, segregation of duties (SoD) with mutually exclusive group memberships, role-based access controls, and risk scores. Hitachi ID Bravura Group enforces a variety of policies to ensure that groups and their membership are business appropriate. This includes rules for selecting authorizers, SoD, risk scoring, temporary assignment, naming, and container selection.

Because it's configured as the sole entity authorized to make changes to groups or group memberships on Active Directory domains, Hitachi ID Bravura Group can detect changes made using other tools as they happen. A real-time connector to Active Directory enables Hitachi ID Bravura Group to respond to changes as they happen, with the option to reverse changes and raise alerts immediately.

### Get Actionable Analytics and Audits

Internal control problems arise when there are more groups than users and group existence and membership assignments are not supported by the change history or business context. Hitachi ID Bravura Group offers a rich set of reports that identifies common data quality problems, including:

- Groups with overlapping membership
- Clusters that might serve as roles
- Nesting cycles
- Too-small or too-large groups
- No owner or an invalid owner
- Groups whose membership violates SoD rules

A feedback path from reports to requests can then automate problem remediation.

**Hitachi ID leverages decades of experience to deliver the industry's only single platform Identity, Privileged Access, and Password Management solution, resulting in rock-solid reliability, performance and scalability.**

**Minimum Requirements: Intel Xeon or similar CPU. Multi-core CPU, Dual core. 16GB RAM – 32GB or more per server, 600GB HD storage in an enterprise RAID configuration, and one Gbit Ethernet NIC.**