Oblix NetPoint:
A Technical Overview

WHITEPAPER

oblix™
Identity-Based Security Solutions

Printed in the United States of America.
Printing Date: March 2003 **Part Number: obx9e**

Oblix, Inc.
18922 Forge Drive
Cupertino, CA 95014, USA
T 408.861.6800 F 408.861.6810

European Headquarters
Atrium Court
The Ring, Bracknell
Berkshire RG12 1BW, UK
T +44(0)1344 393 054

www.oblix.com
info@oblix.com

E-Business Identity Management 1
The Challenge of Internet Infrastructures 1
The Complete Solution with Oblix NetPoint . . 2
Enterprise Identity Management 2
Web Single Sign-On 2
Oblix NetPoint Overview 4
Integrated Systems 4
NetPoint COREid System 4
NetPoint Access System 5
Comprehensive Integration and
Interoperability Services 5
The Details: Oblix NetPoint Systems & Services . . . 6
NetPoint COREid System 6
A Brief Overview 6
User Manager 9
Group Manager 11
Organization Manager 14
Identity Workflow Services 16
Multi-Level Identity Delegation 17
Data Management Services 18
Certificate Management Services 19
Password Management Services 20
PresentationXML 21
NetPoint Access System 22
Authentication Services 24
Authorization Services 25
Auditing Services 26
Multi-Level Policy Delegation 27
Federation Services 28
Associate Portal Services 28
FEDERATEDid Layer 29
Passport Authentication Plugin 29
NetPoint SAML Services 30
Integration Services 31
XML Services and API 32
Portal Inserts 35
Personalization Services 35
Application Server Integration 35
Oblix NetPoint Mainframe Support 36
Packaged Enterprise Management
Application Integration 37
Portal Integration 38
Provisioning Solution Integration 38
Infrastructure Design, Implementation,
and Administration 40
Oblix NetPoint Architecture 40
Three-Tier Design 40
Reliability and Scalability Features 40
Multi-Level Caching Support 41
SSL Communication 41
Connection Pooling 41
Standards Compliance 41
Locale Ready 42
Directory and Third Party Security Systems
Integration 42
Security and Intrusion Detection Systems . . . 42
Reporting Tools 42
Real-Time Monitoring Tools 43
Directory Servers 43
Deployment 44
Directory Schema and Object Classes 44
Productized User Identity, Group, and
Organization Management 44
Virtual Host IDs 44
Installation, Configuration,
and Administration 45
The NetPoint Installer 45
The NetPoint System Consoles 45
Oblix NetPoint Benefits 47
Rapid Return on Investment 47
Stronger Security 47
Greater Scalability 48
Conclusion 48

E-Business Identity Management

At unprecedented speed, Internet technology has permanently transformed business processes. The most agile enterprises have rapidly found that they can do more with less by rebuilding their business models around e-mail, Web-based commerce, and network-centered applications. Moreover, they have revamped their once closely guarded business networks as new, collaborative environments connecting their employees, customers, partners, and suppliers.

By linking everyone involved in their e-business initiatives, these innovators have harnessed the potential to increase revenue, reduce costs, and improve productivity. But to realize this competitive advantage, companies must overcome a technological challenge at the core of e-business: how to securely and cost-effectively manage the expanding numbers of people, in a wide variety of roles, requesting network information.

As enterprises have raced to build and implement new Internet applications, this issue of identity management has often been lost in the chase. Typically, each new application has been independently deployed with its own security system, its own set of information about authorized users, and its own management interface. The result? An IT nightmare that threatens to cancel out the essential benefits of e-business. Disjointed information systems about network users and their access privileges slow application deployment, raise network ownership costs, drain expensive IT resources, and threaten enterprise security.

The Challenge of Internet Infrastructures

The answer to this problem is a fully integrated identity infrastructure at the heart of e-business that is powerful and flexible enough to be used across all enterprise applications. The solution must support an ironclad Web access management scheme that protects all online resources through a centralized, manageable platform. At the same time, it must be able to handle a huge number of interactions and scale quickly and reliably, so that new employees, partners, and customers have immediate support as the e-business network grows.

Of course, creating this kind of flexible, adaptable infrastructure is not easy. As they migrate to Web-based business models, most companies must contend with significant technical and operational challenges, such as:

- Heterogeneous network environments, including legacy systems, Web servers, application servers, applications, and other e-business resources
- Platforms and applications that cannot scale to meet future needs
- Disjointed, independent authentication and authorization systems

- The lack of a centralized directory or other storage repository for user and policy information
- Limited management of overall system security and access control
- Constantly changing user populations whose access privileges must be rapidly and securely managed in a cost-effective way

Yet, overcoming these challenges is fundamental to e-business success. Until an enterprise effectively manages who is accessing its Web-based information—and securely controls what each person can use—it cannot derive real competitive advantage from its e-business network.

The Complete Solution with Oblix NetPoint

One unified enterprise identity and Web access management system provides an infrastructure that can serve as the foundation for an entire e-business network: Oblix NetPoint™. This integrated solution allows the centralization of all user identity and security policy information across all enterprise applications. With comprehensive identity management at the heart of its e-business, an organization can easily and cost-effectively control Web access even in highly dynamic, expanding network environments.

Oblix is the recognized industry leader in providing identity management solutions to e-businesses and has been doing so successfully for over six years. For a well-integrated identity infrastructure, Oblix NetPoint delivers two key capabilities right out of the box.

Enterprise Identity Management

This capability keeps all identity information about network users up-to-date and reliable, ensuring that access control is accurately enforced. Data about individual users, groups, and organizations can be entered, removed, or changed quickly and easily so that e-business security remains effective despite ongoing changes in the user population.

Web Single Sign-On

This capability gives every user in an e-business environment quick, one-step authentication for access to multiple resources: applications, content, services, and objects in applications. With Web single sign-on, developers can establish and maintain one centralized security scheme, without struggling with separate information databases for each network resource and complicating the user experience.

Together, the components of Oblix NetPoint add up to an intelligent enterprise identity and Web access management solution that can not only integrate with an existing network but also adapt and scale to meet emerging applications and business needs. While competing systems offer authentication and authorization products, none provides the winning combination of user identity and security policy management; delegated administration; and workflow found in Oblix NetPoint.

Additionally, its Web services architecture enables other vendors' systems and applications to integrate with and extend Oblix NetPoint's identity infrastructure for more nimble network services and processes. Other applications that require access to user and policy information (such as provisioning and password management systems) can be easily integrated into the environment and deployed more quickly. These additional applications essentially reside on top of the identity infrastructure at the heart of the e-business network.

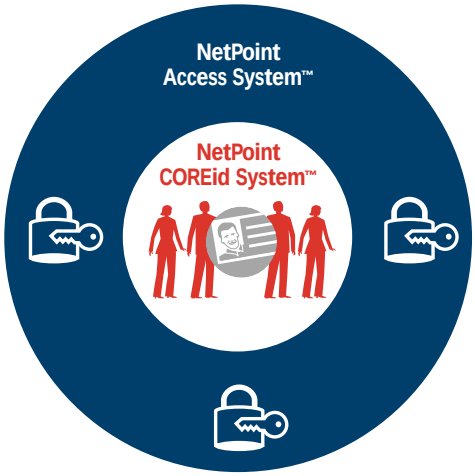
Overall, by providing a unified identity management system, Oblix NetPoint
- **delivers rapid return on investment**,
- **enables stronger security**, and
- **ensures e-business scalability**.

It's the identity infrastructure that all applications, systems, and users in an e-business environment can profitably leverage for today's business interactions—and tomorrow's.

Oblix NetPoint Overview

Integrated Systems

Oblix NetPoint is composed of two powerful systems: the NetPoint Access System™ and the NetPoint COREid System™. Although replete with the most sophisticated functionality, both systems are designed for use by nontechnical business workers—rather than by designated IT professionals alone. This means that the workload of Web access management and upkeep can be efficiently distributed throughout an e-business environment, giving each typical user and administrator appropriate responsibilities for managing identity information and thereby eliminating IT bottlenecks. Only Oblix NetPoint offers this capability for administrative delegation as well as a robust, multi-step workflow that is easily aligned with a company's preferred business processes and policies.



NetPoint's tightly integrated systems ensure comprehensive enterprise identity management with Web access control.

NetPoint COREid System

The NetPoint COREid System delivers the ability to manage the identity, group, and organization information and access privileges related to every constituent within the e-business community, and truly puts identity management at the foundation of an e-business network.

Powerful self-service security features and delegated administration ensure that this information is continually kept current, even in dynamic e-business environments. This delegation of identity management significantly reduces administrative costs and burden. Because user identities are always kept up-to-date, Oblix NetPoint increases

the effectiveness of security policies that define access privileges based upon user identity attributes. In turn, this secures the overall business network in real time.

NetPoint Access System

Business information is constantly changing. The arrival and departure of employees, address and name changes, the creation of new employee teams, and changes in partner roles keep identity information in a state of flux. The NetPoint Access System has been designed from the ground up to support Web access management in the face of dynamically changing user identity information. A centralized policy store for all resources in the entire e-business environment, it provides policy-based authorization, Web single sign-on, and common resource security across multiple servers and applications.

Comprehensive Integration and Interoperability Services

The ability to seamlessly integrate any e-business platform within a corporate Web infrastructure, and to extend its reach across corporate boundaries to those of partners and customers, is key to success in both the short and long term. That is why Oblix NetPoint was designed with most advanced options for seamless integration and interoperability both within and across Internet infrastructures.

NetPoint ensures seamless enterprise integration and interoperability through the following:

- **Federation Services:** NetPoint Federation Services™ enable interoperability between multiple security domains, even when those domains are governed by disparate security systems.
- **Integration Services:** Oblix NetPoint is the only solution that offers comprehensive access and identity APIs and XML Web-based services spanning both identity and access functionality.
- **Partnerships for Seamless Integrations:** As an enterprise software provider committed to customer satisfaction, Oblix understand the value in delivering validated and supported integrations between best-of-breed products. Therefore, Oblix have teamed together with leading enterprise application and application platform providers to ensure seamless integration of Oblix NetPoint with application platforms, packaged e-business applications, and portals.

The Details: Oblix NetPoint Systems & Services

NetPoint COREid System

Today's dynamic organizations are continually in flux, as employees join and depart, partnerships are formed and dissolved, and new business relationships continually emerge. The administrative burden of getting thousands of users into an e-business system, giving them appropriate access privileges and services—and keeping their data accurate over time—can be a costly drain on IT resources. Moreover, it can threaten the security of the overall system.

Clearly, without a robust identity infrastructure, a virtual organization cannot hope to implement and expand a secure e-business environment. COREid™—Oblix's unique approach to identity management—allows a company to dynamically manage identity information about each individual user, group of users, or organization profiled in its e-business network. The NetPoint COREid System puts digital identity at the center of an e-business environment. The result is a flexible and secure infrastructure that can include a maximum number of people while being managed with minimal costs.

A Brief Overview

The COREid System is composed of three applications, which effectively handle the identity profiles and privileges of the user population.

- **User Manager™:** Manages all information related to each individual user within a Web enterprise.

- **Group Manager™:** Allows for the definition and management of user groups, allowing for secure access control to resource on a group-membership basis.

- **Organization Manager™:** Allows for the definition and management of entire external organizations (such as partners, suppliers, or internal business units) or other large organizational containers, allowing for secure access control to resources at the highest organizational level within an enterprise.

Underlying each of these applications is a set of common services, interfaces and functionality for comprehensive identity management:

- **Identity Workflow:** NetPoint provides a unique, multi-step workflow engine (see p. 16) for companies to tailor the functionality of each COREid application to its own operating processes. Having flexible administrative workflows for every step in user, group, and organization management not only lowers e-business transaction costs, it also ensures consistent services and tight security across the entire distributed environment. With NetPoint's sophisticated workflow engine, companies can quickly and cost-effectively bring diverse users in and out of their systems—from initial registration, to access approvals, to eventual deactivation—in a way that closely aligns with business rules and logic.

- **Delegated Identity Administration:** NetPoint provides a unique multi-level delegation model that the COREid system leverages to allow companies to distribute responsibility for maintaining user identity information throughout their networks (see p. 17). In this way, identity data can be entered, approved, and maintained by the individuals who are most knowledgeable about it—whether in internal or external organizations. Companies have complete flexibility in how much responsibility they delegate, and to what parties. The result? No central IT bottlenecks and higher levels of security and scalability.

- **Data Management Services:** The NetPoint COREid System offers granular attribute access control to determine self-service and modify rights on an attribute-by-attribute basis, and a restricted search base for the display and modification of information. For more information

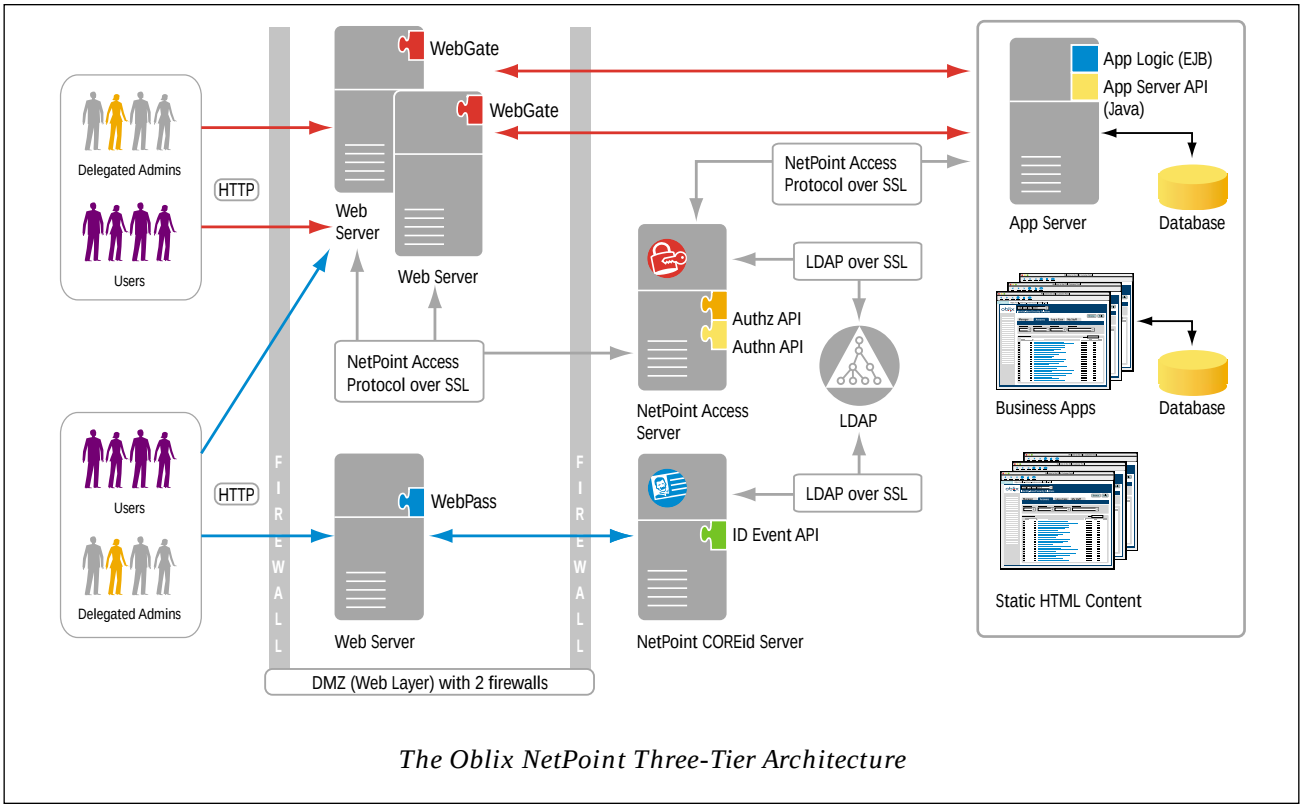
- **Digital Certificate Management:** The NetPoint COREid System provides a Certificate Processing Server™ for managing digital certificates.

- **Password Management:** Oblix NetPoint provides a wide range of password management functions for increased user satisfaction and productivity:

- **PresentationXML:** PresentationXML allows organizations to leverage XSL style sheets for the customization of user interfaces. NetPoint's XSL style sheets can be used to create the most appropriate layout of NetPoint COREid System pages for different types of users.

- **Custom Reports:** Each of the NetPoint COREid applications provide a GUI-based framework through which custom reports of identity information may be easily generated. For example, users can quickly search for a listing of all the vice-presidents within the enterprise.

- **Flexible APIs:** The NetPoint COREid System provides flexible APIs that enable developers to extend and customize its already rich set of identity management functionality. See "Integration Services"on page 30 for more information.



The Oblix NetPoint Three-Tier Architecture

The NetPoint COREid System features two types of servers and a plug-in that may be configured to support a three-tier architecture. The system's functionality is processed by the NetPoint COREid Server™(s), which communicates with a Web server plug-in called WebPass. WebPass sends information back and forth between the COREid Server and the Web server, enabling a three-tier architecture for maximum security and reliability. The system also provides a Certificate Processing Server for managing digital certificates.

COREid Server

The NetPoint COREid Server is an installable, standalone server that processes all requests for user identity, group, organization, and credentials management. Organizations can set up multiple instances of the server if necessary.

WebPass™

The WebPass component of the NetPoint COREid System is a plug-in that is placed on the Web server to pass information back and forth between the Web server and the COREid Server. This three-tier architecture enables an organization to host the COREid Server behind its server firewall and outside its DMZ. This capability delivers improved security since the LDAP directory server is not exposed outside the firewall.

Certificate Processing Server (CPS)

This component serves as an LRA (local registration authority) enabling requests coming from the COREid Server to be communicated to the VeriSign CA Processing Center. The NetPoint CPS is based on technology Oblix has licensed from VeriSign and then further enhanced with identity management functionality. For more information on NetPoint Certificate Management Services (see p. 19).

User Manager

The User Manager application enables complete management of all the information related to the individual network user. Its intuitive Web interface, flexible workflows, and multi-level delegation model streamline the difficult task of extending multiple privileges and services to a massive user population.

Features and Functionality

User Manager handles all the key functions related to user identities:

- **Creation and deletion of user identity profiles**
- **Modification of user identity profile data**
- **Determination of access privileges**
- **Credentials management of both passwords and digital certificates**

With User Manager, the Create, Delete, and Modify functions of user identity management can be set as flexible, multi-step workflows. Each business can customize its own approval, setup, and management processes without restriction—and have multiple processes for different kinds of users. Having workflows for this functionality lets a company

- **easily route information and approval requests** through many internal and external steps and decision makers;
- **provide modifiable information entry forms for different kinds of users**; and
- grant access privileges and services automatically according to preset default values.

Multi-level delegation features also simplify individual user management. Companies can assign the responsibility for maintaining user identity data to the people closest to it. For example, individual users can be allowed to:

- **add themselves to the user directory** by filling out customized forms;
- **modify personal or professional information about themselves** (such as addresses, personal preferences, or name changes);
- **change a piece of information in their identity profiles**, which in turn can determine their access rights; or
- **allow someone else to log in as their temporary substitute** while they are out of the office or on vacation.

Likewise, any number of delegated administrators (both inside and outside the company) can be given the authority to

- **create and delete users in the user directory**;
- **approve a change a user has requested**; and
- **change the information about users to grant or revoke services**.

Any administrator can be delegated any degree of responsibility. For example, a company might decide that only IT staff can assign application access, whereas a department manager can add new users. This allows management responsibility to be distributed evenly and efficiently.

Finally, external legacy systems—such as human resource management systems—can be allowed to trigger automated workflows. With this feature, a new user could be created, a departing employee could be deleted, or certain services could be granted or revoked following an event change in an external system. This robust delegation functionality enables rapidly growing e-businesses to distribute identity management workloads externally or internally, eliminating IT bottlenecks. It particularly reduces the burden in two key areas—user registration and user deactivation/reactivation.

User Self-Registration

Nobody wants to individually register thousands of users, so self-registration provides a valuable way for organizations to accommodate growing user bases. User Manager enables individuals to self-register in situations when it's appropriate and then authorizes delegated administrators to verify self-registration information and approve or deny self-registration requests.

Self-registration on the NetPoint COREid System is defined by a customizable, multi-step workflow. Organizations can flexibly configure the process and specify different formats and approval processes for different types of users.

The Oblix solution offers a full array of customizable formats to enable new employees, partners, and associates to fill out personal information about themselves and their organizations. Companies can configure specific workflow processes for different users. Upon completion of the registration process, delegated administrators confirm and approve the information, ensuring that the NetPoint Access System is making policy decisions based on the most up-to-date information about users. Upon approval, User Manager automatically places new users in the specified part of the virtual company.

User Deactivation/Reactivation

From time to time, organizations also need the ability to rapidly deny individuals access to Web information. With User Manager, a delegated administrator can deactivate users who have left company or have been terminated, ensuring that they are no longer active in the system and able to access information and resources. Caches are immediately updated to prevent any security breaches. This is facilitated through a one-button deactivation feature.

User Manager also lets companies temporarily deactivate the user identity profile of a user who is taking a temporary transfer or leave of absence, without losing all of the information and definitions of access privileges that reside in his or her profile. At a later time, when the user returns, the identity profile can be easily reactivated and new information added or removed if desired.

Benefits

User Manager's key benefits include the following:

- **Reduced operating costs.** Efficient processes to manage ongoing user changes and access privileges lower IT expenses and operating costs.
- **Higher levels of security.** Network users who own control of data close to them are motivated and empowered to keep it current; this yields a more up-to-date user database on which to build security.
- **Greater flexibility in modeling business processes.** Most competing products offer limited "all-or-nothing" delegation schemes. User Manager lets companies design approval and setup processes without restriction—for greater productivity.
- **Increased scalability.** As an e-business grows, processes are in place at every level to accommodate new users and provision them quickly with the resources they need.
- **Greater accessibility and user productivity throughout the e-business enterprise.** The User Manager is designed to be used easily and productively by all types of users—internal and external—ranging from non-technical end users to the most sophisticated IT administrators.

Group Manager

The Group Manager application allows companies to identify groups of users who need identical access privileges to a specific resource or set of resources. Managing and controlling privileges for a group of related people—rather than handling their needs individually—yields valuable economies of scale.

Features and Functionality

No other vendor provides as rich or as flexible a set of functionality related to group management, all supported by delegated administration and identity workflow processes. Group Manager meets a wide range of e-business needs:

- **Easy creation, maintenance, and deletion of permanent, ad hoc, and dynamic groups** of users who may be allowed or denied access to particular resources
- **Modification and adaptation of groups and their access privileges** with minimal disruption to the directory server's underlying schema
- **Efficient addition and deletion of users** from established groups
- **Delegation of administrative responsibility** for group membership and subscription requests and approvals
- **Through dynamic groups**, which defines group membership based on user identity attributes, provides a framework for role-based access control

With so many users needing access to so many different resources, growing e-businesses must have ways to restrict who can request access, to distribute the approval process, and to maintain an audit trail of who gave whom which right. NetPoint's unique multi-level delegation model dramatically and cost-effectively reduces these administrative complexities for group management. With Group Manager, companies can allow individual users to

- **self-subscribe to and unsubscribe from groups**;
- **see the groups that they are eligible to join or have joined**; and
- **request subscription to groups that have access to the applications they need**.

Multi-step workflows can then define which users must obtain approval before being added to a group and which can be added instantly.

Group Creation and Modification

Using the Group Manager application, a company can form groups proactively or in response to user demand. Oblix NetPoint provides support for static groups (members manually added and removed), dynamic groups (lists automatically generated based on user identity attributes), hybrid groups (a combination of static and dynamic groups), or nested groups (memberships formed inside other group memberships). Dynamic groups are formed by applying LDAP filters to query the directory server. For example, a dynamic group may be formed by identifying all Tier-1 suppliers who have the words "Accounts Receivable" in their titles. Alternatively, users can request to be added to a group, such as a newly formed cross-functional team.

The ability to create and use dynamic groups is extremely valuable because it eliminates the administrative headache of continually keeping individual, static membership up-to-date. With dynamic group management features, users can be automatically added or removed if they meet the criteria specified by the LDAP URL (query on the directory data). The Group Manager also provides a Query Builder to manage and test the creation of the groups. Dynamic groups also greatly enhance security since changes in user identities that disqualify someone from membership in a group are automatically reflected in the dynamic group membership.

Companies also want to be able to modify or adapt groups of users and their associated privileges over time, with as little disruption as possible. They need to be able to add, change, and remove groups of users and their respective access privileges without changing the underlying schema of their directory servers. Group Manager takes care of this requirement in a flexible, transparent way, so that users can reliably get access to what they need.

Group Membership

Membership can be determined by explicitly adding a person to a group or by setting a specific attribute value in that user's identity profile such that the user becomes a member of a dynamic group. Companies can use both methods to grant or deny user privileges.

There are some cases in which determining group membership with a user identity profile makes sense. However, using this approach exclusively presents problems. Consider the negative consequences if access to all network applications were controlled with user identity profile attributes:

- Because user schema changes are global changes to the directory, they might possibly affect the core operation of the directory server. Given how critical this server is, schema changes should best be kept to a minimum, especially changes to user objects.
- Because applications change constantly, administrators would likely not be able to keep up with changes to the schema of the directory server.
- Privileges to certain applications are often granted to only hundreds of people within an e-business environment that comprises hundreds of thousands of users. It would not be space efficient to store rights that are so infrequently granted.

Consequently, a better way to store access privileges is to create group objects in the directory server that specify which users can access an application. Additionally, these groups can be used by other applications, such as portal products, content management systems, and the NetPoint Access System.

Group Subscription

Different companies have different processes and policies for allowing users to subscribe to a group (which is equivalent to subscribing/requesting access to an application or content). NetPoint is the only Web access management solution to offer a flexible policy-based subscription model. For each group created and managed by NetPoint, authorized users have a range of options for how the subscription policy is applied. The options include:

- **Self-service with no approval needed**
- **Subscription with one or multiple required approval(s)**
- **Rules-based subscription**:
    - Users who meet a certain criteria automatically get added to the group (e.g., all Gold partners automatically are included in the group), OR
    - Users who meet certain criteria can apply to be in the group, but need approval (e.g., all Gold partners can request to be added to the group, but they need to go through one or more approvals, as configured).
- **Closed groups** for which subscription is not allowed

Benefits

Group Manager's key benefits include the following:

- **Greater efficiency in managing access policies.** The definition of groups is a flexible, effective way to control application access—without modifying directory schema.
- **Reduced administrative burdens and costs.** Users can be easily moved in and out of groups through the policy-based subscription and multi-level delegation models, greatly reducing the IT and administrative time and costs associated with getting users access to the applications that they need.
- **Flexible support for customary business processes.** Using groups for access management and other purposes is common in enterprises. Oblix NetPoint provides a way for managing groups, which can be leveraged by multiple applications.
- **Complete accessibility and usability across users.** The Group Manager is designed to be used by all types of users—internal and external—ranging from non-technical end users to the most sophisticated IT administrators.
- **Higher level of security**. Access privileges can be enforced based on real-time changes in group membership—with no lags in updates to compromise security.

Organization Manager

The third application in the NetPoint COREid System, Organization Manager, streamlines the management of large numbers of organizations within an e-business network—partners, suppliers, or even major internal organizations such as sales offices and business units. Certain infrastructure security and management operations are best handled—or can only be handled—at the highest organizational unit (OU) level rather than at the individual or group level. NetPoint is the only solution with the sophisticated functionality to execute these organizational management operations efficiently and cost-effectively. Like User Manager and Group Manager, this application relies on NetPoint's multi-step workflow and delegation capabilities for its flexibility and power. Additionally, the Organization Manager provides the ability to manage any additional Object Classes not supported by the User Manager or Group Manager. This allows for all of the management and administrative features to be applied to other objects without having to build custom administration tools.

Features and Functionality

There are three fundamental data structures that are used to organize data in a directory server. User objects define information about each user; group objects define collections of users; and containers called organization objects define a collection of user, group, and other organization objects.

Organization Manager handles the following administrative tasks:

- **Organization lifecycle management**, whereby companies can create, register, and delete organizations in their systems using customizable workflows
- **Maintenance of organization profiles** on an attribute by attribute basis through self-service, delegated administration, and system-initiated activities.
- **Organization self-registration**, whereby organizations such as business partners, customers, and suppliers can self-generate a request to be added to the e-business network
- **Creation of reusable rules and processes** through multi-step workflows

The same rules and access privileges can be applied to multiple organizations so that each time an entry is created, delegation and setup processes are automatically created for each subsequent organization.

Organization Manager also allows companies to set up container limits, which establish the number of entries (users, groups, or organizations) that can be created under a particular organization. For example, a partner might be allowed to establish a limited number of entries under a company account. Container limits allow the hosting company to keep track of the usage of its system by external parties. This tracking mechanism can be used to limit the usage of its services or to charge users that need their limits increased. External administrators can indicate the point at which they would like to be notified that their company is about to reach its overall container limit.

Organization Manager also allows companies to publish location information (such as maps or floor plans) and apply NetPoint's rich functionality to its management, controlling access and modification privileges. Companies can also define a map hierarchy for any set of locations.

Benefits

NetPoint is the only solution that offers delegated administration and sophisticated management (attribute-level access control) of organization objects stored in directories, as well as customizable multi-step workflows for organization management. With Organization Manager, companies running an e-business site can efficiently create accounts for all their participants and manage their ongoing changes. This functionality allows companies to reduce the cost of managing organizations that they do business with and gives them the ability to more efficiently scale their e-business.

Identity Workflow Services

Oblix NetPoint COREid features a multi-step, flexible workflow engine for the automated management of user identity, group and organization information. All the functionality described below can be set up as a customizable workflow process that can scale easily as the e-business grows. Companies use these processes to implement, approve, and execute tasks such as:

- **Creation, Deletion and, Modification of users identities, group objects and organization objects**
- **User Self-registration and Partner (company) Self-registration**
- **Subscription and Unsubscription to group**
- **Issuance, Revocation, or Renewal of digital certificates**

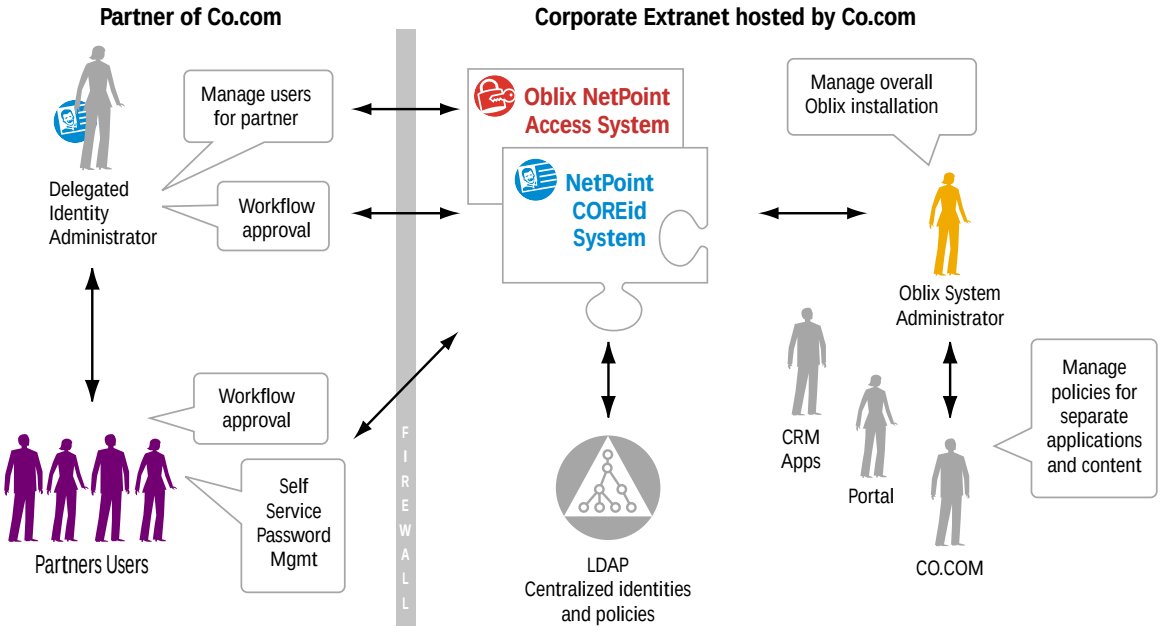
Using NetPoint's flexible workflow engine, organizations can map their business processes without restriction. They can create multi-step workflows, workflows that spawn simultaneous sub-flows, and they can route workflow requests to both internal and external users. NetPoint provides an easy-to-use GUI for creating workflows, and even provides a "Quick Start" feature that provides common workflow templates such as "Create New User" and "Delete User" for quick configuration of workflows.
The customizable workflows also allow for automated access privileges and services management. For example, when new suppliers are entered into a system, they can be automatically given certain access privileges and services. Full-time employees, on the other hand, can have different privileges and services set up by default. The workflow allows for customizable forms and automatic account information creation (for example, "a user is subscribed to specific groups if that person is a Premier partner").

In addition to their ability to flexibly define workflows, organizations can use the Identity Event Plug-in API to call out to an external program from any point in the workflow process. There can also be cross-product workflows, whereby a step in one process triggers another workflow. NetPoint also supports participant-based workflow, which allows organizations to define and apply workflows consistently across different organizations, but route workflow tickets to different participants. Finally, NetPoint provides complete facilities for managing workflows tickets, including the ability to track and search for workflow tickets.

Having a powerful, sophisticated multi-step workflow engine for all user, group, organization, and certificate management is extremely valuable for organizations that wish to tailor functionality on their e-business sites to fit their business processes and reduce the costs of all site transactions. No competitor offers such a flexible engine.

Multi-Level Identity Delegation

NetPoint provides a multi-level delegation model for distributing responsibility for identity information management throughout a network of internal and external users. Responsibility for identity administration can be delegated on a full or partial basis, to internal and external users. It can also be delegated to people with different responsibilities, including IT personnel, business line managers, or end users. Each user to whom this responsibility is delegated can further assign equal or lesser privileges to another user, if he or she has been given the rights to do so.



The NetPoint COREid delegation model is fully workflow-enabled, providing maximum automation for business processes.

All data management and administrative rights within NetPoint can be delegated. Data Management rights are View, Create, Modify, Delete for user, group, and organization identity information. The right to modify a user, group, or organization identity profile can be set with a very high degree of granularity at the attribute level. For example, with NetPoint you can specify that a partner organization can manage its own passwords and four identity attributes, but not any other attributes in the directory.

Administrative rights can also be delegated in NetPoint. They include Set Attribute Level, Access Control, Set Workflow Definition, Monitor Workflow, Set Containment Limit, and Expand Groups.

NetPoint has a unique fine-grained delegation model that allows companies to specify for each single data management or administrative right (e.g., View, Create, Set Access Control) who can be delegated that right. Companies can also specify over which domain the right applies. The domain is either specified as a node in the tree and/or by a filter that gives a virtual domain (e.g., all identity profiles with an organization equal to Gold supplier). This is used for delegation schemes with flat trees.

Oblix uniquely offers both grant and delegate rights. Grant rights allow a user to perform a given right, such as viewing or managing an attribute, for a set of objects. Delegate rights allow users to further delegate any rights they have been granted. This delegation process can continue for an unlimited number of levels to lower overall network management costs.

This flexible, multi-level delegation model lets organizations logically distribute the workload involved in user, group, organization, and certificate management. It also eliminates bottlenecks in all the processes necessary for e-business growth. No other company offers limitless multi-level delegation in identity management.

Data Management Services

Oblix NetPoint features granular, attribute-level access controls for companies managing users, groups, and organizations. With the ability to specify who can view or modify user, group, or organization information at the attribute level, companies can reduce the administrative cost of identity management. By permitting certain users or delegated administrators to update some—but not all—attributes themselves, a company can keep identity information very current without having to extend blanket rights to change all data. For example, a company running an extranet might want its users to update their contact information and be able to view their account status, but not modify it.

Delegating data management to end users and delegated administrators allows changes to user identity information to happen more quickly than if a central IT department were to handle them. Also, the users that are closest to and most knowledgeable about the data will make the changes, improving the accuracy of the information on which security policies are based.

To specify who can view or modify an attribute, or who can be notified of an attribute change, organizations can designate users, groups (both static and dynamic), roles, or relationships between users (e.g., supervisor or account manager).

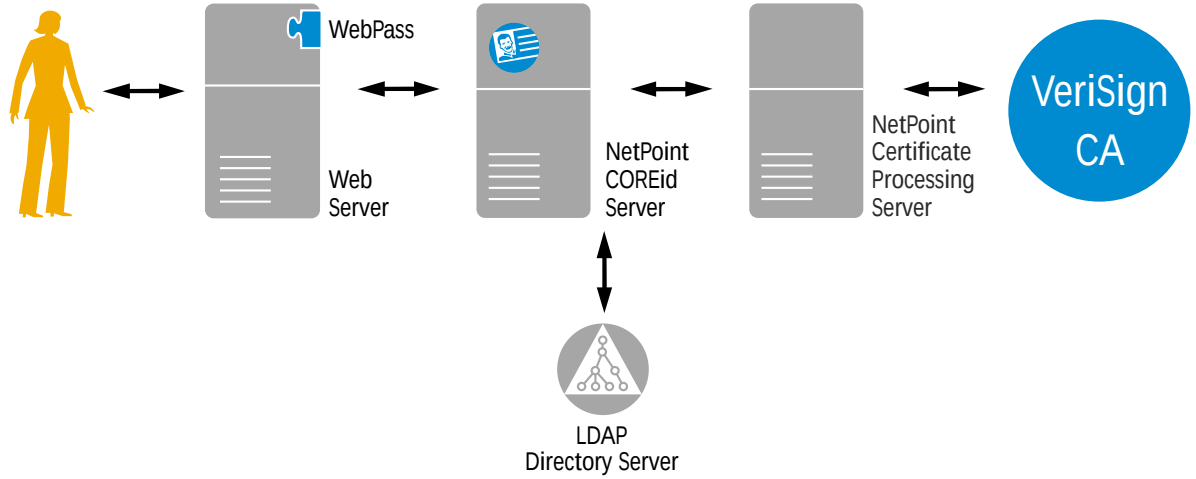
Organizations can also specify a restricted search base to be used to display and modify information for different audiences. A dynamic search base can be set up for different types of users that limits the information they can see and who they can add to a group. For example, an e-business host can set up its site so that its partners cannot see each other, or an ASP can prevent its customers from seeing each other. Multiple, disjoint search bases can be specified. The search base that generates this localized access can be set both with flat and branchy trees.

Certificate Management Services

PKI certificate management is being hailed as a key e-business technology for increasing the security of online transactions and interactions between companies and across the Internet. Although PKI sales are expected to increase in the coming years, current solutions face a number of challenges related to deployment, manageability, and interoperability.

NetPoint Certificate Management Services tightly integrate the management of digital certificates within the user identity lifecycle and organizational processes so that businesses can efficiently deploy PKI. These services include:

- **Turnkey integration with VeriSign Certificate Authority (CA)**
- **Flexible, multi-step workflows to issue, renew, revoke certificates**
- **Access control and delegation within the certificate management process**



Certificate Management Services are integrated within the NetPoint COREid System.

With Oblix NetPoint, e-businesses can have "turn-key" PKI without having to set up complex infrastructures (such as a local Certificate Authority) for issuing, managing, and revoking certificates. Given the complexities and associated liability of being a local CA, there is a trend in the marketplace to outsource the management of certificates, while still allowing customers to maintain control of their data.

The certificate lifecycle management functionality that Oblix provides eliminates the complexities and liability issues of setting up such a system, while allowing companies to maintain their certificate data in-house. The Oblix solution provides very attractive features for extranets, ASPs, trading networks, and intranets that want to outsource PKI management. Furthermore, NetPoint supports the Online Certificate Status Protocol (OCSP), which gives timely information about the validity of a certificate by checking through the Internet.

NetPoint delivers customizable, multi-step workflow processes for issuing, renewing, and revoking digital certificates, as well as controls for making certificate requests. Companies can also determine which types of certificate approval processes are needed. For example, in order to request a certificate, an external party might have to acquire approval, whereas an internal user might have the right to request a certificate without this step. This streamlined workflow of all management processes related to digital certificates provides advanced automation and the lowest possible cost of ownership.

Certificate management is integrated with the user lifecycle and organizational processes that NetPoint manages—a unique feature that can eliminate security holes and expedite certificate distribution. For example, companies can issue and renew certificates when users are created or change status. A user's certificate can be immediately revoked during the user deactivation or deletion process if that person should no longer have access. And organizations can also have consistent policies both for giving access to certificate-authenticated resources and for issuing certificates after they have set up a resource that requires them in the Access Manager.

Certificate Management Services also take advantage of all other Oblix features, such as delegated administration, self-service, and identity workflow.

Password Management Services

Oblix NetPoint provides a wide range of password management functions for increased user satisfaction and productivity:

- **Multiple password policies**
- **Constraints on password composition**
- **Configuration of password validity and notification processes**
- **Forced password changes**
- **Lost password management**
- **Password creation/change**

Organizations can, for example, specify minimum or maximum password lengths, number of alphanumeric characters, number of upper-case and lower-case characters as well as other constraints. With the Identity Event Plug-in API, a company can check or enforce any password composition requirement it desires, such as a dictionary check.

Password validity and notification processes can also be configured to meet an organization's specific needs. It can specify the length of time a password can be valid, the point at which a user should be notified that a password expiration date is approaching, and the length of time a password must be used before it's allowed to change. Organizations can also limit the number of retries allowed and lock out unauthorized users for a specific amount of time.

To provide system support for one-time log-ins or administrator resets, NetPoint lets companies set up forced password changes. And, to prevent users from employing the same passwords and compromising security, NetPoint maintains a password history.

The system also offers a range of password change and lost password management options. Specific password change and lost password management functionality can be embedded anywhere on a Web page or portal for additional convenience through the use of Portal Inserts (see p. 30) For example, if a password is about to expire, NetPoint can notify a user and direct him to a Change Password screen, where he can enter the old password and then choose and input a new one. The lost password management functionality includes a challenge/response approach that allows for self-service.

Using workflow services provided by Oblix NetPoint, passwords can be specified as part of new user creation or any other business process. This is another example of the flexibility NetPoint offers in its processes for streamlining and securing e-business.

PresentationXML

With Oblix NetPoint's unique PresentationXML functionality, organizations can leverage XSL style sheets to customize user interfaces. NetPoint's XSL style sheets can be used to create the most appropriate layout of NetPoint COREid System pages for different types of users. Creating multicolumn pages, changing text colors, and providing graphical links to other programs are just a few of the many layout options. This capability gives companies ultimate flexibility in how they display, via the NetPoint user interface, the identity information stored in the LDAP directory.

NetPoint's user interface customization allows the use of multiple XSL style sheets for specific types of audiences. For example, an online investment bank might have two primary customer audiences—institutional and individual investors. Although the bank wants to have a consistent look-and-feel and brand experience for both audiences, it also wants to tailor information specific to each group with a particular style, layout, and design. The NetPoint COREid System allows it to meet these design requirements by modifying XSL style sheets, giving it ultimate UI flexibility.

NetPoint Access System

The Oblix NetPoint Access System enables Web single sign-on and common security across multiple Web and non-Web resources and applications. It ensures that only authorized users can gain access to information, applications, and resources residing across virtual organizations. Access is controlled by strict, standards-based authentication, authorization, and auditing policies that protect both Web and non-Web resources residing on a company's servers. The system also provides flexible APIs that enable developers to extend and customize its already rich set of functionality.

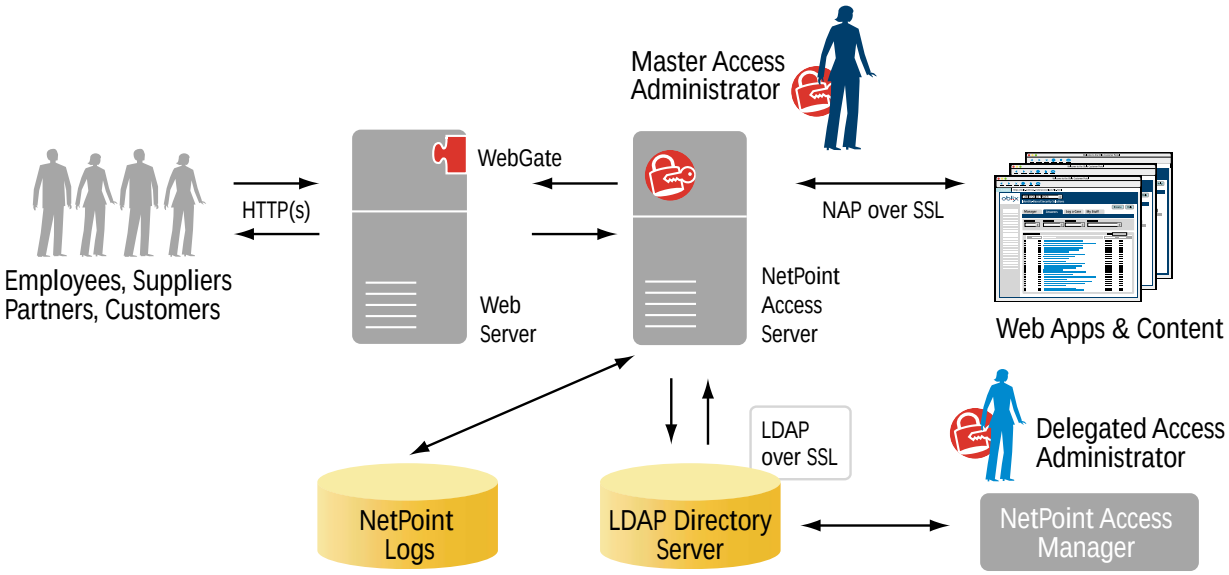
The NetPoint Access System consists of the following application and three components.

- **Access Manager™:** This application features an intuitive graphical user interface for managing policies, setting up Web and non-Web resources to be protected, and testing policies through the simulation of user access.

- **Access Server™:** The Access Server is a standalone server (of which there can be several instances) that provides dynamic policy evaluation services for both Web-based and non-Web resources and applications. Different applications and Web servers can make use of its authentication, authorization, and auditing services.

- **WebGate™:** WebGate is a component that acts as the interface between individual Web servers and the Access Server. Installed on a Web server as a plug-in, the WebGate intercepts requests from users for Web resources and authorizes them via the Access Server. The Access Server is then able to provide centralized authentication, authorization, and auditing services for the content and applications hosted on each of the Web servers. Non-Web resources can also be protected by using the Access Server SDK (see p. 32) to create custom WebGate(s), known as AccessGate(s).

- **Shared Secret Storage:** Oblix NetPoint stores shared secret keys in memory. Unlike other competitive products that store shared secrets on a file system, NetPoint does not leave these keys on open file systems. After shared secret keys are read from the directory, which is well protected behind multiple firewalls, they are confined to the system memory only, not written into files.



Oblix NetPoint centralizes and automates Authentication and Authorization Services across multiple protected resources

The NetPoint Access System also provides a set of services and functionality for comprehensive Web access management:

- **Authentication Services:** Oblix NetPoint supports all the industry's most popular authentication schemes out of the box
- **Authorization Services:** Oblix NetPoint security policies enable the definition of the authentication, authorization, and auditing rules for the most flexible and granular protection of enterprise resources.
- **Auditing Services:** Oblix NetPoint provides a comprehensive set of auditing and reporting functions, enabling organizations to perform security-level auditing of user access to resources, as well as business-level auditing and user profiling
- **Multi-level Policy Delegation:** NetPoint provides a unique multi-level delegation model that the Access system leverages to allow companies to distribute responsibility for maintaining security policies throughout their networks.

In anticipation of the impending ratification of the SAML (Security Assertions Markup Language) standard being developed by the OASIS Security Services Technical Committee, the NetPoint Access System is designed for SAML-readiness; it will be able to produce and consume SAML assertions upon ratification of the standard.

Authentication Services

The first time a user tries to access an application Web page protected by Oblix NetPoint, she will be asked to authenticate. Authentication is the process by which a user's identity is validated. This can be done by requiring the user to present a username and password or by employing stronger methods of authentication such as digital certificates or SecurID™ cards. Oblix NetPoint then validates the presented credentials against the user's stored credentials to make sure that they match. Once the user's identity is authenticated, Oblix NetPoint creates a single sign-on session for the user that frees her from having to sign on again to any other resources or applications she wants to access. For greatest flexibility and security, NetPoint supports multi-level authentication, including the ability to set authentication levels based on static variables, user context variables, or request context variables. Having an identity infrastructure that enables single sign-on to applications and systems greatly enhances the overall user experience and improves productivity.

Oblix NetPoint supports all the industry's most popular authentication schemes out of the box, including the following:

- **HTTP Basic Authentication (Support over SSL)**
- **X.509 Digital Certificate (Support over SSL)**
- **Forms-Based Authentication**

HTTP Basic Authentication (Support over SSL)

HTTP basic authentication capabilities accelerate deployment by simply using usernames and passwords. Oblix NetPoint enables even these most basic credentials to be sent over a secure socket layer (SSL) connection instead of clear text. This is done by redirecting the username and password challenge and verification to a secure SSL port on the Web server, and then passing the user back to the normal, unencrypted link for use of the site. Therefore, organizations can enjoy the performance benefits of non-SSL deployments without sending passwords unsecured over the Internet.

X.509 Digital Certificate (Support over SSL)

Public Key Infrastructure (PKI) is gaining recognition as an essential component of secure e-business infrastructures. By deploying PKI, an organization can implement stronger authentication and credential management for its site, which can in turn enable it to expose more sensitive applications and content.

The Oblix NetPoint Access System provides support for X.509 digital certificates, which users can present for authentication to a site. By using Oblix NetPoint in this way during the authentication stage, organizations can PKI-enable all of their Web-based applications without having to build PKI support into each one. As an added security measure, Oblix NetPoint allows digital certificates to be sent over SSL during the authentication phase, avoiding the risk of transmitting a user's certificate unsecured over the Internet.

In a PKI environment, a digital certificate has a fixed lifetime. However, a certificate may need to be revoked by an administrator if a user private key is compromised or if the administrator is no longer willing to support the certification (for example, because the holder of the private key terminated employment). Oblix NetPoint provides support for certificate revocation for all leading PKI vendors, enabling organizations to maintain security and control over access at all times. Oblix used ValiCert's Validator Toolkit to implement a NetPoint authentication plug-in that checks the validity of a user's digital certificate. Using the OCSP (Online Certificate Status Protocol) service, this toolkit enables applications to check the revocation status of a certificate in real time online.

Forms-Based Authentication

Practically every site needs to personalize and integrate the authentication step with the rest of its operation. Forms-based authentication allows organizations to employ a customized HTML form that requires users to enter their usernames and credentials (or other authentication information).

Every type of user and information resource in an e-business is different. That's why Oblix NetPoint supports multiple authentication levels for different Web and non-Web resources. In this way, administrators can protect different levels of the site according to their degree of sensitivity. If a user is cleared at a high level of access, he is automatically cleared to access less sensitive information as well. In the event a user tries to access information with higher security, Oblix NetPoint can challenge her by requiring additional credentials, or divert her to a predetermined URL for further processing.

For more secure applications and resources, Oblix NetPoint can support chained authentication—which requires users to perform multiple authentication processes through several methods before they can be authenticated.

Authorization Services

Once a user is authenticated, the system can then grant her permission to access various parts of the organization's environment (for example, Web and non-Web applications and resources such as EJBs, Web pages, or applications). Oblix NetPoint uses policy domains as the basic building block for protecting information or resources. A policy domain specifies a set of URLs that are to be protected together. An administrator creates a policy domain for a resource (such as customer information on a Web site), or set of resources, specifies a delegated policy administrator with the authority to control access to it, and specifies a default set of authentication, authorization, and audit rules that govern access to the resources within a policy domain. An administrator may then create policies within the policy domain to protect specific subsets of policy domain resources at a more granular level (also by specifying a set of authentication, authorization, and audit rules) and to specify the kinds of operations that can be performed on those resources. This is known as policy-based authorization.

One of the most powerful features of Oblix NetPoint security policies is its ability to extend the power of COREid group management to access control. Administrators may configure authorization rules to grant access based on a user's membership within a NetPoint COREid group (static, dynamic, nested, or hybrid), thereby providing a highly scalable and cost-effective role-based access control framework. Authorization rights may also be granted based on other parameters, such as static variables, user context, request context, or post data.

A unique feature provided by the NetPoint Access System is the Access Tester. This feature enables an administrator to find out which policies apply to a given resource (for example, by typing in an URL and seeing which policies are in effect for that resource and which users are granted or denied access). This capability is particularly helpful when policies are modified for a particular set of resources, and an administrator wants to check the effect of that change before making it active. This feature also helps determine who has access to a given resource.

Authorization policies can be extended to other services via the Access Server SDK (see p. 32). This SDK allows developers to flexibly define and manage authorizations rules within policies to be applied directly within their systems.

Oblix NetPoint Authorization Services deliver centralized, consistent management of policies across applications, while giving users granular access to Web and non-Web-based content and resources. This capability gives growing e-business organizations the control and consistency they require to secure sensitive information, while granting users easy access to the information and applications they need.

Auditing Services

Oblix NetPoint provides a comprehensive set of auditing and reporting functions, enabling organizations to perform security-level auditing of user access to resources, as well as business-level auditing and user profiling. Oblix NetPoint is the only solution on the market that logs both access activities (authentication, authorization, and policy changes) and identity management activities, as well as the user data associated with those activities. Companies can configure very precisely which activities they want to log and which identity data should be logged when a specific activity happens.

The NetPoint Access System logs and tracks all activities conducted by each person using the e-business network. This includes data on authentication, which URLs were used at what time, and other details. It also tracks any incorrect uses of resources, such as failed authentication attempts or uses of unauthorized resources—as well as an instances of policy modification.

As with all the components of the NetPoint Access System, administrators have flexible control over configuration, allowing them to tailor auditing and reporting to fit their business needs. Audit policies can be set on a per-resource basis to enable focused tracking of specific areas of the e-business environment. And audit output can be customized to include identity profile information when a specific activity happens.

The NetPoint COREid System also yields auditing and logging data that can be used in conjunction with the access logs for a consolidated approach to system monitoring. Oblix NetPoint logs and tracks all modifications, additions, and deletions made in the course of managing user identity, group, and organization information. Overall, the audit data provided by Oblix NetPoint constitutes an excellent, detailed source for e-business analysis.

Multi-Level Policy Delegation

Oblix NetPoint enables access policy administrative tasks to be delegated to trusted individuals at all levels throughout an organization so that these responsibilities can be distributed evenly and efficiently. Each administrator to whom privileges are delegated can further assign equal or lesser privileges to another administrator if he or she has been given the rights to do so. Organizations can carry on this delegation without limit to lower administrative costs, increase security, and enable real-time changes enterprisewide.

For example, whereas the Master Access Administrator of a company has complete authority over all access policies, she can delegate a subset of that responsibility to a Delegated Access Administrator in the sales department for any policies related to customers. Likewise, she can also empower a Delegated Access Administrator in the purchasing department to have authority over any supplier-related policies. The Delegated Access Administrator in the sales department can then choose to further delegate a subset of her privileges so that individual account managers in the sales department have authority over the access policies for all sales prospects in their respective regions. This delegation process can continue for an unlimited number of levels.

Oblix NetPoint is the only solution available that features this multi-level policy delegation. Its Web-based (thin-client) administration console can be run from anywhere a user can access a browser and can work across firewalls, since all communication is over HTTP. It also takes much less time to run and is immune to the security issues related to running Java applets over the Internet.

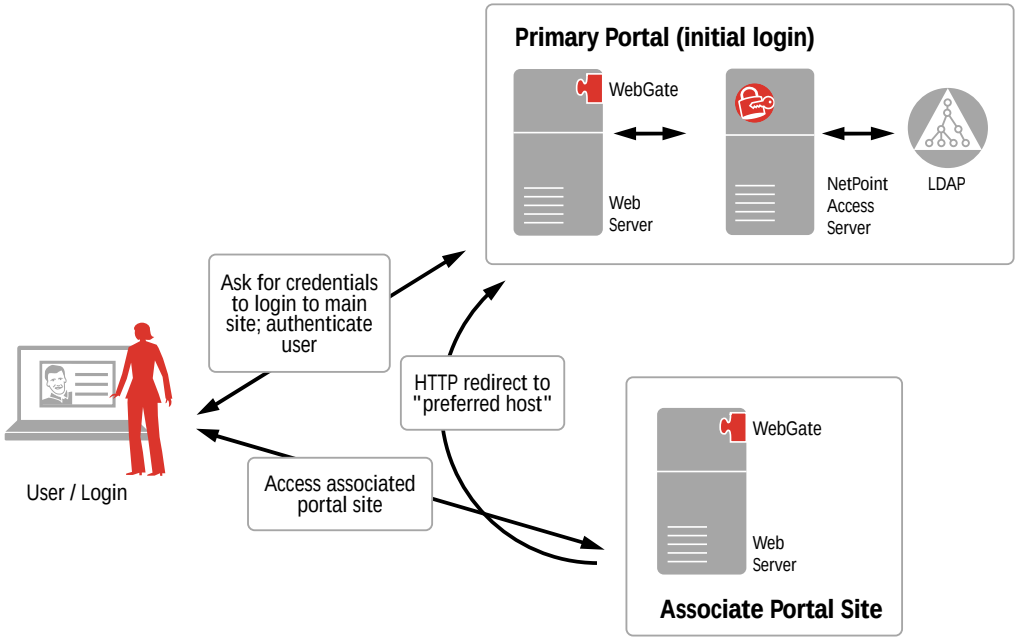
Federation Services™

NetPoint Federation Services addresses the problem of interoperation between loosely coupled security domains, each operating with different platforms and applications, and possibly even under the government of differing security infrastructures. Oblix NetPoint is the only solution of its kind that provides both full-featured identity management for within a given enterprise security domain, as well as interoperability between a NetPoint-secured domain and external security systems. This ability becomes important to corporations developing relationships with business partners or customers; they must be able to empower their constituents to easily and securely access one another's enterprise resources in order to facilitate that relationship.

NetPoint Federation Services are provided through **Associate Portal Services**™, the **NetPoint FEDERATEDid Layer**™, and through **NetPoint SAML Services**.

Associate Portal Services

As more organizations partner and merge with one another, the ability to present a cohesive Internet presence is key. For example, an online investment organization might want to link to the portals of its partners and subsidiaries that offer related services. This feature supports Web single sign-on across multiple associated portals and DNS domains, combining top security with ease-of-use for growing virtual organizations.



Associate Portal Services within NetPoint enable single sign-on across multiple DNS domains.

Associate Portal Services for multi-domain single sign-on is designed to accommodate a large number of partner/associate sites and is also well suited for exchanges. When using Associate Portal Services, administrators designate one Web site as the master site and the others as associate sites. When a user accesses a master site, she is authenticated there directly.

If she initially accesses an associate site, however, a WebGate installed at the associate site, called the associate WebGate, transparently redirects her request to the main site for authentication. This method requires no persistent connection between associate WebGates and the Access Server at the master site. All communication between associate WebGates and the Access Server at the master site is accomplished through redirection of the client browser. Because the WebGates at each of the associate sites operate as simplified "lightweight" versions of the full-blown WebGate (in that they only redirect access requests to a master site and thus do not require Access Server installed at the associate site), deployment of associate WebGates is simple – an installer need only know the URL of the master site.

In addition, associate sites can be placed on a "trusted associate domain site" list, so that once a user is authenticated to any one such site, she can access any other site on that list without further authentication. This ensures single sign-on across multiple domains.

FEDERATEDid Layer

The NetPoint FEDERATEDid Layer is an integration layer within the NetPoint Access System that allows NetPoint to integrate with other security or authentication systems. With the NetPoint FEDERATEDid Layer, the NetPoint Access System can accept an authentication token and perform authorization for that user. This allows both the NetPoint COREid and Access Systems to integrate and interoperated with multiple types of authentication or security systems. The NetPoint FEDERATEDid Layer can work with existing security or single sign-on systems and ensure support for future systems and standards such as Microsoft.NET Passport, Liberty Alliance, and Magic Carpet. Companies can extend the life of their existing systems and with NetPoint reduce the future risk.

Passport Authentication Plugin

Designed to sit on top of the NetPoint FEDERATEDid Layer, the Passport Authentication Plugin is a third party authentication agent that enables single sign-on between NetPoint-protected sites and Microsoft .NET Passport-protected sites. This agent is capable of receiving and passing Passport authentication tokens between NetPoint and the Microsoft .NET Passport Server.

This integration option provides some significant benefits to customers. Microsoft Passport is primarily a way of authenticating users on the internet, and focuses on providing single sign-on between internet websites. Oblix NetPoint is deployed within enterprises to secure, among other web resources, internet web sites for large enterprises. Therefore, if a large enterprise wishes to deploy Passport as a way of

authenticating users to their website, they can do so using the standard Passport toolkit and service. However, once a user is authenticated, the website still needs to authorize the user and secure access to the different web resources on the site. This is not provided by Passport, but is provided by Oblix NetPoint. The integration enables a seamless handoff between the Passport session and the Oblix NetPoint session.

NetPoint SAML Services

A standard developed by the OASIS Security Services Technical Committee (SSTC), SAML enables interoperability between security systems that provide authentication and authorization services. Oblix has taken an active role in closely driving the definition of SAML as a co-chair of the SSTC. Through this involvement, Oblix has produced an industry-leading integrated SAML solution in Oblix NetPoint.

Oblix NetPoint's SAML solution offers some significant benefits to customers. SAML itself provides an interoperable secure mechanism for passing credentials and other related information between Web sites with their own authentication and authorization system. With SAML, a transaction initiated at one site can be completed at a different site, through sharing of security information required to complete the transaction between two sites. These capabilities enable businesses to more easily and more securely interoperate with other entities, such as business partners and customers, using methods based on open industry standards.

Oblix NetPoint's SAML solution is differentiated from other solutions on the market by its pairing with the NetPoint COREid System, as well as by its ability to deliver single sign-on between SAML-enabled sites today. SAML solution owners need shared capabilities for maintaining accurate user information on all of the entities they exchange SAML assertions with. They should also have open capabilities for allowing external entities to self-register for SAML access. All of these capabilities are provided for through NetPoint COREid's self-registration, workflow, IdentityXML, attribute access control, dynamic groups, and granular delegated administration services. No other provider pairs an entire identity management framework with SAML capabilities complete with SAML-based single sign-on.

Let's take a look at how NetPoint SAML Services can help solve a real world business extranet problem. Consider a scenario in which a company wishes to provide a number of partner companies with access to one of its internal applications. This company, the host company, faces a number of challenges in trying to provide this access in a secure manner. How does it ensure the security of its application? Would this require that it manage partner identity information – for example, manage password resets and lost passwords, and keep partner identities up to date? If so, how can it do this in a scalable and cost-efficient manner? At the same time, partner companies want to avoid having their employees remember yet another login ID and password.

The NetPoint SAML Services meets all of these challenges by enabling the host company to establish a SAML trust relationship with each of its partners. For example, the host company and each of it partners can agree on a common identifier for each partner employee. Partner companies can then configure their corporate portal with a link to the hosted application. After partner employees successfully log in to their corporate portal, they click on that link, which initiates a SAML exchange with the host company. The common identifier is passed in SAML security assertions to create secure sessions for authenticated and authorized partner users. Using a common identifier to map users from each partner into the host company greatly reduces the ongoing administrative costs and help desk calls for the host company. In addition, the host company maintains complete control of the authorization policies that protect its highly sensitive information. Finally, the partner employees gain single sign-on access to the host application, thereby eliminating the need for yet another login ID and password.

The Oblix NetPoint SAML implementation provides the SOAP over HTTP binding of the SAML protocol, including Authentication, Attribute, and Authorization Decision Queries. These queries allow SAML-enabled applications to retrieve SAML assertions with information about subjects in a security domain protected by Oblix NetPoint.

Oblix NetPoint SAML Services also implements the Web SSO Browser/Artifact and Browser/POST profiles, which allow Web browser users to sign in to a Web site protected by one SAML-compliant security product and transfer to another Web site protected by a different SAML-compliant product, without having to sign in again. Oblix NetPoint can be used to protect either the originating site (the producer) or the receiving site (the consumer), or both.

Integration Services

Oblix NetPoint is the central identity infrastructure that binds all resources and users in an e-business network. It eliminates the inefficiencies of having multiple disconnected security and user stores for each application server, portal, personalization server, and legacy application. Oblix NetPoint is designed specifically to work in heterogeneous, mixed-vendor environments. With Oblix NetPoint, companies can take advantage of reusable security and identity services that can be leveraged across all applications and users.

By dedicating its own engineering resources and the expertise of partner organizations to the challenge of infrastructure integration, Oblix takes this burden away from its customers. The result is a fully integrated identity and Web access management solution built and tested to scale. Integration with security and application partners is critical to helping Oblix customers maintain and grow their e-business networks with consistently low ownership costs.

Oblix NetPoint provides a wide range of Web services, API, and other product components to facilitate seamless integration into a company's infrastructure. With these services, the reach of Oblix NetPoint is extensible into every critical point within an existing infrastructure—to applications, portals, provisioning systems, and back-end systems.

XML Services and API

These extensive APIs and XML Web-based services open up Oblix NetPoint to other parts of the infrastructure, accelerating Internet application development. They allow developers to leverage the capabilities of NetPoint across all their applications and e-business efforts, and extend the value of NetPoint by providing integration points with other vendors' systems and applications. Through these services, NetPoint can transparently call upon other parts of the organization for resources or information. Code samples are provided for NetPoint APIs on the product CD.

Authentication Plug-in API

This API allows custom or third-party authentication methods to be added, including Kerberos, RADIUS, and biometrics.

Authorization Plug-in API

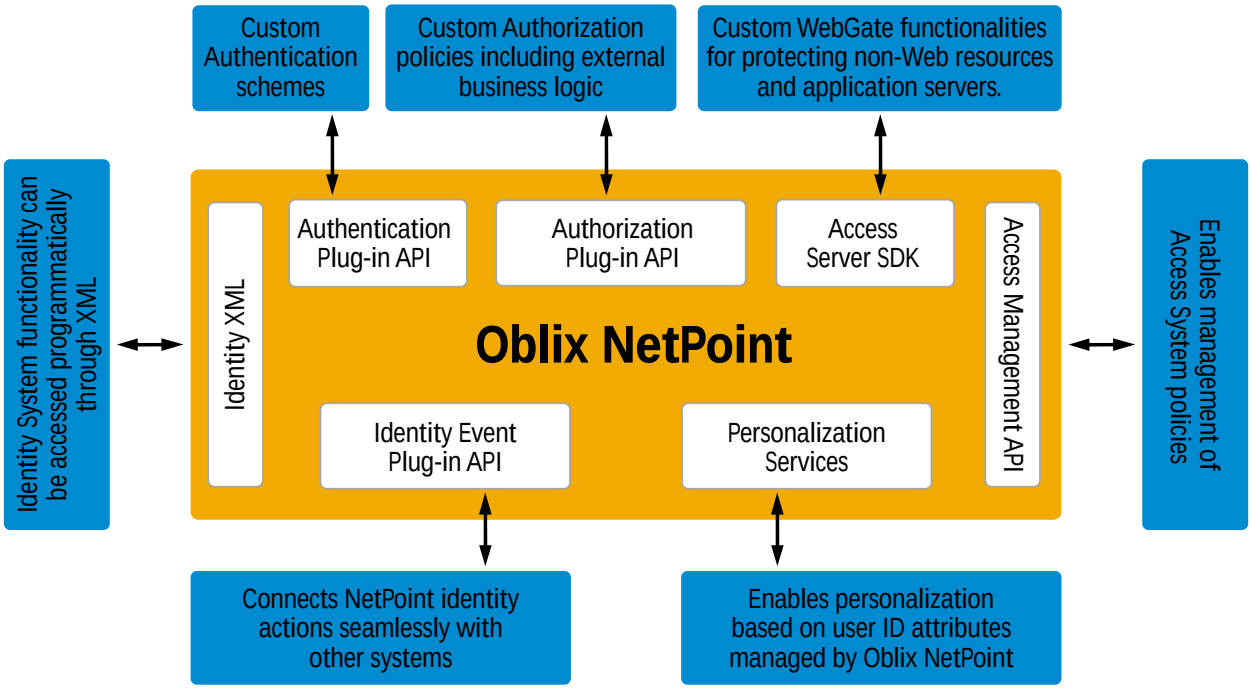
The server-side Authorization Plug-in API enables policy administrators to implement custom access control policies, thereby incorporating dynamic data from external business logic in the authorization process. For example, an administrator might set policies to allow a customer access to a particular set of resources if and only if her bank balance exceeded a certain amount. This bank balance could reside in a separate database or repository.

This API, which supports C and C++, lets companies create custom authorization modules based on an external program. The Authorization Plug-in API works by providing access to a custom shared library that policy administrators can define and that can accept or deny resource authorization requests.

Access Server SDK

The Access Server SDK enables Oblix NetPoint to function as a general-service policy engine, providing the same level of control over non-Web resources as is provided over Web resources. A benefit of NetPoint is that a single set of policies can be used to control access to all applications, regardless of the application platform, within the enterprise. NetPoint lets companies implement one set of policies that any application in the enterprise can leverage using the Java, C, C++, or COM+ Access Server APIs within the SDK.

The Access Server SDK enables e-businesses to create AccessGates that implement functionality equivalent to WebGates on any application/system that can use the API provided. AccessGate(s) can be created to protect non-HTTP resources – such as servlets or EJB methods on application servers or other servers– ASPs, JSPs, and even objects embedded within portal pages.



NetPoint Integration Services offer a variety of options for extending identity and access management functionality across an enterprise.

Access Management API

The Access Management API provides interfaces for the creation, modification or deletion of access policies, thus enabling external applications to manage Access System policy objects. Through the Java and C API, companies can reduce operating costs by automating the management of access policies, and extend the reach of policy management to the entire enterprise through the development of custom applications. For example, a document-management application may automatically create Access System policy objects for the protection of newly created documents or document directories through the Access Management API. Alternatively, a company may custom develop a GUI-based application for simplified assignment of user access to applications.

IdentityXML™

As a critical component of a company's e-business infrastructure, NetPoint is able to integrate with existing systems as well as to provide services that can be leveraged across other applications. IdentityXML allows applications and systems to easily access all the NetPoint COREid System functionality programmatically through XML. For example, with IdentityXML, the creation of a new user in an HRMS system can trigger an Oblix NetPoint workflow, or a portal/personalization product can use IdentityXML to find out whether a user is part of a particular group or organization.

Leveraging IdentityXML, all applications and systems can make use of NetPoint COREid System functionality without having to go through a Web browser. No other vendor in the marketplace offers XML integration for identity management. With this unique Web services architecture, Oblix NetPoint can serve as the centralized e-business hub for security and user identity management enterprisewide.

Applications and legacy systems that want to access or modify the centralized information that Oblix manages about users, groups, and organizations can do so relatively easily through XML, without having to write LDAP calls to access information for each system. The calls that NetPoint offers are not low-level APIs that require a lot of coding, but are well-defined points of entry into the NetPoint COREid System functionality. Oblix NetPoint leverages XML remote procedure calls to make requests, with SOAP as the transfer protocol.

Applications and systems coming across firewalls can access and modify data in LDAP. Without IdentityXML, organizations would have to expose their LDAP ports to outside applications, creating a significant security breach.

Identity Event Plug-in API

The powerful Identity Event Plug-in API allows companies to extend the business logic of the NetPoint COREid System by communicating with other systems before or after a COREid System event occurs. For example, when a new customer is created via NetPoint in the LDAP directory, the Identity Event Plug-in API can be used to communicate with a mainframe that automatically generates user IDs or an Oracle database that contains user account status. This information can then be inserted into identity attributes in order to determine the new user's access privileges. Companies can communicate with shared libraries, PERL scripts, or any other application that can be called from specific, well-defined points in the processing logic of Oblix NetPoint applications (both DLLs and executables).

The Identity Event Plug-in API can also be used to do data validation. For example, when used for password management, the Identity Event Plug-in API can check whether the password that the user submits meets specified criteria defined by the enterprise, such as a prohibition against using family names in a password.

This API can also be used to set default values. For example, all Gold suppliers could automatically be given pre-populated identity attributes upon creation through NetPoint. These auto-populated attributes would grant automatic access to certain applications or resources. Additionally, the Identity Event Plug-in API can be used as a notification engine that sends e-mail when a given action occurs.

This API gives organizations a unique flexibility to set up business logic and processes any way that they desire. As a result, Oblix NetPoint can offer the highest level of customization and extensibility available.

Portal Inserts

Organizations may wish to embed specific NetPoint functions within a portal site. Portal Inserts are embeddable URLs that reference different pieces of NetPoint COREid functionality. For example, a company can use Portal Inserts to embed the NetPoint Search function or Group Subscription function in a specific location, such as the upper-right corner of a portal. NetPoint Portal Inserts support dynamic navigation, allowing users to return to their originating application after using some piece of NetPoint COREid functionality.

With Portal Inserts, organizations can group functionality that should be exposed only to certain users without compromising performance by having to evaluate whether every portal user should see those functions or not. For example, functions that should be used only by administrators can be placed in a separate section of the portal rather than in a place all portal end users go.

Personalization Services

NetPoint enables personalization and Web single sign-on for other applications through HTTP header variables and redirection URLs. For example, it can be used for integration with portals. Whenever NetPoint authenticates or authorizes a user request, the HTTP response that it returns can contain HTTP header variables or redirection URLs for personalization purposes.

The HTTP header variables can contain any user data stored under the authenticated user's identity profile in the directory, delivering a rich source of information that the downstream application can decode and use for personalization.

Additionally, the NetPoint Access System can pass header variables to the NetPoint COREid System for dynamic style sheet customization. Based on who a user is, he or she can be presented with dynamic Identity System style sheets that have a different look and feel or customized content (see "PresentationXML", p. 21).

Application Server Integration

Tight integration between Oblix NetPoint and leading application and security servers simplifies network management and enables single sign-on and access control for applications. Oblix NetPoint provides deep out-of-the-box integration with the leading application server platforms, BEA WebLogic and IBM WebSphere, as well as single sign-on integration with the Oracle 9iAS application server framework. Oblix NetPoint also supports any J2EE standards-compliant application server, such as SunOne (formerly iPlanet) Application Server and others.

NetPoint Ready Realm™ for BEA and NetPoint Connector for WebSphere

The NetPoint Ready Realm for BEA and the NetPoint Connector for WebSphere are a custom realm and registry that allow native integration with the BEA WebLogic Server™ and the IBM WebSphere Server™, all without custom coding. These uniquely powerful and flexible implementations of the BEA custom realm and IBM custom

registry allow tight integration of Oblix NetPoint single sign-on and identity functionality to J2EE applications that utilize the BEA WebLogic and IBM WebSphere e-business platforms. These components allow WebLogic and WebSphere customers to transparently integrate applications, including the WebLogic Portal and WebSphere Portal, with Oblix NetPoint. Customers can now protect EJBs, JSPs, Servlets, CGI, HTML, on BEA WebLogic and IBM WebSphere with the enhanced management flexibility provided by Oblix NetPoint.

Customers can also create and manage security policies in Oblix NetPoint that include policies specific to BEA WebLogic and IBM WebSphere. The NetPoint Ready Realm for BEA and NetPoint Connector for WebSphere map application server users, acls, and permissions to security policies managed by Oblix NetPoint. This tight integration enables applications hosted on BEA WebLogic Servers and IBM WebSphere Servers to take full advantage of the COREid management features, including multi-level delegated administration, workflow, and managing user, group, and organizational access privileges.

Oblix NetPoint Mainframe Support

The NetPoint Mainframe Security Connector™ allows companies to integrate mainframe databases such as RACF, CA-ACF2, and CA-TopSecret into their e-business initiatives. This leverages the investments companies have in large mainframe systems for Web-based applications. It is still a fact that much of the core processing for the most critical applications at large companies are currently running on mainframe systems today.

The NetPoint Mainframe Security Connector, a joint effort between Oblix and Security Integration, Inc., offers a unique method of integrating existing RACF, CA-ACF2, CA-TSS security repositories with Oblix NetPoint. The Security Bridge product line from Security Integration makes the RACF, CA-ACF2, and CA-TopSecret databases available to authorized clients via the LDAP protocol. Oblix has integrated the Security Bridge product with Oblix NetPoint, delivering a tightly integrated productized solution. Using Oblix NetPoint's COREid and Access Systems, the NetPoint Mainframe Security Connector allows large corporations to integrate the vast intelligence buried within their OS/390 security repositories with their enterprisewide e-business security framework.

The NetPoint Mainframe Security Connector simulates e-business deployments by instantly integrating OS/390 users into a company's existing security environment. Administrators are able to create policies based on existing OS/390 security permissions, such as membership in RACF groups or access to CA-TopSecret profiles. This further reduces administrative time, improves customer responsiveness, and significantly reduces overall administrative costs.

When a user attempts to authenticate to Oblix NetPoint, the Access Server contacts the Security Bridge and passes the user's identity information for authentication. The user is then authenticated from the mainframe directory, and Oblix NetPoint sends an encrypted session cookie. Using the session cookie, Oblix NetPoint provides single sign-on capability to users stored in mainframe repositories as they navigate the Web across applications, servers, and other Internet domains.

NetPoint Security Connector features include:

- Seamless operation across all OS/390 security repositories (RACF, CA-ACF2, or CA-TSS)
- Out-of-the-box, full compatibility with all Oblix NetPoint functionality
- No requirement for a proprietary database (such as DB2)
- User authentication and policy administration management using information in mainframe databases
- Capability for applications to complete searches using the Mainframe Security Connector to OS/390 for selective content
- Easy loading and incremental updating of enterprise directories with information from the OS/390 security repositories
- Seamlessly sharing of information with any LDAP directory or LDAP-compatible application
- Availability of authentication and authorization services to other applications outside Oblix NetPoint that need to harness the intelligence in the OS/390 environment
- Robust, 24x7 high-volume performance
- Proven and patented technology
- Centralized policy management using existing host security repositories (RACF, CA-ACF2, or CA-TSS)
- Flexible administration using familiar user and resource structures
- Easy installation and deployment; enterprise and host directory communication support
- Full support for Web application requirements including password changes, searches, notifications, and more

Packaged Enterprise Management Application Integration

Packaged enterprise management applications have been developed to automate every key aspect of business operations in specific corporate areas, such as customer relationship management, human resources management, supply chain management, and so on. Oblix NetPoint features turn-key SSO integrations with products provided by leading vendors such as PeopleSoft, SAP, and Siebel.

Portal Integration

Intranet/extranet portals play an increasingly important role in opening access to business resources and back-end applications. Oblix NetPoint can create a common security and user model for disparate applications (including portals).

Portals are useful for delivering customized information to specific users. For example, based on the information a portal user enters about himself, a portal can personalize the Web pages delivered to him. Oblix NetPoint can set specific policies for specific resources. These policies can then direct NetPoint to pull specific user identity information from the directory server and send it via NetPoint Personalization Services (HTTP header variables) to the portal. This enables Oblix to supply granular information to the portal based on the policy, creating a more compelling and personal experience for the end user. Furthermore, Oblix allows single sign-on and Web access control to the portal and other applications found in an enterprise.

Oblix has partnered with a number of third-party vendors to facilitate intelligent portal and content/ personalization solutions, including BEA Portal, Plumtree Corporate Portal, SAP Portal, and Vignette Application Portal (formerly Epicentric Foundation Server), IBM WebSphere Portal, and Viador E-Portal.

Provisioning Solution Integration

True end-to-end identity management is achieved when enterprise identity events are automatically synchronized with appropriate Web access management and provisioning events. For example, when a new user is hired into a corporation, an end-to-end enterprise identity management system would not only establish the user's enterprise identity—it would also automatically provision this user with the various system accounts she needs to perform her job, as well as grant her the appropriate privileges to access the resources she needs. Designed for seamless integration into any corporate enterprise, including those with already-existing provisioning solutions, Oblix provides many options for NetPoint integration with provisioning solutions.

Oblix NetPoint provides extranet provisioning for most common LDAP directories. For some company extranets, this is all that is needed to provision accounts. For many other intranet environments, however, companies have many identity stores beyond a central LDAP directory. For example, it is not uncommon for corporate enterprises to have Microsoft Windows, a messaging system, a development platform like BEA, and applications from vendors such as Siebel and PeopleSoft. To address this more complex intranet provisioning problem, Oblix NetPoint integrates with a number of dedicated provisioning solutions.

Integration between Oblix NetPoint and most provisioning solutions is possible with many deployment options. Companies that choose to have NetPoint identity workflows drive provisioning events only need to make minor changes to the workflows. Companies who want the provisioning software to drive the provisioning experience have two options for integrating NetPoint with provisioning solutions. To kick off additional workflow processes, or to take advantage of other value-added NetPoint functionality, the provisioning product can call directly into Oblix NetPoint APIs. Or, if less functionality is required, the two products can synchronize their activities simply by polling the same directory server.

Oblix NetPoint also features the highest level of integration with CONTROL-SA® from BMC Software, in the form of Oblix IDLink™.

Oblix IDLink

Developed in partnership with leading provisioning solution provider BMC Software. Oblix IDLink provides out-of-the-box integration between Oblix NetPoint and BMC CONTROL-SA. With Oblix IDLink, NetPoint's identity workflows kick off corresponding BMC CONTROL-SA provisioning events using native BMC Job Codes. This solution supports both role-based (based on a single attribute) and rule-based (based on a combination of roles or a specific business rule) provisioning. Oblix IDLink is the first product of its kind on the market to provide complete out-of-the-box end-to-end enterprise identity management. For more information on Oblix IDLink, please reference the Oblix IDLink for BMC Software White Paper.

Infrastructure Design, Implementation, and Administration

Oblix NetPoint Architecture

Oblix NetPoint is designed to seamlessly integrate with existing infrastructures. Its scalable architecture enables an e-business to incrementally grow its Web infrastructure and build upon it. A complete set of APIs and XML Web-based services support emerging new third-party applications and standards, setting the stage for easy growth as an organization matures and faster time to market.

Three-Tier Design

Oblix NetPoint features a three-tier architecture for highly secure deployment. This architecture allows the COREid and Access Servers to be located outside the DMZ, ensuring that valuable data and applications receive maximum protection.

The NetPoint three-tier architecture also adds substantially more redundancy to the entire system, enabling organizations to set up a number of front-end Web servers to handle most of the load, thereby freeing the COREid and Access Servers to support multiple Web servers. The architecture also provides additional points in the system to perform failover and load-balancing.

Oblix NetPoint, built for enterprisewide deployments, is native on NT, Solaris, Windows 2000, and Windows Server 2003. This design delivers high performance, reliability, and scalability.

Reliability and Scalability Features

Complete end-to-end reliability and failover support throughout the Oblix NetPoint system enables NetPoint Access Servers, COREid Servers, and their underlying directory servers to automatically switch to other servers, ensuring continuous protection of mission-critical e-businesses.
Features include:

Failover support, enabling organizations to quickly restore the NetPoint system in the event of failure or data loss, saving critical time and money. NetPoint allows companies to specify primary and secondary servers for failover purposes. If a server is not available, another primary server will be brought up or, if none is available, a secondary server.

Smart restore, for automating continuous polling of unavailable NetPoint servers so that load can be restored to them once they have been restarted.

Weighted round-robin support, enabling administrators to set up Web servers in a round-robin configuration for added reliability and performance.

SMP (Symmetric Multiprocessing) optimization (performance optimization for multi-CPU architectures or machines), for increased reliability and high performance.

Replicated directory support, enabling directories with stored identity and policy information to be replicated throughout the virtual organization for improved performance and accurate information.

NetPoint System monitoring, for continuous monitoring of all NetPoint components.

Multi-Level Caching Support

Oblix NetPoint supports caching throughout every component of its architecture, thereby preserving overall performance for end users even as deployments grow. Each component of Oblix NetPoint includes a built-in cache for recent authentications and authorizations. Having this user information available at the Web-server level obviates the need for a trip to the server for each request.

SSL Communication

Oblix NetPoint supports SSL communication among all its components. This substantially increases the security of the product not only externally but also internally. Data communicated between the directory server, the Access Server, COREid Server, WebGate, WebPass, and Certificate Processing Servers are constantly protected and never left in the clear.

Connection Pooling

Oblix NetPoint supports connection pooling between clients and servers to maintain and optimize persistent or virtually persistent connections. Connection pooling to a directory server involves opening a "pool" of threads or connections rather than having to set up a separate connection for each request. This eliminates the overhead of having to set up connections that require a protocol handshake and helps to eliminate bottlenecks. NetPoint supports connection pooling from WebGates to Access Servers, WebPasses to COREid Servers, and from Access/COREid Servers to back-end directories.

Standards Compliance

Oblix NetPoint complies with current and emerging industry standards, which assures maximum interoperability with existing systems as well as adaptability to future infrastructure needs. This promotes faster deployments today and greater investment protection in the long run.

Key standards of compliance include:

- **LDAP**
- **OCSP**
- **SSL**
- **SOAP**
- **ADSO**
- **SAML**

Oblix also actively participates in the World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF), and actively drives the definition of the SSTC SAML standard

Locale Ready

Oblix recognizes the challenges in trying to extend the reach of enterprise products to employees, partners, and other constituents around the world. NetPoint features localized product versions in languages such as English, French and German, enabling global companies to implement common directories in support of multiple languages.

Directory and Third Party Security Systems Integration

Oblix NetPoint is designed to integrate with a wide variety of third-party authentication and security applications and directory servers, so that companies can leverage their existing security infrastructure.

Security and Intrusion Detection Systems

Oblix NetPoint integrates with a variety of third-party authentication and security applications, so that companies can continue to leverage their legacy systems to keep security management costs low. For example, NetPoint is SecurID- and Keon-certified by RSA. Oblix NetPoint also supports Valicert's Online Certificate Status Protocol (OCSP) for CRL checking (for certificate authentication). Furthermore, NetPoint's extensive logs can be integrated with products from ISS, Counterpane and ArcSight to offer real-time intrusion detection.

Reporting Tools

Integration with reporting tools gives e-business leaders the ability to monitor security as well as to understand site usage. For instance, once an e-business site is up and running, an organization can request reports on who is accessing which specific resource. By default, Oblix NetPoint records full user information into its audit logs, and is configurable to include any type of user information from the directory server, as well as detailed information on authentication, authorization actions, and identity changes.

NetPoint is fully compatible with leading reporting tools from vendors such as the WebTrends, and can be integrated with any reporting tool capable of reading a simple flat log file. Organizations with reporting tools already in place can simply point the server to accept NetPoint log files. In addition, NetPoint provides a number of pre-configured system reports that may be exported in .CSV (Comma Separated Value) format.

Included with Oblix NetPoint is a standalone Database Sync Utility. This valuable tool takes NetPoint log files and assembles them into a single log file, simplifying reporting and analysis. A log file of access and identity information is created for each NetPoint Access Server protecting a network. If multiple Access Servers are running in a distributed environment, then multiple log files are created. Likewise, information processed by the COREid Servers can also be logged with the corresponding identity attributes that are customer specified.

The Database Sync Utility aggregates these log files. Once consolidated, intrusion detection tools can be used to monitor the log files in efforts to identify access patterns across the entire distributed system. This increases overall security and simplifies management. The log files can also be used in conjunction with business reporting tools.

Real-Time Monitoring Tools

With Oblix NetPoint, a company is equipped to secure and expose mission-critical business applications on the Web. However, as a company exposes more and more applications, it needs real-time, around-the-clock assurance that its e-business is safely up and running. Therefore, Oblix NetPoint is designed to be fully compatible with real-time monitoring tools, such as:

- **Resonate Central Dispatch**
- **Resonate Commander/Control Modules**

Resonate Central Dispatch is a tool that monitors the health and availability of NetPoint components: Access Servers, WebGates, COREid Servers, WebPasses, as well as Web servers on which WebGates and WebPasses run. Companies can view capacity utilization and other server metrics through a Central Dispatch console, ensuring that Oblix NetPoint is a high-availability system.

Directory Servers

Directory services provide the cornerstone of e-business strategies: a standard means of looking up and storing information that can be extracted by other applications. Furthermore, security infrastructures such as PKI leverage LDAP-based directories.

Oblix NetPoint supports the following directory servers:

- **Sun ONE Directory Server** (formerly iPlanet Directory Server)
- **Microsoft Active Directory and Windows 2000**, including multi-domain and ADSI support
- **Critical Path InJoin Directory Server**
- **Novell NDS eDirectory**
- **IBM SecureWay**

Please visit our Web site at www.oblix.com/platforms to get details on the latest supported platforms for Oblix NetPoint.

Deployment

To speed the deployment of integrated infrastructures, Oblix NetPoint comes equipped with a range of flexible configuration and deployment options.

Directory Schema and Object Classes

Oblix NetPoint provides support for distributed directory topologies—master/slave and multi-mastered replication—as well as various directory deployment models, such as specific DIT structures and existing schema. All Oblix NetPoint functionality works with both flat and branchy trees.

NetPoint works with any directory schema that a company has set up for maximum flexibility. It dynamically detects an existing schema and does not presuppose any specific object classes or attributes. If a company makes any schema changes, NetPoint is also able to detect them and include those object classes or attributes for use.

Oblix NetPoint also supports any existing or future auxiliary object classes that may be added. Auxiliary class support provides great flexibility in the way an organization may arrange its data. Directory servers support the notion of auxiliary classes, which allow new object classes to be added to the end of existing ones. Auxiliary object classes add data for other applications using the directory server. NetPoint allows companies to manage the attributes in those auxiliary classes.

Productized User Identity, Group, and Organization Management

For faster deployments, NetPoint features productized user identity, group, and organization management, rather than templates. In fact, the NetPoint Installer provides the option for automatic configuration of user and group objects into the LDAP directory for fast initial install. This enables an e-business network to get up and running faster without losing any flexibility. COREid User Manager, Group Manager, and Organization Manager have creation, deletion, and modification functionality that are completely customizable and configurable.

Virtual Host IDs

For each given server, that the Access System is protecting, NetPoint has the ability to process different host IDs, called Virtual Host IDs. This feature is useful in a variety of situations:

- When a company has many different host names for a given server. In this case, each host name can have a set of policies associated with it. Depending on which host name the user uses to access the server resources, different policies will be invoked. If a company would like to have one set of policies and not maintain different policies for different Virtual Host IDs, a Preferred Host name can be set. Using this approach, Virtual Host IDs for the same server will first be translated to the Preferred Host name, and the single set of policies associated with that Preferred Host name will be applied.

- When servers, typically in a server farm configuration, have similar directory structures that need to be protected. For example, if the same /gif directory on both Server 1 and Server 2 needs to be protected, the Virtual Host ID feature can enable its protection through just one policy.

In such a case, Server 1 and Server 2 can be configured as Virtual Host IDs for a virtual server and both share one set of policies.

Installation, Configuration, and Administration

Because Oblix recognizes that fast return-on-investment remains of utmost importance to its customers, NetPoint is built for fast installation and deployment, and intuitive system configuration and administration. NetPoint is replete with GUI-based applications and tools that abstract complex system life-cycle management tasks to the highest level. Its installation, configuration, administration and deployment applications and tools provide attribute validation and dependency checking, as well as sophisticated error-handling capabilities.

The NetPoint Installer

Built upon industry-standard InstallShield platform, the NetPoint Installer features separately packaged components for maximum installation flexibility. For truly fast installation and deployment, the Installer also provides the option to load basic productized user and group object instances, as well as simple delegated administration and attribute access configurations—all of which may be customized or modified after initial system install. In addition, NetPoint provides tools for multi-server installs, system maintenance, and the application of patches without system uninstall/reinstall.

The NetPoint System Consoles

To provide the most effective administration, configuration and management of an organization's infrastructure, the NetPoint Access System Console and the NetPoint COREid System Console provide single, integrated points of control for each of the NetPoint systems. User's can access these Web-based thin clients from any location, even through firewalls.

Organizations are free to specify the most appropriate administrator for each system, which helps ensure that those who are most knowledgeable about the users manage their information, policies, and resource needs. Administrator access privileges are not rigid, enabling organizations to specify and delegate access privileges in the ways that best suit them. System managers can decide which roles and grouping of privileges make sense for their organization; the roles below are samples.

NetPoint Administrator

A NetPoint Administrator can handle the following tasks:

- Managing the installation and general configuration of the Identity System and Access System
- Managing both the Identity and Access Systems, including functions such as managing logs and audit settings
- Creating Master Access Administrators and Master Identity Administrators

Master Identity Administrator

The Master Identity Administrator can have responsibility for the following:

- Setting up and configuring COREid Servers
- Setting up and configuring WebPasses
- Defining and configuring identity attributes
- Configuring workflow definitions, delegated administration, attribute access control for each identity attribute, search base, group expansion, container limits, and who can monitor workflow
- Assigning Delegated Identity Administrators throughout internal and external user communities

Master Access Administrator

The Master Access Administrator can take charge of the following responsibilities:

- Setting up and configuring Access Servers
- Setting up and configuring WebGates
- Setting up the different authentication schemes to use
- Setting up the basic policy domains (based on the resources being protected)
- Assigning the Delegated Policy Administrators to manage specific policy domains

Delegated Identity Administrator

Delegated Identity Administrators can be assigned most of the same responsibilities as the Master Identity Administrator, handling user identity attributes and access for smaller portions of the virtual organization and lesser responsibilities.

Delegated Access Administrator

A Master Access Administrator can assign responsibilities to a Delegated Access Administrator, enabling him or her to create and manage security policies for specified resources (such as all the supplier applications related to an organization).

Oblix NetPoint Benefits

Designed to integrate seamlessly with a company's existing applications, systems, and processes, Oblix NetPoint delivers the essential identity and Web access management infrastructure required for today's challenging e-business models. COREid—Oblix's unique approach to identity management—allows a company to dynamically manage identity information about each individual user, group of users, or organization profiled in its e-business network. The NetPoint COREid System puts digital identity at the center of an e-business environment. The result is a flexible and secure infrastructure that can include a maximum number of people while being managed with minimal costs.

The business benefits offered by NetPoint are substantial—and measurable—for organizations building and managing a dynamic e-business.

Rapid Return on Investment

By eliminating the manual tasks of maintaining individual user information, Oblix NetPoint dramatically reduces IT staffing costs. With the system's unique sophisticated group management capabilities, critical identity data and access privileges for huge user populations are kept up-to-date in real time using fewer resources.

Administrative workloads that once created costly IT bottlenecks are automated—and distributed throughout the broad e-business environment. No other Web access management solution has a completely integrated workflow engine driving this automation. Because NetPoint's multi-level delegated administration lets the people closest to user information assume responsibility for its management, organizations are able to expand e-business networks without incurring heavy operational expenses. And business rules can be applied consistently throughout a growing network since one definitive set of identity information and policies implements the rules throughout the enterprise.

Stronger Security

Oblix NetPoint's rich functionality distinguishes it as the most secure Web access management solution available. Its robust COREid and Access Systems let companies rapidly and consistently manage changes in identity and policy information—eliminating latency that creates dangerous security holes.

A unifying point within an Internet infrastructure, Oblix NetPoint makes it possible for e-businesses to proliferate security-based policies to all corners of their growing networks: applications, portals, and back-end system tools. Only Oblix NetPoint enables attribute-level access control, enabling organizations to develop and apply security policies that directly map to business rules. Plus, with Oblix NetPoint, organizations also have the flexibility to apply security policies for granular protection of applications based on security need.

The same strong security offered by NetPoint within an enterprise is extensible beyond enterprise boundaries through NetPoint Federation Services, thereby enabling secure collaboration between partners, customers, and other business constituents.

Greater Scalability

Oblix NetPoint was designed for large enterprises planning extensive growth of their e-business operations. Features such as NetPoint's delegated identity administration mean that corporations need not scale their IT organizations directly with the number of its employees, yielding valuable economies of scale.

Designed with extensive caching and built-in fail-over features, Oblix NetPoint provides a highly secure, reliable, and scalable deployment. Not only does Oblix NetPoint deliver the highest performance in single sign-on log-ins per second, the NetPoint COREid System is designed to scale corporate boundaries. This is particularly important for high-capacity extranets.

Finally, through its numerous integration options, NetPoint ensures that current enterprise technology investments are well protected, and that future enabling investments can be easily integrated into the environment.

Conclusion

Together, the components of Oblix NetPoint add up to a comprehensive Web access management solution that can not only integrate with an existing network but also adapt and scale to meet emerging business needs. With the most sophisticated identity management functionality and the highest performance on the market, it delivers the only identity infrastructure able to power e-business for immediate gain and long-term success.