Oracle® COREid
Access and Identity

Introduction to NetPoint

10*g* Release 2 (10.1.2)
Part No. B19006-01

May 2005

Copyright © 1996-2005, Oracle. All rights reserved. US Patent Numbers 6,539,379; 6,675,261; 6,782,379; 6,816,871.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle COREid Access and Identity products includes RSA BSAFE™ cryptographic or security protocol software from RSA Security. Copyright © 2003 RSA Security Inc. All rights reserved. RSA and RC4 are trademarks of RSA Data Security. Portions of Oracle Internet Directory have been licensed by Oracle Corporation from RSA Data Security. This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999-2003 The Apache Software Foundation. All rights reserved. Copyright © 2003 The Apache Software Foundation.

This program contains third-party code from Apache. Under the terms of the Apache Software License, Oracle is required to provide the following notices. Note, however, that the Oracle program license that accompanied this product determines your right to use the Oracle program, including the Apache software, and the terms contained in the following notices do not change those rights. Notwithstanding anything to the contrary in the Oracle program license, the Apache software is provided by Oracle "AS IS" and without warranty or support of any kind from Oracle or Apache.

* The Apache Software License, Version 1.1
 *
 * Copyright (c) 2000 The Apache Software Foundation. All rights
 * reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *   notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *   notice, this list of conditions and the following disclaimer in
 *   the documentation and/or other materials provided with the
 *   distribution.
 *
 * 3. The end-user documentation included with the redistribution,
 *   if any, must include the following acknowledgment:
 *   "This product includes software developed by the
 *   Apache Software Foundation (http://www.apache.org/)."
 *   Alternately, this acknowledgment may appear in the software itself,
 *   if and wherever such third-party acknowledgments normally appear.

```
* 4. The names "Apache" and "Apache Software Foundation" must
 *    not be used to endorse or promote products derived from this
 *    software without prior written permission. For written
 *    permission, please contact apache@apache.org.
 *
 * 5. Products derived from this software may not be called "Apache",
 *    nor may "Apache" appear in their name, without prior written
 *    permission of the Apache Software Foundation.
 *
 * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED
 * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
 * DISCLAIMED.  IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
 * LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
 * USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
 * ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
 * OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
 * OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 * ====================================================================
 *
 * This software consists of voluntary contributions made by many
 * individuals on behalf of the Apache Software Foundation.  For more
 * information on the Apache Software Foundation, please see
 * <http://www.apache.org/>.
 *
 * Portions of this software are based upon public domain software
 * originally written at the National Center for Supercomputing Applications,
 * University of Illinois, Urbana-Champaign.
 */
```

Fax:408/861-6810
Web:http://www.Oblix.com

Contents

Preface

This *Introduction to COREid* provides an introduction to COREid and a road map to COREid manuals that introduces their content, audiences, and prerequisites. The COREid glossary is included with this manual for your quick reference.

Note: Oracle *COREid* was previously known as Oblix *Netpoint*. All legacy references to Oblix and NetPoint, for example, in screen shots, illustrations, and documentation titles, should be understood to refer to Oracle and COREid, respectively.

This Preface covers the following topics:

- "Intended Audience" on page 9
- "COREid Documentation" on page 9
- "Typographical Conventions" on page 10
- "Contact Information" on page 11

Intended Audience

This guide is intended for anyone who is interested in an introduction to COREid, COREid terminology, and the COREid manuals.

COREid Documentation

The manuals that are available for this release include:

Introduction to COREid—Provides an introduction to COREid, a road map to COREid manuals, and a COREid glossary of terms.

COREid Release Notes—Provides up-to-the minute details about the latest COREid release.

COREid Installation Guide—Explains how to install and configure the COREid components.

COREid Upgrade Guide—Explains how to upgrade earlier versions of COREid to the latest version of COREid.

COREid Administration Guide—Explains how to configure COREid applications to display information stored in the directory, how to assign view and modify permissions for data displayed on the COREid applications, and how to assign access controls to users.

COREid Deployment Guide—Provides information for people who plan and manage the environment in which COREid runs. This guide covers capacity planning, system tuning, failover, load balancing, caching, and migration planning.

COREid Customization Guide—Explains how to change the appearance of COREid applications and how to control COREid by making changes to operating systems, Web servers, directory servers, directory content, or by connecting CGI files or JavaScripts to COREid screens. This guide also describes the Access Server API and the Authorization and Authentication Plug-in APIs.

COREid Developer Guide—Explains how to create AccessGates and how to develop plug-ins. This guide also provides information to be aware of when creating CGI files or JavaScripts for COREid.

COREid Integration Guide—Explains how to set up COREid to run with third-party products such as BEA WebLogic, the Plumtree portal, and IBM Websphere.

COREid Schema Description—Provides details about the COREid schema.

Online Help is available from each COREid screen.

Typographical Conventions

COREid manuals use the following typographical conventions:

- When you are instructed to select elements sequentially, the actions are separated with angle brackets, as shown below:

  Click System Admin > System Configuration > View Server Settings.

- Paths to a file are shown using syntax for either the Unix or Windows platform:

  /*COREid_install_dir*/identity/oblix/logs/debugfile.lst
  \COREid_install_dir\\identity\\oblix\\logs\\debugfile.lst

  where *COREid_install_dir* refers to the directory where the component, in this case, the COREid Server, is installed.

Contact Information

For a list of contacts including corporate offices world wide, sales, and other details, visit the Oracle Web site at:

```
http://www.oracle.com
```

You can contact Oracle with questions or comments as follows:

Customer Care—http://www.oracle.com/support/contact.html

Corporate Headquarters

Oracle maintains offices world wide. Oracle corporate headquarters is located at:

500 Oracle Parkway
Redwood Shores, CA 94065
Phone: (650) 506-7000

Before Contacting Customer Care

Before contacting Customer Care, please have available the following:

- Oracle product name and version number
- Type of computer and operating system you are using

Accessing the Customer Care Knowledge Base

For more information about using COREid, see the Oracle Customer Care Knowledge Base. To access the Knowledge Base, you need a login name and password, which you can obtain from your Oracle sales representative.

To access the Knowledge Base:

1. Enter the following URL in your browser and press Return.

   ```
   http://www.oracle.com/support/contact.html
   ```

2. Click the phrase, Login to the Oracle PremiumCare Online Portal.
3. Enter your user name and password in the box that appears, then click Login.
4. Under Oracle Support Tools, click Case Manager.
5. In the next screen, click Find Answers to gain access to the Knowledge Base.

1 NetPoint Introduction

This chapter provides an overview of Oblix NetPoint® product suite and includes the following topics:

About Oblix NetPoint

The Oblix NetPoint® product solves the problem of how to manage a business over the Internet. While the NetPoint name is changing to COREid™, in manuals and within the product itself you will see the name NetPoint. NetPoint SAML Services have been renamed to SHAREid. See the Oblix *SHAREid Administration Guide*.

Using NetPoint, you can integrate business applications and apply the Internet to critical business systems to drive down costs and increase customer satisfaction. NetPoint provides centralized identity management products for user management, account provisioning, and Web single sign-on (SSO) that help you:

- Facilitate delivery of corporate functions to extended groups of employees, customers, partners, and suppliers
- Maintain a high level of security across applications
- Enable users and business partners to access information

For example, suppose that your internal users, your suppliers, and your customers require access to unique data sets. In addition, suppose that you also have common data that everyone should see. Using NetPoint, your identity-based policies can provide the right levels of access to each group while ensuring that everyone can securely access only the data that they need and that they have the right to access.

Automated bank tellers (ATMs) provide a useful analogy for the NetPoint solution. At one time, people had to conduct bank transactions in person. With the advent of ATM technology, banks could move to a self-service model for most transactions. Similarly, NetPoint enables you to move away from a centralized administration model to a distributed model where you provide data and applications securely over the Internet.

NetPoint enables you to change your business from a perimeter defense model in which you unilaterally block outside access to your resources to a security model based on business rules. Using NetPoint, you can securely provide business systems and data to employees, customers, and suppliers.

NetPoint offers a DMZ-type three-tier architecture to provide a highly secure deployment with maximum protection of data and applications. NetPoint includes an enterprise identity-management system known as the COREid™ System (to become COREid Identity System), an access-control system known as the Access System™ (to become COREid Access System), and NetPoint Federation Services™ (SHAREid™).

The Web-based interface provides a single point of entry, the NetPoint System Console, which enables administrators to assign and delegate administrative responsibilities and manage the appearance and behavior of NetPoint components and applications.

The NetPoint Administrator is a super user, empowered to configure the NetPoint deployment and assign administrative tasks. The NetPoint Administrator is assigned when NetPoint is initially installed and set up. Using the NetPoint System Console, the NetPoint Administrator can create additional NetPoint Administrators, Master Identity Administrators, and Master Access Administrators.

NetPoint identity management allows simple information gathering and self-service functions for end users, such as the ability to:

- Search for and view other users and groups, depending on the rights granted to them by an administrator.
- Modify personal information such as phone numbers and passwords.
- Display organizational information such as floor plans and asset lists.

In addition, NetPoint access control, customization, and XML-based integration features provide you with control over what applications users can see and what functions they can perform.

Examples of NetPoint Use

Using NetPoint, it is possible to manage a corporate portal that is open to external business partners. For instance, for a portal that allows customers to order manufacturing materials and equipment, all applications exposed through the portal are protected with one platform, NetPoint, which grants access rights. Administration of the access policies protecting these resources can be delegated throughout the corporation so that business units, rather than the IT department, make decisions about the customers, suppliers, and partners who are to be given access rights. This is possible even for companies with billions of dollars of revenue and tens of thousands of employees.

Using NetPoint, it is also possible to grant different types of privileges to different classes of users. For instance, a health-care organization can manage its data so that different groups can view different kinds of data, as follows:

- Health-care plan members can view their health-care information.
- Companies providing health-care services to their employees can manage their health-care plans.
- Doctors and hospitals can view patient information.

Finally, an organization can use NetPoint to aggregate application accounts. For example, financial institutions can configure self-service portals to allow their customers to access different accounts from a single login, including online banking, mortgage information, and insurance.

Key Features

Figure 1 outlines several key features of NetPoint.

Figure 1 Features and Benefits of the COREid and Access System

NetPoint COREid System	
Features	Benefits
• **Centralized user management** • **Self-service** • **Delegated administration** • **Identity workflow** • **Password management** • **Group management** • **Organization management** • **User interface customization**	• **Lowered cost of administration through delegated administration and self-service (for instance, self-service password management)** • **Security driven by user identity-based access privileges** • **Improved user experience through real-time change management**

NetPoint Access System	
Features	Benefits
• **Single sign-on** • **Authentication** • **Authorization** • **Auditing** • **Personalization** • **Security administration**	• **Improved user experience by eliminating multiple logins** • **Centralized policy management** • **Granular control over security across heterogeneous applications and systems** • **Strong security**

In addition to the items above, the COREid Data Management Layer (also known as COREid Data Anywhere) aggregates and consolidates data from RDBMS and LDAP directories into a virtual LDAP tree.

For more information about NetPoint features, see:

- “NetPoint COREid System Features” on page 17
- “NetPoint Access System Features” on page 18
- “NetPoint External Authentication Features” on page 20
- “NetPoint Enhancements” on page 21

NetPoint COREid System Features

The NetPoint COREid identity management system is both powerful and flexible. Benefits of the NetPoint COREid System include a lowered cost of administration through delegated administration and self-service, and an improved user experience through real-time change management.

For example, you can create, manage, and delete groups in the directory server. You can define a subscription policy for a group, including self-service with no approval needed, subscription with approval(s), rule-based subscription, and no subscription allowed.

Using the COREid System, you can build application account provisioning, password management, and other functions on top of the identity management system. You can integrate other applications with the primary NetPoint components using a single identity management system so that, when an employee leaves an organization, access cards, computer accounts, and payroll functions can all be modified from one identity change function.

Key COREid System features include:

- **Centralized User, Group, and Organization (object) Management**—Allows you to provide different access policies for different people and groups and to manage organizational entities, such as assets and maps. Information in the COREid System can then be leveraged by the NetPoint Access System to manage access privileges based on user attributes, group membership, or association with an organizational entity.
- **Dynamic Role-Based Identity Administration**—Provides security driven by user identity-based access privileges. For example, a role may include all users or all managers or direct-reports only, and so on.
- **A Customizable Multi-Step Identity Workflow Engine**—Allows you to map and automate business processes, policies, and approvals relating to identity data. For example, you can model your business processes in NetPoint using workflows to:
    - Create, delete, and modify users, groups, and organizations.
    - Implement self-registration of users and organizations.
    - Issue, revoke, and renew certificates.
    - Subscribe and unsubscribe to groups.
- **Multi-Level Delegation of Identity Administration**—Allows you to scale up to millions of users by delegating NetPoint administration. Administrators can delegate all or some of the rights they have been granted, and they can choose whether or not to allow their delegates to pass these rights on to others. The tasks that are delegated are specific to the right, the target, and the tree path.

- **COREid Data Management Layer**—Aggregates and consolidates data from RDBMS and LDAP directories into a virtual LDAP tree that can be managed by the NetPoint COREid System and used to support authentication and authorization using the NetPoint Access System. This feature is also known as COREid Data Anywhere and is available only when you integrate NetPoint with the OctetString Virtual Directory Engine (VDE). For complete details, see the *NetPoint Integration Guide*.
- **Password Management Services**—Provides comprehensive password management services that enable you to specify multiple password policies, constraints on password composition, a configurable password validity period and notification, forced password change, lost password management setup, and password creation/change rules.
- **Self-Service**—Allows you to implement a secure self-service model for organizational functions such as password change. Users with self-service permissions can manage their own information without the use of a workflow.
- **Self-Registration**—Enables limited access to your system through the initiation and processing of a self-registration workflow.

  For example, you can set up a self-registration workflow such that when a user self-registers, the registration request is forwarded to appropriate people for approval, and upon approval, the user is immediately and automatically granted access to all appropriate resources based on his or her identity attributes.
- **User Interface Customization**—Allows you to change the appearance of NetPoint applications, control how NetPoint operates, and connect CGI files or JavaScripts to NetPoint screens.
- **Extensive APIs for Identity Integration**—Allows you to gain access and interact with NetPoint without using a browser and implement functions and executables triggered by events within NetPoint.

For more information and a sample COREid System installation, see “About the NetPoint COREid System” on page 23.

NetPoint Access System Features

The NetPoint Access System is an optional companion to the COREid System that provides centralized authentication, authorization, and auditing to enable single sign-on and secure access control across enterprise resources. Resources include content, applications, services, objects in applications on the Web, and similar types of data in non-Web (non-HTTP) resources.

The Access System stores information about configuration settings and security policies that control access to resources in a directory server that uses Oblix-specific object classes. You can use the same directory to store the Access System configuration settings, access policy data, and the COREid user data, or you can store this data on separate directory servers.

The NetPoint Access System protects Web resources and enterprise resources such as J2EE applications, servlets, Enterprise Java Beans (EJBs), and legacy systems. NetPoint supports both Web (HTTP) and similar types of data in non-Web (non-HTTP) resources.

Using the NetPoint Access System for security administration:

- Enforces your company’s access security policies for Web applications and content.
- Provides common security measures across multiple Web servers and applications.
- Combines centralized policy creation with decentralized management and enforcement.
- Enables granular control over security across heterogeneous applications and systems.

Key NetPoint Access System features include:

- **Authentication, Authorization, and Auditing**—These services enforce your company’s access security policies for Web applications and content through policy-based authentication, authorization, and auditing.
    - **Authentication Services**—NetPoint authentication services provide a generalized means to authenticate users and systems when they try to access resources protected by NetPoint. These services support both the basic username and password authentication method as well as stronger methods such as digital certificates or SecurID cards.

      You can further expand the authentication capabilities with the NetPoint Authentication Plug-in API. Once a user is authenticated by the authentication services, NetPoint creates a single-sign-on session for the client that frees the user from having to sign on again to access other resources or applications.
    - **Authorization Services**—NetPoint authorization services deliver centralized, consistent management of policies across applications, while providing users granular access to Web-based content and resources. You can secure sensitive information while helping ensure that users and systems have the easy access they need.
    - **Auditing Services**—NetPoint auditing services provide flexible and detailed reporting, auditing, and logging of events in the Access System and

COREid System. The auditing and log files enable you to perform threat and intrusion detection, security monitoring, and business-level reporting by integrating with third party products.

- **Personalization Services**—NetPoint enables personalization for other applications through HTTP header variables and redirection URLs. When NetPoint authenticates and/or authorizes user requests, the URL it returns can contain HTTP header variables which in turn can contain any user data stored under the authenticated user's ID in the directory.

  The downstream application can decode this information and use it to personalize the user experience. You can include a redirection URL in the URL returned by NetPoint, which may take the user to another Web page tailored to the identity of the user.

- **Single Sign-On**—This enables users and groups of users to access multiple applications after a single login and authentication, which improves the user experience by eliminating multiple logins. Users needing access to single-domain servers store a generated cookie for subsequent requests to the Web site. Users needing access to multi-domain servers store a cookie generated by a central Web login server; this occurs transparently for each accessed server within the associated Web system.

- **Delegated Access Administration**—When the responsibility for managing the Access System falls on a few people, you may want these people to appoint others to share the work. NetPoint allows you to delegate the ability to modify the revoked user list and to add, modify, or delete configuration details and schemes.

For more information and illustration of a sample Access System installation, see "About the NetPoint Access System" on page 26.

NetPoint External Authentication Features

NetPoint external authentication enables you to integrate multiple security systems across corporate boundaries through trust and technology relationships, as shown in Table 1.

Table 1 NetPoint External Authentication Features

NetPoint FEDERATEDid Layer™	Provides identity federation and the freedom to accept authentications from many trusted sources.
Passport Authentication Plug-in	This certified integration enables Microsoft .NET Passport to act as the authentication service while Oblix NetPoint enforces local authorization and provides single sign-on.

For more information, see "About NetPoint External Authentication" on page 32.

NetPoint Enhancements

NetPoint 7.0 provides the new functions and enhancements identified in Table 2. For more information, see the *NetPoint 7.0 Release Notes*.

Table 2 NetPoint 7.0 Functions and Enhancements

Support for Siemens DirX and IBM Directory Servers
The COREid data management layer (COREid Data Anywhere) supports multiple LDAP environments, RDBMS databases, and split directory profiles, as described in the *NetPoint Integration Guide*.
New workflow features support dynamic participants, time-based escalation, and a new Out of Office Participants tab.
Support for Microsoft Identity Integration Server (MIIS) and template-based workflow
SSO integration with Microsoft SharePoint Portal Server (SPS) 2003 and SSO integration with Microsoft Content Management Server (CMS) 2002, as described in the *NetPoint Integration Guide*.
WS-Federation Passive Requestor Profile
Logging and diagnostics enhancements for troubleshooting and failure recovery, as described in the *NetPoint 7.0 Administration Guide Volume 1.*
Reporting and auditing enhancements with out-of-the-box reports for Crystal Reports, as described in the *NetPoint 7.0 Administration Guide Volume 1*.
Upgrade capability to bring earlier versions of NetPoint up to 7.0, as described in the *NetPoint 7.0 Upgrade Guide*.
Support for Oblix SHAREid, a stand-alone SAML-based product for exchanging authentication and authorization information among Web access management and security products in different domains. See the Oblix *SHAREid Administration Guide*.
Support for storing various types of data on different directory server types, as described in the *NetPoint Installation Guide*.

NetPoint 6.5 introduced a number of new functions and enhancements outlined in Table 3.

Table 3 NetPoint 6.5 Functions and Enhancements

Multi-language support enabling localized NetPoint applications for end users.
Chained authorization and authentication mechanisms
Access Server clustering enables you to group Access Servers reducing the time needed to manage configuration tasks because NetPoint automatically performs some of these tasks

Table 3 NetPoint 6.5 Functions and Enhancements

Enhanced delegated access administration and platform and third-party support
Database profile enhancements

NetPoint 6.5 introduced enhanced compatibility with the Microsoft .NET framework and functions of the Windows 2003 Server, as shown in Table 4:.

Table 4 Compatibility with Microsoft .NET and Windows 2003

Co-existence with Windows 2000 and .NET Server 2003 Active Directory
Ambiguous name resolution (ANR)
A fast bind with the LDAP server
Dynamic-auxiliary classes
Windows Impersonation
.NET Managed code and the common language runtime (CLR)
.NET Web Services Interface Definition Language and Universal Description, Discovery, and Integration (UDDI) Services
Integration with ASP.NET using the NetPoint Security Connector for ASP.NET
Integration with the Windows Authorization Manager
Integration with Smart Card authentication

The *NetPoint Integration Guide* provides details about integrating NetPoint with ASP.NET, the Authorization Manager, Smart Card authentication, and more. Managed code is discussed in the *NetPoint 7.0 Developer Guide*.

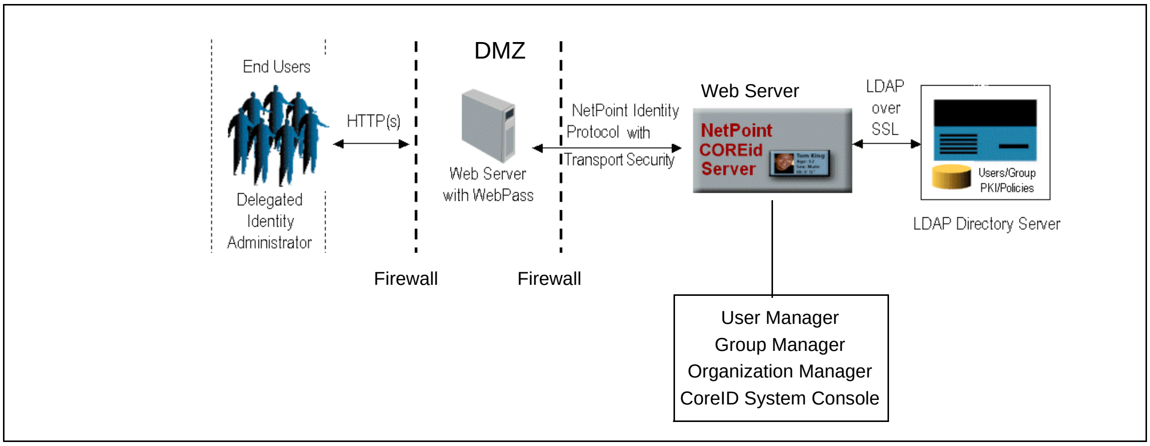
About the NetPoint COREid System

The NetPoint COREid System enables you to manage identity information about individuals, groups, organizations, and other objects and provides the infrastructure needed for other applications and systems to leverage user identity and policy information across the enterprise. This eliminates the need to create and manage separate user identity repositories for each application.

A COREid System Master Identity Administrator can delegate authority to other administrators, which enables management of millions of users. In addition to managing identity information, using the COREid System you can manage access privileges for a user based on a specific user attribute, membership in a group, or association with an organization. You can link privileges together into a workflow so that, for example, when a user self-registers, the registration request is forwarded to appropriate people for signoff.

Figure 2 illustrates the basic components of the COREid System in a simple environment as well as transport security between NetPoint components over the NetPoint Identity Protocol (NIP). For more about NetPoint component communications, see the *NetPoint 7.0 Installation Guide*.

Figure 2 COREid System Components



During COREid System installation and setup, the LDAP directory server is updated to include the Oblix NetPoint schema with object classes and attributes for the NetPoint COREid System. NetPoint enables you to store various types of data on the same directory server type, or separate directory server types. Data types include:

- **User Data**—User directory entries managed by the COREid System.
- **Configuration Data**—NetPoint configuration details stored in the directory and managed by the COREid System.

- **Policy Data**—Policy definitions that the Access Manager maintains in the directory server.

Communication between COREid System components and the directory server may be either open or SSL-enabled as long as the same mode is used between all COREid Servers and the directory server. For more information about directory server and data storage requirements and support, see the *NetPoint 7.0 Installation Guide.*

The COREid System is required in all NetPoint installations and consists of the following components:

- “The COREid Server and Applications” on page 24
- “WebPass” on page 26

The COREid Server and Applications

The COREid Server is one or more stand-alone servers that you use to manage identity information about users, groups, organizations, and other objects. The COREid Server performs three main functions:

- Reads and writes to your LDAP directory server across a network connection
- Stores user information on a directory server and keeps the directory current
- Processes all requests related to user, group, and organization identification

Each instance of the COREid Server communicates with a Web server through a WebPass plug-in. For more information, see “WebPass” on page 26.

The COREid Server provides the following applications through a Web-based interface:

- **User Manager**—Enables complete management of all identity information related to individual network users.

  If you are an administrator, the User Manager enables you to add, modify, and delete user identities and to provide users with access privileges based on their directory profiles. The User Manager also has reporting capability.

  The User Manager typically enables end users to view other users and to modify their own identity information. The users that a person can view and the identity information that someone can modify depends on the privileges granted by a NetPoint Administrator.

- **Group Manager**—Allows your authorized personnel to create, manage and delete static, dynamic, or nested groups or to delegate group administration.

  If you are an administrator, the Group Manager enables you to create or delete groups, and enables users to subscribe or unsubscribe from groups. The Group Manager also has reporting capability.

The Group Manager typically enables end users to view groups and to subscribe to membership in a group. The groups that a person can view and subscription rights are granted by a NetPoint Administrator.

- **Organization Manager**—Helps you manage system rules, access privileges, and workflows to manage ongoing changes for entire organizations.

  If you are an administrator, the Organization Manager enables you to create and delete organizations and other objects (such as floor plans and assets) that do not belong in the User Manager or Group Manager. The Organization Manager also has reporting capability.

  The Organization Manager enables end users to view organizational entities such as floor plans. The organizational entities that a person can view depend upon the rights granted by a NetPoint Administrator.

- **COREid System Console**—Provides Web-based administration and configuration of the NetPoint COREid System. In addition, you create NetPoint Administrators and assign the right to delegate administrative tasks. Specifically, the COREid System Console provides these functional options:

  - *Common Configuration*—Allows you to configure functionality common to NetPoint Identity applications, including object classes, workflow panels, master audit policies, and logging and auditing policies.
  - *User Manager Configuration*—Enables you to manage and customize the User Manager's appearance and behavior, including tabs, reports, and auditing policies.
  - *Group Manager Configuration*—Permits you to manage and customize Group Manager's appearance and behavior, including:
    - Tabs
    - Reports
    - Group types
    - Group Manager options
    - Auditing policies
    - Group cache
  - *Organization Manager Configuration*—Enables you to manage and customize Organization Manager appearance and behavior, including tabs, reports, and auditing policies.
  - *System Management*—Diagnostics to verify the state of the COREid Servers and their connectivity to the Directory Server.
  - *System Configuration*—Permits you to configure the general appearance and behavior of your NetPoint installation, and define and manage your administrator list.

Administrators access the COREid System Console by entering the following URL in a browser:

http://*hostname*:*port*/identity/oblix

where *hostname* refers to the machine that hosts the Web server; *port* refers to the HTTP port number of the WebPass Web server instance; /identity/oblix connects to the COREid System Console.

WebPass

A WebPass is a Web server plug-in that passes information back and forth between a Web server and the COREid Server. Depending upon its configuration, the COREid Server processes the request either as an XML or HTML file.

A WebPass can communicate with multiple COREid Servers. Each Web server instance that communicates with the COREid Server must be configured with a WebPass. In a NetPoint installation:

- At least one WebPass must be installed on a Web server and configured to communicate with at least one COREid Server.
- A WebPass is required on each machine hosting an Access Manager.

After installing a COREid Server and a WebPass, you must complete an initial COREid System setup process. The WebPass completes the following process.

Process overview: Accessing a resource where a WebPass is installed

1. The WebPass receives the user request and maps the URL to a message format.
2. The WebPass forwards the request to a COREid Server.
3. The WebPass receives information from the COREid Server and returns it to the user’s browser.

About the NetPoint Access System

The optional NetPoint Access System provides centralized authentication, authorization, and auditing to enable single sign-on and secure access control across enterprise resources. This enables you to centralize policy creation while decentralizing policy management and enforcement.

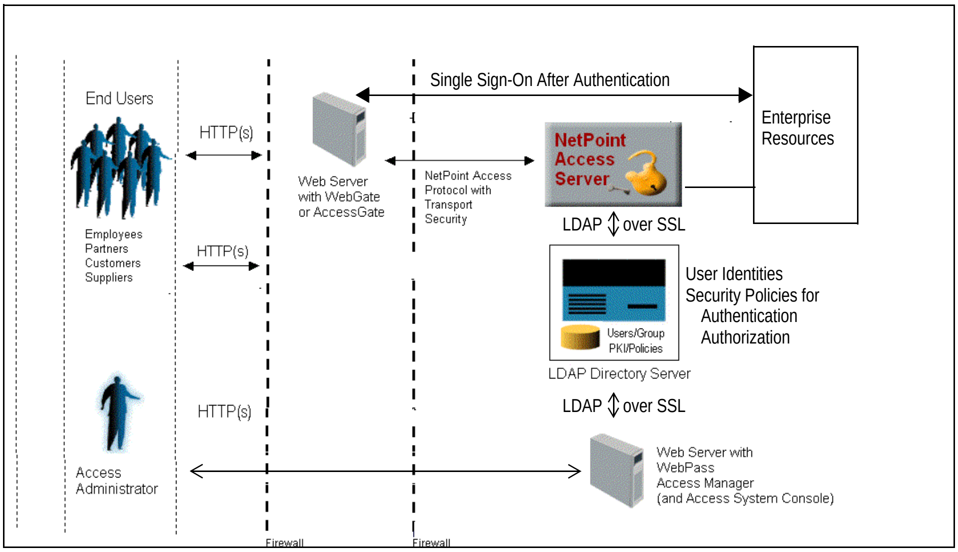
The following types of resources can be protected using the NetPoint Access System:

- HTTP resources including directories, pages, Web-based applications, query strings, and so forth

- J2EE application server resources, including Java server pages (JSPs), servlets, and enterprise Java beans (EJBs)
- Other resources, including stand-alone programs (Java, C, C++), ERP applications, CRM applications, and the like

Figure 3 illustrates the basic components of the Access System and transport security protocols between NetPoint components over NetPoint Access Protocol (NAP). For more information, see “Access System Operation” on page 31. For details about NetPoint transport security, see the *NetPoint 7.0 Installation Guide*.

Figure 3 Access System Components



The Access System stores information about configuration settings and access policies in the directory server that uses Oblix-specific object classes. This information is stored in a special policy branch of the directory information tree (DIT), which can be either in the same directory as the user information or on a separate directory server.

Communication between Access System components and the directory server can be either open or SSL-enabled as long as the same mode is used between all Access Managers and the directory server. For more information about directory server and data storage requirements and support, see the *NetPoint 7.0 Installation Guide*.

The Access System consists of several components and applications, as discussed in the following topics:

- “Access Manager and Access System Console” on page 28
- “The Access Server” on page 29
- “WebGates and AccessGates” on page 30

- "Access System Operation" on page 31

Access Manager and Access System Console

The Access Manager must be installed on a Web server instance with a WebPass and at the same directory level as the WebPass. Oblix recommends that you install multiple Access Managers for fault tolerance. For details about installing the Access Manager, see the *NetPoint 7.0 Installation Guide*.

Access Manager—Communicates with the directory server to write policy data and communicates with the Access Server over the NAP to update the Access Server when you make certain policy modifications.

Master Access Administrators and Delegated Access Administrators use the Access Manager to:

- Create and manage policy domains that consist of:
  - Resource types to protect
  - Authentication, authorization, and audit rules
  - Policies (exceptions)
  - Administrative rights
- Add resources to policy domains
- Test policy enforcement

Access System Console—Included with the Access Manager. Provides a login interface to the Access System Console and the functions that allow any NetPoint Administrator, Master Access Administrator, and Delegated Access Administrator to use the functional options below:

- *System Configuration*—Enables a NetPoint Administrator to specify the users who can administer NetPoint as a Master Access Administrator, and configure various server settings.
- *System Management*—Enables a NetPoint Administrator to manage:
  - Diagnostics—Show Access Server details, including connection information.
  - Manage Reports—Create, or view, or modify user access privilege reports.
  - Manage Sync Records—Archive or purge sync records generated before a given date.
- *Access System Configuration*—Enables a Master Access Administrator or delegated administrators to complete the following tasks:
  - View, add, modify, and delete AccessGates, Access Servers, Access Server clusters, Host Identifiers

- View and modify authentication and authorization parameters; Web resource user rights; and common information
- Configure NetPoint BEA Ready Realm

Administrators access the Access System Console by entering the following URL in a browser:

http://*hostname*:*port*/access/oblix

where *hostname* refers to the machine that hosts the Web server; *port* refers to the HTTP port number of the WebPass Web server instance; and /access/oblix connects to the targeted Access System Console.

The Access Server

The Access Server plays a key role in authentication and authorization:

- Authentication involves determining what authentication method is required for a resource and gathering credentials from the directory server, then returning an HTTP response based on the results of credential validation to the access client (WebGate or AccessGate).
- Authorization involves gathering access information and granting access based on a policy domain stored in the directory and the identity established during authentication.

To perform these operations, you may have one or more stand-alone Access Server instances that communicate with both the directory server and WebGate. Before you can install an Access Server instance, you must define it in the Access System Console.

Note: Oblix recommends that you install multiple Access Servers for failover and load balancing.

Process overview: Access Server functions

1. Receives requests from an access client (WebGate or AccessGate)
2. Queries authentication, authorization, and auditing rules in the directory server to determine whether:
   a) The resource is protected (and if so, how)
   b) The user is already authenticated (if the user is not yet authenticated, a challenge is provided)
   c) The user credentials are valid
   d) The user is authorized for the requested resource, and under what conditions

3. Responds to the access client as follows:

   a) Sends the authentication scheme

   b) Validates credentials

   c) Authorizes the user

   d) Audits

4. Manages the session, by:

   a) Helping the WebGate terminate user sessions

   b) Re-authenticating when there is a time out

   c) Tracking user activity during a session

   d) Setting session timeouts for users

WebGates and AccessGates

Throughout NetPoint manuals, the terms AccessGate and WebGate may be used interchangeably. However, there are differences worth noting:

- A WebGate is a Web server plug-in access client that intercepts HTTP requests for Web resources and forwards them to the Access Server for authentication and authorization. A WebGate is shipped out-of-the-box with NetPoint.
- An AccessGate is a NetPoint component that is specifically developed using the NetPoint Access Server SDK, either by you (the customer) or by Oblix. An AccessGate is a form of access client that processes requests for Web *and* non-Web resources from users or applications. For more information about the Access Server SDK, see the *NetPoint 7.0 Developer Guide*.

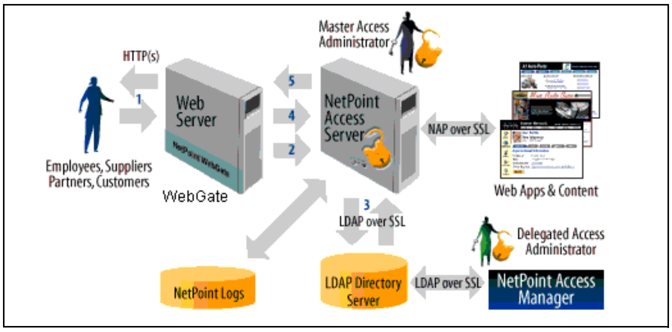
Before you can install a WebGate, you must define it in the Access System Console and associate it with an Access Server or cluster of Access Servers. For details, see *NetPoint 7.0 Installation Guide*.

The WebGate intercepts HTTP requests for resources from users or applications and forwards requests to the Access Server for authentication and authorization. See “Access System Operation” on page 31 for more information.

Access System Operation

Figure 4 and the description following it illustrate how the Access System works in concert during authentication and authorization.

Figure 4 Access System Functions



Process overview: When a user requests access

1. The NetPoint WebGate intercepts the request.

   Servers that can be protected include Web servers, application servers, and FTP servers (using the Access Server SDK), among others.

2. The WebGate forwards the request to the Access Server to determine whether the resource is protected, how, and if the user is authenticated (if not, there is a challenge).

3. The Access Server checks the directory server for credentials such as a user ID and password, sends the information back to WebGate, and generates an encrypted cookie to authenticate the user.

   The Access Server authenticates the user with a customer-specified authentication method to determine the identity, leveraging information stored in the directory server. Oblix NetPoint authentication supports any third-party authentication method as well as different authentication levels. Resources with varying degrees of sensitivity can be protected by requiring higher levels of authentication that correspond to more stringent authentication methods.

4. Following authentication, the WebGate prompts the Access Server to look up the appropriate security policies, compare them to the user's identity, and determine the user's level of authorization.

   - If the access policy is valid, the user is allowed to access the desired content and/or applications.
   - If the policy is false, the user is denied access and redirected to another URL determined by the organization's administrator.

About NetPoint External Authentication

The term *federation* is derived from the Latin word for *trust*. When used in the context of security management, Federation essentially means integrating multiple security systems together through trust and technology relationships.

The FEDERATEDid Layer is a built-in integration layer within NetPoint that allows an enterprise to separate an authentication source from authorization and identity-management actions.

After installing NetPoint, the FEDERATEDid Layer must be configured to trust an external SSO solution for authentication. During authentication runtime, NetPoint accepts identity information provided by the third-party authentication mechanism and maps it to the appropriate user being authorized by NetPoint.

The Passport Authentication Plug-In—A certified integration module that enables Microsoft .NET Passport to act as the authentication service while Oblix NetPoint enforces local authorization and provides single sign-on between .NET Passport sites and Oblix NetPoint protected sites. The distinction among services is important:

- .NET Passport acts as authentication method only.
- NetPoint provides authorization and identity management infrastructure.
- The NetPoint FEDERATEDid Layer provides the integration point.

For example, suppose your financial services enterprise is protecting Web applications with NetPoint and one of your customers, a consumer banker, first logs in to a Microsoft Passport-enabled Internet site. After authenticating there, they try to access an application on your Web site. The following process overview outlines what happens and describes how NetPoint handles authentication from an active Microsoft Passport session.

Process overview: During NetPoint Passport authentication

1. NetPoint automatically recognizes that the user already has an active Microsoft Passport session and automatically creates a NetPoint session from that.
2. All authorization is done locally by NetPoint once the user has been authenticated to the site protected by NetPoint.
3. The user can access the application on your Web site without re-authenticating.

For more information, see the *NetPoint Integration Guide*.

About NetPoint Installations

NetPoint provides Language Packs that enable you to localize NetPoint applications to display static data to users in their native language. The applications that access sensitive data reside within the firewall. The directory server is isolated so it is not exposed. The only server outside the firewall (or in the DMZ) is a Web server with a WebGate or WebPass.

For more information, see:

- "Language Packs" on page 33
- "Monitoring Tools" on page 33
- "Non-Production Environments" on page 33
- "Production Environments" on page 34

Language Packs

NetPoint provides the capability to localize NetPoint applications and present static data such as error messages and display names for tabs, panels, and attributes to users in their native language. English is the default language for NetPoint and other Language Packs are available. For more information, see the *NetPoint 7.0 Installation Guide*.

Monitoring Tools

NetPoint provides an optional Simple Network Management Protocol (SNMP) agent and data that can be used by SNMP and a Network Management System (NMS). This enables you to monitor the status and activity of the COREid and Access Servers resident on the same server host where the agent was installed. For installation details, see the *NetPoint 7.0 Installation Guide*. For SNMP monitoring details, see the *NetPoint 7.0 Administration Guide Volume 1*.

Non-Production Environments

In a non-production or test environment, NetPoint components may be installed on one machine. In this case, the machine must be hosting a Web server and you:

- Install the COREid Server.
- Install a WebPass.

  You cannot install the WebPass in the same directory as the COREid Server. For example, if the COREid Server is installed in C:\NetPoint\, then you would install the WebPass in C:\NetPoint\WebComponent.
- Setup the COREid System.

- Install the Access Manager at the same directory level as the WebPass and set up the Access Manager.
- Install the Access Server.
- Install the WebGate.

For more information, see the *NetPoint 7.0 Installation Guide*.

Production Environments

In a production environment, NetPoint components are usually installed on different machines in your network. For example, a simple deployment may include:

- The COREid Server and Access Server can be installed on separate machines, protected by the firewall.

  Note: For better performance, the COREid and Access Servers should reside on different hosts.

- The Web servers, WebPass, WebGate, and Access Manager can reside in the DMZ.

For more information, see the *NetPoint 7.0 Installation Guide* and the *NetPoint 7.0 Deployment Guide*.

About NetPoint Integrations

NetPoint Integration Services extend NetPoint capabilities to all your applications and provide integration points with systems and applications from other vendors: The following is only a *short* list of the integration options Oblix offers:

- Integrating NetPoint with OctetString Virtual Directory Engine (VDE)
- Single sign-on integrations
- Portal integrations
- Integrations with application servers
- Integrating Workflows With MIIS Provisioning
- Integrating Smart Card Authentication or the RSA SecurID Authentication Plug-in

For more information about integrating NetPoint with third-party applications, see the *NetPoint Integration Guide*. You can customize NetPoint to look or behave in a way that is consistent with the rest of your enterprise, as introduced next.

About NetPoint Customization

You can customize the COREid System and Access System using several components and methods discussed next:

- “COREid System Customization” on page 35
- “Access System Customization” on page 36

COREid System Customization

NetPoint provides various components and methods to help you customize the COREid System, which are introduced in the following topics:

- “Identity Event API Plug-In” on page 35
- “PresentationXML” on page 35
- “Portal Inserts” on page 36
- “IdentityXML” on page 36

Identity Event API Plug-In

The Identity Event API plug-in enables you to integrate COREid functionality with your other applications.

For example, when defining a workflow for user creation, you may want to call out to a Human Resources Management System, which in turn creates an account for a user. The new user ID can then be returned to the COREid System.

More information is provided in the *NetPoint 7.0 Developer Guide*.

PresentationXML

PresentationXML enables you to tailor the COREid user interface. For example, you can:

- Apply your organization’s look and feel to the NetPoint user pages, including color schemes, fonts, button images, and logos.
- Add, modify, or remove functions on a COREid page.
- Create hidden information on a COREid page for the Identity Event API to use.
- Create new pages and functionality.

More information on PresentationXML is provided in the *NetPoint 7.0 Customization Guide*.

Portal Inserts

Portal inserts are embeddable pieces of NetPoint functionality that are available as URLs. You can place a portal insert anywhere on your site or portal to insert content generated by NetPoint into other applications, without programming.

You can, for instance, use the NetPoint COREid System's searching capabilities to add a company directory search feature to your site or embed a page from the Group Manager into your extranet portal. Users can access this functionality directly from the portal without viewing the standard COREid System interface.

More information about portal inserts is available in the *NetPoint 7.0 Customization Guide.*

IdentityXML

IdentityXML enables you to access COREid functionality without a browser. Through IdentityXML, external applications can initiate remote procedure calls that pass arguments to the COREid System.

For example, an external application can initiate batch processing of new users in the COREid System without going through the COREid System browser interface. IdentityXML allows for cross-firewall integration without exposing the directory.

More information on this component is provided in the *NetPoint 7.0 Developer Guide*.

Access System Customization

NetPoint provides various components and methods to help you customize the Access System, which are introduced in the following discussions:

- "Custom Access Clients" on page 36
- "Access Server SDK" on page 37

Custom Access Clients

An AccessGate is similar to the WebGate access client provided by NetPoint. The WebGate client acts as the interface between individual Web servers and the NetPoint Access Server. The WebGate intercepts requests from users for Web resources and authorizes the requests through the Access Server.

An AccessGate custom access client is an interface between enterprise resources and the Access Server that is developed using the NetPoint Access Server SDK. A custom access client is, in other words, a customized WebGate that is configured using the Access Server API. A custom access client is referred to as an AccessGate.

An AccessGate uses an Access Server to control attempts to access a Web site. AccessGates allow you to extend authorization and authentication rules to other resources in addition to URLs and to control user interaction with applications outside of NetPoint. This provides you with centralized policy information that applies to Web and non-Web resources.

For more information, see the *NetPoint 7.0 Developer Guide*.

Access Server SDK

The Access Server SDK is a toolkit you use to build access clients. The Access Server SDK gives developers the ability to construct interfaces for other applications so that they can use NetPoint authentication and authorization. NetPoint includes an *Access Server API* that lets you create custom access clients (also known as AccessGates) that interface with both Web and non-Web (non-HTTP) resources.

The Access Server Software Developer's Kit (SDK) allows developers to enhance NetPoint's access management capabilities. The Access Server SDK consists of libraries, build instructions, and examples that you (or Oblix) can use to build a custom *AccessGate* for Web and non-Web resources.

The Access Server SDK allows you to create an interface that can be built into commercially available application servers such as BEA WebLogic, IBM WebSphere, Sun, or another application that can access the NetPoint Access Server. The Access Server API can integrate with Java and C/C++ applications.

The use of the Access Server SDK is optional and of interest only to developers. Therefore, information about installing the Access Server SDK is located in the *NetPoint 7.0 Developer Guide*.

Looking Ahead

For an introduction to NetPoint manuals, see "Road Map to Manuals" on page 39. For an in depth look at NetPoint terminology, see "Glossary" on page 63.

If you are ready to install NetPoint, see the *NetPoint 7.0 Installation Guide*.

If you have an older version of NetPoint installed and want to upgrade it, see the *NetPoint 7.0 Upgrade Guide.*

2 Road Map to Manuals

Each COREid product manual is written to help the individuals responsible for certain tasks complete their work. Each COREid implementation may involve the following individuals at various times during the overall process:

- Technical architects
- Network, system, database, and Web administrators
- IT and application developers
- Quality Assurance (QA) engineers
- Business analysts

This chapter provides a brief overview of each COREid manual, its intended audience, and recommended prerequisite knowledge and skills.

This Guide: Introduction to NetPoint

Look to this introduction to NetPoint for:

- An introduction to NetPoint concepts, features, and applications
- An overview of NetPoint integrations and customization
- A road map to all NetPoint manuals and their audiences, with suggested prerequisite knowledge and skills
- A glossary of NetPoint terminology

Audiences

Anyone interested in learning about NetPoint should begin with this guide.

Prerequisites

None.

Looking Ahead

After reviewing this guide, you may want to print the glossary and keep it handy as you work with NetPoint.

The manuals in the NetPoint suite that are relevant to you will depend in part on your role and responsibilities within the enterprise:

- Locate the latest information about your NetPoint release, as described in “Release Notes” on page 42.
- Install and set up NetPoint, as described in “NetPoint Installation Guide” on page 43.
- Assign additional administrators, configure and manage servers, configure applications and workflows, protect resources, and perform other administrative tasks as explained in “NetPoint Administration Guide” on page 47.
- Fine-tune and manage your NetPoint installation or prepare to migrate from a test environment to a production environment as described in “NetPoint Deployment Guide” on page 49.
- Customize NetPoint to change the appearance of applications or change how to control NetPoint as described in “NetPoint Customization Guide” on page 51.

- Create custom AccessGates and develop plug-ins or examine considerations for CGI files or JavaScripts created for NetPoint as described in “NetPoint Developer Guide” on page 53.
- Integrate NetPoint with one or more supported third-party products as described in “NetPoint Integration Guide” on page 55.
- Review the schema description, as described in “NetPoint Schema Description” on page 56.
- Install, set up, and administer Oblix SHAREid to enable a Federated identity management system for single sign-on across organizations that use different security systems (allowing locally authenticated users to access resources on remote Web sites without re-authenticating), as described in “Oblix SHAREid Guide” on page 57.
- Transition existing NetPoint SAML Services to SHAREid, as described in “NetPoint SAML to SHAREid Migration Guide” on page 58.
- Upgrade an earlier version of SHAREid to the latest version of SHAREid, as described in “SHAREid Upgrade Guide” on page 59.

Release Notes

For up-to-the-minute details about the product, see the *Release Notes* where you will find information about:

- Changes and new features
- Patches included in the release
- Documentation updates and resolved issues
- Installation
- And more

Release Notes are cumulative and include all previous notes within the same series. For example, *NetPoint 6.1.1.9 Release Notes* include details for NetPoint 6.1.1 and later releases within the NetPoint 6.1.1 series, but not for NetPoint 6.5 or 7.0 releases. *SHAREid Release Notes* are relevant only to SHAREid users. COREsv *Release Notes* are relevant only to COREsv users.

Audiences

Everyone should review the latest release notes for their product and installation.

- If you are new to a product (NetPoint COREid, SHAREid, or COREsv) and want to ensure you have the latest details, check the *Release Notes*.
- If you have used a product previously and want to quickly update your knowledge, *Release Notes* summarize the latest enhancements and changes.

Prerequisites

None.

Looking Ahead

After you have reviewed the *Release Notes*, you are ready to proceed with activities described in the product manuals.

NetPoint Installation Guide

The *NetPoint Installation Guide* helps you prepare your environment, then install and set up NetPoint, including:

- Details about supported environments
- Installation prerequisites, considerations, and options
- Preparation worksheets that you can complete to help streamline your experience and document your NetPoint installation
- Step-by-step instructions to help ensure a successful NetPoint installation
- Troubleshooting tips

Audiences

The *NetPoint Installation Guide* is required for anyone who installs or sets up NetPoint, with emphasis on the following:

- COREid Server and applications
- WebPass to communicate with the COREid Server
- Access Manager and Access System Console
- Access Server to communicate with the directory server
- WebGate to communicate with the Access Server

Prerequisites

The *NetPoint Installation Guide* presumes that you have knowledge of and experience with the following:

- Operating and file systems: Windows or Unix based
- Sites connected to the Internet and networking protocols
- Network security: building firewalls, deploying authentication systems, etc.
- Host security: passwords, uids, file permissions, file system integrity, etc.
- Web server, Web browser, and configuration details
- Database administration

Looking Ahead

After NetPoint is installed and set up, one or more members of your team: may perform the following

- Assign additional administrators, configure and manage servers, configure applications and workflows, protect resources, and perform other administrative tasks as explained in “NetPoint Administration Guide” on page 47.
- Fine-tune and manage your NetPoint installation or prepare to migrate from a test environment to a production environment as described in “NetPoint Deployment Guide” on page 49.
- Customize NetPoint to change the appearance of applications or change how to control NetPoint as described in “NetPoint Customization Guide” on page 51.
- Create custom AccessGates and develop plug-ins or examine considerations for CGI files or JavaScripts created for NetPoint as described in “NetPoint Developer Guide” on page 53.
- Integrate NetPoint with one or more supported third-party products as described in “NetPoint Integration Guide” on page 55.
- Review the schema description, as described in “NetPoint Schema Description” on page 56.
- Install, set up, and administer Oblix SHAREid to enable a Federated identity management system for single sign-on across organizations that use different security systems (allowing locally authenticated users to access resources on remote Web sites without re-authenticating), as described in “Oblix SHAREid Guide” on page 57.
- Transition existing NetPoint SAML Services to SHAREid, as described in “NetPoint SAML to SHAREid Migration Guide” on page 58.
- Upgrade an earlier version of SHAREid to the latest version of SHAREid, as described in “SHAREid Upgrade Guide” on page 59.

NetPoint Upgrade Guide

The *NetPoint Upgrade Guide* provides information to upgrade an existing NetPoint installation to the latest version. This guide includes:

- Details about supported environments
- Upgrade prerequisites, considerations, and options
- Preparation worksheets that you can complete to help streamline your experience and document your NetPoint installation
- Step-by-step instructions to help ensure a successful NetPoint upgrade
- Troubleshooting tips

Audiences

The *NetPoint Upgrade Guide* is required for anyone who upgrades an older version of NetPoint to the latest version. Emphasis is on the following:

- COREid Server and applications
- WebPass to communicate with the COREid Server
- Access Manager and Access System Console
- Access Server to communicate with the directory server
- WebGate to communicate with the Access Server
- Access Server SDK and other optional software
- Post-upgrade processes

Prerequisites

The *NetPoint Upgrade Guide* presumes that you have knowledge of and experience with the following:

- The existing NetPoint installation
- Operating and file systems: Windows or Unix based
- Sites connected to the Internet and networking protocols
- Network security: building firewalls, deploying authentication systems, etc.
- Host security: passwords, uids, file permissions, file system integrity, etc.
- Web server, Web browser, and configuration details
- Database administration

Looking Ahead

After NetPoint is upgraded, one or more members of your team may perform the following tasks:

- Assign additional administrators, configure and manage servers, configure applications and workflows, protect resources, and perform other administrative tasks as explained in “NetPoint Administration Guide” on page 47.
- Fine-tune and manage your NetPoint installation or prepare to migrate from a test environment to a production environment as described in “NetPoint Deployment Guide” on page 49.
- Customize NetPoint to change the appearance of applications or change how to control NetPoint as described in “NetPoint Customization Guide” on page 51.
- Create custom AccessGates and develop plug-ins or examine considerations for CGI files or JavaScripts created for NetPoint as described in “NetPoint Developer Guide” on page 53.
- Integrate NetPoint with one or more supported third-party products as described in “NetPoint Integration Guide” on page 55.
- Review the schema description, as described in “NetPoint Schema Description” on page 56.
- Install, set up, and administer Oblix SHAREid to enable a Federated identity management system for single sign-on across organizations that use different security systems (allowing locally authenticated users to access resources on remote Web sites without re-authenticating), as described in “Oblix SHAREid Guide” on page 57.
- Transition existing NetPoint SAML Services to SHAREid, as described in “NetPoint SAML to SHAREid Migration Guide” on page 58.
- Upgrade an earlier version of SHAREid to the latest version of SHAREid, as described in “SHAREid Upgrade Guide” on page 59.

NetPoint Administration Guide

The *NetPoint Administration Guide* is divided into two volumes:

- Volume 1 focuses on the COREid System and common administration tasks
- Volume 2 focuses on the Access System.

Together, these volumes provide the information needed to:

- Configure the rights and tasks available to administrators and end users
- Configure NetPoint to read and use data in the directory
- Configure NetPoint applications to display directory data
- Assign read and write permissions to users
- Configure and manage servers
- Define workflows to complete activities such as creating users
- Protect resources to control user access to applications and data
- Set up single sign-on

During this phase of the implementation, the “NetPoint Schema Description” on page 56 may also provide a useful tool.

Audiences

The *NetPoint Administration Guide* targets the following audiences:

- NetPoint Administrators and delegated administrators
- Individuals who enter or manage information about users, groups, and resources
- Individuals who manage servers
- Individuals who audit or monitor system events and user-session activity
- Individuals who generate reports

Prerequisites

NetPoint should be installed and its operation confirmed as described in the *NetPoint Installation Guide*. To complete activities in the *NetPoint Administration Guide* volumes, the reader should have some knowledge of and experience with the following:

- Browser-based interfaces, windows, and menus
- Your Web servers and LDAP directory server

- Data entry
- Policy setting
- Report generation

Helpful

- Knowledge of authentication and authorization concepts
- System or database administration

Looking Ahead

After NetPoint configuration, you can perform the following tasks:

- Fine-tune and manage your NetPoint installation or prepare to migrate from a test environment to a production environment as described in "NetPoint Deployment Guide" on page 49.
- Customize NetPoint to change the appearance of applications or change how to control NetPoint as described in "NetPoint Customization Guide" on page 51.
- Create custom AccessGates and develop plug-ins or examine considerations for CGI files or JavaScripts created for NetPoint as described in "NetPoint Developer Guide" on page 53.
- Integrate NetPoint with one or more supported third-party products as described in "NetPoint Integration Guide" on page 55.
- Review the schema description, as described in "NetPoint Schema Description" on page 56.
- Install, set up, and administer Oblix SHAREid to enable a Federated identity management system for single sign-on across organizations that use different security systems (allowing locally authenticated users to access resources on remote Web sites without re-authenticating), as described in "Oblix SHAREid Guide" on page 57.
- Transition existing NetPoint SAML Services to SHAREid, as described in "NetPoint SAML to SHAREid Migration Guide" on page 58.
- Upgrade an earlier version of SHAREid to the latest version of SHAREid, as described in "SHAREid Upgrade Guide" on page 59.

NetPoint Deployment Guide

The *NetPoint Deployment Guide* provides the information needed to fine-tune and manage the NetPoint installation. The scope of this guide encompasses:

- Capacity planning
- System tuning
- Performance and scalability considerations
- Failover and load balancing
- Caching
- Migration planning to move NetPoint from a test environment to a production environment

Audiences

The *NetPoint Deployment Guide* targets the knowledge and skill requirements of system, network, or NetPoint Administrators responsible for optimizing the NetPoint implementation.

Prerequisites

To complete activities in the *NetPoint Deployment Guide* the reader should have strong knowledge of and experience with the following:

- Network, site planning, and networking concepts
- Distributed computing environment concepts
- Consistent network-wide file system layout design
- Routing principles
- Client/server programming
- Operating system details and inter-process communication
- System performance tuning
- Firewall and Internet security
- Computing policies

Helpful

- Familiarity with failover concepts and practices
- Network communications

Looking Ahead

You may complete other activities either before, during, or after deployment tuning. For example:

- Customize NetPoint to change the appearance of applications or change how to control NetPoint as described in “NetPoint Customization Guide” on page 51.
- Create custom AccessGates and develop plug-ins or examine considerations for CGI files or JavaScripts created for NetPoint as described in “NetPoint Developer Guide” on page 53.
- Integrate NetPoint with one or more supported third-party products as described in “NetPoint Integration Guide” on page 55.
- Review the schema description, as described in “NetPoint Schema Description” on page 56.
- Install, set up, and administer Oblix SHAREid to enable a Federated identity management system for single sign-on across organizations that use different security systems (allowing locally authenticated users to access resources on remote Web sites without re-authenticating), as described in “Oblix SHAREid Guide” on page 57.
- Transition existing NetPoint SAML Services to SHAREid, as described in “NetPoint SAML to SHAREid Migration Guide” on page 58.
- Upgrade an earlier version of SHAREid to the latest version of SHAREid, as described in “SHAREid Upgrade Guide” on page 59.

NetPoint Customization Guide

The *NetPoint Customization Guide* explains how to control the way NetPoint operates, without programming. Topics in this guide include:

- Changing the appearance of NetPoint applications
- Tuning catalog files
- Designing the GUI by editing XML files
- Connecting CGI files or JavaScripts to NetPoint screens
- Controlling how NetPoint operates by making configuration changes to the operating system, Web or directory servers, or directory content
- Introducing Access Server API and the Authorization and Authentication Plug-in APIs from an administrator's point of view

Audiences

The *NetPoint Customization Guide* is a valuable asset to anyone responsible for customizing NetPoint to control operations.

Prerequisites

Techniques provided here are vulnerable to error and should be used with the utmost care. This guide assumes that you have some prior knowledge of and experience with:

- Using Netpoint
- Logical connections between the COREid and Access systems
- General working knowledge of directories and LDAP
- Comfort manipulating files and running applications at the command-line level

NetPoint should be installed and its operation confirmed, as described in the *NetPoint Installation Guide.*

Helpful

- System and/or database administration
- Familiarity with CGI files or JavaScripts
- Your Web server, Web browser, operating system, and configuration details

Looking Ahead

Before, during, or after customizing NetPoint as described in the *Customization Guide*, your team can complete tasks described earlier in this chapter or:

- Create custom AccessGates and develop plug-ins or examine considerations for CGI files or JavaScripts created for NetPoint as described in “NetPoint Developer Guide” on page 53.
- Integrate NetPoint with one or more supported third-party products as described in “NetPoint Integration Guide” on page 55.
- Review the schema description, as described in “NetPoint Schema Description” on page 56.
- Install, set up, and administer Oblix SHAREid to enable a Federated identity management system for single sign-on across organizations that use different security systems (allowing locally authenticated users to access resources on remote Web sites without re-authenticating), as described in “Oblix SHAREid Guide” on page 57.
- Transition existing NetPoint SAML Services to SHAREid, as described in “NetPoint SAML to SHAREid Migration Guide” on page 58.
- Upgrade an earlier version of SHAREid to the latest version of SHAREid, as described in “SHAREid Upgrade Guide” on page 59.

NetPoint Developer Guide

The *NetPoint Developer Guide* describes the application programming interfaces (APIs) provided by NetPoint and explains how to write custom applications and plug-ins that use the programmatic access provided by NetPoint to gain access to NetPoint functionality, and, in some cases, to extend that functionality. This guide shows you how to:

- Use IdentityXML to interact with NetPoint without using a browser.
- Use the Identity Event API to implement functions and executables triggered by events within NetPoint.
- Use AccessXML to gain access to NetPoint without using a browser.
- Develop custom AccessGates using the Access Server API and the Access Management API in Java, C, C++, and managed code.
- Develop server-side plug-ins to apply custom filters and logic using the Authentication and Authorization Plug-in APIs.

Audiences

The *NetPoint Developer Guide* is for NetPoint Administrators and experienced developers who want to write applications that extend the capabilities of NetPoint.

Prerequisites

The *NetPoint Developer Guide* presumes that you have knowledge of and experience with the following:

- The C programming language (or C++, C#, Java code, Managed code) concepts and fundamentals
- APIs, wrappers, variables, constructors
- Extensions, events, parameters, and exceptions
- Cookies
- Certificates

Looking Ahead

In addition to customizing NetPoint and writing applications to extend NetPoint capabilities, your team can complete tasks described earlier in this chapter or:

- Integrate NetPoint with one or more supported third-party products as described in “NetPoint Integration Guide” on page 55.

- Review the schema description, as described in “NetPoint Schema Description” on page 56.
- Install, set up, and administer Oblix SHAREid to enable a Federated identity management system for single sign-on across organizations that use different security systems (allowing locally authenticated users to access resources on remote Web sites without re-authenticating), as described in “Oblix SHAREid Guide” on page 57.
- Transition existing NetPoint SAML Services to SHAREid, as described in “NetPoint SAML to SHAREid Migration Guide” on page 58.
- Upgrade an earlier version of SHAREid to the latest version of SHAREid, as described in “SHAREid Upgrade Guide” on page 59.

NetPoint Integration Guide

The *NetPoint Integration Guide* explains how to integrate NetPoint with one or more third-party products, such as:

- BEA WebLogic
- Plumtree portal
- IBM WebSphere
- RSA SecurID
- Microsoft Smart Card, SharePoint Portal Server, and Content Management Server
- Oracle Application Servers
- OctetString VDE
- and others

For a complete list of supported integrations, see the latest *NetPoint Integration Guide* which includes both considerations and steps to complete each integration.

Audiences

Anyone who is responsible to integrate NetPoint with a supported third-party product.

Prerequisites

NetPoint should be installed and its operation confirmed as described in *NetPoint Installation Guide*. The *NetPoint Integration Guide* presumes that you have knowledge of and experience with NetPoint installation and set up, and the product you are integrating with NetPoint.

Looking Ahead

At any time during your implementation of NetPoint, your team can complete tasks described earlier in this chapter or:

- Review the schema description, as described in “NetPoint Schema Description” on page 56.
- Install, set up, and administer Oblix SHAREid, as described in “Oblix SHAREid Guide” on page 57.
- Transition existing NetPoint SAML Services to SHAREid, as described in “NetPoint SAML to SHAREid Migration Guide” on page 58.

NetPoint Schema Description

The *NetPoint Schema Description* identifies the Oblix-provided objects and attributes that control the behavior of NetPoint. This information is being provided to help you understand the structure and behavior of the NetPoint product.

Important: This document is *not* intended to be used as a guide for modifying the NetPoint schema. Oblix does not support modified versions of its schema.

Audiences

The *NetPoint Schema Description* is intended for anyone who needs to understand the structure and behavior of the NetPoint product.

Prerequisites

The *NetPoint Schema Description* assumes that you are familiar with your LDAP directory and concepts.

Looking Ahead

At any time during your implementation of NetPoint, your team can:

- Complete any of the activities described earlier in this chapter.
- Install, set up, and administer Oblix SHAREid to enable a Federated identity management system for single sign-on across organizations that use different security systems (allowing locally authenticated users to access resources on remote Web sites without re-authenticating), as described in “Oblix SHAREid Guide” on page 57.
- Transition existing NetPoint SAML Services to SHAREid, as described in “NetPoint SAML to SHAREid Migration Guide” on page 58.
- Upgrade an earlier version of SHAREid to the latest version of SHAREid, as described in “SHAREid Upgrade Guide” on page 59.

Oblix SHAREid Guide

Oblix SHAREid may be installed with NetPoint or a stand-alone LDAP directory to provide cross-domain SSO, secure inter-operability, and external authentication. The Oblix *SHAREid Guide* includes concepts and considerations and describes how to:

- Install Oblix SHAREid
- Configure source and destination domains
- Configure keys and certificates
- Manage audits and logs
- Setup SHAREid security
- Tune SHAREid for performance

Audiences

The Oblix *SHAREid Guide* is intended for anyone who installs or administers Oblix SHAREid.

Prerequisites

NetPoint should be installed and its operation confirmed as described in the *NetPoint Installation Guide*. The Oblix *SHAREid Guide* presumes that you have knowledge of and experience with the following:

- Your network architecture
- LDAP directory concepts
- NetPoint, if you are in the role of a destination domain

Looking Ahead

Any of the activities described earlier in this chapter may be completed before you install, set up, and administer Oblix SHAREid. In addition, you may:

- Transition existing NetPoint SAML Services to SHAREid, as described in “NetPoint SAML to SHAREid Migration Guide” on page 58.
- Upgrade an earlier version of SHAREid to the latest version of SHAREid, as described in “SHAREid Upgrade Guide” on page 59.

NetPoint SAML to SHAREid Migration Guide

The *NetPoint SAML to SHAREid Migration Guide* describes how to transition existing NetPoint SAML Services to SHAREid 2.0, including:

- Preparing your environment
- Upgrading to NetPoint 7.0
- Migrating NetPoint SAML Services to SHAREid 2.0
- Reverting a migrated environment

Audiences

The *NetPoint SAML to SHAREid Migration Guide* is intended for anyone who needs to transition NetPoint SAML Services to Oblix SHAREid 2.0.

This document assumes that you are familiar with your LDAP directory and Web servers, NetPoint and NetPoint SAML Services, and Oblix SHAREid 2.0.

Prerequisites

NetPoint SAML Services should be installed and operation confirmed as described in your *NetPoint Installation Guide*. The *NetPoint SAML to SHAREid Migration Guide* presumes that you have knowledge of and experience with the following:

- Your network architecture
- LDAP directory concepts
- NetPoint SAML Services
- SHAREid 2.0

Looking Ahead

After transitioning NetPoint SAML Services to SHAREid 2.0, you may:

- Configure SHAREid, as discussed in the “Oblix SHAREid Guide” on page 57.
- Upgrade an earlier version of SHAREid to the latest version of SHAREid, as described in “SHAREid Upgrade Guide” on page 59.

SHAREid Upgrade Guide

The Oblix *SHAREid Upgrade Guide* includes information about upgrading an existing SHAREid 2.0 installation to SHAREid 2.5, including:

- Preparing your existing SHAREid 2.0 installation for the upgrade
- Upgrading to SHAREid 2.5

Audiences

The Oblix *SHAREid Upgrade Guide* is intended for anyone who needs to upgrade a SHAREid 2.0 environment to SHAREid 2.5.

Prerequisites

SHAREid 2.0 should be installed and its operation confirmed as described in the Oblix *SHAREid 2.0 Guide*. If you have NetPoint SAML Services, you can transition these to SHAREid 2.0 as described in the *NetPoint SAML to SHAREid Migration Guide*.

The *SHAREid Upgrade Guide* presumes that you have knowledge of and experience with the following:

- Your network architecture
- LDAP directory concepts
- SHAREid 2.0

Looking Ahead

Any of the activities described earlier in this chapter may be completed before you upgrade Oblix SHAREid.

Installing and Deploying COREsv

Oblix provides an integrated, comprehensive identity management and Web services security and monitoring system based on the integration between NetPoint (also known as COREid) and Oblix COREsv.

The Oblix *Installing and Deploying COREsv Guide* shows you how to install and deploy COREsv and in addition, how to integrate COREsv and COREid to authenticate users and verify their privileges. Topics include:

- Planning a COREsv deployment
- Preparing for COREsv installation
- Installing and deploying COREsv components
- Managing COREsv Roles
- Installing Security Certificates and Keystores
- Integrating COREsv with COREid for authentication and authorization
- Configuring COREsv to use an AccessGate
- Creating Policies using the Access Manager
- Integrating COREsv with Netegrity SiteMinder and TransactionMinder

Audiences

This guide is intended for individuals who are responsible for the installation, deployment, and overall operation of COREsv at a particular site. In addition, to installing and deploying COREsv, these users are also typically responsible for assigning roles to other users to perform COREsv tasks and operations such as defining and enforcing policies on managed services

Prerequisites

The *Installing and Deploying COREsv Guide* presumes that you have knowledge of and experience with the following:

- Operating and file systems: Windows or Unix based
- Sites connected to the Internet and networking protocols
- Network security: building firewalls, deploying authentication systems, etc.
- Host security: passwords, uids, file permissions, file system integrity, etc.
- Web server, Web browser, and configuration details

Looking Ahead

Any of the activities described earlier in this chapter may be completed before you install and configure COREsv.

Using and Administering COREsv

Provides instructions on using the COREsv Console web application to manage web services as well as perform daily tasks to monitor status and performance in a production environment.

Extending COREsv

Provides information on extending COREsv by creating and deploying new custom policy steps.

Extending COREsv provides application developers with information on customizing COREsv policy steps and using COREsv APIs to extend COREsv functionality.

Glossary

access administrator

A user able to modify data within the NetPoint Access System (NPAS). The system administrator and master access administrators can modify any of this data. Delegated access administrators can modify only subsets of this data.

access control

The protection of system resources against unauthorized use. The process is regulated according to a security policy and permits only authorized system entities (users, programs, processes, or other systems) to access the resource. See also ACL (access control list).

AccessGate

A NetPoint component that is specifically developed using the NetPoint Access Server SDK. An AccessGate is a form of access client that processes requests for Web and non-Web resources from users or applications and uses the NetPoint Access Server to provide authorization and authentication services to monitor and control attempts to access a Website. Customers can also use the Application Server API to build a client into an application server or standalone application. NetPoint provides an out-of-the-box WebGate client. See also WebGate.

Access Manager

This NPAS application through which users can perform policy management, designation of resources (both Web and non-Web), and policy testing through simulated user access.

Access Server

This stand-alone server (of which there can be several instances) provides dynamic policy evaluation services for both Web-based and non-Web resources and applications. Different applications and web servers can make use of the authentication, authorization, and auditing services it provides.

Access Management API

A NetPoint standard API used to create customer-defined access interfaces.

Access Server API

A collection of libraries, build instructions, and examples that can be used to build a customer-specific AccessGate for non-Web resources. This helps the customer to extend authorization and authentication rules to other resources in addition to URLs, and to control user interaction with applications outside of NetPoint. In this way, customers can have centralized policy information in a single system that can be leveraged across both Web and non-Web resources. This API can integrate with Java and C/C++ applications. The Java API allows application servers and other Java-based systems to leverage NetPoint infrastructure. The C/C++ API allows client-server or non-Java applications to leverage NetPoint infrastructure. The API is available as a distinct product. See also API (Application Programming Interface).

Access Tester

The NetPoint Access Manager tool used to determine whether a policy domain’s authentication, authorization, and auditing rules deliver the level of access control required.

ACI (access control item)

An entry in an access control list (ACL) specifying users, their access rights, and the target entries or attributes to which those rights apply.

ACL (access control list)

The set of roles and policies used for controlling access to resources such as directories and NetPoint applications. The ACL describes the users or groups, the type of access permitted and the attributes being accessed.

action

A task within a NetPoint workflow that results in changed information (for example, a change to a user’s phone number).

activate

The process followed to make a user’s directory information accessible within NetPoint. See also deactivate.

actor

The participant who performs a specific action in a NetPoint workflow.

API (Application Programming Interface)

A set of commands used to extend the capabilities of an existing application. APIs contain a library of functions and an interface that can be easily added to the application.

artifact

The SAML Browser Artifact Profile provides a method for transmission of assertions using a compact reference to the assertion called an artifact. The artifact is used in place of the full assertion.

Artifact Profile

The SAML Browser Artifact Profile provides a method for transmission of assertions using a compact reference to the assertion called an artifact. The artifact is used in place of the full assertion.

Assertion

Assertions are SAML XML request and response queries containing security information that pertains to a user who is the subject of the assertion. Assertions contain statements that attest to a user’s identity or access rights, or specify attributes for that user.

attribute

A characteristic or trait associated with a directory object, which can have one or more values. For example, the object class “person” can be identified with the attribute “cn” with the specific value: “Joe Smith”.

attribute authority

An attribute statement asserts that the subject of the assertion has certain attributes defined in a security repository or other database. In SAML terms, the repository (or database) is referred to as an attribute authority.

audit

The process of collecting information on NetPoint System events such as authentication success or authorization failure, and which user or administrator triggered them. This data, when presented in report form, helps NetPoint Administrators understand NetPoint usage patterns.

audit files

Disk files that record audit information. Each Access Server and COREid Server can record audit information to a file, to the consolidated audit database, or to both.

audit file rotation

The process by which a specified audit file is closed, stamped with the date and time, and given a new name. When an audit log is closed, a new audit log file is created.

audit rule

A named filter that determines the tracking level of the authentication and authorization activities performed by an Access Server.

Auditing Services

Provide flexible and detailed recording of events in the Access System and COREid System. You can use this information both for security purposes and for monitoring NetPoint System usage. Audit files enable you to detect intrusion threats, monitor security, and create business-level reports by integrating with third party products such as Crystal Reports.

authentication

The process of establishing and proving a user's identity. In the world of brick-and-mortar business transactions, this process is often a visual one (comparing the information on a document such as a driver's license with the bearer of that document.) Electronic, online transactions require a more complex authentication method.

authentication authority

An authentication statement asserts that the subject of the assertion, the user, has logged in with a given identity. The subject's identity has already been authenticated at a particular time by a security service. The security service used to authenticate the subject is referred to in SAML as an authentication authority.

authentication plug-in

A set of instructions for performing authentication. NetPoint provides default authentication instructions. Customers can also write their own plug-ins using the Authentication Plug-in API.

Authentication Plug-in API

A NetPoint standard API used to create customer-defined authentication plug-ins. For use within authentication schemes and chained authentication processes to be used by the NetPoint application server.

authentication rule

A named logic flow that describes the process to get an authentication result, generally over a set of resources within a NetPoint policy domain. An authentication rule generally contains an authentication scheme.

authentication scheme

A named set of plug-ins that defines the challenge method and steps required to authenticate a user.

Authentication Services

Provide a generalized means to authenticate users and systems when they try to access resources protected by NetPoint. These services support not only the basic username and password authentication method but also stronger methods such as digital certificates or SecurID cards. You can further expand the authentication capabilities with the NetPoint Authentication Plug-in API. Once a user is authenticated by the authentication services, NetPoint creates a single-sign-on session for the client that frees the user from having to sign on again to access other resources or applications.

authorization

The process that determines the access permitted to users after they have been authenticated.

authorization plug-in

A set of instructions for performing authorization, which can be included in an authorization scheme to extend the set of NetPoint default authorization schemes. Customers can write their own plug-ins using the Authorization Plug-in API.

Authorization Plug-in API

A NetPoint standard API, used to create customer-defined plug-ins for use within authorization schemes to be used by the NetPoint application server. This API allows customers to extend policy evaluations through dynamic callouts to custom code. As an example, a policy administrator can set a policy that allows an end user to access some resource if their bank balance exceeds a certain amount. Use the Authorization Plug-in API to check the bank balance that resides in a database.

authorization rule

A named logic flow that describes the process to be followed to get an authorization result, generally over a set of resources within a NetPoint policy domain. An authorization rule usually contains an authorization scheme.

authorization scheme

A named link to a shared library holding an authorization plug-in that defines a method to be used to authorize a user.

Authorization Services

Once a user or system is authenticated, these services specify what information they can access. They deliver the centralized, consistent management of policies across applications, while providing users granular access to Web-based content and resources. This capability gives growing e-business organizations the control and consistency they require for secure, sensitive information, while helping ensure that users and systems have easy access to the information and applications they need.

Authorization statement

Also referred to as an authorization decision statement, it asserts that a security service has granted or denied the subject authority to perform one or more actions on a specified resource. In SAML terms, this security service is referred to as a policy decision point or PDP.

auxiliary object class

An object class that contains supplementary attributes not necessarily found in a structural object class; also called mix-in classes because they allow additional attributes to be "mixed into" an existing class. An auxiliary object class cannot stand by itself. Its attributes must be assigned to an entry that is based on an existing object class.

CA (Certification Authority)

Certifies the mapping of the public and private key pair with the subject identity (user name, email, machine name, and so on) by digital signature.

cert

A transport security mode under which the data transferred between points is encrypted using SSL and a public key certificate.

certificate

A collection of data used for authentication, which uniquely associates an entity (for example, an individual, a company, or a machine) with a public encryption key. The ITU-T Recommendation X.509 is the most widely used format for providing this information. A certificate is issued by a CA.

Certificate Management Services

Allow customers to issue, revoke, and renew certificates in conjunction with user life cycle management and organizational processes. They allow customers to have a turnkey PKI rather than having to set up complex infrastructures (such as LCAs) for managing certificates.

class

In object-oriented programming, a class is a template definition of the method and variable in a particular kind of object. Specific to NetPoint, the Access Server API uses a library based on Java classes. For directories, see object class.

class attribute

The attribute that links search results to a profile.

Cloning

Instead of using the command line or the installation GUI to install a NetPoint component, you can automatically install a component by cloning the configuration of an already-installed component. Cloning creates a copy of a component on a remote system using an already-installed component as a template.

CMS (Cryptographic Message Syntax)

The Internet standards track protocol that is used to digitally sign, digest, authenticate, or encrypt arbitrary messages.

component

A part. For NetPoint, any of its major out of the box parts, such as the Identity Manager within the COREid System or the Access Manager within the Access System.

configuration DN

The node in the directory tree under which the schema information that defines all NetPoint operations is stored.

container

An object in an LDAP directory that contains other objects. For example, the object `dc=yourcompany` may contain the `ou=marketing` and `ou=engineering` objects. These objects may in turn contain other objects.

container limit

Specifies the maximum number of objects that a container can hold.

COREid Data Anywhere

The COREid data management layer (COREid Data Anywhere) aggregates and consolidates data from RDBMS and LDAP directories into a virtual LDAP tree that can be managed by the NetPoint Identity System and used to support authentication and authorization using the NetPoint Access System. COREid Data Anywhere supports multiple LDAP environments, RDBMS databases, and split directory profiles. See the *NetPoint Integration Guide*.

COREid Server

This stand-alone server (of which there can be several instances) processes all the requests related to user identity, group, organization, and credentials management requests

CRS (Certificate Request Syntax)

The PKCS standard (#10) that defines the information content and format required in a subscriber's application for a certificate.

CSV (character-separated value)

A method of representing data that was originally stored as a number of variable length fields within a record. The data is extracted as a series of variable length text strings, separated by some defined character (often a comma). Also a file extension type, as in `myfile.csv`.

Data Management Services

Allow companies to set fine-grained attribute-level access controls for managing users, groups, and organizations. Setting attribute-level access controls determines self-service and modify rights. Customers can also specify a restricted searchbase used for display and modification of information for different audiences. These services reduce the costs of identity administration and enforce security for data changes.

data transport mode

See transport security mode.

data type

A syntax type describing how the values for an attribute are stored. NetPoint supports the following data types: Binary, Distinguished Name, Integer, Postal Address, String Case-insensitive, String Case-sensitive, and Telephone. The data type helps determine what display type NetPoint uses to portray that attribute.

deactivate

In the NetPoint environment, deactivate means to make objects inaccessible but not remove them from the directory. For example, users who have had their identity profiles deactivated cannot log in to the system, and their identities are not found during searches.

deactivate user

The immediate removal of a user’s access privileges. Deactivation is done system-wide and without going through standard workflow processes.

default audit rule

The audit rule that applies to a policy domain if there are no more specific audit rules defined for the domain. Also called the master audit rule.

default authentication rule

The authentication rule that applies to a policy domain unless there are more specific authentication rules defined for the domain.

default authorization rule

The authorization rule that applies to a policy domain unless there are more specific authorization rules defined for the domain.

default rules

Blanket rules that apply to all resources within a policy domain, created to ensure that access is always controlled. The default rules apply for authentication, authorization, and auditing, unless overridden by more specific rules.

delegated access administrator

See access administrator.

delegated identity administrator

Administrator with responsibilities delegated by the master identity administrator. Delegated identity administrators have responsibilities for the Configuration tab in each of the NetPoint COREid System managers (User Manager, Group Manager, and Organization Manager). This includes delegation administration, attribute access control, and workflow definition.

delegation

The sharing of authority. The authority to change directory information or perform tasks can be delegated. Also, the authority to delegate can itself be delegated. For example, the NetPoint system administrator delegates responsibility for the COREid System and the power to delegate to a master identity administrator who might then delegate the power to start certain workflows to a delegated identity administrator.

delete

To remove the profile information for an object from the LDAP directory. User profiles must be deactivated before you can delete them. Oblix recommends you archive your profiles before you delete them.

derived attribute

A stored pointer from an entry in one object class to a target entry in another object class, based upon matching information in the two classes.

directory

A directory is a specialized database optimized for frequent read operations. A directory organizes data in a hierarchical information model, represented as a directory tree. A tree contains entries, which are made up of attributes and their values.

directory administrator

The user responsible for maintaining the directory.

directory server

A server specifically designed to manage a directory of users and resources. The directory server provides for the retrieval and storage of data, in contrast to a web server that serves up pages from a Web site.

directory service

The collection of hardware, software, processes, and administrative policies required to make the directory's information available to users.

display name

For NetPoint, the user-provided descriptive text associated with an attribute that appears in reports and screens in place of the formal directory attribute name. For example, an attribute with the name `departmentnumber` could be shown as "Dept. #," "Department Number," or "DEP-ID" in the Display Name field.

display type

The format in which NetPoint displays stored directory information. Display types available to an attribute are determined by its associated data type and semantic type. Examples of display types are Check Box, Multi-Line Text, and Radio Buttons.

distinguished name (DN)

A string that uniquely identifies each entry in an LDAP directory. DNs are organized in a hierarchy; each consisting of the name of an entry plus a path of names tracing the entry back to the root of the DIT.

DIT (directory information tree)

The directory's hierarchical structure, containing all data objects.

DLL (dynamically linked library)

See DSO (dynamic shared object)The term DLL is more common in the Windows environment, but the two terms are synonymous.

domain

See policy domain.

domain attribute

Domain attributes help you specify mutually exclusive sets of users, regardless of their location on the directory tree.

DSO (dynamic shared object)

The generic term for a library of software routines and/or data resources that has been specifically packaged to be linked with application programs when they are loaded by the operating system, or later when explicitly requested by the applications. If many running programs require services from the same library, the operating system can share elements of the library, and achieve significant savings in resources. Synonyms: DLL (dynamically shared library); .so (pronounced dot-ess-oh)

dynamic group

A group whose list of members is dynamically generated (for example, by exercising an LDAP rule). Group membership can vary as users meet or do not meet the membership criteria.

dynamic member

A member of a dynamic group.

End User

The basic NetPoint user-type.

Dynamic Participants

One or more users selected on the basis of runtime LDAP-attribute values or business logic. All possible sets of dynamic participants for a given step are specified by person, group, role, or rule in a workflow plug-in or application, which executes when workflow execution reaches that step.

End User

The basic NetPoint user-type.

entry

The most basic unit of information stored in a directory. Consists of one or more attributes and their values.

embedded virtual data source

A virtual object that VDE "sees" as a target data store it can present to NetPoint or federate in a virtual directory, then present to NetPoint. Each embedded virtual data store aggregates two or more target data stores. The three types of embedded virtual data stores are: split profile, native RDBMS Join, and native RDBMS View. In general, embedded virtual data stores are suitable for authentication and authorization activities only, because they necessarily involve secondary data sources, which are sometimes not available for the full range of NetPoint identity management activities.

fat tree

A directory tree structure that contains many container objects all at the same level. For example, 150 organizations, each holding a few people, within a company.

Federation

A method by which VDE makes a data source visible in the virtual directory it presents to NetPoint. All the data for a given user profile comes from a single data store such as an LDAP directory, a single-table database, or an embedded virtual data source. Different user profiles can come from different federated data stores.

Filter Builder

NetPoint feature that helps users create dynamic LDAP filters.

flat tree

A directory tree structure that contains a large number of objects under one container. For example, 150 people within a single organization within a company.

granting rights

The process of assigning view, modify, and change rights to other users.

Group Manager

This application allows companies to create/ delete groups, delegate group administration, and allow users to subscribe/unsubscribe from groups. Group management can be delegated.

group type

A label describing how group content is constructed. NetPoint Group Manager supports static, nested, and dynamic group types.

host ID

The label by which a computer can be identified. Labels include a host URL (such as `oblix.com:80`) and IP address (such as 111.111.11.1:80).

Identity Event Plug-in API

Allows customers to extend the business logic of the NetPoint COREid System by calling out to other systems before or after an event happens in the COREid System. Some of the uses of this API are to: bring data from external systems back into NetPoint; do data validation; and pre-populate fields based on other information provided.

identity management

The creation, removal, and ongoing changes of identity information relating to individual users, groups, and organizations. The determination of whether or not a person qualifies for an access privilege. This can be determined by a specific user attribute value, membership in a group, and/or association with an organization.

identity profile

A collection of directory information describing a user object, such as a telephone number, password, location, and reporting relationship. See also profile.

identity server

Previous name of the COREid Server. See COREid Server.

Identity Workflow

Allow customers to have a flexible workflow engine to which they can map their business processes without restrictions. Users and systems can submit requests that can go through multiple steps and be routed internally and/or externally. Customers can set workflow definitions for:

Creating, deleting, and modifying users, groups and organizations

Self-registration of users and organizations

Subscribing to groups and unsubscribing

Issuing, revoking, and renewing certificates

IdentityXML

Allows applications and systems to access COREid System functionality programmatically through XML. You can access the COREid System functionality without having to go through a Web browser. Applications and systems can access or modify centralized information about users, groups, organizations through XML. IdentityXML allows for cross firewall integration without the need to expose the customer directory.

integration Services

Allow developers to leverage the capabilities of NetPoint across all of their applications and e-business efforts and extend the value of NetPoint by providing integration points with other vendors' systems and applications. These services consist of: Access Server API, Authentication Plug-in API, Authorization Plug-in API, Identity Event Plug-in API, IdentityXML, Access Management API.

ISAPI (Internet Server Application Procedural Interface)

An Internet web server extension, which NetPoint uses to communicate with Microsoft Internet Information Server (IIS). ISAPI extends the functionality of IIS by allowing programmers to create modules that add or replace functionality, such as authentication, authorization, error logging, or content generation.

LCA (local Certificate Authority)

A CA located within the same firewall as your NetPoint installation.

LDAP (lightweight directory access protocol)

A standard protocol for managing information in a directory.

LDAP filter

A string of characters interpreted by LDAP to generate custom search results. Also known as an LDAP rule.

LDAP rule

See LDAP filter.

LDAP URL rule

In the Access System, a rule which follows the formal LDAP URL syntax and specifies a host, port and user combination that can be accessed.

LDIF (LDAP Data Interchange Format)

A file format used to import or export data from an LDAP directory or database. LDIF files are ASCII text files that represent data in a format that is recognizable to an LDAP directory or database.

localized access control

A NetPoint feature that lets an administrator restrict users and groups to searching only a permitted domain within the LDAP directory. It also restricts delegated administrators to hiring only within permitted domains.

logging

The process of collecting information about NetPoint program execution to assess the health of NetPoint System components.

administrative changes to policies, configuration, and other events. NetPoint helps administrators to specify the types of events that are logged for each NetPoint application.

LRA (local Registration Authority)

The server that captures the CSRs from multiple clients and forwards them to the CA. With a NetPoint installation, NetPoint serves as the local RA. The Oblix LRA interacts with the CA (local or remote) to automate the process for certificate enrollment, certificate renewal, and certificate revocation. Oblix selects the correct access method to different CAs, depending on customers' configuration.

master access administrator

The administrator who configures the NetPoint Access System, including WebGates, Access Servers, authentication parameters, and the initial set of policy domains. In addition, master access administrators assign individuals to the delegated access administrator role. Master access administrators are assigned by the NetPoint system administrator. See also access administrator.

master audit rule

The audit rule that applies in the absence of audit rules created at the policy domain level.

master identity administrator

The administrator authorized to configure the NetPoint COREid System. In addition, master identity administrators assign individuals to be delegated identity administrators. Master identity administrators are assigned by the NetPoint system administrator.

monitoring

The process of collecting Small Network Monitoring Protocol (SNMP) data for assessing the health of a network hosting a NetPoint system. See also SNMP Agent.

Multi-level Identity Delegation

Enables the delegation of identity administration to multiple levels of individuals throughout an e-business network. You can delegate rights such that some users can pass on the rights they have been given or a subset of them (delegate rights), or you can prevent someone who has received rights from passing them on to others (grant rights). There is no restriction on the number of delegation levels. Delegated identity management lowers overall administrative costs by distributing work across the entire e-business network.

Multi-level Policy Delegation

Enables the delegation of access policy administration to multiple levels of individuals throughout an e-business network. You can delegate rights such that some users can pass on the rights they have been given or a subset of them (delegate rights), or you can prevent someone who has received rights from passing them on to others (grant rights). There is no restriction on the number of delegation levels. Delegated policy management lowers overall administrative costs by distributing work across the entire e-business network.

multi-table database

A database that stores in more than one table the user profile attributes that get mapped into the virtual directory.

NAP (NetPoint access protocol)

The protocol governing communications between the NetPoint Access System and a web server.

nested group

A group that contains other groups as members.

nested member

A member of a nested group. Membership indicates the nested group contains one or more groups that the member belongs to (either statically or dynamically).

NetPoint Access System (NPAS)

This system allows companies to do policy-based authorization and Web single sign-on. Companies can set up security policies to control access to Web and non-Web resources and audit the usage (such as applications, content, services, and objects in applications). It provides the following applications and components:

Access Manager

Access Server

WebGate/AccessGate

NetPoint COREid System

(Formerly: NetPoint Identity System) This system allows companies to create, remove, and manage ongoing changes of identity information relating to individual users, groups, and organizations. It also allows companies to manage which access privileges a user should get. The system provides the following applications and components:

User Manager

Group Manager

Organization Manager

COREid Server

OIS Client

WebPass

NetPoint Certificate Processing Server

NetPoint FEDERATEDid Layer

An integration layer within Oblix NetPoint that allows an enterprise to identify users from multiple authentication sources while maintaining tight control over access to Web-based applications and resources.

NetPoint Federation Services

Organizes an enterprise’s user identification policies to allow a wide range of associates such as vendors, distributors and customers to access protected resources using authentication proofs from a variety of sources.

NetPoint System Administrator (NPSA)

This component is used for Web-based administration and configuration of the overall NetPoint system.

NetPoint system administrator

The NetPoint superuser, who is empowered to configure the NetPoint deployment and assign administrative tasks. The NetPoint Administrator is assigned when NetPoint is initially installed and set up. Through NetPoint’s System Console, this person can create additional NetPoint Administrators and master access and master identity administrators.

NSAPI (Netscape Server Application Programming Interface)

The Internet web server extension that NetPoint uses to communicate with Netscape. NSAPI extends the functionality of Netscape servers by allowing programmers to create modules that add or replace functionality, such as authentication, authorization, error logging, or content generation.

object

An entity in an LDAP directory, such as a person, group, or other resources.

object class

A group of common objects in an LDAP directory. An example is the person object class, which groups all attributes describing individuals.

object class attribute

The attribute the NetPoint applications use to reference object profiles during operations (such as search). User Manager uses an attribute that contains a user's name. Group Manager uses an attribute that contains a group's name. Organization Manager uses an attribute that contains an organization's name.

Oblix

The NetPoint component that routes requests from the web server to perform transactions in NetPoint’s User Manager, Group Manager, and Organization Manager applications. This component is referred to as OIS.

Oblix NetPoint

The Oblix unified solution product, integrating identity management and Web access management for E-business networks. It contains two integrated modules: the NetPoint COREid System and the NetPoint Access System. The naming will change to COREid Identity System and COREid Access System.

OID (Object Identifier)

A unique value identifying an LDAP attribute.

OIS (Oblix Identity Server)

The service name for the Oblix Identity Server (also known as the COREid Server and COREid Identity Server).

open

A transport security mode where no authentication and no encryption is performed. The AccessGate does not demand any proof of the Access Server’s identity, and the Access Server accepts connections from all WebGates connected to it.

Optional attributes

During request processing, those attributes whose value specifications are defined as optional.

Organization Manager

This application allows companies to create and delete organizations and manage their ongoing changes. Organization management can be delegated.

Oblix Specific Data (OSD)

NetPoint configuration settings.

Password Management Services

Provide comprehensive password management. Customers can specify multiple password policies, constraints on password composition, configurable password validity period and notification, forced password change, lost password management setup, and password creation/change rules.

Personalization Services

NetPoint enables personalization and Web SSO for other applications through HTTP header variables and redirection URLs. When NetPoint authenticates and/or authorizes user requests, the URL it returns can contain HTTP header variables, redirection URLs, or encrypted cookies. The HTTP header variables can contain any user data stored under the authenticated user’s ID in the directory, thereby providing a rich source of information for personalization purposes on that particular user. The downstream application can decode this information and use it to personalize the user experience. You can also include a redirection URL in the URL returned by NetPoint after an authentication and/or authorization event. This redirection URL may take the user to another Web page, for example, tailored to the identity of the user. In addition to providing personalization services, an encrypted cookie can be included in the URL returned by NetPoint to enable Web single sign-on.

PKI (Public-Key Infrastructure)

A security infrastructure that provides services implemented by public key concepts and techniques.

plug-in

A component added to NetPoint to change or enhance its behavior.

policy

The set of authentication, authorization, and auditing rules that apply to one or more resource types within a policy domain. In the absence of a policy for a specific resource type, the default rules for all resource types in the policy domain apply.

policy base

The location in the DIT under which all Oblix policy data is stored.

policy-based authorization

The use of security policies for controlling access to Web and non-Web resources (such as applications, content, services, and objects in applications).

policy domain

A policy domain encompasses the resources you want to protect, the rules for protection, the policies for protection, and the administrative rights. Policy domains are defined in the Access Manager.

pooling

The process of defining a hierarchy of primary and secondary Access Servers. NPAS opens and closes connections to these Access Servers in order to evenly distribute the work load.

pooling Access Servers

The process of an Access Server opening or closing connections to Access Servers in order to maintain adequate load balancing.

Portal Inserts

Embeddable pieces of NetPoint functionality and workflows that are available as URLs and can be placed anywhere on a customer site or portal.

POST Profile

The Web Browser POST Profile sends an assertion requested by a destination SAML domain from the source SAML domain to the destination domain using the Web browser. This method sends the full assertion to the destination SAML domain as a hidden variable in a form. The browser submits the form to the destination SAML domain. For this reason, the Web Browser POST Profile is also referred to as the Push Profile or the form-based Push Profile.

pre and post processing (PPP)

External actions that can take place before or after a step in a NetPoint workflow. For example, an administrator can choose to have specific persons emailed after a workflow step takes place.

Presentation Services

Allow companies to customize the NetPoint user interface and to integrate NetPoint functionality seamlessly into their portals. These services include: Portal Inserts and PresentationXML.

PresentationXML

Allows the NetPoint product user interface to be completely customized. The product outputs XML, and you can combine this output the with the XSL style sheets that Oblix provides to allow the customer to change the interface to fit their needs.

profile

A set of attributes that describe an object.

query string variables

Variables that allow you to determine who can send certain input parameters to a program, which in turn can control the behavior of the program itself.

RA (Registration Authority)

The certification component that manages certificate management events such as enrollment, renewal, and revocation. An RA is composed of a Registration Server and Authentication Server. With a NetPoint installation, NetPoint serves as the local RA. Oblix interacts with the directory to store and publish certificates.

relative distinguished name (RDN)

The leftmost (bottom) attribute value in the DN.

reporting

The process of collecting NetPoint audit information in an SQL-compatible database and presenting this using one of the specially configured Crystal Report templates supplied by NetPoint.

request

An in-process workflow definition that was initiated by a user. Requests can include multiple tickets.

request ticket

See ticket.

Required attributes

When you are defining a workflow step, any attributes you set as required must have values assigned to them when a user processes this workflow.

resource

Within NetPoint, the information or activity that can be protected by the Access Server. A policy domain is an example of a protected information resource, a method within an application is an example of a protected activity.

rights

NetPoint Administrators can assign the following kinds of rights:

View: Users with View rights can view the name and value of an assigned attribute in an object profile.

Modify: Users with Modify rights can change the value of an assigned attribute in an object profile.

Notify: Users with Notify rights receive an email notification whenever an assigned attribute is changed.

Basic: Administrators with Basic rights can assign View, Modify, or Notify permissions to users for all attributes under their control.

Grant: Administrators with Grant rights can assign basic rights to users and other administrators for all attributes under their control.

Delegate: Administrators with Delegate rights can assign grant and delegate rights to users and other administrators for all attributes under their control.

roles

The predefined lists of users. Roles can include all users, all managers, direct reports, and so on.

root directory

The first URL prefix entered into the system. This is the starting point for all policy domains.

rules

In NetPoint, the list of conditions during which access is allowed or denied and to which end user(s) these conditions apply. Rules also govern the way in which auditing is done.

rule, LDAP

See LDAP filter.

rule, URL

See LDAP URL rule.

SAML (Security Assertion Markup Language)

A proposed standard for exchanging authentication and authorization information among disparate Web access management and security products. It is being standardized through the Organization for the Advancement of Structured Information Standards (OASIS).

SASL (simple authentication and security layer)

SASL provides a means for clients and servers to negotiate an authentication mechanism dynamically.

schema

A schema defines the type of information stored in a directory. It consists of object classes and attributes.

searchbase

The location in the DIT where users can begin their searches.

Selector

The NetPoint utility used to locate and select one or more users and/or groups.

self registration

The process a new user can employ to gain limited access to your system through the initiation and processing of a self-registration workflow.

self-service

The process of modifying attributes without the use of a workflow.

semantic type

Semantic types apply a NetPoint business rule to an attribute. Examples of business rules are reporting relationship and on-screen location of an end user’s photo and job title.

shared secret

The NetPoint feature that allows administrators to generate a cryptographic key that encrypts cookies sent from a WebGate to a browser.

signing authority

RSA signing identity that is hosted by the main domain site and can issue digital certificates to the associate domain site.

simple

A transport security mode where the communication between the WebGate AccessGate and the Access Server is encrypted using TLS v1 (Transport Layer Security, RFC 2246). WebGate and the Access Server authenticate one another using a global password, which must be the same across installations.

single sign-on (SSO)

The method of transparently accessing multiple protected web servers with only a single login. Users needing access to single-domain servers store a generated cookie, used for subsequent requests to the Web site. Users needing access to multi-domain servers store a cookie generated by a central Web login server; this is transparently done for each accessed server within the associated Web system.

single-table database

A single-table database does not necessarily refer to a database that contains just one table, but rather, a database that stores in just one table all the user profile attributes that get mapped into the top level virtual directory.

SNMP Agent

The Simple Network Management Protocol (SNMP) is an application-layer protocol that enables network devices to exchange information. By using SNMP-transported data (such as successful operations and failure conditions), administrators can monitor network performance and solve problems. The NetPoint SNMP agent enables you to implement SNMP-based data collection for the NetPoint COREid Server and Access Server.

split profile

A special type of embedded virtual data source created from more than one data source. Each data store contributes some of the attributes necessary to complete the full set of user profile attributes that gets mapped into the VDE virtual directory. These attributes can come from LDAP directories or database tables. All the NetPoint user schema attributes must reside in the primary data store, because not all NetPoint operations can be performed on the attributes in the secondary stores.

VDE can make a split profile visible to NetPoint as a standard LDAP directory. Alternatively, a split profile can be federated as part of a virtual directory. For an illustration, see the *NetPoint Integration Guide*.

SSL (Secure Sockets Layer)

A method for establishing an encrypted connection between a client and a server.

static group

A group whose member list is explicitly defined.

static member

A member of a static group.

Static Participants

One or more users assigned responsibility for completing a given workflow step. These users are specified in the workflow applet by person, group, role or rule.

structural object class

Structural object classes contain basic attributes required for use within NetPoint applications. When you create a tab within a NetPoint application, you must assign a structural object class to it.

subclassing

The process of creating a new object class based on an existing object class and specifying that the existing class is its superior. The new object class inherits the set of required attribute types, the set of optional attribute types, and the kind of object class from its superior.

subflow

Subflows are workflows spawned by another workflow. Subflows operate independently and can spawn subflows of their own.

substitute administrator

Substitute administrators are users who have permission to temporarily take all of your rights and responsibilities. This is useful in the case of vacations or extended leaves, where the job needs to be done but it would be too difficult administratively to remove all permissions from the absent employee and assign them to someone else.

super directory

A special type of virtual directory that facilitates namespace mapping and directory-wise searches. It can contain any combination of federated LDAP directories, RDBMS databases, and embedded virtual data sources. The embedded virtual data sources can be split profiles, native RDBMS Joins, and native RDBMS Views. The super directory, which is the only supported method for producing a single, contiguous searchbase aggregated from multiple data stores, connects to NetPoint by means of a VDE local store adapter. For details, see “virtual directory” on page 83.

superior

The class that another class inherits some of its characteristics from in the subclassing process.

Surrogate Participants

One or more users assigned workflow ticket-processing responsibilities whenever a given static participant or dynamic participant activates the Out of Office flag in his or her user profile. The surrogate receives incoming tickets as long as that Out of Office flag remains active.

synchronizing

Synchronizing allows you to harmonize two installations of the same NetPoint component when one is more up-to-date than the other. Synchronization can be used to upgrade or repair installations on similar platforms.

ticket

A pending activity for a user to perform (usually an administrator or delegated administrator). For workflows, the ticket ID contains an appended step ID number.

Time-based Escalation

Whenever a workflow ticket is not processed within a specified interval, responsibility for processing the ticket is transferred from the original participant who failed to act to a new participant, such as the manager of the original participant. If the new participant fails to process the ticket within the specified interval, the ticket is escalated again, and so on, until it ultimately reaches the NetPoint Administrator.

transport security mode

The method used to protect the information transfer path between two points, often a client and a server. In NetPoint, the transport security mode is most often used to highlight that the transfer path is secured (for example with SSL encryption) rather than left in the clear. See the NetPoint security modes open, simple, and cert.

trusted associate domain site

Associate domain site that has established a trusted relationship with the main domain site. It can require the main domain site to perform authentication as well as validate and decrypt the cookie generated by the main domain site after authentication.

untrusted associate domain site

Associate domain site that has not yet established a trusted relationship with the main domain site. It can not require the main domain site to perform authentication and cannot validate and decrypt the cookie generated by the main domain site after authentication.

URI

Uniform Resource Identifier - the generic term for the unique name of any resource on a network. A URL is one kind of URI.

URL

Uniform Resource Locator - a type of URI specific to the World Wide Web.

URL pattern

The fine-grained portion of the policy domain’s Web namespace is specified as a pattern. The specific URL pattern syntax is described in the NetPoint Administration Guide.

URL prefix

Starting point for your policy domain. The URL prefix maps to a directory on your web server’s file system.

User Action Steps

Workflow steps that require explicit (non-automated) processing by a step participant.

User Manager

This application allows companies to create, remove, and manage ongoing changes in user identities and access privileges based on the user profile. User identity administration can be delegated.

virtual directory

A logical, aggregated directory that presents user data drawn from multiple sources, just as if all that data came from a standard LDAP directory to which a customer-defined schema has been uniformly applied. For the purposes of NetPoint integration, VDE does not create permanent copies of user profiles outside the native data sources. Rather, VDE retrieves and transforms each user profile as it is requested by a NetPoint application. For details, see the *NetPoint Integration Guide*.

virtual directory schema

This is the schema developed by the customer for use by the top-level directory that VDE makes visible to NetPoint. It must be extended with the NetPoint user schema. Optionally, you can further extend the virtual directory schema with customer attributes drawn from the target data sources. For details, see the *NetPoint Integration Guide*.

VSAA (Verisign Auto Administration)

The main API NetPoint uses to process any VeriSign-related information.

VSAA Socket

The socket interface API from VeriSign.

Web resources

Any subset of an HTTP URL. Typically, they can be Web pages, directories, CGI scripts, or Web-enabled applications.

Web server

Program that, using the client/server model and the World Wide Web's Hypertext Transfer Protocol (Hypertext Transfer Protocol), serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests).

Web single sign-on

Single authentication to multiple resources (applications, content, services, objects in applications). To achieve single sign-on, customers centralize the security for various resources, so that developers can re-use the centralized information and avoid having a different security scheme and user database associated with each application.

WebGate

A NetPoint-provided out-of-the-box Web server plug-in access client that intercepts HTTP requests for Web resources and forwards them to the Access Server for authentication and authorization. You can create a custom AccessGate using the Access Server SDK. See also AccessGate.

WebPass

This component is a plug-in that is placed on the web server to shuttle information back and forth between the web server and the COREid Server.

workflow

The automation of procedures where information or tasks are passed between participants and programs according to a defined set of business rules. Introduced into Oblix's products to give customers the flexibility to tailor the operation procedures to match their business processes.

workflow actions

Each step within a workflow allows one action (approval, provide info, and so on).

workflow definition

The flow of responsibility, defined actions, and responsible individuals combined together to perform the process necessary to complete a workflow type.

workflow participant

All of the people, groups, roles, and so om that can take part in a workflow step, therefore receiving a ticket.

Index