Oracle® COREid Access and Identity

Installation Guide

10*g* Release 2 (10.1.2)
Part No. B19009-02

June 2005

ORACLE

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.
```

Contents

Preface

This installation guide provides information about basic installation and setup of COREid components on supported platforms. Included are considerations, prerequisites, preparation worksheets that you can complete to help streamline your experience, and step-by-step instructions to help ensure your success.

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

Read this guide if you will install any COREid component. You should be familiar 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

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.

Section I: Installation Preparation

1 NetPoint Installation Introduction

This chapter provides an introduction to Oblix NetPoint® installation. Topics include:

- "About NetPoint Installations" on page 23
- "About the Installation Process" on page 27
- "Installation Options" on page 29

Upgrading to NetPoint 7.0 is described in the *NetPoint 7.0 Upgrade Guide*.

Note: 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 and are discussed in the Oblix *SHAREid 2.0 Administration Guide.*

About NetPoint Installations

As described in the *Introduction to NetPoint 7.0 guide*, the NetPoint system includes the COREid System and Access System. The COREid System is required in all NetPoint installations. The Access System is optional.

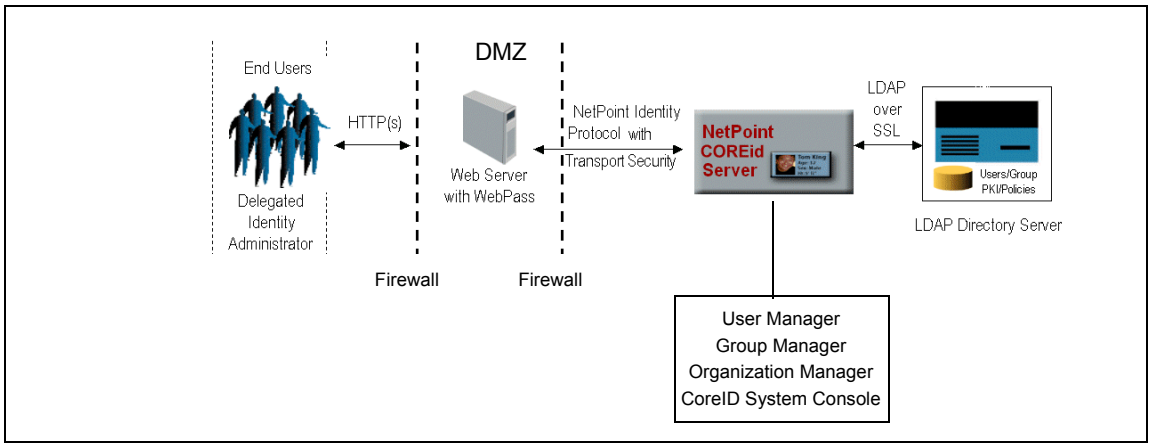
The applications that access sensitive data, for example, the COREid Server and Access Server, reside within the firewall. The directory server is isolated so it is not exposed. The only server outside the firewall (or in the DMZ) is a Web server with a WebGate or WebPass.

In a non-production or test environment, NetPoint components may be installed on one machine. 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 on separate machines, protected by the firewall. For better performance, the COREid and Access Servers should reside on different hosts.
- The Web servers, WebPass, WebGate and Access Manager reside in the DMZ.

Figure 1 illustrates the basic components of the COREid System. Transport security between COREid System components is provided over the NetPoint Identity Protocol (NIP). For more information, see "Securing NetPoint Component Communications" on page 45.

Figure 1 COREid System Components

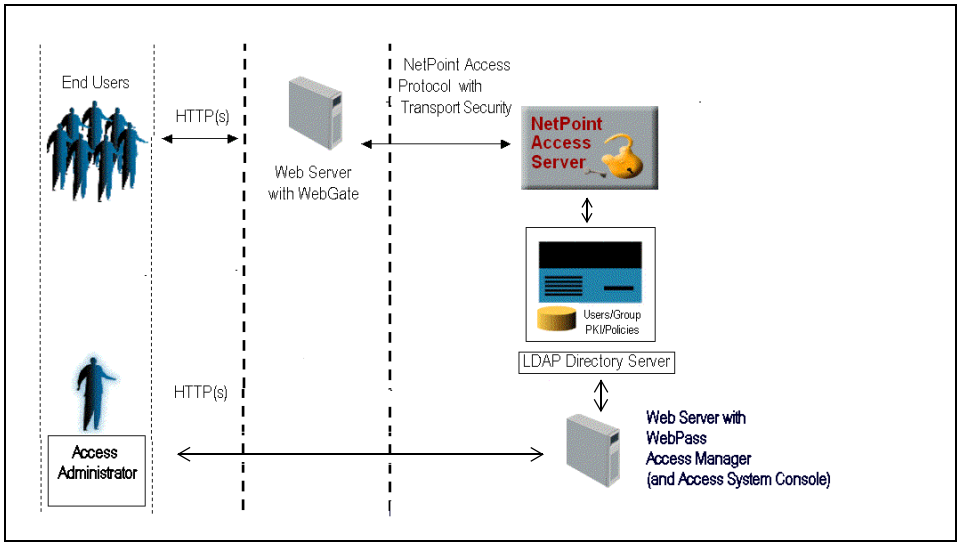


During COREid System installation and setup, the LDAP directory server is updated to include the Oblix schema with object classes and attributes for the NetPoint COREid System. On the same or separate directory servers, you will store various types of data. Communication between COREid System components and the directory server may be either open or SSL-enabled, as long as the same mode is used between each of the COREid Servers and the directory server. For more information, see:

- "Directory Server Requirements" on page 52
- "Data Storage Requirements" on page 59
- "LDAP and Virtual Directory Support" on page 68

The NetPoint Access System is optional. The Access System provides centralized authentication, authorization, and auditing to enable single sign-on and secure access control across enterprise resources. Figure 2 illustrates the basic components of the Access System. Transport security between Access System components is provided over NetPoint Access Protocol (NAP). For more information, see “Securing Directory Server Communications” on page 56.

Figure 2 Access System Components

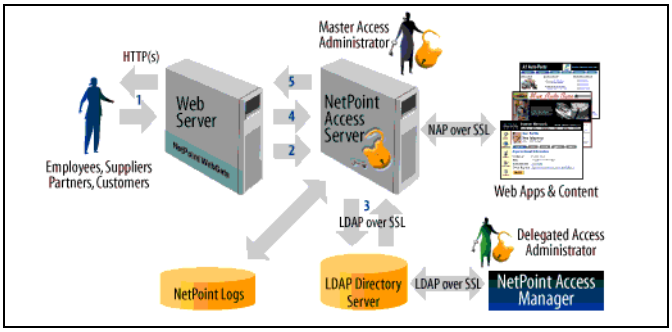


The Access System stores information about configuration settings and access policies in the directory server. This information is stored in a special policy branch of the directory information tree (DIT), which can be either in the same directory as the user information or on a separate directory server.

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 each Access Manager and the directory server. For more information, see “LDAP and Virtual Directory Support” on page 68.

Figure 3 and the description following it illustrate how the Access System works in concert during authentication and authorization.

Figure 3 Access System Functions



Process overview: When a user requests access

1. The 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 if the resource is protected, how, and whether 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 and the Access Server looks up the appropriate security policies, compares them to the user's identity, and determines 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 the Installation Process

You must install NetPoint components in a structured sequence. See:

- "Installation Guidelines" on page 27
- "Installation Sequence" on page 28

Installation Guidelines

The following guidelines will help ensure a smooth installation.

Task overview: Ensuring a successful installation

1. Review and complete all installation prerequisites, as described in "Preparing to Install NetPoint" on page 39.
2. Review installation options and decide which are best for your environment and installation, as described in "Installation Options" on page 29.
3. Review your directory, as described in:
   - "Directory Server Requirements" on page 52
   - "Data Storage Requirements" on page 59
4. Confirm that your environment meets all NetPoint requirements, as described in "NetPoint Requirements" on page 44.
5. Ensure that your environment conforms to directory server requirements, as described in "Directory Server Requirements" on page 52.
6. Verify that your environment conforms to platform requirements, as described in "Platform Requirements" on page 66.
7. Collect and record data about your environment and where the NetPoint components will be installed, as described in "Installation Preparation Checklists" on page 83.
8. Review and follow the recommended installation and setup sequence described in "Installation Sequence" on page 28, and start and stop services in the recommended sequence.

Note: If you are installing multiple instances of a NetPoint component, you can automatically install multiple instances after the first instance is installed and set up. See "Replicating Components" on page 241 for information about automated installation, cloning, and synchronizing NetPoint components.

Installation Sequence

The sequence of tasks you must complete to install NetPoint components is outlined in the following task overview.

Task overview: Installing NetPoint

1. Complete all prerequisites in “Preparing to Install NetPoint” on page 39.
2. Install the COREid Server, as described in “Installing the COREid Server” on page 99.
3. Install WebPass, as described in “Installing WebPass” on page 121.

Important: If you are installing NetPoint for use with COREid Data Anywhere, see the chapter on integrating NetPoint with the OctetString Virtual Directory Engine (VDE) in the *NetPoint Integration Guide* and complete all prerequisite tasks *before* you setup the COREid System.

---

4. Set up the COREid System to ensure that object classes and attributes appear in the directory server and that the COREid Server is working correctly with the WebPass, as described in “Setting Up the COREid System” on page 133.
5. Install and set up the Access Manager, as described in “Installing the Access Manager” on page 159.
6. Install the Access Server, which includes adding an Access Server instance in the Access System Console, as described in “Installing the Access Server” on page 187.
7. Install the WebGate, which includes adding a WebGate instance in the Access System Console and associating the WebGate with an Access Server before installation, as described in “Installing the AccessGate/WebGate” on page 199.
8. Install optional components, as described in:
   - “Section IV: Language Packs and Monitoring Tools Installation” on page 223
   - *NetPoint Developer Guide* (Access Server SDK installation and setup)
   - *SHAREid Administration Guide* (SHAREid installation and setup)

Important: Immediately after installation and setup, you can configure the NetPoint Access System to restrict the ability of users to access NetPoint itself. For details, see the *NetPoint 7.0 Administration Guide Volume 2*.

Task overview: Configuring NetPoint

1. Use NetPoint to define an administrator who can access the installed components, as described in the *NetPoint 7.0 Administration Guide Volume 1*.
2. Use NetPoint to protect NetPoint components and other resources, as described in the *NetPoint 7.0 Administration Guide Volume 2*.
3. Customize NetPoint, as described in the *NetPoint 7.0 Customization Guide.*
4. Complete one or more integrations, as described in the *NetPoint Integration Guide.*

Installation Options

This discussion identifies the options available to you during installation, and tells you where to find more information.

Task overview: Choosing your installation options

1. Install an optional Language Pack to enable the display of static data to users in their native language, as described in "Installing Optional Language Packs" on page 30.
2. Enable automatic updates of the schema using system-provided defaults, or input your own values for attributes during COREid System and Access Manager setup, as described in "Updating the Schema and Attributes Automatically vs. Manually" on page 32.
3. Install NetPoint using GUI mode or the command line, as described in "Installing from the GUI vs. Command Line" on page 34.
4. Install multiple instances of NetPoint components manually or use an automated installation method for multiple instances, as described in "Replicating an Installed Component" on page 36
5. Provide more security for communications between NetPoint components, as described in "Securing NetPoint Component Communications" on page 45.
6. Provide greater security for communications between NetPoint and the directory server, as described in "Securing Directory Server Communications" on page 56
7. Install NetPoint 7.0.

Important: Upgrading to NetPoint 7.0 is discussed in the NetPoint 7.0 Upgrade Guide.

Installing Optional Language Packs

NetPoint provides the capability to localize NetPoint applications to display static data such as error messages and display names for tabs, panels, and attributes to users in their native language. The default language for NetPoint is English, which requires no special installation or configuration. Additional Language Packs can be installed together with NetPoint components or independently, after NetPoint installation and setup.

Note: NetPoint supports UTF8 data but not multi-byte languages such as Chinese, Japanese, and so on. Contact Oblix for information about specific Language Packs.

Installing additional languages to enable multi-language functionality in NetPoint may be done either during or after installation of each NetPoint component.

Installing additional languages to enable multi-language functionality in NetPoint may be done either during or after installation of each NetPoint component.

For each additional language that Oblix supports, one Language Pack installer is provided for the COREid System and one is provided for the Access System. You must run the Language Pack installer more than once for each system. For details, see “Task overview: Installing Language Packs in concert with NetPoint” on page 31.

During installation, a *langTag* directory is created in the file system under *Component_install_dir*\identity|access\oblix\lang, where *langTag* represents specific language, such as en-us or fr-fr. See “Installed Files” on page 230 for an example. The \lang directory and the \lang\en-us and \lang\shared subdirectories are included with all NetPoint components. A *langTag* subdirectory includes the same type of content as \en-us, only localized.

A language entry is created for each installed language under the Oblix node in the LDAP directory as follows: obid=*langTag*, *configDN*, where *configDN* is the configuration DN in the directory.

The obnls.lst configuration file is updated in *Component_install_dir*\identity|access\oblix\config, where *Component_install_dir* is the directory where the main NetPoint component is installed and identity|access represents the appropriate suffix appended to the path during installation. In the sample obnls.lst file below, English is the only language:

```
BEGIN:vCompoundList
default:en-us
languages:
BEGIN:vList
en-us
END:vList
en-us:
BEGIN:vNameList
```

```
#
# Relative to <INSTALLDIR>
#
sortRulesFile:
#obDateSep:-
#obDateType:ObMDYDate
#
# For future use;
#
dirPath:en-us
END:vNameList
END:vCompoundList
```

The task overview below outlines the procedures needed to install Language Packs at the time you install NetPoint components. The NetPoint component installer will call the Language Pack installer silently and complete the Language Pack installation during NetPoint component installation.

Task overview: Installing Language Packs in concert with NetPoint

1. Before NetPoint installation, move any Language Pack installers into the same temporary directory as the NetPoint component installer as described in individual installation chapters in this guide.
2. Before NetPoint installation on Unix systems, ensure that the Language Pack has execute permissions as described in installation chapters in this guide.
3. During component installation, you are asked to select a Default Locale and additional locales based on the Language Pack installers detected. For example:

4. After installation, you must configure the COREid services to use additional installed languages by manually entering the display names for labels and attributes in the COREid System Console, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

Note: If you are installing the COREid Server with a Language Pack on a Unix system, you must ensure that the Language Pack has execute permissions before launching the main installer. For example:
chmod +x "NetPoint7_0_FR_sparc-s2_LP_COREid_System"

You may also install Language Packs independently, after NetPoint components have been installed and setup.

Task overview: Installing a Language Pack independently

1. Install NetPoint components, as described elsewhere in this guide.
2. Run the COREid System Language Pack installer for each installed COREid Server and installed WebPass, as described in "Installing the Language Pack Independently" on page 228.
3. Confirm that the installed languages are enabled, as described in "Confirming Language Status" on page 231.
4. Run the Access System Language Pack installer on each installed Access Manager, Access Server, and WebGate as described in "Installing the Language Pack Independently" on page 228.

Updating the Schema and Attributes Automatically vs. Manually

During COREid Server and Access Manager installation, you are asked if you want to automatically update the schema with the Oblix branch. The schema update must occur before you begin the setup process.

Note: Oblix recommends that you update the schema automatically during installation to obtain NetPoint-specific object classes and attributes. If you decline the automatic update during installation, a Schema Changes page appears at the beginning of the COREid System and Access Manager setup process.

Custom schema changes must be added after the COREid installation because the COREid Server installation changes the schema. During COREid System and Access Manager setup, you are prompted to configure various object classes. For example, the NetPoint COREid System requires attributes assigned to the Full Name, Login, and Password semantic types for Person and Group object classes. Oblix recommends that you automatically configure attributes using the Auto Configure option during setup to save time and avoid errors. You can reconfigure the attributes afterward if needed.

Automatically configuring attributes is a single step in the installation and setup processes, as shown in Table 1.

Table 1 Automatically Configure the Schema

NetPoint Component	Automatic Schema Configuration
COREid Server installation	Select "Yes". For second and subsequent COREid Servers, select No.

Table 1 Automatically Configure the Schema

NetPoint Component	Automatic Schema Configuration
WebPass installation	There are *no* options for the schema.
COREid System set up	Select Auto Configure when the option is offered. After setup, you may reconfigure attributes, if needed.
Access Manager installation and set up	Select Auto Configure when the option is offered. After setup, you may reconfigure attributes, if needed.
Access Server installation	There are *no* options for the schema update.
WebGate installation	There are *no* options for the schema.

Manually configuring attributes occurs after installation, during the setup process, and requires one or more ldif files located in:

COREid_install_dir\identity\oblix\data.ldap\common
AccessManager_install_dir\access\oblix\data.ldap\common

Each ldif file is prefixed with a specific directory server type, as shown in Table 2 In most cases, you use the ldapmodify tool to perform the update. For example:

ldapmodify –h *DS_hostname* -p *DS_port_number* -D *bind_dn* -w *password* -a –c *DS_type*_oblix_schema_add.ldif

Table 2 provides details about the schema update files needed for each directory server type. Included are any index files required for Oblix data or user data.

Table 2 Manual Schema Update Files

Directory Server Type	Manual Schema Update Files
Active Directory	ADSchema.ldif (*Windows 2000 only*) ADdotNetSchema_add.ldif (*Windows 2003 only*) ADAuxSchema.ldif (*Windows 2003, statically-linked auxiliary classes*) ADUserSchema.ldif **Note**: The Active Directory schema is extensible using Ldifde.exe. For more information, see “Installing NetPoint with Active Directory” on page 379.
ADAM	ADAM_oblix_schema_add.ldif ADAM_user_schema_add.ldif ADAMAuxSchema.ldif (*statically-linked auxiliary classes)* **Note**: The ADAM schema is extensible using Ldifde.exe. For more information, see “Installing NetPoint with ADAM” on page 407.

Table 2 Manual Schema Update Files

Directory Server Type	Manual Schema Update Files
COREid Data Anywhere	VDE_user_schema_add.ldif See the *NetPoint Integration Guide* for details about: • Integrating NetPoint with OctetString Virtual Directory Engine (VDE) • Prerequisites and NetPoint installation with VDE • schema.oblix.xml • Adapter and mapping script templates • DN conversion program and configuration file to patch user and group DNs in the Oblix tree for use with VDE in *existing* NetPoint installations
IBM Directory Server	V3.oblix.ibm_at.ldif V3.oblix.ibm_oc.ldif V3.user.ibm_at.ldif V3.user.ibm_oc.ldif
Novell Directory Server	NDS_oblix_index_add.ldif NDS_oblix_schema_add.ldif NDS_user_index_add.ldif NDS_user_schema_add.ldif
Siemens DirX **Note**: Indexes require 2.5 MB and grow. For more information, see “Data Storage Requirements” on page 59	DirX_oblix_schema_add.ldif DirX_oblix_index.txt DirX_user_schema_add.ldif (required only if user data is on a different directory instance) DirX_user_index.txt
Sun Directory Servers	iPlanet_oblix_schema_add.ldif. iPlanet_user_schema_add.ldif iPlanet5_oblix_index_add.ldif iPlanet5_user_index_add.ldif

Installing from the GUI vs. Command Line

Regardless of the method you choose to install NetPoint components, the process is the same and the sequence and prompts are detailed in this manual. Any differences will be identified as they occur.

- Installing from the GUI is known as GUI mode installation, as discussed under “GUI Mode” on page 35.
- Installing from the command line is known as console mode installation, as discussed under “Console Mode” on page 35.

Different installation packages are available for NetPoint components, depending on your platform and Web server. The sequence of events and messages are the same regardless of the mode you choose for installation.

GUI Mode

You download the software from the Oblix Customer Care Web site:

- GUI mode is the default for Windows systems when you select the installation package. For example:

  NetPoint7_0_win32_COREid_Server

- GUI mode may also be used with Unix systems by appending one of the following parameters to the install command: -gui or -awt. For example:

  ./NetPoint7_0_sparc-s2_COREid_Server -gui
  ./NetPoint7_0_sparc-s2_COREid_Server -awt

  Note: When you start a GUI mode installation on a Unix system, you may receive warnings regarding fonts and scroll bars. These warnings refer to a purely cosmetic change and may be ignored.

Due to known problems with third-party Installshield's ISMP framework, if any inputs supplied during installation contain the character $, the installer might interpret it unpredictably. For example, if the bind password supplied during the schema update for the first COREid Server is Admin$$, ISMP interprets this as Admin$ while invoking the schema update tool and the update fails citing a “bad credentials error(49)”. If this problem is observed during invocation of a particular tool, you may run that tool from the command line.

Note: Every NetPoint installer that uses the same password may also fail with a credential problem of some type.

Console Mode

You may choose to use console mode when installing NetPoint components on Unix and Windows systems. For example:

- Console mode is the default for Unix systems, for example:

  ./NetPoint7_0_sparc-s2_COREid_Server

- Console mode may also be used with Windows systems when you use a command window. For example, issue the following command with the -console parameter:

  NetPoint7_0_win32_COREid_Server -console

Note: During a console mode installation, you will be instructed to:
Press 1 for Next—1 is the default if you press the Enter key.
Press 3 to Cancel
Press 4 to Re-display the information
Occasionally, you will be asked to specify an option number then enter zero, 0, to confirm your choice.

Replicating an Installed Component

Rather than manually installing every instance of a NetPoint component, you can replicate the configuration of one instance to another after installation and setup of the first instance of a particular component.

There are three methods to choose from:

- Automate the installation process using a file that contains installation parameters (known as installing in *silent mode*).
- Clone the configuration.
- Synchronize two components or parts of two components.

Silent Mode

Silent mode permits installation without user intervention. The NetPoint installation script takes option and configuration information from a silent mode option file.

Important: Silent mode is intended for new NetPoint installations only.

For more information on silent mode, see “Replicating Components” on page 241.

Cloning and Synchronizing Components

You can also replicate an installed component by *cloning* it, or you can *synchronize* two components or parts of two components.

For more information, see “Cloning and Synchronizing Installed Components” on page 283.

Upgrading from a Previous Version of NetPoint

When you start installing a component and specify a target installation directory that contains a previous version of NetPoint, the component is detected and you are asked if you want to upgrade that component to NetPoint 7.0.

- To avoid an upgrade, you must specify a new installation directory path.
- To accept the upgrade and continue, see the *NetPoint 7.0 Upgrade Guide*.

2 Preparing to Install NetPoint

This chapter provides important information you need to prepare your environment before starting the installation process for NetPoint components. Topics include:

Note: Failure to complete all prerequisites may adversely affect your NetPoint installation.

For an overview of NetPoint components, features, functions, audiences, and manuals, see the Introduction to *NetPoint 7.0 Guide*. Upgrading to NetPoint 7.0 is described in the *NetPoint 7.0 Upgrade Guide*.

Installation Prerequisites

You can help ensure a successful installation by completing the following prerequisites before you install NetPoint.

Task overview: Preparing to install NetPoint

1. Synchronize the host clocks if you are installing across multiple machines, as described in "Synchronizing System Clocks" on page 41.
2. Choose your installation directory path names, as described in "Choosing an Installation Directory" on page 43.
3. Decide which installation options are best for your environment, as described in "Installation Options" on page 29.
4. Create a Web server instance and refer to "COREid and Access System Requirements" on page 45.

   Creating new instances of your Web server and directory server ensures it is easier to make changes without stopping the service for other applications.
5. Create a supported directory server instance, as described in "Directory Server Requirements" on page 52 and your vendor documentation, and define at least one administrator-level user on your directory server. In addition:
   - SSL communications between the COREid Server and the directory server require that you secure the directory server instance with a certificate.
   - SSL is required for ADAM to support password changes.
   - SSL is not required for Active Directory ADSI configurations.
6. Prepare the environment for the COREid Server and Access Server services, as described in "COREid and Access System Requirements" on page 45.
7. Review the latest release notes and the Oblix Customer Care Web site for up-to-date information on platform support.
8. On Unix platforms, confirm that the right commands are installed and verify the user name under which your Web server runs. For example:

   a) Locate the following commands (usually found in /usr/bin, /usr/sbin, or /usr/csb) and make sure their location is included in the search path:

      sed, tar, cp, ls, mkdir, rmdir

   b) The user name under which your Web server runs could be nobody, root, or some other user name, such as Web. You can determine this by checking your Web server configuration files or by running your Web server's administration console and looking under View Server Settings.
9. Download the NetPoint software from the Oblix Customer Care Web site, as described in "Downloading NetPoint Components" on page 44.

10. Collect and document information about your environment to provide during the installation process, as described in “Installation Preparation Checklists” on page 83.

Synchronizing System Clocks

If you plan to install NetPoint components across multiple machines, make sure all system clocks are synchronized. This is particularly important if you will be running the software in Cert or Simple mode.

Important: Each secure request includes a timestamp. Differences in system clocks could cause all requests to the COREid Server to be rejected.

For example, if the Web server clock is set ahead of the COREid Server clock, a login request sent from the WebPass plug-in on the Web server will contain a time that, to the COREid Server, has not yet occurred. The same is true for the Access System. If a Web server clock is ahead of the Access Server clock, a request sent from the Access Manager to the Access Server will contain a time that, to the Access Server, has not yet occurred.

For successful operation:

- Ensure all machines are synchronized within 60 seconds.
- Ensure each machine running a WebGate is not running ahead of the Access Servers with which it is associated.
- Confirm that all machines running the WebPass component are not running ahead of the COREid Servers with which they are associated.
- Confirm that all machines running the WebGate component are not running ahead of the Access Servers with which they are associated.

About the Network Time Protocol

To synchronize NetPoint components across geographically diverse time zones, you can use the Network Time Protocol (NTP). NTP can synchronize the time on machines to within a few milliseconds. For more information about time synchronization, go to the Web site:

http://www.ntp.org/

and the comp.protocols.time.ntp news group.

An ntp.conf file at minimum would contain the following:

server <*some NTP server name*>.com
driftfile /etc/ntp.drift

Instructions for creating the ntp.conf file can be found at the following locations:

- http://www.sun.com/products-n-solutions/hardware/docs/html/816-3626-10/after.html
- http://www16.boulder.ibm.com/pseries/en_US/files/aixfiles/ntp.conf.htm
- http://www.developer.ibm.com/tech/faq/individual/0,,2:14789,00.html

Unix machines use UTC (also known as GMT) internally and convert to the local time that is needed on the display. Windows machines keep the clock in local time, but NTP synchronization programs compensate to ensure accurate times on Windows.

On Unix Systems

All Unix operating systems ship with a version of NTP. To configure NTP on Solaris, create an ntp.conf file. The name of the ntp.conf file to use the Solaris provided NTP daemon is /etc/inet/ntp.conf. Once this is created, xntp is started automatically at boot time.

- **On HP-UX**—Use sam to start NTP.
- **On AIX**—Create an /etc/ntp.conf file and enable or create a start script.
- **For all Unix platforms**—Get the current (and more secure) version of the NTP daemon from http://www.ntp.org/.

On Windows Systems

Windows machines synchronize their times automatically with their domain controller using a version of NTP. The domain controller needs to be configured to synchronize with a time source.

To obtain an official time for synchronization across your network many ISPs provide a time service for their customers.

- NTP, which has a list of open stratum-1 servers available at http://www.ntp.org.

  However, that this site may not be the most secure choice. For an example of a time-based attack, imagine unexpiring a cookie by spoofing the time to be earlier than the real time.

- GPS-based clocks, which use satellite technology to provide very accurate time, are available.

  These clocks can be used to set your whole network to the same time. GPS technology requires very accurate times; each satellite contains 3 atomic clocks with continuing corrections provided from the ground that compensate for relativistic effects. This means that an accurate estimate of the current time is developed as a side effect of figuring out where the GPS receiver is.

Choosing an Installation Directory

You may install NetPoint components in the default directory or in a directory of your choosing. When you change the path name, you may include any characters that are acceptable to your operating system. For example, you may include spaces on Windows systems but not on Unix systems.

Typically, the default installation directory for NetPoint is as follows:

\Program Files\NetPoint on Windows
/opt/netpoint (all lowercase) on Unix platforms

Depending on the NetPoint component and system you are installing, the path will vary slightly, as shown in Table 3. For example:

- \WebComponent is included in the default path name for WebPass, Access Manager, and WebGate installations.
- \identity is appended to all COREid System path names.
- \access is appended to all Access System path names.

Table 3 Installation Directory Path Names

NetPoint Component	Installation Directory
COREid Server	Windows: \Program Files\NetPoint\identity Unix: /opt/netpoint/identity In This Guide: *COREid_install_dir*\identity
WebPass	Windows: \Program Files\NetPoint\WebComponent\identity Unix: /opt/netpoint/WebComponent/identity In This Guide: *WebPass_install_dir*\identity
Access Server	Windows: \Program Files\NetPoint\access Unix: /opt/netpoint/access In This Guide: *AccessServer_install_dir*\access
Access Manager	Windows: \Program Files\NetPoint\WebComponent\access Unix: /opt/netpoint/WebComponent/access In This Guide: *AccessManager_install_dir*\access
WebGate	Windows: \Program Files\NetPoint\WebComponent\access Unix: /opt/netpoint/WebComponent/access In This Guide: *WebGate_install_dir*\access

In this manual, the installation directory path for each NetPoint component will be expressed as *Component_install_dir* followed by any suffix that is automatically appended to this path, as shown in Table 3. When the generic form is used, *Component_install_dir,* a generic suffix, identity|access, follows: for example, *Component_install_dir*/identity|access.

Downloading NetPoint Components

When you download the NetPoint software from the Oblix Customer Care Web site, be sure to place NetPoint installation packages in a temporary directory, not in the directory where you plan to install NetPoint components.

To download NetPoint components

1. Log in to the Oblix Customer Care Web site.

   http://www.oblix.com

   Note: If you do not have a login ID for the Oblix Customer Care Web site, click the Register button to obtain one.

2. Select Product Information and Downloads > NetPoint 7.0.
3. Store NetPoint installation packages in a temporary directory, **not** in the directory where you plan to install NetPoint components.

NetPoint Requirements

The following information is provided for your convenience.

- "Disk Space Requirements" on page 44
- "COREid and Access System Requirements" on page 45
- "Securing NetPoint Component Communications" on page 45

Disk Space Requirements

Table 4 provides estimates regarding the free disk space needed for each NetPoint component are provided for your convenience.

Table 4 Disk Space Requirements

	Windows	Unix
COREid Server	128 MB	90 MB
WebPass	93 MB	200 MB
Access Manager	122 MB	130 MB
Access Server	95 MB	200 MB
WebGate	76 MB	150 MB
SNMP Agent	50 MB	75 MB

COREid and Access System Requirements

Following are COREid and Access System requirements:

- You need a supported host machine for the COREid Server and Access Server. See “Operating System Support” on page 67 for details.
- During installation and setup, you will be asked to supply the DNS host name of the machine.
- During COREid System setup, you need to define a user who will be granted access to all COREid functionality. This is the NetPoint Master Identity Administrator.

The COREid Server and Access Server run as services. You must be able to ping the host name of the server on which the following NetPoint components will run:

- COREid Server
- Access Server

On Microsoft Windows, the account that performs installation of NetPoint must have administration privileges. The user account that is used to run the COREid Server and Access Server services must have the “Log on as a service” right, which can be set through Administrative Tools > Local Security Policy > Local Policies > User Rights Assignments > Log on as a service.

The “Installation Preparation Checklists” on page 83 provides a tool to document your environment. See also, “Securing NetPoint Component Communications” on page 45, “Securing Directory Server Communications” on page 56, and “Directory Server Requirements” on page 52.

Securing NetPoint Component Communications

Before installation, you must decide which type of transport security you will use between NetPoint components. NetPoint supports three types of transport security for communication that occurs between NetPoint components:

- **Open**—Allows unencrypted communication, see “Open Mode” on page 46
- **Simple**—Supports encryption by Oblix, see “Simple Mode” on page 46
- **Cert**—Requires a third-party certificate, see “Cert Mode” on page 47

Transport Security Guidelines

The following guidelines should be observed when planning and implementing transport security between NetPoint components during installation. Specifically:

- Transport security between all COREid System components (COREid Servers and WebPass instances) must match: either all open, all Simple mode, or all Cert.
- Transport security between all Access System components (Access Managers, Access Servers, and associated WebGates) must match: either all open, all Simple mode, or all Cert.

Caveats

When access cache flushing is enabled on the COREid Server, the COREid Server communicates with the Access Server. In this case, the transport security mode between all five of the following components must be in the same mode.

- COREid Servers and WebPass instances
- Access Managers, Access Servers, and associated WebGates

Open Mode

Use *Open* mode if transport security is not an issue in your environment. In Open mode, there is no authentication or encryption between the AccessGate and Access Server. The AccessGate does not ask for proof of the Access Server's identity and the Access Server accepts connections from all AccessGates. Similarly, COREid Server does not require proof of identity from WebPass.

Simple Mode

Use *Simple* mode if you have some security concerns, such as not wanting to transmit passwords as plain text, but you do not manage your own Certificate Authority (CA).

In Simple mode communications between WebGate, Access Server, and COREid are encrypted using TLS v1. The AccessGate and Access Server authenticate to each other using x.509 digital certificates. However, the CA private key used to sign Simple certificates is less secure than Cert mode.

NetPoint ships a CA with its own private key that is installed across all AccessGates and Access Server components. NetPoint does an additional password check to prevent other NetPoint customers from using the same CA.

For each public key there is a corresponding private key that NetPoint stores in the aaa_key.pem file (or ois_key.pem for COREid). A program named openSSL in the \tools subdirectory generates the private key. The openSSL program is called automatically during installation of each AccessGate and Access Server. Unlike Cert mode, NetPoint has already generated the private key. The key is presented automatically during installation.

In Simple mode, as in Cert mode, you secure the private key with a Privacy Enhanced Mail (PEM) pass phrase that you specify during installation of each component. During installation, the PEM pass phrase may also be referred to as the Global NetPoint Access Protocol pass phrase. The generic term “pass phrase” is often used in this manual.

Note: Before an AccessGate or Access Server can use a private key, it must have the correct pass phrase. The pass phrase is stored in a nominally encrypted file called password.lst. For Simple mode, the PEM pass phrase is the same for each WebGate and Access Server instance.

If you do not store the password in a file during Access Server installation:

- On Windows, you are prompted for the pass phrase every time you start the Access Server.
- On Unix, you must use the -P option to pass the password whenever you launch the start_access_server script.

Cert Mode

Use *Cert* (SSL) mode if you have an internal Certificate Authority (CA) for processing server certificates. In Cert mode, communication between WebGate, Access Server, and COREid are encrypted using Transport Layer Security, RFC 2246 (TLS v1). The AccessGate and Access Server authenticate using x.509 digital certificates signed by a Certificate Authority (CA).

For each public key there exists a corresponding private key that NetPoint stores in the aaa_key.pem file for the Access Server (or ois_key.pem for COREid Server).

A program named openSSL in the \tools subdirectory generates the private key. This program is called automatically during installation of each AccessGate and Access Server. During installation, you present a certificate obtained from a CA.

You secure the private key with a Privacy Enhanced Mail (PEM) pass phrase that you specify when you install each component. In this manual, the term pass phrase is used.

Note: Before a WebGate or Access Server can use a private key, it must have the correct PEM pass phrase. The PEM pass phrase is also referred to as WebGate Pass Phrase and NetPoint Transport Password. It can be stored in a nominally encrypted file called password.lst (or password.xml for COREid). It can be different for each WebGate and Access Server.

During NetPoint installation, if you do not yet have a certificate you may request one. In this case, you can complete installation despite the pending certificate status. However, the component or system cannot be setup until the certificates are issued and copied into the appropriate directory.

It is important to note, that if you generate a certificate request:

- You may complete installation as usual but you cannot set up NetPoint if a request is pending.
- You must locate the request in the NetPoint component installation directory. For example:

  COREid_install_dir\identity\oblix\config\ois_req.pem

  Usually, the .pem file contains some extra data plus the encrypted string that represents the request.
- You must copy the following information into a certificate request field from your chosen CA and send the request to your CA; Oblix does not do this:

  ```
  *-----------Begin request---------------
  A97C7u54Sd0000lotsofrandomstuff864Ouwst
  89111mmmIyoSSTKHS9670sd
  *-----------End request-----------------
  ```
- When the CA returns the certificate, you can copy the certificate files to the appropriate component installation directory, then restart the component server or service. For example:

  COREid_install_dir\identity\oblix\config

  See the *NetPoint 7.0 Administration Guide Volume 1* for details.

If you do *not* store the pass phrase or password in a file during Access Server installation:

- **On Windows**—You are prompted for the pass phrase every time you start the Access Server.
- **On Unix**—You must use the -P option to pass the password whenever you launch the start_access_server script.

For more information on transport security modes, see the *NetPoint 7.0 Administration Guide Volume 1*.

Web Server Requirements

You will need one or more Web servers to host WebPass, Access Manager, and WebGate components. The COREid Server and Access Server do *not* require a Web server instance.

If you install WebPass and COREid on the same Web server, the installation destination for WebPass *cannot* be the same as for COREid.

If you install Access Manager and WebPass on the same Web server, you *must* place them at the same directory level. For example, if you specify C:\NetPoint\WebComponent as the WebPass installation directory, you must also specify this as the Access Manager installation directory when the two components will reside on the same machine. \identity is appended to the WebPass installation directory and \access is appended to the Access Manager installation directory.

Be sure that your Web server meets all requirements before you being installation.

Task overview: Preparing your Web server

1. Ensure your Web server version is on the list of supported platforms in "Platform Requirements" on page 66.
2. Create new instances of your Web server running with your data to make it easier to make changes without taking down the service for other applications. See your Web server documentation for details.
3. Plan the Web server installation destination, and record details on "Installation Preparation Checklists" on page 83.

For more information, see:

- "Web Server-Specific Installation Packages" on page 49
- "General Considerations for Web Servers" on page 51
- "WebGate Web Server Considerations" on page 52

Web Server-Specific Installation Packages

Separate Web server-specific installation packages are provided for WebPass, Access Manager, and WebGate components. Be sure to choose the appropriate installation package for your Web server and platform:

- **ISAPI**—An Internet Web server extension that NetPoint uses to identify Web server components that communicate with the Microsoft Internet Information Server (IIS Web server for Windows environments).
- **NSAPI**—An Internet Web server extension that NetPoint uses to identify Web components that communicate with the Sun (formerly Netscape/iPlanet) Web servers running on either Windows or Solaris.

- **Apache**—An Internet Web server extension that NetPoint uses to identify Web components that communicate with the Apache Web servers running on various platforms including Windows, Solaris, and Linux. For details, see "Platform Requirements" on page 66.

  Note: NetPoint supports Apache with or without SSL enabled. For SSL-enabled communication, NetPoint supports Apache with mod_ssl only, not Apache-SSL. mod_ssl is a derivative of, and alternative to, Apache-SSL.

  Newer versions of NetPoint provide a single package for components that supports Apache with or without SSL enabled. For example:

  - The APACHE_WebGate supports v1.3.x with or without SSL.
  - The APACHE2_WebGate supports v2 with or without SSL (and with or without reverse proxy enabled on Solaris and Linux).

  Older versions of NetPoint provided individual packages for use with components that are either SSL enabled or not. For example:

  - APACHE_WebPass
    APACHESSL_WebPass (for Apache with mod_ssl)
  - APACHE_Access_Manager
    APACHESSL_Access_Manager

  See "Configuring the Apache v1.3 Web Server" on page 291 and "Configuring Apache and IHS v2 Web Servers for NetPoint" on page 301.

- **IHS**—An Internet Web server extension that NetPoint uses to identify Web components that communicate with the IBM HTTP (IHS) Web servers powered by Apache running on various platforms. For example:

  - IHS_WebGate powered by Apache v.1.3.x on Solaris, Linux, and Windows
  - IHS2_WebGate powered by Apache v2 on IBM-AIX

  See "Configuring Apache and IHS v2 Web Servers for NetPoint" on page 301.

- **Domino**—An Internet Web server extension that NetPoint uses to identify Web components that communicate with Lotus Domino Web servers running on various platforms. For example:

  Domino_WebGate for Lotus Domino Web servers on Windows and Solaris

  See "Setting Up Lotus Domino Web Servers for NetPoint WebGates" on page 341.

  For version support, see "Platform Requirements" on page 66.

General Considerations for Web Servers

It's a good idea to familiarize yourself with the following general considerations for Web servers in NetPoint installations:

- Each instance of the COREid Server communicates with a Web server through a WebPass plug-in that must be installed on a Web server host.
- A WebPass must be installed on the machine to host the Access Manager, on the same Web server instance and at the same directory level as you will install the Access Manager.

  If you install Access Manager and WebPass on the same Web server, you *must* place them at the same directory level. For example, if you specify C:\NetPoint\WebComponent as the WebPass installation directory, you must also specify this as the Access Manager installation directory when the two components will reside on the same machine. \identity is appended to the WebPass installation directory and \access is appended to the Access Manager installation directory.
- During WebPass, Access Manager, and WebGate installation, your Web server must be configured to work with NetPoint. You can direct this Web server configuration update to occur either automatically or manually.

  Note: Oblix recommends that you use the automatic configuration option to streamline the Web server update process and avoid errors.

- When accessing the COREid System or Access Manager, you must specify the *hostname* of the Web server for the WebPass instance that connects to the targeted COREid System or Access Manager and the HTTP port of the WebPass Web server instance.
- On a Unix system during WebPass, Access Manager, and WebGate installation, you must specify the user name and group that the Web server will use. Typically, the defaults are nobody.

  Note: For HP-UX, the defaults are WWW (username) and others (group).

For specific details for Apache and Domino Web servers, see "Section VI: Web Server Details" on page 289.

- For HP-UX, the defaults are WWW (username) and others (group).

WebGate Web Server Considerations

The WebGate *must* be installed on a machine hosting a Web server. You can install the WebGate in any directory that your Web server can access.

The WebGate can be installed with the same Web server instance as the WebPass and Access Manager to protect these components. You should install a WebGate on any Web server that you want to protect with the NetPoint Access System, including the Web server on which the Access Manager is installed.

If you install the WebGate to protect an Access Manager and WebPass, the WebGate *must* be installed in the same directory as the Access Manager and WebPass. For example, if the WebPass and Access Manager are installed in *\NetPoint\WebComponent*, then the WebGate must also be installed there.

The WebGate may be configured to run at either the machine level or the virtual Web server level. Do *not* install at both levels. The WebGate may be installed at the root level or the site level. Installing WebGate on multiple virtual sites amounts to only one instance of WebGate. The WebGate can also be installed using a non-root user if the Web server process runs as a non-root user.

Web server type and operating system type are not factors in WebGate-to-Access Server communication.

For more information, see “Installing the AccessGate/WebGate” on page 199.

Directory Server Requirements

Your installation requires one or more directory servers. You need to ensure that your directory server meets requirements for NetPoint and is properly prepared before NetPoint installation.

If you are installing NetPoint with Active Directory, see “Installing NetPoint with Active Directory” on page 379 in addition to the following discussions. See also, “Installing NetPoint with ADAM” on page 407, if needed.

Task overview: Preparing your directory server

1. Ensure the directory server is on the list of supported platforms, as described in “LDAP and Virtual Directory Support” on page 68.
2. Ensure that one or more directory server instances are available for NetPoint installation and decide if you want to store user data separately from Oblix configuration and policy data, as described in “Data Storage Requirements” on page 59.

3. Identify at least one person in your directory to use as the NetPoint Administrator to complete installation and setup, as described in “Assigning a Bind DN” on page 54.
4. Estimate and ensure that you have adequate directory server space, as described in “Assessing Directory Server Space” on page 54.
5. Determine whether you will secure directory server communication with NetPoint components or not, as described in “Securing Directory Server Communications” on page 56.
6. Establish a searchbase, configuration DN, and policy base for NetPoint data, as described in:
   - “User Data and the Searchbase” on page 64
   - “Configuration Data and the Configuration DN” on page 64
   - “Policy Data and the Policybase” on page 65
7. Define and record your Person and Group object classes, as described in “About Person and Group Object Classes” on page 65.
8. Record directory server details, as described in “Installation Preparation Checklists” on page 83, including:
   a) Root DN, network port, host name, and IP address of each directory server.
   b) User logon id and password for the directory server.

   Note: On Sun (formerly iPlanet) directory servers, Oblix recommends that the bind DN user is *not* Directory Manager. Instead, create another user as a bind DN. The Directory Manager account will ignore your directory server's size and timeout limits. As a result, large searches could tie up the directory server. See also, “Assigning a Bind DN” on page 54.
9. Decide how you plan to update the schema, as described in “Updating the Schema and Attributes Automatically vs. Manually” on page 32.
10. See the *NetPoint 7.0 Administration Guide Volume 1* for details about making schema data available to NetPoint.

    The inheritance of all objects is based on the premise of a common super class for both the structural object class and the auxiliary class. Otherwise, object class extension is not feasible.

Assigning a Bind DN

During installation and setup of the COREid Server and Access Manager, you are asked to provide a bind DN (also known as Root DN in NetPoint). The directory account that NetPoint binds to should have Read, Write, Add, Delete, Search, Compare, and Selfwrite permissions. The method to create a user with these privileges varies among directory vendors. See your directory documentation for details.

Be sure that the native directory access control instructions (ACIs) and/or access control lists (ACLs) do not restrict the NetPoint bind DN account access to the user and configuration branches. Otherwise, the NetPoint bind DN may be affected by native directory server constraints such as password policies.

In addition, the user you create as the bind DN must have access to the schema when NetPoint software upgrades are performed, because the schema may be modified during the upgrade. If the schema is not accessible to the bind DN, the upgrade will fail, then manual action will be required to complete the upgrade. This includes having the ACLs modify directory schema entries.

Note: On Sun (formerly iPlanet) directory servers, Oblix recommends that the bind DN user is *not* Directory Manager. The Directory Manager account will ignore your directory server's size and timeout limits. As a result, large searches could tie up the directory server.

Assessing Directory Server Space

The directory server should have at least 1 KB of RAM for each user object. Each Oblix object should have at least 16 KB of RAM.

The following information is provided to help you calculate the space that will be required for you installation:

- A directory server with 250,000 user objects requires ~250 MB of RAM.
- A directory of this size may have 5,000 Oblix objects (a high estimate for 250,000 user entries), which would require an additional 80 MB.
- The indexes for this amount of data would require about twice the space of Oblix objects, approximately 160 MB.

Siemens DirX—You need to plan for and provide DirX disk space for NetPoint indexes *during* DirX installation. For example, as a general guideline, if you plan to have 1,000,000 entries under the Oblix/User tree with a Real Object size of 1kb, density of attributes of 20% and cluster size of 32MB, then you need to allocate 12 GB to indexes. For details about increasing the DirX disk space for NetPoint indexes, see the procedure below.

To increase the DirX disk space for NetPoint indexes

1. Install DirX, as described in the Siemens DirX documentation, but do *not* start the DirX service.
2. Start the DirX service.
3. On the machine hosting Siemens DirX, run the command below to increase the maximum allowable number of indexes:

   dbamboot -P<*profileName*> -a 60

   where <*profileName*> is the profile that is currently used by DirX.

   The command above allows you to create a maximum of 60 indexes. For more information, see the *DirX EE Disc Dimensioning Guide*.

   If you need to delete collective attribute subentries, complete step 4. Otherwise, skip to step 5.

4. **Delete Collective Attribute Subentries**—Use the lettered steps below, if needed:

   a) From the directory manager interface, go to the Configuration section.

   b) In the tree in the right panel, navigate to Collective Attribute Subentries.

      For example:

      Root > o=*my-company* > Collective Attribute Subentries

   c) Delete the node under Collective Attribute Subentries.

   Note: These steps refer to the example database shipped with DirX EE. Your directory will have a different tree structure.

5. Start the DirX service.

   Note: The indexes required for Oblix attributes need to be installed *after* NetPoint COREid Server installation, either before COREid System setup or after setup. Without the indexes, search operations for these attributes may be slower than expected. For more information, see “Installing Indexes for Siemens DirX” on page 119.

Securing Directory Server Communications

The NetPoint CoreID Server, Access Manager, and Access Server communicate with the directory server. During NetPoint installation and setup, default directory profiles are created for the components that communicate with the directory server. Each directory profile includes a database (DB) instance profile where the directory server communication method is indicated, among other things.

Two communication methods are available between NetPoint and the directory server: unsecured or secured. Secure communication between NetPoint and the directory server is also known as *SSL-enabled*. Unsecured communication is also referred to as *Open*. NetPoint supports CA certificates in base-64 format.

SSL-enabled communication requires a signer's certificate (root CA certificate) from a third-party Certificate Authority in base-64 format. For example, if you want to use SSL between a COREid Server and directory server, you will be prompted to provide the path to the certificate to establish SSL-enabled communication during COREid Server installation. In this case, a certificate must be installed on your directory server according to the instructions for the directory server. The directory server should *not* require client authentication (see the directory server documentation for instructions).

Guidelines

When planning and configuring communication between NetPoint and the directory server, the following guidelines apply:

- Communication between COREid Servers and the directory server may differ.
- Communication between Access Servers and the directory server may differ.
- Communication between all Access Managers and the directory server must be consistent: all SSL-enabled or all open.

Note: When storing user data on a different directory server type than NetPoint configuration and policy data, multiple root CA certificates are supported. When storing user data, configuration data, and policy data on directory server types, each can use a separate root CA. For more information, see "Data Storage Requirements" on page 59.

Caveats

SSL-enabled communication with the directory server is *not* supported when the Access Manager is installed on Solaris with a Sun (previously Netscape) Web server. In a heterogeneous environment that includes an Access Manager on Solaris, be sure to specify open communication between the directory server and all Access Managers you install.

NetPoint components can share a DB profile even when components were not installed to use the same communication mode with the directory server. For example, suppose the COREid Server and Access Server were installed in open mode and the Access Manager was installed with SSL enabled. In this case, the cert8.db and key3.db files must exist for each NetPoint component that communicates with the directory server and must reside in the NetPoint *Component_install_dir*\identity|access\oblix\config directory. You may either copy these files from other NetPoint component directories or run genCert (Access Manager) or other utilities to generate them.

Note: With NetPoint 7.0, the default certificate store format and name has changed from cert7.db to cert8.db. When you upgrade to NetPoint 7.0, you continue to use the old certificate store (cert7.db). When you run the configureAAAServer, setup_ois, or setup_accessmanager utilities, the certificate store format and name is automatically modified to cert8.db. NetPoint 7.0 works with both the cert7.db (upgraded environments) and cert8.db (new installations) certificate store.

Siemens DirX—Is shipped for SSL/TLS connections with files containing a self-signed server certificate and the associated key material. Siemens DirX also supports server certificates issued by any CA such as a Verisign public CA, as described in Siemens DirX documentation. The following conditions should be taken into account:

- When Siemens DirX SSL is configured with the shipped self-signed CA (the default), you need to specify the file containing the CA certificate in Base 64 format during NetPoint installation.
- When DirX SSL is configured with a server certificate issued by a CA, you need to specify a file containing the CA certificate in Base 64 format during NetPoint installation. The files containing the self-signed certificates can be found in:

  DirX_install_dir/ldap/conf/

  cert_ldapserver.pem
  cert_ldapserver.der

  where cert_ldapserver.pem contains the self-signed certificate in Base 64 format and cert_ldapserver.der contains the self-signed certificate in binary encoded ASN.1 der format.

  Note: If the cert_ldapserver.pem file is not present, you need to convert cert_ldapserver.der into Base 64 format.

For details about converting cert_ldapserver.der into Base 64 format, see the procedures below:

- “To convert the self-signed certificate file into Base 64 format” on page 58

- "Alternative to convert the self-signed certificate file into Base 64 format" on page 58

To convert the self-signed certificate file into Base 64 format

1. Open the self-signed CA file with Windows Cert Viewer by double clicking cert_ldapserver.der and selecting the Details tab.
2. Select Copy to file and save it to a file in Base 64 encoded.

Alternative to convert the self-signed certificate file into Base 64 format

1. Locate the program named openSSL in your NetPoint installation:

   Component_install_dir/oblix/tools/openssl

2. Use the following the key command:

   openssl x509 -inform DER -in *binary_encoded_cert*.file -outform PEM -out *new_base64_encoded_cert*.file

Task overview: Defining directory server communication

1. Before NetPoint installation, review all directory server requirements for NetPoint, as described here and in "Directory Server Requirements" on page 52.
2. Before NetPoint installation, enable SSL on your directory server, if desired, as described in the documentation for your directory server vendors and certificate. For example:

   a) Create a directory server instance if you do not have one.

   b) Apply to your CA for a certificate for that instance.

   c) Install the certificate to encrypt your directory server instance and restart the directory server.

   Note: When storing user data on a different directory server type than NetPoint configuration and policy data, multiple root CA certificates are supported.

3. During COREid Server installation, choose the appropriate communication between the directory server and the COREid Server, as described here and in "Installing the COREid Server" on page 105.

4. During COREid System setup, choose the appropriate communication between the directory server and the COREid System, as described here and in "Setting up the COREid System" on page 136.

Note: When using certificates generated by a subordinate CA, the root CA's certificate must be present in the *xxx*_chain.pem along with the subordinate CA certificate. Both certificates must be present to ensure appropriate verification and successful COREid System setup.

---

5. During Access Manager installation and setup, choose the appropriate communication between the directory server and the Access Manager, as described here and in "Installing the Access Manager" on page 159.
6. During Access Server installation, choose the appropriate communication between the directory server and the Access Server, as described here and in "Installing the Access Server" on page 187.
7. After installation, you may change the communication mode between NetPoint and the directory server, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

Data Storage Requirements

This discussion provides details about data storage options and requirements. This information affects the COREid Server, Access Manager, and Access Server.

All Directory Server Types—NetPoint supports storing user data, Oblix (NetPoint) configuration data, and NetPoint policy data in a single directory server.

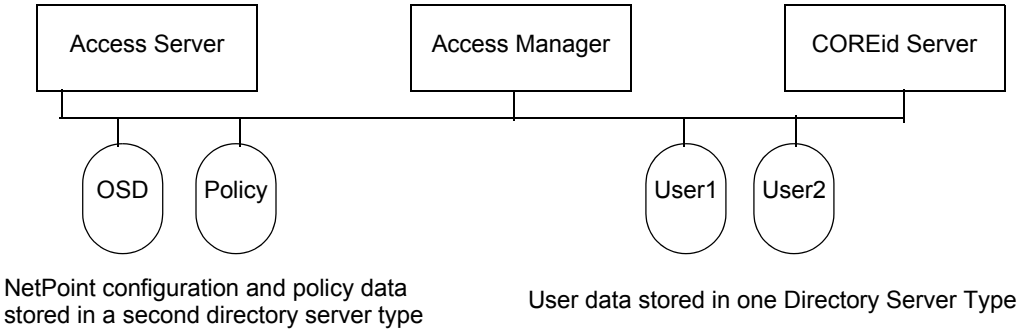
NetPoint also allows you to store user data separately on one directory server type and NetPoint configuration and policy data on a different type of directory server. For example, you may store user data in Active Directory and NetPoint configuration and policy data on ADAM.

When storing user data on a separate directory server type from configuration and policy data:

- All user data must be stored on the same directory server type.
- Configuration and policy data must be stored on the same type of directory server.
- With SSL, separate root CA's are supported.

Figure 4 illustrates storing user data in a separate directory server type.

Figure 4 User Data Stored in a Separate Directory Server Type



The user data searchbase, configuration DN, and policybase, should be unique if the data is stored in different directory types.

During NetPoint installation and setup, you need to select proper user and configuration directory server types for your environment.

When you have configuration and policy data stored together in a different directory server type from user data, the file below comes into play:

COREid_install_dir\identity\oblix\data\common\ldaposdreferentialintegrityparams.xml

This is because the "referential_integrity_using" Value="oblix" in the ldapreferentialintegrityparams.xml file does not apply when configuration and policy data are stored on a different directory server type from user data:

Also, in this case, the following files are used by the COREid and Access System to map servers to DB profiles rather than the original exclude_attrs files:

COREid_install_dir\identity\oblix\data\common\

exclude_user_attrs.xml
exclude_oblix_attrs.xml

AccessManager_install_dir\access\oblix\data\common\
AccessServer_install_dir\access\oblix\data\common\

exclude_oblix_attrs.lst

All parameters for the user data directory server are read using the DB profile. For the configuration data directory server, the DB subtype is read from:

Component_install_dir\identity|access\oblix\config\ldap\

*DB.xml and *DB.lst files

COREid Data Anywhere—Requires integrating NetPoint with the OctetString Virtual Directory Engine (VDE).

COREid Data Anywhere is a data management layer that aggregates and consolidates *user data* from multiple sources (including 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.

The LDAP directory branches containing NetPoint configuration and policy data must reside on one or more directory servers *other than* the one hosting VDE or user data. NetPoint applications only recognize configuration and policy information that resides outside the VDE virtual directory.

Important: *Before* you install NetPoint for use with COREid Data Anywhere, read the chapter on integrating NetPoint with VDE in the *NetPoint Integration Guide* and complete activities as specified.

IBM Directory Server (formerly SecureWay)—See details above for all directory server types.

Siemens DirX and Sun—When using either Siemens DirX or Sun (formerly iPlanet) exclusively, you have the option to store data anywhere, as follows:

- User data may be stored separately or with NetPoint-related data.
- Oblix configuration data may be stored either with user data in the same directory server or separately.
- NetPoint policy data may either be stored with user data or stored separately.

The user data searchbase, configuration DN, and policybase, should be disjoint if the data is stored in different directories. In other words, these DNs must be unique if you are storing your policy and configuration data in different Siemens DirX or Sun directories.

If you intend to have more than one user data directory and searchbase, be sure to specify the main user data directory and searchbase during installation and setup.

For information about disk space for DirX indexes, see “Assessing Directory Server Space” on page 54.

Active Directory, ADAM, and Novell eDirectory Caveats

Due to the strict adherence to referential integrity by Novell's eDirectory, Active Directory, and Active Directory Application Mode (ADAM), NetPoint configuration data and policy data must be stored under a common directory environment. Novell eDirectory, Active Directory, and ADAM are more rigid in the implementation of LDAP and will enforce referential integrity. These directory servers will *not* allow data in two separate trees/forests with cross references [like DN references] to each other.

With NetPoint, what is meant by having separate directories for user vs. Oblix configuration data and policy data is that you can have separate LDAP [disjoint] trees on different servers all of which happen to be in the same Novell directory server tree or Active Directory forest. The NetPoint configuration data and policy data can be stored in separate parts of the overall directory environment, which does allow for a level of segregation of the NetPoint-specific information away from your user data.

On Active Directory—In an Active Directory environment you may store NetPoint configuration data on one specific domain controller and policy data on another. The policy data and configuration data domain controllers should be in the same forest. user data may reside in a different forest. It is important that replication be either avoided, or very well understood. For more information, see "Installing NetPoint with Active Directory" on page 379.

When storing user data on a separate directory server type from configuration and policy data, auxiliary class support should match. NetPoint does not support a mixed mode for dynamic-auxiliary support. You can connect to either the user data directory server or Oblix (configuration) data directory server using ADSI, if they are in separate forests. ADSI does not allow a bind against both forests at the same time. With ADSI enabled for:

- **The User Data Directory Server**—During CoreID Server and Access Manager setup, if ADSI is selected for the user data directory server type then the ADSI checkbox is not available when choosing Oblix (configuration) directory server type details.
- **The Oblix Configuration Data Server**—When this directory type is ADSI enabled:
  - In the globalparams.xml file on the COREid Server, the parameter "IsADSIEnabled" and value "true" should appear.
  - In the globalparams.lst file on the Access Manager, the parameter "adsiEnabled"=true appears.

    The dbSubType "adsiEnabled" flags for Active Directory are read using the DB profile. Its value is ADSI when ADSI is enabled for the user data

directory server. The ActiveDirectory and ADAM flags are removed from the globalparams.xml and .lst files.

See “Installing NetPoint with Active Directory” on page 379 for more information.

If the user data directory server type is Active Directory, content of exclude_attrs-ad.xml are copied to:

COREid_install_dir\identity\oblix\data\common\exclude_user_attrs.xml

If the configuration and policy data directory type is Active Directory, content of exclude_attrs-ad.xml .lst are copied to the following locations:

COREid_install_dir\identity\oblix\data\common\exclude_oblix_attrs.xml

AccessManager_install_dir and *AccessServer_install_dir* \access\oblix\data\common\exclude_oblix_attrs.lst

---

Note: The ActiveDirectory flag longer appears in globalparams.xml.

With ADAM—Data can be stored as mentioned below:

- User data may be stored on a different partition from NetPoint configuration and policy data.
- User data may be stored on a separate directory server type from configuration and policy data.
- NetPoint requires a node with the object class attribute value of organizationalUnit (ou) for the configuration and policy DNs.
- Configuration and policy data can share the same ADAM instance or be stored on different ADAM instances.

For more information, see “Installing NetPoint with ADAM” on page 407.

Novell eDirectory—To avoid problems with GroupOfUniqueNames, change the class mapping for Groups in the LDAP Group object to reference GroupOfUniqueNames instead of groupOfNames (the default). Otherwise, each time you save any attribute, the schema may be violated and your groups may not work correctly. For example, for NDS the “groupOfUniqueNames” LDAP group object should be listed above the “groupOfNames” object.

To change the order using the NDS Console1

1. Expanding the NDS tree.
2. For the NDS node in the left pane, right-click the “LDAP Group” object in the right pane and select Properties > Class Map tab.

3. Change the order in which the two group objects appear.

   See your Novell eDirectory documentation for details about adding this mapping.

User Data and the Searchbase

User data consists of user directory entries managed by the COREid System. This data includes the information related to users, groups, locations, and other generic objects managed by the COREid System.

When installing NetPoint, you need to provide the following information to setup the main directory server profile:

- Directory server type where user data is stored
- Bind information, including the DNS host name, port, user name (bind DN), password
- Searchbase, to identify the node in the directory information tree (DIT) under which this data is stored and the highest possible base for all user data searches

  Note: If you intend to have more than one user data directory and searchbase, you must specify the main user data directory and searchbase during installation and setup. After setup, you must manually add one or more database profiles to add the disjoint namespaces.

- Master Identity Administrators (one or more)

Automatically updating the directory during setup is recommended to load Oblix schema classes with configuration information.

For more information, see “Data Storage Requirements” on page 59.

Configuration Data and the Configuration DN

Configuration data, also known as *Oblix data,* consists of NetPoint configuration details stored in the directory. This data includes workflow and configuration information that governs the appearance and functionality of the COREid System and Access System. Configuration data is managed by the COREid System.

When installing NetPoint, you need to provide details for the directory server where you plan to store configuration data. If you store configuration data and user data together, this information will be the same. The following caveats apply:

- The bind DN for Oblix (NetPoint) configuration data may be anywhere except at the base suffix.
- A bind DN for the configuration (known as the configuration DN), similar to the searchbase for user data, must be specified to identify the node in the DIT

under which the Oblix schema and all configuration data is stored for the COREid and Access System.

- Additional caveats may apply, as described under “Data Storage Requirements” on page 59.

Again, automatically updating the directory during setup is recommended to load Oblix schema classes with configuration information.

Policy Data and the Policybase

Policy data consists of policy definitions and rules that govern access to resources. This data is maintained in the directory server by the Access Manager.

When installing NetPoint, you need to provide details for the directory server where you plan to install policy data. If you store policy data separately from user data, directory server details will differ from those specified for user or configuration data. For more information, see “Data Storage Requirements” on page 59.

During Access Manager setup, you must also provide the policybase to identify the location in the DIT under which all NetPoint policy data is stored and the highest possible base for all policy searches. Accepting the default “/” as the policy domain when setting up the Access Manager protects the entire Web server.

About Person and Group Object Classes

NetPoint supports User and Group as standard Person and Group object classes, respectively. In addition, NetPoint supports User and Group.

The Person object class defines the user’s profile information. If you do not have a specific object class to use, NetPoint can automatically configure commonly found Person object class definitions.

Person Object Class

- **User**—Active Directory
- **InetOrgPerson**—ADAM, COREid Data Anywhere, IBM, and Sun directory servers
- **organizationalPerson**—NDS
- **gensiteorgperson**—Siemens DirX

The Group object class defines group attributes. If you do not have a specific object class to use, NetPoint can automatically configure commonly found Group object class definitions as follows:

Group Object Class

- **Group**—Active Directory
- **GroupofUniqueNames**—ADAM, COREid Data Anywhere, IBM, NDS, Siemens DirX, and Sun directory servers

Platform Requirements

NetPoint 7 supports a variety of operating systems, directory servers, Web servers, compilers, and browsers, as documented in the following sections (read from left to right).

Note: NetPoint applications for Solaris are built with compilers that can run only on Sparc-based Solaris machines, *not* on machines using Solaris x86 processors. NetPoint applications for Windows do not support 64-bit chips.

For the most up-to-date platform support, see the *NetPoint 7.0 Release Notes* and the Oblix Customer Care Web site, which includes details about our support policy:

https://customers.oblix.com/shared/prodinfo/prod_roadmap.cfm

Operating System Support

Table 5 provides operating system support for the COREid Server and Access Server.

Table 5 Operating System Support

NetPoint Component	Server
COREid Server	Sun Microsystems Solaris 8 Sun Microsystems Solaris 9 Microsoft Windows 2000 Advanced Server SP4 Microsoft Windows Server 2003 (Enterprise Edition) Red Hat Enterprise Linux AS v3.0
Access Server **Note**: NetPoint 7.0.3 Access Server is required for SHAREid 2.5	Sun Microsystems Solaris 8 Sun Microsystems Solaris 9 Microsoft Windows 2000 Advanced Server SP4 Microsoft Windows Server 2003 (Enterprise Edition) Red Hat Enterprise Linux AS v3.0

NetPoint Reports Server Support

NetPoint provides a reports server capability and Crystal Reports v9 templates. Table 6 lists supported platforms. In addition, note that:

- Crystal Reports supports Windows platforms only.
- MS-SQL 2000 and mySQL are supported as the reporting, auditing, and logging data store.
- mySQL is supported as the reporting, auditing, and logging data store on Red Hat Enterprise Linux AS 3.0

Table 6 NetPoint Reports Server Support

Operating System	NetPoint Reports Server
Microsoft Windows 2000 Advanced Server SP4	•
Microsoft Windows Server 2003 (Enterprise Edition)	•

LDAP and Virtual Directory Support

Supported directories for the COREid Server, Access Manager, and Access Server are listed in Table 7. For more information, see “Directory Server Requirements” on page 52 and “Data Storage Requirements” on page 59.

Table 7 Directory Server Support

Directory	Running on
COREid Data Anywhere (OctetString VDE) v3.0 **Note**: See also “COREid Data Anywhere Adaptor Support” on page 68.	Sun Microsystems Solaris 8 Sun Microsystems Solaris 9 Microsoft Windows 2000 Advanced Server SP4 Microsoft Windows Server 2003 (Enterprise Edition) Red Hat Enterprise Linux AS v2.1
IBM Directory Server v5.1 (formerly SecureWay)	Solaris 8 AIX 5.2
Microsoft Active Directory	Microsoft Windows 2000 Advanced Server SP4 Microsoft Windows Server 2003 (Enterprise Edition)
Microsoft Active Directory Application Mode (ADAM)	LDAP Only Microsoft Windows Server 2003 (Enterprise Edition)
Novell eDirectory 8.7.3	All NetPoint-supported operating systems, including AIX 5.2
Sun Directory Server 5.2 (Sun ONE)	Microsoft Windows 2000 Advanced Server SP4 Sun Microsystems Solaris 8 Sun Microsystems Solaris 9
Siemens DirX Extranet Edition (EE) 2.0B directory server	Microsoft Windows 2000 Advanced Server SP4 Microsoft Windows Server 2003 (Enterprise Edition)

COREid Data Anywhere Adaptor Support

OctetString VDE v3.0 (only) see above LDAP directory support

The following data stores are supported through COREid Data Anywhere, as discussed in Table 7:

- Sun Java System Directory Server 5.2
- Novell eDirectory 8.7.3
- IBM Directory Server (formerly SecureWay) 5.1
- Microsoft Active Directory

- Microsoft Active Directory Application Mode (ADAM)
- IBM DB2
- Oracle
- Microsoft SQL Server

Web Server Support for Access Manager and WebPass

Table 8 shows supported Web servers the Access Manager and WebPass components. The .NET framework is required for NetPoint components on Windows systems.

Table 8 Web Server Support for Access Manager and WebPass

Web Server	Running On
IBM HTTP Server 1.3.26	IBM AIX 5.2
Sun Web Server 6.0 SP5 (Sun ONE)	Microsoft Windows 2000 Advanced Server SP4 Sun Microsystems Solaris 8 and 9 **Note**: Access Manager support limited to Open mode on Solaris.
Sun Java System 6.1	Microsoft Windows 2000 Advanced Server SP4 Sun Microsystems Solaris 8 and 9 **Note**: Access Manager support limited to Open mode on Solaris.
Sun Java System 6.1 SP2	HP-UX 11.11—**WebPass Only**
Apache 1.3.29 Apache 1.3.31	Sun Microsystems Solaris 8 Sun Microsystems Solaris 9
Apache 2.0.52	Red Hat Enterprise Linux AS v3.0
Microsoft IIS 5.0	Microsoft Windows 2000 Advanced Server SP4
Microsoft IIS 6.0	Microsoft Windows Server 2003 (Enterprise Edition)

Web Server Support for WebGate Plug-In

The .NET framework is required for NetPoint components on Windows systems. On the ISA proxy server, ensure that the internal and external communication layers are configured and working properly before you begin installing NetPoint. Table 9 lists the Web servers supported for the WebGate plug-in.

Table 9 Web Server Support for WebGate

Operating System	Web Server Support for WebGate
AIX 5.1	IHS (IBM HTTP Server) 2.0.47 IHS (IBM HTTP Server) Reverse Proxy 2.0.47
AIX 5.2	Apache 1.3.33 IHS 1.3.2.6 Lotus Domino R6.5.3
HP-UX 11i (11.11)	Apache 1.3.33 Apache 2.0.52 Sun Java System Web server 6.1 SP2
Red Hat Enterprise Linux AS 2.1	Apache 1.3.29 Apache Reverse Proxy 1.3.29 Apache 2.0.48 Apache Reverse Proxy 2.0.48 IHS (IBM HTTP Server) 1.3.26
Red Hat Enterprise Linux AS 3.0	Apache 1.3.33 Apache 2.0.52 IHS (IBM HTTP Server) 1.3.26
Solaris 8	Apache 1.3.31 Apache 1.3.29 Apache 1.3.29 Reverse Proxy Apache 2.0.48 Apache Reverse Proxy 2.0.48 IHS (IBM HTTP Server) 1.3.26 IHS (IBM HTTP Server) 2.0.47 IHS (IBM HTTP Server) Reverse Proxy 2.0.47 Lotus Domino R6.5.3 Lotus Domino R6.5 Sun ONE Web server 6.0 Sun Java System 6.1

Table 9 Web Server Support for WebGate

Operating System	Web Server Support for WebGate
Sun Microsystems Solaris 9	Apache 1.3.31 Apache 1.3.29 Apache 1.3.29 Reverse Proxy Apache 2.0.48 Apache Reverse Proxy 2.0.48 IHS (IBM HTTP Server) 1.3.26 Sun ONE Web server 6.0 Sun Java System 6.1
Microsoft Windows 2000 Advanced Server SP4	Apache 1.3.29 Apache 2.0.48 Apache Reverse Proxy 2.0.48 IHS (IBM HTTP Server) 1.3.26 Lotus Domino R6 Lotus Domino R6.5.3 Microsoft IIS 5.0 Microsoft ISA 2000 SP1 Sun ONE Web server 6.0 SP5 Sun Java System 6.1
Microsoft Windows Server 2003 (Enterprise Server)	Apache 2.0.48 Apache Reverse Proxy 2.0.48 Lotus Domino R6.5.3 Microsoft IIS 6.0 Microsoft ISA 2000 SP1

Older NetPoint WebGates may co-exist with NetPoint 7 WebGates; however, encryption schemes may differ:

- Use RC4 as the encryption scheme if you have NetPoint 5.x and NetPoint 7.x WebGates co-existing in the same system.
- Use RC6 as the encryption scheme if you have NetPoint 6.x and NetPoint 7.x WebGates co-existing in the same system.
- Use the AES encryption scheme if you have only 7.0 WebGates installed.

See the *NetPoint 7.0 Administration Guide Volume 2* for details.

Passport Authentication Plug-In Support

The Passport Authentication plug-in runs on Microsoft Windows 2000 Advanced Server SP4 with Microsoft IIS v5.0. Microsoft IIS v6 has built-in support for Passport on Windows Server 2003.

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

Access Server API and Access Manager API Support

Table 10 shows supported platforms/compilers for Access Server API and Access Manager API. Any commercially available C or Java (JDK 1.2.2, 1.3.1, or 1.4) compiler is supported. The COM/COM+ interface is no longer supported; functionality has been replaced with a Managed Code API.

Table 10 OS Support for Access Server API and Access Manager API

Operating System	API Platform/Compiler and COM/COM+ interface
AIX 5.2	AIX C v6
HP-UX 11i	HP ANSI C++ 3.25
Microsoft Windows 2000 Advanced Server SP4	Visual Studio 6.x (API platform/compiler)
Microsoft Windows Server 2003 (Enterprise Edition)	Visual Studio .NET 7.0 Visual Studio .NET 7.0 (.NET Managed Code)
Red Hat Enterprise Linux AS v2.1 Red Hat Enterprise Linux AS v3.0	GNU 3.2.2 (API platform/compiler) GNU 3.3.2 (API platform/compiler)
Solaris 8 Solaris 9	GNU 3.2.2 (API platform/compiler)

Access Server SDK Support

Table 11 shows OS support for the Access Server SDK. The .NET API is included in the NetPoint Access Server SDK installation.

Table 11 OS Support for Access Server SDK

Operating System	Access Server SDK
Red Hat Enterprise Linux AS 3.0	Access API Access Manager API
Red Hat Enterprise Linux AS 2.1	SHAREid support
Sun Solaris 8	Access API Access Manager API

Table 11 OS Support for Access Server SDK

Microsoft Windows 2000 Advanced Server SP4	Access API Access Manager API
Microsoft Windows Server 2003 (Enterprise Edition)	Access API Access Manager API

The NetPoint Access Server SDK operates with the following JDK versions:

- JDK v1.2.2
- JDK v1.3.1
- JDK v1.4

Red Hat Linux AS 3.0 Prerequisites

The ASDK 7.0 sample C++ programs need GCC 3.3.2 compiler. No compat libraries need to be installed when using ASDK 7.0 on Linux AS 3. Instead the GCC compiler needs to be upgraded to GCC 3.3.2

- **Runtime Requirements**—For Java ASDK, Sun JVM 1.4.1 or IBM JVM 1.4.1 are recommended.
- **JVM and JDK Requirements**—Sun v1.4.1 and IBM v1.4.1 are supported.

To compile sample programs

1. Use the supported GCC compiler v3.3.2.
2. Locate the sample file in *install_dir*/samples/makefile.sample.
3. Change JAVA_HOME=<IBM/SUN JDK 1.4.1>.

NetPoint SHAREid Support

SHAREid is a stand-alone SAML-based Oblix product enables single sign-on across organizations that use different security systems, allowing users who have logged in locally to access resources on remote Web sites without re-authenticating.

Table 12 provides the support for SHAREid, which must be installed separately. For more information, see the *SHAREid Administration Guide*.

If you have an older version of NetPoint installed with SAML services, you may upgrade NetPoint SAML services to SHAREid. For more information about transitioning NetPoint SAML to SHAREid 2.0, see the *SAML to SHAREid 2.0 Migration Guide.*

Note: The NetPoint 7.0.3 Access Server is required for SHAREid 2.5.

Table 12 Support for NetPoint SHAREid 2.0

Operating System	Apache Tomcat 4.1.24
Sun Microsystems Solaris 8	•
Microsoft Windows 2000 Advanced Server SP4	•
Microsoft Windows 2003 (Enterprise Edition)	•

NetPoint SNMP Monitor Support

Table 13 shows the support for the NetPoint SNMP Monitor, which is SNMP v2 compatible and utilizes the UTF-8character format. Non US ASCI characters may not display properly with network management systems that do not support UTF-8. Supported network management software includes HP Oven View B.06 31 and IBM Tivoli Netview 7.1.3.

Table 13 NetPoint Support for SNMP Monitor

NetPoint Component	Operating System
COREid Server	Solaris 8 Solaris 9 Microsoft Windows Server 2000 SP 4 Microsoft Windows 2003 Server (Enterprise Edition) Red Hat Enterprise Linux AS 3.0
Access Server	Solaris 8 Solaris 9 Microsoft Windows 2000 Advanced Server SP 4 Microsoft Windows 2003 Server (Enterprise Edition) Red Hat Enterprise Linux AS 3.0

Network Management Software Support

NetPoint provides support for the following network management software:

- HP Open View B.06.31
- IBM Tivoli Netview 7.1.3

NetPoint Connector for MIIS Support

The NetPoint Connector for the Microsoft Identity Integration Server (MIIS) supports Microsoft MIIS 3.0 on Windows 2000 Advanced Server, SP4, and Windows Server 2003.

The NetPoint Connector for MIIS uses the MIIS SQL Managed Agent. For more information, see "ODBC Drivers Support" on page 75.

ODBC Drivers Support

NetPoint provides support for ODBC drivers to access the RDBMS where auditing, logging, and/or MIIS information is stored. MS-SQL and mySQL are supported for Windows and Solaris environments, respectively. Cross-platform environments are not supported. Table 14 lists supported ODBC drivers.

Table 14 ODBC Driver Support

Operating System	MS-SQL Driver
Solaris 8	
Solaris 9	
Windows 2000 Advanced Server SP4	•
Windows Server 2003 (Enterprise Edition)	•
Red Hat Linux AS 3.0	•

SSO Integration Support for Microsoft Applications

Table 15 lists support for NetPoint SSO integrations with Microsoft applications.

Table 15 SSO Integration for Microsoft Applications

Operating System	Microsoft SharePoint Portal Server 2003	Microsoft Content Management Server 2002
Windows 2000 Advanced Server SP4	•	
Windows Server 2003 (Enterprise Edition)	•	•
Web Server		
Microsoft IIS v6.0 Web Server	•	•

BMC Control/SA and Oblix IDLink Support

The Oblix IDLink module is supported on the following platforms:

- Sun Solaris 8 and Solaris 9
- Microsoft Windows 2000 Advanced Server SP4

BMC Control-SA allows security administrators to manage users, access rights, and security policies. Oblix IDLink integrates NetPoint identity and access management with Control-SA provisioning.

Provisioning involves setting up, changing, and disabling privileges. These privileges are user or system access and entitlement rights to applications, servers and network services.

NetPoint IDLink 1.0 is sold and packaged separately from NetPoint. Refer to the *Oblix IDLink 1.0 Administration Guide* for information about installing IDLink.

RSA SecurID Support

NetPoint 7.0 has successfully completed all certification criteria and is certified as ACE/Server 5 Ready. The ACE/Server must be installed on one of the platforms in Table 16.

Table 16 RSA ACE/Server Platform Support

Platform	ACE Server Version	SecurID Web Server Support
Solaris 8	ACE Server 5.1.1	Apache v1.3.27 Sun ONE v6 SP5
Windows 2000 Advanced Server SP4	ACE Server 5.1.1	IIS 5.0
Red Hat Enterprise Linux AS 3.0 **Note**: RSA SecurID—RSA does *not* currently support Linux AS 3.0 for the SecurID client. Therefore, the NetPoint 7.0.3 Access Server for Linux does not support SecurID authentication.	ACE Server 5.2	Apache v1.3.27 Sun ONE v6 SP5

See the *NetPoint Integration Guide* for more information about integrating the SecurID authentication plug-in with NetPoint.

Smart Card Authentication Support

NetPoint 7.0 supports Smart Card authentication, as follows:

- **Environments**—Homogeneous Windows environments with Active Directory

- **Operating System**—Windows 2000 Server SP4 and Windows XP
- **Client**—ActivCard Gold v2.2a Client, USB, or PCMCIA Card Reader
- **Web Server**—IIS Web server
- **Browsers**—Microsoft IE 5.5 or 6.0 SP1, or Netscape 6.2.2

See the *NetPoint Integration Guide* for more information about integrating the Smart Card authentication with NetPoint. See ActivCard Gold specifications and details about Smart Card standards and compatibility at www.activcard.com.

Oracle Application Server Support

NetPoint supports integration with Oracle Application Servers as described below.

Table 17 identifies NetPoint support for Oracle Application Server 10g:

Table 17 NetPoint Support for Oracle Application Server 10g

Oracle Application Server 10g	Platforms
Oracle Application Server 10g v9.0.4	Solaris 8 or 9 Windows HP-UX 11.11 (using NetPoint 6.1.1 WebGate only)

Table 18 identifies NetPoint support for Oracle9iAS:

Table 18 NetPoint v7.0.1 Support for Oracle9iAS

Oracle9iAS	Platforms
Oracle9iAS R2 (SSO) v9.0.4	Solaris 8 or 9 Windows

Plumtree Corporate Portal Support

NetPoint supports the Plumtree Corporate Portal 4.5 WS, 5, on Windows 2000 Server and Advanced Server, SP4.

IBM WebSphere Application Server and Portal Support

Table 19 lists COREid support for Websphere across various operating system platforms.l

Table 19 COREid Versions Supported for Specific WebSphere Products on Specific Operating System Platforms

Operating System Platform	WebSphere Application Server				WebSphere Portal Server			
	4.0.4 +	5.0 (Enterprise Edition)	5.1	6.0	4.2	4.1.4 with CMR	5.0.2 with CMR	5.1 with CMR
Solaris 8	**COREid...** 6.1.1.15 6.5.2 6.5.5 7.0 7.0.1 *Not* 7.0.2	6.5.2 6.5.5 7.0 7.0 7.0.1 7.0.2 7.0.4	7.0.2 7.0.4		6.5.2 6.5.5 7.0 7.0.1 *Not 7.0.2*	6.1.1.15 6.5.5 7.0 7.0.1 *Not 7.0.2*	6.5.5 7.0 7.0.1 7.0.2 7.0.4	
Windows 2000 (Adv. Server with SP4)	6.1.1.16 6.5.2 7.0 7.0.1 *Not 7.0.2*	6.5.2 7.0 7.0.1 7.0.2 7.0.4	7.0.2 7.0.4		6.5.2 7.0 7.0.1 *Not 7.0.2*	6.1.1.16 6.5.5 7.0 7.0.1 *Not 7.0.2*	6.5.5 7.0 7.0.1 7.0.2 7.0.4	
AIX 5.1	6.1.1.12 6.5.5 7.0	6.5.5 7.0 7.0.4			6.5.5 7.0	6.1.1.12 6.5.5 7.0	6.5.5 7.0 7.0.4	7.0.4
AIX 5.2	6.1.1.12 6.5.5 7.0	6.5.5 7.0 7.0.3 7.0.4	7.0.3 7.0.4		6.5.5 7.0	6.1.1.12 6.5.5 7.0	6.5.5 7.0 7.0.3 7.0.4	7.0.4
RedHat Linux AS 3			7.0.4					
SUSE Linux Enterprise Server 9				7.0.4				

The NetPoint Connector for WebSphere includes the NetPoint Custom Member Repository (CMR) for the WebSphere Portal Server.

The NetPoint 7.0.2 and 7.0.3 Connectors for WebSphere support the WebSphere Application Server v5 with the NetPoint CMR (not WAS v4).

The WebSphere Portal Server v4 operates only with WebSphere Application Server 4.x. WebSphere 4.0.x is bundled with IBM Directory Server (SecureWay) v3.2.2 and IBM HTTP Server 1.3.19.

BEA WebLogic Application Server and Portal Support

NetPoint Ready Realm supports the BEA WebLogic Application and Portal Servers v8.1 SP3 via SSPI on the platforms below:

- HP-UX 11.0i
- Red Hat Enterprise Linux AS 2.1
- Solaris 8
- Windows 2000 Advanced Server SP4

Note: BEA WebLogic 7.0 and WebLogic Portal 7.0 are supported via compatibility. WebLogic 6.1 and WebLogic Portal 4.0 are deprecated and support is not planned for future releases of NetPoint.

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

Browser Support

Table 20 lists Web browsers that are fully supported.

Table 20 Web Browser Support

Full Browser Support	Operating System
Microsoft IE 6.0	Microsoft Windows 2000 Microsoft Windows XP
Microsoft IE 6 SP1	Microsoft Windows 2000 SP4 Microsoft Windows XP
Microsoft IE 5.5 SP1/SP2	Microsoft Windows 2000
Netscape 6.2.2	Microsoft Windows 2000 Microsoft Windows XP Sun Microsystems Solaris

Table 21 shows the Web browsers with limited support. Limited support refers to support that is primarily extended to end users. For example, end user browsing and portal access, the ability to conduct searches, user self-service to modify and save changes to attribute values, and the ability to change passwords when prompted.

Limited support does not include administrative functions such as giving users the ability to view and modify attributes, defining workflows, system configuration, and access management.

Table 21 Limited Web Browser Support

Limited Support	Operating System
Safari	Apple MacOS (10.x)
Netscape 4.08	Apple MacOS (9.2, 10.x)
Netscape 4.7x (4.7 and 4.78)	Apple MacOS RedHat Linux Microsoft Windows NT and 2000 Solaris
Netscape 6 (6.1)	Apple MacOS Linux Microsoft Windows NT Microsoft Windows 2000 Microsoft Windows XP
Netscape 6.2	Apple MacOS Linux Microsoft Windows NT
Netscape 7	Apple MacOS Linux Microsoft Windows NT Microsoft Windows 2000 Microsoft Windows XP Solaris
Microsoft IE 4.0	Microsoft Windows 95 Microsoft Windows NT4.0
Microsoft IE 4.5	Apple MacOS
Microsoft IE 5.0x	Apple MacOS Microsoft Windows 9x Microsoft Windows NT
AOL 6 (IE 5.5)	Apple MacOS Microsoft Windows 9x
AOL 7.0 and 8.0	Apple MacOS Microsoft Windows 9x Microsoft Windows 2000 Microsoft Windows NT Microsoft Windows XP

Specifying a Temporary Directory on Unix

When launching a NetPoint installation on a Unix system, you can direct an installation to a directory with sufficient space using the -is:tempdir *path* parameter.

To specify a temporary directory

1. Use the -is:*tempdir* parameter in the following command. For example:

   ./NetPoint7_0_sparc-s2_COREid_Server -is:tempdir /export/home/oblix/temp

   The path must be an absolute path, not a relative path.

2. The path /export/home/oblix/temp should be replaced with a file system with sufficient space.

Uninstalling NetPoint

During NetPoint 7.0 installation, information is saved after certain operations. Until information is saved, you may return and restate details. However, after you are informed that a component is being installed, NetPoint files are added to the file system.

Note: If you cancel the installation process after receiving the message that a component is being installed and before completing all procedures, you must restore the system to it's previous condition to remove NetPoint related information.

There are several steps you need to complete to remove a NetPoint application, as outlined below. Web server configuration changes for NetPoint and schema updates are not handled automatically and must be manually removed, as needed, when the Uninstaller program finishes.

For example, the ISAPI transfilter will be installed in IIS on WebPass. However, when you uninstall WebPass this is not removed automatically. Also, the created Web service extension and the link to the identity directory will not be removed. This type of information must be removed manually.

To uninstall NetPoint

1. Turn off your Web server, if appropriate.

   Note: If you don't turn off the Web server, uninstall may not succeed and the backup folder won't be removed. If this happens, you need to manually remove the backup folder.

   ---

2. Locate and run the Uninstaller program for the specific NetPoint component to remove NetPoint files:

   For example:

   COREid_install_dir\identity_uninstIdentity\uninstaller.exe
   WebPass_install_dir\identity_uninstWebPass\uninstaller.exe

   Note: On Unix systems, use uninstall.bin.

3. Remove NetPoint-related schema updates from your directory.
4. Remove NetPoint-related updates to your Web server configuration.
5. If you have multiple instances of a component and want to remove one or all of them, you must use a specific method for your platform:
   - **Windows**—The last component can be uninstalled from Add/Remove programs. Others can be uninstalled by running the uninstall program from the \identity or \access \uninst*Component* directory.
   - **Unix**—You must always run uninstall.bin.

Recycling a COREid Server Instance Name

Under certain circumstances, you may want to use an existing COREid Server name. For example, you may want to use an existing COREid Server name if you are rolling NetPoint out from a test environment to a production environment or if you need to remove a COREid Server for some reason.

If you do not delete the original COREid Server name from the System Console, a login following set up of a new instance may result in the message “Application has not been set up”. Special steps must be taken to ensure you can set up the application and login when recycling a COREid Server name.

The steps below presume that you have another COREid Server and WebPass setup within the same installation.

To recycle a COREid Server instance name

1. Delete the COREid Server name in the directory server under:

   Oblix > Policies > WebResrcDB > *name*

2. Re-run COREid Server setup, as described in “Setting Up the COREid System” on page 133.

3. Go to the COREid System Console, delete the inoperable COREid instance.

   For example:

   COREid System Console > Sys Admin > System Configuration > Configure COREid Server

   name > Delete

4. From the List all COREid Servers page, re-create the instance using the same ID as described in the *NetPoint 7.0 Administration Guide Volume 1*.

   For example:

   Add

   Name
   Host name
   Port
   Transport Security

Installation Preparation Checklists

Installation of NetPoint requires some advance planning and the checklists in this discussion are provided for your convenience. For example, the checklists in Table 22:

- Provide a space where you can map out and record your environment.
- Help you prepare to answer prompts during NetPoint installation and setup.
- Are organized according to the recommended component installation sequence described under "About the Installation Process" on page 27, and the installation process for each component.
- Provide a reference to a specific page number in this manual where you will find additional information.

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation	Page
	Prerequisites Create a Web server instance.	40
	Create a directory server instance. The user directory server must have at least one administrative user to act as the NetPoint Administrator.	56
	Synchronize the host's clock. Required if you are installing across multiple machines.	41

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation		Page
	Prepare for COREid System Installation		
1	Prepare to Install the COREid Server. Decide on the following:		99
	(Unix only) COREid Server user name:		
	(Unix only) COREid Server group:		
	COREid Server installation directory:		
	Default Locale		30
	Language Packs		30
	Transport security mode between the COREid Server and WebPass:	☐ Open ☐ Simple ☐ Cert	45
	Unique COREid Server ID to be used within NetPoint to identify this COREid Server instance:		
	Host name of the machine where the COREid Server is to be installed:		
	Port number for COREid Server/WebPass communication:		
	Is this the first COREid Server installed for this directory server?	☐ Yes ☐ No	
	Security mode between directory server and COREid Server:	☐ SSL ☐ Open	
	If SSL, path to the Root CA certificate:		
	Simple mode only Global NetPoint Access Protocol pass phrase		
	Cert Mode Only Certificate PEM pass phrase:		

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation		Page
	Path of the certificate request file (Cert request only):		
	Path of the certificate file (Cert mode only):		
	Path of the key file (Cert mode only):		
	Path of the chain file (Cert mode only):		
	Prepare directory server details Location of Oblix data in the directory server:	☐ User data directory server ☐ Separate directory server ☐ Manual install	
	Directory server type: **Note**: COREid Data Anywhere is available only for the *user data* directory server. Configuration and policy data *must* be stored in a native directory. Before you install NetPoint with COREid Data Anywhere, see the chapter on integrating NetPoint with VDE in the *NetPoint Integration Guide*.	☐ Sun Directory Server 5.x ☐ NDS ☐ Active Directory ☐ Active Directory on Windows Server 2003 ☐ Active Directory Application Mode ☐ Siemens DirX ☐ IBM Directory Server ☐ COREid Data Anywhere	
	Directory server host machine name or IP address:		
	Directory server port #:		
	Directory server bind DN:		
	Directory server administration password:		
	(Windows only) Unique COREid Server service name that will differentiate this instance in the Services window if you install several instances of COREid Server):		
2.1	Prepare to install WebPass. Decide on the following:		121
	Default Locale		30
	Language Packs		30
	Web server user name (Unix only):		

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation		Page
	Web server group (Unix only):		
	WebPass installation directory. If installing on the same machine as COREid, this cannot be the same as the COREid installation directory:		
	Transport security mode between the COREid Server and WebPass:	See task 1, this table.	
	WebPass ID used by NetPoint to identify the WebPass instance:		
	WebPass host name:		
	Port # for COREid Server/WebPass communication:	See task 1, this table.	
	Simple mode only Global NetPoint Access Protocol pass phrase	See task 1, this table.	
	Cert mode only Certificate PEM phrase:		
	Path of the certificate request file (Cert request only):		
	Path of the certificate file (Cert mode only):		
	Path of the key file (Cert mode only):		
	Path of the chain file (Cert mode only):		
	Automatically update your Web server with WebPass information?	☐Yes ☐No	
	If Yes, absolute path of the Web server configuration directory containing the obj.conf file (or the httpd.conf file on Apache):		
2.2	Restart the Web server.		

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation		Page
	Prepare for COREid System Setup		
3.1	Prepare to set up the COREid Server. Decide on the following:		133
	Directory server type:	See task 1, this table.	
	Directory server host machine name or IP address:	See task 1, this table.	
	Directory server port #:	See task 1, this table.	
	Directory server bind DN:	See task 1, this table.	
	Directory server administration password:	See task 1, this table.	
	Security mode between directory server and COREid Server:	See task 1, this table.	
	Is the Oblix data stored in the user data directory server?	See task 1, this table.	
	Configuration DN:		
	Directory searchbase where user data is stored:		
	Person object class:		
	Auto-configure the Person object class?	☐Yes ☐No	
	Group object class:		
	Auto-configure the Group object class?	☐Yes ☐No	
3.2	Configure the Person object class (manual process is optional). Configure the following attributes if you chose *not* to auto-configure your Person object class:		140

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation		Page
	User full name attribute:		
	User login ID attribute:		
	Password attribute:		
3.3	Configure the Group object class (manual process is optional). Configure the following attributes if you chose *not* to auto-configure your Group object class:		140
	Group name attribute:		
3.4	Prepare to define the NetPoint Administrators.		143
	NetPoint system administrators:		
	Prepare for Access System Installation and Setup		
4.1	Prepare to install the Access Manager. Decide on the following:		160
	Optional Language Packs		30
	Web server user name (Unix only):	See task 2.1, this table.	
	Web server group (Unix only):	See task 2.1, this table.	
	WebPass installation directory:	See task 2.1, this table.	
	Directory server type: Note: COREid Data Anywhere is available only for the *user data* directory server and is *not* an option for the Access Manager or Access Server. Configuration and policy data must be stored in a native directory, as described in the *NetPoint Integration Guide*.	☐ Sun Directory Server 5.x ☐ NDS ☐ Active Directory ☐ Active Directory on Windows Server 2003 ☐ Active Directory Application Mode ☐ Siemens DirX ☐ IBM Directory Server	
	Are you storing your policy data separate from your user data directory server?	☐Yes ☐No	

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation		Page
	Transport security mode between the Access Manager and Access Servers:	☐Open ☐Simple ☐Cert	See task 1, this table.
	Simple mode only Global NetPoint Access Protocol pass phrase:		
	Cert mode only Certificate PEM pass phrase:		
	Path of the certificate request file (Cert mode only):		
	Path of the certificate file (Cert mode only):		
	Path of the key file (Cert mode only):		
	Path of the chain file (Cert mode only):		
	Automatically update the obj.conf file with Access System information?	☐Yes ☐No	
	If Yes, absolute path of the Web server configuration directory containing the obj.conf file (or the httpd.conf file on Apache):	See task 2.1	
4.2	Prepare to set up the Access Manager. Decide on the following:		161
	Optional Language Packs		30
	Directory server type:	See task 4.1.	
	Directory server host machine name or IP address:	See task 1.	
	Directory server port #:	See task 1.	
	Directory server bind DN:	See task 1.	
	Directory server administration password:	See task 1.	
	Security mode between the directory server and the Access Manager:	☐Open ☐SSL	56

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation		Page
	If SSL, path to the SSL certificate:		
	Location of Oblix data in the directory server:	☐ User data directory server ☐ Separate directory server	
	If on separate directory server, the directory server host machine name or IP address:		
	If on separate directory server, the directory server port #:		
	If on separate directory server, the directory server bind DN:		
	If on separate directory server, the directory server administration password:		
	If on separate directory server, the security mode between the directory server and the Access Manager:	☐Open ☐SSL	56
	If SSL, path to the SSL certificate:		
	Location of policy data in the directory server:	☐ User data directory server ☐ Oblix data directory server ☐ Separate directory server	
	If on separate directory server, the directory server host machine:		
	If on separate directory server, the directory server port #:		
	If on separate directory server, the directory server bind DN:		
	If on separate directory server, the directory server administration password:		
	If on separate directory server, the security mode between the directory server and the Access Manager:	☐Open ☐SSL	56
	If SSL, path to the SSL certificate:		

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation		Page
	Directory searchbase where user data is stored:	See task 3.1.	
	Configuration DN:	See task 3.1.	
	Policy base:		
	Person object class name:	See task 3.1.	
	Access Manager policy domain root:		
	Configure authentication schemes?	☐Yes ☐No	
	If Yes, select authentication scheme or schemes:	☐Basic Over LDAP ☐Client Certificate	
	Configure NetPoint-related authentication schemes and policies	☐NetPoint None Authentication ☐NetPoint Basic over LDAP ☐NetPoint Basic over LDAP for AD Forest ☐NetPoint Identity Domain ☐NetPoint Access Manager	
	Configure policies to protect NetPoint-related URLs?	☐Yes ☐No	
5.1	Prepare to create an instance for the Access Server in the Access Manager. Before you continue, you must decide on the following:		191
	Access Server name (do not include spaces):		
	Access Server host name:		
	Port # the Access Server listens to:		
	Transport security mode between the Access Server and WebGate:	☐Open ☐Simple ☐Cert	See task 1.

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation		Page
	Access management service enabled?	☐On ☐Off	
5.2	Prepare to Install the Access Server.		194
	Optional Language Packs		30
	Web server user name (Unix only):		
	Web server group (Unix only):		
	Access Server installation directory:		
	Transport security mode between the Access Server and the WebGate/AccessGate:	☐Open ☐Simple ☐Cert	See task 1.
	Security mode between the directory server and the Access Server:	☐Open ☐SSL	56
	Directory server host machine:	See task 1.	
	Directory server port #:	See task 1.	
	Directory server bind DN:	See task 1.	
	Directory server administration password:	See task 1.	
	Directory server type: Note: You will be asked about Active Directory using ADSI whenever the Access Server installation occurs on a Windows platform.	☐ Sun Directory Server 5.x ☐ NDS ☐ Active Directory ☐ Active Directory Application Mode ☐ Siemens DirX ☐ IBM Directory Server	
	Which directory server stores the Oblix data?	See task 1.	
	Which directory server stores the policy data?	See task 4.2.	
	Simple mode only Global NetPoint Access Protocol pass phrase:	See task 4.1.	

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation		Page
	Cert mode only Certificate PEM phrase:		
	Save PEM phrase in a password file? (Simple and Cert modes only):	☐Yes ☐No	
	Path of the certificate request file (Cert mode only):		
	Path of the certificate file (Cert mode only):		
	Path of the key file (Cert mode only):		
	Path of the chain file (Cert mode only):		
	Access Server name:	See task 5.1.	
	Configuration DN:	See task 3.1.	
	Policy Base:	See task 4.2.	
6.1	Prepare to create an instance for the WebGate in the Access Manager. Before you continue, you must decide on the following:		**204**
	WebGate name (do not include spaces):		
	WebGate host name:		
	Web server port #:		
	WebGate password/confirm password:		
	Transport security mode between the Access Server and WebGate:	See task 5.1.	
6.2	Associate the WebGate with an Access Server.		207
6.3	Prepare to install the WebGate. Before you continue, you must decide on the following:		200
	Optional Language Packs		30
	Web server user name (Unix only):		

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation		Page
	Web server group (Unix only):		
	WebGate installation directory (can be same as WebPass installation directory):		
	Transport security mode between the Access Server and the WebGate:	See task 5.1.	
	WebGate ID:	See task 6.1.	
	WebGate password:	See task 6.1.	
	Access Server ID:	See task 5.1.	
	Access Server host name:	See task 5.1.	
	Access Server port #:	See task 5.1.	
	Simple mode only Global NetPoint Access Protocol pass phrase:	See task 4.1.	
	Cert mode only Certificate PEM phrase:		
	Path of the certificate request file (Cert mode only):		
	Path of the certificate file (Cert mode only):		
	Path of the key file (Cert mode only):		
	Path of the chain file (Cert mode only):		
	Automatically update the obj.conf file?	☐Yes ☐No	
	If Yes, absolute path of the Web server configuration directory containing the obj.conf file (or the httpd.conf file on Apache):		See task 2.1.
	Intended Optional Language Packs or Monitoring Tools		
8.1	Language Packs, Independent Installation (optional).		225

Table 22 Installation Preparation Checklists

Task	Checklist: Prepare for Installation	Page
8.1	SNMP Agent (optional).	233
	Other Intended Optional Components	
9.1	Ready Realm for BEA (optional).	See the *NetPoint Integration Guide*
9.3	Access Server SDK (optional).	See the *NetPoint 7.0 Developer Guide*

Section II: COREid System Installation and Setup

3 Installing the COREid Server

The COREid System must be installed before the Access System is installed. The COREid Server must be the first NetPoint component you install. This chapter covers the following topics:

Upgrading to NetPoint 7.0 is described in the *NetPoint 7.0 Upgrade Guide*. For an overview of NetPoint components, see the Introduction to *NetPoint 7.0 Guide*.

About the COREid Server and Installation

The NetPoint COREid Server provides applications through a Web-based interface and processes all requests related to user, group, and organization identification.

Each instance of the COREid Server receives requests through a WebPass plug-in installed on a Web server host. Each instance of the COREid Server reads and writes to your LDAP directory server across a network connection. For more information, see “About NetPoint Installations” on page 23.

The COREid Server must be the first NetPoint component you install. The installation task has been divided into several functional procedures.

Task overview: Installing a COREid Server

1. Start the installation as described in “Starting the Installation” on page 106.
2. Continue by “Installing the COREid Server” on page 107.
3. Continue with “Specifying a Transport Security Mode” on page 108.
4. Identify the COREid Server, as described in “Specifying COREid Server Configuration Details” on page 108.
5. Define communication details, as described in “Defining Communication Details” on page 110.
6. Define directory server details, as described in “Defining Directory Server Details” on page 113.
7. Conclude with “Finishing the COREid Server Installation” on page 117.

You must complete all procedures for a successful installation. Information will be saved at various points during this task. Should an error be detected in the information you supply, you will be offered the opportunity to restate information or complete a sequence again. After information is saved, you will not be able to return and restate information.

If you cancel the installation before completing all procedures and after being informed that the COREid Server is being installed, you must uninstall NetPoint as described in “Upgrading from a Previous Version of NetPoint” on page 37.

You may complete NetPoint installations using either GUI mode or console mode. Separate platform-specific installation packages are provided for the COREid Server in \win32 and \solaris subdirectories. Platform differences are noted as needed.

Be sure there is enough disk space and the COREid Server can communicate with your Web server.

The installation process is similar regardless of the installation mode you choose and your operating system. Any caveats are identified and may be skipped when they do not apply to your environment. For example:

Windows—\Software\Win32\COREidSystem\COREidServer
Solaris—/Software/Solaris/COREidSystem/COREidServer

Note: If you intend to reuse a COREid Server instance name, see “Recycling a COREid Server Instance Name” on page 82.

About the COREid Server Installation Directory

You may install the COREid Server in the default directory or in a directory of your choosing. When you change the path name, you may include any characters that are acceptable to your operating system. For example, you may include spaces on Windows systems but not on Unix systems. It may be a good idea to use consistent naming regardless of platform. For example, use an underscore rather than a space in names on Windows platforms.

During installation the \identity subdirectory is added to the destination you specified, making the full path to the COREid Server installation directory:

Default on Windows—\Program Files\NetPoint\identity
Default on Unix—/opt/netpoint/identity
In This Guide—*COREid_install_dir*\identity

Certain functions in the COREid System require the Access Server SDK. By default, the Access Server SDK is installed in a subdirectory under *COREid_install_dir*\identity. Following COREid System set up, you must manually configure the Access Server SDK for the COREid System to enable these functions, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

About Installing Multiple COREid Servers

You may want to install multiple COREid Servers, all associated with the same directory server.

Task overview: Installing additional COREid Servers

1. Install your first COREid Server, as explained in this chapter.
2. Install a WebPass, as explained in "Installing WebPass" on page 121.
3. Set up the first COREid Server in the COREid System, as explained in "Setting up the COREid System" on page 136.
4. Add a new COREid Server instance in the COREid System Console, as described in the *NetPoint 7.0 Administration Guide Volume 1*.
5. Associate the new COREID Server instance with a WebPass and specify the priority as Primary, as described in the *NetPoint 7.0 Administration Guide Volume 1*.
6. Modify the WebPass instance to set the maximum connections to the appropriate number to communicate with all primary COREid Servers, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

   You must wait at least one minute before step 7 to ensure that the WebPass configuration file, webpass.xml, is updated with the new instance information. Otherwise, the WebPass instance may not receive the new information and cannot connect to the new COREid Server instance.

7. Wait at least one minute before stopping all installed COREid Servers.
8. Install the new COREid Server and indicate that this is *not* the first COREid Server for this directory server.

   You do not need to update the schema again.
9. Set up the new COREid Server, as explained in "Setting Up Other COREid Server Instances" on page 154.
10. Configure this COREid Server as a failover server, if desired, as explained in the *NetPoint 7.0 Deployment Guide*.

COREid Server Installation Considerations

Following are several installation considerations for the COREid Server.

Administrative Privileges—The account that performs NetPoint installation must have administration privileges.

On Microsoft Windows, the user account that is used to run the COREid Server service must have the right to "Log on as a service". This can be set through Administrative Tools > Local Security Policy > Local Policies > User Rights Assignments > Log on as a service.

COREid Data Anywhere—This directory server option is available for *only* the user data directory server and integration with OctetString Virtual Directory Engine (VDE). The LDAP directory branches containing NetPoint configuration (and policy) data must reside on one or more directory servers *other than* the one hosting VDE or user data. NetPoint applications only recognize configuration and policy information that resides outside the VDE virtual directory.

Important: *Before* you install the first COREid Server for use with COREid Data Anywhere, read the chapter on integrating NetPoint with VDE in the *NetPoint Integration Guide* and complete activities as specified. For more information about directory server requirements, see "Directory Server Requirements" on page 52.

Host Systems—Oblix recommends you install the COREid Server and Access Server on different machines. The COREid Server does not need to be on the same host system as any other NetPoint component or application.

Language Packs—If you are installing the COREid Server with a Language Pack on a Unix system, you must ensure that the Language Pack has execute permissions before launching the main installer. For example:

```
chmod +x "NetPoint7_0_FR_sparc-s2_LP_Access_System"
```

For more information about Language Packs, see "Installing Optional Language Packs" on page 30.

Multiple COREid Servers—To install more than one COREid Server in your environment, see "About Installing Multiple COREid Servers" on page 101.

Novell eDirectory—To avoid problems with GroupOfUniqueNames, change the class mapping for Groups in the LDAP Group object to reference GroupOfUniqueNames instead of groupOfNames (the default), as described in "Data Storage Requirements" on page 59.

Siemens DirX—Before NetPoint installation, ensure that the machine hosting DirX has enough disk space for the NetPoint indexes. For more information, see "Assessing Directory Server Space" on page 54 and the *DirX EE Disc Dimensioning Guide*. The indexes required for Oblix attributes need to be installed *after* NetPoint COREid Server installation to optimize performance during search operations for these attributes. For details, see "Installing Indexes for Siemens DirX" on page 119.

Currently, NetPoint does not support collective attributes and their subentries. As a result, the user data tree stored in the Siemens DirX directory server must *not* contain any collective attribute subentry. You need to delete collective attributes and their subentries before starting NetPoint setup, otherwise setup may not be complete.

Note: If you use the example database o=my-company shipped with DirX EE for test purposes, remove all existing collective attribute subentries, if any, *before* installing the COREid Server. See "COREid Server Prerequisites Checklist" on page 105.

Siemens DirX is shipped for SSL/TLS connections with files containing a self-signed server certificate and the associated key material. Siemens DirX also supports server certificates issued by any CA. This self-signed certificate can be specified during NetPoint installation and used immediately for SSL/TLS session encryption. For more information, see "Securing Directory Server Communications" on page 56.

NetPoint does not currently support UTCTime and GeneralizedTime syntaxes directly. When using Siemens DirX, be sure to map these attributes as CaseIgnoreStrings in NetPoint *after* installation and setup, as described in "Mapping Attributes for Siemens DirX" on page 151.

Separate Storage of User Data and Configuration Data—NetPoint supports storing user data separately from configuration and policy data. In previous releases, this was supported with only a Sun directory server. However, NetPoint 7.0 extends this capability to Siemens DirX directory servers. With Siemens DirX or Sun directory servers, data may be stored anywhere. This includes storing data either together on the same directory server or on different directory servers of the same type.

NetPoint 7.0 also supports storing user data on a separate directory server *type* from configuration and policy data, regardless of directory server type. For example, you may want to store user data in Active Directory and NetPoint configuration and policy data on ADAM.

In either case, when storing data separately:

- The searchbase (user data) and configuration DN (NetPoint configuration base) must be unique.
- The request for details about SSL-enabled communication will be repeated if you have SSL-enabled between the COREid Server and each directory server.

Note: If you intend to have more than one user data directory and searchbase with Sun or Siemens DirX, be sure to specify the main user data directory and searchbase during installation and setup.

For directory server requirements, see "Directory Server Requirements" on page 52. With Active Directory, see "Installing NetPoint with Active Directory" on page 394 before you start NetPoint installation. With Active Directory Application Mode, see "Installing NetPoint with ADAM" on page 407.

Transport Security Modes—During installation, the transport security mode you choose will impact the scope of communication details you will be asked for in a later procedure. When you provide COREid Server details, you will be asked if this is the first COREid Server being installed for the directory server. Your response will determine the scope of activities in later procedures. Instructions in this chapter cover installing both the first COREid Server and installing other COREid servers.

Scope of Activities—The scope of activities when you define communication details is determined in part by the transport security mode you choose and in part by the directory server communication security you choose. Steps are provided for most sequences. You may skip those that do not apply to your installation. For example:

- **Simple—**Complete step 4.
- **Certificate—**Continue with step 5.

Two procedures are provided to guide you as you specify directory server details:

- One procedure walks you through installing the first COREid Server for the directory server.
- A second procedure walks you through specifying details for additional COREid Servers installed on a Windows system. When you install additional COREid Servers on a Unix system, no additional directory server details are needed.

A default directory profile will be created for this COREid Server based on the information you supply. This profile will be available after you setup the COREid System, as described in “Setting up the COREid System” on page 136.

COREid Server Prerequisites Checklist

Before you begin installing the COREid Server, check the tasks in Table 23 to ensure they have been completed. Failure to complete prerequisites may adversely affect your NetPoint installation.

Table 23 COREid Server Installation Prerequisites Checklist

Checklist	COREid Server Installation Prerequisites
	Review prerequisites, requirements, and options in “Preparing to Install NetPoint” on page 39.
	Review “About the COREid Server and Installation” on page 99.
	Review “COREid Server Installation Considerations” on page 102.
	Review “COREid Server Installation Considerations” on page 102: • **COREid Data Anywhere**—Complete activities in the *NetPoint Integration Guide.* • **Siemens DirX**—Complete activities in “Assessing Directory Server Space” on page 54.
	Move Language Pack installers into the same directory as the COREid Server installer, if desired, and ensure that the Language Pack installer on Unix systems has execute permissions, as described in “COREid Server Installation Considerations” on page 102.

Installing the COREid Server

Refer to your completed installation preparation worksheets as you install the COREid Server. The installation task has been divided into the following procedures:

- “Starting the Installation” on page 106
- “Installing the COREid Server” on page 107
- “Specifying a Transport Security Mode” on page 108
- “Specifying COREid Server Configuration Details” on page 108
- “Defining Communication Details” on page 110
- “Defining Directory Server Details” on page 113

- “Finishing the COREid Server Installation” on page 117

Starting the Installation

You can start the installer in either GUI or console mode, as described in:

- “To start the installation in GUI mode” on page 106
- “To start the installation in Console mode” on page 106

Following the program launch, one set of procedures will be provided because the sequence is similar regardless of your platform.

Note: Skip any details that do not apply to your installation. If you are installing with Microsoft Active Directory, see “Installing NetPoint with Active Directory” on page 394 before proceeding.

To start the installation in GUI mode

1. Log in as a user with administrator privileges.
2. Locate and launch the component installer stored in a temporary directory created when you downloaded the software.

   For example:

   Windows—NetPoint7_0_Win32_COREid_Server.exe
   Solaris—./NetPoint7_0_sparc-s2_COREid_Server -gui

   The Welcome screen appears.
3. Dismiss the Welcome screen by clicking Next, then continue as described in “Installing the COREid Server” on page 107.

   Important: Due to a problem with Installshield, passwords containing $ or other special character sequences may not be interpreted properly. See “Installing from the GUI vs. Command Line” on page 34.

To start the installation in Console mode

1. Log in as a user with administrator privileges.
2. Locate and launch the installation packages in a temporary directory created when you downloaded the software.

   For example:

   Solaris—./NetPoint7_0_sparc-s2_COREid_Server
   Windows Command Window—
   NetPoint7_0_Win32_COREid_Server.exe -console

   The Welcome screen appears.

3. Dismiss the Welcome screen by clicking Next, then continue as described in “Installing the COREid Server” on page 107.

Installing the COREid Server

During this sequence, you must accept the terms of the license agreement and specify the installation directory for your COREid Server. If you have a Language Pack in the same directory as the COREid Server installation package, you will be asked to choose a language.

To install the COREid Server

1. Read and accept the terms of the license agreement, then click Next to continue.
2. Respond to the next question based upon your platform. For example:
   - **Windows**—If you are logged in with administrator rights, click Next (otherwise click Cancel, log in as a user with administrator privileges, then restart the installation).
   - **Unix**—Specify the username and group that the COREid Server will use, then click Next. Typically, the defaults are “nobody”.

     For HP-UX, the defaults are WWW (username) and others (group).

   You are asked to specify the installation directory for the COREid Server. When you do this and click Next, the installation will begin and you will not be able to return to restate the name.
3. Accept the default directory by clicking Next (or change the destination, then click Next).

   For example:

   \NetPoint_70

   You complete step 4 to choose a locale (base language) and other locales (languages) to install. Otherwise, skip to step 5.
4. **Language Pack**—Choose a Default Locale and any other Locales to install, then click Next.

   For example:

   English
   French

   A summary identifies the installation directory and required disk space and asks you to make a note of this information for future reference.

5. Write the installation directory name in the preparation worksheet if you haven't already, then click Next to continue.

   You are notified that the COREid Server is being installed, which may take several seconds. On Windows systems, the Microsoft Managed Interfaces are being configured.

   Note: If a previous version of a NetPoint component or file is detected, you must specify a new installation directory path or uninstall the existing version.

   You are now asked to specify the transport security mode. At this point you cannot return to restate previous details.

Specifying a Transport Security Mode

For more information, see "Securing NetPoint Component Communications" on page 45.

To specify a transport security mode

1. Choose the desired mode to use between the COREid Server and its clients: Open, Simple, or Cert.

   If you chose either Simple or Cert, you will be asked for more information later.

2. Click Next.

   You are now asked for COREid Server configuration details.

Specifying COREid Server Configuration Details

You are asked to identify this COREid Server by entering a unique name that will be used in the COREid System Console. The COREid Server name you specify must uniquely identify this COREid Server in the COREid System Console. This name must differ from the name of any other COREid Server that accesses the same instance of your LDAP directory server, and cannot contain any blank spaces. You may use this name as a Windows Service name for the COREid Server.

In addition, you are asked to identify the DNS hostname where this COREid Server will be installed and the port number on which this COREid Server communicates with the WebPass and, by extension, with your Web server.

After you describe the COREid Server, you will be asked if this is the first COREid Server to be installed for the directory server. Your answer will determine the scope of activities now and during the setup process after WebPass installation. Selecting *Yes* indicates that this is the first COREid server and you will be asked about directory server communication, schema updates, and directory server configuration details. Selecting *No* indicates that a COREid Server has already been set up with this directory server. When you select *No*, you will be asked about directory server communication. On a Windows system, you will also be asked for Active Directory details.

To identify this COREid Server

1. Enter a unique name for this COREid Server that adheres to the guidelines above.

   For example:

   COREid_70_1_6025

2. Enter the DNS hostname where this COREid Server will be installed.

   For example:

   DNS_hostname.domain.com

3. Enter the port number on which this COREid Server communicates with its clients, then click Next.

   For example:

   6025

4. Respond when asked if this is the first COREid Server to be installed for the directory server, then click Next.

   For example, when you are installing the *first* COREid Server only, choose:

   Yes

Regardless of your response to the question about this being the first COREid Server, you are now asked to specify communication details for the directory server and for the transport security mode you chose earlier.

Defining Communication Details

During this sequence, you are asked about securing communication between the COREid Server and your directory server. You may answer No during installation, then set up an SSL connection to the directory later as described in the *NetPoint 7.0 Administration Guide Volume 1*. In addition, you will be asked to specify NetPoint transport security details based on the information you supplied earlier.

COREid Data Anywhere—This directory server option is available for *only* the user data directory server and integration with OctetString Virtual Directory Engine (VDE). *Before* you install the first COREid Server for use with COREid Data Anywhere, read the chapter on integrating NetPoint with VDE in the *NetPoint Integration Guide* and complete activities as specified.

Siemens DirX—When DirX SSL is configured with a server certificate issued by a CA, you need to specify a file containing the CA certificate in Base 64 format during NetPoint installation. See "Securing Directory Server Communications" on page 56.

Separate Data Storage—If you plan to store user data separately from Oblix (NetPoint) configuration data, see "COREid Server Installation Considerations" on page 102 for more information.

Unix Systems—If you are installing on a Unix system using either Open or Simple transport security for NetPoint, *and* this is *not* the first COREid server, there are few security options and no directory server details required. In this case, complete steps below, as needed, then skip to "Finishing the COREid Server Installation" on page 117.

To define communication details

1. Check the box beside the appropriate option if you have a certificate and want to enable SSL between the COREid Server and the directory server, then click Next.

   For example:

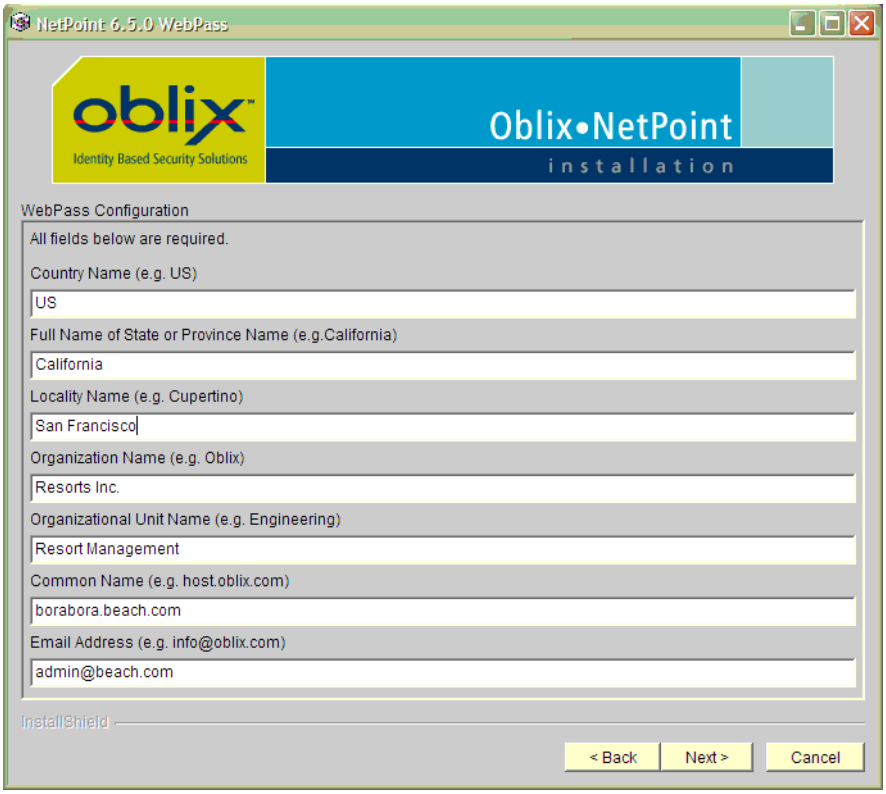
   Directory Server ... user data is in SSL
   Directory Server ... Oblix data is in SSL

   Note: Ensure you have a check mark beside each option if you have a certificate and want to enable SSL for each.

2. **SSL**—Specify the path to the root CA certificate, and click Next.

   If you are installing on an Active Directory forest, enter the directory and file name of the retrieved CA certificate. See "Installing NetPoint with Active Directory" on page 394.

3. Complete the transport security dialog according to the mode you chose earlier. For example:
   - **Open—**Skip to "Defining Directory Server Details" on page 113 unless you are installing on a Unix system *and* this is *not* the first COREid server. In the later case, skip to "Finishing the COREid Server Installation" on page 117.
   - **Simple—**Complete step 4.
   - **Certificate—**Continue with step 5.
4. **Simple**—Enter and confirm the Pass Phrase to authenticate between the COREid Server and WebPass, then click Next and continue as follows:
   - If this is the first COREid Server *or* if you are installing an additional COREid Server on a Windows system, skip to "Defining Directory Server Details" on page 113.
   - If you are installing on a Unix system *and* this is *not* the first COREid server, skip to "Finishing the COREid Server Installation" on page 117.
5. **Certificate**—Indicate if you are requesting or installing a certificate, then click Next and continue.
6. **Certificate**—Enter and confirm the Pass Phrase to authenticate between the COREid Server and WebPass, then click Next.
   - If you are installing a certificate, skip to step 10.
   - If you are requesting a certificate, continue with step 7.
7. **Request Certificate**—Enter the following information, then click Next and issue your request for a certificate to your CA. For example:



Two Characters

Your Company

Division or Dept.

Full DNS Hostname

Valid email

8. **Request Certificate**—Record certificate file locations, if they are displayed.
9. **Request Certificate**—Click Yes if your certificates are available and continue with step 10 (otherwise click No and skip to "Defining Directory Server Details" on page 113).

   If you selected No, instructions are provided.

Note: You do not need a certificate in hand to finish the installation. However, the COREid System cannot be setup until the certificates are copied to *COREid_install_dir*\identity\oblix\config and the COREid Server is restarted. See the *NetPoint 7.0 Administration Guide Volume 1* for details.

---

10. **Install Certificate** —Specify the full paths to the following three files, then click Next:

    COREid_install_dir\identity\oblix\config

    - Certificate file (ois_cert.pem)
    - Key file (ois_key.pem) the installer may know where this is.

- Chain file (ois_chain.pem)

Note: When using certificates generated by a subordinate CA, the root CA's certificate must be present in the *xxx*_chain.pem along with the subordinate CA certificate. Both certificates must be present to ensure appropriate verification and successful COREid System setup.

The information you provided has been saved and you are asked if you want to update the schema. You cannot return to restate details.

11. Continue with "Defining Directory Server Details" on page 113.

Defining Directory Server Details

What you see and do during this sequence depends in part upon how you responded when asked if this was the first COREid Server to be installed for this directory sever. Refer to the topics below and choose the one for this installation.

- "Installing the First COREid Server" on page 113
- "Installing Additional COREid Servers on Windows" on page 116

Note: If you are installing on a Unix system *and* this is *not* the first COREid server, skip to "Finishing the COREid Server Installation" on page 117.

Installing the First COREid Server

If you indicated that this is the first COREid Server being installed for the directory server, you will be asked if you want to update your directory server with the Oblix schema. This will include NetPoint-specific workflow definitions, attribute policies, tab and panel configurations, configuration attributes, and the like.

Schema Extension—Oblix recommends that you automatically extend the schema during installation of the first COREid Server. You update the schema only once. Either Yes response will result in questions about directory server type and specifications.

A No response on a Windows system will lead to questions for Active Directory. A No response on a Unix system will conclude the installation.

Separate Data Storage—If you plan to store user data separately from Oblix (NetPoint) configuration data, see "COREid Server Installation Considerations" on page 102 and "Data Storage Requirements" on page 59 for more information.

By default, Oblix configuration and user data are presumed to be on the same directory server. With Siemens DirX or Sun directory servers, data may be stored either together on the same directory server or on different directory servers of the same type.

To specify directory server details for the first COREid Server

1. Select the option that describes your environment.

   For example:

   Oblix data will be in the user data directory

2. Select the appropriate schema update option for your environment, then click Next.

   For example:

   Yes

   - If Yes, continue with step 3.
   - If No and you are installing on a *Windows* system, skip to "Installing Additional COREid Servers on Windows" on page 116
   - If No and you are installing on a *Unix* system, skip to "Finishing the COREid Server Installation" on page 117.

3. Select your directory server type for automatic configuration, and click Next.

   For example:

   Siemens DirX

   You are asked for directory server configuration details. If you chose Active Directory for Windows 2003, you will be asked about dynamic auxiliary class support.

4. Specify your directory server configuration details, then click next.

   For example:

   - **Host name**—The DNS hostname of the directory server machine
   - **Port number**—On which the directory server listens (for SSL connections, provide the encrypted port)

- **Bind DN**—For the *user data* directory server

  Note: The distinguished name you enter as the bind DN must have full permissions for the user and/or Oblix branches of the directory information tree (DIT). NetPoint will access the directory server as this account. Examples are provided in Table 24. Your directory server configuration may differ.

Table 24 Bind DN for Various Directory Servers

Directory Server	Bind DN
Active Directory **or** Active Directory on Windows Server 2003	cn=*administrator*,cn=users,<domain DN> **Note**: This information is required even if you are using ADSI with implicit bind. See "Installing NetPoint with Active Directory" on page 379 and the *NetPoint 7.0 Administration Guide Volume 1* for more information.
ADAM	cn=*administrator,o=domain.com* The values represent: • A Windows security principal user name. • Domain name of the machine where ADAM is installed. **Notes**: The Netpoint Administrator must be an ADAM user with administrative privileges, not a Windows Security Principal. See "Installing NetPoint with ADAM" on page 407 for more information.
COREid Data Anywhere	cn=*admin*
IBM Directory Server	cn=*root*
NDS	cn=*admin*,o=nds
Siemens DirX	cn=*admin*,o=*my-company*
Sun Directory Server 5.x	cn=*administrator* **Note**: Oblix recommends that you do **not** use cn=Directory Manager. For details, see "Directory Server Requirements" on page 52.

- **Password**—The password for the user data directory server bind DN

5. Click Next and continue as indicated below:

   - **If Active Directory 2003**—You are asked about ADSI (for user data).

- **If Oblix Data is Separate**—Repeat step 4 to specify details for the Oblix data directory. The SSL sequence will repeat for this directory, if needed.

If the schema cannot be updated, you are offered the opportunity to run the sequence again and restate information. If you decline, you must manually update the schema using the ldapmodify utility that ships with LDAP SDK or the following file:

COREid_install_dir\identity\oblix\tools\ldap_tools\ds_conf_update.exe

---

Note: All ldapmodify options can be viewed by using -h option. All ds_conf_update options can be viewed by using the --help option. Both utilities may be used with the COREid Server and Access Manager installations.

For an example of the ldapmodify command, see "Updating the Schema and Attributes Automatically vs. Manually" on page 32. If you choose to update the Siemens DirX schema with NetPoint configuration data using ds_conf_update, the command is:

```
ds_conf_update -h DS_hostname -p 389 -D cn=admin,o=my-company
-w passwd -i C:\np\ois\identity -d 8 -e C:\errFile.txt -n 3
```

For more information on the -d option and directory server type input, see "Silent Mode Parameters" on page 249.

6. Continue with "Finishing the COREid Server Installation" on page 117.

Installing Additional COREid Servers on Windows

In this sequence you are asked to supply information related to Active Directory. This sequence occurs only when:

- You indicated that this is *not* the first COREid Server in the installation
- You declined the automatic schema update on a Windows system

---

Note: Your responses determine the scope of this sequence. Whenever your sequence ends, skip to "Finishing the COREid Server Installation" on page 117.

To specify Active Directory Details on a Windows system

1. Select No when asked if you want to update the schema, then click Next.
2. Click Yes if you are using Active Directory with ADSI (or No if you are not), then click Next.

   For example:

   Yes

   If Yes, continue with step 3. If No, skip to "Finishing the COREid Server Installation" on page 117.
3. Click Yes if the machine on which you are installing this COREid Server is in a separate Active Directory domain from the NetPoint data (otherwise, click No), then click Next.

   For example:

   No

   If No, continue with step 4. If Yes, skip to "Finishing the COREid Server Installation" on page 117.
4. Click Yes if you want to use implicit bind with the directory server (or No if you don't), then click Next.

   For example:

   Yes
5. See "Finishing the COREid Server Installation" on page 117.

Finishing the COREid Server Installation

You complete the first step only if you are installing on Microsoft Windows. Otherwise, skip to step 2

To finish the installation

1. **Windows**—Specify a unique service name to identify your COREid Server in the Windows Services window, then click Next.

   If the name is already registered as a Windows Service name on this host, you will be asked if you want to try again. In this case, you can either choose Yes to provide a unique name now or No to set this up manually using *COREid_install_dir*\identity\oblix\apps\common\bin\config_ois.exe.

   Oblix NetPoint ReadMe information appears.
2. Scroll through the ReadMe information to find out how to reach the documentation online and contact Oblix.

3. Click Next to display an installation summary.

   The installation summary provides the details that you specified during this installation and instructs you to start the COREid Server at the conclusion of this installation.

4. Write the details about this installation, if needed, then click Next.

5. Click Finish to complete the sequence.

6. Start the COREid Server as described below, which will confirm that the COREid Server is installed and operating properly.

   - **Windows**—Open the Services Window then locate and start the NetPoint COREid Server service.

     By default, the COREid Server (also known as the Oblix Identity Server (OIS)) starts manually, but you can set its startup type to Automatic. See the Microsoft Windows Help for details.

   - **Unix**—Execute the following command:
     /*COREid_install_dir*/identity/oblix/apps/common/bin/start_ois_server

7. Continue your NetPoint installation, as follows:

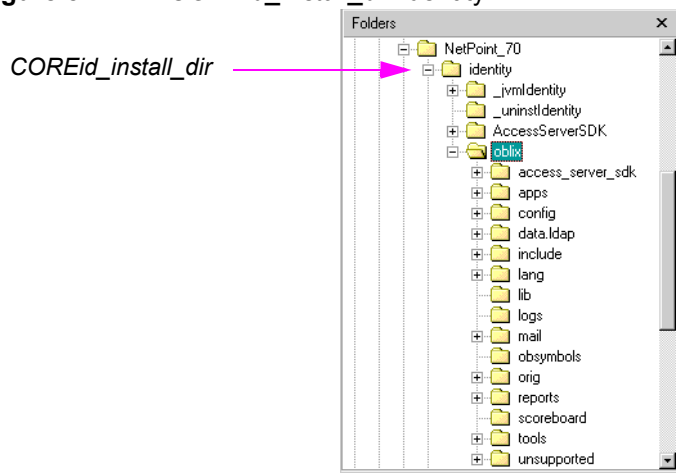
   - **Siemens DirX**—See “Installing Indexes for Siemens DirX” on page 119 before “Installing WebPass” on page 121.

   - **All Platforms**—See “Installing WebPass” on page 121.

Installed Files

During installation, a *COREid_install_dir*\identity directory was created, as shown next.

Figure 5 *COREid_install_dir*\identity



Installing Indexes for Siemens DirX

After installing the COREid Server, you need to install the indexes required for Oblix attributes to ensure adequate performance of searches for these attributes. You need at least 60 indexes for the NetPoint configuration data directory and at least 25 for user data indexes. DirX provides a default maximum of 20 indexes, which must be changed before installing Oblix indexes.

Note: As noted in "COREid Server Installation Considerations" on page 102, you need enough disk space for the indexes using information available in "Assessing Directory Server Space" on page 54 and the *DirX EE Disc Dimensioning Guide*.

To install Oblix indexes for Siemens DirX

1. Ensure that you have enough DirX disk space allocated on the machine hosting Siemens DirX, as described in "To increase the DirX disk space for NetPoint indexes" on page 55.
2. Ensure that the DirX service is started.

3. On the machine hosting the COREid Server, locate the index files for DirX:

   COREid_install_dir/identity/oblix/data.ldap/common/
   DirX_oblix_index_add.txt
   DirX_user_index_add.txt (needed only if user data is on a different directory instance)

4. Copy the NetPoint DirX index files above to the machine hosting Siemens DirX.

5. On the machine hosting DirX, start the DirX administration command-line tool in a directory where NetPoint DirX index files are present by calling:

   dirxadm

6. From the dirxadm prompt, complete the steps below:

   a) Bind as the administrator.

      For example:

      dirxadm> bind -u /o=*my-company*/cn=*admin* -password *passwd* -auth simple

   b) Import the index files to DirX.

      For example:

      import_dbconfig DirX_oblix_index_add.txt

      OR

      import_dbconfig DirX_user_index_add.txt

7. Proceed to “Installing WebPass” on page 121.

4 Installing WebPass

The NetPoint WebPass is second in the sequence of NetPoint components to install. This chapter explains how to install the WebPass and configure your Web server to work with it. For details, see:

Upgrading to NetPoint 7.0 is described in the *NetPoint 7.0 Upgrade Guide*. For an overview of NetPoint components, see the Introduction to *NetPoint 7.0 Guide*.

About WebPass and Installation

The WebPass is a Web server plug-in that shuttles information back and forth between the Web server and the COREid Server, as described in “About NetPoint Installations” on page 23.

Installing a WebPass follows a similar sequence and includes a number of the same procedures as the COREid Server installation. However, the WebPass does *not* communicate with the directory server. Therefore, no directory server details are needed. The WebPass *does* communicate with a Web server. As a result, the Web server configuration needs to be updated, which can be accomplished either automatically during WebPass installation or manually after installation.

There must be enough disk space and the WebPass must be able to communicate with the Web server host.

Task overview: Installing a WebPass

1. Install the WebPass and specify a unique identifier (different than COREid Server identifier), as described in “Installing the WebPass” on page 125.
2. Conclude with the appropriate procedures for your installation. For example:
   - “Manually Configuring Your Web Server” on page 130 if you don’t do this automatically during installation
   - “Verifying WebPass Permissions on IIS” on page 131
   - “Confirming WebPass Installation” on page 132

Important: Be sure to choose the proper package for your Web server and platform, as described in “Platform Requirements” on page 66. Differences for specific operating systems and Web servers are noted within the installation procedures when appropriate. Also, be sure the identifier you specify for the WebPass is unique and different from the identifier you specified for the COREid Server.

Again, you must complete all procedures for a successful installation. Information is saved at certain points during the installation process. If you cancel the installation after being informed that the WebPass is being installed, you must uninstall the component, as described in “Upgrading from a Previous Version of NetPoint” on page 37.

The installation process is similar regardless of the installation mode you choose and your operating system. Any caveats are identified and may be skipped when they do not apply to your environment.

During WebPass installation on a Windows system, you will be not be asked to specify a Windows Service name. Rather than starting and stopping a WebPass service, you will start and stop the WebPass Web server.

After installation, you must establish communications between WebPass and its COREid System when the Web server restarts using the following procedure.

To establish communications between WebPass and its COREid System

1. Stop the WebPass Web server instance.
2. Stop then restart COREid Server service.
3. Start the WebPass Web server instance.

For more information, see “WebPass Installation Considerations” on page 123.

About the WebPass Installation Directory

You may install the WebPass in the default directory or in a directory of your choosing. However, 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.

When you change the path name, you may include any characters that are acceptable to your operating system. For example, you may include spaces on Windows systems but not on Unix systems. During installation, \identity is added to the WebPass installation directory path, which becomes:

Default on Windows—\Program Files\NetPoint\WebComponent\identity
Default on Unix—/opt/netpoint/webcomponent/identity
In This Guide—*WebPass_install_dir*\identity

Important: The WebPass cannot reside in the same directory as the COREid Server or Access Manager.

If you specify C:\NetPoint\WebComponent as the WebPass installation directory, you must also specify this as the Access Manager installation directory when the two components will reside on the same machine. Remember that \access is appended to the Access Manager installation directory.

About Installing Multiple WebPass Instances

If you plan to install multiple WebPass instances, pay close attention to the following items:

- Oblix NetPoint supports one WebPass per Web server instance; each WebPass must have its own Web server instance.
- You must have at least one WebPass installed before you complete COREid Server setup described under “Setting up the COREid System” on page 136.

  After the first COREid Sever is set up, you can install any number of WebPass instances. No extra setup is required.
- All WebPass instances must be installed with the same transport security mode as the COREid Server to which they are connecting.

WebPass Installation Considerations

Each Web server instance that communicates with the COREid Server must be configured with a WebPass. One WebPass can communicate with multiple COREid Servers. More than one WebPass can communicate with the same COREid Server, which is recommended for load balancing.

A WebPass must also be installed with each Access Manager on the same Web server instance, at the same directory level.

The WebPass identifier that you specify during installation must be unique. The WebPass identifier is not validated until after the installation, when the Web server is started.

NetPoint supports Apache with or without SSL enabled. For SSL-enabled communication, NetPoint supports Apache with mod_ssl only, not Apache-SSL. mod_ssl is a derivative of, and alternative to, Apache-SSL.

The account that performs NetPoint installation must have administration privileges.

If you installed the COREid Server with a Language Pack, you must install the WebPass with the same Language Pack. On a Unix system, ensure that the Language Pack has execute permissions before launching the main installer. For example:

```
chmod +x "NetPoint7_0_FR_sparc-s2_LP_Access_System"
```

See also, "About WebPass and Installation" on page 121.

WebPass Prerequisites Checklist

Before you begin installing the WebPass, check the tasks in Table to ensure they have been completed. Failure to complete prerequisites may adversely affect your NetPoint installation

Table 25 WebPass Installation Prerequisites Checklist

Checklist	WebPass Installation Prerequisites
	Complete a COREid Server Installation, as discussed in "Installing the COREid Server" on page 105.
	Move Language Pack installers into the same directory as the WebPass installer, if needed, and ensure that the Language Pack installer on Unix systems has execute permissions, as described in "WebPass Installation Considerations" on page 123.

Installing the WebPass

Refer to your completed installation preparation worksheets as you install the WebPass. The procedures in this sequence cover both GUI and console mode. Following the program launch, one set of procedures will be provided because the sequence is similar.

The following procedures must be completed to install the WebPass:

- "Starting the Installation" on page 125
- "Specifying a Transport Security Mode" on page 126
- "Specifying WebPass Configuration Details" on page 127
- "Updating the WebPass Web Server Configuration" on page 128
- "Finishing the WebPass Installation" on page 129

Starting the Installation

Be sure to choose the appropriate package for your Web server and platform.

To start the installation

1. Log in as a user with administrator privileges.
2. Locate and launch the component installer stored in a temporary directory created when you downloaded the software:
3. Launch the installation for your preferred platform, installation mode, and Web server.

   For example:

   - **GUI Mode**
     Windows—NetPoint7_0_Win32_*API*_WebPass
     Solaris—./NetPoint7_0_sparc-s2_*API*_WebPass -gui
   - **Console Mode**
     Solaris—./NetPoint7_0_sparc-s2_*API*_WebPass
     Windows Command Window—
     NetPoint7_0_Win32_*API*_WebPass.exe -console

   The Welcome screen appears.
4. Dismiss the Welcome screen by clicking Next.
5. Read and accept the terms of the license agreement, then click Next to continue.
6. Respond to the next question based upon your platform. For example:

- **Windows**—If you are logged in with administrator rights, click Next (otherwise click Cancel, log in as a user with administrator privileges, then restart the installation).
- **Unix**—Specify a dedicated username and group that the Web server will use, then click Next. Typically, the defaults are nobody.

  For HP-UX, the defaults are WWW (username) and others (group).

You are asked to specify the installation directory for the WebPass.

7. Choose the installation destination, then click Next.

   For example:

   NetPoint_70\WebComponent

8. **Language Pack**—Choose a Default Locale and any other Locales to install, then click Next.

   A summary identifies the installation directory and required disk space and asks you to make a note of this information for future reference.

9. Write the installation directory name, if needed, then click Next to continue.

   You are notified that the WebPass is being installed and kept informed about the status of the process, which may take several seconds. On Windows systems, the Microsoft Managed Interfaces are also being configured.

   You are asked to specify a transport security mode to use between the NetPoint WebPass and COREid Server. At this point, you cannot return to restate the installation directory.

Specifying a Transport Security Mode

For more information, see “Securing NetPoint Component Communications” on page 45.

To specify a transport security mode

1. Choose the same transport security mode for the WebPass as you did for the COREid Server.
2. Click Next.

   When you specify Simple or Cert, you will be asked for additional information later. You are asked now for WebPass configuration details.

Specifying WebPass Configuration Details

Now, you are asked to enter a unique name to use for this WebPass, which will appear in the COREid System Console after setup.

Each WebPass must have a unique name that identifies it. The WebPass name you specify cannot contain any blank spaces and must uniquely identify this WebPass in the COREid System Console and LDAP directory.

You are also asked to identify the DNS hostname and port number of a COREid Server with which this WebPass should communicate. In addition, you may be asked to specify additional information about the transport security mode you selected when you selected either Simple or Certificate mode only.

To specify WebPass configuration details

1. Enter a unique name for this WebPass that adheres to the guidelines above.

   For example:

   WebPass_70_1_72

2. Enter the DNS hostname of the COREid Server with which this WebPass should communicate.

   For example:

   COREid_DNS_hostname

3. Enter the port number of the COREid Server with which this WebPass should communicate, then click Next.

   For example:

   COREid_port

4. Perform the following operations according to the transport security mode you chose earlier.

   - **Open**—Skip to "Updating the WebPass Web Server Configuration" on page 128.
   - **Simple**—Specify and confirm the Pass Phrase to authenticate between the COREid Server and WebPass, click Next, then continue with "Updating the WebPass Web Server Configuration" on page 128.
   - **Certificate**—Continue with step 5.

5. **Certificate**—Indicate if you are requesting or installing a certificate, then click Next and continue as follows:

   - If you are requesting a certificate, enter information about your organization, click Next, issue the request to your CA, and continue with step 6.
   - If you are installing a certificate, skip to step 8.

6. **Request Certificate**—Record the location of the private key and certificate request files, if displayed, then click Next.
7. **Request Certificate**—Click Yes if your certificates are available (otherwise click No), then click Next and continue with step 8.

   If certificates are not ready, complete the installation. When you receive the certificates, copy these to the *WebPass_install_dir**identity*\oblix\config directory and restart the WebPass Web server.
8. **Install Certificate**—Specify the full paths to the requested files, then click Next and continue with "Updating the WebPass Web Server Configuration" on page 128.

   You are notified that the WebPass is being configured, which may take a few seconds. The information has been saved and you may not return to previous screens to restate details.

   You are now asked to update the WebPass Web server configuration.

Updating the WebPass Web Server Configuration

Your WebPass Web server must be configured with NetPoint-related configuration information to use the WebPass component. You can direct this update to occur either automatically or manually. Updating the Web server configuration:

- On Sun Web servers a configuration update involves updating the obj.conf and magnus.conf files.
- On IIS Web servers a configuration update involves updating the Web server directly by adding the ISAPI filter and creating extensions required by NetPoint.
- On Apache Web servers a configuration update involves updating the httpd.conf file.

Oblix recommends automatically updating your Web server configuration. However, instructions for manual configuration are included.

To automatically update your Web server configuration

1. Click Yes to automatically update your Web server, then click Next. For example:
   - **Most Web Servers**—Specify the absolute path of the directory containing the Web server configuration files.
   - **IIS Web Servers**—The process begins immediately and may take more than a minute.

   A screen appears when the Web server configuration has been updated.

2. **Sun Web Servers**—Apply the changes in the Web server Administration console *before* you continue.
3. Stop the WebPass Web server instance, then stop the COREid Server service.
4. Start the COREid Server service, then start the WebPass Web server instance.
5. Click Next to dismiss the announcement, then continue with "Finishing the WebPass Installation" on page 129.

   ReadMe information appears.

To manually update your Web server configuration

1. Click No when asked if you want to proceed with the automatic update, then click Next.

   ReadMe information appears along with a new screen to assist you in manually setting up your Web server for NetPoint.
2. Return to the WebPass installation screen and click Next to finish the installation.
3. Complete "Manually Configuring Your Web Server" on page 130.

Finishing the WebPass Installation

The ReadMe information provides details about documentation and Oblix.

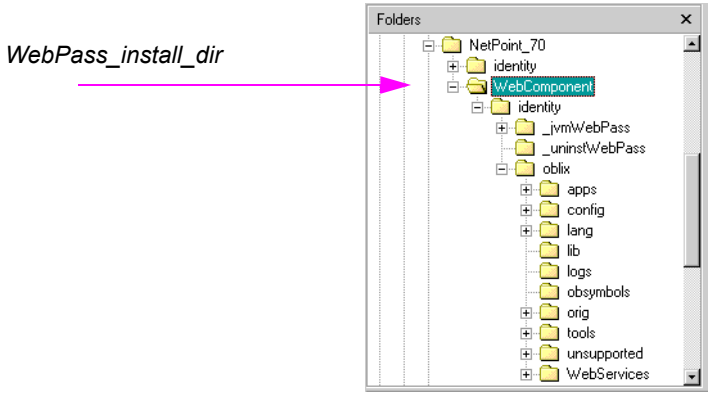
To finish the WebPass installation

1. Review the ReadMe information.
2. Click Next to complete the installation.
3. Continue with the following procedures, as needed:
   - "Manually Configuring Your Web Server" on page 130 if you did not do this automatically during WebPass installation.
   - "Verifying WebPass Permissions on IIS" on page 131
   - "Confirming WebPass Installation" on page 132
   - "Setting up the COREid System" on page 136

Installed Files

The following subdirectories were created under *WebPass_install_dir*\identity, where *WebPass_install_dir* is the installation directory you specified.

Figure 6 *WebPass_install_dir*\identity



Manually Configuring Your Web Server

If you do not want the installation wizard to update your Web server configuration during WebPass installation, you must do it manually before you set up the COREid Server.

Note: You complete step 1 only if needed to display online instructions.

To configure your Web server for the WebPass

1. Launch your Web browser, and open the following file, if needed. For example:

   WebPass_install_dir\identity\oblix\lang*langTag*\docs\config.htm

   where *WebPass_install_dir* is the directory where you installed the WebPass and *langTag* is a language, en-us, for example.

2. Select the appropriate Web server interface configuration protocol from the table on the screen, shown next.

Supported Server OS	Web Server	Interface Configurations
	Microsoft IIS	Netscape Servers
Windows Server 2003	ISAPI	-
Windows 2000	ISAPI	NSAPI
Sun Solaris	-	NSAPI

3. Follow all instructions specific to your Web server type and:
   - Make a back up copy of any file that you are required to modify during Web server set up, so it is available if you need to start over.
   - Some setups launch a new browser window or require you to launch a Command window to input information, so ensure that you return to and complete all original setup instructions to enable your Web server to recognize the appropriate NetPoint files.

     Note: If you accidentally close the window, you can open the *WebPass_install_dir*\identity\oblix\apps\common\docs\config.htm file in a browser window and click the appropriate link again.
4. Continue with the appropriate task for your environment when you finish your Web server update. For example:
   - "Verifying WebPass Permissions on IIS" on page 131
   - "Confirming WebPass Installation" on page 132

Verifying WebPass Permissions on IIS

Once you have installed WebPass and updated the Web server configuration, you should ensure that the WebPass installation directory has the proper permissions to run correctly.

To verify the WebPass IIS Web server configuration

1. Locate the directory below:

   WebPass_install_dir\identity\oblix\apps\webpass\bin
2. Right click on the \bin directory, then select Properties.
3. Select the Security tab and ensure that "Allow" for "Read" and "Write" rights are granted to user "SERVICE".

To verify when WebPass was set up in Simple or Cert mode

1. Locate *WebPass_install_dir*\identity\oblix\config\password.xml.
2. Right click on password.xml, then select Properties.

3. Select the Security tab and ensure that “Allow” for “Read” rights are granted to users:

   “IUSR_<machine_name>”
   “IWAM_<machine_name>”
   “NETWORK SERVICE”
   “IIS_WPG” (only for IIS 6.0)

Confirming WebPass Installation

A good way to ensure that the WebPass is installed correctly is to complete the following procedure.

To confirm your WebPass installation

1. Make sure your COREid Server and WebPass Web server are running.
2. Navigate to the NetPoint COREid System Console from your browser by specifying the following URL. For example:

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

   where *hostname* refers to 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.

   The NetPoint COREid System main page should appear.

Note: Do not select any link on the COREid System main page, because the system has not yet been set up. See “Setting up the COREid System” on page 136.

---

5 Setting Up the COREid System

After you install the COREid Server and the WebPass, you must set up and configure the COREid System to work within your environment.

This chapter explains how to set up the COREid System and configure the required attributes. See the following topics:

Important: During setup, specifications are saved whenever you click the Next button. If you leave setup and restart it later, you are returned to the same place.

About Setting Up the COREid System

After a COREid Server and a WebPass are installed, you need to setup the COREid System to complete associations and make the system functional. This process is completed using a Web browser.

During the setup process, you enter information about your directory server and configure required LDAP person and group object classes with NetPoint-specific information. This associates the COREid Server with the WebPass and extends the directory server schema to include the Oblix branch and attributes. For example, the NetPoint COREid System requires attributes assigned to the Full Name, Login, and Password semantic types for Person and Group object classes. For details, see "About NetPoint Object Classes" on page 140.

The setup process described in this chapter applies only to the first COREid Server instance that connects to a given directory server. You may install multiple COREid Servers, all associated with the same directory server. For details, see “About Installing Multiple COREid Servers” on page 101. The setup process for the second or successive COREid Server instances is described in “Setting Up Other COREid Server Instances” on page 154.

The setup process for the first COREid Server is divided into the following procedures.

Task overview: Setting up the COREid System

1. Start the setup process, as described in “Starting the Setup Process” on page 137
2. Define directory server details, as described in “Specifying Directory Server and Data Location Details” on page 138
3. Define object class details, as described in “Specifying Object Class Details” on page 140
4. Verify object class details, as described in “Confirming Object Class Changes” on page 142
5. Define NetPoint administrators, as described in “Configuring NetPoint Administrators” on page 143
6. Finish the setup process, “Completing COREid System Setup” on page 145

You must complete the entire setup process before you can use the COREid applications. During setup, the information that you supply is saved as you progress from one page to the next. You may leave the setup process and restart it at any time. In this case, you will continue with the question that follows your last entry.

Some information may appear in the setup pages automatically based on the updated schema. If you did *not* automatically update your schema during COREid server installation, a sequence of Schema Changes pages appear when you begin the setup. The pages are self explanatory and are not covered here.

COREid System Setup Considerations

One or more of these items may apply to your installation:

Certificates Generated by a Subordinate CA—The root CA's certificate must be present in the ois_chain.pem along with the subordinate CA certificate. Both certificates must be present to ensure appropriate verification for successful COREid System setup.

Separate User and Configuration Data—As discussed earlier, user data may be stored on a separate directory server *type* from configuration and policy data. Also, when you have Siemens DirX or Sun directory servers, you may store user data separately from configuration and policy data (on the same directory server type). In such cases, the searchbase and configuration DN should be unique.

Multiple User Data Directories—If you intend to have more than one user data directory and searchbase, specify the main user data directory and searchbase during COREid System setup. Add one or more database profiles for the disjoint namespaces after setup is complete, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

Active Directory—Read "Installing NetPoint with Active Directory" on page 394 before proceeding. When you are installing NetPoint within a Microsoft Active Directory forest, additional steps are needed during setup:

- Check the box beside Dynamic Auxiliary Object Classes, to enable this feature when asked.
- Ensure the semantic-type "Login" has been assigned to one attribute and that the people you select as NetPoint Administrators all have a value for the login attribute. For more information, see "Configuring NetPoint Administrators" on page 143 and the *NetPoint 7.0 Administration Guide Volume 1*.

If you are using Active Directory with ADSI, you must:

- Complete the ADSI setup procedure *before* COREid System setup, as described in "Setting Up ADSI (Optional)" on page 398.
- Check the Enable ADSI option when you specify the directory server type *during* setup to enable native integration with Active Directory and allow implicit failover and native password changes.

  This creates a default directory profile and an associated database agent. With this configuration, the directory profile (db agent) is automatically assigned a name using a default-ois-machinename convention. You should modify this name to reflect your respective domain name to facilitate user authentication. The resulting directory profile enables the associated COREid Server to perform all operations with a primary domain controller in your Active Directory tree using an Implicit Bind.

Active Directory Application Mode—Read "Installing NetPoint with ADAM" on page 407 before proceeding.

COREid Data Anywhere—This directory server option is available for *only* the user data directory server and integration with OctetString Virtual Directory Engine (VDE). The LDAP directory branches containing NetPoint configuration (and policy) data must reside on one or more directory servers other than the one hosting VDE or user data. NetPoint applications only recognize configuration and policy information that resides outside the VDE virtual directory.

Important: *Before* you setup the first COREid Server for use with COREid Data Anywhere, read the chapter on integrating NetPoint with VDE in the *NetPoint Integration Guide* and complete activities as specified.

Siemens DirX—NetPoint does not currently support UTCTime and GeneralizedTime syntaxes directly. *After* COREid System setup, you need to map these attributes as CaseIgnoreStrings in NetPoint. See "Mapping Attributes for Siemens DirX" on page 151. Also, if you have not yet installed the NetPoint indexes, you may do so before *or* after the setup procedures explained here. For details, see "Installing Indexes for Siemens DirX" on page 119.

COREid System Setup Prerequisites Checklist

Before you begin installing the WebGate, confirm that you have completed the tasks in Table 26. Failure to complete all prerequisites may adversely affect your installation.

Table 26 COREid System Setup Prerequisites Checklist

Checklist	COREid System Setup Prerequisites
	Install a COREid Server, as described in "Installing the COREid Server" on page 105.
	Install a WebPass, as described in "Installing WebPass" on page 121.
	COREid Data Anywhere—Before starting COREid System setup, complete activities described in the chapter on integrating NetPoint with OctetString VDE in the *NetPoint Integration Guide*.
	Active Directory—Before starting COREid System setup, set up ADSI for Active Directory, if needed, as described under "Setting Up ADSI (Optional)" on page 398.

Setting up the COREid System

Refer to your completed installation preparation worksheets as you complete COREid Server setup. The setup process has been divided into the following procedures to help guide you:

- "Starting the Setup Process" on page 137
- "Specifying Directory Server and Data Location Details" on page 138
- "Specifying Object Class Details" on page 140

- “Confirming Object Class Changes” on page 142
- “Configuring NetPoint Administrators” on page 143
- “Completing COREid System Setup” on page 145

Starting the Setup Process

You complete this procedure to start the COREid System setup.

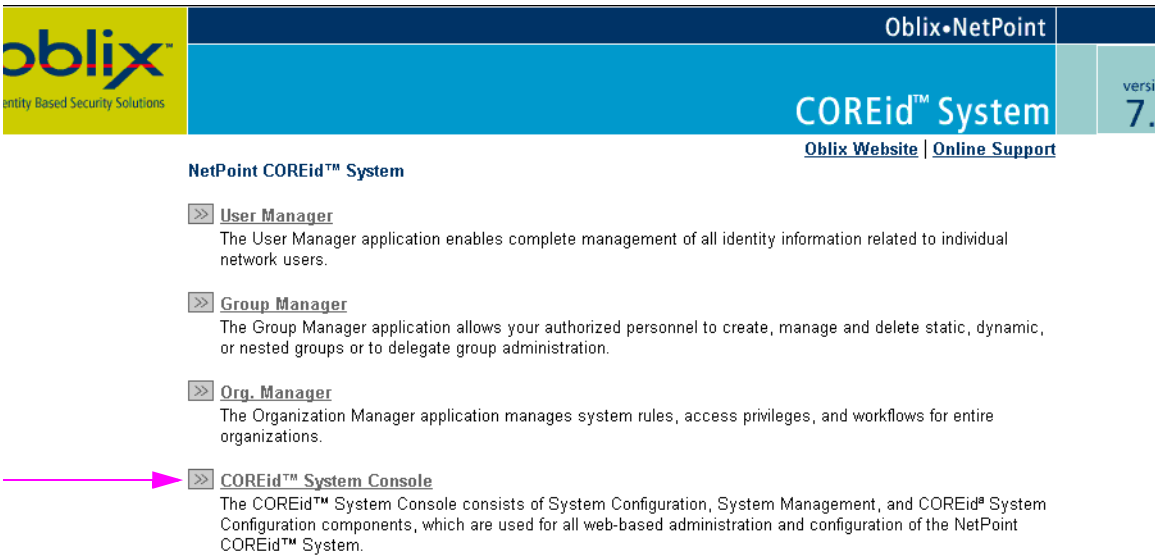
Important: If you just confirmed your WebPass installation and the COREid System Console setup page is currently available, skip to step 2.

To set up the COREid System

1. Navigate to the NetPoint COREid System Console from your browser by specifying the following URL. For example:

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

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



2. Click the COREid System Console link.

   The System Console setup page appears.

3. Click the Setup button.
   - If the license key setup page appears, complete step 4.
   - If the Schema Changes page appears complete step 5.

4. **License Key Setup**—Provide your license key information if this page appears, then continue.

Note: You will be operating a temporary license until you request, receive, and enter your permanent license. The temporary license is good for 60 days and up to 100 users. For details, see the *NetPoint 7.0 Administration Guide Volume 1*.

- **If You Updated the Schema During COREid Server Installation**—Skip to "Specifying Directory Server and Data Location Details" on page 138.
- **If You Did *Not* Update the Schema During COREid Server Installation**—A Schema Changes page appears and you complete step 5. For additional information, see "Updating the Schema and Attributes Automatically vs. Manually" on page 32.

5. **Schema Changes**—Complete activities described on the Schema Changes page, if this appears, then continue.
6. Complete the procedures in following discussions and see the file important_notes.txt:

   WebPass_install_dir\identity\oblix\lang*langTag*\important_notes.txt

   where *langTag* refers to a specific language, such as en-us (the default).

Specifying Directory Server and Data Location Details

You need to specify details about the directory server where user data and configuration data are stored.

Note: The COREid Data Anywhere directory server option is available for only the *user* data directory server and integration with OctetString Virtual Directory Engine (VDE). *Before* you setup the first COREid Server for use with COREid Data Anywhere, read the chapter on integrating NetPoint with VDE in the *NetPoint Integration Guide* and complete activities as specified.

Typically, details about the *user* data are requested first, then details about configuration data. Information you supplied during the schema update usually appears on setup pages.

When user data and configuration data are stored separately, you repeat the sequence to specify directory server details.

To specify directory server details

1. Specify your *user data* directory server type.

   For example:

   Siemens DirX

   Next, you are asked for the *location* of the user data directory server. If you updated the schema during installation, most details will be filled in already.

2. Specify the user data directory server details based on your installation, then click Next.

   For example:

   - **Host**—The user data directory server DNS hostname
   - **Port Number**—The user data directory server port number
   - **Root DN**—The user data directory server bind DN
   - **Root Password**—Password for the bind DN
   - **Directory Server Security Mode**—Unsecured or SSL-enabled between the user data directory server and COREid Server
   - **Is Oblix data stored in this directory also**?—Yes (default) or No

   Note: If user data is stored separately from configuration data, a similar page appears where you can enter information for the configuration data directory. However, that sequence is *not* repeated here.

   A new page asks you to specify the location of user and configuration data.

3. Enter the configuration bind DN and user data searchbase to be used.

   For example, when the data is stored in the same directory:

   - **Configuration DN**—o=*my-company*,c=*us*
   - **Searchbase**—o=*my-company*,c=*us*

   Note: When user data and configuration data are stored separately, the configuration DN and searchbase must be unique. Also, you will see details about each directory to the right of each field.

4. Click Next and continue with “Specifying Object Class Details” on page 140.

Specifying Object Class Details

The next sequence in the COREid System setup process asks for details about your Person and Group object classes. This discussion is divided into the topics:

- "About NetPoint Object Classes" on page 140 provides an overview, which you may skip if you are already familiar with these concepts.
- "Specifying Person and Group Object Classes" on page 141 provides the procedure to accomplish this task.

About NetPoint Object Classes

In the directory server, NetPoint stores data as objects. Each object is composed of attributes and their values, which are displayed on Profile pages for each application in the NetPoint COREid System. All objects are associated with an object class.

The NetPoint COREid System includes its own object classes, which must be added to your directory server schema. These object classes begin with the prefix "ob" and contain functional information for the COREid System. You may configure additional object classes after you setup the COREid System.

NetPoint requires at least one Person object class and one Group object class, which must be setup before you can log in to COREid applications. For more information, see "About Person and Group Object Classes" on page 65.

Note: To save time and avoid errors, Oblix recommends that you automatically configure both the person and Group object classes during COREid System setup.

Automatic configuration adds attributes to the Person and Group object classes. Specifically, the attributes for default display name, semantic type, and display type are added. Before you can log in to COREid applications, attributes must be assigned to the following semantic types: Full Name, Login, and Password.

You may reconfigure attributes after setup, if needed, to define your own object classes and attributes and to incorporate unique requirements for your enterprise.

Specifying Person and Group Object Classes

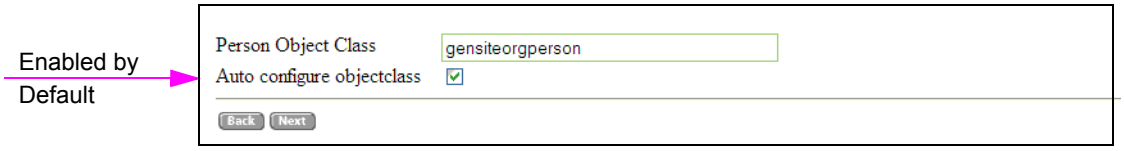
You complete the following procedure to specify Person and Group object class details. If you do not use the recommended Auto configure option, you must do this manually, as described in “Configuring Attributes Manually” on page 147. Only partial pages are shown below to illustrate a completed setup page.

To specify Person and Group object class details

1. Enter your Person object class for the User Manager.

   For example:

   Person Object Class—gensiteorgperson



   As shown above, the Auto configure objectclass feature is enabled by default to help streamline the configuration process. Later during this setup process, you can verify and accept, or change, the automatic configuration. You may disable this feature to manually configure the object class.

   These instructions are based on automatic configuration of both Person and Group object classes.

2. Click Next to complete the Person object class configuration (or disable Auto configure object class, then click Next).

   The Group object class page appears.

3. Enter your Group object class for the Group Manager, then click Next to complete the Group object class configuration.

   For example:

   Group Object Class—GroupofUniqueNames

   The next page that appears asks you to restart your COREid System. The time it takes for the COREid Server to automatically configure object classes may exceed your Web browser’s timeout. If your browser times out waiting for the COREid Server, wait a minute or two and click your browser’s Refresh button to continue.

4. Stop the WebPass Web server instance.

5. Stop, then restart the COREid Server service.

6. Start the WebPass Web server instance.

7. Return to the COREid System setup window and click Next.

What you do after restarting the COREid System depends upon the update method you chose earlier in the setup. For example:

- If you chose to automatically configure the Person or Group object class, continue "Confirming Object Class Changes" on page 142.
- If you disabled automatic configuration of the Person or Group object class, continue with "Configuring Attributes Manually" on page 147.

Confirming Object Class Changes

You are presented with object class changes made automatically during this setup. Just review the changes for the specified object class, then click Yes to accept them. You may click No to launch the Configure Attributes function where you can make any corrections.

The procedure below presumes that you enabled automatic configuration for both the Person and Group object classes.

To confirm object class changes

1. Review the Person object class attribute list, as shown in part below.

Is the following configuration correct for objectclass 'gensiteorgperson'?

Attribute	Display Name	Semantic Type	Display Type
audio	Audio	*none*	Media
businessCategory	Business Category	*none*	Single Line Text
carLicense	Car License	*none*	Single Line Text
cn	Full Name	DN Prefix, Full Name	Single Line Text
departmentNumber	Department Number	*none*	Single Line Text
description	Description	*none*	Multi-Line Text

2. Click Yes to accept the changes (or No to launch the Configure Attributes function).
   - If Yes, continue with step 3.
   - If No, continue with "Configuring Attributes Manually" on page 147.
3. Review the Group object class attribute list, then click Yes to accept the changes (or click No to decline the changes) and continue as follows:
   - If Yes, continue with "Configuring NetPoint Administrators" on page 143.
   - If No, continue with "Configuring Attributes Manually" on page 147.

Configuring NetPoint Administrators

After you configure object classes and attributes, you are asked to identify one or more people as a NetPoint Administrator.

Note: Be sure to select a person with the appropriate Person object class as the NetPoint Administrator.

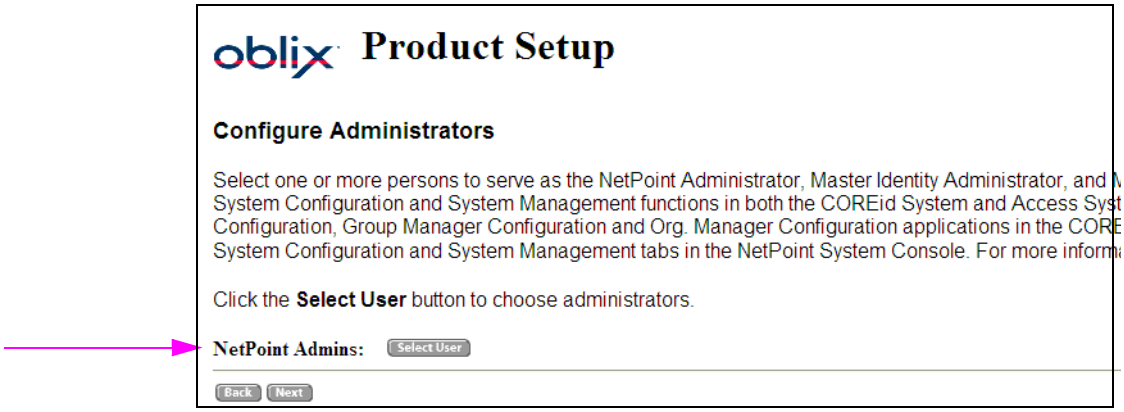
The NetPoint Administrator has access to all COREid and Access System configuration and management functions. This includes the rights to assign other administrators and perform all tasks other NetPoint administrators can perform. For example, after the set up process a NetPoint Administrator can assign one or more:

- Master Identity Administrators who have rights to configure the COREid System and assign individuals to be Delegated Identity Administrators.
- Master Access Administrators who have rights to configure the NetPoint Access System, including WebGates, Access Servers, authentication parameters, and the initial set of policy domains. This includes the rights to assign individuals to the role of Delegated Access Administrators.

  For more information, see the *NetPoint 7.0 Administration Guide Volume 1* and *2*.

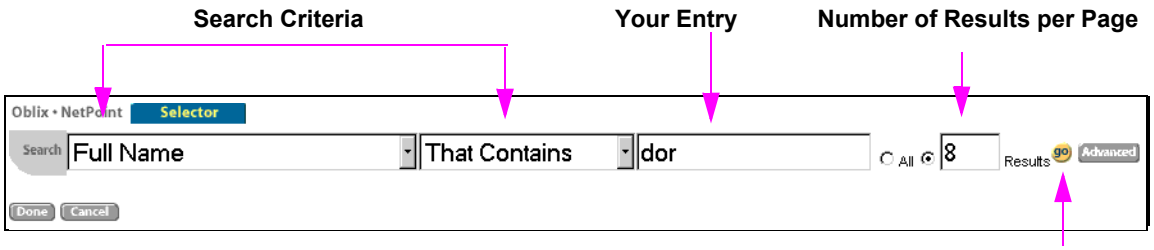
To assign NetPoint Administrators

1. On the Configure Administrators setup page, click the Select User button beside NetPoint Admins.

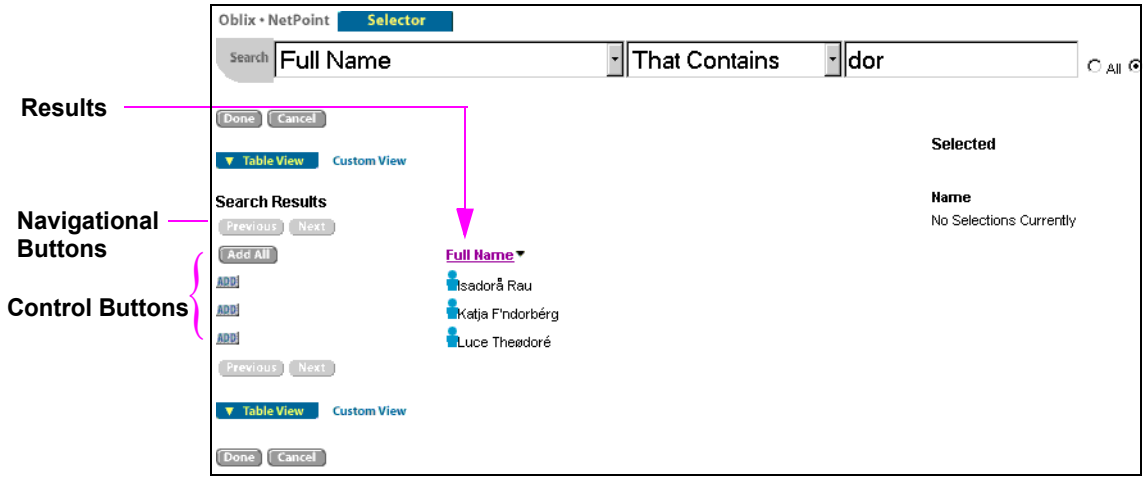


   The Selector page appears providing two search criteria lists, an empty field where you enter at least three characters on which to search, and buttons to display results.

2. Locate the person or persons you want by choosing search criteria from the two drop-down lists on the top left, then entering at least three characters in the empty field, and selecting the Go button, as shown next.



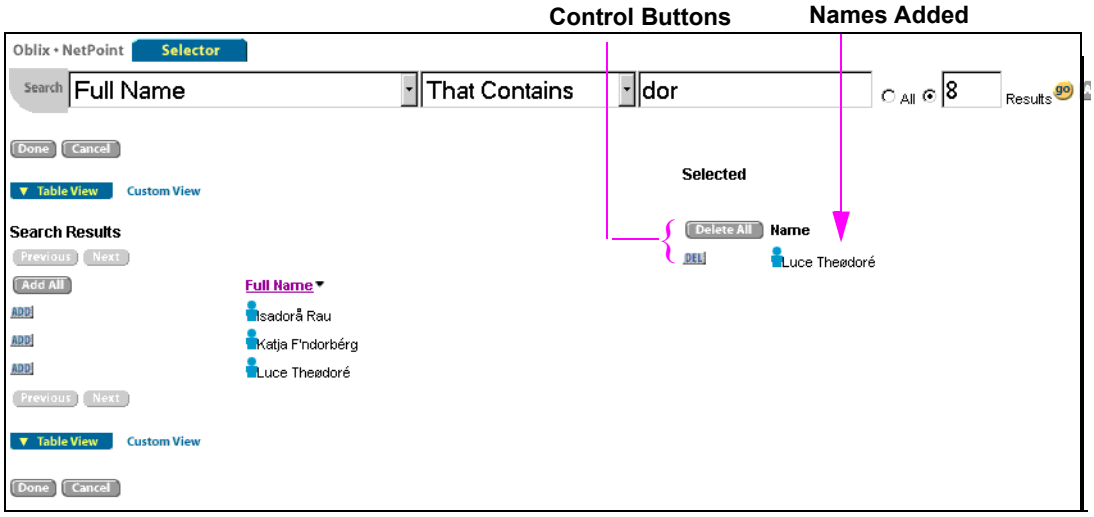
Your search results will appear beneath the criteria on the left side of the page, as shown next. By default, 8 results appear as designated in the field beside the Go button. You can use the Previous and Next buttons to navigate through the results, as shown next.



Included on the left are control buttons to add everyone in the list (Add all), or add individuals (by choosing the Add button beside the desired name). When you choose one of these buttons, the name or names you add will appear on the right side of the window under “Selected”.

3. Click the Add button beside the name of the person you want to assign as a NetPoint Administrator.

4. Confirm that the name you added now appears on both the right side of the window under “Selected”, as shown next, and on the left side.



You may continue to add names as you did in step 3. Also, you can remove names from the "Selected" list using the DEL button beside the name or using the Delete All button.

5. Click Done to return to the original Configure Administrators page and confirm that the person or persons you wanted to add appear beside NetPoint Admins.

6. Click Next.

   The Securing Data Directories page appears explaining things to do following COREid System setup.

Completing COREid System Setup

The Securing Data Directories page lists the NetPoint directories that you should protect to maintain the security of the NetPoint COREid System and to both:

- Restrict access both from browsers and network users who access the directory through the file system. See the documentation for your Web server and operating system if you need instructions on how to protect directories.
- Protect the NetPoint COREid System within a NetPoint policy domain. See the *NetPoint 7.0 Administration Guide Volume 2* for more information.

To complete the COREid System setup

1. Click Done to complete COREid System setup.

   The login page for the COREid System appears. Your NetPoint COREid System setup and minimum configuration are complete.

   A default directory profile for this COREid Server is available in the COREid System Console.

2. Perform any of the following tasks.

   a) Enter the appropriate format for UTCTime and GeneralizedTime syntaxes for Siemens DirX, as described in "Mapping Attributes for Siemens DirX" on page 151.

   b) Set up more than one COREid Server instance, as described under "Setting Up Other COREid Server Instances" on page 154.

   c) Start to install the Oblix Management Agent for MIIS, if desired, as described in the *NetPoint 7.0 Integration Guide*.

   d) Start to install the Access System as described under "Installing the Access Manager" on page 165.

   e) Log in to the COREid System as a NetPoint Administrator and complete any of the following tasks, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

      For example:

      - View the directory profile for this COREid Server by selecting COREid System Console > System Configuration > Configure Directory Options > *default-link_to_this_profile*
      - Set up panels in the User Manager, Group Manager, Organization Manager.
      - Set up object-based searchbases in the User Manager.
      - Set up access controls in the User Manager, Group Manager, or Organization. Manager.
      - Create workflow definitions.
      - Configure options such as the mail server and session settings.

Configuring Attributes Manually

The attribute configuration function helps you either manually complete the minimum configuration necessary to make the COREid System functional or fine-tune attributes that were configured automatically during setup. You can use the procedures here to modify attributes at any time after setup.

The Configure Attributes page appears in the following situations:

- You disabled Auto configure object class during COREid System setup, and restart your COREid Server and Web server.
- You enabled Auto configure object classes during COREid System setup, restart your COREid Server and Web server, then click No when asked if the configuration is correct.
- You navigated to the Modify Attributes page after setup by selecting COREid System Console > Common Configuration > Configure Object Class > *object_class_link* > Modify Attributes.

Novell Directory Server Considerations

Novell Directory Server (NDS) maps attribute and object class names from the native directory server to the LDAP layer of NDS. Some attributes or object classes will have multiple mappings (aliases) in the LDAP layer. For example, the native NDS object class is Group, while the LDAP layer of NDS maps two aliases called GroupofNames and GroupofUniqueNames.

To ensure that NetPoint and the NDS work correctly

1. Confirm that the object class or attribute name you provide during configuration is the one that occurs ahead of the other mappings for the same object class or attribute.
2. Check the mapping order through consoleOne.

Siemens DirX Considerations

NetPoint currently does *not* support attributes with UTCTime or GeneralizedTime syntax. As a result, these must be mapped as CaseIgnoreStrings in the COREid System. You can complete this mapping either during COREid System setup, as described in Configuring or Refining Attributes, next, or after setup as described in “Mapping Attributes for Siemens DirX” on page 151.

Configuring or Refining Attributes

Use these instructions to manually setup Person and Group object classes.

Note: If you are mapping Siemens DirX attributes with the UTCTime or GeneralizedTime syntax, see "Mapping Attributes for Siemens DirX" on page 151 for additional information.

To define the minimum Person object class attribute set

1. On the Configure Attributes page, Attribute list, select or enter the following Person object class attribute details:

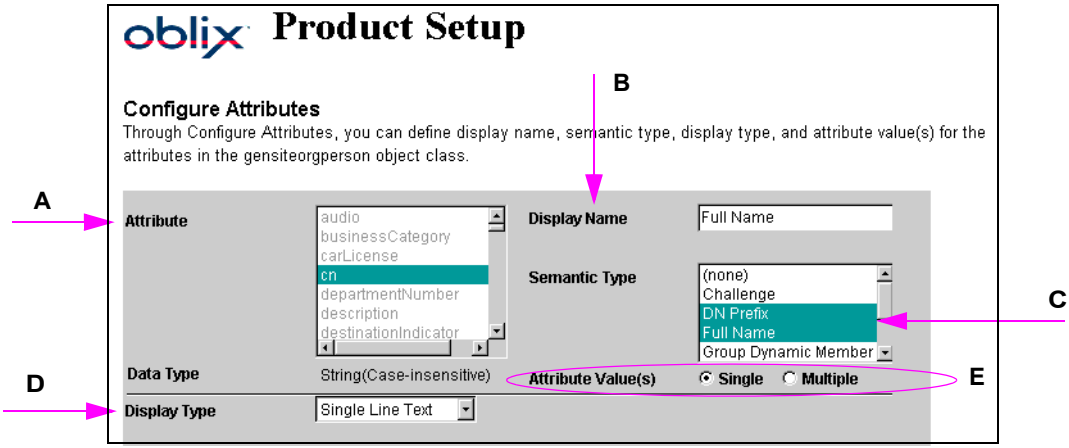
   a) **Attribute**—The class attribute for your Person object class; often cn.

   b) **Display Name**—Name or Full Name

   c) **Semantic Type**—DN Prefix and Full Name

   d) **Display Type**—Single Line Text

   e) **Attribute Value(s)**—Single

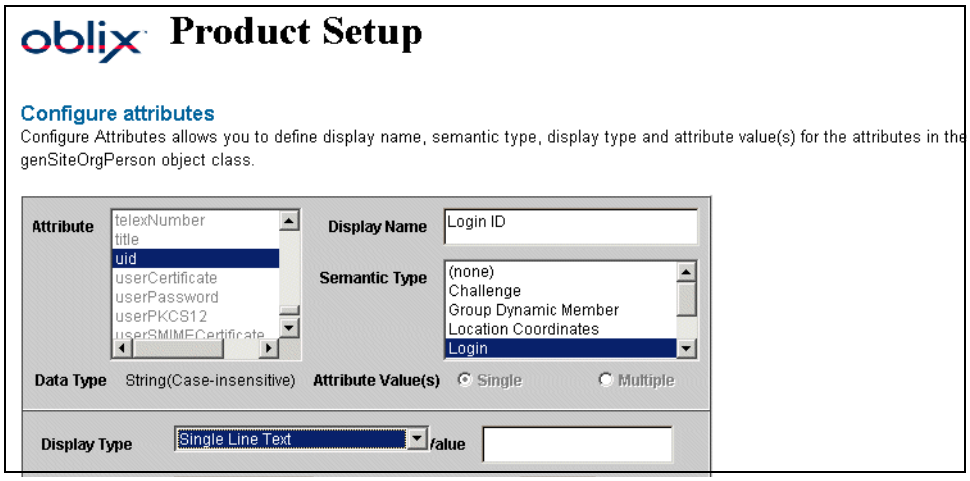


2. Click Save, then click OK to close the confirmation message.

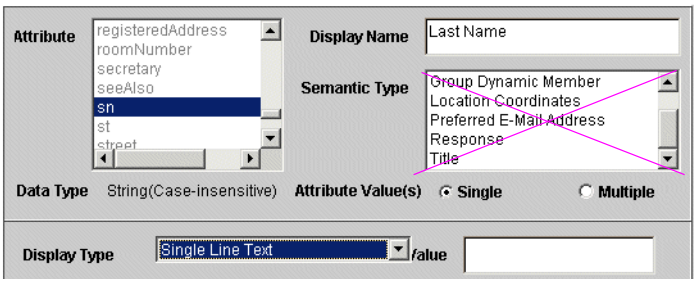
3. In the Attribute List, select or enter the following details to define the login ID attribute:

   - **Attribute**—The attribute that defines the login ID of your users; often the uid attribute.
   - **Display Name**—Such as Login ID
   - **Semantic Type**—Login
   - **Display Type**—Single Line Text

- **Attribute Value(s)**—Single



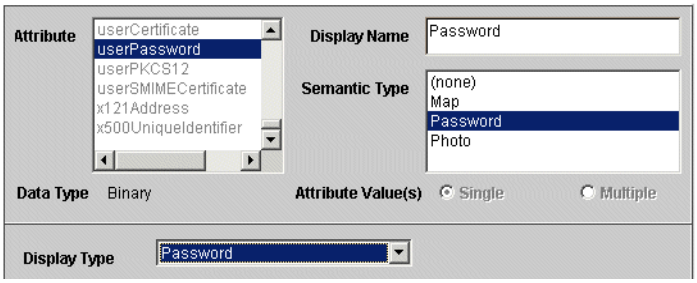
4. Click Save, then click OK to close the confirmation message.
5. In the Attribute List, select or enter the following details to define the surname attribute:
   - **Attribute**—The attribute that defines the surname of your users; often sn.
   - **Display Name**—(such as Last Name)
   - **Display Type**—Single Line Text
   - **Attribute Value**—Single
   - Do *not* specify a Semantic Type



Do not specify a Semantic Type

6. Click Save, the click OK to close the confirmation message.
7. In the Attribute List, select or enter the following details to define the user password attribute:
   - **Attribute**—The attribute that defines the user password; often the password or userPassword attribute.

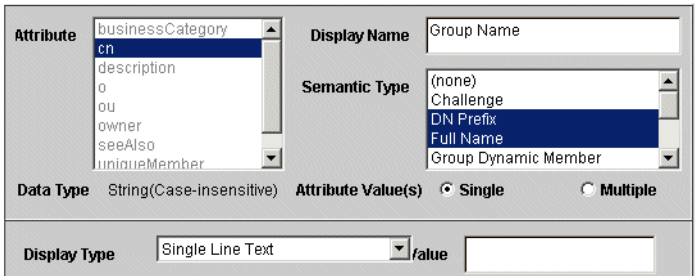
- **Display Name**—Such as Password
- **Semantic Type**—Password
- **Display Type**—Password
- **Attribute Value(s)**—Single



8. Click Save, then click OK to close the confirmation message.
9. Click Next to proceed to the page where you configure the Group object class.

To specify the minimum set of Group object class attributes

1. In the Attribute List, select or enter the following details:
   - **Attribute**—The attribute that defines the Group name; often the cn attribute.
   - **Display Name**—Such as Group Name
   - **Semantic Type**—DN Prefix and Full Name
   - **Display Type**—Single Line Text
   - **Attribute Value(s)**—Single



2. Click Save, then click OK.
3. Continue with the following, as needed:
   - "Setting Up Other COREid Server Instances" on page 154

- “Installing the Access Manager” on page 165
- Configuring the Access Server SDK for the COREid System, as described in the *NetPoint 7.0 Administration Guide Volume 1*

  Certain functions in the COREid System require the Access Server SDK. By default, the Access Server SDK is installed in a subdirectory under *COREid_install_dir*\identity. Following COREid System set up, you must manually configure the Access Server SDK for the COREid System to enable these functions.
- Install the Oblix Management Agent for MIIS, if desired, as described in the *NetPoint 7.0 Integration Guide*.

Mapping Attributes for Siemens DirX

As mentioned earlier, NetPoint currently does not support attributes with UTCTime or GeneralizedTime syntax. As a result, these must be mapped as CaseIgnoreStrings in the COREid System. You can complete this mapping either during COREid System setup, as described in “Configuring Attributes Manually” on page 147, or after setup as described below. In either case, see the procedure below for specific information.

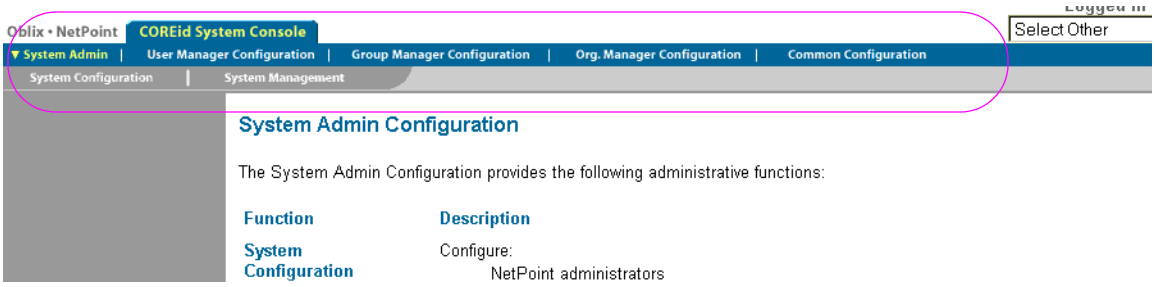
To navigate to the Modify Attributes page after setup

1. Navigate to the COREid System Console from your browser by specifying the following URL.

   For example:

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

   where *hostname* refers to machine that hosts the WebPass Web server; *port* refers to the HTTP port number of the WebPass Web server instance; /identity/oblix connects to the COREid System Console.
2. Select COREid System Console to display the main page, a portion of which is shown below.



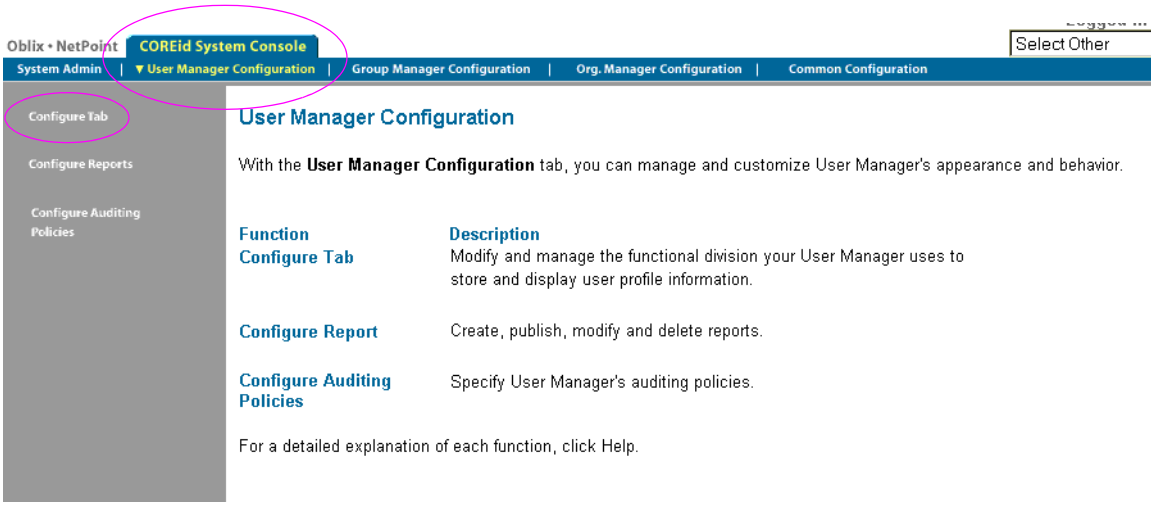
The tabs across the top of the page are highlighted in the figure above and may be selected to display corresponding functions.

3. From the tabs across the top of the page, click one of the following: User Manager Configuration, Group Manager Configuration, or Organization Manager Configuration.

   For example:

   User Manager Configuration

   The specified Configuration page appears, as shown in the example below. The tabs across the top of the page highlight the current selection. The side navigation bar contains the functions you can select. The main body of the page provides information on each function.



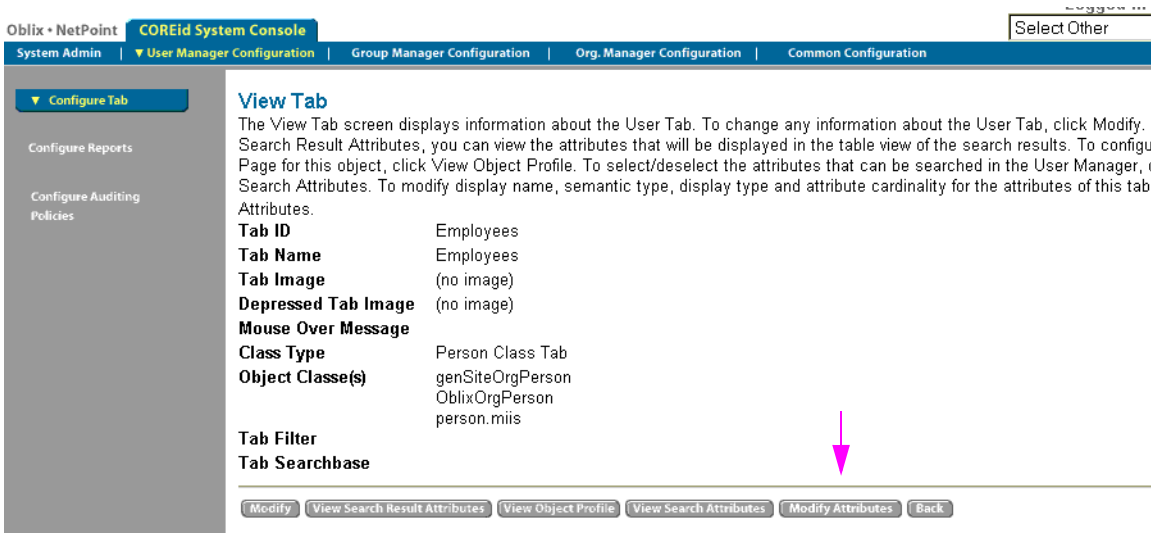
4. From the side navigation bar, select Configure Tab.

   The page appears. The structural object class for that tab is displayed as a link under the heading “Existing Tabs”. The link you see depends on the application. For example, the User Manager Configuration provides a link to Employees; in Group Manager Configuration you see a link to Groups; in Organization Manager Configuration you see a link to Locations.

5. From the Configure Tab page, click a link under the Existing Tabs label to display the View Tab page.

   For example:

   Employees



6. From the View Tab page, click the Modify Attributes button (bottom, right).

   For example:

   Modify Attributes

   The Modify Attributes page appears where you can modify the semantic type, display type, and attribute value(s) for attributes under the tab.

To map attributes for Siemens DirX

1. Use the procedure "To navigate to the Modify Attributes page after setup" on page 151, if needed (or see "Configuring or Refining Attributes" on page 148 if you are doing this during setup).
2. On either the Modify Attributes or Configure Attributes page, select an attribute whose syntax is either UTCTime or GeneralizedTime and change the settings as indicated below:

   a) **Attribute**—Any class attribute with either UTCTime or GeneralizedTime syntax

   b) **Display Name**—Can be anything

   c) **Semantic Type**—None

   d) **Data Type**—String (Case Insensitive)

   e) **Attribute Value(s)**—Can be either Single or Multiple

f) **Display Type**—Single Line Text

Note: With a Data Type of "String" and Display Type of "Single Line Text", NetPoint treats the attribute as a string and displays the value as a single line. For modification, you need to enter your value using appropriate directory syntax. If you attempt to save with an incorrect format, an error occurs.

---

3. Save the changes.
4. Repeat step 2 for each attribute whose syntax is either UTCTime or GeneralizedTime.
5. Click Done when you finish all changes.

   For more information on functional areas of the screen and configuring attributes, see the *NetPoint 7.0 Administration Guide Volume 1*.

Setting Up Other COREid Server Instances

Setting up additional COREid Server instances involves two procedures, as described below.

Task overview: Setting up other COREid Servers

1. Prepare additional COREid Servers, as described in "Preparing Additional COREid Servers" on page 154.
2. Set up the new COREid Server, as described in "Preparing to Set Up Additional COREid Servers" on page 154.

Preparing Additional COREid Servers

Be sure you have installed the first COREid Server and WebPass, then setup the first COREid Server, as described in "Section II: COREid System Installation and Setup" on page 97.

Table 27 lists the procedures that should be completed before you continue.

Table 27 Preparing to Set Up Additional COREid Servers

Checklist	Setting Up Additional COREid Server Prerequisites
	Install additional COREid Servers, as described in "Installing the COREid Server" on page 105.
	Stop all COREid Server services, if you haven't already.
	Start the new COREid Server service only and continue with "Preparing to Set Up Additional COREid Servers" on page 154.

Setting Up a New Additional COREid Server

Setting up additional COREid Servers involves only a subset of the original setup process.

To setup the COREid Server and associate it with a WebPass

1. Navigate to the COREid System Console, as usual.

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

   The WebPass will attempt to connect to the original COREid Server. When it is unavailable, the WebPass will connect to the new COREid Server and launch the setup page.

2. Click Setup and follow the instructions to set up the COREid Server, and see "Setting up the COREid System" on page 136 for more information.

3. Restart the new COREid Server service when instructed to do so during setup.

4. Restart other COREid Server services.

5. Repeat as needed for each additional COREid Server.

Section III: Access System Installation and Setup

6 Installing the Access Manager

After you install the COREid System, you can begin to install the Access System, which includes three components: the Access Manager, the Access Server, and the WebGate. The Access Manager is the first component that must be installed, as topics in this chapter describe:

Upgrading to NetPoint 7.0 is described in the *NetPoint 7.0 Upgrade Guide*. For an overview of NetPoint components, see the Introduction to *NetPoint 7.0 Guide*.

About Access Manager Installation and Setup

The NetPoint Access Manager provides the login interface for the Access System. Master Access Administrators and Delegated Access Administrators use the Access Manager to define resources to be protected and to group resources into policy domains.

The Access Manager installation includes the Access System Console. Access Manager installation and setup are divided into the following procedures.

Task overview: Installing and setting up the Access Manager

1. Install the Access Manager, as described in "Installing the Access Manager" on page 165, which is divided into the following procedures:
2. Complete the following procedures, if needed, to prepare for setup:
   - "Manually Configuring Your Web Server" on page 173
   - "Verifying Access Manager Permissions on IIS" on page 175
3. Set up the Access Manager, as described in "Setting Up the Access Manager" on page 175.
4. Confirm the setup, as described in "Confirming Access Manager Setup" on page 184.

Again, you must complete all procedures for a successful installation. Information is saved at certain points during the installation process. If you cancel the installation after being informed that the Access Manager is being installed, you must uninstall the component, as described in "Upgrading from a Previous Version of NetPoint" on page 37.

Installing the Access Manager is similar to installing the COREid Server. In both cases, you must specify directory server details. During Access Manager installation, you will identify where to store NetPoint policy data. A default Access Manager directory profile is created and becomes available after setup.

You also need to update your Web server configuration for the Access Manager, as you did for the WebPass. Rather than starting and stopping an Access Manager service, you will start and stop the Access Manager Web server.

Separate Web server-specific installation packages are provided for the Access Manager in platform-specific directories. The installation process is similar regardless of the installation mode you choose and your operating system. Any caveats are identified and may be skipped when they do not apply to your environment.

After installation, you must complete the Access Manager setup process before installing other Access System components. Again, your information is saved as you progress from one page to the next during setup. You may return to previous pages at any time and you may leave the setup process and restart it at any time. If you restart the setup process, you will continue with the question that follows your last saved entry.

For more information, see “Access Manager Installation Considerations” on page 162.

About the Access Manager Installation Directory

You may install the Access Manager in the default directory or in another directory that is at the same directory level as a WebPass. For example, if you specified C:\NetPoint\WebComponent as the installation directory for the WebPass, you must also specify this as the Access Manager installation directory.

When you change the path name, you may include any characters that are acceptable to your operating system. For example, you may include spaces on Windows systems but not on Unix systems. During Access Manager installation, \access is appended to the installation directory path you specified. The path becomes:

Default on Windows—\Program Files\NetPoint\WebComponent\access
Default on Unix—/opt/netpoint/webcomponent/access
In This Guide—*AccessManager_install_dir*\access

About Installing Multiple Access Managers

Oblix recommends you install multiple Access Managers for fault tolerance. To install multiple Access Managers, you simply perform the installation and setup described in this chapter for each new Access Manager instance.

An Access Manager installed with an IIS Web server depends on the Registry to obtain the *AccessManager_install_dir*. To avoid a conflict in the Registry when you install two Access Managers on a single machine, one with an IIS Web server and the other with a Sun Web server, you must install the Access Managers as outlined in the following procedure.

To avoid a conflict with IIS and Sun Web server instances

1. Install the Access Manager with the Sun Web server first.
2. Install the Access Manager with the IIS Web server second.

Access Manager Installation Considerations

Oblix recommends that you do not put a firewall between the Access Manager and the directory server because no “health check” is performed. After a period of inactivity, the firewall may drop the Access Manager connection without warning. To avoid such problems, either ensure the Access Manager and directory server are on the same side of the fire wall or disable the firewall connection timeout between the Access Manager and directory server, if possible. However, not all firewalls support this.

The Access Manager must be installed on the same Web server instance as a WebPass, at the same directory level as a WebPass.

If you are installing the Access Manager with a Language Pack on a Unix system, you must ensure that the Language Pack has execute permissions before launching the main installer. For example:

```
chmod +x “NetPoint7_0_FR_sparc-s2_LP_COREid_System”
```

The account that performs NetPoint installation must have administration privileges.

Directory Server Considerations

SSL-secured communication with the directory server is not supported when the Access Manager is installed on Solaris with a Sun (formerly Netscape) Web server.

A default directory profile will be created for this Access Manager based on the information you supply. This profile will be available in NetPoint after you setup the Access Manager.

Separate Storage of User Data and Configuration Data—As discussed earlier, NetPoint 7.0 supports storing user data separately from configuration and policy data. With a Siemens DirX or Sun directory server, data may be stored either together on the same directory server or on different directory servers of the same type.

NetPoint 7.0 also supports storing user data on a separate directory server *type* from configuration and policy data. For example, you may want to store user data in Active Directory and NetPoint configuration and policy data on ADAM.

In either case, the user data searchbase, configuration DN, and NetPoint policy base must be unique and you must provide details about only the main user data directory and searchbase during Access Manager installation and setup. For more information, see “Data Storage Requirements” on page 59.

Active Directory—When you are installing NetPoint with a Microsoft Active Directory forest, be sure to read considerations in “Data Storage Requirements” on page 59 and “Installing NetPoint with Active Directory” on page 394 before proceeding.

If you specify Active Directory on Windows Server 2003 during Access Manager installation, a new page appears asking if dynamic auxiliary classes are to be supported. If you are using ADSI, you need to set the IIS Web server Anonymous User Login Account to a Domain User after installation and before setting up the Access Manager.

Active Directory Application Mode (ADAM)—When you are installing NetPoint with ADAM, be sure to read “Installing NetPoint with ADAM” on page 407 before proceeding. **COREid Data Anywhere**—Available only for *user data* when NetPoint is integrated with OctetString Virtual Directory Engine (VDE). The LDAP directory branches containing NetPoint configuration and policy data must reside on one or more directory servers other than the one hosting VDE or user data. NetPoint applications only recognize configuration and policy information that resides outside the VDE virtual directory. See the *NetPoint Integration Guide*.

Network Account Rights for Volume Root

The NETWORK Account must have Modify rights at the volume root.

Web Server Considerations

There are several considerations depending upon the Web server you are using for this installation.

Apache—NetPoint supports Apache with or without SSL enabled. For SSL-enabled communication, NetPoint supports Apache with mod_ssl only, not Apache-SSL. mod_ssl is a derivative of, and alternative to, Apache-SSL.

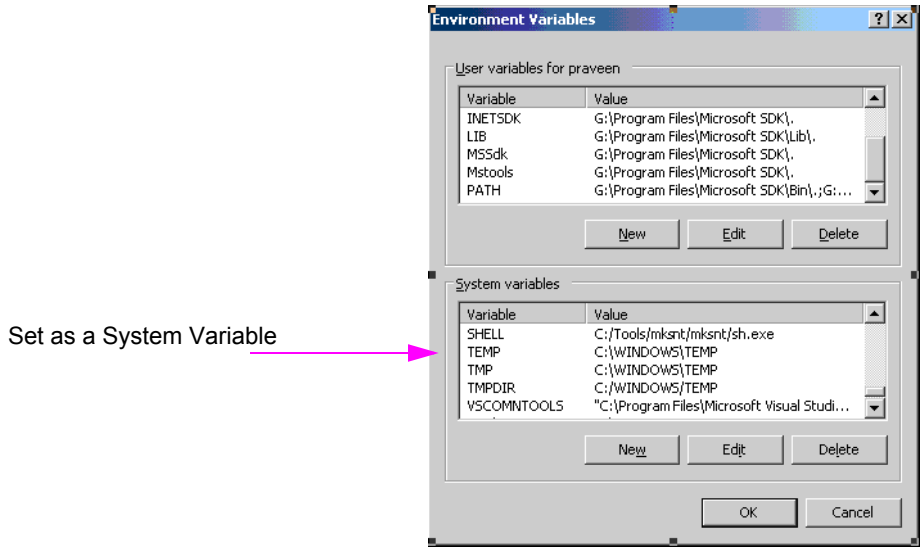
IIS—The Access Manager installer cannot update multiple Web servers instances. If you have multiple IIS Web server instances installed, be sure to install a separate Access Manager on each Web server instance.

When installing the Access Manager on Windows 2000 with IIS, ensure that the group named Everyone has full access to the \temp directory and the drive (for example, C or D) to which the \temp directory belongs.

The TEMP variable needs to be set to point to a valid directory, either for the entire system or for the IIS user. Oblix recommends setting the TEMP variable for the entire system, as shown in Figure 7.

Sun—formerly NetScape—NetPoint does not support SSL-enabled communication between the directory server and Access Manager installations on Solaris platforms that include a Sun Web server.

Figure 7 The TEMP Variable Set for the System



Access Manager Prerequisites Checklist

Before you begin installing the WebGate, confirm that you have completed the tasks in Table 28. Failure to complete all prerequisites may adversely affect your NetPoint installation.

Table 28 Access Manager Prerequisites Checklist

Checklist	Access Manager Prerequisites
	Install a COREid Server, as described in “Installing the COREid Server” on page 105.
	• Install a WebPass, as described in “Installing WebPass” on page 121 and: Ensure that the WebPass is installed on the same Web server instance and at the same directory level as you will install the Access Manager. • Ensure that the Webpass has been configured to work with a particular COREid Server.
	Complete COREid System setup and confirm that your COREid System is working, as described in “Setting Up the COREid System” on page 133.
	Move Language Pack installers into the same directory as the Access Manager installer, if needed, and ensure that the Language Pack installer on Unix systems has execute permissions, as described in “Access Manager Installation Considerations” on page 162.

Installing the Access Manager

You must install your Access Manager in the same directory as your WebPass. If you specify a directory that does not include a WebPass, you will be asked if you want to install a WebPass or specify a different directory. If you choose to install a WebPass, this may launch automatically. With Siemens DirX, automatically launching with WebPass installer may *not* occur.

Refer to your completed installation preparation worksheets as you install the Access Manager. The installation task has been divided into the following procedures:

- "Starting the Installation" on page 165
- "Defining a Directory Server Type and Policy Data Location" on page 166
- "Specifying a Transport Security Mode" on page 170
- "Updating Your Access Manager Web Server Configuration" on page 171
- "Finishing the Access Manager Installation" on page 172

Starting the Installation

Be sure to choose the appropriate installation package for your Web server.

To start the installation

1. Log in as a user with administrator privileges.
2. Locate and launch the installation for your preferred platform, installation mode, and Web server.

   For example:

   - **GUI Mode**
     Windows—NetPoint7_0_Win32_*API*_Access_Manager.exe
     Solaris—./NetPoint7_0_sparc-s2_*API*_Access_Manager -gui
   - **Console Mode**
     Solaris—./NetPoint7_0_sparc-s2_*API*_Access_Manager
     Windows Command Window—
     NetPoint7_0_Win32_*API*_Access_Manager.exe -console

   The Welcome screen appears.
3. Dismiss the Welcome screen by clicking Next.

4. Accept the terms of the license agreement, then click Next.

Note: You will be operating a temporary license until you request, receive, and enter your permanent license. The temporary license is good for 60 days and up to 100 users. For details, see the *NetPoint 7.0 Administration Guide Volume 2*.

---

5. Respond to the next question based upon your platform. For example:
   - **Windows**—If you are logged in with administrator rights, click Next (otherwise click Cancel, log in as a user with administrator privileges, then restart the installation).
   - **Unix**—Specify a dedicated username and group that the Web server will use, then click Next. Typically, the defaults are nobody.

     For HP-UX, the defaults are WWW (username) and others (group).

   You are asked to specify the installation directory for the Access Manager.
6. Choose the installation destination, then click Next.

   For example:

   NetPoint_70\WebComponent
7. **Language Pack**—Choose a Default Locale and any other Locales to install, if this screen appears, then click Next.

   A summary identifies the installation directory and required disk space and asks you to make a note of this information for future reference.
8. Write the installation directory name, if needed, then click Next.

   You are notified that the Access Manager is being installed, which may take several seconds. On Windows systems, you are informed that the Microsoft Managed Interfaces are being configured. Information is saved and you cannot return to previous screens to restate information.

   The installation process is not complete. You are asked about the location for NetPoint policy data.

Defining a Directory Server Type and Policy Data Location

NetPoint policy data includes the rules that govern access to resources. You are asked to specify where NetPoint policy data will be stored and if you want to add the Oblix schema now or later. If your policy data is stored on the:

- **Same Directory Server**—Respond with No. When NetPoint policy data will be stored in the *same* directory server as Oblix data or user data, an update is *not* needed because the Oblix schema was added during the COREid Server installation.

- **Separate Directory Server**—When NetPoint policy data will be stored in a *separate* directory server than either the Oblix data or user data, the Oblix schema *must* be added. You can direct this addition to occur either:
  - **Automatically**—Respond with Yes to automatically update the schema now.
  - **Manually**—Respond with No to update the schema manually later. For additional information, see "Updating the Schema and Attributes Automatically vs. Manually" on page 32.

To identify the location of policy data

1. Select your directory server type, then click Next.

   For example:

   Siemens DirX

2. Respond to the question about where policy data will be stored:
   - **No**—Answer No if policy data will be stored with user and Oblix data *or* if you want to manually update the schema later.
   - **Yes**—Answer Yes when policy data will be stored separately *and* you want to automatically update the schema now.

   This information will be saved and you will not be allowed to return restate it.

3. Click Next and skip to the appropriate procedure for your environment:
   - "Continuing on Solaris Without Updating the Schema" on page 167
   - "Continuing on Windows Without Updating the Schema" on page 168
   - "Storing Policy Data Separately and Updating the Schema" on page 169

Continuing on Solaris Without Updating the Schema

During installation on a Solaris system, when policy data is stored with other NetPoint data you will be asked about the communication method for the existing directory server.

To specify directory server communication details

1. Respond to the question about securing directory server communication with SSL, then click Next.

   Note: SSL is not supported on Access Managers installed on Solaris with Sun Web servers.

2. **SSL**—Specify the path to the certificate, then click Next.

3. Continue with “Specifying a Transport Security Mode” on page 170.

Continuing on Windows Without Updating the Schema

During installation on a Windows system, when policy data is stored with other NetPoint data you will be asked about communication with the directory server.

Note: When this sequence concludes, you will be asked for transport security details. When this occurs, skip to “Specifying a Transport Security Mode” on page 170.

To specify details about the existing directory server

1. Click Yes if you are using Active Directory with ADSI (or No if you are not), then click Next.

   For example:

   No

   Next you are asked about the communication between the directory server and the Access Manager for each of the three types of data: user, configuration, and policy data.

2. Check the box beside each type of data for which SSL communication with the directory server is needed, then click Next.

   For example:

   Directory Server ... user data is in SSL
   Directory Server ... Oblix data is in SSL
   Directory Server ... Policy data is in SSL

3. **SSL**—Specify the path to each certificate, then click Next.

4. Continue with “Specifying a Transport Security Mode” on page 170.

Storing Policy Data Separately and Updating the Schema

When your policy data is stored separately you need to identify the type of directory server and other relevant details. For additional information, see “Data Storage Requirements” on page 59.

To specify directory server type and configuration details

1. Specify your directory server type for policy data stored separately, then click Next.

   For example:

   Siemens DirX

2. Specify the following directory server configuration information, then click Next. For example:

   - **Host name**—The DNS hostname of the policy data directory server machine
   - **Port number**—The port on which the policy data directory server listens (for SSL connections, provide the encrypted port)
   - **Bind DN**—The DN for the policy data directory server

     Note: The distinguished name you enter as the bind DN must have full permissions for the policy data branch of the directory information tree (DIT). NetPoint will access the directory server as this account. Examples are provided in Table 29. Your configuration may be different.

Table 29 Sample Bind DNs for Supported Directory Servers

Directory Server	Bind DN
Siemens DirX	cn=*admin*,o=*my-company*
Sun Directory Server 5.x	cn=*administrator* **Note**: Oblix recommends that you do not use cn=Directory Manager. For details, see “Directory Server Requirements” on page 52.

   - **Password**—The password for the user data directory server bind DN
   - **Update through SSL connection**? (Yes or No)—If you are installing on Solaris with a Sun Web server, SSL is not supported and communication must be Open.

   You complete step 3 when you indicated SSL.

3. **SSL only**—Enter the certificate path, then click Next.

   If there is an error in the information you provide, the schema cannot be updated. You can either restate the configuration information during installation or manually update the schema later using the file: *AccessManager_install_dir*\access\oblix\tools\ldap_tools\ds_conf_update. See also, "Updating the Schema and Attributes Automatically vs. Manually" on page 32.

   Next, you are asked about transport security.

Specifying a Transport Security Mode

You must specify a transport security mode for the Access Manager and its WebPass. For more information, see "Transport Security Guidelines" on page 46.

To specify a transport security mode

1. Specify the transport security mode this Access Manager will use to communicate with the rest of the Access System.
2. Click Next and perform the following operations according to the transport security mode you chose. For example:
   - **Open**—Skip to "Updating Your Access Manager Web Server Configuration" on page 171.
   - **Simple**—Specify and confirm the Access System Pass Phrase, click Next, then continue with "Updating Your Access Manager Web Server Configuration" on page 171.
   - **Certificate**—Specify and confirm the certificate password (PEM phrase), click Next, and continue with step 3.
3. **Certificate**—Indicate if you are requesting or installing a certificate, complete the sequence, then continue with "Updating Your Access Manager Web Server Configuration" on page 171.

   You cannot setup the Access Manager until the certificates are copied to the *AccessManager_install_dir*\access\oblix\config directory, and the Access Manager Web server is restarted. See the *NetPoint 7.0 Administration Guide Volume 1* for more information.

   You are ready to update the Access Manager Web server configuration.

Updating Your Access Manager Web Server Configuration

Your Web server must be configured to work with the Access Manager. You can direct this Web server configuration update to occur either automatically or manually.

Note: Oblix recommends automatically updating your Web server configuration. However, instructions for manual configuration are also provided.

To automatically update your Web server configuration

1. Click Yes to automatically update your Web server, then click Next.
   - **Most Web Servers—**Specify the absolute path of the directory containing the Web server configuration file, then click Next.
   - **IIS Web Servers—**The process begins immediately and may take more than a minute.

   A screen announces that the Web server configuration has been updated.
2. **Sun Web Servers**—Apply the changes in the Web server Administration console *before* you continue.
3. Stop the Access Manager Web server instance, stop and restart the COREid Server service, then start the Access Manager Web server instance.
4. Click Next to dismiss the announcement and continue with "Finishing the Access Manager Installation" on page 172.

   ReadMe information appears.

To manually update your Web server configuration

1. Click No when asked if you want to proceed with the automatic update, then click Next.

   A new window opens to assist you in manually setting up your Web server for NetPoint.
2. Return to the Access Manager installation and click Next.
3. Refer to "Manually Configuring Your Web Server" on page 173 after you finish the installation and before you setup the Access Manager.

Finishing the Access Manager Installation

The ReadMe information provides details about documentation and contacting Oblix.

To finish the Access Manager installation

1. Review the ReadMe information, then click Next.

   You are informed that the Access Manager has been successfully installed.

2. Click Finish to close the wizard.

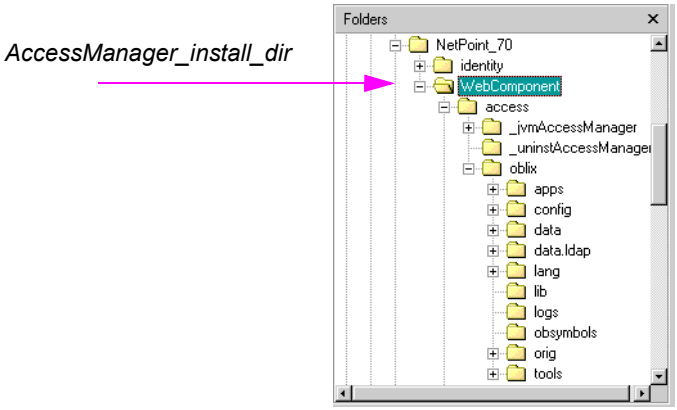
3. Continue with the following procedures, as needed:

   - "Manually Configuring Your Web Server" on page 173 if you did *not* do this automatically during installation
   - Checking installed files, as shown in "Installed Files" on page 173
   - "Verifying Access Manager Permissions on IIS" on page 175
   - "Setting Up the Access Manager" on page 175

Installed Files

The subdirectories in Figure 8 were created and stored under the directory you specified as a destination during Access Manager installation. *AccessManager_install_dir* is the installation directory you specified.

Figure 8 *AccessManager_install_dir*\access



Manually Configuring Your Web Server

During Access Manager installation you are asked if you want to automatically update your Web server installation. If you selected No, you must do this manually before you set up the Access Manager.

Note: If the manual configuration process was launched during Access Manager installation, you can skip step 1 in the following procedure.

To configure your Web server for the Access Manager

1. Launch your Web browser, and open the following file, if needed:

   AccessManager_install_dir\access\oblix\lang*langTag*\docs\config.htm

   where *AccessManager_install_dir* is the directory where you installed the Access Manager.

2. Select the appropriate supported Web server interface configuration protocol from the table on the screen.

Supported Server OS	Web Server					
	Microsoft IIS	ISA Server	Netscape Servers	Apache 1.3 and Apache1.3 -based Servers		
				Plain Apache	Apache with mod_ssl	IBM HTTP Servers
Windows Server 2003	ISAPI	ISAPI	NSAPI	-	-	-
Windows 2000	ISAPI	ISAPI	NSAPI	-	-	IHS-APACHE API
Windows NT	ISAPI	-	NSAPI	APACHE API	APACHE API	IHS-APACHE API
Sun Solaris	-	-	NSAPI	APACHE API	APACHE EAPI	IHS-APACHE API
AIX	-	-	NSAPI	APACHE API	APACHE EAPI	IHS-APACHE API
HP-UX	-	-	NSAPI	APACHE API	APACHE EAPI	-
Linux	-	-	-	APACHE API	APACHE EAPI	IHS-APACHE API

3. Follow all instructions that appear, which are specific to each type of Web server, and note the following:
   - Make a back up copy of any file that you are required to modify during Web server set up, so it is available if you need to start over.
   - Some setups launch a new browser window or require you to launch a Command window to input information, so ensure that you return to and complete all original setup instructions to enable your Web server to recognize the appropriate NetPoint files.

     Note: If you accidentally closed the window, return to step 1 and click the appropriate link again.
4. Continue with the appropriate procedure below.
   - “Verifying Access Manager Permissions on IIS” on page 175, if needed.
   - “Setting Up the Access Manager” on page 175

Verifying Access Manager Permissions on IIS

Whether you updated your configuration automatically during Access Manager installation or manually, you can easily verify that the directory permissions are properly set for NetPoint.

To verify the Access Manager IIS Web server configuration

1. Launch your Web browser, and open the following file, if needed. For example:

   AccessManager_install_dir\access\oblix\lang*langTag*\docs\config.htm

2. Select the appropriate Web server interface configuration protocol from the table on the screen, also shown under "Manually Configuring Your Web Server" on page 173.

3. Review the directory permissions and compare them to those set on the Access Manager Web server.

Setting Up the Access Manager

The Access Manager must communicate with your directory server to write the new policies you create. The following procedures guide you as you make the connections that are necessary for this communication.

During setup, specifications are saved whenever you click the Next button. If you leave setup and restart it later, you are returned to the same place.

Task overview: Setting up the Access Manager

1. Start the process, as described in "Starting the Setup Process" on page 176.

2. Define directory details, as described in "Specifying Directory Server Details and Data Locations" on page 177.

3. Set up authentication schemes, as described in "Configuring Authentication Schemes" on page 180.

4. Finish the setup process, as described in "Completing Access Manager Setup" on page 183.

Starting the Setup Process

Access Manager setup cannot be completed if the directory server used to store policy information is not loaded with the Oblix schema.

You must manually update the policy data directory server schema before you begin the setup process, when the following conditions are *both true:*

- You plan to store policy data in a separate directory server
- You did not update this directory server schema during COREid System setup

If you need to do this, use the instructions in the following file:

AccessManager_install_dir\access\oblix\lang*langTag*\ ldap_schema_changes_*directory_server*.html

where *directory_server* in the path name refers to your specific directory server type and *langTag* refers to the language you are using, for example \en-us.

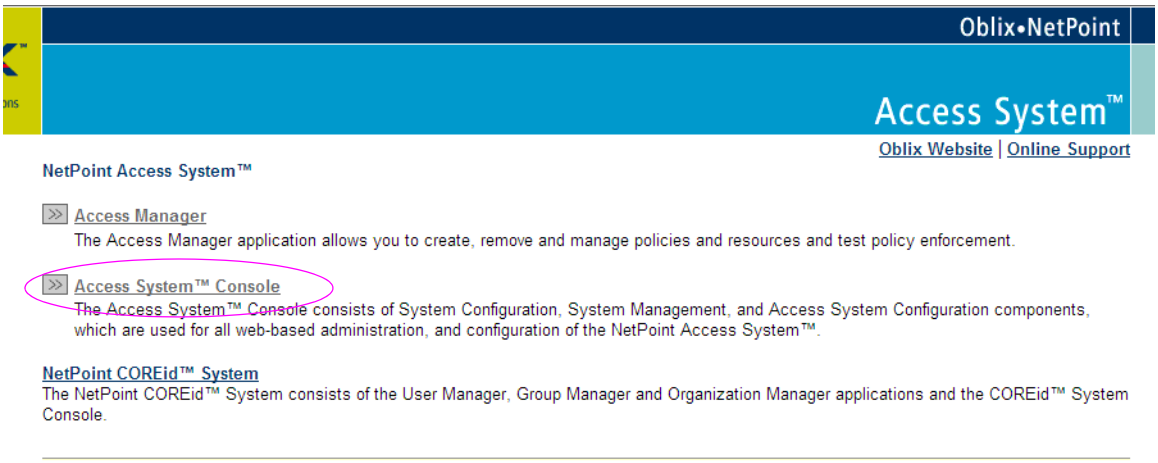
To start setting up the Access Manager

1. Make sure your Web server is running.
2. Navigate to the NetPoint Access System Console from your browser by specifying the URL of the WebPass instance that connects to the Access Manager. For example:

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

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

   You will see the main Access System page.



3. Click the Access System Console link.

   You are informed that the application is not yet set up.

4. Click the Setup button.

   The next page asks about the directory server type.

5. Continue with "Specifying Directory Server Details and Data Locations" on page 177 and see the file below for additional details:

   AccessManager_install_dir\access\oblix\lang*langTag*\important_notes.txt

   where *langTag* refers to a specific language, such as en-us (the default).

Specifying Directory Server Details and Data Locations

You need to specify details about the directory servers where user data, Oblix data, and policy data are stored. You will be asked to provide information about the directory server for each type of data:

- User data
- Configuration data
- Policy data

Your directory server type affects the scope of activities. With Siemens DirX or Sun directory servers, you may store policy data on a different directory server than configuration or user data. All policy data must be stored together on the same directory server.

With Active Directory, a pure ADSI configuration is created and communication to the directory servers will be configured over ADSI when you select the ADSI option. If you want to enable Dynamic Auxiliary Object Classes (Windows 2003 only), see "About Dynamically-Linked Auxiliary Classes" on page 382.

The information you see during setup will depend on your environment. In this example, user data, Oblix data, and policy data are stored together on the same directory server. Your environment may be different.

To specify directory server details

1. Select your *user data* directory server type, then click Next.

   For example:

   Siemens DirX

   Now you specify details for the *user data* directory server to help the Access Manager locate your directory server and copy information into it.

2. Specify the *user data* directory server details based on your installation, then click Next.

   For example:

   - **Machine**—The user data directory server DNS hostname
   - **Port Number**—The user data directory server port number
   - **Root DN**—The user data directory server bind DN
   - **Root Password**—The password for the bind DN

   Note: For Active Directory, a Domain Name field is included to fill in. With ADSI, a User-Principle-Name field is included where you enter the UserPrincipleName of the Root DN, such as :admin@mycompany.com.

   You are asked about where the user data and Oblix configuration data are stored.

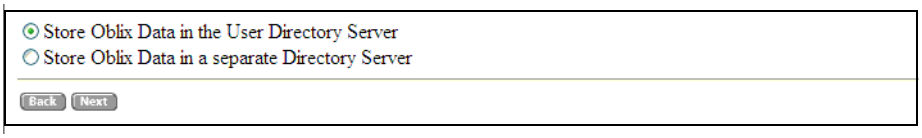
3. Select your Oblix (configuration) data directory server type, then click Next.

   For example:

   Siemens DirX

   Next you are informed that you can store your user data and Oblix data either in the same directory or in separate directories and asked to choose a configuration for your deployment.

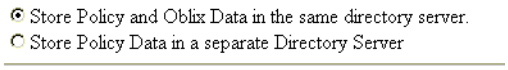
4. Choose the item that describes where you user data and Oblix configuration data are stored (together or separately), then click Next.

   - If the data is stored together, you are asked where policy data should be stored. In this case, continue with step 5.

- If the data is stored separately, you are asked to specify details for the configuration data directory server before you continue.

5. Choose the item that describes where your policy data and Oblix data are stored (together or separately), then click Next.



- If the data is stored together, continue with step 6.
- If the data is stored separately, you are asked to specify details for the policy data directory server before you continue.

The Setup Help button appears on the next page, which you can select to obtain additional information during the setup process. You are now asked to specify the location Of Oblix tree, searchbase, and policy base.

Note: The configuration DN, searchbase, and policy base may be at the same level or at different levels of the directory tree. However, when the searchbase and the policy base are in separate directories, they must have unique DNs. That is, the searchbase can not be o=Oblix,<Policy Base> or ou=Oblix,<Policy Base> if they are in separate directories. Similarly, the policy base and the configuration DN cannot be same if they are in separate directories.

---

6. Specify the following information for your installation, then click Next:

   For example:

   - **Searchbase**—o=*my-company*,c=*us*

     This *must* be the same searchbase you specified during COREid System configuration.

   - **Configuration DN**—o=*my-company*,c=*us*

     This *must* be the same Oblix data configuration DN you specified during COREid System configuration.

   - **Policy Base**—o=*my-company*,c=*us*

     This node resides within the policy directory server. If this node does not already exist, create it manually.

   You are now asked to specify the Person object class, which must match the one you specified during COREid System setup. For more information, see your preparation worksheets and “To specify Person and Group object class details” on page 141.

7. Enter the Person object class name, then click Next.

   For example:

   Person Object Class—gensiteOrgPerson

   At this point, you are prompted to restart your Web server.

   Note: If you are using IIS, be sure to follow additional on-screen instructions.

8. Stop and restart your WebPass/Access Manager Web server instance and the related COREid Server instance, as usual, then click Next to continue.

   Now you are asked to specify the root directory for NetPoint policy domains.

   Oblix recommends that you accept the default value "/" unless you want to restrict the NetPoint Administrator's ability to define and protect policy domains. For more information, see the *NetPoint 7.0 Administration Guide Volume 2*.

9. Accept the default root directory for policy domains (or specify a new root directory), then click Next.

   For example:

   Policy Domain Root /

   The next page asks about configuring authentication schemes.

Configuring Authentication Schemes

During Access Manager setup, the following two authentication schemes are configured automatically:

- **NetPoint Basic Over LDAP**—Used to protect NetPoint-related resources (URLs) and NetPoint-related resources (URLs) for Active Directory.
- **NetPoint None Authentication**—Used to unprotect specific NetPoint URLs.

  The NetPoint None authentication method is especially useful because it provides for anonymous users. Users are allowed access to NetPoint-specific URLs you do not want protected with the Access System, such as Self Registration and Lost Password Management.

In addition, you can automatically configure a Basic and a Client Certificate authentication scheme based on the configuration information from your user directory:

- **Basic Over LDAP**—This built-in Web server challenge mechanism requires the user to enter their login ID and password. The credentials supplied are then compared to the users profile in the LDAP directory server.

- **Client Certificate**—This is a certificate-based user identification method. To use this method, a certificate must be installed on your browser and the Web server must be SSL-enabled.

The fields on the setup page for each scheme must be completed with information that is consistent with the NetPoint environment you are setting up. In most cases, appropriate defaults will appear on the setup page. You can modify these parameters later using the Access System Console.

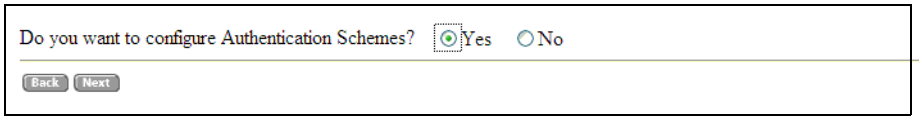
You are also asked if you want to setup policies. If you accept this option, the following two policy domains are created automatically:

- NP Access Manager
- NetPoint Identity Domain

Of course, you can decline automatic configuration and set up Basic over LDAP and Client Certificate authentication schemes in the Access System Console later. For more information about authentication schemes and policy domains, see the *NetPoint 7.0 Administration Guide Volume 2.*

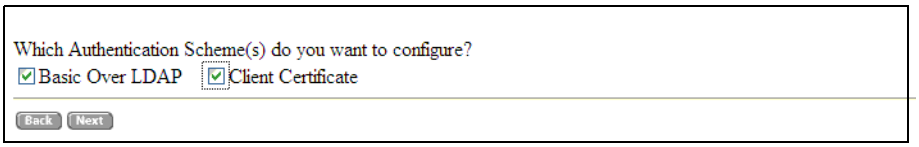
To complete the authentication scheme sequence

1. Select Yes to initiate the automatic configuration sequence, or No to set up all authentication schemes yourself, then click Next.



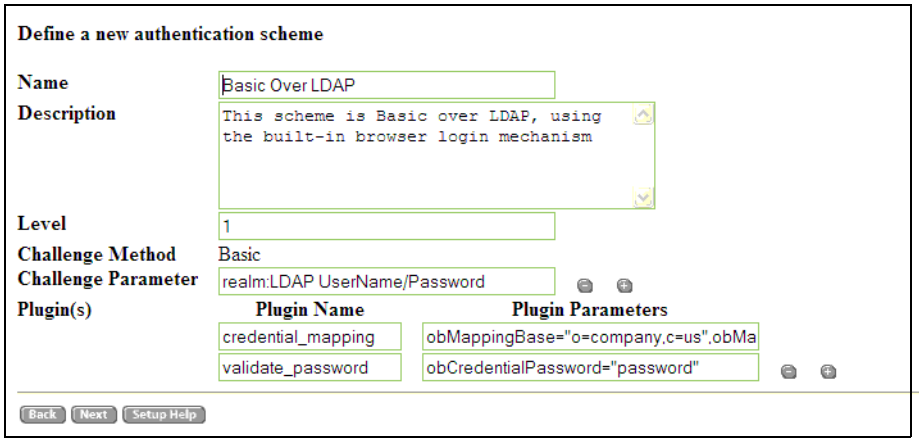
   - If you selected Yes, continue with step 2.
   - Otherwise, skip to step 5.

2. Choose the authentication scheme or schemes you want to configure automatically, then click Next.

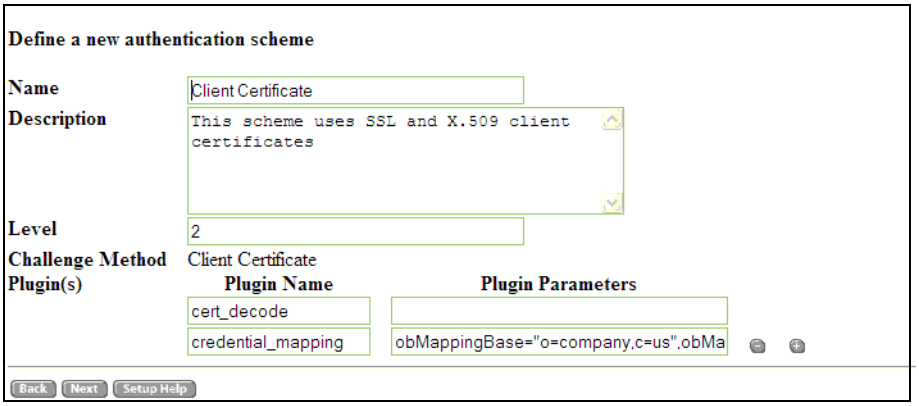


   - If you chose Basic Over LDAP, a page appears with its definition, which you can change now or later. In this case, continue with step 3.
   - If you chose only Client Certificate, skip to step 4.

3. Review and change Basic Over LDAP parameters, as needed, then click Next.

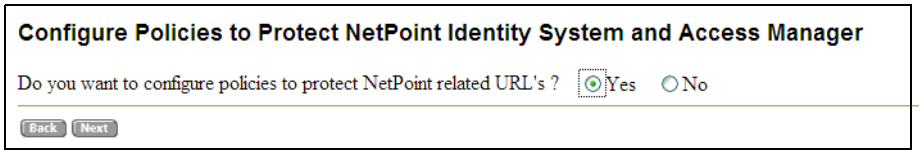


4. Review and change Client Certificate parameters, as needed, then click Next.



Next you are asked if you want to configure policies to protect NetPoint-related (URLs). The default is No.

5. Select Yes to configure the policies or No, then click Next. For example:



You must associate and install WebGates and Access Servers before you can use the policy domains. For more information about policy domains, see the *NetPoint 7.0 Administration Guide Volume 2*.

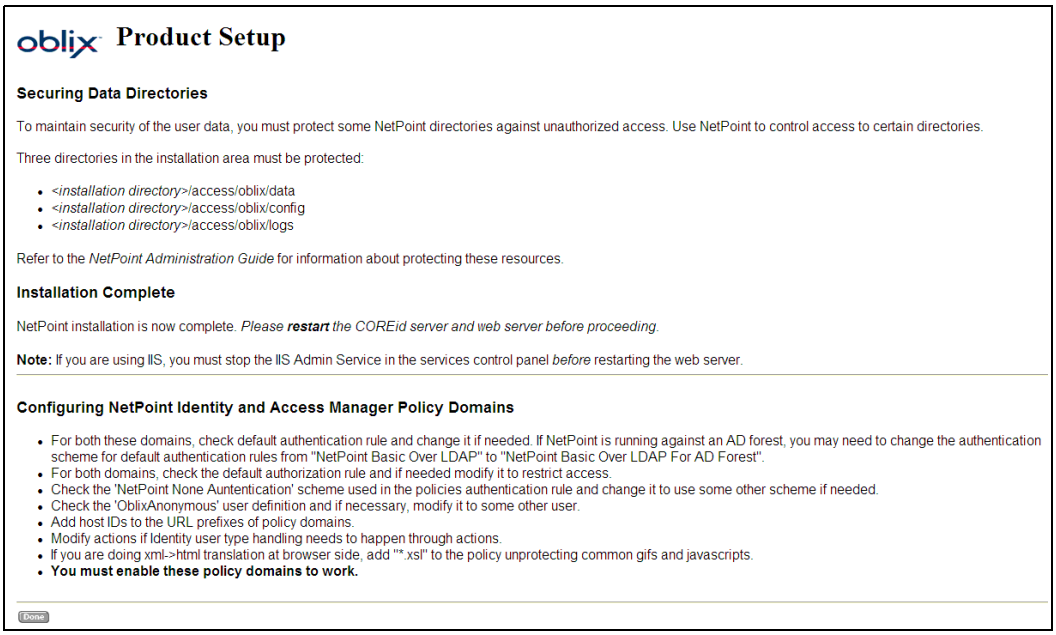
The next page provides instructions to complete the Access Manager setup.

Completing Access Manager Setup

The Securing Data Directories page lists the NetPoint directories that you must protect to maintain the security of the NetPoint COREid System.

- You must restrict access both from browsers and from network users who access the directory through the file system. See the documentation for your Web server and operating system if you need instructions on how to protect directories.
- You can also protect the NetPoint Access System within a NetPoint policy domain. See the *NetPoint 7.0 Administration Guide Volume 2* for more information.

The second half of the page on-screen provides additional information about configuring NetPoint policy domains.



oblix **Product Setup**

Securing Data Directories

To maintain security of the user data, you must protect some NetPoint directories against unauthorized access. Use NetPoint to control access to certain directories.

Three directories in the installation area must be protected:

- *<installation directory>*/access/oblix/data
- *<installation directory>*/access/oblix/config
- *<installation directory>*/access/oblix/logs

Refer to the *NetPoint Administration Guide* for information about protecting these resources.

Installation Complete

NetPoint installation is now complete. *Please **restart** the COREid server and web server before proceeding.*

Note: If you are using IIS, you must stop the IIS Admin Service in the services control panel *before* restarting the web server.

Configuring NetPoint Identity and Access Manager Policy Domains

- For both these domains, check default authentication rule and change it if needed. If NetPoint is running against an AD forest, you may need to change the authentication scheme for default authentication rules from "NetPoint Basic Over LDAP" to "NetPoint Basic Over LDAP For AD Forest".
- For both domains, check the default authorization rule and if needed modify it to restrict access.
- Check the 'NetPoint None Auntentication' scheme used in the policies authentication rule and change it to use some other scheme if needed.
- Check the 'OblixAnonymous' user definition and if necessary, modify it to some other user.
- Add host IDs to the URL prefixes of policy domains.
- Modify actions if Identity user type handling needs to happen through actions.
- If you are doing xml->html translation at browser side, add "*.xsl" to the policy unprotecting common gifs and javascripts.
- **You must enable these policy domains to work.**

Done

To complete the Access Manager setup

1. Read all information on the page before you continue.

   Important: If you are using Active Directory, see “Installing and Setting Up the Access System” on page 401 for additional information before you continue.

2. Restart the Web server and COREid Server service in the following order:

   a) Stop the WebPass Web server instance, which is the same as the Access Manager.

b) Stop, then restart the COREid Server service for the WebPass.

c) Restart the WebPass/Access Manager Web server instance.

3. After the Web server restarts, click Done.

   The Access Manager home page appears.

4. Review the following information; you may perform any of the following procedures.

   - "Confirming Access Manager Setup" on page 184.
   - "Installing the Access Server" on page 194.
   - Protect the directories as indicated on the Securing Directories page during setup, as described in the *NetPoint 7.0 Administrator Guide*.

Confirming Access Manager Setup

An easy way to confirm your Access Manager setup is to log in and review the authentication schemes automatically configured during the setup process. You may also begin to use the Access System Console to setup the Access Server instance and define other administrators, as described in the *NetPoint 7.0 Administration Guide Volume 2*.

Note: If the Access Manager home page is on your screen, you may skip step 1.

To confirm Access Manager setup

1. Navigate to the NetPoint Access System Console from your browser. For example:

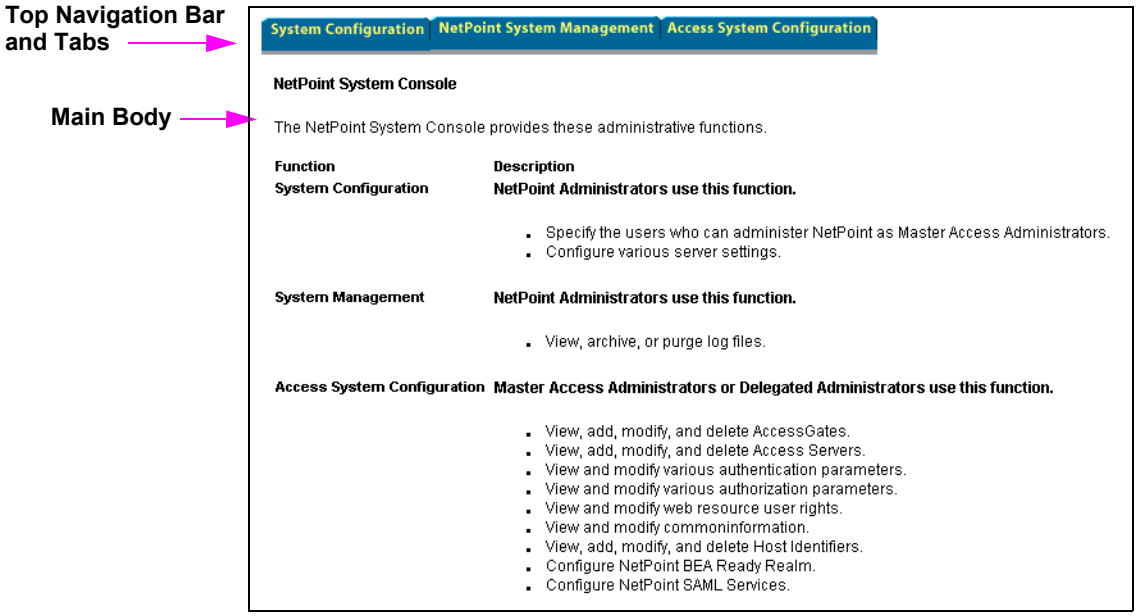
   http://*hostname*:*port*/access/oblix

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

2. Select the Access System Console link.

3. Log in as a user with NetPoint Administrator privileges.

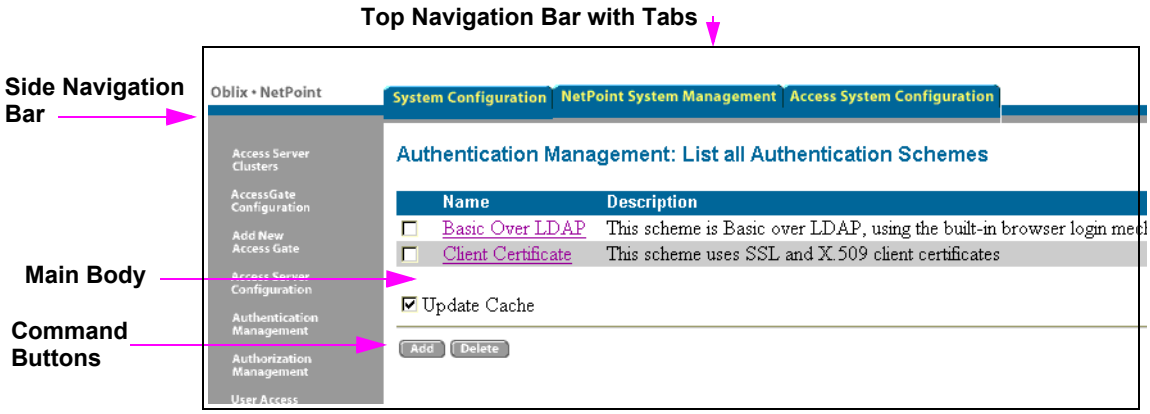
   The Access System Console appears, as shown next.



You can click a tab in the top navigation bar to display a list of options, which will appear along the left side of the on-screen page. For example, complete step 4 to display a list of currently configured authentication schemes.

4. Select the Access System Configuration tab, then click Authentication Management when it appears in the left column.

A list of currently configured authentication schemes appears in the main body of the new page, as shown next. If you did not choose to automatically configure schemes, none will be listed.



At this point, you can:

- Display configuration details for an authentication scheme by clicking the link that corresponds to the scheme.
- Add an Access Server instance by selecting Access Server Configuration in the side navigation bar (this is a prerequisite to installing an Access Server). For more information, see “Installing the Access Server” on page 194.
- Continue to explore the Access System Console and Access Manager.

  For example, you can define or modify policy domains The fact that Access Server or WebGate has not yet been installed has no impact on your ability to define them. Once these components are installed, the policy domains will be in affect.
- Log out by selecting Logout in the side navigation bar.

  For more information, see the *NetPoint 7.0 Administration Guide Volume 2*.
- Install the Access Server. For details, see “Installing the Access Server” on page 194.

7 Installing the Access Server

This chapter explains how to install the Access Server, which is the second Access System component you must install. See the following topics:

Upgrading to NetPoint 7.0 is described in the *NetPoint 7.0 Upgrade Guide*. For an overview of NetPoint components, see the Introduction to *NetPoint 7.0 Guide*.

About the Access Server and Installation

The Access Server is a stand-alone component that provides dynamic policy evaluation services for both Web-based and non-Web resources and applications.

The Access Server receives requests from an access client, either a WebGate or a custom AccessGate; queries your LDAP directory for authentication, authorization, and auditing rules; and validates credentials, authorizes users, and manages user sessions for NetPoint. For more information, see "About NetPoint Installations" on page 23.

Before you install the Access Server you need to create an instance for it within the Access System Console.

Task overview: Installing the Access Server

1. Create an Access Server instance in the Access System Console, as described in "Creating an Access Server Instance" on page 191.
2. Install the Access Server, as described in "Installing the Access Server" on page 194.
3. Install additional Access Servers, if needed, as described in "About Installing Multiple Access Servers" on page 189.

Installing the Access Server is similar to installing the COREid Server. You will specify directory server details during this installation and a default directory profile is created for this Access Server. The default profile is available after you create an Access Server instance; the completed profile is available after installation. There is no Web server involved in Access Server installation.

The following two installation packages are provided for the Access Server:

Windows—NetPoint7_0_win32_Access_Server
Unix—NetPoint7_0_sparc-s2_Access_Server

You must complete all procedures for a successful installation. Information is saved at certain points during the installation process. If you cancel the installation after being informed that the Access Server is being installed, you must uninstall the component, as described in "Upgrading from a Previous Version of NetPoint" on page 37.

The installation process is similar regardless of the installation mode you choose and your operating system. Any caveats are identified and may be skipped when they do not apply to your environment.

For more information, see "Access Server Installation Considerations" on page 189.

About the Access Server Installation Directory

You may install the Access Server in the default directory or in a directory of your choosing. When you change the path name, you may include any characters that are acceptable to your operating system. For example, you may include spaces on Windows systems but not on Unix systems. During installation, /access is appended to the directory path you specify. The installation directory for an Access Server installation is shown below:

Default on Windows—\Program Files\NetPoint\access
Default on Unix—/opt/netpoint/access
In This Guide—*AccessServer_install_dir*\access

Note: Do not install the Access Server in the same directory as the Access Manager. Do not install multiple Access Servers in the same directory.

About Installing Multiple Access Servers

Oblix recommends you install multiple Access Servers for failover and load balancing. The procedures to do this are similar to those for installing a single Access Server.

Task overview: Installing multiple Access Servers

1. Create instances for each Access Server in the Access System Console, as described in "Creating an Access Server Instance" on page 191.

   Note: Do not install multiple Access Servers in the same directory.

2. Install the Access Server, as described in "Installing the Access Server" on page 194, and specify a different installation directory for each Access Server.

   You can replicate an existing installation using an options file, as described in "Replicating Components" on page 241.

3. Install one or more AccessGates/WebGates and assign the Access Servers to them as either primary or secondary Access Servers, as described in "Installing the AccessGate/WebGate" on page 199.

Refer to the *NetPoint 7.0 Administration Guide Volume 2* for complete instructions on how to enable these features.

Access Server Installation Considerations

Following are several considerations to take into account before you install the Access Server.

Administration Privileges—The account that performs NetPoint installation must have administration privileges. On Microsoft Windows, the user account that is used to run the Access Server service must have the "Log on as a service" right, which can be set through Administrative Tools > Local Security Policy > Local Policies > User Rights Assignments > Log on as a service.

Active Directory—When you are installing NetPoint with Active Directory, read "Installing NetPoint with Active Directory" on page 394. Pay close attention to the information "To install and set up the Access Server and WebGate" on page 403, and perform additional steps as needed. Also, complete the procedure under "To set up ADSI on the Access Server" on page 404 after installation, if needed.

COREid Data Anywhere—Available only for *user data* when NetPoint is integrated with OctetString Virtual Directory Engine (VDE). The LDAP directory branches containing NetPoint configuration and policy data must reside on one or

more directory servers other than the one hosting VDE or user data. NetPoint applications only recognize configuration and policy information that resides outside the VDE virtual directory. See the *NetPoint Integration Guide*.

Failover and Load Balancing—Oblix recommends installing multiple Access Servers for failover and load balancing.

Firewall—Oblix recommends protecting the machine on which you will install the Access Server with a firewall.

Language Pack—If you have installed a Language Pack with other NetPoint components, you must install the same Language Pack with the Access Server. Execute permissions are required for Language Pack installers on Unix systems.

Secure Communications with a Directory Server—If you plan to use SSL for communications between the Access Server and your directory server, your directory server instance must be secured with a certificate.

Access Server Prerequisites Checklist

Before you begin installing the Access Server, confirm that you have completed the tasks in Table 30. Failure to complete all prerequisites may adversely affect your NetPoint installation.

Table 30 Access Server Prerequisites Checklist

Checklist	WebGate Prerequisites
	Complete COREid System setup and confirm that your COREid System is working, as described in “Setting up the COREid System” on page 136.
	Install, set up, and confirm that you have a working Access Manager, as described in “Installing the Access Manager” on page 159.
	Protect the machine on which you will install the Access Server with a firewall.
	Move Language Pack installers into the same directory as the Access Manager installer, if needed, and ensure that the Language Pack installer on Unix systems has execute permissions, as described in “Access Server Installation Considerations” on page 189.

Creating an Access Server Instance

Before you can install the Access Server you must create an instance for it within the Access Manager, Access System Console. This can be accomplished by either the NetPoint Administrator or the Master Access Administrator if one has been defined.

The Access Server ID you specify when you create the instance must be unique and cannot contain spaces, a colon ":", the pound sign "#", or non-English keyboard characters. On Windows systems, this Access Server ID will be used as the Windows Service name, with "NetPoint AAA Server" as a prefix.

To create an Access Server instance

1. Connect to the Access System Console. For example:

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

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

   The Access System main page appears.

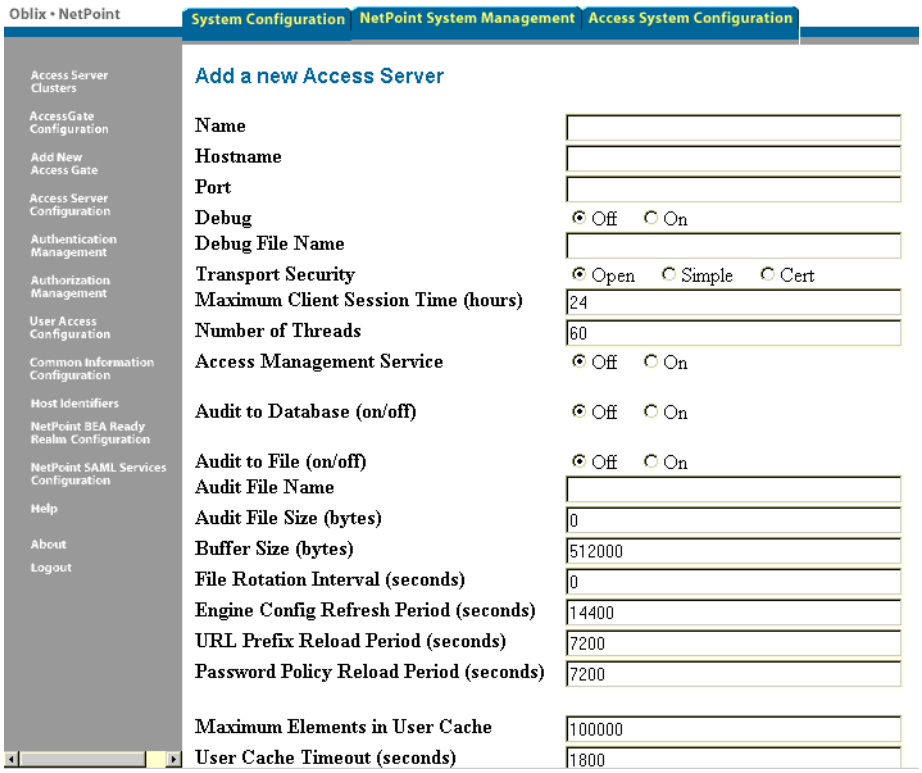
2. Click the Access System Console link, then log in as a NetPoint Administrator.

   The Access System Console main page provides three tabs across the top and information about the functions in the center.

3. Click the Access System Configuration tab, then click Access Server Configuration when the side navigation bar appears.

   If this is the first Access Server, the main page will inform you that no Access Servers were found in the directory server. Otherwise, Access Servers that have been added will be listed.

4. Click the Add button to display the Add a new Access Server page with some defaults.



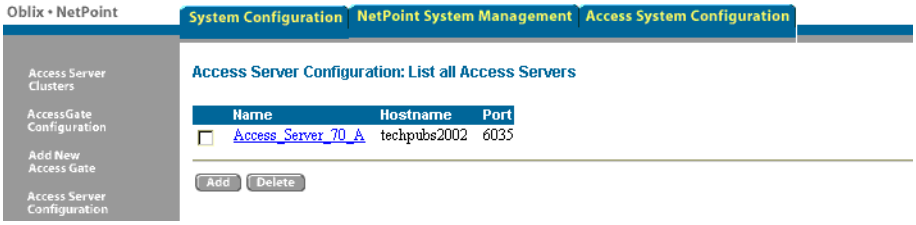
You need only supply basic information to create the instance. After installation, you can complete additional configuration as discussed in the *NetPoint 7.0 Administrator Guide*. Online help is also provided.

5. Specify the following parameters for the Access Server you plan to install. For example:

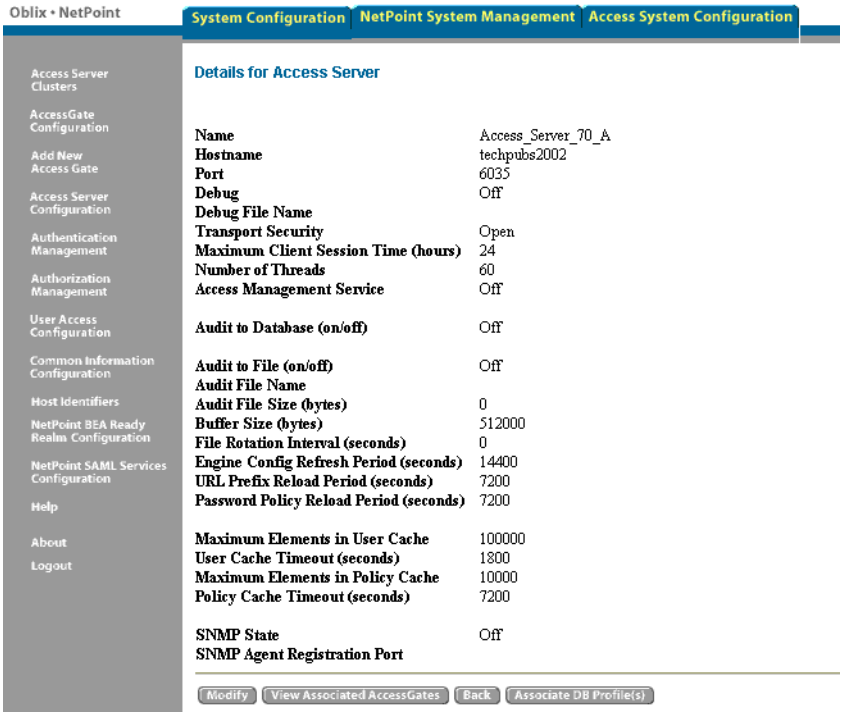
   - **Name**—Descriptive name for the Access Server that is different from any others already in use on this directory server. Do not include spaces, a colon (“:”), or the pound sign (“#”) in the name.
   - **Hostname**—Name of the machine where the Access Server will be installed. The Access Server does not require a Web server instance.
   - **Port**—Port on which the Access Server will listen.
   - **Transport Security**—Transport security between all Access Servers and associated WebGates must match: either all open, all Simple mode, or all Cert.

6. Click Save.

   The List All Access Servers page appears with a link to this instance.



7. Click the link to the Access Server instance, print the Details page for later reference, then click the Back button at the bottom of the page.



8. Repeat step 3 through step 7 for each additional Access Server instance you want to install.

9. Click Logout, close the browser window, and continue with “Installing the Access Server” on page 194.

Installing the Access Server

Refer to your completed installation preparation worksheets as you install the Access Server. The following procedures must be completed for each Access Server:

- "Starting the Installation" on page 194
- "Specifying a Transport Security Mode" on page 195
- "Specifying Directory Server and Communication Details" on page 195
- "Finishing the Access Server Installation" on page 197

Starting the Installation

The Access Server installation sequence is similar to those you have performed for other NetPoint components.

Note: Do not install the Access Server in the same directory as the Access Manager. Do not install multiple Access Servers in the same directory.

To start the Access Server installation

1. Log in as a user with Administrator privileges.
2. Locate and launch the component installer for your preferred platform and installation mode.

   For example:

   - **GUI Mode**
     Windows—NetPoint7_0_Win32_Access_Server.exe
     Solaris—./NetPoint7_0_sparc-s2_Access_Server -gui
   - **Console Mode**
     Solaris—./NetPoint7_0_sparc-s2_Access_Server
     Windows Command Window—
     NetPoint7_0_Win32_Access_Server -console
3. Dismiss the Welcome screen by clicking Next
4. Accept the license agreement terms, then click Next.

   Note: You will be operating a temporary license, good for 60 days and up to 100 users, until you request, receive, and enter your permanent license. For details, see the *NetPoint 7.0 Administration Guide Volume 2*.

   ---

5. Respond to the next question based upon your platform. For example:

- **Windows**—If you are logged in with administrator rights, click Next (otherwise click Cancel, log in as a user with administrator privileges, then restart the installation).
- **Unix**—Specify a dedicated username and group that the Access Server will use, then click Next. Typically, the defaults are “nobody”.

  For HP-UX, the defaults are WWW (username) and others (group).

6. Identify the installation directory, then click Next.

   For example:

   \NetPoint_70

7. **Language Pack**—Choose a Default Locale and any other Locales to install, then click Next.
8. Record the installation directory name, then click Next.

   The Access Server is installed, which may take a few seconds. On Windows systems, a screen appears informing you that the Microsoft Managed Interfaces are being configured.

   You are asked to specify the transport security mode.

Specifying a Transport Security Mode

For details, see “Securing NetPoint Component Communications” on page 45.

To specify a transport security mode

1. Choose a transport security mode: Open, Simple, or Cert.
2. Click Next.

   Regardless of your transport security choice, you are asked to specify directory server details next.

Specifying Directory Server and Communication Details

During this sequence, you are asked to provide details about your environment and the Oblix configuration and policy data directory servers. NetPoint adds additional configuration entries to the directory server.

To specify directory server details

1. Provide the information requested for the Oblix *configuration data* directory server, then click Next.
   - Open or SSL
   - **Host machine**—The DNS hostname of the directory server with Oblix configuration data

- **Port number**—Port on which the directory server with Oblix configuration data listens (for SSL connections, provide the encrypted port)
- **Root DN**—Bind DN for the directory server with Oblix configuration data
- **Root Password**—Bind DN password for the directory server with Oblix configuration data
- **Oblix Directory**—Type of directory server with Oblix configuration data

  For example:

  Siemens DirX

2. **SSL Only**—Enter the path to the SSL certificate.

   You need to identity where NetPoint policy data is stored: either with Oblix configuration data or in a separate directory server. For more information, see "Data Storage Requirements" on page 59.

3. Identify where the NetPoint *policy data* is stored.

   For example:

   Oblix Directory

   Note: If your policy data is stored separately, you need to provide information for the policy data directory server. The configuration DN and policy base must be unique. See "Data Storage Requirements" on page 59.

   You are now asked for the Access Server instance ID that you specified in the Access System Console and the configuration DN and policy base.

4. Enter the requested details, then click Next.

   For example:

   Access Server ID—Access_Server_70_A
   Configuration DN—o=*my-company*,c=us
   Policy Base—o=*my-company*,c=us

5. Perform the following operations according to the transport security mode you chose earlier:

   - **Open**—Skip to "Finishing the Access Server Installation" on page 197.
   - **Simple**—Continue with step 6.
   - **Certificate**—Indicate whether you are requesting or installing a certificate, click Next, then continue with step 6.

6. Specify and confirm the Pass Phrase, click Yes (or No) when asked to store the password in a file, click Next.

Note: When you select No on Windows, you are prompted for the PEM phrase every time you start the Access Server. When you select No on Unix, you must use the -P option to pass the password whenever you launch the start_access_server script.

---

7. **Simple**—Skip to "Finishing the Access Server Installation" on page 197.
8. **Certificate**—Complete your certificate request and installation sequence, then continue with "Finishing the Access Server Installation" on page 197.

Note: If you requested certificates and they are not ready during this installation, the Access Server cannot be used until the you copy certificates to the *AccessServer_install_dir*\access\oblix\config directory, and restart the Access Server.

You are informed that the Access Server is being configured, then ReadMe information appears.

Finishing the Access Server Installation

The ReadMe information provides details about documentation and contacting Oblix.

To finish the Access Server installation

1. Review the ReadMe information, then click Next to dismiss it.

   You are informed that the installation is complete and that you need to start your Access Server.

2. Click Finish to close the wizard.

   You need to start your Access Server, which confirms that the Access Server installation was successful and prepares for WebGate installation.

3. Start your Access Server to confirm that it is installed and operating properly:
   - **Windows**—The Access Server ID you specified in the Access System Console will be used as the Windows Service name with the prefix "NetPoint AAA Server" included.
   - **Unix**—Go to your /*AccessServer_install_dir*/access/oblix/apps/common/bin directory and execute ./start_access_server.

Note: For installations that do not use a password file, you must start the Access Server locally. Attempting this remotely (through a terminal emulator such as NetMeeting or Windows 2000 remote service restart) will fail.

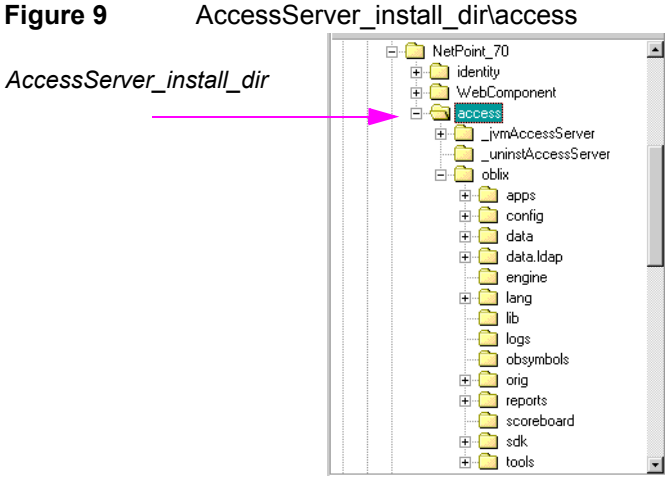
What you do next depends on your environment:

- Check the installed files, as described in “Installed Files” on page 198.
- Setup ADSI, if needed, as described in “Setting Up ADSI (Optional)” on page 398.
- Install a WebGate, as described in “Installing the AccessGate/WebGate” on page 199.

Installed Files

The subdirectories in Figure 9 were created and stored under *AccessServer_install_dir*\access during installation, which is the installation directory you specified for the Access Server.

Figure 9 AccessServer_install_dir\access



8 Installing the AccessGate/ WebGate

This chapter explains how to install an AccessGate or WebGate and how to configure the WebGate to work with the Web server. This chapter covers the following topics:

Upgrading to NetPoint 7.0 is described in the *NetPoint 7.0 Upgrade Guide*. For an overview of NetPoint components, see the Introduction to *NetPoint 7.0 Guide*.

About WebGate/AccessGate and Installation

A WebGate is a Web server plug-in that is shipped out-of-the-box with NetPoint. The WebGate intercepts HTTP requests from users for Web resources and forwards them to the Access Server for authentication and authorization. An AccessGate is a NetPoint access client that processes requests for Web and non-Web resources and is developed using the NetPoint Access Server SDK.

The terms AccessGate and WebGate may be used interchangeably. Before you can install a WebGate, you must associate it with an Access Server.

Task overview: Installing a WebGate

1. Create an instance, as described in "Creating a WebGate Instance" on page 204.
2. Associate the instance, as described in "Associating a WebGate and Access Server" on page 207.
3. Install the WebGate, as described in "Installing the WebGate" on page 208:
4. Complete the following procedures as needed:
   - "Manually Configuring Your Web Server" on page 213 if you did not do this automatically during installation.
   - "Completing IIS WebGate Installations" on page 214, if needed
   - "Completing httpd.conf Updates" on page 219, if needed
5. Finish by "Confirming WebGate Installation" on page 220, which is a good practice.

Installing the WebGate is similar to installing the WebPass. There are no directory server details to specify and the WebGate Web server configuration must be updated.

Separate Web server-specific installation packages are provided for the WebGate on various platforms, as described in "Platform Requirements" on page 66. Be sure you choose the one for your environment.

You must complete all procedures for a successful installation. Information is saved at certain points during the installation process. If you cancel the installation after being informed that the WebGate is being installed, you must uninstall the component, as described in "Upgrading from a Previous Version of NetPoint" on page 37. Any caveats are identified and may be skipped when they do not apply to your environment.

For more information, see "WebGate Installation Considerations" on page 201.

WebGate Installation Directory

You may install the WebGate either in the default directory or in a directory of your choosing. When you change the path name, you may include any characters that are acceptable to your operating system. For example, you may include spaces on Windows systems but not on Unix systems.

During installation, \access is appended to the installation directory path you specify. For example:

Default on Windows—\Program Files\NetPoint\WebComponent\access
Default on Unix—/opt/netpoint/WebComponent/access
In This Guide—*WebGate_install_dir*\access

If you install the WebGate to protect the Access Manager and WebPass, the WebGate *must* be installed in the same directory as the Access Manager and WebPass. In this case, separate _jvmWebGate and _uninstWebGate subdirectories are included and WebGate information is added to the \oblix subdirectory.

About Installing Multiple WebGates

Oblix recommends you install multiple WebGates for failover and load balancing. Oblix recommends you use the cloning feature to facilitate installation on multiple systems, as described in “Replicating Components” on page 241.

Installing multiple WebGates follows the same process as described in this chapter.

WebGate Installation Considerations

You need to install a WebGate on any Web server that you want to protect with the NetPoint Access System, including the Web server on which the Access Manager is installed.

You can install the WebGate in any directory that your Web server can access. To protect the Access Manager and WebPass, the WebGate must be installed in the same directory as the Access Manager and WebPass.

The WebGate *must* be installed on a machine hosting a Web server. The Webgate may be configured to run at either the machine level or the virtual Web server level. However, do not install at both the machine level and the virtual Web server levels.

The WebGate may be installed at the root level or the site level. However, installing WebGate on multiple virtual sites amounts to only one instance of WebGate.

The WebGate can be installed with the same Web server instance as the WebPass and Access Manager to protect these components. In this case, the WebGate *must* be installed in the same directory as the Access Manager and WebPass. For example, if the WebPass and Access Manager are installed in *\NetPoint\WebComponent*, then the WebGate must also be installed there.

The account that performs NetPoint installation must have administration privileges.

Web server and operating system types are not factors in WebGate-to-Access Server communication. However, there are considerations for WebGates in various environments:

- **Unix WebGates**—You may be logged in as root to install the WebGate. The WebGate can be installed using a non-root user if the Web server process runs as a non-root user.
- **Apache Web Servers**—NetPoint supports Apache with or without SSL enabled. For SSL-enabled communication, NetPoint supports Apache with mod_ssl only, not Apache-SSL. mod_ssl is a derivative of, and alternative to, Apache-SSL.
- **IHS v2 Web Servers**—NetPoint supports IHS v2 and IHS v2 Reverse Proxy servers with or without SSL enabled. For details, see "Configuring Apache and IHS v2 Web Servers for NetPoint" on page 301.
- **Domino Web Servers**—Before you install the NetPoint WebGate with a Domino Web server, you must have properly installed and set up the Domino Enterprise Server R5. For more information, see "Setting Up Lotus Domino Web Servers for NetPoint WebGates" on page 341.
- **IIS Web Servers**—Before installing the WebGate, ensure that your IIS Web server is *not* in lockdown mode. Otherwise things will appear to be working until the server is rebooted and the metabase reinitialized, at which time IIS will disregard activity that occured after the lockdown.

  If you are using client certificate authentication, before enabling client certificates for the WebGate you must enable SSL on the IIS Web server hosting the WebGate.

  Each IIS Virtual Web server can have it's own WebGate.dll file installed at the virtual level, or can have one WebGate affecting all sites installed at the site level. Either install the WebGate.dll at the site level to control all virtual hosts or install the WebGate.dll for one or all virtual hosts.

  You may also need to install the postgate.dll file at the machine level. The postgate.dll is located in the *\WebGate_install_dir*, as described in "Installing postgate.dll on IIS Web Servers" on page 216. If you perform multiple installations, multiple versions of this file may be created which may cause unusual NetPoint behavior. In this case, you should verify that only one webgate.dll and one postgate.dll exist.

Note: The postgate.dll is always installed at the site level. If for some reason the WebGate is re-installed, the postgate.dll is also re-installed. In this case, ensure that only *one* copy of the postgate.dll exists at the site level.

To fully remove a WebGate and related filters from IIS, you must do more than simply remove the filters from the list in IIS. IIS retains all of its settings in a metabase file. On Windows 2000 and later, this is an XML file that can be modified by hand. There is also a tool available, MetaEdit, to edit the metabase. MetaEdit looks like Regedit and has a consistency checker and a browser/editor. To fully remove a WebGate from IIS, use MetaEdit to edit the metabase.

- **ISA Proxy Servers**—On the ISA proxy server, all ISAPI filters must be installed within the ISA installation directory. They can be anywhere within the ISA installation directory structure.

  a) Before installing the WebGate on the ISA proxy server:

     - Check for general ISAPI filter with ISA instructions on: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/isa/isaisapi_5cq8.asp
     - Ensure that the internal and external communication layers are configured and working properly.

  b) During installation you will asked if this is an ISA installation; be sure to:

     - Indicate that this is an ISA proxy server installation, when asked.
     - Specify the ISA installation directory path as the WebGate installation path.
     - Use the automatic Web server update feature to update the ISA proxy server during WebGate installation.

  c) After WebGate installation, locate the file configureISA4webgate.bat, which calls a number of vbscripts and the process to configure the ISA server filters that must be added programmatically.

If you have installed a Language Pack with other NetPoint components, you must install the same Language Pack with the WebGate. Execute permissions are required for Language Pack installers on Unix systems.

WebGate Prerequisites Checklist

Before you begin installing the WebGate, confirm that you have completed the tasks in Table 31. Failure to complete all prerequisites may adversely affect your NetPoint installation.

Table 31 WebGate Prerequisites Checklist

Checklist	WebGate Prerequisites
	Review and complete any needed preparation, as described in “Preparing to Install NetPoint” on page 39.
	Install, set up, and confirm that you have a working Access Manager, as described in “Installing the Access Manager” on page 159.
	Install the Access Server, as described in “Installing the Access Server” on page 187.
	Move Language Pack installers into the same directory as the Access Manager installer, if needed, and ensure that the Language Pack installer on Unix systems has execute permissions, as described in “WebGate Installation Considerations” on page 201.

Creating a WebGate Instance

Before you install an AccessGate or WebGate, you must define an instance in the Access Manager, Access System Console. The WebGate ID you specify in the Access System Console must be unique and cannot contain spaces, a colon “:”, the pound sign “#”, or non-English keyboard characters.

To define a WebGate instance in the Access Manager

1. Navigate to the Access System Console. For example:

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

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

   The Access System main page appears.

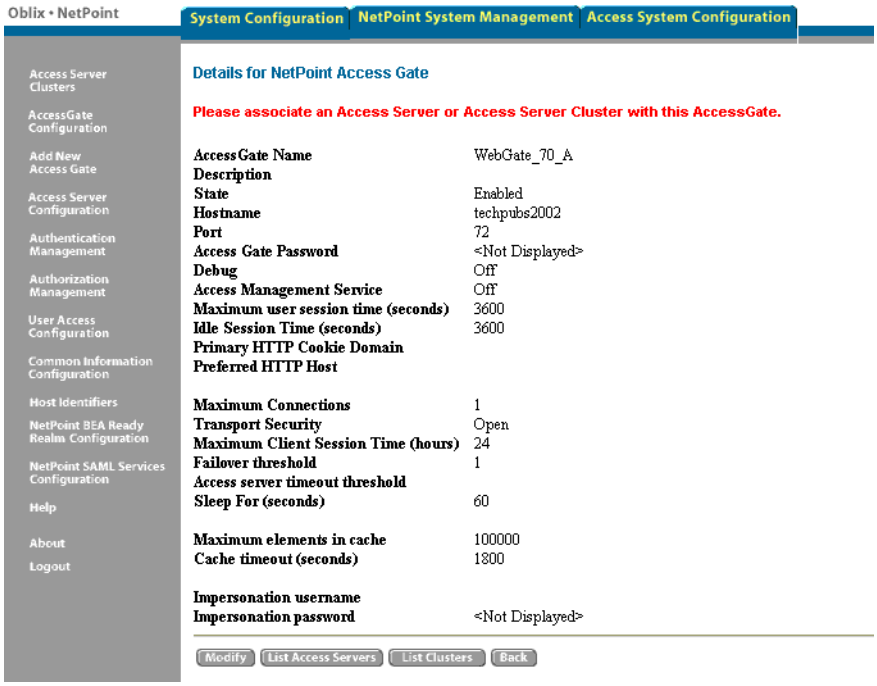
2. Click the Access System Console link, then log in as a NetPoint Administrator.

   The Access System Console main page appears.

3. Click Access System Configuration > Add new Access Gate.

4. Specify the following parameters for your WebGate and click Save:

- **AccessGate Name**—A unique, descriptive name for this WebGate/AccessGate. Do not include spaces in the name.
- **Description**—This is optional; you can add it later. This is case insensitive; if you change capitalization of information in this field it will not be accepted unless you include new information.
- **Hostname**—The name of the machine where the WebGate/AccessGate will be installed.
- **Port**—The port the WebGate Web server is listening to. For more information, see "WebGate Prerequisites Checklist" on page 204.
- **AccessGate Password** and **Re-type AccessGate Password**—This is an optional, unique password to verify and identify the component regardless of the transport security mode. This should differ for each WebGate instance.
- **Transport Security**—The level of transport security between the Access Server and associated WebGates. The default value is Open. For details see, "Securing NetPoint Component Communications" on page 45. You can change the mode later, as described in the *NetPoint 7.0 Administration Guide Volume 1*.



Details for your WebGate appear and you are asked to associate an Access Server or Access Server cluster with this AccessGate. Buttons at the bottom of this page help you modify the specifications, List Access Servers, or go back to the previous page.

5. Print this page, then click the Back button.
6. Continue with “Associating a WebGate and Access Server” on page 207.

Associating a WebGate and Access Server

Each Access Server functions as either a primary server or secondary server in association with a WebGate/AccessGate. If this is the only Access Server you are associating with this WebGate it should be a primary server. Multiple primary servers share incoming requests as they arrive. Secondary servers become active only if the primary servers go down. When you have multiple Access Servers, define at least one primary Access Server for this WebGate and define other Access Servers as either primary or secondary servers.

The number of connections identifies the number of Access Servers this WebGate can connect to, and the relative priority of the Access Servers for requests that come through the WebGate. For example, if you have two primary Access Servers and specify 2 connections for the first and 1 connection for the second, the first would receive two requests for every one the second receives. The default is 1. The number of requests the WebGate receives at one time is controlled by the Maximum Connections parameter in the AccessGate Configuration page.

Note: If you are continuing from step 5 above, you may skip step 1.

To assign an Access Server to the WebGate

1. Navigate to the Details for NetPoint AccessGate page, if needed: Access System Console > Access System Configuration > AccessGate Configuration > *WebGate_Link*

   You may associate this WebGate with an individual Access Server or with a cluster of Access Servers. For information about clusters, see the *NetPoint 7.0 Administration Guide Volume 2*.

2. On the Details for NetPoint AccessGate page, click the List Access Servers (or List Clusters) button at the bottom of the page.

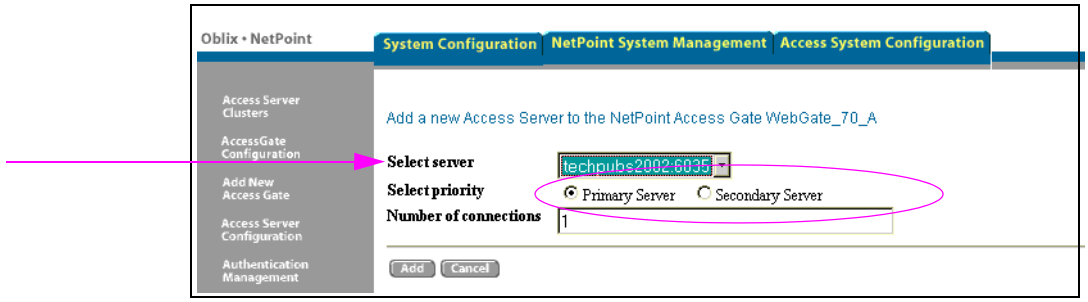
   A page appears saying that there are no primary or secondary Access Servers currently configured for this WebGate.

3. Click the Add button to advance to the Add a new Access Server page.

4. Select an Access Server from the Select Server list, specify a priority, and define the number of Access Servers (connections) to which this WebGate can connect.

   For example:

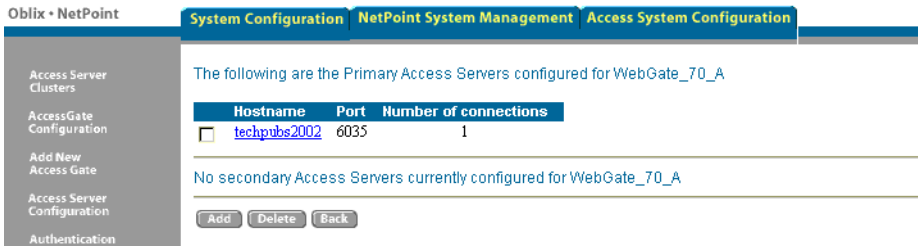
   Select server—*Your_Choice*
   Select priority—Primary Server
   Number of connections—1



If the Access Server you want is not listed, you may need to configure it. For details, see “Creating an Access Server Instance” on page 191.

5. Click the Add button to complete the association.

   A page appears listing the Access Server associated with this WebGate.



6. Click the link to display a summary and print this page for use later.
7. Repeat step 3 through step 6 to associate another WebGate and Access Server, if needed.
8. Logout and continue with “Installing the WebGate” on page 208.

Installing the WebGate

Once you have created a WebGate instance and associated it with an Access Server, you are ready to install the WebGate. Refer to your completed installation preparation worksheets complete the procedures below.

- “Starting the Installation” on page 209
- “Specifying a Transport Security Mode” on page 210
- “Specifying WebGate Configuration Details” on page 210
- “Updating the WebGate Web Server Configuration” on page 211
- “Finishing the WebGate Installation” on page 212

Starting the Installation

The WebGate installation sequence is similar to those you have performed for other NetPoint components.

To start the installation

1. Log in as a user with Administrator privileges.
2. Locate the component and launch the installation for your preferred platform, installation mode, and Web server.

   For example:

   GUI Mode
   Windows—NetPoint7_0_Win32_*API*_WebGate.exe
   Solaris—./NetPoint7_0_sparc-s2_*API*_WebGate -gui
   Linux—./NetPoint7_0_linux_*API*_WebGate -gui

   Console Mode
   Windows—NetPoint7_0_Win32_*API*_WebGate.exe -console
   Solaris—./NetPoint7_0_sparc-s2_*API*_WebGate
   Linux—./NetPoint7_0_linux_*API*_WebGate

   where *API* refers to the API used by your Web server. For example ISAPI for IIS Web servers.

   On HP-UX and AIX systems, you can direct an installation to a directory with sufficient space using the -is:tempdir *path* parameter. The *path* must be an absolute path to a file system with sufficient space.
3. Dismiss the Welcome screen by clicking Next.
4. Accept the terms of the license agreement, then click Next.
5. Respond to the next question based upon your platform. For example:
   - **Windows**—If you are logged in with administrator rights, click Next (otherwise click Cancel, log in as a user with administrator privileges, then restart the installation).
   - **Unix**—Specify a dedicated username and group that the Web server will use, then click Next. Typically, the defaults are nobody.

     For HP-UX, the defaults are WWW (username) and others (group).

   You are asked to specify the installation directory for the WebGate. If you intend to use this WebGate to protect a WebPass installation, locate and select the WebPass installation directory.
6. Specify the installation directory for the WebGate.

   For example:

   \NetPoint_70\WebComponent\

7. **Language Pack**—Choose a Default Locale and any other Locales to install, then click Next. For example:
8. Record the installation directory name in the preparation worksheet if you haven't already, then click Next to continue.

   The WebGate is installed, which may take a few seconds. On Windows systems, a screen appears informing you that the Microsoft Managed Interfaces are being configured.

   The installation process is not yet complete. You are asked to specify a transport security mode. At this point, you cannot go back to restate information.

Specifying a Transport Security Mode

For details, see "Securing NetPoint Component Communications" on page 45.

To specify a transport security mode

1. Choose Open, Simple, or Cert for the WebGate.
2. Click Next.

   You are now asked to specify WebGate configuration details.

Specifying WebGate Configuration Details

It's a good idea to refer to the printed pages from your Access System Console as you complete the following procedure. During this sequence, you are asked to provide details about your WebGate and its associated Access Server.

To provide WebGate configuration details

1. Provide the information requested for the WebGate as specified in the Access System Console.
   - **WebGate ID**—The unique ID specified in the Access System Console
   - **WebGate password**—The password you defined in the Access System Console (if no password was entered, leave the field blank)
   - **Access Server ID**—The Access Server ID associated with this WebGate
   - **DNS hostname**—For the Access Server associated with this WebGate
   - **Port number**—On which the Access Server that listens for this WebGate

   Note: If you specified the Simple transport security mode, you are also asked for the Global Network Protocol pass phrase. If you specified Cert mode, you are asked for the password phrase.

2. Click Next to continue.

3. Perform the following operations according to the transport security mode you chose earlier:
   - **Open or Simple**—Skip to "Updating the WebGate Web Server Configuration" on page 211.
   - **Certificate**—Complete your certificate sequence, then continue with "Updating the WebGate Web Server Configuration" on page 211.

   If you requested certificates and they are not ready during this installation, be sure to copy them to the *WebGate_install_dir*\access\oblix\config directory and restart the WebGate when they arrive.

Important: The certificate request for WebGate generates the certificate-request file aaa_req.pem. You need to send this WebGate certificate request to a root CA that is trusted by the AAA server. The root CA returns the WebGate certificates, which can then be installed either during or after WebGate installation.

Updating the WebGate Web Server Configuration

Your Web server must be configured to operate with the WebGate. Oblix recommends automatically updating your Web server configuration during installation. However, procedures for both automatic and manual updates are included.

To automatically update your Web server configuration

1. Click Yes to automatically update your Web server, then click Next.
   - **Most Web servers**—Specify the absolute path of the directory containing the Web server configuration file.
   - **IIS Web Servers**—The process begins immediately and may take more than a minute.

   A screen announces that the Web server configuration has been updated.
2. **Sun Web Servers**—Be sure to apply the changes in the Web server Administration console *before* you continue.
3. **IIS Web Servers**—You may receive special instructions to perform *before* you continue.
4. Stop and restart your Web server to enable configuration updates to take affect.
5. Click Next and continue with "Finishing the WebGate Installation" on page 212.

To manually update your Web server configuration

1. Click No when asked if you want to proceed with the automatic update, then click Next.

   ReadMe information appears and a new screen also appears to assist you in manually setting up your Web server for the WebGate.

2. Return to the WebGate installation screen and click Next.
3. Continue with “Manually Configuring Your Web Server” on page 213.

Finishing the WebGate Installation

The ReadMe information provides details about documentation and Oblix.

To finish the WebGate installation

1. Review the ReadMe information, then click Next to dismiss it.
2. Click Finish to conclude the installation.
3. Restart your computer now or at a later time.
4. Continue with the appropriate procedures, as needed. For example:
   - “Manually Configuring Your Web Server” on page 213, if you did not do this automatically during installation.
   - “Installing postgate.dll on IIS Web Servers” on page 216
   - “Completing httpd.conf Updates” on page 219
5. Finish by “Confirming WebGate Installation” on page 220.

Installed Files

The subdirectories in Figure 10 were created under *WebGate_install_dir*\access, which is the directory you specified during installation. This WebGate was installed in the same directory as the WebPass and Access Manager.

Figure 10 *WebGate_install_dir*\access

Manually Configuring Your Web Server

During WebGate installation you are asked if you want to automatically update your Web server installation. If you selected No, you must do this manually.

Note: If the manual configuration process was launched during WebGate installation, you can skip the step 1 in the following procedure.

To manually configure your Web server for the WebGate

1. Launch your Web browser, and open the following file, if needed. For example:

   WebGate_install_dir\access\oblix\lang*langTag*\docs\config.htm

   where *WebGate_install_dir* is the directory where you installed the WebGate.

2. Select from the following supported Web servers.

Supported Server OS	Web Server					
	Microsoft IIS	ISA Server	Netscape Servers	Apache 1.3 and Apache1.3 -based Servers		
				Plain Apache	Apache with mod_ssl	IBM HTTP Servers
Windows Server 2003	ISAPI	ISAPI	NSAPI	-	-	-
Windows 2000	ISAPI	ISAPI	NSAPI	-	-	IHS-APACHE API
Windows NT	ISAPI	-	NSAPI	APACHE API	APACHE API	IHS-APACHE API
Sun Solaris	-	-	NSAPI	APACHE API	APACHE EAPI	IHS-APACHE API
AIX	-	-	NSAPI	APACHE API	APACHE EAPI	IHS-APACHE API
HP-UX	-	-	NSAPI	APACHE API	APACHE EAPI	-
Linux	-	-	-	APACHE API	APACHE EAPI	IHS-APACHE API

3. Follow all instructions that appear, which are specific to each Web server type, and:
   - Make a back up copy of any file that you are required to modify during Web server set up, so it is available if you need to start over.
   - Some setups launch a new browser window or require you to launch a Command window to input information, so ensure that you return to and complete all original setup instructions to enable your Web server to recognize the appropriate Oblix files.

     Note: If you accidentally closed the window, return to step 1 and click the appropriate link again.
4. Continue with one of the following, if needed:
   - "Completing IIS WebGate Installations" on page 214
   - "Completing httpd.conf Updates" on page 219

Completing IIS WebGate Installations

On IIS, if you are using client certificate authentication you must enable SSL on the IIS Web server hosting the WebGate before enabling client certificates for WebGate. You must also ensure that various filters are installed in a particular order. In addition, you may need to install the postgate.dll as an ISAPI filter.

Task overview: Completing IIS WebGate installations

1. "Enabling SSL on the IIS Web Server" on page 215
2. "Ordering the ISAPI Filters" on page 216
3. "Installing postgate.dll on IIS Web Servers" on page 216

Enabling SSL on the IIS Web Server

Use the following procedures as a guide, which reflects the sequence for IIS v5.

To enable SSL on the IIS Web server

1. Start the Internet Information Services console, if needed: Start > Programs > Administration Tools > Internet Information Services
2. Expand the local computer to display your Web Sites.
3. Expand the Default Web Site or the appropriate Web site, then expand \access\oblix\apps\webgate\bin.
4. Right click cert_authn.dll and select Properties.
5. Select the File Security tab in the Properties panel.
6. In the Secure Communications subpanel, click Edit.
7. In the Client Certificate Authentication subpanel, click Accept Certificates and click OK.
8. Click OK in the cert_authn.dll Properties panel.

If you select client certificate authentication during setup, you must also add the cert_authn.dll as one of the ISAPI filters.

To add cert_authn.dll as an ISAPI filter

1. Start the Internet Information Services console, if needed: Start > Programs > Administration Tools > Internet Information Services
2. Expand the local computer to display your Web Sites.
3. Right click the appropriate Web Site to display the Properties panel.
4. Click the ISAPI Filters tab, then click the Add button to display the Filter Properties panel.
5. Enter filter name “cert_authn”.
6. Click the Browse button and navigate to the following directory:

   WebGate_install_dir\access\oblix\apps\webgate\bin
7. Select cert_authn.dll as the executable.
8. Click OK on the Filter Properties panel.
9. Click Apply on the ISAPI Filters panel.
10. Click OK.
11. Ensure the filters are listed in the correct order.

Ordering the ISAPI Filters

It is important to ensure that the WebGate ISAPI filters are included in the right order.

To order the WebGate ISAPI filters

1. Start the Internet Information Services console, if needed: Start > Programs > Administration Tools > Internet Information Services
2. Expand the local computer to display your Web Sites.
3. Right-click the Web Site and select Properties.
4. Click Properties > ISAPI filters.
5. Confirm the following .dll files appear.

   For example:

   cert_authn.dll
   webgate.dll
   oblixlock.dll
   transfilter.dll

6. Add any missing filters, if needed, then select a filter name and use the up and down arrows to arrange the filter order as shown in step 5.

Important: Confirm that there is only one webgate.dll and one postgate.dll filter.

Installing postgate.dll on IIS Web Servers

Following WebGate installation, you may need to install the postgate.dll manually. POST data is required for pass through during a form login on the IIS Web server when using the WebGate extension method (where the WebGate is the action of the form). In other words, if a form authentication scheme on the IIS Web server is configured with the passthrough option, and the target of the login form requires the data posted by the form, the WebGate extension method (where the WebGate DLL is the action of the form) cannot be used. The WebGate filter method (where the action of the form is a protected URL that is not the WebGate DLL) must be used instead, and the postdate DLL must be installed and enabled.

POST data is used in an authorization decision that include rule parameters for the AzMan authorization plug-in. In this case, postgate.dll must be installed.

The following procedures presume that you are familiar with the IIS Web server commands. Two procedures are provided:

- “Setting Up IIS Web Server Isolation Mode” on page 217

- “Installing the Postgate ISAPI Filter” on page 217

Setting Up IIS Web Server Isolation Mode

On IIS 6 Web servers only, you must run the WWW service in IIS 5.0 isolation mode. This is required by the ISAPI postgate filter.

To set IIS 5.0 isolation on IIS 6 Web servers

1. Start the Internet Information Services console: Start > Programs > Administration Tools > Internet Information Services
2. Expand the local computer to display your Web Sites.
3. Right-click on the Web Site and select Properties.
4. Select the Service tab in the Web Site Properties window.
5. Check the box beside Run WWW service in IIS 5.0 Isolation Mode.
6. Click OK.

Installing the Postgate ISAPI Filter

If you perform multiple WebGate installations on one machine, multiple versions of the postgate.dll file may be created which may cause unusual NetPoint behavior.

There can only be one postgate.dll configured at the (top) Web Sites level of a machine. You may have multiple webgate.dlls configured at different levels below the top level Web Sites. However, they share the same postgate.dll. Install the filters in the order below:

- The ISAPI Webgate filter should be installed after the sspifitt filter and before any others.
- The postgate filter should be installed before the WebGate filter, only if needed.
- All other NetPoint filters can be installed at the end.

Note: Before installation (or after uninstallation) the filters must be removed manually. If multiple copies of a filter are installed, this means that they were not manually removed before installing the new filters.

The following procedures guide as you install and position the postgate ISAPI filter.

To install the postgate ISAPI filter

1. Start the Internet Information Services console: Start > Programs > Administration Tools > Internet Information Services
2. Expand the local computer to display your Web Sites.
3. Right-click on the Web Site and select Properties.
4. Select the ISAPI Filters tab in the Web Site Properties window.
5. Click the Add button to display the Filter Properties panel.
6. Enter the filter name “postgate”.
7. Click the Browse button and navigate to the following directory:

   WebGate_install_dir\access\oblix\apps\webgate\bin
8. Select postgate.dll as the executable.
9. Click OK on the Filter Properties panel.
10. Click Apply on the ISAPI Filters panel.

To restart IIS and reposition the postgate ISAPI filter

1. Start the Internet Information Services console, if needed.
2. Right-click your local computer, then select All Tasks > Restart IIS.
3. Select the ISAPI Filters tab on the Properties panel.
4. Select the postgate filter and move it above WebGate, using the up arrow.

   For example:

   postgate.dll
   webgate.dll
   oblixlock.dll
5. Restart IIS.

Completing httpd.conf Updates

You must complete the following procedure to update the Apache 1.3.27 httpd.conf file after you finish the WebGate installation and automatic Web server updates conclude.

To update the WebGate section in httpd.conf

1. Locate the updated httpd.conf file on the machine hosting the WebGate.
2. Ensure the section that loads WebGate in the httpd.conf file appears as shown next (tailored for your environment, which will differ from the example).

   For example:

```
#*** BEGIN Oblix NetPoint Specific ****
# The path to this library may need to be changed to suit your
installation
LoadFile
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity/oblix/lib/
libgcc_s.so.1"
LoadFile
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity/oblix/lib/
libstdc++.so.5"
<IfModule mod_ssl.c>
      ObWebGateInstalldir
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity"
      ObWebGateMode PEER
      Obwebgateload obWebgateModule
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity/oblix/apps/
webgate/bin/webgatessl.so"
</IfModule>
<IfModule !mod_ssl.c>
      ObWebGateInstalldir
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity"
      ObWebGateMode PEER
      Obwebgateload obWebgateModule
"/home/usr/sparc-s2/obdevsun1_wp_apache/identity/oblix/apps/
webgate/bin/webgate.so"
</IfModule>
<Location /access/oblix/apps/webgate/bin/webgate.cgi>
SetHandler obwebgateerr
</Location>
<Location "/oberr.cgi">
SetHandler obwebgateerr
</Location>
<LocationMatch "/*">
AuthType Oblix
require valid-user
</LocationMatch>
#*** END Oblix NetPoint Specific ****
```

3. Add the following lines only if you are using Solaris.

   You don't need them if you are using HP-UX.

```
 #LoadFile /usr/lib/libC.so.5
...
# WebGateInstalldir "/export/home/apache_test"
# WebGateMode "PEER"
```

Note: On HP-UX, do *not* use nobody for User or Group, as shared memory may not work. The workaround is to use your login name as User Name and Group is oblix, or www as User Name and others as Group Name. www on HP-UX is equivalent to nobody on Solaris.

---

4. Use the chmod -r username:groupname directory/file to change the User Name and Group Name of a directory or a file.

   When you do this, you need to change the User and Group parameters in the httpd.conf file accordingly.

Confirming WebGate Installation

After WebGate installation and Web server updates, you can enable WebGate diagnostics to confirm that your WebGate is running properly.

To enable WebGate diagnostics

1. Make sure your COREid Server, WebPass Web server, and Access Server are running.
2. Specify the following URL for WebGate diagnostics.

   For example:

   Most Web Servers—`http(s)://hostname:port/access/oblix/apps/webgate/bin/webgate.cgi?progid=1`

   IIS Web Servers—`http(s)://host:port/access/oblix/apps/webgate/bin/webgate.dll?progid=1`

   where *hostname* refers to the WebGate's hostname; *port* refers to the Web server instance port number.

The WebGate diagnostic page should appear. If it does not open, the WebGate is not functioning properly and should be uninstalled and reinstalled.

At this point, you are ready to:

- Configure NetPoint, as described in the *NetPoint 7.0 Administration Guide Volume 1* and *2*
- Customize NetPoint, as described in the *NetPoint 7.0 Customization Guide*

- Perform integrations, as described in the *NetPoint Integration Guide*.

Section IV: Language Packs and Monitoring Tools Installation

9 Installing a Language Pack Independently

This chapter describes how to add an optional Language Pack after installing and setting up NetPoint components. Topics include:

For details about configuring NetPoint for additional languages after Language Pack installation, see the *NetPoint 7.0 Administration Guide Volume 1*.

About Language Packs and Installation

NetPoint provides the capability to localize NetPoint applications to display static data such as error messages and display names for tabs, panels, and attributes to users in their native language. The default language for NetPoint is English, which requires no special installation or configuration.

When you have more then one language installed and enabled, a Select Language drop-down list is available in the upper-right corner of the COREid System Console and Access System Console. From this list, you can choose which the language in which to display the page.

Note: NetPoint supports UTF8 data but not multi-byte languages such as Chinese, Japanese, and so on. Contact Oblix for information about specific Language Packs.

For each language that Oblix supports, one Language Pack installer is provided for the COREid System and one is provided for the Access System. Language Packs can be installed together with NetPoint components, as described in other chapters. However you may also install a Language Pack independently, after NetPoint installation and setup, as discussed in this chapter.

As discussed in "Installing Optional Language Packs" on page 30, the installation directory you specify for the Language Pack must match the installation directory of the component with which it is to operate. For example:

\COREid_install_dir
\WebPass_install_dir

\AccessManager_install_dir
\AccessServer_install_dir
\WebGate_install_dir

During installation, a *langTag* directory is created in the filesystem under the main NetPoint component's installation directory. For example, *Component_install_dir*\identity|access\oblix\lang*langTag*, where *langTag* represents specific language, such as en-us or fr-fr. See "Installed Files" on page 230 for an example.

A language entry is created for each installed language under the Oblix node in the LDAP directory as follows: obid=*langTag*, *configDN*, where *configDN* is the configuration DN in the directory.

The obnls.lst configuration file is updated. For example, *Component_install_dir*\identity|access\oblix\config\obnls.lst. In the sample obnls.lst file below, English is the only language:

```
BEGIN:vCompoundList

default:en-us

languages:
BEGIN:vList
en-us
END:vList

en-us:
BEGIN:vNameList

#
# Relative to <INSTALLDIR>
#

sortRulesFile:
#obDateSep:-
#obDateType:ObMDYDate
#
# For future use;
#

dirPath:en-us
```

```
END:vNameList
END:vCompoundList
```

Task overview: Installing a Language Pack independently

1. Run the COREid System Language Pack installer, as described in “Installing the Language Pack Independently” on page 228, on each machine hosting an installed COREid Server and an installed WebPass.
2. Confirm that the languages you installed are enabled, as described in “Confirming Language Status” on page 231.
3. Run the Access System Language Pack installer, as described in “Installing the Language Pack Independently” on page 228, on each machine hosting an installed Access Manager, Access Server, and WebGate.

   Even though there are no user interfaces for the Access Server and WebGate, you need to install the same Language Packs for these components as you do for others.
4. Confirm that the languages you installed are enabled, as described in “Confirming Language Status” on page 231.

Language Pack Installation Considerations

Installing additional languages to enable multi-language functionality in NetPoint may be done either during or after installation of each NetPoint component.

You do not need to install a Language Pack on any WebGate that resides in the same directory as an Access Manager for which a Language Pack has been installed.

On Unix systems, you must ensure that the Language Pack has execute permissions before launching the installer. For example:

chmod +x “NetPoint7_0_FR_sparc-s2_LP_Access_System”

If you prefer to install the Language Pack silently while installing each NetPoint component, the Language Pack installer must reside in the same temporary directory as the NetPoint component installer. See individual installation chapters in this guide for more information.

Language Pack Prerequisites Checklist

Before you begin installing the Language Pack, check the tasks in Table 32 to ensure they have been completed. Failure to complete prerequisites may adversely affect your NetPoint installation.

Table 32 Language Pack Installation Prerequisites Checklist

Checklist	Language Pack Installation Prerequisites
	Install the COREid System, as described in “Section II: COREid System Installation and Setup” on page 97.
	Install the Access System, as described in “Section III: Access System Installation and Setup” on page 157.
	On Unix systems, ensure that the Language Pack has execute permissions before launching the installer.

To install a Language Pack at the same time as the NetPoint component, move any Language Pack installation packages into the same directory as the NetPoint component installation package and refer to the appropriate chapter in this guide.

Installing the Language Pack Independently

This procedure walks you through adding a Language Pack independently, after NetPoint component installation and setup.

To complete a Language Pack installation

1. Log in as a user with Administrator privileges.
2. Locate and launch the installation package for the desired Language Pack and NetPoint component and launch the installer.

   For example:

   - **GUI Mode—Windows**
     NetPoint7_0_win32_*langTag*_COREidSystem.exe
     NetPoint7_0_win32_*langTag*_AccessSystem.exe
   - **GUI Mode—Unix**
     ./NetPoint7_0_sparc-s2_*langTag*_COREidSystem -gui
     ./NetPoint7_0_sparc-s2_*langTag*_AccessSystem -gui
   - **Console Mode—Windows**
     NetPoint7_0_win32_*langTag*_COREidSystem.exe -console
     NetPoint7_0_win32_*langTag*_AccessSystem.exe -console

- **Console Mode—Unix**
  ./NetPoint7_0_sparc-s2_*langTag*_COREidSystem
  ./NetPoint7_0_sparc-s2_*langTag*_AccessSystem

where *langTag* refers to a specific language tag, such as FR (French).

The Welcome screen appears.

3. Click Next to dismiss the Welcome screen.
4. Accept the license agreement terms, then click Next to continue.
5. Respond to the next question based on your platform:
   - **Windows**—If you are logged in with administrator rights, click Next (otherwise click Cancel, log in as a user with administrator privileges, then restart the installation).
   - **Unix**—Specify the username and group of the dedicated owner, if asked, then click Next.

     For HP-UX, the defaults are WWW (username) and others (group).
6. Change the destination directory to match the main component for which this is being installed, then click Next.

   For example:

   COREid_install_dir
   WebPass_install_dir

   AccessManager_install_dir
   AccessServer_install_dir
   WebGate_install_dir

   You are informed that the Language Pack is being installed, which may take a few seconds. ReadMe information appears next.
7. Review the ReadMe information, then click Next to dismiss it.

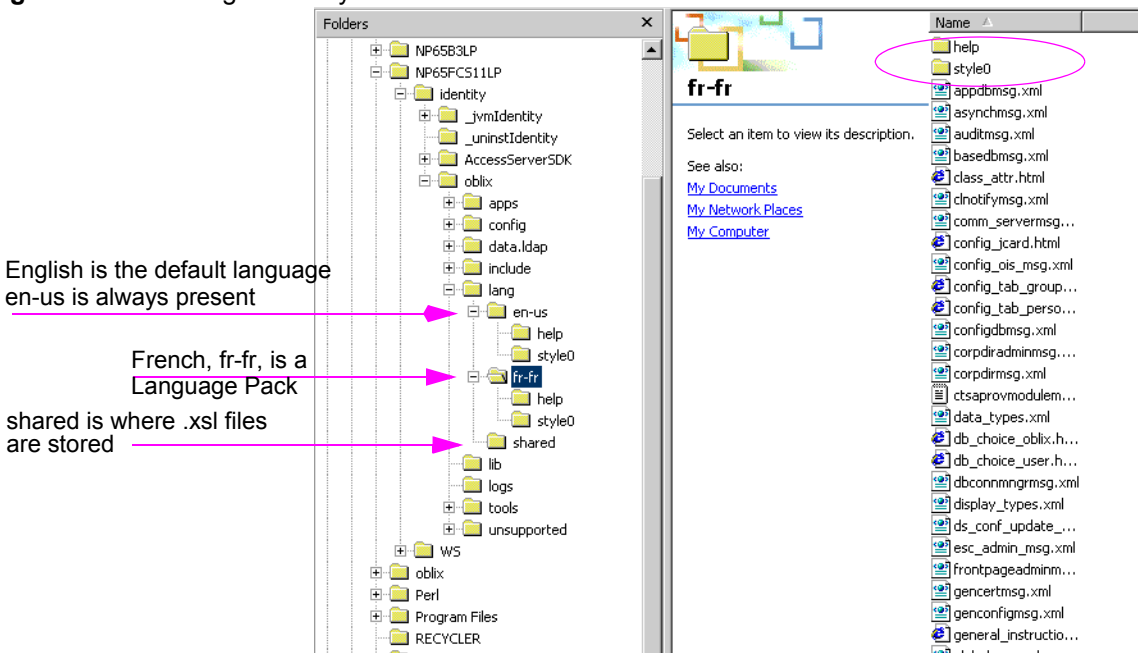
   A summary screen appears.
8. Click Finish to complete this installation.
9. Restart the service for which you just installed the Language Pack.
10. Repeat the Language Pack installation for:
    - All WebPass components, using the COREid System Language Pack
    - All Access System components, using the Access System Language Pack
      - Access Managers
      - Access Servers
      - WebGates that do not reside in the same directory as an Access Manager

11. Confirm language status, as described in “Confirming Language Status” on page 231.

Installed Files

The \lang directory and the \lang\en-us and \lang\shared subdirectories are included with all NetPoint installations. When you install additional languages, a *langTag* subdirectory is created under \lang. For example, Figure 11 shows both English and French subdirectories. On the right, you can see the content of the French language subdirectory. It includes the same type of content as \en-us, only localized.

Figure 11 Lang Directory and Subdirectories



Confirming Language Status

Use the procedure below to confirm which languages are installed and enabled within NetPoint.

To confirm which languages are enabled

1. Navigate to the COREid System Console, as usual.

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

   where *hostname* refers to 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.

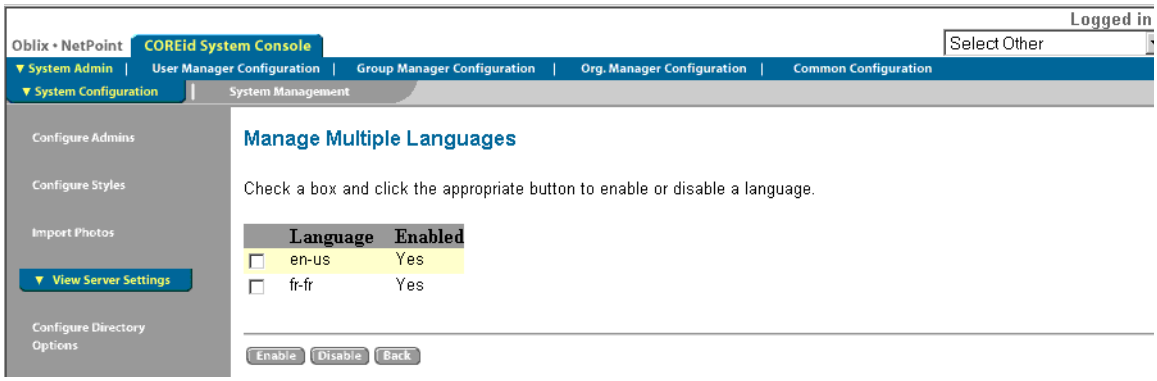
2. Navigate to the View Server Settings page by selecting COREid System Console > System Admin > System Configuration > View Server Settings.

3. Click the Multi-Language link at the bottom of the page. For example:

   The Manage Multiple Languages page appears showing which languages are currently installed and which are enabled. You complete step 4 to enable a language. Otherwise, skip to step 6.

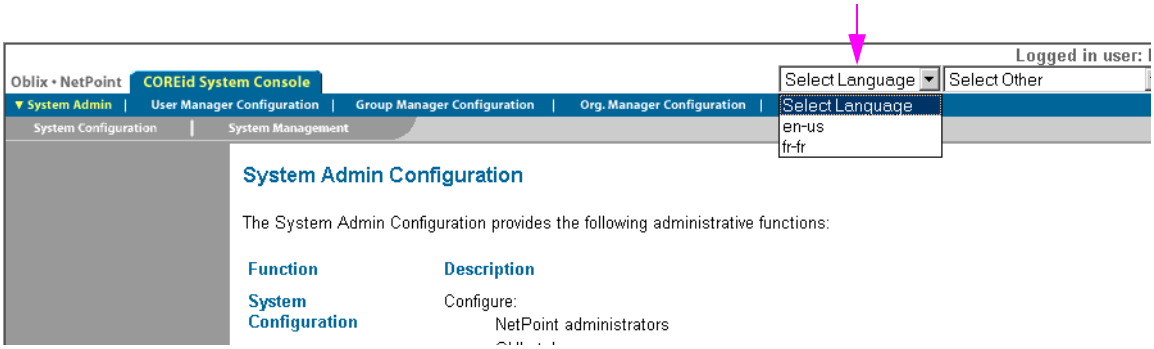
4. Click the box beside the language you want to enable, then click the Enable button.



5. Refresh the browser screen or reopen the browser.

   If you have installed and configured more than one language, the Select Language drop-down list is displayed at the top of the System Console page both here and in the Access System Console. From the drop-down list, you can choose a different language in which to display the NetPoint Administration Console and NetPoint applications.

6. Locate the Select Language drop-down list in the upper right corner of the System Console.



7. Refer to the *NetPoint 7.0 Administration Guide Volume 1* for more information about setting language preferences and localizing NetPoint information.

10 Installing the SNMP Agent

This chapter describes how to install the Simple Network Management Protocol (SNMP) Agent that enables you to monitor the activity of different components on your network. See:

- "About the SNMP Agent and Installation" on page 233
- "SNMP Agent Installation Considerations" on page 234
- "SNMP Installation Prerequisites Checklist" on page 234
- "Installing the SNMP Agent" on page 234

For details about configuring the SNMP agent after installation, see the *NetPoint 7.0 Administration Guide Volume 1*.

About the SNMP Agent and Installation

NetPoint provides data that can be used by SNMP and a Network Management System (NMS), which enables you to monitor the status and activity of the COREid and Access Servers.

The NetPoint SNMP Agent is an optional component. If installed, the SNMP Agent accesses information about the COREid or Access Server resident on the same server host on which the agent was installed. The installation process for the SNMP Agent is similar to other NetPoint components. The installation directory is shown below:

Default on Windows—\Program Files\NetPointSnmpAgent\snmp
Default on Unix—/opt/NetPointSnmpAgent\snmp
In This Guide—*SNMP_install_dir*\snmp

SNMP Agent Installation Considerations

The NetPoint SNMP Agent must be installed on the same machine as the NetPoint server that it is going to service: COREid Server or Access Server. The NetPoint SNMP Agent should run as the same user as the COREid Server or Access Server.

You need a community name for NetPoint SNMP data in your network management station (NMS) host.You also need to configure trap destinations for NetPoint SNMP traps in your NMS host.

The SNMP Agent needs to be owned by a dedicated user. On Unix, only root or the dedicated user may be able to start the agent service. Most of the time the agent is run as “root” or “nobody”. On Unix, you also enter a group to which the user belongs.

SNMP Installation Prerequisites Checklist

Table 33 provides a checklist of items that must be completed before you install the SNMP Agent with NetPoint.

Table 33 SNMP Agent

	Install and setup the COREid System, as described in “Section II: COREid System Installation and Setup” on page 97.
	Install and setup the Access System, as described in “Section III: Access System Installation and Setup” on page 157.
	Create a Community Name for NetPoint SNMP data in your network management station (NMS) host.
	Configure trap destinations for NetPoint SNMP traps in your NMS host.

Installing the SNMP Agent

The following discussions explain how to install the SNMP agent.

- “Starting the Installation” on page 235
- “Installing the SNMP Agent” on page 234
- “Specifying SNMP Agent Configuration Details” on page 236
- “Finishing the Installation” on page 237

Starting the Installation

The installation is similar to other NetPoint components with differences specific to the SNMP Agent.

To install the SNMP Agent

1. Log in as a user with Administrator privileges.
2. Locate and launch the component installer in a temporary directory created when you downloaded the software.

   For example:

   - **GUI Mode**
     Windows—NetPoint7_0_win32_Snmp_Agent.exe
     Unix—./NetPoint7_0_sparc-s2_Snmp_Agent -gui
   - **Console Mode**
     Unix—./NetPoint7_0_sparc-s2_Snmp_Agent
     Windows Command Window—
     NetPoint7_0_win32_Snmp_Agent.exe -console

   The Welcome dialog appears.
3. Click Next to dismiss the Welcome screen.
4. Accept the terms of the license agreement, then click Next to continue.
5. Respond to the next question based upon your platform. For example:
   - **Windows**—If you are logged in with administrator rights, click Next (otherwise click Cancel, log in as a user with administrator privileges, then restart the installation).
   - **Unix**—Specify the username that the SNMP Agent will use, click Next, specify the group that the SNMP agent will use, then click Next.

     For HP-UX, the defaults are WWW (username) and others (group).
6. Specify the installation directory, then click Next).

   For example:

   \NetPoint_70SnmpAgent

   A summary of the installation directory and required disk space appears.
7. Record the installation directory and click Next.

   The SNMP Agent is installed, which may take a few seconds. On Windows systems, a screen appears informing you that the Microsoft Managed Interfaces are being configured.
8. **Windows—**Enter the following information to distinguish this SNMP Agent in the Windows Service window, then click Next. For example:

- **Windows service name—**A unique name for this SNMP Agent.

  For example, if you provide the name SNMP_70_1, the name in the Service window will appear as NetPoint SNMP Agent (SNMP_70_1).

- **Account name—**DomainName\UserName for this SNMP Agent (the default is LocalSystem).

- **Password—**The password for this account.

Next, you are asked to define specific details for this SNMP Agent.

Specifying SNMP Agent Configuration Details

During this sequence, you will enter the port and community information for this SNMP Agent.

To specify SNMP Agent details

1. Enter the SNMP Agent TCP port that NetPoint will use to publish SNMP statistics.

   For example:

   6012

   This is the same port number that you specify when enabling the SNMP agent from the NetPoint server. NetPoint components will communicate with this port to publish their statistics to your Manager Station.

   Next, you are asked for the UDP port and the Community Name defined in your Network Management System, which you will use to query this SNMP Agent. These should be same as those used by your Network Manager Station to query this SNMP Agent.

2. Enter the SNMP Agent UDP port and community name, then click next.

   For example:

   - **SNMP Agent UDP port—***161*
   - **Community Name—Your***Community*

   Now you are asked to enter the network monitor station name and trap port from your Network Management System, which the NetPoint SNMP Agent should use when sending SNMP traps. The trap port is the port that will receive NetPoint SNMP traps.

3. Enter the following information, then click Next.

   For example:

   - **Manager Station name—Your_***Station_Name*

- **Trap port—***162*

You now need to specify whether you want to configure another Manager Station for this NetPoint SNMP Agent.

4. Click Yes to indicate that you want to configure another Manager Station now (otherwise, click No), then click Next.

   - If Yes, you will be asked to repeat step 3 for the new station, then you will be asked if you want to configure another station.
   - If No, you may manually configure another Manager Station using the following tool later: *SNMP_install_dir*\snmp\tools\setup\setup_agent.

   A confirmation dialog appears.

Finishing the Installation

The installation concludes as other NetPoint component installations have.

To finish the installation

1. Review the ReadMe information, then click Next.

   A summary screen appears.

2. Write the details of this installation on the preparation worksheets, if you have not yet done so, then click Next to finish the installation.

You are ready to configure the SNMP Agent, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

Section V: Replication

11 Replicating Components

Rather than using the command line or the installation GUI to install a NetPoint component, you can automate the installation process by replicating the configuration of one installed component to another. You do this by installing from an options file or by cloning an installed component. You can also partially replicate a component by synchronizing two installed components.

This chapter describes installation using an options file, cloning, and synchronization. It covers the following topics:

About the Silent Mode Options File

In addition to installing NetPoint from a GUI or the console, you can perform an automated installation using a file that contains installation parameters and values. This is called installing in *silent mode*. Silent mode permits installation without user intervention.

Important: Silent mode is intended for new NetPoint installations only, not for migrations or upgrades. For details about ADAM and silent installation, see "NetPoint Silent Mode Installation Parameters" on page 426.

You perform silent mode installations using an options file. When you install a NetPoint component, the installation program automatically creates a file named install_options.txt. This file is written to the installation directory for the component. The general path is:

/*Component_install_dir*/identity|access/oblix/config/install_options.txt

Component_install_dir is the top-level directory in the path and identity|access represents the suffix for the respective NetPoint component,. For example:

/NetPoint/identity/oblix/config/install_options.txt

Your installation session is recorded in the installation options file. This file contains information about the prompts you received and the values that you supplied during installation. You can use this file as a template for future installations, changing parameter values as needed.

You need to edit the file if you re-entered any values during installation. The entire installation session is recorded in this file, so you may need to delete information if you input data several times for the same option. You also need to edit this file to change parameter values for the new installation. For COREid Server and WebPass, you at least need to specify a unique ID for the new component. Passwords entered during installation are not stored for security reasons.

Additional Uses of the Silent Mode Options File

The silent mode options file can also be used to provide default values for an interactive installation. This is useful if you want to provide default values for installing multiple instances of a NetPoint component. To provide default values for an installation, follow the instructions in this chapter with the following exceptions:

- Remove any parameters and values from the options file that have no defaults, such as password values.
- Invoke the installation program without the -silent option described next.

Running the Silent Mode Options File

The procedure to run the silent mode options file follows.

Note: Silent mode is intended for new NetPoint installations only, not for migrations or upgrades.

To install new components in silent mode

1. Make a copy of the original options file if you have not already done so.
2. Run NetPoint 7.0 installation from the command prompt using the following options:

   -options *path_to_install_options.txt* -silent

   where *path_to_install_options.txt* is the location of the silent mode options file.You must include the file name in the path. The file name does not have to be install_options.txt.

   Note: To suppress the installation dialog box, add the –is:silent option to this command.

Selecting an Installation Directory on HP-UX and AIX

To direct an installation to a directory with sufficient space, you can use the -is:tempdir path parameter. The path must be an absolute path, to a file system with sufficient space.

Inputting Installation Passwords

You must supply a password at the command line or edit the silent mode options file and store the password there. If you do not supply a password, the installation will fail. Here is an example of entering the password using the command line:

installer -is:silent -silent -options *path_to install_options.txt* -W oblixDSinfoBean.dsPassword=*Your_Password*

where *path_to_install_options.txt* is the location of the silent mode options file.

Editing the Silent Mode Options File

You can find the options file in the following location:

/*Component_install_dir*/identity|access/oblix/config/install_options.txt

where *Component_install_dir* is the top-level directory in the path and identity|access represents the component type.

You need to copy the options file and edit the copy to match your environment, using the following guidelines:

- Parameters and values are case-sensitive
- All values should be enclosed in quotes

See the following examples:

- "Sample COREid Options File" on page 244
- "Sample Access Server Options Files" on page 244

Sample COREid Options File

An example of a COREid options file is shown in Figure 16.

Note: By default, the password field is commented out and a password is not provided when the silent mode options file is first created. Edit the password field if you want to insert a password. Delete the "#" and enter the correct password.

Sample Access Server Options Files

Several examples are presented here:

- "Sample: Same directory server" on page 245
- "Sample: Separate directory servers" on page 246
- "Sample: Separate directory servers with SSL enabled for user data" on page 247
- "Sample: Separate directory servers with SSL enabled for policies" on page 248

Sample: Same directory server

An example of an Access Server options file is shown in Figure 12. In this example, the Oblix configuration and policy data are stored in the same directory server.

Figure 12 Access Server Options File, Same Directory Server

```
# Log file for this installation is located at C:\DOC\AMIT\LOCAL\Temp/aaa.log
-P aaa.installLocation="C:\NetPoint\access"
-W securityModeBean.securityModeChoices="open"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsType="NCSP10"
-W oblixDSInfoBean.dsMode="open"
-W oblixDSInfoBean.dsHostMachine="marinello"
-W oblixDSInfoBean.dsPortNumber="999"
-W oblixDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsPassword="mypassword"
-W policyDataInWhichDSBean.askPolicyDataInWhichDS="OBLIX"
-W aaaInfoBean.accessServerID="aaa"
-W aaaInfoBean.policyDataConfigDN="o=company,c=us"
-W aaaInfoBean.policyDSBase="o=company,c=us"
```

Sample: Separate directory servers

In this example of an Access Server options file, the Oblix and policy data are stored in separate directory servers. See Figure 13.

Figure 13 Access Server Options File, Configuration and Policy Data in Separate Directories

```
# Log file for this installation is located at C:\DOC\AMIT\LOCAL\Temp/aaa.log
-P aaa.installLocation="C:\NetPoint\access"
-W securityModeBean.securityModeChoices="open"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsType="NCSP10"
-W oblixDSInfoBean.dsMode="open"
-W oblixDSInfoBean.dsHostMachine="marinello"
-W oblixDSInfoBean.dsPortNumber="999"
-W oblixDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsPassword="mypassword"
-W policyDataInWhichDSBean.askPolicyDataInWhichDS="POLICY"
-W policyDSInfoBean.dsMode="open"
-W policyDSInfoBean.dsHostMachine="marinello"
-W policyDSInfoBean.dsPortNumber="999"
-W policyDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W policyDSInfoBean.dsPassword="mypassword"
-W aaaInfoBean.accessServerID="aaa"
-W aaaInfoBean.policyDataConfigDN="o=company,c=us"
-W aaaInfoBean.policyDSBase=o=company,c=us"
```

Sample: Separate directory servers with SSL enabled for user data

In this example of an Access Server options file, Figure 14, the oblix and policy data are stored in separate directory servers and the user directory server is operating in SSL mode.

Figure 14 Access Server Options with Separate Directory Servers with SSL-Enabled

```
# Log file for this installation is located at C:\DOC\AMIT\LOCAL\Temp/aaa.log
-P aaa.installLocation="C:\NetPoint\access"
-W securityModeBean.securityModeChoices="open"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsType="NCSP10"
-W oblixDSInfoBean.dsMode="open"
-W oblixDSInfoBean.dsHostMachine="marinello"
-W oblixDSInfoBean.dsPortNumber="999"
-W oblixDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsPassword="mypassword"
-W policyDataInWhichDSBean.askPolicyDataInWhichDS="POLICY"
-W policyDSInfoBean.dsMode="open"
-W policyDSInfoBean.dsHostMachine="marinello"
-W oblixDSInfoBean.dsPortNumber="999"
-W policyDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W policyDSInfoBean.dsPassword="mypassword"
-W aaaInfoBean.accessServerID="aaa"
-W aaaInfoBean.policyDataConfigDN="o=company,c=us"
-W aaaInfoBean.policyDSBase=o=company,c=us"
-W userDSSSLCertPath.sslCertPath="C:\Cert\ca.cert"
```

Sample: Separate directory servers with SSL enabled for policies

In this example of an Access Server options file, Figure 15, the oblix and policy data are stored in separate directory servers and the policy directory server is operating in SSL mode.

Figure 15 Access Server Options, Separate Configuration and Policy Data, SSL-Enabled

```
# Log file for this installation is located at C:\DOC\AMIT\LOCAL\Temp/aaa.log
-P aaa.installLocation="C:\NetPoint\access"
-W securityModeBean.securityModeChoices="open"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsType="NCSP10"
-W oblixDSInfoBean.dsMode="open"
-W oblixDSInfoBean.dsHostMachine="marinello"
-W oblixDSInfoBean.dsPortNumber="999"
-W oblixDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W oblixDSInfoBean.dsPassword="mypassword"
-W policyDataInWhichDSBean.askPolicyDataInWhichDS="POLICY"
-W policyDSInfoBean.dsMode="ssl"
-W policyDSInfoBean.dsHostMachine="marinello"
-W policyDSInfoBean.dsPortNumber="333"
-W policyDSInfoBean.dsBindDN="cn=administrator"
# The following are recommended to be entered as command line arguments.
-W policyDSInfoBean.dsPassword="mypassword"
-W userDSSSLCertPath.sslCertPath="C:\Cert\ca.cert"
-W aaaInfoBean.accessServerID="aaa"
-W aaaInfoBean.policyDataConfigDN="o=company,c=us"
-W aaaInfoBean.policyDSBase=o=company,c=us"
```

Sample: COREid Server Installation using Active Directory

In this example of a COREid Server options file, Figure 16, the installation is being done on Active Directory.

Figure 16 COREid Server Installation Options using Active Directory

```
# Log file for this installation is located at
C:\DOCUME~1\ADMINI~1\Temp/COREid.log
-P ois.installLocation="D:\test\adsi\ois\identity"
-W secruityModeBean.securityModeChoices="open"
-WoisInfoBean.hostName="test001"
-W oisInfoBean.serverID="test002"
-W oisInfoBean.portNumber="9002"
-W askFirstIdentityServer.askFirstIdentityServerField="n"
-W askSSLSetup.askSSLSetupField="No"
-W askADSI.isADSI="yes"
-W askUseImplicitBind.useImplicitBind="yes"
-W askNTServiceName.netServiceNameField="testcoreidad"
-W askNTServiceAccount.ntServiceUserAccount=".\Administrator"
# The following is recommended to be entered as a command line argument
# -W askNTServiceAccount.netServiceUserPassword=<your password>
```

Silent Mode Parameters

The following discussions describe options you may edit in the silent installation options file for each NetPoint 7.0 component. Anything shown in *italics* is a value you supply for a parameter. You must supply a value for each parameter in the file. Enclose all values in double quotes.

For details on installation prompts and their values, refer to the other chapters in this installation guide. For example, see "Installing the COREid Server" on page 105 for information on COREid installation prompts and values.

The following sections are sequenced in the recommended order for installing NetPoint components. The parameters are listed in the same order that they appear in the installation GUI.

Note: When installing a component, you may not need to supply every parameter. You need only supply values for parameters that apply to your installation.

COREid Server Parameters

Table 34 describes silent installation parameters for the COREid Server.

Table 34 Silent Installation Parameters for the COREid Server

COREid Parameter and Description	Possible Values
-P ois.installLocation—The installation directory. The default directory is "C:\NetPoint" on Windows and "/NetPoint" on Unix.	"*installation directory*"
-W userInfoBean.user—Unix only. The user ID that the product will be running as.	"*user ID*"
-W userInfoBean.group—Unix only. The group that corresponds to the userInfoBean.user.	"*group id*"
-W localePanel.defaultLang—Required when extra languages are to be installed with the main installation.	"en-us"
-W localePanel.installLanguages—Required when extra languages are to be installed with the main installation.	"en-us;fr-fr"
-W securityModeBean.securityModeChoices—Security mode for the COREid Server. A value of "open" means no security is used, a value of "simple" means encryption is used, and a value of "cert" means you are running your own CA.	"open", "simple", "cert"
-W oisInfoBean.hostName—Host name where COREid Server is installed.	"*ip address*" or "*hostname*"
-W oisInfoBean.serverID—COREid Server ID. This is a unique ID that you create.	"*server id*"
-W oisInfoBean.portNumber—Port number of the COREid Server. This port number cannot be used by another instance on the same machine.	"*port number*"
-W askFirstIdentityServer.askFirstIdentityServerField—This parameter specifies whether this is the first COREid Server being installed. The value “y” means yes, this is the first COREid Server installed, “n” means no.	"y" or "n"
-W askSSLSetup.askSSLSetupField—This parameter specifies whether to set up SSL between the COREid Server and the directory server.	"Yes" or "No"
-W askSSLCertPath.sslCertPath—The absolute path to the SSL certificate. Use only if "askSSLSetup.askSSLSetupField" = "Yes".	"*absolute path including the file name*"

Table 34 Silent Installation Parameters for the COREid Server

COREid Parameter and Description	Possible Values
-W simpleModeBean.passphrase—This parameter is used if you are using the Simple transport security mode. This is a pass phrase allowing the COREid Server to communicate with the WebPass. Use only if "securityModeBean.securityModeChoices" = "simple".	"*passphrase*"
-W simpleModeBean.passphraseVerify—This parameter is used if you are using the Simple transport security mode. This parameter verifies that the pass phrase matches that of simpleModeBean.passphrase. Use only if securityModeBean.securityModeChoices = "simple".	"*passphrase*"
-W certModeBean.passphrase—This parameter is used if you are using the Cert transport security mode. This is a pass phrase allowing the COREid Server to communicate with the WebPass. Use only if securityModeBean.securityModeChoices = "cert".	"*passphrase*"
-W certModeBean.passphraseVerify—This parameter is used if you are using the Cert transport security mode. This parameter verifies that the pass phrase matches that of certModeBean.passphrase. Use only if securityModeBean.securityModeChoices = "cert".	"*passphrase*"
-W installOrRequestCertBean.installOrRequest—Determines whether to install or request a certificate to be used to configure the COREid system. Used if your security mode is set to "cert". If you already have a certificate, use "install". If you want NetPoint to request a certificate, use "request".	"request" or "install"
-W certReqInfoBean.countryName—Country name. This is a two-letter country code that is valid for use in a DN. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*country code*"
-W certReqInfoBean.stateOrProvinceName—State or province name. This is a two-letter state or province code. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request"	"*state or province code*"
-W certReqInfoBean.localityName—Locality name. This is usually the name of a geographic region. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request"	"*locality name*"
-W certReqInfoBean.organizationName— Organization name. This is usually the name of an organization. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*organization name*"
-W certReqInfoBean.organizationalUnitName—Organizational unit name. This is usually the name of a department. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*organization unit name*"

Table 34 Silent Installation Parameters for the COREid Server

COREid Parameter and Description	Possible Values
-W certReqInfoBean.commonName—Common name. This is usually the name of a person or entity. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*name*"
-W certReqInfoBean.emailAddress—Email address. This is usually a valid email address. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*email address*"
-W readyToInstallCertBean.readyToInstallField—If you requested that NetPoint request a certificate, this verifies that the certificate is ready for installation. Only use if installOrRequestCertBean.installOrRequest = "request". Oblix recommends that you use a value of "No" for silent mode. It is unlikely that you can take the request generated by NetPoint and receive the certificate faster than the NetPoint installation script can run from one step to the next.	"Yes" or "No"
-W copyCertificatesInputBean.certFile—A certificate is composed of three files: a certificate file, a key file, and a chain file. This parameter specifies the absolute path, including the file name for the certificate file (for example: ois_cert.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	"*absolute path including the file name*"
-W copyCertificatesInputBean.keyFile—A certificate is composed of three files: a certificate file, a key file, and a chain file. This parameter specifies the absolute path including the file name for the key file (for example: ois_key.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	"*absolute path including the file name*"
-W copyCertificatesInputBean.chainFile—A certificate is composed of three files: a certificate file, a key file, and a chain file. This parameter specifies the absolute path including the file name for the chain file (for example: ois_chain.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	"*absolute path including the file name*"
-W updateDSInfo.updateDSInfoChoice—Determines whether to automatically update the Oblix and User schemas. Used only if askFirstIdentityServer.askFirstIdentityServeField= "y". "YesOneDS" performs an automatic update. Oblix and User directory server are the same. "YesTwoDS" performs an automatic update. Oblix and User directory servers are separate. "No" does not perform an automatic update.	"YesOneDS", "YesTwoDS", "No"

Table 34 Silent Installation Parameters for the COREid Server

COREid Parameter and Description	Possible Values
-W dsTypeInput.dsType—Use this parameter if NetPoint is automatically updating the Oblix and User schemas (that is, if updateDSInfo.updateDSInfoChoice = "YesOneDS" or "YesTwoDS"). User directory server Types are: 1 - Sun Directory Server 5.x 2 - NDS 3 - Active Directory 4 - ADSI (Schema will be uploaded using LDAP) 5 - Active Directory on Windows Server 2003 6 - ADSI on Windows Server 2003 7 - Active Directory Application Mode (On Windows 2003 Only) 8 - Siemens DirX 9 - IBM Directory Server 10 - COREid Data Anywhere **Note:** COREid Data Anywhere may be used with *user* data only and requires integration with OctetString Virtual Directory Engine (VDE), as described in the *NetPoint Integration Guide*. The LDAP directory branches containing NetPoint configuration (and policy) data must reside on one or more directory servers other than the one hosting VDE or user data. **Also Note**: When the directory server type for user data differs from the directory server type for configuration data, use the following to specify the directory server type for configuration data: -W dsTypeInput1.dsType=#.	“1”, "2", "3", “4”, "5",”6”, “7”, “8”, “9”, “10”
-W dsUserDynAuxClassInput.dynamicAuxiliary—Set this parameter to "y" if you want to support dynamic auxiliary classes with Active Directory. Use only if you have set -W dsTypeInput.dsType to "5" or "7".	"y" or "n"
-W dsInfoInput.dsName—For most directory types, this is the User directory server host name. For Active Directory, use the Schema Master host name. Use only if updateDSInfo.updateDSInfoChoice = "YesOneDS" or "YesTwoDS".	"*ip address*" or "*hostname*"
-W dsInfoInput.dsName—For most directory types, this is the User directory server host name. For Active Directory, use the Schema Master host name. Use only if updateDSInfo.updateDSInfoChoice = "YesOneDS" or "YesTwoDS".	"*ip address*" or "*hostname*"
-W dsInfoInput.dsPortNumber—For most directory types, this is the User directory server port number. For Active Directory, use the Schema Master port number. Use only if updateDSInfo.updateDSInfoChoice = "YesOneDS" or "YesTwoDS".	"*port number*"
-W dsInfoInput.bindDN—For most directory types, this is the DN used to authenticate to the User directory server. For Active Directory, use the Schema Master bind DN. Use only if updateDSInfo.updateDSInfoChoice = "YesOneDS" or "YesTwoDS". Enter this value using valid DN syntax, for example, "cn=User Directory, o=Oblix".	"*bind DN*"

Table 34 Silent Installation Parameters for the COREid Server

COREid Parameter and Description	Possible Values
-W dsInfoInput.password—For most directory types, this is the User directory server password. For Active Directory, use the Schema Master password. Use only if updateDSInfo.updateDSInfoChoice = "YesOneDS" or "YesTwoDS". See the note in “Running the Silent Mode Options File” on page 243 regarding secure password input.	"*password*"
-W dsOblixInfoInput.dsName—Oblix directory server name. Use only if Oblix and User directory servers are separate and you are not using NDS or Active Directory, that is: updateDSInfo.updateDSInfoChoice = "YesTwoDS" and dsTypeInput.dsType does not equal to "2" or "3".	
-W dsOblixInfoInput.dsPortNumber—Oblix directory server port number. Use only if Oblix and User directory servers are separate and you are not using NDS or Active Directory, that is: updateDSInfo.updateDSInfoChoice = "YesTwoDS" and dsTypeInput.dsType does not equal to "2" or "3".	"*port number*"
-W dsOblixInfoInput.bindDN—DN used to authenticate to the Oblix directory server. Use only if Oblix and User directory servers are separate and you are not using NDS or Active Directory, that is: updateDSInfo.updateDSInfoChoice = "YesTwoDS" and dsTypeInput.dsType does not equal to "2" or "3". Enter this value using valid DN syntax, for example: "cn=Oblix Directory, o=Oblix".	"*bind DN*"
-W dsOblixInfoInput.password—Oblix directory server password. Use only if Oblix and User directory servers are separate and you are not using NDS or Active Directory, that is:: updateDSInfo.updateDSInfoChoice = "YesTwoDS" and dsTypeInput.dsType does not equal "2" or "3".	"*password*"
-W askNTServiceName.ntServiceNameField—Windows only. A service name for the COREid Server. This name will appear in the services control panel.	"*name*"
-W askADSI.isADSI—Confirms if you are using Active Directory with ADSI.	“yes”, “no”
-W askSeparateDomain.isSeparateDomain—Specifies if the machine where you are installing this COREid instance is in a different forest from the target Active Directory Forest that Netpoint is configured to use.	“yes”, “no”
-W askUseImplicitBind.useImplicitBind—If the installation machine is in the same domain, do you want to use the Service account credentials to access Active Directory? A “yes” sets the parameter useImplicitBind in the adsi_params.xml file.	“yes”, “no”
-W askNTServiceAccount.ntServiceUserAcount—If you set the value of askUseImplicitBind to “yes,” this is the account that the service runs as, for example, “.\Administrator”.	“*account ID*”

Table 34 Silent Installation Parameters for the COREid Server

COREid Parameter and Description	Possible Values
-W askNTServiceAccount.ntServiceUserPassword—If you set the value of askUseImplicitBind to “yes”, this is the service account password. Oblix recommends that you supply this value at the command line.	“*password*”

WebPass Parameters

Table 35 describes silent installation parameters for WebPass.

Table 35 Silent Installation Parameters for WebPass

WebPass Parameter and Description	Possible Values
-P webpass.installLocation—Installation directory. The default directory is "C:\NetPoint\WebComponent" on Windows and "/NetPoint/WebComponent" on Unix.	"*installation directory*"
-W userInfoBean.user—Unix only. The user ID that the product will be running as.	"*user ID*"
-W userInfoBean.group—Unix only. The group that corresponds to the userInfoBean.user.	"*group id*"
-W localePanel.defaultLang—Required when extra languages are to be installed with the main installation.	"en-us"
-W localePanel.installLanguages—Required when extra languages are to be installed with the main installation.	"en-us;fr-fr"
-W securityModeBean.securityModeChoices—The security mode for the COREid Server. A value of "open" means no security is used, a value of "simple" means encryption is used, and a value of "cert" means you are running your own CA.	"open", "simple", "cert"
-W webpassInfoBean.hostName—Host name of the COREid Server.	"*ip address*" or "*hostname*"
-W webpassInfoBean.webpassID—WebPass ID. This is an unique ID you specify during installation.	"*ID*"
-W webpassInfoBean.portNumber—Port number of the COREid Server.	"*port number*"
-W simpleModeBean.passphrase—Pass phrase allowing the COREid Server to communicate with the WebPass. Use only if securityModeBean.securityModeChoices = "simple".	"*passphrase*"
-W simpleModeBean.passphraseVerify—Pass phrase allowing the COREid Server to communicate with the WebPass. This parameter is used to verify that the pass phrase matches that of certModeBean.passphrase. Use only if securityModeBean.securityModeChoices = "simple".	"*passphrase*"
-W certModeBean.passphrase—Pass phrase allowing the COREid Server to communicate with the WebPass. Use only if securityModeBean.securityModeChoices = "cert".	"*passphrase*"

Table 35 Silent Installation Parameters for WebPass

WebPass Parameter and Description	Possible Values
-W certModeBean.passphraseVerify—Pass phrase allowing the COREid Server to communicate with the WebPass. This parameter verifies that the pass phrase matches that of certModeBean.passphrase. Use only if securityModeBean.securityModeChoices = "cert".	"*passphrase*"
-W installOrRequestCertBean.installOrRequest—Determines whether to install or request a certificate that is used to configure the COREid system. Use if your security mode is set to "cert". If you already have requested a certificate, choose "install". If you want NetPoint to to request a certificate that can be submitted to the CA, choose "request".	"install" or "request"
-W certReqInfoBean.countryName—Country name. This is a two-letter country code that is valid for use in a DN. It is part of the information that NetPoint uses to request a certificate. Use this parameter if you have opted to have NetPoint request a certificate, that is, if installOrRequestCertBean.installOrRequest = "request".	"*country code*"
-W certReqInfoBean.stateOrProvinceName—State or province name. This is a two-letter state or province code that is valid for use in a DN. It is part of the information that NetPoint uses to request certificate. Use if you have opted to have NetPoint request a certificate, that is, if installOrRequestCertBean.installOrRequest = "request".	"*state or province code*"
-W certReqInfoBean.localityName—Locality name. Part of the information that NetPoint uses to request a certificate. Use if you have opted to have NetPoint request a certificate, that is, if installOrRequestCertBean.installOrRequest = "request".	"*locality name*"
-W certReqInfoBean.organizationName—Organiziation name. This is usually the name of an organization. It is part of the information that NetPoint uses to request a certificate. Use if you have opted to have NetPoint request a certificate, that is, if installOrRequestCertBean.installOrRequest = "request".	"*organization name*"
-W certReqInfoBean.organizationalUnitName—Organizational unit name. This is usually the name of a department. It is part of the information that NetPoint uses to request a certificate. Use if you have opted to have NetPoint request a certificate, that is, if installOrRequestCertBean.installOrRequest = "request".	"*organization unit name*"
-W certReqInfoBean.commonName—Common name. This is usually the name of a person or entity. This is part of the information that NetPoint uses to request a certificate. Use if you have opted to have NetPoint request a certificate, that is, if installOrRequestCertBean.installOrRequest = "request".	"*name*"
-W certReqInfoBean.emailAddress—Email address. This is usually a valid email address. This is part of the information that NetPoint uses to request a certificate. Use if you have opted to have NetPoint request a certificate, that is, if installOrRequestCertBean.installOrRequest = "request".	"*email address*"

Table 35 Silent Installation Parameters for WebPass

WebPass Parameter and Description	Possible Values
-W readyToInstallCertBean.readyToInstallField—If you requested that NetPoint request a certificate, this parameter asks if the certificate is ready for installation. Only use if installOrRequestCertBean.installOrRequest = "request". NetPoint recommends you do not use "Yes" for silent mode. It is unlikely that you can take the request generated by NetPoint and receive the certificates faster than the NetPoint installation can run from one step to the next.	"Yes" or "No"
-W copyCertificatesInputBean.certFile—A certificate is composed of three files: a certificate file, a key file, and a chain file. This parameter specifies the absolute path including the file name for the certificate file (for example: ois_cert.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	"*absolute path including the file name*"
-W copyCertificatesInputBean.keyFile—A certificate is composed of three files: a certificate file, a key file, and a chain file. This parameter specifies the absolute path including the file name for the key file (for example: ois_key.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	"*absolute path including the file name*"
-W copyCertificatesInputBean.chainFile—A certificate is composed of three files: a certificate file, a key file, and a chain file. This parameter specifies the absolute path including the file name for the chain file (for example: ois_chain.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	"*absolute path including the file name*"
-W askAutoUpdateWSBean.askAutoUpdateWSField—Determines whether to update the Web server configuration automatically.	"Yes" or "No"
-W askConfFilePathBean.askConfFilePathField—For NSAPI, this is the absolute path of the Web server configuration directory containing obj.conf (for example: /export/Sun/servers/https-oblix/config). For Apache/Apache SSL, this is the absolute path of httpd.conf in your Web server configuration directory (for example: /export/apache/conf/httpd.conf). Use only for Apache, Apache SSL, and NSAPI Web servers and if askAutoUpdateWSBean.askAutoUpdateWSField = "Yes".	"*absolute path (including the file name for Apache)*"
-W askLaunchBrowserBean.launchBrowser—Determines whether to launch a browser to display instructions to manually update the Web server configuration. Use only if installing on Unix and askAutoUpdateWSBean.askAutoUpdateWSField = "No”.	"Yes" or "No"

Access Manager Parameters

Table 36 describes silent installation parameters for the Access Manager.

Table 36 Silent Installation Parameters for the Access Manager

Access Manager Parameter and Description	Possible Values
-P manager.installLocation—Installation directory. The default directory is "C:\NetPoint" on Windows and "/NetPoint" on Unix.	"*installation directory*"
-**W userInfoBean.user**—Unix only. The user ID that the product will be running as. This can be any valid user ID.	"*user ID*"
-W userInfoBean.group—Unix only. The group that corresponds to the userInfoBean.user.	"*group name*"
-W localePanel.defaultLang—Required when extra languages are to be installed with the main installation.	"en-us"
-W localePanel.installLanguages—Required when extra languages are to be installed with the main installation.	"en-us;fr-fr"
-W updateDSInfo.updateDSInfoChoice—This parameter determines whether NetPoint updates the policy schema automatically. Use this parameter if the Policy directory server is the same as the Oblix server, but different from the User directory server.	"Yes" or "No"
-W dsTypeInput.dsType— If the Policy directory server is the same as the Oblix server, but different from the User directory server updateDSInfo.updateDSInfoChoice = "Yes", you need to specify the Policy directory server type: 1 - Sun Directory Server 5.x 2 - NDS 3 - Active Directory 4 - ADSI (Schema will be uploaded using LDAP) 5 - Active Directory on Windows Server 2003 6 - ADSI on Windows Server 2003 7 - Active Directory Application Mode (On Windows 2003 Only) 8 - Siemens DirX 9 - IBM Directory Server	“1”, "2", "3", “4”, "5",”6”, “7”, “8”, “9”
-W dsInfoInput.dsName—Policy directory server name. Use this parameter if the Policy directory server is the same as the Oblix server, but different from the User directory server, and you are not using NDS or Active Directory. updateDSInfo.updateDSInfoChoice = "Yes" and dsTypeInput.dsType does not equal "2" or "3".	"*ip address*" or "*hostname*"

Table 36 Silent Installation Parameters for the Access Manager

Access Manager Parameter and Description	Possible Values
-W dsInfoInput.dsPortNumber—Policy directory server port number. Use this parameter if the Policy directory server is the same as the Oblix server, but different from the User directory server, and you are not using NDS or Active Directory updateDSInfo.updateDSInfoChoice = "Yes" and dsTypeInput.dsType does not equal "2" or "3".	"*port*"
-W dsInfoInput.bindDN—DN used to authenticate to the the Policy directory server. Use this parameter if the Policy directory server is the same as the Oblix server, but different from the User directory server, and you are not using NDS or Active Directory: updateDSInfo.updateDSInfoChoice = "Yes" and dsTypeInput.dsType does not equal "2" or "3". Use conventional DN syntax for this entry, for example: "cn=Policy Directory, o=Oblix".	"*bind DN*"
-W dsInfoInput.password—Policy directory server password. Use this parameter if the Policy directory server is the same as the Oblix server, but different from the User directory server, and you are not using NDS or Active Directory: updateDSInfo.updateDSInfoChoice = "Yes" and dsTypeInput.dsType does not equal "2" or "3".	"*password*"
-W dsInfoInput.dsSSLConnect—Determines whether the Policy directory server uses an SSL connection. Use this parameter if the Policy directory server is the same as the Oblix server, but different from the User directory server, and you are not using NDS or Active Directory: updateDSInfo.updateDSInfoChoice = "Yes" and dsTypeInput.dsType does not equal "2" or "3".	"Yes" or "No"
-W askSSLCertPath.askSSLCertificatePathField—The absolute path to the SSL certificate. Use this parameter if the Policy directory server is the same as the Oblix server, but different from the User directory server, and you are not using NDS or Active Directory: updateDSInfo.updateDSInfoChoice = "Yes" and dsTypeInput.dsType does not equal "2" or "3" and dsInfoInput.dsSSLConnect = "Yes".	"*absolute path including the file name*"
-W askAutoUpdateWSBean.askAutoUpdateWSField—Determines whether to update the Web server configuration automatically.	"Yes" or "No"
-W askConfFilePathBean.askConfFilePathField—For NSAPI, this is the absolute path of the Web server config directory containing obj.conf (for example: /export/Sun/servers/https-oblix/config). For Apache and Apache SSL, this is the absolute path of httpd.conf in your Web server config directory (for example: /export/apache/conf/httpd.conf). Use only for Apache, Apache SSL, and NSAPI Web servers and if askAutoUpdateWSBean.askAutoUpdateWSField = "Yes".	"*absolute path (including the file name for Apache)*"

Table 36 Silent Installation Parameters for the Access Manager

Access Manager Parameter and Description	Possible Values
-W askLaunchBrowserBean.launchBrowser—Determines whether to launch a browser that displays instructions to manually update the Web server configuration. Use only on Unix and only if askAutoUpdateWSBean.askAutoUpdateWSField = "No".	"Yes" or "No"
-W askADSI.isADSI—Confirms if you are running Active Directory with ADSI.	“yes”, “no”
-W askADSISSL.isADSISSL—Confirms if you are running Active Directory with ADSI using SSL.	“yes”, “no”

Access Server Parameters

Table 37 describes silent installation parameters for the Access Server.

Table 37 Silent Installation Parameters for the Access Server

Access Server Parameter and Description	Possible Values
-P aaa.installLocation—The installation directory. The default directory is "C:\NetPoint" on Windows and "/NetPoint" on Unix.	"*installation directory*"
-W userInfoBean.user—Unix only. The user ID that the product will be running as.	"*user ID*"
-W userInfoBean.group—Unix only. The group that corresponds to the userInfoBean.user.	"*group name*"
-W localePanel.defaultLang—Required when extra languages are to be installed with the main installation.	"en-us"
-W localePanel.installLanguages—Required when extra languages are to be installed with the main installation.	"en-us;fr-fr"
-W securityModeBean.securityModeChoices—The security mode for the Access Server. A value of "open" means no security is used, a value of "simple" means encryption is used, and a value of "cert" means you are running your own CA.	"open", "simple", or "cert"
- W userDSSSLCerPath.sslCertPath—The abolute path to the SSL certificate. Use only if the user directory is in SSL mode.	"*absolute path including the file name*"
-W oblixDSInfoBean.dsHostMachine—Oblix directory server host machine.	"*ip address*" or "*hostname*"

Table 37 Silent Installation Parameters for the Access Server

Access Server Parameter and Description	Possible Values
-W oblixDSInfoBean.dsPortNumber—Oblix directory server port number.	"*port number*"
-W oblixDSInfoBean.dsBindDN—DN used to authenticate to the Oblix directory server.	"*bind DN*"
-W oblixDSInfoBean.dsPassword—Oblix directory server password.	"*password*"
-W oblixDSInfoBean.dsMode—Oblix directory server's mode (open or ssl).	"open" or "ssl"
-W oblixDSInfoBean.dsType—The Oblix directory server type: NS5 - Sun Directory Server 5.x NOVELL - NDS MSAD - Microsoft Active Directory MSAD_ADSI - Microsoft Active Directory with ADSI MSADAM - Active Directory Application Mode DIRX - Siemens DirX IBMSWAY - IBM Directory Server?	"NS5", "NOVELL", "MSAD", "MSAD_ADSI" “MSADAM” “DirX” “IBMSWAY”
-W oblixDSSSLCertPath.sslCertPath—The absolute path to the ssl certificate. Use only if oblixDSInfoBean.dsMode = "ssl".	"*absolute path including the file name*"
-W policyDataInWhichDSBean.askPolicyDataInWhichDS—Determines whether the Policy directory server is the same as the User or Oblix directory server. The value "OBLIX" means that the Policy and Oblix directory server are the same. The value "POLICY" means that the Policy directory server is different from that of User and Oblix directory server.	"OBLIX" or "POLICY"
-W policyDSInfoBean.dsHostMachine—The Policy directory server host machine. Use only if the Policy directory server is the same as the Oblix server, but different from the User directory server, policyDataInWhichDSBean.askPolicyDataInWhichDS = "OBLIX".	"*ip address*" or "*hostname*"
-W policyDSInfoBean.dsPortNumber—The Policy directory server port number. Use only if the Policy directory server is the same as the Oblix server, but different from the User directory server, policyDataInWhichDSBean.askPolicyDataInWhichDS = "OBLIX".	"*port number*"
-W policyDSInfoBean.dsBindDN—The DN used to authenticate to the Policy directory server. Use only if the Policy directory server is different from that of User and Oblix directory server policyDataInWhichDSBean.askPolicyDataInWhichDS = "POLICY". Use conventional DN syntax for this entry. Example: "cn=Policy Directory, o=Oblix".	"*bind DN*"

Table 37 Silent Installation Parameters for the Access Server

Access Server Parameter and Description	Possible Values
-W policyDSInfoBean.dsPassword—Policy directory server password. Use only if the Policy directory server is different from that of User and Oblix directory server policyDataInWhichDSBean.askPolicyDataInWhichDS = "POLICY".	"*password*"
-W policyDSInfoBean.dsMode—Policy directory server mode (open or ssl). Use only if the Policy directory server is different from that of User and Oblix directory server policyDataInWhichDSBean.askPolicyDataInWhichDS = "POLICY".	"open" or "ssl"
-W policyDSSSLCertPath.sslCertPath—The absolute path to the ssl certificate. Use only if the Policy directory server is the same as the Oblix server, but different from the User directory server, policyDataInWhichDSBean.askPolicyDataInWhichDS = "OBLIX".	"*absolute path including the file name*"
-W aaaInfoBean.accessServerID—The ID of the Access Server registered in the Access System Console. Supply the value you entered at the Access System Console for this Access Server.	"*value*"
-W aaaInfoBean.policyDataConfigDN—The configuration DN for the policy data. Use conventional DN syntax for this entry. Example: "cn=Policy Data, o=Oblix".	"*DN*"
-W aaaInfoBean.policyDSBase—The policy base, which is the node in the Policy directory below which Oblix stores its policy-related data.Example: "cn=Policy Data, o=Oblix".	"*DN*"
-W simpleModeInfoBean.passphrase—The pass phrase. Use only if securityModeBean.securityModeChoices = "simple".	"*passphrase*"
-W simpleModeInfoBean.passphraseVerify—The pass phrase again, used for verification. This should be the same as simpleModeInfoBean.passphrase. Use only if securityModeBean.securityModeChoices = "simple".	"*passphrase*"
-W simpleModeInfoBean.storePassPhraseinFile—Determines whether the pass phrase is stored in a file. If stored in a file, the Access Server can be started without a user or a script providing the pass phrase when the Access Server starts up.	"true" or "false"
-W certModeInfoBean.passphrase—Pass phrase. Use only if securityModeBean.securityModeChoices = "cert".	"*passphrase*"
-W certModeInfoBean.passphraseVerify—Pass phrase again, used for verification. This should be the same as certModeInfoBean.passphrase. Use only if securityModeBean.securityModeChoices = "cert".	"*passphrase*"
-W certModeInfoBean.storePassPhraseinFile—Determines whether the password or pass phrase is stored in a file. If stored in a file, the Access Server can be started without a user providing the pass phrase when the Access Server starts up.	"true" or "false"

Table 37 Silent Installation Parameters for the Access Server

Access Server Parameter and Description	Possible Values
-W installOrRequestCertBean.installOrRequest—Determines whether to install or request a certificate that is used to configure the Access System. Used if your security mode is set to "cert". If you already have a certificate, use “install.” If you want NetPoint to request a request for a certificate, use "request".	"request" or "install"
-W certReqInfoBean.countryName—Country name. This is usually a two-letter country code that is valid for use in DNs. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*country code*"
-W certReqInfoBean.stateOrProvinceName—State or province name. This is usually a two-letter state or province code that this valid for use in DNs. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*state or province code*"
-W certReqInfoBean.localityName—Locality name. This is usually the name of a geographic region. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*locality name*"
-W certReqInfoBean.organizationName—Organization name. This is usually the name of an organization. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*organization name*"
-W certReqInfoBean.organizationalUnitName—Organization unit name. This is usually the name of a department. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*organization name*"
-W certReqInfoBean.commonName—Common name. This is usually the name of a person or another entity. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*name*"
-W certReqInfoBean.emailAddress—Email address. This is usually a valid email address. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*email address*"
-W readyToInstallCertBean.readyToInstallField—If you requested that NetPoint request a certificate, this verifies that the certificate is ready for installation. Only use if installOrRequestCertBean.installOrRequest = "request". Oblix recommends you do not use "Yes" for silent mode. You probably cannot take the request generated by NetPoint and receive the certificates faster than the NetPoint installation can run from one step in the installation to the next.	"Yes" or "No"
-W copyCertificatesInputBean.certFile—The absolute path including the file name for the certificate file (for example: aaa_cert.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	"*absolute path including the file name*"

Table 37 Silent Installation Parameters for the Access Server

Access Server Parameter and Description	Possible Values
-W copyCertificatesInputBean.keyFile—The absolute path including the file name for the key file (example: aaa_key.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	"*absolute path including the file name*"
-W copyCertificatesInputBean.chainFile—The absolute path including the file name for the chain file (example: aaa_chain.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	"*absolute path including the file name*"
-W askSeparateDomain.isSeparateDomain—Specifies if the machine where you are installing this COREid instance is in a different forest from the target Active Directory Forest that Netpoint is configured to use.	“yes”, “no”
-W askUseImplicitBind.useImplicitBind—If the installation machine is in the same domain, do you want to use the Service account credentials to access Active Directory? A “yes” sets the parameter useImplicitBind in the adsi_params.xml file.	“yes”, “no”
-W askNTServiceAccount.ntServiceUserAcount—If you set the value of askUseImplicitBind to “yes,” this is the account that the service runs as, for example, “.\Administrator”.	“*account ID*”
-W askNTServiceAccount.ntServiceUserPassword—If you set the value of askUseImplicitBind to “yes”, this is the service account password. Oblix recommends that you supply this value at the command line.	“*password*”

WebGate Parameters

Table 38 describes silent installation parameters for WebGate.

Table 38 Silent Installation Parameters for the WebGate

WebGate Parameter and Description	Possible Values
-P webgate.installLocation—Installation directory. The default directory is "C:\NetPoint\WebComponent" on Windows and "/NetPoint/WebComponent" on Unix.	"*installation directory*"
-W userInfoBean.user—Unix only. The user ID that the product will be running as.	"*user ID*"
-W userInfoBean.group—Unix only. The group that corresponds to the userInfoBean.user.	"*group id*"
-W localePanel.defaultLang—Required when extra languages are to be installed with the main installation.	"en-us"
-W localePanel.installLanguages—Required when extra languages are to be installed with the main installation.	"en-us;fr-fr"
-W securityModeBean.securityModeChoices—Security mode for WebGate. A value of "open" means no security is used, a value of "simple" means encryption is used, and a value of "cert" means you are running your own CA.	"open", "simple", "cert"
-W openModeBean.serverID—Access Server ID. Use the value you supplied at the Access System Console before installation. Use only if securityModeBean.securityModeChoices = "open".	"*server id*"
-W openModeBean.hostName—Access Server host name. Use only if securityModeBean.securityModeChoices = "open".	"*ip address*" or "*hostname*"
-W openModeBean.webgateID—WebGate ID. Use the ID that you entered in the Access System Console before running the installation. Use only if securityModeBean.securityModeChoices = "open".	"*value*"
-W openModeBean.portNumber—Access Server port number. Use only if securityModeBean.securityModeChoices = "open".	"*port number*"
-W openModeBean.password—WebGate password (optional). Use only if securityModeBean.securityModeChoices = "open".	"*password*"
-W simpleModeBean.serverID—Access Server ID. Use the value you supplied at the Access System Console before installation. Use only if securityModeBean.securityModeChoices = "simple".	"*value*"
-W simpleModeBean.hostName—Access Server host name. Use only if securityModeBean.securityModeChoices = "simple".	"*ip address*" or "*hostname*"

Table 38 Silent Installation Parameters for the WebGate

WebGate Parameter and Description	Possible Values
-W simpleModeBean.webgateID—The WebGate ID. Use the value you supplied at the Access System Console. Use only if securityModeBean.securityModeChoices = "simple".	"*value*"
-W simpleModeBean.portNumber—The Access Server port number. Use only if securityModeBean.securityModeChoices = "simple".	"*port number*"
-W simpleModeBean.password—The WebGate password (optional). Use only if securityModeBean.securityModeChoices = "simple".	"*password*"
-W simpleModeBean.passphrase—The pass phrase. Use only if securityModeBean.securityModeChoices = "simple".	"*passphrase*"
-W simpleModeBean.passphraseVerify—The pass phrase again, used for verification and should be the same as simpleModeInfoBean.passphrase. Use only if securityModeBean.securityModeChoices = "simple".	"*passphrase*"
-W certModeBean.serverID—The Access Server ID. Use the value you supplied at the Access System Console before installation. Use only if securityModeBean.securityModeChoices = "cert".	"*value*"
-W certModeBean.hostName—The Access Server host name use only if securityModeBean.securityModeChoices = "cert".	"*ip address*" or "*hostname*"
-W certModeBean.webgateID—The WebGate ID (optional). Use the value you supplied at the Access System Console. Use only if securityModeBean.securityModeChoices = "cert".	"*value*"
-W certModeBean.portNumber—The Access Server port number. Use only if securityModeBean.securityModeChoices = "cert".	"*port number*"
-W certModeBean.password—The WebGate password. Use only if securityModeBean.securityModeChoices = "cert".	"*password*"
-W certModeBean.passphrase—The pass phrase. Use only if securityModeBean.securityModeChoices = "cert".	"*passphrase*"
-W askAutoUpdateWSBean.askAutoUpdateWSField—Determines whether to perform an automatic update of the Web server configuration.	"Yes" or "No"
-W askConfFilePathBean.askConfFilePathField—For NSAPI, this is the absolute path of the Web server configuration directory containing the obj.conf (for example: /export/Planet/servers/https-oblix/config). For Apache/Apache SSL, this is the absolute path of httpd.conf in your Web server config directory (for example: /export/apache/conf/httpd.conf). Use only for Apache, Apache SSL, and NSAPI Web servers and if askAutoUpdateWSBean.askAutoUpdateWSField = "Yes".	"*absolute path (including the file name for Apache)*"

Table 38 Silent Installation Parameters for the WebGate

WebGate Parameter and Description	Possible Values
-W certModeBean.passphraseVerify—The pass phrase again, used for verification and should be the same as certModeInfoBean.passphrase. Use only if securityModeBean.securityModeChoices = "cert".	"*passphrase*"
-W installOrRequestCertBean.installOrRequest—Determines whether to install or request a certificate to be used to configure the Access System. Used if your security mode is set to "cert". If you already have a certificate, use "install". If you want NetPoint to request and request a certificate, use "request".	"request" or "install"
-W certReqInfoBean.countryName—Country name. This is a two-letter country code that is valid for use in a DN. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*country code*"
-W certReqInfoBean.stateOrProvinceName—State or province name. This is a two-letter code that is valid for use in a DN. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*state or province code*"
-W certReqInfoBean.localityName—Locality name. This is usually a geographic region. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*locality name*"
-W certReqInfoBean.organizationName—Organization name. This is usually the name of the organization. It is part of the information used to request certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*organization name*"
-W certReqInfoBean.organizationalUnitName—Organization unit name. This is usually a department name. It is part of the information used to request certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*organization unit name*"
-W certReqInfoBean.commonName—Common name. This is usually a person's or entity's name. It is part of the information used to request certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*common name*"
-W certReqInfoBean.emailAddress—Email address. This is usually a valid email address. This is part of the information used to request certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	"*email address*"
-W readyToInstallCertBean.readyToInstallField—If you requested that NetPoint request a certificate, this verifies that the certificate is ready for installation. Only used if installOrRequestCertBean.installOrRequest = "request". Oblix recommends that you use a value of "No" for silent mode. It is unlikely that you can take the request generated by NetPoint and receive the certificate faster than the NetPoint installation can run from one step to the next.	"Yes" or "No"

Table 38 Silent Installation Parameters for the WebGate

WebGate Parameter and Description	Possible Values
-W copyCertificatesInputBean.certFile—A certificate is composed of three files: a certificate file, a key file, and a chain file. This parameter specifies the absolute path including the file name for the certificate file (for example: aaa_cert.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	"*absolute path including the file name*"
-W copyCertificatesInputBean.keyFile—A certificate is composed of three files: a certificate file, a key file, and a chain file. This parameter specifies the absolute path including the file name for the key file (for example: aaa_key.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	"*absolute path including the file name*"
-W copyCertificatesInputBean.chainFile—A certificate is composed of three files: a certificate file, a key file, and a chain file. This parameter specifies the absolute path including the file name for the chain file (for example: aaa_chain.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes."	"*absolute path including the file name*"

Access Server SDK Parameters

Table 39 describes silent installation parameters for the Access Server SDK.

Table 39 Silent Installation Parameters for the Access Server SDK

Access SDK Parameter and Description	Possible Values
-P sdk.installLocation—The installation directory. The default directory is "C:\NetPoint" on Windows and "/NetPoint" on Unix.	"*installation directory*"
-W userInfoBean.user—Unix only. The user ID that the product will be running as.	"*user ID*"
-W userInfoBean.group—Unix only. The group that corresponds to the userInfoBean.user.	"*group id*"

Ready Realm for BEA

Table 40 describes silent installation parameters for Ready Realm.

Note: Include HTTPClient.jar jnet.jar jsse.jar in the CLASSPATH environment variable when installing on BEA Weblogic.

Table 40 Silent Installation Parameters for the Ready Realm for BEA

Ready Realm Parameter and Description	Possible Values
-P bea.installLocation—The installation directory. The default directory is "C:\NetPoint" on Windows and /NetPoint on Unix.	*"installation directory"*
-W verifyUserBean.verifyUserBeanField—Determines whether the user installing the product is the same one that the product should be running as. If the value is No, the installation exits.	"Yes" or "No"
-W realmConfig.userCacheSize—The size of the authenticated user cache, in number of users, for example, "1000".	*"number of users"*
-W realmConfig.systemUser—The login ID of the user to be mapped to the system user of the WebLogic server, for instance "weblogic_system."	*"login ID"*
-W realmConfig.debug—Set debug log. Set this value to “false” for better performance.	"true" or "false"
-W webPassConfig.policyDomain—The name of the policy domain under which J2EERoles will be created from the administrative tools of WebLogic and Portal Server, for example, "weblogic".	*"domain name"*
-W webPassConfig.webPassProtected—Determines whether NetPoint WebPass is protected with NetPoint WebGate.	"true" or "false"
-W webPassConfig.webPassSSL—Determines whether the Web server on which WebPass is installed requires browsers to connect to it in SSL mode (transmitting data via https).	"true" or "false"
-W webPassSSO.cookieDomain—Cookie domain set for NetPoint WebGate, for example "company.com".	*"domain name"*
-W webPassSSO.cookiePath—Cookie path set for NetPoint WebGate, for example "/".	*"path"*
-W cacheConfig.guestUser—The login id for the user to be mapped to the guest user of the WebLogic server.	*"login ID"*
-W cacheConfig.AllUserCacheEnabled—This value enables caching of all users.	"true" or "false"

Table 40 Silent Installation Parameters for the Ready Realm for BEA

Ready Realm Parameter and Description	Possible Values
-W cacheConfig.AllUserCacheTimeout—This is the amount of time the list of all users is kept in the cache, for instance, "3600".	*"number of seconds"*
-W cacheConfig.GroupCacheEnabled—This enables the caching of all groups and membership information for these groups.	"true" or "false"
-W cacheConfig.GroupCacheTimeout—This is the amount of time the list of all groups is kept in the cache, for instance, "3600".	*"number of seconds"*
-W securityModeBean.securityModeChoice—The security mode for the Access Server. A value of "open" means no security is used, a value of "simple" means encryption is used, and a value of "cert" means you are running your own CA.	"open", "simple", or "cert"
-W openModeBean.serverID—Access Server ID. Use the value you supplied at the Access System Console before installation. Use only if securityModeBean.securityModeChoices = "open". Example: "AccessServer1".	*"server ID"*
-W openModeBean.hostName—Host name where Access Server is installed. Use only if securityModeBean.securityModeChoices = "open".	*"ip address" or "hostname"*
-W openModeBean.accessGateID—Access Gate ID. Use only if securityModeBean.securityModeChoices = "open". Example: "WeblogicRealm1".	*"ID"*
-W openModeBean.portNumber—Port number of the Access Server. Use only if securityModeBean.securityModeChoices = "open".	*"port number"*
-W openModeBean.password—Password for Access Gate, if one is set. Use only if securityModeBean.securityModeChoices = "open".	*"password"*
-W simpleModeBean.serverID—Access Server ID. Use the value you supplied at the Access System Console before installation. Use only if securityModeBean.securityModeChoices = "simple".	*Access Server ID*
-W simpleModeBean.hostName—Host name where Access Server is installed. Use only if securityModeBean.securityModeChoices = "simple".	*"ip address" or "hostname"*
-W simpleModeBean.accessGateID—Access Gate ID. This value has to match the one you specified at the Access System Console. Use only if securityModeBean.securityModeChoices = "simple".	*"value"*
-W simpleModeBean.portNumber—Port number of the Access Server. Use only if securityModeBean.securityModeChoices = "simple".	*"port number"*
-W simpleModeBean.password—Password for Access Gate, if one is set. Use only if securityModeBean.securityModeChoices = "simple".	*"password"*

Table 40 Silent Installation Parameters for the Ready Realm for BEA

Ready Realm Parameter and Description	Possible Values
-W simpleModeBean.passphrase—Pass phrase for the Access Gate to communicate with the Access Server. Use only if securityModeBean.securityModeChoices = "simple".	*"passphrase"*
-W simpleModeBean.passphraseVerify—Pass phrase for the Access Gate to communicate with the Access Server. This parameter verifies that the pass phrase matches that of certModeBean.passphrase. Use only if securityModeBean.securityModeChoices = "simple".	*"passphrase"*
-W certModeBean.serverID—Access Server ID. Use the value you supplied at the Access System Console before installation. This value has to match the one you specified at the Access System Console. Use only if securityModeBean.securityModeChoices = "cert".	*"value"*
-W certModeBean.hostName—Host name where Access Server is installed. Use only if securityModeBean.securityModeChoices = "cert".	*"ip address" or "hostname"*
-W certModeBean.accessGateID—Access Gate ID. This value has to match the one you specified at the Access System Console. Use only if securityModeBean.securityModeChoices = "cert".	*"value"*
-W certModeBean.portNumber—Port number of the Access Server. Use only if securityModeBean.securityModeChoices = "cert".	*"port number"*
-W certModeBean.password—Password for Access Gate, if one is set. Use only if securityModeBean.securityModeChoices = "cert".	*"password"*
-W certModeBean.passphrase—Pass phrase allowing the Access Gate to communicate with the Access Server. Use only if securityModeBean.securityModeChoices = "cert".	*"passphrase"*
-W certModeBean.passphraseVerify—Pass phrase allowing the Access Gate to communicate with the Access Server. This parameter verifies that the pass phrase matches that of certModeBean.passphrase. Use only if securityModeBean.securityModeChoices = "cert".	*"passphrase"*
-W installOrRequestCertBean.installOrRequest—Determines whether to install or request a certificate to be used to configure the Access System. Used if your security mode is set to "cert". If you already have a certificate, choose "install". If you want NetPoint to request and request a certificate, choose "request".	*"install", "request"*
-W certReqInfoBean.countryName—Country name. This is usually a two-letter country code that is valid for use in DNs. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"country code"*

Table 40 Silent Installation Parameters for the Ready Realm for BEA

Ready Realm Parameter and Description	Possible Values
-W certReqInfoBean.stateOrProvinceName—State or province name. This is usually a two-letter state or province code that is valid for use in a DN. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"state or province code"*
-W certReqInfoBean.localityName—Locality name. This is usually the name of a geographic region. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"locality name"*
-W certReqInfoBean.organizationName— Organization name. This is usually the name of an organization. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"organization name"*
-W certReqInfoBean.organizationalUnitName—Organization unit name. This is usually the name of a department. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"organization unit name"*
-W certReqInfoBean.commonName—Common name. This is usually the name of a person or an entity. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"name"*
-W certReqInfoBean.emailAddress—Email address. This is usually a valid email address. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"email address"*
-W readyToInstallCertBean.readyToInstallField—If you requested that NetPoint request a certificate, this verifies that the certificate is ready for installation. This is only used if installOrRequestCertBean.installOrRequest = "request".Oblix recommends that you do not use “Yes" for silent mode. You probably cannot take the request generated by NetPoint and receive the certificates faster than the NetPoint installation can run from one step in the installation to the next.	*"Yes" or "No"*
-W copyCertificatesInputBean.certFile—The absolute path including the file name for the certificate file (for example: aaa_cert.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	*"absolute path including the file name"*
-W copyCertificatesInputBean.keyFile—The absolute path including the file name for the key file (for example: aaa_key.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	*"absolute path including the file name"*

Table 40 Silent Installation Parameters for the Ready Realm for BEA

Ready Realm Parameter and Description	Possible Values
-W copyCertificatesInputBean.chainFile—The absolute path including the file name to the chain file (for example: aaa_chain.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	*"absolute path including the file name"*

BEA SSPI Parameters

Table 41 describes silent installation parameters for BEA SSPI.

Table 41 Silent Installation Parameters for the BEA SSPI Parameters

BEA SSPI Parameters and Description	*Possible Value*
-P bea.installLocation—The installation directory. The default directory is "C:\NetPoint" on Windows and "/NetPoint" on Unix.	*"installation directory"*
-W localePanel.defaultLang—Required when extra languages are to be installed with the main installation.	"en-us"
-W localePanel.installLanguages—Required when extra languages are to be installed with the main installation	"en-us;fr-fr"
-W sspiConfigLevel.ConfigMode—Configuration options. Typical option will require minimal inputs. Advanced option enables overriding of all defaults.	"typical;advanced"
-W verifyUserBean.verifyUserBeanField—Determines whether the user installing the product is the same one that the product should be running as. If the value is No, the installation exits.	"Yes" or "No"
-W sspiAdv1.authResType—Resource type used by NetPoint Security Provider in the policy to authenticate users in Weblogic.wl_authen	*wl_authen*
-W sspiAdv1.authRes—Resource name used by NetPoint Security Provider in the policy to authenticate users in Weblogic.	*/Authen/Basic*
-W sspiAdv1.authResOp—Resource operation used by NetPoint Security Provider in the policy to authenticate users in Weblogic.LOGIN	*LOGIN*
-W sspiAdv1.authAnonymousRes—Resource name used for anonymous access by NetPoint Security Provider in the policy to authenticate users in Weblogic./Authen/Anonymous	*Authen/Anonymous*
-W sspiAdv1.authUID—LoginId—parameter used in credential_mapping plugin of authentication.userid	*userid*
-W sspiAdv1.authPass—Password parameter used in validate password of authentication scheme.Password	*Password*

Table 41 Silent Installation Parameters for the BEA SSPI Parameters

BEA SSPI Parameters and Description	*Possible Value*
-W sspiAdv1.authnActionType—Action Type (action is configured to get the loginId from ObSSOCookie).WL_REALM	*WL_REALM*
-W sspiAdv1.authnActionName—Action Name (action is configured to get the loginId from ObSSOCookie).uid	*uid*
-W sspiAdv1.obDummyUser—Dummy username used by form login for doing SSO when there is no webgate on proxy HTTP server.Obdummyuser	*Obdummyuser*
-W sspiAdv2.webAppResourceTypes—Weblogic resource types used for web applications(comma separated)<url>,<web>	*url>,<web>*
-W sspiAdv2.roleResType—Resource type used by NetPoint Security Provider in the policy to get roles for a user.	*wl_authen*
-W sspiAdv2.roleRes—Resource name used by NetPoint Security Provider in the policy to get roles for a user.	*/Authen/Roles*
-W sspiAdv2.roleResOp—Resource operation used by NetPoint Security Provider in the policy to get roles for a user.	*LOGIN*
-W sspiAdv2.rolesCacheTTL—TTL(time to live) of elements in roles cache.	60
-W sspiAdv2.rolesCacheCleanupSchedule—Time to delete expired elements of cache (in seconds).	60
-W sspiAdv2.roleActionType—Action Type in authorization rule to get roles.	*WL_REALM*
-W sspiAdv3.notProtecedAction—Default access to resources not protected by NetPoint.	*allow;deny;abstain*
-W sspiAdv3.abstainMapsTo—Map the authorization result ABSTAIN to (allow,deny).	*allow;deny*
-W sspiAdv3.debug—Set debugging (This should be set to Off for production systems).	1 - On 2 - Off
-W securityModeBean.securityModeChoices—The security mode for BEA SSPI. A value of "open" means no security is used, a value of "simple" means encryption is used, and a value of "cert" means you are running your own CA.	"open", "simple", "cert"
-W openModeBean.serverID—Access Server ID. Use the value you supplied at the Access System Console before installation. Use only if securityModeBean.securityModeChoices = "open". Example: "AccessServer1".	*"server ID"*
-W openModeBean.hostName—Host name where Access Server is installed. Use only if securityModeBean.securityModeChoices = "open".	*"ip_address"* *or "hostname"*
-W openModeBean.accessGateID—Access Gate ID. Use only if securityModeBean.securityModeChoices = "open". Example: "WeblogicRealm1".	*"value"*

Table 41 Silent Installation Parameters for the BEA SSPI Parameters

BEA SSPI Parameters and Description	*Possible Value*
-W openModeBean.portNumber—Port number of the Access Server. Use only if securityModeBean.securityModeChoices = "open".	*"port_number"*
#-W openModeBean.password—Password for Access Gate, if one is set. Use only if securityModeBean.securityModeChoices = "open".	*"password"*
-W simpleModeBean.serverID—Access Server ID. Use the value you supplied at the Access System Console before installation. Use only if securityModeBean.securityModeChoices = "simple".	*"server ID"*
-W simpleModeBean.hostName—Host name where Access Server is installed. Use only if securityModeBean.securityModeChoices = "simple".	*"ip address" or "hostname"*
-W simpleModeBean.accessGateID—Access Gate ID. This value has to match the one you specified at the Access System Console. Use only if securityModeBean.securityModeChoices = "simple".	*"value"*
-W simpleModeBean.portNumber—Port number of the Access Server. Use only if securityModeBean.securityModeChoices = "simple".	*"port number"*
#-W simpleModeBean.password—Password for Access Gate, if one is set. Use only if securityModeBean.securityModeChoices = "simple".	*"password"*
#-W simpleModeBean.passphrase—Pass phrase for the Access Gate to communicate with the Access Server. Use only if securityModeBean.securityModeChoices = "simple".	*"passphrase"*
#-W simpleModeBean.passphraseVerify—Pass phrase for the Access Gate to communicate with the Access Server. This parameter verifies that the pass phrase matches that of securityModeBean.passphrase. Use only if securityModeBean.securityModeChoices = "simple".	*"passphrase"*
-W certModeBean.serverID—Access Server ID. Use the value you supplied at the Access System Console before installation. This value has to match the one you specified at the Access System Console. Use only if securityModeBean.securityModeChoices = "cert".	*"value"*
-W certModeBean.hostname—Host name where Access Server is installed. Use only if securityModeBean.securityModeChoices = "cert".	*"ip address" or "hostname"*
-W certModeBean.accessGateID—Access Gate ID. This value has to match the one you specified at the Access System Console. Use only if securityModeBean.securityModeChoices = "cert".	*"value"*
-W certModeBean.portNumber—Port number of the Access Server. Use only if securityModeBean.securityModeChoices = "cert".	*"port number"*
-W certModeBean.password—Password for Access Gate, if one is set. Use only if securityModeBean.securityModeChoices = "cert"."password"	*"port number"*

Table 41 Silent Installation Parameters for the BEA SSPI Parameters

BEA SSPI Parameters and Description	*Possible Value*
-W certModeBean.passphrase—Pass phrase allowing the Access Gate to communicate with the Access Server. Use only if securityModeBean.securityModeChoices = "cert".	*"passphrase"*
-W certModeBean.passphraseVerify—Pass phrase allowing the Access Gate to communicate with the Access Server. Use only if securityModeBean.securityModeChoices = "cert".	*"passphrase"*
-W installOrRequestCertBean.installOrRequest—Determines whether to install or request a certificate to be used to configure the Access System. Used if your security mode is set to "cert". If you already have a certificate, choose "install". If you want NetPoint to request and request a certificate, choose "request".	*"install", "request"*
-W certReqInfoBean.countryName—Country name. This is usually a two-letter country code that is valid for use in DNs. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"country code"*
-W certReqInfoBean.stateOrProvinceName—State or province name. This is usually a two-letter state or province code that is valid for use in a DN. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"state or province code"*
-W certReqInfoBean.localityName—Locality name. This is usually the name of a geographic region. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"locality name"*
-W certReqInfoBean.organizationName—Organization name. This is usually the name of an organization. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"organization name"*
-W certReqInfoBean.organizationalUnitName—Organization unit name. This is usually the name of a department. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"organization unit name"*
-W certReqInfoBean.commonName—Common name. This is usually the name of a person or an entity. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"name"*
-W certReqInfoBean.emailAddress—Email address. This is usually a valid email address. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"email address"*
-W readyToInstallCertBean.readyToInstallField—If you requested that NetPoint request a certificate, this verifies that the certificate is ready for installation. This is only used if installOrRequestCertBean.installOrRequest = "request".Oblix recommends that you do not use "Yes" for silent mode. You probably cannot take the request generated by NetPoint and receive the certificates faster than the NetPoint installation can run from one step in the installation to the next.	"Yes" or "No"

Table 41 Silent Installation Parameters for the BEA SSPI Parameters

BEA SSPI Parameters and Description	*Possible Value*
-W copyCertificatesInputBean.certFile—The absolute path including the file name for the certificate file (for example: aaa_cert.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	*"absolute path including the file name"*
-W copyCertificatesInputBean.keyFile—The absolute path including the file name for the key file (for example: aaa_key.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	*"absolute path including the file name"*
-W copyCertificatesInputBean.chainFile—The absolute path including the file name to the chain file (for example: aaa_chain.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	*"absolute path including the file name"*

WAS Registry Parameters

Table 42 provides silent installation parameters for the WAS registry.

Table 42 Silent Installation Parameters for WAS Registry

WAS Registry Parameter—Description	Possible Values
-P was_registry.installLocation—The installation directory. The default directory is "C:\Program Files\NetPoint" on windows and "/opt/Netpoint" on Unix.	*"installation directry"*
-W verifyUserBean.verifyUserBeanField—Determines whether the user installing the product is the same one that the product should be running as. If the value is No, the installation exists.	"Yes" or "No"
-W wasConfig.WPHostName—Hostname of Webpass	*"machine name"*
-W wasConfig.WPPortNumber—Port Number of webpass	*"port number"*
-W wasConfig.WPIsProtected—Is webpass protected by webgate.	"true" or "false"
-W wasWebPassConfig.cookieDomainCookie domain set for Netpoint webgate, for example "company.com"	*"domain name"*
-W wasWebPassConfig.cookiePath—Cookie path set for Netpoint WebGate e.g. "/"	*"path"*
-W wasDSConfig.WPSSL—Determines whether the Netpoint connector for websphere requires webpass to connect to it in SSL mode (transmitting data via https).	*"true" or "false"*
-W wasDSConfig.UserAttr—User attribute.	*"uid"*
-W wasDSConfig.UserSearchAttr—User search attrinute.	*"cn"*
-W wasDSConfig.GroupSearchAttr—Group search attribute	*"cn"*
-W wasWSClassesDir.classesDir—Full Path of the WebSphere classes directory.	*"path"*
-W configPortalInput.isPortalTobeUsed—Netpoint websphere connector requires certain files to be copied to WebSphere Application directory for websphere portal server integration. This parameter asks if portal server needs to be integrated.	"true" or "false"
-W wasInfoBean.wasInstallDir—If -W configPortalInput.isPortalTobeUsed = "true" then enter WebSphere Application directory path.	*$Websphere_install_dir/ AppServer*
-W securityModeBean.securityModeChoices—AccessGate mode configuration. A value of "open" means no security is required, a value of "simple" means encryption is used, and a value of "cert" means you are running your own CA.	"open", "simple" or "cert'

Table 42 Silent Installation Parameters for WAS Registry

WAS Registry Parameter—Description	Possible Values
-W openModeBean.serverID—Access server ID. Use value you specified at the Access System Console before installation. Use only if securityModeBean.securityModeChoices = "open".	*"server id"*
-W openModeBean.hostname—Machine name where Access Server is installed. Use only if securityModeBean.securityModeChoices = "open".	*"ip_addr"* *or* *"machine_name"*
-W openModeBean.accessGateID—AccessGate ID. Use only if securityModeBean.securityModeChoices = "open"	*“AccessGate ID”*
-W openModeBean.portNumber—Port number of the access server.	*"port number"*
#-W openModeBean.password—Password for access gate if one is set. Use only if securityModeBean.securityModeChoices = "open".	*"password"*
-W simpleModeBean.serverID—Access Server ID. Use value you specified at the Access System Console before installation. Use only if securityModeBean.securityModeChoices = "simple"	*“Access Server ID”*
-W simpleModeBean.hostname—Host name where access server is installed. Use only if securityModeBean.securityModeChoices = "simple"	*"ip_addr"* *or* *"machine_name"*
-W simpleModeBean.accessGateID—AccessGate ID. Use only if securityModeBean.securityModeChoices = "simple"	*"AccessGate ID"*
-W simpleModeBean.portNumber—Port number of the access server. Use only if securityModeBean.securityModeChoices = "simple"	*"port number"*
#-W simpleModeBean.password—Password for access gate. Use only if securityModeBean.securityModeChoices = "simple"	*"password"*
#-W simpleModeBean.passphrase—Pass phrase for the access gate to communicate with the Access Server. Use only if securityModeBean.securityModeChoices = "simple"	*"passphrase"*
#-W simpleModeBean.passphraseVerify—Pass phrase for the access gate to communicate with the access server. This parameter verifies that the pass phrase matches the simpleModeBean.passphrase. Use only if securityModeBean.securityModeChoices = "simple"	*"passphrase"*
-W certModeBean.serverID—Access Server ID. Use the value you supplied at theAccess System Console before installation. This value has to match the one you specified at the Access System Console. Use only if securityModeBean.securityModeChoices = "cert".	*"server id"*
-W certModeBean.hostname—Host name where Access Server is installed. Use only if securityModeBean.securityModeChoices = "cert".	*"ip address"* *"ip addr"* *or* *"machine name"*

Table 42 Silent Installation Parameters for WAS Registry

WAS Registry Parameter—Description	Possible Values
-W certModeBean.accessGateID—AccessGate ID. This value has to match the one you specified at the Access System Console. Use only if securityModeBean.securityModeChoices = "cert".	*"AccessGate ID"*
-W certModeBean.portNumber—Port number of the Access Server. Use only if securityModeBean.securityModeChoices = "cert".	*“port number"*
#-W certModeBean.passwordPassword for Access Gate, if one is set. Use only if securityModeBean.securityModeChoices = "cert".	*"password"*
#-W certModeBean.passphrasePass phrase allowing the AccessGate to communicate with the Access Server. Use only if securityModeBean.securityModeChoices = "cert".	*"passphrase"*
#-W certModeBean.passphraseVerifyPass phrase allowing the Access Gate to communicate with the Access Server. This parameter verifies that the pass phrase matches that of certModeBean.passphrase. Use only if securityModeBean.securityModeChoices = "cert".	*"passphrase"*
-W installOrRequestCertBean.installOrRequest—Determines whether to install or request a certificate to be used to configure the Access System. Used if your security mode is set to "cert". If you already have a certificate, choose "install". If you want NetPoint to request and request a certificate, choose "request".	*"install", "request"*
-W certReqInfoBean.countryName—Country name. This is usually a two-letter country code that is valid for use in DNs. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"country code"*
-W certReqInfoBean.stateOrProvinceName—State or province name. This is usually a two-letter state or province code that is valid for use in a DN. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"state or province code"*
-W certReqInfoBean.localityName—Locality name. This is usually the name of a geographic region. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"locality name"*
-W certReqInfoBean.organizationName—Organization name. This is usually the name of an organization. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*“organization name"*
-W certReqInfoBean.organizationalUnitName—Organization unit name. This is usually the name of a department. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*“organization unit name"*

Table 42 Silent Installation Parameters for WAS Registry

WAS Registry Parameter—Description	Possible Values
-W certReqInfoBean.commonName—Common name. This is usually the name of a person or an entity. It is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*"name"*
-W certReqInfoBean.emailAddress—Email address. This is usually a valid email address. This is part of the information used to request a certificate. Use only if installOrRequestCertBean.installOrRequest = "request".	*“email address”*
-W readyToInstallCertBean.readyToInstallField—If you requested that NetPoint request a certificate, this verifies that the certificate is ready for installation. This is only used if installOrRequestCertBean.installOrRequest = "request". Oblix recommends that you do not use "Yes" for silent mode. You probably cannot take the request generated by NetPoint and receive the certificates faster than the NetPoint installation can run from one step in the installation to the next.	*"Yes" or "No"*
-W copyCertificatesInputBean.certFile—The absolute path including the file name for the certificate file (for example: aaa_cert.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	*"absolute path including the file name"*
-W copyCertificatesInputBean.keyFile—The absolute path including the file name for the key file (for example: aaa_key.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	*"absolute path including the file name"*
-W copyCertificatesInputBean.chainFile—The absolute path including the file name to the chain file (for example: aaa_chain.pem). Use if: installOrRequestCertBean.installOrRequest = "install" or if installOrRequestCertBean.installOrRequest = "request" and readyToInstallCertBean.readyToInstallField = "Yes".	*"absolute path including the file name"*
-W localePanel.defaultLang—Required when extra languages are to be installed with the main installation.	"en-us"
-W localePanel.installLanguagesRequired when extra languages are to be installed with the main installation.	“en-us;fr-fr”

Passport Parameters

Table 43 provides Passport parameters.

Table 43 Silent Installation Parameters for Passport

Passport Parameter and Description	Possible Values
-P passport.installLocation—The installation directory. The default directory is "C:\NetPoint" on Windows and "/NetPoint" on Unix.	"*installation directory*"

Uninstalling a Component Installed With Silent Mode

The method to uninstall a component that was installed using silent mode depends upon your platform.

On Windows—Run:

Component_install_dir\identity|access\oblix_uninstNetPoint component\uninstaller.exe -silent

On Solaris—Run:

Component_install_dir/identity|access/oblix/_uninstNetPoint component/uninstaller.bin -silent

Cloning and Synchronizing Installed Components

Rather than 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 mirrored copy of a component. That is, cloning creates a copy of a component on a local or remote system using an already-installed component as a template. Once a COREid Server or Access Server is cloned, you can:

- Start the cloned server on the remote system
- Reconfigure a cloned server after it has been started
- Partially replicate a configuration by synchronizing two installed components.

On Windows and Unix, in the directory oblix/tools/np_sync, you can use the command np_sync to clone a component. The np_sync tool is described in *"Syntax and Options for np_synch" on page 284*.

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. To synchronize two components, use the -sync or -sync-all command-line options for the np_synch tool.

Note: For the Web server plug-ins WebPass, Access Manager, and WebGate, the Web server configuration files are not updated using np_synch. This must be done either automatically during NetPoint installation or manually afterward, as discussed earlier.

An Example of Using np_synch

Once a NetPoint component has been installed and configured, a command such as:

```
np_sync -clone test2.oblix.com /export/home1/np7test2
```

clones the current machine to the system test2.oblix.com in the directory /export/home1/np7test2.

Syntax and Options for np_synch

The basic syntax for np_synch is as follows:

./np_sync -*mode* [-*opts*] *host destination_dir*

where *mode* is one of the following, sync, sync-all, or clone. For example:

-sync—The -sync command only updates files that are machine independent. These are customization (text) files. This command can be used to upgrade or repair installations on similar platforms. For example, if you have an AIX system and a Solaris system, you should be able to synchronize them.

-sync-all—The -sync-all command includes binaries, shared libraries, executable files, and so on as well as customization (text) files. This command can be used to upgrade or repair installations on similar platforms.

-clone—The -clone option copies the entire installation. This option also requires using the -p *port* and -n *servername* options described below.

where -*opts* is any combination from the following:

-u *username*—Unix only. When you issue the np_sync command to connect to a remote system as a user other than the one you are logged in as, use the -u

username option. This does not change the credentials that you use, but rather changes the user who executes the receiving end of the remote-copy command.

-rsync—Unix only. Use the rsync command (rdist is used by default, see "Unix-Specific Notes" on page 285).

-ssh—Unix only. Use ssh, the secure shell that uses an encrypted connection, to transfer data when using rsync. When using the rsync command, you may use ssh instead of the standard Unix remote shell connection (rsh or remsh).

-path rsyncpath—Unix only. Look for rsync in rsyncpath on the remote system (when using rsync).

-d—Debug mode: do not copy, just indicate what will be updated.

-l *srcdir*—Use *srcdir* as the source directory. By default, the current NetPoint installation area (where this program is located) is used as the source.

-n *servername*—For cloning a COREid or Access Server, you must specify a new NetPoint server name. Use *servername* for the new server.

-p *portnumber*—For cloning a COREid or Access Server, you need to specify a port. Use *portnumber* for the new server port.

Windows Only

-F—Windows only. This option forces an installation (ignore sanity checks). You may use the -F flag to force an installation to take place, even if some normal checks fail. This can be useful for re-executing a cloning operation that failed midway.

-f—Windows only. The -f flag forces a copy, ignoring the file modification times on the remote system, and updates all relevant files.

-r—Windows only. This option reboots the remote host after installation, if necessary. Use this option with cloning if system libraries need to be updated.

See also, "Windows-Specific Notes" on page 286.

Unix-Specific Notes

On Unix, remote copy permissions must be enabled using .rhosts.

The exact list of files to be copied for the -clone, -sync-all, and -sync command options is defined in the np_sync script. You may need to tune these files for special cases.

By default, Unix uses the rdist command to update the remote system. Solaris assumes that rdist exists in /usr/ucb/ on the remote system, so it may not work on a different platform.

The rdist command is not usually shipped on Linux. You can use the rsync program on Linux. The rsync program is not usually shipped with Solaris, HP-UX, or AIX.

On Unix, the remote system must grant permission for remote access, typically by using the .rhosts file of the remote system.The format of this file is any number of lines of the form *host username*, where *host* refers to the system that the copy is coming from, and *username* specifies the user who is permitted to issue the remote copy command.

Windows-Specific Notes

The Windows version of np_sync is an executable program (np_sync.exe).

The definitions for what files are transferred for the -clone, -sync, or -sync-all command options is defined in the patterns file in the np_sync subdirectory on Windows. You may need to tune the patterns files for special cases.

On Windows, the np_sync command automatically mounts the network drives necessary to complete cloning or synchronization. It unmounts the network drives when finished if the user does not interrupt the process.

When cloning on Windows, the np_sync tool also updates the system registry, updates any necessary system DLL files, and installs the appropriate entry in the system services. The np_sync command does not start or stop system services. Use the program NPServMgr.exe, in the directory oblix/tools/NPServMgr/ (on Windows only) to start, stop, add, or remove any NetPoint servers in the Windows system services.

Updating the registry and system services requires the local Windows user to have system administrator privileges on the remote system. To achieve this, use a network administrator login or assign administration privileges to the same user name and password on the remote system.

Note: If the system drive is on a partition other than C: the "-S" or "-R" flag needs to be used.

The np_sync command uses the default system directory C:\WINNT\system32. However, on Windows XP and Windows Server 2003 the system directory is C:\Windows\system32. When the local system or remote system OS version is above Windows 2000, you need to use the following in the np_sync command:

"-S" flag for local system directory
"-R" flag for remote system directory

Uninstalling a Cloned Component

The following sections describe how to uninstall a cloned component on Unix and on Windows.

Uninstalling a Cloned Component on Unix

The procedure to uninstall on Unix systems follows.

To uninstall on Unix

1. If the component is WebPass, Access Manager, or WebGate, delete the Oblix-specific entries in their Web server's obj.conf file.
2. If the component runs a process (COREid Server, Access Server), stop the process.
3. Delete the component's directory.

Uninstalling a Cloned Component on Windows

You cannot uninstall a cloned component using InstallShield. On Windows, uninstallation requires removing registry entries. Installed services must be removed using a utility provided by Oblix.

Uninstalling COREid and Access System

Two procedures follow.

To uninstall COREid and Access Server

1. Uninstall the COREid or AAA service using NPServMgr.exe located in the *Component_install_dir*\access\oblix\tools directory.
   Usage information is displayed by running NPServMgr.exe without any arguments.
2. Delete the registry entries associated with the component.
3. Delete the COREid or AAA installation directory.

To uninstall WebPass, WebGate, and Access Manager

1. Remove the Oblix modifications from the Web server's obj.conf (NSAPI), or the Oblix .dll's and virtual directories (ISAPI).
2. Stop the Web server instance that is hosting the component.
3. Delete the registry entries.
4. Delete the installation directory.

Section VI: Web Server Details

12 Configuring the Apache v1.3 Web Server

This chapter explains how to configure the Apache v1.3 Web server for NetPoint and includes the following topics:

Note: NetPoint also provides a WebGate for the Apache v2.0.4.8 Web server and a WebGate for the IBM HTTP Server powered by Apache v2.0.47. The IBM HTTP Server (IHS) is a variation of Apache v2. For details, see "Configuring Apache and IHS v2 Web Servers for NetPoint" on page 301.

Apache v1.3 Architecture and NetPoint

This section explains how Apache's process-based architecture affects various NetPoint components.

For a COREid Server accessed through WebPass

- Each WebPass instance connects to the COREid Server.

- Each connection takes up system sources, and each connection has *n* file descriptors.
- Set the tuning parameters for Apache so that Apache does not need to start or stop processes too frequently. These settings would be similar with or without NetPoint.

For a WebGate

- There is no shared cache between processes.
- Each process maintains its own connections to the Access Server.
- Because each process has its own connection, you should limit the number of WebGate connections. This issue is partially affected by the performance of the systems running the Web servers and Access Servers.
- Reverse proxy capability may be enabled for Apache Web servers on Solaris and Linux platforms.

For the Access Manager

- Each Web server process is an instance of the Access Manager application.
- Each application maintains its own connections to the directory server. This may not directly affect performance. However, there may be a limit on the directory server side that you may want to consider when other directory server clients are involved.
- Multiple processes respond to a user's request (multiple HTTP events are triggered to build the frames).
- Latency of responses cannot be predicted.
- Fewer processes are better from a UI perspective, but this affects the number of concurrent users.

Apache v1.3 Requirements

Your system must also meet these requirements to implement an Apache or Stronghold Web server:

- Dynamic Shared Object (DSO) support for WebGate and WebPass. On Apache, this means that mod_so must be enabled.

  Note: DSO is required for all NetPoint plug-ins.

  - Multi-threading is required for WebPass.
  - When WebGate and WebPass are installed on the same Web server, DSO and multi-threading for WebPass are required.

- Building the Apache Web server requires access to the gcc and make commands in your path. Alternatively, you can use another ANSI-compliant C compiler.
- Reverse proxy capability may be enabled for Apache Web servers on Solaris and Linux platforms.

Apache v1.3 Web Server Support

NetPoint 7.0 server plug-ins operate with Apache Web server 1.3 and higher. WebGate, WebPass, and Access Manager were ported and tested on Apache version 1.3.29.

Recent versions of Apache 1.3 contain important security fixes. It is strongly recommended that you use the most recent release of Apache 1.3. For details, see:

http://apache.org

The base Apache 1.3 Web server does not use SSL for browser connections (responding to https:// requests). An add-on module for SSL support known as mod_ssl is available at:

http://www.modssl.org

The NetPoint plug-ins for base Apache servers are different from those for Apache with mod_ssl (also referred to as using EAPI).

- NetPoint supports Apache with mod_ssl only.

  Note: openssl is needed by mod_ssl when building Apache to support SSL. openssl should be part of the Apache server built with mod_ssl.

- No SSL-specific features of NetPoint operate with the version of Apache 1.3 known as Apache-SSL.

IHS (the IBM HTTP Server powered by Apache) is a variation of Apache 1.3. IHS uses a different implementation of SSL.

- NetPoint supports only the base IHS (non-SSL) plug-in interface.
- Support for SSL in IHS is anticipated in the near future.

For more information, see “Preparing to Install NetPoint” on page 39 and “Downloading and Compiling the Base Apache Web Server” on page 294.

NetPoint also provides a WebGate for the Apache v2 Web server and a WebGate for the IBM HTTP Server powered by Apache v2. For details, see “Configuring Apache and IHS v2 Web Servers for NetPoint” on page 301. NetPoint also provides support for Access Manager and WebPass components for Apache v2

Web servers running on RedHat Enterprise Linux AS v3.0. For more information, see “Platform Requirements” on page 66.

Downloading and Compiling the Base Apache Web Server

You can download the latest version of Apache 1.3 from the Apache Web site:

http://apache.org

The SSL plug-in mod_ssl is available from:

http://www.modssl.org

These sites point you to other sites for any additional software needed by Apache or mod_ssl (such as openssl). Instructions for compiling the Apache Web server are included with the software distribution.

In order for the Apache Web server to support NetPoint plug-ins, the module mod-so must be compiled into the server binary.

To compile Apache or Apache with mod_ssl with mod-so

1. Include the configuration option before compiling:

   `--enable-module=so`

2. Ensure the configuration meets other NetPoint requirements and compile.

Apache 1.3.29 Release Notes

The following URL contains information about the latest version of Apache and a link to pick up binary files for the Apache server:

http://www.apache.org/dist/httpd/Announcement.html

Other Useful Links

The following links provide information on building an Apache release and source code:

Apache source code—http://www.apache.org/dist/httpd

Mod_SSL source code—http://www.modssl.org/source/

OpenSSL source code—http://www.openssl.org/source/

What is ApacheSSL—http://www.apache-ssl.org/#What_is_Apache-SSL

Compiling and Installing Apache 1.3—http://httpd.apache.org/docs/install.html

ApacheSSL build instructions for Win32—http://www.galatea.com/flashguides/apache-ssl-win32.xml

How to build an Apache Unix release—http://httpd.apache.planetmirror.com/dev/how-to-release.html

How to build a release of Apache for Windows—http://httpd.apache.planetmirror.com/dev/how-to-release-win32

Platform-Specific Compilation Options

Some operating systems require additional options during configuration. Some options listed here may be redundant for some releases of Apache 1.3 but are necessary for other releases.

The following are environment settings for the operating system configuration command on Solaris:

```
CFLAGS=-D_REENTRANT
LDFLAGS=-lpthreads
```

AIX:

```
CFLAGS=-D_REENTRANT
LDFLAGS=-lpthreads
```

HP-UX:

```
CFLAGS=-D_REENTRANT
LDFLAGS="-lcl -lpthreads"
```

On HP-UX, you need to use PA-RISC1 compile options (the default).Do not use PA-RISC2 (64-bit) options. When using PA-RISC2, you will receive load errors such as “missing symbol,” “bad magic number,” or “share object is garbled.” Similar errors may also appear under any operating system when loading Apache EAPI (mod_ssl) compiled modules into a plain Apache server.

Configuring the Web Server for NetPoint

During installation of NetPoint, you can choose to update your Apache Web server configuration file (httpd.conf) manually or automatically. If you choose to update httpd.conf manually, instructions are provided.

To re-update the httpd.conf file after installation, refer to the file oblix/apps/common/docs/config.htm, or use the program ManageHttpConf located in oblix/tools/setup/InstallTools/ManageHttpConf. Running this program without any options will print instructions on its use.

Platform Specific Run-Time Settings for AIX

On AIX, you must set the environment variable AIXTHREAD_SCOPE to the value S (uppercase). Otherwise, there may be a segmentation fault when a worker process exits. This, however, does not affect the delivery of content, authentication, or authorization decisions by WebGate.

Also on AIX, you may wish to place the following directive in the httpd.conf file:

```
AcceptMutex fcntl
```

This directive is only supported in Apache 1.3.24 and later. It does not affect the delivery of content, authentication, or authorization decisions by WebGate. However, those familiar with the behavior of Apache on other platforms (via the /server-status URL) may prefer to use this setting.

Tuning Apache 1.3 and NetPoint Plug-Ins

Apache 1.3 uses a process model for serving multiple http requests at once. This is different from the single process (thread) model employed by other Web servers, which manage several requests simultaneously in one process. Each subordinate Apache worker-process responds to an incoming http request independently of every other worker-process.

Several parameters in the Apache server configuration file (httpd.conf) affect how an Apache server decides to create or destroy worker processes. The following affect the performance of the server:

- **MaxServers**—The number of simultaneous http requests that a system can handle depends on the maximum performance of the system.
- **Performance Tuning**—Performance tuning for a system should be done using an http load generating tool such as the ab program supplied with Apache.
- **MaxSpareServers**—Sets the desired maximum number of idle child server processes. An idle process is one which is not handling a request. If there are more than MaxSpareServers idle, then the parent process will kill off the excess processes.

  To preserve as much state as possible in the server, set the MaxSpareServers to a high value. Setting this value to the maximum of 255 keeps all Apache worker-processes available indefinitely, but it does not provide an opportunity for worker-process recycling during low-load periods.
- **MaxClients**—Sets the limit on the number of simultaneous requests that can be supported; more than this number of child server processes will *not* be created. Any connection attempts over the MaxClients limit will normally be queued, up to a number based on the ListenBacklog directive. Once a child

process is freed at the end of a different request, the connection is then serviced.

- **MaxClientRequests**—Apache provides a safety mechanism to prevent a worker process from slowly acquiring too many system resources to be efficient. Setting MaxClientRequests to a value greater than zero limits the number of requests that a worker process can respond to, after which that process exits, to be replaced by a new, fresh worker process as soon as the need arises. This safety mechanism is not unreasonable, but the start-up delay for NetPoint plug-ins is noticeable at the Web browser.

  If you use this parameter, set it high enough for end users to rarely notice the startup delay. NetPoint plug-ins are designed to run under Web servers without this safety mechanism.

- **MinSpareServers**—Sets the desired minimum number of idle child server processes. An idle process is one that is not handling a request. If there are fewer than MinSpareServers idle, then the parent process creates new children at a maximum rate of 1 per second. Use this with the Access Manager.

  Note: Setting this directive to some value *m* ensures that you will always have at least *n* + *m* httpd processes running when you have *n* active client requests.

  Since NetPoint plug-in initialization is deferred until the first request, using a high value for the MinSpareServers parameter provides minimal advantage. However, it is useful to keep this parameter as high as possible. For dedicated Web server systems, this should pose no great burden.

- **StartServer**—As with the MinSpareServers parameter, the advantage of the StartServers parameter is limited by the delayed initialization of the NetPoint plug-ins.

Appropriate values for the parameters described above depend on the expected load and the performance class of the systems involved, including the Access Server and LDAP server.

Apache servers on very high performance systems with high expected loads may be recompiled with a larger limit on the number of worker processes. These systems may see a greater performance impact on the StartServers and MinSpareServers parameters for dealing with sudden load spikes.

You may need to adjust operating system limits for the Access Server for proper operation. In particular, the maximum number of file descriptors available for any one Access Server may need to be increased beyond the default value. Configuring more than one connection between each Apache-based WebGate and an Access Server may quickly exceed this limit.

Access Manager Tuning Factors

Both Apache and NetPoint configuration parameters can have a considerable impact on Access Manager performance. The following factors should be considered when tuning the Access Manager:

- The idle child processes ensure that a new incoming request is serviced immediately. The more spare child processes, the faster the ramp up.
- Each child process opens separate connections to the directory server. The more child processes you have, the more directory server connections you have.

Assuming that each user is using one browser, there are four to five simultaneous requests to the Web server for images and/or js and/or HTML from the browser. Assuming that there are four simultaneous users, the total number of simultaneous requests to the Web server is 4 * 5 = 20.

Given these factors, Oblix recommends the following to maintain a balance between how fast a new user is serviced and the number of connections to the directory server:

MaxClients = 25
MinSpareServers = 4
MaxSpareServers = 5

Note: The Access Manager does not open connections on Web Server startup. Instead, the Access Manager creates connections on the first request.

To help compensate for any delay when the Access Manager creates connections, the Access Manager may be configured such that all directory server connections for all directory server profiles are set to 1. In this case, the Apache configuration may be as follows:

MinSpareServers = 1
MaxSpareServers = 2
MaxServers = 2

In the case above, the Access Manager responds in a reasonable time with some delay on the initial request.

Installing WebPass on the Apache Server

When starting the NetPoint installation, choose to install the Apache WebPass. When prompted for the Web server configuration file, choose httpd.conf and enter the path information. The httpd.conf file can be found in *Apache_install_dir*/conf.

Starting and Stopping Apache

The following discussions provide information specific to running the Apache server on Unix and Windows:

- "Starting and Stopping Apache on Unix" on page 299
- "Starting and Stopping Apache on Windows" on page 300

Starting and Stopping Apache on Unix

Typically, you perform a single step to start or stop the Apache Web server, as discussed in the procedures below.

To start and stop the Apache Web server on Unix

1. Locate the *Apache_install_dir*/bin.
2. Use the apachectl command.

   For example:

   ./apachectl start

To stop your Apache Web server on Unix

1. Locate the *Apache_install_dir*/bin.
2. Type

   ./apachect1 stop

To start the server with SSL mode

1. Locate the *Apache_install_dir*/bin.
2. Type:

   ./apachectl startssl

Starting and Stopping Apache on Windows

On Windows systems, you typically perform a single step to start or stop the Apache Web server. See the procedures below.

To start the Apache server

1. Change to the *Apache_install_dir*/bin.
2. Enter the following command:

   apache

To stop the server

1. Hold down Control, then type the letter c.

13 Configuring Apache and IHS v2 Web Servers for NetPoint

NetPoint provides components for Apache v2 Web Servers and for the IBM HTTP Server powered by Apache v2. The IBM HTTP Server (IHS) is a variation of Apache v2.

For brevity, this chapter provides details about configuring both Apache v2 Web servers and IHS powered by Apache v2, including:

About NetPoint with Apache and IHS v2

NetPoint provides components for Apache v2 Web servers and the IBM HTTP Server (IHS) Web server as outlined below and described in "Compatibility and Platform Support" on page 306:

- NetPoint 7.0.3 WebPass, Access Manager, and WebGate for Apache v2.0.5.2
- NetPoint 7.0 WebGate for Apache v2.0.48, including reverse proxy if you choose to activate this capability.
- NetPoint 7.0.x WebGate for the IBM HTTP Server (IHS) powered by Apache v2.0.47, including reverse proxy if you choose to activate this capability.

Each platform-specific installation package supports both plain and SSL-capable Apache modes. For example:

AIX—NetPoint7_0_0_power-aix_IHS2_WebGate

Linux—NetPoint7_0_3_linux_Apache2_Access_Manager
Linux—NetPoint7_0_3_linux_Apache2_WebGate
Linux—NetPoint7_0_3_linux_Apache2_WebPass

Solaris—NetPoint7_0_0_sparc-s2_Apache2_WebGate

Windows—NetPoint7_0_0_Win32_APACHE2_WebGate

Earlier NetPoint releases included separate platform-specific installation packages for plain vs. SSL-capable modes. For example, two WebGate files were provided for each platform: the APACHE_WebGate, and the APACHESSL_WebGate.

There have been no functional changes to NetPoint components to support these Web servers. NetPoint authentication occurs through the WebGate using HTTP basic, form, or SSL client certificates as usual. Authorization for Web resources by authenticated users, and simple and multi-domain SSO with other Web servers or applications, also occurs through the WebGate as usual.

Important: Information in this chapter focuses on WebGate. However, it applies to Access Manager and WebPass components equally.

About the Apache HTTP Server

The Apache HTTP Server is an open-source HTTP Web server project of the Apache Software Foundation. The project goal is to provide a secure, efficient and extensible server and HTTP services that meet current HTTP standards.

For more information, see "About Apache v2 Architecture and NetPoint" on page 304.

About the IBM HTTP Server

The IBM HTTP Server (IHS) is a variation of Apache v2. Portions of the IBM HTTP Server are based on software developed by The Apache Group. The IBM HTTP Server component also includes software developed by the OpenSSL Project and software developed by Eric Young.

Details about the Apache architecture and NetPoint, discussed in "About Apache v2 Architecture and NetPoint" on page 304, apply to IHS with the following exceptions:

- Previous versions of IHS required a separate IDS Client to use the mod_ibm_ldap module. With IHS powered by Apache v2.0.47, this is *not* a requirement.
- IHS v2.0.47 supports FIPS 140-2. FIPS support is disabled by default. To enable FIPS support, just add the SSLFIPSEnable directive to the httpd.conf file. Similarly, use SSLFIPSDisable directive to disable FIPS support.
- On AIX, ensure that the appropriate runtime library is installed before you install IHS v2.0.47.

  For example on AIX 5.1, the xlC.rte 6.0 runtime library (for example: xlC.rte.6.0.0.0) must be installed before you install IHS v2.0.47. This library is required on AIX to install and use SSL with IHS v2. You can download this library from the following Web site:

  http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp

About the Apache and IBM HTTP Reverse Proxy Server

Typically, a reverse proxy is used in the following situations:

- To provide Internet users with access to a server behind a firewall
- To balance the load among several back-end servers, or to provide caching for a slower back-end server
- To bring several servers into the same URL space

The proxy_module implements a proxy/gateway for Apache and IHS powered by Apache. The client requires no special configuration; a reverse proxy appears like an ordinary Web server. The client makes requests as usual for content in the name-space of the reverse proxy. It is the reverse proxy that decides where those requests are sent. Content is returned as if the reverse proxy was the origin.

Important: Although the proxy_module can be used to implement a proxy capability for FTP, CONNECT (for SSL), HTTP/0.9, HTTP/1.0, and HTTP/1.1. *Only* the reverse proxy capability is supported with the NetPoint WebGate.

For more information, see “Requirements for Apache and IHS Reverse Proxy Servers” on page 308.

About Apache v2 Architecture and NetPoint

The Apache v2 Web server provides a hybrid multi-threaded, multi-process architecture that is compatible with the thread-safe NetPoint libraries.

Important: Unless explicitly stated otherwise, all details in this discussion apply equally to Apache v2 and IHS v2 Web Servers and to NetPoint Access Manager, WebPass, and WebGate.

In addition to the standard set of modules, the Apache v2 Web server includes Multi-Process Modules (MPMs) to bind network ports on the machine and to accept and process requests. The appropriate MPM must be compiled into the server and activated before you install a NetPoint component for Apache or IHS v2:

- **On Windows**—mpm_winnt is the default MPM on Windows platforms. mpm_winnt can use native networking features rather than the POSIX layer used in Apache 1.3.
- **On Unix**—The prefork MPM is the default MPM for Apache v2 Web servers on Unix platforms. The prefork MPM implements a non-threaded, pre-forking Web server that handles requests in a manner similar to Apache v1.3.

  Note: If you compile Apache on Unix with the mpm_worker_module, you need to modify the thread.c file from the Apache source for the Unix environment as described in “Tips and Troubleshooting” on page 338.

- **On AIX**—The worker MPM is the default MPM for IHS v2 on the AIX platform. The worker MPM implements a hybrid multi-process, multi-threaded server. The most important directives used to control this MPM are ThreadsPerChild and MaxClients. For details, see “Tuning Apache/IHS v2 for NetPoint Plug-Ins” on page 337.

The Apache v2 Web server includes an Apache Portable Runtime (APR) library that provides an interface to platform-specific implementations, assures API developers predictable if not identical behavior regardless of platform, and eliminates the need for conditional compilation #lfdefs. Although backward compatibility is supported with the include/apu_compat.h file, using the Apache v2 APR is recommended.

For more information, see your Apache v2 documentation. See also, “Tuning Apache/IHS v2 for NetPoint Plug-Ins” on page 337.

The Apache architecture affects NetPoint components in different ways, as discussed below. For additional information, see “Compatibility and Platform Support” on page 306.

For a WebPass installed with Apache v1.3 and v2

- Each WebPass instance connects to the COREid Server.
- Each connection takes up system sources, and each connection has *n* file descriptors.
- The tuning parameters for Apache must be set so that Apache does not need to start or stop processes too frequently. These settings would be similar with or without NetPoint.

For an Access Manager installed with Apache v1.3 and v2

- Each Web server process is an instance of the Access Manager application.
- Each application maintains its own connections to the directory server. This may not directly affect performance. However, there may be a limit on the directory server side that you may want to consider when other directory server clients are involved.
- Multiple processes respond to a user’s request (multiple HTTP events are triggered to build the frames).
- Latency of responses cannot be predicted.
- Fewer processes are better from a UI perspective, but this affects the number of concurrent users.

For WebGates installed with IHS and Apache v1.3 and v2

- There is no shared cache between processes.
- Each process maintains its own connections to the Access Server. Therefore, you should limit the number of WebGate connections. This issue is partially affected by the performance of the systems running the Web servers and Access Servers.

Note: NetPoint WebGates can be used in installations that contain WebPass, Access Manager, and WebGates for Apache 1.3.2.7 Web servers. NetPoint provides support for Access Manager and WebPass components for Apache v2 as described in “Compatibility and Platform Support” on page 306.

Limitations of Apache and IHS v2 Web Servers

Due to limitations of the Apache v2 Web server, plug-ins configured for the NetPoint form-based authentication scheme do *not* pass variables when:

- The optional challenge parameter, *passthrough:Yes*, is included in the authentication scheme to pass login credentials through to a post-processing program.
- The form action is a CGI script that dumps all headers and variables passed to it and the method is called using the HTTP POST method.

  For example:

  ```
  <html>
  <form name="myloginform" action="/access/...cgi" method="post">
  ```

Note: If you have two policies, where policy1 protects the CGI script using the NONE authentication scheme, and policy2 protects the resource using form-based authentication with *passthrough:Yes*, you can access the protected resource by providing valid credentials. In this case, redirection to the CGI script occurs, but no variables are passed to it. When the login form has method="GET", the variables are passed across successfully.

Compatibility and Platform Support

The NetPoint WebGate for Apache v2 and IHS v2 may be the only WebGates in your installation or may coexist with WebGates from other supported versions of NetPoint as shown in Table 44.

Table 44 WebGate Compatibility for Apache v2 and IHS v2

NetPoint WebGate Versions	IHS v2.0.47 Apache v2.0.48 With or Without Reverse Proxy
NetPoint 6.1.1.x **Note**: WebGates operate seamlessly.	•
NetPoint 6.5.x.x **Notes**: NetPoint 6.5.0.x, and 6.5.1 releases are included. However, Language Pack installers are not compatible with NetPoint 6.5.2 and 6.5.3, which is an English-only release.	•
NetPoint 7.0	•
NetPoint 7.0.3	See Table 45 on page 307.

Table 45 provides details about current NetPoint support.

Table 45 NetPoint Components and Support for Apache v2 Platform Suport

NetPoint 7.0	Operating System	Apache Web Server v2.0.48 With or Without Reverse Proxy
WebGate	Windows 2000 Advanced Server, SP4 Windows Server 2003, Enterprise Edition	• •
WebGate	Solaris 8 Solaris 9	• •
WebGate	Red Hat Enterprise Linux AS v2.1	•
NetPoint 7.0.3	**Operating System**	**Apache Web Server v2.0.52 Without Reverse Proxy**
WebGate	HP-UX 11i (11.11)	•
WebPass Access Manager WebGate	Red Hat Enterprise Linux AS 3.0	• • •
NetPoint 7.0.x	**Operating System**	**IHS (IBM HTTP Server) 2.0.47 With or Without Reverse Proxy**
7.0 WebGate 7.0.3 WebGate 7.0.3 WebGate	AIX 5.1 AIX 5.2 Solaris 8	• • •

Requirements for IHS/Apache v2 Web Servers

Topics below explain all:

- "Requirements for IHS v2 Web Servers" on page 308
- "Requirements for Apache and IHS Reverse Proxy Servers" on page 308
- "Requirements for Apache v2 Web Servers" on page 308

Important: Unless explicitly stated otherwise, information here applies to WebPass, Access Manager, and WebGate components equally.

Requirements for IHS v2 Web Servers

This discussion identifies specific requirements for IHS v2 with NetPoint. With IHS v2, you do *not* compile any source code to get the binaries. However, the following requirements do apply to IHS v2 Web servers:

- For an SSL-capable configuration on AIX, the xLC.rte.6.0 runtime library is required.
- For an SSL-capable configuration, the GSKit7 is required and can be downloaded from:

  `https://techsupport.services.ibm.com/server/aix.fdc`

Requirements for Apache and IHS Reverse Proxy Servers

As discussed earlier, the proxy_module implements a proxy/gateway. The client requires no special configuration. Although the proxy_module can be used to implement a proxy capability for FTP, CONNECT (for SSL), HTTP/0.9, HTTP/1.0, and HTTP/1.1, only the reverse proxy capability is supported with certain NetPoint Apache and IHS v2 WebGates. For details, see "Compatibility and Platform Support" on page 306.

For Apache Web Servers—To use reverse proxy functions with NetPoint, you need to include the proxy module in the configure command. For example:

--enable-proxy	Apache proxy module
--enable-proxy-connect	Apache proxy CONNECT module
--enable-proxy-ftp	Apache proxy FTP module
--enable-proxy-http	Apache proxy HTTP module

You also need to load mod_proxy and the mod_proxy_http module into the server dynamically. A reverse proxy is activated using the ProxyPass directive or the [P] flag to the RewriteRule directive.

For IHS Web Servers—After installing the IHS Web server, reverse proxy configurations must be completed in the httpd.conf file in the directory below:

IHS_install_dir/conf directory

For more information, see "Activating Reverse Proxy" on page 323.

Requirements for Apache v2 Web Servers

This discussion identifies specific requirements for Apache v2 with NetPoint. Additional information can be found in your Apache documentation:

PATH Variable—On Unix systems, your PATH variable must contain the gcc location before you compile Apache v2. However, the Sun C compiler location must *not* be in your PATH variable. On Windows systems, Apache can be built

using either command-line tools or the Visual Studio IDE Workbench. The command-line build requires that the environment reflect the PATH, INCLUDE, LIB and other variables that can be configured with the vcvars32 batch file.

Multi-Process Module (MPM)—With Apache v2, a default MPM is provided for each platform to bind network ports on the machine and to accept and process requests. Apache must have one, and *only* one, MPM in use at any time. If no MPM is selected during compilation, the default will be loaded into the Web server. You may activate the MPM during compilation.

mod_ssl—NetPoint supports Apache with or without SSL-capable communication. The base Apache Web server does not use SSL for browser connections and will not respond to https:// requests. For SSL-capable communication, NetPoint supports Apache with mod_ssl only. No SSL-specific NetPoint features operate with Apache-SSL.

mod_ssl relies on OpenSSL to provide the cryptography engine; mod_ssl provides an interface to the OpenSSL library. The OpenSSL library provides Strong Encryption using the Secure Sockets Layer and Transport Layer Security protocols.

With previous versions of Apache, the mod_ssl module had to be downloaded separately and compiled into the server. With Apache HTTP Server v2 module, mod_ssl comes as a loadable module that you can enable during configuration.

Multi-threading—Multi-threading is required for WebPass installations with Apache v1.3.27. NetPoint WebGates for Apache v2 can be used in NetPoint installations that contain WebPass, Access Manager, and WebGates for Apache 1.3.2.7 Web servers. NetPoint 7.0.3 provides support for WebPass and Access Managers for Apache v2 Web servers as described in “Compatibility and Platform Support” on page 306.

Dynamic Shared Object (DSO)—DSO support is *required* for all NetPoint plug-ins (WebGate and WebPass). Apache modules that extend basic core server functionality may be either *statically compiled* for permanent inclusion in the Apache binary, or *dynamically compiled* and stored separately to load at runtime without recompiling. With Apache v1.3, mod_so had to be compiled. With Apache v2 on Windows systems, mod_so is a Base module and always included. With Apache v2 on Unix, the loaded code typically comes from shared object files.

Note: Dynamically loaded Apache 1.3 modules *cannot* be used directly with Apache v2. Apache v1.3 modules must be modified to load dynamically or compile into Apache v2.

---

mod_perl—mod_perl embeds the Perl programming language in the Apache Web server. Without Perl, Apache v2 can still be built and installed; however, some support scripts written in Perl cannot be used.

Note: With Apache v.1.3.2x, some operating systems required additional options during configuration. However, to build Apache v2, there is no need to set any additional variables.

Preparing Your Web Server

The methods and steps to prepare your host machine for the NetPoint WebGate installation depends upon the Web server and platform, as discussed in the following task overview.

To use reverse proxy functions with NetPoint, you need to include the proxy module in the configure command, as discussed in "About the Apache and IBM HTTP Reverse Proxy Server" on page 303. See also "Activating Reverse Proxy" on page 323.

Task overview: Preparing your Web server and installing NetPoint

1. Install the IHS v2 Web server or compile and install the Apache v2 Web server as discussed in:
   - "Preparing the IHS v2 Web Server" on page 311
   - "Preparing the Apache v2 Web Server on Unix" on page 315
   - "Preparing the Apache v2 SSL Web Server on AIX" on page 320
   - "Preparing the Apache v2 Web Server on Windows" on page 321
2. Activate reverse proxy capability if desired, as described in "Activating Reverse Proxy" on page 323.
3. Install NetPoint components, as described in "Installing NetPoint" on page 327.
4. Finish Web server configuration, as described in "Verifying httpd.conf Updates for NetPoint" on page 329.
5. Refer to "Tuning Apache/IHS v2 for NetPoint Plug-Ins" on page 337.

Note: In all the procedures that follow, path name variables, modules, and options are examples provided *only* to illustrate the steps. Your environment *will* vary. Refer to your Web server documentation for additional details.

Preparing the IHS v2 Web Server

To prepare your IHS v2 Web server to accept and use the NetPoint WebGate for IHS v2, you need to complete one or more of the following procedures, depending on your environment and requirements:

- "Preparing the IHS v2 Web Server" on page 311
- "Installing the IBM HTTP Server v2" on page 312
- "Setting Up SSL-Capability" on page 313
- "Starting a Secure Virtual Host" on page 314
- "Activating Reverse Proxy" on page 323

When you have completed the appropriate procedures, you are ready to install the NetPoint WebGate for IHS v2.

Preparing the Host for IHS v2 Installation

You need to complete this procedure to set up the host machine before you install the IHS Web server. For additional information, see "Requirements for IHS/ Apache v2 Web Servers" on page 307.

This example illustrates installation on AIX 5.1. Your environment may vary.

To prepare for IHS v2 installation

1. On the host machine, download and install the IBM Developer Kit, Java Technology Edition version 1.4 from the site below:

   `http://www.ibm.com/java/jdk`

   The IBM Developer Kit ships with the WebSphere Application Server on the CD or can be downloaded from the site above.

2. On the host machine, download and install the xlC.rte 6.0 runtime for AIX 5.1, which is required by the GSKit7 runtime executable from the site below:

   `https://techsupport.services.ibm.com/server/aix.fdc`

3. On the host machine, create a new directory in which you will uncompress the IBM HTTP Server install image.

4. On the host machine, download the IBM HTTP Server install image from the Web site below:

   `http://www-306.ibm.com/software/webservers/httpservers/`

5. On the host machine, uncompress the install image in your new directory.

   For example:

```
tar -xf IHS.tar
```

A listing of the following files appears, based on your operating system:

```
gskit.sh
setup.jar
gskta.rte
```
(a GSKit runtime executable for AIX)

You are ready to begin the installation, as described next.

6. Proceed to "Installing the IBM HTTP Server v2" on page 312.

Installing the IBM HTTP Server v2

The procedure below walks you through a typical IBM HTTP Web server installation. Alternatively, you may choose to perform a silent installation. In this case, you use silent.res file with the java -jar setup.jar -silent -options silent.res command. You can customize silent install options by editing the silent.res text file. All options are set to true by default. To disable an option, set its value to false.

To install the IBM HTTP Web server powered by Apache v2

1. Set your path to point to the Java Technology Edition version 1.4 installed on your machine in the previous example.

   For example:

   ```
   export PATH=$PATH:/usr/java14/java/bin
   ```

2. From to the directory where you uncompress the install image, type the following command:

   ```
   java -jar setup.jar
   ```

3. Choose the language in which to run the installation.

   The Welcome to the InstallShield Wizard for the IBM HTTP Server appears.

4. Click Next to dismiss the Welcome screen.

   The license agreement appears.

5. Click I accept the terms of the license agreement, then click Next to continue.

6. Specify the directory name.

   For example:

   ```
   AIX: /usr/IBMIHS/
   ```

7. Click Next to continue.

   Options appear for a typical, custom, or developer installation. When you choose a typical installation, a list will appear with everything included and the size of the image. If you choose a custom installation, a list of components appears and you can clear the box next to the any components you do not want to install.

8. Select the type of installation you would like to perform, then click Next.

   For example:

   ```
   Typical
   ```

   The following message appears. You can click Cancel to stop the installation.

   ```
   Installing IBM HTTP Server. Please wait.
   ```

   The next message also appears. You can click Cancel to stop the inventory update.

   ```
   Updating the inventory.
   ```

9. Click Finish to complete your installation.

10. Stop then start the IHS server using the apachectl commands, as indicated below.

    For example:

    ```
    IHS2_install_dir/bin
    ./apachectl stop
    ./apachectl start
    ```

    where *IHS2_install_dir* is the directory where you installed the IHS v2 Web server.

You may configure the IHS v2 Web server in the following modes either before or after installing the NetPoint WebGate for IHS v2:

- "Setting Up SSL-Capability" on page 313
- "Starting a Secure Virtual Host" on page 314
- "Activating Reverse Proxy" on page 323
- "Installing NetPoint" on page 327.

Setting Up SSL-Capability

If you need to setup SSL-capability, use the procedure below either before or after installing the NetPoint WebGate for IHS v2.

To setup SSL for IHS v2 using the default configuration file

1. Locate and open the file below:

   For example:

   ```
   IHS2_install_dir/conf/httpd.conf
   ```

2. Specify the SSLEnable directive to enable SSL.

3. Specify a Keyfile directive and any SSL directives you want to enable.

4. Stop then start the IHS server, as indicated below.

   For example:

   ```
   IHS2_install_dir/bin
   ./apachectl stop
   ./apachectl start
   ```

   where *IHS2_install_dir* is the directory where you installed the IHS v2 Web server.

5. Continue with the appropriate procedures below:

   - "Starting a Secure Virtual Host" on page 314
   - "Activating Reverse Proxy" on page 323
   - "Installing NetPoint" on page 327.

Starting a Secure Virtual Host

If you need to start a secure virtual host, use the following procedure either before or after installing the NetPoint WebGate for IHS v2.

To start an IHS v2 secure virtual host

1. Locate and open the file below:

   For example:

   ```
   IHS2_install_dir/conf/httpd.conf
   ```

   where *IHS2_install_dir* is the directory where you installed the IHS v2 Web server.

2. Specify the SSLEnable directive in the virtual host stanza of the configuration file, to enable SSL for a virtual host.

   You can specify any directive, with the exception of the cache directives, inside a virtual host.

3. Specify a Keyfile directive and any SSL directives you want to enable for that particular virtual host.

4. Load the mod_ibm_ssl.so using the LoadModule directive in the conf file.

5. Stop then start the IHS virtual host, as indicated below.

   For example:

   ```
   IHS2_install_dir/bin
   ./apachectl stop
   ./apachectl start
   ```

Note: The start and stop instructions for an SSL implementation are the same as non-SSL-capable implementations.

---

6. Continue with the appropriate procedures below:
   - “Activating Reverse Proxy” on page 323
   - “Installing NetPoint” on page 327.

Preparing the Apache v2 Web Server on Unix

This discussion provides an overview and steps to prepare the Apache v2 HTTP Web server for NetPoint on Unix platforms, including Solaris, Unix, Linux, and AIX. See also “Preparing the Apache v2 SSL Web Server on AIX” on page 320.

Apache v2 can be configured, built, and installed plain or as SSL-capable. After downloading and extracting Apache source files, you use a script (configure script on Unix and the makefile.win make script for Windows) to compile the source tree for your environment.

Note: Basic requirements are the same regardless of your platform. However, the remainder of this discussion and the procedures that follow focus on Unix platforms. For more information, see also “Preparing the Apache v2 SSL Web Server on AIX” on page 320.

When you configure Apache v2 on Unix platforms, you specify the installation directory path name using the --prefix= option with the ./configure command. During configuration you enable the modules that are appropriate for your environment. For example, mod_so is included in the server automatically when dynamic modules are included in the compilation. However, you can ensure the server is capable of loading DSOs by including the --enable-so option with the configure command. If you have multiple Perl interpreters installed, you can include the --with-perl option to ensure the correct interpreter is selected during configuration.

In the configure command, you can also include the options to enable mod_ssl, and to activate an MPM. After configuration, you can verify which MPM was chosen using ./httpd -l to list every module that is compiled into the server.

When you finish configuring Apache, you build the various parts that form the Apache package using the make command then install the package under the installation directory you specified with the --prefix= option during configuration.

For steps and examples, see the procedures below and your Apache documentation:

- “To prepare plain Apache v2 for Unix” on page 316
- “To prepare SSL-capable Apache v2 on Unix” on page 317
- “Preparing the Apache v2 SSL Web Server on AIX” on page 320
- “Activating Reverse Proxy” on page 323

In the procedures that follow, path name variables, modules, and options are examples provided *only* to illustrate the steps. Your environment *will* vary. Refer to your Web server documentation for additional details. There is no difference in the build procedure between Apache v2.0.48 and v2.0.52.

To prepare plain Apache v2 for Unix

1. Confirm that your environment meets Apache requirements for the appropriate compiler and build tools, as described in Apache documentation located at:

   `http://httpd.apache.org/docs-2.0/install.html#requirements`

   Note: There are no known restrictions with regard to supported compiler versions for Apache v2 and NetPoint plug-ins. See the Apache documentation.

2. Download a complete, unmodified version of the Apache HTTP Server v2, as described in the Apache documentation.

   For example:

   `http://httpd.apache.org/download.cgi`

   Note: Be sure to download Perl, if needed.

3. Extract (uncompress, then untar) source files from the tarball, as described in the Apache documentation.

   For example:

   ```
   gzip -d httpd-2_0_48.tar.gz
   tar -xvf httpd-2_0_48.tar
   ```

   You can use the step below as an example of configuring the Apache source tree. If you compile Apache on Unix with the mpm_worker_module, see "Tips and Troubleshooting" on page 338.

   Note: To use reverse proxy functions with NetPoint, you need to include the proxy module in the configure command, as discussed in "About the Apache and IBM HTTP Reverse Proxy Server" on page 303.

4. Configure the Apache source tree and enable or activate the desired modules using details in the Apache documentation.

   For example:

   ```
   cd apache_source_dir
   ./configure --prefix=apache_install_dir --enable-so \
   --with-mpm='prefork' --with-perl=perl_interpreter_path \
   --with-port=non_ssl_port_number
   ```

   where *apache_source_dir* refers to the directory where you extracted Apache and *apache_install_dir* refers to the directory where you want to install Apache.

5. Compile the Apache package you configured using the make command.

   For example:

   ```
   make
   ```

6. Install the Apache package in the configured directory path that you specified earlier using the --prefix= option.

   For example:

   ```
   make install
   ```

7. Customize the installation using instructions in the Apache documentation.

   For example, you may need to tune the httpd.conf to set basic values for:

   ```
   ServerName
   User/owner of the WebServer
   Group
   ```

   Note: To view the complete list of values, use the command: ./configure --help.

8. Stop then restart the Apache Web server to test the installation using commands in the *apache_install_dir*/bin directory.

   For example:

   ```
   ./apachect1 stop
   ./apachectl start
   ```

9. Continue with appropriate tasks for your environment, as listed below:

   - "To prepare SSL-capable Apache v2 on Unix" on page 317
   - "Preparing the Apache v2 SSL Web Server on AIX" on page 320
   - "Activating Reverse Proxy" on page 323
   - "Installing NetPoint" on page 327

Note: The following procedure outlines how to prepare an SSL-capable Apache v2 Web server on Unix. The Apache mod_ssl is loadable; however, this installation requires the Open Source toolkit for SSL/TLS. Again, be sure to download Perl, if needed. If AIX is the platform you are using, be sure to see "Preparing the Apache v2 SSL Web Server on AIX" on page 320 for additional information.

To prepare SSL-capable Apache v2 on Unix

1. Confirm that your environment meets Apache requirements for the appropriate compiler and build tools, as described in Apache documentation located at:

   ```
   http://httpd.apache.org/docs-2.0/install.html
   ```

2. Download a complete, unmodified version of the Apache HTTP Server v2 and Open Source, as described in the Apache documentation.

   For example:

   ```
   http://httpd.apache.org/download.cgi
   http://www.openssl.org/
   ```

3. Extract (uncompress, then untar) source files from the tarballs, as described in the Apache documentation.

   For example:

   ```
   gzip -d httpd-2_0_48.tar.gz
   tar -xvf httpd-2_0_48.tar
   ```

   ```
   gzip -d openssl-0_9_6f.tar.gz
   tar -xvf openssl-0_9_6f.tar
   ```

4. Configure the OpenSSL source tree, as described in Apache documentation.

   For example:

   ```
   cd openssl_source_dir
   ./configure -fPIC --prefix=openssl_install_dir
   ```

   where *openssl_source_dir* refers to the directory where you extracted OpenSSL and *openssl_install_dir* refers to the directory where you want to install the configured OpenSSL package.

5. Compile the OpenSSL package in the installation directory you configured using the make command with the --prefix= option.

   For example:

   ```
   make
   ```

6. Issue the make test command to complete any sanity testing of OpenSSL and check the correct version of the tools required.

   For example:

   ```
   make test
   ```

7. Install the OpenSSL package in the configured directory path that you specified earlier using the --prefix= option.

   For example:

   ```
   make install
   ```

8. Configure the Apache source tree and enable or activate desired modules, as described in your Apache documentation.

   For example:

```
cd apache_source_dir
./configure --prefix=apache_install_dir --enable-so \
--with-mpm='prefork' --with-perl=perl_interpreter_path \
--with-port=non_ssl_port --enable-ssl \
--with-ssl=openssl_install_dir
```

where *apache_source_dir* refers to the directory where you extracted Apache; *apache_install_dir* refers to the directory where you want to install Apache; and *openssl_install_dir* refers to the directory where you installed the configured OpenSSL package.

9. Compile using the make command to build the Apache SSL-capable package in the installation directory you configured using the --prefix= option.

   For example:

   ```
   make
   ```

10. Install the Apache SSL-capable package in the configured directory path that you specified earlier using the --prefix= option.

    For example:

    ```
    make install
    ```

    You must explicitly make certificates for the Apache v2 server to enable SSL using the openssl tool located at *openssl_install_dir*/bin/. The make certificate command does not work with Apache v2.

11. Make certificates using the OpenSSL tool in the *openssl_install_dir*/bin directory, as described in your OpenSSL documentation and remember that "Common Name" is the fully qualified host name.

12. Customize the installation using instructions in the Apache documentation:

    - Tune the httpd.conf to set basic values for:

      ```
      ServerName
      User/owner of the WebServer
      Group
      ```

      Note: To view the complete list of values, use the command: ./configure --help.

    - Tune the ssl.conf to set basic values for:

      ```
      Listen 7000
      <VirtualHost _default_:7000>
      ServerName ps0733.persistent.co.in:7000
      SSLCertificateFile /home/qa/software/ws/apache/
        apache-2.0.48_ssl_7000/conf/ssl.crt/server.crt
      SSLCertificateKeyFile /home/qa/software/ws/apache?
        apache-2.0.48_ssl_7000/conf/ssl.key/server.key
      ```

13. Stop then restart the Apache Web server to test the installation using commands in the *apache_install_dir*/bin directory.

    For example:

```
./apachectl stop
./apachectl startssl
```

14. Continue with the appropriate procedures below:
    - "Activating Reverse Proxy" on page 323
    - "Installing NetPoint" on page 327.

Preparing the Apache v2 SSL Web Server on AIX

While building the Apache v2 SSL Web server, the symbols from the OpenSSL Library libssl.a are exported into the httpd executable in Apache. The symbols needed by NetPoint from the OpenSSL library are:

- SSL_get_peer_certificate( )
- i2d_X509( )

During linking and binding on the AIX platform, any unused or unreferenced symbols are deleted. Therefore, the two symbols required by NetPoint are missing from the httpd executable.

You need to use openssl-0.9.7d to compile on AIX (openssl-0.9.7e does *not* compile on AIX). The rest of the steps are the same as on UNIXopenssl-0.9.7d.

Client Cert Authentication—If you are using Client Cert Authentication on the AIX platform, be sure to use AIX 5.2 Maintenance Level 4 with the following hotfix applied for dlsym problem on AIX:

http://www-1.ibm.com/support/docview.wss?uid=isg1IY63366

To prepare the AIX platform for Apache v2

1. Ensure that your AIX platform meets the system requirements for NetPoint, as described in "Preparing to Install NetPoint" on page 39.
2. See details in "Preparing the Apache v2 Web Server on Unix" on page 315 and when building the Apache v2 Web server:
    - Use openssl-0.9.7d to compile the Web server for AIX.
    - Use the make command in the following manner:

    ```
    make MFLAGS=EXTRA_LDFLAGS='-Wl,-bE:OpenSSL_Symbols.exp'
    ```

    where OpenSSL_Symbols.exp is the file containing the two required symbols. The symbol must be exported using the export file only, as shown above.

Note: Do *not* export the symbol on AIX with the following methods:
-bnog : To supress garbage collection of symbols
-bexpal : To export all symbols
-uSymbolName: To export a particular symbol

Preparing the Apache v2 Web Server on Windows

Following are some details about how installing and configuring Apache v2 on Windows differs from Apache v2 on Unix. For more information, see your Apache documentation.

During Installation—Apache will configure files in the \conf subdirectory to reflect the chosen installation directory. If any configuration files in this directory already exist, a new copy of the corresponding file will be written with the extension .ORIG. For example, \conf\httpd.conf.ORIG.

After Installation—Apache is configured using the files in the \conf subdirectory. These are the same files used to configure the Unix version. However, there are a few differences.

You must edit the configuration files in the \conf subdirectory to customize Apache for your environment. These files will be configured during the installation; Apache is ready to run from the installation directory, with the documents server from the subdirectory htdocs. There are many options you should set before starting to use Apache. For example, Apache listens on port 80 unless you change the Listen directive in the configuration files or install Apache only for the current user.

Multi-Threading—Apache for Windows is multi-threaded, which means that it does not use a separate process for each request as Apache does on Unix. Instead there are usually only two Apache processes running: a parent process, and a child which handles the requests. Within the child process each request is handled by a separate thread.

Unix-Style Names—Apache uses Unix-style names internally. The directives that accept filenames as arguments must use Windows filenames instead of Unix filenames. However, you must use forward slashes, not back slashes. Drive letters may be used. However, if a drive letter is omitted, the drive with the Apache executable is assumed.

LoadModule Directive—Apache for Windows includes the ability to load modules at runtime without recompiling the server. If Apache is compiled normally, it will install a number of optional modules in the \Apache2\modules directory. To activate these or other modules, you must use the LoadModule directive. For example, to activate the status module, use the following (in addition to the status-activating directives in access.conf):

```
LoadModule status_module modules/mod_status.so
```

On Unix, the loaded code typically comes from shared object files (.so extension), on Windows this may be either the .so or .dll extension.

Process Management Directives—These directives are also different for Apache on Windows.

Error Logging—During Apache startup, any errors are logged into the Windows event log, which provides a backup to the error.log file. For more information, see your Apache documentation.

Apache Service Monitor—Apache comes with an Apache Service Monitor utility. With it you can see and manage the state of all installed Apache services on any machine on your network. To manage an Apache service with the monitor, you must first install the service. Apache may be run as a service on Windows. For details, see your Apache documentation.

Starting, Restarting, Shutting Down—Running Apache as a service is the recommended method. An Apache service is typically started, restarted, and shut down using the Apache Service Monitor and commands like NET START Apache2 and NET STOP Apache2. You may also use standard Windows service management.

You may work with Apache from the command line using the apache command. Apache will execute and remain running until it is stopped by pressing Control-C. You may also run Apache from the Start Menu during installation.

Note: Pressing Control-C may not allow Apache to end any current operations and clean up gracefully.

Apache Services Accounts—By default, all Apache services are registered to run as the system user (the LocalSystem account). The LocalSystem account has no network privileges through any Windows-secured mechanism. However, the LocalSystem account has wide privileges locally. For details about creating a separate account to run one or more Apache services, see your Apache documentation.

To prepare Apache v2 for Windows

1. Confirm that your environment meets Apache requirements, as described in Apache documentation located at:

   `http://httpd.apache.org/docs-2.0/install.html`

   For Windows installations a list of HTTP and FTP mirrors from which you can download Apache v2 is provided online.

   When you complete the next step, be sure to download the version of Apache for Windows with the .msi extension.

2. Download a complete, unmodified version of the Apache HTTP Server v2 (and OpenSSL), as described in the Apache documentation.

   For example:

   ```
   http://httpd.apache.org/download.cgi
   http://www.openssl.org/
   ```

3. Install Apache v2 (run the .msi file you downloaded and supply requested information), using your Apache documentation as a guide.
4. Locate the .default.conf file, verify new settings, then update your existing configuration file if needed.
5. Start Apache, either in a console window or as a service.
6. Launch a browser and enter the following URL to connect to the server and access the default page.

   For example:

   `http://localhost/`

   A welcome page and a link to the Apache manual should appear. If not, look in the error.log file in the logs subdirectory.

   Once your basic installation is working, you need to configure it properly by editing the files in the \conf subdirectory.
7. Configure the Apache installation for your environment, using the Apache documentation as a guide.
8. Test your customized environment.
9. Continue with the following as needed:
   - "Activating Reverse Proxy" on page 323
   - "Installing NetPoint" on page 327.

Activating Reverse Proxy

The WebGates for Apache v2 and IHS v2 powered by Apache support reverse proxy capability, if you choose to activate this capability. The procedures to implement reverse proxy capability differ, depending on your environment:

- "To activate reverse proxy capability for Apache v2 Web servers" on page 324
- "To activate reverse proxy capability for IHS v2 Web servers" on page 325

Activating Reverse Proxy For Apache v2 Web Servers

For reverse proxy functions with NetPoint, you need to include the Apache proxy module in the configure command for the Web server. You also need to load mod_proxy and the mod_proxy_http module into the server dynamically. A reverse proxy is activated using the ProxyPass directive or the [P] flag to the RewriteRule directive.

Reverse proxy capability is activated using the ProxyPass directive or the [P] flag to the RewriteRule directive. It is *not* necessary to turn ProxyRequests on to

configure a reverse proxy. Access control is less critical when using a reverse proxy (ProxyPass directive with ProxyRequests Off), because clients can contact only the hosts that you have specifically configured. You can control access to your proxy using the <Proxy> control block.

To activate reverse proxy capability for Apache v2 Web servers

1. Review "About the Apache and IBM HTTP Reverse Proxy Server" on page 303.
2. Include the Apache proxy module in the configure command for the Web server, if needed.

   For example:

   ```
   --enable-proxy
   --enable-proxy-connect
   --enable-proxy-ftp
   --enable-proxy-http
   ```

   See the Apache documentation for more information.
3. Use the ProxyPass directive or the [P] flag to the RewriteRule directive to activate a reverse proxy, as shown below:

   ```
   Reverse Proxy
   ProxyRequests Off
   <Proxy *>
     Order deny,allow
     Allow from all
   </Proxy>
   ProxyPass /foo http://foo.example.com/bar
   ProxyPassReverse /foo http://foo.example.com/bar
   ```
4. Control access to your proxy using the <Proxy> control block shown below:

   ```
   <Proxy *>
     Order Deny,Allow
     Deny from all
     Allow from 192.168.0
   </Proxy>
   ```
5. Complete "Installing NetPoint" on page 327, if you haven't yet done so.

Activating Reverse Proxy For IHS v2 Web Servers

Use the following procedure after installing the Web server.

To activate reverse proxy capability for IHS v2 Web servers

1. Review “About the Apache and IBM HTTP Reverse Proxy Server” on page 303.
2. Install the IHS v2 Web server, as described in “Preparing the IHS v2 Web Server” on page 311.
3. Load the modules below by including these lines (uncommented) in the Dynamic Shared Object section of the httpd.conf file in:

   IHS_install_dir/conf/httpd.conf

   ```
   LoadModule access_module modules/mod_access.so
   LoadModule auth_module modules/mod_auth.so
   LoadModule auth_dbm_module modules/mod_auth_dbm.so
   LoadModule include_module modules/mod_include.so
   LoadModule log_config_module modules/mod_log_config.so
   LoadModule env_module modules/mod_env.so
   LoadModule unique_id_module modules/mod_unique_id.so
   LoadModule setenvif_module modules/mod_setenvif.so
   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_connect_module modules/mod_proxy_connect.so
   LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   LoadModule mime_module modules/mod_mime.so
   LoadModule dav_module modules/mod_dav.so
   LoadModule autoindex_module modules/mod_autoindex.so
   LoadModule asis_module modules/mod_asis.so
   LoadModule info_module modules/mod_info.so
   LoadModule cgid_module modules/mod_cgid.so
   LoadModule dav_fs_module modules/mod_dav_fs.so
   LoadModule vhost_alias_module modules/mod_vhost_alias.so
   LoadModule dir_module modules/mod_dir.so
   LoadModule imap_module modules/mod_imap.so
   LoadModule actions_module modules/mod_actions.so
   LoadModule userdir_module modules/mod_userdir.so
   LoadModule alias_module modules/mod_alias.so
   LoadModule rewrite_module modules/mod_rewrite.so
   ```

4. **Directives Under the IfModule mod_proxy.c Tag**—Use the information and examples below to ensure that:

   - Allow and Deny conditions are appropriately commented.

   For example:

   ```
   <Proxy *>
     Order deny, allow
   #    Deny from all
     Allow from all
   ```

```
#Allow from .domain.com
</Proxy>
```

- URLs to be protected are mentioned in *both* the ProxyPass and the ProxyPassReverse directives.

For example:

```
<IfModule mod_proxy.c>
ProxyRequests Off
ProxyPass /testproxy http://bedford: 8809/testrev/
ProxyPassReverse /testproxy http://bedford: 8809/testrev/
ProxyPass /test2 http://bedford: 8809/testrev/
ProxyPassReverse /test2 http://bedford: 8809/testrev/
```

5. Restart the Web server after any modifications to the httpd.conf file.
6. **Testing**—To access the proxy URL, access http://<*proxy_host*>:80/testproxy/

Note: While testing, make sure the URLs have a trailing forward slash. Sometimes resources cannot be accessed without the forward slash at the end.

---

7. **Enabling SSL on Reverse Proxy Server**—Use the documentation on the IHS default page.

   For example, sample SSL settings in the DSO section of the httpd.conf file load the ibm_ssl_module as:

   ```
   LoadModule ibm_ssl_module  modules/mod_ibm_ssl.so
   ```

8. Include the following directives in your httpd.conf file:

   ```
   SSLEnable
   Keyfile /opt/IBMIHS/bin/key.kdb
   SSLClientAuth none
   SSLProxyEngine on
   ```

9. Restart server.
10. Access the Web server URL and confirm that the browser is presented with a certificate.

Note: You can switch back to open mode for the Web server simply by commenting out the above directives and restarting the server.

---

11. **key.kdb**—To generate the key.kdb, use the ikeyman utility (preferrably in GUI mode) provided in the *IHS_install_dir*/bin directory.

Note: The ikeyman utility uses the gsk7bas utility. However, you need to apply fix pack PQ83048 on gsk7bas.

---

12. Complete “Installing NetPoint” on page 327, if you haven’t yet done so.

Installing NetPoint

As discussed earlier, the NetPoint provides one installation package per component per platform, which handles both plain and SSL-capable installations. The NetPoint WebGate (or WebPass or Access Manager) for Apache v2 and IHS v2 may be the only type of WebGate (or WebPass or Access Manager) in your NetPoint environment or may coexist with other NetPoint WebGates (or WebPass or Access Manager). See “Compatibility and Platform Support” on page 306.

Before you begin installing NetPoint, confirm that you have completed all tasks in Table 46. For more information, see individual chapters in this guide.

Failure to complete all prerequisites may adversely affect your installation.

Table 46 NetPoint Installation Checklist

Checklist	NetPoint Installation Prerequisites
	Complete all activities in “Preparing Your Web Server” on page 310.
	Complete activities in “Activating Reverse Proxy” on page 323, as appropriate for your environment.
	Complete all activities in “Preparing to Install NetPoint” on page 39.
	Review Task overview: Installing NetPoint, below.

Installing NetPoint components is similar for all platforms and Web servers. Oblix recommends that you automatically update your Web server configuration for NetPoint when asked during NetPoint component installation.

Task overview: Installing NetPoint

1. Before installing NetPoint, complete all activities in Table 46.
2. **COREid Server**—Locate the appropriate installation package for each NetPoint component and platform and install, set up, and confirm that you have a working COREid Server, as described in “Installing the COREid Server” on page 99.
3. **WebPass**—Locate the appropriate installation package for your platform and complete activities in:
   - “Installing WebPass” on page 121
   - “Manually Updating a Web Server Configuration for NetPoint” on page 328, if needed
   - “Verifying httpd.conf Updates for NetPoint” on page 329
   - “Tuning Apache/IHS v2 for NetPoint Plug-Ins” on page 337

4. **Access Manager**—Locate the appropriate installation package for your platform and and complete activities in:
   - "Installing the Access Manager" on page 159
   - "Manually Updating a Web Server Configuration for NetPoint" on page 328, if needed
   - "Verifying httpd.conf Updates for NetPoint" on page 329
   - "Tuning Apache/IHS v2 for NetPoint Plug-Ins" on page 337
5. **Access Server**—Locate the NetPoint package for your platform and install the Access Server, as described in "Installing the Access Server" on page 187.
6. **WebGate**—Locate the appropriate installation package for your platform and complete activities in:
   - "Installing the AccessGate/WebGate" on page 199
   - "Manually Updating a Web Server Configuration for NetPoint" on page 328, if needed
   - "Verifying httpd.conf Updates for NetPoint" on page 329
   - "Tuning Apache/IHS v2 for NetPoint Plug-Ins" on page 337
7. After installing NetPoint, you can complete the following activities:
   - Configure NetPoint, as described in the *NetPoint Administration Guide.*
   - Customize NetPoint, as described in the *NetPoint Customization Guide.*
   - Perform integrations, as described in the *NetPoint Integration Guide*.

Manually Updating a Web Server Configuration for NetPoint

Oblix recommends that you automatically update your Web server configuration for NetPoint. During NetPoint installation you are asked if you want to automatically update your Web server installation. If you selected No, you must do this manually.

Note: If the manual configuration process was launched during NetPoint installation, you can skip step 1 in the following procedure, which shows the steps for a WebGate Web server.

To manually configure your Web server for NetPoint

1. Launch your Web browser, and open the following file, if needed.

   For example:

/WebGate_install_dir/access/oblix/lang/*langTag*/docs/config.htm

where /*WebGate_install_dir* is the directory where you installed the WebGate.

2. Select the Apache v2 or IHS v2 Web server link.
3. Follow all instructions that appear and make a back up copy of any file that you are required to modify during Web server set up, so it is available if you need to start over.

   Some setups launch a new browser window or require you to launch a Command window to input information, so ensure that you return to and complete all original setup instructions to enable your Web server to recognize the appropriate Oblix files.

   Note: If you accidentally closed the window, return to step 1 and click the appropriate link again.

4. Continue with "Verifying httpd.conf Updates for NetPoint" on page 329.

Verifying httpd.conf Updates for NetPoint

It is a good idea to complete the following procedures to ensure that the Apache or IHS v2 httpd.conf file includes Web server configuration updates for NetPoint. For details, see:

- "Verifying WebPass Details" on page 330
- "Verifying Access Manager Details" on page 332
- "Verifying WebGate Details" on page 334

To update httpd.conf for reverse proxy on IHS Web servers, see "Activating Reverse Proxy For IHS v2 Web Servers" on page 325. To customize httpd.conf for your Web server, see your Web server documentation.

Verifying WebPass Details

The example below shows the WebPass section in the httpd.conf file following an update for NetPoint. Specific details will vary, depending on your environment. This example is provided only to illustrate the type of changes you will see in httpd.conf for NetPoint.

To verify WebPass entries in httpd.conf

1. Locate the updated httpd.conf file on the machine hosting the WebPass.
2. Open the httpd.conf file and ensure that the section that loads the WebPass in your platform is present.

   For example:

```
# Note: Copy the lines below only if they do not already exist in your httpd.conf
##**** BEGIN Oblix NetPoint WebPass Specific ****
include "/home/netpoint/703/wp/identity/oblix/.apacheconfig"
    LoadFile "/home/netpoint/703/wp/identity/oblix/lib/libgcc_s.so.1"
    LoadFile "/home/netpoint/703/wp/identity/oblix/lib/libstdc++.so.5"
<IfModule mod_ssl.c>
    LoadModule OBWebPass_Module "/home/netpoint/703/wp/identity/oblix/apps/
webpass/bin/libwebpassssl.so"
</IfModule>
<IfModule !mod_ssl.c>
    LoadModule OBWebPass_Module "/home/netpoint/703/wp/identity/oblix/apps/
webpass/bin/libwebpass.so"
</IfModule>
obwebpassinstalldir "/home/netpoint/703/wp/identity"
    Alias /identity/oblix  "/home/netpoint/703/wp/identity/oblix/"
<Directory "/home/netpoint/703/wp/identity/oblix/">
        DirectoryIndex index.htm index.html
    </Directory>
<Location /identity/oblix/apps/asynch/bin/asynch.cgi>
        SetHandler asynch
    </Location>
<Location /identity/oblix/apps/common/bin/common.cgi>
        SetHandler common
    </Location>
<Location /identity/oblix/apps/corpdir/bin/corpdir.cgi>
        SetHandler corpdir
    </Location>
```

```
<Location /identity/oblix/apps/admin/bin/corpdir_admin.cgi>
        SetHandler corpdiradmin
    </Location>
<Location /identity/oblix/apps/admin/bin/front_page_admin.cgi>
        SetHandler front_pageadmin
    </Location>
<Location /identity/oblix/apps/admin/bin/genconfig.cgi>
        SetHandler genconfig
    </Location>
<Location /identity/oblix/apps/groupservcenter/bin/groupservcenter.cgi>
        SetHandler groupservcenter
    </Location>
<Location /identity/oblix/apps/admin/bin/groupservcenter_admin.cgi>
        SetHandler groupservcenteradmin
    </Location>
<Location /identity/oblix/apps/help/bin/help.cgi>
        SetHandler help
    </Location>
<Location /identity/oblix/apps/lost_pwd_mgmt/bin/lost_pwd_mgmt.cgi>
        SetHandler lost_pwd_mgmt
    </Location>
<Location /identity/oblix/apps/objservcenter/bin/objservcenter.cgi>
        SetHandler objservcenter
    </Location>
<Location /identity/oblix/apps/admin/bin/objservcenter_admin.cgi>
        SetHandler objservcenteradmin
    </Location>
<Location /identity/oblix/apps/querybuilder/bin/querybuilder.cgi>
        SetHandler querybuilder
    </Location>
<Location /identity/oblix/apps/selector/bin/selector.cgi>
        SetHandler selector
    </Location>
<Location /identity/oblix/apps/admin/bin/servcenter_admin.cgi>
        SetHandler servcenteradmin
    </Location>
<Location /identity/oblix/apps/admin/bin/setup_admin.cgi>
        SetHandler setupadmin
    </Location>
```

```
<Location /identity/oblix/apps/admin/bin/sysmgmt.cgi>
        SetHandler sysmgmt
    </Location>
<Location /identity/oblix/apps/userservcenter/bin/userservcenter.cgi>
        SetHandler userservcenter
    </Location>
<Location /identity/oblix/apps/admin/bin/wrsc_admin.cgi>
        SetHandler wrscadmin
    </Location>
##**** END Oblix NetPoint WebPass Specific ****
```

Verifying Access Manager Details

The example below shows the Access Manager section in the httpd.conf file following an update for NetPoint. Specific details will vary, depending on your environment. This example is provided only to illustrate the type of changes you will see in httpd.conf for NetPoint.

To verify Access Manager entries in httpd.conf

1. Locate the updated httpd.conf file on the machine hosting the Access Manager.
2. Open the httpd.conf file and ensure that the section that loads the Access Manager in your platform is present.

   For example:

```
#*** BEGIN Oblix NetPoint Access Manager Specific ****
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libgcc_s.so.1"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libstdc++.so.5"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobnspr4.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobplc4.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobplds4.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobsoftokn3.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobnss3.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobssl3.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobldap50.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobprldap50.so"
LoadFile "/home/netpoint/703/wp/access/oblix/lib/libobssldap50.so"
Alias /access/oblix "/home/netpoint/703/wp/access/oblix/"
<IfModule mod_ssl.c>
```

```
   LoadModule OBAccessManager "/home/netpoint/703/wp/access/oblix/lib/
webpluginsssl.so"
</IfModule>
<IfModule !mod_ssl.c>
   LoadModule OBAccessManager "/home/netpoint/703/wp/access/oblix/lib/
webplugins.so"
</IfModule>
obinstalldir "/home/netpoint/703/wp/access"
<Location /access/oblix/apps/front_page/bin/front_page.cgi>
     SetHandler obfrontpage
</Location>
<Location /access/oblix/apps/common/bin/common.cgi>
     SetHandler obcommon
</Location>
<Location /access/oblix/apps/admin/bin/genconfig.cgi>
     SetHandler obgenconfig
</Location>
<Location /access/oblix/apps/admin/bin/sysmgmt.cgi>
     SetHandler obsysmgmt
</Location>
<Location /access/oblix/apps/admin/bin/setup_admin.cgi>
     SetHandler obsetupadmin
</Location>
<Location /access/oblix/apps/admin/bin/front_page_admin.cgi>
     SetHandler obfrontpageadmin
</Location>
<Location /access/oblix/apps/admin/bin/wrsc_admin.cgi>
    SetHandler obwrscadmin
</Location>
<Location /access/oblix/apps/help/bin/help.cgi>
    SetHandler obhelp
</Location>
<Location /access/oblix/apps/policyservcenter/bin/policyservcenter.cgi>
    SetHandler obpolicyservcenter
</Location>
#*** END Oblix NetPoint Access Manager Specific ****
```

Verifying WebGate Details

The example below shows the WebGate section in the httpd.conf file. The details will vary, depending on your environment. This example is provided only to illustrate the type of changes you will see in httpd.conf.

To verify the WebGate section in httpd.conf

1. Locate the updated httpd.conf file on the machine hosting the WebGate.
2. Open the httpd.conf file and ensure that the section that loads the WebGate in your platform is present.

   For example:

On Windows

```
#*** BEGIN Oblix NetPoint WebGate Specific ****

<IfModule mod_ssl.c>
LoadModule obWebgateModule
"WebGate_install_dir\access\oblix\apps\webgate\bin\webgatessl.d
ll"
WebGateInstalldir "WebGate_install_dir"
WebGateMode PEER
</IfModule>

<IfModule !mod_ssl.c>
LoadModule obWebgateModule
"WebGate_install_dir\access\oblix\apps\webgate\bin\webgate.dll"
WebGateInstalldir "WebGate_install_dir"
WebGateMode PEER
</IfModule>

<Location "\oberr.cgi">
SetHandler obwebgateerr
</Location>
<LocationMatch "/*">
AuthType Oblix
require valid-user
</LocationMatch>

#*** END Oblix NetPoint WebGate Specific ****
```

On Unix

```
#*** BEGIN Oblix NetPoint WebGate Specific ****

LoadFile "/home/qa/netpoint/703/c1-copy/wg/access/oblix/lib/libgcc_s.so.1"

LoadFile "/home/qa/netpoint/703/c1-copy/wg/access/oblix/lib/libstdc++.so.5"

<IfModule mod_ssl.c>

   LoadModule obWebgateModule "/home/qa/netpoint/703/c1-copy/wg/access/oblix/
apps/webgate/bin/webgatessl.so"
```

```
</IfModule>
<IfModule !mod_ssl.c>
   LoadModule obWebgateModule "/home/qa/netpoint/703/c1-copy/wg/access/oblix/
apps/webgate/bin/webgate.so"
</IfModule>
WebGateInstalldir "/home/qa/netpoint/703/c1-copy/wg/access"
WebGateMode PEER
<Location /access/oblix/apps/webgate/bin/webgate.cgi>
SetHandler obwebgateerr
</Location>
<Location "/oberr.cgi">
SetHandler obwebgateerr
</Location>
<LocationMatch "/*">
AuthType Oblix
require valid-user
</LocationMatch>
#*** END Oblix NetPoint WebGate Specific ****
```

Notes for Unix

When running Apache v2 on HP-UX, do *not* use nobody for User or Group, because shared memory may not work. Instead, use your login name as User Name with a group Group as “Oblix” (or “www” as User Name and “others” as Group Name). On HP-UX, “www” is equivalent to “nobody” on Solaris.

When running Apache v2 on HPUX 11.11, ensure that the AcceptMutex directive in the Apache httpd.conf file is set to “fcntl”. If the directive is not present, add it to the httpd.conf file (AcceptMutex fcntl). For more information, see http://issues.apache.org/bugzilla/show_bug.cgi?id=22484).

For more information about Unix implementations, see “Tips and Troubleshooting” on page 338.

For IHS on AIX

```
#*** BEGIN Oblix NetPoint WebGate Specific ****
   LoadModule obWebgateModule DR/oblix/apps/webgate/bin/webgate.so
   WebGateInstalldir DR
   WebGateMode PEER
   <Location "/oberr.cgi">
      SetHandler obwebgateerr
   </Location>
```

```
   <LocationMatch "/*">
      AuthType Oblix
      require valid-user
   </LocationMatch>
#*** END Oblix NetPoint WebGate Specific ****
```

3. Use the chmod -r username:groupname directory/file to change the User Name and Group Name of a directory or a file.

   When you do this, you need to change the User and Group parameters in the httpd.conf file accordingly.

4. See "Tuning Apache/IHS v2 for NetPoint Plug-Ins" on page 337 for more information and complete any additional steps needed to finish the NetPoint implementation for Apache v2.

Important: You use the following procedure *only* if you need to clear the httpd.conf file of WebGate-related changes, then complete the Apache v2 Web server configuration for the NetPoint WebGate anew.

To start httpd.conf updates anew

1. Restore the original httpd.conf file to remove any NetPoint entries that are present.

2. Update the httpd.conf file for NetPoint using one of the following methods:

   - Either open the file *Component_install_dir*/access/oblix/lang/*LangTag*/docs/config.htm and perform a manual configuration, as described in "Manually Updating a Web Server Configuration for NetPoint" on page 328.

   - Or launch the ManageHttpConf program in *Component_install_dir*/access/oblix/tools/setup/InstallTools/ManageHttpConf without any options to print instructions on its use.

   Note: If the ManageHttpConf program is run with WebGate entries already present in the httpd.conf file, an error message will be printed and the httpd.conf file will not be updated.

   ---

3. Complete activities in "Tuning Apache/IHS v2 for NetPoint Plug-Ins" on page 337, then you are ready to:

   - Configure NetPoint, as described in the *NetPoint Administration Guide.*

   - Customize NetPoint, as described in the *NetPoint Customization Guide.*

   - Perform integrations, as described in the *NetPoint Integration Guide*.

Tuning Apache/IHS v2 for NetPoint Plug-Ins

Unless explicitly stated, information here applies to both Apache and IHS v2, and to NetPoint Access Manager, WebPass, and WebGate components.

Apache 1.3 uses a process model for serving multiple HTTP requests at once. This differs from the single process (thread) model employed by other Web servers, which manage several requests simultaneously in one process. For more information about Apache v1.3 Web Servers and NetPoint, see the *NetPoint 7.0 Installation Guide*.

Note: Only the prefork MPM in Apache v2 uses the same process model for serving HTTP requests as Apache v1.3. For all other MPMs, Apache v2 uses a hybrid process-thread model.

Several directives in the Apache v2 Web server configuration file (httpd.conf) affect how the Apache Web server decides to create or destroy worker processes. The following parameters affect the performance of the Apache v2 Web server:

- **ThreadsPerChild**—This directive sets the number of threads created by each child process. The child creates these threads at startup and never creates more.
  - If you are using an MPM like mpm_winnt, where there is only one child process, this number should be high enough to handle the entire load of the server.
  - If you are using an MPM like mpm_worker, where there are multiple child processes, the total number of threads should be high enough to handle the common load on the server.
- **MinSpareThreads**—This value is only used with mpm_worker. Since NetPoint plug-in initialization is deferred until the first request, there is minimal advantage of keeping high value for this directive. However, it is useful to keep this parameter as high as possible.
- **MaxSpareThreads**—This value is only used with mpm_worker. The value for MaxSpareThreads must be greater than or equal to the sum of MinSpareThreads and ThreadsPerChild or the Apache HTTP Server automatically corrects it.

  Recommendation—Keep the value high. For a dedicated server this will not be a problem.
- **MaxSpareServers**—With Apache v2, this is used only with the prefork MPM model. To preserve as much state as possible in the server, set the MaxSpareServers to a high value. Setting this value to the maximum of 255 keeps all Apache worker-processes available indefinitely, but it does not provide an opportunity for worker-process recycling during low-load periods.

- **MinSpareServers**—With Apache v2, this is used only with the prefork MPM model. Since NetPoint plug-in initialization is deferred until the first request, using a high value for the MinSpareServers parameter provides minimal advantage. However, it is useful to keep this parameter as high as possible. For dedicated Web server systems, this should pose no great burden.
- **MaxClients**—With IHS v2 and the worker MPM, MaxClients restricts the total number of threads that will be available to serve clients. For hybrid MPMs, the default value is 16 (ServerLimit) multiplied by a value of 25 (ThreadsPerChild). To increase MaxClients to a value that requires more than 16 processes, you must also raise ServerLimit.

Appropriate values for the parameters described above depend on the expected load and the performance class of the systems involved, including the Access Server and LDAP server.

Apache servers on very high performance systems with high expected loads may be recompiled with a larger limit on the number of worker processes. These systems may see a greater performance impact on the StartServers and MinSpareServers parameters for dealing with sudden load spikes.

You may need to adjust operating system limits for the Access Server for proper operation. In particular, the maximum number of file descriptors available for any one Access Server may need to be increased beyond the default value. Configuring more than one connection between each Apache-based WebGate and an Access Server may quickly exceed this limit.

For additional information, see your Apache documentation.

Tips and Troubleshooting

When running Apache v2 on HP-UX, do *not* use nobody for User or Group, because shared memory may not work. Instead, use your login name as User Name with a group Group as “Oblix” (or “www” as User Name and “others” as Group Name). On HP-UX, “www” is equivalent to “nobody” on Solaris.

When running Apache v2 on HPUX 11.11, ensure that the AcceptMutex directive in the Apache httpd.conf file is set to “fcntl”. If the directive is not present, add it to the httpd.conf file (AcceptMutex fcntl). For more information, see:

http://issues.apache.org/bugzilla/show_bug.cgi?id=22484).

If you compile Apache on Unix with the mpm_worker_module, you need to modify the thread.c file from the Apache source for the Unix environment.

To modify the thread.c file for the Unix environment

1. Locate the thread.c file.

   For example:

   ```
   APACHE 2.0.52 source/srclib/apr/threadproc/unix/thread.c
   ```

2. Locate the function named apr_threadattr_create(apr_threadattr_t **new,apr_pool_t *pool) in the following code segment:

   ```
   1-----> apr_status_t stat;
   2
   3-----> (*new) = (apr_threadattr_t *)apr_pcalloc(pool,
   sizeof(apr_threadattr_t));
   4-----> (*new)->attr = (pthread_attr_t *)apr_pcalloc(pool,
   sizeof(pthread_attr_t));
   5
   6-----> if ((*new) == NULL || (*new)->attr == NULL) {
   7----->              return APR_ENOMEM;
   8-----> }
   9
   10----->(*new)->pool = pool;
   11----->stat = pthread_attr_init((*new)->attr);
   12
   13-----> if (stat == 0) {
   14----->            return APR_SUCCESS;
   15-----> }
   16----->#ifdef PTHREAD_SETS_ERRNO
   17----->stat = errno;
   18----->#endif
   19
   20----->return stat;
   21
   ```

3. Add the following code *before* line 13 shown above.

   ```
   int stacksize = 1 << 20;
   pthread_attr_setstacksize(&(*new)->attr, stacksize);
   ```

4. Run configure, make, and make install to set up the Apache Web server with the mpm_worker_module.

Helpful URLs

The following URLs provide information about building an Apache release and source code:

Apache v2 documentation—http://httpd.apache.org/docs-2.0/

Apache v2 source code—http://httpd.apache.org/download.cgi

Mod-SSL documentation—http://httpd.apache.org/docs-2.0/mod/mod_ssl.html

OpenSSL documentation—http://www.openssl.org/docs/

OpenSSL source code—http://www.openssl.org/source/

Compiling and Installing Apache v2—http://httpd.apache.org/docs-2.0/install.html#test

IHS—http://www-306.ibm.com/software/webservers/httpservers/doc/v2047/manual/readme.html

14 Setting Up Lotus Domino Web Servers for NetPoint WebGates

Before you can install the NetPoint WebGate with a Domino Web server, you must have properly installed and set up the Domino Enterprise Server.

This chapter provides tips about installing and configuring Lotus Domino to operate with the NetPoint WebGate. Topics include:

Note: The information here presumes that you are familiar with your operating system commands, Lotus Notes, and the Domino Web server.

Installing the Domino Web Server

The following information focuses on Solaris. However, with some modifications, these steps can be used as a guide for other Unix systems.

Note: You will need to register if this is the first time you download from lotus.com

To download the Domino Web server on Unix

1. Download Lotus Domino from the URL below:

   http://www-10.lotus.com/ldd/down.nsf

2. Untar the downloaded file to your staging area. For example:

```
gct@planetearth[/export/users2/gct/temp] 433 : ls
C37UUNA.tar
gct@planetearth[/export/users2/gct/temp] 434 : tar xf
C37UUNA.tar
gct@planetearth[/export/users2/gct/temp] 435 : ls
C37UUNA.tar sol/
```

You need to install Domino as user “root”. The installation script creates soft link, /opt/lotus, to link to your Lotus Domino installation directory.

To install the Domino Web server on Unix

1. Run the install script for the Domino Web server. For example:

```
gct@planetearth[/export/users2/gct/temp/sol] 441 : su root
Password:
root@planetearth[/export/users2/gct/temp/sol] 1 : ls
install* license.txt script.dat sets/ tools/
root@planetearth[/export/users2/gct/temp/sol] 2 :
root@planetearth[/export/users2/gct/temp/sol] 2 : ./install
=========================================================
Domino Server Installation
=========================================================
Welcome to the Domino Server Install Program.
Type h for help on how to use this program.
Press TAB to begin the installation.
---------------------------------------------------------
Type h for help
Type e to exit installation
Press TAB to continue to the next screen.
---------------------------------------------------------
```

   You are asked to select the setup type.

2. Select Setup type. For example:

```
Select Setup type: [Domino Enterprise Server]
```

3. Complete the installation with the following considerations in mind. For example:
   - The default program directory is set to /opt/lotus. You may over write it to another directory. For example, /export/home/WWW/lotus.
   - The default data directory is set to /local/notesdata1. You may also over write this to something else. For example, /export/home/WWW/lotus/data1.
   - Over write Domino UNIX user to own data directory. The default user is set to notes. You may change it to a valid Unix user. For example, *gct* or *root*.
   - Over write "The UNIX user for this directory must be a member of this group". The default group is set to notes. You may change it to a valid Unix group name. For example: oblix.

Important: Be sure to put Domino data directory in your $PATH before you proceed from here.

Setting Up the First Domino Web Server

After successfully installing, you must set up the first Domino server.

To set up first Domino server

1. Run /opt/lotus/bin/http httpsetup.

   By default, Domino will use port 8081.
2. Ensure that port 8081 is not already in use.
3. Launch your browser and enter the URL below. For example:

   http://*hostname*:*8081*
4. Follow instructions on the screen and keep the following in mind.
   - Check HTTP to get the Web server.
   - Ensure the designated administrator has a first and last name.
   - Keep passwords simple, and record them in a safe location. For example, *oblixoblix*.
5. Run all commands as the Unix user that you've configured for this Domino Web server.

Important: Do not run as root.

Starting the Domino Web Server

After successfully setting up the first Domino Web server, you must start it.

To start Domino server

1. Run /opt/lotus/bin/server.
2. Launch your browser and enter the following URL.

   For example:

   http://*hostname*:*80*/names.nsf

   You will be prompted for login name and password.
3. Select Server-Server.
4. Select your intended server.
5. Select Edit Server.
6. Select Ports > Internet Ports > Web.
7. Change the value for TCP/IP port number to your desired port number.
8. Click Save and Close to save all your changes.
9. Restart server /opt/lotus/bin/server.

Enabling SSL (Optional)

Enabling SSL is not mandatory for the NetPoint WebGate. However, if you need to generate a keyring file (.kyr) and its corresponding stash file (.sth) from the Lotus Notes client on a Windows system to the Unix system, steps are provided below.

To generate the keyring and stash files

1. Launch the Lotus Notes Client on your Windows system.

   For example:

   File > Databases > Open
2. Select Server Certificate Admin.
3. Create the key ring file.
4. Create the certificate request.
5. Install the trusted root certificate into the key ring file.
6. Install the certificate into the key ring file.

7. Copy or ftp the newly created keyring file and stash file from the Windows system to your Unix machine.
8. Store both files in your Domino data directory.

To enable SSL

1. Launch your browser and enter the following URL.

   For example:

   http://*hostname*:*port*/names.nsf

   You will be prompted for login name and password
2. Select Server-Server.
3. Select your intended server.
4. Select Edit Server.
5. Select Ports > Internet Ports > Web.
6. In the SSL Key file name field, enter the absolute path to the keyring file.
7. Change the SSL Port number value to your desired port number.
8. Enable SSL port status.
9. Select Client Certificate “Yes” for NetPoint Client Certificate authentication.
10. Click Save and Close to save all your changes.
11. Restart the Web server.

    For example:

    /opt/lotus/bin/server

Installing a Domino Security (DSAPI) Filter

The Domino security API filter, DSAPI, is an authentication method that allows you to register a DLL with the Domino Web server. In this case, the Web server calls the WebGate DLL to authenticate the user when a request for authentication occurs rather than using SSL or basic authentication.

Authentication within Domino is optional with the NetPoint DSAPI filter. You can implement certain aspects of authentication that the default Web server does not support.

Task overview: Completing WebGate and filter installation

1. Before you install the WebGate on a Domino Web server, complete all steps described above.
2. Complete the WebGate installation and Web server update as described in "Installing the AccessGate/WebGate" on page 199.
3. See "Completing the WebGate Installation" on page 346 and choose one of the two options discussed there.

Completing the WebGate Installation

To ensure the Domino Web Server can use the WebGate DLL, you need to edit the enter the name or names of the DLL/DLLs (DSAPI libraries) to be called for authentication in the DSAPI filter file names field of the HTTP tab under the Internet Protocols tab in the Server document.

Note: Relative paths will be based on the Domino executable directory. DSAPI filter libraries will be called to handle events in the order they appear in this list.

There are two ways to install the filter:

- Through a Web browser and names.nsf (option 1)
- Through a Lotus Notes workstation and the Address Book (option 2)

Option 1: To setup the DSAPI filter to access names.nsf

1. Go to the names.nsf URL and log in. For example:

   http://*hostname*:*port*/names.nsf
2. Click the Server-Servers link.

   A Java applet will be loaded.
3. Select a server from those listed.
4. Click the Edit Server link to go to Edit mode.

5. Click the Internet Protocols link.

   By default, the HTTP tab is selected and information is displayed in Edit mode.

6. Look for DSAPI where it says “DSAPI filter file names:”, then type in the absolute path to the libwebgate.so file.
7. Save your changes.
8. Restart the Domino http server task.

Option 2: To access the Address Book through Lotus Notes

1. Open Domino Name and Address book. For example:

   File >Database > Open > Address Book

2. Switch to server view and open the server document.
3. Edit the server document.
4. Click the Internet Protocols tab.

   By default, the HTTP tab is selected and information is displayed in Edit mode.

5. Look for DSAPI where it says “DSAPI filter file names:”, then type in the absolute path to the libwebgate.so file.
6. Save your changes.
7. Restart the Domino http server task.

Tips

The following tips may be helpful in your installation:

Failure Authentication Event—For Domino Web servers, the redirection of a URL through NetPoint may not work if the authentication type is set as Basic Over LDAP and the URL to be redirected is mentioned as one of the following:

Either a relative path present on the same Web server

Or the Full path URL on the same Web server containing a machine name defined in the host identifier string combinations.

To overcome a failure authentication event, you must set the redirected URL with a machine name that is *not* defined under the host identifier group. For example, the IP address of the machine.

This problem does *not* occur with a form-based authentication type.

Header Variables—It may not be possible to pass header variables other than REMOTE_USER to WebGates installed on Lotus Notes Domino Web servers when using Client Certificate authentication scheme.

For example, header variables cannot be set on the one request where Client Certificate authentication occurs. However, all other requests do allow header variables to be set.

See the *Release Notes* for the latest information.

Section VII:

Troubleshooting

15 Troubleshooting

This chapter describes how to access the NetPoint knowledge base. It also describes common troubleshooting issues related to NetPoint installation and setup.

This chapter covers the following topics:

The NetPoint Knowledge Base

You can search the PremiumCare Online Portal Knowledge Base for resolved problems and other information. You can search the knowledge base by product, category, keywords, or phrases.

The knowledge base is available for PremiumCare Online Portal registered users. If you have a current support contract, you may register to use the PremiumCare Online Portal at:

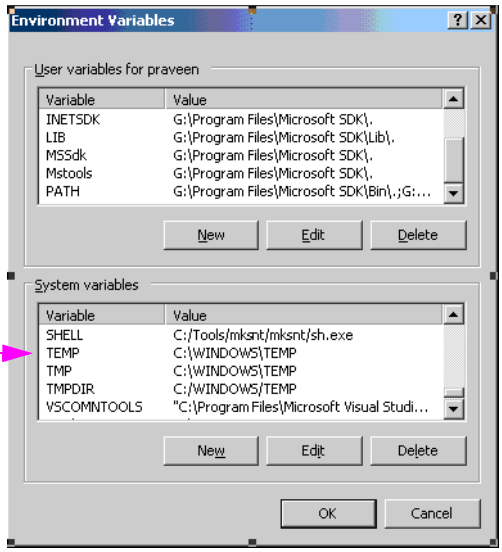
https://customers.oblix.com/public/other/register/pre_reg.cfm

This link provides instructions for registration. Once registered, click the Search for Knowledge link to access the Knowledge Base.

Access Manager Issues

You need to set the TEMP environment variable to point to a valid directory. Oblix recommends that you do this for the entire system, as shown above. However, you can also set the TEMP variable for the IIS user.

Set TEMP to a Valid Directory for the Entire System



Without this variable, the Access Manager attempts to create temporary intermediate files in the root directory and if IIS doesn't have permission to create the files at that level, you may see an error in the following circumstances. For example:

- When setting up the Access Manager

- When selecting either the Access Manager or Access System Console link from the Access System Console main page

  In this case, you may see an error message on setup pages warning about not being able to locate the TEMP directory.

Cannot Delete Access Manager Policy Profile

Symptom—You receive the message below

"You cannot delete the Directory Server Profile that accesses the Policy base."

after uninstalling the optional Access Manager and deleting the setup* and config* files in *AccessManager_install_dir*. You may be able to delete the Access Manager profile for user and configuration data from the COREid System Console, but not the profile for policy data.

Solution—After uninstalling the optional Access Manager, you need to complete the steps below before you can remove remaining Access Manager policy profiles.

To delete a leftover Access Manager policy profile

1. Uninstall the Access Manager.
2. In the directory server, remove all oblix-related entries and be sure to delete the obpolicybase attribute from the top node.

   For example:

   o=Oblix,o=oblixdata,c=uk
3. Restart the COREid Server.
4. In the COREid System Console, delete the Access Manager policy profile.

See the following topics for more information about issues that may affect the Access Manager:

- "Active Directory Search Halts" on page 359
- "Dynamically-Linked Auxiliary Classes" on page 360
- "Windows 2000 Users Cannot Log in After Installation" on page 366
- "Unable to log in to NetPoint on IIS" on page 367
- "Restricting Access to NetPoint" on page 367

Browser Issues

The following issues are browser specific:

- "Microsoft Internet Explorer 6 with Sun VM v1.4.2_04" on page 354
- "Unable to Authenticate Resource" on page 354

Microsoft Internet Explorer 6 with Sun VM v1.4.2_04

With this configuration, when you create a container limits policy and specify a user to receive notification for a containment limit event then click Done in the Person Selector you may notice that the Save, Cancel, and Reset buttons do not appear and the policy cannot be saved.

To work around this problem

1. Open the oblixbaseparams.xml file:

   COREid_install_dir\identity\oblix\apps\common\bin\oblixbaseparams.xml

2. Locate the section "applet_customizations" and find the subsection for the applet where the problem is observed.

   For example:

   containmentlimit_applet subsection

3. Adjust the width and height parameters suitably for this applet to resolve the issue.

   For example:

   modify the applet_dimension_height parameter to a value of 530

4. Restart the COREid Server.
5. Open a new browser window and view the same applet.

Unable to Authenticate Resource

Symptom—You receive Unable to Authenticate Resource errors on Internet Explorer.

Cause—Internet Explorer provides the advanced option to always convert UTF characters in URLs. NetPoint automatically does this as well. Having both enabled causes authentication errors.

Solution—Complete the steps below to remedy "Unable to Authenticate Resource" errors on IE.

To remedy this

1. Set the doUtfConversion parameter to YES and save your changes.

   Note: If you set this after importing the UTF8 data, restart the Web server, close all browsers, and open a new browser window. Today, NetPoint does not support non Latin-1 languages. While data can be stored in UTF8, NetPoint supports only Latin-1 languages.

2. Open the globalparams.xml/lst file in a text editor.

   This file is stored in two locations, and both must be edited:

   *COREid_Server_install*dir\identity\oblix\apps\common\bin\globalparams.xml

   *Access_Server_install*dir\access\oblix\apps\common\bin\globalparams.lst

3. In Microsoft Internet Explorer, select Internet Options from the Tools menu.
4. In the Internet Options dialog box, select the Advanced tab.
5. Under Browsing, deselect the Always sent URLs as UTF-8 check box.

COREid System Issues

This discussion covers the following COREid Server issues that may arise:

Application Has Not Been Set Up

Under certain circumstances, you may want to use an existing COREid Server name. For example, you may want to use an existing COREid Server name if you are rolling NetPoint out from a test environment to a production environment or if you need to remove a COREid Server for some reason.

If you do not delete the original COREid Server name from the System Console, a login following set up of a new instance may result in the message "Application has not been set up". Special steps must be taken to ensure you can set up the application and login when recycling a COREid Server name.

Cannot Set Up COREid System

When COREid and WebPass are installed in Cert mode using certificates issued by a subordinate CA, you may see a blank page when you click the COREid System Console link to start COREid System setup. The event viewer may show a NetPoint error without specifying any cause.

When using certificates generated by a subordinate CA, the root CA's certificate must be present in the *xxx*_chain.pem along with the subordinate CA certificate. Both certificates must be present to ensure appropriate verification and successful COREid System setup. For more information, see the information on transport security modes in the *NetPoint 7.0 Administration Guide Volume 1*.

COREid Server Does Not Start

Symptom—During COREid setup you are asked to restart the COREid and Web servers. After a long wait, the browser returns a message, “The page cannot be displayed”.

Cause—Your Web browser may time out waiting for a COREid server response after specifying directory server details and automatically configuring user object classes, and Group object classes because the schema update may exceed the browser’s timeout.

Solution—Wait for a minute or so and refresh the browser to continue.

If the COREid Server does not start, there are three items you can check that may cause the issue.

To troubleshoot the COREid Server

1. Ensure that the LDAP directory is clean. For example:
   a) Is the configuration branch empty?
   b) Does the configuration branch have the right data?
   c) Does the configuration branch have data from a previous install with a different COREid server entry?
2. Confirm that the files below are correct and in the correct folder:

   COREid_install_dir\identity\oblix\config\configinfo.xml
   COREid_install_dir\identity\oblix\config\ois_server_config.xml
   COREid_install_dir\identity\oblix\config\setup.xml
3. Verify that the port chosen for the COREid Server is not already in use by another application.

Could Not Get Any DB Profile

Symptom—You receive a message “Could Not Get any DB Profile used by COREid2 during initialization of DBManager. Please verify that there exists enabled DB profile for COREid2”.

Cause—This can occur when you:

a) Install a second (or later) COREid Server

b) Answer Yes during installation when asked if this is “the first COREid Server in the network for this LDAP directory server”.

c) Restart the COREid and Web servers.

Solution—Uninstall the COREid Server, then reinstall the COREid Server and answer No when asked if this is “the first COREid Server in the network for this LDAP directory server.

Checking Access Server or COREid Availability

To see if Access Server is running, Telnet to it using the port it is listening to. The following is a Telnet session to an Access Server running on a server named myserver.mycompany.com running on Port 6021:

```
myserver% telnet myserver.mycompany.com 6021
Trying 192.168.5.18. . .
Connected to myserver.mycompany.com.
Escape character is ‘^]’.
^]
telnet> q
Connection closed.
myserver%
```

In the example above, the system’s response:

```
Connected to myserver.mycompany.com.
Escape character is ‘^]’.
```

indicates that the Access Server accepted the Telnet request and is operational. If you cannot connect to the server on the port it was installed to listen on, there is a problem with the Access Server. Possible problems include:

- The connection is blocked by a firewall
- The server is not running

Check the firewall to see if the connection is open. Check the Access Server process to see if it is running. At the Access System server, you can use the netstat command to verify that the server is communicating through the ports you specified when you installed the Access Server.

WebPass Identifier Not Available After Setup

The COREid Server identifier that you enter during installation must be unique and must differ from the WebPass identifier that you enter during WebPass installation.

If the WebPass identifier you enter during installation matches the COREid Server identifier entered during the COREid Server installation, the WebPass identifier is not created and will not be available in the COREid System Console after setup.

To reconfigure the WebPass

1. Locate the setup_webpass utility.

   For example:

   WebPass_install_dir\identity\oblix\tools\setup\setup_webpass.exe.

   where *WebPass_install_dir* is the directory where you installed the WebPass (c:*NetPoint*\identity, for instance).

2. Run the setup_webpass utility with the following options:

   setup_webpass -i <*WebPass_install_dir*> [-q] [-n <*WebPass ID*>]

   [-h <OIS hostname>] [-p <OIS port #>] [-s <open|simple|cert>]

   [-P <simple|cert mode password>] [-c (request|install)]

   [-W iis]

To change the WebPass password for simple/cert mode

1. Locate the setup_webpass utility.

   For example:

   WebPass_install_dir\identity\oblix\tools\setup\setup_webpass.exe

2. Run the setup_webpass utility with the following options:

   setup_webpass -i <*WebPass_install_dir*> -k

To reconfigure Webpass mode

1. Locate the setup_webpass utility.

   For example:

   WebPass_install_dir\identity\oblix\tools\setup\setup_webpass.exe.

2. Run the setup_webpass utility with the following options:

   setup_webpass -i <*WebPass_install_dir*> -m

Directory Server Issues

The following discussions identify several directory server issues:

- "Active Directory Issues" on page 359
- "Siemens DirX Issues" on page 361

Active Directory Issues

See the following topics for more information:

- "Active Directory Search Halts" on page 359
- "ADSI Cannot Be Enabled for this DB Profile" on page 359
- "Dynamically-Linked Auxiliary Classes" on page 360

Active Directory Search Halts

Symptom—400 policy domains were created in NetPoint, each with 10 resources and 10 policies. The limitAMPolicyDomainResourceDisplay is set to true in the Access Manager globalparams.lst file. When the Search icon is selected an error page appears stating "The following messages were produced by the product. Please contact your webmaster to fix the problem."

Cause—The number of policy domains exceeds the current limit.

Solution—Do not exceed 350 policy domains with Active Directory.

ADSI Cannot Be Enabled for this DB Profile

NetPoint supports changing the user data DB profile between ADSI and LDAP using the NetPoint System Console. However, NetPoint does not support changing the Oblix and/or policy DB profile between ADSI and LDAP using the NetPoint System Console.

Symptom—Suppose you have user data stored in an Active Directory forest using LDAP and NetPoint configuration and policy data stored in another Active Directory forest using ADSI. When you change the ADSI flag in the Oblix data DB profile to LDAP using the NetPoint System Console and restart NetPoint servers and services, the ADSI flag remains enabled and the message below appears:

> "ADSI can be enabled for either User or Oblix DB Profile if they are in a separate forest. ADSI Cannot be Enabled for this DB Profile."

Further, attempting to modify the user data DB profile to ADSI produces an error because NetPoint recognizes the DB profile for Oblix and policy data as ADSI enabled.

Solution—Rerun the setup program to modify the DB profile for Oblix configuration and policy data.

Dynamically-Linked Auxiliary Classes

If you installed Active Directory with Windows Server 2003 and experience difficulty with dynamically-linked auxiliary classes, ensure that you have completed all items below. For more information, see "Installing NetPoint with Active Directory" on page 379.

Task overview: Enabling dynamically-linked auxiliary classes

1. Before NetPoint installation, you must ensure that the Active Directory domain and forest functionality are operating at a Windows 2003 Server level.

   You must raise both the domain and the forest to a Windows 2003 Server level, as described in the Microsoft documentation.

2. During COREid System installation and set up, you must specify dynamically-linked auxiliary classes when asked.

3. During Access Manager installation and set up, you must specify dynamically-linked auxiliary classes when asked.

4. During Access Server installation, you must specify dynamically-linked auxiliary classes when asked.

5. After setup, it's a good idea to verify that the dynamicAuxiliary flag is set to true in the files below:

   COREid_install_dir\identity\oblix\data.ldap\common\ldapconfigdbparams.xml
   AccessManager_install_dir\access\oblix\data.ldap\common\ldapconfigdbparams.lst
   AccessServer_install_dir\access\oblix\data.ldap\common\ldapconfigdbparams.lst

   NameValPair ParamName= "dynamicAuxiliary" Value= "true"

   - NetPoint also sets a dynamicAuxiliary tag to true in the following file:

     COREid_install_dir\identity\oblix\config\setup.xml

   Note: The directory is the best place to look for any static associations.

6. Configure NetPoint for dynamically-linked auxiliary class support, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

Siemens DirX Issues

With Siemens DirX, all user attributes with string/integer syntax need to include “Ordering Matching Rule” in their attribute syntax definitions. Without this, NetPoint searches with conditions “<=” and “>=” on these attributes and doesn’t give the expected results because Siemens DirX doesn’t have any default ordering matching rule.

For example, the attribute “cn” has syntax Directory string (this attribute is present in gensiteorgperson).

You can modify the schema and add the matching rule caseIgnoreOrderingMatch for cn. See the DirX documentation for more details.

IIS and Windows Issues

The account that performs NetPoint installation must have administration privileges. The user account that is used to run the COREid Server and Access Server services must have the “Log on as a service” right, which can be set through Administrative Tools > Local Security Policy > Local Policies > User Rights Assignements > Log on as a service.

On IIS 6 Web servers only, you must run the WWW service in IIS 5.0 isolation mode. This is required by the ISAPI postgate filter. During NetPoint installation, this is usually set automatically. If it is not, you must set it manually for the Default Web site.

Installation Issues

The following issues arise during or immediately after installation.

Access Server Installation Halts

Symptom—The Access Server installation halts with a message explaining that there is no DB profile for this server.

Solution—Perform these steps:

1. Navigate to the NetPoint Access System Console from your browser by specifying the URL of the WebPass instance for the Access Manager. For example:

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

   where *hostname* refers to Web server host of the WebPass instance; *port* refers to the HTTP port number of the WebPass Web server instance; /access/oblix targets the Access System Console.

2. Select the Access System Console link, then log in as a user with NetPoint Administrator privileges.

3. Select the Access System Configuration tab, Access Server Configurataion in the left column, and *AccessServer_Link*. For example:

   Access System Configuration > Access Server Configurataion > *AccessServer_Link*

4. Click the Associate DB Profiles button at the bottom of the details page.

   Associate DB Profiles

5. Click the AccessServer_default_user_profile link at the bottom of the page.

   AccessServer_default_user_profile

6. Confirm that AAA Servers is checked, with either All Servers or the appopriate servers identified. For example:

   AAA Servers
   All Servers

7. Confirm that the profile is enabled, at the bottom of the page. For example:

   Enable Profile

8. Click Save.

9. Log out and continue the Access Server installation.

CGI Programs Do not Run After Installation

Symptom—Your Web server's CGI programs do not run after you install NetPoint.

Solution—Perform these steps:

1. In the ../https:*server name*/config directory obj.conf file, add this line above the other Oblix Init functions:

   ```
   Init fn="Init-cgi" timeout-300 LateInit="yes"
   ```

   Type the line exactly as shown above.

2. Restart your Web server.

File Replace Warning When Installing on Windows

Symptom—When installing a COREid Server on a new machine, sometimes the installer attempts to replace the winnt/system32/Msvcrt.dll file with an updated one. Because this file is locked by Windows, you get “File is locked cannot replace” message.

Cause—The NetPoint installer sometimes attempts to replace a file that is locked by the Windows operating system.

Solution—Click Restart in the warning box to replace the DLL.

Installation Fails with a “bad credentials error (49)”

Symptom—COREid Server installation in GUI mode may fail with a “bad credentials error (49)”, though the credentials are valid.

Cause—Known problems with third-party Installshield's ISMP framework. If any inputs supplied during installation contain the character $, the installer might interpret it unpredictably. For example, if the bind password supplied during the schema update for the first COREid Server is Admin$$, ISMP interprets this as Admin$ while invoking the schema update tool and the update fails citing a "bad credentials error(49)".

Suggested Workaround—If this problem is observed during invocation of a particular tool, you may run that tool from the command line.

Note: Every NetPoint installer that uses the same password may also fail with a credential problem of some type.

Installer Prompts to Replace DLL Files

Symptom—During a subsequent installation of a NetPoint component on the same machine, or when installing a second instance of a NetPoint component on the same machine, the user is prompted to replace one or more of the following DLL files even if the files had been updated during a previous installation:

- authn_valicert.dll
- authn_valicert_d.dll

- messagedll.dll
- mtl70mt.dll

Cause—The above DLLs are not NetPoint DLLs. Because these DLLs do not contain version information, NetPoint uses a DLL's data stamp to evaluate whether the file needs to be replaced. Upon subsequent installations, the user is prompted to replace the file because the date stamp is older.

Solution—Click OK to replace the DLLs.

Performing Unix Installation in GUI Mode

Symptom—When starting a GUI installation on Unix, you may receive a warning regarding fonts and scroll bars.

Solution—These warnings can be ignored. They indicate a change in the appearance of the installation wizard GUI.

Quitting a Windows Installation

Symptom—If you terminate the Windows installation wizard abnormally (such as by hitting Control+C or terminating it from the Task Manager), the wizard is not able to properly clean up its files and leaves a large amount of data in the TEMP directory.

Solution—Delete these files manually.

Running as Non-Root User When Installing on AIX

To run Install Shield as a non-root user on AIX, set the environment variable as:

AIX_ISMP_SUPPORT=NONROOT

Installing WebGate with Apache Web Server on AIX

Symptom—You install WebGate on an Apache Web server running on AIX in SSL mode. You make changes to httpd.conf file from the sample.obj.conf file. The Apache Web server fails to start after changing the httpd.conf file. You may receive this message:

"Name of server certificate chain file is hardcoded as ca.cert in the httpd.conf file."

Solution—Change the Server-Certificate-Chain-filename to match the actual name of the server certificate chain file for the user.

Specifying Installation Directories

Install the NetPoint components COREid System, Access Server, and WebGate in directories that have only normal alphanumeric characters in their pathname.

Testing Your Installation

Once you finish installing NetPoint, test your installation.

To test a NetPoint installation

1. Close all browsers.
2. Shut down your Access Server.
3. Try to open a page protected by NetPoint.

   You should receive a NetPoint operation error indicating it was unable to authenticate your login.
4. Restart the Access Server and the Web server.
5. Attempt to connect to the same page as in Step 3.

   The page you specified should open.

Unable to Leave Person Object Class Page

Symptom—You cannot get past the Person object class page during installation and setup.

Cause—Your directory schema is probably invalid.

Solution—Review the changes you made to the directory schema to see if you have done them correctly.

Login Issues

This discussion covers the following issues that may arise during login:

COREid Server Logged You In, Access System Logged You Out

The message "COREid Server Logged You In, Access System Logged You Out" could be triggered by one or more events. For example:

- You did not restart the COREid servers after setting up Access System components.
- The COREid and Access Servers are running on different machines and the clock is set to a different time.

  In this case, change the login slack parameter or synchronize system clocks.
- You have protected the COREid System with a policy domain but not the Access System, or vice versa.

  Both systems must be protected.
- The shared secret needs to be regenerated.

To regenerate a shared secret

1. Delete the shared secret from the directory server.
2. Log in to the COREid Server to regenerate the shared secret.

Windows 2000 Users Cannot Log in After Installation

Symptom—Users are unable to log in after NetPoint installation.

Cause—When you import user data into Active Directory, all passwords are cleared. This is a security feature of Active Directory.

Solution—In the Active Directory User and Computer MMC, be sure the Change password on next login check box is *not* selected. Have your users change their passwords.

In the Access Manager, enable access control for the Password attribute. This forces users to create a service ticket to change their passwords.

Receiving Repeated Login Prompts

Symptom—Users receive repeated login prompts.

Cause—This can occur when you install NetPoint on a Web server that has security policies enforced through a Web browser.

Solution—Enable NetPoint security and disable the browser's security.

Unable to log in to NetPoint on IIS

Symptom—Users may experience unpredictable behavior when they attempt to browse the /identity or /access directory or click the System Console and Access Manager links (such as receiving File Download dialog boxes).

Cause—This can occur when you install NetPoint on a Web server that has security policies enforced through a Web browser.When the Oblix virtual directory has "Scripts only" permission, users are unable to log in to either the NetPoint System Console or Access Manager.

Solution—Change the Oblix virtual directory's permissions from "Scripts only" to "Scripts and Executables".

To change permissions for the Oblix virtual directory

1. Select the machine configured for NetPoint.
2. Expand the Default Web Site.
3. Right-click on either identity or access (the virtual directory you created during COREid System or Access System install).
4. Select Properties and select "Scripts and Executables".

Restricting Access to NetPoint

Symptom—After installation, while NetPoint is protecting access to your resources, access to NetPoint itself is still unrestricted.

Solution—Use the NetPoint Access Manager to restrict access to NetPoint.

Transport Security Mode Issues

Oblix NetPoint supports three different transport security modes: (Open, Simple, or Cert). While Open is initially easier to implement, it is not secure.

Rather than starting with open and changing later, Oblix recommends you install Oblix NetPoint with the desired transport security mode in place. Changing the transport security mode is outlined below. For details, see the *NetPoint 7.0 Administration Guide Volume 1*.

To change transport security modes on the COREid System

1. For each COREid Server, run the COREidServer certutil program located at *COREidServer_install_dir/*identity/oblix/tools/certutil.

   You must configure the COREid Server before the WebPass. You do not need to use the same password and PEM keys for all COREid System components.

2. For each WebPass, run the WebPass gencert program located at *WebPass_install_dir*/identity/oblix/tools/gencert.

To change transport security modes on the Access System

1. For each Access Server, run the configureAAAServer program located at *AccessServer_install_dir*/access/oblix/tools/configureAAAServer.

   You must configure the Access Server before the WebGate. Use the same password and PEM keys for all Access System components.

2. For each WebGate, run the configureWebGate program located at *WebGate_install_dir*/access/oblix/tools/configureWebGate.

User Directory Issues

The following issues pertain to directories.

Adding User to Replicated Directory

If you replicate your Sun directory server and make a change to a user, you are notified that the write will be delayed. However, you are not notified during new user creation.

New users appear in the COREid System pages that are configured against consumers the next time synchronization occurs between the supplier and its consumers.

Synchronization can either occur immediately or at scheduled times, depending on the replication agreement.

Data Corruption

Symptom—While using features in the System Console or in one of the NetPoint Applications, NetPoint begins to display bug reports or error messages. This may occur because of corrupt data. Data corruption can be difficult to diagnose. Though data may appear to be valid as displayed in the directory interface tools, the actual data files may be corrupt. One way to verify this is to perform the same search using another tool such as ldapsearch. If the expected data is not returned, then the data is corrupt.

Solution—Consult with your directory vendor to determine the most appropriate solution. If possible, export the directory data to an LDIF and examine the LDIF for errors. If the data has obvious errors, correct these errors as appropriate and then import the corrected data.

Web Server Issues

The following issues with Web servers may arise:

- "Access Server Crashes on an Apache Web Server" on page 369
- "PCLOSE Error When Starting Sun Web server" on page 370
- "Errors, Loss of Access, and Unpredictable Behavior" on page 370
- "Removing and Re-Installing IIS DLLs" on page 370

Access Server Crashes on an Apache Web Server

Symptom—You are running an Apache Web server, and an Access Server crashes, displaying the following message:

```
libthread panic: cannot create new lwp
(PID: 9035 LWP 2). stackrace:
ff3424cc
0
```

This symptom may be caused by the Apache Web server launching more instances of itself. This can happen when the server determines that more instances are needed to service the number of connections between one or more WebGates and the Access Server.

The additional instances create even more connections, which exceed the number of connections by the Access Server.

Solution—Reduce the number of MinSpareServers, MaxSpareServers, StartServers, and MaxClients parameters.

Go to the Access Server's configuration directory and open the http.d configuration file.

Recommended parameter settings:

- MinSpareServers 1
- MaxSpareServers 5
- StartServers 3
- MaxClients 5

PCLOSE Error When Starting Sun Web server

Symptom—When attempting to start the Sun Web server, you get an error like the following:

```
Unable to start, PCLOSE
```

Solution—A number of problems can cause this error:

- A syntax error in your obj.conf file
- Leading spaces in your obj.conf file
- Installing Oblix NetPoint as a different user ID than what you used to create your Web server instance
    - A carriage return at the end of the obj.conf file

Errors, Loss of Access, and Unpredictable Behavior

Symptom—If you installed NetPoint on Unix under a different user ID than you used to create your Web server instance, NetPoint can become unstable. Users may experience behavior such as:

- Random bug report pages
- Failure to write to log file errors
- Loss of access to Web pages

Solution—Change file permissions using the chown command. Change the NetPoint directory to the same user ID that you used to create your Web server instance.

Removing and Re-Installing IIS DLLs

When NetPoint is running with Microsoft's IIS Web server, you must manually uninstall and re-install the following ISAPI filters when re-installing NetPoint.

- tranfilter.dll
- oblixlock.dll (if you installed WebGate)
- webgate.dll (if you installed WebGate)

To remove and re-install IIS DLLs

1. Uninstall Oblix NetPoint.
2. Manually uninstall the above DLLs.
3. Re-install Oblix NetPoint.Active Directory.

4. Manually re-install the DLLs.

Note: These filters can change depending on the version of IIS you are using. If these filters do not exist or there are others present, contact Oblix Customer Care to determine if the filters that are present need to be removed.

WebGate Issues

The following issues may arise with WebGate:

Access Server and WebGate Naming

Access Servers and WebGates cannot be named using non-English keyboard characters.

Descriptions on the Modify NetPoint AccessGate page of the Access System Console are case insensitive. For example, if you change capitalization of the description but do not alter any other details, you will see no change after the save. To work around this problem, add or alter other information so that the change is recognized.

To change capitalization in an AccessGate description

1. Navigate to the Access System Console > Access System Configuration > AccessGate Configuration.
2. Search for a particular AccessGate or just select the Go button to display a list of all AccessGates.
3. Double-click the link to the WebGate you want to change.
4. Click the Modify button at the bottom of the page.

5. Enter a new description with the capitalization you would like some new information.

   For example:

   From—webgate

   To—WebGate with IIS 6.0

Enabling WebGate Diagnostics

After WebGate installation and configuration, point your browser to the following URL for WebGate diagnostics:

http(s)://host:port/access/oblix/apps/webgate/bin/webgate.cgi?progid=1

Host and *port* are the WebGate's hostname and Web server instance port number. If the diagnostics page does not open, the WebGate was installed improperly.

Error Messages After Installing WebGate

Symptom—If you are running an Access Server with debugging enabled on a Solaris computer, then install a WebGate on a Windows server that uses that Access Server, you will probably see messages like the following in the Access Server's debug log:

```
Got a client!
SSL handshake failed:
error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no
certificate returned
```

Solution—These messages are harmless and may be ignored.

Installing WebGate and COREid in Same Directory

To provide maximum protection for the COREid System, install the WebGate and COREid System in the same directory.

Receiving Access Server Down Errors

Symptom—When attempting to connect, you receive errors indicating that your Access Server is down.

Solution—The clocks of computers hosting various NetPoint components must be synchronized to within 75 or fewer seconds of each other. If the clocks are out-of-sync by more than 75 seconds, installation will fail.

WebGate Cannot Connect to Access Server

Symptom—You get the following error when you attempt to start the NetPoint COREid System:

```
NetPoint Access Server error
WebGate cannot connect to Access Server
```

Cause—When configuring a WebGate in the System Console, you must link each WebGate with at least one Access Server.

Solution—In Access Manager, associate your WebGate with an Access Server. Then configure WebGate.

Miscellaneous Issues

The following are miscellaneous issues.

Unable to Flush the Cache

Symptom—If the Access Manager uses Simple or Cert transport security mode, flushing the cache from Access Manager requires certificates. If your Access Manager is protected by a WebGate that was installed in Simple or Cert mode, the certificates exist and there is no problem. However, if you did not install WebGate in Simple or Cert Mode, you cannot update Access System caches because the Access Manager will not be able to communicate with the Access Servers.

Solution—For a COREid installation that has no WebGate, use the GenCert tool to generate the certificates. This tool is stored at *COREid_Server*/identity/oblix/tools, where *COREid_Server* is your COREid installation directory.

To generate certificates for cache flushing, type

```
genCert install_dir
```

Install_dir is your NetPoint COREid System installation directory. You must be the user with the permissions to write files into the installation directory.

Giving View Rights to the NetPoint Administrator

The NetPoint Administrator is specified during NetPoint installation and setup. Even though this is the highest-ranking NetPoint Administrator, this role does not have view rights for attributes until this right is specifically assigned to it.

The administrator must have permission to view the cn attribute (usually configured as Full Name) at the top level of the directory tree. Then the administrator can configure Access Control for attributes for others.

Refer to the *NetPoint 7.0 Administration Guide Volume 1* for instructions on completing this task.

Idle Session Time, Maximum Cookie Session Time

Symptom—When using either Simple or Cert transport security mode, the user's browser caches the credentials and automatically resends them when a WebGate session times out.This causes the illusion that the timeout settings are not working when in fact a new authentication exchange is taking place without any action on the user's part.

Solution—Use form-based authentication. The browser does not cache form-based authentication information.

Loading the Directory in Secure Mode

Loading your directory can take much longer when SSL is activated. You can load your directory, then activate SSL on the Web server and directory server.

Peer Does Not Use NetPoint Access Protocol

Symptom—When a non-NetPoint program that is set to an incorrect TCP port tries to communicate with your Access Server, you receive an error in your Access Server's debug output. Your Access Server's debug output displays the following error:

```
Peer does not use NetPoint Access Protocol. Connection dropped.
```

Other than the message in your Access Server's debug output, there probably is no impact to your NetPoint installation. However, the non-NetPoint peer attempting to communicate with the Access Server will probably fail.

Solution—Check your TCP port numbers. Something is connecting to the wrong thing.

Receiving Bug Report After Replication Attempt

NetPoint does not support replication with Sun by default.

Symptom—After making a write to a Sun consumer/slave, you get a bug report form.

Solution—To update the enableLDAPReferral parameter:

1. Open the ldapconfigdbparams.xml/lst file in a text editor.

   This file is stored in two locations, and both must be edited:

   - *COREid_install_dir*/identity/oblix/data/common/ldapconfigdbparams.xml
   - *Access_Server_install_*dir/access/oblix/data/common/ldapconfigdbparams.lst
2. Change the enableLDAPReferral parameter to true.
3. Save your changes.
4. Restart the consumer/slave's Web server.

Search and Query Error Message (Defect 4547)

Symptom—When performing a search or a query, you receive a "Bad request" message.

Cause—Your search or query string is too long for your browser. Browsers handle search and query strings as URLs. They generate an error if the string exceeds the maximum URL length.

Solution—Shorten the search or query string.

Identity Server Logged You in but Access System Logged You Out

Symptom—You receive the message "Identity Server logged you in but Access System (Access Manager or System Console) logged you out." This occurs when the NetPoint Access Manager policy is disabled and the NetPoint Identity Domain policy is enabled when logging into the Access Manager as a valid user.

Solution—For security reasons, both the Access Manager (/access) policy and Identity Domain (/identity) policy must be enabled and protected when logging in to the Access Manager.

To make FrontPage work correctly with NetPoint, the settings for IIS must be set up to allow NetPoint to do *all* of the authentication and authorization.

To allow NetPoint to do all authentication and authorization

1. The Web server needs to run as a user that has full control of all directories containing Web content.
2. Use the Web server MMC and click on the directory security tab.
3. Click on the anonymous user and authentication Edit button.

   Make sure that only the allow anonymous users check box is checked. Un-check the other two (basic authentication and nlm authentication)
4. Add the Web server process user (such as IUSR_OBLIX) to the FrontPage admins by using the FrontPage server admin tools (these are different for every version of FrontPage.

java.lang.NoClassDefFoundError: HTTPClient/ ModuleException

Symptom—You receive the message "java.lang.NoClassDefFoundError: HTTPClient/ModuleException" message when installing on WebLogic Realm on Windows, which produces the following error log:

```
Throwable: java.lang.NoClassDefFoundError: HTTPClient/ModuleException
java.lang.NoClassDefFoundError: HTTPClient/ModuleException
at com.oblix.realm.NetPointBEARealm.init(NetPointBEARealm.java:384)
at weblogic.security.acl.Realm.getRealm(Realm.java:85)
at weblogic.security.acl.Realm.getRealm(Realm.java:62)
at weblogic.security.SecurityService.initializeRealm(SecurityService.java:258)
at weblogic.security.SecurityService.initialize(SecurityService.java:115)
at weblogic.t3.srvr.T
```

Solution—It is necessary to include a jars definition such as:

```
HTTPClient.jar jnet.jar jsse.jar
```

in the CLASSPATH statement when doing the installation preparation.

Section VIII: Appendices and Index

A Installing NetPoint with Active Directory

This chapter summarizes prerequisites, installation, and set up for NetPoint with Active Directory. The following topics are included:

Some introductory information is included for configurations that use both LDAP (the default), LDAP over SSL, and the optional Active Directory Services Interface (ASDI) as the communication protocol between NetPoint and Active Directory.

The *NetPoint 7.0 Administration Guide Volume 1* also includes details about:

- "Configuring NetPoint for ADSI"
- "Configuring NetPoint for Active Directory using LDAP"
- Deploying NetPoint with Active Directory and configuring NetPoint for specific Active Directory features
- Configuring NetPoint for .NET features

Important: This reflects information for NetPoint 6.5 and has not yet been updated to 7.0.

About Active Directory

This discussion provides a general overview of Active Directory in broad strokes. See also, “About NetPoint and Active Directory” on page 381.

Active Directory stores information about objects in one or more domains on a network and makes this information available to users and network administrators.

- An Active Directory domain defines an administrative boundary for a collection of objects that are relevant to a specific group of users on a network.
- A domain controller stores directory partitions, also known as "naming contexts", that correspond to the logically distributed segments of the Active Directory that are replicated as discrete units.

An Active Directory that supports multiple trees or domains is called an Active Directory forest. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information. The Active Directory includes:

- A schema that defines the classes of objects and attributes contained in the directory, the constraints and limits on instances of these objects, and the format of their names.
- A Global Catalog is a domain controller that stores a copy of all Active Directory objects in a forest that applications and clients can query to locate any object in a forest. This is no longer needed with NetPoint.
- A query and index mechanism, so that objects and their properties can be published and found by network users or applications.
- A replication service that synchronizes schema, configuration, application, and domain directory partitions between domain controllers and distributes directory data across a network.

Domain Controllers and Partitions

Every Active Directory server (domain controller) in an Active Directory forest participates in replication and contains a complete copy of all directory information for their domain. Any change to directory data is replicated to all domain controllers within the domain.

Every domain controller in an Active Directory forest stores three full, writable directory partitions. In Active Directory, a directory partition is a contiguous Active Directory subtree that is replicated as a unit to other domain controllers in the forest that contain a replica of the same subtree.

A single domain controller always holds at least three directory partitions:

- Schema: one per forest with class and attribute definitions for the directory

- Configuration: one per forest with replication topology and related metadata
- Domain: many in a forest with a subtree that contains the per-domain objects for one domain

About NetPoint and Active Directory

NetPoint 7.0 supports Active Directory on Windows Server 2000 and Windows 2003 Server platforms. On a server running Windows Server 2003, Web Edition:

- You cannot install Active Directory on a server running Windows Server 2003, Web Edition.
- You can join the Windows Server 2003 Web Edition server to an Active Directory domain as a member server (that is not a domain controller) joined to a domain.

NetPoint supports storing user data on a separate directory server type from configuration and policy data. For more information, see "Data Storage Requirements" on page 59 and details about "ADSI Option Considerations" on page 390. With NetPoint, use of the Global Catalog is not required.

NetPoint supports structural and auxiliary object classes. A structural object class can stand on its own and contains basic attributes required for use within NetPoint applications. A structural object class must be assigned when you create a tab within a NetPoint application. An auxiliary object class cannot stand alone because it contains supplementary attributes not necessarily found in a structural object class, for example, a billing address, challenge phrase, or a response to a challenge phrase. An auxiliary object class must be assigned to an entry that is based on an existing structural object class.

NetPoint supports both InetOrgperson and GroupofUniqueNames as standard Person and Group object classes, respectively, in addition to User and Group. NetPoint also supports both statically-linked and dynamically-linked auxiliary classes.

For additional information, see "About NetPoint and Active Directory Forests" on page 383 and "Installation and Setup Considerations" on page 386.

About Statically-Linked Auxiliary Classes

With Windows Server 2000, Active Directory supported only statically-linked auxiliary classes. A statically-linked object class is one that is included in the auxiliaryClass or systemAuxiliaryClass attribute of an object class's classSchema definition in the schema. A statically-linked object class is part of every instance of the class with which it is associated.

When designing the schema for implementation on Active Directory, the following guidelines should be observed for statically-linked auxiliary classes:

- Define oblixorgperson auxiliary in the Person object class.
- Define oblixgroup and oblixadvancegroup auxiliaries in Group object class.
- Modify Active Directory for the group service center or for any operation that assumes an auxiliary class must be attached to a structural class.

Using statically-linked auxiliary classes is the default with NetPoint.

About Dynamically-Linked Auxiliary Classes

With a Windows 2003 Server, Active Directory supports a dynamically-linked auxiliary class, which is attached to an individual object rather than to an object class. NetPoint supports both statically- and dynamically-linked auxiliary classes, but *not* both simultaneously.

Dynamic linking enables you to store additional attributes with an individual object without the forest-wide impact of extending the schema definition for an entire class. For example, an enterprise can use dynamic linking to attach a sales-specific auxiliary class to the user objects of its sales people, and other department-specific auxiliary classes to the user objects of employees in other departments.

During NetPoint COREid Server setup and Access System installation and setup, you will be asked if you want the target directory to support dynamically-linked auxiliary classes. The following overview identifies the tasks that will ensure dynamically-linked auxiliary classes are associated in NetPoint at runtime.

Important: You must raise both the domain and the forest to a Windows 2003 functional level. A mixed environment, where you have 2003 domain controllers and earlier domain controllers, is not supported. Be sure to restart the Active Directory server after raising the forest level.

Task overview: Enabling dynamically-linked auxiliary classes

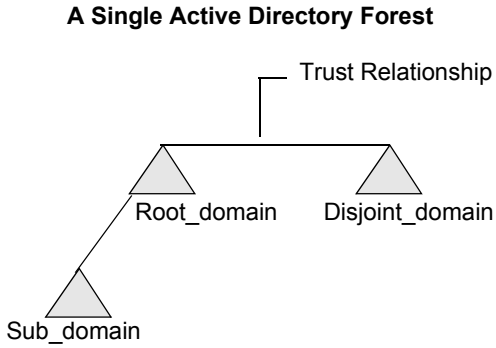
1. Before NetPoint installation, you must ensure that the Active Directory domain and forest functionality are operating at a Windows 2003 Server level, as described in the Microsoft documentation.
2. During COREid System installation and set up, specify dynamically-linked auxiliary classes as described in “Installing the COREid Server” on page 99 and “Setting Up the COREid System” on page 133.
3. During Access Manager installation and set up, specify dynamically-linked auxiliary classes as described in “Installing the Access Manager” on page 159.

4. During Access Server installation, specify dynamically-linked auxiliary classes as described in “Installing the Access Server” on page 187.
5. After installation and setup, configure NetPoint for dynamic auxiliary class support, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

About NetPoint and Active Directory Forests

Until NetPoint 6.0.1, it was possible to install NetPoint within only one Active Directory forest. Figure 17 depicts a single Active Directory forest with three domains: Root_domain, Sub_domain, and Disjoint_domain.

Figure 17 A single Active Directory Forest



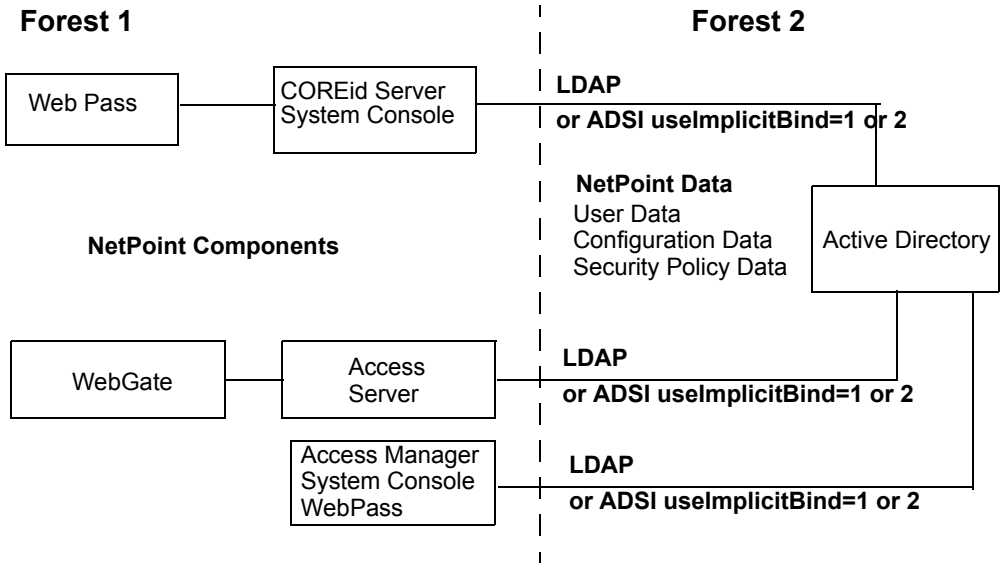
Today, NetPoint components may reside either inside the Active Directory forest with NetPoint user, configuration, and policy data, or outside the forest containing NetPoint data.

If you have installed NetPoint components inside a single Active Directory forest, you may use either of the following communication protocols between NetPoint and Active Directory:

- LDAP (the default)
- LDAP over SSL
- ADSI

Figure 18 shows NetPoint components installed in one forest (Forest 1) with NetPoint user, configuration, and policy data in another (Forest 2). This type of configuration is also known as having “NetPoint outside the forest”. Using ADSI is optional.

Figure 18 NetPoint Components in Forest 1 and NetPoint Data in Forest 2



In a two forest configuration a single domain controller in a forest, the schema master, is responsible for all changes to the schema directory partition. One domain controller per forest, the domain-naming master, is responsible for ensuring that domain names are unique in the forest and that cross-reference objects to external directories are maintained. For more information, see your Microsoft documentation.

A two forest configuration does *not* require setting up a trust relationship between the forest containing user, policy, and configuration data and the forest where the NetPoint servers are installed.

Your environment may include configuration and policy data in one forest and user data in another forest.

NetPoint and the Searchbase in a Parent-Child Domain

Active Directory domains can be organized into parent-child relationships to form a hierarchy. A parent domain is one that is directly superior in the hierarchy to one or more subordinate, or child, domains. A child domain may also be the parent of one or more child domains.

The searchbase in NetPoint defines the node in the directory information tree under which data is stored and the highest possible base for all searches. However, you may not locate an entry in a child domain. The default NetPoint directory server profile is created for only your Root_domain. You must set up directory profiles for the remaining domains in your installation, for example, Disjoint_domain and Sub_domain. For more information, see the *NetPoint 7.0 Administration Guide Volume 1*.

In the NetPoint Access System, a sub-tree-level search is performed during authentication using the credential_mapping plug-in and during authorization using LDAP rules when the rule (for instance, LDAP URL) explicitly states the search is to occur at a sub-tree-level. Using the ObMyGroups action with an LDAP URL returns all groups to which the user belongs.

Table 47 summarizes configurations that support a parent-child domain.

Table 47 Parent-Child Domain Configurations

Function	Configurations for Parent-Child Domains
Authentication	Use credential mapping to authenticate users against both the parent and child domain. The NetPoint credential_mapping plug-in can be used to obtain the user's DN. For an Active Directory forest, typical credential_mapping plug-in parameters are similar to those below: credential_mapping?ObMappingBase="%domain%, ObMappingFilter="(&(objectclass=user) (samaccountname=%login%))", Obdomain="domain" accountname=%login%))", Obdomain="domain"
Authorization	Use multiple LDAP URLs within an authorization rule.

Table 47 Parent-Child Domain Configurations

Function	Configurations for Parent-Child Domains
ObMyGroups	Use ObMyGroups with an LDAP URL. If the user belongs to groups from both parent and child domains, you must define separate header variables for groups from each domain. Using ObMyGroups with no URL will yield groups from the Access System searchbase only. If the searchbase is that of the parent domain, groups from the child domain will not be obtained at all. For example, suppose you have two domains and you want to obtain groups from both searchbases: dc=goodwill,dc=oblix,dc=com and dc=dilbert,dc=goodwill,dc=oblix,dc=com In this case, you must have two separate header variables, one for each domain. **Return** TypeNameReturn Attribute headervarHTTP_PARENT_GROUP"obmygroups:ldap:///dc=goodwill,dc=oblix,dc=com??sub?(group_type=role)" headervarHTTP_CHILD_GROUP"obmygroups:ldap:///dc=dilbert,dc=goodwill,dc=oblix,dc=com??sub?(group_type=role)" **Hence** in HTTP_PARENT_GROUP: all the groups in "dc=goodwill,dc=oblix,dc=com" tree for which the logged-in user is a member and the group_type is "role" is returned. HTTP_CHILD_GROUP: all the groups in "dc=dilbert,dc=goodwill,dc=oblix,dc=com" tree for which the logged-in user is a member and the group_type is "role" is returned.

Installation and Setup Considerations

An overview of specific considerations are summarized below for your review before you begin installing NetPoint with Active Directory:

- “Active Directory Schema Choices” on page 387
- “All Configurations” on page 389
- “ADSI Option Considerations” on page 390
- “LDAP Open Bind Considerations” on page 393
- “LDAP Over SSL Considerations” on page 394
- “SSL Considerations” on page 394

Details will be provided in “Installing NetPoint with Active Directory” on page 394

Active Directory Schema Choices

There are several differences between the Active Directory 2000 and Active Directory 2003 schemas and how they apply to NetPoint:

Key Differences—The key differences between the Windows 2000 (ADSchema.ldif) and Windows 2003 schemas (dotnetschema.ldif) as it relates to NetPoint are the support of inetOrgPerson and groupofuniquenames. These two object classes exist in most other LDAP directories and were officially added to the Windows 2003 schema. The addition of the inetOrgPerson object class allows NetPoint to be configured using this object class without manually adding that object class as was required in Windows 2000.

Affect on NetPoint Schema Files—The main differences between the NetPoint Windows 2000 schema file (ADschema.ldif) and the Windows 2003 schema file (ADdotnetschema.ldif) are outlined below:

- The following entries are in the ADSchema.ldif, but *not* in ADdotnetschema.ldif

  dn: cn=groupOfUniqueNames,cn=schema,cn=configuration,<domain-dn>
  dn: cn=uniquemember,cn=schema,cn=configuration,<domain-dn>

- The oblixgroupofuniquenames class definition is different between the two files, due to differences in how Oblix defined groupofuniquenames in the 2000 schema file and how Microsoft implemented it in the 2003 schema.

Objectclass Differences Between the Two Schemas—The following shows how the objectclasses differ between the two schemas:

- **ADSchema.ldif**:

  Must Contain/Required Attributes—There are *no* required attributes.

  MayContain/Optional Attributes—

  obuniquemember
  businesscategory
  obver

- **ADdotNetschema.ldif**:

  Must Contain/Required Attributes

  cn

  businesscategory
  obuniquemember
  obver
  description
  o
  ou

owner
seeAlso
uniqueMember

Determining which Schema to Load

The file named ADschema.ldif is the Oblix schema file for Windows 2000 and the file named ADdotnetschema.ldif is the Oblix schema file for Windows 2003. Consider the following when deciding which schema to load in your environment:

ADdotnetschema.ldif—Install NetPoint with the .NETSchema (Windows 2003 Schema) when you have the Active Directory 2003 schema loaded whether you are running Windows 2000 or Windows 2003.

For example, some companies are preparing for an upgrade to Windows 2003 and have loaded the Windows 2003 schema in their existing Windows 2000 domain.

If this is the case, you should use the ADdotnetschema.ldif file when installing NetPoint.

ADschema.ldif—Load the Windows 2000 schema if you have the Windows 2000 Schema.

Note: If you don't load the schema files manually, the installer decides which schema file to use based on the answer you provide when asked whether you are installing on Windows 2003 or not. If you indicate that you are installing on Windows 2003, the installer uses the ADdotnetschema.ldif.

Determining the Schema Type—The easiest way to find out whether the environment has a Windows 2000 schema versus the Windows 2003 schema is to use the schema snapin and look for the new string syntax in the 2003 schema. For example:

- In the 2000 schema the string type used the the Unicode format of attributesyntax 2.5.5.12.
- In the 2003 schema it changed to the new syntax of IA5 attributesyntax 2.5.5.5., omysyntax: 22.

All Configurations

The following is intended as an overview for all NetPoint installations with Active Directory.

Oblix recommends that you accept automatic schema updates during COREid Server and Access System installation and setup procedures to save time and eliminate errors. You can always make changes later. However, for manual schema updates you must use one or more of the following files during the setup process depending on your environment:

- For Windows 2003 and dynamically-linked auxiliary classes, you need only the file below:

  install_dir\identity|access\oblix\data\common\ADDotNetSchema.ldif

  ldifde -i credentials -c "<*domain*-dn>" "*your domain*" -f ADDotNetSchema.ldif

- For Windows 2003 and statically-linked auxiliary classes, you need both of the files below:

  install_dir\identity|access\oblix\data\common\ADDotNetSchema.ldif
  install_dir\identity|access\oblix\data\common\ADAuxSchema.ldif

- For Windows 2000, you need only:

  install_dir\identity|access\oblix\data\common\ADSchema.ldif

It's a good idea to add the properties of the administrative user to members of:

Main Administrators
Schema Administrators
Group Policy Administrators
Enterprise Administrators
Domain Administrators
Users, Administrators

The following guidelines apply to all NetPoint configurations with Active Directory.

Guidelines: Installing NetPoint with Active Directory

1. During NetPoint installation and setup, be sure to specify the version of Active Directory you are using, as well as responding appropriately to any related questions you are asked.
2. During NetPoint installation and setup, use the same configuration DN for the COREid Server and for the Access Manager and Access Server.

Note: The login name for a multi domain forest is the display name from Access Server DB profile.

---

3. After installation and setup, you may create or change your authentication scheme or schemes for Active Directory as described in the *NetPoint 7.0 Administration Guide Volume 1*.

4. After installation and setup, you can expand a large dynamic group on Active Directory by adding the following to the globalparams.xml on the COREid server:

```
<SimpleList >
<NameValPair ParamName="maxForRangedMemberRetrieval"
Value="1500"/>
</SimpleList>
```

ADSI Option Considerations

The following is intended as an overview for configurations using ADSI. Using ADSI is optional.

The credentials for ADSI are used to bind to the entire forest. A forest can contain multiple Active Directory hosts. When user data and configuration data are stored on separate Active Directory hosts in separate forests, you cannot connect to these simultaneously using ADSI. For additional information, see "ADSI Cannot Be Enabled for this DB Profile" on page 359.

ADSI does *not* require specific host and port numbers for different domains in the forest. ADSI connects to Active directory hosts using an LDAP URL like the one shown below:

LDAP://*domain*.*oblix*.com/ou=oblix,dc=*domain*,dc=*oblix*,dc=com

When user data and configuration data are stored on separate Active Directory hosts in the same forest, you can connect to these using ADSI. The data will be searched and modified in respective Active Directory servers in the forest using the domain-naming context.

During installation you will be asked if Oblix (configuration) data will be stored in the user data directory. When user data and configuration data are stored on separate Active Directory hosts in the same forest *and* you are using ADSI for the user tree, be sure to indicate that Oblix data will be stored in the user data directory. If you indicate that user data and configuration data are stored separately, you will not be allowed to connect to the configuration data directory server using ADSI and cannot create the DB profile for the Oblix tree by selecting ADSI from the COREid System Console page. Although you can connect to the configuration data directory server using LDAP.

- When using ADSI for the entire forest, the credentials of the NetPoint Administrator should be that of an Enterprise Administrator with administrative privileges over the entire forest.

  The same user tree credentials should be valid for the entire forest. If you decide to configure ADSI for the user tree and LDAP for the Oblix/Policy tree, you can change parameters in the globalparams file and define the appropriate profiles after setup is complete as described in the *NetPint 7.0 Administration Guide Volume 1*.

- When NetPoint data and components are in the same domain, you must run the COREid Server in the context of a privileged administrative user who has change-password permissions after the NetPoint COREid System is installed and set up.

- When storing user data on a separate Active Directory server from configuration and policy data in a separate forest, ADSI may be used for connecting to one or the other but not both.

  - **During NetPoint Installation**—Select Yes when asked if Oblix data is stored with user data, select ADSI for the user data directory server (you won't be asked about ADSI for Oblix data).

  - **During NetPoint Setup**—The directory type for the DB profiles will be indicated as follows:

    User DB Profile—Microsoft Active Directory and ASDI
    Oblix Configuration DB Profile—Microsoft Directory only (no ADSI)

- With NetPoint components in one domain and data in another, you may use either ADSI or LDAP between NetPoint components and Active Directory.

During installation and setup, NetPoint automatically updates certain parameters in the adsi_params.xml file on the COREid Server and the adsi_params.lst file on the Access Manager. The path to these files is shown below:

COREid_install_dir\identity\oblix\config\adsi_params.xml
AccessServer_install_dir\access\oblix\config\adsi_params.lst

Included in the files above is a useImplicitBind value for the user bind DN. Table 48 provides a summary of possible bind parameters.

Table 48 Summary of Bind Parameters in NetPoint adsi_params Files

useImplicitBind Value	Definition	Description
0	Use the implicit credentials of the current process for the bind.	Single Active Directory Forest The default for the COREid Server in the adsi_params.xml file.

Table 48 Summary of Bind Parameters in NetPoint adsi_params Files

1	Use explicit credentials with the DN of the user for the bind.	Two Active Directory Forests Ensure that useImplicitBind value is set to 1 in the adsi_params.xml and .lst files.
2	Use userPrincipalName for the bind.	Two Active Directory Forests • The default for the Access Manager in the adsi_params.lst file. • The preferred value when NetPoint components are in a different domain than NetPoint data. • The UPN should be specified in the adsiUPN parameter in the adsi_params.xml file.

If you are using ADSI with:

- **useImplicitBind=1**—You do *not* need to have your service login credentials set by the COREid Server if the value of useImplicitBind is 1. When NetPoint components reside in one forest and data in another, set useDNSPrefixedLDAPPaths=true.
- **implicitBind=0**—You *do* need to set the permissions of the IIS Anonymous user to a domain user if you are using implicitBind=0. The defaults are implicitBind=0, useDNSPrefixedLDAPPaths=false.

  In this case, ADSI uses the context of the process to bind to the Active Directory server. By default the anonymous user (IWAM*) does not have rights on the directory server.
- **useDNSPrefixedLDAPPath**—You can prefix the domain name to LDAP strings using the useDNSPrefixedLDAPPath parameter in the adsi_params.xml and adsi_params.lst files. The default value is false.

Guidelines: Setting up ADSI

1. Before you install NetPoint, you need to set up Active Directory as described in the Microsoft documentation and “Setting Up Your Environment” on page 395.
2. During COREid Server installation, enable ADSI as described in “Installing the COREid Server” on page 99 and “Installing the COREid System” on page 397.
3. Before COREid System setup, complete steps in “Setting Up ADSI (Optional)” on page 398.
4. During COREid System setup, specify ADSI as described in “Setting Up the COREid System” on page 133 and “Setting Up the COREid System” on page 400.

5. During Access Manager installation and set up, specify ADSI as described in "Installing the Access Manager" on page 159 and "Installing and Setting Up the Access System" on page 402.

6. During Access Server installation, enable ADSI as described in "Installing the Access Server" on page 187 and complete any additional steps in "Setting Up ADSI on the Access Server (Optional)" on page 404.

   If you have NetPoint components in one forest and NetPoint data in another forest, as shown in Figure 18, before you set up the COREid System and Access System complete the task below.

7. After installation and setup, you should confirm the following parameters and values are set as shown below in the NetPoint adsi_params files. For example:

   COREid_install_dir\identity\oblix\config\adsi_params.xml
   AccessServer_install_dir\access\oblix\config\adsi_params.lst

   NameValPair ParamName="useDNSPrefixedLDAPPaths"
   Value="true"

   COREid_install_dir\identity\oblix\config\adsi_params.xml

   NameValPair ParamName="adsiCredential"
   Value="cn=*Administrator*,cn=*users*,dc=*goodwill*,dc=*oblix*,dc=com"

For more information about the adsi_params files and parameters, see the *NetPoint 7.0 Administration Guide Volume 1*.

LDAP Open Bind Considerations

The following is intended as an overview.

LDAP open bind is the default (presumed) communication method between NetPoint and the directory server. If you are using an LDAP open bind between NetPoint components and Active Directory, you may complete some additional steps during NetPoint installation and set up.

Guidelines: Setting up an LDAP open bind

1. Before you install NetPoint, you need to set up Active Directory as described in the Microsoft documentation and "Setting Up Your Environment" on page 395.

2. During COREid System installation and setup, be sure to indicate that there is no SSL connection between NetPoint and Active Directory.

3. After Access Server installation, you are prompted to specify failover information and timeouts for LDAP and the port number.

   - Be sure to configure timeouts for the Access Server when it is installed against Active Directory, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

- Later, you may reconfigure failover information, as described in the *NetPoint 7.0 Deployment Guide*.

LDAP Over SSL Considerations

The following is intended as an overview.

If you are using LDAP over SSL between NetPoint components and Active Directory, you will complete additional steps during NetPoint installation and set up.

Guidelines: Setting up LDAP over SSL

1. Before you install NetPoint, ensure that you have a certificate on the machine, as described in "Setting Up Your Environment" on page 395.
2. During NetPoint installation and setup, ensure that you specify SSL as the communication method between NetPoint and Active Directory.

SSL Considerations

Directory server communication guidelines are described in "Securing NetPoint Component Communications" on page 45.

Guidelines: Setting up SSL

1. Before you install NetPoint, ensure that you have a certificate on the machine, as described in "Setting Up Your Environment" on page 395.
2. After installation and setup, you may reconfigure communication with the directory server, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

   If you have ADSI enabled and you reconfigure communication with the directory server, you must also edit the adsi_params.xml and adsi_params.lst files to reset the encryption parameter to false.

Installing NetPoint with Active Directory

With the above considerations in mind, you are ready to set up your Active Directory and install NetPoint. Following discussions explain all procedures and the order in which they must be completed.

Task overview: Installing NetPoint with Active Directory includes

1. "Setting Up Your Environment" on page 395
2. "Installing the COREid System" on page 397

3. “Setting Up the COREid System” on page 399
4. “Validating Your COREid System Setup” on page 401
5. “Installing and Setting Up the Access System” on page 401

Each of the items in the task overview above may include multiple procedures. When this is the case, additional task overviews will be provided to outline the order in which procedures must be completed.

Setting Up Your Environment

The topics below outline how to set up your Active Directory before installing NetPoint components.

Task overview: Setting up your environment includes

1. “Setting Up Domain Controllers” on page 395
2. “Installing the Certificate Server” on page 395
3. “Retrieving the Certificate” on page 396

Setting Up Domain Controllers

Before you install NetPoint components, you must set up the domain controller.

Important: If you intend to enable dynamically-linked auxiliary classes, you must raise both the domain and the forest to a Windows 2003 Server level, as described in the Microsoft documentation.

To prepare the domain controllers

1. Set up and configure a domain controller for each machine in the Active Directory forest, using the instructions from Microsoft.
2. Specify the desired method for all auxiliary classes, either dynamically-linked or statically-linked auxiliary classes, using instructions from Microsoft.

Installing the Certificate Server

When you use LDAP over SSL, you must install the Microsoft CA Certificate Server and retrieve a certificate.

Note: If you are using LDAP (the default) or ADSI, skip this discussion.

You can install the certificate server on any machine in the Active Directory forest. However, Oblix recommends that you install it on the root domain of the Active Directory forest (for example, Root_domain). When enabled, all domain controllers will automatically request a certificate and support LDAP using SSL port 636.

To set up the Microsoft CA certificate server on other domain controllers

1. Set up a policy to enable other domain controllers to automatically request certificates, using the instructions from Microsoft.
2. Set up and configure the Microsoft CA certificate server, using your Microsoft documentation.

Retrieving the Certificate

After the certificate server is setup, you must retrieve the Microsoft CA certificate from the machine where the certificate server is installed and save it on the machine where you will install the NetPoint component. For example, on the COREid Server, Root_domain.

Important: A certificate is required on each machine on which SSL is enabled.

Task overview: Retrieving and setting up a certificate inclues

1. "To retrieve a certificate for the intended COREid Server" on page 396
2. "To set up the certificate" on page 397

To retrieve a certificate for the intended COREid Server

1. On the machine where you will install the COREid Server, navigate to the machine where the Microsoft CA certificate server is installed. For example:

   http://*Root_domain*/certsrv/
2. Select Retrieve the CA certificate or certificate revocation list.
3. Select Base 64 encoded.
4. Double-click the Download CA certificate link.
5. Select Save this file on the machine where you will install the COREid Server.
6. Enter a directory and file name.
7. Record the full path to this file so you will have it when you install the COREid Server. For example:

   F:\NetPoint\certnew.cer

You are ready to install the NetPoint COREid System. See also, “To set up the certificate” on page 397.

To set up the certificate

1. Navigate to the certificate server. For example:

   http://*Root_domain*/certsrv/

2. Download the certificate chain to a file and save the certificate.

   When you import the file and store it on the local computer, as described next, IE imports the CA to the personal certificate store of the user who is currently logged in by default.

3. Import the file to a trusted root CA store on the local computer. For example:

   Internet Explorer > Tools > Internet options
   Content > Certificates > Trusted Root Certificate > *CertName* > Import > Next
   Browse > *Filename* > Next
   Trusted Root Certification Authorities > Local Computer

Installing the COREid System

After the preliminary set up of Active Directory, you need to install the NetPoint COREid Server and WebPass, the two main components of the COREid System.

Task overview: Installing the COREid System with Active Directory includes

1. “Installing the COREid System” on page 397
2. “Setting Up ADSI (Optional)” on page 398

Installing the COREid System

During installation and setup, you will be asked to respond to the same questions as those who install NetPoint with other directory servers. In addition, you will be asked to specify options for ADSI and dynamically-linked auxiliary classes.

To install the NetPoint COREid Server

1. Review “Installation and Setup Considerations” on page 386 and “Data Storage Requirements” on page 59.
2. Complete “Setting Up Your Environment” on page 395, as needed.

3. Follow the instructions in “Installing the COREid Server” on page 99, and include specifications and preferences for your Active Directory environment.

   The bind DN you specify can be any user as long as there are sufficient privileges to modifiy/read the attributes and access the schema, including changing password permissions if using LDAP/SSL. With ADSI, the COREid Server service credentials need to be appropriate.

4. To expand large dynamic groups on Active Directory, if desired, add the following to the globalparams.xml file, then restart the COREid server:

   COREid_install_dir\identity\oblix\apps\common\bin\globalparams.xml

```
<SimpleList >
<NameValPair ParamName="maxForRangedMemberRetrieval"
Value="1500"/>
</SimpleList>
```

To complete COREid System installation

1. Follow the instructions under “Installing WebPass” on page 121.
2. Complete the appropriate task below, depending upon your environment:
   a) Either set up ADSI, as described under “Setting Up ADSI (Optional)” on page 398
   b) Or complete the COREId System set up, as described under “Setting Up the COREid System” on page 399

Setting Up ADSI (Optional)

If you want to use optional ADSI, you need to complete the steps below:

- Immediately after COREid System installation (COREid Server and WebPass)
- Before setting up the COREid System

By default, ADSI uses an implicit bind. This corresponds to the Windows 2000 Server and Windows Server 2003 service logon credentials. For more information, see, “ADSI Option Considerations” on page 390 and the *NetPoint 7.0 Administration Guide Volume 1*.

To set up ADSI, before you set up the COREid System

1. Choose the proper bind mechanism for your environment in the *COREid_install_dir*\identity\oblix\config\adsi_params.xml. For example:
   - **ADSI with a Single Forest**—
     <NameValPair ParamName=“useImplicitBind”
     Value=“0”/>

- **ADSI when NetPoint and Data are in Different Forests**—
  <NameValPair ParamName="useImplicitBind"
  Value="1"/>

  <NameValPair ParamName="useDNSPrefixedLDAPPaths"
  Value="true">

2. **When useImplicitBind=0**—Set the service logon credentials for the COREid Server to an administrative user in the domain with the same privileges as the user you designated as the root bind DN during COREid installation.
3. Set up the COREid System as described under "Setting Up the COREid System" on page 399.

Setting Up the COREid System

After you install the COREid Server and WebPass components, you are ready to set up the COREid System.

Discussions below explain what to do before and during COREid System set up to ensure success. Several situations are covered:

- "Enabling Active Directory Attributes" on page 399

  Note: If you do *not* want to enable specific Active Directory attributes, go directly to "Setting Up the COREid System" on page 399.

- "Enabling Change-Password Permissions" on page 400
- "Setting Up the COREid System" on page 399

Enabling Active Directory Attributes

To enable specific Active Directory attributes, you need to complete the procedure below. For example, if you want to use the userPrincipalName as a login attribute and you want this attribute to be available during COREid setup, complete the activities below before COREid System setup.

Note: If you do *not* want to enable specific Active Directory attributes, skip this task and go directly to "Setting Up the COREid System" on page 399.

To enable Active Directory attributes

1. Locate the ad_exlude_attrs.xml and exclude_attrs-ad.xml files. For example:

   COREid_install_dir\identity\oblix\data.ldap\common\ad_exlude_attrs.xml
   COREid_install_dir\identity\oblix\data.ldap\common\exclude_attrs-ad.xml

2. Edit the files to make specific Active Directory attributes available within COREid System user profiles. For example:

   <ValNameList ListName="userPrincipalName">
   <NameValPair ParameterName="appliesto" Value="None" />

To modify your schema for statically-linked auxiliary classes

1. Modify your schema to attach the oblixOrgPerson and oblixPersonPwdPlicy objects to your user object class and oblixGroup to your Group object class.
2. Perform a schema reload within the MMC Schema Manager Application after making the changes above and allow approximately fifteen minutes for the schema changes to be replicated to all domain controllers.

Enabling Change-Password Permissions

When NetPoint data and components are in the same forest, you must run the COREid Server in the context of a privileged administrative user who has change-password permissions.

Note: With LDAP over SSL, you do not need to set service credentials for the COREid Server.

Setting Up the COREid System

After completing the tasks above, you are ready to set up the COREid System for the Active Directory forest, using the Root_domain.

To set up the COREid System for an Active Directory forest

1. Navigate to the COREId System set up page:

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

2. Click COREid System Console then click Setup to activate the process.
3. Follow the instructions in "Setting Up the COREid System" on page 133.
   - Enable ADSI, if appropriate.
   - Check the Dynamic Auxiliary Object Class box, if appropriate.
4. When setup is complete, you can perform the tasks outlined below:
   - Validate your COREid System setup, as described in "Validating Your COREid System Setup" on page 401.
   - Define directory server profiles for remaining domains, if needed, as described in the *NetPoint 7.0 Administration Guide Volume 1*.

Note: If you are using ADSI, see the *NetPoint 7.0 Administration Guide Volume 1* for details about enabling ADSI for the Default Directory Profile and additional directory profiles.

- Set up disjoint searchbases for the disjoint domain, if needed, as described in the *NetPoint 7.0 Administration Guide Volume 1*.
- Install and setup the Access System, as described in "Installing and Setting Up the Access System" on page 401.

Validating Your COREid System Setup

It is a good idea to validate that your COREid System is set up and properly operating with Active Directory before you being installing the Access System.

To validate your COREid System setup

1. Navigate to the COREid System login page.

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

2. Verify that all domain names appear in the drop-down list on the login page.
3. Log in.
4. Navigate to the Configure Directory Options page and confirm that your disjoint searchbase is listed.

   COREid System Console > System Admin > System Configuration > Configure Directory Options

   Note: If your disjoint searchbase is not listed, you can add it now. For more information, see the *NetPoint 7.0 Administration Guide Volume 1*.

After validating that your COREid System is working properly, you can install and set up the NetPoint Access System.

Installing and Setting Up the Access System

Refer to topics below as you install the Access System with your Active Directory forest.

- "Preparing for Access System Installation" on page 402
- "Installing and Setting Up the Access System" on page 402
- "Setting Up ADSI on the Access Server (Optional)" on page 404

Preparing for Access System Installation

Be sure to verify that the steps below have been completed before you attempt to install the NetPoint Access System.

To prepare for the Access System installation and setup

1. Review “Installation and Setup Considerations” on page 386.
2. Install the COREid System, as discussed in “Installing the COREid System” on page 397.
3. Set up the COREid System, as discussed in “Setting Up the COREid System” on page 399.
4. Validate your COREid System, as discussed in “Validating Your COREid System Setup” on page 401.

Important: To prepare the Access Manager host for ADSI when the machine is not a domain controller and resides in the same forest with other NetPoint data, ensure that useImplicitBind=1 or 2 and useDNSPrefixedLDAPPaths=true.

Installing and Setting Up the Access System

Use the steps below as a guide when you install and set up the Access System in this environment.

- “To install and set up the Access Manager” on page 402
- “To install and set up the Access Server and WebGate” on page 403

To install and set up the Access Manager

1. Confirm that you have a certificate on each machine, if needed, for ADSI or LDAP over SSL before you begin NetPoint installation.

   In the next step, use the same directory server details that you used for the COREid Server installation **only** if your Oblix data, user data, and NetPoint policy data will reside on the same directory server. Also, ensure that the distinguished name specified as the bind DN has full permissions for the user and Oblix branches of the directory information tree (DIT).
2. Install the Access Manager, as described in “Installing the Access Manager” on page 159.
   - Select Active Directory using ADSI, if appropriate.
   - Select dynamically-linked auxiliary classes, if appropriate.
3. Set up the Access Manager as described in “Setting Up the Access Manager” on page 175 and consider the following:

- With ADSI, select Enable ADSI and enter the userPrincipleName as the bind DN (for example, user@company.com), then complete set up.
- With LDAP open bind, see the *NetPoint 7.0 Administration Guide Volume 1* to complete Access Manager set up.

Important: You complete the steps below only when NetPoint server components reside in one forest and data in another.

---

4. Verify that the useDNSPrefixedLDAPPaths value in the *\AccessManager_install_dir*\access\oblix\config\adsi_params.lst fie is set to true. For example:

   <NameValPair
   ParamName="useDNSPrefixedLDAPPaths"
   Value="true" />

5. Verify the forceExplicitBindUsingDN and set its value to true in the *\AccessManager_install_dir*\access\oblix\apps\common\bin\globalparams.lst file. For example:

   forceExplicitBindUsingDN:true

6. Restart the COREid Server and WebPass Web server.

To install and set up the Access Server and WebGate

1. Confirm that you have a certificate on each machine, if needed, for ADSI or LDAP over SSL before you begin NetPoint installation.
2. Install the Access Server, as described in "Installing the Access Server" on page 187 and consider the following items:
   - Select Active Directory using ADSI, if appropriate, enter the adsiCredential and adsiPassword when prompted, then complete "Setting Up ADSI on the Access Server (Optional)" on page 404 *before* restarting the Access Server.

     adsiCredential and adsiPassword are required to generate an encrypted password that can be used when explicitly binding to Active Directory using ADSI. Because NetPoint does not include an encryption tool, you must enter values for adsiCredential and adsiPassword when asked.
   - Select dynamic auxiliary classes, if appropriate.

Note: You will be asked where the user data, Oblix data, and policy data are stored and for configuration details for the directory server.

You need to complete step 3 when you have Active Directory 2000, because it does *not* support concurrent bind requests coming from different NetPoint threads on the same LDAP connection. For more information, see "Tips and Troubleshooting" on page 405

3. **Active Directory 2000**—On the Access Server, open the globalparams.lst file and add a new flag called exclusiveAuthnConnection set to true to force NetPoint threads to use separate LDAP connections for bind requests being sent to the directory server.

4. **WebGate**—Install and configure the WebGate, as described in "Installing the AccessGate/WebGate" on page 199.

   See the *NetPoint 7.0 Administration Guide Volume 1* for more information about authentication and authorization with Active Directory and configuring NetPoint for specific Active Directory features.

Setting Up ADSI on the Access Server (Optional)

If you choose to use ADSI, which is optional, you must set up ADSI on the Access Server:

- After installing the Access Server
- Before restarting the Access Server

To set up ADSI on the Access Server

1. Log in to the domain as an administrative user.

2. Set the service logon credentials for the Access Server to an administrative user in the domain.

   This user must have the same privileges as the user that you provide in the Root DN during Access Manager and Access Server installations.

3. Choose the proper bind mechanism in the adsi_params.lst file. For example, in a two forest configuration:

   AccessServer_install_dir\access\oblix\config\adsi_params.lst

   useImplicitBind Value="1"

   By default, the Access Server useImplicitBind is set to 0 for a single-forest configuration. ADSI uses an implicit bind. This corresponds to Windows 2000 Server, or Windows Server 2003 service logon credentials. See the *NetPoint 7.0 Administration Guide Volume 1* for more information on ADSI bind mechanics.

   You complete step 4 and step 5, below, as needed for your environment.

4. When you have NetPoint components installed outside the Active Directory forest, you need to verify the useDNSPrefixedLDAPPaths parameter value in the adsi_params.lst is set to true. For example:

   useDNSPrefixedLDAPPaths Value="true"

5. When you have NetPoint components installed in one forest and data in another, set the forceExplicitBindUsingDN parameter value to true in the globalparams.lst file. For example:

   AccessServer_install_dir\access\oblix\apps\common\bin\globalparams.lst

   forceExplicitBindUsingDN Value="true"

6. See the *NetPoint 7.0 Administration Guide Volume 1* for more information about authentication and authorization with Active Directory and configuring NetPoint for Active Directory features.

Tips and Troubleshooting

Active Directory 2000 does *not* support concurrent bind requests coming from different NetPoint threads on the same LDAP connection.

NetPoint servers are multi-threaded and maintain a pool multiple LDAP connections to the directory server. Several NetPoint threads may share the LDAP connection for efficient processing of requests. However, Active Directory 2000 does not support concurrent binds requests coming from different NetPoint threads on the same LDAP connection. This may cause spurious authentication failures.

To avoid this situation

1. On the Access Server, locate the globalparams.lst file and open this in an editor.

2. Add a new flag called exclusiveAuthnConnection and set it to true.

   This forces NetPoint threads to use separate LDAP connections for bind requests being sent to the directory server.

B Installing NetPoint with ADAM

NetPoint supports the Microsoft Active Directory Application Mode (ADAM) as a stand-alone directory server. This chapter includes the discussions below:

Upgrading to NetPoint 7.0 is explained in the *NetPoint 7.0 Upgrade Guide*.

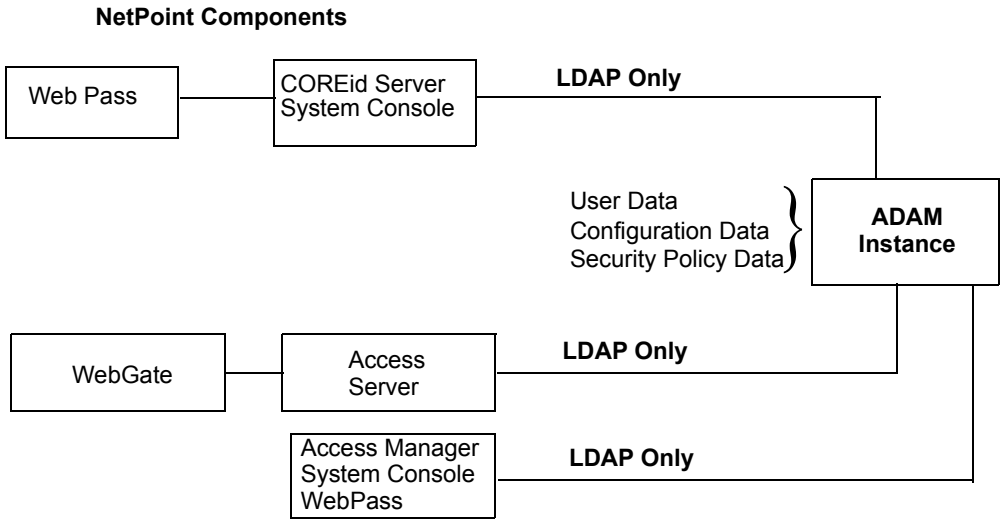
About NetPoint and ADAM

This discussion introduces ADAM in general terms and provides details about using ADAM as a directory server for NetPoint. Differences between ADAM and Active Directory are also discussed.

Note: NetPoint 7.0 supports storing user data on a separate *type* of directory server and storing Oblix (NetPoint) configuration and policy data on one or more instances of ADAM. This means that, for example, you may store user data on Active Directory and configuration and policy data on ADAM. Configuration and policy data must be stored on the same directory server type.

Whether you install NetPoint on a single machine with ADAM or in a distributed environment, as shown in Figure 19, NetPoint supports ADAM as a stand-alone directory server.

Figure 19 ADAM as a Stand-Alone Directory Server for NetPoint



ADAM uses the same storage management and the same programming model as the .NET Active Directory. In addition, ADAM provides a similar replication and administration model as Active Directory. However, ADAM is independent of Active Directory and Active Directory domains and forests. ADAM does not include Active Directory infrastructure features, does not include directory services for the Windows operating system, and does not require a domain controller. ADAM runs as an independent service, not an operating system service.

ADAM typically provides dedicated directory services for applications, including a data store and services to access the data store. For example, ADAM can provide an application-specific directory store for a small business unit. The information in ADAM may require specific local schema changes, may be relevant to only a small group of users, and may not require wide distribution.

During installation of each unique ADAM instance, you specify a name and port for the instance. The name ties the files, service, registry, and ports together. Ports may be configured for LDAP and SSL. An open LDAP port is required to extend the ADAM schema with NetPoint-related information. There have been no changes to the NetPoint schema for ADAM.

For more information, see:

- “ADAM Instances and Partitions” on page 409
- “The ADAM Schema” on page 410
- “The NetPoint Schema Extension for ADAM” on page 411
- “Windows Users and Security Principals” on page 413

ADAM Instances and Partitions

During installation of a unique ADAM instance, a schema directory partition (SDP) and configuration directory partition (CDP) are created. With ADAM, there is no domain partition. Each unique instance can be configured independently and may include multiple application directory partitions (ADPs) created either during ADAM installation and setup or later.

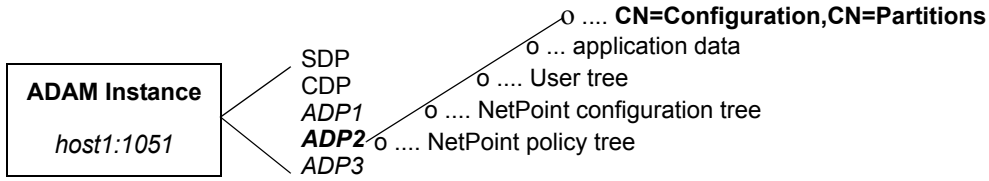
Important: Be sure to create your application directory partitions within ADAM before installing NetPoint. NetPoint does not create an ADP within ADAM.

ADAM ADPs are similar to Active Directory ADPs. Each ADAM ADP contains the data (objects) for an ADAM instance. However, ADAM ADPs cannot store a security principal (an account holder that is automatically assigned a security identifier (SID) to control access to resources). Applications and services can use ADAM ADPs to store application-specific data, which may contain highly volatile information with high replication requirements that could strain resources if stored in your Network Operating System (NOS) directory.

Originally NetPoint supported a single ADP within a single ADAM instance, which included application-specific data as well as the user tree, the Oblix (NetPoint) configuration tree, and the NetPoint policy tree, as shown in Figure 20.

Figure 20 Single ADAM Instance and Partitions

Web Server Name and Port: ***host1:1050***



Note: NetPoint supports multiple ADPs within a single instance and multiple instances. NetPoint will support a master instance and its replicas.

Also: NetPoint requires a node with the objectclass attribute value of organizationalUnit for the configuration and policy DNs. When you create an ou, this is added by default.

Note: NetPoint 7.0 supports multiple ADAM instances and multiple ADPs. Now, user data may be stored on a different directory server *type*. For example, NetPoint configuration and policy data may be stored on ADAM in a single ADAM ADP or instance or on different ADAM ADPs or instances while user data is stored on Active Directory.

The ADAM Schema

ADAM, like Active Directory on Windows Server 2003 platforms, supports dynamically-linked auxiliary classes. NetPoint supports both dynamically-linked and statically-linked auxiliary classes.

The ADAM schema contains definitions of the object classes that ADAM can access within a configuration set. The schema also includes definitions of the attributes that ADAM can access in an ADAM object. For more information about configuration sets, see “Replication of an ADAM Instance” on page 414.

The ADAM schema is flexible. There are no namespace restrictions. ADAM can use X.500-style naming contexts (o=,c=) for various types of information (schema, sites, partitions, and services). Within the ADP, the user searchbase, configuration DN, and policybase may be the same (o=*company,*c=us) or may differ.

Note: NetPoint requires a node with the objectclass attribute value of organizationalUnit (ou) for the configuration and policy DNs. When you create an ou, this is added by default.

An example of *different* namespaces is shown below:

Searchbase—o=*company,*c=us
Configuration DN—ou=config,o=*company,*c=us
Policybase—ou=policy,o=*company*,c=us

Note: When storing user data on a separate *type* of directory server and NetPoint configuration and policy data on one or more ADPs or one or more ADAM instances, different namespaces are required.

While the ADAM schema is similar to the Active Directory schema, the user object class is described differently in ADAM than in Active Directory. There is no security principal attached to ADAM. For example, *saMAccountName* is mandatory with Active Directory for user and group but does not exist in ADAM. However, *grouptype* is still required.

The grouptype attribute in the ADAM group object class "group" can have *only* the following values, which should be configured in the meta-attribute configuration applet (COREid System Console > Group Manager > Configure Tab > Modify Attributes) for the object class with a Display Type of radio button:

global - 2
domain local - 4
universal - 8
secure domain - -2147683644
secure global - -2147482646

In Active Directory, the password attribute is unicodePwd. The password attribute on ADAM is *userpassword*. The *uid* attribute is assigned the Semantic Type "Login" by default.

The Active Directory Application Mode schema is extensible using the Ldifde.exe command-line tool.

The NetPoint Schema Extension for ADAM

The NetPoint schema extension for ADAM must be loaded using a Windows Security Principal credential. At runtime, however, NetPoint communicates only with users within ADAM, not with security principals. For more information, see "Windows Users and Security Principals" on page 413.

When you install NetPoint on a Windows Server 2003 platform, you may automatically update the ADAM schema. However, when you install NetPoint on a Windows 2000 Server, you must manually update the ADAM schema.

NetPoint supports both InetOrgperson and GroupofUniqueNames as standard Person and Group object classes, respectively, in addition to user and group. You may have an object class already in use and do not need to use a specific object class. NetPoint also supports both statically-linked and dynamically-linked auxiliary classes.

The ADAM schema cannot be modified with a simple LDAP bind and must be modified using ldifde, *not* ldapmodify. Currently, ldifde does *not* support binding to an SSL port on ADAM; therefore, the ADAM schema may be extended for NetPoint only on an *open* port. During COREid Server installation, you can specify an SSL connection and obtain the SSL certificate for ADAM, then specify an *open* port number for the schema update.

Note: With ADAM the schema update must be completed using an open port and a Windows security principal credential.

NetPoint provides the following schema files for NetPoint configuration and user directories. To update the schema manually, you must use the files below:

COREid_install_dir\identity\oblix\data.ldap\common\
ADAM_oblix_schema_add.ldif
ADAM_user_schema_add.ldif

In addition, if you are using statically-linked auxiliary classes, you also need to run the ldifde command with the following file:

COREid_install_dir\identity\oblix\data.ldap\common\ADAMAuxSchema.ldif

A sample ldifde command to manually update the schema is shown below and described in Table 49. For more information, see your Microsoft documentation:

ldifde -k -b
“*<user_distinguished_name>*”“*<domain_name>*”“*<user_password>*”
-c“<GUID>”*<ADAM_instance_ID>* -i -f ADAM_oblix_schema_add -s
<ADAM_server_name> -t *<port>*

Table 49 ldifde Command Description

Option	Description
-k	This option ignores errors.
-b “*<user_distinguished_name>*” “*<domain_name>*” “*<user_password>*” For example: cn=*administrator,o=oblix.com,c=us password*	To extend the schema, the values represent: • a Windows security principal user name • domain name of the machine where ADAM is installed • password

Table 49 Ldifde Command Description

Option	Description
-c "<GUID>" *<ADAM_instance_ID>*	In this option, "<GUID>" should be retained as is, not replaced by any value; do include the quotes. *<ADAM_instance_ID>* should be substituted by the ADAM root DSE using tools like ldp.exe. When the initial connection is made, the root DSE is shown. For example, an ADAM root DSE value may be EC31B31B-19FC-4FD4-8590-3BD57D6A3E77.
-i -f *<filename>*	The -i option specifies the import option. The -f option identifies a file name; the value identifies the file you are importing. For example: ADAM_oblix_schema_add.ldif ADAMAuxSchema.ldif
-s *<ADAM_server_name>*	This value is the name of the machine where ADAM is installed.
-t *<port >*	This value is the port number on which this instance listens for the schema update (an open port is needed).

Windows Users and Security Principals

ADAM supports user credentials and uses Windows security principal credentials for authentication and access control. For example, the Windows security principal provides the rights to define users and replicate an instance of the ADAM directory store. However, NetPoint requires Windows security principal credentials only to update the ADAM schema.

Windows Security Principal for Schema Updates—When you install the NetPoint COREid Server with ADAM and update the schema, you must supply directory server details as follows:

- *Automatic Schema Updates*—If you automatically update the schema (Windows Server 2003 only), you will be asked for directory server details including the Windows security principal name and password for the schema extension. For example:

  Windows User Name: *administrator* (Windows Security Principal only)

- *Manual Schema Updates*—If you manually extend the schema, you must supply the Windows security principal name and password with the ldifde command as discussed in “The NetPoint Schema Extension for ADAM” on page 411. For example:

  -b “*<user_distinguished_name>*”“*<domain_name>*”“*<user_password>*”

Windows User within ADAM for Root (Bind) DN—At runtime, NetPoint communicates only with users within ADAM, not with a Windows security principal. During COREid System setup you must specify the Root (bind) DN for ADAM and password for that user on the page where you specify Directory Server with User Data Configuration. This must be the name of a *bindable* user within ADAM with administrator privileges:

Root DN: Name of a *bindable* user within ADAM with administrator privileges

Root DN Password of the bindable user within ADAM with administrator privileges

You create a bindable user in ADAM by adding the ms-bindable-object auxiliary object class to the object class you are using for people objects, inetOrgPerson, for example.

The NetPoint Administrator must be a bindable user in ADAM with administrative privileges, *not* a Windows Security Principal.

NetPoint Directory Profiles

When you setup NetPoint, individual directory profiles are created for the COREid Server, Access Manager, and Access Server, as usual. During COREid System setup, you specify the SSL-enabled port to properly configure the directory profile within NetPoint.

For details about configuring directory profiles after NetPoint installation, see the *NetPoint 7.0 Administration Guide Volume 1*.

Replication of an ADAM Instance

Replication of an ADAM instance creates a configuration set. All ADAM instances within a configuration set replicate a common schema partition and configuration partition, and can also replicate ADPs such as o=*company*,c=*US*. Only complete replicas are supported by NetPoint.

NetPoint will provide failover and load balancing between a master instance and its replicas; however, NetPoint does *not* support ADSI with ADAM. For more information, see “ADSI with NetPoint and ADAM” on page 415.

Typically, multiple instances of ADAM may run concurrently on a single server, each with its own schema and configuration.

Note: You cannot replicate ADAM instances across the forest. In a production environment, ADAM instances within the same configuration set *cannot* reside on the same machine. See your Microsoft documentation for more information.

ADSI with NetPoint and ADAM

ADSI provides failover support in Active Directory environments and NetPoint supports ADSI with Active Directory. ADAM supports Active Directory Service Interfaces (ADSI). However, NetPoint does *not* support ADSI with ADAM.

With ADAM there is no domain controller, therefore, the native NetPoint directory server failover and connection management toolkits are recommended. For details about configuring failover and load balancing, see the *NetPoint 7.0 Deployment Guide*.

ADAM and APIs

ADAM uses standard application programming interfaces (APIs) to access application data. These include Active Directory APIs, Lightweight Data Access Protocol, and System-Directory Services.

ADAM does *not* support the Messaging Application Programming Interface (API). Therefore, Microsoft Exchange cannot use ADAM. For more information, see your Microsoft documentation.

Authentication, Authorization, and Password Changes

Authentication and authorization processes should be managed in NetPoint, rather than in ADAM. This will avoid contentions between NetPoint “rules” and ADAM “rules” regarding authentication and authorization. NetPoint authentication and authorization processes are the same whether you are using ADAM or Active Directory. For more information, see the *NetPoint 7.0 Administration Guide Volume 1*.

With NetPoint, ADAM cannot use proxy objects that point to Active Directory. Users must be enabled within ADAM and must have a password.

With Active Directory and NetPoint, you can use native password management and/or NetPoint. Password management is available with ADAM. Both Active Directory and ADAM support changing passwords over a secure connection, either SSL or ADSI. However, NetPoint does *not* support ADSI with ADAM, therefore, SSL must be used for password changes with ADAM.

ADAM and Active Directory Differences

Differences between ADAM and Active Directory are summarized below along with the page numbers where you can find more information in this guide.

Table 50 Differences between ADAM and Active Directory with NetPoint

Description	Page
ADAM and Active Directory can operate concurrently in the same network; NetPoint supports the use of both independently and together.	407
The information in ADAM may require specific local schema changes, may be relevant to only a small group of users, and may not require *wide* distribution.	407
Applications and services can use ADAM ADPs to store application-specific data, which may contain highly volatile information with high replication requirements.	409
There is no security principal attached to ADAM. For example, saMAccountName is mandatory with Active Directory for user and group but does not exist in ADAM.	410
The password attribute on ADAM is userpassword.	410
An automatic ADAM schema update is available only when NetPoint COREid Server is installed on a Windows Server 2003 system.	411
NetPoint requires Windows security principal credentials to update the ADAM schema. At runtime, NetPoint communicates only with users within ADAM, not with security principals.	413
Both Active Directory and ADAM support ADSI. However, NetPoint supports ADSI only with Active Directory. An implicit bind is available only with Active Directory, not ADAM.	415
Both Active Directory and ADAM support changing passwords. NetPoint with ADAM requires an SSL-enabled port for password changes.	415

For more information about ADAM, see your Microsoft documentation.

Support Requirements

ADAM and Active Directory can operate concurrently within the same network. NetPoint supports the use of ADAM alone. In addition, NetPoint supports ADAM with Active Directory and ADAM with other directory server types for storing user data separately from configuration and policy data:

- All user data must be stored on the same directory server type.
- Configuration and policy data must be stored on the same type of directory server.
- NetPoint requires a node with the objectclass attribute value of organizationalUnit (ou) for the configuration and policy DNs.

Table 51 summarizes LDAP support with NetPoint.

Table 51 LDAP Support: COREid Server, Access Manager, Access Server

Operating System	Directory Server
Windows Server 2003 Enterprise Edition	Microsoft ADAM (LDAP Only)
Microsoft Windows 2000	Microsoft Active Directory Sun One 5.2
Solaris 8 and 9	Sun One 5.2

When you install the NetPoint COREid Server on a Windows Server 2003 system, you may update the schema automatically. On a Windows 2000 Server, the schema update must be performed manually using the ldifde command. For more information, see "The NetPoint Schema Extension for ADAM" on page 411.

Installing NetPoint with ADAM

Several tasks are included in the installation procedures, as introduced below.

Task overview: Installing NetPoint with ADAM

1. Prepare your environment, as described in "Preparing to Install NetPoint" on page 39.
2. Prepare ADAM, as described in "Preparing ADAM for NetPoint" on page 418.

   Note: NetPoint requires a node with the objectclass attribute value of organizationalUnit (ou) for the configuration and policy DNs.

3. Install and setup the NetPoint COREid System, as described in "Installing and Setting the COREid System with ADAM" on page 420.
4. Install and setup the NetPoint Access System, if this is part of your environment, as described in "Installing the Access System with ADAM" on page 423.
5. Complete any of the following activities after successful NetPoint installation and setup:
   - Add ADAM users to NetPoint, as described in the *NetPoint 7.0 Administration Guide Volume 1*.
   - Replicate an ADAM instance, as described in your Microsoft documentation.

- Configure failover and load balancing, for the ADAM master and replicas, as described in the *NetPoint 7.0 Deployment Guide.*

Preparing ADAM for NetPoint

The steps below outline how to prepare your ADAM instance and ADP so that NetPoint can manage authentication and authorization. You will install a unique ADAM instance, create an ADP and a top DN for user data, and create users in ADAM. Remember the following important points:

ADPs—You must create the application directory partition within ADAM. NetPoint does *not* create the ADP.

Administrators—At least one account should be designated as the ADAM instance administrator. An ADAM instance administrator should also be designated as a NetPoint Administrator during COREid System setup. The NetPoint Administrator must be a bindable user in ADAM with administrative privileges, *not* a Windows Security Principal.

Configuration and Policy DNs—NetPoint requires a node with the objectclass attribute value of organizationalUnit (ou) for the configuration and policy DNs.

ADSI—NetPoint does *not* support ADSI with ADAM. You will need to use native NetPoint directory server failover and connection management toolkits with ADAM.

Binding through Proxy Objects—NetPoint does *not* support binding through an ADAM proxy object.

Important: Failure to complete the following steps may result in an unsuccessful installation with NetPoint. For complete details about installing ADAM, setting up the instance, and other tasks, as well as details about tools such as ADAM ADSI Edit and Ldp.exe, see the Microsoft documentation that accompanies your ADAM download.

To install ADAM for NetPoint

1. Familiarize yourself with ADAM concepts, practices, and tools, as described in the Microsoft documentation that accompanies your ADAM download.
2. Install a unique ADAM instance on a machine with Windows Server 2003 by running ADAMSetup.exe from the ADAM installation directory.

   The installation program will prompt you with the following screens:

   a) A unique instance

   b) A valid Instance name (for example, NetPoint)

   c) Port number where you want this instance to run.

d) Creation of application directory partition. (Yes/No).

- Yes to create a new partition For example, o=company, c=us, (Default)
- No will refer it to an already existing partition.

e) Directory to install ADAM.

f) Service Account selection (Select an account you would like to use for further processing).

- Network Service Account (Default)
- Custom Account (Make sure this account is active)

g) Assign Permissions to the selected account

h) Import user LDIF file (for example, MS_User.ldf)

3. Be sure to:

a) Specify an open LDAP port number to extend the ADAM schema for NetPoint, and an SSL-enabled port for password changes, authentication, and authorization with NetPoint.

b) Create an Application Directory Partition (naming context) to contain user data and NetPoint configuration and policy data by specifying any distinguished name that does not already exist within the instance--or to contain configuration and/or policy data while storing user data on another directory server type.

4. Start the ADAM instance.

For example:

Start > Programs > ADAM > ADAM ADSI EDIT

5. Right-click on ADAM ADSI EDIT then select Connect to from the menu.

A user screen appears with the following options:

a) **Connection Name**—For example, NetPoint

b) **Host Name**—Local Host

c) **Port**—Port number of the instance you have created

d) **DN**—The bind DN

e) **Credentials**

Note: The ms-bindable-object should be added to ADAM. For more information, see “Windows Users and Security Principals” on page 413.

---

6. Create and enable a bindable ADAM user account *and* use ADAM ADSI Edit to add the user you want to designate as the NetPoint Administrator to the *member* attribute of the following:

   `CN=Administrators,CN=Roles,CN=Configuration,CN={your GUID}`

7. Reset the user password.
8. Activate the user.
9. Manage directory partitions in the ADAM instance.
10. Manage ADAM configuration sets.
11. Ensure that your ADAM installation is operating properly before you continue.

Installing and Setting the COREid System with ADAM

Procedures in this discussion presume that you have completed all steps in "Preparing ADAM for NetPoint" on page 418. Following are several important items to review before you begin:

Schema Update—The ADAM schema update for NetPoint must be completed using an open port. For more information, see "The NetPoint Schema Extension for ADAM" on page 411.

The schema update must be completed with a Windows security principal credential. However, the root (bind) DN you specify during COREid System setup must be a user with an explicit physical location within ADAM. For more information, see "Windows Users and Security Principals" on page 413.

COREid System Setup—During COREid System setup, an SSL-enabled connection should be specified for password changes. For more information, see "Authentication, Authorization, and Password Changes" on page 415.

Administrators—The NetPoint Administrator you designate during COREid System setup must be an ADAM user with administrative privileges, *not* a Windows Security Principal.

The procedures below provide specific information for NetPoint and ADAM.

- "To install the COREid Server and update the ADAM schema" on page 420
- "To install WebPass and set up the COREid System" on page 423

To install the COREid Server and update the ADAM schema

1. Start the installation by selecting the COREid Server installation package that you downloaded.

   The *NetPoint 7.0 Installation Guide* can provide additional information.

2. Supply your installation directory, transport security mode, and COREid Server configuration details for NetPoint.
3. Select Yes to use SSL between the COREid Server and ADAM (required for password changes). Later you may specify an open port to extend the ADAM schema for NetPoint.
4. Supply the following details for ADAM:

   a) **Directory Server Type**—Select Active Directory Application Mode from the Directory Server drop-down list to specify ADAM.

   b) **Schema Update**—Respond as follows when asked if you want to automatically configure your directory server with the Oblix schema:

      - Select Yes if you are installing the *first* COREid Server on Windows Server 2003 *and* you want to automatically update the schema, continue with item step 5.
      - Select No to manually update the schema or when this is *not* the first COREid Server:

        If you choose No, *or* if you are installing the first COREid Server on a Windows 2000 Server, instructions to manually update the schema will appear. You may continue the installation and update the schema as described in step 7.

   c) **Directory Server Details**—Supply the ADAM details below for the automatic schema update on Windows Server 2003.

      - **Host Name**—Specify the name of the machine on which ADAM resides.
      - **Port Number**—Specify the number of the *open* port on which ADAM is listening to extend the ADAM schema for NetPoint.
      - **Windows User Name**—Specify a Windows security principal name to update the ADAM schema; this will *not* be used as a bind DN.
      - **Password**—Specify the password of the Windows security principal.
      - **Windows Domain Name**—Specify the name of the Windows domain where ADAM is installed.
5. Finish the installation and start the COREid Server, as described in the "Installing the COREid Server" on page 99.

Note: You complete step 6 and step 7 *only* if you need to manually update the ADAM schema for NetPoint. Otherwise, skip to "To install WebPass and set up the COREid System" on page 423.

---

6. **Manual Schema Update Preparation**—Modify the files below to replace <guid> with {*your GUID*} before you run a manual schema update using step 7:

   - ADAM_oblix_schema_add.ldif
   - ADAM_oblix_user_schema_add.ldif
   - ADAMAuxSchema_add.ldif

7. **Manual Schema Updates**—Update the schema manually as a domain user if needed, using the appropriate file and ldifde command, then restart the COREid Server:

   For example:

   COREid_install_dir\identity\oblix\data.ldap\common\
   ADAM_oblix_schema_add.ldif
   ADAM_oblix_user_schema_add.ldif

   ldifde -k -b <cn=*administrator,o=company,c=us password*>
   -c“<GUID>”<*ADAM_instance_ID*> -i -f ADAM_oblix_schema_add.ldif -s
   <*ADAM_server_name*> -t <*port*>

   ldifde -k -b <cn=*administrator,o=company,c=us password*>
   -c“<GUID>”<*ADAM_instance_ID*> -i -f
   ADAM_oblix_user_schema_add.ldif -s <*ADAM_server_name*> -t <*port*>

   Note: The Windows security principal name and domain in the example above are samples only. Your environment will differ.

   After executing the command above, if you *don't* plan to use dynamic auxiliary classes:

   - Use the ldifde command to import the NetPoint schema file ADAMAuxSchema.ldif for statically-linked auxiliary classes from the *COREid_install_dir*\identity\oblix\data.ldap\common directory.
   - Ensure that the object classes “oblixorgperson” and “oblixgroup” are explicitly attached as auxiliary classes to the Person and Group object classes, respectively.

   Note: Be sure to restart the COREid Server after updating the schema manually.

The steps below summarize the information you need to supply when you install the WebPass and set up the COREid System with ADAM.

To install WebPass and set up the COREid System

1. Install the WebPass your downloaded, as described in "Installing WebPass" on page 121.
2. Start the COREid System setup, as described in the "Setting Up the COREid System" on page 133, then specify the following details for ADAM:
   a) **Directory Server Type**—Select Microsoft Active Directory Application Mode when you specify a directory server type, *and* select Dynamic Auxiliary Object Class if appropriate for your environment.
   b) **Location of Directory Server**—Specify the following for ADAM:
      - **Port Number**—Specify the port to be used during runtime (SSL is required for password changes).
      - **Root DN**—The name of a *bindable* user in ADAM with administrator privileges as the bind DN; do *not* specify a Windows security principal.
      - **Root Password**—Password for the *bindable* user in ADAM
      - **Directory Server Security Mode**—Specify SSL for password changes.
3. Finish setting up the COREid System, as usual.
4. Continue with any of the following activities when COREid System setup is finished:
   - Install the Access System with ADAM, if this is included in your environment, as described in "Installing the Access System with ADAM" on page 423.
   - Add ADAM users to NetPoint, as described in the *NetPoint 7.0 Administration Guide Volume 1*.
   - Replicate an ADAM instance, as described in your Microsoft documentation.
   - Configure failover and load balancing, for the ADAM master and replicas, as described in the *NetPoint 7.0 Deployment Guide.*

Installing the Access System with ADAM

The NetPoint Access System, which is optional, includes the Access Manager, Access Server, and WebGate. The steps below provide specific details to install and setup the optional Access System with ADAM.

For details, see the procedures below:

- "To install the Access Manager with ADAM" on page 424
- "To install the Access Server" on page 425

- "To set up the Access Manager with ADAM" on page 424
- "To install the WebGate" on page 426

With ADAM, policy data may be stored with user and Oblix (configuration) data. Alternatively, NetPoint supports separate ADAM instances for configuration, user and policy data.

To install the Access Manager with ADAM

1. Locate and launch the Access Manager installation and specify your installation directory, as described in "Installing the Access Manager" on page 159.
2. Select Microsoft Active Directory Application Mode when asked for the directory server type.
3. Select Yes if dynamically-linked auxiliary object classes are enabled in your environment, otherwise select No.
4. Update the schema automatically during the installation, or manually update the schema after installation.
5. Specify the directory server security mode—SSL-enabled is required for password change with ADAM.
6. Specify a transport security mode for the Access System, configure your Web server, and complete the Access Manager installation, as described in the "Installing the Access Manager" on page 159.
7. Continue with the next procedure to set up the Access Manager.

To set up the Access Manager with ADAM

1. Start the Access Manager setup process, as described in "Installing the Access Manager" on page 159, and specify the following details for ADAM:
   a) **Directory Server Type**—Select Microsoft Active Directory Application Mode when you specify a directory server type, and select Dynamic Auxiliary Object Class if this is appropriate for your environment.
   b) **Directory Server Details**—Specify the following for ADAM:
      - **Port Number**—Specify the port to be used during runtime (SSL is required for password changes).
      - **Root (bind) DN**—Specify the Root DN you provided when setting up the COREid Server; do *not* use a Windows security principal.
      - **Password**—Specify the password of the bind DN user.
      - **Directory Server Security Mode**—Specify SSL for password changes.

2. Specify the searchbase, configuration DN, and policy base for ADAM, see "The ADAM Schema" on page 410 for details.
3. Complete the Access Manager setup process, as described in "Setting Up the Access Manager" on page 175.

Note: A warning may appear at the end of this setup instructing you to create the OblixAnonymous user before enabling NetPoint policies.

---

4. Ensure that the OblixAnonymous user has been created within ADAM at the top of the searchbase you specified during Access Manager setup.
5. Continue with the next procedure to install the Access Server.

To install the Access Server

1. Create an Access Server instance in the Access System Console, as described in "Creating an Access Server Instance" on page 191.
2. Locate and launch the Access Server installation package and specify your installation directory, as described in "Installing the Access Server" on page 194.
3. Select the transport security mode for the Access Server.
4. Specify ADAM details when asked.
   - **SSL**—SSL is required for password changes.
   - **Port Number**—The directory server port to be used during runtime.
   - **Bind (root) DN**—The Root DN you provided when setting up the COREid Server and Access Manager; do *not* use a Windows security principal.
   - **Password**—The password for the bind DN.
   - **Directory Server Type**—Active Directory Application Mode.
5. Select Yes if dynamically-linked auxiliary classes are enabled in your environment, otherwise select No.
6. Provide the path to the directory server's certificate file.
7. Specify the Access Server ID and the NetPoint configuration DN and policybase, which may be unique within the ADP.

   For example:

   Access Server ID: *Access_Server_70_1*
   Configuration DN—ou=config,o=*company,*c=us
   Policybase—ou=policy,o=*company*,c=us

Note: The example above presumes you are storing all data within a single ADAM instance and ADP.

---

8. Finish Access Server installation, as described in “Finishing the Access Server Installation” on page 197.
9. Continue with the next procedure to install the WebGate.

To install the WebGate

1. Create a WebGate instance in the Access System Console, as described in “Creating a WebGate Instance” on page 204.
2. Associate the WebGate with the Access Server, as described in “Associating a WebGate and Access Server” on page 207.
3. Install the WebGate, as described in “Installing the WebGate” on page 208.
4. Complete any of the following activities when the Access System installation and setup is finished:
   - Add ADAM users to NetPoint, as described in the *NetPoint 7.0 Administration Guide Volume 1*.
   - Replicate an ADAM instance, as described in your Microsoft documentation.
   - Configure failover and load balancing, for the ADAM master and replicas, as described in the *NetPoint 7.0 Deployment Guide.*

NetPoint Silent Mode Installation Parameters

Several parameter changes have been made in the NetPoint silent mode installer to support ADAM as a stand-alone directory server. For details, see:

- “COREid Server Silent Mode Installer for ADAM” on page 426
- “Access Manager Silent Mode Installer for ADAM” on page 428
- “Access Server Silent Model Installer for ADAM” on page 428

Note: The dynamic-auxiliary flag can be configured for ADAM in NetPoint as it is for Active Directory on Windows 2003.

COREid Server Silent Mode Installer for ADAM

The following changes have been made for ADAM in the COREid Server silent installer:

- **Windows User Name and Windows Domain**—Specify a Windows security principal name, Windows domain name, and password to update the ADAM schema; this will *not* be used as a bind DN.
- **Schema Update, Automatic**—To specify an automatic schema update when installing the first COREid Server on Windows Server 2003 use:

  -W AutoUpdateInput.AutoUpdateInputChoice=“Yes”

- **Schema Update, Manual**—To specify a manual schema update when installing the first COREid Server on Windows Server 2003 use:

  -W AutoUpdateInput.AutoUpdateInputChoice=“No”

  (Replaced with parameter: -W updateDSInfo.updateDSInfoChoice=“No”)

  For example:

-W AutoUpdateInput.AutoUpdateInputChoice—Determines whether to automatically update the schema. "Yes" indicates that you want to perform an automatic schema update. "No" indicates that you want to manually update the schema.	"Yes", "No"

- **Directory Server Type for ADAM**—To specify ADAM as the directory server type use:

  -W dsTypeInput.dsType=“9”

  For example:

-W dsTypeInput.dsType—Use this parameter if NetPoint is automatically updating the Oblix and User schemas in conjunction with –W AutoUpdateInput.AutoUpdateInputChoice=Yes. User directory server Types are: 2 - Sun 5.x 3 - NDS 5 - Active Directory 7 - Active Directory (Windows Server 2003) 9 - Active Directory Application Mode	"2", "3", "5", “7”, “9”
-W updateDSInfo.updateDSInfoChoice—-Used only if AutoUpdateInput.AutoUpdateInputChoice="Yes" "YesOneDS" performs an automatic update. Oblix and User directory server are the same. "YesTwoDS" performs an automatic update. Oblix and User directory servers are separate. "No" has been *removed*.	"YesOneDS", "YesTwoDS"

- **Windows Domain Name for ADAM**—To specify a Windows domain name for ADAM use:

  -W dsInfoInput.domainName="*domainname*.com"

  This is new and does not alter or replace an existing silent installer parameter.

  For example:

-W dsInfoInput.domainName—Use this parameter to specify the Windows Domain Name for ADAM when -W dsTypeInput.dsType=9 (ADAM). The domainName in which the ADAM machine resides. If an incorrect domain name is given, the authentication to the directory will fail.	"*domainname* .com"

Access Manager Silent Mode Installer for ADAM

To specify ADAM as the directory server type during Access Manager installation use the following:

-W dsTypeInput.dsType="9"

For example:

-W dsTypeInput.dsType— Specify the directory server type where policy data is stored. Later select Dynamic Auxiliary Object Class if this is appropriate for your environment, For ADAM, the option "-W updateDSInfo.updateDSInfoChoice" is not applicable. Otherwise, use "-W updateDSInfo.updateDSInfoChoice = "Yes"" to specify the Policy directory server type: 2 - Sun 5.x 3 - NDS 5 - Active Directory 7 - Active Directory (Windows Server 2003) 9 - Active Directory Application Mode	"2", "3","5", "7", "9"

Access Server Silent Model Installer for ADAM

To specify ADAM as the directory server type during Access Server installation use:

-W oblixDSInfoBean.dsType="MSADAM"

For example:

-W oblixDSInfoBean.dsType—The Oblix directory server type: NS5 - Sun 5.x NOVELL - NDS MSAD - Microsoft Active Directory MSAD_ADSI - Microsoft Active Directory with ADSI MSADAM - Microsoft Active Directory Application Mode	"NS5", "NOVELL", "MSAD", "MSAD_ADSI" “MSADAM”

Troubleshooting

The following discussions provide several considerations for ADAM.

- “Cannot find the Config DN or Searchbase” on page 429
- “Schema Updates” on page 429
- “Object Classes” on page 429
- “Password Changes” on page 430

Cannot find the Config DN or Searchbase

Please make sure the configuration DN and/or searchbase exist.

This error message may also indicate that you are not using ous for the configuration and policy DNs.

Schema Updates

Currently ldifde, which is used to extend the ADAM schema, does *not* support binding to an SSL port. If you are having trouble updating the schema, ensure that you specified the *open* ADAM port during COREid Server installation. You may still install certificates and specify SSL during COREid Server installation.

Object Classes

ADAM describes the user object class differently than Active Directory. samaccountname, which is required with Active Directory, does not exist in ADAM. grouptype is still required with ADAM. NetPoint configures a grouptype attribute when you automatically configure attributes during setup.

Keep the following in mind with manual schema updates when you *don’t* plan to use dynamic auxiliary classes:

- Update the schema manually using *COREid_install_dir*\identity\oblix\data.ldap\common\ADAM_oblix_schema

_add.ldif, as described in “Installing and Setting the COREid System with ADAM” on page 420.

- Use the ldifde command to import the NetPoint schema file ADAMAuxSchema.ldif from the *COREid_install_dir*\identity\oblix\data.ldap\common directory.
- Ensure that the object classes “oblixorgperson” and “oblixgroup” are explicitly attached as auxiliary classes to the Person and Group object classes, respectively.

Password Changes

Password changes require SSL. If you have a problem changing a password, the directory server may have a native password policy that is not being honored.

When creating a user, ensure the user has a password. If you activate a user and the operation fails, the user may not have a password.

Users must be enabled within ADAM. If you search for a user in the NetPoint User Manager, and the user does *not* appear as the result of the search, check the msDS-UserAccountDisabled= user attribute in the object class to see if it is disabled or enabled.

Directory Server Security

The ADAM schema must be updated through an open port. For details, see “Schema Updates” on page 429.

Password changes can be made only through an SSL-enabled port. For details, see “Password Changes” on page 430.

C Adding Directory Certificates after NetPoint Installation

This appendix provides the information you need to change your directory server communication mode to SSL-enabled or to add certificates to connect to multiple directory servers without uninstalling and re-installing NetPoint. Topics include:

About Directory Certificates

During installation of the NetPoint COREid Server, Access Manager, and Access Server, you specify a directory server communication mode, either open or SSL-enabled, as discussed in "Securing Directory Server Communications" on page 56. The certificate must be stored on the directory server before NetPoint installation.

At times, you may want to enable SSL after NetPoint installation. For example, you may want change from an open communication mode to an SSL-enabled mode or you may want add directory certificates to connect to additional directory servers.

In such cases, you could either uninstall and re-install NetPoint *or* use the steps below to create the cert8.db file needed by the COREid Server, Access Manager, and Access Server.

Note: NetPoint 7.0 works with both the cert7.db (upgraded environments) and cert8.db (new installations) certificate store.

With NetPoint 7.0, the default certificate store format and name has changed from cert7.db to cert8.db. When you upgrade to NetPoint 7.0, you continue to use the old certificate store (cert7.db). When you run the configureAAAServer, setup_ois, or setup_accessmanager utilities, the certificate store format and name is automatically modified to cert8.db.

Task overview: Enabling directory SSL after NetPoint installation

1. Complete all “Prerequisites” on page 432.
2. Create a new certificate store, as described in “Creating a New Certificate Store” on page 433.
3. Populate the new store, as described in “Adding Certificates” on page 433.
4. Change the directory profile in NetPoint, as described in “Changing the Directory Server Configuration” on page 435.
5. Repeat the sequence above on the Access Manager and Access Server, as needed, or copy the store with the new certificates to the Access Manager and Access Server, as needed.
6. See the *NetPoint 7.0 Administration Guide Volume 1* for details about transport security changes for NetPoint and the directory server using the appropriate utility for your platform: start_setup_ois (Unix) or setup_ois (Windows).

Prerequisites

You need to have a copy of the Base 64 encoded root certificate from the certificate authority for all directory servers with whom the communication will be in SSL mode. This needs to be stored in the cert8.db store used by the COREid Server to establish the SSL connection.

Note: If you have a cert8.db file in *Component_install_dir*\identity\oblix\config, be sure to delete it before you start the procedures below.

With Active Directory, you need to enable SSL for all domain controllers and have a copy of the Microsoft CA Root Certificate available in Base 64 encoded format.

Creating a New Certificate Store

The following procedure walks you through creating a new cert8.db certificate store. You can complete this task on the COREid Server, Access Manager, and Access Server. Be sure to complete the prerequisites before you start.

Table 52 lists the options you supply the command you provide to create the data store.

Table 52 Options to Create the Data Store

Option	Description
-d *directory*	This option identifies the directory for the cert8.db store.
-N	This option creates a new certificate database.

To create the new certificate store

1. Obtain a copy of the Base 64 encoded CA Root Certificate from your CA and store it on the machine hosting the installed COREid Server.
2. Locate the certutil utility in *COREid_install_dir*\identity\oblix\tools\certutil.
3. In a command window, enter:

```
C:\COREid_install_dir\identity\oblix\tools\certutil>certutil -d
c:\COREid_install_dir\identity\oblix\config -N
```

   You will be prompted for the cert8.db store password, which must be entered to encrypt this key and any future keys. The password must be at least 8 characters in length and must contain at least one non-alphabetic character.

4. Enter the cert8.db store password, then re-enter the password.

   The cert8.db store is created on the COREid Server and ready to populate.

Adding Certificates

Once you have created the new cert8.db store, you need to add the CA Root Certificate. Table 53 lists the command options to complete this task.

Table 53 Options to Add Certificates to the Data Store

Options	Description
-d *directory*	The value is the full path to the cert8.db store.
-A	This option adds a certificate to the store.
-a	This option indicates an ASCII encoded certificate.

Table 53 Options to Add Certificates to the Data Store

Options	Description
-n	This option indicates the certificate nickname.
-t C,,	This option provides trust attributes, where C,, indicates the Trusted CA to Certs (only for SSL, and implies a valid CA).
-i CAROOT.cer	This option provides input, where CAROOT.cer is the name of your Base 64 encoded CA root certificate.
-L	This option requests a list of certificates in the data store directory.

To add certificates to the data store

1. At the command prompt, enter the following to add certificates to the data store:

```
C:\NetPoint\identity\oblix\tools\certutil>certutil -d
C:\NetPoint\identity\oblix\config -A -a -n CAROOT -t C,, -i CAROOT.cer
```

2. Verify that your certificate was added to the cert8.db store using the command below to list the content of the cert8.db store directory.

   For example:

```
C:\NetPoint\identity\oblix\tools\certutil>certutil -d
C:\NetPoint\identity\oblix\config -L
```

   Table 54 shows sample results from the list command, which confirms that the certificate was added to the database with the Nickname of CAROOT:

Table 54 Sample Results of the List Command

Certificate Name	Trust Attributes
CAROOT	C,,
Example.com Code Signing CA	,,C
Example.com Individual CA	,C,
Example.com Server CA	CG,,

Changing the Directory Server Configuration

After adding certificates you need to complete the process for the directory server configuration within the NetPoint System Console.

To change the directory profile

1. Navigate to the Configure Directory Options page: COREid Server System Console > System Configuration > Configure Directory Options.
2. Click Directory Server under Configure Profiles.
3. Select the appropriate Directory Server Security Mode*.

   Note: When you change fields marked with an asterisk, *, you must repeat product setup. For more information about re-running COREid System setup, see the *NetPoint 7.0 Administration Guide Volume 1*.

4. Restart the COREid Server to have directory server changes take affect.
5. Verify that the COREid Server is running in SSL / Cert Mode by checking the process start-up message.

   For example:

   Unix—A message is returned to the console saying the Process has started. The port number and communication mode are included in the message.

   Windows—Look in the Event Viewer under Applications for the port number and communication mode.

6. Create and populate Access Manager and Access Server stores, configure their directory profiles, then restart the Access Manager Web server and Access Server.

   Note: If directory server and CA details are the same for all NetPoint components that communicate with the directory, you can copy the COREid Server cert8.db store to the Access Manager and Access Server. Be sure to complete all steps to finish and verify the configuration.

For more information about changing transport security modes after installation, see the *NetPoint 7.0 Administration Guide Volume 1*.

D Changing Directory Server Hosts

The information here explains how to reconfigure NetPoint to recognize a new directory server host. Topics include:

About Changing Directory Server Hosts

After installing and setting up NetPoint, you may need to change the host machine for the directory server with which NetPoint communicates. If this occurs, you need to reconfigure NetPoint to recognize the new directory server host.

Task overview: Changing Directory Server hosts includes

1. "Minimizing Down Time" on page 438
2. "Preparing the New Directory Server Instance" on page 441
3. "Reconfiguring the Primary COREid Server" on page 443
4. "Reconfiguring the Access Manager" on page 444
5. "Reconfiguring the Access Server" on page 446

Minimizing Down Time

When you reconfigure NetPoint to communicate with a new directory server instance (one that has moved to a different host), there will be some down time. You can minimize the downtime by configuring *failover* between NetPoint Web components and NetPoint servers.

NetPoint uses failover to provide uninterrupted service by re-directing requests to another server when the original request destination fails. Failover is accomplished by configuring a primary and secondary server and identifying specific parameters for the failover process. NetPoint Web components first attempt to connect to a primary server. If the primary server is unavailable, a connection attempt is made to a secondary server:

- WebPass requests are re-directed to secondary COREid Servers
- WebGate requests are re-directed to secondary Access Servers

Task overview: Minimizing down time

1. "Configuring Failover between a COREid Server and WebPass" on page 438
2. "Configuring Failover between an Access Server and WebGate" on page 440

Completing the tasks above ensures that users will enjoy uninterrupted service when you reconfigure the primary COREid and Access Servers for the new directory server instance.

For additional information on failover, see the *NetPoint 7.0 Deployment Guide*.

Configuring Failover between a COREid Server and WebPass

Setting up a secondary COREid Server ensures that the WebPass fails-over to the secondary COREid Server if the primary COREid Server is stopped while you reconfigure this to communicate with the new directory server instance.

To configure failover between a COREid Server and WebPass

1. Confirm that you have a *second* COREid Server installed that meets the requirements below:
   - The second COREid Server must communicate with the existing directory server.
   - The second COREid Server must be associated with the existing WebPass as a *secondary* server.

Note: If your NetPoint installation does *not* include a second COREid Server that meets the requirements above, you need to install one that does. See "About Installing Multiple COREid Servers" on page 101.

2. Configure failover between the secondary COREid Server and WebPass:

   a) From the COREid System Console, select System Admin > System Configuration > Configure WebPass > *Name* > Modify.

      See the *NetPoint 7.0 Administration Guide Volume 1* for more information about configuring a WebPass.

   b) Complete the information below, then save your changes:

      Failover Threshold—Enter the required number of live connections from the Web component to its *primary* NetPoint server.

      COREid Server Timeout Threshold—Enter a Timeout Threshold to specify how long (in seconds) the Web component waits for a non-responsive NetPoint server before it considers it unreachable and attempts to contact another.

      Sleep For (seconds)—Enter the interval in seconds. After this interval, the WebGate verifies whether the number of valid connections equals the maximum number of connections configured

3. Configure relevant directory profiles to use all COREid Servers:

   a) In the System Console, locate the list of LDAP Directory Server Profiles"

      COREid System Console > System Admin > System Configuration > Configure Directory Options

      The Configure Profiles page appears with Directory Server information as well as sections for Configure LDAP Directory Server Profiles and Configure RDBMS Profiles.

   b) Under the Configure LDAP Directory Server Profiles heading, select the name of the COREid Server profile:

      Configure LDAP Directory Server Profiles

      name

      The Modify Directory Server Profile page.

   c) In the Modify Directory Server Profile page, locate the Used by field and select All COREid Servers. For example:

   d) Save the change.

4. Proceed with "Configuring Failover between an Access Server and WebGate" on page 440.

Configuring Failover between an Access Server and WebGate

As with the COREid Server, setting up a secondary Access Server ensures that the WebGate fails-over to the secondary Access Server while the primary Access Server is stopped as you reconfigure this to communicate with the new directory server instance.

To configure failover between an Access Server and WebGate

1. Confirm that you have a *second* Access Server installed that meets the requirements below:
   - The second Access Server must communicates with the existing directory server containing NetPoint configuration and policy data.
   - The second Access Server must be associated with the existing WebGate as a *secondary* server.

   Note: If your NetPoint installation does *not* include a second Access Server that meets the requirements above, you need to install one. See "About Installing Multiple Access Servers" on page 189.

2. Configure failover between the secondary Access Server and WebGate, as described in the *NetPoint 7.0 Deployment Guide*:

   a) From the Access System Console, select Access System Configuration > AccessGate Configuration > All > Go > *Name*

      See the *NetPoint 7.0 Administration Guide Volume 2* for more information about configuring a WebGate.

      The NetPoint AccessGate page appears.

   b) Complete the information below, then save your changes:

      Failover Threshold—Enter the required number of live connections from the Web component to its *primary* NetPoint server.

      Access Server Timeout Threshold—Enter a value to specify how long (in seconds) the Web component waits for a non-responsive NetPoint server before it considers it unreachable and attempts to contact another.

      Sleep For (seconds)—Enter the interval in seconds. After this interval, the WebGate verifies whether the number of valid connections equals the maximum number of connections configured

3. Configure the relevant directory server profiles to use all Access Servers:

   a) In the System Console, locate the list of LDAP Directory Server Profiles:

      Access System Console > System Configuration > View Server Settings

      The View Server Settings page appears with Directory Server information as well as sections for Configure LDAP Directory Server Profiles and Configure RDBMS Profiles.

   b) Under the Configure LDAP Directory Server Profiles heading, select the name of the Access Server profile:

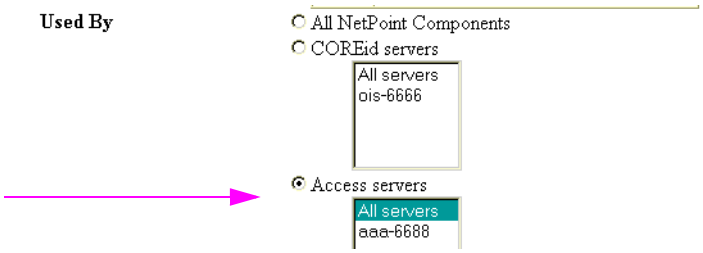
      Configure LDAP Directory Server Profiles

      name

      The Modify Directory Server Profile page.

   c) In the Modify Directory Server Profile page, locate the Used by field and select all Access Servers.

      For example:



4. Save the change.
5. Proceed with “Preparing the New Directory Server Instance” on page 441.

Preparing the New Directory Server Instance

You must ensure that the new directory server instance is an exact replica of the directory server instance with which NetPoint communicates. This means that the schema, user data, NetPoint configuration data, and policy data must match. In addition:

- If any data is stored separately in the existing directory server instance, the new directory server instance must match this configuration.
- If the existing directory server uses SSL, the new directory server must have a certificate issued by the same Root CA as the one issued for the existing directory server.

As you prepare the new directory server instance, pay close attention to the following:

- If policy data is stored in a separate directory server than configuration data (o=oblix), you must also export (then import) an LDIF for policy data.
- If you are using NetPoint 6.5 or later (7.x), you must remove the entries under obcontainerId=DBAgents,<*Configuration DN*>… that are associated with the Access Manager and Access Servers.

Note: When removing entries for DB agents, do *not* delete the container (obcontainerId=DBAgents).

To prepare the new directory server instance

1. Export the *original* NetPoint configuration tree (o=oblix) from the existing directory server instance to an LDIF file using the ldapsearch command below; repeat for policy data if this is stored separately.

   For example:

```
ldapsearch -h DS_hostname -p DS_port_number -b Configuration_DN (o=oblix...) -D
bind_dn -w password -s sub  (objectClass=*) > Oblix_Data_original.ldif
```

   where *DS_hostname* is the name of the machine hosting the new directory server instance (from which you export data); *DS_port_number* is the port on which the directory server is listening; *bind_dn* is the DN for NetPoint configuration data; *password* is the password for the bind DN; and *Oblix_Data_original.ldif* is the name of your configuration data ldif file.

2. Remove the entries for DB Agents *without* deleting the container (obcontainerId=DBAgents).

   For example:

```
obcontainerId=DBAgents,<Configuration DN>…
```

3. Import the *modified* LDIF you created to the new directory server instance using the ldapmodify command below.

   For example:

```
ldapmodify -h DS_hostname -p DS_port_number -D bind_dn -w password -a -f
Oblix_Data_modified.ldif
```

   where *DS_hostname* is the name of the machine hosting the new directory server instance (to which you would import the data); *DS_port_number* is the port on which the directory server is listening; *bind_dn* is the DN for NetPoint configuration data; *password* is the password for the bind DN; and *Oblix_Data_modified.ldif* is the name of your configuration data ldif file.

4. Proceed to “Reconfiguring the Primary COREid Server” on page 443 to add directory server profiles for the new directory server instance to the COREid System Console.

Reconfiguring the Primary COREid Server

The procedure below describes how to reconfigure the primary COREid Server, the one that communicates with the existing directory server instance, so that it communicates with the new directory server instance.

To configure the COREid Server to communicate with a new directory server instance

1. From the COREid System Console, select System Admin > System Configuration > Configure Directory Options > Directory Server
2. On the Directory Server Configuration page, change the following information to reflect the new directory server instance, then save your changes:

   Machine*—*new_hostname.domain*.com

   Port Number*—*new_host_port*

   When you change fields marked with an asterisk (*), you must manually re-run the COREid System setup.
3. Shut down all COREid Servers except the secondary server, if more than one are running.
4. On the only running COREid Server host, open the setup.xml file:

   COREid_install_dir/identity/oblix/config/setup.xml
5. Remove the status parameter (or change the status parameter value from “done” to “incomplete”), as shown below, then save the file:

   For example:

```
<NameValPair ParamName="status" Value="incomplete"></NameValPair>
```

6. Restart this COREid Server.
7. From your Web browser, launch the COREid System Console.

   A Setup page appears, like the one for the initial COREid System setup.
8. Click the Setup button and proceed through the setup process:

   a) Specify *new* directory server instance information, as indicated below:

      Host—The *new* user data directory server DNS hostname

      Port Number—The *new* user data directory server port number

      Note: If user data is stored separately from configuration data, a similar page appears where you can enter information for the configuration data directory. However, that sequence is *not* repeated here.

   b) Complete setup as described in the *NetPoint 7.0 Installation Guide*.
9. Restart the COREid Servers, which should pick up the new information.

10. In the System Console, verify that a new database profile was created:

    a) Navigate to the Configure Profiles page:

    COREid System Console > System Admin > System Configuration > Configure Directory Options

    b) In the Configure Profiles page, select the name of the relevant profile under the heading Configure LDAP Directory Server Profiles.

    c) In the Modify Directory Server Profile page, locate the name of the *new* Database Instance and confirm the *new* machine and port number.

    Note: You can proceed with creating any additional DB profiles that you need. See the *NetPoint 7.0 Administration Guide Volume 1* for details.

11. Complete "Reconfiguring the Access Manager" on page 444.

Reconfiguring the Access Manager

You need to reconfigure the Access Manager to use the new directory server instance.

To reconfigure the Access Manager for the new directory server instance

1. View server settings in the Access System Console, as follows:

   Access System Console > Access System Configuration > View Server Settings > Directory Server

2. On the Directory Server Configuration page, change the following information to reflect the new directory server instance, then save your changes:

   Machine*—*new_hostname.domain*.com

   Port Number*—*new_host_port*

   When you change fields marked with an asterisk (*), you must manually re-run the Access Manager setup.

3. Shut down all but one Access Manager Web server if there is more than one running.

4. On the only remaining running Access Manager host and open the setup.lst file:

   AccessManager_install\dir\oblix\config\setup.lst

5. Remove the status parameter (or change the status parameter value from "done" to "incomplete"), and save the file as shown below:

   For example:

```
<NameValPair ParamName="status" Value="incomplete"></NameValPair>
```

6. Restart the Access Manager Web server.
7. From your Web browser, launch the Access System Console.

   You will see a Setup page similar to the one that appears during the initial Access System setup. You need to specify details about the directory servers where user data, configuration data, and policy data are stored and asked to provide information about the directory server for each type of data.
8. Initiate setup again and, when asked, specify the following:
   - If user data and configuration data are stored together, you are asked where policy data should be stored.
   - If the data is stored separately, you are asked to specify details for configuration data.

   For more information about this, see the *NetPoint 7.0 Installation Guide*.
9. When asked, specify the *new* directory server instance information, as shown below:

   a) Specify *new* directory server instance information, as indicated below:

      Host—The *new* directory server DNS hostname

      Port Number—The *new* directory server port number

      Note: Depending on how your data is stored, you may see an additional screen for policy data. However, that sequence is *not* repeated here.

   b) Complete setup as described in the *NetPoint 7.0 Installation Guide*.
10. After completing setup, restart the other Access Manager Web servers.

    The other Access Managers should pick up the new information.
11. Confirm the new Database Instance in the Access System Console, as follows:

    a) View server settings in the Access System Console, as follows:

       Access System Console > Access System Configuration > View Server Settings

    b) In the View Server Settings page, select the name of the relevant profile under the heading Configure LDAP Directory Server Profiles.

    c) In the Modify Directory Server Profile page, locate the name of the *new* Database Instance and confirm the *new* machine and port number.

    Note: You can proceed with creating any additional DB profiles that you need. See the *NetPoint 7.0 Administration Guide Volume 1* for details.
12. Rerun Access Server setup, as described in "Reconfiguring the Access Server" on page 446.

Reconfiguring the Access Server

After manually rerunning setup for the Access Manager, you need to reconfigure the Access Server as indicated below. For additional information on using the configureAAAServer tool, see *Volume 2*.

To reconfigure the Access Server

1. Locate the configureAAAServer tool.

   For example:

   AccessServer_install_dir/access/oblix/tools/configureAAAServer

2. Use the command below with the configureAAAServer tool to set up the Access Server.

   For example:

   configureAAAServer install -i *AccessServer_install_dir/util/access*

3. Specify new information for the host on which the new directory server instance resides.

4. Restart your Access Server.

5. Confirm the new Database Instance in the Access System Console, as follows:

   a) View server settings in the Access System Console, as follows:

      Access System Console > Access System Configuration > View Server Settings

   b) In the View Server Settings page, select the name of the relevant profile under the heading Configure LDAP Directory Server Profiles.

   c) In the Modify Directory Server Profile page, locate the name of the *new* Database Instance and confirm the *new* machine and port number.

   You may see one more Database Profile created, in addition to the default, when the policy tree and the configuration tree are on the same directory server yet are using two different suffixes.

Note: You can proceed with creating any additional DB profiles that you need. See the *NetPoint 7.0 Administration Guide Volume 1* for details.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

X