IBM Security Identity Manager

Deliver intelligent identity and access assurance across the enterprise

Highlights

- Empower managers to set up user access rights with an intuitive user interface
- Improve decision making with enhanced identity analytics reporting
- Support managers on the go with a mobile interface for processing employee requests from a smartphone
- Increase efficiency and reduce administration costs with centralized user self-service, automated approvals processing, role mining and password management
- Simplify the design, implementation and validation of role and access structure across the organization
- Strengthen compliance and security through separation-of-duty enforcement and recertification of user entitlements

IBM® Security Identity Manager is an automated and policy-based solution that manages user access rights across the extended enterprise. Through the use of roles, accounts and access permissions, the product helps automate the creation, modification and termination of user privileges throughout the entire user lifecycle. Its embedded role lifecycle management component can streamline the role structure approval process and reduce errors when validating access with the business.

What's more, Security Identity Manager includes an easy-to-use, intuitive user interface that can help business managers make intelligent access decisions. It also provides direct access to enhanced reporting and analytic capabilities.

As part of its core functionality, Security Identity Manager delivers:

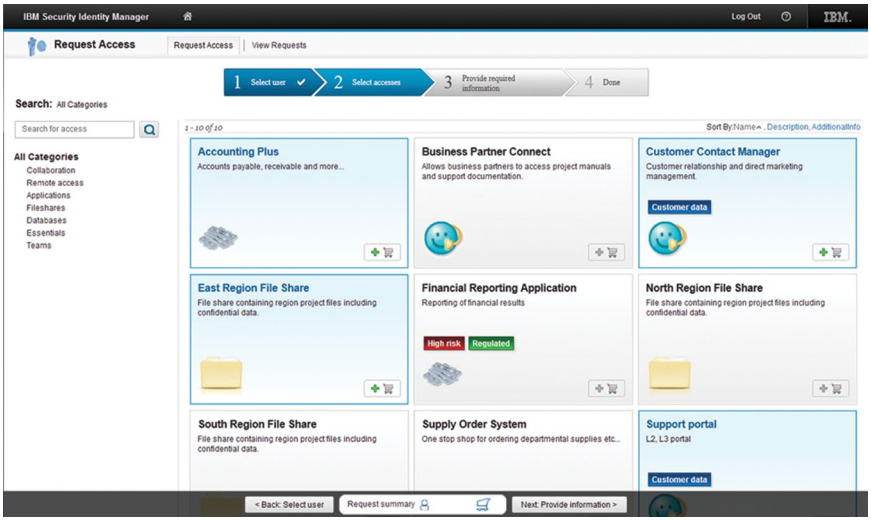
- User lifecycle management capabilities, such as automated onboarding of users, that can help improve productivity and lower costs
- Effective and actionable compliance with centralized identity and access management across the enterprise
- Web self-service for managing business roles, accounts, group membership and passwords
- A set of controls that enhance security, including preventive separation of duties and closed-loop reconciliation that detects and corrects changes to native target systems
- Broad, out-of-the-box support for managing user access rights and passwords on various applications and systems, plus a rapid integration toolkit for managing custom applications
- Flexible reporting for user access rights leveraging automatic synchronization of user data from different repositories

- A role hierarchy that streamlines administration, provides visibility of user access, and helps bridge the gap between how business users view their IT resources and the actual IT implementation of user access rights
- A robust provisioning engine that adds and removes user access rights based on membership in business roles or requests for user accounts and fine-grained entitlements such as shared folders or web portlets
- An embedded workflow engine for automated submission and approval of user requests and periodic certification of user access rights
- Group management to help simplify and reduce the cost of user administration by offering the ability to add, remove or change the attributes of a group entity within the IBM Security Identity Manager console

Security Identity Manager is part of a broad portfolio of threat-aware identity and access management solutions from IBM. These solutions are designed to help clients manage and secure identities as a key line of defense across multiple perimeters, providing secure online access in mobile, cloud and social environments. As a result, organizations can improve identity assurance, facilitate compliance, and reduce operational costs by enforcing secure user access to data, applications and infrastructure across the extended enterprise.

Simplify access management with an intuitive user interface

Security Identity Manager comes with the Identity Service Center, an easy-to-use, intuitive user interface that can help business managers request access rights—including accounts, roles and group membership—for their employees. These self-service capabilities can help save valuable time for IT staff. In addition, the Identity Service Center lets managers make multiple access requests for an individual employee, helping to improve productivity and accuracy.



IBM Security Identity Manager features the Identity Service Center, an intuitive user interface that can help managers make intelligent access decisions.

Create audit trails with detailed reports

To further strengthen identity and access controls, Security Identity Manager includes native IBM Cognos® reporting capabilities and expanded Cognos report samples. This can help you easily deliver reports on consolidated workflows as well as changes to access rights. Security Identity Manager also includes audit trail collection, correlation and detailed reporting to address compliance mandates. Report examples include:

- Recertification history
- Orphan and dormant accounts
- Separation-of-duties summary

By using Cognos reporting with Security Identity Manager, you can also leverage custom report authoring and report distribution to meet the unique needs of your organization.

Automatically recertify access rights

Security Identity Manager helps keep the simple tasks simple while still allowing for advanced customization. Powerful access rights recertification features provide granular, auditor-friendly details for compliance along with policies that can be easily configured using wizards and templates. You can use Security Identity Manager to:

- Quickly define recertification policies based on frequently used scenarios such as requiring an employee's manager to approve the employee's access to the financial data warehouse once per quarter
- Ease administrative impact of manager approval through bulk recertification of a user's roles, accounts and groups
- Model advanced workflows and organization processes with the web-based graphical workflow designer
- Conduct compliance attestation for a large number of IT resources not configured for automated account provisioning

Establish separation of duties to manage business process conflict

Security Identity Manager helps manage business process conflicts with IT user access rights. Preventive, policy-based separation of duties enables you to define a business conflict (for example, an investment banker cannot also be a stock broker at the same time) and ensure proper administration of user access rights. This associates the appropriate security and compliance requirements that are critical to preventing business conflicts with the roles and provisioning policies governing user access rights. Organizations can still maintain business flexibility by utilizing an exception workflow that gathers the business justification when an exception to the separation-of-duties policy is required.

Use automated reconciliation to detect and correct noncompliant accounts

"Closed loop" reconciliation features can automatically detect and repair access policy violations that occur due to erroneous changes made on a managed resource's administrative console. You can use access rights reconciliation, recertification and reporting to:

- Automatically load and reconcile account data
- Identify and eliminate dormant and ghost accounts
- Provide ongoing proof for compliance and auditing
- Maintain records of changes related to access rights

Leverage request-based provisioning and access entitlements

Managers and delegated administrators can take advantage of comprehensive, request-based provisioning to easily request (with approval workflow) and approve user access to roles, accounts or fine-grained access entitlements such as shared folders. Using an intuitive user interface, managers can quickly

and easily request access rights for employees—including roles, accounts and access groups—and change or delete access. They can also approve access requests and recertify users.

Using the mobile application, managers can also approve employee entitlement requests, and users can change or reset their passwords—all from their own smartphone.

Reduce costs with self-service and password management

Security Identity Manager enables end users to perform tasks such as password changes, profile updates and requests for new access rights, helping to reduce costly help-desk calls. For example, a self-service challenge/response system is included to enable users to correct forgotten passwords without calling the help desk. Requests can be viewed, modified, approved or rejected through a web-based interface, and users can be automatically notified of the status of their requests. Security Identity Manager can also help improve access control and overall security by enforcing policy-based password controls, such as hard-to-guess passwords and frequent password changes.

Web-based, self-service, role- and rule-based administration features in Security Identity Manager—as well as its embedded workflow engine—enable administrators to group users according to business needs and delegate functionality as needed. For example, they can easily specify who can add, delete, modify and view users and reset user passwords. By delegating these tasks to other organizations and business units, administrators can have more time for more strategic activities.

Support existing, new and customized environments with little or no coding

Security Identity Manager provides out-of-the-box support for more than 50 endpoint-managed systems that can be managed remotely or with a local adapter to simplify deployment. It also provides tools to help assimilate these new business resources as they are added.

Through its dynamic schema discovery process and flexible architecture, embedded IBM Security Directory Integrator technology can provide Security Identity Manager with administrative control over organizations' homegrown applications—without requiring you to write or maintain code.

Streamline the design of an effective role access structure

Chief information officers and IT directors are taking steps to improve or streamline the manner in which role-based access is provided. These processes are labor intensive due to the necessary analytics, and they require regular interaction with the business owners. Generally, these projects end up taking too long and the results are obsolete by the time they are implemented.

The IBM Security Role and Policy Modeler component of Security Identity Manager provides a platform that facilitates the iterative role modeling and mining process. It creates a business-user friendly sandbox environment that models and simulates access scenarios and policies for a more effective role and access structure for the business. Business analysts are able to hone the role definitions with a broad set of best-practice role analytics tools. The solution also helps automate role lifecycle management using a business process automation platform for role structure approvals by business owners. This capability can help you:

- Reduce the time to collect, clean and validate user access data, analyze it for common patterns of access and produce an effective role structure
- Obtain quick approval from the business for rapid deployment or certification of the role structure
- Offload decisions about user access policies to the business owners

Deliver access through a hierarchical role structure

Security Identity Manager offers a role hierarchy that establishes parent/member role relationships to automatically create user access rights through the notion of inheritance between roles. You can administer a role structure that contains business roles (collections of users) and application roles (collections of permissions). And when roles are associated with provisioning policies, they can automatically grant, modify or remove user access rights. This can simplify and reduce the cost of administering user access to resources, while also helping reduce the potential for administrative errors and inconsistencies inherent in manual processes.

Quickly configure systems and onboard new services

Security Identity Manager can help you significantly reduce the time required to activate new accounts and onboard new managed services. Preinstalled adapters, wizard-driven templates and built-in account defaults help accelerate deployments and reduce the learning curve for new users.

The powerful workflow and policy engine within Security Identity Manager can easily be configured in either "simple" or "advanced" mode. Simple mode uses predefined best-practice templates to implement basic provisioning, recertification and compliance-alert workflows. Configuration and setup is easy using only drop-down lists, check boxes and radio buttons—no scripting or programming knowledge is required. Advanced mode provides a graphical, drag-and-drop workflow designer to quickly organize and easily develop workflow processes to support the organization's provisioning policies. For example, the workflow engine supports parallel and serial approval processes and also provides checkpoints in a workflow process to allow input of additional provisioning information.

Establish group management

Security Identity Manager helps automate and centralize the definition of groups used to manage user access on native applications and systems. You can add, modify or delete groups directly from Security Identity Manager and streamline the process for defining access and assigning user membership to groups.

Take advantage of customizable interfaces for optimal usability

Security Identity Manager is not built with a "one-size-fits-all" approach to identity management. You can easily customize and integrate the user interfaces into an existing intranet or extranet site, allowing disparate users— such as auditors, end users, managers, help-desk personnel, application owners and administrators—to see the information that is most important to them. Customization options include style sheets and on/off configuration options, such as whether or not to show navigation "breadcrumbs" or a header banner. And there is no need to re-implement customizations during software upgrades.

Why IBM?

Security Identity Manager is a comprehensive identity and access governance solution that provides embedded core role management functionality—role hierarchy, separation of duties, role modeling and role lifecycle management—integrated into a single product. It also includes the IBM Security Role and Policy Modeler, which helps you quickly design and fine tune the role structure into an effective access template that is validated with the business owners throughout its lifecycle.

IBM Security offers threat-aware identity and access management solutions to help clients manage and secure identities as a key line of defense across multiple perimeters, providing secure online access in today's mobile, cloud and social environments. IBM Security solutions can help organizations prevent insider threats, protect online resources from unauthorized access, comply with security regulations, and meet some of today's biggest security challenges.

IBM Security Identity Manager at a glance

Supported platforms:

- IBM AIX®
- Microsoft Windows Server
- SUSE Linux Enterprise Server
- Red Hat Enterprise Linux

Supported managed systems:

Integrates with dozens of popular applications and platforms, through the use of adapters:

- Operating systems
- Databases, directories, content management systems
- Cloud applications such as Salesforce.com and Google Apps
- Access control systems
- Email and messaging systems
- Business applications and enterprise resource planning (ERP) systems

For more information

To learn more about how IBM Security Identity Manager, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/us/en/identity-manager/

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
November 2013

TID10294-USEN-05