Hitachi ID

Reduce IT security risk and enhance authorized access and accountability the frictionless, time-limited privileged access of Hitachi ID Bravura Privilege.

DATA SHEET

Hitachi ID Bravura Privilege

Provide frictionless, elevated, and time-limited access to reduce IT security risk and enhance accountability with Hitachi ID Bravura Privilege. Our privileged access management (PAM) solution supports over a million daily password randomizations and facilitates access for thousands of authorized users, applications, and systems through a highly available, geo-redundant architecture. Use Hitachi ID Bravura Privilege to create custom accountability by documenting every disclosure of access to every privileged account through custom reports to fine-tune the data and gain valuable insight.

Hitachi ID Bravura Privilege can integrate with every client, server, hypervisor, database, and application, on-premise or in the cloud. It is part of the Hitachi ID Bravura Security Fabric, a singular IAM platform and framework that includes Hitachi ID Bravura Privilege, Identity, Pass, Group, and Discover. Working within a singular security fabric, you can easily weave access and privilege patterns by combining Hitachi ID Bravura services as your access management program evolves without having to install separate solutions.

Randomize Privileged Account Passwords

As the scope of an organization's IT assets grows – sometimes with thousands of privileged accounts across a wide variety of platforms – it can become increasingly difficult to securely manage those assets. Coordinating password changes or tracking changes back to individuals can be even more painful without a privileged access management (PAM) system. Hitachi ID Bravura Privilege replaces shared and static passwords tied to privileged accounts with periodically new and random values based on robust password policy controls. It can enforce multiple scheduled or event-triggered password policies on fixed IT assets, laptops, and rapidly provisioned virtual machines.

Securely Store Credentials

When passwords are changed regularly, a robust storage mechanism prevents unauthorized disclosure and ensures maximum availability when faced with a site outage. Hitachi ID Bravura Privilege includes a unique, geographically distributed active-active architecture that replicates this critical data set in real time across all instances for high-availability and disaster recovery scenarios. Data at rest and in transit is encrypted using a 256 AES encryption key unique to each customer.

POWER OF ONE

Hitachi ID Bravura Identity

Revolutionize your digital identity program with Hitachi ID Bravura Identity. Implement the best-in-class Hitachi ID solution to enforce security, cross-platform access policies, and uphold the principles of least privilege.

Hitachi ID Bravura Privilege

Reduce IT security risk and enhance accountability with frictionless, time-limited privileged access. Hitachi ID Bravura Privilege facilitates millions of daily password randomizations and authorizes access with a highly available, geo-redundant solution.

Hitachi ID Bravura Pass

Improve login security processes and simplify credential management for passwords, tokens, smart cards, security questions and biometrics management across systems and applications with Hitachi ID Bravura Pass.

Hitachi ID Bravura Safe

An easy-to-implement enterprise password safe that centrally, consistently, and securely manages decentralized passwords, secrets, and files to protect against cyberattacks. Employees can securely send time-bound passwords for new accounts, encryption keys for files, or entire files without them being leaked or intercepted.

Hitachi ID Bravura Discover

Hitachi ID Bravura Discover delivers a powerful risk and threat assessment for both IAM and PAM solutions to get your organization on the right track–quickly. Its automated discovery analysis takes just a day to provide the most accurate data to close identity and privileged access security gaps with confidence by removing the potential for human error or intervention.

Enable Robust Access Control Policies

Hitachi ID Bravura Privilege provides access to shared accounts and elevated group memberships based on flexible, robust, and easily managed access control policies. High- frequency users can be pre-authorized based on group memberships or identity attributes without waiting for approvals. On the other hand, infrequent users can request to gain access when appropriate and for a defined time interval.

Get Just-in-Time Access

By leveraging the Hitachi ID Bravura Security Fabric, Bravura Privilege customers can take just-in-time (JIT) access to the next level, incorporating create, read, update, and delete (CRUD) operations and groups as part of their privileged access disclosure processes on both accounts. Bravura Privilege supports the creation, updating, and deleting of privileged accounts and groups to help customers achieve the principle of Zero Standing Privileges (ZSP) where and when it makes sense to do so.

Ensure Administrator Accountability

IT staff often manage the highest privilege accounts using generic login IDs without administrative change auditability and accountability. Hitachi ID Bravura Privilege randomizes administrator passwords frequently, so that each password is different, changes over time and is not known to anyone. It mediates logins to these accounts, requiring that users be personally identified, strongly authenticated, and specifically authorized for the access. Shared account usage with elevated privileges is linked to individual IT staff to create strong accountability for administrative changes.

Generate Forensic Audits of Privileged Logins

In rare instances, staff may be suspected of causing harm. When this happens, it is helpful to be able to see what the user did while connected to privileged accounts. Audit logs can support forensic audits where policy may dictate login sessions be recorded for vendor access, to high-risk systems, or to systems in certain jurisdictions or processing certain kinds of data. Hitachi ID Bravura Privilege can record keyboard input, take a picture with time and day stamp info, and collect other data key for forensic audits and internal knowledge sharing and training. Session recording, search and playback provide a high level of accountability. Recorded sessions are secured through a combination of access control policies and workflow approvals, designed to safeguard user privacy.

Discover SSH Trust Relationships

Discover and analyze existing SSH trust relationships and create temporary access disclosure to build a trust graph to prevent unauthorized access. Hitachi ID Bravura Privilege can take into consideration when computing requires approvals for access, and report on the trust relationships. Trust graph analytics, in turn, can identify high-risk accounts and disable unnecessary trust relationships.

Easily Scale Up

In organizations with tens of thousands of accounts added and retired at a pace of hundreds daily, it is not feasible to manually configure every managed system and account. Hitachi ID Bravura Privilege includes advanced infrastructure and auto- discovery to collect system inventory data from multiple sources and apply rules to decide which systems to connect and what credentials to use. Systems can be probed to find all accounts, groups, and services. Organizations can apply further rules to decide which accounts and groups to manage and policies to attach to each one. Regular auto-discovery with policy-driven classification lets you easily scale

Manage Personal Administrator Accounts

Technical staff in many organizations are assigned secondary accounts with elevated privileges to perform administrative duties. This helps prevent excessive privileges being associated with regular user accounts and reduces the risk of escalation and other attack vectors targeting logged-in users.

Delegate and Maintain Tight Policy Control

Hitachi ID Bravura Privilege encompasses the ability to designate trustees who can allocate responsibilities to other team members. Delegating authority ensures that those directly responsible for each system type maintain tight control over all of the policies governing who can access what, when, and how.regular user accounts and reduces the risk of escalation and other attack vectors targeting logged-in users.

MINIMUM REQUIREMENTS

Type	
Processor	• Intel Xeon or similar CPU. Multi-core CPU, Dual core.
Memory	• 16GB RAM – 32GB or more per server
HD	• 600GB HD storage in an enterprise RAID configuration
OTHER	• Gbit Ethernet NIC. Windows Server 2019 (Version 10.0.17763.1397) including updates to 09-2020. Docker version 19.03.11 or higher.

Hitachi ID

Corporate Headquarters
1401 - 1st Street S.E., Suite 500
Calgary, Alberta, Canada T2G 2J3
hitachi-id.com

Contact Information
1.403.233.0740
Sales Toll Free: 1.877.386.0372 / 1.877.495.0459
sales@Hitachi-ID.com