



---

Buyer's Checklist for Identity Management

# Key Considerations for Evaluating Identity Management Solutions



# Key Considerations for Evaluating Identity Management Solutions

As a leading Sun Microsystems iForce<sup>SM</sup> partner, Dewpoint is proud to present this useful tool to help you evaluate and select the right solution for your company's critical business and security needs.

If you are currently evaluating identity management solutions, this checklist will help you make the right decisions. By using this checklist, you ensure that your selection is best suited to your business needs and technology environment.

The right identity management solution will provide:

**Seamless Integration:** Integrated and integratable solutions enable business processes, people, and heterogeneous applications to work together seamlessly and securely across traditional business boundaries.

**Secure Control:** Being able to view and control who has access to what resources — regardless of how many users there are or how the user base changes — allows organizations to protect sensitive information. That includes enabling compliance with legislative mandates and regulatory requirements relating to security, privacy, and governance.

**Improved User Experience:** Directory-based identity management can help to ensure that the user's experience of interacting with multiple entities in multiple ways is transparent and uninterrupted. A positive user experience translates to competitive advantage for the entity that provides it.

**Cost Reduction:** The right solutions can help reduce administrative costs by automating manual processes; they can reduce spiraling help desk and other support expenses through capabilities such as automation, self-service, and delegation.

As you evaluate various identity management solutions, compare key architecture components and designs along with features and functions available in the solutions under review.

## Get Started with Dewpoint Today!

Dewpoint has a proven track record of helping companies integrate and manage identities across a variety of platforms. Our solutions reduce time associated with provisioning transactions; decrease cost of password management; boost employee productivity; and, much more. Our IdM consultants can also put their expertise to work to meet your audit and compliance objectives.

Get started today. Call a Dewpoint IdM consultant: 1-888-274-8274.

## Buyer's Checklist for Identity Management

# Key Considerations for Evaluating Identity Management Solutions

As you evaluate various identity management solutions, use this checklist to compare key architecture components and designs along with features and functions available in the solutions under review.

### User Provisioning, Identity Synchronization, and Identity Audit

<b>Automated Account Provisioning</b>	<b>Yes</b>	<b>No</b>
Does the solution create, update, and delete user accounts across the enterprise environment, including Web-based and legacy systems and applications?		
Is the solution Web-based and available to administrators from any Web browser?		
Is the solution designed to support users both inside (employees) and outside (partners, suppliers, contractors) the enterprise?		
Can you easily and quickly find a user (or a group of users) and view their access privileges?		
Does the solution allow you to instantly revoke all of a user's access privileges?		
Does the product leverage existing infrastructure (e-mail, browsers) to facilitate automated approvals for account creation?		
Does the product offer an automated approval mechanism with zero-client footprint?		
Does the solution provide the flexibility to map to your existing business processes? If yes: <ul style="list-style-type: none"><li>• Are serial approval processes supported?</li><li>• Are parallel approval processes supported?</li></ul>		
Does the solution provide automatic approval routing to persons appropriate to system access requested (e.g., system owners) and organizational structure (e.g., managers)?		
Can the solution dynamically determine routing of approvals based on defined organizational information (for example, real-time look up in Active Directory to determine who the user's manager is and route approval to manager)?		
Does the solution allow delegation of approval authority to another approver (or multiple approvers)?		

<b>Automated Account Provisioning</b>	<b>Yes</b>	<b>No</b>
Can the solution automatically escalate a request to an alternative approver if allotted time elapses?		
Can the solution request information from applications or data stores during the approval process?		
Can the product support rule-based routing for approvals?		
Can the solution require automated approvals for deleting or disabling accounts?		
Can the solution require automated approvals for changing account values?		
Does the solution provide the ability to request information from approval participants to define account-specific information during the process?		
Does the product support creating custom approval screens and keeping them compatible in the upgrade process?		
Can the product fully automate the routine identity management processes in your environment?		
Can added accounts for new users in an authoritative source (e.g., HR database, directory) drive automated approvals and account creation?		
Can changes in user status (e.g., job promotion captured in HR system) automatically drive changes in user access privileges?		
Can information in an HR database on employees departing the organization be used to completely and automatically delete all access privileges on the day of departure?		
Can the above processes be fully automated for large groups of users in addition to individuals (e.g., when an acquisition closes or a layoff occurs and a large group of users require automated action)?		
Will the solution detect manual changes made in managed systems and automatically respond?		
When changes are detected, can the solution alert/notify designated personnel of access rights changes made outside the provisioning system to verify if changes are legitimate?		
Once detected changes are approved, will the solution update itself to include those changes?		
Can the solution filter manual changes made on target systems so that only relevant identity changes trigger alerts?		
If a detected account is not legitimate, can the solution automatically suspend the account?		
Can the solution be used to enforce privacy policy?		
Does the solution support role-based access control?		
Does the solution support assignment of users to multiple roles?		
Does the solution support the assignment of users to hierarchical or inherited roles?		
Does the solution provide the ability to specify exclusionary roles that prevent certain roles from being assigned a conflicting role?		
Can the solution assign resource account attribute values with the role?		
Does the solution allow roles to be defined at any time or not at all, rather than requiring role definitions prior to implementation?		
Does the solution enable you to leverage key information systems in your environment as a source of authority on identity information to drive automated provisioning (e.g., detect new employees added to PeopleSoft and automate provisioning based on that change)?		

<b>Automated Account Provisioning</b>	<b>Yes</b>	<b>No</b>
Can the solution assign resource account attribute values with the role?		
Does the solution allow roles to be defined at any time or not at all, rather than requiring role definitions prior to implementation?		
Can the solution assign users to more than one role?		
Can the solution assign users individual access rights in addition to a role?		
Does the solution dynamically and automatically change access rights based on changes in user roles?		
Can the solution generate unique user IDs consistent with corporate policies?		
Does the solution support rule-based access control that allows provisioning rules to be set and enforced on roles, users, organizations, and resources as needed in order to align with business needs?		
Is the solution easy to use for both end users and administrators?		
Is the solution highly scalable to adapt to growth in users, applications, and access methods?		
Does the solution work securely over WANs and across firewalls?		
Does the solution provide an interface to third-party workflow management applications?		
Does the solution allow resource groups (such as a Windows NT group) to be created from the interface?		
Does the product provide directory management capabilities, specifically the ability to create, update, and delete organizational units and directory groups?		
Does the product support pass-through authentication where a user can be validated by a managed user account?		
Does the product support all of the leading database servers and application servers?		
Does the product provide an interface creation tool to customize the user experience?		
<hr/>		
<b>Key Architecture Considerations</b>	<b>Yes</b>	<b>No</b>
Is the solution specifically architected for rapid deployment?		
Does the solution have a proven track record of rapid deployments?		
Does the solution offer agentless connections to managed resources in order to reduce deployment time and simplify operations and maintenance?		
Does the solution leverage an intelligent indexing system to manage user identities and access privileges, leaving account information with the information owner, avoiding the time-consuming effort of building and maintaining another user repository?		
Does the solution provide an automated way to discover and correlate all accounts associated with an individual to speed the account mapping process? If yes, does it provide a way to engage end users in the discovery process for their own accounts?		
Does the vendor offer a wizard-style toolkit to extend coverage of managed platforms to custom and proprietary applications? If yes, is this toolkit provided free of charge?		

<b>Key Architecture Considerations</b>	<b>Yes</b>	<b>No</b>
Does the solution adhere to industry standards for ease of integration with existing systems and future IT investments?		
Is the vendor participating in and leading new provisioning interoperability standards (e.g., SPML)?		

<b>Identity Synchronization Services</b>	<b>Yes</b>	<b>No</b>
Does the product provide a Web-based interface for individuals to view and edit their personal profile information (such as legal name, mailing address, cell phone, and emergency contact)?		
Does the solution provide integration with authoritative systems to detect profile changes and synchronize them where needed (for example, detect title and salary changes in the payroll system and update those attributes in the CRM system and LDAP directory)?		
Does the product provide enterprise-wide identity data synchronization, ensuring that profiles are accurate and consistent?		
Does the solution provide one interface to view all identity profile data? If so, does this require the building of another identity repository?		
Does the product provide a fast scheduling capability to execute time sensitive actions?		
Is the product agentless or does it require installing software on each managed resource?		
Does the product provide an incremental synchronization capability to increase performance?		
Does the product provide data transformation and validation rules during synchronization?		
Does the product support business rules by automatically completing access privilege or profile data changes according to corporate policies?		
Does the product support a large number of connectors to synchronize between many systems?		
Does the product have an attribute mapping interface?		

<b>Identity Audit</b>	<b>Yes</b>	<b>No</b>
Does the product provide object-level security and auditing to track system change configuration?		
Does the solution provide a comprehensive set of predefined reports?		
Can the solution be configured to audit and report any and every provisioning action that occurs (e.g., new accounts created, provisioning requests by approver, account changes, failed administrator access attempts, failed user access attempts, password changes, password resets, accounts disabled, accounts deleted, rejected provisioning requests, etc.)?		
Does the solution provide a comprehensive view into who has access to which resources?		
Does the solution report on who had access to what on a given date?		
Does the solution provide the ability to quickly find and report on a user's (or a group of users) access privileges?		
Can reports be run on demand?		

<b>Identity Audit</b>	<b>Yes</b>	<b>No</b>
Can reports be scheduled to run on a regular basis?		
Does the solution report by administrator (accounts created, accounts modified, accounts deleted, password changes, complete audit history per administrator, administrative capabilities per administrator)?		
Does the solution report by platform or application (users per platform, provisioning history per platform, who performed the provisioning actions on the target platform)?		
Does the solution report on workflow (requests made by user, requests approved by approver, requests denied by approver, requests escalated, delegation of approvals including to whom and for what period of time)?		
Does the solution report on roles (users per role, resources per role, approvers per role, changes to roles)?		
Does the solution report on delegated administration (delegated administrators, what their administrative privileges are, over what user groups and what managed platforms)?		
Does the solution provide a comprehensive audit log of all actions/modifications carried out through the system?		
Does the product easily integrate with corporate reporting tools (e.g., Crystal Reports, Actuate)?		
Can the reports be easily exported into Excel, Word, or databases directly from the user interface?		
Does the solution report by user (audit history per user, accounts/privileges by user, self-service activity by user, role membership)?		
Can the product proactively detect risks such as dormant accounts across all managed platforms? If so, can automated action be taken when certain results are found (e.g., automatically disable dormant accounts, send alert to administrator)?		
Can the solution easily report on account-related security risks in the environment?		
Can the product check for these risks on demand?		
Can the product check for account risks on a regularly scheduled basis?		
Does the product provide performance tracking and performance tools such as provisioning time metrics and tracing?		
Does the product provide a graphical interface for creating and managing provisioning workflows, rules, and interface screens?		

## **Password Management**

<b>Password Management</b>	<b>Yes</b>	<b>No</b>
Does the solution provide password strength enforcement? If yes: <ul style="list-style-type: none"> <li>• Does the solution provide a password exclusion dictionary?</li> <li>• Does the solution provide a password history store to prevent reuse of old passwords?</li> </ul>		
Does the solution allow users to manage their own passwords, including resetting passwords?		
If you provide an automated process for users managing passwords, does the solution include a challenge/response?		
Can policy be set on challenge authentication questions (e.g., how many responses are required based on a user's organization)?		
Does the solution allow end users to synchronize their passwords across multiple accounts?		

<b>Password Management</b>	<b>Yes</b>	<b>No</b>
When users change or synchronize passwords, does the product enforce password strength policy?		
Does the solution include a success/failure notification for password reset and synchronization?		
Does the solution allow end users to request new accounts/access to new services or applications? If so, are required approvals enforced?		
Can users update personal attribute information (address, cell phone, etc.) and have that information automatically propagated to the appropriate resources?		
Can the solution support accessing the Web-based user self-service functions without requiring network log-in?		
Does the solution integrate with interactive voice response (IVR) for password reset functions?		
Can the user view the status of the request from a Web interface? Does the product support a kiosk mode to be configured for users to change passwords from any terminal?		

## Access Management and Federation Services

<b>Access Management</b>	<b>Yes</b>	<b>No</b>
Does the solution include support for open standards for federation (SAML, Liberty) and authentication/authorization (Java Authentication and Authorization Service)?		
Does the product offer support for all required authentication schemes, including passwords, forms-based, UNIX®, X.509 Digital Certificates, RSA SecurID, SafeWord, Windows SPNEGO, Windows NT, RADIUS, SAML, JDBC™, and MSISDN?		
Does the solution implement the open-standard Java Authentication and Authorization Service (JAAS) framework, to allow any JAAS-compliant authentication module to be simply plugged in and to allow customers a standards-based means to easily develop their own?		
Does the solution offer customer choice in protection of an enterprise's applications and information assets through a broad suite of policy control agents as well as a proxy approach?		
Does the product offer only a proxy-only approach where network traffic must be routed through a central, bottlenecked proxy server?		
Does the solution provide policy agents for the enterprise applications/platforms deployed by most customers, such as SAP (Enterprise Portal, Internet Transaction Server, Web Application Server), Lotus Domino, Apache (1.x and 2.x), BEA WebLogic (6.x, 7.x, and 8.x), IBM WebSphere, Microsoft IIS (4.x, 5.x, and 6.x), Oracle (9i, 11i, and 10g), Jrun, and Tomcat?		
Can the product challenge authenticated users (i.e., passwords) to present a stronger credential (i.e., X.509 Certificate) when they attempt to access a more sensitive resource?		
Can the product disable a user account after a configurable number of authentication failure events?		
Does the product support single sign-on across security domains?		
Is the product able to offer true single sign-on in Microsoft Windows environments beginning with the sign-on event at a Windows user's desktop?		
Does the product provide centralized security policy enforcement of user entitlements by leveraging role- and rule-based access control?		



## Directory Services

Directory Services	Yes	No
Is the solution a complete directory service solution?		
Does it provide proxy services for high availability, enhanced security, and client interoperability?		
Does it provide Microsoft Active Directory synchronization?		
Does it provide a Web-based viewer/editor for the data?		

LDAP Directory Services	Yes	No
Does the solution install easily?		
Does the solution allow bulk loading? If so, can it load over 1000 entries per second?		
Does the solution's bulk load ensure data conformance and schema compliance?		
Does the solution support multiple platforms, including the Solaris™ 8 and 9 Operating Systems (SPARC® and x86 Platform Editions), HP-UX, AIX, Red Hat Linux, and Windows 2000/2003?		
Does the solution support DSML? Natively?		
Does the solution provide a complete command line interface (CLI)?		
Does the solution provide the ability to change the configuration using a CLI or GUI?		
Does the solution provide the ability to make most changes to the service while online?		
Does the solution allow you to backup the data while online?		
Does the solution allow you to re-create indexes while online?		
Does the solution allow you to reinitialize a replica while online?		
Does the solution allow you to change the schema while online?		
Does the schema replicate automatically?		
Does the solution allow online access control changes?		
Does the solution include attribute encryption to protect sensitive data?		
Does the solution include fractional replication?		
Does the solution support an unlimited number of password policies?		
Does the solution provide both roles and class of service (dynamic attribute assignment)?		
Does the solution support access control determination dynamically based on the bind DN and target entries?		
Does the solution provide high availability for write operations?		
Does the solution have extensive documentation?		
Is it easy to read and does it cover all capabilities?		
Does it include detailed examples of deployment configurations?		
Does it include online help?		
Does the product include localized versions of the administration console?		

<b>LDAP Directory Services</b>	<b>Yes</b>	<b>No</b>
Does the solution include utilities for tuning and performance testing?		
Does the solution include complete application programming interfaces (APIs) and software development kits (SDKs) for creating applications?		
Does the solution include sample applications?		
Does the solution include an out-of-the-box white pages application?		
Is the solution supported by most major system integrators?		
Is the solution supported by most ISVs in the identity management market?		
Does the solution provide a plug-in architecture with a fully documented SDK to extend server capabilities?		
Does the solution provide fast initialization through binary copy of another replica?		
Does the solution provide virtual attribute capabilities?		
Does the solution provide dynamic access control?		
Does the solution support vertical scalability?		
Does the solution have performance that scales beyond four CPUs?		
Does the solution support 64-bit hardware to support large cache?		
Does the solution support horizontal scalability?		
Can it support tens of thousands of search requests to the same data set?		

<b>Directory Proxy Services</b>	<b>Yes</b>	<b>No</b>
Does the solution provide transparent server failover and failback?		
Does it automatically reallocate traffic load?		
Does the solution provide automatic referral following?		
Does the solution provide detection of denial-of-service attacks?		
Does the solution detect and prevent malformed LDAP requests?		
Does the solution allow you to limit the number of connections?		
Does the solution allow you to rate limit connections?		
Does the solution allow you to limit the number of simultaneous operations per connection?		
Does the solution allow you to time-out inactive sessions?		
Does the solution allow you to configure SSL from clients?		
Does the solution allow you to configure SSL to LDAP servers?		
Does the solution allow you to create access control groups based on IP address or authentication?		
Does the solution support dynamic query and response filtering?		
Does the solution support disallowing specific query filters?		
Does the solution support dynamic schema mapping?		

<b>Directory Proxy Services</b>	<b>Yes</b>	<b>No</b>
Does the solution allow you to hide parts of the directory information tree (DIT)?		
Does the solution allow you to hide attributes?		
Does the solution allow you to distribute a flat name space across multiple sets of servers?		
Does the solution allow configuration changes to be made using the LDAP protocol?		
Does the solution support distributed servers for the proxy layer?		
Does the solution support centralized configuration for distribution?		

<b>Active Directory Synchronization</b>	<b>Yes</b>	<b>No</b>
Does the solution do synchronization with Microsoft Active Directory (2000 and 2003)?		
Does the solution provide a nonintrusive, zero-install footprint on Active Directory? If so, can users still change their password using Ctrl-Alt-Delete?		
Does the solution do bidirectional synchronization?		
Does the solution do bidirectional synchronization for Passwords?		
Does the solution do bidirectional synchronization for entry creation?		
Does the solution do bidirectional synchronization for entry deletion?		
Does the solution do bidirectional synchronization for account activation/inactivation?		
Does the solution support existing entry populations?		
Does the solution support existing entry populations, including existing password synchronization, without forcing users to change the password?		
Does the solution support custom schema in both Active Directory and Directory Server?		
Does the solution support mapping between hierarchical and flat name spaces?		
Can the solution target subsets of users in either Active Directory or Directory Server?		
Is the filtering capability fine-grained and configurable?		
Does the solution support aux object classes?		
Does the solution allow default attribute values to be specified?		
Can the default values be parameterized?		
Can the solution be configured centrally, but deployed in a distributed fashion?		
Does the solution support centralized logging of all synchronization activity?		
Does the solution support persistence of password changes even in the case of network failure?		
Does the solution provide for failover of Active Directory?		
Is the solution highly secure with SSL connections between all elements?		

<b>Web-based Viewer/Editor</b>	<b>Yes</b>	<b>No</b>
Can access be done over and optionally limited to SSL?		
Can forms for editing objects be created and modified without writing code?		
Can the interface be easily and completely branded?		
Is the product J2EE technology-based and does it support all major Web containers?		
Does the product include an SDK to extend the functionality beyond what is provided out of the box?		

© 2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 USA  
All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California.

Sun, Sun Microsystems, the Sun logo, Java, JDBC, J2EE, Solaris, iForce and The Network is the Computer are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries.

Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS HELD TO BE LEGALLY INVALID.

## **Dewpoint**

75 Executive Drive

Suite E

Carmel, IN 46032

USA

Phone 1-317-218-1110 or 1-888-274-8274

[www.dewpoint.com](http://www.dewpoint.com).

Dewpoint is a leading Sun Microsystems iForce™ Partner