IBM Security Directory Server

Build a powerful and security-rich data foundation for enterprise identity management

Highlights

- Support hundreds of millions of entries with proven IBM® DB2® technology and built-in proxy server
- Extend on-demand identity infrastructure to leading business solutions through Lightweight Directory Access Protocol compliance
- Maintain high availability with master/subordinate and peer-to-peer replication capabilities
- Easily integrate with IBM middleware, identity management and security products; leverage open integration with non-IBM offerings
- Use web-based graphical user interface and social networking capabilities via IBM Security Directory Server White Pages
- Support leading platforms from IBM, Oracle, Microsoft, AMD and Linux

Enterprise security and identity management are top concerns for most IT departments. Leveraging advanced on-demand capabilities, such as compliance management and IT service management, increasingly depends on a comprehensive identity data infrastructure. Today's directories serve as central identity data repositories and key integration points where identity, security, applications, systems and network management, and other network services all converge to store and retrieve data.

IBM Security Directory Server helps organizations meet today's IT challenges by providing a high-performance Lightweight Directory Access Protocol (LDAP) identity infrastructure. A powerful, security-rich and standards-compliant enterprise directory, IBM Security Directory Server is built to serve as the identity data foundation for web applications and identity management initiatives. It helps enable rapid development and deployment with strong management, replication and security features.

Enable mission-critical security and authentication

IBM Security Directory Server is built for identity management within a complex environment, supporting both self service and delegated administration. Consequently, organizations can use IBM Security Directory Server to reliably authenticate users and help protect their on-demand business environments as they open up their internal business processes to customers, supply-chain partners and automated-transaction systems.

With its advanced security capabilities, IBM Security Directory Server helps organizations:

- Implement self service and delegated administration by controlling data access down to the individual attribute level
- Limit access to attributes within an entry so that users can update a specific number of attributes and just read the rest
- Securely encrypt the values stored within the directory using the latest encryption algorithms, including:
  - Advanced Encryption Standard (AES)-based encryption
  - Salted Secure Hash Algorithm (SHA) encryption
- Offer secure access to directory data by providing:
  - Certified compliance with Common Criteria security standards at Evaluation Assurance Level 4 (EAL4)
  - Secure Sockets Layer (SSL) technology to encrypt data that is transmitted on the wire
  - Support for Public-Key Cryptography Standards (PKCS) #11 hardware key storage and cryptographic acceleration
  - Cryptographic modules that have received Federal Information Processing Standards (FIPS) 140-2 certification
- Define global, group and individual password policies
- Allow delegation of authority to multiple directory administrators with granular administrative roles such as:
  - Password administrator
  - Server start/stop administrator
- Set and enforce password policies for logins used by directory server administrators
- Protect directory data against denial-of-service attacks by using user- and group-specific search limits and identity assertions

Flexibly integrate with other applications

Client software-development kits (SDKs) for IBM Security Directory Server feature 32- and 64-bit clients so that the directory server can be used with a variety of platforms. Java access can be handled through standard Java Naming and Directory Interfaces (JNDIs), while a provided Java toolkit helps address LDAP controls and extended operations. In addition to the provided SDK and Java toolkit, IBM Security Directory Server supports access from all standard LDAP clients, including those for Java and C.

Meet reliability and scalability requirements

When organizations require 24x7 availability and exceptional performance to meet their global, mission-critical enterprise requirements, IBM Security Directory Server is an ideal solution. It leverages DB2 technology to provide the performance, reliability and scalability needed for an on-demand enterprise directory. Consequently, IBM Security Directory Server makes directory information highly available for important business applications across a variety of operating systems. It provides authentication mechanisms with configurable unique attributes, such as emails or employee IDs, in addition to traditional distinguished name (DN) syntax.

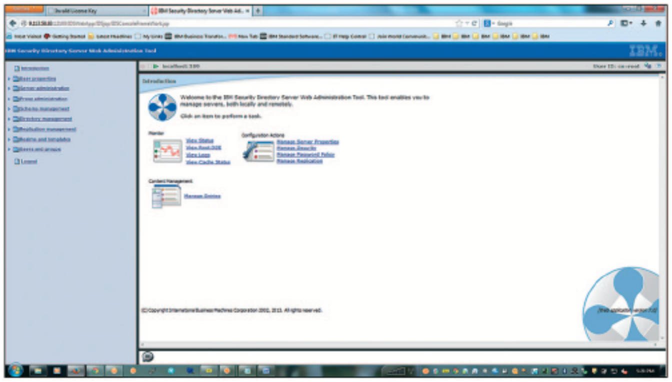
IBM Security Directory Server also extends scalability and reliability by including a front-end proxy server. The proxy server automatically distributes, reads and writes across a number of directory partitions. As a result, it can scale to handle hundreds of millions of entries. For additional availability and performance, this proxy server provides fast automatic failover and load balancing between partitions running on backend servers, which are transparent to LDAP clients.

IBM Security Directory Server further enhances scalability by supporting 64-bit server implementations. At the same time, it maintains support for 32-bit implementations to provide greater flexibility.

Further maximize reliability with advanced replication

Robust replication options in IBM Security Directory Server not only help enhance performance, but also provide greater flexibility. IBM Security Directory Server supports:

- Peer-to-peer replication, which enables the use of dozens of master servers; replication conflict resolution based on timestamps helps guarantee data convergence
- Partial and subtree replication, so that a filtered subset of entries or attributes can be replicated for use in special-purpose directory instances
- Multi-threaded replication, to help improve performance in environments that have a large amount of replication traffic
- Improved searches on large and complex subtrees, thanks to significant performance enhancements to subtree and one-level search capabilities
- Improved performance with IBM AIX® systems for all types of LDAP operations
- Flexible authentication feature, enabling use of unique attributes to authenticate with IBM Security Directory Server



Welcome to the IBM Security Directory Server Web Administration Tool. This tool enables you to manage servers, both locally and remotely.

Click an item to perform a task.

IBM Security Directory Server web administration handles directory server management.

Help optimize flexibility in directory infrastructure

By allowing users to place multiple instances of the directory server on a single hardware server, IBM Security Directory Server provides extreme configuration flexibility. It also enables users to host multiple IBM Security Directory Server instances at different version levels. As a result, they can configure different environments for test and production purposes or mix directory server versions on a single server.

Other capabilities designed to provide substantial configuration flexibility include:

- Comprehensive and extensible schema—Update all schema dynamically without server restarts
- Plug-in support—Comprehensively extend additional server capabilities
- National Language Support (NLS)—Make consoles and documentation available in many languages

Simplify synchronization with other directories

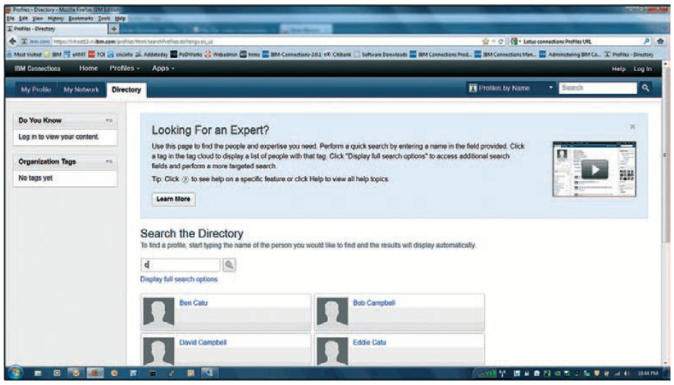
IBM Security Directory Server helps minimize the administration costs and inconsistencies that accompany manual synchronization of different directories. A built-in application synchronizes IBM Security Directory Server content with Microsoft Active Directory so that entries made in one directory are immediately applied in the other. As a result, organizations that deploy both directories can do so without duplicating administration.

Furthermore, the directory server can automate or eliminate the need to synchronize passwords with other LDAP directories. IBM Security Directory Server offers pass-through authentication. It can validate passwords with another directory, providing the option to store validated passwords for improved performance or to migrate to IBM Security Directory Server.

Optimize implementation and flexibility with integration and an open approach

To help organizations using a variety of IBM software, IBM Security Directory Server easily integrates with IBM middleware, identity management and security products. It functions as the default directory for IBM WebSphere® Application Server, IBM WebSphere Portal, IBM Security Identity Manager, IBM Security Access Manager and AIX.

At the same time, the IBM open approach to directory technology offers a wide array of choice in identity provisioning and on-demand business applications. IBM Security Directory Server avoids proprietary extensions into the directory that "prefer" IBM provisioning applications.



Log in to view your content.

No tags yet

Looking For an Expert?

Use this page to find the people and expertise you need. Perform a quick search by entering a name in the field provided. Click a tag in the tag cloud to display a list of people with that tag. Click "Display full search options" to access additional search fields and perform a more targeted search.

Tip: Click ? to see help on a specific feature or click Help to view all help topics.

Search the Directory

To find a profile, start typing the name of the person you would like to find and the results will display automatically.

IBM Security Directory Server White Pages provides end users with access to personal and organizational information in a customizable format.

Manage identities in the cloud

IBM Security Directory Server eases user and group management in the cloud by supporting System for Cross-domain Identity Management (SCIM). It supports all the necessary create, read, update and delete (CRUD) operations through the Representational State Transfer (REST) application programming interface (API) to simplify user management in cloud-based applications and services.

Offer web-based White Pages to end users

IBM Security Directory Server offers a ready-to-use White Pages application that can be easily customized to feature an interface that fits an organization's brand or look-and-feel requirements. This web-based application can be used to look up phone numbers, email addresses, organizational charts and other personal information within IBM Security Directory Server. Furthermore, end users can maintain personal entries to ease the administrative burden on IT staff. White Pages is based on IBM Connections, a profiles-based application that includes social-networking capabilities.

Take advantage of additional services and integrations

As part of its comprehensive line of directory services offerings, IBM offers professional services that include implementation services and identity provisioning. Additionally, organizations can use IBM Security Directory Integrator to synchronize and exchange identity data in heterogeneous environments across directories, databases, flat files and applications, helping to significantly minimize the cost of integrating and maintaining data silos. It also helps build a single, authoritative, enterprise-level view of identity or generic data using a rich pool of out-of-the-box integration assets.

IBM Security Directory Server at a glance	
Supported operating systems*	• Microsoft Windows Server 2012 Standard and 2008 Standard, Enterprise, Datacenter SP1 and R2 (32- and 64-bit) • AIX v7.1 and v6.1 • Red Hat Enterprise Linux v6 and v5 (32- and 64-bit Intel, AMD, IBM System z , IBM PowerPC and IBM System i) • SUSE Linux Enterprise Server v11 and v10 (32- and 64-bit Intel, AMD, System z, PowerPC and System i) • Oracle Solaris for SPARC v10 and v11

Use enhanced manageability features to help avoid problems

Because IBM Security Directory Server is instrumented for Simple Network Management Protocol (SNMP) monitoring of server status, users can easily incorporate it into their broader efforts to help maximize availability. What's more, the directory server maintains audit, change and error logs that help IT staff quickly detect and prevent potential problems.

Among enhancements that increase usability and help increase productivity, IBM Security Directory Server offers a web-based administration console. Users can perform all data-administration tasks from a remote client.

Enable advanced auditing and reporting

Using out-of-the-box connectivity, IBM Security Directory Server logs can integrate with IBM Security QRadar® SIEM to provide advanced auditing and intelligence. These capabilities help provide deeper user insights and visibility into developing threats, while helping organizations meet compliance requirements. IBM Security Directory Server also enables sample reporting on various objects, groups and users that administrators can either use in the same form or extend capabilities via simple customization.

Why IBM?

IBM Security solutions are trusted by organizations worldwide for identity and access management. The proven technologies enable organizations to protect their most business-critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives.

For more information

To learn more about IBM Security Directory Server, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/directoryserv/

About IBM Security solutions

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.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.

* For detailed system requirements and additional information on each operating system, visit: **ibm.com**/infocenter/prodguid/v1r0/clarity/index.html

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2013

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Please Recycle