

Hitachi ID Identity Manager Features at a Glance

FEATURE: Automatically provision new users

Description

Identity Manager monitors one or more systems of record, such as HR or a corporate directory, for changes. When it detects new users it can automatically provision login accounts for those users on multiple systems and applications.

Benefit

Auto-provisioning reduces the time that new hires must wait for systems access and eliminates a significant amount of manual administration.

FEATURE: Automatically deactivate users

Description

The same automation which can provision new users can detect when users have either been removed from or disabled on a system of record and automatically deactivate their access to other systems.

Benefit

Automatic access deactivation eliminates orphan accounts and closes a significant security exposure for many organizations.

FEATURE: Identity synchronization

Description

Changes made to user records on one system can be automatically propagated to other systems. For example, if a user's department code is changed in the HR system, or the user's phone number changes in a white pages application, or the user's e-mail address changes in the corporate directory, the new value can be automatically propagated to every other system where the user has an account or other record.

Benefit

Identity synchronization reduces the burden of ongoing administration on system administrators. Improved data consistency and reliability helps other applications with both user service and security.

FEATURE: Self-service profile updates and change requests

Description

Users can sign into Identity Manager to update their personal information and to request access to systems, applications and security groups. This allows organizations to replace multiple, home-grown request systems with a single, consolidated and automated request system.

Benefit

When users can make self-service updates and requests, user service is improved while the cost of delivering IT services is reduced.

FEATURE: Delegated administration of users and entitlements

Description

Identity Manager empowers managers, application owners and other business users to submit requests to make changes to user profiles, to grant security entitlements to users and to deactivate entitlements.

Benefit

This capability helps to eliminate both custom change request systems and calls to the security administration team. It puts the power and responsibility to change user entitlements in the hands of the business users who understand the context in which those changes are made.

FEATURE: Policy enforcement: role based access control and segregation of duties

Description

Identity Manager can assign entitlements using roles – pre-defined collections of security entitlements that are attached to users either through human requests or because users match conditions based on their profiles (e.g., department code, job code and location). When entitlements are assigned to users, either through automation or requests, they are subjected to policy review and may be rejected because they violate segregation of duties rules.

Benefit

Policy enforcement helps organizations ensure that users have appropriate security entitlements – based on a policy of least privilege, prevent fraud and identify high risk users who should be subjected to closer surveillance.

FEATURE: Authorization workflow

Description

When Identity Manager processes change requests, it applies a policy to determine whether authorization is required before the changes are applied to integrated systems. This is done regardless of whether requests came from the automation engine or user requests.

When authorizers are needed, Identity Manager may invite multiple users to review and either approve or reject a change request. Authorizers are invited concurrently, so as to limit the delay between when a change request is received and when it is either fulfilled or rejected.

Benefit

Reliable change authorization enables Identity Manager to manage requests for sensitive resources. It is a security feature, because without authorization, users could help themselves to sensitive access to systems and applications.

FEATURE: Implementer operations / One stop shopping experience

Description

Identity Manager can accept, validate, authorize and fulfill requests for changes both on systems to which it has been integrated and systems where human beings have been designated as “implementers.” Once requests for action by implementers have been approved, e-mails are sent to implementers, inviting them to fulfill the requests manually. A full workflow process is used here – including reminders, escalation, delegation and feedback from implementers to describe the work they have completed.

Benefit

Implementer operations enable organizations to implement a “one stop shopping” experience for users. Requesters need not be concerned about whether the changes they would like will be implemented by software or by a person – and they need not use different applications for each kind of request.

FEATURE: Inventory management / Physical access control

Description

Identity Manager can manage requests for physical objects – building access badges, cell phones, smart cards, OTP tokens, PCs, etc. When this is done, it can track physical inventory of such items and allocate items from inventory to approved recipients.

Benefit

Traditional asset management systems are more suited to financial management – depreciation of bulk purchases and the like – rather than allocation of individual, low-cost devices such as badges to individuals. Identity Manager fills this gap, which supports its use as a “one stop shopping” portal for both logical access and physical devices.

FEATURE: Reporting and auditing

Description

Identity Manager collects, correlates and manages information about user access to a variety of systems, including login IDs, group memberships, last login dates and change history. This data is available for reporting and audit.

Benefit

Consolidated reporting allows auditors to see who has what security entitlements, when they got those rights, who approved them, etc.

FEATURE: Rich set of included connectors

Description

Identity Manager includes integrations for over 113 types of systems and applications, plus a variety of one time password devices, smart cards, help desk incident management systems and more. It also includes flexible connectors, which can be scripted to quickly integrate with additional (non-standard) systems and applications.

Benefit

A rich set of included connectors plus flexible scripted integrations mean that Identity Manager can be quickly and inexpensively integrated with the majority of enterprise systems and applications within any given organization.