Abstract

Web technologies have revolutionized the delivery of information and services. Providing business functions, such as customer service, sales, and purchasing, via the Web is a prerequisite to competitiveness. Customers, partners, and business constituents need real-time access to corporate information. They need to develop new capabilities to respond to whatever the market throws at them, becoming more efficient and cost-effective and gaining advantages over their competitors. At the same time, compliance has assumed a prominent position in terms of the very real concerns that business managers are faced with. One of the primary signs that compliance concerns are on the rise is the Sarbanes-Oxley Act (sometimes referred to as SOX). This act forces the issue with many companies to maintain and certify the validity of their records and disclosures of pertinent information.

To automate core business processes, a company should give its users, who are as likely to be customers or suppliers as employees, access to corporate information and applications through a comprehensive extranet. Unfortunately, Web applications and individual Web security solution packages provide, at best, piecemeal security and access control. Organizations need a unified approach for making authorization decisions, instead of relying on a custom access control service for each server, application, or environment. And to address e-business on demand, those same organizations need an adaptable solution that can both scale up, as demand requires and meet the ever-changing business and user conditions that can instantaneously change the outcome of a request for data or function.

By providing highly available, directory-based, and centralized authorization services, IBM Tivoli Access Manager for e-business enables you to better manage and secure your business-critical distributed information, while ensuring you can meet the time-to-market, compliance, flexibility and scalability requirements that today's on demand world requires.

Introduction

Corporate use of Web technology has exploded in recent years. While most organizations used their first Web applications to offer generally available information over the public Internet, intranets, and extranets, supporting key business functions via the Web has become the norm for many competitive businesses today. As a result, more corporate information and
application functions are being made available over the Web. Successfully managing and securing corporate Web resources have become more complex challenges as Web use has matured. Organizations that need their employees to access their intranets remotely via the Internet, or that want to automate their supply chains through extranets, should consider the security and management concerns that are unique to these situations.

The nature of security threats and the way information is managed have changed. As organizations expand their intranets, moving from static content to include self-service applications and enable electronic business value chains, more sensitive information is made accessible via the Web. For example, providing access to account information for customers and business partners and forming extranets to automate the supply chain are strategies that require selective access to sensitive information via the corporate Web. This expansion of Web usage has changed what it means to secure the Web space. An organization should control not only who accesses its corporate Web, but also, which resources each individual user can access. To reap the benefits of a sophisticated intranet or extranet, an organization should control access to all information available through the Web, allowing users to access everything they need, but nothing more.

Clearly, a top priority is “keeping the bad guys out”. The ability to provide ubiquitous access to information means that corporate intranets can leave an organization vulnerable to internal attacks if they are not adequately secured. The 2004 CSI/FBI Survey reports that 58% of respondents answered in the affirmative when asked about security incidents overall, from both internal and external sources . . . a 2% increase from the previous year.

To take advantage of the Internet, organizations are providing Web-based access to confidential information. With these configurations, internal and external users with varying needs and permissions should be able to access different resources maintained in the corporate intranet-and users should be able to access only information for which they are authorized. Adding to the complexity of the problem, few organizations have the luxury of building their information systems from scratch. Most companies need tools that can blend new technology with their existing systems to provide security to all resources and applications accessed through the Web.

There are several key requirements that should be met in order to manage information securely on a corporate intranet. First, the identity of an individual wishing to access the intranet should be authenticated. Authentication is the process of verifying that a requester has been issued a unique identifier and knows the secret (for example, a password or PIN) that is associated with that identifier.

This process is complicated when employees or business partners access information from multiple computers and, often, from remote locations over the Internet. Users should be able to authenticate from a Web browser or a wireless device (cell phone or PDA), with no client software requirements. In addition, there are often hundreds of Web servers in a large enterprise, and users need access privileges for each server they access. This can lead to many problems: users must remember passwords for many servers, significant help-desk time needs to be devoted to answering password calls, administrators need to manage the access controls for each individual server, certifying the validity of information disclosure, and many separate entries must be added or removed when a user's access privileges change or when employees join or leave the company. As shown in Figure 1 on page 3, Tivoli offers a security solution that:

- Lets the organization manage access controls for all of these servers centrally.
- Presents users with a single sign-on to the Web space.
- Greatly simplifies security management.
- Offers centralized auditing, enabling certification of proper information disclosure.
Tivoli Access Manager for e-business provides a unified set of security services. Among the supported security services are authentication services (supported by a user registry), policy-based authorization services, allowing access decisions to be based on a clear policy, and audit services, to enable you to show records of disclosures of information. These services are in line with relevant standards. In particular, Tivoli Access Manager for e-business's authorization services implement the decider-enforcer model prescribed by ISO 10181-3.

In a transaction controlled by Tivoli Access Manager for e-business, the first step is authentication. Once a user's identity has been authenticated, their access privileges are determined. An authenticated user does not necessarily have any permissions to access resources. An effective, policy-based approach to determining who can access what resource in what way involves two steps:

- Security policies should be defined to explicitly decide access rights to Web resources.
- An access control enforcement function must establish whether requests for specific information should be granted or denied, based on pre-established policy.

Administration is complicated if access controls must be configured at each Web server. Furthermore, it is difficult to construct a comprehensive picture of a user's privileges in the Web space if an administrator must consult each Web server's configuration information. A centralized authorization approach greatly simplifies administration.

Additionally, a system needs to audit all attempts to access corporate resources to determine if the system is secure. In addition to being a key element of any compliance strategy, this auditing can also facilitate management decisions (such as level and frequency of intrusion detection testing) by allowing analysis of use patterns.

Another important consideration for large businesses is delegating the management of security and privileges for certain information resources to either the individual or group responsible for them. A security system should facilitate secure delegation of permissions.

An important concern with any security management solution, along with how effectively it provides secure transmission, authentication, access control, and auditing, is how easy it is to implement, administer and automate. For any security solution to be truly effective, it should integrate easily with the organization's existing infrastructure, and the security features must be easy to administer. Many customers find it essential that toolkits and APIs be available, to automate various aspects of the security solution, and to tailor it to unique customer needs. Any complexities in security management increase the possibility of human errors.
Finally, keep in mind that Identities pervade every aspect of e-business, and as a result, accounts are issued for access to many different systems for many different purposes. Some of these systems may reside within a company, and others may be applications hosted by a service provider that a company has a partnership with as part of a federation. Managing identities and account data in such federated implementations introduces new business compliance issues and security exposures. Working together with Tivoli Federated Identity Manager, Tivoli Access Manager for e-business helps address these issues and exposures.

This paper will discuss these management and security issues in greater detail and will explain how Tivoli Access Manager for e-business answers these concerns. The paper has two main sections. The first, "Integrated Identity Management", describes Tivoli Access Manager's capabilities, and relates them to customer requirements. The second "Customer Value" describes the value of Tivoli Access Manager for e-business in administrator, end user and applications developer terms.

## Integrated identity access management

Tivoli Access Manager for e-business is the access component of Tivoli's identity management solutions. Tivoli Identity Management solutions can help you get users, systems and applications online and productive fast, reduce costs and maximize return on investment. As shown in Figure 2 on page 5, Tivoli Identity Management provides:

- Identity lifecycle management (user self-care, enrollment and provisioning).
- Identity control (access and privacy control, single sign-on and auditing).
- Identity foundation (directory, metadirectory and other foundation technologies) to effectively manage internal users as well as an increasing number of customers and partners through the Internet.
Identity federation (sharing user authentication and attribute information among trusted Web services applications) is also part of this blueprint; we will cover identity federation as part of a later section called "Web Services Security".

Note that IBM's Identity Blueprint is fulfilled by robust security and directory solutions, in use at many customer locations today. Tivoli Access Manager for e-business, the focus of this paper, addresses Identity Control.

Tivoli Access Manager for e-business is focused on providing robust, policy-based security to a corporate Web environment. This means several things. Authentication of users, control of access privileges, auditing, single sign-on, high availability and logging are all essential elements of any security management solution. Further on, we will explain how the control of access privileges is expansive, with Tivoli Access Manager for e-business's proxy (WebSEAL) or the its Plug-In for Web Servers component able to enforce access control to Web servers and with advanced Java-based and .NET-based capabilities to manage access control at the application level. The following sections cover these topics in more detail.
**Policy-based access control**

Tivoli Access Manager for e-business allows you to define a comprehensive policy and administer security based on that policy-giving your employees, partners, suppliers and customers specific access based on each user's responsibilities. You can group users and assign permissions to groups, simplifying administration of access control across multiple applications and resources. There is support for dynamic roles, dynamic rules, dynamic business entitlements and authorization decisions based on external data for applications that require it.

With a Web-based tool called Web Portal Manager, administrators can manage users, groups, permissions, and policies. Web Portal Manager extends beyond delegated user management to also deliver delegated security administration.

Multiple levels of delegated administration are possible, with great flexibility in capabilities assigned to lower-level administrators. This allows banks or insurance companies, for example, to delegate certain administration responsibilities to their branch office personnel, as desired. The SSL-enabled management application program interfaces (APIs) used by Web Portal Manager are available if you need to integrate or build your own customer-care management applications. These include full support for Java, C, C++ and C#.

Web Portal Manager (WPM) enables administration over a broad range of target resources, including resources protected by a scalable proxy (Tivoli Access Manager for e-business's WebSEAL component), resources protected by Tivoli Access Manager for e-business Web Server Plug-Ins, and J2EE resources, and custom applications that have been factored into the secure environment. Using other members of the Tivoli Access Manager family-Tivoli Access Manager for Operating Systems, for protection of UNIX and Linux resources and/or Tivoli Access Manager for Business Integration, for protection of WebSphere MQ messages-expands the resources managed by the WPM administrator. All of these resources are represented in a single Protected Object Space that a single administrator or a coordinated team of delegated administrators can manage. Figure 3 on page 7 shows how Tivoli Access Manager family's single policy can secure many different resources, through multiple enforcement points.
Architectural choices

When an administrator defines a security policy, the policy becomes effective when it is enforced, and that enforcement often needs to take place at various points in an operational environment. Earlier, we mentioned that two key enforcement points that Tivoli Access Manager for e-business provides are a Web security proxy and a Web server security plug-in. Here, we describe these in more detail.

Tivoli Access Manager for e-business includes a security proxy component called WebSEAL. WebSEAL enforces access to your Web servers-regardless of their platforms. WebSEAL manages the Web space centrally, linking all Web servers into one logical Web space. Tivoli Access Manager for e-business also offers Web Server Plug-Ins, which largely cover WebSEAL functionality, but are implemented as a Web Server security plug-in rather than a security proxy. In this paper, we will primarily describe Web security as WebSEAL accomplishes it. But keep in mind that if a plug-in approach is desired, that component is included as well.

Tivoli Access Manager for e-business's Plug-In for Web Servers enables easy integration for securing Web servers. This approach, which does not require placing a proxy in the DMZ, instead places a piece of code on each Web server that is to be secured. This allows for easy deployment of Tivoli Access Manager for e-business in those environments where existing architectures do not easily allow for the installation of a reverse proxy for business or technical reasons.

The Access Manager for e-business Plug-in for Web Servers provides these benefits:

- Allows use of preferred Web server in DMZ
- Eliminates the need for changes to edge network topology
- Provides many of the features provided by WebSEAL

For optimum security, the Tivoli Access Manager for e-business Plug-in for Web Servers should only be used in configurations that limit security exposures. One example is a configuration where the Web server is only hosting the presentation tier of J2EE applications and where the business logic executes on an application server in the secure network.

One of the main reasons for a focus on the WebSEAL, proxy-based approach is the fact that it can be used to enforce defense in depth protection. Defense in depth involves layering access enforcement points, and separating an untrusted requester's network from a secure network with some sort of buffer network (often referred to as a demilitarized zone, or DMZ). Figure 4 on page 8 shows WebSEAL running in a DMZ, and checking incoming requests to be sure that only authenticated and authorized requesters are allowed to take their desired action on target intranet resources.

![Figure 4](image)

**Figure 4  WebSEAL typically configured in a DMZ**

Such a configuration offers high levels of security, with configuration options that can dictate that only certificate-based, mutually authenticated traffic passes through the inner firewall. Even further security can be provided by storing private keys on tamper-resistant adapter cards—a feature available for those customers who feel they need the extra security that those cards afford.

Defense-in-depth architecture limits the externally facing Web servers to the hardened, battle-tested, streamlined and relatively few WebSEAL servers that are deployed. (In contrast to tacking security onto a Web/application server with a plug-in and authenticating incoming requests right at the Web server.) With WebSEAL, only authenticated and authorized requests get to the target Web servers, whose actual structure is shielded from the users. So even from the standpoint of virus attacks, the ability to harden and maintain the host that runs WebSEAL is far more effective than directly running your security on tens or hundreds of Web/application servers. Tivoli Access Manager for e-business is a mature product that undergoes rigorous in-house testing, according to IBM testing standards, and which undergoes "ethical hacks" by experts hired by customers to test every exploit they can think of.

Finally, keep in mind that it is good practice to deploy good risk management techniques/technologies (such as Tivoli Risk Manager), with a particular focus on the DMZ, to be sure that in the event of an attack, a quick and effective response is possible.
**Authentication**

Tivoli Access Manager for e-business provides a set of default authentication mechanisms-in the form of built-in shared libraries-to support login to Tivoli Access Manager via usernames and passwords, client-side certificates, RSA SecurID tokens, or trusted user information contained in the HTTP header. For authentication to succeed, these users must be members of the Tivoli Access Manager for e-business user registry.

For special custom authentication requirements, Tivoli Access Manager for e-business supports the ability to implement new authentication schemes using a C shared library or a Web application. This provides high levels of flexibility for how the authentication scheme operates (including support for multi-phased interaction with the user at the browser) as well as how the authentication data is collected from the client.

When users are authenticated, Tivoli Access Manager for e-business grants authorization credentials that include an indication of the groups to which the users belong.

**Authorization**

Managing access according to a unified, sound security policy is key to enabling Web-based e-commerce. When a user's identity is determined, the most important question becomes what can this user do and see? After a user is authenticated, Tivoli Access Manager for e-business allows users to access only information for which they are authorized. The administrative graphical user interface-Web Portal Manager-presents a logical Web space for the association of access control information with resources. This namespace is discussed in more detail in “The Administrator” on page 24 of this paper. Tivoli Access Manager for e-business maintains authorization policy in a central repository for administration purposes, yet meets and exceeds typical high availability and performance requirements by providing secure replication of the policy out to local enforcement points. The repository lists the Policy Templates and their attachment points-providing enough information to associate policy with each resource, and yet staying “lean” enough to foster high performance. The ability to replicate policy to local enforcement points is key. As shown in Figure 5 on page 10, there are a number of possible local enforcement points, which can be efficiently making policy-based enforcement decisions, even though the Policy Server might be down.
There are three types of authorization policy: Access Control Lists, Protected Object Policies, and authorization rules. Figure 6 on page 11 shows the role these play in Tivoli Access Manager for e-business authorization decision processing.
Access Control Lists (ACL) defines who has access to an object, and what operations can be performed on the object. Each ACL policy has a unique name and can be applied to multiple objects within a domain. An ACL policy consists of one or more entries describing:

- The names of users and groups whose access to the object is explicitly controlled.
- The specific operations permitted to each user, group, or role.
- The specific operations permitted to the special any-other and unauthenticated user categories.

A key design point regarding ACLs is the desirability to define permitted operations based on groups, rather than on individual users. Well-defined groups can greatly ease the addition of new users and the accommodation of changes to users' roles.

Where ACLs are focused on permissions for users or groups, Protected Object Policies (POPs) are focused on resources. They prescribe additional characteristics that apply globally to the resource in question. Examples of Protected Object Policies or POPs are:

- Auditing characteristics
- Restrictions on access according to time-of-day and day-of-week
- Forcing re-authentication for each access to a particularly sensitive resource, if that's desired

Finally, authorization rules can be defined that make real time, dynamic, access decisions based on information from external sources (in addition to information from the user credential and the object/action requested). These logic rules are “attached” to an object in the Tivoli Access Manager for e-business object space. Each time a user requests access to the object the rule must be evaluated and access is only permitted if the rule returns TRUE.

Authorization rules are evaluated at run time and are held external to the application allowing you to change access-influencing policy parameters without having to rewrite and recompile applications. This feature can dramatically improve both how quickly your applications are deployed and how quickly they adapt. There is great flexibility regarding the authorization rules that can be written and regarding the source of the data used in evaluating authorization rules. A simple example can involve the decision being based on a check of a current credit limit and a more complex example might involve querying fields in a database, to see the latest terms and conditions in a contract with a customer.
Authorization rules greatly expand the possibilities for translating business rules into Tivoli Access Manager authorization policy. And with authorization rules, the number of groups and ACLs your authorization scheme involves can be greatly reduced.

The Tivoli Access Manager for e-business model allows authorization policy information to be maintained centrally—not passed to the user desktop.

Tivoli Access Manager for e-business provides access policy inheritance and authorization by group membership. Its Authorization Services can be replicated for high availability. Availability will be discussed in more detail in “Load balancing, scalability and high availability” on page 18.

Tivoli Access Manager for e-business represents resources to be protected using a virtual representation called the object space or the protected object space. An object space consists of resource objects and container objects. Resource objects are the logical representation of resources to be protected. Container objects allow you to group resource objects and other container objects hierarchically into logical groups or regions. Grouping similar objects together makes it easier for you to administer a consistent security policy. The Tivoli Access Manager for e-business administrator applies an inheritance scheme to all resources. Unless a Policy Template is set explicitly for a resource, it automatically inherits the Policy Template of the object immediately above it in the tree. This means that Policy Templates need to be applied only where access policy changes. Figure 7 on page 12 shows an example of this structure.

![Figure 7  Policy template inheritance](image)

In this example, the general corporate security policy is set at the top of the tree. This limits intranet access to employees only. Below this, the “sales group” has established its own authorization policy for its departmental sub-tree, and the ytd.html (“year to date”) information is set explicitly to be accessed only by members of the group “sales - vp.” All information that does not have an explicit ACL inherits the next-highest-specified Policy Template in the tree. In the case of sales information, all information except “year to date” inherits the ACL set at the “sales/” level; the rest of the information in the example inherits the ACL set at the Web server.

Inheritance eliminates the need to explicitly define a policy template for each individual object, reducing the memory requirements for storing authorization policies, easing its administrative burden and enhancing performance by minimizing the size of the policy database. In the figure, each of the objects represented by an oval has inherited policy from an object higher in tree. For example, hr.html inherits the policy from the top object in the tree, and sales.html inherits the policy from the “Sales/” object.
Applications can use the Authorization API, or aznAPI, to integrate with Tivoli Access Manager for e-business. This API was standardized by The Open Group, an international vendor- and technology-neutral consortium dedicated to technology interoperability. This API allows third-party or custom applications to implement authorization decisions in line with the overall Tivoli Access Manager for e-business model. Tivoli Access Manager for e-business maintains the trust required to provide security at any level of a multi-tiered application, providing the appropriate credentials at all levels.

WebSEAL allows an administrator to set access privileges for dynamically generated Web content using the same policies that govern static resources. This lets an organization secure access to databases and other back-end applications that are accessed through a Web interface.

Logging and auditing

The ability to log and audit all access attempts is essential to secure the corporate Web. Monitoring access attempts by all users lets administrators detect security risks. Tivoli Access Manager for e-business centrally logs all access attempts using a standardized format. Audit logs contain data about system activities that affect the secure operation of Access Manager for e-business' authorization process. The data is comprised of audit records of authentication and authorization events that can include successful and unsuccessful access to resources, password changes, and administrative or management events.

Tivoli Access Manager for e-business can produce audit records for any defined policy (password variables, account lockout, inappropriate access, and so on). Whenever a policy is violated (such as exceeding the maximum login failures threshold), an audit record is generated.

Each process is configured to specify exactly which audit events are to be captured. These parameters include settings for authentication events, authorization events, management commands, and HTTP request handling, as well as defining the location and name of each process' audit log file. Audit log files are monitored for such occurrences as growth beyond threshold settings, rollover to a new file, and so on. Support for standard HTTP logging allows you to see which IP addresses are submitting which types of requests.

Tivoli Access Manager for e-business writes audit records in an XML-like format that allows easy parsing for extracting required information. An information-gathering tool allows secure, centralized collection and reporting of audit, log, statistics and other information across the extended enterprise. Logs can be securely passed to Tivoli Enterprise Data Warehouse or any of a number of third-party database systems for analysis and reporting.

Single sign-on

As shown in Figure 8 on page 14, Tivoli Access Manager for e-business's single sign-on support is multi-faceted. We describe each of these facets in the order shown in the figure.
Client Web App SSO
The first facet of this support that might come to mind is "Client-Web App SSO", where a client signs in once and is given access to multiple Web applications without the user needing to reauthenticate. If done well, this capability will result in higher user productivity and lower help desk costs. Tivoli Access Manager for e-business offers robust client Web Application SSO support, covering Web trust configurations (using, for example, a Trust Association Interceptor implementation), basic authentication SSO, forms-based SSO, Lightweight Third-Party Authentication (LTPA) SSO, and passing of user information in the HTTP header.

Portal/Back-End SSO
Tivoli Access Manager for e-business's SSO extends to back-end applications/portals. User information can be passed to an application server or portal server, and that information can be used to build a credential appropriate to the back-end application environment. Tivoli Access Manager for e-business includes special support for WebSphere Portal credential vault capability, extending SSO support to the portal's back-end applications. Designed to work in concert, Tivoli Access Manager for e-business, WebSphere, RACF and Java Connection Architecture (JCA) capability can enable user information to be mapped and used in each environment that is involved in a user's request for mainframe data, typically referred to as a 3-tier transaction.

Cross-Domain SSO
And finally, on the left-hand side of the figure, there is the area that is growing in significance, largely spurred by the popularity of Desktop SSO and the Web Services revolution, and that's cross-domain SSO. TAMeb is able to handle each of these 3 types of cross-domain SSO scenarios:

- Desktop SSO
  Here, signing on to the Windows Operating System is the single sign-on that will enable access to any subsequent and authorized application access under the control of Tivoli Access Manager for e-business.
Sign-on from one Tivoli Access Manager domain to another
This can be enabled through Cross-Domain SSO or eCommunity SSO.

Sign-on from another source
Here, Tivoli Access Manager for e-business's toolkit enables accommodation of SAML assertions. Generally, Tivoli Access Manager for e-business has an extensible SSO interface. And Tivoli Access Manager for e-business is well integrated with Tivoli Federated Identity Manager, to address Cross-Domain SSO and Web Services security with enterprise management.

Logical Web namespace
Management of information can be simplified if the company organizes corporate Web resources in a logical Web namespace-in which content is accessed through an Internet address, or URL, that reflects a logical structure chosen by the organization. This allows information to be organized logically, such as by department or on a project basis, rather than by the physical location of the resource.

To create a logical Web space, WebSEAL is positioned in front of an existing Web server and its corporate Web resource tree. WebSEAL associates a user-defined logical name (as part of the logical URL) to refer to the Web server content. When a user requests a resource (using the logical URL), the server intercepts the request and uses what are called junctions to match the logical name with the physical address of the Web server. In effect, Tivoli Access Manager for e-business translates the logical URL, locates the information, and returns it to the user-who remains unaware of the physical location of the information.

Readers familiar with Network File System (NFS) and its concept of mounting remote directories will find that the concepts behind WebSEAL junctioning are very similar. No changes happen to the directories in the NFS case or to the back-end Web content in the WebSEAL case. Nor are there any changes to the physical boxes that hold the directories or Web pages. Just like NFS can set up a logical relationship where it seems as if remote directories have become part of a local file system, so too does WebSEAL configure the Web spaces on multiple attached Web Servers to seem as if they were all a single, hierarchical and unified Web space on the WebSEAL server.

This structure allows access policy to be set at WebSEAL, rather than individually at the physical servers on which the information resides. Junctions enable support for any back-end Web server, including Microsoft® IIS, Domino, Netscape, and Apache.

In addition to transparently supporting any standard Web server, the Tivoli Access Manager for e-business logical Web space can also include resources accessed by Web-enabled applications, such as SAP Enterprise Portal, SAP Internet Transaction Server, Siebel 2000 and Siebel 7. This means Tivoli Access Manager for e-business controls access to information accessed from legacy databases and other back-end applications in exactly the same manner as static Web resources. Figure 9 on page 16 shows how use of junctions facilitates one type of logical addressing scheme.
Figure 9  Junctions in the Web namespace

In this example, the company has developed an addressing scheme in which all the information for one department can be found in a single location-marketing—even though it is maintained on multiple machines. This makes it easier for a user to access information and makes the Web easier to administer. Junctions allow an organization to create whatever type of address structure will be most useful for it. For example, information can be grouped on a project basis or by subject matter, rather than by department. Also, the groupings can be easily adjusted as the needs of the organization change. Using Tivoli Access Manager for e-business, an organization can reorganize its Web namespace without moving Web-based information between servers.

The logical addressing scheme also makes it easier to make changes to the network. If information must be moved between servers, or a new server added, the Web administrator can make the change and then adjust the junctions. Users never know a change took place—unless they realize it as greater speed and efficiency.

WebSEAL's logical Web namespace is part of the overall Tivoli Access Manager for e-business Protected Object Space. The Protected Object Space also includes resources protected by the Tivoli Access Manager for e-business Plug-In for Web Servers. Where WebSEAL uses junctions to define security policy, the Tivoli Access Manager for e-business Plug-Ins for Web Servers define security policy in terms of virtual hosts. The virtual host defines the mapping of URIs to Tivoli Access Manager for e-business Protected Object Space names.

As discussed in the Security Policy Management section of this paper, the use of a logical Web namespace also simplifies security administration as WebSEAL and the Web Server Plug-Ins can set access policy against the logical Web space instead of at each server.

### Finer-grained authorization

As part of the definition of the junction between WebSEAL and a target URL (or the virtual host definition for the Tivoli Access Manager for e-business Plug-In for Web Servers), you can designate what should be inserted into an HTTP header, to pass along the specific client's identity and group membership information to a target application. The Tivoli Access Manager for e-business-specific HTTP header information enables applications on junctioned third-party servers to perform user-specific actions based on the user's Tivoli Access Manager for e-business identity.

In order to further drive application development efficiencies and thereby minimize time-to-market for the application, there are other configuration options that can be specified. Two examples are
- **Tag-value information**, which can be stored in an LDAP directory and sent along to the application that needs the information. Typically, this would be some additional, useful information about the user, such as their email address or a credit limit.

- **Entitlement information**, wherein the request designates a user, a permission and a subset of the protected object namespace, and what's returned is the list of objects that the user has that permission for.

Tivoli Access Manager for e-business offers two means by which applications can directly make authentication and authorization requests:

- Using PDPermission extensions, Java applications can use Tivoli Access Manager for e-business as the authorization backend for Java 2 permission checks

- Tivoli Access Manager for e-business also implements The Open Group's Authorization API (aznAPI)

Tivoli Access Manager for e-business includes support for WebSphere Application Server or BEA WebLogic Server container-based authorization checks to be done using Tivoli Access Manager for e-business's services. Container-based authorization is yet another example of separating application business logic (the servlet, or EJB or JSP) from security, which is handled by the container that the application runs in. Java applications built this way can use standards-based calls for fine-grained (method level) security that is in line with Tivoli Access Manager for e-business's unified approach to policy-based security management. Initial development of the application is quicker and updating security rules doesn't require changes to the application. (Some authorization products require complicated and questionable practices such as decompiling/modifying/ recompiling Java files in order to secure them.) Businesses with developers familiar with Java programming do not need any special training to take advantage of Tivoli Access Manager for e-business's Java security support.

Tivoli Access Manager for e-business also addresses the other significant programming paradigm-the .NET world. Similar to the aforementioned Java-based capabilities, the AM for .NET component addresses role-based, method-level security for two approaches:

- Programmatic security, via calls to our administrative and authorization APIs using C#.

- Declarative security, using ASP .NET containers

**Dynamic URLs**

Dynamic URLs augment the standard URL address with information about a desired operation and its parameter values. The query string portion of the URL provides operations, parameters, and values to the Web application interface. An example is shown in Figure 10 on page 17.
Because dynamic URLs exist only temporarily, it is not possible to have entries for them in a pre-configured authorization policy database. Tivoli Access Manager for e-business solves this problem by providing a mechanism where many dynamic URLs can be mapped to a single static protected object. Using pattern-matching characters, this mapping can be made general, or specific, as desired.

**Load balancing, scalability and high availability**

Tivoli Access Manager for e-business includes a number of features that help ensure scalable, high performing, and highly available implementations. Figure 11 on page 18 depicts how junctions can be used to mount multiple Web servers with replicated contents at the same point in the logical Web space. When this is done, WebSEAL performs intelligent load balancing across the replicated servers for improved performance and fault recovery. This allows policy-based access control of Web resources to be available at all times, even in the event of system maintenance or failure. Using junctions, Web server capacity can be added in a linear fashion as demand increases on the corporate Web infrastructure.

The figure also shows that WebSEAL can be replicated and a front-end load balancer, such as the Network Dispatcher component of the WebSphere Edge Server, Coyote Point's Equalizer, or F5 Network's BIG-IP, can balance the traffic to WebSEAL.

Although not shown in the figure, Tivoli Access Manager for e-business also offers load balancing and fail-over of replicated directory servers. Further performance gains can be realized by taking advantage of Access Manager for e-business's support for SSL accelerator cards, as well as the ability to offload authentication and authorization services to separate servers.

Proof of Tivoli Access Manager for e-business's scalability and performance capabilities comes from the testing in labs that has shown it continues to perform well, even in environments involving 30 million users. In live customer production environments, Tivoli Access Manager for e-business is being used in a number of implementations involving 1 million users or more.

Web Server plug-ins work well with load balancers in front of them. This allows such capabilities as:

- Distributing Web traffic to multiple geographically dispersed sites on a least-busy basis
- Rolling over to alternate servers in the event of failures
Use of customer-defined rules for determining load and routing

**Access Manager as part of an enterprise security solution**

Tivoli Access Manager for e-business fits in well with Tivoli enterprise solutions such as Identity Manager and Risk Manager. End-user enrollment for Access Manager for e-business can be provided through Identity Manager. Tivoli Identity Manager is a Web-based solution that provides a unifying interface for all aspects related to end-users and their interactions with a business. The Web interface accessed by a user reflects that person's level of responsibility by displaying only the roles and tasks available to that user onscreen.

Identity Manager provides self-care and workflow capabilities to a wide range of enterprise targets, including Tivoli Access Manager for e-business. Self-care enables users to update password policies without involving an administrator. It is a timesaving feature that relieves higher-level administrators of frequent tasks. These self-care capabilities are highly customizable. Workflow gives businesses the flexibility to incorporate their own business process policies to enforce the degree to which end-users' requests are routed for approval.

Tivoli Access Manager for e-business alerts, events, and audit information can be sent to:
- IBM Tivoli Risk Manager, which can include Access Manager for e-business information in the vast amount of information it analyzes to help administrators determine whether there is an attack underway, and
- Tivoli Enterprise Data Warehouse, which can produce reports and provide decision-support capability.

Figure 12 on page 19 shows Tivoli Access Manager for e-business working with Tivoli Identity Manager to provide end-to-end Identity Management.
Enterprises involved in incorporating, monitoring and enforcing privacy policy into their business processes can benefit from the fact that IBM Tivoli Privacy Manager for e-business works with IBM Tivoli Access Manager for e-business. Integration between these products enables Privacy Manager to incorporate business-purpose specifications and end-user choices into access requests secured by Tivoli Access Manager for e-business. Ultimately, the combination of these two products helps ensure that sensitive data is being accessed for approved purposes. Auditing capabilities help meet some of the requirements being set in place by privacy legislation.

Tivoli Access Manager for e-business makes it easy to accommodate infrastructure elements that might be part of an existing operational environment, or that might be planned for enhancing an existing operational environment. This includes authentication mechanisms, directories, virtual directories, hardware accelerators, VPN products, XML gateways and load balancers/IP sprayers. Examples of such products include:

- Aelita Directory Manager 4.1
- Blockade ESconnect
- Citrix MetaFrame XP 1.0/Nfuse 1.51
- Citrix MetaFrame Presentation Server 3.0
- Computer Associates eTrust Directory
- DaonConnect
- DataPower XS40 XML Security Gateway
- Digital Evolution Web Services Management
- Entrust TruePass
- Eracom Protect Server Orange
- Forum Sentry
- F5 Networks BIG-IP
- IBM 4758
- IBM 4960
- Intelliden R-Series
- Lotus Domino 5.0.8 and 6.5
- Microsoft Active Directory (incl. GSO Synchronization)
- nCipher NFast
- nCipher NForce
- Novell eDirectory
- OctetString Virtual Directory Engine
- Ping Identity SourceID Liberty ID-FF 1.1 Tool Kit
- Priva SSO
- Radiant Logic
- Rainbow CryptoSwift
- Reactivity XML Firewall 2300 Series
- Rocksteady RockNet
- Sanctum AppShield
- SecurIT CDAS for Vasco DigiPass
- SecurIT Biometric Voice Authentication Solution for SentryCom
- Siemens DirX 6.0
- Sun ONE Directory Server
- Westbridge Technology XML Message Server or XMS and the XA2500/2700 Appliance
- WinCom Switching Server

Another primary consideration in terms of whether Tivoli Access Manager for e-business can offer effective security for an enterprise is whether Tivoli Access Manager for e-business supports many of the applications around which the enterprise has standardized. Tivoli Access Manager for e-business integrates with many industry-leading Web applications and appliances including:

- Adexa (Collaboration Family)
To pick two significant solutions from that list, let’s consider WebSphere Application Server and WebSphere Portal and how Tivoli Access Manager for e-business can provide value to their implementations.

**Access Manager and WebSphere Application Server**

WebSphere has its own security, but there are several reasons to externalize security management from WebSphere Application Server and have Access Manager provide security for WebSphere Application Server and applications running in it. Access Manager lets you centralize security management across WebSphere Application Server and non-WebSphere Application Server applications, thus allowing a complete single sign-on, authentication and authorization solution across the enterprise.

Access Manager can secure non-HTTP and non-RMI/IIOP access to resources like WebSphere MQ queues with Access Manager for Business Integration and operating systems with Access Manager for Operating Systems. This access lets WebSphere Application Server participate in a broader and more cohesive single sign-on, authentication and authorization architecture than if WebSphere Application Server were managing its own security.
Externalized security also allows single sign-on across old and new applications, enabling legacy applications to participate in the same overall security architecture. Beyond WebSphere Application Server’s own security, Access Manager provides unified, flexible management of strong security with a high performing, flexible architecture that extends to include rules-based decisions, and that can integrate with existing user registry data and authorization databases.

The key security features Access Manager offers WebSphere Application Server are:

- User authentication with WebSEAL.
- Lightweight Third-Party Authentication (LTPA) support for single sign-on with WebSEAL.
- Shared user registry capability.
- Java security classes for programmatic use.
- A Java administration application that runs on WebSphere Application Server.
- Single sign-on to forms-based login.
- A J2EE authorization module that replaces built-in WebSphere Application Server security.

The integration of IBM Tivoli Access Manager and WebSphere Application Server is a powerful and flexible combination that offers robust, scalable, multilayer application security. With Tivoli Access Manager for e-business as its security engine, WebSphere Application Server can participate in a seamless, unified, centrally-managed enterprise security architecture. The current version of WebSphere Application Server is packaged with certain Tivoli Access Manager components, offering the option of utilizing Access Manager security as the native WebSphere security feature. Each new version and release of these products demonstrates increasing levels of integration.

**Access Manager and WebSphere Portal**

WebSphere Portal can be tightly integrated with Tivoli Access Manager for e-business, to take maximum advantage of Tivoli Access Manager as an e-business security platform. The main ways in which Tivoli Access Manager for e-business and WebSphere Portal integrate are:

- Sharing user and group information in LDAP.
- Single sign-on can be established between WebSEAL and WebSphere Portal using the trust association interceptor approach. For more information on TAI, you can access the IBM Redbook *IBM WebSphere V5.0 Security WebSphere Handbook Series*, SG24-6573 at http://www.redbooks.ibm.com.
- Tivoli Access Manager for e-business can provide access control to portlets and page groups within WebSphere Portal. WebSphere Portal can externalize its security and Tivoli Access Manager for e-business is supported out-of-the-box as an external security engine. When enabled, Tivoli Access Manager for e-business can control who can see which portlets/page groups.
- Portlets can use Tivoli Access Manager for e-business for fine-grained access control. The portlets can leverage Tivoli Access Manager for e-business’s JAAS support for authorization checking down to the method level.
- Finally, WebSphere Portal includes the ability to have Tivoli Access Manager for e-business’s more robust GSO ID/password transformation capability integrated with WebSphere Portal Server’s credential vault SSO service.
Web Services Security

IBM Tivoli Software is in a leadership position with regard to security for Web Services. IBM, along with Microsoft and VeriSign, has helped ensure a workable, industry-wide approach to Web Services security by promoting the WS-Security standards, via the Organization for the Advancement of Structured Information Standards (OASIS). In line with WS-Security, IBM Tivoli Software has already achieved a number of milestones regarding advancing the state of secure Web Services, including:

- Completing thorough testing to ensure compatibility of SOAP message transactions, through its WebSEAL proxy. This testing included SOAP transactions in J2EE and .Net implementations.
- Defining a "Federated Identity Interface" in IBM Tivoli Access Manager for e-business V4.1 that enables customized accommodation of multiple token types (including SAML tokens), enabling business-to-business (cross-domain) single sign-on and provides a SAML toolkit.
- Successful participation in two key Burton Group Security Assertion Markup Language (SAML) "bake-offs" held in 2002 (July in the U.S. and September in Europe), where Web Services compatibility and communication was shown through the successful exchange of SAML tokens with other vendors' SAML-capable solutions.

Tivoli Access Manager for e-business supports SAML tokens, trust services, authentication services, and both coarse- and fine-grained access control for Web Services, all available as part of a unified, policy-based, Tivoli Access Manager for e-business authorization solution. Tivoli Access Manager for e-business is integrated with IBM Tivoli Federated Identity Manager, a flexible solution that allows customers to federate with partners using any one of the three standards relevant to federated identity management—Liberty, WS-Federation, and SAML. More information on this topic can be found in the IBM Redbook Federated Identity Management with IBM Tivoli Security Solutions, SG24-6394 at http://www.redbooks.ibm.com.

Supported Platforms

This paper describes Tivoli Access Manager Version 5.1, which runs on:

- IBM AIX® 5.1, 5.2, or 5.3
- Sun Solaris™ 8 or 9
- Microsoft Windows® 2000 Advanced Edition
- Microsoft Windows 2003 Standard Server and Enterprise Server
- Hewlett-Packard HP-UX 11.0, 11i
- SuSE Linux Enterprise Server 8 for S/390 and zSeries (32- and 64-bit)
- SuSE Linux Enterprise Server 8 for IA32 (Intel)
- Red Hat Linux Advanced Server 3.0
- United Linux 1.0 SP2 (includes applicable releases from United Linux 1.0 distributors, including Connectiva, Turbolinux, SCO, and SuSE Linux Enterprise Server 8)

The Access Manager for e-business plug-in for Web Servers supports:

- Sun ONE Server 6.0 on Solaris 8 and 9
- IBM HTTP Server 1.3.19 on:
Customer value

We discuss the value Tivoli Access Manager for e-business brings to the table from three points of view:

► The administrator who manages security, ideally according to a well-defined policy.
► Users who are the customers, employees, partners, or other participants in a secure e-business transaction tailored to them.
► Web application developers, under pressure to deliver more useful function in order to address users' needs, while ensuring that their applications are secure.

The Administrator

Web Portal Manager (WPM), which is a component of Access Manager for e-business, is a Web-based interface used to manage security policy. WPM provides management and administration of users, groups, permissions, and policies. Delegated administration using WPM provides the capability to create delegated user domains, create new users, add existing users to additional domains, and assign various types of administrators to the domains. WPM contains a rich set of delegated management services that will enable customers to delegate user administration, group and role administration, security administration, and application access provisioning to the appropriate business unit personnel.

Web Portal Manager also gives administrators a centralized view of user privileges. Because all access rights information is maintained centrally, an administrator can easily examine a user’s total privileges in the Web space and can easily change those privileges.

Using a unified Web-based administrative tool such as WPM means administrators no longer need to manage accounts on the hundreds of Web servers and applications used in a large, modern Web-driven enterprise.

Tivoli Access Manager for e-business is a complete Web authorization solution, and includes registry technology in the form of the IBM Directory Server V4.1 and V5.1 on:

► AIX V5.1 or V5.2
► HP-UX 11.0 and 11i
► Linux on xSeries
  – United Linux 1.0 with SP2
  – SuSE Linux Enterprise Server 8
IBM Tivoli Access Manager for e-business

The IBM Tivoli Directory Server is scalable to 10’s of millions of entries. For customers who prefer to use other directory technology that they might already have implemented, Tivoli Access Manager for e-business also supports the following directories as its user registry:

- Netscape iPlanet Directory Server V5.1 and Sun ONE Directory Server 5.2
- Novell eDirectory 8.6.2 and 8.7
- Lotus Domino 5.0.10 and 6.0, on any platform supported by TAMeb V5.1

Mainframe customers can implement Tivoli Access Manager for e-business, using the OS/390 Directory Server backed by DB2. With this configuration, users can either be authenticated using the Directory Server (LDAP) or they can be authenticated using:

- OS/390 Security Server on OS/390 V2R10
- z/OS Security Server on z/OS V1R2 and higher

Working in a mainframe environment, Tivoli Access Manager for e-business can authenticate designated users against RACF or TopSecret. Figure 13 on page 26 shows how Tivoli Access Manager for e-business components can run in virtual machines on a mainframe and protect 3-tier transactions (browser-to-Web-Server-to-mainframe). These transactions benefit from high performing, highly secure communications through z/OS HiperSocket or Guest LAN capability.
Secure, unified user experience

Tivoli Access Manager for e-business includes support to help large numbers of users participate in convenient, available and personalized transactions. With authentication and access-control services for e-business and enterprise applications and resources, you can secure customer, supplier, employee and partner connectivity across:

- Web servers
- J2EE-based application servers
- Industry-leading Web applications

SAP, Siebel and PeopleSoft have certified the integration between their applications and Tivoli Access Manager for e-business.

Tivoli Access Manager for e-business accommodates a broad range of possible user-authentication mechanisms, including user IDs and passwords, client-side certificates, RSA SecurID tokens and mobile and wireless identities. It supports e-business configurations common to many of today’s enterprises, involving subsets of users requiring their transactions to be conducted in different languages. It also supports both the Wireless Application Protocol and the i-mode protocol. Customers with unique authentication requirements can use the plug-in authentication mechanism that comes with Tivoli Access Manager for e-business.

Tivoli Access Manager for e-business helps you deliver a consistent and secure user experience by having end users use a single identity to log in once to gain access to resources according to authorization rules, regardless of the server the resources are on. With support for Web SSO and secure session management across e-communities, Tivoli Access Manager for e-business helps securely extend your business processes to partners and business affiliates.

Tivoli Access Manager for e-business performs intelligent load balancing over replicated servers and can scale with your server deployment. It supports production environments in excess of 3 million users (with testing showing no problems with user populations on the
order of 30 million users), takes advantage of SSL accelerator card technology and secure hardware key store and provides a fail-over capability that allows automatic switchover to a backup Web server.

**Speeding Web application deployment**

The modular architecture of Tivoli Access Manager for e-business allows the separation of security code from application code. This can translate to an improved time to market for your e-business initiatives, because typically you can change the security code without affecting application code and vice versa. This separation also accommodates “defense in depth” designs that involve enforcing security in a sub-network, such as a demilitarized zone.

Tivoli Access Manager for e-business can help lower your cost of building security into new applications by reducing the need to write complex security code. It integrates with Web application servers that support Java 2-or JAAS-without requiring nonstandard tasks such as extra precompiles. Your Java developers simply use familiar Java constructs and calls; they don’t need to learn anything new to take advantage of Tivoli Access Manager for e-business’s security services.

Tivoli Access Manager for e-business also has focused J2EE-based support for securing WebSphere Application Server and BEA WebLogic Server as well as .NET-based support for securing ASP .net applications. The centralized authentication and authorization services of Tivoli Access Manager for e-business can be provided to servlets, JSPs Enterprise JavaBeans™, and ASP .NET applications to keep the programming model simple.

In addition to the Java 2 and .NET services and The Open Group authorization API, Tivoli Access Manager for e-business supports many open industry standards and integration, including:

- LDAP and other de facto standards for storing user and group information. IBM Directory Server, Sun ONE Directory Server, Novell eDirectory, Microsoft Active Directory and Lotus Domino Server are among the supported user registries.
- X.509 V3 client certificates for strong authentication to Web-based resources. Many certificate providers, including VeriSign, Entrust and Baltimore, are supported.
- Mutually authenticated and confidential component interactions through SSL. Tivoli Access Manager for e-business is an open-standards-based implementation.
- Integration with Tivoli Identity Manager lets you share user information in a common directory and create and manage Tivoli Access Manager for e-business users and assign users to existing Tivoli Access Manager for e-business groups through Tivoli Identity Manager-offering a single point of security management for the enterprise.
- Tivoli Access Manager for e-business audit information can be sent to IBM Tivoli Risk Manager and Tivoli Enterprise Data Warehouse, which can produce reports and provide decision-support capability.
- IBM Tivoli Configuration Manager can use the authentication and authorization capabilities of Tivoli Access Manager for e-business to allow users to selectively manage the configuration of their workstations on their own. This can help improve user productivity and reduce administration workload.
Tivoli Access Manager for e-business supports on demand computing

Tivoli Access Manager for e-business helps provide a self-protecting environment through:

- Dynamic authorization rules, which allow the factoring in of real-time consideration into decisions to grant or deny access.
- Prevention of unauthorized access by using a single security policy server to enforce security across multiple file types, application providers, devices and protocols.
- Web SSO for maintaining password and user integrity.
- Robust auditing and information-gathering tools for discovering problems or potential problems.

It also helps provide a self-optimizing environment through:

- Load balancing and automated reflection of Web object spaces.
- Highly available and scalable architecture, based on open standards.

Summary

Businesses today need solutions that address security, scalability, and management for all Web-based traffic. Tivoli Access Manager for e-business plays an integral part in IBM's e-business on demand strategy. It is an authorization and management solution that scales up as demand requires, for flexible support across the entire enterprise. With Tivoli Access Manager for e-business, you can support a wide range of architectural requirements for addressing Web security, provide centralized authentication and access control administration, and support replication of Web servers and immediate updates to access control information. Tivoli Access Manager for e-business can improve system performance by load-balancing traffic and maintaining a highly available system. It can significantly reduce administration costs by delegating privilege-management functions to business owners.

Tivoli Access Manager for e-business's robust support for Linux enables companies to fully leverage the cost efficiencies that accrue to Linux, while integrating with legacy systems and leveraging existing applications. New Web applications can be securely deployed much faster, based on Tivoli Access Manager for e-business's focus on separation of security code from business logic. Changes to security policy don't require changes to the applications themselves, and initial application development is quicker as well.

Tivoli Access Manager for e-business provides fine-grained access level authorization that protects Web resources across multiple operating systems, Web servers, and Web-enabled databases and applications. By providing a centralized access control solution, Tivoli Access Manager for e-business's Web security enforcers enable the deployment of an e-commerce infrastructure. With Tivoli Access Manager for e-business, management can be confident that only users with a need to know will be able to access information. Because security concerns have been answered, a company can make information available to users to a far greater degree than was previously possible. Tivoli Access Manager for e-business users have complete mobility. Their identities follow them wherever they go, allowing secure access to corporate information from their homes or hotel rooms throughout the world.

Tivoli Access Manager for e-business is based on open standards; it supports both symmetric-key and public-key encryption and authentication. It is far and away the leader in providing Java 2 and J2EE security for Java applications. Tivoli Access was the first Web access management product to achieve Common Criteria EAL3 certification. Tivoli Access Manager for e-business secures access to third-party Web servers, including those developed by IBM, Lotus®, Apache, Microsoft, and Netscape. Tivoli Access Manager for
e-business has been integrated with many http-based applications, and many of those integration efforts have been tested and/or certified, including WebSphere, Siebel, PeopleSoft, SAP, Lotus Domino™, Microsoft and other applications. WebSEAL and the Web Server Plug-In provide a single sign-on to all resources accessed through the Web.

Why the obsession with standards? Why focus on scalability? Why offer the option of running on multiple Linux platforms? We're helping you do what you tell us you want to do - make faster, better decisions, reduce risk, leverage your core competencies, and increase your return-on-investment.

By helping customers become on-demand businesses, Tivoli Access Manager for e-business helps them change the way they operate. They can lower costs, serve their customers better, improve their speed and agility in the marketplace, and gain an edge over their competitors.

To find out more about Tivoli Access Manager for e-business, visit: http://www.ibm.com/software/tivoli/products/access-mgr-e-bus/

The team that wrote this Redpaper

This Redpaper was produced by a team of specialists from around the world working at the International Technical Support Organization, Austin Center.

Axel Buecker is a Certified Consulting Software I/T Specialist at the International Technical Support Organization, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of Software Security Architecture. He holds a degree in computer science from the University of Bremen, Germany. He has 18 years of experience in a variety of areas related to Workstation and Systems Management, Network Computing, and e-business solutions. Before joining the ITSO in March 2000, Axel was working for IBM in Germany as a Senior I/T Specialist in Software Security Architecture.

Mike Campbell is a Senior Security Specialist responsible for worldwide technical marketing for IBM Tivoli Access Manager. Previously, Mike was a Product Manager and Systems Management Consultant for IBM Corp. He specializes in IT security, especially pertaining to authentication and authorization frameworks. In addition to IBM Redbooks, Mike has authored numerous articles, briefs, and courses on IT security. He attended Villanova University where he graduated with a B.S. degree in Mathematics in 1974.

Thanks to the following people for their contributions to this project:

EDITOR
International Technical Support Organization, Austin Center

Sridhar Muppidi, Neil Readshaw, Carl Hovi, Jeffrey Miller, Ben Harmon, Gerard Joseph, Amanda Watkins and the Integration Factory team, Vaughan Harper

IBM
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.